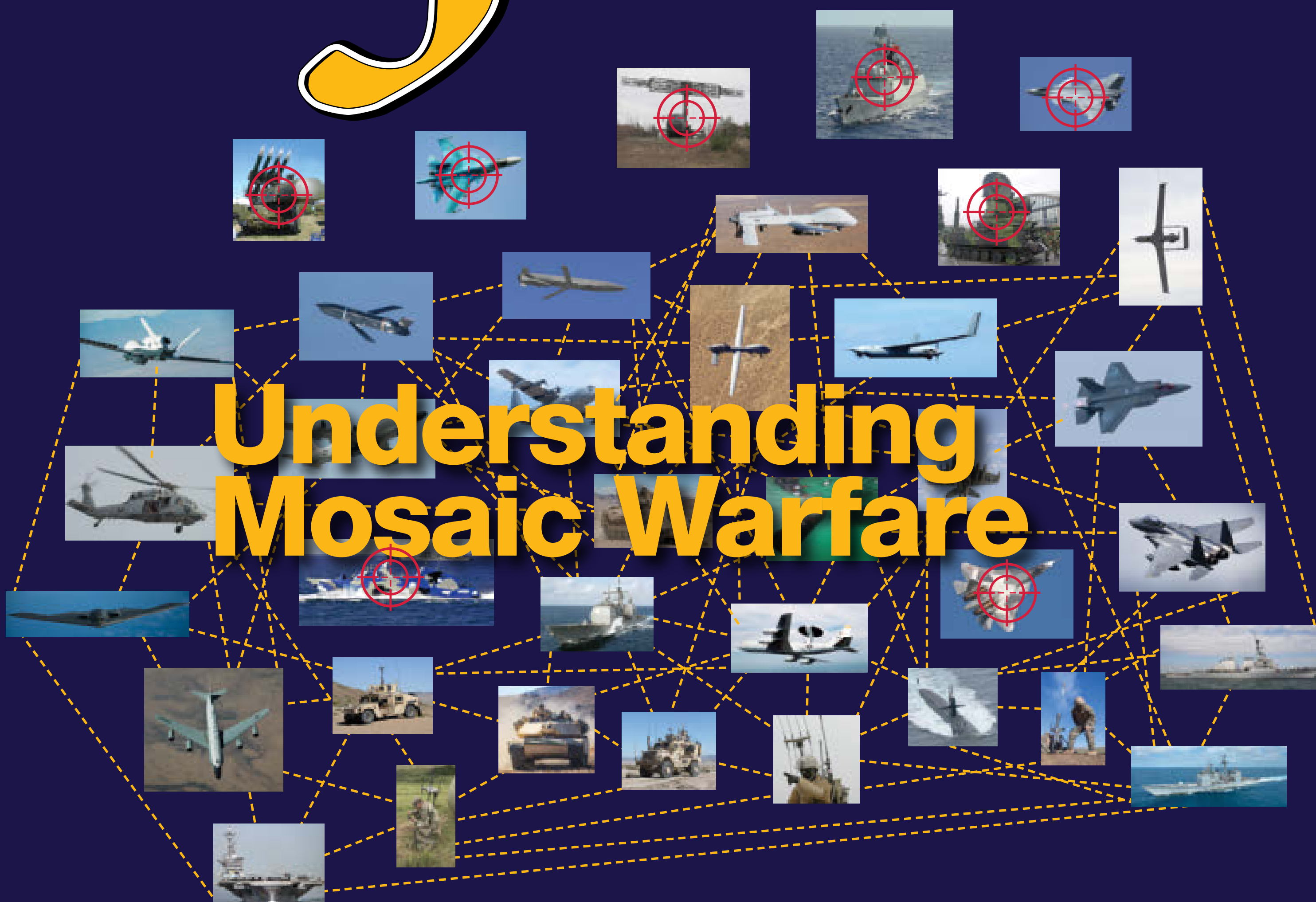
FEBRUARY 2020
Vol. 43, No. 2

ASSOCIATION OF OLD CROWS

crows.org

JED

The Journal of Electronic Defense



Understanding Mosaic Warfare

Also in this issue:

Technology Survey: FPGA Boards

EW 101: New EA Techniques

EM Domain: Cyber-EW Synergies

Highly specialised in market-leading, multi-spectral threat and countermeasure simulators, Ultra EWST strengthens naval, air force and army customers with electronic warfare testing, evaluation and training.

RWR Tester

The Ultra Radar Warning Receiver Tester is highly modular and easy to scale to meet your evolving testing needs.

- 16 Multiplexed Emitters
- 0.5-2GHz Omni port
- 2-18GHz 4 port Amplitude DF
- 10u chassis for portability
- Optional portable Calibration kit

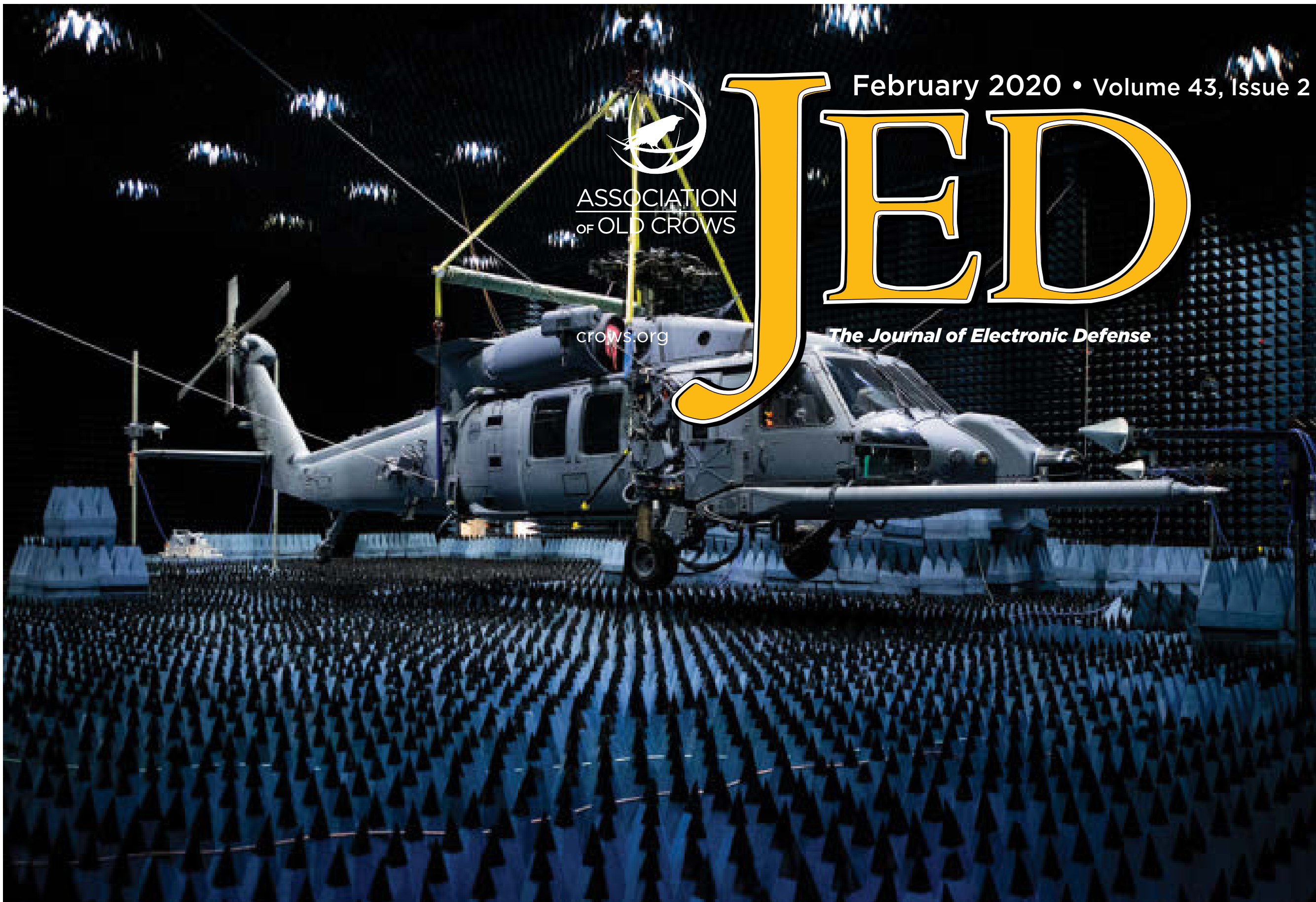
RF Photonic Link

Used in conjunction with the RWR tester to extend the reach to SUT. It can also extend distribution of RF in Laboratories, Anechoic chambers or Installed Test Facilities

- Move RF across long distances >100m
- Wideband operation 0.5-18GHz
- Low insertion loss
- Low Harmonics and Spurious
- Large Dynamic Range

Ultra ELECTRONICS | EWST

Ultra Electronics Limited - EWST
A8 Cody Technology Park, Ively Road
Farnborough, Hants GU14 0LX
Tel: +44 (0)1252 512951
Fax: +44(0)1252 512428
info@ewst.co.uk
www.ewst.co.uk



At the Joint Preflight Integration of Munitions and Electronic Systems (J-PRIMES) hangar at Eglin Air Force Base, FL, a 413th Flight Test Squadron HH-60W hangs in the anechoic chamber. The Whiskey entered the chamber for approximately seven weeks of EW systems testing.

U.S. AIR FORCE PHOTO/SAMUEL KING JR.

COVER PHOTOS COURTESY OF DOD, DMITRY ZHERDIN, TOSHIRO AOKI, AJVOL, KB RADAR, ALERT5, SRDAN POPOVIC.

Planar Monolithics Industries, Inc.

Instantaneous Frequency Measurement (IFM) & Direction Finding (DF) Assemblies & Modules

PMI offers the highest quality multi-function modules and integrated microwave assemblies for industrial and military applications that include radar warning (RW), electronic countermeasures (ECM), electronic support measures (ESM) and electronic intelligence (ELINT) systems. We built to your specifications with functions that include amplification, attenuation, filtering, switching, phase shifting, power detection, modulation, coupling, limiting and digital/analog control. PMI offers many other standard models with various options that are available at:
https://www.pmi-rf.com/categories/frequency-discriminators,
https://www.pmi-rf.com/categories/integrated-mic-mmic-assemblies

- Amplifiers - Solid State
- Attenuators - Variable/ Programmable
- Bi-Phase Modulators
- Couplers (Quadrature, 180, Directional)
- Detectors - RF / Microwave
- DLVAs, ERDLVAs & SDLVAs
- Filters & Switched Filter Banks
- Form, Fit, Functional Products & Services
- Frequency Converters
- Frequency Sources
- Frequency Discriminators & IFM
- Frequency Synthesizers
- Gain & Loss Equalizers
- Integrated MIC/MMIC Assemblies (IMAs)
- IQ Vector Modulators
- Limiters - RF / Microwave
- Log Amps
- Miscellaneous Products
- Monopulse Comparators
- Multifunction Integrated Assemblies (IMAs)
- Phase Shifters & Bi-Phase Modulators
- Power Dividers/Combiners (Passive & Active)
- Pulse Modulators - SP1T
- Rack & Chassis Mount Products
- Receiver Front Ends & Transceivers
- Single Side Band Modulators
- SMT & QFN Products
- Switch Matrices
- Switch Filter Banks
- Switches - Solid-State
- Systems - Radar Sense & Avoid
- Systems - Fly Eye Radar
- Threshold Detectors
- USB Products

Receiver Front-End IFM Systems

RSM-218-65 & RSM-618-65

https://www.pmi-rf.com/product-details/rsm-218-65
https://www.pmi-rf.com/product-details/rsm-618-65

- Broadband Frequency Coverage
- -65 dBm To 0 dBm Dynamic Range
- 100 ns Minimum Pulsewidth Handling
- Includes DC-Coupled Log Video Amplifier
- DC-Coupled Frequency Discriminator Video Outputs:
  RSM-218-65: 2.0 GHz to 4.0 GHz, 4.0 to 6.0 GHz, 6.0 to 10.0 GHz, 10.0 GHz to 14.0 GHz, and 14.0 GHz to 18.0 GHz
  RSM-618-65: 6.0 GHz to 10.0 GHz, 10.0 GHz to 14.0 GHz and 14.0 GHz to 18.0 GHz

SPECIFICATIONS

Frequency Range	RSM-218-65: 2 -18 GHz RSM-618-65: 6 - 18 GHz
Frequency Flatness	±2.5 dB Max, ±1.75 dB Typ
Dynamic Range	-65 dBm to 0 dBm
LOG Linearity	±2.5 dB Max
VSWR Input	3.0:1 Max @ -20 dBm, 2.5:1 Typ
Tangential Sensitivity	-68 dBm Max
LOG Video Output	Rise Time: 25 ns Max Slope: 50 mV/dB (±10% Max)
RF Input Power	+15 dBm
Power	+15 VDC @ <950 mA (850 mA Typ) -15 VDC @ <450 mA (275 mA Typ)
Frequency Discriminator	Accuracy: ±300 MHz Max, ±200 MHz Typ Slope: -50 mV/GHz (±10% Max)
Physical	Connectors: SMA Female Size: 5.5” x 9.6” x 1.5”

Direction Finding Modules

LBDFM-052-BD-DP & HBDFM-218-BD-DP

https://www.pmi-rf.com/product-details/lbdfm-052-bd-dp
https://www.pmi-rf.com/product-details/hbdfm-218-bd-dp

- Low Band (0.5 - 2 GHz) & High Band (2.0-18.0 GHz) Configurations
- Uni-Directional, Multi-Function Device that routes the signal present at the RF Input Connector through one of its four channels to the RF Output Connector, to amplitude modulate the input signal.
- Input and output ports can be switched to internal 50 Ohm terminations to ensure matched source and load impedance for interfacing devices during off-times and Isolation or VSWR tests.

SPECIFICATIONS

Frequency Range	LBDFM-052-BD-DP: 0.5 - 2.0 GHz HBDFM-218-BD-DP: 2.0-18.0 GHz
RF Input Signal Level Range LBDFM-052-BD-DP: +5 dBm to +8 dBm Typ, +10 dBm Max HBDFM-218-BD-DP: 0 dBm to +3 dBm Typ, +6 dBm Max	
RF Input Spectral Purity Input Spurious Levels: - 60 dBc Max Input Harmonic Levels: - 10 dBc Max	
RF Input Signal-To-Noise Ratio: 70 dB Min	
RF Output Power Level & Gain Compression: LBDFM-052-BD-DP: Power Out = +14 dBm Min at all frequencies with Input Power = +5 dBm and Attenuation set at minimum, Gain Compression at 0.9 dB Max HBDFM-218-BD-DP: Power Out = +21 dBm Min at all frequencies with Input Power = +0 dBm and Attenuation set at minimum, Gain Compression at 0.9 dB Max	
Physical	Connectors: SMA Female Size: 6.9” x 2.48” x 0.85”

Digital Frequency Discriminator (DFD)

DFD-2G18G-5512

https://www.pmi-rf.com/product-details/dfd-2g18g-5512

- Broadband frequency coverage (2 to 18 GHz)
- Incorporates conduction cooling and the ability to be mounted via screw holes located on the underside of the unit or via the wedge locks located at the top of the unit.

SPECIFICATIONS

Frequency Range	2.0 to 18.0 GHz
Frequency Accuracy	3 MHz (Peak RMS) @ 3 dB SNR Typ
Peak Frequency Error	15 MHz
Linear Bandwidth	16 GHz
Dynamic Range	-50 to +15 dBm
Max Input Power, Survival	+17 dBm CW
Mean Frequency Resolution	1 MHz
Recovery Time (After High Power Pulse Input)	100 ns Max
Control Logic:	14-Bit TTL Digital Output (Single Ended)
Physical	RF Connectors: SMA female Power/Control: 51-Pin Micro-D Calibration/Test: 15-Pin Micro-D Size: 5.98” x 5.79” x 1.28”

Analog Frequency Discriminator

FD-0518-10-118

https://www.pmi-rf.com/product-details/fd-0518-10-118

- 1.0 to 18.0 GHz frequency coverage
- Six Output Channels, Voltage vs Frequency
- Modular Design and Rugged Construction

SPECIFICATIONS

Frequency Range	1.0 to 18.0 GHz
Output Channels (6)	Channel 1: 1 to 2 GHz Channel 2: 2 to 4.2 GHz Channel 3: 4.2 to 6.1 GHz Channel 4: 6.1 to 8.7 GHz Channel 5: 8.7 to 12.5 GHz Channel 6: 12.5 to 18 GHz
Input VSWR:	2.0:1
Video Output Rise/Fall Time	20 ns Max
Video Impedance	100 Ω
Operating Input Power	+10 ± 0.1 dBm
Accuracy:	±300 MHz Typ, ±450 MHz Max
Physical	RF Connectors: SMA female TTL Control Connector: DB9 Size: 8.5”L x 5.0”W x 3.75”H

West Coast Operation:
4921 Robert J. Mathews Pkwy, Suite 1
El Dorado Hills, CA 95762 USA
Tel: 916-542-1401, Fax: 916-265-2597

East Coast Operation:
7311-F Grove Road
Frederick, MD 21704 USA
Tel: 301-662-5019, Fax: 301-662-1731

sales@pmi-rf.com • www.pmi-rf.com

ISO9001-2015 REGISTERED

MOSAIC THINKING

This month's cover story is an excellent article by John Haystead about the DOD's Mosaic Warfare concept. As John's article points out, Mosaic Warfare is not a single program but more like a family of programs being pursued by the Defense Advanced Research Projects Agency's Strategic Technology Office. The goal of the Mosaic Warfare effort is to push beyond the monolithic weapons systems the DOD relies on today and to support the transition to a new force structure that incorporates a much greater number of smaller, unmanned, autonomous, and networked sensor and weapons platforms that represent the "pointy end of the stick." The idea is to create a force with greater mass by networking these smaller, cheaper, autonomous "tiles" with each other and with the legacy weapons platforms that will launch them, fight alongside them and sometimes recover them. The result should be more sensors and more effectors for an enemy to contend with.

The way I envision what Mosaic Warfare could look like, operationally, is to imagine the DOD's current "monolithic" force structure of large manned weapons platforms (transport aircraft and bombers, surface combatants, submarines, tanks and APCs) and use them to carry hundreds, if not thousands, of unmanned autonomous platforms (unmanned air, ground, surface and subsurface vehicles) to the edge of the A2/AD threat environment and then launch them deeper into the threat environment. The unmanned platforms, collectively equipped with multi-spectral sensors, datalinks, non-kinetic effectors and hard-kill munitions, will form sensor-to-shooter networks between them – and with the larger monolithic weapons platforms. If some of these unmanned "tiles" are defeated, the remaining tiles will constantly re-form, re-assign and adapt in real-time to complete the mission, even if the mission focus changes. It sounds very "pie in the sky," but DARPA is working on some key enabling programs that can make the Mosaic Warfare vision a reality.

Ultimately, Mosaic Warfare is much more than a family of technology programs. It will push the DOD to evolve some of its most basic assumptions about force structure, personnel and warfighting. For one thing, Mosaic Warfare will certainly require the DOD to make a greater commitment to EMSO. The Mosaic Warfare concept inherently depends on the DOD's ability to access, manage and control the EM Domain throughout the A2/AD environment. Without this control, the tiles in the mosaic will become disconnected, and they will have to fight alone – if they can fight at all.

Secondly, the ability to respond to evolving mission requirements by changing the configuration and capabilities of each "tile" or weapons system is going to reside much closer to the warfighter. Not only will the small unmanned tiles will be less complex than legacy monolithic weapons systems, but the ability to write the software that reconfigures the way the tiles work together on the network is something that will become easier to achieve in the field, as well. Ultimately, Mosaic Warfare could pave the way for some interesting innovations. – *J. Knowles*

ASSOCIATION OF OLD CROWS
crows.org
JED
The Journal of Electronic Defense
FEBRUARY 2020 • VOL. 43, NO. 2

Subscription Information: Please contact Glorianne O'Neilin at (703) 549-1600 or e-mail oneilin@crows.org.

The Journal of Electronic Defense is published for the AOC by
NAYLOR
ASSOCIATION SOLUTIONS
5950 NW 1st Place
Gainesville, FL 32607
Phone: (800) 369-6220 • Fax: (352) 331-3525
www.naylor.com

COVER PHOTOS COURTESY OF DOD, DMITRY ZHERDIN, TOSHIRO AOKI, AJVOL, KB RADAR, ALERT5, SRDAN POPOVIC.
PUBLISHED JANUARY 2020/JED-M0220/1324

FEBRUARY

AOC EW Asia
February 4-5
Singapore
crows.org

Defexpo 2018
February 5-8
Lucknow, Uttar Pradesh, India
defexpoindia.in

Singapore Airshow
February 6-11
Singapore
www.singaporeairshow.com

6th International Conference on EW – EWCI 2018
February 18-20
Bangalore, India
www.aoc-india.org

EW Releasability and Export Control Workshop
February 25-26
Washington, DC
crows.org

AFA Air Warfare Symposium
February 26-28
Orlando, FL
www.afa.org

MARCH

AFCEA West Conference and Exhibition
March 2-3
San Diego, CA
www.westconference.org

Annual Directed Energy Science and Technology Symposium
March 9-13
Destin, FL
www.deps.org

DIMDEX 2018
March 16-18
Doha, Qatar
www.dimdex.com

Dixie Crow Symposium 45
March 23-26
Robins AFB, GA
www.dixiecrowsymposium.com

Robins AFB and AIC Requirements Symposium
March 26
Robins AFB, GA
https://chamber.robinsregion.com

Directed Energy to DC Exhibition (DE2DC)
March 30 - April 1
Washington, DC
www.deps.org

49th Annual Collaborative Electronic Warfare Symposium
March 31 – April 2
Point Mugu, CA
crows.org

FIDAE 2020
March 31 – April 5
Santiago, Chile
www.fidae.cl/en

APRIL

Directed Energy Summit
April 1-2
Washington, DC
www.boozallen.com/d/event/directed-energy-summit.html

Navy League Sea-Air-Space
April 6-8
National Harbor, MD
www.seaairspace.org

Defense Services Asia
April 20-23
Kuala Lumpur, Malaysia
www.dsaexhibition.com

2020 Army Aviation Mission Solutions Summit (AAAA)
April 22-24
Nashville, TN
www.quad-a.org

SPIE Defense + Commercial Sensing
April 28-30
Anaheim, CA
www.spie.orgr

AOC conferences are noted in red. For more info or to register, visit crows.org. Items in blue denote AOC Chapter events.

FEBRUARY

Radar Electronic Warfare
February 3-7
Swindon, UK
www.cranfield.ac.uk

AOC Live Professional Development Web Course: 21st Century Electronic Warfare, Systems, Technology and Techniques
February 3-21
8 sessions, 1300-1700 EST
crows.org

Communications Electronic Warfare
February 10-14
Swindon, UK
www.cranfield.ac.uk

Basic RF Electronic Warfare Concepts
February 11-13
Atlanta, GA
www.pe.gatech.edu

AOC Virtual Series Webinar: Electronic Warfare in the New Threat Environment
February 13
1400-1500 EST
crows.org

Advanced Radar
February 24-28
Swindon, UK
www.cranfield.ac.uk

Advanced RF Electronic Warfare Principles
Feb 24-28
Atlanta, GA
www.pe.gatech.edu

Principles of Millimeter Wave Radar Electronic Warfare
February 26-27
Atlanta, GA
www.pe.gatech.edu

AOC Virtual Series Webinar: Using COTS Equipment to Generate Complex Radar Signals
February 27
1400-1500 EST
crows.org

MARCH

AOC Live Professional Development Web Course: EW Modeling and Simulation
March 2-25
8 sessions, 1300-1600 EST
crows.org

Aircraft Survivability
March 9-13
Swindon, UK
www.cranfield.ac.uk

AOC Virtual Series Webinar: RF Challenges in the Modern EW Battlespace
March 12
1400-1500 EST
crows.org

AOC Virtual Series Webinar: How the West Is Losing the Navigation and Timing War – and Risking Everything
March 26
1400-1500 EST
crows.org

APRIL

Radar Warning Receivers Fundamentals
April 1-2
Atlanta, GA
www.pe.gatech.edu

AOC Virtual Series Webinar: Overview of Missile Design, Development, and System Engineering
April 9
1400-1500 EST
crows.org

AOC Live Professional Development Web Course: EW Against a New Generation of Threats
April 13-29
8 sessions, 1300-1600 EDT
crows.org

AOC courses are noted in red. For more info or to register, visit crows.org. Items in blue denote AOC Chapter courses.

message from the president

HYBRID WARFARE

This month, I'd like to expand on the editorial ("Flipping the Gray Zone") in the December 2019 *JED*. Looking at the world today as we prepare to man, equip and train for conventional warfare and the A2/AD environment, we may not have enough focus on how we equip, man and train, prepare for, or fight in today's Hybrid Warfare environment.

There are a lot of definitions out there. But, in general, Hybrid Warfare is a military strategy which employs political warfare and blends conventional warfare, irregular warfare and cyber warfare with the other influence methods, primarily social, tactical, operational and strategic information warfare. By combining kinetic operations with subversive efforts, an aggressor intends to avoid attribution or retribution. Hybrid Warfare can be used to describe the flexible and complex dynamics of the battlespace requiring a highly adaptable and resilient response.

Recent events include Ukraine, Libya, the Baltics and China's global expansion, and they involve efforts ranging from building sovereign islands to interference in national elections. Hybrid Warfare is conducted by state actors and irregular forces, and it supports the geopolitical goals of governments such as Russia, China, Korea and Iran. So where does the Electromagnetic Environment play in this? LTG Karen H. Gibson, USA, Deputy Director of National Intelligence for National Security Partnerships, stated that the difference today "…is the unprecedented ability to use information as an element of warfare with much greater volume, velocity, breadth and depth and precision than previously possible, because global IT systems have made us more connected, more automated and allowed for more precise messaging than ever before." In eastern Ukraine, we've seen Russian and separatist forces employ numerous jammers against Ukraine's VHF, UHF, and GSM communications, as well as jamming UAVs, satellite communications and GPS jamming. The Internet has been taken down, degraded, infiltrated and corrupted.

When you consider our reliance on the Electromagnetic Environment and our dependence on information in all facets of our lives, then how vulnerable are we? What capabilities have we developed or are we investing in to counter or conduct Hybrid Warfare? When you consider Hybrid Warfare and some of its dimensions – information, military, socio-political, economic, how are we organized and equipped and how are we training our forces for this? But more importantly, how are we planning and developing policy, strategy and rules of engagement at the strategic, operational and tactical levels? This specifically highlights the requirements for cyber warfare, electronic warfare, information warfare and information operations being integrated and coordinated.

The Russian concept of non-linear warfare is an example of how we need to be thinking. How do we influence or counter Hybrid Warfare? How do we employ Hybrid Warfare to influence, shape and/or prepare the battlefield utilizing political and/or military responses? This debate has been going on for decades. But as the DOD has refocused its strategy on near-peer conflict, it can't forget Hybrid Warfare and where the Electromagnetic Environment plays. – *Muddy Watters*

FEATURED LIVE COURSES

21st Century Electronic Warfare, Systems, Technology, and Techniques

Dr. Clayton Stewart

Mondays, Wednesdays, & Fridays
13:00 – 17:00 EST | February 3 – 21, 2020
This course offers a comprehensive overview of modern electronic (EW) warfare systems, technology, and techniques.

EW Modeling and Simulation

Dave Adamy

Mondays & Wednesdays
13:00 – 16:00 EST | March 2 – 25, 2020
This is a practical course in which the basic concepts and techniques of Electronic Warfare modeling and simulation are presented and applied to practical problems.

EW Against a New Generation of Threats

Dave Adamy

Mondays, Wednesdays & Fridays
13:00 – 16:00 EDT | April 13 – 29, 2020
This is a practical, hands-on course which covers Spectrum Warfare and current EW approaches, and moves on to discuss the new equipment capabilities and Tactics that are required to meet the new threat challenges.

Intermediate Electronic Warfare
EW EUROPE 2020

Dr. Clayton Stewart

Friday & Saturday | **08:00 – 17:00 BST**
June 19 – 20, 2020 | Liverpool, UK
We will begin with a historical perspective and introduce use of radar, integrated air defense system, early EA functions and conclude with an overview of modern EA, ES, and EP.

Missile Design, Development, and System Engineering

Eugene Fleeman

Mondays, Wednesdays, & Fridays
13:00 – 16:00 EDT | July 13 – 31, 2020
Missiles provide the essential accuracy and standoff range capabilities that are required in modern warfare. Technologies for missiles are rapidly emerging, resulting in the frequent introduction of new missile systems.

Electronic Warfare Signal Processing

Kyle Davidson

Mondays, Wednesdays, & Fridays
13:00 – 16:00 EDT | September 14 – 30, 2020
This course introduces students to Electronic Warfare (EW) signal processing systems and their implementation, providing a foundation in learning to solve modern EW problems.

Electro-Optical/Infrared Sensor Engineering

Dr. Phillip Pace

Mondays & Wednesdays
13:00 – 16:00 EDT | October 5 – 28, 2020
This course presents the fundamentals of electro-optical (EO) & infrared (IR) sensor technology, its analysis and its application to military search, track and imaging systems. Electronic warfare (electronic attack and electronic protection) are emphasized.

RF Theory for ES Operations

57 AOC INTERNATIONAL SYMPOSIUM & CONVENTION

Dr. Patrick Ford

Sunday & Monday | **09:00 – 17:00 EST**
Dec 6 – 7, 2020 | Washington, DC
This course will include a thorough overview of key electromagnetic spectrum (EMS) concepts, with an emphasis on the RF spectrum and commensurate propagation mechanisms and environmental impacts.

= Web Course, no travel required!

FOR COURSE LISTINGS AND MORE VISIT **CROWS.ORG**


EW Releasability and
Export Control Workshop
ASSOCIATION
OF OLD CROWS
25-26 FEBRUARY 2020
Arlington, VA

the monitor

news

US AIR FORCE TO EVALUATE OPEN ARCHITECTURE EW SYSTEMS

The US Air Force Life Cycle Management Center, Electronic Warfare and Avionics (EWA) Program Office (AFLCMC/WNY) (Warner Robins, GA) has issued a Request for Information (RFI) for electronic warfare (EW) solutions that can support its Electronic Warfare Open Architecture effort.

According to the RFI, its purpose is to "assess industry capability to design, build, and demonstrate a rapidly configurable EW system to include both Electronic Attack (EA) and Electronic Support (ES) capabilities postured for responding to software-defined, highly-agile, 21st century EW enemy systems while still addressing all legacy threats. The USAF future strategy for EW systems is for advanced, wideband EW systems incorporating a flexible architecture to enable multiple platform EW coordination for prosecuting diverse mission sets. Additionally the United States Air Force (USAF) is looking at adaptable, scalable, government-owned, modular system architectures with common interfaces. Incorporation of the latest Sensor Open System Architecture (SOSA), Open Mission Systems (OMS), Universal Command and Control Interface (UCI) standards is a must. Implementation of these standards permits multi-domain coordinated non-platform specific capabilities with an adaptable hardware and software upgrade path."

Program officials will assess the RFI responses and may invite selected companies to participate in an EW Open Architecture demonstration in June. The Air Force will provide a SOSA-compliant interface control document and backplane, and the contractor will deliver card-level ES and EA capabilities that will be "tested in government labs with direct inject of RF signals." Any demonstrations held at the unclassified level will consist of six notional signals with "generic" (unclassified) jamming techniques. Because the EW capabilities are to be demonstrated at the card level (no antennas, high-power amplifiers or open air testing), the EW Open Architecture effort is expected to draw interest from a wide range of EW businesses – large and small.

The EW Open Architecture initiative represents the Air Force's most significant effort to date in its decades-long quest to modernize its inventory of legacy EW systems. While the Air Force wants to continue to implement open architectures into its 5th-generation force structure, it also faces EW sustainment challenges across its legacy platforms as it struggles to stay on top of creeping hardware obsolescence and myriad software languages – some of which date back to the 1960s. While these challenges are not new, the issue of EW modernization has become "top of mind" for Air Force leaders over the past year. The EW Open Architecture effort is also reflected in the theme of next month's Electronic Warfare and Avionics Conference (March 24-26) in Warner Robins. The theme of the conference is "Maintaining Dominance in the Electromagnetic Spectrum (EMS) by Rapidly Fielding and Modifying Systems Using Open Standards and Innovation."

Responses to the EW Open Architecture RFI are due by February 28. The contracting point of contact for the EW Open Architecture RFI is Kesia Dawson, (478) 926-1748), e-mail lakesia.dawson@us.af.mil. The point of contact for the demonstrations is Mike Wilke, (478) 926-3539, e-mail Michael.wilke.2@us.af.mil. – *J. Knowles*

US ARMY SEEKS UAS PAYLOADS FOR SEAD MISSION

The US Army's Unmanned Aircraft Systems Program Office (UAS PO), Medium Altitude Endurance Product Manager (PdM MAE), has issued a Request for Information (RFI) for EW, SIGINT and radar payloads that could be integrated onto the MQ-1C Gray Eagle UAS to support suppression of enemy air defense (SEAD) missions.

The Multi-Domain Support Equipment RFI, released in late December, calls for three specific capabilities. The first is a radar warning receiver / electronic support measures (RWR/ESM) system that can "detect and identify Low Probability of Detection (LPI) emissions from threat radar systems, perform direction finding (Angle-of-Arrival) and precision geolocation, to provide tactical situational awareness to battlefield commanders through a digital data link and support cueing of Air Launched Effects (ALE) and Precision Fires." The system should cover 0.5-40 GHz and provide up to 2 GHz of instantaneous bandwidth "to increase probability of detection and minimize time to correct ID of modern radar threats."

The second payload type is electronic intelligence (ELINT) systems. Here, the PdM MAE is interested in ELINT systems that can perform "direction finding, precision geolocation, and raw signal data recording functions" of emissions from "LPI tactical radars and tactical Electronic Warfare (EW) threat systems" over the 0.5- to 40-GHz range.

Finally, the third payload type described in the RFI is a Synthetic Aperture RADAR (SAR) / Moving Target Indicator (MTI) that can perform wide area surveillance, imaging of stationary targets at distances up to 60 km (with enough resolution to perform target and threat identification), and detection of moving targets. The payload will provide on-board processing and will support transmission of near-real-time imagery and moving target detection data to battlefield commanders through a digital data link.

The Multi-Domain Support Equipment RFI reflects the Army's growing interest in SEAD, a mission it currently performs with its AH-64 Apache Longbow helicopters, which are being upgraded with new APR-48B RF Interferometer systems. However, the Longbow Apaches typically operate at lower altitudes and are more suited for shorter range engagements of about 8-12 km. While the Army can bring other assets such as precision artillery to bear against an enemy's medium-range air defense systems, the Army's Division commanders are mostly dependent on Joint assets to detect, identify and geolocate modern LPI, frequency-agile radars at medium-range distances. The MQ-1C, equipped with EW, SIGINT and radar payloads, could help fill this gap.

Responses to the RFI were due on January 27. The point of contact within PdM MAE is Doug Wheelock, (256) 313-2920, e-mail douglas.s.wheelock.ctr@mail.mil. – *J. Knowles*

UNICORN BLUE TO DEVELOP DIGITAL SIGNAL PROCESSING FOR PRIORITY EMISSIONS

The Air Force Research Laboratory, Information Directorate (Rome, NY) has identified a requirement for research, development, enhancement and integration of technologies to develop digital signal processing capabilities that will scan through the RF spectrum to detect high priority emissions.

Known as Unicorn Blue, the project encompasses the research, development and integration of technologies that will provide collection, detection, exploitation and geo-location capabilities of emerging signals of interest to various collection platforms.

Work will include providing real-time processing solutions and expanding the unique knowledge and experience base to automatically extract the contents of the transmissions and provide time-critical alerts and information on the signals collected. Additionally, this effort will develop prototypes that can be rapidly fielded, upgraded and transitioned to address current and emerging requirements.

A multiple-award Indefinite-Delivery, Indefinite-Quantity research and development contract is contemplated, and cost-plus-fixed-fee orders may be issued under this contract. The program is expected to run five years and is valued at $49.9 million.

The Air Force is expected to post a draft Request for Proposals (RFP) later this month. The formal solicitation is expected to be released in March 2020. The technical point of contact is Daniel Robbins, e-mail Daniel.Robbins.8@us.af.mil. – *R. Scott*

DOD ISSUES SMALL BUSINESS SOLICITATION

The Department of Defense (DOD) has released its first 2020 Small Business Innovation Research (SBIR) solicitation, which includes several EW- and SIGINT-related topics. Among the topics are:

ARMY

Integrated Radar and Electronic Surveillance (ES) system (Topic A20-016): The objective of this topic is to "design and prototype a combined radar and ES system to detect, track, and identify unmanned aircraft systems (UASs). The system should be able to detect and track a UAS system using a radar and then transition to an ES mode at a much higher bandwidth to determine the UAS link characteristics to be able to correctly identify the threat. The system should be able to interleave both ES and radar dwells, as well as have a large enough bandwidth to accommodate all UAS bands." The technical point of contact is Kerolos Nashed, (973) 724-8235, e-mail kerolos.nashed.civ@mail.mil.

High Power Coherent Beam Combined Laser for Army Platforms (Topic A20-088): This topic's objective is to "develop a high-power laser system with high beam quality utilizing coherent beam combination methods" to support high-energy laser (HEL) applications. The technical point of contact is Daniel Maytas, (256) 424-3882, Daniel.j.maytas3.civ@mail.mil.

Tactical Ultrashort Pulsed Laser for Army Platforms (Topic A20-091): The objective of this topic is to "develop an ultrashort pulse laser (USPL) system with sufficient SWaP and ruggedization" for use in high-energy laser (HEL) applications on Army relevant platforms. The technical point of contact is Daniel Maytas, (256) 424-3882, Daniel.j.maytas3.civ@mail.mil.

Sensor suite for Ground Vehicle Survivability (Topic A20-096): The goal of this topic to is to: "Develop a Hostile Fire Detection (HFD) and Active Protection System (APS) cueing and tracking sensor suite. Sensors of interest are stationary, non-imaging, multi-aperture combinations for ground vehicle threats." The technical point of contact is John Conrad, (586) 282-4292, e-mail john.b.conrad.civ@mail.mil.

NAVY

Broadband for Photonic Receiver (Topic N201-001) is a Navy project sponsored by PfM CES, PMIS, Multi-Function Electronic Warfare (MFEW) ACAT IV-M POR. This topic's objective is to "develop an innovative and operationally suitable consolidated (minimized size and weight) antenna solution for sensing and transmitting broadly across the electromagnetic spectrum." The technical point of contact is Alicia Owsiak, (703) 432-2765, e-mail Alicia.owsiak@usmc.mil.

Focused Directed Energy Antenna System (FoDEAS) for Long-Range Vehicle/Vessel Stopping with reduced overall system size, weight, power consumption, thermal cooling, and system cost (SWAP/C2) (Topic N201-002): This topic is sponsored by the Joint Non-Lethal Weapons Directorate. This topic aims to "develop a Focused Directed Energy Antenna System (FoDEAS) using high power microwave (HPM) – (wideband) frequencies to electronically attack threat vehicle and vessel engines and embedded threat electronics. It should provide long-range, non-lethal vehicle/vessel stopping capabilities with a wideband HPM antenna that incorporates frequency carve-outs that allows the use of this Non-Lethal Weapon (NLW) without interference to or with critical communication, navigation, and/or radar (frequencies) systems." The technical point of contact is David Law, (703) 432-0900, e-mail david.b.law1@usmc.mil.

Multi-Octave, High Power Efficiency Active Electronically Scanned Array (AESA) (Topic N201-012): This topic is sponsored by the NAE Chief Technology Office with the following objective: "Develop electronically steerable radio frequency (RF) transmitters over multi-octave bandwidth yet with optimum power efficiency to achieve simultaneous multi-octave bandwidth high-efficiency performance." The technical point of contact is Jean Santos, (805) 989-0582.

High Power Quantum Cascade Lasers in the Spectral Range between 3.8 and 4.1 Microns (Topic N201-013): Sponsored by the PMA272 Tactical Aircraft Protection Systems at NAVAIR, this topic's objective is to "develop quantum cascade lasers in the 3.8-4.1 micron wavelength range with high output power and brightness." The technical point of contact is Benjamin Decker, (301) 757-5396.

Mid-Wave Infrared Fiber Amplifier (Topic N201-016): Also sponsored by PMA272 Tactical Aircraft Protection Systems, this topic's objective is to "develop and demonstrate a high-power mid-wave infrared (MWIR) fiber amplifier for quantum cascade lasers (QCLs) capable of output power scaling up to 1 kilowatt (kW)." The technical point of contact is Benjamin Decker, (301) 757-5396.

The original DOD solicitation was released December 10 and opened for responses January 14. Proposals for all topics are due February 12. – *H. Swedeen*

IN BRIEF

Northrop Grumman's Common Infrared Countermeasures (CIRCM) system has successfully completed free flight missile testing at the US Army's White Sands Missile Range's Aerial Cable Range, according to the company. As part of this test, the CIRCM system was mounted on a representative aircraft fuselage, which was suspended 1,000 feet above the ground on an aerial cable. The CIRCM system was presented with engagements in both single- and multiple-shot scenarios. The cable tests mark an important milestone in the program's path to full-rate production.

✪ ✪ ✪

SRC Inc. (North Syracuse, NY) has received a $13 million contract option from the US Air Force to continue support of the Sensor Beam program. Under the contract, the company will research, analyze, technically document and perform reviews on electromagnetic systems, events and signatures required by all services and other US agencies. Work will be performed at Joint Base San Antonio-Lackland, TX, and is scheduled to run through January 2021. In other company news, Kevin Unger has been named assistant vice president of the Electronic Warfare & Signals Intelligence Solutions business unit. Unger, who has been with the company for 33 years, was previously the assistant VP of business development. Sean O'Hara has been promoted as director of the newly created Machine Intelligence and Autonomy Center of Excellence. In his previous role, he served as Technology Director, Electronic Warfare.

✪ ✪ ✪

Raytheon Missile Systems (Tucson, AZ) has received a $112.3 million contract modification for non-recurring engineering support throughout the Engineering and Manufacturing Development phase, as well as through payload integration and transition to production, for the Miniature Air Launched Decoy-Navy (MALD-N).

✪ ✪ ✪

Northrop Grumman Mission Systems (Baltimore, MD) has received a $35.2 million contract from the US Navy to produce and deliver modification kits for the ALQ-218 ES receiver on the EA-18G Growler. The kits will be installed on EA-18Gs in service with the US Navy and the Royal Australian Air Force. Deliveries are expected to be complete by May 2022.

✪ ✪ ✪

The Naval Research Laboratory (NRL) has awarded **Abaco Systems** (Huntsville, AL) a $24 million firm-fixed-price, indefinite-delivery/indefinite-quantity contract for specially developed embedded computing systems known as Multiple False Targets Box Phase two (MFTBOX2) flight units, MFTBOX Phase three (MFTBOX3) flight units, and their associated spare components. The MFTBOX2 and MFTBOX3 flight units, which will be used in fleet training exercises to train navy radar operators in modern jamming techniques during predeployment qualification trials, will be integrated with NRL-owned software to create electronic warfare jamming systems capable of generating advanced jamming techniques. The systems will be used to support EW training and readiness in both air-to-air and air-to-surface scenarios.

✪ ✪ ✪

Northrop Grumman delivered its 1,000th AGM-88E Advanced Anti-Radiation Guided Munition (AARGM) in a ceremony at its Northridge, CA, office. The AARGM has been operational with the US Navy since 2012.

✪ ✪ ✪

Leonardo DRS Electro-Optical and Infrared Systems (Melbourne, FL) has received a $7.6 million modification to an existing US Navy contract for program management, engineering and logistics support to mitigate identified risks to the Distributed Aperture Infrared Countermeasure program. Work under this modification is expected to be completed in December 2020.

✪ ✪ ✪

Scientific Research Corp. (Atlanta, GA) has received a $39.4 million modification to an existing contract to support the operations and maintenance of the ground threat systems at the Joint Base Alaska Range Complex (Eielson Air Force Base, AK). Work will be completed in May.

world report

TEMPEST RADAR RECEIVER TECHNOLOGY DEMONSTRATED

Leonardo (Luton, UK), as part of Team Tempest, has demonstrated the performance of novel miniaturized digital radar warning receiver technology as part of continuing development work for the UK's next-generation Tempest future combat air system (FCAS).

In a laboratory demonstration for the UK Ministry of Defence (MoD) and other Team Tempest partners, the new sensor "demonstrated direction finding performance of four times what is possible with a typical radar warning receiver while being just one tenth the size of a standard system," the company said.

According to Leonardo, the reduced size and weight of the new radar receiver technology, together with its reduced power requirement, means it will be possible to integrate the sensor into a multifunction array aperture. "This would potentially allow a number of multi-purpose sensors to spread around the aircraft, simultaneously sensing and tracking enemy aircraft, incoming missiles and other threats while being fully integrated with a forward-facing multimode radar," the company added.

Leonardo UK, alongside BAE Systems, MBDA and Rolls-Royce, is one of the founding members of Team Tempest, which was assembled by the MoD to develop a next-generation FCAS for the UK and partner nations. Italy and Sweden have also announced their intent to work with the UK on the Tempest program. – *R. Scott*

RAAF C-130J DIRCM UPGRADE ACHIEVES FOC

The Royal Australian Air Force (RAAF) has announced achievement of Final Operational Capability (FOC) for the upgrade of its C-130J Hercules fleet with the Northrop Grumman AAQ-24(V) Large Aircraft Infrared Countermeasures (LAIRCM) directed infrared countermeasures (DIRCM) system.

Under Project AIR 5416 Phase 4B, the RAAF has rolled out an electronic warfare self-protection (EWSP) upgrade for its 12-strong C-130J Hercules fleet that encompasses both radar warning and IR countermeasure systems. Defence's Capability Acquisition and Sustainment Group's Airborne Self Protection System Program Office has taken responsibility for program delivery.

The LAIRCM upgrade has been delivered under AIR 5416 Phase 4B2. The RAAF announced FOC on December 4, 2019, some three months ahead of schedule and significantly under budget.

Eight of the RAAF's 12 C-130J aircraft were modified in Australia by Airbus Australia Pacific under a local commercial licensing arrangement. CAE Australia has also modified the C-130J Full Flight Simulator to reflect the changes to the aircraft.

Logistics and operational support infrastructure has been constructed at RAAF Base Richmond, including a laser test firing facility, secure storage in compliance with Defence's obligations under ITAR and an updated air base security system.

Project AIR 5416 Phase 4B1 had previously addressed the introduction of the BAE Systems AN/ALR-56M radar warning receiver (RWR). Covering the C-J bands, the ALR-56M RWR employs a wideband superheterodyne receiver architecture.

Australia's DST Group provided science and technology advice in support of the levels of survivability that could be delivered by various EWSP options, including the DIRCM. DST also provided advice on the performance and advantages of several installation options, including turret location and various types of sensors for the RAAF's C-130J LAIRCM.

The RAAF has also acquired the LAIRCM system for its 12 P-8A Poseidon maritime patrol aircraft, which are being delivered trough 2023. – *R. Scott*

IN BRIEF

- Elbit Systems (Haifa, Israel) has won an initial $31 million contract to supply its Iron Fist active protection system (APS) for the Israeli Defense Forces' Eitan Armored Fighting Vehicle. The company will equip the AFVs with Iron Fist Light Decoupled (IFLD) systems, which utilize optical sensors, tracking radar, launchers and countermeasure munitions to defeat threats at a safe distance. Deliveries under the contract will be performed over a five-year period.
- RUAG (Emmen, Switzerland) announced that it has sold its "missim" handheld flightline tester to the German Bundeswehr. The device will be used to evaluate EW sensors performance on its NH-90 and Tiger helicopters. The Bundeswehr bought 16 second-generation missim systems, which stimulate the helicopters' radar warning, missile warning and laser warning sensors by simulating radars, IR guided missiles, the muzzle flash from small arms and laser-based threats.
- In mid-December, the Japanese Government approved a ¥5.23 trillion (US$48.5 billion) FY2020 budget that includes ¥15 billion ($138 million) for development of a standoff jamming aircraft, according to Kyodo News. The budget also included ¥28 billion to develop a replacement fighter aircraft for its aging F-2 fleet and ¥107.4 billion for F-35A and F-35B Joint Strike Fighter aircraft.

DARPA's Mosaic

Moving to Address the Ever-More-Rapidly-Paced

By John Haystead

Leaping well past evolutionary developmental methodologies to what represents a revolutionary new approach to maneuver warfare, the US military is pursuing a warfighting concept known as Mosaic Warfare. Under the auspices of the Defense Advanced Research Projects Agency (DARPA) Strategic Technology Office (STO), Mosaic Warfare aims to provide for an unprecedented level of autonomy and flexibility in battlefield operations through access to rapidly-composable networks of low-cost sensors, joint multi-domain command and control nodes, and all-available weapon system effectors – both kinetic and non-kinetic.

In contrast to the US military's 20th-Century reliance upon individual, monolithic military systems (bombers, large surface combatants, tanks, etc.) Mosaic Warfare allows any or all available resources (large or small, manned or unmanned) to be rapidly tailored to the requirement, adapt to dynamic threats, and be resilient to losses and attrition. Looking back to the concept's origins, and as illustrated by Dan Patt, Deputy Director of STO in 2017, "When building a mosaic, the key is the simple and versatile building blocks that artists have at their disposal from which to make complex designs. Applying the great flexibility of the mosaic concept to warfare, lower-cost, less complex systems may be linked together in a vast number of ways to create desired, interwoven effects tailored to any scenario. The individual parts of a mosaic are attritable, but together are invaluable for how they contribute to the whole. This means that, even if an adversary can neutralize a number of pieces of the mosaic, the collective can instantly respond as needed to still achieve the desired, overall effect."

Accomplishing the daunting goals of the Mosaic Warfare effort will require a major re-direction of both the DOD's current thinking regarding how threats are viewed, as well as its approach to fielding capabilities to defeat them. It demands an immediate shift from the current path aimed at developing all-inclusive "monolithic systems," that while effective for specific tasks, are highly-limited for wide-scale flexible application. Instead, the future path calls for being able to simultaneously harness, combine and apply all the available assets of all the Services to provide for an exponentially-superior and unmatchable unified operational capability.

As observed by Dr. Tim Grayson, STO Director, "Our warfighters do a great job with the operational Observe–Orient–Decide–Act (OODA) loop cycle inside the battle, but we're losing the OODA loop in terms of fielding new systems compared to what our adversaries are doing – not just fielding new capabilities, but the speed at which they're fielding these capabilities, and the speed at which they're developing and cycling (perhaps 3-5 years). Even more frightening, is that some of these adversaries have learned from the approach of Silicon Valley that says, 'Do minimum viable products, take little steps, pivot.' So, within just one of these rapidly-fielded programs, they may go through multiple cycles in a year, maybe model changes after just a few serial numbers, then they try another variant and then change again. This is not the way that we function today."

"Mosaic Warfare is a growing and evolving portfolio of programs," explains Grayson.

MONOLITH BUSTING

Dr. Grayson explains how Mosaic Warfare is being developed to address this capability gap, and the overall driving principle that will make it possible. "Within our Mosaic Warfare theme, we have a subtitle called 'Monolith Busting,' and there's already a lot of discussion within the DOD about 'Joint All-Domain C2,' or 'Joint All-Domain Battle,' which is focused on the notion of replacing monolithic platforms with distributed sets of capabilities. So, instead of saying, I've got to have a monolithic, self-contained effects chain on a particular platform including the sensor, all the C2 capabilities, and the actual effector, be it a kinetic weapon or non-kinetic effect, the System-of-Systems (SOS) approach says we're going to distribute it instead. And, we're going to allow those things to be pieced together – i.e., whatever is the best sensor, is going to provide me the targeting for whatever the best effect is."

In fact, as pointed out by Dr. Grayson, "By 2018, convincing the DOD of the value of SOS and moving away from monolithic platforms was all of a sudden not an issue anymore." But, he emphasizes, Mosaic Warfare goes beyond just busting monolithic platforms, and it includes busting monolithic architectures as well. In fact, says Grayson, "The danger we see, and this is really the motivation behind Mosaic Warfare, is that there's a risk in the enthusiasm toward SOS, that we replace monolithic plat-

Warfare

Advances/Changes in Fielded Threat Capabilities

forms with monolithic SOS architectures – replacing vertical stovepipes with horizontal stovepipes. In some ways, this is even worse, because the operational complexity of these monolithic SOS architectures grows significantly, as does the risk and the cost."

In any event, Grayson says there will always be a lot of questions about what future architectures will be. "Developing an architecture is really hard, and because it's really hard, there's a danger in trying to decide today what an architecture is going to be that will last us for the next 20 or 30 years. Because of this, if we design and build architectures the way we design and build an F-35 or any other major weapon platform, we're going to be in big trouble. Instead, what we're trying to do with Mosaic Warfare is bust monolithic architectures. With a mosaic, I can take whatever tiles I think might be relevant and combine them to get to a desired effect – providing more diversity of options for the warfighter, but at a speed that allows adaptation, ideally at the time of need."

Mosaic Warfare actually embodies and attempts to bring to fruition a number of long-recognized principles regarding the most effective (implementation of) maneuver warfare together with comprehensive and flexible operational capabilities. One of these is 'Jointness,' or real-time sharing and efficient implementation of all available tactical resources among the Services to best meet immediate battlefield requirements. In fact, one of the fundamental themes within the Mosaic Warfare concept is the notion of federated capabilities – not being locked into one particular architecture. Another overriding principle is that of Multi-Domain Operations (MDO), and Mosaic Warfare

Figure 1: DARPA STO delineates the challenges associated with realizing Mosaic Warfare capabilities into three categories: Planning and Composition; Interoperability; and Execution. Icons indicate where DARPA STO has an existing program. Blank spaces are where DARPA is interested in additional ideas and potentially new programs. FROM A PRESENTATION BY DR. TIM GRAYSON, DARPA STO, AT THE 56TH AOC INTERNATIONAL SYMPOSIUM AND CONVENTION IN OCTOBER 2019.

is seen as an important enabler for the new Joint multi-domain concepts that the Services are pursuing at both the operational and tactical levels.

DEFINING THE CHALLENGE

Although Mosaic Warfare is a major focus area for DARPA's STO, it is actually not an identifiable program in and of itself. Rather, it encompasses a number of existing DARPA programs, past efforts, and new startups. Says Grayson, "Mosaic Warfare is a growing and evolving portfolio of programs. Because 'we have to eat our own dog food,' so to speak, the way we're building this portfolio is in fact as a federation of programs. As such, I'm not going to guarantee you that, on a given day on the calendar, that I will deliver you Mosaic Warfare. Instead, we're asking what are the functions needed to enable this vision. Where do those functions line up against the problem that by itself is useful to a warfighter today, and where we have a traditional transition path identifiable for that particular capability. In aggregate, they're moving us in this direction of Mosaic Warfare and toward more dynamic battlefield adaptation."

In outlining the overall plan and structure of the Mosaic Warfare effort, Grayson says, "Our overarching principle, in creating and managing Mosaic Warfare-relevant programs, is to both focus on the major long-term vision of Mosaic Warfare and how a program's capability contributes to it, but also to make sure that it serves as a traditional DARPA program with demonstrable stand-alone value, that solves someone's problem, and has a customer to potentially transition to, even if Mosaic Warfare never happens. In this way, while we're advancing individual technological capabilities, at the same time, we're setting the table for a future where the DOD will be able to put together these Mosaic Warfare strategies."

DARPA delineates the challenges associated with realizing Mosaic Warfare capabilities into three categories (See **Figure 1**). As outlined by Grayson in very general terms, "They are Planning and Composition, which is how to decide what a particular SOS architecture will be; Interoperability, which is how to actually connect the machines together; and Execution, which is how to hand this new complex architecture to a bunch of warfighters and have them actually fight with it."

An essential principle in Mosaic Warfare is "monolith busting," or supplementing large manned weapons systems, such as this Ticonderoga-*Class cruiser, with distributed sets of capabilities.*

US NAVY

ADAPTING CROSS-DOMAIN KILL-WEBS (ACK)

One DARPA STO program of particular relevance and importance to the Mosaic Warfare effort is "Adapting Cross-Domain Kill-Webs (ACK)**."** Falling within the Execution category, DARPA describes the goal of the ACK program as "assisting military decision-makers with rapidly identifying and selecting options for tasking – and re-tasking – assets within and across organizational boundaries. Specifically, ACK will assist users with selecting sensors, effectors, and support elements across military domains to form and adapt kill webs to deliver desired effects on targets. ACK will enable multiple warfighters to define distributed effects and adapt them at up to combat speed using a shared set of resources. This will create greater lethality by pairing the right sensor and weapon together for a given target and operational problem, and will create greater resilience by enabling rapid substitutions if a capability is lost."

Grayson says ACK is right at the core of Mosaic Warfare. "At the standalone level, you can view it as a new set of decision aids that would sit at any of the Service's current C2 centers to help with the allocation and tasking process – target/sensor/datalink/weapon pairing – but as it relates to Mosaic Warfare, it really is the engine." As described by Grayson, everything in the battlespace can be viewed as an ACK entity – from an individual platform, an EW pod, an infantry company, to an entire satellite constellation. "ACK gives us the tools to abstract those different capabilities in the battlespace in a very modular manner that we can then give tasking to."

In terms of an EMS Operations (EMSO) example, Grayson says, "Let's assume I'm a warfighter who knows nothing about spectrum or EW. In fact, I don't need to, because I have my ACK 'chiclet' that says deliver a non-kinetic effect against this target, and ACK will generate tasking to some appropriate module, such as an EW pod. It greatly simplifies what an operator needs to know."

"By 2018, convincing the DOD of the value of SOS and moving away from monolithic platforms was all of a sudden not an issue anymore."

CASCADE

Another significant program contributing to Mosaic Warfare is the Complex Adaptive System Composition and Design Environment (CASCADE). The CASCADE program is aimed at addressing shortcomings in modeling SOS architectures and at fundamentally changing how systems are designed for real-time resilient response to dynamic, unexpected contingencies.

A Planning and Composition category program, CASCADE feeds technology into another program within the same program office known as Proteus. As described by Grayson, "At the simplest level, Proteus helps operators sort through the many possible choices regarding what capabilities to put into an SOS architecture on the fly.

Proteus is being developed in partnership with the Marine Corps, and as told by Grayson, although they are only about halfway through the effort, "In the spirit of providing a minimum viable product, the Marine Corps loves it already. They see it as a great experimentation tool where they can sit at a battlelab or Marine Corps University, and experiment with new force-structure constructs and new tactics."

Grayson views Proteus as an excellent example of how an ongoing research program can potentially seamlessly transition to a program office that can then move the capability into more of an operational battle planning/battle management tool. "We would love to get to the point someday where a theater commander can look at a problem that they have today, recognize that they don't have exactly the right force structure in place, and then just go ahead and build a new force structure on the fly.”

DyNAMO

One program within the Interoperability category is Dynamic Network Adaptation for Mission Optimization (DyNAMO). As stressed by Grayson, available and flexible communications and networking are critical to the vision of Mosaic Warfare. “If I can’t actually connect boxes, I can’t go in and do this notion of a dynamic architecture. DyNAMO allows us to build networks of networks. Instead of rolling out a hugely expensive, entirely new network or communication standard, we’re saying, how can we create a network-of-networks that allows links to be formed across existing federated, heterogeneous tactical networks? This capability creates the abstraction that actually forms that virtual network link, it also does the routing – vision driven routing – that says here is the list of publishers and subscribers based upon a battlefield profile, and it figures out how to route the data based upon need. And, because these are very heterogeneous networks, with very different performance characteristics, it also provides the ‘throttle’ to figure out what’s the most high-priority data that has to go through at low latency, where maybe other things can be buffered or dropped. Instead of just looking at getting more bandwidth or more spectrum, DyNAMO looks at how to best use what we have more efficiently and effectively.”

ACK will assist users with selecting sensors, effectors, and support elements across military domains to form and adapt kill webs to deliver desired effects on targets.

In principle, DyNAMO can be seen as an ACK service that serves to figure out how to stitch together physical tactical networks and route data over them. As Grayson observes, “The objective is definitely not to make ACK decision makers experts in comms, having to make choices about how to hook together five different data links. You just want them to be able to say, I don’t care where the data links come from, just go ahead and connect Point A to Point B.”

ARCHITECTURES-ON-DEMAND

Dr. Grayson describes the System of Systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES) program as “one of the most profound and transformative things we have relative to Mosaic Warfare in terms of the way it’s actually transitioning into users’ hands.” Initially developed under DARPA’s System of Systems Integration Technology and Experimentation (SoSITE) program, STITCHES is a software tool that allows warfighters to automatically connect multiple, diverse, federated systems and capabilities, translating between different standards and software where interoperability doesn't already exist.

With regard to the general notion of open systems and interoperability standards, Grayson says, "We love standards and love that they exist," but he adds that, "We also have absolutely zero confidence and an extreme cynicism that we will ever figure out how to do universal global standards." Grayson says to "think of STITCHES as a kind of compiler, where a warfighter can go in and say, here are the five black boxes that I want to use for this mission today and I need exactly three out of ten functions from each of them, not every function, to fight the fight today. A maintainer then hits compile and the STITCHES tool automatically generates the glue software."

STITCHES has actually been tested over the last two years in what are called "gauntlets," which, as described by Grayson, are 'integration hackathons' where program offices and vendors come to participate with their individual payload capabilities (a gauntlet can include anywhere from 5-25 systems). At the same time, there are operators that come in to provide various operational scenarios and to define notional SOS architectures. Together with advice and support from the STITCHES software team, software engineers are then able to layout the architecture that the operators have defined and STITCHES will then auto-generate a stack of software that translates between those different payloads and instantiates the architecture.

From his perspective, Grayson sees the STITCHES model as an ideal example of how to avoid the traditional time-consuming acquisition and program office approach to delivering these types of architectures. "We can provide a tool that can ultimately be used close to the operational edge to generate architectures on demand."

The STITCHES program, under Lt. Col. Jimmy "Rev" Jones, has already been working with multiple Services to introduce their personnel to the tool, demonstrating its utility to operational elements and to their maintainers and depot support functions. As explained by Grayson, "The objective is to teach them how to use the tool and then to just leave it with them. We've already seen this happen scuccessfully in the course of some of our gauntlets, so the hope is that over the course of the next FYDP, there will be such an ecosystem in place as well as sufficient communities of interest among these STITCHES users, that it will be self-sustaining at that point."

Manned-unmanned teaming – something DARPA has explored in its SQUAD-X program – is an important aspect of the Mosaic Warfare concept. DARPA

GAINING NEW INSIGHTS

Dr. Grayson highlights one particularly interesting insight that has been revealed repeatedly as they implement some of the contributing programs to Mosaic Warfare. "We're actually finding that Mosaic Warfare isn't just about machine to machine and connecting sensors to effects, it applies to human beings as well. For example, with regard to planning, there's a fundamental human condition that the more options you give a human being, the harder it is to make a choice. This is one of the first things that we need to address. Today, this is not even considered a technology problem, but rather as a battle-planning or mission problem – a doctrine-development problem that happens in battle labs and wargames. We're looking at how technology applies to this area." In terms of execution, on the one level, the goal is to make the machines as easy to use as possible, because a lot of the button pushing and complex technical skills get automated and abstracted away. At the same time, however, we're also allowing the human to learn faster what his or her new operational or tactical duties are. So we're doing a lot of things maybe even converging into training within that execution column, and we think there is a heck of a lot of technology in that execution column that involves AI and automation."

Another overall insight from their Mosaic Warfare development work, says Grayson, is that "Architecture is a very overloaded word." To avoid confusion, Grayson says he likes to use the term architecture to refer to the actual weapon systems, the way the weapon systems are put together, and how they are used for a particular combat need. Separate from this, he likes to discuss architecture in the context of tools and infrastructure. "This is where we're heavily focused. We're not trying to define the warfighter architecture, but to define the tools and infrastructure that enable the warfighter to build those architectures."

Grayson says his "dream endstate is to get to the point where the questions about what is the architecture are left to the warfighter at the operational edge at the time of need. As a result, the uncertainty over what is actually needed is taken off the table. The warfighter can simply say, 'I know my enemy, I know my mission objectives, and I need exactly this capability.' We're trying to build the enabling core technology, tools, and infrastructure to try to move in that direction – to enable the warfighter to create architectures-on-demand."

"Integrating Force Level EW Capabilities with Kinetic Fires to Achieve Distributed Lethality"

Conference Objective:

The National Defense Strategy and the update to the Chief of Naval Operations Design for Maintaining Maritime Superiority identify the need to deliver warfighting solutions to achieve distributed operations and enable an integrated Naval Force structure as an urgent priority. This year's conference will focus on the Electronic Warfare gaps and enabling technologies required to develop distributed Force Level Electronic Warfare capabilities, integrated with kinetic fires, in order to provide enhanced platform survivability and lethality. EW and military leaders from across the Department of Defense will present EW warfighting gaps and requirements for integrated, multi-domain system of systems EW solutions and motivate the EW community to explore innovative concepts and agile solutions to address their needs. The forum will provide a Joint Services venue for EW professionals across DoD, Industry and Academia to gain insight on emerging technologies, digital engineering methodologies and capabilities that will enable distributed lethality.

FOR MORE DETAILS, VISIT CROWS.ORG/CAPABILITYGAPS2020

NEW FOR 2020: Live Testing Demo Opportunities Available! See website for details

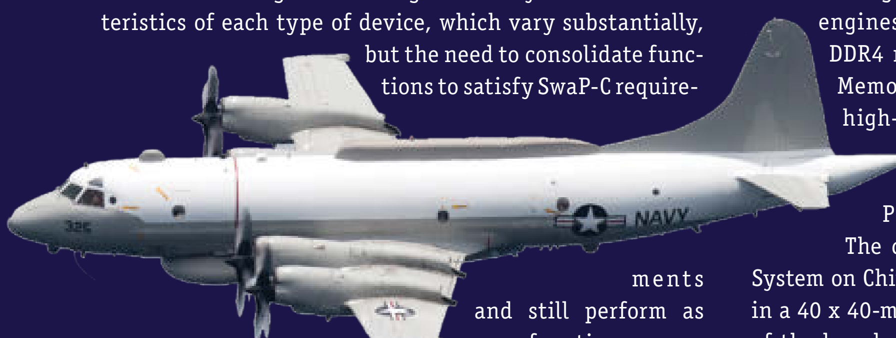
TECHNOLOGY SURVEY

A SAMPLING OF FPGA BOARDS

By Barry Manz

The term, "digital signal processing" (DSP) entered the dictionary as a generic term referring to the processing of information as bits rather than a continuous stream of analog information. At the time, DSP was performed using discrete components until Texas Instruments introduced the first single-chip DSP in 1982 (used in the company's Speak & Spell), a field it dominated for many years. The story is entirely different today, as DSP is a core function in almost all electronic consumer, commercial, and defense products, and it is being performed not just by dedicated DSPs, but by ASICs, GPUs, FPGAs and CPUs.

What's driving this trend goes far beyond the characteristics of each type of device, which vary substantially, but the need to consolidate functions to satisfy SwaP-C requirements and still perform as many functions as possible within a given form factor, subsystem or system. Not surprisingly, EW, SIGINT, radar, and other data-intensive applications are some of the most demanding applications driving this consolidation, as boards must increasingly capture, convert, process and analyze, reconvert, store and offload this data.



So the "DSP board," once dedicated solely to this function (and still offered by many vendors), has largely been absorbed within multi-device, multi-function embedded systems that use an Arm, Intel, or other CPU as the host processor, one or more FPGAs, a high-speed memory infrastructure, and the required ADCs and DACs and increasing amounts of very fast I/O. In some cases, the host processor is integrated within the FPGA to perform various administrative tasks, although as a programmable logic device rather than an ASIC like a CPU, it's generally not as well suited for this purpose in many cases.

And that's just the beginning, as DSP has become an assumed function within many board-level products, which today sometimes form a complete subsystem up to and increasingly including RF functionality. Connect them to a signal source at the front, and storage and high-speed buses at the back, add software and custom IP, and there's not much else required to create a formidable platform, from which to build a more extensive application-specific system if desired.

As becomes immediately obvious from a quick look at our latest survey, the FPGA is the major disrupter as it gobbles up functions previously performed by other devices, so much so, there isn't a single product on this list without at least one, and often two or three, FPGAs. That's not surprising considering the latest capabilities of today's FPGAs.

A great example is the VU19P within the Xilinx UltraScale+ family, the world's largest FPGA, with 9 million logic cells, a quad-core Arm Cortex-A53 and Arm Cortex R5F real-time processor, up to 12,000 DSP slices with up to 22 x10 trillion operations per second fixed- and floating-point performance, multiple encryption engines and secure boot, 500 Mbytes of on-chip DDR4 memory and 16 Gbytes of High Bandwidth Memory (HBM) with 460 GB/s bandwidth, 80 high-speed serial transceivers with total bandwidth of 4.5 Tb/s bandwidth, as well as I/O for USB, Ethernet, and eight lanes of PCIe Gen. 4, I2C. communication.

The company has taken this further with its RF System on Chip (RFSoC), a complete software-defined radio in a 40 x 40-mm BGA package, which can be found in a few of the boards in the survey. The device incorporates both ADCs and DACs, (formerly on their own and connected with JESD204B or LVDS), a major step toward "total" functional integration while accommodating SWAP-C.

Most recently, the company has introduced VERSAL, an "adaptive compute acceleration platform (ACAP)" that combines multiple hardware processing platforms (CPU, FPGA, and vector processors) and software programmability to make life easier for designers while providing 20 times the performance of current FPGAs and 100 times the performance of CPUs, a bold claim indeed.

The device's vector engines are very interesting, as they mark the first time these processors have been used in an FPGA, and offer the unique benefits of this technology that made them the "go-to" solution for supercomputers until the momentum behind commercial use of scalar processors pushed them to the side.

Over the past decade, the FPGA has taken the embedded world by storm, along with, in some cases, the GPU (or when combining functions, a general-purpose GPGPU), and the DSP board is rapidly becoming a "digital processing board" instead, as so many different processing functions are performed by them today. And buried within these extraoral complex devices is an essential ingredient – DSP functionality.

FPGA BOARDS

MODEL	FUNCTION	PROCESSOR TYPE	MEMORY	FORMAT
Abaco Systems; Huntsville, AL, USA; +1 866-652-2226; www.abaco.com				
VP460 Direct RF Processing System	EW, SIGINT, COMINT, ELINT, Radar	Xilinx® Zynq® Ultrascale+™ RF system-on-chip (RFSoC) and the latest Xilinx® Virtex™ Ultrascale+ High Bandwidth Memory (HBM) FPGA device	Up to 8 GB DDR4 memory available to the RFSoC; up to 12 GB DDR4 memory available to the Virtex UltraScale+™	VPX 6U
VP430 Direct RF Processing System	EW, SIGINT, COMINT, Radar, ELINT	Zynq® UltraScale+™ RFSoC	Two 64-bit 4GBytes DDR4 (8GB total) memory blocks. Up to 2400 Mb/s; RFSOC - 256KB on-chip with ECC	VPX 3U
FMC172 Wideband Low Latency FMC Module	DRFM, SDR, Radar, Sonar, EW	*	*	FMC HPC
Acromag; Wixom, MI, USA; +1 248-295-0310; www.acromag.com				
XMC-K7	COMINT, ELINT, adaptive filtering	FPGA, Xilinx® Kintex-7	8Gb (128M x 64-bit) DDR3 SDRAM; 512Mb (32M x 16-bit) parallel flash	XMC
XMC-A7	COMINT, ELINT, adaptive filtering	FPGA, Xilinx® Artix-7	8Gb (128M x 64-bit) DDR3 SDRAM, 512Mb (32M x 16-bit) parallel flash	XMC
Alpha Data; Golden, CO, USA & Edinburgh, UK; +1 303-954-8768; www.alpha-data.com				
ADM-VPX3-9Z2	Radar/Sonar Beamforming ELINT/ISR Image/Video Processing/Machine Vision DSP Data Encryption	Xilinx® Zynq® UltraScale+™ MPSoC - ZU15EG	8GB DDR4, 32GB SSD, 2Gb QSPI Flash, uSD Flash Slot	3U VPX (OpenVPX
ADM-XRC-KU1	Configurable platform for multiple applications including SIGINT, EW and image processing	Xilinx® UltraScale™ - KU060 or KU115	8GB DDR4, 2Gb QSPI Flash	XMC (VITA 42, VITA 61
ADM-XRC-9R1	EW, Radar, SIGINT, MIMO (5G), Signal Detection / Jamming	Xilinx® Zynq® UltraScale+™ RFSoC - ZU27DR	4GB DDR4, uSD Flash Slot, 1Gb QSPI Flash	XMC (VITA 42, VITA 61
Annapolis Micro Systems, Inc.; Annapolis, MD, USA; +1 410-841-2514; www.annapmicro.com				
WILD FMC+ GM60/61/62 ADC & DAC	EW, ELINT, phased array radar, SDR, SIGINT, COMINT, DRFM, beamforming	Xilinx Zynq UltraScale+™ RFSoC (ZU27DR, ZU28DR, ZU47DR, ZU49DR or ZU58DR)	2 GB of LPDDR4 DRAM	WILD FMC+
WILDSTAR 3XBM/3XB0 3U OpenVPX FPGA Processor	EW, ELINT, phased array radar, SDR, SIGINT, COMINT, DRFM, beamforming	Xilinx® Zynq® UltraScale™ (XCKU115) or Virtex UltraScale+™ (XCVU5P or XCVU7P or XCVU9P) plus Xilinx® Zynq® UltraScale+™ MPSoC (XCZU7EV)	Up to 10 GB of DDR4 DRAM and up to 40 GB/s of DRAM bandwidth	3U OpenVPX
WILDSTAR 6XB2/6XBU 6U OpenVPX FPGA Processor	EW, ELINT, phased array radar, SDR, SIGINT, COMINT, DRFM, beamforming	2 Xilinx® Zynq® UltraScale+™ (XCVU9P or XCVU13P) plus Xilinx® Zynq® UltraScale+™ MPSoC (XCZU11EG or XCZU19EG)	Up to 29 GB of DDR4 DRAM and up to 125 GB/s of DRAM bandwidth	6U OpenVPX

	I/O, INTERFACE/BS TYPES	ENVIRONMENT	POWER	FEATURES
	PCIe Gen3 x 16 links from HBM to the backplane and x8 from the RFSoC; 16x MGT lanes capable of PCIe Gen3 to the backplane; 16x MGT lanes capable of 10/40GigE; and more	Operating temp.: 0°C to + 55°C	145W (typ)	ADC 16 channels 2 GSPS 12-bit; DAC 16 channel 6.4 GSPS 14-bit; low latency, high-bandwidth parallel data bus between the Zynq UltraScale+ RFSoC and Virtex UltraScale+ HBM devices; user I/O to backplane RTM; Linux® and Windows® BSP available; SOSA backplane option; convection cooled
	PCIe Gen3 x8; 1000BASE-BX; 16 LVDS pairs; DisplayPort™; SATA 3.1; VITA 66.4 8x FireFly™ Optical Interface for transfers up to 12GB/s; 12-position NanoRF RF-to-the-backplane	Operating temp.: 0°C to +55° C (commercial); -40°C to +70° C (Industrial)	40W (typ), 70W (max)	ADC 8-channel 4GSPS 12-bit; DAC 8-channel 6.4GSPS 14-bit; application processing unit; quad-core ARM Cortex-A53; real-time processing unit; dual-core ARM Cortex-R5; up to 8 GBytes DDR4; single serial BLAST site
	VITA 57.1 FMC compliant	Operating temp.: 0°C to +55° C w/ 400LFM (commercial); -40°C to +70° C (industrial)	<14W (typ), <16W (max)	AC-coupled analog signals; 5 SSMC front panel connectors; sampling frequency and calibration through I2C communication; flexible clock tree enables internal clock source and external reference clock; trigger signal to enable multi-board synchronization; power-down modes to switch off unused functions for system power savings; air cooled; conduction-cooled version available
	I/O: LVDS, SFP+, 10GbE, A/D, D/A, TTL, CMOS, RS485; Bus: VITA 42, P15 (PCIe Gen 2, Serial RapidI/O, 10GbE, Aurora)	Air-cooled: -40°C to 55°C; conduction-cooled: -40°C to 70°C; Storage: -55°C to 125°C	3.3V (±5%): 7.8W typical. 12V (±5%): 2.7W typical. 3.3V AUX (±5%): 57µW	Available with plug-in front I/O module (A/D, D/A, DIO); dual SFP+ ports for 10GbE or Fibre Channel; or conduction-cooled rear I/O
	I/O: LVDS, A/D, D/A, TTL, CMOS, RS485; Bus: VITA 42, P15 (PCIe Gen 2, Serial RapidI/O, 10GbE, Aurora)	Air-cooled: -40°C to 55°C; conduction-cooled: -40°C to 70°C; Storage: -55°C to 125°C	3.3V (±5%): 7W typical. 12V (±5%): 2W typical. 3.3V AUX (±5%): 57µW	Available with plug-in front I/O module (A/D, D/A, DIO) or conduction-cooled rear I/O
)	VITA 57.4 FMC+, VITA 66.4 Optical	-4°C0 to +70°C (Air-Cooled), -40°C to +85°C (Conduction Cooled)	25-50W (application dependent)	Integration of SBC and FPGA functionality into a single 3U slot; quad-core ARM A53 application processor; dual-core ARM R5 real-time processor
)	Alpha Data XRM I/O modules: Analog, Video, Optical, Comm, GPIO…	-40°C to +70°C (Air-Cooled), -40°C to +85°C (Conduction Cooled)	15-40W (application dependent)	Comprehensive SDK with Linux, VxWorks, and Signed Windows device drivers
)	Multi-giga-sample RF data converters	-40°C to +70°C (Air-Cooled), -40°C to +85°C (Conduction Cooled)	20-45W (application dependent)	8x 4GSPS 12-bit ADCs; 8x 6.4GSPS 14-bit DACs; ARM® Cortex™-A53 processing subsystem
	50Ω SSMC or VITA 67	Air cooled; Operating: -40˚C to +70˚C; Storage: -65˚C to +105˚C	Up to 60W	ADC Performance: 2/4/8 Channels, 5.0 GSps, 14 bits; DAC Performance: 2/4/8 Channels, 10.0 GSps, 14 bits; BSP: Open Project Builder or VHDL; Linux and VxWorks; suitable for UAVs, backpacks, handheld devices, and custom-integrated applications
	Front panel I/O: WILD FMC+ 32 HSS and 100 LVDS connections; backplane I/O: VITA 66 & VITA 67 connectivity; Up to 20 HSS lanes; 2 PCIe Gen3 4x HSS connections; up to 16 LVDS lines; half-size 8- or 12-contact VITA 67.3 NanoRF connection	Operating: -55˚C to +85˚C; Storage: -65˚C to +105˚C	50-175W per slot	Aligns with SOSA Technical Standard and is 100GbE-capable; BSP: Open Project Builder or VHDL; Linux and VxWorks; air, conduction, or air-flow-through cooled
	Front Panel I/O: 2 WILD FMC+ 32 HSS and 100 LVDS connections; Up to four x4 FireFly optical transceivers (VITA 66); Backplane I/O: VITA 66 & VITA 67 connectivity; 38 HSS lanes; 2 PCIe Gen3 8x HSS connections; 32 LVDS and 8 single-ended lines	Operating: -55˚C to +85˚C; Storage: -65˚C to +105˚C	50-300W per slot	Aligns with SOSA Technical Standard and is 100GbE-capable; ADC Performance: 2 channels at 32.0 GSps and 4 channels at 16.0 GSps, 10 bits; BSP: Open Project Builder or VHDL; Linux and VxWorks; air or conduction cooled

FPGA BOARDS

MODEL	FUNCTION	PROCESSOR TYPE	MEMORY	FORMAT
ApisSys; Archamps, France; +33-450360758; www.appissys.com				
AV125	12-BIT 4.5 Gsps ADC, DAC, wideband radar transceiver, EW DRFM	Xlinx® Kintex Ultrascale™ KU115	800 MHz 2 x 256M64 DDR3 SDRAM	3U OpenVPX
AV122	Octal 14 bit 3 Gsps ADC Phased-Array-AESA Radar Receiver EW-ESM-MIMO, COMINT	Xlinx® Kintex Ultrascale™ KU115	800 MHz 2 x 256M64 DDR3 SDRAM	3U OpenVPX
AV129	Single-board computer	Xlinx® Zynq® 7030 or 7045	256M32 DDR3 SDRAM	3U OpenVPX
Colorado Engineering, Inc. (CEI); Colorado Springs, CO, USA; +1 719-388-8582; www.coloradoengineering.com				
Crestone Model #: 3DR-S5-T4240	DSP, radar receiver/exciter, EW/EA Systems, ELINT, COMINT, remote sensing	FPGA: Altera Stratix V (5SGS-ED8N1F45I2N); Power PC: Freescale T4240	DDR3: 12GB DDR3@1600; MT/s (3 memory controllers with 4GB each); NAND flash: 512MB	Proprietary 3DR F
Thunder II Model #: 3DR-A10-DAC-12.6 GSPS	DSP, radar exciters and digital waveform generation (DWG), EW/EA Systems, ELINT, COMINT	FPGA: Intel Arria 10 10AX115U3F45E2SG	DDR3: 4GB; NOR Flash	Proprietary 3DR F
Lightning II Model #: 3DR-A10-ADC-3GSPS	DSP/ data acquisition, radar receiver, digital array processing & beamforming, EW/EA	FPGA: Altera Arria 10 10AX115U2F45I2SG	DDR3: 4GB; NOR Flash	Proprietary 3DR F
Curtiss-Wright Defense Solutions; Ashburn, VA, USA; +1 613-254-5112; www.cwcdefense.com				
VPX3-534	User configurable for EW, SIGINT, RADAR, SDR and DRFM applications	Xilinx KU115 FPGA with dual ARM CPU based MPSoC	On FPGA memory and 8GB DDR4 SDRAM for ARM/MPSoC	3U VPX
Delphi Engineering Group, Inc.; Irvine, CA, USA; +1 949-537-7701; www.delphieng.com				
PCU-085/115	PCI Express FPGA Carrier Board	Kintex UltraScale™ KU085/KU115	16 Gbytes DDR 4 @ 2400 MB/s	PCI Express Gen 3
VPU-085/115	3U VPX FPGA Carrier Board	Kintex UltraScale™ KU085/KU115	8 Gbytes DDR 4 @ 2400 MB/s	VITA 46, VPX
PC7-690	PCI Express FPGA Carrier Board	Virtex 7 VX330T/690T	8 Gbytes DDR 4 @ 2400 MB/s	PCI Express Gen 3
Dynamic Signals LLC; Lockport, IL, USA; +1 815-838-0005; www.signatec.com				
Signatec PX1500-4-SP95	High-speed digitizer	Xilinx® Virtex-5 SX95T	2 GB	PCI Express PC Ca
Signatec PX14400(A/D/D2)-SP95	High Speed Digitizer	Xilinx® Virtex-5 SX95T	1 GB	PCI Express PC Ca
Gage Eon Express CS123G2/ CS126G1	High Speed Digitizer	Altera Stratix V	4-8 GB	PCI Express PC Ca
Extreme Engineering Solutions (X-ES); Middletown, WI, USA; +1 608-833-1155; www.xes-inc.com				
XPedite2400	SIGINT, EW, SDR	Xilinx® Virtex-7 690T	Up to 2 GB DDR3 in two channels	XMC
XPedite2402	SIGINT, EW, SDR	Xilinx® Virtex-7 690T	Up to 8 GB DDR3 in two channels	XMC
XPedite2470	SIGINT, EW, SDR	Xilinx® Virtex-7 485T	Up to 4 GB DDR3 in four channels	3U VPX
Interface Concept; Quimper, France; 0033 2 98 57 30 30; www.interfaceconcept.com				
IC-INT-VPX6d	EW, radar, COMINT, ELINT, SDR, ISR	Processor: Dual Intel® Xeon® D-1500	128GB DDR4	6U
IC-FEP-VPX3f	EW, radar, COMINT, ELINT, SDR, ISR	FPGA: Kintex® UltraScale™ KU060, KU85 or KU115	8GB DDR4	3U

	I/O, INTERFACE/BS TYPES	ENVIRONMENT	POWER	FEATURES
	VITA 65 OpenVPX	VITA 47 AEC4 - ECC4, Air or conduction cooled	100W	C-band capable ADC-DAC-FPGA combines 2 GHz of instantaneous bandwidth with a total latency of 40 nanoseconds from ADC input to DAC output.
	VITA 65 OpenVPX	VITA 47 AEC4 - ECC4, Air or conduction cooled	108W max	Up to X-band direct RF sampling capabilities; 16 independent digital down converters, decimation factor 2 to 48
	VITA 65 OpenVPX	VITA 47 AEC4 - ECC4, Air or conduction cooled	40W	1 GHz Dual ARM Cortex A9 MPCore, PCIe GEN2, Dual GigE, USB, HDMI, XMC and FMC carrier.
.A.R.E.	I/O: 2x 10G Ethernet ports; Gen3 PCIe; FPGA: SerDes, LVDS, PCIe; PPC: PCIe; UART-over-USB: PPC; RS-232:PPC	Operating temp.: 0°C to +50°C; storage temp.: (est) -40°C to +105°C	Power Consumption: 12V @ 6Amps (subject to FPGA loading)	Altera Stratix V FPGA; Free Scale T4240; Freescale K61; PLX PCIe 3D Mesh; SerDes 3D Mesh; LVDS 3D Mesh; DDR3; NAND flash: 512MB; PPC local bus: up to 100MHz at 16 bits; Cooling: airflow recommended, FPGA app. dep.
.A.R.E.	I/O: Gen 3 PCIe, LVDS, SerDes; external interfaces: Y1, connectors: PCIe & LVDS (FPGA), Y2, Z2 Connectors: LVDS (FPGA)	Operating temp.: 0°C to 50°C (commercial config.; storage temp.: (est) -55°C to 100°C	Power Consumption: 12V @ 15.5 Amps (Subject to FPGA loading)	Intel Arria 10 FPGA: flash memory for up to two FPGA configurations, JTAG programmable, 2 NOR flash configuration; DAC: 8-channel, 16-bit, 12.6 GSPS; cooling: air flow recommended
.A.R.E.	I/O: Gen 3 PCIe, LVDS, SerDes External Interfaces: Y1, connectors: PCIe & LVDS (FPGA); Y2, Z2 Connectors: LVDS (FPGA); PCIe	Operating temp.: 0°C to 50°C (commercial config.; storage temp.: (est) -55°C to 100°C	Power Consumption: 12V @ 15.5 Amps (Subject to FPGA loading)	Altera Arria 10 FPGA: 4GB DDR, ENOB AD 9208; ADC: configurable sample rate up to 3GSPS, 14-bit; Tailored clocking and triggering flexibility; cooling: air flow recommended, FPGA app. dep. (heat sink mounts avail.)
	Dual 6Gsps ADC/DACs, LVDS, Ethernet, high speed serial IO	Conduction-cooled (-40°C to 71°C with -54°C turn on)	90W (user application dependent)	User FPGA and CPU programmable.
3 x16	FMC+ , PCI Express	Commercial Convection	35w	x16 Gen 3, PCIe Interface, FMC+ Interface, 10 Gbytes/sec PCIe Throughput Performance
	FMC+ , PCI Express	Convection and Conduction Cooled	35w	x8 Gen 3 PCIe Interface, FMC+ Interface
3 x8	Dual FMC Sites, PCI Express	Commercial Convection	35w	x8 Gen 3 PCIe Interface, dual FMC Interface
ard	PCI Express (PCIe) x8	Operating temp: 0°C to +50°C	25W	Streaming data acquisition digitizer, 4-Channels 1.5GS/s 8-bits with onboard FPGA processing; programmable FPGA FIR filtering program.
ard	PCI Express (PCIe) x8	Operating temp: 0°C to +50°C	25W	Streaming data acquisition digitizer, 2-channels 400MS/s 14-bits with onboard FPGA processing; programmable FPGA FIR filtering program.
ard	PCI Express (PCIe) x8 Gen III	Operating temp: 0°C to +50°C	25W	Streaming data acquisition digitizer 1/2 channels 6/3GS/s, 12-bits with onboard FPGA processing; options for on-board averaging / peak / FIR / FFT / DDC programs.
	x8 Gen3, x10 GTH, 22 LVDS, 2500MSPS DAC	-40°C to +70°C (Air-Cooled), -40°C to +85°C (Conduction Cooled)	*	Optional 14-Bit 2500MSPS DAC, FPGA Development Kit (FDK).
	x12 10.3125 Gbps optical, x8 Gen3, x8 GTH (PCIe), 18 LVDS	-40°C to +70°C (Air-Cooled), -40°C to +85°C (Conduction Cooled)	*	12 Channels 10.3125 Gbps Optical, FPGA Development Kit (FDK).
	x8 Gen2, x3 GTX, VITA 57.1 FMC with LVDS I/O and x8 GTX	-40°C to +70°C (Air-Cooled), -40°C to +85°C (Conduction Cooled)	*	Freescale P1010 CPU, USB, 1000BASE-T, MicroSD, RS232, FPGA Development Kit (FDK).
	VPX VITA 65	Air-cooled, conduction-cooled	90W	1* Xilinx Kintex®-7 FPGA 1* PCIe Switch 1*XMC Slot
	VPX VITA 66.5	Air-cooled, conduction-cooled	80W	1*Artix-7 control node 1*FMC+ site (VITA 57.4)

FPGA BOARDS

MODEL	FUNCTION	PROCESSOR TYPE	MEMORY	FORMAT
Interface Concept; Quimper, France; 0033 2 98 57 30 30; www.interfaceconcept.com ***cont'd***				
IC-FEP-VPX6e	EW, radar, COMINT, ELINT, SDR, ISR	FPGA: 2*Kintex® UltraScale™ KU115	4GB DDR4	6U
iVeia LLC; Annapolis, MD, USA; +1 410-858-4560; www.iveia.com				
Atlas-I-LPe	Multifunction system-on-a-module (SoM)	Xilinx® Spartan 6 LX45	LPDDR, 1GB Micro SD, 16GB	Flex-COM I (sub c card size)
Atlas-I-Z7e	Multifunction system-on-a-module (SoM)	Xilinx® Zynq® 7020	• LPDDR2, 512MB (Processor) • LPDDR2, 512MB (FPGA) • Micro-SD Slot or NAND Flash, 32GB	Flex-COM I (sub c card size)
Atlas-II-Z7x	Multifunction system-on-a-module (SoM)	Xilinx® Zynq® 7030 Xilinx® Zynq® 7045	1GB DDR3-1066 SDRAM dedicated to PS 1GB DDR3-1066 SDRAM dedicated to PL MicroSD slot supports up to 32 GB 4MB boot flash	Flex-COM II (sub c card size)
Kontron; San Diego, CA, USA; + 1 888 294 4558; www.kontron.com				
VX3327	EW, SIGINT, radar	AMD Radeon™ 6760 GPU	1 GB GDDR5, 128 bits, 800 MHz	3U VPX
Mercury Systems; Huntsville, AL, USA; +1 866-627-6951; www.mrcy.com				
SCFE6120	FPGA Carrier Board	One Xilinx® Zynq® Ultrascale+™ ZU11EG Governor Two Xilinx® Virtex® Ultrascale+™ VU9P Prosecutors	20 GB of DDR4 SDRAM	6U oVPX
SCFE6110	FPGA Carrier Board	One Xilinx® Zynq® UltraScale+™ ZU9 System Processor Embedded PetaLinux Board Support Package Two Xilinx® Kintex UltraScale™ KU115 Prosecutors One Xilinx® Kintex UltraScale™ KU115 Governor	16 GB of DDR4 SDRAM & 36 MB of QDR4 SRAM	6U oVPX
Parsec; Centurion, South Africa; +27 12 678 9740; www.parsec.co.za				
VF360-D5-3I4-4-2-2-2	Radar, SIGINT, EW, SDR, video	Intel Stratix V GS D5	FPGA:1GB DDR3, 16MB QDRII+; DSP: 1GB DDR3	3U VPX
Pentek; Upper Saddle River, NJ, USA; +1 201-898-5900; www.pentek.com				
Model 5950	DSP, data acquisition, radar, EW	Zynq® UltraScale+™ RFSoC	16 GB	3U VPX Board
Model 6001	DSP, data acquisition, radar, EW	Zynq® UltraScale+™ RFSoC	16 GB	2.5 x 4.0 in.
Model 5550	DSP, data acquisition, radar, EW	Zynq® UltraScale+™ RFSoC	16 GB	3U VPX Board

	I/O, INTERFACE/BS TYPES	ENVIRONMENT	POWER	FEATURES
	VPX VITA 65	Air-cooled, conduction-cooled	180W	1*QorIQ LS1046A 1*Gen2/3 PCIe switch 1*Giga Ethernet L2 switch 2 FMC+ sites (VITA 57.4)
redit	User-configurable flex I/O, 2 banks; Gigabit Ethernet (RGMII)	Operating Temp: -40°C to +85°CC	• Typical: 1-2W • Max: 4W	Ideal for low-power / battery-powered applications; Texas Instruments DM3730.
redit	User-configurable flex I/O, 2 banks; Gigabit Ethernet (RGMII)	Operating Temp: -40°C to +85°CC	• Typical: 1.5-3W • Max: 9W	Ideal for compute-intensive low-power applications; low-power modes including FPGA core sleep.
credit	User-configurable flex I/O, 4 banks; User-configurable multi-Gigabit transceivers; 10 Gigabit Ethernet	Operating Temp: -40°C to +85°C	• Typical: 4-8W • Max: 16W	Ideal for compute-intensive high-performance applications; royalty-free application-ready framework.
	PCI Express	-40°C to +85°C	*	480 cores at 600 MHz and 1 GByte GDDR5 for up to 576 GFlops single-precision floatingpoint performance; conduction cooled.
	VITA 65.0 SLT6-PAY-4F1Q2U2T-10.2.1 Slot Profile *PCIe Gen3 *40 GbE *VITA 49.2	Air-cooled: Rugged L1 Conduction-cooled: Rugged L3 Air Flow-by: Rugged L4 Liquid Flow-By: Rugged L7	Dependant on FPGA Usage, consult factory	• Multi-channel, highly configurable FMC carrier • Virtex UltraScale+ FPGA processing power • Processing subsystems in data path for max performance • OpenVPX compliant for easy integration • Multiple high-reliability cooling options
	VITA 65.0 SLT6-PAY-4F1Q2U2T-10.2.1 Slot Profile *PCIe Gen3 *40 GbE *VITA 49.2	Air-cooled: Rugged L1 Conduction-cooled: Rugged L3 Air Flow-by: Rugged L4 Liquid Flow-By: Rugged L7	Dependant on FPGA Usage, consult factory	• Designed for System Security Engineering (SSE) • Multi-channel, highly configurable FMC carrier • Kintex® UltraScale™ FPGA processing power • Built-in IPMI controller • OpenVPX compliant for easy integration • High Reliability Design
	VPX: 3x PCIe fat pipes, 2x GigE ultra-thin pipes, 10x SERDES, 24x I/O; FMC site: 10x HSSI, LVDS	-40 to +55°C, Air cooled -40 to +70°C, Conduction cooled	35W	Stratix® V FPGA, combined with Texas Instruments multi-core KeyStone DSP; master or slave; PCIe and SERDES channels total at 32x 5Gbps; FMC site for I/O.
	PCI Express (Gen. 1, 2 and 3) interface up to x8; LVDS connections to the Zynq UltraScale+ FPGA for custom I/O	Operating temp: Operating temp: -40°C to +70°C	*	8 Channel A/D & D/A; Ruggedized and conduction-cooled versions available; Unique QuartzXM eXpress Module enables migration to other form factors; Optional VITA-66.4 optical interface for backplane gigabit serial communication; Dual 100 GigE UDP interface; Compatible with several VITA standards including: VITA-46, VITA-48, VITA-66.4, VITA-57.4 and VITA-65 (OpenVPXTM System Specification).
	LVDS connections to the Zynq UltraScale+ FPGA for custom I/O	Operating temp: -40°C to +70°C	*	8 Channel A/D & D/A; Ruggedized and conduction-cooled versions available; Unique QuartzXM eXpress Module enables migration to other form factors; GTY connections for gigabit serial communication; Includes a complete suite of IP functions and example applications.
	Compatible with several VITA standards including: VITA-46, VITA-48, VITA-66.4, VITA-67.3D and VITA-65 (OpenVPXTM System Specification)	Operating temp: -40°C to +70°C	*	SOSA-Aligned; 8 Channel A/D & D/A; Ruggedized and conduction-cooled versions available; Unique QuartzXM eXpress Module enables migration to other form factors.

FPGA BOARDS

MODEL	FUNCTION	PROCESSOR TYPE	MEMORY	FORMAT
Red Rapids; Richardson, TX, USA; +1 972-671-9573; www.redrapids.com				
Model 273	SIGINT, SDR, RADAR	FPGA	Optional 32 MB QDR II+	PCIe, XMC, CCXM
Model 277	SIGINT, SDR, RADAR	FPGA	Optional 32 MB QDR II+	PCIe, XMC, CCXM
Model 278	COMINT, SDR	FPGA	Optional 32 MB QDR II+	PCIe, XMC, CCXM
Sundance Multiprocessor Technology Ltd.; Chesham, Bucks, United Kingdom; +44 1494 793167; www.sundance.com				
SMT6657	Embedded computing	TI KeyStone and Xilinx® Kintex	Variable	PC/104
VF360	Radar, networking, SIGINT, EW, SDR, video	TI KeyStone and Intel® Stratix	Variable	3U OpenVPX
Sundance DSP; Reno, Nevada, USA; West +1 775-827-3103, East + 514-684 8315; www.sundancedsp.com				
SE120	SIGINT, Imaging, Machine Vision	Zynq® Ultrascale+™ MPSo	Up to 32 GB of SDRAM via DDR4 SODIMM to PS; 4GB of DDR4 to PL	x8 lanes PCIe Ger
PXIe800Z	SIGINT, imaging, machine vision	Zynq® Ultrascale+™ MPSoC in C1156 package (XCZU7EV / XCZU7EG / XCZU11EG / XCZU7CG)	Up to 4GB of DDR4 to PL	PXIe x8 lanes PCIe Ger
Ultraview Corporation; Berkeley, CA, USA; +1 925-253-2960; www.ultraviewcorp.com				
AD12-2000x2	SIGINT, comms, radar, test and measurement	Xilinx® Virtex-5 FPGA	8GB DRAM	PCIe x8
AD16-250x2,x4	SIGINT, comms, radar, test and measurement	Xilinx® Virtex-5 FPGA	8GB DRAM	PCIe x8
AD14-500x2	SIGINT, comms, radar, test and measurement	Xilinx Virtex-5 FPGA	8GB DRAM	PCIe x8

SURVEY KEY – DSP BOARDS

MODEL

Product name or model number

FUNCTION

Board application (analog I/O, digital I/O, multifunction, controller/timer, etc.)

Processor/FPGA TYPE

Model of DSP/FPGA used in board

MEMORY

Type and amount

FORMAT

(6U, 3U, PMC, XMC, etc.)

I/O, INTERFACE BUS TYPES
VITA standard or bus interface

ENVIRONMENT

Operating temperature range

FEATURES

Additional features

* *Indicates answer is classified, not releasable or no answer was given.*

MARCH 2020 TECHNOLOGY SURVEY: PORTABLE AND HANDHELD SPECTRUM ANALYZERS

This survey will look at portable and handheld spectrum analyzers. Please e-mail JEDEditor@naylor.com to request a survey.

	I/O, INTERFACE/BS TYPES	ENVIRONMENT	POWER	FEATURES
IC, VPX	PCI Express, GPIO	-30°C to +85°C (air cooled); +90°C max cold plate (conduction cooled)	12 W	Dual 16-bit (310 Msps) ADC; continuous, snapshot, or periodic capture modes; programmable digital down converter; ANSI/VITA 49 compliant data format.
IC, VPX	PCI Express, GPIO	-30°C to +85°C (air cooled); +90°C max cold plate (conduction cooled)	13 W	Quad 16-bit (250 Msps) ADC; continuous, snapshot, or periodic capture modes; programmable digital down converter; ANSI/VITA 49 compliant data format.
IC, VPX	PCI Express, GPIO	-30°C to +85°C (air cooled); +90°C max cold plate (conduction cooled)	13W	Octal 16-bit (125 Msps) ADC, continuous, snapshot, or periodic capture modes; programmable digital down converter; ANSI/VITA 49 compliant data format.
	PCIe, FMC, Ethernent	Industrial	12W and upwards	For DSP requiring high-performance integer and floating-point computation.
	PCIe, FMC, Ethernent	Industrial, MilCom	24W and upwards	Leverages Altera Stratix® V FPGA and Texas Instruments KeyStone Multicore DSP technology.
n4	USB JTAG through USB2.0; SFP+ attached to PL; 2x USB UART; 1x CAN	*	*	Zynq Ultrascale+ MPSoC (XCZU7EV-2FFVC1156E / XCZU7EG / XCZU11EG / XCZU7CG); Build option to use SE120 as PCIe host cooling fan for attached FMC.
n4	HPC FMC expansion site with 10 GTH at 16.3Gb/s transceivers and 56 LVDS IO pairs; and more	Different Temperature Range	*	x1 HPC FMC expansion site with 10 GTH at 16.3Gb/s transceivers and 56 LVDS IO pairs.
	4 Concurrent TTL inputs, sampled at same rate as ADCs	0°C to 70°C	25W Max	Zero-dead-time full speed signal averaging, external and internal clock and triggering.
	*	0°C to 70°C	25W Max	Analog waveform triggering.
	4 Concurrent TTL inputs sampled at same rate as ADCs.	0°C to 70°C	25W Max	Allows rapidly swept external clock.

GENERAL ABBERVIATIONS

ADC = analog-to-digital converter
comms = communications
DAC = digital-to-analog converter
DRFM = digital RF memory
EW = electronic warfare
FMC = FPGA Mezzanine Card
I/O = input/output
SATCOM = Satellite Communications
SDR = software defined radio
SIGINT = signals intelligence

CYBER-EW SYNERGIES

By John Knowles

For nearly 15 years, *JED* has served as platform to dispel the myth that the Cyberspace Domain is somehow "converging" with the EM Domain (a physical impossibility) or worse, that the EM Domain is actually part of Cyberspace. It's not clear when these misconceptions began, but they were certainly boosted when the Air Force's Cyberspace Task Force rolled out its Cyberspace initiative in 2006 and claimed that the Electromagnetic Spectrum is the maneuver space of cyber operations. Whatever the origin, this confusion spread to Cyber advocates from the other Services in short order. While "Cyber-EM convergence" is certainly the wrong term to describe the relationship between Cyberspace and the EM Domain, there is a synergistic relationship between Cyber operations and EMS Operations (EMSO), which is what we will be exploring in this month's column.

Before we jump into this discussion, however, it's worth reviewing how and when the Cyber Community began to embrace the EM Domain. Back in the 1990s and before, Computer Network Operations (CNO) was mainly a "wired" activity. Computers communicated in a world connected by copper wires and fiber-optic cables. As the 2000s got underway, the wider adoption of wireless communications networks enabled Cyber systems to utilize the EM Domain as a major part of its operational transport layer for moving information in the form of modulated signals across the EM Domain. The Cyber Community decided to perceive its operational dependence on the EM Domain as "convergence" between Cyberspace and the EM Domain; from its particular Cyber perspective, this appeared to be true.

This convergence perception is unique to the Cyber Community. Over the past 100 years, when weapon systems in the other major warfighting domains (Air, Land, Sea and Space) became more dependent on the EM Domain, their respective communities did not advocate for domain convergence. When aircraft began to utilize radios, then radars, EW, GPS, IFF and other systems that depend on access to the EM Domain, Air Power leaders did not argue for convergence between the Air and EM Domains or assert that the EMS was part of the Air Domain. The same is true for ships and submarines in the Maritime Domain, ground vehicles and in the Land Domain and satellites in the Space Domain. As these various types of weapons systems became more dependent on using the EM Domain, no one advocated for convergence between the Maritime Domain and the EM Domain or between the Land Domain and the EM Domain. Even the Space Community has avoided calling for Space-EM Domain convergence, despite the fact that space operations are completely dependent on the EM Domain to send and receive signals from ground stations to orbiting satellites. Yet the Cyber Community saw the Cyber systems' growing dependence on the EM Domain very differently – it perceived convergence.

OPERATIONAL SYNERGY

So, if "convergence" isn't the correct paradigm for describing the Cyber-EM Domain relationship, what is? The best framework for understanding this relationship is "operational synergy" or combined arms. As Jesse "Judge" Bourque has written in *JED* (see "The Electromagnetic Battle Management Challenge," *JED,* April 2014, p. 30), "Control of energy (Joint EMS Operations) and control of data (Cyber Operations) remain two distinct mission areas to be integrated in a combined arms framework including all four of the fundamental operational responsibilities: controlling ideas, energy, data, and mass." So, let's take a closer look at how EW and Cyber activities can be combined to create operational synergies.

TARGET EFFECTS

The widespread adoption of software defined radio (SDR) technology by military forces over the past 15-20 years has transformed the design of radios, radars, GPS systems and other electromagnetic systems. Prior to this SDR technology revolution, radios, radars and other electronic systems were mainly vulnerable to jamming (energy), as well as kinetic weapons (mass) on the battlefield. As these systems began to incorporate SDR technology (which made them easier to reprogram) and to rely on datalinks to receive software updates, it created a new vulnerability, in which malicious software code could generate any number of system effects from false data to minor operating malfunctions to complete system shutdown and even physical damage to processors.

In a cyber attack through the EM Domain, the malicious software code is transmitted as RF and microwave signals (analog energy – photons) to the receiver in the victim system that converts these signals back into digital code. As an aside, it is important to recognize that software code does not transit the EM Domain in its digital form. (Dave Adamy explains to his EW101 students: "You don't unscrew an antenna cable and see 1s and 0s spill onto the floor.") This may seem obvious, because the EM Domain is not part of the Information Environment. Yet we sometimes "talk in shorthand" about transmitting data packets or software code through the EM Domain. So, it is worth clarifying for those who may be confused by our sometimes sloppy language.

In terms of Cyber-EW operational synergy, the upshot is that an SDR-based system can be attacked non-kinetically in two ways: with a cyber attack (software code) or via electronic attack (jamming). Both methods utilize the EM Domain, and both can be transmitted by an EW system. The easiest way to envision this target effects synergy is to think of an EW system as a gun that can fire two different types of bullets: a cyber bullet or a jamming bullet. Each type of bullet attacks the victim system in different ways.

Sometimes these effects can appear to overlap, such as using electronic attack to overstress a threat radar's signal processor and force it to compute errors, slow down or even shut down. This is an example of electronic attack causing cyber effects. However, there are two main criteria for distinguishing a cyber attack from an electronic attack. The first is to identify the payload. Is the EW system sending a modulated signal that will be processed by the victim system only as a signal (electronic attack), or is it a modulated signal that will be converted into software code (cyber attack)? The second is the persistence of the effect. If the payload's effect continues long after the EW system stops transmitting, it is characteristic of a cyber attack. If the payload effect stops once the EW system stops transmitting, then it is more characteristic of jamming. You'll notice that I'm hedging with my language by saying "characteristic of…" because there are forms of electronic attack that are persistent (directed energy), and there are cyber attacks that may be designed to be less persistent – mimicking an electronic attack in order to obscure the cyber payload, for example. Payload and persistence are far from perfect criteria in terms of distinguishing electronic attack and cyber attack. But they can provide some clarity. In an operational context, this distinction is not very important. At the Service level, however, distinguishing between a cyber attack payload and an electronic attack technique does matter because cyber payloads and jamming techniques are developed in different organizations, under different programs, with different sources of funding.

It is also important to recognize that you do not need to use an EW system to deliver a cyber attack via the EM Domain. The EW system merely offers high effective radiated power and wideband performance, which means it can deliver the attack at long range and send it into different types of victim systems that use various frequencies. At shorter distances, a cyber attack could also be delivered via a false communications base station or a digital radio that is near the victim receiver. This is because a cyber attack delivered through the EM Domain is essentially a successful communication between a transmitter that is sending the cyber attack payload (as signals) and the victim system that is receiving the signals and converting them into software code.

FINDING A CYBER TARGET

The other major area of current operational Cyber-EW synergy lies in the targeting process. In order to deliver a cyber attack, the operator first needs to find the target. In a wired computer network, cyber targeting is accomplished by gaining access to various parts of the victim network, usually through a physical node, such as a desktop computer. In a tactical battlespace, however, the cyber nodes are typically SDRs (i.e, radars, radios, etc. equipped with digital datalinks). Which can most easily be detected, identified and geolocated via their emissions in the EM Domain. In this environment, these emissions are detected using an electronic support measures (ESM) system or a signals intelligence (SIGINT) system. Thus, tactical offensive cyber operations are very dependent on EW systems to support targeting.

To be clear, most of the electromagnetic systems in a tactical battlespace are not viable cyber targets, because they are not SDRs. However, most of the cyber targets (SDRs) in the tactical battlespace are electromagnetic systems (i.e., radars and radios that are vulnerable to cyber attacks via their digital datalinks). In other words, most of the tactical cyber target set in the battlespace is a subset of the entire EW target set – not the other way around. Why? In order to attack a target, you must have "access" to the target and the "opportunity" to affect the target in a timely manner. In terms of the thousands and sometimes millions of electromagnetic systems in a given tactical battlespace, EW has tremendous flexibility with regard to access and opportunity, while cyber operations are relatively limited in these respects. This is because an EW system must simply deliver energy onto the victim system's apertures (any one of them) in order to generate a jamming effect. A cyber attack typically must enter via the system's datalinks and convert signals into software code (the "access" factor) and also generate its effect in a timely manner (opportunity). For example, an SA-7 IR guided missile closing in on a helicopter needs just a few seconds (very limited opportunity) and it does not provide at datalink to attack (no access) for a cyber attack to generate an effect. An RCIED that uses a smart phone to trigger the explosives may provide access (an SDR), but not timely opportunity (typically less than a second between detecting the RCIED and its detonation).

CYBER DEFENSE AND ELECTRONIC PROTECTION

So far, we have discussed Cyber-EW operational synergies that are mainly focused on target effects and targeting opportunities. However, another operational synergy is emerging – this one between cyber defense and electronic protection (EP). At the system level (in a friendly radio, radar or GPS receiver, for example), EP measures have focused on mitigating the effects of enemy jamming by using anti-jam antennas, such as controlled reception pattern antenna (CRPA) arrays, as well as signal processing techniques that distinguish between enemy jamming signals and friendly signals. However, in a datalink application, these EP approaches can also be used to help protect against an enemy cyber attack. For example, if the datalink is equipped with a CRPA array, it can null out enemy signals carrying cyber attack payloads based on their direction of arrival. Also, EP techniques in the datalink's signal processing chain can enable the friendly system to distinguish between an adversary's cyber attack payload and friendly signals. These types of EP approaches can provide a frontline defense (think of it as a signal gatekeeper) that can reduce the number of enemy cyber attacks faced by the friendly system.

In summary, the operational synergies between EW and cyber operations are both powerful and plentiful. But it is important to recognize when we are talking about synergies and when we are describing those few limited areas of Cyber-EW technology convergence and target effects convergence. Otherwise, the failure to understand the Cyber-EW relationship can result in profound strategic misunderstandings that can translate into major operational failures.

EXHIBIT AND SPONSORSHIP OPPORTUNITIES AVAILABLE!

DIXIE CROW SYMPOSIUM XLV

MARCH 22-25, 2020 // MUSEUM OF AVIATION, ROBINS AFB, GA

KEYNOTE SPEAKER
Brig Gen David Gaedecke, HQAF/A5L

BANQUET SPEAKER
Confirming – to be announced

7TH ANNUAL THE CROW'S

N.E.S.T.

(Novel Experiments with Science & Technology)

WEDNESDAY, MARCH 25 // 10:00 A.M. - 2:00 P.M. // MUSEUM OF AVIATION CENTURY OF FLIGHT HANGAR

The Dixie Crow Chapter of the Association of Old Crows Science, Technology, Engineering, and Mathematics (STEM) Robotics displays and technology demonstrations, are an interactive experience that will capture the minds and hearts of students, parents and teachers. The displays are a collaborative effort between local military, government civil service, academia, defense industry and volunteers designed to inspire students to pursue STEM careers. Interacting with the robotics displays and technology demonstrations will demonstrate to students that STEM can be both fun and engaging. Enthusiastic workers in STEM fields will also be on hand to answer questions and help students learn how they can prepare to enter the exciting world of STEM. Make time to visit and participate in our Crows N.E.S.T. displays and technology demonstrations.

We are looking for Academia, Industry, Government/Military and other Organizations to display their creative robotic talents and/or interactive technological products!!!

We look forward to your participation in this fantastic opportunity to interface with our STEM Leaders of tomorrow!

If you have any questions and/or would like to participate, please feel free to contact:
Robert Usher at Robert.Usher@gmail.com (478) 222-0022
Event open to Students age 8 and up.

PREPARE TO BE AMAZED!

SCHEDULE OF EVENTS

SUNDAY, MARCH 22

Registration	Marriott Courtyard, Warner Robins, Georgia	5:00 PM-8:00 PM
Hospitality Suite	Marriott Courtyard, Warner Robins, Georgia	5:00 PM-8:00 PM

MONDAY, MARCH 23

Registration	Southern Landings Golf Course, Warner Robins, Georgia	10:30 AM-12:30 PM
Registration	Century of Flight Hangar, Museum of Aviation	2:30 PM-5:00 PM
Spring Golf Tourney	Southern Landings Golf Course, Warner Robins, Georgia	12:00 PM Tee Time
BBQ Sports Banquet	Southern Landings Golf Course, Warner Robins, Georgia	5:00 PM-7:00 PM

TUESDAY, MARCH 24

Registration	Century of Flight Hangar, Museum of Aviation	7:30 AM-6:00 PM
Plenary Session	Scott Theater, Eagle Building, Museum of Aviation	8:00 AM-11:00 AM
Exhibits Open	Century of Flight Hangar, Museum of Aviation	10:00 AM-7:00 PM
Exhibitor Reception	Century of Flight Hangar, Museum of Aviation	5:00 PM-7:00 PM

WEDNESDAY, MARCH 25

Registration	Century of Flight Hangar, Museum of Aviation	9:00 AM-2:00 PM
Exhibits Open	Century of Flight Hangar, Museum of Aviation	9:45 AM-3:00 PM
Crows N.E.S.T.	Century of Flight Hangar, Museum of Aviation	10:00 AM-2:00 PM
AOC Chapter President's Mtg	Century of Flight Hangar, Museum of Aviation	11:30 AM-1:00 PM
Banquet	Nugteren Exhibit Hangar, Museum of Aviation	Cocktails – 5:30 PM-6:30 PM
		Dinner – 6:30 PM-8:30 PM

WELCOME TO DIXIE CROW SYMPOSIUM 45!

Our Symposium Committee, Dixie Crow Chapter President, Matthew Bryant, and the Chapter Directors cordially invite you to join us for all the exciting events described here. Thank you in advance for your support of this important electronic warfare/information operations trade show.

Sincerely, Karen Brigance, *Co-Chair* | Kbrigance@merc-mercer.org
Lisa Frugè-Cirilli, *Co-Chair* | lisa.fruge@baesystems.com

REGISTER NOW! WWW.DIXIECROWSYMPOSIUM.COM

Electronic Warfare and Avionics (EWA) Conference (Formerly: the Air Force Technical Program)

www.robins.af.mil/About-Us/EWA-Conference
or email: AFLCMC.WNY.AFTechProg@us.af.mil

Technical Courses are being solely sponsored by AFLCMC/WNY, Robins AFB

New EA Techniques (Part 13)

Burn-Through Modes, Frequency Agility and PRF Jitter

By Dave Adamy

BURN-THROUGH MODES

"Burn through" refers to a radar being able to reacquire a signal in the presence of jamming – the radar is said to "burn through" the jamming. In self-protection jamming, the jammer is located on the target and jams into the boresight of the target radar as shown in **Figure 1.** The equation for the jamming-to-signal ratio in self-protection jamming is:

$$J/S = ERP_J - ERP_s + 71 + 20 \log R - 10 \log RCS$$

Where: *J/S* is the ratio of the received jamming power in the target radar to the received skin return power,
ERP_J is the effective radiated power of the jammer in dBm,
ERP_S is the effective radiated power of the radar in dBm,
R is the range from the radar to the target (and jammer) in kilometers, and
RCS is the radar cross section of the target in square meters.

The burn-through equation gives the maximum range from the radar to the jammer at which the jammer can protect the target. Within this range, the radar is said to be able to "burn through" the jamming. The burn-through range for self-protection jamming (as presented in the "EW101" column of the February 2018 *JED*) is given by:

20 log RBT = ERPS - ERPJ - 71 + 10 log RCS + J/S Req

Where: R_{BT} is the range from the radar to the target at burn-through in kilometers and
J/S Req is the J/S value at which the jammer can no longer effectively jam the radar.

The required J/S for burn-through varies with the type of jamming employed. Sometimes, 0 dB J/S is adequate to protect the target, but it can be as much as 20 to 40 dB. Now, we determine the burn-through range from the range term with the formula:

$$R_{BT} = \text{Anti-log } \{(20 \log R_{BT}) / 20\}$$

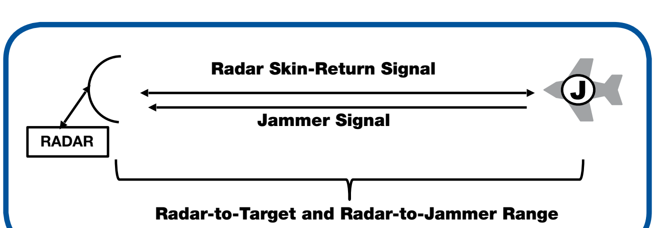


Figure 1: Self protection jamming uses a jammer on the target and transmits directly into the main beam of the jammed radar.

Remote Jamming

As shown in **Figure 2,** remote jamming includes both stand-off and stand-in jamming. In both cases, the jammer is not located at the target and is assumed to jam into the side-lobes of the target radar. The jamming-to-signal ratio for remote jamming is given by:

$$J/S = ERP_J - ERP_S + 71 + G_S - G_M - 20 \log R_J + 40 \log R_T - 10 \log RCS$$

Where: *J/S* is the jamming to signal noise ratio in dB,
ERP_J is the effective radiated power of the jammer in dBm,
ERP_S is the effective radiated power of the jammed radar in dBm,
G_S is the side-lobe gain of the radar antenna in dB,
G_M is the main lobe bore-sight gain of the radar antenna in dB,
R_J is the range from the radar to the jammer in kilometers,
R_T is the range from the radar to the target in kilometers, and
RCS is the radar cross section of the target in square meters.

The remote burn-though range formula (from the March "EW101" column) is:

40 log RBT = ERPS - ERPJ - 71 – GS + GM + 20 log RJ + 10 log RCS + J/S Req

Where: R_{BT} is the range from the radar to the target at burn-through in kilometers and *J/S Req* is the minimum required J/S value at which the jammer can effectively jam the radar.

The formula for the burn through *range* solves the *range term* for the actual range:

$$R_{BT} = \text{Anti-log } \{[40 \log R_{BT}[/ 40\}$$

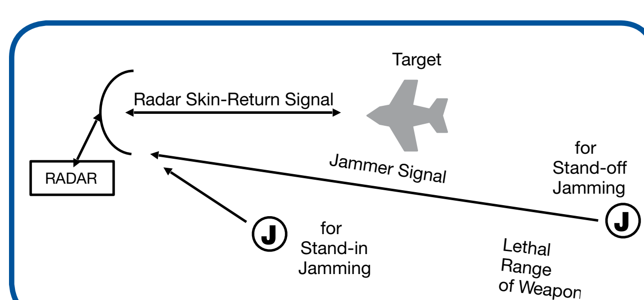


Figure 2: Remote jamming can be stand-off or stand-in. The jammer is not located on the target, and is assumed to transmit into a side lobe of the target jammer.

HOW DO YOU INCREASE THE BURN-THROUGH RANGE?

From all of these formulas, you can see that the radar's burn-through range will increase if the radar power is increased. This important electronic protection measure makes a radar more effective by being able to track a target earlier in an engagement.

At this point, it is important to understand that the radar works not on *power* but on *energy*. The radar range equation calculates the radar range in term of the received energy at the radar receiver. The energy is the product of the received power and the time over which that power is received as shown in **Figure 3.**

One way to increase the radar's energy is by *increasing its power*. Modern radars reduce their transmitted power to the minimum level that supports the effective tracking of a target. This minimizes the radar's detectability. However, if the radar determines that it is being jammed, the transmitter power can be increased to its maximum level, thus maximizing the burn-through range.

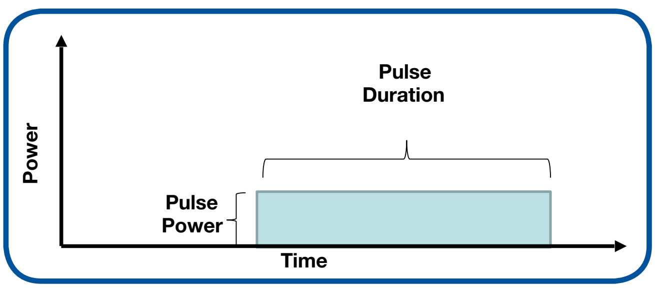


Figure 3: The energy of a pulse is the product of the pulse power and the pulse duration.

The second way to increase the energy is to increase the *time* over which the radar power is applied to the target. This is done by either increasing the pulse duration or by increasing the duty factor by increasing the pulse repetition frequency (PRF). Note that increasing the pulse duration reduces the range resolution unless some pulse compression technique is practical. Also, the ability to increase the PRF is limited by range ambiguity.

FREQUENCY AGILITY

In order to jam a radar, the jammer must either jam a broad frequency range or measure the radar's specific operating frequency(ies) and jam that. If the radar has a fixed-frequency, the frequency of one received pulse will be the same as that for subsequent pulses. Thus, the jammer can place all of its power within the receiver bandwidth of the radar for maximum jamming efficiency.

The radar can vary its frequency by changing tuning for each antenna sweep or some other scheme. However, the radar can achieve a more effective degree of electronic protection by changing the frequency for each pulse using a random pseudo frequency pattern as shown in **Figure 4.** In this way, the jammer will never know the frequency of the next pulse.

Overcoming random frequency selection requires that the jammer measure the frequency of each pulse before initiating jamming. This can be achieved by use of a digital RF memory

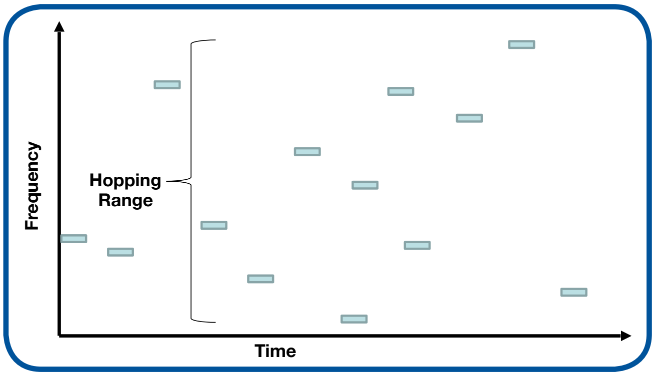


Figure 4: A frequency-agile radar transmits at different frequencies, either for each pulse or for groups of pulses.

(DRFM). Since DRFMs can measure the frequency of a pulse in a very short time (50 nanoseconds is often mentioned in literature) it can start jamming before much of the pulse has been transmitted. For example, if a pulse is 10 microseconds long and the DRFM equipped jammer can start its jamming within 50 nsec, 90% of the pulse will be covered by jamming. This means that the jamming energy will be 95% of the skin return energy – increased by the jamming-to-signal ratio. It should be noted that this requires a wide-band DRFM – one that is wide enough to cover the radar's entire hopping range.

PRF JITTER

PRF jitter refers to radars in which the delay between pulses is a random or pseudo-random function. This means that a jammer cannot include a "PRF tracker" to predict the timing of subsequent pulses. This prevents the use of a range-gate-pull-in (RGPI) jamming technique, as described in the December 2019 "EW101" column. Also, if cover pulses are employed by a jammer to improve jamming efficiency, they must be extended to cover the full range of the pulse timing uncertainty, as shown in **Figure 5**. This significantly reduces the jamming efficiency.

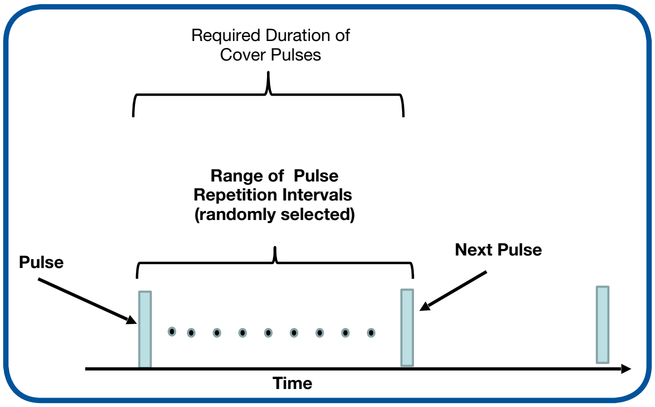


Figure 5: The energy of a pulse is the product of the pulse power and the pulse duration.

WHAT'S NEXT

Next month, we will continue our coverage of the impact of electronic protection techniques by discussing anti-side-lobe-jamming techniques. For your comments and suggestions, Dave Adamy can be reached at dave@lynxpub.com.

ASSOCIATION OF OLD CROWS *news*

AOC CAPITOL CLUB HOSTS ANNUAL HOLIDAY PARTY

The annual AOC Capitol Club Holiday Party was hosted by outgoing President Troy "Bucket" Orwan, USAF (Ret.) and incoming President Colonel Donald "Don" Revell, Colonel U.S. Marine (Ret.) at the Army Navy Country Club, Arlington Virginia on December 13. With past dignitaries such as former Presidents Eisenhower and Kennedy, members of Congress, and distinguished military general officers, including Omar Bradley, the Army Navy Country Club continues to serve as an excellent venue to show our appreciation for CapClub members' support throughout the year. The chapter's largest Holiday gathering yet, over one hundred members and their guests, representing government, military, civilian and industry stakeholders throughout the Washington DC area, were in attendance. As outgoing president Orwan delivered awards, incoming president Revell presented his vision for the future of the CapClub chapter, which is supported by over 1,000 members. In part, Colonel Revell stressed the need for continued growth in STEM outreach, scholarship offerings, research & development grants, professional speaker series, multi-national engagements, sponsorship, "sister" chapter alliances and Capitol Hill engagement, to name a few. The future is bright for the AOC Capitol Club, and we look forward to growing our board and delivering on our commitment to serve the ever-expanding interests of our valued members.

2020 AOC AWARDS NOMINATIONS ARE NOW OPEN!

Nominate someone today for an AOC award in 2020. The deadline to submit nominations is March 15, 2020.

A central tenant of the AOC's mission is recognizing individuals, groups, and military units for their outstanding performance in furthering the aims of the AOC and the Electromagnetic Warfare enterprise. The AOC has a number of awards that are available each year, with two categories – Competitive and Non-Competitive. Nominate someone today to go to https://app.reviewr.com/s1/site//AOC_Awards. Contact oneilin@crows.org for more information.

CALL FOR NOMINATIONS FOR THE 2020 AOC BOARD OF DIRECTORS IS NOW OPEN!

Decide the future of the Association of Old Crows! Nominations for the AOC board of directors for the 2020 elections are now open. For regional directors, only members from that region are eligible to vote for their potential representative. Nominations are due NLT March 15, 2020. Positions that are eligible for election this year are:

- At-Large Director (2 available)
- International Region II
- Northeast Region
- Southern Region

Go to https://crows.org/page/elections to download the nomination form or contact oneilin@crows.org for more information.

DIXIE CROW CHAPTER CELEBRATES THE HOLIDAY SEASON

The Dixie Crow Chapter held its annual holiday party on December 14, with 79 guests in attendance at the Southern Landings Club House. Matt Bryant, Dixie Crow Chapter president, welcomed all in attendance and introduced Col James Wilson, senior material leader AFLCMC/WNY, to provide an overview of 2019 prior to the festivities, including a catered meal, door prizes and music by the Chris Anderson Band. Thank you to Greg and Denise Carter for coordinating the event.

AOC Industry and Institute/University Members

SUSTAINING
BAE Systems
The Boeing Company
CACI
Collins Aerospace
DRS Defense Solutions
Electronic Warfare Associates
General Atomics
General Dynamics
Keysight Technologies
L-3 Harris
Leonardo MW Ltd.
Mercury Systems
Raytheon Company
Rohde & Schwarz USA
Saab

MILITARY UNITS
30 Cdo IX Gp RM
51 Sqn, Royal Air Force
57 IS/DOD
Air Command Denmark
French Air Force EW Unit
Helicopter Wing 53
Japan Air Self-Defense Force
NIWTG SD
Osan AB 25 FS
Zentrum Elektronischer Kampf Fliegende Waffensysteme

INSTITUTES/UNIVERSITIES
Electronic Warfare Studying Group, Korean Institute of Electromagnetic Engineering & Science
Georgia Tech Research Institute (GTRI)
Mercer Engineering Research Center
Research Association of Syracuse
Riverside Research Institute

GOVERNMENT GROUPS
Defence Science & Technology Agency (DSTA)
SAGE

GROUPS
3dB Labs Inc.
3SDL
A.G. Franz, LLC
Abaco Systems
Advanced Test Equipment Rentals
Aeronix, Inc.
Aethercomm, Inc.
ALARIS Antennas
Alion Science and Technology
Allen-Vanguard
Amplus Corporation
Annapolis Micro Systems, Inc.
Anritsu Company
Antenna Research Associates, Inc.
ApisSys SAS
Arctan, Inc.
Aselsan A.S.
Atkinson Aeronautics & Technology, Inc.
Atlanta Micro, Inc.
Azure Summit Technologies, Inc.
Babcock International Group
Base2 Engineering LLC
Battlespace Simulations, Inc.
Beca Applied Technologies Ltd
Bird Technologies
Blue Ridge Envisioneering, Inc.
Booz Allen Hamilton, Inc.
Boyd Corporation
Cablex PTY LTD
CEA Technologies LLC
Centerline Technologies LLC
Chemring Group
CISR Babcock International Group
Clearbox Systems
Cobham Advanced Electronic Solutions
Colorado Engineering Inc.
Communication Power Corporation
Communications & Power Industries LLC
COMSEC LLC
Comtech PST Corporation
CRFS Inc.
CSIR DPSS
Cubic Global Defence
Darkblade Systems
Dayton-Granger, Inc.
dB Control
DCS Corp
Decodio AG
Defense Research Associates
DEFTEC Corporation
DEWC Pty Ltd
DHPC Technologies, Inc.
DragoonITCN
Dreamlab Technologies AG
DRT, Inc.
D-TA Systems, Inc.
Dynetics, Inc.
ELBIT Systems of America
Elbit Systems of EW & SIGINT Elisra
Elettronica SpA
ELTA Systems Ltd.
Empower RF Systems
Epiq Design Solutions, Inc.
ERZIA Technologies S.L.
ESROE Limited
Evans Capacitor Company
EW Solutions
FEI-Elcom Tech, Inc.
Galleon Embedded Computing Norway
GFB GmbH
Gigatronics Incorporated
Hammer Defense Technologies LLC
Hanwha Systems
HASCALL-DENKE
Headmark Consulting
Hegarty Research LLC
Hensoldt Sensors GmbH
Hermetic Solutions
Herrick Technology Laboratories, Inc.
Independent Consultant, Jeffry Edgar
Innovationszentrum Fur Telekommunikations -technik GmbH (IZT)
Intelligent RF Solutions
Interface Concept
Invisible Interdiction, Inc.
ISPIN AG
IW Microwave Products Division
IWTG Norfolk
JEM Engineering
Kerberos International, Inc.
Kihomac, Inc.
Kirintec
Kranze Technology Solutions, Inc. (KTS)
KRATOS GENERAL MICROWAVE CORPORATION
Kudelski Security, A Division of Nagravision S.A.
LCR Embedded Systems
Leonardo DRS
Liteye Systems, Inc.
LS Telcom AG
MarServices GmbH
Mass Consultants Ltd
MBDA France
MC Countermeasures, Inc.
Meggitt Baltimore
Meggitt Defense Systems
Metamagnetics
Micro Lambda Wireless
Microwave Products Group
Microwave Specialty Company
Military College of Telecommunication Engineering
Milso AB
MilSource
Mission Microwave Technologies
The MITRE Corporation
Modern Technology Solutions, Inc.
Motorola Solutions
MRC Gigacomp
My-konsult
MYDEFENCE
N-Ask Incorporated
Narda Safety Test Solutions GmbH
National Instruments Corporation
NEL Frequency Controls, Inc.
Northeast Information Discovery, Inc.
Northrop Grumman Innovation Systems
Northrop Grumman Innovation Systems - Defense Electronics Systems
Novator Solutions
Nuvotronics, Inc.
OCS America, Inc.
Parry Labs
Parsons
Pentek
Peralex
Phasor Innovation
Photonis Defense, Inc.
Physical Optics Corporation
Plath GmbH
Qnion Co., Ltd.
QuantiTech
RADA Technologies LLC
RADX Technologies, Inc.
Rincon Research Corporation
Rohde & Schwarz GmbH & Co. KG
Rohde & Schwarz Norge AS
Roschi Rohde & Schwarz AG
Rotating Precision Mechanisms
S2 Corporation
Scientific Research Corp.
Selex Galileo, Inc. (a Leonardo-Finmeccanica company)
Serpikom
Sierra Nevada Corporation
Signal Hound
Silentium Defence
Silver Palm Technologies
SimVentions
SMAG Mobile Antenna Masts GmbH
Smiths Interconnect
Spectranetix, Inc.
Spherea GmbH
Spirent Communications
SR Technologies
SRC, Inc.
SRI International
Swedish Defence Materiel Administration T&E Directorate (FMV T&E)
Systems & Processes Engineering Corp. (SPEC)
TCI International, Inc.
Tech Resources, Inc.
Tektronix, Inc.
Teledyne Technologies, Inc.
Teleplan Globe Defence
Tevet LLC
Textron Systems
Textron Systems Electronic Systems UK Ltd.
TINEX AS
TMC Design
TMD Technologies Ltd.
Transformational Security LLC
Transhield Inc.
TrustComm
TUALCOM, Inc.
Ultra Electronics - EWST
Ultra Electronics Avalon Systems
Ultra Electronics TCS, Inc.
US Technologies-Aldetec
Valkyrie Enterprises LLC
Verus Research
VIAVI Solutions
Warrior Support Solutions LLC
WGS Systems, Inc.
ZARGES, Inc

JED, The Journal of Electronic Defense (ISSN 0192-429X), is published monthly by Naylor, LLC, for the Association of Old Crows, 1555 King St., Suite 500, Alexandria, VA 22314.

Periodicals postage paid at Alexandria, VA, and additional mailing offices. Subscriptions: *JED, The Journal of Electronic Defense*, is sent to AOC members and subscribers only. Subscription rates for paid subscribers are $160 per year in the US, $240 per year elsewhere; single copies and back issues (if available) $12 each in the US; $25 elsewhere.

POSTMASTER:
Send address changes to
JED, The Journal of Electronic Defense,
c/o Association of Old Crows,
1555 King St., Suite 500
Alexandria, VA 22314-1652

Subscription Information:
Glorianne O'Neilin
(703) 549-1600
oneilin@crows.org

JED Sales Offices

NAYLOR
ASSOCIATION SOLUTIONS
5950 NW 1st Place
Gainesville, FL 32607
Toll Free (US): (800) 369-6220
Fax: +1 (352) 331-3525

Project Manager:
Tabitha Jenkins
Direct: +1 (352) 333-3468
tjenkins@naylor.com

Project Coordinator:
Amanda Glass
Direct: +1 (352) 333-3469
aglass@naylor.com

Advertising Sales Representatives:
Shaun Greyling
Direct: +1 (352) 333-3385
sgreylin@naylor.com

Erik Henson
Direct: +1 (352) 333-3443
ehenson@naylor.com

Chris Zabel
Direct: +1 (352) 333-3420
czabel@naylor.com

NAYLOR (Canada) Inc.
200 – 1200 Portage Ave.
Winnipeg, MB R3G 0T5 Canada
Toll Free (US): (800) 665-2456
Fax: +1 (204) 947-2047

Index of advertisers

The Big Thing in RFSoC is Here.

(And it's only 2.5 inches wide!)

Small | Powerful | Deployable

Pentek's Model 6001 FPGA board lets you quickly develop and deploy RFSoC technology, while optimizing your system for SWaP.

Mounted on your custom carrier or Pentek's proven 3U VPX carrier, the new QuartzXM® comes pre-loaded with a full suite of IP modules, robust software, and fully integrated hardware — all geared to shorten time to market and reduce design risk.

And at only 4"x2.5", it can be deployed in extremely compact environments, including aircraft pods, unmanned vehicles, mast-mounted radars and more.

- **QuartzXM eXpress Module** speeds migration to custom form factors
- **Powerful Zynq® Ultrascale+™ RFSoC** with built-in wideband A/Ds, D/As & ARM processors
- **Dual 100 GigE** interfaces for extreme system connectivity
- **Robust Factory-Installed IP** for waveform generation, real-time data acquisition and more
- **Board Resources** include PCIe Gen.3 x8 and 16 GB DDR4 SDRAM
- **Navigator® Design Suite** BSP and FPGA design kit for seamless integration with Xilinx Vivado®

All this plus FREE lifetime applications support!

QUARTZ NAVIGATOR Design Suite

Unleash the Power of the RFSoC.
Download the FREE White Paper!
www.pentek.com/go/rfsocjed

SOSA Sensor Open Systems Architecture

30 YEARS

PENTEK
Setting the Standard for Digital Signal Processing

Pentek, Inc., One Park Way, Upper Saddle River, NJ 07458
Phone: 201-818-5900 • Fax: 201-818-5904 • email: info@pentek.com • www.pentek.com


Disrupting enemy command and control
With a multi-million dollar expansion in support of electronic warfare, BAE Systems is driving unparalleled enhancements to the EC-37B. Integrating our innovative Compass Call mission system into the platform enables warfighters to combat advanced threats and support special missions.
EC-37B
Join us
We're looking for driven individuals who are ready to build the future of electronic warfare. Learn more at baesystems.com/EWJOBS.
baesystems.com/compasscall
BAE SYSTEMS