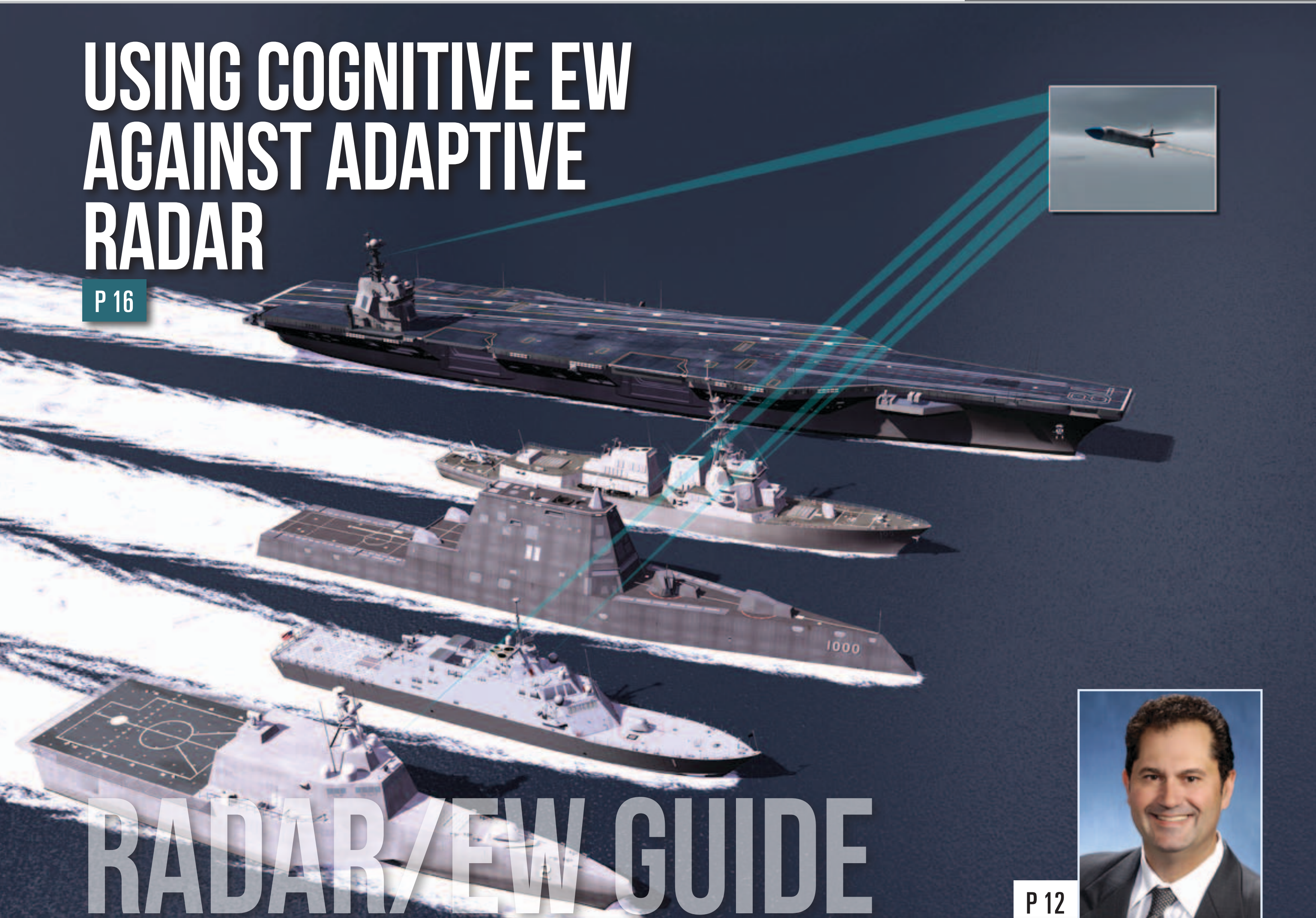
Military EMBEDDED SYSTEMS

@military_cots

MIL-EMBEDDED.COM

Jan/Feb 2017 | Volume 13 | Number 1



USING COGNITIVE EW AGAINST ADAPTIVE RADAR

P 16

RADAR/EW GUIDE

P 12

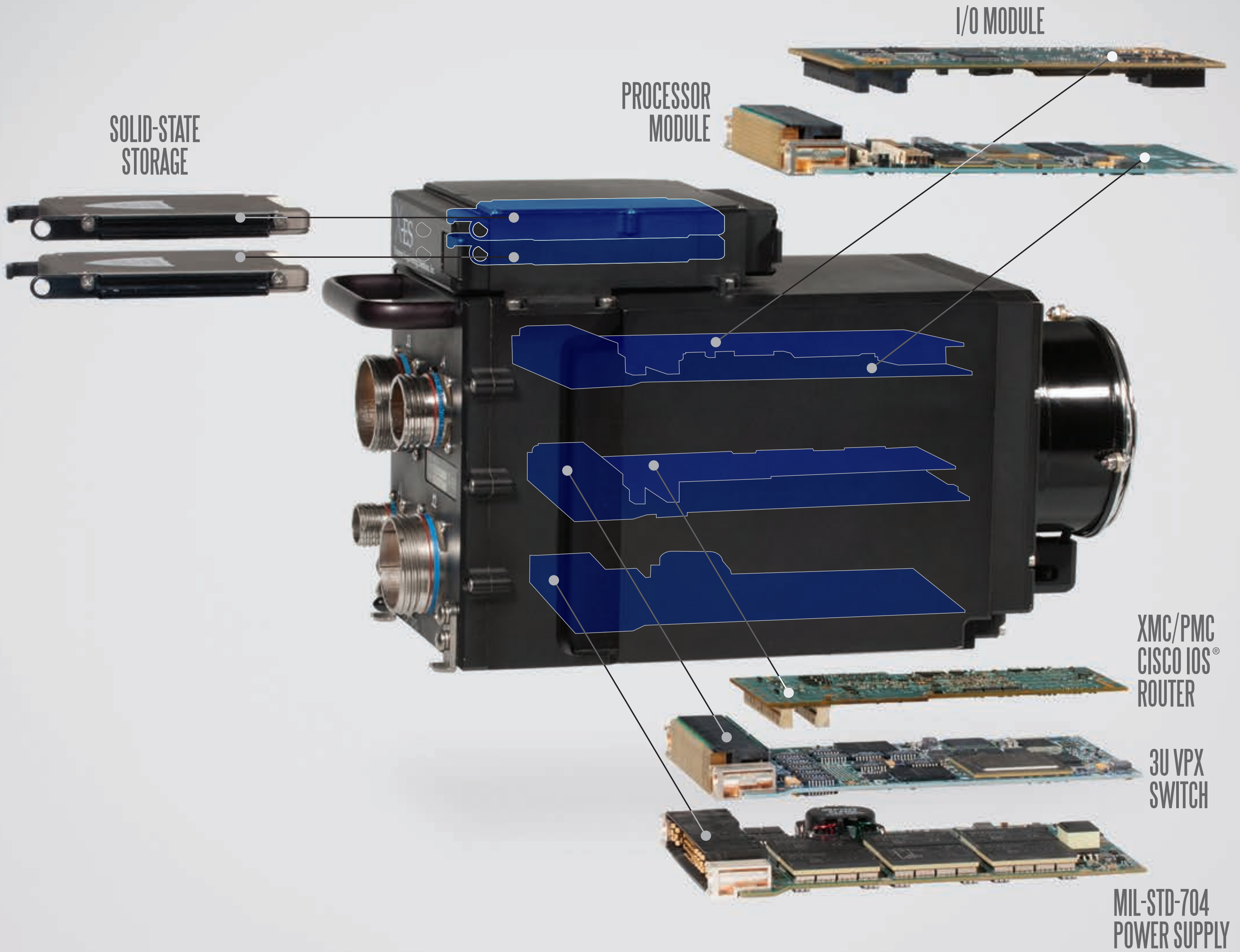
Interview with Ed Zoiss, president of the Electronic Systems segment at Harris

Low latency, open architectures for enhanced radar and EW

P 24

Rugged 3U VPX Chassis

For Extreme Environments



Every component in an X-ES high-performance, embedded system is designed, tested, manufactured, and supported in the USA in order to provide our customers with a superior level of quality and service.

X-ES

Extreme Engineering Solutions
608.833.1155 www.xes-inc.com

MADE IN THE USA

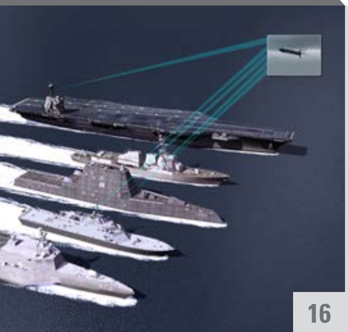
Designed, manufactured, and supported in the USA

Volume 13
Number 1

Military EMBEDDED SYSTEMS

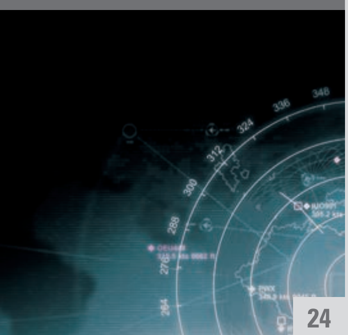
January/February 2017

www.mil-embedded.com

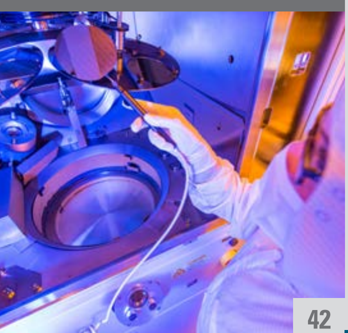


16

20



24



42

PERSPECTIVES: Executive Interview

SPECIAL REPORT

Radar Design Trends

MIL TECH TRENDS

Signal Processing Trends in Radar, Sonar, and Electronic Warfare

INDUSTRY SPOTLIGHT

RF and Microwave for Radar and Electronic Warfare Systems

COLUMNS

Editor's Perspective

Field Intelligence

Mil Tech Insider

Cybersecurity Update

DEPARTMENTS

ECAST

Leveraging the range of sub-1 GHz technology to connect ultra-low-power sensors to the cloud
Presented by Avnet
ecast.opensystemsmedia.com/718

WEB RESOURCES

Subscribe to the magazine or E-letter
Live industry news | Submit new products
http://submit.opensystemsmedia.com

White papers:
Read: http://whitepapers.opensystemsmedia.com
Submit: http://submit.opensystemsmedia.com

www.linkedin.com/groups/Military-Embedded-Systems-1864255

@military_cots

Published by:
OpenSystems media

ISSN: Print 1557-3222

ENVIROINK

ON THE COVER:

Top image:
The U.S. Navy's Surface Electronic Warfare Improvement Program (SEWIP) will leverage open architectures as it replaces the legacy AN/SLQ-32(V) electronic warfare system through a series of block upgrades. Photo courtesy of Lockheed Martin.

Bottom image:
System-performance requirements and open architectures are driving development of smarter radar and electronic warfare (EW) systems.


Proven Performance
GORE-FLIGHT™ Microwave Assemblies, 6 Series are ruggedized, lightweight and vapor-sealed airframe assemblies that withstand the challenges of aerospace.
With GORE-FLIGHT™ Microwave Assemblies, 6 Series, a fit-and-forget philosophy is now a reality – providing the most cost-effective solution that ensures mission-critical system performance for military and civil aircraft operators.
Find out why at:
www.gore.com/GORE-FLIGHT
GORE
Creative Technologies Worldwide
precision
lightweight
durability
GORE, GORE-FLIGHT, the purple cable and designs are trademarks of W. L. Gore & Associates.
Follow us on
You Tube

ADVERTISER INFORMATION

EVENTS

Unmanned Aircraft Systems Symposium – West
March 7-8, 2017 • San Diego, CA
www.uaswest.com

Navy League Sea – Air-Space Exposition 2017
April 3-5, 2017 • National Harbor, MD
www.seaairspace.org

AFCEA Spring Intelligence Symposium 2017
April 26-27, 2017 • Springfield, VA
www.afcea.org

Military EMBEDDED SYSTEMS

GROUP EDITORIAL DIRECTOR John McHale jmchale@opensystemsmedia.com
ASSISTANT MANAGING EDITOR Lisa Daigle ldaigle@opensystemsmedia.com
SENIOR EDITOR Sally Cole scole@opensystemsmedia.com
ASSOCIATE EDITOR Mariana Iriarte miriarte@opensystemsmedia.com
DIRECTOR OF E-CAST LEAD GENERATION AND AUDIENCE ENGAGEMENT Joy Gilmore jgilmore@opensystemsmedia.com
CREATIVE DIRECTOR Steph Sweet ssweet@opensystemsmedia.com
SENIOR WEB DEVELOPER Konrad Witte kwitte@opensystemsmedia.com
WEB DEVELOPER Paul Nelson pnelson@opensystemsmedia.com
DIGITAL MEDIA MANAGER Rachel Wallace rwallace@opensystemsmedia.com
CONTRIBUTING DESIGNER Joann Toth jtoth@opensystemsmedia.com

VITA EDITORIAL DIRECTOR Jerry Gipper jgipper@opensystemsmedia.com
INDUSTRY EDITOR Jessica Isquith jisquith@opensystemsmedia.com

SALES

SALES MANAGER Tom Varcie tvarcie@opensystemsmedia.com (586) 415-6500
MARKETING MANAGER Eric Henry ehenry@opensystemsmedia.com (541) 760-5361
STRATEGIC ACCOUNT MANAGER Rebecca Barker rbarker@opensystemsmedia.com (281) 724-8021
STRATEGIC ACCOUNT MANAGER Bill Barron bbarron@opensystemsmedia.com (516) 376-9838
STRATEGIC ACCOUNT MANAGER Kathleen Wackowski kwackowski@opensystemsmedia.com (978) 888-7367
SOUTHERN CAL REGIONAL SALES MANAGER Len Pettek lpettek@opensystemsmedia.com (805) 231-9582
SOUTHWEST REGIONAL SALES MANAGER Barbara Quinlan bquinlan@opensystemsmedia.com (480) 236-8818
NORTHERN CAL STRATEGIC ACCOUNT MANAGER Sean Raman sraman@opensystemsmedia.com (510) 378-8288
ASIA-PACIFIC SALES ACCOUNT MANAGER Elvi Lee elvi@aceforum.com.tw
BUSINESS DEVELOPMENT EUROPE Rory Dear rdear@opensystemsmedia.com +44 (0)7921337498

OpenSystems media®
WWW.OPENSYSTEMSMEDIA.COM

PUBLISHER Patrick Hopper phopper@opensystemsmedia.com
PRESIDENT Rosemary Kristoff rkristoff@opensystemsmedia.com
EXECUTIVE VICE PRESIDENT John McHale jmchale@opensystemsmedia.com
EXECUTIVE VICE PRESIDENT Rich Nass rnass@opensystemsmedia.com
CHIEF TECHNICAL OFFICER Wayne Kristoff
EMBEDDED COMPUTING BRAND DIRECTOR Rich Nass rnass@opensystemsmedia.com
EMBEDDED COMPUTING EDITORIAL DIRECTOR Curt Schwaderer cschwaderer@opensystemsmedia.com
TECHNOLOGY EDITOR Brandon Lewis blewis@opensystemsmedia.com
CONTENT ASSISTANT Jamie Leland jleland@opensystemsmedia.com
CREATIVE PROJECTS Chris Rassiccia crassiccia@opensystemsmedia.com
INDUSTRY EDITOR Jessica Isquith jisquith@opensystemsmedia.com
FINANCIAL ASSISTANT Emily Verhoeks everhoeks@opensystemsmedia.com
SUBSCRIPTION MANAGER subscriptions@opensystemsmedia.com

CORPORATE OFFICE
16626 E. Avenue of the Fountains, Ste. 201 • Fountain Hills, AZ 85268 • Tel: (480) 967-5581

SALES AND MARKETING OFFICE
30233 Jefferson • St. Clair Shores, MI 48082

REPRINTS

WRIGHT'S MEDIA REPRINT COORDINATOR Wyndell Hamilton whamilton@wrightsmedia.com (281) 419-5725

President Trump, sequestration, and the COTS market

By John McHale, Editorial Director

During his campaign for the presidency, Donald Trump promised increased military spending if elected. Now that he has assumed office, many in the defense electronics industry have their fingers crossed that he will follow through.

The hope of increased defense funding following a Republican presidential win after eight years of Democratic rule is not a new concept. Back in 2000, I was on the floor of the COTSCon West show in San Diego when an announcement was made that the Supreme Court had ruled – about a month after the presidential election – in favor of George W. Bush. A cheer went up from the exhibitors and attendees, as they knew that meant increased business for them. They deemed it a certainty.

With a Republican president backed by a Republican Congress in 2017, it would also seem a certainty that a healthier defense market is just around the corner, but Donald Trump is not a traditional Republican – having been a Democrat most of his life – so the industry is cautiously optimistic.

However, if Trump and the Republican-led Congress end sequestration – the automatic, across-the-board cuts to the defense budget – then he will be a hero to military leadership, prime contractors, system integrators, and commercial off-the-shelf (COTS) suppliers.

Sequestration has cost thousands of defense industry jobs, slowed product development, hindered platform upgrades, and, if it continues, will likely hurt military readiness, if it hasn't already.

Former chairman and CEO of Lockheed Martin, Bob Stevens, once called sequestration "a meat axe." Cutting across the board is "an inefficient way to manage a business," he said back in 2012, fearing the loss of thousands of jobs within the U.S. defense sector.

He was right. "The impact to date has meant the loss of tens of thousands of good, high-paying jobs in the defense industry, as well as the delay or cancellation of many national security programs," said Bobby Sturgell, senior vice president of Washington Operations for Rockwell Collins and former acting administrator of the Federal Aviation Administration (FAA) in a roundtable article on mil-embedded.com.

Sometimes it seems sequestration was designed so congressional leaders and the president could avoid making decisions. We need leaders more concerned with solving problems than passing them off to their successors. In this sense, sequestration is like procrastination; the more you procrastinate on solving a problem, the worse it becomes.

Trump touts himself as a problem solver. If he works with Congress to successfully end sequestration, it will ultimately be a win for the defense industry.

Some think he will do just that. "Whether you like him or not, he is an action-oriented businessperson," said Eric Sivertson, founder and CEO of QuantumTrace, earlier this year in an article titled "Presidential politics and defense electronics." "Sequestration has created problems for the business industry and he [was] the only candidate taking a firm stand. However, it may not be a good thing at first for defense firms as he would likely kill programs, but he will remove the malaise of sequestration."

Trump and COTS

An end to sequestration and increased defense funding still may not mean more funding for COTS technology. With sequestration gone, the budget will be more aligned with mission priorities. Those priorities will determine whether funding addresses more troop deployments or investment in technology research and development (R&D).

More mission clarity will enable more certainty on spending directions, enabling industry to channel their internal R&D dollars appropriately.

If mission requirements call for more intelligence, surveillance, and reconnaissance, radar, and electronic warfare technology, then the outlook for embedded computing suppliers will be bright.

And doubly so, as the push toward commonality resulting from the budget restraints will likely grow as DoD leaders see the associated cost advantages. It's a new procurement reality and likely to continue under a Trump Administration that prides itself on trimming expensive platforms such as the F-35.

Trump's appointment of retired Marine Corps General James Mattis as DoD Secretary also bodes well for more mission clarity. Military historian Thomas Ricks says in article on ForeignPolicy.com, titled "Mattis as defense secretary, what it means for us, the military, and for Trump," that Mattis is a strategic thinker, an avid reader, a fiscal conservative, a straight shooter, and loved by the troops.

"In the long run I think [a Trump presidency] will be excellent for the defense industry, but in the near term a Trump presidency will create even more pain, more than Clinton or Sanders would," Sivertson added. "Trump is all about the art of the deal; he will make deals and some will be painful, but it will probably be the right pill the DoD needs to take to clean it up and make it more economically efficient."

Software: King of SWaP

By Charlotte Adams

An Abaco Systems perspective on embedded military electronics trends

Developers of the processing systems aimed at deployment on unmanned aerial vehicles (UAVs) and other small, intelligent, sometimes battery-operated platforms at the tactical edge find it increasingly important to scrutinize hardware and software to maximize size, weight, and power (SWaP) considerations.

Hardware issues

System developers often start the design process with a list of hardware specifications: the size of a box, its processing throughput, the power budget, and cooling requirements. Other decisions involve the form factor of the board or boards, the memory space – it may not be much – the I/O fabric, and the processing chips.

Special-purpose graphics processing units (GPUs), for example, might improve throughput by such a wide margin that they are the go-to silicon. GPUs burn a lot of power, but if one GPU can do the work of four or five general-purpose processors, it would save system size, weight, and power. Small platforms need just enough performance to do the job – that is, not too much. Program managers want room for growth but do not want to leave unused MIPS or FLOPS – and associated power penalties – on the table.

To maximize collaboration between software and hardware, application developers require real-time, dynamic, and highly granular insights into hardware metrics such as CPU utilization and timing issues, CPU events such as cache and pipeline stalls, number of interrupts, memory bottlenecks, and inefficiencies at every step in the execution of an algorithm.

Software to optimize SWaP

Good software-development tools provide windows into the software's potential and actual interaction with the hardware, allowing the application to be tuned to execute with the fewest penalties. Among the most important tools at the developer's disposal are middleware libraries; math libraries; and algorithm optimization, profiling, and visualization software.

Middleware is a key to application performance and power efficiency. Middleware has many roles, one of the most important of which – in embedded applications – is to enable the most effective distribution of data between hardware nodes. Modern CPUs typically are designed as complex multiprocessors on a chip, where each core can run many threads simultaneously. The smaller the embedded system, the more critical efficient data flows become.

A popular middleware choice is MPI (message passing interface), which is available in open-source and proprietary implementations. For reasons having to do with its origins in processor-rich environments such as data centers, some versions of MPI are more focused on low latency than on power efficiency. A typical example of a middleware-induced inefficiency is the "spin loop." This event occurs when a processor waits for data to arrive while consuming cycles, burning power, and dissipating heat without accomplishing anything. A better approach for miserly embedded systems is to let the cores either sleep or perform other tasks while waiting for data to arrive.

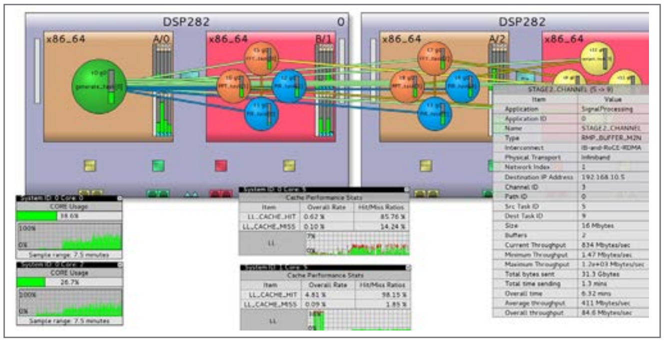


Figure 1 | Abaco's AXIS software-development environment can help identify how well code runs on the target hardware, which enables designers to optimize SWaP up front.

Another tool for tuning applications involves optimization of algorithms, the core logic that instructs the computer how to execute its functions. The more efficiently the algorithm is coded, the faster the application.

Software analysis, however, requires insight not only into the structure of the code but into how well the program executes on the target hardware. Especially where deterministic performance is required, developers must identify bottlenecks and scrutinize functions that may be consuming excessive processor time or memory space. Much of this information can be gleaned by visualizing timing issues as the code is running via an intuitive graphical user interface (GUI) that highlights performance issues across multiple cores and their distributed threads.

An example of such technology is Abaco Systems' AXIS Pro toolkit, which includes an integrated GUI, optimized MPI libraries, extensive math function libraries, and the EventView profiling and analysis program. (Figure 1.) All of the tools are aimed at reducing the complexity, time, and cost of developing and debugging multiprocessor embedded applications without getting lost in the hardware weeds.

Accurate, immediate, and detailed insight into the interaction between the software and the hardware is the best recipe for a successful, SWaP-optimized system.

www.abaco.com

Best practices for COTS supplier counterfeit mitigation

By Larry McHenry

An industry perspective from Curtiss-Wright Defense Solutions

Leading commercial off-the-shelf (COTS) vendors and military/aerospace electronics suppliers routinely engage with customers and suppliers in the development and maintenance of internal processes for the mitigation and prevention of counterfeit electronics components.

Many of the best practices for counterfeit mitigation – including methods, systems, and trend monitoring – result from participation in industry committees. Leading the way in efforts to circumvent counterfeiting are the Society of Automotive Engineers' (SAE's) [www.sae.org] G19 committee and various other industry consortia, such as the Electronic Resellers Association International (ERAI) and the Independent Distributors of Electronics Association (IDEA).

The continued development and evolution of important standards and methods of practice results from ongoing, in-depth partnerships with suppliers and customers and through development of multidisciplined counterfeit-mitigation systems. New relevant regulatory standards are continually released: For example, the SAE's AS6174 ("Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel") standard now includes nonelectrical component counterfeit mitigation. Defense and aerospace suppliers – all of whom are routinely audited by customers to illustrate their compliance for electrical, electronic, and electromechanical (EEE) parts – must now evolve their methods in recognition of the non-EEE component counterfeit threat.

In addition, suppliers must also be prepared to address customer-specific counterfeit-mitigation standards. Globally, supply-chain and quality professionals focus their efforts on acquisition of parts from trusted sources including franchised distribution and/or direct from original component manufacturers/original equipment manufacturers (OCMs/OEMs). Most have processes in place to engage suppliers to test, source, certify, and track alternate sources of components where required.

The ability to audit compliance with today's existing standards and with emerging new standards requires a deep knowledge of the industry and of trusted franchised distributors to ensure that the OCM/OEM chain of custody is in place all the way from the OEM through to the component's sale. An interdisciplinary approach in organizations is not restricted to supply-chain management, but must also include a partnership with the COTS supplier's engineering, quality engineering, regulatory and procurement, and life-cycle services teams.

Supply-chain organizations should minimize the risk of obsolescence by executing "last-time buys" (LTB) to extend product life and avoid the need to procure obsolete parts from brokers post-LTB.

In the situation where a component does become obsolete, the supply chain should consider nonfranchised sources only where there is no drop-in alternative. In such a case, applicable internal or external approvals are pursued if a broker-sourced part is to be used, and then only from a limited and approved source base. These sources must be subject to intense audits, and any device provided by a broker must be tested by the source's internal or accredited labs in compliance with customer (if required), supplier, and industry-mandated validation methods. When an authenticated broker part is used, the COTS supplier must perform disciplined configuration-control practices to ensure that the brokered part receives a unique part number.

To ensure that their supplier is staying up to date with the latest trends in underworld counterfeiting and the most up-to-date techniques for mitigating them, systems integrators should query their supplier about what industry organizations they are members of and/or which they actively monitor. Maintaining membership in and monitoring the latest proposals from committees such as SAE G19 AS5553 is critical for staying ahead of the counterfeit game.

Leading COTS suppliers should monitor vocal industry and nongovernmental agencies that report on and track sources of and trends in detected counterfeit materials. It's also important for COTS suppliers to monitor counterfeit occurrences and share these experiences via reporting bodies such as the Government Industry Data Exchange Program (GIDEP), the U.K.'s ESCO Council, and counterfeit-mitigation suppliers such as ERAI. Active involvement and communication with these bodies is critical for reducing the risk posed by counterfeits; it is the COTS industry's duty to report violators in order to prevent any further violations.

One proven way of verifying a COTS supplier's ability to mitigate counterfeits is to ask what formal certifications they have earned, such as AS5553, AS6081, or ISO/IEC 17025. Recently, SAE released a technical certification in their NADCAP [National Aerospace and Defense Contractors Accreditation Program] suite that will provide technical acknowledgement, via auditing, that a supplier adheres to AS5553 requirements.

In addition, that old adage made popular by President Ronald Reagan, "Trust, but verify," comes into play: Trust in your supplier's certification but verify by their performance to ensure that they, and any brokers and distributors they use, have demonstrated their commitment and adherence to the world of counterfeit mitigation and prevention.

***Larry McHenry**, CET/CQE, is senior manager for Quality Assurance, C4S-ISR, for Curtiss-Wright Defense Solutions.*

www.cwcdefense.com

DEFENSE TECH WIRE

NEWS | TRENDS | DOD SPENDS | CONTRACTS | TECHNOLOGY UPDATES

By Mariana Iriarte, Associate Editor

NEWS

Harris Corp. tapped for $91 million in EW systems on RMAF fleet

Harris Corporation won a $91 million contract to provide its AN/ALQ-211 Advanced Integrated Defensive Electronic Warfare Suite (AIDEWS) systems to the Royal Moroccan air force (RMAF) for installation on its fleet of F-16 aircraft.

The Harris AIDEWS system is a modular electronic warfare (EW) solution that includes radar warning and radio-frequency countermeasures capabilities. In addition, it is compatible with a variety of aircraft and is available in an externally mounted pod.

Harris is also on tap to provide support equipment and services that will help protect the RMAF's fleet of F-16 aircraft – made by General Dynamics and known as the "Fighting Falcon" – against current and evolving electronic threats.

Figure 1 | An F-16 Fighting Falcon departs after being refueled. Photo courtesy of U.S. Air Force/Senior Airman Solomon Cook.

NATO country buys $17 million multispectral vision system from Elbit

Elbit Systems won a $17 million/30-month contract to supply its BrightNite multispectral helicopter-pilot vision systems to an air force in a NATO country; the company did not specify the country in the announcement.

According to Elbit, the BrightNite panoramic piloting solution delivers the landscape scenery – including 2-D flight symbology and 3-D mission symbology – directly to both eyes of the pilot, which enables intuitive head-up, eyes-out orientation flight in full darkness, sandstorms, whiteouts, and other low-visibility conditions.

The multispectral sensor constructs the scenery picture by fusing multiple day and night cameras into a single image that is projected onto a pilot's helmet visor, regardless of exterior light conditions.

Marine F-35B squadron relocates to Japan

Marine Fighter Attack Squadron (VMFA) 121 "Green Knights," an F-35B squadron with the 3rd Marine Aircraft Wing, recently left Marine Corps Air Station Yuma and has transferred to Marine Corps Air Station Iwakuni, Japan.

The squadron's move is a first, says Maj. Michael O'Brien, the operations officer for VMFA-121: "It's the first time that any fifth-generation fighter unit has moved and been permanently based overseas, specifically in Japan."

The F-35B short takeoff/vertical-landing aircraft combines stealth measures, radar and sensor technology, and updated electronic warfare systems. Data and lessons learned during field testing at sea during 2016 laid the groundwork for planned F-35B deployments aboard U.S. Navy amphibious carriers, the first two of which will take place in 2018.

DARPA awards Sikorsky ALIAS Phase 3

The Defense Advanced Research Projects Agency (DARPA) awarded Sikorsky with Phase 3 of the Aircrew Labor In-Cockpit Automation System (ALIAS) program, a package of hardware, software, and sensors that are aimed at capitalizing on advances in autonomy to reduce pilot workload, augment mission performance, and improve aircraft safety and reliability.

In the first two phases of the program, Sikorsky integrated its Matrix Technology into Sikorsky's Autonomy Research Aircraft (SARA) and also placed the system on a Cessna Caravan.

The National Aeronautics and Space Administration (NASA), the U.S. Air Force, the U.S. Army, and the U.S. Navy have expressed interest and are providing support to the program. These stakeholders and DARPA say that they intend to continue working closely with government and commercial bodies to identify potential transition opportunities for ALIAS technology.

Figure 2 | DARPA's ALIAS program demonstrates its technology on a Sikorsky S-76 helicopter during Phase 2 flight tests. Photo courtesy of DARPA.

U.S. Navy officials accept delivery of 50th P-8A Poseidon aircraft

U.S. Navy officials accepted the 50th P-8A Poseidon (P-8A) aircraft at the Naval Air Station (NAS) Jacksonville, Florida. The P-8A program of record calls for a total requirement for 117 of the 737-based antisubmarine warfare jets. The fleet is expected to convert fully to the P-8A by fiscal year 2019.

Officials say that the Poseidon, which is replacing the legacy P-3 Orion, will improve an operator's ability to conduct antisubmarine warfare; antisurface warfare; and intelligence, surveillance, and reconnaissance (ISR) missions. The program has reduced P-8 costs by more than 30 percent since the initial contract award; officials say that this cost reduction has saved the U.S. Navy more than $2.1 billion.

"The P-8A is special," says Capt. Tony Rossi, the Navy's program manager for Maritime Patrol and Reconnaissance Aircraft. "This is the first time a Navy combat aircraft was built from the ground up on a commercial production line. We've leveraged commercial expertise and experience, and a highly reliable airframe, the 737, which has reduced production time and overall production costs."

Figure 3 | All squadrons will complete transition training from the P-3C to the P-8A by fiscal year 2019. Photo courtesy of the U.S. Navy.

DoD approves Raytheon's SM-6 missile for international sales

U.S. Department of Defense (DoD) officials have approved the release of Raytheon's Standard Missile-6 (SM-6) to several international customers.

Officials say that most of the countries approved for the sale are seeking the SM-6 to bolster their shipbuilding programs. In the U.S., SM-6 currently provides Navy vessels with extended-range protection against fixed- and rotary-wing aircraft, unmanned aerial vehicles (UAVs), cruise missiles, and ballistic missiles in the terminal phase of flight.

In April 2015, Raytheon delivered the first full-rate production SM-6 from its production facility at Redstone Arsenal in Huntsville, Alabama. To date Raytheon has delivered more than 300 SM-6 missiles, with continuing production.

Saab signs agreement to invest and grow its business in New York

New York state and officials from Saab have signed an agreement to develop Saab's business in the U.S. and increase its local presence. The goal is to drive technology transfers, improve facilities, and grow organic engineering, research, development, testing, and production capabilities.

Under the agreement, Saab will invest in its subsidiary, Saab Defense and Security USA, and will relocate its U.S. headquarters to the company's Syracuse-based office. The state will also provide Saab with incentives aimed at supporting Saab's efforts, which are expected to stimulate industrial growth and create new jobs within Saab's New York-based subsidiaries.

Michael Andersson, Head of Market Area North America for Saab says, "[New York state] will experience an influx of technology and job growth, and Saab will continue to develop our capabilities and expand our U.S. footprint."

Textron starts on-water testing of unmanned maritime vehicle

Textron System Unmanned Systems has begun on-water testing for the fourth-generation Common Unmanned Surface Vehicle (CUSV) – a multimission unmanned surface vehicle with a large, configurable payload bay – that is supporting the U.S. Navy's Unmanned Influence Sweep System (UISS) mine-countermeasure program.

The CUSV is capable of carrying multiple payloads, including side-scan sonar; mine-neutralization apparatus; nonlethal weapons; and ISR sensors.

Textron Systems is slated to hold builders' trials upon completion of the integration and test phase and then move into formal testing to validate system functionality with the U.S. Navy later in 2017.

Figure 4 | Textron Systems completed the design, build, and component test phases of the UISS program in November 2016. Photo courtesy of Textron Systems.

EXECUTIVE INTERVIEW

Open architecture's role in avionics and electronic warfare designs

By Mariana Iriarte, Associate Editor

Ed Zoiss

An F/A-18C Hornet assigned to Strike Fighter Squadron (VFA) 34 takes off from the aircraft carrier USS Carl Vinson (CVN 70) during flight operations. (U.S. Navy photo by Mass Communication Specialist 2nd Class Sean M. Castellano/Released)

Enabling commonality across multiple platforms is a priority within the U.S. Department of Defense (DoD) procurement authority for new and upgraded avionics platforms and this open architecture approach is gaining traction in the electronic warfare community as well. In this Q&A with Ed Zoiss, president of the Electronic Systems segment at Harris, he discusses how Harris and Boeing are pursuing open architectures in their collaboration, which is focused on developing next-generation military avionics systems, the impact of reduced size, weight, and power (SWaP) on electronic warfare (EW) technology, and how increasing complex threats are driving mission funding of both avionics and EW systems. Edited excerpts follow.

MIL-EMBEDDED: ***Please provide a brief description of your responsibility within Harris and your group's role within the company.***

ZOISS: I've been with Harris for 22 years and currently am president of the Electronic Systems segment at Harris, which is one of four segments within the company. Electronic Systems, which generates about $4.5 billion in revenue annually, develops high-performance avionics, electronic warfare systems, wireless solutions, command, control, communications, computers and intelligence (C4I) systems, and undersea systems, for defense electronics applications.

MIL-EMBEDDED: ***Harris recently announced its collaboration with Boeing Phantom Works for next-generation avionics technology. Can you provide details on that effort and how the future avionics systems will enable commonality through open architectures and commercial off-the-shelf (COTS) solutions?***

ZOISS: It is a proof point of where the whole industry is headed. An excellent example is the Future Airborne Capability Environment (FACE) consortium, developed by NAVAIR (U.S. Naval Air Systems Command). Harris is a founding member of the consortium. FACE is a standards body focused on driving industry and government together to deliver solutions faster to the warfighter that are affordable and not proprietary, but rather based on a common standard.

Along those lines, Harris and Boeing are working together to deliver an open systems architecture, based on open standards that builds off our long-standing relationship with Boeing, which includes supplying avionics for the F/A-18 aircraft.

Open systems are the future of avionics and we are investing heavily in developing these solutions. Where standards may fail is when user-defined elements are added to a piece of hardware. Once that happens, it is no longer an open architecture, but more proprietary. The work we are doing with Boeing works to avoid this and enable more commonality in future avionics systems. The collaboration will create advanced core mission processing architectures to manage many of an aircraft's

critical capabilities, such as communication, sensors, navigation, and displays. Under the partnership, Harris will produce the collaborative design for the common processing hardware that will be integrated with the Boeing Secure Computing Solution hardware, Boeing Phantom Fusion mission software, and a multilevel communication network.

Harris will provide custom-designed high-speed interfaces, security, COTS processors, and military-quality packaging to enable scalable mission processing via open system architectures. We will design modules or a community of modules that will enable open system performance by leveraging solutions such as fiber-optic backplanes and switched-fabric standards.

MIL-EMBEDDED: ***How do you manage the associated obsolescence challenges that come with COTS use?***

ZOISS: We work with our customer on managing the product life cycle process, which can get especially expensive and complicated because of the required recertification of safety-critical avionics components. We factor in obsolescence mitigation of COTS components from the start of the process by refraining from using sole-source providers, leveraging instead multisourced systems, subsystems, and components. Having multiple choices on sourcing is the most effective way to mitigate obsolescence challenges.

> OPEN SYSTEMS ARE THE FUTURE OF AVIONICS AND WE ARE INVESTING HEAVILY IN DEVELOPING THESE SOLUTIONS. WHERE STANDARDS MAY FAIL IS WHEN USER-DEFINED ELEMENTS ARE ADDED TO A PIECE OF HARDWARE.

MIL-EMBEDDED: ***Reduced SWaP requirements are hitting all applications in defense electronics. How are they impacting future avionics designs? What are the tradeoffs with smaller tech?***

ZOISS: In rotary-aircraft avionics, reduced SWaP is critical. For example, on platforms such as the MH-60 Blackhawk and the MH-47 Chinook, each of which carry quite a bit of mission equipment, keeping the weight down is a huge challenge. Therefore, as we modernize an avionics system, the first thing we look at is how to reduce SWaP.

For EW, customers SWaP is also important, which is why we developed our small-form-factor Disruptor SRx – a multifunction EW system. By reducing SWaP you can enable EW in places never before contemplated, such as on small umanned aircraft systems (UAS) platforms. As platforms become smaller, inspiring creativity with electronic designs expands the market opportunities exponentially. You can innovate small SWaP around full communications or EW subsystems to develop completely new uses such as networking systems that were never networked before. The requirement we hear over and over again from our customer is for more multifunctionality, such as having electronic intelligence (ELINT) and signals intelligence (SIGINT) functions in one system with the ability to switch between them and in smaller packages.

As the technology curve moved away from analog toward digital systems and the size of electronics scaled down with Moore's Law, you no longer need all the real estate you needed in the B-1 Bomber, for example. EW systems today are vastly different in capability and size; I think this trend will continue.

MIL-EMBEDDED: ***With fewer new aircraft platforms being developed, the military avionics market seems to be one of sustainment and upgrades/refreshes. Do you agree with that statement and how do you see this market behaving the next few years? Do you include UAS avionics in your assessment?***

ZOISS: What's really driving the market are new threats, which are becoming much more peer. As the DoD looks at its inventories of systems – air, ground, and sea – they are determining which systems need upgrades. These upgrades are not based in the old sense of managing life cycles or adding capability, rather modernizations are being determined based on the mission they must perform or the threat they have to counter, such as a threat with an agility we haven't seen before. As they look to upgrade to this new environment there is also technology being developed across the services to leap past current threats.

The modernization of the electronics in these upgrades will mostly leverage non-proprietary systems enabling commonality and allowing industry to participate in ways they couldn't in the previous market environment, as with our partnership with Boeing.

Unmanned aircraft have traditionally been focused ISR missions in permissive airspace, but now our customers are exploring new applications such as swarming teams of small

UAS – with one aircraft acting as the eyes, one as the ears, one for deploying weapons, etc., the swarm is essentially a network. At Harris we are working on how to enable aircraft to form this network. This new generation of UAS, yet to be born, is a whole new market that will be enabled by smaller UAS with reduced SWaP in their electronics.

MIL-EMBEDDED: ***Please provide an example of other current avionics platforms that Harris supports.***

ZOISS: Harris has avionics on virtually every military aircraft. In addition to the F/A-18 mentioned above, we're also on the F-35, and the F-22 Raptor. Our solutions are provided both for U.S. and international platforms, and ranging from mission processors to smart weapons release units.

MIL-EMBEDDED: ***Another area under your responsibility at Harris is for electronic warfare (EW) solutions. Traditionally this niche has been slower to adapt open architectures and commonality than other military application areas? Is that changing and if so how?***

ZOISS: It is changing, but slowly. Often EW solutions are particular to the hardware they run on, so it will take time for a transition to more open standards to evolve. Our customers are definitely thinking along those lines and we are also preparing. To apply open standards, you begin at the chassis level, develop the common backplane interfaces, and then move toward replacing modules, which are often the most vendor-specific, meaning they are not compatible with other vendor designs. Developing commonality at that level will take time, but the military customers are discussing that path and industry is starting to align to those goals.

MIL-EMBEDDED: ***Please name/describe current EW platforms Harris supports?***

ZOISS: Along with the Disruptor SRx, we produce EW solutions for the B-52 bomber and F-16, F/A-18, B-1B, B-52, as well as ground-based EW solutions to the Special Operations Command (SOCOM) and the Marine Corps.

A good deal of our EW business is also international. For example we develop advanced EW systems for allied F-16 platforms. Sophisticated EW systems are in demand internationally because, like the U.S., nations such as Chile, Pakistan, Morocco, etc., need to counter similar threats in their regions.

MIL-EMBEDDED: ***Recent budget requests from the DoD showed increased funding efforts for EW technology. How do you view the DoD funding outlook for these systems?***

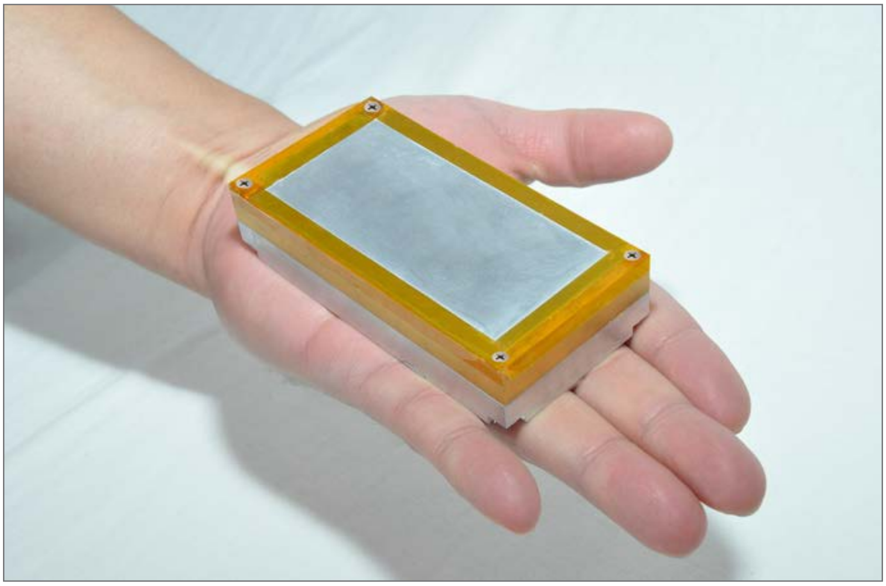


Figure 1 | The Harris Disruptor SRx. Photo courtesy of Harris.

ZOISS: I do think military customers will spend more on EW. There is always a tradeoff on whether to add new capability through new platforms versus modernization of existing platforms. Regardless, everyone needs these new avionics systems and new EW capabilities to counter threats, so I see robust funding going forward for this technology.

MIL-EMBEDDED: ***Looking forward, what disruptive technology/innovation will be a game changer for avionics and electronic warfare technology? Predict the future.***

ZOISS: The game changer for avionics is in open systems and will continue to be so, but total adoption of open architectures will take time.

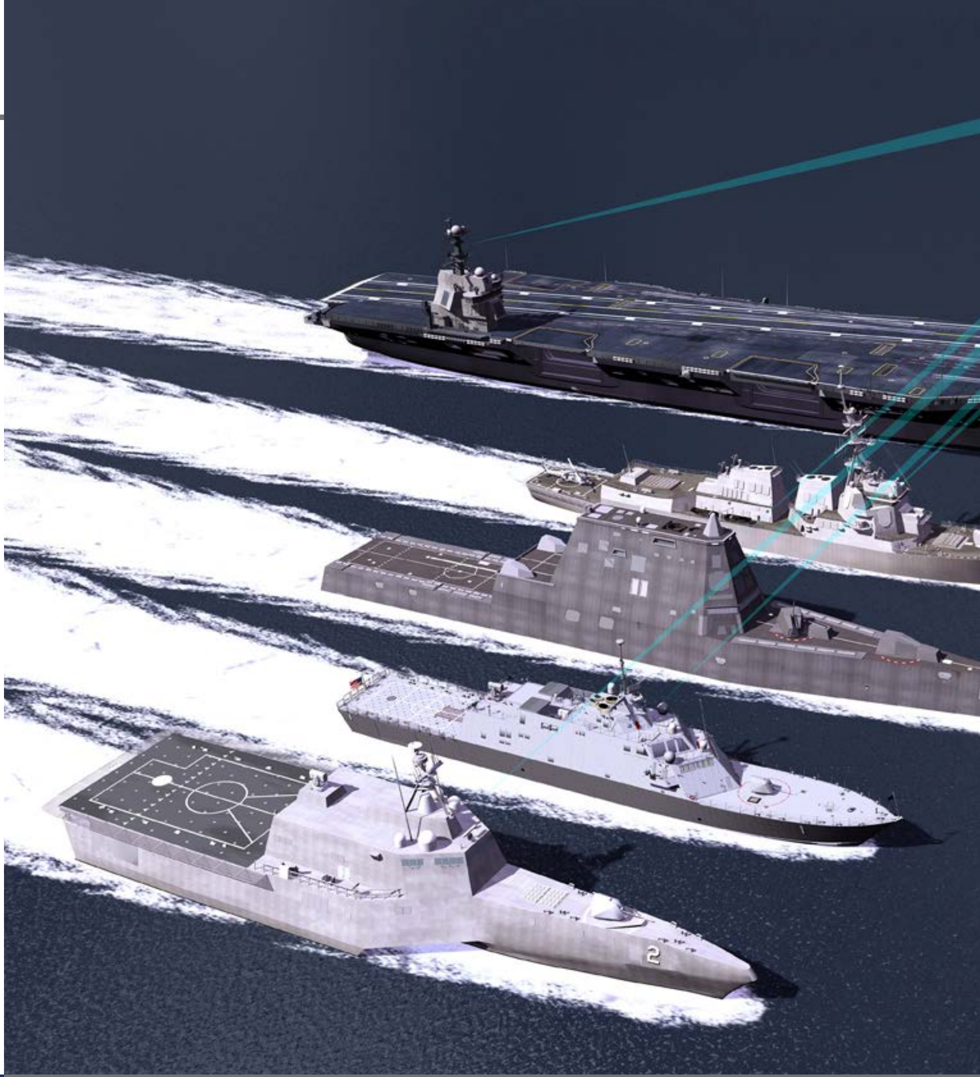
For electronic warfare, it will be the development of adaptive and cognitive EW to counter threats that are becoming more agile, more complex, more adaptable and all in real time. Harris is investing in this technology and creating techniques for EW systems to adapt on the fly to counter any threat. We are working on it, along with many others, to mature these technologies. **MES**

Edward J. (Ed) Zoiss, *president of Harris Corporation's Electronic Systems segment, is responsible for business strategy, financial performance, successful execution, and growth for Electronic Systems, which covers solutions in electronic warfare, avionics (including carriage and release systems), wireless solutions, C4I systems, and undersea systems. Previously, he was vice president and general manager of the defense business unit within Harris Government Communications Systems. Prior to that role, he served as vice president of C4ISR Electronics, which provided specialized solutions to defense, intelligence, and public-safety agencies. Before assuming responsibility for the C4ISR business, Zoiss was vice president of Advanced Programs and Technology, where he led the division strategy, business development, marketing, and all internal research and development. Joining Harris in 1995 as a principal mechanical engineer, Zoiss assumed positions of increasing responsibility, including director of research and development and vice president of business development for National Programs. He is the recipient of 13 patents. Zoiss received his undergraduate degree from the United States Merchant Marine Academy at Kings Point, New York, and his master's in mechanical engineering from California State University at Northridge. In addition, he received an honorable discharge from the U.S. Navy as a lieutenant.*

Cognitive electronic warfare: Countering threats posed by adaptive radars

By Sally Cole, Senior Editor

Threats posed by adaptive radars to electronic warfare systems are a colossal challenge for the U.S. Navy, but a combo of advanced signal processing, intelligent algorithms, and machine learning techniques are being developed to help warfighters detect and counter them.



The U.S. Navy's Surface Electronic Warfare Improvement Program (SEWIP) will leverage open architectures as it replaces the legacy AN/SLQ-32(V) electronic warfare system through a series of block upgrades. Photo courtesy of Lockheed Martin.

Electronic warfare (EW) systems – whether on land or aboard U.S. military ships and aircraft – tap the electromagnetic spectrum to sense, protect, and communicate. But, when necessary, these same systems can be turned against adversaries to deny their ability to disrupt or use radio, infrared, or radar signals.

Today's EW systems tend to rely on databases of known threats with predefined countermeasures, which can limit their ability to quickly adapt and respond to new advanced threats. Soon, these systems may increasingly be tasked with isolating unknown hostile radar signals within dense electromagnetic environments and responding quickly with effective electronic countermeasures.

Threats from adaptive radars aren't necessarily new, according to Joe Ottaviano, director, Electronic Warfare, for Lockheed Martin (www.lockheed-martin.com), but are challenging for EW systems to detect.

Years ago, back when the U.S. Navy's Surface Electronic Warfare Improvement Program (SEWIP) Block 1, 2, and 3 were formed, "it was a key requirement to be able to detect and counter adaptive radars to provide warfighters with the best information about the radar and its mission," Ottaviano explains. "We need to do this while performing our mission – before the enemy knows we're there. Block 2 is designed to deal with adaptive radars."

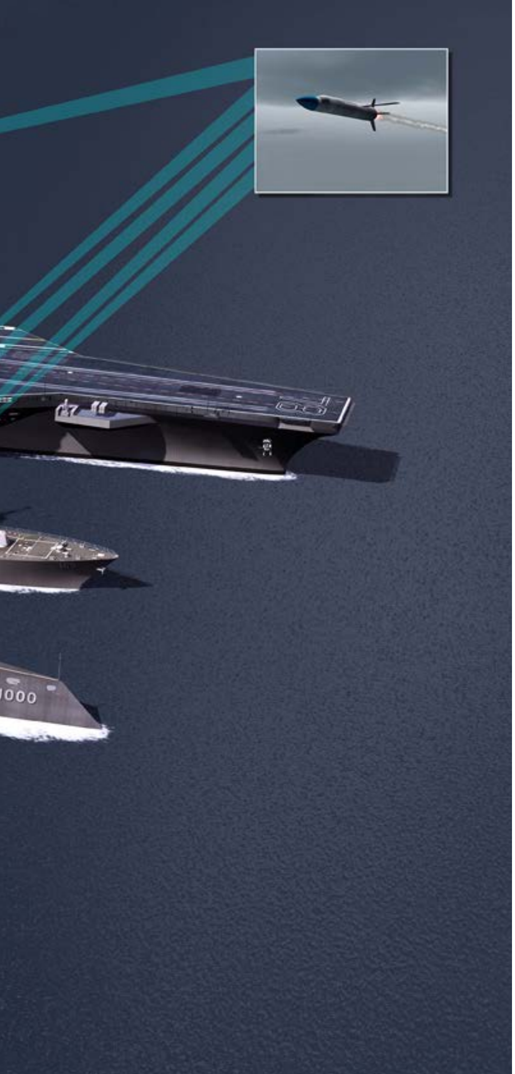
BAE Systems (www.baesystems.com), another defense contractor working within the realm of adaptive radars, was recently awarded a $13.3 million contract by the U.S. Defense Advanced Research Projects Agency (DARPA) to extend its work on the Adaptive Radar Countermeasures (ARC) project, with the goal of enabling airborne EW systems to counter new, unknown, and adaptive radars in real time.

Cognitive EW technologies developed by BAE Systems for the ARC project rely on advanced signal processing, intelligent algorithms, and machine-learning techniques.

Adaptive radar vs. "unknown" radar

Adaptive radars, for starters, shouldn't be confused with "unknown radars," both of which cognitive EW addresses, as John Tranquilli, technical director for signals and communications processing at BAE Systems, points out.

Both radar types do pose challenges for EW systems and warfighters, albeit with differences. "For the class of unknown radars, current systems rely on a database of threat knowledge to compare observed characteristics to a list of known radars," Tranquilli explains. "When a radar comes up as unknown or is misclassified as some other radar – because it's either a really new radar or an existing one that's behaving



outside prior known bounds – today's systems have very limited ability to characterize the threat or turn around an appropriate response."

Radars are currently evolving away from fixed analog systems – which aren't easy to add new capabilities to – toward digitally programmable variants that can easily add or change to unknown behaviors with agile waveform characteristics. "This challenge will increase the prevalence of 'unknown radars' and lead to truly adaptive radars," Tranquilli continues.

Adaptive radars, which pose an even greater challenge, can sense their environment and design transmission characteristics on the fly to maximize radar performance. "This allows a radar to have new waveforms – or new pulse processing – for every transmission, whether it's improving target resolution or mitigating interference effects," Tranquilli says.

The objective of cognitive EW "is to enable EW systems to autonomously characterize these threats, automatically generate effective countermeasures against them, and monitor the effectiveness of our countermeasures so we can adapt our techniques if they're either ineffective or if an adaptive radar attempts to adapt around our responses," he adds.

Recognizing and countering adaptive radars

How complex is recognizing and countering hostile adaptive radars? It falls under the category of "very complex."

For SEWIP, a significant amount of software was developed as part of Block 2 to specifically address these challenges. "While development is a challenge, testing is becoming even more of a challenge," Ottaviano notes. "Defining what's effective and how effective the detection and response are requires a tremendous effort. We're working with our Navy partners to continue to improve how we define success within a highly adaptive environment … and right now it's our biggest challenge."

From BAE Systems' perspective, "adaptive radars challenge our ability to isolate the pulses from threatening radars from other hostile, friendly, and neutral signals, our ability to deduce the threat posed by the radars, and our ability to select and configure an appropriate response to achieve our desired effect," Tranquilli says. "A host of adaptive and machine-learning algorithms are necessary because these challenges are too complex to design a simple series of rules around."

Role of machine learning and artificial intelligence

What role are machine learning and artificial intelligence (AI) playing in adaptive radars? There's already a "fair amount of intelligence built into the new operational systems such as SEWIP," Ottaviano says.

Is there a role for a fully autonomous system? "It depends on the application," Ottaviano notes. "I can easily see small packages being fully autonomous within a five-year window. For systems that deal with weapons, you can view it as another tool within the toolbox to allow warfighters to own the electromagnetic battlespace."

For its part, AI can be "a loaded term," Tranquilli cautions. "Typically, it refers to systems that attempt to have algorithms replace the functions a human would perform in an operation," he adds.

> " ... AS THREAT SYSTEMS CONTINUE TO ADVANCE THEY'LL ADAPT MORE QUICKLY AND CHANGE THEIR BEHAVIOR FASTER ... SO ALGORITHMS AND DECISION ENGINES THAT CAN OUTPACE OUR ADVERSARIES ARE KEY TO FUTURE SUCCESS."
> – JOHN TRANQUILLI, BAE SYSTEMS

But Tranquilli thinks there's likely "a place for AI in the near future of cognitive EW, because as threat environments become more contested and complex, it can help reduce the mental load on pilots and planners." This is "autonomy," a field in which BAE Systems is an active player.

Machine-learning techniques, on the other hand, "involve data-driven processing that allows a system to not be beholden to a static set of features, databases, or rules," Tranquilli points out. "I can't speak to the level of adaptation and autonomy allowed by today's systems, but as threat systems continue to advance they'll adapt more quickly and change their behavior faster ... so algorithms and decision engines that can outpace our adversaries are key to future success. This is the central tenant of Bob Work's Third Offset Strategy – pursuing next-gen technologies and concepts – and is funding advances within the cognitive EW arena."

Future cognitive EW

Interestingly, in terms of the hardware involved, Lockheed Martin is finding that a commercial off-the-shelf (COTS) open-architecture approach allows a rapid insertion of new capability to continually improve the ability and performance of the SEWIP Block 2 system.

"These systems can and have been upgraded in an immediate fashion to provide the warfighter with new tools," Ottaviano says. "We've seen a resurgence of this capability now beyond the surface EW community ... even moving into decoy and off-board platforms. This provides a quick time to solution because the approaches we're taking aren't hardware specific and don't require long development cycles."

Tranquilli sees a place for advanced hardware in the future of cognitive EW "because systems will need faster response times, more prevalent RF and spatial coverage, and

Basic cognitive EW concepts

The basic concepts of cognitive electronic warfare (EW) fall into one of three categories: signal analysis and characterization, countermeasure response design, and countermeasure effectiveness assessment, according to BAE Systems' John Tranquilli, technical director for signals and communications processing.

Without giving away specific algorithm approaches used for any given cognitive EW program, Tranquilli notes that "the 'advanced signal processing' BAE refers to typically consists of approaches that generate, train, and adapt features and models to characterize the behavior of a threat, design a response based on a mix of expert a priori knowledge and online observations of effectiveness, and use our models to infer the impact of our techniques based on the physics of what a radar must do to accomplish its task as opposed to what our techniques must do to deny them success."

Beyond DARPA's ARC program, BAE Systems is working with DARPA on other projects to bring advanced "adaptive" algorithms to the RF domain. This includes the Communications in Extreme RF Spectrum Conditions program, the Cognitive Spectrum Sensing component of the Computational Leverage Against Surveillance Systems program, and others.

During the past decade, his group – Signals and Communications Processing, within the Technology Solutions Business Area of BAE Systems' Electronic Systems – has focused on "bringing the combination of domain knowledge and adaptive algorithm expertise needed to architect and implement these concepts for existing and future electronic systems," Tranquilli says.

broader sets of available responses," he explains. "The great thing about cognitive EW is that it can be a scalable capability so portions of the technology can be implemented into systems that exist today, while advances in the hardware, firmware, and software resources will unlock the ability to get more power out of the technology."

Lockheed Martin is also currently working on a new U.S. Navy development contract to provide MH-60 helicopters with enhanced EW surveillance and countermeasure capabilities against antiship missile threats. (Figure 1.)

As part of it, they've developed a system – known as the Advanced Off-Board Electronic Warfare Active Mission Payload (AOEW AMP AN/ALQ-248) – that is essentially a self-contained EW pod hosted by an MH-60R or MH-60S to provide the Navy with advanced anti-ship missile detection and response capabilities. It's designed to work independently or with the ship's onboard electronic surveillance sensor, SEWIP Block 2 AN/SLQ-32(V)6, to detect incoming missiles and evaluate where they're going. AOEW then uses RF countermeasures to deter any incoming missiles.

Figure 1 | A U.S. Navy MH-60R Seahawk helicopter attached to Helicopter Maritime Strike Squadron (HSM) 74 lands on the flight deck of the aircraft carrier USS Harry S. Truman (CVN 75). (DoD photo by Mass Communication Specialist 2nd Class Lyle H. Wilkie III, U.S. Navy/Released)

"Our system will help create a coordinated attack against these threats to keep our warfighters safe by controlling the electromagnetic spectrum and disrupting adversaries," Ottaviano says. **MES**

Radar processing for naval upgrades: Software architecture is key to flexibility

By Dr. David G. Johnson

Advances in naval radar capabilities need to be matched with flexible software architectures that can exploit the radar sensor to identify threats and provide robust software solutions – including multihypothesis, multimodel tracking – that can evolve over extended military program life cycles.

The British Royal Navy's Type 23 frigates will be fitted with Lockheed Martin's Naval Vigilance Radar systems over the next five years. The new radar approach combines advanced naval radar with a modular processing and display architecture. Photo courtesy U.K. Ministry of Defence.

The latest generation of naval radars using coherent pulse Doppler technology provide enhanced detection of targets, including detection of asymmetric threats such as rigid-hulled inflatable boats (RHIBs) and jet skis. Such radars are optimized to detect small targets, even in clutter and in high-sea-state conditions to deliver enhanced situational awareness.

However, such advances in the sensor hardware must be matched by corresponding developments in the software processing of the data to automatically extract target information and to present the radar imagery on a naval radar display for operator interpretation. The software architecture must be flexible enough to accommodate evolutions in the capabilities of the radar, the operational requirements of the display, and the underlying technology that supports the implementation.

Modular software architecture is key

It is well understood that computer-processing hardware has a finite lifetime, beyond which it becomes uneconomic or just impossible to maintain. It is less well-known that software also has a lifetime and eventually needs replacing. The reasons are different, but the end result is the same: Unlike hardware, software is generally subjected to a process of continuous advancement to incorporate new capabilities or meet changing requirements. These changes beyond the original implementation make the software progressively more difficult to maintain and manage.

The software architecture to support radar processing and display in a naval console can be logically structured into modules for radar display, target tracking, and data fusion. Within these major subsystems, individual modules are required to provide the data-processing functions. The modular interaction of the processing functions ensures that modifications to the processing chain can be accomplished with minimal impact of other components in the system.

THE SOFTWARE ARCHITECTURE TO SUPPORT RADAR PROCESSING AND DISPLAY IN A NAVAL CONSOLE CAN BE LOGICALLY STRUCTURED INTO MODULES FOR RADAR DISPLAY, TARGET TRACKING, AND DATA FUSION. WITHIN THESE MAJOR SUBSYSTEMS, INDIVIDUAL MODULES ARE REQUIRED TO PROVIDE THE DATA-PROCESSING FUNCTIONS.

Take, for example, the target-tracking function. A software-based track extractor processes detections from the radar to identify targets of interest. These targets include other large vessels in range of the ship but also include small targets that may be potential threats, including wooden boats, RHIBs, periscopes, jet skis, and icebergs. Detecting these small targets is the challenge, with the goal being to detect a real target as soon as possible while minimizing the false-alarm rate.

The reliable detection of small, weak targets against a background of clutter takes time. It's a statistical process, which means that repeated detection of a radar return around the same location builds confidence that the radar echo is derived from a real target, rather than from a random process associated with sea or weather. The time taken to distinguish clutter from noise depends on the degree of clutter – a small target in an otherwise flat, calm sea is considerably easier to detect than the same target surrounded by clutter.

Multihypothesis, multimodel tracking

A modern implementation of a target tracker is built around the principles of multiple hypotheses and multiple models. The multiple hypotheses permit the tracker to consider different interpretations of the radar data. Is it a highly maneuverable target? Is it a stationary target seen in different locations because of measurement noise, or is it clutter? Then consider the different possibilities in parallel until the evidence for one hypothesis dominates. The multiple models permit the tracker to consider different target types in the same data, looking for different behaviors that conform to specific rules for the model.

Detecting very small targets, for example, requires some assumptions to be made to limit the search space and avoid clutter detections being incorrectly interpreted as highly maneuvering targets. Without intelligence in the processing, any number of "targets" can be observed by joining together the positions of random clutter detections.

The application of a multihypothesis, multimodel tracker enables the same radar data to be analyzed to detect both the obvious targets representing other ships in the coverage and also the smallest targets, potentially representing threats of interest. Target models exist as a package of target parameters that are chosen to reflect the types and behaviors of targets being searched for. This can include targets moving towards the radar operator's own ship, for example.

The ability to create new tracking models that can drop in to the tracker architecture with minimal changes is a significant advantage for future upgrades and enhancements of a deployed radar processor. It means that the capabilities of the radar processor can evolve both as the capabilities of the sensor evolve, and also as the nature of the targets change. The pattern of behavior of a target can be represented by a model and searched for in the input. It's a case of knowing what to look for, then building a model that detects that pattern.

Cambridge Pixel's SPx software provides components for key radar-processing functions, including receipt from network, enhancement, scan conversion, tracking, fusion, and recording (Figure 1).

However, in the context of delivering a scalable, adaptable solution for evolving requirements, the architecture of the software is as important as its function. The expectation of change, whether through enhancements to the radar, the need to detect specific types of target, or changes in the underlying operating system or graphics libraries, are

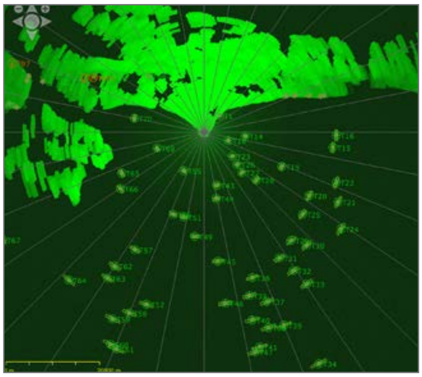


Figure 1 | The target-tracking processor provides a local display enabling the visualization of radar video, plots, and track. This interface supports configuration and maintenance of the server.

fundamentally built into the SPx software architecture.

Naval Vigilance Radar system

Lockheed Martin UK-Integrated Systems' new Naval Vigilance Radar system is a working example of such an approach, combining an advanced naval radar with a modular processing and display architecture to deliver enhanced radar surveillance now and provide a clear route to adding extra functionality in the future.

Lockheed Martin UK-Integrated Systems is under contract to the UK Ministry of Defence to install upgraded navigation radars on more than 60 Royal Navy platforms including on board type 23 frigates (as shown in lead photo). The contract will replace existing radars with the solid-state SharpEye radars from Kelvin Hughes. The software solution being developed by Lockheed Martin UK-Integrated Systems uses core radar processing and display modules from Cambridge Pixel to handle the radar acquisition from the radar, the scan conversion, target tracking, and radar fusion.

As shown in Figure 2, in the case of the radar scan conversion, for example, a separate software application called the radar display coprocessor (RDC) handles the radar receipt, processing, and display. The RDC is loosely coupled to the main software applications through a network interface that supports the messages to control the radar view. The radar data itself flows only through the RDC software, not through the main application. The output of the RDC is a radar image that is made available to the main application to composite with the application graphics. Similarly, the radar-tracking capability is handled by a separate software application that interfaces to the radar video and provides track data into the main application.

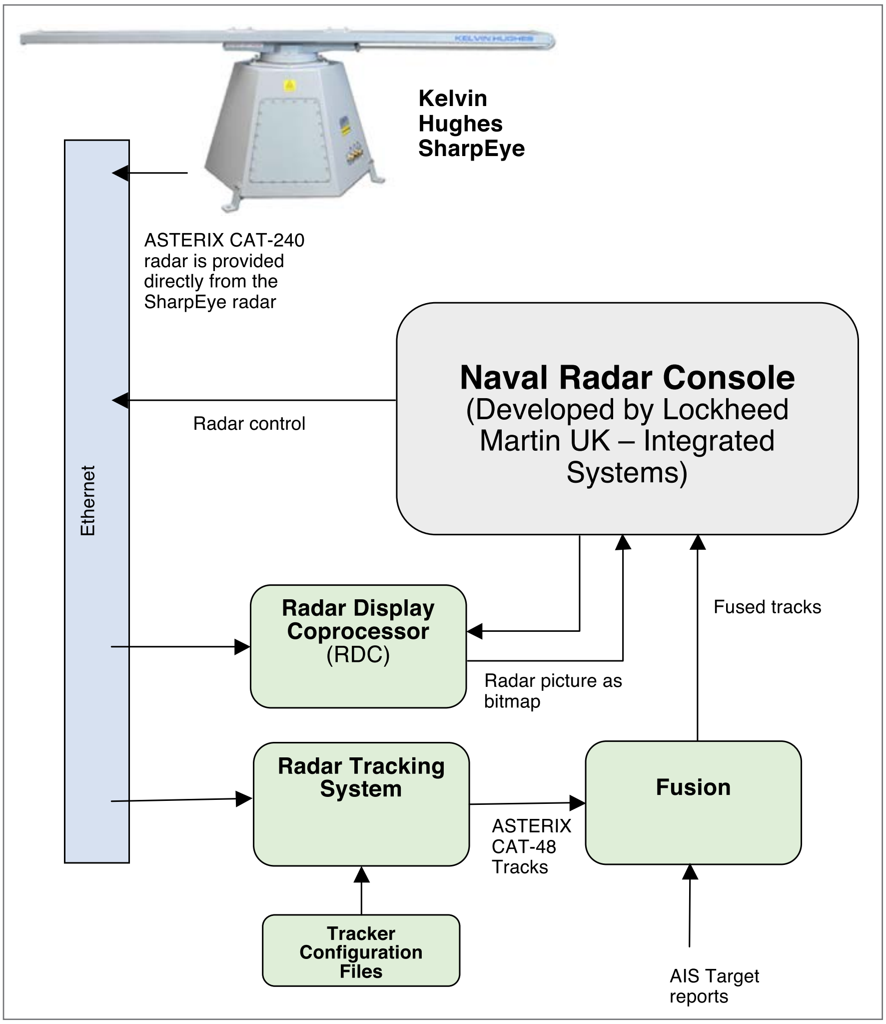


Figure 2 | The modular software architecture for Lockheed Martin UK-Integrated Systems' Naval Vigilance Radar system has the radar scan converter and target tracking running in separate software applications with a control interface to the main console application.

Such modular software architecture for naval radar upgrades enables system integrators to implement enhanced radar systems today that exploit all the features of solid-state Doppler radars but also provide the flexibility for ongoing technology refresh throughout the ten- to 15-year program life cycle. **MES**

Dr. David G. Johnson is technical director at Cambridge Pixel. He holds a BSc electronic engineering degree and a PhD in sensor technology from the U.K.'s University of Hull. He has worked in radar processing and display for 20 years and led teams developing software solutions for military radar tracking and radar scan conversion. Dave can be reached at dave@cambridgepixel.com.

Cambridge Pixel
www.cambridgepixel.com

Low-latency processing, open architectures key for smarter radar/EW systems

By Mariana Iriarte, Associate Editor

System-performance requirements and open architectures are driving development of smarter radar and electronic warfare (EW) systems. For EW systems, low-latency processing is a key requirement.

Meeting system performance requirements and delivering radar and EW systems that can face current and emerging threats is an ongoing battle for system designers. What it comes down to for the warfighter, is how "fast [they] can respond to an incoming signal and define what it is," says Lorne Graves, technical director at Mercury Systems in Chelmsford, Massachusetts. Engineers need to take into account the challenges of getting that information and translating it into actionable intelligence. For this arc to happen, Graves says, "Low-latency processing is key. It's similar with radar systems, which are going to be looking for low-latency processing and in some cases you'll see a trend to adaptive or cognitive radars."

With slight differences in radar and EW systems, engineers face challenges when developing these systems, because each has a different goal. In radar and EW systems, "the sensor and the system to defeat a sensor use similar technology – but have fundamentally different objectives. We often see signal processing on a radar system that performs functions such as phase calculations for beamforming or frequency domain Doppler processing; many of these operations are too complex and impose too much latency on the data path in an EW system," says Haydn Nelson, director, marketing and applications engineering, 4DSP Products, at Abaco Systems in Austin, Texas.

Radar/EW differences

The system designer must know the mission goal or application: "The largest difference is that electronic warfare systems often require extremely low latency. An EW system must often respond to a threat in nanoseconds, whereas radar can tolerate latencies in the milliseconds," Nelson explains.

Threats also factor into these systems, particularly if the user is unaware of where the threat is within the EW domain. "The spectrum is very broad, so it has to be very low-latency processing because you have to respond anywhere in that broad radio frequency (RF) spectrum to look for a particular threat," Graves notes.

"In the radar domain, one of the things that you do know is what was transmitted and you understand where that is," Graves continues. With radar systems, "you have some fixed latency and there is a certain amount of time to respond."

To handle the low-latency processing, Nelson says, "radar applications can often tolerate the latency of serial interfaces, allowing the use of higher sampling rates and more channels; as such, they can leverage the benefits of JESD204B interfaces, which typically deliver higher bandwidth and more channels on a single interface."

Where they come together "in some of the multifunction system that we're beginning to see today is where both of these systems are doing some type of cognitive or

WITH SLIGHT DIFFERENCES IN RADAR AND EW SYSTEMS, ENGINEERS FACE CHALLENGES WHEN DEVELOPING THESE SYSTEMS, BECAUSE EACH HAS A DIFFERENT GOAL.

adaptive algorithms; those typically are done on the same kind of processing machines," Graves says.

To increase system performance, "In terms of I/O implementation, there are two ways to interface: serial and parallel," Nelson notes. "Parallel interfaces are often implemented with buses, whereas serial interfaces often use specialized FPGA [field-programmable gate array] I/O with multigigabit transceivers with a JESD204B protocol on top. The latency of a JESD204B interface is typically higher than 100 ns, which is unacceptable to many EW applications. Thus, parallel LVDS [low-voltage differential signaling] is preferred," notes Nelson.

COTS driving cognitive systems

Commercial off-the-shelf (COTS) solutions help solve the processing issue. "One of the things that COTS signal-processing solutions are doing to enable cognitive EW applications is bringing a server asset," Graves says. "What we're doing at Mercury is bringing a server class asset directly behind the very fast, very agile, low-latency processing board for the EW domain."

The beauty of COTS solutions is that "If the DoD needs to deploy a certain application within four months and has defined that application and need now, COTS solutions are programmable and configurable and can address that new mission and threat," says Rodger Hosking, vice president and cofounder of Pentek in Upper Saddle River, New Jersey.

Ideally, when the human is taken out of the picture, Nelson says, "A cognitive EW system would need a processor architecture that can dynamically adapt using machine learning algorithms. The execution of a machine-learning algorithm isn't addressed by an FPGA-only architecture. Typically, GPPs [general-purpose processors], and sometimes GPUs [graphics processing units], handle these types of problems better, with their ability to execute modern languages like C/C++. Traditional processor architectures handle branching and complex decision trees much more efficiently than an FPGA device. Today's GPUs are better at branching than their predecessors, but it is still not a strength for them. GPPs continue to handle this better.

"The 'cognitive' aspect of cognitive EW is such that the system would have the intelligence to dynamically adapt, based on the effectiveness of a specific technique, and learn in real time," he continues. "This type of machine-learning approach to EW is considerably more advanced and requires a different computational architecture."

What it comes down to is using the right tool for the job: "The same high-channel-count I/O and FPGA system is still needed, but the added signal intelligence and cognitive aspect of the system requires a parallel module based on a leading edge commercial GPP or GPU technology," Nelson says. The Abaco Systems GRA113 graphics module is an example of such a module," says Nelson. (See Figure 1.)

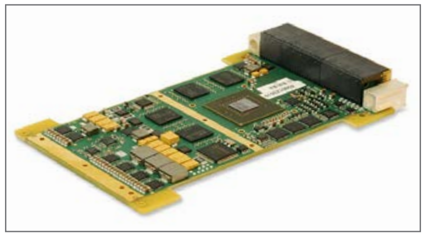


Figure 1 | The GRA113 leverages commercial NVIDIA technology on a form factor aimed at use in rugged radar and electronic warfare applications. Photo courtesy of Abaco Systems.

The open systems architecture agenda

A COTS discussion also necessitates the use of open architectures to enable faster, cost-effective technology refreshes.

"The desire to maintain technologically advanced radar and EW systems has driven many programs to adopt open standard architectures to have better control of technology refreshes," Nelson explains. "The adoption of open architectures has benefits in terms of technology, mitigation of program risk, and reduction of cost, which accounts for the significant adoption of the 3U VPX platform in the past few years."

The benefits expand throughout the life cycle of the system: "COTS solutions have a shorter development time," Hosking says. "Because of open standards, engineers can repurpose the system for other solutions, depending on the demand or new mission requirements. COTS technology is really great for putting together a system that is low cost and has a shorter development cycle."

Products like Pentek's Model 5973 (Figure 2) is an FMC carrier board that has an optical backplane interface and is compliant with several VITA standards including VITA-46, VITA-48, VITA-66.4, and VITA-65 (OpenVPXTM System Specification). The idea behind these systems is to remain configurable and modular, even down the road.

The main impetus for the shift toward open standards is to "move towards open architectures for signal processing in these areas; [because they] have the ability to adapt quickly to newer threats that evolve and they are evolving at a very rapid pace due to commercial technology that is now available to our adversaries that used to always be locked away in the United States DoD," says Mercury's Graves. "Those areas are no longer available just to us; they are now available through commercial products to our adversaries."

The industry is finding that open architecture is "becoming a bigger and bigger deal across different domains within the DoD. This is particularly true with radar systems, when they look at what is best of breed in terms of different modes, the different capabilities, and what all the providers are delivering," says Shaun McQuaid, director of product management for Mercury Systems' Embedded Products Group in Chelmsford, Massachusetts.

DoD program officials are pushing the industry to support open architectures and the standards that underpin them. "Examples include FACE [Future Airborne Capability Environment, an open avionics environment for military airborne platforms], SOSA [Sensor Open Systems Architecture for interfacing sensor suites], OMS [Open Mission Systems standards for integrating subsystems and services into airborne platforms], etc.," Nelson says. "Beyond the technology, risk, and cost benefits of open architectures, they also allow the government to have more control over system designs and technology refreshes."

Smarter radar/EW systems

Open architectures and COTS processing solutions have combined to evolve radar and EW systems toward the cognitive side, creating smarter systems for the warfighter.

"Radar/EW signals have become exponentially more sophisticated over the years and customers are looking to exploit new technology to deal with them. Radars must glean more detailed information from targets to gain actionable intelligence, while countermeasures must struggle to defeat detection from the first moment of each threat," Hosking says.

Figure 2 | Pentek's Model 5973 has a user-configurable gigabit serial interface. Photo courtesy of Pentek.

The desire to handle the sophisticated technology and have the upper hand in system performance for radar and EW has pushed engineers to increase synchronized channels enabled by wider bandwidth receivers and transmitters, Nelson says: "The inclusion of more channels has several applications. The most obvious is beamforming systems for radar and being able to create more advanced EW techniques like simulating the polarization of a rotating aircraft turbine in a spoofed radar return. The

Cybersecurity in radar/electronic warfare systems

The U.S. Department of Defense (DoD) is pushing for more security in radar and electronic warfare (EW) systems. "What used to be kind of the split between system integrity or antitamper and information assurance really is falling under the same cybersecurity umbrella," says Shaun McQuaid, director of product management for Mercury Systems' Embedded Products Group in Chelmsford, Massachusetts.

"At the end of the day there is a real desire, at least amongst all of the government folks that I've been interacting with, to have that capability baked into the solution from the start as opposed to bolted on at the end," he continues. "That's primarily driven by two reasons: one is affordability, because it's much more costly to retrofit security after the fact. Two is that the bolt-on solution tends to be less agile and less able to respond to new threats as they come forth."

As radar and EW systems continually get smarter "it's clear that IP [intellectual property] security is a critical aspect going forward," says Haydn Nelson, director, Marketing and Applications Engineering, 4DSP Products at Abaco Systems in Austin, Texas. "The algorithms to sense and deny sensing are often classified; thus, our signal-processing products need to be open so our customers can insert their classified IP and keep it protected and under the control of defense agencies. We see Xilinx reacting to this demand with many security features included in their new Zynq Ultrascale+ MPSOC [multiprocessor system-on-chip] devices. We expect IP security to be more of a focus in 2017 than ever before."

Going forward, "the cyber resiliency side of the world is going to become more and more critical for these platforms because they are going to have less and less oversight from humans," McQuaid says. "They have to be able to survive when they are either damaged or fall into the wrong hands. These systems need to make sure that they are protected and that their critical capabilities are not exposed."

combination of wideband and multichannel systems has a direct consequence on the analog I/O and FPGA signal processing.

"An increase in bandwidth means that data is coming faster and often requires more FPGA resources to handle this volume of data," he continues. "The result is that designers often require larger FPGA devices like the Xilinx Ultrascale class of products. Further increasing the requirement for FPGA resources: this 'faster data' is coming on multiple channels."

Since there is an increase in channels, the data coming in requires a significant amount of bandwidth, "which ends up looking like a big-data problem," McQuaid says. "On the other side of that is a processing solution that can handle that and you know that is analogous to commercial big-data solutions."

Engineers are then accommodating the needs of the users with "multiple Ultrascale FPGAs and FMC+ interfaces to accommodate both wideband digital receivers and transmitters and the accompanying increase in signal processing load," Nelson says.

Driven by the additional complexity of new FPGA devices, "there's a push to abstract low level resources to boost design productivity," Hosking says. "That means software, hardware, and FPGA designers are working at a higher level of design entry. They can now choose from libraries of high-level functional blocks, create their own custom blocks, and interconnect them all using graphical tools. The tools take care of most of the lower details of this process, saving significant time for engineers."

These advances in technology and "the new techniques we have made are what people are looking for," Hosking continues. "It's the ability to do a better job of developing advanced signal-processing technology – for both incoming and outgoing signals – to improve detection and threat-avoidance capabilities. Users are looking for smarter, faster, and more capable systems." **MES**

Funding for new technology versus upgrades

Funding for radar and EW systems remains strong, especially for upgrades within radar. President Trump has already promised to rebuild naval, airborne, and ground platforms. However, even with the uncertainty of a new administration, businesses find that while rebuilding capabilities may be good for business, it is also sometimes cheaper to replace systems with new technology versus upgrading older technology.

"Sometimes you can keep the same antenna and microwave circuitry, but all of the signal processing for the outgoing pulse and return radar signal is often replaced with new technology," says Rodger Hosking, vice president and cofounder of Pentek in Upper Saddle River, New Jersey.

The monetary benefits of upgrading are of particular interest to DoD officials "because of the maintenance costs for older technology," he continues. "Often annual maintenance costs of these systems can pay for new technology upgrades within few years. And these new signal-processing radar solutions significantly strengthen our defenses and military operations."

Funding for radar and EW systems is "trending upward and more than half of what we see for radar businesses has to do with upgrades," Hosking notes. "A radar system that is 20 years old is probably easy to exploit. It's not doing its job because the enemy is probably able to defeat its capability with new technology."

"Both electronic warfare and radar funding are trending upwards and I don't see those decreasing especially if you also take into account the cyber aspect of things," says Lorne Graves, technical director at Mercury Systems in Chelmsford, Massachusetts. "Especially for the EW domain, cybersecurity is getting a lot of focus."

Building highly parallel rugged computers for electronic warfare

By Mark Littlefield

Electronic warfare (EW) systems are among the most challenging embedded systems to design and deploy. Not only do they require voracious amounts of signal processing, they also require more mundane server-style processing (for signal library maintenance, data logging, etc.) and are often packaged in extremely size, weight, and power (SWaP)-constrained environments such as under wing pods. As a result, advanced EW systems can benefit from consolidating workloads on a single machine with the means to efficiently execute these two very different processing problems using parallel virtual machine (VM) execution. Modern commercial off-the-shelf (COTS) 3U VPX boards based on Intel server-class processors are a compelling option for these sorts of systems.

Each generation of EW systems increases the demands for high-performance processing and increasingly larger bandwidth for both streaming data in and out of the system as well as for interprocessor communications. Military systems designers face an ever-growing need to meet escalating requirements and provide platforms that can be packaged and deployed in harsh environments. Furthermore, proprietary systems no longer make sense from an engineering resource, budget, and deployment schedule perspective. Facing the limitations of tightening budgets, defense OEMs must find a way to cost-effectively meet the mounting data throughput and processing needs of these systems. A key way the market has curbed costs is to move from closed, proprietary solutions to open-standard COTS solutions in smaller form factors that are durable and reliable.

Matching technology needs

Suppliers of both components and boards/systems have responded in meeting higher performing standardized solution needs. Leveraging the consumer electronics drive for larger numbers of cores, streaming video and audio processing, and greater integration, Intel and other processor suppliers are offering components with these features that include the added bonus of extended temperature ratings and longer-than-typical consumer life cycles that can satisfy lengthier embedded defense application lifespans. Boards and system suppliers are making use of these components and developing both board-level and packaged systems solutions that simultaneously push performance limits and I/O features while maintaining tough SWaP limits and driving down costs. This approach is a real win for the EW market, which generally will use every ounce of performance they can fit into a package.

This insertion of commercially available technologies into defense-ready platforms continues a trend that was started in the early to mid-1990s. Over that time, defense system integrators have become very adept at utilizing high performance embedded computing (HPEC)-like technologies such as multicore and multicomputing platforms linked with high-speed buses or data links to solve their particular problems. As a result, current systems designers can expect to leverage tens (or even hundreds) of processor cores, each linked by very-high-speed/low-latency data paths using commercially available – and often standards-based – operating systems (OSs), software libraries, and middleware. This way gives the designer unprecedented

power to integrate and deploy the system with a minimum of effort and time. It also means that designers generally no longer need to compromise on either performance or I/O bandwidth, and don't need to move to proprietary or customized solutions.

Driving electronic warfare innovation

High-density HPEC platforms that, for example, integrate the server-class Intel Xeon processor D-1540, provide the basis for continued EW innovation. These types of sophisticated processing systems enable military system developers to take advantage of the extensive capital and operational efficiencies provided by isolated workloads configured to dynamically share common resources specifically enabling multipurpose or multifunction EW systems. For instance, developers can use such systems to powerfully consolidate workloads into a single system to run both jamming and surveillance EW applications.

Jammers often operate by taking a radar signal in and transmitting a corresponding different signal to effectively mask a vehicle's true position, velocity, or even composition. To do this, jammers require extremely fast digital signal processing (DSP) capabilities such as those offered by the AVX2 floating-point vector math units in the Intel Xeon processor D. By bringing exceptional eight-core performance and advanced features into dense, lower-power industry-standard systems-on-chip (SoCs), EW developers can scale their designs for quick data capture and processing. Additional features supporting fast distributed data transfer are reliable PCI Express (PCIe) Gen3 and 10 Gigabit Ethernet (GbE) that deliver extremely low latency at as fast as 10 GHz per lane.

Jamming applications can also benefit from using the interprocessor switch fabric these new dense HPEC platforms offer between payload slots. Based on PCIe and 10 GbE, they give designers a plug-and-play solution capable of moving data at ultra-high speeds by implementing extremely fast serial link point-to-point connections between boards. Using advanced standards-based communications fabrics enables developers to quickly implement or port applications using standard TCP/IP or other communications protocol stacks, resulting in high performance and efficient system convergence. In addition, many devices and subsystems offer native PCIe, which allows immediate use of an existing infrastructure, thereby lowering latency, cost, and power.

Different EW systems can have different demands on a system. Electronic surveillance, for its part, requires much more detailed and compute-intensive processing of sensor data. The Xeon processor D not only delivers essential DSP performance, but it offers extremely efficient general-purpose processing as well as a rich assortment of peripheral I/O such as SATA III. In addition, the Xeon processor D offers virtualization technology (Intel VT), which enables the system developer to direct these divergent tasks to efficiently share the processing hardware. This functionality makes it an ideal platform for electronic surveillance applications.

Next-generation VPX-based boards, based upon the OpenVPX standard, leverage the power of the Xeon-D processor in a flexible 3U package. These boards combine the DSP and general-purpose processing features of the Xeon processor D with advanced ECC DDR4 memory and an embedded graphics controller. The result is a rugged and flexible computing platform ideal for EW applications. For math-intensive surveillance operations, these octo-core-based boards fully use the AVX2 SIMD units, where each core has two AVX2 units and can provide up to 128 floating point operations per clock, or a potential 230.4 gigaflops of DSP performance. Able to be employed in the wide range of complex and extreme electronic surveillance environments, these platforms support widening the operational margins on the backplane to support intelligent multifunction EW solutions.

The OpenVPX standard – inherently known for its high performance, rugged operation in harsh environments, and small form factor – enable today's HPEC solutions to be used to simplify logistics, installation, and maintenance of complex EW systems. These platforms can be air- and conduction-cooled, offering extended operating temperature capability where airflow temperature is controlled on each slot; moreover, payload boards can be held in standby mode to meet low-energy surveillance requirements.

Advanced HPEC platforms also take the guesswork out of mastering multigigabit rate communication on standard backplane technology by supporting PCIe and 10 GbE, between all boards in the backplane, across the full operational domain of a rugged computer design. This broadened bandwidth capacity enables systems integrators to evolve applications to more effectively respond to immediate threats. The combination of dense processing with rich standards-based communications fabric and I/O connectivity means that these platforms are equally suited for streaming signal- or image-processing EW applications that include combined jammer and electronic surveillance functions.

In addition, new multicore high performance platforms increasingly help meet tight budgets and future-proof their technology investments. For example, the virtualization features integrated in new HPEC systems enable OEMs to leverage a single application design based on mainstream technologies to be easily adapted to match CPU count, available I/O, form factor, memory, or other hardware evolution needs.

More efficient EW design

A key evolution in HPEC design is the balancing of CPU power with I/O bandwidth to increase overall performance. Traditional HPECs have featured excellent CPU power based on continually increasing computing performance, but I/O bandwidth has not always kept up with processor performance, causing potential bottlenecks and performance issues.

A balanced HPEC approach is the Kontron StarVX: It enables ease of development because it is based on only nonproprietary technology such as x86, Linux, TCP/IP, and PCIe, which eliminates niche-based deployments and reduces obsolescence risk. It delivers the I/O bandwidth and IP sockets EW application designers need in order to successfully use mainstream IT servers and deploy the system unmodified.

Additionally, Kontron's VxFabric API technology provides a TCP/IP protocol over the PCIe infrastructure towards the application to help accelerate the design process. Its 10 GbE switch and a PCIe switch can be complemented with two single star data planes for 10 GbE and for PCIe, respectively. Designers are able to use this API with TCP/IP sockets that enable multicore computing node architectures that permit high-speed socket-based communication between blades using multiple switched-fabric interconnects within the backplane.

Figure 1 | Kontron's StarVX 3U blade combines dual ports of integrated 10 GbE and integrated I/Os (PCIe, USB, SATA, and other general purpose I/Os) into a single system.

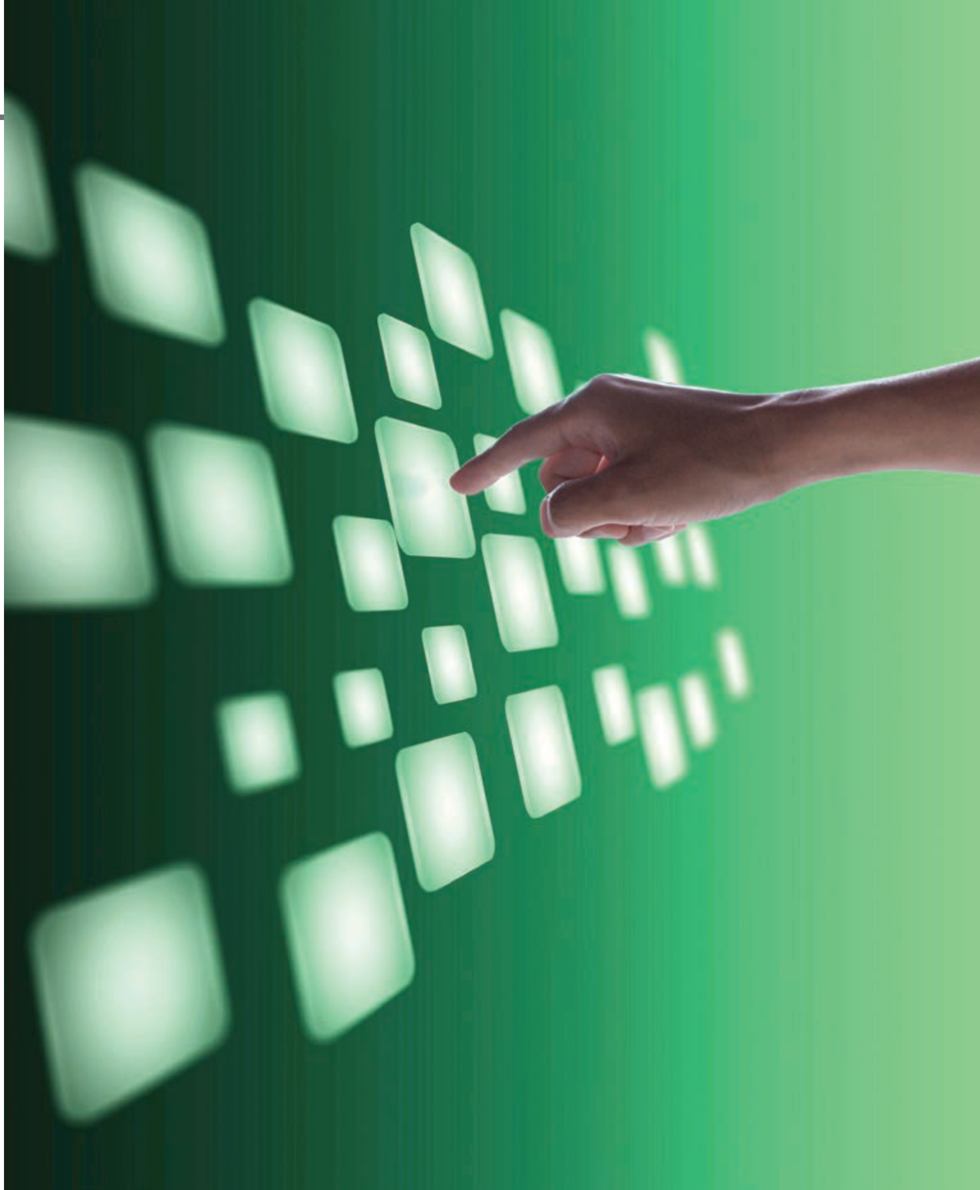
Leveraging data center performance benefits

Bringing data center performance benefits to EW applications, the Xeon processor D delivers 10 times greater performance than currently available in other ruggedized HPEC platforms. Using the eight-core version of the processor D, computing blades are able to support heavier throughput by delivering as much as 3.4 times faster performance per node and up to 1.7 times the better performance per watt when compared to the Intel Atom processor C2750.

Intel's latest processors include support for error-correcting code memory, combined with enhanced hardware-based Intel VT and Intel Advanced Encryption (AES-NI). This advanced integration is inherently SWaP-C optimized, and offers long-life availability and enhanced silicon reliability through Intel's 10-year simulation aging tests, making it an optimal engine for HPEC platforms. **MES**

Mark Littlefield *is a vertical product manager for the defense business line for Kontron. He has more than 25 years of experience in embedded computing, where he has held a range of technical and professional roles supporting defense, medical, and commercial applications. Littlefield holds bachelors and master's degrees in control systems engineering from the University of West Florida, where he wrote his thesis on a neural net application for image processing.*

Kontron • www.kontron.com



Asking the right questions about HPEC software development tools for radar, SIGINT, and EW applications

By Tammy Carter

High performance embedded computing (HPEC) system designers tasked with architecting large-scale supercomputer-class processing systems for radar, signal intelligence (SIGINT), and electronic warfare (EW) applications depend greatly on the software development tools available to them. The choice of development tools – such as debuggers, profilers, and cluster managers – can result in an intimate relationship; often the choice means the success or failure of the system design.

How then does a system designer select those tools upon which so much depends? In the spirit of viewing the importance of software development tools much like an intimate relationship, let's consider the selection process in that light, with the benefits and attributes of the tools discussed, and considered as one might interview a potential life partner. When the right questions are asked, the replies can be a revelation.

What follows is an "interview" of the sort that a system designer should undertake when considering the selection of these critical tools, using Allinea's debugger and profiler and Bright Computing's Cluster Manager, software developed for use with supercomputers in the commercial High Performance Computing (HPC) market as the examples. Knowing the right questions to ask can make all the difference in speeding development and reducing program risk when designing an HPEC system. System designers should consider asking the following types of questions when selecting their suite of HPEC development tools. The answers can result in a beautiful relationship or in heartbreak, a successful outcome or a sad failure of the project.

Q ***(System Designer):***
How large is your user base and are you proprietary?

A ***(HPEC Development Tool Suite):*** I use open standards-based tools already proven in the realm of supercomputers. Imagine all those new engineers you can hire that will already be familiar with me.

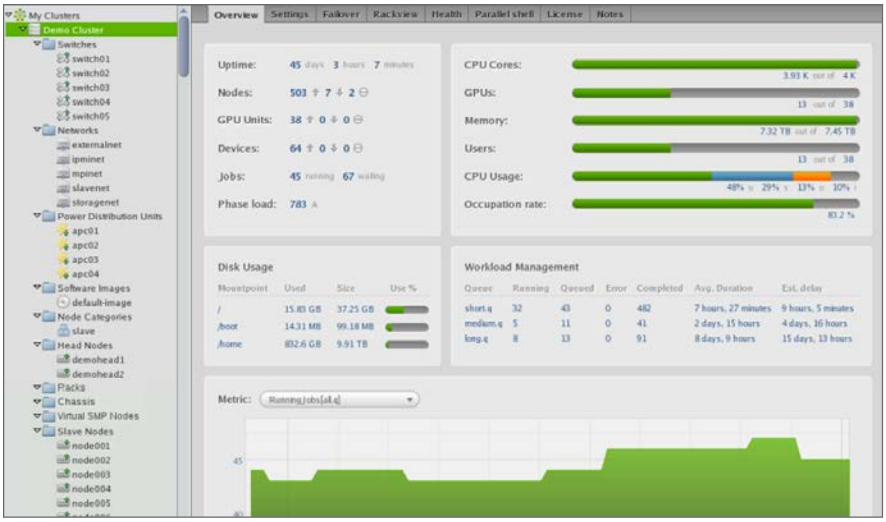


Figure 1 | The Bright Cluster Manager enables initial setup of all system resources.

Q *Can you handle diversity?*

A Yes, I am very flexible, I handle a broad mixture of types from single-board computers to digital signal processors (DSPs) and graphics processing units (GPUs). I also easily scale across multiple processors and boards. I also work with both 6U and 3U OpenVPX systems.

Q *Can you speak multiple languages?*

A Of course: C, C++, CUDA, OpenCL, five dialects of MPI, and OpenMP. My other communication skills should also pique your interest, as they include Infiniband, TC/IP sockets (Regular and Encrypted), RoCE, just to name a few. I also speak Centos and Red Hat.

Q *How about setting up and managing the system?*

A I'm a relationship manager. With Bright Computing's Cluster Manager (Figure 1), the initial setup of all system resources – including the operating systems, boards, disks, and networks – can be achieved by answering a few simple questions. You know, all that "small talk" such as provisioning, memory size and allocation, and the like. Using the image-based provisioning, software build images can be maintained for different board types, configurations, and different developers. The revision-control feature enables the user to track changes to software images using standardized methods. Using the same controls, the user can add, delete, move boards, or change network configurations with the same ease.

Q *Can you monitor my system's health, check my pulse, and provide status checks?*

A I can provide both a visual status of the entire system and a log. Temperature, CPU loading, and disk space for each card are just a few of the parameters that can be monitored. Boot-up messages for all of the boards, along with any errors and warnings, are captured. For any device that can be monitored, an action (either a standalone script or a built-in command) will be executed when the condition is met.

Q *Can you manage my power?*

A Through the use of power distribution units (PDUs), intelligent platform management interface (IPMI)-based power control, or software daemons, I can manage the power to the system's nodes. For devices that cannot be controlled through any of the standard existing power control options, a custom power management script can be created and invoked. To conserve power during certain scenarios, I can control CPU core frequencies and power up certain nodes in a predefined sequence or by node groups. For example, while a drone is sitting on the tarmac, the group of nodes designated as "ground control" could be turned on at power-up. Once in the air, the rest of the nodes can be brought online.

Q *Can you help me with fault tolerance?*

A Because of my monitoring and power-management capabilities, I can detect the failure and handle the switching of the hardware and the rerouting of the data flow. So far, I can tell you that your memory is up to speed, and your I/O is flowing freely.

Q *How are you at debugging?*

A HPEC designers need a true system debugger, one that can debug and control threads and processes, both individually and collectively, as defined by variable or expression values, current code location, or process state. This includes setting breakpoints, stepping, or playing individual or predefined groups of threads on a single board or across boards. My memory debugging detects dangling pointers, finds memory leaks, fixes misuse of stack and heap memory, and catches out-of-bounds data accesses. My ability to log variables and events in the background without affecting system timing helps catch the nonrepeatable bugs by allowing the system to collect data overnight, or however long it takes for the problem to occur. I can diagnose deadlocks, live locks, and message synchronization errors with both graphical and table-based message queue displays. I also have the ability to debug and profile across multiple GPUs.

Q *Can you help me verify the correctness of my data?*

A How does automatic change detection of variables, smart highlighting, and graphs of values across threads and processes sound? I can also graph any data (including multi- dimensional data) in the system. Imagine being able to plot your data before and after every filter and FFT, and compare it to your Matlab results or data previously gathered from your sensor. I can also generate statistical analysis of the data structures – No longer will you have to search your data looking for NaNs ["not a number" messages].

"UNLIKE THE CLASSIC TRACE-BASED PERFORMANCE TOOLS, I WILL NOT DROWN YOU IN DATA."

Q *Can you guide me through the optimization of my code?*

A By monitoring the expired instruction pipeline, I am able to provide advanced profiling functionality without requiring any application code changes. Unlike the classic trace-based performance tools, I will not drown you in data. Adaptive sampling rates, combined with on-cluster merge technology, ensure that the right amount of data is recorded. I will show the functions and source code lines that consume the most time. We will discover memory bottlenecks together over time. I will help you balance the CPU processing cycles, I/O accesses, and memory fetches. We will use the CPU performance extension to your best advantage, as well as the mapping of the threads to the cores.

Q *Can you help me with system BIT [built-in test]?*

A I can provide a toolbox to create a system-level BIT to help you customize your system. My framework provides application program interfaces (APIs), and a command line interface (CLI), to create PBIT/CBIT/IBIT by using the tests included in the board support package and other tests scripted by you. I can also analyze the results and report back to you. The framework can support custom sequences of the test, as well as custom tests using single or multiple processors.

Q *What can you tell me about the throughput and latency of my system?*

A My Dataflow tool not only shows the processor loading and temperature, but also their relationship to latency and throughput for PCIe, InfiniBand, and Ethernet. Supported APIs include IB Verbs, RoCE, MPI, and both regular and encrypted TCP/IP sockets. In addition to helping verify your data movements, it will also be useful in your testing. The results can be displayed in a real-time graph and/or stored in CSV format.

Q *What type of math libraries do you support?*

A I include a vendor-supplied math library, with over 2,600 functions. Open standards are supported, with the inclusion of both VSIPL and the FFTW APIs, while the underlying function calls have been optimized for the AVX2, with support for both single-threaded and multiple-threaded versions.

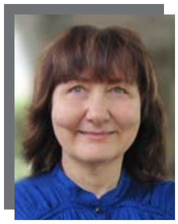
Q *Tell me more about your GPU support.*

A So, are you into deep learning? The Bright Cluster Manager provides the provisioning and monitoring for GPUs as well as support for all GPU programming models. Administrators can have direct access to the performance-enhancing NVIDIA GPU Boost technology. There is also automatic synchronization with the latest NVIDIA CUDA software (verified for your environment), a fully configured modules environment for NVIDIA GPU clusters.

Q *Can I work remotely on the system or do I have to be next to the hardware in a noisy lab?*

A You can work from your desktop or laptop. And you no longer have to fight the tangle of serial cables for configuring, monitoring, debugging, and working with multiple terminal windows.

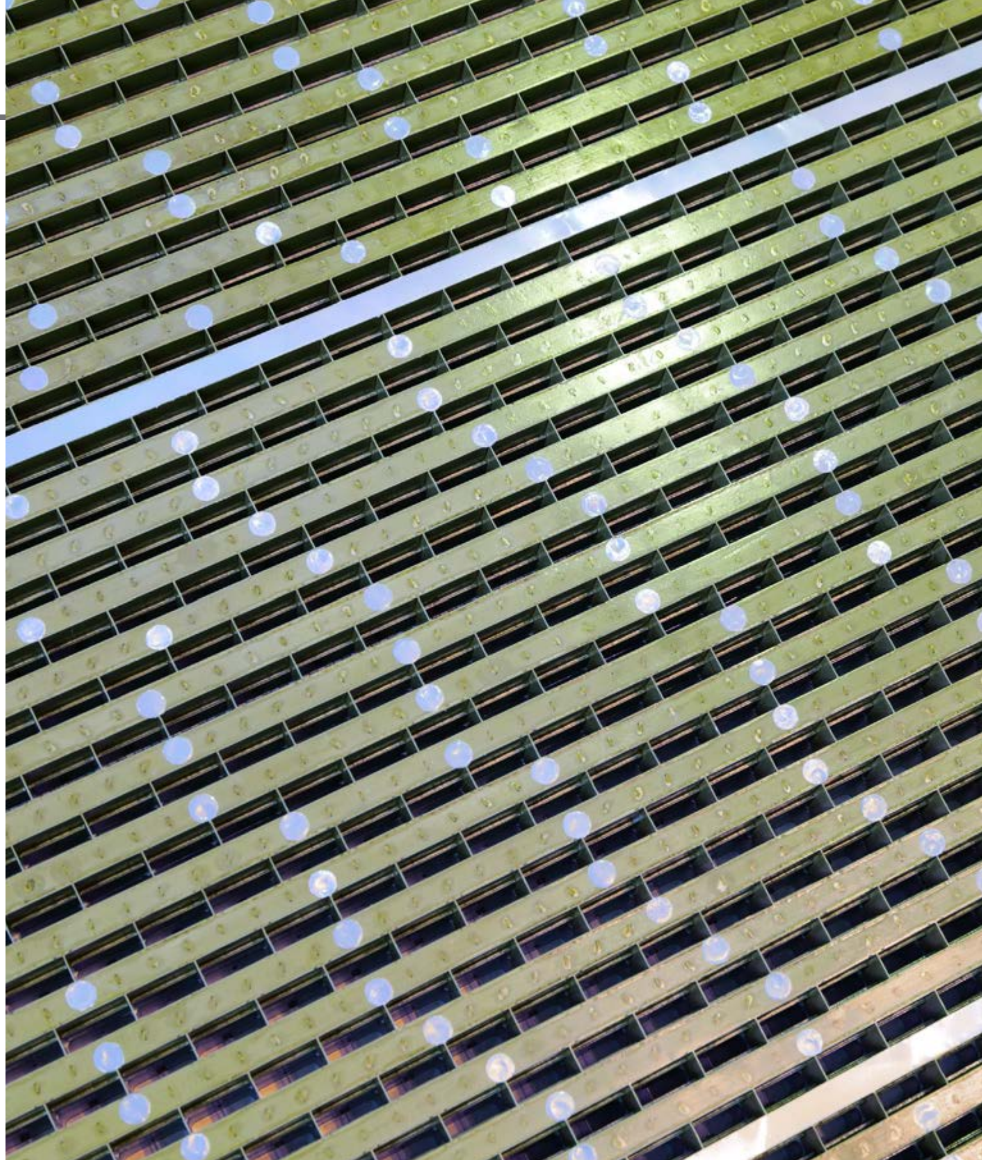
System developers who make the effort to conduct this type of dialogue with their prospective commercial off-the-shelf (COTS) hardware and software development tool suppliers are more likely to end up in a productive relationship that results in a radar, SIGINT, or EW solution that meets their unique requirements, reduces program risk, and gets deployed without avoidable delays. **MES**



__Tammy Carter__ is the senior product manager for OpenHPEC products for Curtiss-Wright Defense Solutions, based out of Ashburn, Virginia. She has more than 20 years of experience in designing, developing, and integrating real-time embedded systems in the defense, communications, and medical arenas. She holds a Master of Science in Computer Science from the University of Central Florida. Readers may reach the author at tcarter@curtisswright.com.

Curtiss-Wright
www.curtisswrightds.com

SIGNAL PROCESSING TRENDS IN RADAR, SONAR, AND ELECTRONIC WARFARE



FPGA coprocessors for low-power adaptive beamforming in hybrid VPX HPEC systems

By Thierry Wastiaux

Beamforming techniques have become very important in the fields of radar, electronic warfare (EW), sonar, wireless communication, and medical imaging. These enable continuous formation of beams from array antennas (or array transducers) towards a tracked target – or a moving user in the case of wireless communication – and cancellation of all the interfering signals coming from other angles. For tactical or airborne radar and EW solutions, the execution speed of the beamforming algorithms and the low power consumption are critical. In these situations, VPX high-performance embedded computing (HPEC) hybrid field-programmable gate array (FPGA) and CPU systems appear to be the best suited approach.

The technique of adaptive beamforming has been developed for detecting and estimating the signal of interest at the output of an active electronically scanned array (AESA). Adaptive beamforming is used in radar, sonar, wireless communication systems, and medical-imaging equipment. Adaptive beamforming uses an array of antennas to achieve maximum reception in the desired direction, while signals of the same frequency from other directions are rejected. The technique computes optimal complex variables, named "weights," for measurement of the signal.

In conventional beamforming, the weights do not depend on input/output array data contrary to adaptive beamforming, aiming at suppressing noise, clutter, and jammers and maximizing signal to interference and noise ratio (SNIR). The optimum array weights need to be continuously adapted to the ever-changing environment. If the desired arrival angles change with time, the user must find a way to keep recalculating the optimum array weights. In this way, if the target is continuously moving, it can be tracked and a continuous beam can be formed towards it by using the adaptive beamforming techniques.

Adaptive beamforming principles

Let us assume an array of M antennas. The signal at each antenna $X_n(t)$ (n=1,..,M) is multiplied by complex numbers, the so-called weights W_m (m=1,..,M). The array output is then $y(t) = w^H.x(t) = \sum_{i=1,m} W_i^*.X_i(t)$ where W^* is the complex conjugate of W, and W^H is the Hermitian transpose of H.

Let us see how the array output signal can approach the desired signal d(t) that is sought in all the signals received. The difference between the array output and the desired signal is called $e(t) = d(t)-y(t)$. If we call E[.] the statistical expectation, the Mean Square Error Criterion is $E[|e(t)|^2]$, e(t) being $d(t)- w^H.x(t)$. It can be shown that the Mean Square Error is minimum when the complex weights W_m satisfy the equation:

$W_{opt} = R^{-1}p$ where R is the correlation matrix of the input x(t), $R = E[x(t).x^H(t)]$ and p is the cross correlation vector between the input vector x(t) and the desired signal d(t) $(E(d^*(t).x(t))$. In practice to estimate the correlation matrix and the correlation vector, the samples are divided in blocks, the length of each block of samples being K. The correlation matrix and the cross correlation vector are then calculated block by block. For the correlation matrix, the K vectors of the samples of a block make a matrix MxK. This matrix is multiplied by its Hermitian transpose to build a MxM matrix R_k that is divided by the integer K. This gives an estimation of the correlation Matrix on the samples.

So getting the optimal weights (or adaptive weights) means inverting each R_k matrix and multiplying the inverse R_k^{-1} by the cross correlation vector. That is why this method of calculating the weights is called the Sample Matrix Inversion Algorithm that is suitable for rapidly changing environment.

R_k is a Hermitian square (MxM) matrix ($R^H=R$) that is invertible in practice, the inverse being also Hermitian. To invert the matrix several approaches are well known as the Gram-Schmidt process that can be very rapidly executed in a high-end FPGA. This process must use floating-point arithmetic to maintain the precision of the adaptive weight solution. In radar applications, the challenge is to perform this matrix inversion in a very short period of time (typically the ms) before the next pulse repetition interval of data is received. This process can be executed in CPUs or in FPGAs. It is now well established that the FPGA approach is much more performant compared to the CPU/GPU one. In its white paper WP452, Xilinx compares a Virtex-7 solution and an ARM-A9 solution and shows that the FPGA approach is consuming less energy by a factor of 18 and is cheaper by a factor of 10.

Example of a beamformer

An example of a beamformer can be built using the last generation of FPGAs and ADC coders. A Xilinx VU13P UltraScale+ FPGA offers more than 3.5 million logic cells, 11,904 DSP enhanced slices for signal processing, and 128 times 32.75 Gb/s GTY transceivers allowing massive data flow and routing and supporting multiterabit per second throughput. The last generation of analog-to-digital (ADC) components can perform a sampling on four channels at 3 Gsps with a resolution of 14 bits. The samples are delivered to an FPGA using the JESD204B protocol, with lane speeds up to 16 Gbps and with two lanes per channel. Using only one Xilinx VU13P UltraScale+ FPGA, a beamformer can be built in the following way (for example):

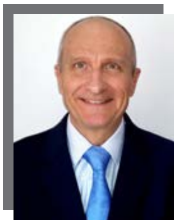
- Eight four-channel, 3 Gsps ADC sampling directly behind the array antenna
- In front of each ADC, a digital downconverter (DDC)
- Behind each DDC, a partial beamformer for the four channels, including all the principles described above with adaptive weights
- A beam adder behind all the eight partial beamformers

VPX HPEC beamforming architecture

One way to build a rugged system implementing the above approach is to use the front-end processing boards from Interface Concept as the dual Virtex-7 6U VPX board IC-FEP-VPX6b (see Figure 1) supporting two four-channel VITA 57.4 ADC FMCs or the upcoming UltraScale/UltraScale+ front-end processing boards (coming soon in the roadmap).

Figure 1 | IC-FEP-VPX6b featuring two Virtex-7 FPGAs.

Several of these boards, together with a dual Intel Broadwell processor board like the IC-INT-VPX6d/e, can make up a rugged beamformer HPEC system able to compute at a very high speed, with reduced power consumption, and using numerous continuously adapted weights to track and search the desired signals. **MES**



***Thierry Wastiaux** is senior vice president of sales at Interface Concept, a European manufacturer of electronic embedded systems for defense, aerospace, telecom, and industrial markets. He has 25 years of experience in the telecom and embedded systems market, having held positions in operations, business development, and executive management. Prior to joining Interface Concept, he was responsible for the operations of the Mobile Communication Group and the Wireless Transmission Business Unit in Alcatel-Lucent. He holds an M.Sc. from France's Ecole Polytechnique. Readers may contact him at twastiaux@interfaceconcept.com.*

Interface Concept
www.interfaceconcept.com

RF AND MICROWAVE
FOR RADAR AND ELECTRONIC
WARFARE SYSTEMS

GaN use in radar/ EW applications gets hot

By John McHale, Editorial Director

Military radar and electronic warfare (EW) designers continue to invest in gallium nitride (GaN) technology for its performance advantages. Meanwhile, the overall military radio frequency (RF) and microwave market continues to be strong, as advances in phased-array systems and other complex applications depend more and more on these components.

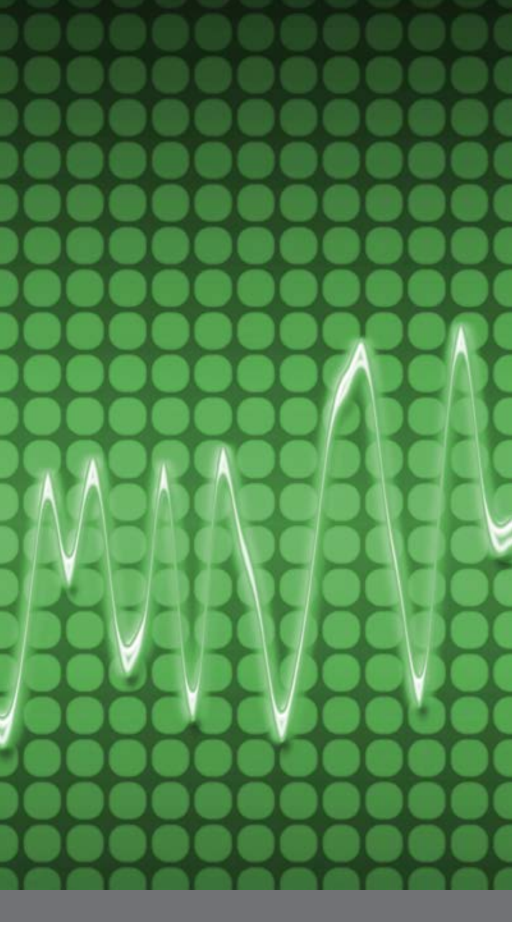
The use of gallium nitride (GaN) components is growing fast in military radar and EW system designs as an alternative or replacement for laterally diffused MOSFET (LDMOS) components. However, some industry experts say the customer base could use more education on GaN's benefits and where and when to use it.

"The benefits that GaN features provide are well publicized, but the relative position of GaN versus other device technology requires careful review based on the design parameters of a particular application," says Gavin Smith, RF Industrial Product Marketing at NXP (Phoenix, Ariz.). "GaN is a rapidly evolving technology, but so are other power semiconductor technologies. New applications emerge over time. For example, GaN got its 'trial by fire' in defense systems, but is already making significant inroads into wireless infrastructure and several other sectors, all in the span of less than 10 years.

"Of the RF and microwave semiconductor technologies GaN is the newest, and its characteristics and requirements are unique from the others," Smith continues. "For example, its power-up sequence must be strictly adhered to, and as GaN has very high power density, circuits incorporating GaN devices must be designed to dissipate large amounts of heat. These are just two of the many factors that must be considered, beginning at the very earliest stages of design."

Despite the huge interest in GaN technology, there is still uncertainty among the user base as to when to leverage GaN and when to leverage LDMOS.

"From my perspective, there seems to be confusion as to when to choose GaN components as opposed to LDMOS and gallium arsenide (GaAs)," says Bryan Goldstein, general manager of the Aerospace and Defense business at Analog Devices (Chelmsford, Mass.). "In some applications the answer is very clear, and in others it is not so clear. If the application requires efficient, pure saturated RF output power at frequencies above 4 to 5 GHz, and power levels above 5 to 7 W, then GaN is the clear choice. However, GaN has much worse linearity characteristics than GaAs, so for communication applications where linearity is critical, tradeoffs need to be made between combining multiple GaAs amplifiers, which are much more linear, or working with a significantly lower number of GaN devices. In the area of low noise amplifiers (LNAs) and RF switches, the performance being achieved on GaN is now coming close to matching that of GaAs in terms of gain/loss and noise figure while achieving much higher levels of power handling. As the volume of GaN increases and the cost decreases, it is expected that GaN will replace GaAs for many future applications. Where LDMOS maintains its position is in the area of power amplifiers below 4 to 5 GHz. Power levels on



par with, if not superior to, GaN can be achieved at a fraction of the current price point. So in these applications, LDMOS will remain strong."

As GaN's price point comes down with each generation, users are able to find new applications for the technology and understand better where it fits with LDMOS.

"GaN's performance benefits are well known to all involved with the RF and microwave industry today," say Dr. Doug Carlson, vice president of strategy, and Thomas Galluccio, director of marketing, aerospace and defense at MACOM (Lowell, Mass.). "But GaN's historical cost structure made it prohibitively expensive, which slowed its mainstream adoption. This is no longer the case, however, and customers' perceptions and expectations for GaN are evolving accordingly.

"Taking into account the inherent power density advantage and scalability to eight-inch substrates, Gen 4 GaN on silicon (GaN on Si) is expected to yield GaN-based devices that are half the semiconductor cost per watt of comparable LDMOS products and significantly lower cost than comparably performing but more expensive GaN on silicon carbide (GaN on SiC) wafers at volume-production levels," they continue. "So parallel advancements in the GaN supply chain and GaN technology roadmap have enabled the manufacturing scale and cost structures necessary to allow GaN to penetrate into commercial domains like wireless base stations, RF energy applications, and beyond. For customers evaluating where GaN does and doesn't fit based on performance and cost metrics, Gen 4 GaN changes the equation considerably."

Military RF and microwave outlook

GaN continues to gain momentum among military system designers, a fact that is also emblematic of the overall health of the military RF and microwave market.

"We anticipate that the demand for RF and microwave technology will continue to grow for military radar applications," say Carlson and Gallucio. "Active electronically scanned arrays (AESAs) will play an increasingly vital role within the overall sensor mesh network, spanning air, land, sea, and space domains. And as these systems become more affordable and easier to manufacture, their proliferation will accelerate. At the system level, the number of RF elements onboard an AESA is considerably higher than with legacy radar systems. As AESA deployments ramp up, the aggregate RF content footprint expands exponentially."

NXP's Smith says that his company focuses their products for aerospace and defense applications on "three major areas: radar, communications, and EW. RF is an essential component in radar applications for DME [distance measuring equipment], TACAN [tactical air navigation system], IFF [identification friend or foe], data links, and more. Although it can take several years to update current systems, the need for technological advances is clear to us."

New radar systems and EW systems are only getting more complex: Whether it's the transition to phased-array antennas or developing cognitive EW capability, the complexity and volume of electronic components is only going to increase.

"RF and microwave technology is prevalent in radar, electronic surveillance/countermeasures, and communications systems for military and space applications," Goldstein says. "As radar systems transition to phased-array antenna, the volume of electronics required increases dramatically from less accurate and less reliable single-rotating-antenna architectures. New radars will have thousands of antenna elements and these architectures will require RF and microwave electronics in the areas of transmit/receive functionality, up/down conversion, and frequency synthesis. Electronic countermeasures/surveillance has been made a priority by the U.S. government; new initiatives require RF and microwave components with wider bandwidths, improved efficiencies, and faster frequency-hopping capabilities.

"The new communications architectures are being simplified by integrated radio-on-a-chip silicon solutions," Goldstein continues. "These new transceiver chips include transmit and receive high-speed converters and frequency up-conversion with frequencies currently as high as 6 GHz. This single-chip solution covers many current military communications applications, which require operating frequencies up through Ka-Band, such as VSAT. These utilize these new transceivers, which can then be cascaded with further RF and microwave content to achieve higher frequency bands. As you can see, these applications are full of microwave content and these areas are the focus of new systems and system upgrades needed by the aerospace and defense industry."

Moreover, the automotive market's investment in radar technology will also help drive innovation and cost reductions due to the high volumes of that industry, Goldstein says. New products have been released that are focused on 24-GHz and 77-GHz automotive radar applications, he notes. "The continued cost reductions achieved through high levels of integration on silicon have enabled the introduction of radar sensors on most models of new automobiles. The volume of cars utilizing RF and microwave technology is growing very quickly." **MES**

Leveraging GaN for radar and soon GaN-on-diamond

By Mariana Iriarte, Associate Editor

U.S. Air Force Research Laboratory officials, in conjunction with the Office of the Secretary of Defense, have selected Raytheon for a follow-on Title III contract to improve its process to produce gallium nitride (GaN)-based semiconductors. In a Q&A with Chris MacDonald, an Engineering Fellow in Raytheon's Integrated Defense Systems (IDS) Microelectronics and Engineering Technology (MET) Department, he discusses the thermal challenges engineers face when implementing GaN technology into radar and electronic warfare (EW) systems, as well as how GaN-on-diamond could effectively help in the future. Edited excerpts follow.

Chris MacDonald

A GaN wafer in the Raytheon foundry. Photo courtesy Raytheon.

MIL-EMBEDDED: ***Please provide a brief description of your responsibility with Raytheon and your role within the company.***

MACDONALD: I serve as the technical lead for the current Title III program. I also serve as the technical lead for many of the GaN process developments as well as the transition and production activities that we have, some of which are internally funded and others that are externally funded, such as the GaN Title III program.

I've been with Raytheon for 15 years, all with the foundry itself. Earlier in my career I focused on gallium arsenide (GaAs) and more recently with GaN. I began working on GaN nine years ago, which was when we started transitioning GaN process into production.

MIL-EMBEDDED: ***U.S. Air Force officials recently granted Raytheon a contract to advance GaN-based technology, and in the release you state that industry has only scratched the surface with the technology. So what is its impact today and what capabilities will it enable five, 10 years down the road?***

MACDONALD: This is a similar follow-on program, similar in that it's Title III and with the Air Force Research Lab. The focus has shifted a little bit from the earlier contract, which focused on the process maturity and manufacturing-readiness level. This most recent contract focuses on improving and tapping additional RF [radio-frequency]

APPLICATIONS THAT WILL INCORPORATE GAN COMPONENTS INCLUDE EASR FOR AIRCRAFT CARRIER AND AMPHIBIOUS-CLASS SHIPS, AS WELL AS AMDR FOR DDG-51 FLIGHT III DESTROYERS.

performance. One of the goals is to gain higher performance from our GaN process, while also maintaining reliability and the cost standard that we achieved in the first Title III contract.

In the long term, five to 10 years down the road, we are looking at alternative material systems like GaN-on-diamond, which we are currently developing. One of the advantages going to diamond in the long term is its thermal benefits: Diamond is the best thermal conductor out there.

MIL-EMBEDDED: ***In a previous GaN Title III contract (completed in 2013), what was the focus on the program and eventual outcome?***

MACDONALD: In the earlier Title III contract, we focused on transitioning the process into production and on maturing the GaN process in terms of the producibility, cost, and reliability of the technology. Some of the improvements that we saw in that contract were in terms of both cost reduction and reliability. Ultimately, that program enabled us to achieve Manufacturing Readiness Level [MRL] 8.

MIL-EMBEDDED: ***What are some of the challenges engineers face when implementing GaN technology into radar systems?***

MACDONALD: One of the things that we see with GaN technology is that we were able to achieve higher power. However, with that higher power, thermal challenges emerge because we are producing more power and more power tends to produce more heat. Those challenges are one of the reasons we're focused on GaN Title III, so we can continue to develop and improve the performance. If we can operate GaN more efficiently, it should ease the thermal concerns.

MIL-EMBEDDED: ***When is GaN not the ideal choice?***

MACDONALD: In addition to GaN, we also use GaAs technology for many systems we design. We actually will have a hybrid mixture of both GaN and GaAs integrated circuits within our system, with the choice being dependent upon the mission and the application, as well on as the requirements and functions of those circuits. In many cases, we will use GaN for higher-power functions in an application where GaAs may still serve a purpose for lower power functions, such as phase or attenuation. In other systems we may use a mixture of GaAs and GaN.

When is it not an ideal choice? It depends on the systems, the function, and what we're trying to get out of that individual circuit.

MIL-EMBEDDED: ***This technology is expected to be fielded into Raytheon's Space and Airborne Systems' Next Generation Jammer (NGJ) program. What are some the benefits associated with using this technology in the program?***

MACDONALD: Some of the benefits we are going to see will be in terms of both performance and cost. Those benefits will then translate at the system level to size and weight reduction, while improving some of the performance of the actual radar itself. These enhancements will spread to the NGJ program as well as to our radar-based systems, such as the U.S. Navy's Air and Missile Defense Radar (AMDR) and Enterprise Air Surveillance Radar (EASR). The improvements can be used across any of our GaN-related systems or applications.

MIL-EMBEDDED: ***What other military applications are likely to take advantage of GaN technology? Electronic warfare? Communications?***

MACDONALD: GaN is at the heart of many Raytheon systems, such as ground- and sea-based radars, electronic warfare systems, missile applications, and communications.

Applications that will incorporate GaN components include EASR for aircraft carrier and amphibious-class ships, as well as AMDR for DDG-51 Flight III destroyers.

MIL-EMBEDDED: ***How will GaN impact those applications?***

MACDONALD: GaN's impact on these platforms is similar to its effect on the NGJ program, as it enables performance and cost benefits. When you move from GaAs to GaN technology, you can get five to 10 times the power, thanks to the increased power density, which in turn improves performance and efficiency. **MES**

***Christopher J. MacDonald** is an Engineering Fellow in Raytheon's Integrated Defense Systems (IDS) Microelectronics and Engineering Technology (MET) Department. He joined Raytheon in March 2001 and was promoted to his current position in 2016. MacDonald is the lead process engineer and the section manager for the Wafer Fabrication Engineering in the MET Department, which provides development and processing engineering support for Raytheon's key GaN and GaAs compound semiconductor processes used in the design of monolithic microwave integrated circuits (MMICs). He received a bachelor's degree in materials science and engineering from Massachusetts Institute of Technology and a master's degree in manufacturing engineering with a concentration in materials processing from Boston University.*

MIL-STD-1553 PCI and cPCI cards feature eight dual-redundant channels

Data Device Corp.'s BU-67X10i/T card series contains as many as eight dual-redundant MIL-STD-1553 channels and is targeted at military and aerospace applications. The PCI and cPCI versions offer front-panel I/O and include a cable to interface to all 1553 channels. The I/O mix and high channel count on a single card, says the company, saves space, power, weight, and cost. The cards include the AceXtreme MIL-STD-1553 C Software Development Kit (SDK) and drivers to support all modes of operation for Linux, VxWorks, and Windows 2000/XP/Vista/7, including source-code samples and detailed documentation.

A common SDK exists across all operating systems for all cards enables the programmer portability across different platforms. The BusTrACEr graphical user interface, available as an option, has point-and-click application source-code generation capability to reduce risk and shorten development cycles. Additional features include a rugged PMC design for harsh environment, shortened developmental cycle, and IRIG-106 Chapter 10 onboard formatting. Applications for the PCI and cPCI versions include mission computers, displays, radar systems, and simulators.

Data Device Corp. | www.ddc-web.com | www.mil-embedded.com/374011

Small-form-factor computer for avionics market

Alligator Designs' rugged small-form-factor (SFF) computer, called the Falcon II, is designed to be configurable and expandable using modules with standard electrical and connector interfaces. It is tailored for the avionics, military, and rugged industrial market. The Falcon II is configurable with the Intel Core i7 and Xeon E3, AMD G-Series system on chip (SoC), Intel Atom Bay Trail, and Free scale PowerPC.

The Falcon II is designed to support all I/O typically needed in the targeted applications, including MIL-STD-1553B, ARINC-429, AS-5643 MIL firewire, video graphics, video frame capture, software-defined radio (SDR), RS-232/422/485, Fibre Channel, GigE and 10GigE, analog and discrete signals, and field-programmable gate array (FPGA)/general-purpose graphics processing unit (GPGPU) processors. The I/O can be in XMC or MiniPCIe, including AcroPack. Users can also opt for inertial measurement and navigation, GPS, Wi-Fi, cellular modem signals, and multi-drive RAID storage solutions. Alligator's chassis is intended to use minimum space while optimized to manage heat dissipation. To prevent high NRE costs, the system architecture makes maximum use of standards-based computer, graphics, I/O modules, and connectors. The standardized midplane design supports a mixture of commercial off-the-shelf (COTS) module types.

Alligator Designs | www.alligatordesigns.com | www.mil-embedded.com/374021

Hermetically sealed relays for extreme environments

TE Connectivity (TE) designed its CII FC-325 series relay for harsh inductive, motor, and lamp load applications within the aerospace, defense, and marine markets. The CII FC-325 Series is a three-pole, 25 amp, nonlatching, hermetically sealed relay that is all welded, lightweight, and has a higher capacity design than similar balanced armature versions. This design, according to TE, provides stable performance and extends the relay's life. The relay's all-welded design creates a reliable alternative to similar solder-sealed relays in the market.

Configured as a 3PST/NO (DM), the double make/break contact design of the CII FC-325 series relays shares the load across two contact sets, resulting in less wear and tear on the relay. It is qualified to MS27418 specifications; the series also features a 1.5-inch corrosion-protected cube enclosure. The relay, weighing 0.452 pounds, is aimed at applications such as commercial and military aircraft, weapons systems, launch systems, ground-support equipment, fuel pumps, galley equipment, and missiles. Both solder hook and terminal block configurations are available.

TE Connectivity | www.te.com | www.mil-embedded.com/p374013

Rhamnousia: Framework for cyberattack attribution

By Sally Cole, Senior Editor

The science of cyberattack attribution gets a boost, thanks to a U.S. Department of Defense $17.3 million award to a team led by Georgia Institute of Technology researchers.

The team is working to develop an attribution framework called Rhamnousia – a nod to the Greek goddess Rhamnous and the spirit of divine retribution – to reliably track virtual illicit actors engaging in cyberattack campaigns.

Attribution is critical for deterrence within cyberspace, because deterrence is impossible without the ability to identify the culprits behind cyberattacks.

Just how challenging is attribution? In the wake of Russia's reported state-sponsored hacking of the Democratic National Committee and others during the 2016 U.S. election, an assessment report issued by the U.S. Office of the Director of National Intelligence describes determining attribution in cyberincidents as "difficult, but not impossible."

That's because every cyberoperation – malicious or not – leaves behind a trail that analysts can trace by tapping a constantly growing knowledge base of previous events and known malicious actors and the tools and techniques they favor, as well as any of their consistent errors or unique characteristics.

But attributions tend to go far beyond simply determining who was behind an attack – including judgments about whether it was an isolated incident, the possible motives behind the attack, and whether a foreign government played a role in ordering or leading it. It's crucial, particularly at the nation-state level, to get the attribution right if sanctions or some other retaliatory response is being considered.

"Attack attribution has been the Holy Grail for the security community for years," says Manos Antonakakis, an assistant professor in Georgia Tech's School of Electrical and Computer Engineering and the principal investigator for the Rhamnousia project. "Once you can reliably track an attack operation against your network infrastructure you're in a better position to defend and reason about necessary policy actions, as an organization or even a state."

The biggest problems with attribution today? It's a complex, largely manual process that requires expertise, resources, and time.

In the case of identifying nation states behind cyberattacks, using forensic analysis to identify them is extremely difficult. "Data-driven identification with actual hard evidence of nation-state actors is even harder," Antonakakis says.

By using public, free, or commercially available data – known as threat intelligence – Rhamnousia will enable users to piece together an attack-attribution analysis that will be easier for investigators to confirm and independently validate.

The team is developing efficient algorithmic methods capable of converting the group's experience with manual attack attribution to novel, tensor-based learning methods. These algorithms will, in turn, allow expansion of existing efforts to create a science of attribution and traceback and will generate reports to be shared within the attribution community.

Artificial intelligence (AI) and machine learning can help speed up the attribution process, which frequently requires weeks or months to complete. "AI and machine learning are among the very few tools we have to help us analyze different datasets in a timely and rigorous manner," Antonakakis explains. Much as it does for internet searches, "machine learning should be able to shrink the time required for an attribution report to be generated, making attribution analysis more relevant and impactful."

It's important to note that "identifying a threat indicator is still a very hard detection problem," he points out. "Every organization needs to be able to 'quickly' identify that something is wrong within their networks, because attack prevention is often an impossible task."

Given enough resources, highly motivated adversaries like nation-state attackers will have access to similar, if not exactly the same, defenses. "Evading them is just a matter of time," Antonakakis notes. "In other words: Attacks are inevitable, breaches will happen, and we should prepare for the actions after such events."

Beyond existing network defenses, by using alternative reasoning and processes, "we want to use the threats and indicators to quickly move from a single attack event to the virtual actor(s) behind an attack," he continues. "Failure to do so leaves you fighting multiple different seemingly independent threats, which effectively saturates the security personnel within your organization."

Timely and accurate attack attribution is an important, if not the most important, action for organizations immediately after they detect a security event. "The Rhamnousia framework is a start and, if we're successful, we should be able to create attribution analysis for a variety of attacks – targeted, nation-state, or otherwise," Antonakakis says.

The Rhamnousia project – a group effort expected to run about four-and-a-half years – includes other academic institutions and companies. The end goal of the project is to combine intrusion detection with attribution to provide a systematic and scientific way of helping U.S. companies and the government cut off attackers more quickly.

CHARITY

Operation Homefront

Each issue in this section, the editorial staff of *Military Embedded Systems* will highlight a different charity that benefits military veterans and their families. We are honored to cover the technology that protects those who protect us every day. To back that up, our parent company – OpenSystems Media – will make a donation to every charity we showcase on this page.

This issue we are highlighting Operation Homefront, a nonprofit organization that provides emergency assistance for U.S. military troops and wounded service members when they return home. The organization also raises funds to provide financial and community assistance to families while troops are participating in a tour of duty.

Founded in San Antonio, Texas, in 2002, Operation Homefront works in close partnership with a variety of corporations and partners to help military families with short-term critical assistance, working toward long-term stability, and recurring family support needs.

One of the organization's major efforts is its "Homes on the Homefront" program: Through a partnership with Chase Bank, Bank of America, and Wells Fargo, the program donates mortgage-free homes to eligible military families. According to Operation Homefront, the program has granted more than 100 homes to qualifying veterans and military families. Another housing program is a transitional housing initiative, which enables young veterans returning from service to live rent-free while they undergo the transition process back to civilian life. These returnees also participate in support groups, financial counseling, and career planning workshops.

Operation Homefront also runs other programs, including "Military Child of the Year," "Hearts of Valor" (for caregivers), the "Back to School Brigade" school-supply collection program, and "Holiday Meals for the Military."

The organization's 23 locations serves 43 U.S. states, with the national office handling cases in states that lack a local office.

For more information, visit www.operationhomefront.net.

E-CAST

Getting the requirements right for safety-critical systems

Sponsored by Jama and AFuzion

Safety-critical systems, whether in avionics, automotive, or medical applications, are built on exacting requirements. The complexity of these systems in each market is expanding at an exponential rate. This added complexity, when combined with compressed product-development schedules, means that the need for a strong requirements foundation has never been greater.

In this e-cast, Vance Hilderman, CEO of safety-critical systems and software-engineering company AFuzion, covers best practices for requirements basics, mistakes to avoid, and regulatory priorities for system requirements including ISO26262, IEC 61508, DO-178C, IEC 62304, and DO-254.

View archived e-cast: ecast.opensystemsmedia.com/713

View upcoming e-casts:
opensystemsmedia.com/events/e-cast/schedule

WHITE PAPER

WFMC+ mezzanine card evolution for low latency and high bandwidth solutions

By Annapolis Micro Systems

Latency, or the time between input and output, can be very important, depending on the application. For processing of communications intelligence (COMINT) like audio conversations, text data, and the like, relatively long latency is tolerable. For applications like radar and electronic warfare, even a small amount of latency is problematic because of the need for quick response times.

Similarly, these demanding applications require very high bandwidth (throughput) due to the volume of data involved.

This white paper covers the way in which mezzanine cards have evolved to address the need for very high bandwidth and super low latency.

Read the white paper: http://mil-embedded.com/white-papers/white-latency-high-bandwidth-solutions/

Read more white papers:
http://whitepapers.opensystemsmedia.com