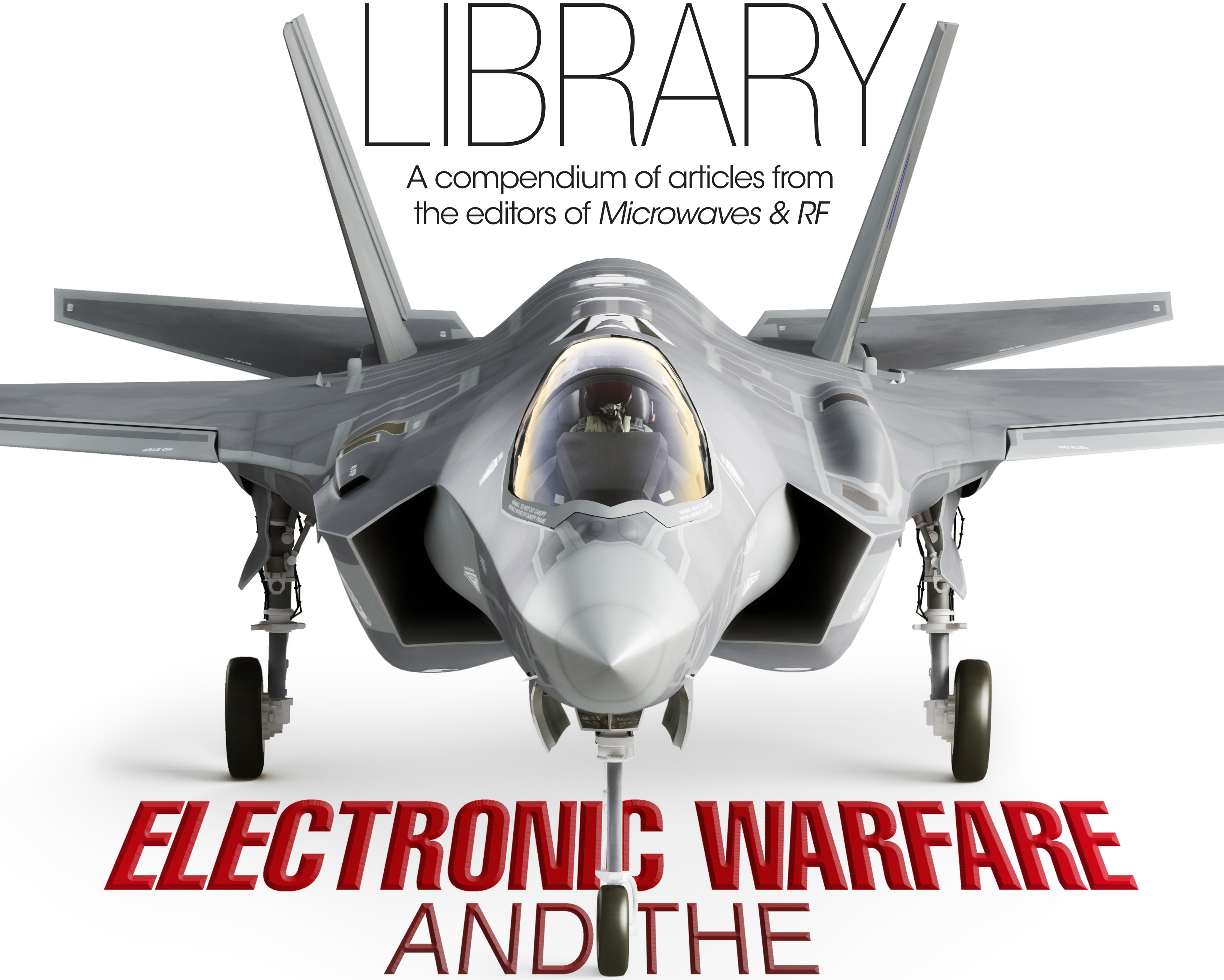
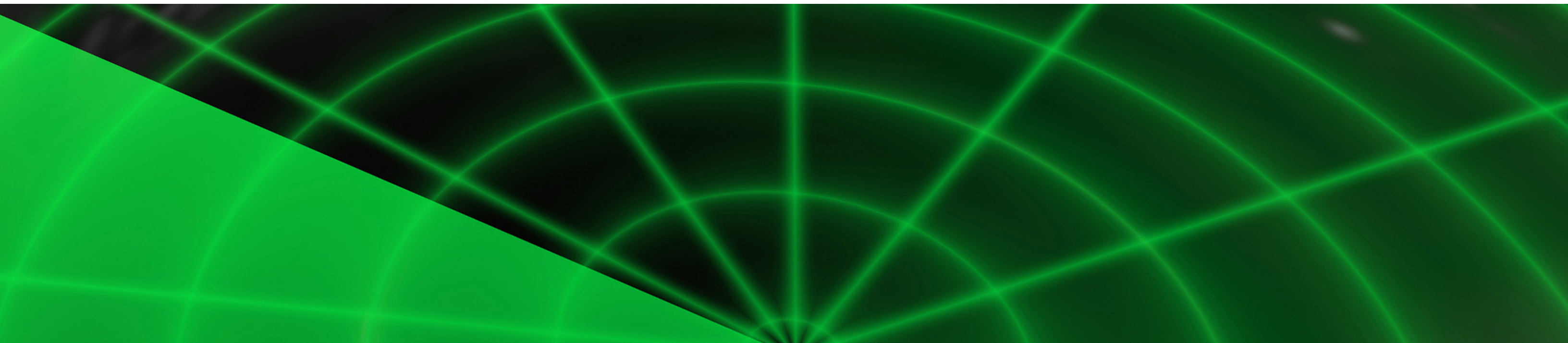
Microwaves & RF®

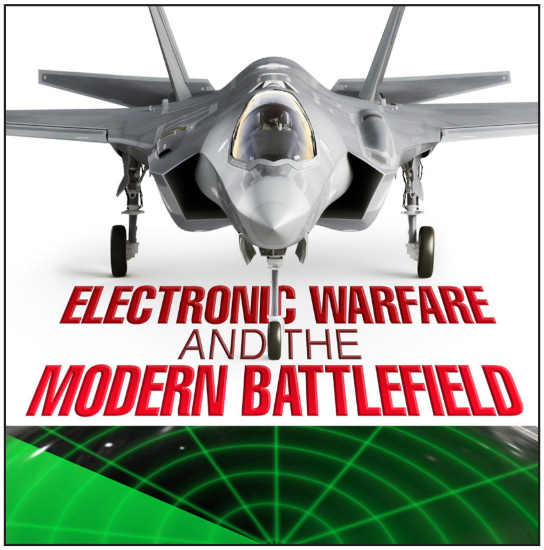
LIBRARY

A compendium of articles from
the editors of *Microwaves & RF*



ELECTRONIC WARFARE AND THE MODERN BATTLEFIELD



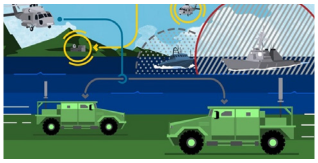


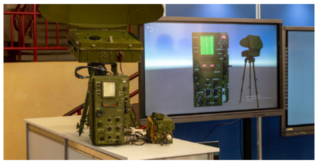
INTRODUCTION

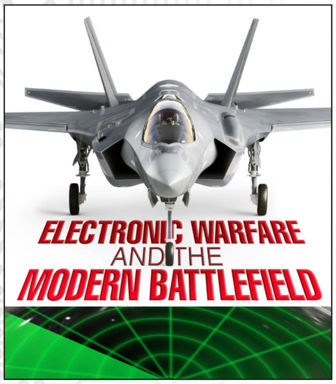
ON TODAY'S BATTLEFIELD, electronic-warfare systems have demonstrated their critical role in combat. Whether active or passive, these systems need the best components, devices, and subsystems to operate in an optimal fashion. The expanding role of EW systems in combat also place situational and environmental demands on the solutions and the systems involved.

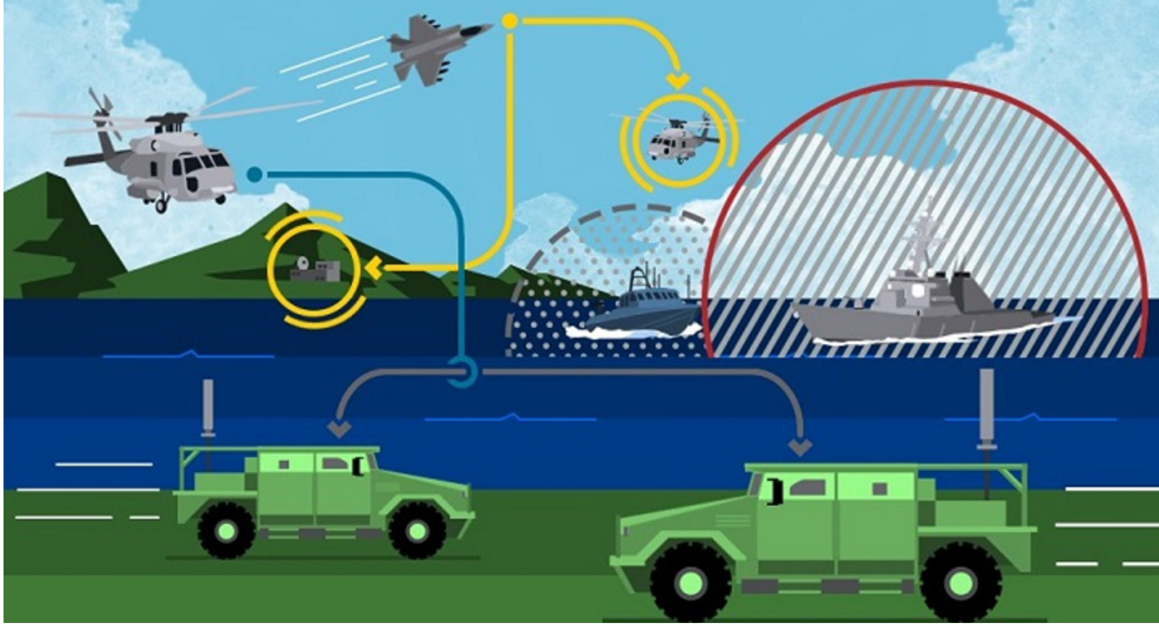
Alix Paultre
Editor-at-Large
Electronic Design,
Microwaves & RF

CONTENTS









CHAPTER 1:

Strengthening EW Systems with Cybersecurity Measures

CELESTE BREYER, Senior Field Application Engineer, *LDRA*, http://www.ldra.com

The article discusses security challenges in electronic-warfare systems and how to address them with static analysis, coding standards, dynamic testing, and more.

Electronic warfare (EW) has been around since the late 1800s when the British Army used a searchlight to “bounce” Morse code signals off the clouds. By the time of World War II, both the Allies and Axis Powers extensively used EW, or what Winston Churchill termed the “Battle of the Beams.”

Today, devices whose functions depend on the electromagnetic spectrum (EMS) are used by both civilian and military organizations and individuals for intelligence; communications; positioning, navigation, and timing; sensing; command and control; attack; ranging; data transmission; and information storage and processing. The military requirement for unimpeded access to, and use of, the EMS means EW is essential for both protecting friendly operations and denying adversary operations.

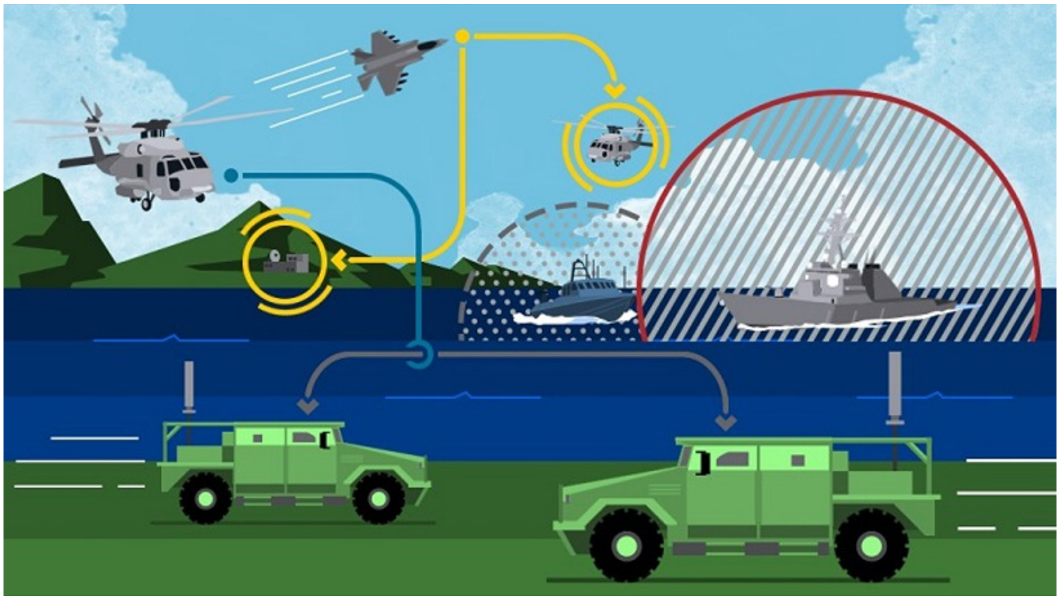
The Electronic-Warfare Ecosystem

EW is the general term given to the use of electromagnetic energy to attack or defend a target. It’s further categorized into electronic attack (EA), electronic protect (EP), and electronic-warfare support (ES).

EA involves the offensive use of electromagnetic-energy weapons, directed-energy weapons, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. The end goal of EA is to create an environment where conventional attacks on an adversary can be more effective.

EP are the defensive techniques to protect against friendly or enemy use of electromagnetic energy.1 Some EP examples include the use of spread spectrum, flare rejection logic, and frequency-hopping communications to resist jamming (**Fig. 1**).

ES is the tactical use of the electromagnetic spectrum to perform Intelligence,



1. Electronic attack (EA), electronic protect (EP), and electronic-warfare support (ES) are terms given to the use of electromagnetic energy to attack or defend a target.

Surveillance, and Reconnaissance (ISR) on the battlefield. ES can be used to locate and identify enemy assets to prioritize their neutralization. This can be done by intercepting messages directly, or by using the EM properties of transmissions with other known enemy tactics, techniques, and procedures (TTPs) to the friendly commander's advantage.

Cybersecurity plays a critical role in EW. The three categories of EW depend heavily on interconnected systems for Command, Control, Communication, Computers, Cyber, and ISR (C5ISR). In everyday cyberwarfare, a common attack method is to put a computer in an unstable state where the processor can be accessed and exploited to execute malicious code remotely. On the battlefield, a targeted energy attack is likely to be used to compromise computers, and if used in conjunction with a cyberattack, could compromise entire networks of systems.

Electronic Warfare and Cybersecurity

The overlapping dependence between EW and cybersecurity poses a unique challenge to designers implementing these systems because they're simultaneously independently functioning, and yet co-dependent on each other's stability.

Software must be constructed in a way that's immune to an EW attack. An EW attack could be used to jam a friendly network while a cyberattack is taking place simultaneously. The attack may consist of a virus or program that's uploaded to the same network and used to infiltrate the software, potentially corrupting data or exposing critical information to the attacker.

One important method to reduce vulnerabilities in software is to use static application security testing (SAST) techniques and a coding standard or a list of programming rules designed to identify and remove known attack vectors within the software (**Fig. 2**). Some commonly accepted coding standards are MISRA, Cert Secure Coding Standards, and CWE.

Because EW is so dependent on digital systems, it faces the same challenges it looks to exploit. Defects can be catastrophic and persistent, and the update process for the EW inventory is generally a lengthy one.

Static-analysis tools can be used on software throughout its development, allowing that analysis to be done early and often, checking code against the chosen coding standard to highlight potential security threats. This reduces the number bugs and the cost of development.

Looking further into the development lifecycle, dynamic application security testing (DAST) along with data and control coupling analysis can be helpful in identifying dependencies and vulnerabilities within software.

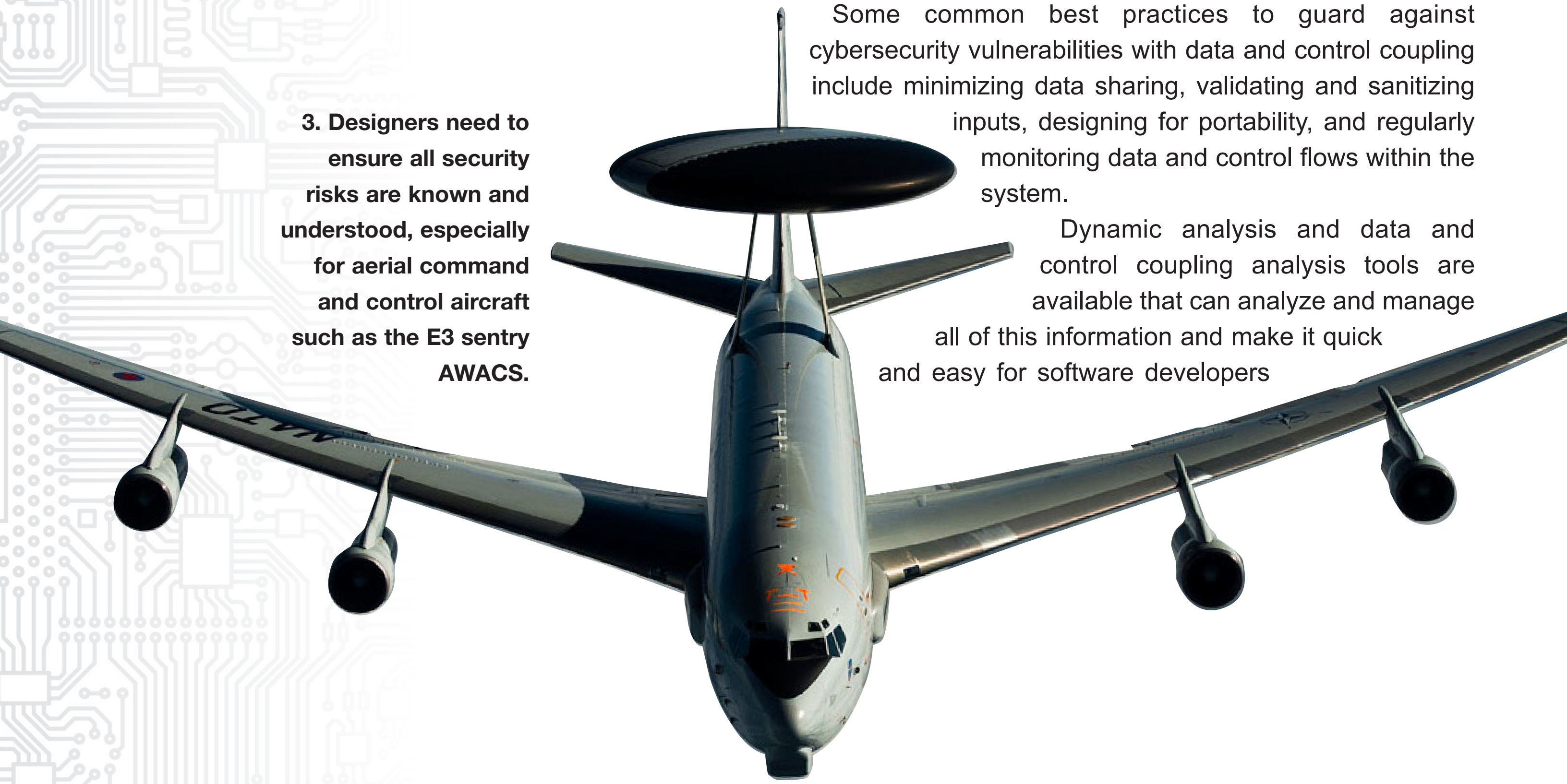
2. Static application security testing and a coding standard are among the techniques that can be used to reduce security vulnerabilities in software used in EW aircraft (photo of EA-18G Growler).

Dynamic analysis quickly identifies which parts of software haven't been executed, and as a result, not tested. It can also help pinpoint weaknesses and vulnerabilities such as memory leaks, buffer overflows, and race conditions. Through unit testing, the effectiveness of security controls and mechanisms can be exercised, validating inputs and verifying access control mechanisms are both implemented correctly and enforced during runtime (**Fig. 3**).

Complementing dynamic testing is data and control coupling analysis. Ensuring appropriate levels of separation exist between modules, and proper protocol is implemented to protect data, is paramount to a secure system.

Some common best practices to guard against cybersecurity vulnerabilities with data and control coupling include minimizing data sharing, validating and sanitizing inputs, designing for portability, and regularly monitoring data and control flows within the system.

Dynamic analysis and data and control coupling analysis tools are available that can analyze and manage all of this information and make it quick and easy for software developers



3. Designers need to ensure all security risks are known and understood, especially for aerial command and control aircraft such as the E3 sentry AWACS.

to verify their software is safe and secure. This idea is also introduced via taint analysis—a method used to identify user inputs and tracked throughout the system, ensuring all possible avenues for security risks are known and understood.

Cybersecure C5ISR Systems

Creating a robust system that resists EW attacks is a challenge. C5ISR systems are independent in their functionality, but a successful attack on one can create a waterfall effect, resulting in widespread damage.

Applying cybersecurity practices such as static analysis and using a coding standard, running dynamic analysis, unit testing software, analyzing the data and control coupling, and reviewing the taint analysis are essential for creating a more resilient system.

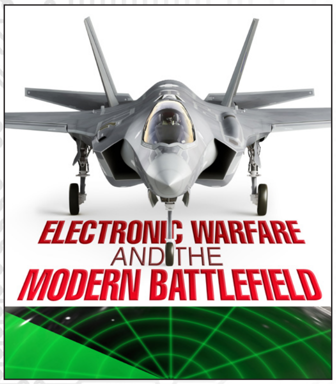
Celeste Breyer joined LDRA Software Solutions in 2016. She applies her expertise in the security- and safety-critical embedded industries to her role as Lead Field Application Engineer, inspiring and advocating adherence to best-practice development techniques in the automotive and other sectors. Celeste graduated from Texas A&M University in December 2013 with a degree in Aerospace Engineering.

Reference

1. Joint Air Power Competence Centre. (n.d.). Electronic Protective Measures. Retrieved July 15, 2024.

to view this article online, ☞ *click here*

☞ BACK TO TABLE OF CONTENTS



dreamstime_ Milan P. Mihajlovic

CHAPTER 2:

Conquer the Challenges Facing Next-Gen Front Ends

IAN DUNN, Chief Technology Officer, *Spectrum Control*

Digitization of RF signals is an important part of modern defense systems. Innovative new direct RF sampling systems promise a more simplified front-end architecture. They allow the analog-to-digital converter (ADC) to sample the RF signal directly at its original frequency without multiple stages of frequency conversion, filtering, and amplification that have burdened traditional approaches.

However, depending on the application, ensuring integrity of the signal all the way through the process to bits isn't so simple. RF segmentation, isolation, and a cascade of analog functions still govern the performance level of any direct RF solution, albeit with fewer components than traditional architectures. The next big leap in miniaturization and simplification will need to come from the RF front end.

Innovative new direct RF sampling systems promise a more simplified front-end architecture by allowing the ADC to sample the RF signal directly at its original frequency.

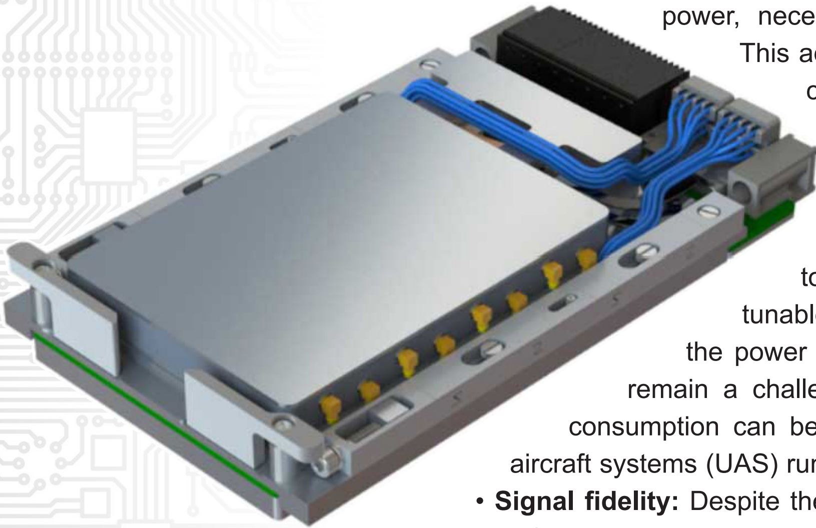
Antenna to Bits with Direct RF Sampling

Direct RF sampling enables the simultaneous capture of a broad spectrum of frequencies, which is essential for wideband applications. This approach can be more efficient and flexible for handling signals and facilitating advanced techniques like digital beamforming, spectrum analysis, and adaptive filtering.

Direct RF is considered the foundational building block (**Fig. 1**) to realize wideband, multifunction antenna-to-bit solutions. Here, the entire chain from the antenna to ADC output is optimized and designed as a cohesive system—miniature and software-definable.

While direct sampling simplifies the architecture, reduces component count, and minimizes signal degradation caused by analog processing, there are tradeoffs:

- **Direct sampling artifacts:** System designers using ADCs need to account for issues with dynamic range, spurious signals, and noise performance.
- **Power and thermal management:** High-performance ADCs can consume significant



1. A front-end module in a 3UVPX card integrates miniaturized RF analog pre-processing with high-speed direct sampling.

power, necessitating effective thermal-management solutions. This adds system complexity and may introduce reliability challenges if not properly managed.

- **Data-processing overhead:** This has kept direct sampling off the market for almost a decade. Only recently has Moore's Law delivered enough digital-signal-processing (DSP) resources to make direct sampling a competitive alternative to tunable analog architectures. Downstream resources and the power required to process the wideband digital spectrum remain a challenge for near-term adoption. For example, power consumption can be a significant challenge for lightweight unmanned aircraft systems (UAS) running on batteries.
- **Signal fidelity:** Despite the reduction in intermediate frequency stages, front-end design for direct RF sampling systems still needs to be carefully optimized and as flat as possible in performance across a much wider band. This includes ensuring adequate filtering and gain control to prevent aliasing as well as equalization across the entire band to make sure maximum performance out of the direct-sampling device. High-speed ADCs can be more susceptible to noise and nonlinearity, which can degrade the performance of the sampled RF signal. Achieving high signal-to-noise ratio (SNR) and spurious-free dynamic range (SFDR) is challenging and critical for maintaining system fidelity.
- **Clocking:** Direct RF sampling is highly sensitive to clock jitter. Any instability in the sampling clock can lead to sampling errors and degrade the quality of the digitized signal. This necessitates the use of low-jitter clock sources and architectures along with careful clock management.
- **EMI/RFI:** The high-frequency operation of ADCs and associated digital circuits can generate electromagnetic and radio-frequency interference (EMI/RFI), which can affect overall performance and neighboring electronic devices.
- **Calibration and compensation:** Direct RF sampling systems may require complex calibration and compensation techniques to correct for ADC imperfections, such as offset, gain errors, and nonlinearities. This increases system design complexity.

ADC technology and DSP continue to innovate, mitigating some of these tradeoffs. The pressure continues to be on the analog components to deliver high-fidelity signal conditioning in smaller, digital-ready packages.

Analog Signal Processing in Direct RF Front Ends

The RF front end is the initial stage of the signal-processing chain that handles the RF reception, conditioning, and distribution, rejecting unwanted signals and noise as well as converting signals of interest to a format that can be further processed and channelized by the system. Key components typically include antennas, filters, low-noise amplifiers, mixers, local oscillators, automatic gain control, power amplifiers, and, finally, switches and duplexers.

Direct sampling bypasses the need for mixers and to some extent, filtering—at least narrowband filtering, which can be done entirely in the digital domain. Filtering to eliminate interference, intentional or otherwise, is another story.

The design and the dynamic performance of the RF front end directly affects the quality and integrity of the direct-sampled spectrum. The holy grail of a direct-sampling RF front end would be the ability to notch-out unwanted, arbitrary signals. Since even the best filtering technology induces some signal loss, amplification takes on additional importance from receive to transmit.

The ability to seamlessly manage the spectrum across different frequency domains with respect to selective filtering, amplification and, for even higher-frequency applications, block up/downconversion, is a potential game-changer for future direct-sampling solutions.

Other intrinsic limitations to ADCs can be more problematic with direct sampling. More bandwidth is generally commensurate with a higher noise floor, and it can reduce the range and/or sensitivity of a direct-sampling solution.

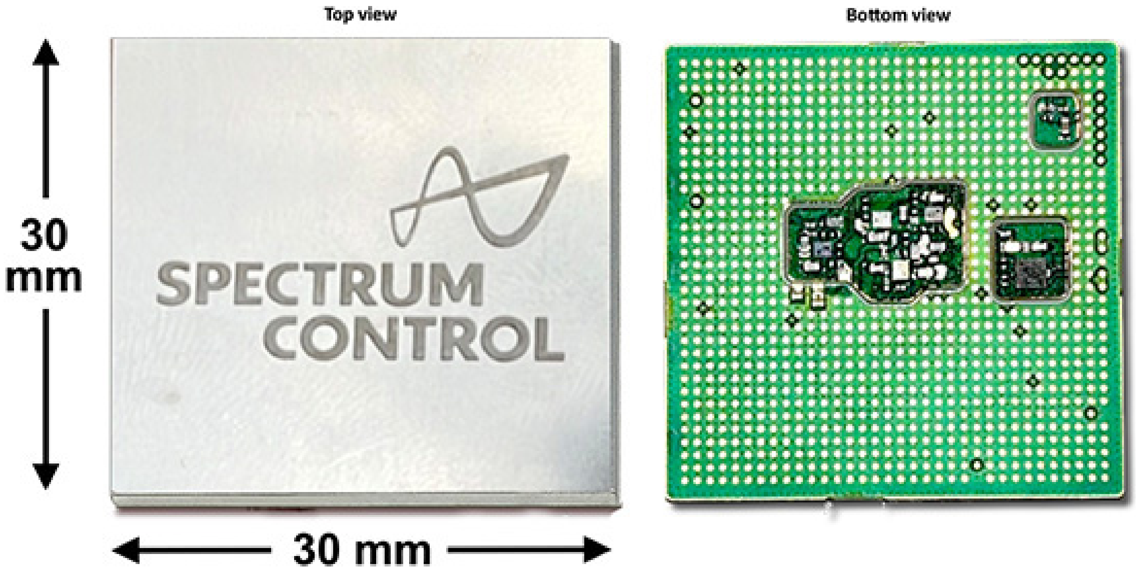
To be economically competitive with narrower-band, analog-oriented approaches, direct-sampling devices need to maximize the number of channels and benefit from new miniaturized RF front ends to offset ADC signal-handling challenges. RF miniaturization is complex and multifaceted due to several technical and physical limitations. The good news is that with direct sampling, fewer RF components need to be minimized.

Challenges and Solutions to RF Front-End Miniaturization

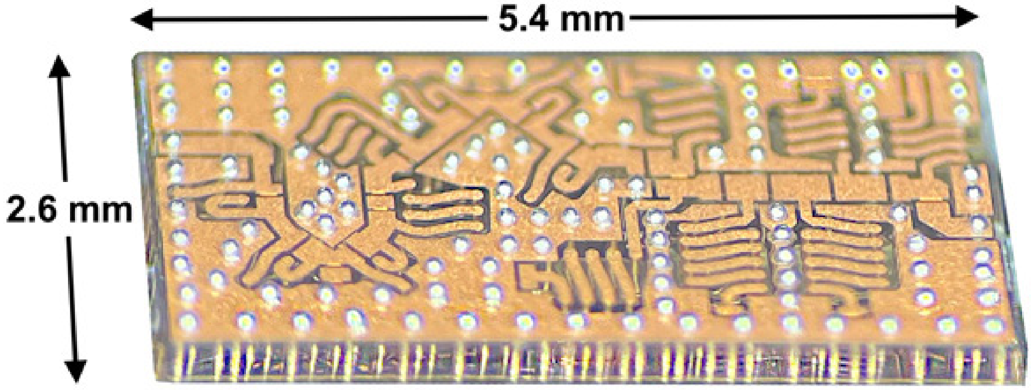
Segmentation and isolation

Segmentation and isolation are not equivalent. Achieving RF isolation in the real world is fundamentally about the physics of the RF circuit. As the complexity of the RF functions is comparatively low to a complex piece of modular software, the easiest and most cost-effective approach is to make segmentation and isolation key parameters of the RF design and manufacturing process.

New system-in-package (SiP) platforms (**Fig. 2**) leverage advances in simulation to incorporate isolation techniques into the electromagnetic simulation of the RF cascade. The design approach decomposes the manufacturing capabilities, models them in simulation, and then uses simulation tools to adjust the level of miniaturization.



2. The latest RF SiP platforms deliver high signal fidelity while reducing size and weight.



3. New solenoid inductor structures in glass are helping miniaturize high-Q RF filters.

Material science

The materials used in RF components must have precise electrical properties to ensure proper signal transmission and reception. Finding suitable materials for high frequency that are compatible with miniaturization is a significant challenge.

Discovering and manufacturing new materials that can advance the state-of-the-art in filter miniaturization and/or tunable filters is a key focus of the RF industry. Simulation can also play an important role in extending the RF performance of existing materials. Two of the most promising are glass substrates and advances in surface-mount technologies for components up through Ka-band. **Figure 3** shows an example.

Reusability and scalability

Though not generally associated with RF, a building-block approach combined with 3D electromagnetic simulations makes it possible to optimize circuit designs for reuse. And every reuse is an opportunity to re-optimize these blocks. Factoring footprint-driven factors into the simulation process allows for reuse and scaling into future devices.

RF integration

Integrating RF devices into digital systems has rarely been plug-and-play. The integrator needs to build control circuitry while accounting for device parasitics. Components that have embedded control, such as a digital gateway, and standard manufacturing rules can greatly ease the burden of integration. As direct sampling devices move the digital line deeper into traditional front ends, RF devices with integrated digital control can remove the need to add single-board computers and operating systems.

Testing and calibration

Testing and calibrating miniaturized RF components and systems is more challenging due to their small size and high frequency of operation. Specialized equipment and techniques are often required to ensure accurate measurements and performance. Embedding extremely small FPGAs into RF SiPs for on-board and in-band testing allows for RF functions to be smaller than is possible with test-and-tune.

Power consumption

Achieving low power consumption is critical in miniaturized devices, especially for battery-operated systems. Balancing performance with power efficiency in a small footprint requires innovative design and optimization techniques. RF SiPs offer a unique opportunity to move the thermal architecture closer to the components.

Antennas

The choice of antenna drives the entire architecture and can impact the level of miniaturization required. Downstream RF is typically optimized once the antenna is chosen.

Overcoming Challenges Facing Next-Gen Front Ends

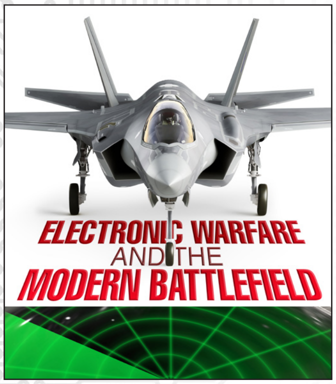
The evolution of semiconductor technology has led to high-performance ADCs with increased speed and resolution, reducing the size, weight, and power requirements for digital signal processing. Direct RF sampling reduces complexity by sampling RF signals directly, moving much of the frequency processing to software, and facilitating more efficient spectrum usage. This enables more efficient and compact RF systems.

However, while it simplifies architecture and lowers component count, challenges include power consumption, thermal issues, data-processing overhead, front-end design, clock jitter sensitivity, EMI/RFI, and calibration.

The future of front-end miniaturization hinges on developing next-generation RF front ends—analog co-processors to complement direct sampling and mitigate system design and performance challenges. This is no small task. This new generation of small-footprint RF front ends must focus on segmentation, isolation, materials, reuse, scalability, RF integration, testing, calibration, and power efficiency. New materials, simulation techniques, modularity, and integrated digital control are key to overcoming these challenges.

to view this article online, ☞ *click here*

☞ BACK TO TABLE OF CONTENTS



CHAPTER 3:

Comprehensive Test Solutions Ensure Reliable EW Systems

PETE ALEXANDER, Anritsu

Proper evaluation, validation, and integration of the amplifiers and signal generators in an EW system is necessary to achieve optimum performance.

The proliferation of sophisticated sensors and electronic weaponry on today's battlefield has created numerous entry points for adversaries. From jamming communications and spoofing signals to launching cyberattacks, electronic warfare (EW) has become increasingly critical in modern defense strategies. Enemies continuously attempt to inject interference in EW systems to disrupt missions, making signal integrity a key element of 21st century warfare.

Weak signals from amplifiers and signal generators may prevent an EW system from operating effectively. Furthermore, kinks in the cable or damaged connectors will cause signal degradation, as can the environmental conditions in which EW operates. All this can lead to system—and potentially mission—failure.

Therefore, measuring these elements' performance is essential to the efficient performance of an EW system. Selecting the proper test solutions is necessary to ensure those measurements are accurate and reliable.

Electronic-Warfare Systems on Military Aircraft

An EW system on modern military airframes is configured with antennas around the extremities connected to the signal-processing systems at the aircraft core. RF cable feeds from antennas to core processing units require regular testing. Other RF elements of an EW system, such as amplifier transmission systems and signal generators, are essential as well.

EW amplifier transmission systems are crucial because they boost the signal strength to enhance communication or disrupt enemy communications. Signal strength is important, so that the systems transmit the jamming signals, deceptive signals, or other signals at the necessary frequency and bandwidth.

Consequently, EW amplifier transmission systems must be robust, reliable, and capable of operating in harsh and dynamic environments typically encountered in warfare, from saltwater exposure and vibrations to electromagnetic interference (EMI).

Effective EW amplifier transmission systems have the ability to operate across different frequencies to adapt to changing battlefield conditions and quickly conduct signal processing to achieve the desired jamming effects. They also optimize power usage to extend operational duration in the field and seamlessly integrate with different aircraft systems and configurations, depending on the mission.

Signal generators help EW systems operate effectively in complex EMI environments. Testing EW signal generators is necessary to ensure they generate the proper signals to jam enemy communications and radar systems, effectively neutralizing threats or creating tactical advantages. EW signal generators also aid in signal intelligence (SIGINT).

Amplifiers and signal generators are susceptible to the same environmental challenges as all EW system components. Their performance can be adversely affected by EMI, shock, vibration, and extreme temperatures.

For amplifiers, technicians need to use spectrum-analysis tools to conduct measurements, including output power, gain, signal quality, and impedance. To monitor signal generator performance, test solutions must accurately measure frequency range, signal amplitude, modulation types, and signal accuracy.

Proper integration of the amplifiers and signal generators within the entire EW system is also necessary to achieve specified performance. Their maintenance is part of a complete system approach that should include testing cable and antenna systems.

How RF Cable Feeds Impact EW System Effectiveness and Reliability

RF cable feeds in military airframes are critical components, too. They enable the effective operation of RF-based systems essential for mission success and aircraft survivability in combat and other operations.

Military aircraft use specialized RF cables that are designed to handle high-frequency signals efficiently while minimizing signal loss and interference. These cables are often shielded to protect against EMI and maintain signal integrity.

RF cables in military airframes use specific connectors and interfaces that are ruggedized, reliable, and suitable for use in high-vibration and harsh environmental conditions encountered during flight. Such connectors ensure secure connections and maintain signal integrity under operational stresses.

RF cables are routed strategically throughout the airframe to connect to EW systems, antennas, and other RF equipment, including amplifiers and signal generators. Routing must account for signal attenuation, impedance matching, and minimizing interference from other electronic systems within the aircraft, as well as natural conditions and nefarious acts. Regular testing must be done to maintain compatibility and interference-free operation.

Comprehensive Testing for Electronic-Warfare Systems: Ensuring Signal Integrity

Military technicians must verify insertion loss and return loss in an EW system. They do this using a cable and antenna analyzer that can conduct return loss and voltage standing wave ratio (VSWR).

Newer instruments (**Fig. 1**) integrate advanced real-time spectrum analysis (RTSA) to quickly identify and address EMI and signal-integrity issues to maintain the security of EW

1. Cable and antenna analysis are integrated with spectrum analysis for comprehensive testing of EW systems. (Courtesy of Anritsu)

systems, along with the cable and antenna analysis. These advanced solutions also have IQ capture and streaming to gather intricate signal data in real-time, allowing for exhaustive analysis and troubleshooting.

While return loss can verify the health of an EW system, distance-to-fault (DTF) is the best technique to troubleshoot systems and locate problems. The most effective DTF measurement uses a fast Fourier transform (FFT) to convert frequency data to the time domain and display signal reflections with respect to distance. A standard trace math feature found in some analyzers can monitor small relative frequency changes over time.

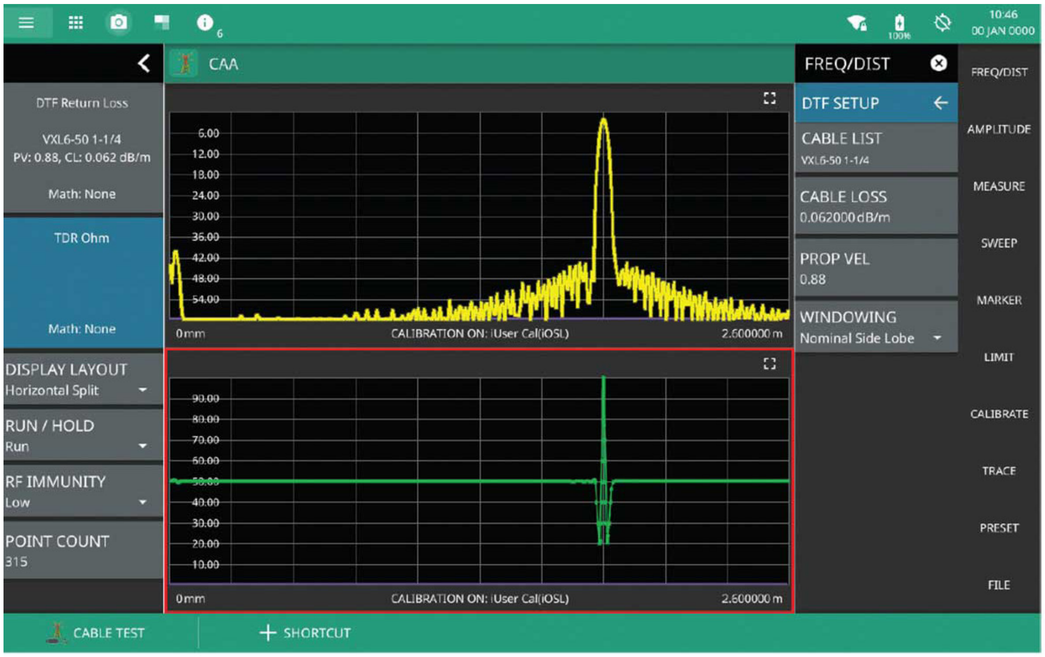
To expedite analysis and locate issues in the EW system, some analyzers have a split screen display (**Fig. 2**). It allows return loss and DTF to be on the same screen. As a result, the position along the RF cable where the highest reflections are taking place can be pinpointed while also showing overall return loss. Identifying the issue through this feature speeds up the resolution of the fault.

The Importance of Speed and Accuracy in EW Testing

Given the mission-critical nature of EW systems, locating and rectifying an issue as fast as possible is paramount. When a return-loss measurement identifies a cable and antenna path that doesn't meet specification, it's necessary to locate the cause of the reflection and repair it.

A basic DTF measurement quickly locates the distance of the individual reflections from the input test port. For long cable runs, the more information known about the reflection cause, the quicker and easier it becomes to the repair it.

That's why TDR measurements are important as well. They show impedance against distance, with a normal 50-Ω line running across the center of the display. Different causes


DTF Return Loss
VXL6-50 1-1/4
PV: 0.88, CL: 0.062 dB/m
Math: None

TDR Ohm
Math: None

DISPLAY LAYOUT: Horizontal Split
RUN / HOLD: Run
RF IMMUNITY: Low
POINT COUNT: 315

CABLE LIST: VXL6-50 1-1/4
CABLE LOSS: 0.062000 dB/m
PROP VEL: 0.88
WINDOWING: Nominal Side Lobe

CALIBRATION ON: iUser Cal(iOSL)

2. A split screen shows DTF and TDR measurements simultaneously to better pinpoint causes of signal degradation. (Courtesy of Anritsu)

of reflections, such as open circuits, short circuits, kinks to the outer cable conductor, and water ingress, will cause characteristic changes to the transmission-line impedance. This aids in identifying the cause of the fault and accelerates the repair process.

A transmission measurement needs to be made on fixed transmission lines, including coaxial cables within aircraft wings and fuselage. A USB sensor can be integrated into an analyzer to conduct transmission measurements. Such a configuration enables technicians to make those measurements quickly and efficiently. Some instruments allow the measurement to be made simultaneously with reflection (return loss or VSWR) or DTF to facilitate system verification.

Compact and Durable Test Equipment for Electronic-Warfare Systems

Much like the EW systems that they test, the instruments must be durable to produce the required consistently accurate results. Analyzers should be designed and tested to meet the MIL-PRF-28800F Section 4.5.6.3 Explosive Atmosphere requirements for safe usage on flight decks and in areas where high volatility may exist. In addition, the solutions must be compact so that they can be carried and used in the tight confines of the aircraft.

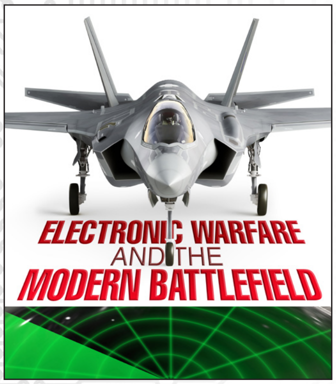
Thorough Testing is Essential to Military Aircraft EW Systems

Testing aircraft EW systems and their components is a proactive approach to maintaining operational readiness. It involves comprehensive testing, dedicated solutions, and stringent maintenance schedules to mitigate risks and maximize mission success.

Measuring signal performance of EW systems involves testing individual components, such as amplifier systems, signal generators, RF cables, and antennas, using solutions that integrate multiple instrument capability and can produce accurate and reliable results in harsh environments.

to view this article online, ☞ *click here*

☞ BACK TO TABLE OF CONTENTS



dreamstime_ Milan P. Mihajlovic

CHAPTER 4:

Electronic-Warfare Testing: Advanced Techniques with Real-World Data

NANCY FRIEDRICH, RF Product Marketing Manager for Aerospace Defense
at *Keysight Technologies*

With unexpected threats constantly arising, stressing an EW system against actual recordings of the environment helps developers gauge real-world performance.

Success in any defense mission means prevailing in the electromagnetic spectrum operations (EMSO) environment. Today's radio-frequency (RF) spectrum environment is becoming increasingly unpredictable, as new threats emerge continuously from often unknown sources. To know that a system will perform in the face of threats, developers ideally simulate the operation planned in the actual mission.

As recording and playback technologies rapidly evolve to better capture the actual RF environment, system developers can rely on streaming to test system performance. Armed with this capability, developers will see if their system responds with appropriate—and successful—countermeasures in a conflict scenario.

A variety of use cases exist for record and playback capabilities. For example, a team may want to perform spectrum monitoring of a dense spectral environment. Here, the goal is to capture everything in a wide bandwidth and record that to storage, so that it can be analyzed in detail afterward. In this scenario, developers often look for particular signals of interest like interferers. They want to monitor the spectrum to make sure there are no malicious interferers and no non-cooperative interferences. Usually, the latter problem arises when other commercial-type transmitters impose on bands that should ideally stay clean of interferers or problem signals.

In aerospace and defense, a common use case for testing is free space testing. It involves large-scale exercises with multiple platforms, including aircraft and ground assets, and requires analyzing a wide range of communication signals and spectrum activity.

Here, the developer may have a need for a ground sensor during a test, which individually records and collects time-stamped data on what's going on in the spectrum. That data can be correlated to specific test activities. If certain effects occur throughout a mission, the developers can then correlate that event to exactly what was happening within the spectrum.

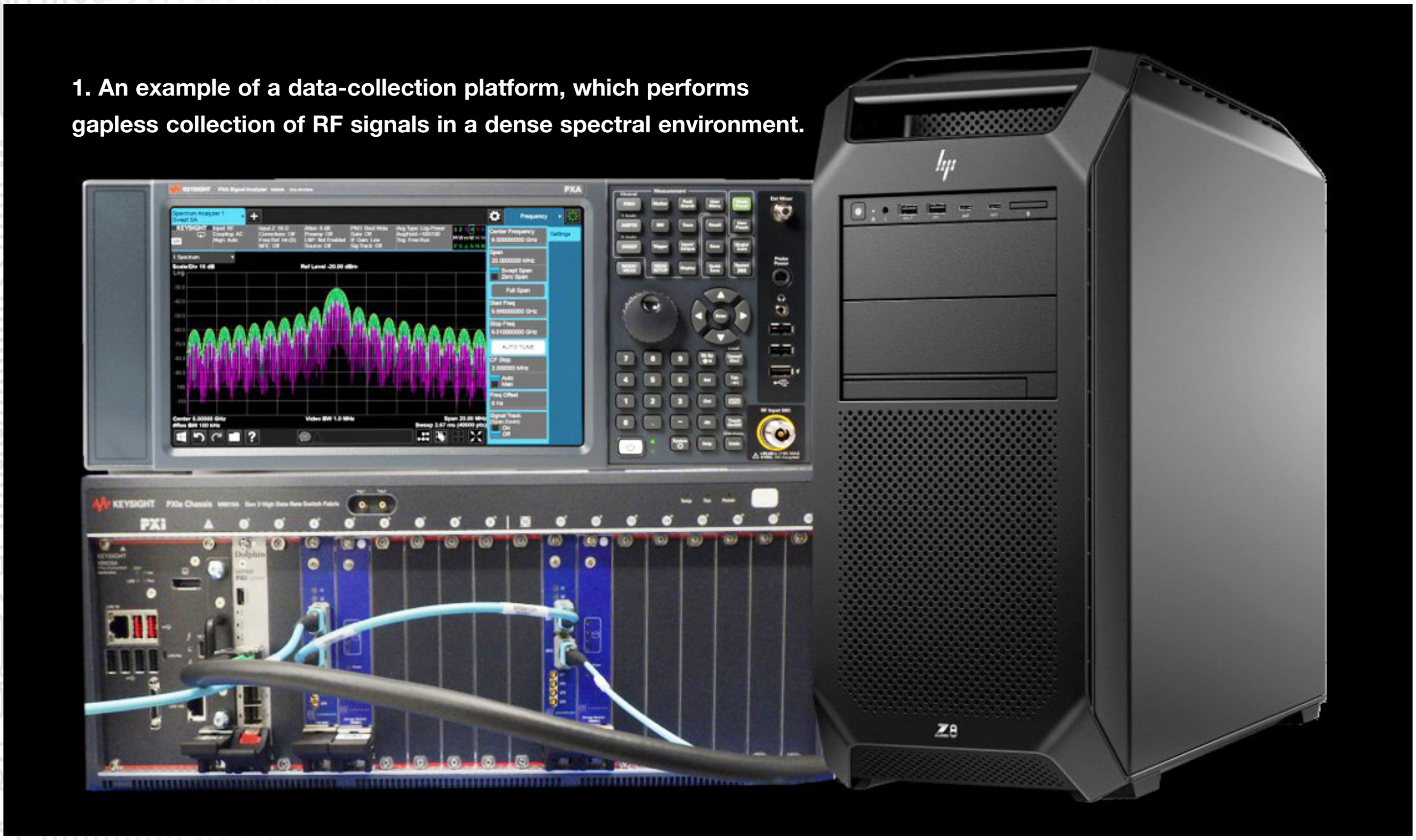
Record and Playback for Electronic Warfare

In terms of electronic warfare (EW), recording and playback can improve performance assessments for the myriad systems encountered. Examples include jamming platforms, radars, ground and airborne systems, satellite communications, and general spectrum operations. The goal of recording is to access the truth source for whatever test activity is occurring, as streaming provides 100% probability of intercept for spurious signals.

This information goes beyond just a picture or trace of the spectrum, providing the actual point-by-point, sampled data of all signal activity. With modern streaming solutions providing long-term storage, the advantage is a gapless, wideband, running truth source for potentially hours of time (**Fig. 1**).

For best results in gauging actual system response and performance, the system developer should not use a clean environment. Ideally, the developer should have access to a comprehensive range of signals, or "clutter," in the environment. This includes cellular, Wi-Fi, commercial radar, marine, and air traffic signals. Everything should be captured, independent of analysis by engineers.

Recording technologies are rapidly evolving to better capture the actual environment. By layering these different recordings, it's possible to play them on top or with the EW-specific signals.



1. An example of a data-collection platform, which performs gapless collection of RF signals in a dense spectral environment.

If a test involves multiple units or branches of the military or government working in conjunction, for example, the goal is to test different types of signal activity. The operators want to see how effectively these systems can come together in an operation. Such tests must contend with the complexities of the spectrum growing more crowded as well as each individual platform's multiple functions, and therefore signals.

An airborne platform, for instance, will likely have a jammer and altimeters as well as communications to ground units and communications air to air. It may be doing its own radar tracking on other targets, such as missile tracking.

In the test scenario, many different systems in addition to the airborne platform are transmitting waveforms and performing spectral activities. If one source can capture all of that activity or at least collect a large portion of the spectrum, that recording and data can be correlated to certain assets and functions. The developer can then identify what's happening and how other systems respond or are impacted.

Jamming is an example of a system failing to overcome a threat. The goal is to look at a number of different systems, their behavior, and their purposes in the spectrum. By recording a radar platform, one can see how it responds to a non-cooperative environment.

Modern Radar in Electronic Warfare

Radar systems play a critical role in the EW ecosystem. They must advance to contend with evolving threats in the dense spectrum environment; as it is, they're currently designed to be more intelligent and automated.

Radar systems may switch modes or channels, searching for clear channels. Once the system encounters jamming or a lot of other activity in the operating band, a radar should respond in a way that preserves its advantage in the operational environment. For radar-system developers, the goal is to see the jamming or spectrum interference begin and assess whether the radar responds accordingly, with the goal of avoiding the jammed portions of spectrum.

For threat simulation in particular, developers can take a recording of a very high-fidelity system in a realistic environment into a lab. There, it can be run through radar warning receivers (RWRs) via a lab bench setup. With that recording running, the developer can create techniques in response to it, repeatedly in a closed environment with no risk to physical or human assets.

If an airborne platform is flying into threat territory, an RWR functions as a receiver looking at the environment. If it sees signals, it matches them up—possibly to a known library. It then summarizes, based on these parameters, the frequency, what the pulses are doing, the threat or type of threat, and the threat location and/or direction it's moving. This approach alerts the pilot to the threat so that they can decide how to respond.

Recording for Mission Success

To develop effective countermeasures, it's crucial to be able to play the recording of new threats. Those recordings also must be inserted into the systems on the plane or other vehicle so they can view it. The EW test system can then verify if the system is detecting the threat and how it's responding.

Introducing that signal into the system requires a flexible architecture for the reprogramming environment. Think of it as a benchtop system of systems. In addition to harnessing the information about the new threat, the system needs to simultaneously consider any preexisting threats and information regarding the environment.

Here's where data advances like machine learning greatly improve capabilities. In the past, a team of analysts would require a week or two to analyze this data, trying to detect and identify all signals of interest. They will rely on custom scripts and need to manually break up large binary files, using software tools to parse the data with custom scripts.

Today, much innovation focuses on the challenge of managing big datasets of raw RF. New options increasingly allow signals and signal events to be identified in real-time, presenting clean results once the recordings are completed.

Performance Needs: Where To Start

With myriad use cases and surprises in the spectrum environment, system developers need confidence in system performance for diverse mission scenarios. To help determine their needs, they should consider what they're searching for during testing.

For example, the priority could be zooming in on a small frequency band or capturing a broader picture. Ideally, the system developer will have some idea of other signals in the environment in which they're transmitting. This knowledge helps direct whether they need to monitor multiple aspects or systems within the same spectrum.

Developers also need to consider if their testing will be done free space or direct-coupled. With free space, the recorder is plugged into some cabling that's attached to an antenna. That antenna may be pointed at something of interest to collect the signals coming off a specific system, such as an airborne or ground-based platform. Alternatively, they can use an omnidirectional antenna that collects data from a much larger area, picking up anything that transmits to the antenna location.

While the antenna approach provides a kind of ground truth, having the signal collection be direct-coupled through an instrument such as a handheld network analyzer (**Fig. 2**) may be more suitable for the radar. With the transmitter and receiver chain and potentially

2. By using handheld network analyzers, military personnel can capture signals of individual systems via the direct-coupled method.

coupled ports that could be tapped, it's possible to record everything coming off the radar. However, this approach delivers findings that are somewhat isolated from the surrounding area, as the developer is only looking at the connected hardware.

The recording system connects directly off a system transmitter or maybe through the receive path to see what the radar sees. With a direct-coupled approach, remember that the findings relate only to a specific system and test point, as opposed to free space, where the developer would see everything going on in the environment.

Simulation in the Future: Leveraging Real-Time Analysis

The next stage of these real-world simulations will see improvements in real-time analysis. Traditionally, the spectrum environment and related data are captured independent of analysis. The engineers and analysts must post-process this data to gain insight into the test objective. By bringing the analysis into real-time, intelligence will be available as soon as the test and signal capture are complete.

For example, a machine-learning-based analysis tool can take these long-term, wide-bandwidth RF recordings to perform energy detection on the signal data. It classifies the signals coming off that energy detection, identifies them, and then does unsupervised clustering of that data. Essentially, it builds a database of what it has identified in the data.

At the end of the processing, the developer can then interact with the data and filter out everything they're not concerned about. They're able to parameterize the data around the things of interest and kind of zoom in on the very narrow pieces of signal events of interest. With these improvements, the tools can help developers find a needle in a haystack—quite a challenge when the haystack is terabytes worth of RF data.

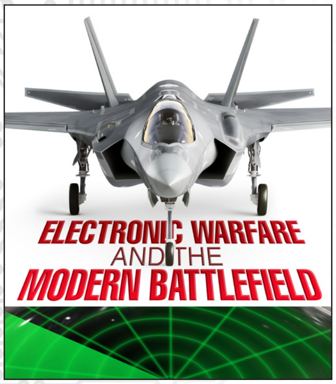
With these advances, EW and radar system developers will increasingly leverage independent capture of a large portion of spectrum, collecting it and correlating it to specific signal sources and events.

As innovations continue to enhance recording and playback solutions, they will push the boundaries of higher frequencies and wider bandwidths in keeping with military systems, providing key insights into system performance as spectrum grows ever denser and more complex. Armed with these capabilities, developers can better predict performance against threats so that the mission isn't jeopardized.

NANCY FRIEDRICH is RF Product Marketing Manager for Aerospace Defense at Keysight Technologies. Nancy Friedrich started a career in engineering media about two decades ago with a stint editing copy and writing news for Electronic Design. A few years later, she began writing full time as technology editor at Wireless Systems Design. In 2005, Nancy was named editor-in-chief of Microwaves & RF, a position she held (along with other positions as group content head) until 2018. Nancy then moved to a position at UBM, where she was editor-in-chief of Design News and content director for tradeshows including DesignCon, ESC, and the Smart Manufacturing shows.

to view this article online, ☞ *click here*

☞ BACK TO TABLE OF CONTENTS



dreamstime_ Skylkigai

CHAPTER 5:

Testing Terrestrial and Airborne Electronic-Warfare Apps

ANDREA VINCI, Senior Technical Marketing Manager, *Tektronix*

Electronic warfare (EW) is a fast-evolving technology application that refers to disrupting, degrading, or completely denying an adversary's situational awareness, communications, and targeting capabilities. EW systems are both terrestrial and airborne, and they increase hand-in-hand with the presence of force power.

Today's "air power" includes targeting long-range weapons, via autonomous air systems such as unmanned air systems (UAS), as well as using new, complex direction-finding/direction-deceiving radar techniques.

Systems equipped to implement electronic attacks, i.e., disrupt and confuse air defense systems, are essential to achieving EW "supremacy." But supremacy requires solving complex R&D challenges, and modern test platforms are needed for system validation. In this article, we will briefly cover several advanced use cases where the goal was EW spectrum supremacy to show what test challenges were faced and what methods can be applied to address them.

Today's battlefield includes autonomous air systems as well as new, complex direction-finding/direction-deceiving radar techniques.

Key Modern Scenarios in EW

Electronic engineers in aerospace and defense confront a continuous escalation of technology in advanced RF attack and countermeasure electronic protection systems. On one hand, they implement ever-more advanced jamming techniques of enemy electronic infrastructure, and on the other hand, increase the sophistication of protection across a wide span of threats and attacks from hostile forces.

In general, EW application scenarios involve advanced radar technologies, electronic countermeasures (ECM) and electronic counter-countermeasures (ECCM), and signal intelligence (SIGINT) gathering. The evolution of EW is now combined with the growing use of controlled unmanned aerial vehicles (UAVs), usually referred to as "military drones."

In the past, test and measurement suppliers focused on providing RF spectrum-analysis solutions to rapidly and accurately detect signals to identify and track objects. The scenario has evolved in complexity as location and analysis of threats has evolved into a multispectral/multichannel radio-frequency context. At the same time, new semiconductor materials such as gallium-nitride (GaN) semiconductor technology made possible new, lighter, and more cost-effective radar components that increased the capabilities of radar systems.

AESA (airborne electronically scanned array), for example, is a technology for airborne surveillance radar. The antenna consists of an array of transmit/receive modules, each equipped with a small solid-state transmitter and receiver. These modules work together to transmit and receive radar signals in a coordinated and electronically controlled manner, all made possible by advanced processing techniques and sensor-fusion algorithms. As a result, engineers need to conduct AESA more efficiently, safely, and effectively.

Engineers demand test solutions capable of generating complex phase-coherent signals to reproduce the scenarios of phased-array radars, MIMO radar, and other quite complex systems such as Jamming- DRFM radar.

The fastest growing trend in the military radar industry involves MIMO systems. These systems are used for simultaneous transmission and reception by multiple antennas or channels and exhibit radar properties having a low probability of intercepting. Engineers in this area need a compact and cost-effective way to characterize digital RF memory (DRFM) and synchronous, multichannel MIMO systems.

DRFM jammers are essentially transceivers capable of digitizing, recording to memory, modifying, and then retransmitting the recorded waveform. This causes the target radar receiving the modified signal to incorrectly deduce the unit’s speed, bearing, range, or altitude.

A key aspect of these jammers is that they can instantaneously adjust the signal power and frequency using super-fast software-defined systems. Depending on the specific technique that they implement, these jammers may be using range gate pull-off (RGPO), velocity gate pull-off (VGPO), false target generation, etc.

Test Challenges and Possible Solutions

Significant investments in cyber and EW are mirrored by the need to equip laboratories with the latest and most sophisticated test equipment as engineers in A&D request solutions for test-scenario simulation of a full range of radar signals. A typical request is for test equipment that can create multiple pulse groups to form a coherent or non-coherent pulse train, where each pulse group either independently or by adding different pulse groups simulates simultaneous multiple target returns.

Engineers also need to be able to define and generate sequences of “pulse-hopping” patterns in both frequency and amplitude. And each pulse should rapidly and easily configure such pulse parameters as start time, rise time, off time, fall time, pulse width, droop, overshoot, and ripple. On the modulation front, a variety of types such as FM Chirp, QPSK, and BPSK, as well as user-defined custom modulation, is needed.

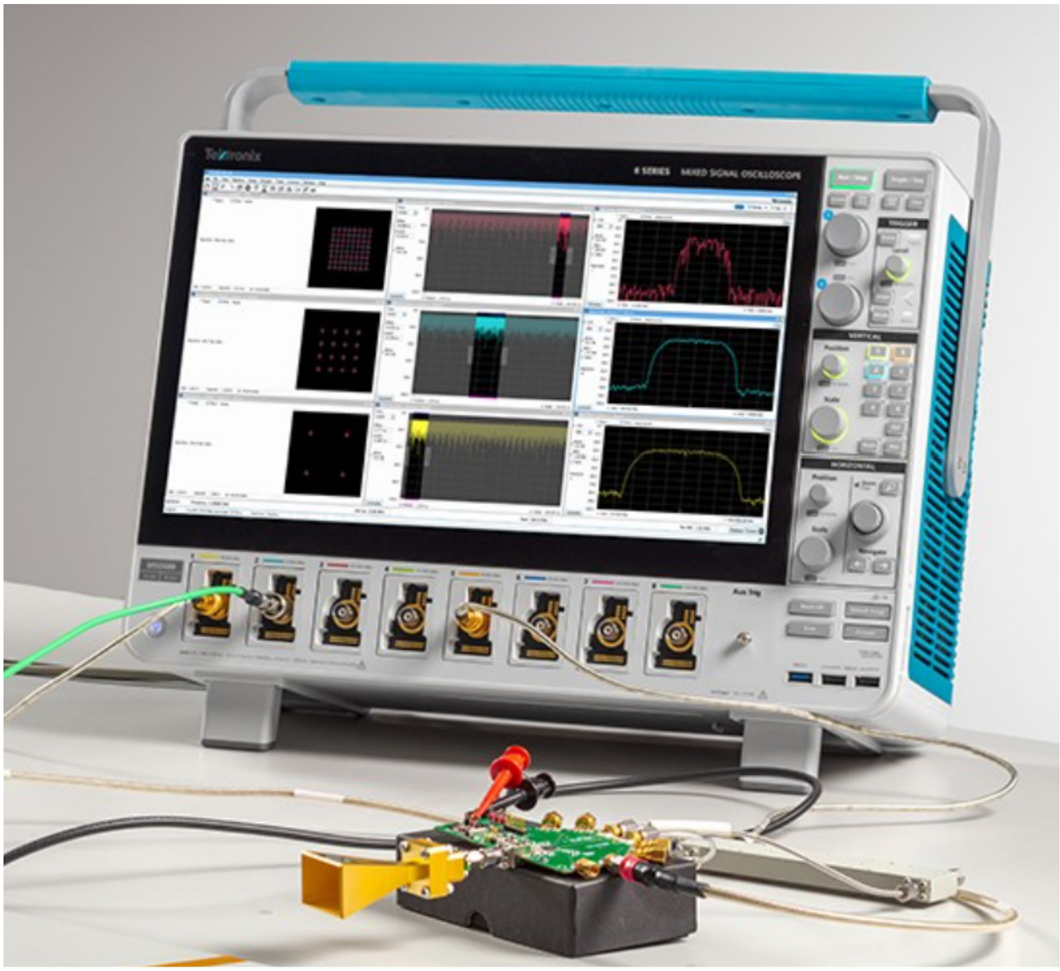
Certain MIMO radar systems employ time, frequency, or coding techniques in each transmit signal to differentiate them in the receiver element to extract target properties. In this case, engineers need a reliable yet cost-effective solution that offers wide bandwidth, phase-coherent and multichannel analysis.

Addressing these demands, Tektronix offers a broad range of multichannel and wideband oscilloscopes, including 6 Series B MSO, DPO70000SX and MSO/DPO70000DX Series Oscilloscopes. All of these oscilloscopes can be paired with SignalVu vector-signal-analysis (VSA) software.

This VSA software provides multichannel control and analysis with independent settings for parameters such as center frequency, span, and RBW (**Fig. 1**). The combined software plus hardware system validates a MIMO phased-array radar configured with different center frequencies, time slots, or modulation parameters.

By effectively controlling the segmented memory, SignalVu supports FastFrame mode for capturing only the pulse-on time while disregarding the pulse-off time, thereby facilitating the analysis of hundreds of pulses and preserving the timescale information. An exhaustive pulse statistics display enables engineers to observe time trend and measurement statistics to see how the PRI varies across pulses both over time as well as the absolute delay between channels or time slot.

In the case of modern AESA radars, multiple beams track or focus on multiple targets simultaneously. The signal and its characteristics for each of these beams can be different. Because the Tektronix 6 Series B MSO can have up to eight channels when used together



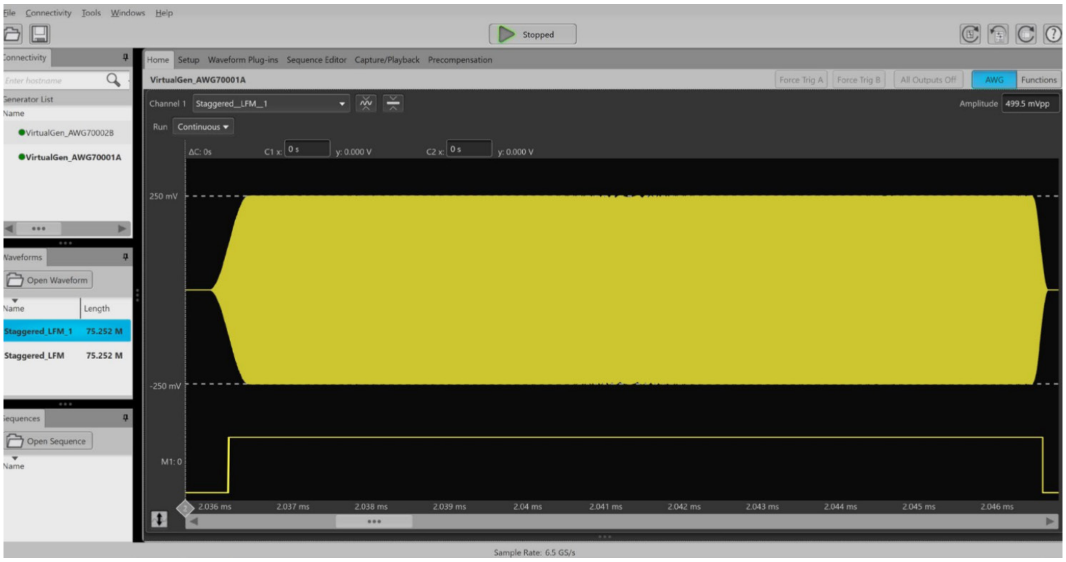
1. A multichannel oscilloscope is configured to simultaneously analyze wide bandwidth, multichannel phase synchronous systems operating at different frequencies. Tektronix

2. An RF engineer analyzes phase-coherent signals using SignalVu software. Tektronix

with SignalVu-PC software (**Fig. 2**), it can support multiple spectral displays for multiple sources. Each source may be assigned to any oscilloscope channel—up to as many as eight—with the span and RBW adjusted for each. The sources can also be either IQ or differential IQ.

New, sophisticated deceptive jamming DRFM-based systems receive and record the frequency, pulse-width, and pulse interval of an enemy system and produce a false return signal by playing back the recorded signal. Engineers can apply Tektronix's arbitrary waveform generation (AWG) technology to reproduce what DRFM systems can do, i.e., creating, modifying arbitrary waveforms digitally in a precise and fast way.

In fact, these AWGs are fully programmable and can compile and "replay" signals from memory (*see an example of staggered PRI pulse waveform in **Fig. 3***). Because they're able to create multiple scenarios and assign them to different AWG channels in one compile, users can create up to 50 scenarios made up of individual RF emitter signals and define up to 100 emitters per scenario. Furthermore, these AWGs are tested to meet military vibration standards.



Generator List

Name
VirtualGen_AWG70002B
VirtualGen_AWG70001A

VirtualGen_AWG70001A

Channel 1 Staggered__LFM__1

Run Continuous

Amplitude 499.5 mVpp

ΔC: 0s C1 x: 0 s y: 0.000 V C2 x: 0 s y: 0.000 V

Name	Length
Staggered_LFM_1	75.252 M
Staggered_LFM	75.252 M

Sample Rate: 6.5 GS/s

3. Shown is an example of a staggered PRI pulse RF voltage waveform with the marker set to coincide with the RF pulse start. Tektronix

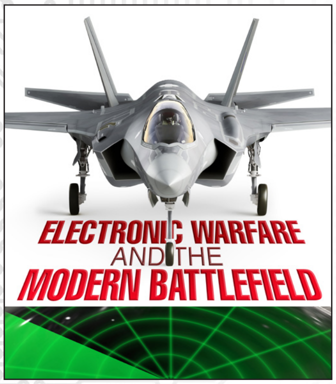
Summary

It's increasingly common for new uncrewed system UASs to carry on-board an advanced radar detection system that's capable of scanning the RF spectrum to gather data on radar emitters for airborne electronic attack. Such a system can also identify new threats and countermeasures to address them.

Airborne electronic attack involves the disabling, degrading, and denying of enemy air defenses. This can be accomplished through communication interference to deceive opponents by using electronic decoys as well as disrupting enemy threats through jamming their radar and communications systems.

to view this article online, ☞ *click here*

☞ BACK TO TABLE OF CONTENTS



dreamstime_ Ratpack2

CHAPTER 6:

The Digital Battlefield: Transforming Military Operations Through Data and Connectivity

MACY SUMMERS, President and CEO, Blu Wireless Inc., https://www.bluwireless.com/

The modern battlefield is undergoing a profound transformation, shifting from traditional voice-centric, analog Command, Control, and Communications (C3) approaches to a more intelligent, data-driven and digitally connected space. This evolution, spanning land, sea, space, and air domains, demands cutting-edge technologies and innovative practices to gain tactical advantages.

The modern battlefield is increasingly shifting from boots on the ground to a more remote, intelligent, digital space that requires a host of new technologies and practices to provide a tactical advantage.

The recent conflict in Ukraine has highlighted the critical role of data in modern warfare. It's showcasing how social media, satellite imagery, and drone surveillance (IMINT) can augment conventional signals intelligence (SIGINT) and human intelligence (HUMINT) information to shape military strategies.

As militaries worldwide adapt to this new paradigm, understanding the intricacies of data collection, analysis, and intelligence dissemination becomes paramount for defense strategists and field commanders.

The Foundation of the Digital Battlefield: Data Collection

At the core of the digital battlefield lies an expansive array of sensors and data-collection methods that are the cornerstone of situational awareness for tactical forces. The various sensors that play crucial roles in gathering intelligence include:

- **Electronic-warfare (EW) sensors:** Capable of detecting emissions from adversary weapon systems and communications.
- **Optical and laser systems:** Used for target illumination and precision guidance.
- **Robotic platforms:** Employing technologies like LiDAR (light detection and ranging) or video cameras with AI-driven analysis for autonomous navigation and threat detection.

- **Aerial surveillance:** Utilizing drones at various altitudes (low, medium, and high) to capture video and imagery of the battlefield.
- **Identification friend or foe (IFF) systems:** Providing critical information on the location and identity of friendly and adversary forces.

This diverse sensor ecosystem forms the foundation of what we commonly refer to as the "common operating picture" and situational awareness. These are essential elements for effective command and control in modern military operations.

In addition, open-source intelligence (OSINT) and HUMINT are important "data points" for a battlefield commander to consider. Do these reports corroborate the frontline representation or are they outliers? All source, real-time intelligence is rapidly becoming possible, giving local (and higher echelon) decision makers the digital tools to make the best choices for their forces.

Connectivity is the Nervous System of the Digital Battlefield

The true power of the digital battlefield lies not just in data collection, but in the ability to process, relay, and act upon that information in real-time. The key connectivity technologies for military leaders to consider are local-area networks (LANs), which facilitate communication between nearby units in tactical scenarios, typically line-of-sight (LOS) spanning a few kilometers, and wide-area networks (WANs) linking tactical units to command posts and support services.

Modern WAN technologies are evolving and some of the most common types of WAN communications are:

- **High-frequency (HF) communications:** Still widely used but extremely limited in data capacity; thus, it's less suited for modern scenarios involving sensor or intelligence data.
- **Satellite communications** is evolving rapidly from large, fixed, or transportable geostationary dishes to more agile on-the-move systems like low-Earth-orbit (LEO) constellations (e.g., Starlink, OneWeb, Kuiper) that are gaining traction in modern warfare.
- **Troposcatter:** A technology gaining renewed interest for its ability to provide beyond-LOS communications without relying on satellites. This method of propagation uses the tropospheric scatter phenomenon, where radio waves at UHF and SHF frequencies are reflected over a large distance as they bounce off the upper layers of the troposphere.

The challenge of integrating these diverse communication methods into a cohesive network that can support the data demands of the digital battlefield—while remaining resilient against EW and other threats—is ongoing and yet to be resolved.

mmWave Connectivity as the Backbone of LANs

If we look at LANs in a high threat environment, e.g., at a mobile command post or on the battlefield, such tactical networks are subject to harsh environmental conditions, EW targeting, and jamming. In this type of environment, military forces need a stealthy tactical network with low probability of detection (LPD). In fact, on the tactical edge, robust networks need to be able to operate independently of the core, Warfighter Information Network (WAN).

Millimeter-wave (mmWave) technology is well-suited to provide high-performing, stealthy networks at the tactical edge. It can link manned or unmanned weapons platforms, (mobile) command posts, ISR, and C2 (fiber optic) with the edge. Importantly, one flavor of mmWave technology exploits the license-exempt, non-commercial spectrum frequency bands (V-Band) at 57-71 GHz, a wide swath of 14 GHz of contiguous radio spectrum.

V-band is unique because it causes radio signals to resonate almost perfectly with oxygen molecules in the air—a phenomenon called oxygen absorption. The oxygen creates an incredible spike in attenuation that almost appears like a brick wall at a distance and creates a curtain of invisibility between a tactical team and its adversary. Within the V-band, connectivity truly has an LPD (stealthy) quality.

What are the Challenges on the Digital Battlefield?

As militaries adopt the digital battlefield concept, several challenges emerge.

One of the most important is possibly an information overload. While more data can lead to better decision-making, there's a risk of overwhelming commanders with information, potentially leading to decision paralysis.

Another challenge is combat effectiveness. Equipping individual soldiers with advanced communications gear must not interfere with their primary combat roles. Therefore, developing communications systems with low size, weight and power (SWaP) for dismounted soldiers remains a major focus for engineers of military communications equipment.

Finally, cross-domain integration across land, air, space, sea, and cyber domains is yet to be achieved. Seamless communication and data sharing across these domains is complex but it will be crucial for coordinated operations.

Artificial Intelligence and Machine Learning in the Digital Mix

While artificial intelligence (AI) and machine learning (ML) hold immense potential for the digital battlefield, their tactical implementation faces significant hurdles. The computational power required for deep-learning algorithms is often not available at the tactical edge.

However, AI is finding applications in areas such as autonomous navigation for robotic platforms, rapid analysis of sensor data, predictive maintenance for military equipment, and pattern recognition in signals and open-source intelligence.

As AI capabilities evolve, their integration into tactical decision-making processes will likely increase, but always under human oversight, especially in matters of weapons engagement.

The Future of the Digital Battlefield

Looking ahead, several trends are shaping the evolution of the digital battlefield. Advanced analytics will play a key role in redefining situational awareness, arming commanders with actionable intelligence from the vast amounts of data collected in real-time.

Another powerful technology making an impact is edge computing. We've mentioned that edge computational power currently doesn't support big-data analysis and ML in tactical scenarios. However, this will change, and by bringing more processing power closer to the point of data collection will reduce latency and support implementation of AI and ML.

We've noted a lack of cross-domain integration. Better integration of land, air, sea, space, and cyber capabilities through advanced IP communications networking technologies is looking possible via LEO WLAN and mmWave mesh networks. The latter can connect a peer-to-peer tactical network to higher echelon C2 networks. Finally, a wideband, fully interoperable solution is envisioned that can provide end-to-end strategic and tactical connectivity while operating with critical LPD and anti-jam features.

The digital battlefield represents a paradigm shift in military operations, offering unprecedented situational awareness and decision-making capabilities. However, it also introduces new complexities and vulnerabilities that must be carefully managed.

No battle plan survives contact with the enemy, and the same holds true for digital systems. The key to success lies in developing flexible, resilient, and integrated systems that can adapt to the fog of war while providing clear, actionable intelligence to commanders at all levels.

For defense leaders, the challenge is clear: Create technologies and systems that harness the power of data and connectivity while remaining robust, secure, and effective in the highly complex environment of modern warfare. As the digital battlefield continues to evolve, those who can best navigate this landscape will hold the tactical advantage in future conflicts.

MACY SUMMERS has an extensive technical background with 30+ years' experience in Information Technology for government and commercial applications. Having held senior positions at Scientific-Atlanta, Pegasus Communications, and Lockheed Martin, he's an accomplished Development Executive with achievements in business development, and innovation. Over his career he has won several awards and patents, including Time Magazine's Best Inventions of The Year in 2012 and a 2011 Edison Award for Best New Product. When not at work, Macy enjoys golfing, CrossFit, and guitar.

References

https://en.wikipedia.org/wiki/Tropospheric_scatter
https://www.bluwireless.com/applications/defence-and-perimeter-security/?utm_source=PR&utm_medium=Article&utm_campaign=MicrowavesRF

to view this article online, ☞ *click here*

☞ BACK TO TABLE OF CONTENTS