

Military

EMBEDDED SYSTEMS

@military_cots

John McHale

Remembering PICMG's Joe Pavlat

7

Industry Spotlight

Cloud security

32

Mil Tech Trends

Shrinking RF transceivers

22

University Update

Robots learn through stories

43

MIL-EMBEDDED.COM

October 2016 | Volume 12 | Number 7

SIMULATION AND TRAINING USING DISTRIBUTED SYSTEMS

P 18

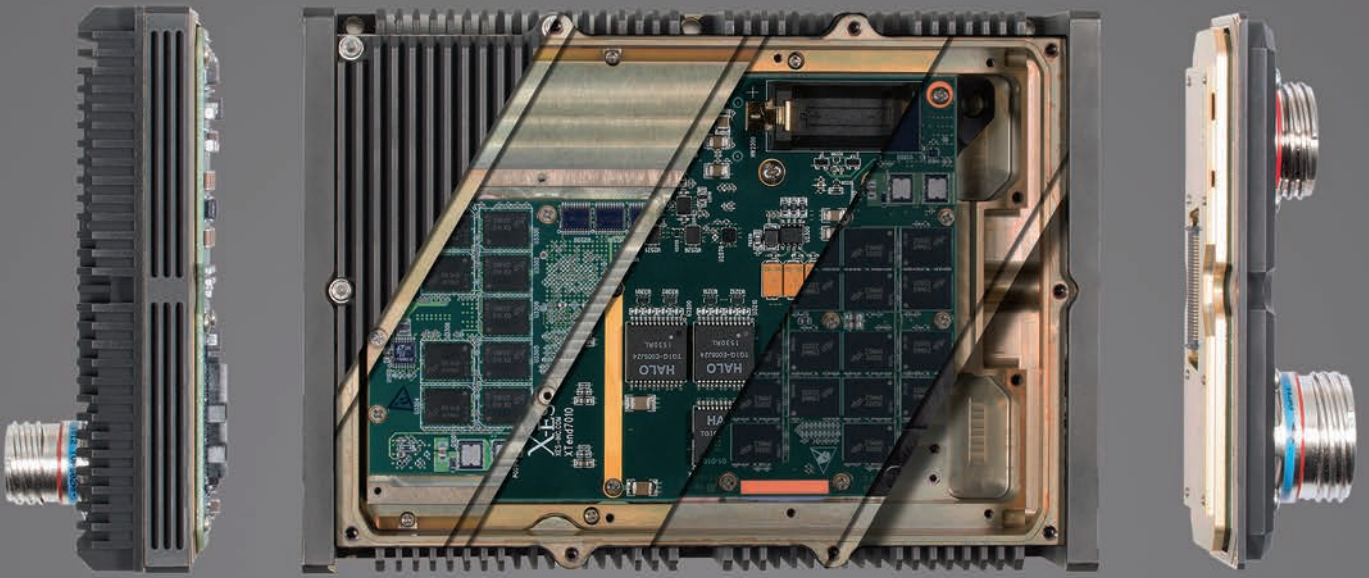


P 12

Interview with LeAnn Ridgeway, Vice President and General Manager of Simulation and Training Solutions for Rockwell Collins

Enhanced SDR for defense communications

P 29



Battlefield-Ready Small Form Factor (SFF) Rugged Systems

Flight-qualified embedded systems designed and tested to meet the rigorous standards of MIL-STD-810 and DO-160 for maximum performance when it matters most.

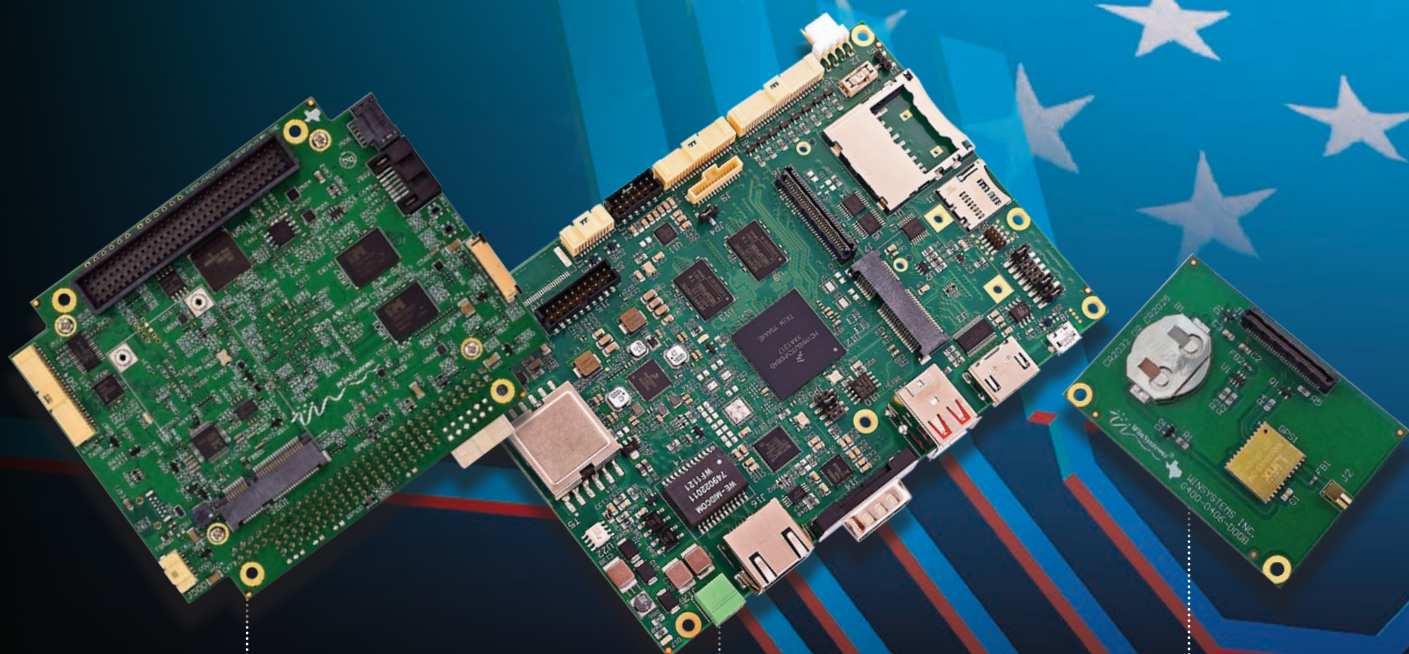


Extreme Engineering Solutions
608.833.1155 www.xes-inc.com



Designed, manufactured, and supported in the USA

RUGGED, RELIABLE, RESILIENT!



PPM-C407 Fanless
E3800 PC/104 SBC Computer

SBC35-C398DL-2-0
Dual-Core Freescale i.MX 6DL
Cortex A9 Industrial ARM®

IO60-GNSS with Global GPS
Receiver Module with
Bus Expansion



SCADA



ENERGY



IOT



TRANSPORTATION



AUTOMATION

Single Board Computers

COM Express Solutions

Power Supplies

I/O Modules

Panel PCs

Across a broad range of industry applications—from energy and IoT, to industrial automation and transportation—WinSystems' embedded single board computers enable the collection, processing and transmission of real-time data requirements at the heart of your overall system.

Our full line of rugged, reliable and resilient embedded computers, I/O cards, cables and accessories help customers design smarter projects that deliver new efficiencies, greater access to information and improved reliability. Whether it's one of our standard products or full custom design, WinSystems brand products are delivered with uncompromising engineering, quality and technical support.

When your reputation and customer satisfaction is on the line, look to ***The Embedded Systems Authority!***

715 Stadium Drive | Arlington, Texas 76011
Call 817-274-7553 or visit www.winsystems.com.

Ask about our product evaluation!



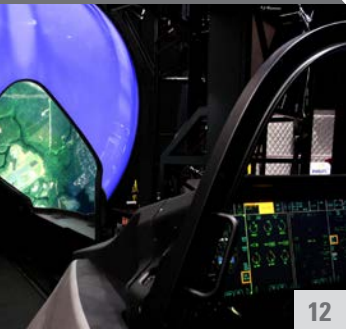
 **WinSystems®**
The Embedded Systems Authority

Military

EMBEDDED SYSTEMS

October 2016

www.mil-embedded.com



12



18



29



32

SPECIAL REPORT

Simulation and Training

- 12** Demand rising for military simulation and training tech, virtual-reality tools, and head-worn displays
Interview with LeAnn Ridgeway, Vice President and General Manager of Simulation and Training Solutions for Rockwell Collins
By John McHale, Editorial Director
- 18** Discrete vs distributed: Transforming military training and simulation systems
By Mike Pape, Dedicated Computing

MIL TECH TRENDS

Military Radio Design Trends

- 22** RF transceivers provide breakthrough SWaP solutions for defense and aerospace applications
By Wyatt Taylor and David Brown, Analog Devices, Inc.
- 26** Software-defined radio: To infinity and beyond
By Manuel Uhm, Ettus Research
- 29** Software-defined radio enables enhanced military communications
By Stephanie Chiao, Per Vices

INDUSTRY SPOTLIGHT

Secure Cloud Computing

- 32** Cloud security for military ops: It's complicated
By Sally Cole, Senior Editor
- 38** Cybersecurity risks: Network-enabled weapon systems and humans
An interview with Gil Nolte, executive advisor to Booz Allen Hamilton
By Mariana Iriarte, Associate Editor



38

COLUMNS

Editor's Perspective

- 7** Remembering Joe Pavlat
By John McHale

Field Intelligence

- 8** Technology insertion: Balancing performance and stability
By Charlotte Adams

Mil Tech Insider

- 9** Enabling Mounted Assured PNT with one COTS-based box
By Mike Southworth

Cybersecurity Update

- 42** Outmaneuvering potential IC sabotage
By Sally Cole, Senior Editor

University Update

- 43** Stories are part of the curriculum for artificial-intelligence robots
By Mariana Iriarte, Associate Editor

DEPARTMENTS

- 10** **Defense Tech Wire**
By Mariana Iriarte
- 44** **Editor's Choice Products**
- 46** **Connecting with Mil Embedded**
By Mil-Embedded.com Editorial Staff

E-CASTS

<http://ecast.opensystemsmedia.com>

Military ISR sensors and embedded signal processing

Presented by Abaco Systems, Curtiss-Wright, Pentek
ecast.opensystemsmedia.com/640

How to design distributed robotic control systems

Presented by RTI and Energid
ecast.opensystemsmedia.com/672



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



@military_cots

Published by:

OpenSystems media.

All registered brands and trademarks within *Military Embedded Systems* magazine are the property of their respective owners.

© 2016 OpenSystems Media © 2016 Military Embedded Systems
ISSN: Print 1557-3222



ON THE COVER:

Top image: The U.S. Army's Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) design for realistic training operations breaks out into three primary elements: the training environment where the soldiers train, training management and assessment processes that build and maintain training readiness, and training infrastructure that incorporates facilities and network services that make it all work. Image courtesy U.S. Army.

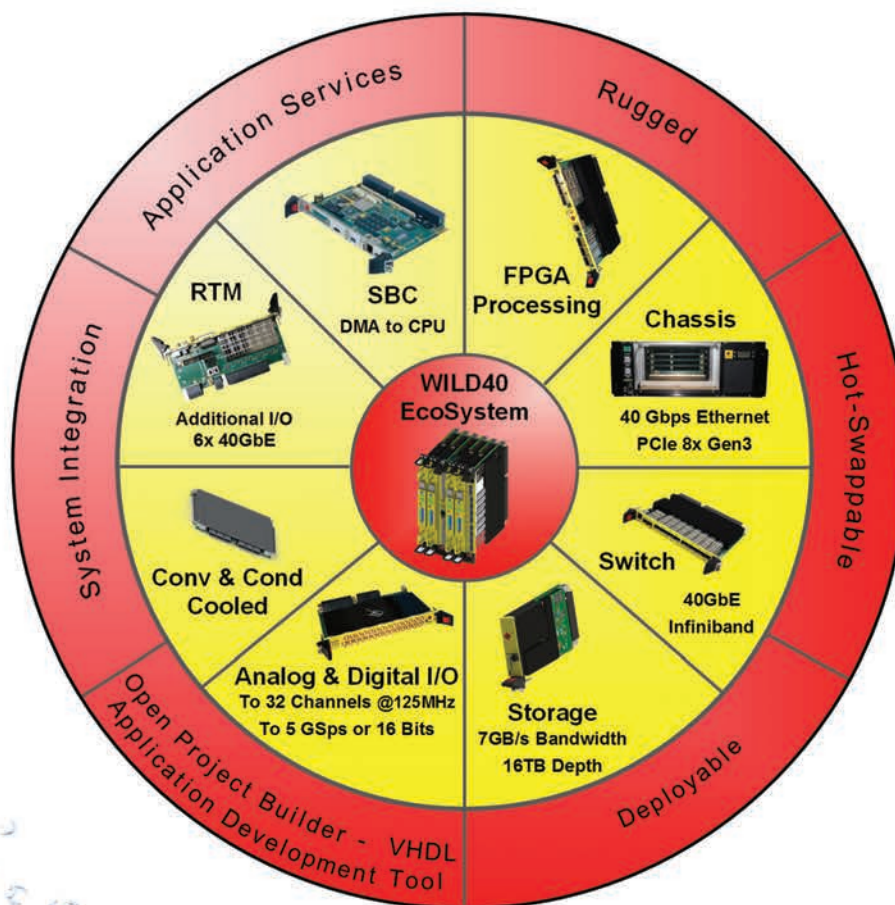
Bottom image: Sgt. Kentrell Billups, a radio technician with 1st Air Naval Gunfire Liaison Company, tries to establish satellite communications with the division fire support cell during Exercise Maple Resolve 2015 aboard Canadian Manoeuvre Training Center, Camp Wainwright. Photo credit: Cpl. Owen Kimbrel/U.S. Marine Corps.





Keep Your FPGA System Integration on Target and above Water

WILDSTAR™ 40Gb 6U and 3U OpenVPX EcoSystem
Altera Arria 10® AND Xilinx UltraScale™



Ultra-Low Latency EW Solutions
24ns Latency from ADC Input to DAC Output!

All Systems Include *Open Project Builder™*
Our Vendor-Independent FPGA Development Tool

See a Demo at www.AnnapMicro.com/OPB

See us at Booth 531 at 53rd AOC International Convention

Made in USA 
Annapolis Micro Systems
www.AnnapMicro.com
410-841-2514

SEE WHAT'S WAITING FOR YOU AT

1 631 435-0410 • sales@behlman.com • www.behlman.com

WWW.ACDCPOWERPLUS.COM

When you need highly regulated AC or DC power, go to www.acdcpowerplus.com for the most reliable power supplies, the broadest selection, and unique innovative power solutions, which help you do your job better. All are designed and manufactured in the USA, including the VPXtra™ series of highly reconfigurable VPX power supplies, which meet the highest quality and reliability requirements of the VITA standards.

VPXtra™



POWER GROUP
Behlman Electronics

VISIT ACDCPOWERPLUS.COM FOR INSTANT FREE ACCESS TO VALUABLE PAPERS AND ARTICLES ON POWER SOLUTIONS.

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
PICMG EDITORIAL DIRECTOR Joe Pavlat jpavlat@opensystemsmedia.com
MANAGING EDITOR Jennifer Hesse jhesse@opensystemsmedia.com

SALES

SALES MANAGER Tom Varcie tvarcie@opensystemsmedia.com
(586) 415-6500
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 Eric Henry ehenry@opensystemsmedia.com
(541) 760-5361
STRATEGIC ACCOUNT MANAGER Kathleen Wackowski kwackowski@opensystemsmedia.com
(978) 888-7367
SOUTHERN CALIFORNIA REGIONAL SALES MANAGER Len Pettek lpettek@opensystemsmedia.com
(805) 231-9582
SOUTHWEST REGIONAL SALES MANAGER Barbara Quinlan bquinlan@opensystemsmedia.com
(480) 236-8818
NORTHERN CALIFORNIA REGIONAL SALES MANAGER Twyla Sulesky tsulesky@opensystemsmedia.com
(408) 779-0005
ASIA-PACIFIC SALES ACCOUNT MANAGER Elvi Lee elvi@aceforum.com.tw
EUROPE SALES ACCOUNT MANAGER James Rhoades-Brown james.rhoadesbrown@husonmedia.com



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
TECHNICAL CONTRIBUTOR Rory Dear rdear@opensystemsmedia.com
CONTENT ASSISTANT Jamie Leland jleland@opensystemsmedia.com
CREATIVE PROJECTS Chris Rassiccia crassiccia@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@wrightsmmedia.com
(281) 419-5725

Remembering Joe Pavlat

By John McHale, Editorial Director



Summer ended with sad news for our OpenSystems Media family when we learned that our friend and coworker, Joe Pavlat, Editorial Director of PICMG Technologies magazine, passed away suddenly at his home in Grass Valley, California. He was only 63 years old.

Joe joined our family back in 1996 when we partnered with him and the PCI Industrial Computer Manufacturers Group (PICMG) to form CompactPCI Systems magazine. The publication reigned as the top magazine in OpenSystems Media's stable for more than a dozen years, even after it evolved to include "AdvancedTCA" in its title as CompactPCI and AdvancedTCA Systems. Its success was attributable to Joe's passion for the technology, which he codeveloped, as well as his leadership as president and chairman of PICMG since its inception 22 years ago.

As my colleague, Pat Hopper, Publisher at OpenSystems Media, said to me when we heard of Joe's passing, "No one did more for CompactPCI and AdvancedTCA than Joe."

On the occasion of PICMG's 20th anniversary, Joe renamed the magazine PICMG Systems & Technology, as the organization's membership had become more global and its standards were embraced by multiple industries worldwide, including telecommunications, industrial, the Internet of Things (IoT), automotive, aerospace, and defense.

Such growth was a tribute to Joe's leadership and enthusiasm for the open standards developed under the PICMG umbrella as well as his knowledge of embedded computing developed over a 36-year career that included leadership roles at Prolog, Motorola, and Parker Hannifin.

From a military electronics perspective, Joe had been a leading advocate for the adoption of open standards and open

architectures in military systems since we met two decades ago.

Ironically, PICMG was founded shortly after the famous commercial off-the-shelf (COTS) memo was issued by then-U.S. Secretary of Defense William Perry; the memo ordered military programs to leverage COTS wherever and whenever possible. Twenty years later, COTS solutions based on PICMG standards such as CompactPCI and COM Express are quite commonly deployed in defense applications from radar to satellite communications. Joe had a right to be proud of that achievement.



Joe Pavlat

Always press-savvy and friendly, Joe had a way of making complicated engineering subjects easy to understand and easy to write about for young trade press reporters. He taught and informed, but never tried to spin me.

When I joined OpenSystems Media five years ago, Joe was one of the first to welcome me and say how excited he was for us to be working together. A gentleman with a kind manner, he was always quick with a compliment when he saw an article he liked and sincere when he asked after his colleagues. Those traits combined with his knowledge, expertise, and reputation made him popular with his coworkers and a valuable member of our team.

"I was lucky to have known him," said Rosemary Kristoff, President of OpenSystems Media. "Just having him around made you feel better, with his candor and his unique ability to keep things in perspective. Joe was a genuine, frank, and loyal friend."

He had an easy way with conversation, as his interests ranged from embedded computing to hiking to physics to flying. A native of Wisconsin, he originally pursued a physics degree at the University of Wisconsin at Madison before turning toward computers and instrumentation. He actively kept up with physics over the years, even participating in experiments in Antarctica and on top of the Haleakala volcano in Hawaii.

Joe also loved to fly and even volunteered his time to fly for the Monterey Sheriff's department Aero Squadron. For years he said he wanted to take me flying, saying there was never a more careful pilot than he. Joe only flew on perfect days because, as he told me: "I hate turbulence." The same could be said for how he approached his work with OSM. We never saw him encounter a bump he couldn't smooth out.

The PICMG Systems & Technology magazine, in all its iterations, was always a reflection of Joe. His was the face of PICMG, CompactPCI, and AdvancedTCA. I cannot think of those without thinking of Joe.

I also cannot imagine having a PICMG Technologies staff meeting and knowing he won't be there to share his advice, tell a story, or reminisce about old friends. I wished I'd flown with him and I wish he were still here, so I could tell him that. We miss you already, Joe, and always will.

Predeceased by his parents and brother, Joe is survived by his wife.

Technology insertion: Balancing performance and stability

By Charlotte Adams

An Abaco Systems perspective on embedded military electronics trends



Embedded computing systems have benefited enormously from the flood of innovation in the electronics industry: Military programs over the years have enjoyed ever faster processors, smaller form factors, and steadily declining prices per unit of performance.

At the same time, military programs have requirements, which fly in the face of commercial market trends. These programs' lives are measured in decades rather than months. A mission computer or fire-control computer procured 20 years ago may have to function for another decade or so with minimal disruption from market turbulence.

Yet military systems can't stand pat – they have to evolve, both to increase performance against threats and to avoid obsolescence. The trick is to manage their evolution in such a way as to minimize cost and risk. Timely and well-designed technology insertions can extend a system's life without costly redevelopment and redesign. Ideally, a system's movement up the technology curve will consist of relatively painless plug-and-play upgrades.

Upgrade strategies

Technology upgrades involve interconnected hardware and software strategies on the part of the board designer, with the aim of increasing performance without making life more difficult for the application software. Ideally, changes to the hardware are masked from the application so that the software can continue to run unhampered.

Of course, some changes do affect the application. The semiconductor industry's move from single-core to multicore integrated circuits, for example, required adaptations. Most of the heavy lifting in this area, however, was done by the operating system vendors with few trickle-down effects at the application level.

Stability is also important on the hardware side. Board vendors, for example, try to keep the pinout stable. It helps to use standard interfaces like VME, although the very longevity of this standard poses its own problems, such as the unavailability of VME bridge silicon. Some board providers substitute field-programmable gate arrays (FPGAs), which implement the bus logic in firmware. If this solution is threatened by FPGA obsolescence, the intellectual property can be transitioned to another device.

Upgrades also maintain interfaces to legacy protocols that customers depend on, such as MIL-STD-1553 and High-Level Data Link Control (HDLC), but such solutions can add newer ones, such as Universal Serial Bus (USB), if users are willing to make trades.

It also helps to have a tight technology-insertion philosophy, where no detail of the board's hardware or software design is too small to consider in planning upgrades. A vague, generalized compatibility between product generations is insufficient to ensure the value of the upgrade.

Within this framework, flexibility is key. Users need options for major performance growth but also for life extension within the existing performance and thermal envelope. There needs to be a certain number of standard variants within a product range.

Software side

Real-time operating systems (RTOSs) also have a limited shelf life: Over a 20-year period, a popular RTOS may cycle through 50 to 60 versions, and the RTOS vendor will eventually drop support for earlier chips.

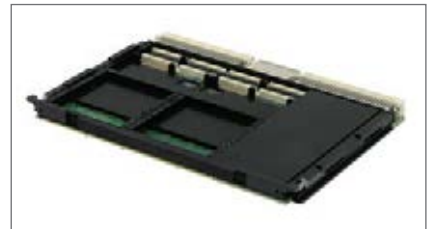


Figure 1 | The Abaco PPC11A, the most recent in a form/fit/function-compatible family of single-board computers dating back over a decade.

Suppliers of embedded computing boards also try to keep software components as stable as possible. Necessary application programming interfaces (APIs) are maintained even as new APIs are added. Abstraction of the software from particular hardware devices means that a customer's application doesn't see anything different even if it's operating on different hardware. The board support package (BSP) that interfaces between the hardware and the operating system also is kept as consistent as possible, maintaining vendor-specific functions that customers rely on.

The Abaco Systems PowerXtreme PPC11A (Figure 1) is a rugged 6U VME single-board computer – the 10th-generation SBC in the PowerXtreme family – and is available in low power consumption (0.5 times its predecessor) and high processing power (2 times its predecessor) versions for those looking to upgrade.

There's much more to technology insertion than meets the eye. By controlling the hardware and software configuration of each upgrade, so that performance increases come at minimal cost, board vendors can help to extend the life of programs for decades. This makes it possible for embedded computing resources to move along the performance curve with maximum value and minimum risk.

www.abaco.com

www.mil-embedded.com

Enabling Mounted Assured PNT with one COTS-based box

By Mike Southworth
An industry perspective from Curtiss-Wright Defense Solutions



Today's warfighter depends on GPS signals to acquire accurate position, navigation, and timing (PNT) data. There's a potential downside to dependence on traditional GPS, however: In some terrains, such as dense foliage or urban canyons, GPS signals can become degraded. GPS receivers can also come under attack from adversaries through jamming or spoofing. Given how critical GPS capabilities are for military services, next-generation PNT technologies are emerging to address vulnerabilities from emerging threats and field conditions.

To ensure that ground combat vehicles have the most reliable and accurate PNT data, the U.S. Army is advancing a Mounted Assured PNT System (MAPS) approach that enables warfighters to transition away from the use of less robust legacy GPS devices. Based on new networkable devices that support integrated military selective availability anti-spoofing module (SAASM) and M-Code ground-based GPS receiver application module (GB-GRAM) receivers, the improved GPS capabilities can give users access to a higher-power signal (more resistant to jamming and interference) along with improved message formats and signal modulation techniques that make it both faster and more accurate. The receivers also have advanced security features aimed at preventing unauthorized access or exploitation by adversaries.



"As a result of the VICTORY initiative, in recent years, COTS technologies have been developed to enable network-enabled switching, shared processing, and assured military PNT services for constrained tactical ground vehicles."



MAPS goes further, adding to the improved positioning data from secure GPS, a chipscale atomic clock (CSAC) for precision timing, and an inertial measurement unit (IMU) for navigation data even in GPS-denied environments. Recognizing the critical value of the data MAPS delivers to the warfighter, the challenge becomes how to best deploy these new capabilities on platforms already struggling with size, weight, power, and cost (SWaP-C) issues.

Today's ground combat vehicles are typically deployed with multiple independent systems that lack the ability to share their functionalities or data. To address and mitigate this problem, the U.S. Army's VICTORY [Vehicle Integration for C4ISR/EW



Figure 1 | The COTS-based DuraDBH-672 is intended to meet the U.S. Army's Mounted Assured PNT (MAPS) approach to distribute Assured Position, Navigation and Timing (A-PNT) to systems on mounted platforms even in GPS-denied environments.

(command, control, communications, computers, intelligence, surveillance, and reconnaissance/electronic warfare)] architecture has encouraged the use of commercial off-the-shelf (COTS) open-system standards, to help reduce redundancy and free up additional space by optimizing SWaP-C.

As a result of the VICTORY initiative, in recent years, COTS technologies have been developed to enable network-enabled switching, shared processing, and assured military PNT services for constrained tactical ground vehicles. Integrators seeking to deploy MAPS without adding additional burden to a ground vehicle find that a single box subsystem designed to support the VICTORY architecture (with a rugged COTS GbE switch and vetronics computer system) can now also be used to host the GB-GRAM, CSAC, and IMU needed to enable MAPS, all without adding any significant SWaP-C to the platform. Implementing VICTORY together with A-PNT services in a single box means that there is only one subsystem to protect, an approach that can help drive standardization of operator data and increase cybersecurity. Today's combat vehicles display geospatial terrain data to operators in multiple ways, depending on which system/platform is used. VICTORY compliance can unify the operator picture and give warfighters in their vehicles or aircraft, as well as those warfighters back at headquarters, the same real-time operating picture.

The COTS-based DuraDBH-672 Digital Beachhead from Curtiss-Wright (Figure 1) has a VICTORY infrastructure switch and shared services processor along with support for an integrated military GB-GRAM, CSAC, and IMU. It is currently being evaluated by the U.S. Army Tank Automotive Research Development and Engineering Center (TARDEC). The all-in-one unit can consolidate support for network switch, vehicle processor, embedded GPS, atomic clock, inertial navigation, solid-state storage, and add-in I/O interface in one LRU.

www.cwcdefense.com



By Mariana Iriarte, Associate Editor



NEWS

Oshkosh Defense begins full-rate production of P-19R vehicle

U.S. Marine Corps officials received Milestone C approval (Department of Defense [DoD] recommendation to enter the production phase) for the P-19 Replacement (P-19R) Aircraft Rescue Fire Fighting (ARFF) vehicle program and gave the green light to Oshkosh Defense, LLC – an Oshkosh Corp. company – to begin full-rate production on the vehicle.

The contract, originally awarded in May 2013, is worth an estimated \$192 million. The company has since completed all required development, testing, and evaluation.

Oshkosh Defense will deliver 164 P-19R ARFFs through 2019 under this contract. Officials say that the P-19R will replace the P-19A fleet, which was first fielded in 1984.



Figure 1 | The Oshkosh P-19R facilitates on- and off-runway emergency response situations. Photo courtesy of Oshkosh Defense.

Defense agency and Rockwell Collins sign MOA to improve commercial procurement process

Defense Contract Management Agency (DCMA) and Rockwell Collins officials have signed a Memorandum of Agreement (MOA) to establish an improved procurement process of commercial items for military applications.

Rockwell Collins officials explain that the MOA outlines the process to include clearly defined information required from the company to support commercial item classification and a reasonable price that is recommended by the government.

Phil Jasper, executive vice president and chief operating officer for Government Systems at Rockwell Collins, says, "This agreement is an important step in eliminating current inefficiencies associated with determining whether or not an item is considered commercial. By having a clearer understanding up front, we can spend less time doing paperwork and more time getting state-of-the-art technologies in the field."

U.S. Navy demonstrates cross-domain communications capabilities between UUVs and UAVs

The U.S. Navy completed an exercise demonstrating that AeroVironment's submarine-launched Blackwing unmanned aerial vehicle (UAV) can link with a swarm of unmanned undersea vehicles (UUVs) and communicate with the submarine combat control system. The exercise was conducted during the Annual Naval Technology Exercise (ANTX), held recently at the Naval Undersea Warfare Center (NUWC) Division in Newport, Rhode Island.

During ANTX, AeroVironment's secure digital data link – called DDLTM – integrated into all Blackwing UAVs and relayed real-time information from the surrogate manned submarine via the Blackwing UAV to and from multiple UUVs.

According to AeroVironment, a deployed UUV has the ability to collect data while conducting diverse missions ranging from mine hunting to wide-area oceanographic sensing.

Collaboration between U.S. Navy and Raytheon improves mine-hunting sonar

Engineers at NUWC and Raytheon worked together to enhance the company's AN/AQS-20A mine-hunting sonar, improving the system's ability to identify and classify mines.

The collaboration between Raytheon and NUWC formally began last year under a "work for private party" contract funded by Raytheon. Raytheon reports that the system was tested at sea and engineers were able to optimize the sonar's capability to capture images of the ocean floor with enough clarity to see the contents of lobster pots.

"Working together with NUWC, we've applied our collective experience to enhance this undersea warfare technology," says Paul Ferraro, vice president of Raytheon Integrated Defense Systems' Seapower Capability Systems.



Figure 2 | The AN/AQS-20A is the only system certified for deployment from the Navy's Littoral Combat Ships. Photo courtesy of Raytheon.

B-21 bomber officially named: Raider

U.S. Air Force officials announced the results of the Air Force Global Strike Command naming contest, formally designating the long-range striker bomber as the B-21 Raider. With more than 2,100 unique naming submissions, Air Force Secretary Deborah Lee James made the announcement at the Air Force Association's Air, Space, and Cyber Conference, held in September.

One of the airmen James recognized during the ceremony was retired Lt. Col. Richard E. Cole, a Doolittle Raider. Air Force officials explain that the Doolittle Raiders are known for their surprise attack against Japan during World War II on April 18, 1942, which forced the Japanese to recall combat forces for home defense and boosted morale among Americans and U.S. allies abroad.

The B-21 Raider is currently in the engineering and manufacturing development phase with Northrop Grumman as the prime contractor; the industry team to design, build, and deliver the aircraft includes BAE Systems, GKN Aerospace, Janicki Industries, Orbital ATK, Pratt & Whitney, Rockwell Collins, and Spirit AeroSystems.



Figure 3 | Air Force Secretary Deborah Lee James (right) announces the name of the Air Force's newest bomber with the help of retired Lt. Col. Richard Cole (left), one of the Doolittle Raiders, and Tech. Sgt. Derek White (center). Photo courtesy of Scott M. Ash/U.S. Air Force.

iGov receives order to provide mobile communications for HMMWVs

U.S. Air Force officials placed a delivery order under a previous indefinite delivery/indefinite quantity (IDIQ) contract to modify M1145 High Mobility Multipurpose Wheeled Vehicles (HMMWVs). The order is worth \$52,533,693.

Under contract, iGov will modify the fleet of HMMWVs (commonly known as the "Humvee") to provide Tactical Air Control Party users with embedded software and systems for voice, data, and video communications. Officials say this modification will allow Joint Terminal Attack Controllers (JTACs) to control close air support (CAS) aircraft from an armored vehicle, while coordinating and conducting joint CAS missions. Work is expected to be completed by January 2021 and will be performed at iGov's facility in Tampa, Florida.

DISA executive dubs Cyber Protection Teams "the new infantry"

During a training course, John Hickey, cyberdevelopment executive to the Defense Information Systems Agency (DISA), dubbed the Cyber Protection Teams (CPTs) as the "new infantry."

"I'm excited to see you guys added to the force. I'll say you are almost like the 'new infantry' in my perspective because on the cyber domain – it is a domain – we're being attacked daily and we need people who can hunt key terrain," he said. Hickey mentioned that the Department of Defense (DoD) spends approximately \$1 billion a year on cyberoperations to protect the network. "The CPTs are the critical link. We can have the best tools in the world, but it still takes [people] to figure out what's going on," he added.

Hickey's remarks focused on protecting the DoD Information Networks (DODIN). DISA's Cyber Development Directorate manages the coursework that allows students to participate in real-world scenarios and in simulated nonproduction environments in an effort to increase their proficiency level and demonstrate their ability to react to real-world threats.

U.S. Navy accepts delivery of fourth Freedom-variant Littoral Combat Ship

U.S. Navy officials accepted delivery by a Lockheed Martin-led industry team of the fourth Freedom-variant Littoral Combat Ship (LCS), the USS Detroit. Officials say it is scheduled for commission in Detroit on October 22.

The team – comprised of Fincantieri Marinette Marine (FMM), Gibbs & Cox, and more than 500 suppliers in 37 states – is under a full-rate production of the Freedom-variant ship, with six ships under construction at FMM and three more in long-lead material procurement.

Navy officials say that the USS Detroit is the eighth LCS to be delivered to the Navy and the fourth Freedom-variant to join the fleet.



Figure 4 | The USS Detroit (LCS 7) conducts acceptance trials. U.S. Navy photo courtesy of Lockheed Martin/Michael Rote.

Demand rising for military simulation and training tech, virtual-reality tools, and head-worn displays

By John McHale, Editorial Director



Rockwell Collins provides the front-to-back training system for the Northrop Grumman E-2D Advanced Hawkeye aircraft. Photo courtesy of Rockwell Collins.

Cuts to the U.S. Department of Defense (DoD) budget over the last few years have created more demand for innovative simulation and training systems for military personnel; these systems range from flight crews to radar technicians to maintenance teams across all services. In this Q&A with LeAnn Ridgeway, Vice President and General Manager of Simulation and Training Solutions for Rockwell Collins, she discusses this trend and shares her outlook for the market in the long term, examines how the industry and the government is leveraging open architectures for simulation and training, and details innovations such as virtual-reality systems that enable the military to train not only on how they fight but also carry the training scenarios with them. Edited excerpts follow.

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

RIDGEWAY: We provide a unique function within Rockwell Collins as we are one of the few business units that serves the company's commercial and government-systems businesses. My role is Vice President and General Manager for the Rockwell Collins Simulation and Training Solutions business, headquartered in Sterling, Virginia. We provide the full spectrum of simulation and training for military and commercial customers. The solutions consist of visual products to complete training systems for aircrew and maintenance training.

MIL-EMBEDDED: Most of this decade has been about Department of Defense (DoD) budget cuts, which often push toward more reliance on training, especially simulated training, as it is overall less expensive. Has that been the case and do you see the investment from the DoD growing over the next five to ten years for simulation and training systems?

RIDGEWAY: We did a whole study on this where we enlisted the Government Business Council to help us survey top-level DoD folks on short-term and long-term procurement trends for military simulation and training. We wanted fact-based data to ensure we are spot-on with our investment and planning. Leaders surveyed in the DoD – the Pentagon and the armed services – confirmed that the DoD's investment in simulation and training technology will continue to grow. We've seen solid growth year over year and are forecasting mid- to reasonably high single-digit growth over the next few years. We are seeing the DoD put money where they've said they were going to for quite some time.

Like the U.S., other ministries of defense (MoDs) around the globe are laying out similar multiyear plans and all have stated goals and plans to reduce the amount of live



training they are doing to save operating dollars and constrain resources. Either they don't have enough assets to train against and have to go to a simulation and training scenario, or they have new platforms such as the F-35 program that can only use simulation and training scenarios to prove out the most advanced technical capabilities.

MIL-EMBEDDED: *Budget cuts also are known to drive more commonality in systems so they can work across multiple platforms, much like the Future Airborne Capability Environment (FACE) standard enables interoperability for avionics applications. Is that happening in simulation and training systems as well?*

RIDGEWAY: We have the same philosophy as our colleagues in avionics at Rockwell Collins and use an open architecture for our simulation and training systems, called CoreSim. It is an open standard commercial off-the-shelf (COTS)-based architecture that we developed about eight years ago as we

saw open architectures as the future not just in simulation and training, but in manned avionics systems as well. Open architectures – much like the avionics community when the FACE standard was first announced – are still more of an aspiration in the military simulation and training community. Everybody wants it and is talking about it, especially for large-scale virtual-training scenarios.

OPEN ARCHITECTURES – MUCH LIKE THE AVIONICS COMMUNITY WHEN THE FACE STANDARD WAS FIRST ANNOUNCED – ARE STILL MORE OF AN ASPIRATION IN THE MILITARY SIMULATION AND TRAINING COMMUNITY. EVERYBODY WANTS IT AND IS TALKING ABOUT IT, ESPECIALLY FOR LARGE-SCALE VIRTUAL-TRAINING SCENARIOS.

The technology is here, as is the plug-and-play capability to make it happen, but it won't appear for a while yet as the different armed services are still a bit like silos when it comes to procedures and legacy equipment. There are three primary standards in the military simulation community – Distributed Interactive Simulations (DIS), High Level Architecture (HLA), and the Test and Training Enabling Architecture (TENA). Getting to one isn't going to happen soon, as there is too much current fielded equipment in play with too many current training scenarios based on them.

However, we have worked with the Navy to demonstrate a common network or layer above the simulation to finally put to bed the fact people don't have to get rid of current fielded tech, because the Navy had multiple vendors plug-and-playing in this live virtual constructive (LVC) scenario (Figure 1). Every vendor could participate thanks to common APIs. The Air Force has also independently released a simulated common architecture standard that is factoring in cybersecurity needs. Right after that announcement the Navy announced it is doing the same thing. The Army has been successfully running a Synthetic Training Environment (STE) that enables modular, open-source, and open-system architectures.



Figure 1 | The Live, Virtual and Constructive (LVC) environment provides interoperability under critical conditions so warfighters on the ground, in the air, and at sea can all train simultaneously, no matter where they are. Image courtesy Rockwell Collins.

MIL-EMBEDDED: *What are your DoD customers looking for in avionics simulations systems? Sensors simulation? Radar?*

RIDGEWAY: They are looking for cloud-based solutions in addition to better realism and looking to train the way they fight. They also want to have more LVC, like we just talked about, and want to reuse current equipment. We've demonstrated a few with the services and did another demonstration in August at our facility. They want to be able to fly and drive ground assets such as dismounted soldiers, trucks, or light aircraft with live pieces interacting, and then throw fictional red forces at the trainees, creating what are almost war-gaming scenarios. For such an operation, training systems and participants are integrated in from multiple locations with live forces and all these independent entities are leveraging the same database, like a map of Afghanistan. This is what the DoD leadership wants and is driving toward – linking that many people together, keeping a database correlated with sensors, then have everything from the avionics to the sensors correlated and viewed out the window – and all in real time.

THIS IS WHAT THE DoD LEADERSHIP WANTS AND IS
DRIVING TOWARD – LINKING THAT MANY PEOPLE TOGETHER,
KEEPING A DATABASE CORRELATED WITH SENSORS, THEN HAVE
EVERYTHING FROM THE AVIONICS TO THE SENSORS CORRELATED
AND VIEWED OUT THE WINDOW – AND ALL IN REAL TIME.

MIL-EMBEDDED: *Please provide an example or two of current simulation and training programs Rockwell Collins is involved with.*

RIDGEWAY: A cornerstone program for us is providing simulation and training for the E2D Advanced Hawkeye's aircrew and maintainer sides. We've been supporting this program for a few years and were recently selected as the sole source for the Hawkeye Integrated Training System (HITS) 3 award. We have paired up with the prime on the aircraft, Northrop Grumman, to provide a comprehensive training system from classroom to computer from the back-end systems to the front-end crewmembers as well as the maintainers. We provide the back-end trainers for tactics, sensor analysis, etc. as well as the flight trainer curriculum courseware, electronic mission debrief, etc.

We are just now implementing a system-integration laboratory (SIL) for software development with Northrop Grumman and taking a live virtual demo from the SIL to the trainers for an LVC training event with the Navy. This work is also proliferating internationally, as we recently won the contract to provide the simulation and training systems for France's E2D upgrade.

Another important program for us is the F-35 Joint Strike Fighter, where we are a subcontractor providing the F-35 pilot's visual system to Lockheed Martin. It centers around the helmet-worn display, but comprises 360-degree field-of-view dome solutions and image generators, projectors, and databases. F-35 pilots are now integrating the new Gen III helmets with a new level of complexity into simulation training scenarios; this is the same helmet they will use in the aircraft.

MIL-EMBEDDED: *Much realism in today's military simulation is said to have come from the commercial gaming community. Do you still leverage commercial-technology COTS equipment or is there still a significant amount of custom work in military simulation systems?*

RIDGEWAY: There is a limitation on what games can do. They are very good in applications such as first-person shooter or dismounted soldiers, and other applications that really don't need moving models, large areas, and complex sensors. If you play a first-person shooter game you may see really detailed scenarios with great clarity, especially with geographically small locations. But in advanced flight scenarios you need high-level computational and texture memory performance. COTS-based gaming components and commercial graphics cards cannot handle that performance requirement. Our image generators use as much COTS as possible, but often when we are looking at graphic cards and FPGAs (field-programmable gate arrays) for these complex scenarios we do custom designs to meet the training requirement and real-time computation. They require flying a jet through extreme weather and full battle conditions, which is a leap that cannot be made by commercial gaming technology at this time.

We are taking the best of both worlds, however, and are partnered with the University of Utah, one of the top gaming universities in the country, and working with students and professors to take the innovation they doing in the gaming world and leverage it for complex defense and aerospace simulation systems.

MIL-EMBEDDED: *How do you manage obsolescence when leveraging COTS? Any lessons learned you can share?*

RIDGEWAY: We use multiple layers of obsolescence prediction. The nice thing about moving into the simulation and training business from a previous role at Rockwell Collins, which focused on obsolescence management, is that we easily brought that process to simulation and training. We work with the component applications engineer and use our system for tracking obsolete parts, as one would expect, but using our own FPGAs also gives us control over the component's life cycle, which we wouldn't get from a commercial chip, where we would be held hostage to the PC and gaming world. In other areas

where we use standard COTS graphics cards and motherboards, we work with manufacturers to create a technology baseline and coincide it with new development. This allows us to change out components every 18 to 24 months if need be and work as best as we can to be backward-compatible. Customers will not have to change out all their top-level equipment, such as getting a new image generator. We use this process to sustain products in the field for as long as 15 to 20 years.

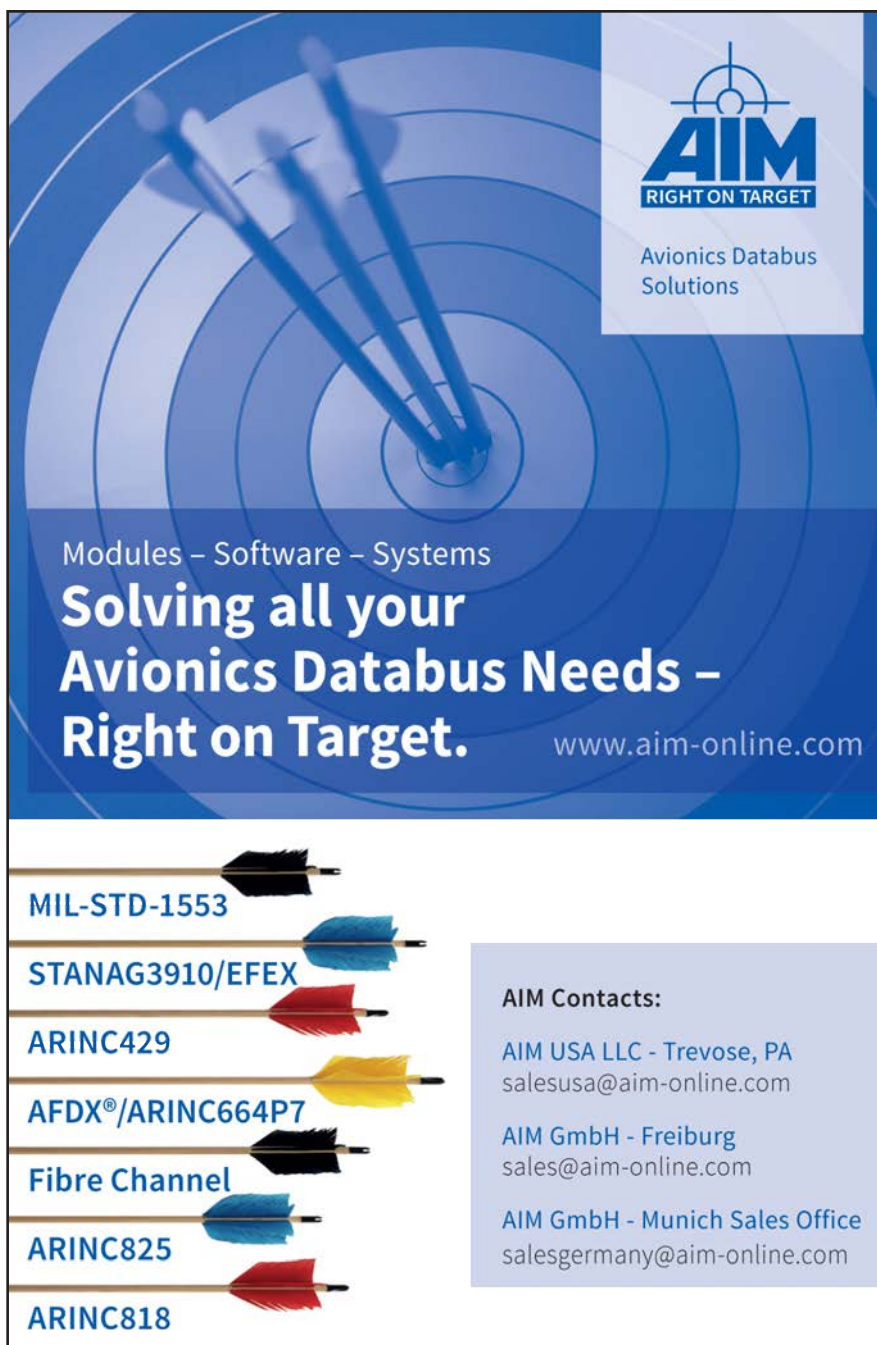
MIL-EMBEDDED: *How are reduced size, weight, and power (SWaP) requirements impacting simulation designs? Have advances in SWaP enabled more portable training solutions, for instance?*

RIDGEWAY: It has for sure. SWaP is important for reducing the cost and being able to provide persistent training and we continue to see an appetite for smaller, lighter, faster technology. There is a huge emphasis on extending battery life and reducing the heat generated in modern computing systems. There are great products in avionics and man-wearable applications that we would like to be able to port into the simulation and training arena. For example, the U.S. Navy is bringing training systems onto aircraft carriers for not only navigation and sensors, but for every area the ship, even maintenance of the engine room. These simulators are no longer huge, basketball-court sized displays, but often handheld or head-worn systems.

Modern transportable simulators are even more powerful than laptop computers, with everything moving toward head-worn applications and virtual reality training. Technology today takes that 11-foot display wall down to a close-to-your-eye visual in a head-worn system. These trends are revolutionizing simulated training. Wearable-type solutions allow the trainee to essentially train anywhere. The reduction in hardware from reduced SWaP requirements fuels the development of portable training and also, indirectly, cloud-based training.

MIL-EMBEDDED: *Many recruiters in the defense industry find it hard to attract engineering talent away from the commercial tech giants such as Google and Facebook. Is that the case for simulation and training as well, or does its similarity to the commercial gaming world negate that trend?*

RIDGEWAY: We have not had any problem. It surprised us when all of our engineering interns chose – once they finished their internship – to come work with us. Many were attracted because, as opposed to the commercial gaming industry, what we develop for the military and aerospace world is real stuff and real life. We've been blessed to have just about 100 percent of our college interns graduate and come to work with us. It even surprised me. I imagine it does help that many are working in our Salt Lake City image generation database facility, which is right across the street from their school, the University of Utah.



AIM
RIGHT ON TARGET

Avionics Databus Solutions

Modules – Software – Systems

Solving all your Avionics Databus Needs – Right on Target.

www.aim-online.com

- MIL-STD-1553
- STANAG3910/EFEX
- ARINC429
- AFDX®/ARINC664P7
- Fibre Channel
- ARINC825
- ARINC818

AIM Contacts:

AIM USA LLC - Trevose, PA
salesusa@aim-online.com

AIM GmbH - Freiburg
sales@aim-online.com

AIM GmbH - Munich Sales Office
salesgermany@aim-online.com

MIL-EMBEDDED: *Looking forward, what disruptive technology/innovation will be a game changer in the simulation and training world? Predict the future.*

RIDGEWAY: The single biggest thing in the near term is going to be head-worn applications. When you think about the advances in near-eye display technology, such as Oculus from Facebook, they're revolutionary for human interactive training and at the same time provide unparalleled situational awareness to

the warfighter. When you look at the combination of near-eye displays and the expansion of cloud-base streaming pipeline, you see a door opening to mixed virtual-reality training.

The technology is here, but it still has challenges such as inefficient resolutions, narrow fields of view, and limited bandwidth. All of this will need to improve before it can be leveraged in real-time military-training simulation environments. The industry is moving to solve

these challenges and will, but I have one caution: While this blend of technology will be huge with what it enables us to do with adaptive and distributed training, we will see so much technology coming out so fast and changing so rapidly that knowing what to adopt and where to put funding will be very confusing. It could also be detrimental to mission effectiveness if the new technology is not tested as to training outcomes first.

Another big trend I see starting is more use of scientifically-based biometrics around equipment training that will enable head-mounted systems with the same level of efficiency as end users get from traditional live or simulated training. We are spending a lot of time and research at Rockwell Collins on these developments to make sure we put our funding where the training objectives will be and with the latest technology hitting the market. The commercial world pours billions into developing technology such as Oculus and making sure people don't get simulation sickness and overcoming other human factor challenges, while in the military simulation and training world, we write the applications to adapt that low-cost technology for mission-critical training. **MES**

As vice president and general manager of Simulation and Training Solutions for Rockwell Collins, **LeAnn Ridgeway** is responsible for areas including technical publications, rehosted avionics, computer and desktop training, device training, and visual systems. Previously, she was vice president and managing director, Americas for Rockwell Collins; served as senior director, Engineering Services for Rockwell Collins; and led the company's Integrated Logistics Support Organization. LeAnn earned her bachelor's degree in business and economics from Mt. Mercy College and her MBA from St. Ambrose University. She is currently a member of the National Training and Simulation Association, belongs to the National Defense Industrial Association, is a member of Women in Defense (D.C. Chapter), and is the Enterprise Chair for the Women's Forum at Rockwell Collins.



**The industry's
most trusted
and widely used
USB interfaces**

Portable Avionics Databus Interfaces

A reliable USB interface from Astronics Ballard Technology does it all – databus test, analysis and simulation. Use it in the lab or in the field – it's fully powered by a single USB port. Simply connect it to any available laptop, desktop or tablet PC and it's ready to go. Add our CoPilot® interactive software for a complete easy-to-use solution.

NEW models with multiple protocols mean the best is now even better!

www.ballardtech.com/USB

or call 425-339-0281

AS9100/ISO 9001 Registered

- MIL-STD-1553, EBR 1553
- ARINC 429, 708, 717
- Serial, Discrete

Get the best solution –
all the protocols and channels
you need in a single device



ASTRONICS
BALLARD TECHNOLOGY



Embedded Solutions for the next 25 years

Acromag Redefines SWaP-C with our New AcroPack® I/O Platform

The AcroPack® product line updates our popular Industry Pack I/O modules by using the mPCIe interface format. We added 19mm and a 100 pin connector to provide up to 50 isolated rear I/O signals, giving you a tremendous amount of capability on an **Extremely Small Footprint - Without Cabling!**

Designed for COTS applications, these general purpose I/O modules deliver high-speed and high-resolution A/D and D/A, digital I/O, serial communication, and re-configurable FPGA functions. Whether it's server-based lab activities, flight or ship-based test systems, if you are looking for that ever-shrinking form factor of I/O that allows you to get one step ahead, contact Acromag to discuss how AcroPacks can help you with tomorrow's applications, today.

Key Features Include:

- A/D, D/A, serial, digital I/O and FPGA
- Low-power consumption
- Solid-state electronics
- -40 to 85°C standard operating temperature
- Conduction cooled models available
- Mix and match endless I/O combinations in a single slot by using our VPX or PCIe-based carriers

Size = 70mm x 30mm

Weight = .05 oz. avg

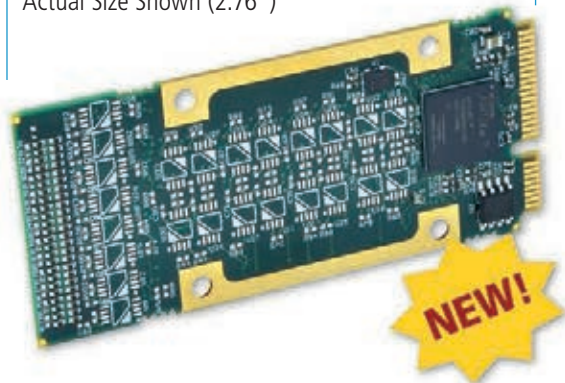
and

Power = <5 watts per module

-

Cost = Starting at \$395

Actual Size Shown (2.76")



Embedded I/O Solutions



FPGA Modules
Acromag.com/FPGAs



I/O Modules
Acromag.com/EmbeddedIO



VME SBCs
Acromag.com/Boards



SFF Embedded Computers
Acromag.com/ARCX

Visit Acromag.com/AcroPacks
TO LEARN MORE

Discrete vs distributed: Transforming military training and simulation systems

By Mike Pape



PEO STRI's design for realistic training operations breaks out into three primary elements: the training environment where the soldiers train, training management and assessment processes that build and maintain training readiness, and training infrastructure that incorporates facilities and network services that make it all work. Image courtesy U.S. Army.

Advances such as augmented reality and virtual reality (AR/VR) are redefining expectations of quality and performance in increasingly diverse military training scenarios. These improvements also demonstrate the need for a philosophical change in system design strategy as system engineers prepare for the next generation of "training as a service." Developers must move away from discrete systems and toward more distributed training environments that are capable of delivering point-of-need training via a single synthetic training environment.

The U.S. Army's Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) has called for industry support in defining "leap ahead and disruptive" technologies that will enable the Synthetic Training Environment (STE). The office wants guidelines for the technologies to create impact now and poise itself for continued evolution over the next several decades. The goal of the STE is to deliver training as a service, using connected technologies to more effectively reach the point of need. According to the PEO STRI, training applications must be modular, composable, scalable, and service-oriented, with a focus on automation to reduce tech support. To respond competitively, designers must offer increasingly agile solutions for customized training on demand, while reducing intrinsic reliance on individual hardware components. This is no easy transition, and requires

new thinking that embraces incremental system efficiencies where they offer performance and value.

To move incrementally toward a distributed environment, elements such as storage, compute processing, image rendering, display, and network architectures should be considered as building blocks (Figure 1). These building blocks must be critically evaluated against needs for mobility, content delivery, and security, in order to align a design vision with the new realities of distributed training. An incremental approach has significant value in this effort – demonstrated here by distributed options for storage and image rendering, and their impact on mobile training applications.

Driving change with distributed storage

Shifting from discrete to distributed storage demands a fundamental change in design philosophy, considering the role of storage as a content hub for live, virtual, constructive (LVC) training rather than as a piece of hardware (Figure 2). This view not only establishes a more global outlook for training systems, but it also ensures that developers have the ability to more easily adapt over the next several years of simulation development. Speed and scalability are central to this shift, addressing integration, interoperability, and composability as the three primary pillars of LVC. The key for designers is to create a foundation capable of supporting these requirements across the spectrum of training, from desktop or instructor-led training all the way up to immersive, full-mission simulation.

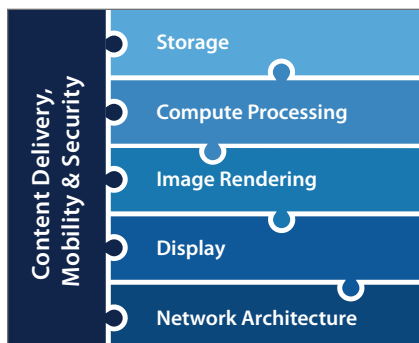


Figure 1 | Elements such as storage, compute processing, image rendering, display, and network architectures should be considered as building blocks and must be critically evaluated against needs for mobility, content delivery, and security. Graphic courtesy Distributed Computing.

Software-defined storage is one way to deliver this value, as it eliminates the focus on underlying hardware and instead allows designers to focus on adaptable, workload-optimized performance. In the software-defined model, storage systems are virtualized, pooled, aggregated, and delivered to users as a software service; this model offers longer life cycle and lowers operating expense and total cost of ownership over time.

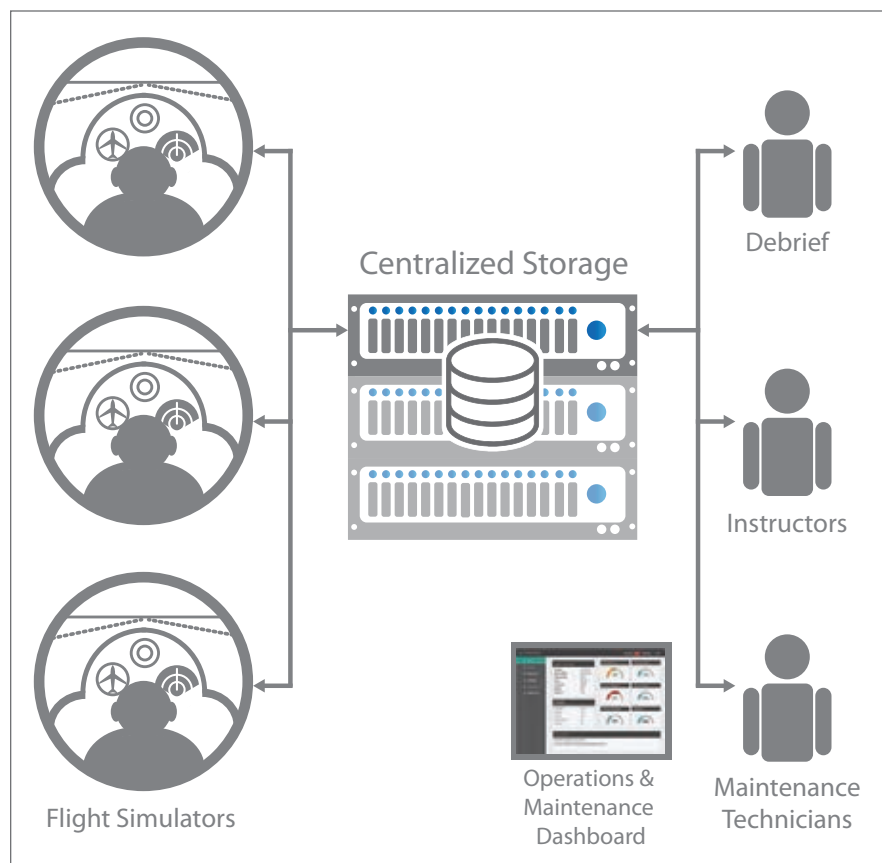


Figure 2 | Distributed designs are capable of connecting more simulation devices to a single, centralized database without slowing the system down, even while scaling to accommodate varying requirements for multiple users. Graphic courtesy Distributed Computing.

Designers using the software-defined model are able to factor in a flexible range of on-demand performance requirements, tailoring distributed solutions based on various network or connected architectures. Adaptability becomes inherent, adding critical value to military training initiatives as the number of displays, array of simulators, and types of data needs change over time.

Redefining compute and rendering

These changing needs necessitate a case-by-case evaluation – managing displays, considering the types of images to be rendered, and recognizing where distributed environments can be used in the future, whether or not they apply today. Solutions must be tailored from both a compute and storage perspective, pertaining specifically to the type of content and its delivery method. This model considers rendering as just one of many types of content, and provides the opportunity to create a flexible, scalable, and reusable structure that enables distributed content delivery.

A multitiered building block approach is required, one that breaks down the distributed network-training infrastructure into various layers, including network execution modeling, decisions, and higher-level collaboration. For example, the end goal may be to create a “rendering farm,” or centralized rendering capacity that can be used at any given time by any given client. Significant architecture changes must take place in the subsystems to support this vision: One subsystem may be the rendering farm itself, while another is the software architecture-enabling specific data to be pulled client by client.

A relatively minor change to software architecture could be an interim step, enabling image rendering to move out of the big box assembly and operate closer to the

display. Such a step is a move away from the “Big Iron” focus on systems – technology can be reused more easily as applications and their performance requirements evolve, and costs related to transmitting rendered images over long distances are reduced. Ultimately, resources are then freed to focus on the rendering farm in the next incremental step, demonstrating a multitiered approach that progresses toward a more centralized distributed environment.

Distributed impact on mobile training and simulation

At first glance, centralized mobility seems to be an oxymoron, in that centralized systems are located in one place and therefore not mobile. However, building blocks such as centralized storage and image rendering actually help create mobility for the user and in the development of training itself. System performance does not require data from multiple locations and users can instead access point-of-need training from a single source; training instructors can access the same centralized infrastructure to make application changes and improvements in real time.

Centralized technology is the driving factor for mobile systems to capitalize more fully on AR/VR applications, which currently exist but are limited by discrete systems (Figure 3). Distributed systems can add new value by enabling point-of-need training that is more immersive for users in multiple locations, such as full mission simulators capable of blending virtual reality with synthetic environments.

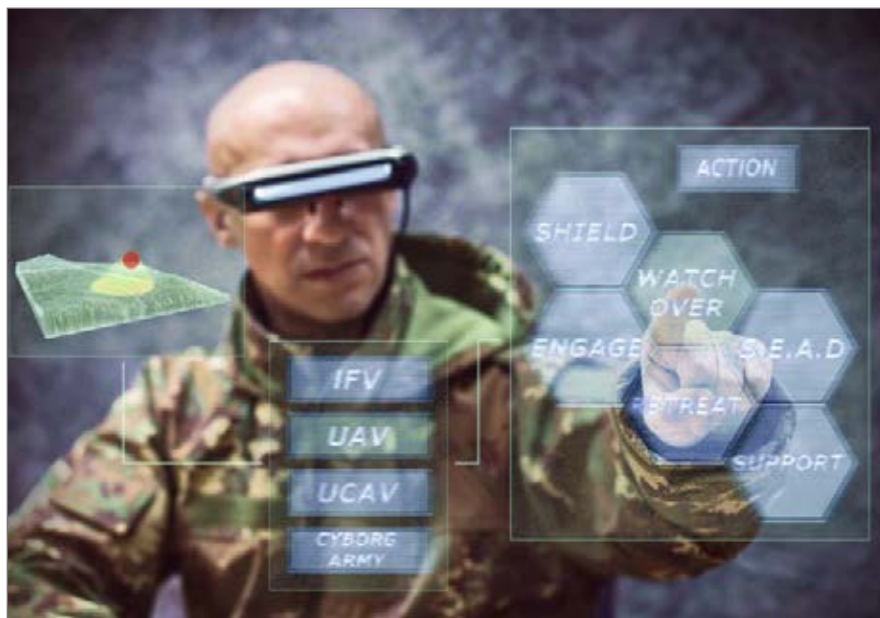


Figure 3 | Mobility is one more layer of reality in terms of how the simulation system feels and acts for the trainee, more closely mirroring a real-life operational environment. Trainers benefit as well, gaining a greater level of global access to resources and users through a mobility infrastructure. Image courtesy Distributed Computing.

Augmented reality may hold even greater potential from a mobile perspective, enabling fully networked, architected systems that train users via an actual real-world device. Instead of investing in training a soldier to handle aircraft inspections supported by procedural manuals or other types of instruction materials, the experience is redefined using system data from flight logs, checklists, or electronic flight bags. Coupled with a head-mounted display (HMD), the trainee executes the aircraft training protocol, and is supported by data such as the last time the aircraft was serviced, schematics, and step-by-step instructions on how to perform a specific service. Military programs can capitalize on the same distributed platform for soldiers training off-site, working in the field, engaged in battle, or handling routine maintenance of equipment and systems.

New security perspectives meet PEO STRI mandates

The PM ITE (PEO STRI's Project Manager Integrated Training Environment) states that its focus today is to “provide capability to train a BCT (Brigade Combat Team) for Decision Action at a home station, with combat multipliers in a doctrinal area of operation.” A strategic priority is to converge virtual, constructive, and gaming products into a single organizational structure, blending capabilities for maximum value in live training scenarios. At the same time, legacy systems must transition to future technologies; replicate the realism, stress, and uncertainty of operational environments; maintain partner interoperability; and enable collective training at the point of need.

To meet these mandates across the spectrum of military training and simulation applications, designers are working to create more accessible training capabilities in which joint intergovernment or interagency partners can train together in a more unified way. Public, private, or hybrid cloud specifics thus become irrelevant, and engineers and users do not need to rely on established “Big Iron” clouds. Deployments depend entirely on how effectively connected solutions can support and streamline a particular training application, including its security requirements.

Security is a key challenge here: Systems benefit from the multitiered approach, as security needs are likely to change faster than any other system element. How to architect a distributed or centralized infrastructure in such a way that it is not only secure, but also has the ability to address new security risks as they arise? One idea: Multiple clouds can be implemented, either within the building or operated externally, creating an inherent security and management advantage that does not currently exist with a “storage everywhere” approach.

This type of design creates multiple tiers with different security levels at each tier – essentially a system of systems, with subsystems in different locations or defined by software architecture as their distribution model demands. While software-defined architectures do not automatically make the solution more secure, they do represent an incremental step in changing the way the industry needs to think about security and overall training architectures.

DISTRIBUTED SOLUTIONS – ILLUSTRATED BY IDEAS
LIKE SOFTWARE-DEFINED STORAGE AND NEW ARCHITECTURES
FOR IMAGE RENDERING – ALSO ENSURE PERFORMANCE
BEYOND A HARDWARE-BASED LIFE CYCLE.

Distributed training and simulation moving forward

Mandated by PEO STRI, the training and simulation industry is moving toward solving the same old problem of how to enable interoperability and connectivity to effectively improve end-user proficiency in complex, evolving training scenarios. Current thinking forces designers to “back into” solutions, working around limitations instead of looking forward to where both the industry and military-training demands are heading.

Instead, by taking incremental steps using a building-block approach, the simulation and training industry can achieve its long-term goals of reducing footprint and operational costs. Distributed solutions – illustrated by ideas like software-defined storage and new architectures for image rendering – also ensure performance beyond a hardware-based life cycle. This approach can have a tangible benefit for the military-procurement community, as the application’s life cycle is solely determined by how long it is needed.

Establishing new ways of presenting information – flexible, scalable, and repeatable for long-term deployment and technology evolution – enables trainers to zero in on how to manage change without changing entire infrastructures. It’s a break from

hardware limitations, a move toward training as a service, and another major transformation for global military forces preparing for increasingly diverse threats and missions. **MES**



Mike Pape is director of training and simulation solutions, Dedicated Computing. The company’s training and simulation

solutions combine hardware, software, and services in the pursuit of advancing the skills of the warfighter. He earned an MS in management from Cardinal Stritch University and a BS in electrical and computer engineering and mathematics from Marquette University. Readers may contact Mike at mike.pape@dedicatedcomputing.com.

Dedicated Computing
www.dedicatedcomputing.com

Rugged Chassis, Backplanes, and Integrated Systems Engineered for Your Application

Standards-based and Highly Customizable

Whether you have a back-of-the-envelope design idea and seek collaborative development with our engineering team, or provide us with a complete set of build specifications, LCR Embedded Systems will turn your product into reality.



LCR™
EMBEDDED
SYSTEMS, INC.

VPX • AdvancedTCA • VME • CompactPCI • Custom
(800) 747-5972 • sales@lcrembedded.com • www.lcrembeddedsystems.com

RF transceivers provide breakthrough SWaP solutions for defense and aerospace applications

By Wyatt Taylor and David Brown

Integrating more software control and cognitive abilities to military radios demands a more frequency- and bandwidth-flexible radio frequency (RF) design. To achieve this goal, static filters need to be removed and replaced with tunable filters. Similarly, the concept of a common platform would allow for shorter development times, reduced manufacturing costs, and provide greater interoperability between systems. The common platform demands that the RF system be capable of providing full performance for applications that traditionally have had very different architectures. Future radio platforms are pushing size and power demands to a new extreme.

Since its inception, the super-heterodyne architecture has been the backbone of radio design for defense and aerospace systems. Whether it is a handheld soldier radio, unmanned aerial vehicle (UAV) data link, or a signal intelligence (SIGINT) receiver, the single- or two-mixing-stage super-heterodyne architecture is the common choice. The benefits of this design are clear: proper frequency planning can enable very low spurious emissions, channel bandwidth and selectivity is set by the intermediate frequency (IF) filters, and the gain distribution across the stages allows for a tradeoff between optimizing noise figure and linearity. (Figure 1.)

During more than nearly one hundred years of use, the super-het architecture has seen significant gains in performance across the entire signal chain. Microwave and RF devices have improved their performance while decreasing power consumption. Analog-to-digital converters (ADCs) and digital-to-analog converters (DACs) have increased sample rate, linearity, and effective number of bits (ENOB). More performance gains: Processing capability in field-programmable gate arrays (FPGAs) and digital signal processors (DSPs) has followed Moore's Law and increased with time, allowing for more efficient algorithms, digital correction, and further integration.

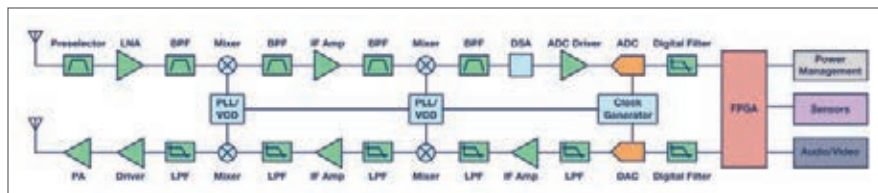


Figure 1 | Basic super-heterodyne architecture

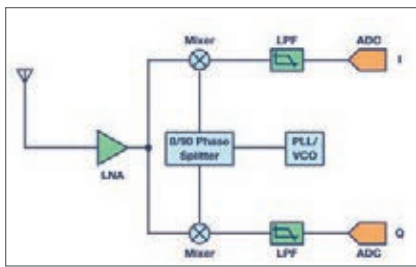


Figure 2 | Zero-IF architecture.

Additionally, strides made in packaging technology have shrunk device pin density while simultaneously improving thermal handling.

However, these device-specific improvements are beginning to reach the point of diminishing returns. While the RF components have followed a reduced size, weight, and power (SWaP) trend, high-performance filters remain physically large and are often custom designs, thus adding to overall system cost. Additionally, the intermediate-frequency (IF) filters set the analog channel bandwidth of the platform, making it difficult to create a common platform design that can be reused across a wide range of systems. For package technology, most manufacturing lines will not go below a 0.65- or 0.8-mm ball pitch, meaning that there is a limit on how physically small a complex device with many input and output (I/O) requirements can become.

Zero-IF architecture

An alternative to the super-het architecture that has re-emerged as a potential solution in recent years is the Zero-IF (ZIF) architecture (Figure 2). A ZIF receiver uses a single frequency mixing stage with the local oscillator (LO) set directly to the frequency band of interest, translating the received signal down to baseband in-phase (I) and quadrature (Q) signals. This architecture alleviates the stringent filtering requirements of the super-het, since all analog filtering takes place at baseband, where filters are much easier to design and less expensive than custom RF/IF filters. The ADC and DAC are now operating on I/Q data at baseband, so the sample rate relative to the converted bandwidth can be reduced, saving significant power. From many design aspects, ZIF transceivers provide significant SWaP reduction as a result of reduced analog front-end complexity and component count.

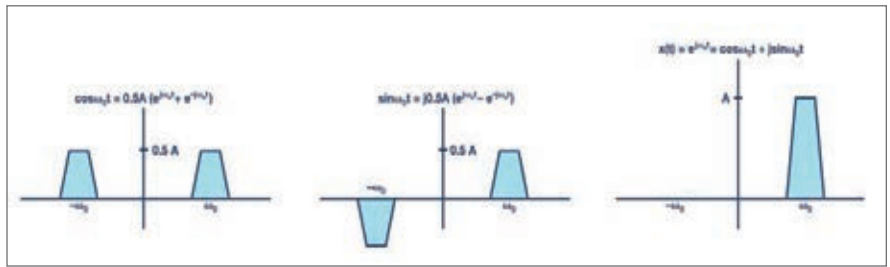


Figure 3 | Zero-IF image cancellation.

There are, however, some drawbacks to this system architecture that need to be addressed. The direct frequency conversion to baseband introduces a carrier-leakage and image-frequency component. Mathematically, the imaginary components of I and Q signals cancel out due to their orthogonality (Figure 3). Due to real-world factors such as process variation and temperature deltas in the signal chain, it is impossible

YOUR SOLUTION PROVIDER FOR...

CONNECTIVITY | POWER | CONTROL

STAY CONNECTED

Scalable, Multi-Protocol Connectivity
Compact Rugged Avionics Interface Computer

Scalable, Multi-Protocol Connectivity

- High Density Computing & Connectivity
- Intel® Atom Architecture
- Expanded Scalable Capabilities
- USB 3.0 Support

SWaP-C Optimized System

- Rugged Deployable Compact Enclosure
- Low Power Computing Performance
- MIL-STD-810G Shock, Vibration & Immersion / MIL-STD-461F EMI

Multi-Protocol Flexibility

- Ethernet, MIL-STD-1553, ARINC 429/717, CANbus 2.0/ARINC 825, RS-232/422/485 & Avionics/Digital Discrete I/O
- 3 modes (Remote Access, Protocol Conversion & Standalone)

Expandable: (2) Mini-PCIe sites & (1) I/O Expansion Module

52

YEARS OF SERVICE

To learn more, visit
www.ddc-web.com/AIC-CR/MES

DATA DEVICE CORPORATION

to maintain a perfect 90-degree phase offset between the I and Q signals, resulting in degraded image rejection. Additionally, imperfect LO isolation in the mixing stage introduces carrier leakage components. When left uncorrected, the image and carrier leakage can degrade a receiver's sensitivity and create undesirable spectral emissions.

Historically, the I/Q imbalance has limited the range of applications that were appropriate for the ZIF architecture. This was due to two reasons: First, a discrete implementation of the ZIF architecture will suffer from mismatches both in the monolithic devices and also the printed circuit board (PCB). In addition, the monolithic devices could pull from different fabrication lots, making exact matching very difficult due to native process variation. A discrete implementation will also have the processor physically separated from the RF components, making a quadrature correction algorithm very difficult to implement across frequency, temperature, and bandwidth.

Integrated transceivers provide SWaP solution

Integrating the ZIF architecture into a monolithic transceiver device provides the path forward for next-generation systems. By having the analog and RF signal chain on a single piece of silicon, process variation will be kept to a minimum. In addition, DSP blocks can be incorporated into the transceiver, removing the boundary between the quadrature calibration algorithm and the signal chain. This approach provides both unparalleled improvements in SWaP and can also match the super-het architecture for performance specifications.

Analog Devices offers two transceivers aimed at use in the defense and aerospace markets: the AD9361 and AD9371 (Figure 4). These devices integrate the RF, analog, and digital signal chain onto a single CMOS device and include digital processing to run quadrature and carrier leakage correction in real time across all process, frequency, and temperature variations. The AD9361 focuses on medium performance specifications and very low power, such as UAV data links,

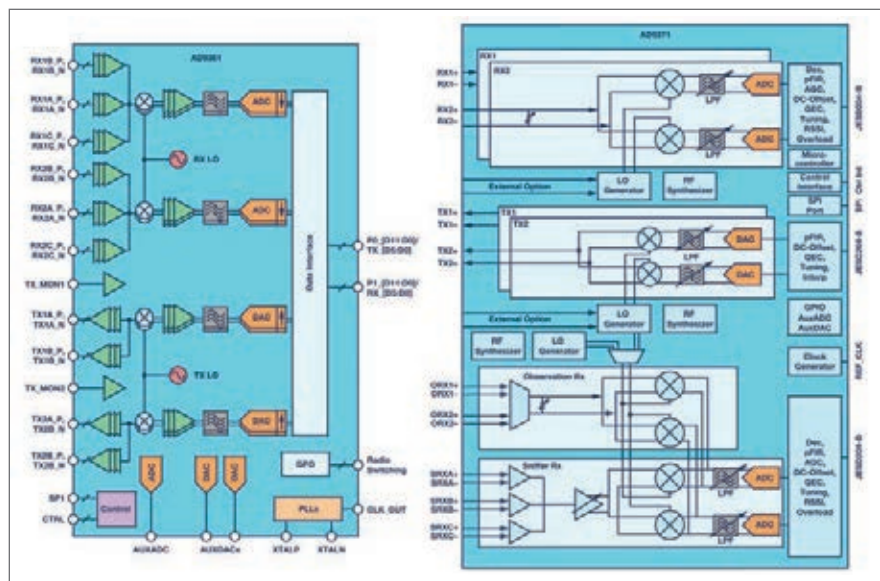
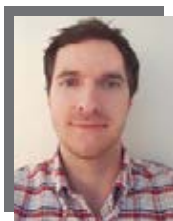


Figure 4 | AD9361 and AD9371 block diagrams.

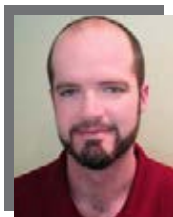
handheld and man-pack communication systems, and small-form-factor SIGINT. The AD9371, optimized for very high performance specifications and medium power, has an integrated ARM microprocessor for refined calibration control, as well as an observation receiver for power amplifier (PA) linearization and a sniffer receiver for white-space detection. These features mean that communication platforms using wideband waveforms, or occupying noncontiguous spectrum, can now be implemented in a much smaller form factor. The high dynamic range and wide bandwidth enables SIGINT, EW, and phased-array radar operation in locations with highly congested RF spectrum.

The next generation is now

One hundred years of device optimization had allowed the super-het to achieve greater and greater performance, in continually smaller and lower-power platforms. Those improvements are beginning to slow, as physical limitations become real. Next-generation aerospace and defense platforms will demand a new approach to RF design, one where several square inches of an existing platform is integrated into a single device. In these devices the boundary between software and hardware is blurred, allowing for greater optimization and integration and where decreased SWaP no longer means decreased performance. **MES**



David Brown is an RF system applications engineer with Analog Devices, Inc., in Greensboro, North Carolina. He joined Analog Devices in 2015 and focuses primarily on defense and aerospace applications. David graduated from NC State University in 2014 with a bachelor's degree in electrical engineering.



Wyatt Taylor is a senior RF systems engineer with Analog Devices, Inc., in Greensboro, North Carolina. He is focused on defense and aerospace radio applications, with a particular emphasis on integrated RF transceivers, small-form-factor microwave design, and software-defined radio (SDR). Formerly, Wyatt was an RF design engineer at Thales Communications Inc., and Digital Receiver Technology, Inc., in the Maryland area. Wyatt received his MSEE and BSEE from Virginia Tech.

Analog Devices, Inc. • www.analog.com

Innovation **That Protects.**

WHEN DATA PROTECTION IS MISSION CRITICAL, YOU CAN TRUST MERCURY'S SECURE SOLID STATE DRIVES (SSDs). OUR SSDs PROVIDE EXCEPTIONAL DATA-AT-REST PROTECTION AGAINST INTRUDERS, EVEN IN THE HARSHTEST ENVIRONMENTS. THESE RUGGED DRIVES ARE ENGINEERED AND MANUFACTURED IN OUR DMEA TRUSTED FACILITY AND OUR COMMITMENT TO LONG-TERM PRODUCT SUPPORT GUARD AGAINST OBSOLESCENCE RISK.



Key Features:

- Densities from 32GB to 1TB
- Multiple form-factors from onboard BGA's to 2.5" removable platforms
- AES 256 XTS encryption
- Multiple key management modes
- High-speed purge, clear and sanitization validation
- Meets all DoD military purge protocols
- Customizable security features and packaging options



INNOVATION THAT MATTERS™



Visit mrcy.com/SSD to learn more.

Software-defined radio: To infinity and beyond

By Manuel Uhm

It's hard to believe that the term "software-defined radio" (SDR) has been around for approximately 30 years. That's a long time in the technology world, but SDR is still a common topic of discussion and carries more than its share of misconceptions. The definition of SDR – per the Wireless Innovation Forum (formerly the SDR Forum) – is "a radio in which some or all of the physical-layer functions are software-defined." The term is really focused on the physical (PHY) layer processing of the waveform, and not related to the radio-frequency (RF) front end, which is a common misconception. Radios with wideband tunable RF front ends capable of dynamic spectrum access are referred to as cognitive radio (CR). A cognitive radio is defined as a radio in which communication systems are aware of their internal state and environment, such as location and utilization on RF frequency spectrum at that location.

After so many years, SDR is now such a dominant industry – standard implementation for radios, from military tactical radios to cellular handsets – that it's almost a given that a radio is an SDR. There will continue to be innovations in semiconductor and software technology that will continue to drive to higher development productivity and more cost effective SDRs, so there really is no end in sight for SDRs. These factors mean that SDR is really a solved problem and radios are now becoming frequency-agile and evolving to be CRs.

SDR evolves to become the de facto industry standard

A demonstration that SDR is a de facto industry standard is shown in Figure 1. Closest to the center, the dark blue section

is representative of the first set of markets to move from hardware radio architectures to SDR architectures, regardless of whether they used the term SDR or not. These markets include signals intelligence (SIGINT), electronic warfare, test and measurement, public-safety communications, spectrum monitoring, and military communications (MILCOM). Some of these markets were using hardwired application-specific integrated circuits (ASICs), while some were already using programmable digital signal processors (DSPs.)

The technology drivers that really drove the move to SDR in these markets were the advent of RFICs from companies like Analog Devices and cost-effective DSP-intensive FPGAs from

THE OBVIOUS QUESTION:

WHAT'S NEXT FOR SDR AND CR?

companies like Xilinx. These two technology drivers all came together to meet a multibillion dollar need in the military tactical radio market, creating something of a "market ripple," where the market had a huge impact on the evolution of SDR technology far beyond just the MILCOM market. The JTRS [Joint Tactical Radio System] program funded the development and productization of both SDR and CR technology for military radios, which created a strong ecosystem of vendors including semiconductor, tools, and software companies. On the tools front, SDR required waveforms to be as portable as possible between different hardware platforms, which resulted in tools like the SCA [Software Communications Architecture] Core Framework, as well as better programming tools from electronic design automation (EDA) and semiconductor companies.

The advancement of RFICs, field-programmable gate arrays (FPGAs), and EDA tools were significant factors in enabling the second generation of SDRs being driven by 4G LTE infrastructure. Virtually all LTE eNBs (eNodeB or basestation) were developed with RFICs and FPGAs. Some of the larger

infrastructure vendors would eventually go to ASICs, but even then, the baseband ASICs were largely programmable, as they used processors coupled to hardened blocks called hardware accelerators for compute-intensive functions such as turbo decoding that would typically exceed the performance or power limitations of the processors.

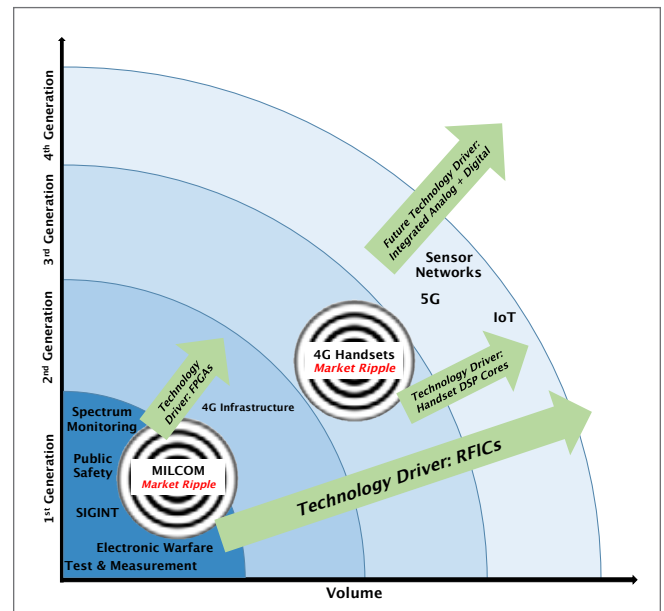


Figure 1 | How successive generations of SDRs have come to dominate the radio industry and will continue to evolve.

Leading the way in RF excellence.

Introducing the SI-9173/CC Vesper Multi-Channel VHF/UHF Tuner and Exciter.

Vesper is a breakthrough in high-performance RF technology and dense channel packaging. In a single-slot 6U VPX form factor, Vesper contains up to ten, 100 MHz RF channels. Vesper's performance, density, scalability and open VPX technology greatly simplifies and extends current system implementation in SIGINT, ESM and EW operations. Learn more at drs.com/RF-Leader



drs.com/RF-Leader

DRS TECHNOLOGIES
a LEONARDO company

The next market ripple, shown in the third generation, occurred when 4G LTE handsets moved consistently to SDR architectures. This shift was enabled by low-power, high-performance DSP cores optimized for handsets offered by companies like Ceva, Tensilica, and Qualcomm. Similar to the baseband ASICs for infrastructure, these cores would be integrated into application-specific standard products (ASSPs) or ASICs for much of the PHY processing, coupled with hardware accelerators. Once this changeover occurred, SDRs increased orders of magnitude in volume and reach to become the de facto industry standard for radios.

The next generation of SDRs

The obvious question: What's next for SDR and CR? As high as the volumes of 4G handsets has propelled SDR, the prospects of 5G, the IoT (Internet of Things), and sensor networks promise to again increase the volume of SDRs by another order of magnitude. What will be the technology driver lifting SDR to these lofty heights? Given that the previous drivers were innovations in analog and digital technology, it follows that the next technology driver would be the combination of analog and digital on a single monolithic chip in order to reduce cost and SWaP (size, weight, and power). For infrastructure, this driver could be FPGAs with integrated analog-to-digital converters (ADCs) and digital-to-analog converters (DACs). For handsets and sensors, this could be application processors, also with integrated ADCs and DACs.



Figure 2 | Two super-heterodyne TwinRX daughtercards inside an Ettus USRP X310 SDR for four phase-aligned RX channels.

Don't forget software and tools, which is the whole point of SDR, after all. In order to enable the development of these chips, as well as the waveforms and application software running on them, there will be a requirement for better system-level tools that can be used to design and debug across the analog and digital domains, as well as program-heterogeneous processors on a single chip, including general-purpose processors (GPPs), DSPs, graphics processing units (GPUs), and/or FPGA fabric.

Breathing new life into old technology

With all this talk about the evolution of SDRs, it's interesting to note that technology becoming more cost-effective has been a major driver in the adoption of SDR technology, enabling SDR to reach previously inaccessible markets such as handsets. This trend is not expected to go away, as high-volume markets are generally very price-sensitive.

Ettus Research, a National Instruments company, offers a super-heterodyne two-channel receiver daughtercard (Figure 2) called TwinRX. All previous Ettus Research RF daughtercards were direct-conversion architectures, which demodulate an RF carrier directly to baseband. Furthermore, the RFICs in Figure 1 that were a key technology driver for SDR used direct conversion; by eliminating the IF (intermediate frequency) stage, direct-conversion receivers could be smaller and lower-cost. This benefit usually came at a penalty of RF performance, however, including nonlinearity and poorer dynamic range. For this reason, super-heterodyne architectures are still common for SIGINT and direction finding (DF), where an increased ability to detect, monitor, and capture a signal of interest is critical. **MES**



Manuel Uhm is the director of marketing at Ettus Research, a National Instruments company. Manuel has business responsibility for the Ettus USRP, NI USRP, and BEEcube portfolios. Manuel is also the chair of the Board of Directors of the Wireless Innovation Forum (formerly the SDR Forum). He has served on the Board since 2003 in various technical, marketing, and financial roles. Manuel can be reached at manuel.uhm@ettus.com.

Ettus Research, a National Instruments Company
www.ettus.com

AIRBORNE, SHIPBOARD, GROUND MOBILE DATA RECORDING AND DATA STORAGE



RPC 24

RUGGED
DEPLOYABLE

Magazine Based
High Performance
RAID Storage

- **24 Solid State or Hard Disk Drives**
- in only 2U of panel height
- **Two Quickly Removable Storage Magazines**
- each containing up to 12 HDDs or SSDs each
- **Fault Tolerant, Hot Swap Components**
- no single point of failure
- **Sustained Read and Write Data Transfer Rates**
- of over 6000 MB/sec and 5000 MB/sec respectively
- **MIL-STD-810G, MIL-STD-461E Certified**





INTERNATIONAL

www.phenxint.com 714-283-4800

Software-defined radio enables enhanced military communications

By Stephanie Chiao



Sgt. Kentrell Billups, a radio technician with 1st Air Naval Gunfire Liaison Company, tries to establish satellite communications with the division fire support cell during Exercise Maple Resolve 2015 aboard Canadian Manoeuvre Training Center, Camp Wainwright. Photo credit: Cpl. Owen Kimbrel/U.S. Marine Corps.

Software-defined radio (SDR) is not a new technology for the military, having been developed for defense communications. However, it has evolved beyond the Joint Tactical Radio System (JTRS) program, which is now obsolete. Although JTRS is no longer an active program, some variations of the system have survived, like the Rifleman Radio, MIDS J, and the HMS Manpack.

The military needs an enhanced communication system to enable collaboration, improve sharing of information, and facilitate shared situational analysis. Furthermore, the military needs a system that is able to engage in spectrum jamming and handle synchronized ground and airborne radio networks.

Software-defined radio ... defined

SDR is a wireless communication device in which the transmitter and receiver modulation/demodulation occurs in software. As a result, the functionality

is modified or changed by software alone, obviating the need to make any physical changes to the hardware. Further, it does not require the use of capacitors and resistors, as the software-based filtering algorithms can be utilized to select specific frequencies.

With SDR, the algorithms can be both downloaded and adapted over the life cycle of the hardware. SDR is also capable of incorporating new functionality enabling it to do much more than voice and data transmission.

As SDR technology evolved, it solved the problem of needing multiple devices to engage in military communication. As SDR is software-driven, functions like encoding/decoding and modulation/demodulation are no longer hardwired and can be modified by software. These features mean that users can adapt to changes in the environment by making changes to the software to perform tasks such as changing modulation schemes, frequencies, and migration.

SDR is also used to monitor communications on several different frequencies, including VHF, UHF, and HF. Several different protocols – such as CDMA, GSM, Bluetooth, WiFi, and LTE – can be operated at the same time while being combined with the ability to monitor a large portion of the spectrum while supporting these protocols. That being said, at the present time, military SDR is facing issues with phase coherency and latency of multiple input/multiple output (MIMO) systems.

Achieving true phase coherency

For any application requiring more than one radio chain (e.g., radar, beam-forming, 3GPP (LTE), other cellular environments, MIMO applications), there is a significant challenge in ensuring that there is a known phase coherency and time delay.

Attaining true phase coherency between several channels of RF signal acquisition requires all clock signals to be shared directly between each ADC and down-converter. However, synchronization becomes increasingly easier with simple downconversion architecture. (Figure 1.)

Systems that use single stage down-conversion or direct downconversion (zero-IF) engage fewer local oscillators (LO). Most of the time, the LO signals can be shared directly between down-converters. In many cases, LO signals can be shared directly between down-converters, making phase-coherent measurements possible.

Consider the following scenario that involves the synchronization of four receive chains set up as a direct conversion quadrature receiver. The LO can be derived from an on-board oven-controlled crystal oscillator (OCXO), or it can be accepted from an external source. In the case of the latter, a common LO can also be shared between two or more separate units. Further, the OCXO can supply a common reference output for the use in some applications.

The OCXO provides a very stable (± 5 ppb) signal that can be tuned using a nanoDAC. The source is then buffered

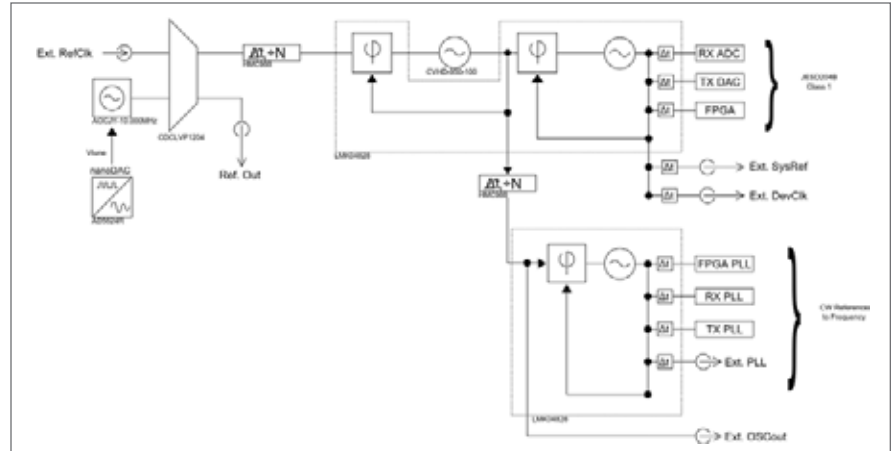
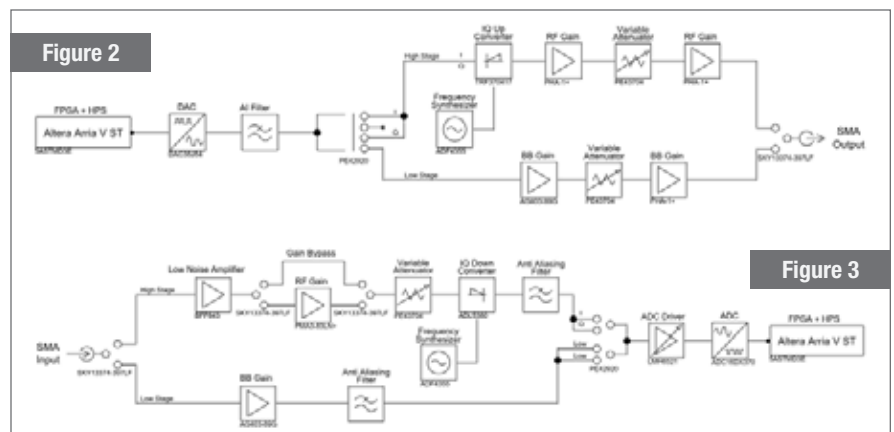


Figure 1 | Clock distribution architecture.



Figures 2 and 3 | Transmit radio architecture (top) and receive radio architecture (bottom) demonstrating high-frequency and baseband stages.

to provide two outputs (one for an external reference clock and one as the primary output for the system internally) where the primary output goes to an ultra-low-noise clock divider and delay, which enables phase shift/group delay capabilities. After the divider, the output goes to the first low-jitter clock generator in the system.

The clock conditioner, by default, has a 10MHz input and uses the internal Phase Locked Loop (PLL1) to control a 100 MHz low phase-noise VCXO. This locks the ultra-low phase-noise 100MHz VCXO to the stability provided by the 10MHz input. The 100 MHz VCXO output subsequently drives PLL2 of the first clock conditioner. This provides a 322 MHz JESD204B (subclass 1) device clock and sysref clock to the converters and transceivers (ADC, DAC, and FPGA).

A buffered copy of the 100 MHz VCXO output is also provided to a second clock conditioner, through a second clock divider. The buffered output drives the second PLL of the second divider and provides clocking to all frequency synthesizers for each front-end channel. (Figures 2 and 3.)

As a result, this default configuration allows for a known (in-phase) deterministic relationship for all outputs.

Visualize phase-coherent measurements in the time domain

All it takes is a limited knowledge of DSP techniques and phase-coherent down-conversion, which can be used to investigate sophisticated methods of calibrating a phase-coherent measurement system.



Figure 4 | The Crimson TNG SDR, in a 1U form factor, is powered by an Altera Arria V FPGA (5ASTMD3E3F31I3N) with an on-chip dual-core ARM Cortex-A9 processor with web-based interface.

This can be achieved by using a vector signal generator connected to the system and a power splitter. As all RF front ends will be tuned to the same center frequency, the measurement system can be calibrated easily by analyzing each of the analyzer's down-converted baseband waveforms.

Baseband sampling, both I and Q, enables direct access to the phase data of an acquired waveform containing both phase and magnitude data. Various software platforms can be used to coordinate the domain and calculate the phase information of each sample. This is done by computing the arctangent of Q/I.

Two important tasks can be accomplished by observing the phase data from an IQ waveform: First, fine adjustments can be made to the start phase of each NCO by measuring the phase information, which then compensates the variation in cable length for both analyzers. The calibration needs to be performed only once to remove the residual skew.

The Crimson TNG SDR platform from Per Vices has architected the clock distribution to provide a multichannel transceiver able to deliver deterministic phase coherency and latency. Its four independent receive chains and four independent transmit chains are each capable of up to 322 MHz of RF bandwidth up to 6 GHz. (Figure 4.)

As a result, when it comes to military SDR, multichannel phase-coherent RF measurements don't have to be an issue anymore as today's modular instrumentation has evolved to meet the new measurement requirements of military communications systems. **MES**



Stephanie Chiao is the Product Marketing Manager at Per Vices Corporation, where she is responsible for marketing strategy, technical promotion, and media relations. She brings over nine years of consumer and enterprise marketing experience and has worked with brands including Microsoft, Rogers Wireless, and Torstar Corporation. She holds an Honours Bachelor of Business Administration degree from the Schulich School of Business in Toronto. She may be reached at stephanie.c@pervices.com.

Per Vices
www.pervices.com

PCI Express Mini Card

mPCIe Embedded I/O Solutions

**24 Digital I/O With
Change-of-State IRQ Generation**

mPCIe Embedded OEM Series

- Rugged, Industrial Strength PCI Express Mini Card Form Factor
- For Embedded and OEM Applications
- High Retention Latching Connectors
- Tiny Module Size and Easy Mounting
- Extended Temperature and Custom Options Available
- Choose From a Wide Variety of Analog, Digital, Serial, and Relay I/O

**Multi-Port, Multi-Protocol,
RS-232/422/485
Serial Communication Modules**

**Isolated RS232/422/485 Serial
Communication Cards with Tru-Iso™
Isolation and Industrial Temperature**

**ACCES I/O Products' PCI Express
Mini Card embedded boards for OEM
data acquisition and control.**

**OEM System SPACE Flexibility
with dozens of mPCIe I/O modules
to choose from and extended
temperature options -
Explore the Possibilities!**

PCI EXPRESS®

**Saving Space,
The Final Frontier**

**ACCES
I/O PRODUCTS, INC.**
The Guys To Know For I/O
To learn more about our Embedded PCI Express Mini Cards
visit <http://aces.io>
or call 800 326 1849. Come visit us at
10623 Roselle Street San Diego CA 92121

USB PC/104 USB/104 Systems

Cloud security for military ops: It's complicated

By Sally Cole, Senior Editor

As the U.S. Department of Defense (DoD) embraces cloud computing, distributed-denial-of-service (DDoS) attacks and other forms of cyberattacks are increasing in sophistication and severity, which makes it extremely challenging for the DoD to ensure cloud availability, reliability, and security.



Navy Ensign Tilghman McCabe, left, reads through surface fire scenarios in the combat information center aboard the USS Curtis Wilbur during Valiant Shield 2016 in the Philippine Sea. The biennial Air Force, Navy and Marine Corps exercise focuses on sustaining joint forces at sea, in the air, on land and in cyberspace. Navy photo by Petty Officer 3rd Class Ellen Hilkowski.

Cloud computing is convenient way to provide on-demand network access to a shared pool of computing resources, and it's helping the DoD rapidly scale up its capabilities, achieve economies of scale, and maintain resiliency. But it also brings along undesirable baggage in the form of a new attack surface and threats to data security.

Beginning in 2015, the DoD started offering a wide selection of commercially owned and operated cloud services to DoD mission owners – as a way to help the military save time and reduce costs.

As the military moves to take advantage of the many benefits the cloud provides, security is understandably a key concern.

Cloud security threats

So what are the biggest cloud security risks for the military?

"There are many good things to be gained from the cloud, but some bad goes along with the good," says George Kamis, chief technology officer for government

markets for Forcepoint in Austin, Texas. "If good failover and backup policies aren't in effect, data and services can be easily disrupted or lost to denial-of-service or physical attacks."

Another factor Kamis cites as increasingly problematic is the broad dependence on a hypervisor to protect and separate the virtual machines operating within the cloud.

"If a successful attack is made on the hypervisor, all hosted virtual machines are instantly vulnerable – no matter how the operating systems and applications are secured," he says. "And there will be no indication within the virtual machines that those systems are compromised because the internal security mechanisms will be blind to the hypervisor attack."

DDoS attacks

Cloud attacks can come in many forms, but distributed-denial-of-service (DDoS) attacks can be particularly devastating. And DDoS attacks appear to be escalating in both frequency and severity.

"On January 2, 2016, the BBC [British Broadcasting Corporation] suffered an attack on all of its applications, which resulted in unavailability for at least three hours," points out Carl Herberger, vice president of security products for Radware in Mahwah, New Jersey. "At the time it was the largest DDoS attack ever recorded – at more than 600 Gbps." There have been several recent examples of stronger, worse attacks, portending even more brutal DDoS attacks in the future.

The group that claimed responsibility for the BBC attack is called the New World Hackers, and they reportedly carried it out via Amazon Web Services (AWS) after bypassing security measures and helping themselves to administrative privileges.



AWS, by the way, was the first commercial cloud provider approved by the Defense Information Systems Agency (DISA) to handle the DoD's sensitive – but unclassified – workloads back in 2014. To date, the DoD has granted provisional authorizations to 59 commercial cloud service offerings.

"Amazon makes a huge amount of infrastructure resources available to its users, so the risk of abuse of these resources for ill purposes via launching a mega DDoS attack has been previously debated," Herberger says.

Large cloud providers tend to leverage several measures to prevent DDoS attacks, including anti-spoofing, network monitoring and protection, and proprietary DDoS prevention. They also tap other common indirect measures like access control, anti-scanning, encryption, and segregation.

"Amazon EC2 [Elastic Compute Cloud] instances can't send spoofed network traffic," Herberger explains. "The AWS-

"THERE ARE MANY GOOD THINGS TO BE GAINED FROM THE CLOUD, BUT SOME BAD GOES ALONG WITH THE GOOD," SAYS GEORGE KAMIS, CHIEF TECHNOLOGY OFFICER FOR GOVERNMENT MARKETS FOR FORCEPOINT IN AUSTIN, TEXAS. "IF GOOD FAILOVER AND BACKUP POLICIES AREN'T IN EFFECT, DATA AND SERVICES CAN BE EASILY DISRUPTED OR LOST TO DENIAL-OF-SERVICE OR PHYSICAL ATTACKS."

controlled, host-based firewall infrastructure won't permit an instance to send traffic with a source IP or MAC address other than its own. So almost all network layer attacks that result in high volumes such as spoofed floods, reflection, and amplification floods, are ruled out."

In terms of network monitoring and protection, AWS relies on "a wide variety of automated monitoring systems to provide a high level of service performance and

HIGH DENSITY CONNECTORS

Micro & Nano Connector Series

- Cable to Board Systems
- Rugged Military Performance
- Compact and Lightweight
- Mission Critical Reliability
- Ruggedized for Extreme Environment Systems

OMNETICS

CONNECTOR CORPORATION

Tel +1 (763) 572 0656 | sales@omnetics.com

www.omnetics.com

availability,” he continues. “Its monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port-scanning activities, application usage, and unauthorized intrusion attempts. They also have the ability to set custom performance-metrics thresholds for unusual activity, so any unusual volume leaving the environment is expected to be detected and cause the relevant nodes to be shut down.”

Then there’s DDoS protection: In the BBC case, “a proprietary protection system was deployed,” Herberger says.



Figure 1 | U.S. Navy ships, which are essentially moving data centers, can host their own clouds. Pictured is the guided-missile destroyer USS Fitzgerald (DDG 62) as it is underway in the Pacific Ocean. U.S. Navy photo by Mass Communication Specialist 3rd Class Paul Kelly/Released.

Assured mission-critical cloud computing across “blue” and “gray” networks

One way the U.S. Air Force Research Laboratory is currently pursuing secure cloud computing science and technologies is by supporting the work of the Assured Cloud Computing (ACC) University Center of Excellence at the University of Illinois (UI) at Urbana-Champaign.

ACC is developing technology for assured, mission-critical cloud computing across “blue” and “gray” networks. Blue networks are military networks that are considered secure, while gray networks are those in private hands or run by other nations that may not be secure. Their goal is to ensure the confidentiality and integrity of data and communications to get missions done – even amidst cyberattacks and failures.

A computational cloud for military purposes may involve both blue and gray networks, so it’s often necessary to coordinate computation across a mixture of these resources.

But this isn’t easy: Overseas commitments and operations can stretch network-centricity with challenges in the form of global networking requirements, government and commercial off-the-shelf (COTS) technology, secure computing across blue and gray networks, and agility and mobility, according to the ACC team.

Assured mission-critical cloud computing across blue and gray networks requires “end-to-end and cross-layered security,” says the ACC team; this level of security involves multiple layers from the end device through the network and up to the applications or computations at the data center.

A survivable and distributed cloud-computing-based infrastructure “requires the configuration and management of dynamic systems-of-systems with both trusted and partially trusted resources – data, sensors, networks, computers, etc. – and services sourced from multiple organizations,” emphasizes the ACC team on its website (assured-cloud-computing.illinois.edu).

To ensure mission-critical computations and workflows that rely on such dynamically configured systems-of-systems, “it’s necessary to ensure that a given configuration doesn’t violate any security or reliability requirements,” the ACC adds. “And it should be possible

to model the trustworthiness of a workflow or computations completion for a given configuration to specify the right configuration for high assurances.”

So far, the ACC team has demonstrated that it’s possible to “build mission-critical cloud computing elements, deliver real-time results to secure the cloud, and make the cloud reliable,” says Roy Campbell, who leads ACC and is also a professor in UI’s Department of Computer Science.

By improving the functioning of NoSQL databases, which cloud systems frequently use, and through developing more advanced scheduling algorithms, the team has increased the performance speed of these databases and has shown that they can be relied upon to finish a task on deadline, which is critical for the military.

Campbell says that the ACC research has the potential to save the government money by allowing the use of “gray” networks for missions, rather than building colossal networks. “It’s also going to provide an additional layer of protection, because we can apply computing resources more liberally to missions,” he adds. “Our research provides more guarantee, allowing the armed forces to have more computing support for its work.”

The team’s next goal is to develop new methods to manage real-time streaming within the cloud. And now that the networking industry is embracing software-defined networking, the team is exploring ways to apply it to cloud systems.

The ACC team is also focusing its efforts on flexible and dynamic distributed cloud-computing-based architectures that are survivable; novel security primitives, protocols, and mechanisms to secure and support assured computations; algorithms and techniques to enhance end-to-end timeliness of computations; algorithms that detect security policy or reliability requirement violations in a given configuration; algorithms that dynamically configure resources for a given workflow based on security policy and reliability requirements; and algorithms, models, and tools to estimate the probability of completion of a workflow for a given configuration.

"While the detailed description of the system wasn't exposed, there is an additional level of monitoring and automated protection targeted at protecting those systems."

Amazon's customers can also report abuse of an account, notes Herberger. "Each report is investigated by the Amazon abuse team and actions are taken accordingly," he adds. "So supposedly an attack would have been reported and actions taken in a timely manner to resolve it."

Dynamic IP attacks

Herberger questions whether the BBC attackers' goal – rather than a high-volume attack – was really a sophisticated, sneaky dynamic IP attack.

What's a dynamic IP attack? "It targets the application layer," he explains. "By using a real IP address, you can generate a three-way handshake with the server and also bypass mitigation techniques

Navy Tactical Cloud contract won by Charles River Analytics

By John McHale, Editorial Director

Officials at the Office of Naval Research (ONR) selected Charles River Analytics Inc. in Cambridge, Massachusetts, for a contract to develop Navalynx, a framework for probabilistic, multisource naval analytics and analytic services, to enable rapid development and deployment of rich, mission-critical analytics. The work will be performed under the Navy Tactical Cloud effort, which brings big-data capabilities to the warfighting environment.

The 11-month, broad agency announcement (BAA) contract is valued over \$400,000, with options, if exercised, for an additional \$1 million over two years.

Navy officials are developing the Navy Tactical Cloud Reference Implementation (TCRI) to enable on-demand access to shared sensors and computing resources. They are looking to leverage TCRI to perform advanced analytics and reasoning, but this also poses potential challenges such as addressing significant uncertainty in warfighting domains; the volume of data available through modern sensors and networks; and the time and cost constraints in building unique analytics for specific data sources and data relationships. To meet these challenges, Navalynx will enable a foundation that supports probabilistic reasoning; handles missing, unreliable, and stale data; and supports fusion of multiple diverse input streams.

Navalynx marries Charles River's Figaro probabilistic programming language with a modular, reusable framework for developing reusable analytics modules. Charles River engineers will add distributed, big data-enabled algorithms to Figaro as part of the Navalynx effort. The reusable architecture for distributed analytics may be used in many domains, such as real-time health monitoring, threat assessment, and intelligence analysis.



SETTING THE STANDARD

Today's next-generation processors require next-generation connectivity to accommodate greater bandwidth needs while becoming smaller, lighter and even more rugged. TE Connectivity (TE) combines its experience with high-speed connectivity and rugged packaging to offer a broad portfolio of VPX-compliant interconnects that are engineered for mission-critical reliability in the harsh environments of military and aerospace applications.

Connect with TE to learn how we are setting the standard in open architecture solutions at te.com/embeddedcomputing



©2016 TE Connectivity Ltd. All Rights Reserved.
EVERY CONNECTION COUNTS, TE, TE Connectivity and TE connectivity (logo) are trademarks of the TE Connectivity Ltd. family of companies. OPEN VPX logo is a trademark of VITA.

EVERY CONNECTION COUNTS



such as JavaScript challenges.” Such an attack would make it nearly impossible to distinguish between attackers and legitimate users.

In this case, “application attacks require a full session, so no IP spoofing is relevant and actual sessions will be created,” Herberger continues. “Nevertheless, the IP can be

changed frequently via the huge ranges Amazon has to offer.”

It’s sneaky in terms of network monitoring and protection because it “uses

Embedded computing in the cloud

By John McHale, Editorial Director

Tactical, or as some call it, combat cloud computing will need to leverage more than commercial data center technologies, but will also need embedded computing – hardware and software – to enable it to work in secure battlefield applications.

“With every platform becoming a sensor and consumer of information in the military, you will see combat clouds on aircraft carriers, fighter jets, and in ground vehicles,” says Richard Jaenicke, director, market development and strategic alliances at Mercury Systems in Chelmsford, Massachusetts.

The term “combat cloud” was coined by Lt. Gen. David A. Deptula, U.S. Air Force (Ret.), Dean, The Mitchell Institute for Aerospace Studies, in his paper titled “Evolving Technologies and Warfare in the 21st Century: Introducing the ‘Combat Cloud,’” he says.

In it, Deptula states that a “combat cloud” is essentially “an operating paradigm where information, data management, connectivity, and command and control (C2) are core mission priorities. The combat cloud treats every platform as a sensor, as well as an “effector,” and will require a C2 paradigm enabling automatic linking, seamless data transfer capabilities, while being reliable, secure, and jam-proof. The combat cloud inverts the paradigm of combined arms warfare – making information the focal point, not operational domains. This concept represents an evolution where individually networked platforms – in any domain – transform into a “system of systems” enterprise, integrated by domain and mission-agnostic linkages.”

Enabling a combat cloud is natural extension of embedded computing, say Mercury Systems engineers.

“The embedded computing industry uses using the same kind of architecture that the cloud industry uses for data centers, but high-performance embedded computing companies can provide the necessary high level signal processing and real-time software necessary for enabling clouds and big data centers in military applications,” says Shaun McQuaid, Director, Product Management at Mercury Systems. “For example, when you look at a warfighter dealing with multiple sensors coordinating with multiple platforms – air, ground, and sea – you see a big data problem as there is much imagery needed to be processed at high bandwidth and in real time. Commercial cloud applications do not have the signal processing hardware and deterministic software necessary to enable this for a combat warfighter scenario.”

You start with the basic cloud technology then apply the embedded technologies to it to make it trusted and secure enough for tactical applications, Jaenicke adds.

Design challenges

To understand the design challenges for enabling a combat cloud, you need to understand how these cloud applications may differ from commercial applications.



Sidebar Figure | Pictured is the HDS 6603 secure server from Mercury Systems.

“Cloud security for the commercial world is much different than cloud security for military tactical applications,” McQuaid explains. “No one is likely to storm the doors of your run-of-the-mill commercial data center to go after their servers. But if a manned or unmanned platform gets taken down unexpectedly and falls into enemy hands it will need extra security such as encryption and methods to prevent reverse engineering. The military also needs to make the technology associated with a combat cloud and data center more deployable through rugged packaging and thermal management techniques, and also enable unrestricted bandwidth via high-speed fabrics such as Infiniband.

“On the bureaucratic side, you have to take a wider, more macro view, by taking into account military platforms communicate with other platforms on the battlefield such as what Gen. Deptula writes about,” he continues.

Hardware vs software and security

Which is more important when securing the cloud: protecting the software from cyberattacks or the hardware used in the data centers?

“I think you have to take both into account,” McQuaid says. “You can have all the hardware in world, but if you don’t have software that works for you then you can’t manage open interfaces and enable portability. Without that, tech refreshes become more difficult.”

From a cloud point of view, once you have the hardware piece developed, “then you start hardening from the software side, where the challenge then is how to make the software solution protected from cyberattacks, secured from reverse engineering, etc.,” Jaenicke says.

Mercury will be announcing a new line of secure, rackmount servers – dubbed HDS 6603 – designed specifically to address combat cloud applications, McQuaid says. “The family also takes technology from the OpenVPX side and the ATCA side and applies it to rackmount architectures. In addition to the cloud applications, it can be used for any kind of mission computing and data exploitation application.” See Figure.

For more on embedded technology and cloud computing, read a blog by VITA Chairman of the Board Ray Alderman, titled “Cloud, fog, mist, fluid, blockchain, and other things that irritate me” at <http://mil-embedded.com/guest-blogs/cloud-fog-mist-fluid-blockchain-and-other-things-that-irritate-me/>.

a low bandwidth per each source node and high distribution to hide it so that each source looks legitimate," he adds. "The low volume of the attack will keep it under the radar of any monitoring and it'll converge only at the final destination. In this destination, it will still be very difficult to distinguish friend from foe."

So while the task of generating an attack using Amazon or any other public cloud service certainly wouldn't be easy with existing security measures, Herberger notes that most measures are designed to prevent traditional, network-related types of DDoS attacks.

"We believe attackers are increasingly aware of high-complexity attacks, which are more difficult to detect and handle but equally devastating," Herberger says.

Beyond attacks: cloud benefits and misconceptions

Potential attacks aside, what are the main benefits of using the cloud for military operations? Its primary appeal appears to be the ability it provides for quickly provisioning and setting up new capabilities for warfighters. "Previously, hardware and software had to be procured, network drops had to be added, etc. But now systems can be quickly deployed," says Forcepoint's Kamis. "In the case of IC DTE [intelligence community desktop environment] and JIE [joint information environment], it enables users' MS Windows desktops to be centrally managed and secured."

Other benefits of the military using the cloud are similar to those adopted by private industry, Herberger says, but center on the "ubiquity, lower costs, higher quality, extensibility, scale, self-provisioning, autonomy, and agility" it can provide.

Misconceptions surrounding the military's cloud use abound, and one of the biggest, according to Kamis, is that "everything will shift to the cloud and be secured."

This is highly unlikely, because "the cloud" is essentially running software on some else's hardware remotely. "All of

the security issues, as with running locally, remain an issue and must be addressed and protected," Kamis continues. "Not everything can be cloud-based – and this is especially true for tactical deployments with limited communications."

Yet agencies are increasingly "forcing everything to the cloud without taking into consideration the impact of the move," Kamis notes. "It doesn't always make sense to move a capability to the cloud."

And viewing the situation from another perspective, perhaps the biggest misconception surrounding DoD use of the cloud "is that the military knows how to effectively leverage it," Herberger points out. "For years, they've run isolated and fundamentally controlled infrastructures ... so migrating to the cloud means more than a policy change ... it's a cultural shift as well." **MES**



SNAP

Are Your OpenVPX
Handles Breaking?

Superior Rugged Metal Claw

If you are ready for a more robust handle/panel solution, come to Pixus! Our OpenVPX handles feature a metal engagement claw and rugged design that ensures the highest reliability. Ask about our new rugged horizontal extruded rails with thicker material for OpenVPX and high insertion force systems today!

pixus TECHNOLOGIES

sales@pixustechnologies.com
pixustechnologies.com

Cybersecurity risks: Network-enabled weapon systems and humans

By Mariana Iriarte, Associate Editor



In this Q&A with Gil Nolte, executive advisor to Booz Allen Hamilton, he discusses the cybersecurity concerns that the Department of Defense (DoD) has with weapon platforms and the human factor that plays into that cybersecurity role. He also covers the various cyberthreats facing the private citizen, financial industry, and the direction the DoD is taking with programs like "Hack the Pentagon."

MIL-EMBEDDED: *Please provide a brief description of your responsibility within Booz Allen Hamilton and your role within the company.*

NOLTE: I am an executive advisor within Booz Allen Hamilton. At present, my job is within the company's strategic innovations group, specifically with the cyber-futures group focusing on industrial cybersecurity. My job is to work with DoD weapons and platforms to help the department think about and address cyber from a full-scope perspective.

MIL-EMBEDDED: *What type of cyberthreat is the DoD most concerned with?*

NOLTE: I think the department is extremely worried about any kind of cyberthreat from any kind of adversary whether it's a nation-state, a hacking group, or even kids trying to find access

to systems. I would agree that cyberthreats would vary across different geographies. Cyberattacks can happen in different ways and from different perspectives. Where an organization sits inside the United States, the safety nets may be bigger versus somewhere in Europe, Asia, or Afghanistan. There are people who are willing to do harm to the United States and I think the threat vector has yet to be thought of from a different perspective.

Scope-wise, I think the department is also worried about what I would consider their core commercial-based information technology. Today, we look at operational technology – like industrial control systems – things that really apply to weapons and platforms from a cyber perspective. We can reference the DoD's Operational Test and Evaluation Organization (OT&E), run by Michael Gilmore. At the end of the year, they typically publish results from

OT&E with a cyber section. For the past two years, it has specifically called out how they have looked at a variety of weapons and platforms; almost universally they have some sort of cyber vulnerability. So think about how we use our military might; and any of that may be at risk from a cyber perspective. That has to be a huge worry point in the department today.

We are starting to take an in-depth look at some of the military platforms, some way a cyber event could degrade that military capability and could put our armed forces and ultimately the U.S. at risk. That is something I'm very worried about. We, as a country, invest lots of money to make sure that we have the military might to do what we need to do around the world and protect the U.S. and its citizens. For some reason that could get degraded in some way and put our people and our country at risk; I think that should keep a lot of people up at night.



today is working and advising on weapons programs or DoD platforms that didn't consider cyber in the beginning days. More and more technology is going to stay out on the field for longer periods of time; cybersecurity was not considered as weapons systems were designed and developed. How do you adapt those platforms? And how do you make operators aware that something that they may see may be either a fault or something malicious from a cyber perspective?

An example we've used: A military helicopter carries a military crew to perform a mission and an "overheat" engine-warning light comes on. What happens? Well, they abort the mission and land as safely as they can to save human life and the equipment. But does the human who really goes through that post-analysis: That light turning on, that fault, was it really a fault or was it something that got inserted into the system? That notion is a cyber effect. That's the human part of understanding what they are working on and operating on, they're looking for phishing attacks, but also when something funny starts to happen, how do you ask the right questions? How do you get more people who are more tech-savvy and would understand that attack vector? That is a huge reason why the human is the problem.

MIL-EMBEDDED: *How do cyberthreats faced by the DoD differ from those faced by the financial industry or everyday citizens?*

NOLTE: Threats differ in a couple of different ways. What I know of the financial industry or everyday citizens, the threat is about – in some cases – financial gain. Sometimes we look at the threat from a DoD perspective, where we could see a cyber event happen that could degrade our military capability and/or steal intellectual property to understand how other systems are designed.

MIL-EMBEDDED: *Is it possible for someone to hack into a weapons system and assume control to use it against the United States?*

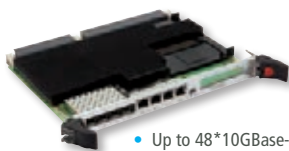
NOLTE: My personal opinion is that you can't ignore the possibility of someone hacking and taking control of a weapons system. If any kind of platform or weapons system connects to something else, there is a potential that it could be vulnerable. An offensive adversary might be thinking that they have time on their side, think about how do they look for that weak link in that system, in that platform, how could they take advantage of it at some point in time? I don't know that we have seen something like that, but again, anything that connects to something could have a mechanism to induce a weakness and be vulnerable from a cyber perspective.

MIL-EMBEDDED: *What is the biggest challenge when implementing cybersecurity measures in DoD platforms?*

NOLTE: Humans are a challenge. Another I have in the work I'm doing

Rugged HPEC boards for your OpenVPX Systems

10/40 GigaEthernet managed Switches



- Up to 48*10GBase-KR or 16 * 40Gbase-KR4 on data plane
- Up to 12* Gigabit ports and 6*10G/40G ports

Front End processing boards



- Virtex®-7 & QorIQ 6U VPX processing board

Digital Signal Processing DSP boards



- Intel® Xeon Broadwell DE
- Dual processor (8 cores per processor)
- PCIe / 10/40 Gigabit dataplane

Signal processing and communication FMCs



- Vita 57.1/4

- Harsh environment applications
- Supplied with a Full set of Development tools (firmware and switchware)
- High-technical support
- High-performance boards



+33 (0)2 98 57 30 30 • info@interfaceconcept.com • www.interfaceconcept.com



The DoD perspective – looking at what we would call “operational technology” is something a little different than what you might see in the financial industry or with everyday citizens. I’ll give you my personal example on the “everyday citizen”: My mother is 85 and went online. Something pops up such as “your system is hacked,” and to call this number, which she dutifully calls. She gives them her credit card, and they said, “Don’t worry, your card is going to show a charge from somewhere not in the U.S.” I worry about folks like her, where she’s just on Facebook or using email. The human in the middle is actually clicking on something that doesn’t look malicious but it’s malicious underneath. Everyday citizens are at a huge risk and they don’t think about what the perils or implications are. Luckily it worked out for Mom.

For the financial industry, I think there’s a record of how a cyberattacker got into a retail company and they got in through their HVAC systems – their heating and air conditioning systems – that had a network-based capability and it was connected to their host network. So, when [the cyberattacker] got in that way, they were able to get access to other things.

MIL-EMBEDDED: *Does the technology to keep all systems secure differ between the financial industry or private citizens and the DoD?*

NOLTE: The department goes way above what’s out there commercially for everyday citizens. What is commercially available is the starting point for every part of the DoD. A good antivirus capability, something that might be looking for malware, but the department goes further. They look at what happens at the boundary between their DoD Internet, the Non-classified Internet Protocol (IP) Router Network (NIPRNet), and the Secret Internet Protocol Router Network (SIPRNet).

They monitor and look for malicious things going on there. They also have huge worries on the DoD classified systems; that security goes further, far above what you see commercially. Everything is built on what is out there available in commercial technology. But the department adapts it and does it in different ways to look for much more than what would typically affect the average citizen.

MIL-EMBEDDED: *Is the DoD heading in the right direction to combat all cyberthreats?*

NOLTE: From a military perspective and where the department is, they’ve done a lot of things right and continue to do a lot of things right. Again, I think the evolving threat is just a continual thing. If you look at the recent press articles from the “Hack the Pentagon” event, [the DoD] went out and publicly had people hack the Pentagon. One of the top guys is 18 years old. Luckily, he is in the U.S. and doing that work. Even with decades of investing and doing the right things, because there are some underlying vulnerabilities in commercial technology or layers of commercial technology, or a human did something in a different setting or violated a policy – there are risks. I think we are going to continue to see risks from all different perspectives. We are not going to be done for a long time from a cyber perspective; it’s going to be something the department and every citizen is going to have worry about for a long time. **MES**

Gil Nolte, Booz Allen Hamilton Executive Advisor, leads the Strategic Innovation Group’s (SIG) Military Systems and Platform activities within the Industrial Cyber Account of the Cyber Futures Group. His team currently delivers cybersecurity and support services throughout the DoD. Mr. Nolte recently retired from the National Security Agency (NSA) and last served as the Director of the Trusted Systems Research Group. His thirty-plus year career at NSA included experiences in the Information Assurance and Cryptographic Security mission. He was also the DoD Program Manager for the implementation of the DoD’s Public Key Infrastructure (PKI). He has been awarded the Department of Defense Exceptional Civilian Service Award and the Presidential Meritorious Executive Rank Award. He has a master’s degree in Engineering Administration from The George Washington University and a Bachelor of Science in Electrical Engineering from West Virginia University.

SPECIAL ADVERTISING FEATURE

AVIONICS

Protocol Converters

- Already Qualified! (MIL-STD-461, MIL-STD-704, MIL-STD-810, MIL-E-5400T)
- ARINC 429, MIL-STD-1553, RS-232/422, SYNCHRO, ARINC-825/CAN, Discrete I/O, Ethernet
- Multi-Protocol
- Firmware allows the unit to operate completely transparent – acting as bridge between systems
- Operates from 28vDC
- Custom designs with little or no NRE with minimum quantity order



KIMDU
TECHNOLOGIES

Kimdu Technologies, LLC
1-800-677-6174
www.kimducorp.com
sales@kimducorp.com

OpenSystems Media

works with industry leaders to develop and publish content that educates our readers.

Check out our white papers.

<http://whitepapers.opensystemsmedia.com/>



Most popular topics:

Managing SWaP

COM Express

MIL-STD-1553

Cockpit Display Systems

Thermal Management

Shock and Vibration Testing Radar

Software Defined Radio

FPGAs

COTS

VPX

UAVs

Counterfeit parts

Data Security



Outmaneuvering potential IC sabotage

By Sally Cole, Senior Editor



To combat growing concerns about integrated circuit (IC) sabotage, cybersecurity researchers at New York University (NYU) are developing ICs that can monitor their own computations and flag defects.

The Pentagon's supply chain for microelectronics manufacturing has gone global – it's no longer strictly the realm of U.S. manufacturers. This outsourcing of microchip design and fabrication increases the odds for surreptitious installation of malicious circuitry.

In the past, relatively few opportunities existed for outside vendors to access IC blueprints or circuitry, but outsourcing is providing fraudsters and malicious actors more points of access to tamper with chips. "Back doors" secretly inserted in hardware can enable attackers to alter or stealthily take over a device or system at a specific time.

To outmaneuver the "bad guys" and prevent sabotage, Siddharth Garg, assistant professor of electrical and computer engineering at NYU's Tandon School of Engineering, and fellow cybersecurity researchers are working to develop a "verifiable computing" approach intended to both keep tabs on a chip's performance and spot signs of malware.

How does it work? The NYU team's approach involves a chip with two modules: an embedded one that proves that its calculations are correct, and an external one to validate the first module's proofs. The key part is a verifying processor that can be fabricated separately from the chip. (Figure 1.)

"Using an external verification unit made by a trusted fabricator means that I can go to an untrusted foundry to produce a chip that has not only the circuitry-performing computations but also a module that presents proofs of correctness," Garg explains.

Chip designers can then turn to a trusted foundry to build a separate, less complex module: an application-specific integrated circuit (ASIC) whose job is to validate the proofs of correctness generated by the internal module of the untrusted chip.

This arrangement provides a safety net for the chipmaker and end user, according to Garg. "Under the current system, I can get a chip back from a foundry with an embedded Trojan. It might not show up during post-fabrication testing, so I'll send it to a customer," he continues. "But two years down the line, it could begin misbehaving. The nice thing about our solution is that I don't have to trust the chip. Each time I give it a new input, it produces the output and the proofs of correctness, and the external module lets me continuously validate those proofs."

An added bonus is that the chip built by the external foundry is smaller, faster, and more power-efficient than the trusted rated ASIC – sometimes by orders of magnitude. So the verifiable computing setup could potentially reduce the time, energy, and chip area needed to generate proofs.

"For certain types of computations, it can even outperform the alternative – performing the computation directly on a trusted chip," Garg notes.

The next step for the researchers is to explore techniques to reduce the overhead that generating and verifying proofs imposes on a system as well as lower the bandwidth required between the "prover and verifier" chips. "With hardware the proof is always in the pudding, so we plan to prototype our ideas with real silicon chips," Garg says.

It's also worth pointing out that this isn't Garg's first big contribution within this field: In 2015, he discovered serious

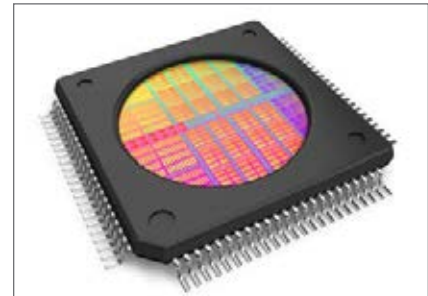


Figure 1 | A chip designed to flag malicious circuitry. Credit: NYU Tandon School of Engineering.

security vulnerabilities in a popular method of camouflaging circuits to prevent intellectual property (IP) theft. These camouflaged circuits could be reverse-engineered within minutes, so he developed a new approach that makes the functionality of a chip dependent on small fluctuations in the concentration of impurities with which the silicon is doped. Optical tools used to "de-layer" a chip for IP theft are unable to discern the functionality of a chip protected via this method.

Further, Garg is cited for helping to create a visionary technique of "split manufacturing" designed to foil attempts to compromise ICs during the fabrication process. The design plan is divvied up between several foundries, making it more difficult for a malicious actor to alter a circuit's functionality.

The group's work with verifiable computing was supported by grants from the National Science Foundation, the Air Force Office of Scientific Research, the Office of Naval Research, a Microsoft Faculty Fellowship, and a Google Faculty Research Award.

Garg and colleagues Ahbi Shelat of the University of Virginia, Rosaria Gennaro of the City University of New York, Mariana Raykova of Yale University, and Michael Taylor of the University of California – San Diego, will share a five-year National Science Foundation grant of \$3 million.

Stories are part of the curriculum for artificial-intelligence robots

By Mariana Iriarte, Associate Editor



Researchers at Georgia Tech with support from the Office of Naval Research (ONR) have designed artificial-intelligence (AI) software that will teach robots the difference between right and wrong. Through the art of storytelling, the software – called Quixote – aims to teach robots acceptable social behavior.

Clearly the AI designers are making an association between the software's name, "Quixote," and the legendary 17th-century story of "The Ingenious Gentleman Don Quixote of La Mancha" by Miguel de Cervantes Saavedra. The main character of the story is driven by his wild fantasies, thought to originate from the romantic, chivalric stories he was so fond of. Essentially, the character has no connection to reality and sets out on a journey where the final result is death, not just of the character, but also the metaphorical death of chivalry.

In an ONR release, program manager Marc Steinberg stated, "For years, researchers have debated how to teach robots to act in ways that are appropriate, non-intrusive, and trustworthy." The question: Is that even possible? "One important question is how to explain complex concepts such as policies, values, or ethics to robots. Humans are really good at using narrative stories to make sense of the world and communicate to other people," Steinberg says. "This could one day be an effective way to interact with robots."

The intriguing aspect of this program is that researchers are teaching digital circuitry driven by binary numbers how to act in the same way humans are taught as children: through the act of storytelling. While stories hold an immense amount of wisdom, it is up to the reader and listener to interpret the meaning of the story. To this effect, how do you teach an artificial intelligence agent the "right" meaning of a story? Especially when humans certainly interpret words differently.

The hope is that the Quixote software serves as a "human user manual," according to Dr. Mark Riedl, associate professor and director of Georgia Tech's Entertainment Intelligence Lab. The software seeks to teach AI robots how to interact with humans, he says, in the safest and most trustworthy way.

Using stories taken from the internet that highlight daily social interactions, the Georgia Tech researchers created a virtual agent and placed it in what they called "game-like scenarios," where it actually earned points and – interestingly enough – also earned positive reinforcements "for emulating the actions of protagonists in the stories." (Figure 1.)

The results? The agent went through approximately 500,000 simulations and had a 90 percent success rate, with a ten percent chance that the virtual AI acted negatively.

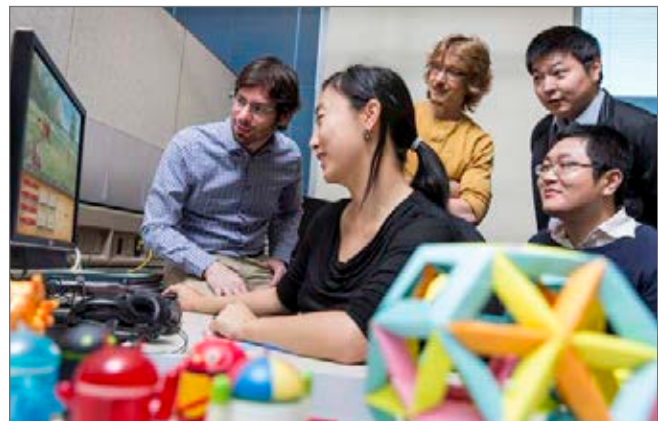


Figure 1 | Dr. Mark Riedl (left) and his team created the Quixote software to act as a "human user manual" for robots. Photo courtesy of U.S. Navy/Georgia Tech College of Computing.

Riedl says, "These games are still fairly simple, more like 'Pac-Man' instead of 'Halo.' However, Quixote enables these artificial-intelligence agents to immerse themselves in a story, learn the proper sequence of events, and be encoded with acceptable behavior patterns. This type of artificial intelligence can be adapted to robots, offering a variety of applications."

The key here is that the robots will have encoded algorithms that will make them act in a certain way. While humans have free will, these robots are driven by code. Over time, will these robots evolve as humans have over many centuries? Will the robots' behavior adapt as society changes and moves from one moral standard to another?

"Within a decade, there will be more robots in society, rubbing elbows with us," Riedl says. "Social conventions grease the wheels of society, and robots will need to understand the nuances of how humans do things. That's where Quixote can serve as a valuable tool. We're already seeing it with virtual agents like Siri and Cortana, which are programmed not to say hurtful or insulting things to users."

Cervantes wrote his story depicting the eventual expiration of chivalry; will this Quixote teach AI robots to preside over the eventual death of humanity? Riedl thinks not: "We believe story comprehension in robots can eliminate psychotic-appearing behavior and reinforce choices that won't harm humans and still achieve the intended purpose," he says.

For more information on Riedl's research under ONR's Science of Autonomy program, visit the webpage: www.onr.navy.mil/en/Science-Technology/Departments/Code-35/All-Programs/aerospace-research-351/Science-Autonomy.aspx.



Rugged embedded computer designed to meet SWaP requirements for C4ISR

The RE1218M rugged embedded computer from Crystal Group is designed for workstation and/or storage capability in extreme environments with reduced size, weight, and power (SWaP) requirements. It is targeted at command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) applications.

The RE1218M accommodates as many as eight 2.5-inch solid-state drives, can handle one PCI2 x16 expansion card, and may be mounted in any orientation. The processor is powered by the Intel Haswell, Xeon D, or Skylake CPUs and has a modular I/O plate with MIL-C-26482 military circular connectors. The RE1218M can be tray- or fixed-mounted and supports expansion for 1x PCIe 3.0 x16 and uses rugged MIL-C-26482 military circular connectors. It is compatible with Windows 10, Redhat 6.5/6.6, Windows Server 2008 and 2012, and VMWare. The aluminum-chassis system conforms to MIL-STD-810F (516) specifications for vibration and can handle 20G of functional shock for 11 msec. The unit measures 4.1 inches high by 10.25 inches wide by 14.4 inches deep, excluding connectors, and is cooled by high-speed/high-volume thermostatically controlled fans.

Crystal Group Inc. | www.crystalrugged.com | www.mil-embedded.com/p373806

GaN transistors for electronic warfare and communication systems

NXP has expanded its family of gallium nitride (GaN) radio frequency (RF) power transistors to include six driver or final-stage amplifiers that have frequency coverage ranging between 1 to 3000 MHz. The additional line of transistors join NXP's portfolio of RF power transistors aimed at defense systems that operate in HF/VHF/UHF/L-band radar, IFF transponders, and avionics systems.

The GaN and SiC transistors combine high power density, ruggedness, and flat frequency response over wide bandwidths. The transistors' broadband frequency coverage from HF to S-band allows users to cover frequencies used by radios or at the lower-frequency sections of electronic systems. The transistors include MMRF5011N (28V) and MMRF5013N (50V), which operate from 1 to 3000 MHz with RF output power up to 12 W CW, 15 dB gain, and 60 percent efficiency, housed in an OM-270-8 overmolded plastic package. The MMRF5015NR5 – which operates from 1 to 2700 MHz with RF output power up to 125 W CW, gain of 16 dB, and efficiency of 64 percent – is housed in an OM-270-2 over-molded plastic package. Additional transistors in the family include the MMRF5019N, MMRF5021H, and MMRF5023N.

NXP | www.nxp.com | www.mil-embedded.com/p373809



Bidirectional optical extender provides optical-electrical bridge by over a mile

Avionics Interface Technologies' MIL-STD-1553 Fibre Optic Databus Extender is an optical-electrical bridge for extending a MIL-STD-1553 databus by over a mile in length. The optical extension offers a low-latency mechanism for sending 1553 data through noisy environments and across long distances. To operate as a bidirectional optical extension, the extender requires two identical units at each end of the optical link for operation.

Engineers designed the bridge so it can be configured to extend one or two dual redundant MIL-STD-1553 databuses. It also can be configured as a transformer or direct coupling. Two or four twinaxial connectors enable connection to the MIL-STD-1553 primary and secondary channels. One duplex-LC connector (with GbE SFP) is used for connection to the fiber-optic link, with the use of multimode or single-mode fiber. The databus extender is intended for applications where test equipment is separated from units under test, including flight-line testing, anechoic chambers, and large simulation systems.

Avionics Interface Technologies | www.avitech.com | www.mil-embedded.com/p373808



Radar and software interface supports VITA 49.0 specifications

Model 71664 is a member of Pentek's Cobalt family of XMC modules based on the Xilinx Virtex-6 field-programmable gate array (FPGA). Designed as a multichannel, high-speed data converter, it uses programmable digital downconverters (DDCs) and its PCIeExpress output supports the VITA 49.0 Radio Transport (VRT) standard. The 71664 is suitable for connection to HF or IF ports of a communications or radar system. The built-in data-capture feature offers users a platform for developing and deploying custom FPGA-processing intellectual property (IP).

The system includes four analog-to-digital converters (ADCs) and four banks of memory. In addition to supporting PCI Express Gen. 2, the Model 71664 includes a general-purpose connector for application-specific I/O. Pentek's Cobalt architecture organizes the FPGA as a container for data-processing applications in which each function exists as an IP module. For applications that require specialized function, users can integrate their own IP with the Pentek factory-installed functions or use the GateFlow kit to completely replace the Pentek IP with their own. The Virtex-6 FPGA site can be populated with two different FPGAs (LX240T or SX315T) to match the specific requirements of the processing task.

Pentek | www.pentek.com | www.mil-embedded.com/p373809

Uninterruptible power supply for extreme environments

IntelliPower's bright uninterruptible power supply (UPS) can be manually selected to 120 or 240 volts AC output and functions as a power-conditioning/conversion system with power factor correction for military applications in a rack. IntelliPower systems are designed with circuit boards, chassis, and components intended for use in extreme environments.

The company's digital double conversion on-line UPS, power conditioner, and frequency/voltage converter solutions use high-efficiency power switching and galvanic isolation for enhanced electrical output performance. Systems are available with global voltage inputs and outputs, AC inputs and outputs, and DC inputs and outputs. The power-management software adheres to standard communications protocols such as SNMP with OID and MIB Support, RS-232, Ethernet/IP – Common Industrial Protocol (CIP), MODBUS, and Dry/Discrete Contacts. The product configurations are designed and manufactured to meet military standards including MIL-STD-461F (Electromagnetic Interference EMI), MIL-STD-464C (Electromagnetic Environmental Effects EME), MIL-STD-1275D (DC Electrical Power Systems), MIL-STD-901D (Shock), MIL-STD-167-A (Vibration), MIL-STD-810G (Environmental; Altitude, Temperature, Humidity, Fungus, Sand & Dust, Rain), and MIL-STD-1399-300B (Interface requirements for AC devices; Voltage Transients [spikes], Frequency Transients, Harmonics, Power Factor).

Intellipower | www.intellipower.com | www.mil-embedded.com/p373810



DAL-C certifiable XMC 2.0 SBC for aerospace and defense applications

Creative Electronics Systems (CES) offers the MFCC-8557, a DAL-C-certifiable XMC 2.0 single-board computer (SBC) for aerospace and defense applications. It is designed to meet the DO-178C/DO-254 certification process and can be delivered with all documentation, certification evidences, and supporting artifacts required to prove compliance with the design-assurance qualifications of the avionic industry.

CES has equipped the MFCC-8557 with a set of power-on, continuous, and initiated built-in tests, together with hardware components to physically disconnect maintenance interfaces during missions. The MFCC-8557 is designed to work with complementary building blocks featuring an XMC 2.0-compatible site. Bundled with CES' VGP-2870 or AVIO-2353, the MFCC-8557 turns into a DAL-C (DO-178C/DO-254)-certifiable subsystem, all contained in a single 3U VPX slot, aimed at computation-intensive video and graphics (bundled with the VGP-2870) or I/O-rich avionics applications (AVIO-2353). The MFCC-8557 is designed to meet DAL safety certification, produced using DO-178C/DO-254 design best practices. Features include extended-range, conduction-cooled operation; low-SWaP bundle options with I/O avionics interfaces or high-performance video graphics; XMC 2.0 (VITA-61) form factor; NXP QorIQ P3041 processor; low power (12W typical); and 4x PCIe Gen2 interfaces on XMC (full mesh support).

Creative Electronics Systems | www.ces-swap.com | www.mil-embedded.com/p373811

Page	Advertiser/Ad Title
------	---------------------

- | | |
|----|--|
| 47 | Abaco Systems –
What makes it mission ready? |
| 31 | ACCES I/O Products, Inc. –
PCI Express mini card mPCIe embedded I/O solutions |
| 17 | Acromag – AcroPacks = SWaP-C |
| 15 | AIM-USA – Modules – Software – Systems |
| 5 | Annapolis Micro Systems, Inc. –
Keep your FPGA system integration on target and above water |
| 16 | Astronics/Ballard Technology –
The industry's most trusted and widely used USB interfaces |
| 6 | Behlman Electronics –
See what's waiting for you at www.acdcpowerplus.com |
| 23 | Data Device Corporation –
Your solution provider for connectivity/power/control |
| 27 | DRS Technologies –
Leading the way in RF excellence |
| 2 | Extreme Engineering Solutions (X-ES) –
Battlefield-ready small form factor (SFF) rugged systems |
| 39 | Interface Concept –
Rugged HPEC boards for your OpenVPX systems |
| 40 | Kimdu Corporation –
Protocol converters |
| 21 | LCR Embedded Systems –
Rugged chassis, backplanes, and integrated systems |
| 25 | Mercury Systems –
Innovation that protects |
| 33 | Omnetics Connector Corp. –
Micro & nano connector series |
| 48 | Pentek, Inc. – Capture. Record. Real-time. Every time |
| 28 | Phoenix International –
Airborne, shipboard, ground mobile data recording and data storage |
| 37 | Pixus Technologies – SNAP –
Are your OpenVPX handles breaking? |
| 35 | TE Connectivity – Setting the standard |
| 3 | WinSystems, Inc. –
Rugged, reliable, resilient! |

EVENTS

MILCOM 2016

November 1-November 3
Baltimore, MD
events.afcea.org/milcom16

AOC (Association of Old Crows) Symposium

November 29-December 1
Washington, DC
www.crows.org

Embedded Tech Trends

January 23-24, 2017
New Orleans, LA
www.vita.com/event-2304553

CONNECTING WITH MIL EMBEDDED

By Mil-Embedded.com Editorial Staff

CHARITY

Air Force Aid Society

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 The Air Force Aid Society (AFAS), a 501(c)(3) organization that has as its mission helping “to relieve distress of Air Force members and their families and assisting them to finance their education.” AFAS was created in 1942, rooted in the original Army Air Corps and the World War II Army Air Forces; their commander, General Henry “Hap” Arnold, wanted a national organization that could provide emergency support to the wives and children of war victims and also assure the availability of educational assistance to those families.

The nonprofit aims to help recipients – according to the AFAS, 89 percent of the emergency assistance dollars go to active-duty enlisted personnel and their families – with short-term, interest-free loans and grants or money for one-time emergencies such as food, rent, and utilities. The Society also serves the Air Force community with programs such as “Give Parents a Break,” which enables base officials to offer periodic child care at specified evening and weekend times. This assistance is particularly helpful when a spouse is deployed or other personal emergencies occur. Recipients can also take advantage of programs such as Bundles for Babies, Car Care Because We Care, Child Care for PCS, the Phone Home program and Youth Employment Skills.

In 2015, the AFAS reported over 57,000 assists to Air Force personnel and their families, totaling nearly \$16 million.

For more information, visit www.afas.org.



WHITE PAPER

Software-defined radio handbook

By Rodger Hosking, Pentek

Software-defined radio (SDR) is used for a variety of applications, including on-field communications, data acquisition, and signal processing. In this white paper, learn how digital downconverters (DDCs) and digital upconverters (DUCs), the fundamental building blocks of SDR, can replace legacy analog receiver and transmitter designs while offering benefits in performance, density, and cost.

The handbook will compare conventional analog receiver and transmitter systems to their digital counterparts, explore the internal structure of the SDR, and present some actual board- and system-level implementations and available off-the-shelf SDR products and applications based on such products.

Read the white paper:

<http://mil-embedded.com/white-papers/white-handbook-11th-edition/>

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



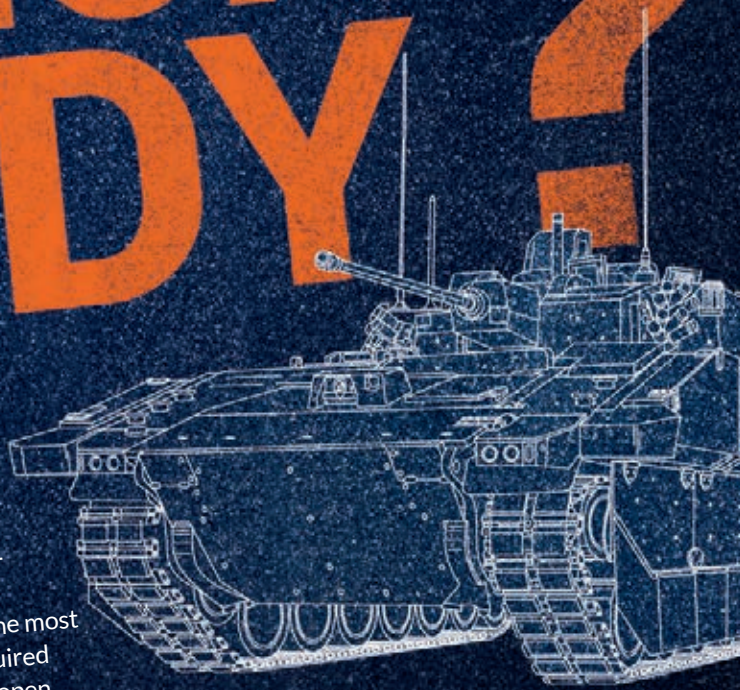
WHAT MAKES IT MISSION READY?

IT MAY BE ITS ALL-WEATHER IMAGING CAPABILITY
IT MAY BE ITS REVOLUTIONARY TURRET
IT MAY BE ITS 40MM CANNON
IT MAY BE ITS ULTRA-QUIET AUXILIARY POWER UNIT

The world's most advanced armored fighting vehicle is also the most digital. It can capture, process and store 6 TBs of sensor-acquired information, transmitting it over a 20 Gb/s Gigabit Ethernet open architecture backbone. It is equipped with a state-of-the-art, scalable ISTAR package that more than doubles the range at which targets can be identified and tracked.

The technology it deploys is not only advanced, but proven. Not only reliable, but ruggedly reliable. And not only for today, but for its lifetime.

**THE WORLD'S MOST ADVANCED ARMORED FIGHTING
VEHICLE IS ALSO MADE MISSION READY BY
TECHNOLOGY FROM ABACO SYSTEMS**



ABACO SYSTEMS: EMBEDDED IN THE WORLD'S MOST CRITICAL MISSIONS SINCE 1986.



WE INNOVATE. WE DELIVER. YOU SUCCEED.

abaco.com | [@AbacoSys](https://twitter.com/AbacoSys)

©2016 Abaco Systems.



Capture. Record. Real-Time. Every Time.

Intelligently record wideband signals continuously...for hours

Capturing critical SIGINT, radar and communications signals requires hardware highly-optimized for precision and performance. Our COTS Talon® recording systems deliver the industry's highest levels of performance, even in the harshest environments. You'll get extended operation, high dynamic range and exceptional recording speed every time!

- **High-speed, real-time recording:** Sustained data capture rates to 8 GB/sec
- **Extended capture periods:** Record real-time for hours or days with storage up to 100+ TB
- **Exceptional signal quality:** Maintain highest dynamic range for critical signals
- **Flexible I/O:** Capture both analog and digital signals
- **Operational in any environment:** Lab, rugged, flight-certified, portable and SFF systems designed for SWaP
- **Out-of-the-box operation:** SystemFlow® GUI, signal analyzer and API provide simple instrument interfaces
- **Intelligent recording:** Sentinel™ Intelligent Scan and Capture software automatically detects and records signals of interest



Eight SSD QuickPac™ canister, removable in seconds!

Download the FREE High-Speed Recording Systems Handbook at: www.pentek.com/go/mestalon or call 201-818-5900 for additional information.



PENTEK
Setting the Standard for Digital Signal Processing

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

Worldwide Distribution & Support, Copyright © 2016 Pentek, Inc. Pentek, Talon, SystemFlow, Sentinel and QuickPac are trademarks of Pentek, Inc. Other trademarks are properties of their respective owners.

