IMPROVING THE CAPABILITIES OF COGNITIVE RADAR AND EW SYSTEMS

White paper | Version 01.00 | Tim Fountain, Leander Humbert

ROHDE&SCHWARZ
Make ideas real

CONTENTS

LIST OF FIGURES

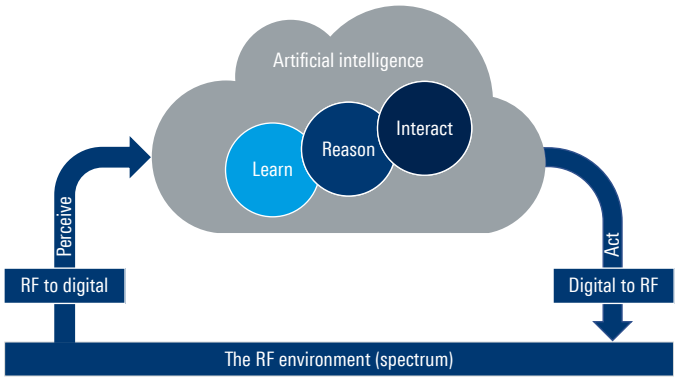
1 ABSTRACT

In this white paper we will review the challenges that mode-agile (WARM) radar and EW threat emitters pose to traditional static threat library implementations in radar and EW systems, and consider the architecture of cognitive artificial intelligence (AI) and machine learning (ML) systems that can be used to deliver effective RF countermeasures. We will discuss how a wideband RF record, simulation and playback system can be used to train the AI/ML engines, and evaluate the responses and effectiveness of those countermeasures on real hardware.

2 INTRODUCTION

A cognitive RF system, as shown in Figure 1, has the ability to perceive its environment, in this case the RF spectrum and associated energy through the conversion of that spectrum into a stream of RF data. Through reasoning and understanding of the context of the data stream, which may be tainted with uncertainty (such as noise or other emitters), the system makes autonomous judgements and determines a course of action without recourse to any other systems or with human intervention. The course of action is typically another stream of RF I/Q data, that is converted back into an RF spectrum. The end goal of the system is to deny the use of the RF spectrum by an adversary (electronic attack, EA), protect a platform, for instance by employing anti-jam techniques to protect a communications link (electronic protect, EP) and/or delivery of supporting information to another system (electronic support, ES). A cognitive system uses a continuous feedback loop of situational perception, learning, reasoning, interaction and action. The system literally learns from its interactions with the RF environment and this is the basis of the term cognitive, from the Latin verb cognoscere, which means “getting to know, acquaintance, notion, knowledge”.

Figure 1: A cognitive radar/EW system

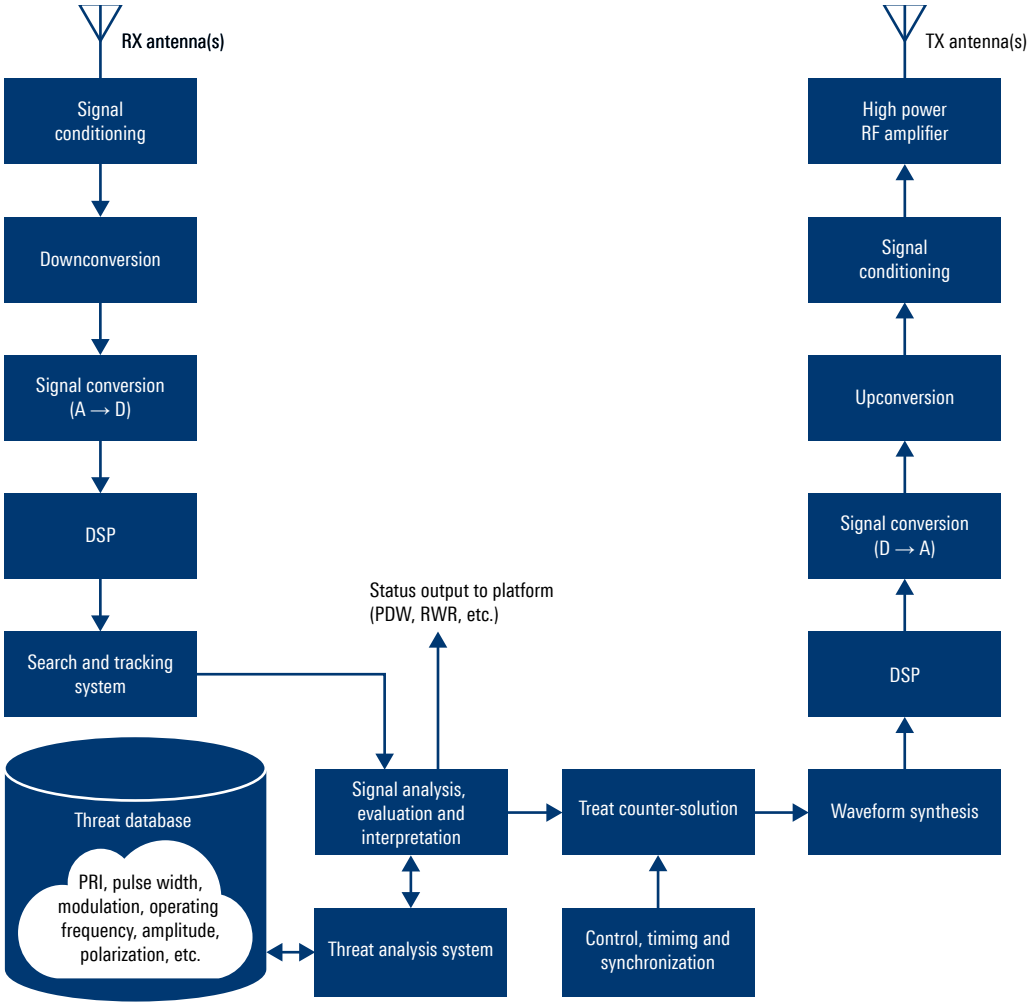


With today's emerging threats, traditional approaches to radar and EW systems that utilize static threat libraries, as shown in Figure 2, are vulnerable to “mode-agile” or wartime reserve modes (WARM) threats operating in nontraditional modes. In a static threat system, traditional threats such as an air surveillance radar or a surface-to-air missile (SAM) 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 these parameters against a database and classifies the emitters, which are then turned into pulse descriptor words (PDW) which are fed to other systems on the platform, potentially with a view to deploying countermeasures.

Wartime reserve modes (WARM) are characteristics and operating procedures of sensors, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. WARM are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use.

Mode-agile threat emitters are capable of deploying new operational modes that do not conform to the predefined parameters in the threat library. These new operational modes may include new operating frequencies, new modulation techniques, new pulse repetition intervals and/or new hopping schemes. Since the threat detector cannot match these new operational modes against the static database of known modes, the electronic protect, attack and support (EP, EA and ES) system has no method in the library to counter this threat. It is worth noting that it is extremely unlikely that many of the mode-agile threat modes will be seen "in the wild" outside of a true conflict.

Figure 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 and are used to develop a counter to the perceived threat in the spectrum. Unlike the static library approach of a traditional system, the cognitive system classifies the threat and develops a counter to the threat "on the fly". It is entirely possible that a mode-agile threat may also be able to detect that it has encountered a system that is utilizing cognitive AI/ML techniques and

may itself change its operating parameters, potentially on a continual basis. Thus, it is imperative that the AL/ML cognitive system is flexible and able to adapt quickly and continually to a changing threat or threats.

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

1. Significant computational resources are required at the tactical edge, i.e. where the threat is encountered. The computational resources may combine high performance field programmable gate arrays (FPGA), general purpose graphic processing units (GP-GPU) and multi-core, host based processors to implement the AI/ML algorithms. Since the compute elements are on-platform, they need to meet the harsh environmental conditions that are often encountered in the theater of operations. Modern modular standards such as Open VPX and SOSA are helpful in the implementation of these fielded systems.

2. The system needs to minimize the detect-to-counter time, sometimes referred to as RF in to RF out latency, in order to be effective. This is often a matter of platform survivability. This presents challenges in the design and implementation of the FPGA and GP-GPU code and, in addition, the modern GP-GPU architecture and most commercial-off-the-shelf (COTS) analog-to-digital converters (ADC) and digital-to-analog converters (DAC) are deeply pipelined, adding to the overall system latency design budget.

3. Mode-agile radar and EW threats may be operating in unexpected frequency bands, change frequency (hop) across wider bandwidths and/or utilize wideband modulation techniques. All of these threat modes require a wide bandwidth stare at a large swath of RF frequency spectrum. This is challenging to implement and has design trade-offs in terms of overall system dynamic range and noise floor, both of which affect standoff, detection and jamming range. These wider bandwidth requirements also complicate the task of data movement and processing within the system.

4. Unlike a traditional threat library approach, a wideband cognitive AI/ML system will use more electrical power, which drives size, weight, power and cost (SWaP-C) requirements. On smaller autonomous platforms such as an unmanned aerial system (UAS), these commodities are always in short supply. The ever-diminishing dimensions of semiconductor process nodes can help to mitigate some of these challenges.

5. Mode-agile emitters may also be expected to enter low(er) RF power or low probability of intercept (LPI) modes. This drives the requirement for higher resolution ADCs and DACs, which is typically orthogonal to wider bandwidths. You can optimize one of these parameters at the expense of the other!

6. Platforms need to be able to share information, which implies that there are reliable communications links between them. The platforms also need a common time reference, such as GPS, in order to provide spatial and temporal information which could be used in direction finding and geotagging of emitters of interest. Traditional GPS is vulnerable to jamming, spoofing and deception, and assured position, navigation and timing (A-PNT) needs to be part of the overall system-level solution.

3 ELEMENTS OF A COGNITIVE RADAR/EW SYSTEM

3.1 Overview of artificial intelligence and machine learning techniques

A cognitive radar/EW system uses artificial intelligence. AI is a computer science discipline that applies non-human intelligence to implement systems that can emulate human reasoning and problem-solving skills. The most commonly used AI techniques used in machine learning (ML) are artificial neural networks (ANN), deep learning (DL) or deep neural networks (DNN), fuzzy logic and genetic algorithms (GA). These techniques are briefly described below:

1. **Artificial neural networks**

   An ANN is a non-parametric computational tool that is trained to perform various computation tasks such as pattern recognition, classification/sorting and data clustering. At its core, the ANN uses a computational unit known as an artificial neuron, which replicates the biological neuron. Neurons are connected via synapses and are weighted and grouped to form a network. The network has an input layer, a processing layer and an output layer. ANNs may incorporate feedforward or feedback topologies. In a feedforward network, information flow is unidirectional. In a feedback network, loops permit information to reoccur and thus flow in both directions. An ANN may incorporate supervised or unsupervised learning. Multi-layer perception (MLP) is the simplest form of feedforward ANN training and utilizes non-parametric learning techniques that can be used for prediction and classification. Another form of feedforward ANN is called the time delay neural network (TDNN). Feedback ANNs include recurrent neural networks (RNN) and nonlinear autoregressive networks with exogenous inputs (NARX). The main difference is that MLP does not have the capability to process data with temporal dependencies whereas TDNN, RNN and NARX can process time-dependent signals.

2. **Deep neural networks**

   DNNs have improved feature expression and ability to fit complex mappings by utilizing multiple layers to progressively extract higher-level features from the raw data. Examples of DNN include deep belief networks (DBN), stacked auto encoder (SAE) and deep convolution neural networks (DCNN).

3. **Fuzzy logic**

   Fuzzy logic utilizes the concept of many-valued logic, in which the truth value of variables may be any real number between 0 and 1. It is employed to handle the concept of partial truth, where the truth value may range between completely true and completely false. This is in contrast to Boolean logic, where the truth values of variables may only be integer values of 0 or 1. Fuzzy logic algorithms attempt to replicate the human decision-making process, in which decisions are often made with imprecise and/or incomplete information. Fuzzy logic systems have no learning capability or memory and for this reason are often combined with other ML techniques to form hybrid systems. An example of a hybrid system is the neuro-fuzzy system, in which neural networks are combined with fuzzy logic. These systems are widely used in radar/EW and signal processing applications.

4. **Genetic algorithms**

   A genetic algorithm emulates the naturally occurring evolution process with "survival of the fittest" logic to derive an optimum solution. It utilizes an iterative process with probability weighting. The better weighted solutions are passed on and the poorer weighted solutions are discarded. The iterative process continues until it is determined that a satisfactory outcome has occurred. In contrast to random search techniques, GA keeps a pool of solutions, which reduces the probability of reaching a false suboptimal solution. As with fuzzy logic, GA is often combined with ANNs and DNNs to form a hybrid system. One potential drawback of a GA is that the algorithm can take a variable amount of time to determine a solution or may never arrive at a solution. Obviously, this is not an ideal situation where speed of response to a threat is paramount.

3.2 Cognitive radar/EW system

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

1. **RF acquisition**

   The RF acquisition block is responsible for the acquisition and conversion of the RF spectrum into a digital data stream. One or more antenna signals are routed to a signal conditioning system that is responsible for filtering (preselection), amplification and/or attenuation of the RF spectrum to maximize the signal's dynamic range, followed by RF downconversion (frequency translation). A set of analog-to-digital converters (ADC) then convert the RF signal into a stream of digital data that may require further digital processing with digital signal processing (DSP). Typical DSP functions include digital filtering, digital downconversion, resampling, demodulation and digital beamforming.

2. **Search and tracking system**

   The search and tracking system continually monitors one or more frequency bands to determine the angle of arrival (AoA), used to identify the location of the emitters.

3. **Core AI/ML system**

   The core AI/ML system consists of the AI-driven analysis engine that determines key parametric information about the signals, such as pulse repetition frequency (PRF), pulse width, signal power, polarization time of arrival (TOA) and AoA. The core AI/ML system will also receive other pertinent information from the platform, such as electro-optic sensors, navigation data and missile awareness system. This information is continually contributed to the threat library to deliver an evolving view of the electronic battlefield, and may be contributed to the electronic order of battle (EOB). The library may also contain a list of counters to previously identified signals of interest (SOI). The function of the signal analysis and inferencing AI block is to determine whether identified signals are friendly emissions or potential threats. It does this by comparing known friendly signals stored in the database. The AI support system is primarily used as a final decision arbiter for a proposed course of action and to communicate both the threat and the proposed action to the rest of the platform and operator. The AI-driven threat counter solution is a block that determines the key parameters of the signal in multiple domains such as time, frequency and amplitude. This could be a continuous jamming of the signal, a spoofing signal to confuse the threat, etc.

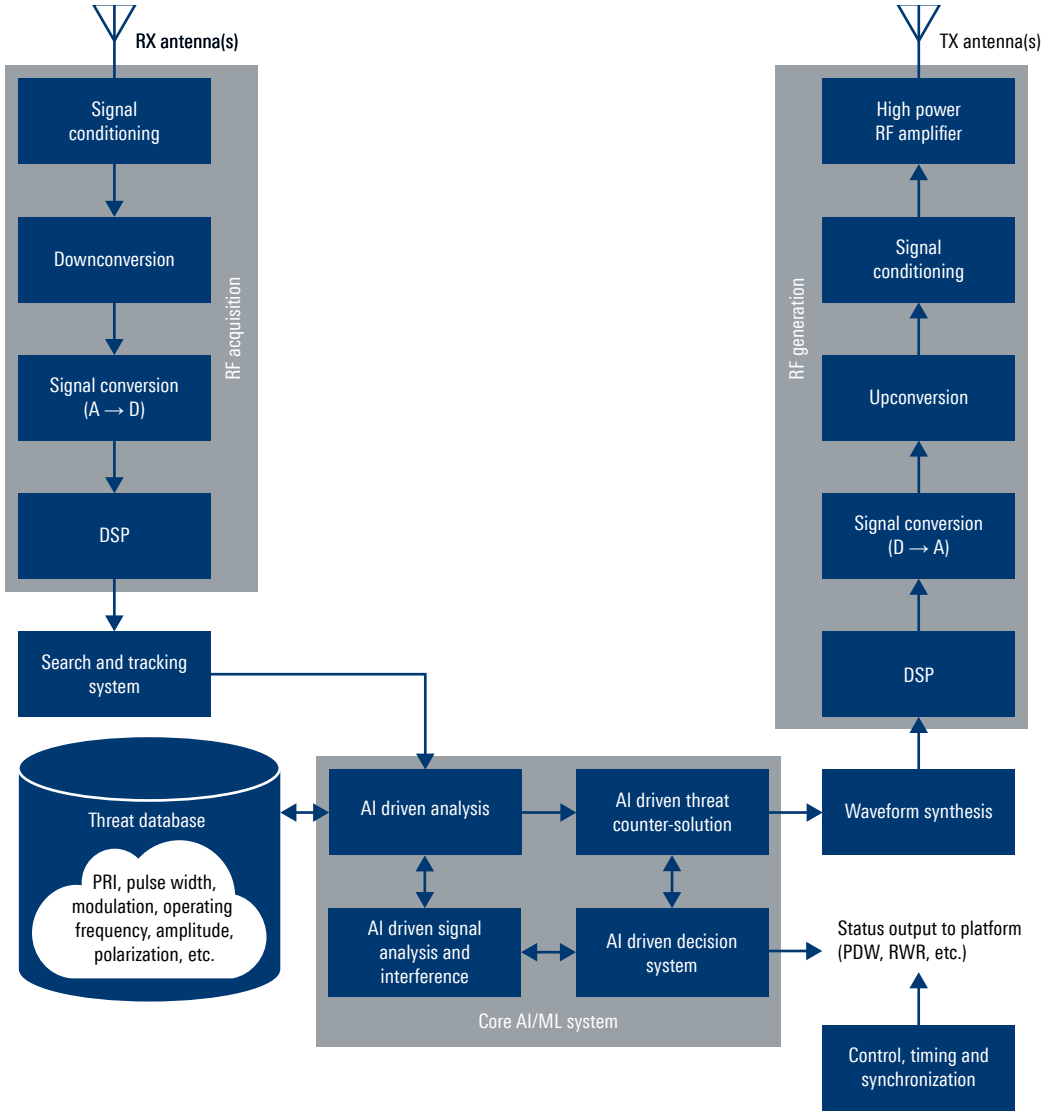
4. Waveform synthesis

The waveform synthesis block is responsible for interpreting the output of the threat counter solution block and turning that information into a digital stream of data that represents the digital implementation of the counter.

5. RF generation

The RF generation block is the opposite of the RF acquisition block. It consists of DSP such as digital upconversion, resampling, digital beamforming and filtering. The digital-to-analog converters (DACs) convert the digital stream into an analog waveform. The frequency converter (upconverter) converts the baseband analog signal from the DACs to an RF frequency and is following by signal conditioning which may include filtering, attenuation, etc. The final step is the amplification of the RF signal so that it has sufficient power to jam or deceive the threat and antennas to transmit that RF signal.

Figure 3: A cognitive radar/EW system



3.3 Challenges in training cognitive radar/EW systems

As discussed in chapter 3.1, the AI techniques used in machine learning (ML) require training. In this context, 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 this loop in an iterative manner. This iterative process, when applied to physical RF hardware, is known as hardware in the loop (HIL) or system in the loop (SIL). HIL and SIL testing can be a long and onerous process, making it a prime candidate for automation, not only for initial algorithm development and tuning, but also for regression testing of newer algorithms against older ones, in reprogramming labs, where mission datasets are established in preparation for deployment in conflicted or contested environments and even at the operational level before a mission is executed to ensure the radar/EW systems are operational.

3.4 Acquisition of data sets

As discussed in chapter 2, it is very unlikely that real-world collect operations will capture the non-traditional operations of mode-agile emitters. However, the collect process can still obtain valuable real-world signals that are useful in the SIL/HIL lab as they will contain representative signals complete with interference, poor quality, poor signal-to-noise ratio (SNR), fading, multipath and many other aberrations.

Another use for an AI/ML system is to de-interleave and classify signals that are often difficult to discern in a complex real-world RF environment, where there are a lot of emitters using many different modulation techniques. The AI/ML system can be used to extract just the signals of interest and save those as potential future training datasets.

A signal collection system can be constructed using commercial-off-the-shelf (COTS) hardware such as the R&S®IRAPS integrated record analysis and playback system shown in Figure 4. This consists of an R&S®FSW signal and spectrum analyzer, connected to an ERISYS SigPro-4000 system via a fiber optic QSFP cable. The R&S®FSW is a laboratory-grade spectrum analyzer capable of up to 8.3 GHz of internal RF analysis bandwidth and a tuning range from 2 Hz to 85 GHz (500 GHz with external harmonic mixers). This system is capable of streaming up to 1 GHz of RF bandwidth and storing the data on high-performance solid-state drives (SSD), providing more than six hours of continuous recording. The SSDs are removable for security purposes as well as for moving the stored data to other systems. The system is expandable to multiple channels and can incorporate timing and synchronization elements such as IRIG and GPS.

The SigPro data visualization application, called ZoomOut® (Figure 5), allows the operator to capture and visualize large amounts of data and to segment that data into smaller portions to extract the core signals of interest. Figure 6 shows the ZoomOut® software extracting a 100 ns Barker coded signal from a crowded and noisy spectrum at a center frequency of 8 GHz. The data is stored in industry standard I/Q format, allowing further processing in standard software applications. The data also has an associated metadata file.

Figure 4: R&S®IRAPS – a COTS based signal collection system

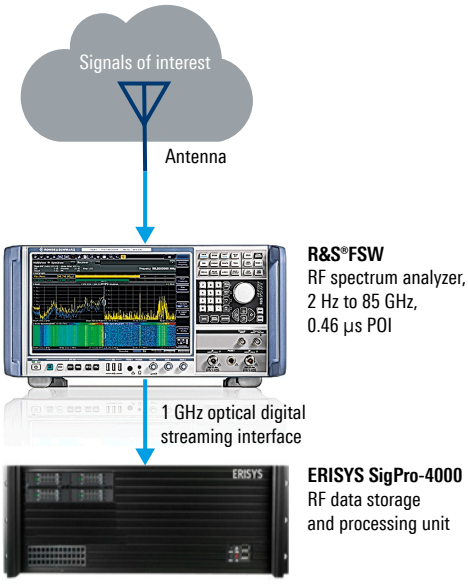


Figure 5: ZoomOut® operator interface

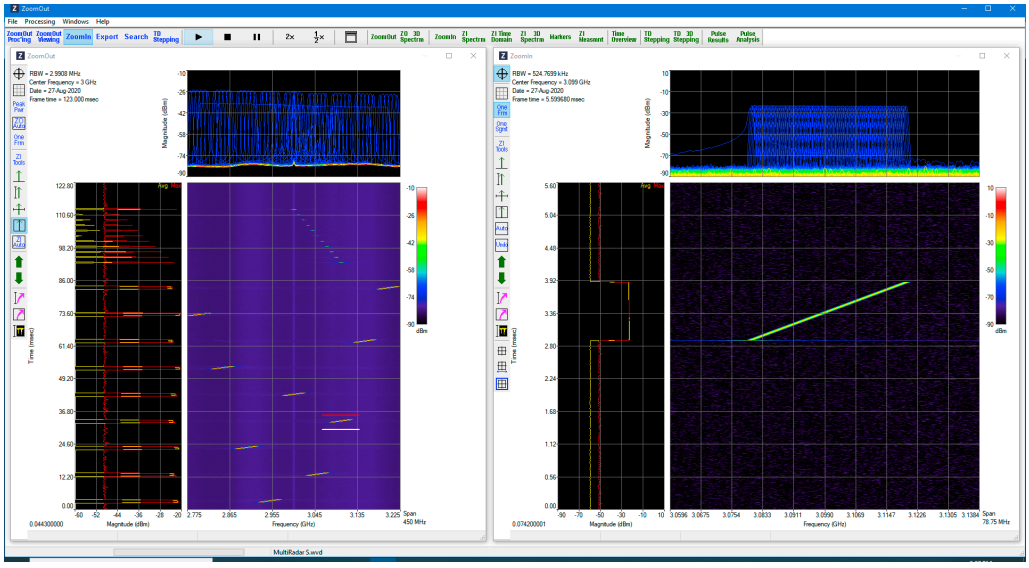
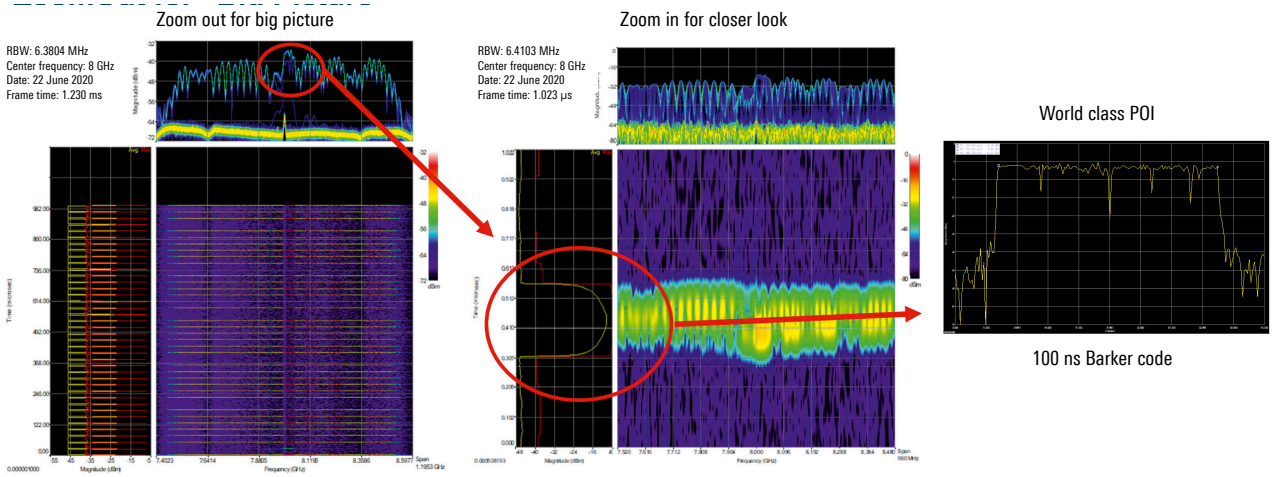
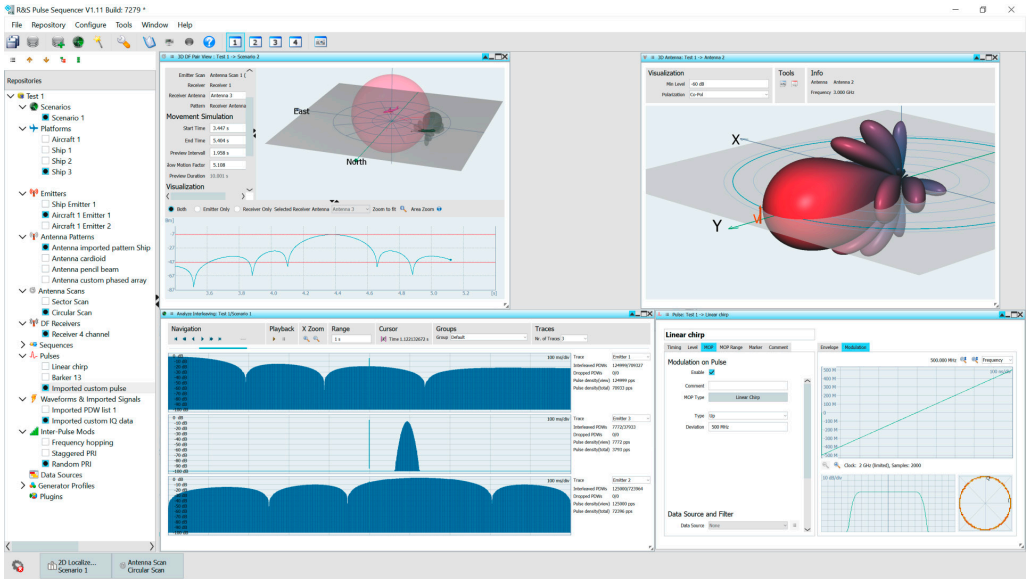


Figure 6: ZoomOut® software capturing a 100 ns Barker code



The other main tool used to develop training data sets is Modelling and Simulation (M&S) software, utilizing industry standard tools such as MATLAB®, Simulink®, R&S®Pulse Sequencer software (Figure 7), R&S®WinIQSIM2 and other commercially available software packages. M&S software is a critical tool for creating data sets as it allows almost infinite variations in the prototypes, the addition of interferers, noise and other aberrations and thus permits the generation of complex scenarios and the ability to learn how the HIL/SIL system reacts to those scenarios in a low-risk controlled laboratory environment.

Figure 7: R&S®Pulse Sequencer software



3.5 HIL/SIL training system

The next step after the system has collected the desired training data sets is to train and refine the AI/ML algorithms with this data. This is accomplished with the R&S®IRAPS system shown in Figure 8. The heart of the R&S®IRAPS system is the ERISYS SigPro-4000, which is a high-performance server-class machine with an 8 to 64 core CPU, 8 Gbyte to 256 Gbyte of system memory, high bandwidth Gen-4 PCI Express bus, high-performance workstation graphics and up to 60 Tbyte of high-speed SSDs which can store 1000s of training sets. The ERISYS SigPro-4000 can include 10 Gbit or 100 Gbit Ethernet interfaces for quick and efficient movement of data between systems. The ERISYS SigPro-4000 includes a large FPGA development board for FPGA algorithm prototyping and in-line DSP of the I/Q data streams. The ERISYS SigPro-4000 also coordinates overall system communications and configuration via Ethernet and stores the results of training runs for further analysis.

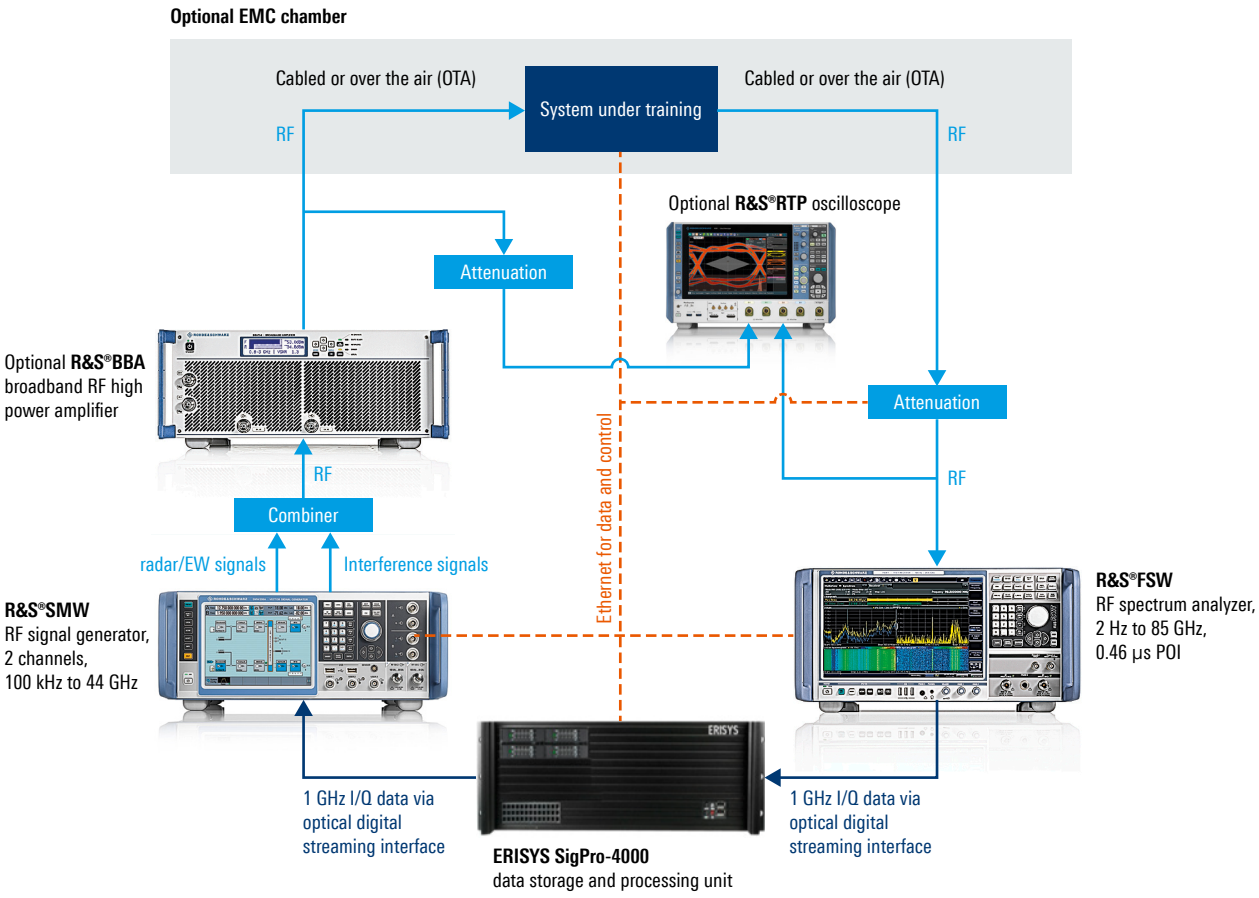
The vector signal generator (VSG) is an R&S®SMW200A and it is used to generate the RF waveforms. It is connected to the SigPro via an optical or copper Quad SFP+ connector which can accommodate up to 1 GHz of I/Q data. The R&S®SMW200A can generate up to two independent signals, which could either be two RF signals played from the SigPro or one signal from the ERISYS SigPro-4000 and one from the R&S®SMW200A onboard memory, such as wideband noise, multipath or fading signals or other commercial RF signals such as FM, AM, PM, terrestrial TV, LTE, 5G and GNSS. These signals are combined and fed to an optional R&S®BBA 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 utilizing OTA testing, then an EMC chamber may be employed to ensure that RF emissions do not emanate from the chamber.

The generated RF response from the SUT, again either cabled or OTA, may need attenuation to bring the amplitude of the generated signal into a range that can be acquired by the R&S®FSW signal and spectrum analyzer. The R&S®FSW converts the RF spectrum into an I/Q data stream that is fed back to the SigPro via an optical or copper Quad SFP+ connector which can accommodate up to 1 GHz of I/Q data.

A multichannel oscilloscope may also be useful to capture the stimulus and response from the system under test (SUT) in order to gain a deeper understanding of the timing relationship, latency and repeatability of the SUT to varying signals. In addition, a modern oscilloscope such as the R&S®RTP, has an extremely wide bandwidth, up to 16 GHz with excellent dynamic range, and can be useful in analyzing the overall RF spectrum to look for unexpected, out-of-band emissions, etc.

Figure 8: IRAPs HIL/SIL block diagram



This closed-loop R&S®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.

4 CONCLUSION

This white paper has described the challenges that mode-agile radar and EW threat emitters pose to traditional static threat library implementations in radar and EW systems. We reviewed the general theory of the algorithms used to create cognitive AI/ML radar and EW systems. Also, we discussed the architecture of a system used to perform real-world signal collect and discussed the applications and tools that can be employed to generate data sets which can be used to train an AI/ML system. We concluded with a discussion of a system that can be used to perform SIL/HIL training of an AI/ML system which can be used to evaluate and improve the effectiveness of the AI/ML algorithms.

5 REFERENCES

1. **A Comprehensive Survey of Machine Learning Applied to radar Signal Processing**
   Journal of LATEX class files, Vol X, No X, September 2020,
   Ping Lang, Xiongjun Fu, Marco Martorella, Jian Dong, Rui Qin, Xianpeng Meng, Min Xie,
   https://arxiv.org/pdf/2009.13702.pdf

2. **Artificial Intelligence Aided Electronic Warfare Systems – Recent Trends and Evolving Applications**
   Purabi Sharma, Kandarpa Kumar Sarma and Nikos E. Mastorakis,
   IEEE Access, Volume 8,
   https://ieeexplore.ieee.org/document/9292960

3. **Effect of DRFM Phase Response on the Doppler Spectrum of a Coherent radar: Critical Implications and Possible Mitigation Techniques**
   PI Herselman, Waj Nel, Je Cilliers,
   CSIR,
   https://researchspace.csir.co.za/dspace/handle/10204/2685

4. **Cognitive electronic warfare: Radio frequency spectrum meets machine learning**
   Charlotte Adams,
   Aviation Today,
   https://interactive.aviationtoday.com/
   cognitive-electronic-warfare-radio-frequency-spectrum-meets-machine-learning/

5. **Performance Metrics for Cognitive Electronic Warfare – Electronic Support Measures**
   Scott Kuzdeba, Andrew Radlbeck, Matthew Anderson, BAE Systems,
   Milcom 2018, track 4, proceedings, Published by the IEEE,
   https://ieeexplore.ieee.org/document/8599698

6. **Joint Publications Operations Series**
   Joint Chiefs of Staff,
   Joint Electronic Library,
   https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/

7. **Cognitive Electronic Warfare: A Move Towards EMS Maneuver Warfare**
   Maj. John Casey, United States Army Command and General Staff College,
   https://othjournal.com/2020/07/03/
   cognitive-electronic-warfare-a-move-towards-ems-maneuver-warfare/

Note: All links have been checked and were functional when this document was created. However, we cannot rule out subsequent changes to the links in the reference list.

Rohde & Schwarz

The Rohde & Schwarz technology group is among the trailblazers when it comes to paving the way for a safer and connected world with its leading solutions in test & measurement, technology systems and networks & cybersecurity. Founded more than 85 years ago, the group is a reliable partner for industry and government customers around the globe. The independent company is headquartered in Munich, Germany and has an extensive sales and service network with locations in more than 70 countries.

www.rohde-schwarz.com

Rohde & Schwarz customer support

www.rohde-schwarz.com/support

PD 3683.7477.52 | Version 01.00 | April 2022 (ch/ja) | White paper
Improving the capabilities of cognitive radar and EW systems
Data without tolerance limits is not binding | Subject to change

3683747752
3683.7477.52 01.00 PDP/PDW 1 en