

Military

EMBEDDED SYSTEMS

@military_cots

MIL-EMBEDDED.COM

John McHale
Visiting Old Ironsides

7

Special Report
SDRs: Design for flexibility

12

Mil Tech Trends
Network-centric warfare

22

Cybersecurity Update
Predicting cyber intrusions

45

October 2017 | Volume 13 | Number 7

MILITARY LOOKS TO GAMING TECHNOLOGY FOR TRAINING TOOLS

P 26

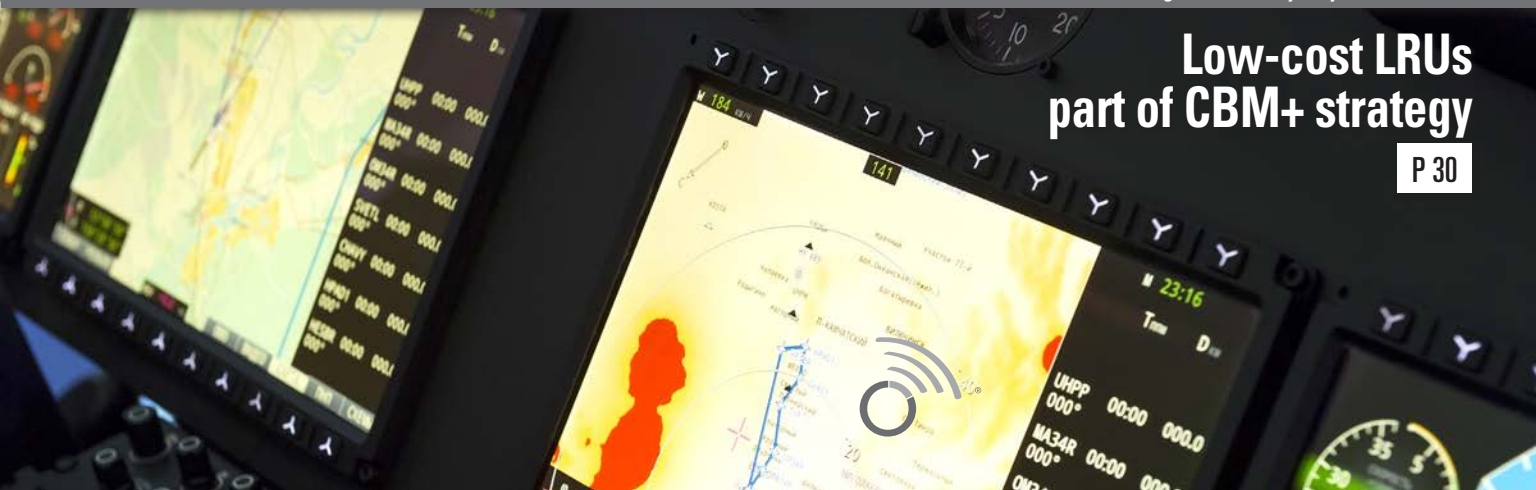
P 36



Military MRO: Solving the maintenance skills shortage with augmented reality – By Kevin Deal, IFS

Low-cost LRUs part of CBM+ strategy

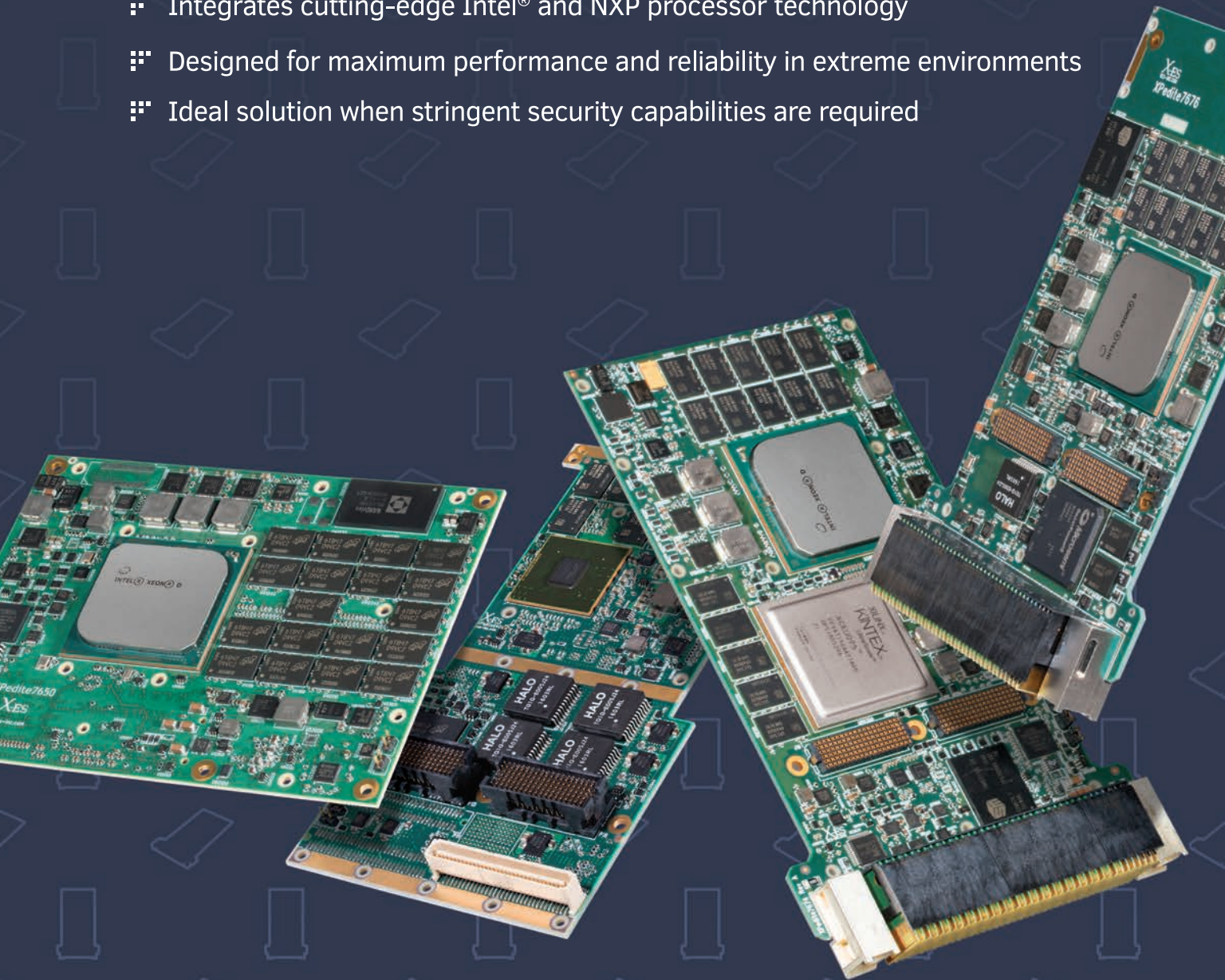
P 30



RUGGED EMBEDDED PROCESSOR BOARDS

Designed, manufactured, tested, and
supported exclusively within the USA

- Integrates cutting-edge Intel® and NXP processor technology
- Designed for maximum performance and reliability in extreme environments
- Ideal solution when stringent security capabilities are required



Extreme Engineering Solutions
608.833.1155 www.xes-inc.com

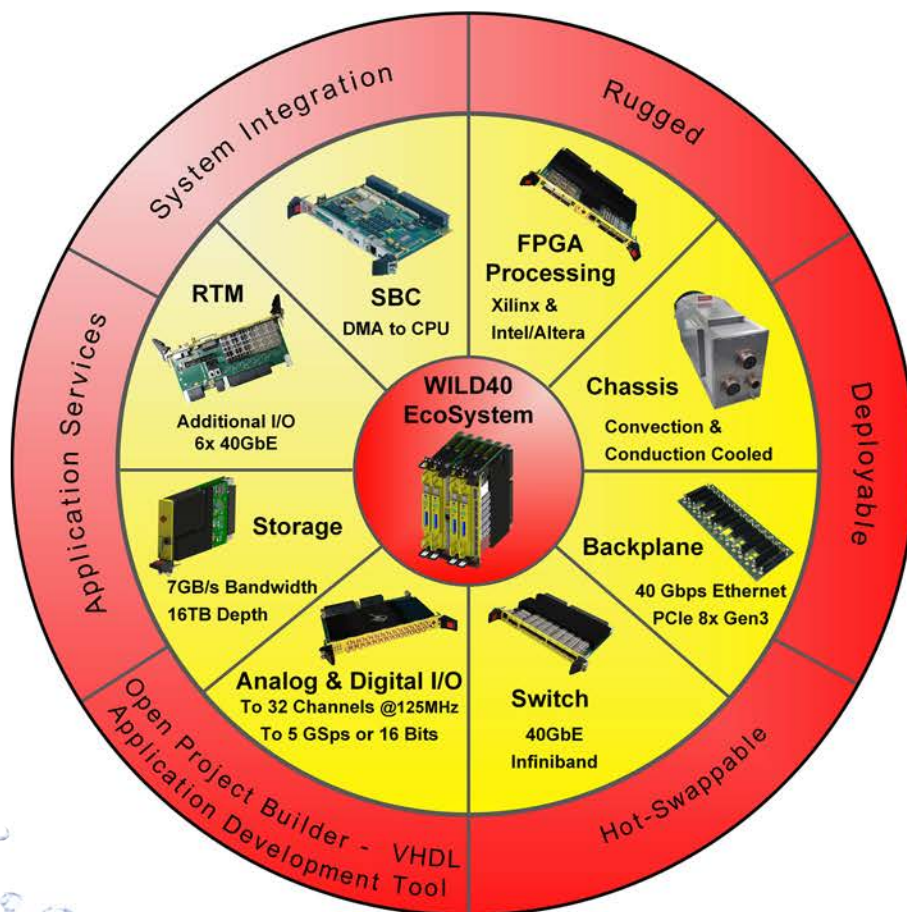


Designed, manufactured, and supported in the USA



Keep Your FPGA System Integration on Target and above Water

WILDSTAR™ 40Gb 6U and 3U OpenVPX EcoSystem
Altera Stratix 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 54th Annual AOC Convention in Washington, D.C.

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

Military

EMBEDDED SYSTEMS

October 2017

www.mil-embedded.com



12



16



22



30

SPECIAL REPORT

Military Radio Design Trends

- 12 SDRs and designing for flexibility
By Brandon Malatest, Per Vices

MIL TECH TRENDS

Network Security

- 16 Software-defined networking:
On-the-fly agility, security
By Sally Cole, Senior Editor
- 20 Where did that software come from?
By Russell Doty, Red Hat
- 22 The network-centric approach:
Solving the challenges of real-time
battlefield communications
By Barry McElroy, Rajant

INDUSTRY SPOTLIGHT

Simulation and Training

- 26 Gaming tech: Shaping the reality of
military training
By Mariana Iriarte, Associate Editor
- 30 How low-cost LRUs can support a
Condition-Based Maintenance Plus environment
By John Rodwig, IEE
- 34 Data-driven design for HMI development in
avionics design
By Raymond Niagaris, ENSCO
- 36 Military MRO: Solving the maintenance skills
shortage with augmented reality
By Kevin Deal, IFS



26

COLUMNS

Editor's Perspective

- 7 Visiting Old Ironsides
By John McHale

Field Intelligence

- 8 Ethernet switches:
Smarter than you think
By Charlotte Adams

Mil Tech Insider

- 9 Ethernet for synchronization:
It's about time
By Andrew McCoubrey

Technology Update

- 44 DARPA's Electronics Resurgence
Initiative addresses eventual
saturation of Moore's Law
By Mariana Iriarte

Cybersecurity Update

- 45 U.S. Army Research Laboratory
models predict cyber intrusions
By Sally Cole

DEPARTMENTS

- 10 **Defense Tech Wire**
By Mariana Iriarte

- 40 **Editor's Choice Products**

- 46 **Connecting with Mil Embedded**
By Mil-Embedded.com Editorial Staff

WEB RESOURCES

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

White papers:

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

Submit: <http://submit.opensystemsmedia.com>

ON THE COVER:

Top image: Bohemia Interactive Solutions' (BISim) Virtual Battlespace 3 (VBS3) is part of the U.S. Army's current Game-For-Training program of record. Photo courtesy of BISim.

Bottom image: Low-cost line replaceable units (LRUs) designed for condition monitoring and health assessment – including those used in military displays – can be a large part of a CBM+ integrated strategy.



[www.linkedin.com/groups/
Military-Embedded-
Systems-1864255](http://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.

© 2017 OpenSystems Media © 2017 Military Embedded Systems
ISSN: Print 1557-3222



Aitech. *Leading the Space Race.*

Stellar Performance, Interstellar Expertise

While you explore new systems, buses and platforms, Aitech works to find ways to make your ideas practical and affordable. It's what we've done for over 30 years.

By providing qualified products ready for space, we help lower your costs and reduce time to market without compromising quality or reliability.

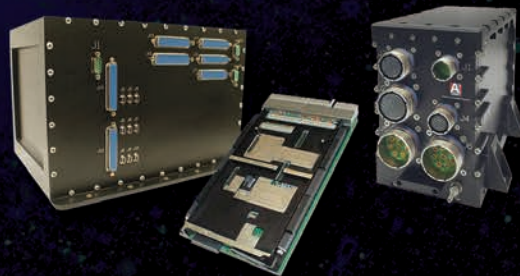
Our experience in providing rad-tolerant, space-qualified products – from SBCs, mass memory and peripheral boards to enclosures and subsystems – makes Aitech uniquely positioned to help you turn your most advanced satellite-based concepts into reality:

- Space-qualified, rad-tolerant, rad-hard
- Largest array of on-board I/O
- Single event effects mitigation
- Total ionizing dose radiation survivability

Our products are tested and proven for near, low, medium, and high Earth orbit applications, lunar and Mars terrestrial platforms, and much more. We've been a part of high-profile, mission critical programs where the highest performance and reliability are required, such as the Space Shuttle, MIR Space Station, ISS and many more.

And with our comprehensive COTS Lifecycle+™ Program, we support your design for a minimum of 12 years with program management that helps mitigate your obsolescence risk.

Learn how Aitech can help get your ideas off the ground. Visit our website or give us a call.



Embedded Computing *without* Compromise

Aitech Defense Systems, Inc.

19756 Prairie Street
Chatsworth, CA 91311
email: sales@rugged.com
Toll Free: 888-Aitech8 - (888) 248-3248
Fax: (818) 407-1502

www.rugged.com



Military

EMBEDDED SYSTEMS

Page Advertiser/Ad Title

- 47 Abaco Systems** –
Now COTS means COTS
- 24 ACCES I/O Products, Inc.** –
PCI Express mini card; mPCIe
embedded I/O solutions
- 19 Acromag** – Great things do come
in small packages
- 5 Aitech Defense Systems** –
Aitech. Leading the space race
- 25 Alphi Technology Corporation** –
Mission-critical I/O solutions
- 3 Annapolis Micro Systems, Inc.** –
Keeping your FPGA system
integration on target and above
water
- 28 Data Device Corporation** –
Stay connected
- 33 Elma Electronic** –
Test and development chassis
with room to maneuver
- 2 Extreme Engineering Solutions
(X-ES)** – Rugged embedded
processor boards
- 37 Interface Concept** –
Highly flexible Ethernet switches
and IP routers
- 14 MPL AG** – Rugged flexible
COTS solutions from MPL
- 48 Pentek, Inc.** – Unfair advantage
- 14 Phoenix International** –
Airborne, shipboard, ground mobile
data recording and storage
- 17 Pico Electronics** –
Size does matter!
- 32 Star Communications Inc** –
Signal processing receivers;
computing accelerators

EVENTS

AOC – Association of Old Crows Int'l Symposium/Convention

November 28-30, 2017

Washington, DC • www.crows.org/conventions

Embedded Tech Trends

January 22 & 23, 2018

Austin, TX • www.embeddedtechtrends.com

E-CAST

Cyber Security: It Starts with the Embedded System

Presented by LDRA, Rogue Wave Software,
Wind River, WinSystems

ecast.opensystemsmedia.com/753

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

CONTRIBUTING DESIGNER Joann Toth jtoth@opensystemsmedia.com

VITA EDITORIAL DIRECTOR Jerry Gipper jgipper@opensystemsmedia.com

SALES

SALES MANAGER Tom Varcie tvarcie@opensystemsmedia.com
(586) 415-6500

MARKETING MANAGER Eric Henry ehenry@opensystemsmedia.com
(541) 760-5361

STRATEGIC ACCOUNT MANAGER Rebecca Barker rbarker@opensystemsmedia.com
(281) 724-8021

STRATEGIC ACCOUNT MANAGER Bill Barron bbarron@opensystemsmedia.com
(516) 376-9838

STRATEGIC ACCOUNT MANAGER Kathleen Wackowski kwackowski@opensystemsmedia.com
(978) 888-7367

SOUTHERN CAL REGIONAL SALES MANAGER Len Pettet lpettet@opensystemsmedia.com
(805) 231-9582

SOUTHWEST REGIONAL SALES MANAGER Barbara Quinlan bquinlan@opensystemsmedia.com
(480) 236-8818

NORTHERN CAL STRATEGIC ACCOUNT MANAGER Sean Raman sraman@opensystemsmedia.com
(510) 378-8288

ASIA-PACIFIC SALES ACCOUNT MANAGER Elvi Lee elvi@aceforum.com.tw

BUSINESS DEVELOPMENT EUROPE Rory Dear rdear@opensystemsmedia.com
+44 (0)7921337498



WWW.OPENSYSTEMSMEDIA.COM

PRESIDENT Patrick Hopper phopper@opensystemsmedia.com

EXECUTIVE VICE PRESIDENT John McHale jmchale@opensystemsmedia.com

EXECUTIVE VICE PRESIDENT Rich Nass rnass@opensystemsmedia.com

CHIEF FINANCIAL OFFICER Rosemary Kristoff rkristoff@opensystemsmedia.com

CHIEF TECHNICAL OFFICER Wayne Kristoff

EMBEDDED COMPUTING BRAND DIRECTOR Rich Nass rnass@opensystemsmedia.com

EMBEDDED COMPUTING EDITORIAL DIRECTOR Curt Schwaderer cschwaderer@opensystemsmedia.com

TECHNOLOGY EDITOR Brandon Lewis blewis@opensystemsmedia.com

CONTENT ASSISTANT Jamie Leland jleland@opensystemsmedia.com

CREATIVE PROJECTS Chris Rassiccia crassiccia@opensystemsmedia.com

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

REPRINTS

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

Visiting Old Ironsides

By John McHale, Editorial Director



One of the benefits of living near Boston is the proximity to U.S. history, especially the USS Constitution, the oldest commissioned ship in the U.S. Navy. Visiting the ancient warship, also known as Old Ironsides, is an activity I prefer to do on a quiet Sunday morning before the tourists hit, as I did this August.

The Constitution had been in dry dock for just over two years undergoing an extensive restoration and had only been out in the water for a week when I visited that recent morning. She looked glorious.

I'd forgotten how much I enjoyed visiting the ship. Looking up at the flags on the masts – Old Glory and the Don't Tread on Me flag (Figure 1) – to the gun placements and the Captain's quarters below, you get a sense of history that is only enhanced by the presence of the current crew: active-duty U.S. Navy personnel who double as historians.

I asked the sailors how much of the original ship is left and was told only about 12 percent remains from the original ship, most of that in the hull. That 12 percent is more than 200 years old (Figure 2).

Commissioned in 1797 and named by President George Washington as the third of eight ships slated to be built under the Naval Act of 1794, the USS Constitution was undefeated in battle and gained its fame during combat with the British Royal navy during the War of 1812, earning her nickname when she defeated the HMS Guerriere. Just as I did, visitors can learn much of this history in the USS Constitution Museum, a non-profit entity located across from the ship, but not run by the Navy. If you want to learn more about the Battle of 1812 and the Constitution's role in it, I recommend reading "1812: The War That Forged A Nation" by Walter R. Borneman.

The latest restoration – and the first in more than 20 years – was performed

by restorers and riggers from the Naval History & Heritage Command Detachment Boston. No electronics engineers needed. The work included:

- › Replacing the lower hull planking and caulking
- › Removing and replacing 2,200 sheets of copper
- › Refurbishing and replacing the ship's rigging, upper masts, and yards
- › Rebuilding sections of the cutwater and trailboards on the bow
- › Refurbishing and rebuilding the gun carriages

Sailors on board told me that she will set sail some time this fall around Boston Harbor. If you're in town at that time, be sure not to miss her sail. If you do tour the ship, make time to engage her crew, as they are friendly experts and happy to answer every question.

The crew is also a group of overachievers, as competition for serving on the USS Constitution is fierce. The sailor I spoke to told me she came right out of boot camp and her duty will be two years, while those who earn the spots from the fleet serve on board for three years.

According to the Navy's website for the USS Constitution (www.navy.mil/local/constitution/), Navy personnel looking to serve onboard "must be able to interact with the public with maturity and tact, and be an exceptional representative of the U.S. Navy. They must have an impeccable appearance and exceptional military bearing. Chief Petty Officers and Petty Officers must be high-caliber individuals ready to serve as sharp military role models for junior crew members and strong leaders."

It is a great honor for sailors and officers to earn this duty. While the ship never goes to battle and doesn't deploy to foreign waters anymore, it remains revered within the Navy and within the

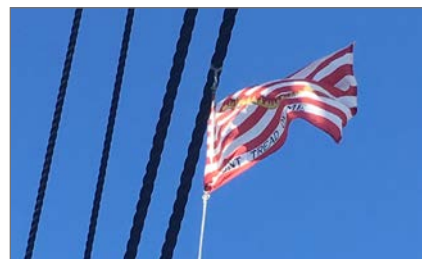


Figure 1 | Don't Tread on Me.



Figure 2 | USS Constitution.

U.S. military. For Navy personnel interested in serving on Old Ironsides, visit www.navy.mil/local/constitution/new_sailors.asp.

During your conversations with them about the Constitution's exploits be sure to thank the crew for their service, too, and for that matter, every serving man and woman you meet. They earned it.

And if you want to back that "thank you" up with money or time, I recommend checking out the charity we highlight in this month's issue on page 46. Each issue, we highlight a different military charity and provide a donation, giving back to those who help protect us.

Some of the charities we've highlighted include Wounded Warrior Foundation, the Folds of Honor Foundation, Operation Homefront, the Navy Seal Foundation, Operation Delta Dog, the Navy-Marine Corps Relief Society, and many more. To view our list of supported military charities, visit www.mil-embedded.com/topics/charities/.

Ethernet switches: Smarter than you think

By Charlotte Adams

An Abaco Systems perspective on embedded military electronics trends



Ethernet switches are so fundamental to our connected world that they sometimes get taken for granted. Attention focuses on splashy end products – like weapons systems and the gee-whiz applications that drive them – rather than on the lower-level components that actually make the applications work.

As networks become more pervasive in aerospace and defense platforms, Ethernet technology is coming into its own, both as the common denominator between different bus dialects and – increasingly – as the basic communications framework for data processing.

High-end applications like synthetic aperture radar (SAR) suck in massive amounts of data, which must be processed rapidly in order to be useful. This reality drives the need for lightning-fast data exchange between processing nodes and calls for the speediest switches. In another situation, combat-vehicle situational awareness applications might prize size, weight, and power efficiency over sheer speed. At both ends of the spectrum, military users want highly granular switch control. Both types of applications have benefited from the technology's evolution.

Switch evolution

As Ethernet technology has proliferated, switch products have adapted to fill each niche in the ecosystem. There are low-bandwidth/low-power units, managed and unmanaged switches; commercial hardware; standalone, hardened tactical switches; and higher-throughput backplane cards. Speeds range from a single gigabit/sec up to 40 gigabits/sec per port.

The hardware has shrunk from large boxes to easy-fit backplane cards and small ruggedized units. Finer-grained lithography has enabled semiconductor manufacturers to squeeze more transistors onto chips, increasing speed and performance while reducing power draw.

This shrinking of transistor size drives integration, allowing more functions to be incorporated into a piece of silicon via system-on-chip (SoC) configurations. SoC-style switches enable designers to integrate conventional processors into the chip set of the specialized switching silicon, which is the “switch fabric” that decides how, when, and where to forward incoming data packets.

SoC switches mean that functions such as switch management can be handled by the switch fabric without a separate CPU. Finer-grained lithography means that the switches can be smaller or can feature more ports. From a systems perspective, higher port density means fewer required switches, thereby reducing overall power consumption and physical footprint.

Software side

Switches come in many flavors, some more attuned to military needs than others. Take managed versus unmanaged units, for example: Unmanaged switches are designed to let nodes communicate in a predetermined manner; a managed programmable switch, by contrast, is more flexible and more controllable, and therefore is more suited to military needs.

Managed switches can be configured and reconfigured and allow a high level of user control, with features such as traffic monitoring, security, priority/sensitivity handling, failover mechanisms, and built-in test.

In the security domain, managed switches can provide access control to individual ports, data on users connecting to and disconnecting from the ports, denial-of-service protection, and filtering of untrusted messages.

Illustrating the range of today's switch technology are the RES3000 rugged enclosure and the SWE540 6U VPX card



Figure 1 | The Abaco RES3000 is a fully managed Ethernet switch offering as many as 28 ports.

from Abaco Systems, both of which run Abaco's OpenWare switch-management software. The RES3000 is a tactical switch, with 12, 24, or 28 Ethernet ports (Figure 1), while the 6U VPX SWE540 data plane Ethernet switch provides as many as twenty 40 gigabit/sec ports.

Military versus commercial

While Ethernet switches abound, the military has some special requirements that benefit from in-depth, software-based control. One example is that the military uses multicast – or one-to-many – which is less common in a commercial environment such as telecommunications.

Another specialized military requirement is the absolute demand for security. Therefore, military users must have such features as access control not only in operations, but also in maintenance, so that only the person with the proper authority can change the system's configuration.

The military also focuses on more than keeping a connection up: For adequate command and control, the military user has an urgent need to know why and where a node went down and to instantly restore bandwidth. A combat-vehicle operator can't afford to go blind for even a moment if the switch controlling external vision fails.

www.abaco.com

Ethernet for synchronization: It's about time

By Andrew McCoubrey

An industry perspective from Curtiss-Wright Defense Solutions



Today's embedded systems often include several counters and clocks that keep track of time, and ensuring that they are accurate – and synchronized across multiple devices – can be critical. For example, synchronized clocks can be used to partition shared resources (such as network links) in distributed systems with critical real-time requirements.

Most computers connected to the Internet use the Network Time Protocol (NTP) to set their clocks, obtaining the time of day from a remote server. NTP servers on the Internet get their time source from one of the authoritative servers connected to an atomic clock. In turn, these servers can relay time data to other NTP servers or clients.

To synchronize with an NTP server, a client first sends a request, then waits for the reply; both the request and reply may need to traverse several hops in the network, suffering delays caused by switches and routers in the path. These delays can add up: When a client receives a time of day response from an NTP server, it may already be hundreds of milliseconds old. While a millisecond may prove trivial in many everyday applications, that delay can be a matter of life and death in deployed command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems.

GPS receivers, with a highly accurate time of day provided by atomic clocks via satellite, can also serve as a useful reference clock. Because many GPS receivers output time of day over a serial port, they are typically only useful for synchronization to within a few milliseconds. To enable high-precision synchronization, many GPS receivers require a so-called 1PPS (one pulse per second) output. This interface produces a pulse once per second, at the top of the second. Using this approach, a clock can be synchronized with an error of as little

as one nanosecond (ns), or a billionth of a second.

One downside for embedded systems, however, is that dedicated hardware must be provided to process the 1PPS signal. In addition, the serial port and 1PPS must be routed to each client device. In larger systems, this can involve significant complexity and cabling. The IEEE 1588 Precision Time Protocol (PTP) – which addresses the limitations of NTP and GPS for synchronization of systems on a local network – can provide submicrosecond synchronization. When all devices in the network provide full hardware support for the latest PTP standard, synchronization within a few ns is possible.

PTP was first promulgated as PTPv1 (1588-2002) in 2002; a major update in 2008 resulted in PTPv2 (1588-2008). The 2008 standard redefined the format of the PTP messages, so the two versions are incompatible.

Since PTP is typically deployed on local networks, any delay is generally smaller and more predictable than when synchronizing using NTP over a wide area network (WAN). However, variable delays due to queueing and processing are present even on high-performance Ethernet switches. To address this situation, PTPv2 introduced the new concept of a "transparent clock." A switch with transparent clock support notes the time that it receives a PTP packet on an ingress interface, and notes it again when the packet is transmitted on an egress interface. The switch can then inform the PTP message recipient of the delay introduced by the switch. In this way, network delay can be fully eliminated as a source of synchronization error.

Although implementing PTP in embedded systems can be as simple as installing a software client, to achieve



Figure 1 | Curtiss-Wright's VPX3-652 Ethernet switch is an example of an IEEE 1588-2008 PTP implementation. When configured as a transparent clock, it uses integrated timing hardware to measure and report packet transit time, enabling submicrosecond sync across the network.

the highest levels of synchronization, designers need more than just software. PTP packet processing in hardware is a common feature in most of the latest PHY devices and Ethernet adapters. When combined with an appropriate driver, support for PTP in networking devices provides application software with access to a high-precision clock that is synchronized to other modules in a system.

Applications that require data to be time-stamped with high precision may call for specialized hardware (for example, in a field-programmable gate array [FPGA]) that can sync with the PTP clock directly. For this reason, many PTP-capable adapters and physical layers (PHYs) will output a hardware signal (similar to the GPS 1PPS) that can be used to drive timing-aware hardware. (Figure 1.)

Maintaining accurate time is critical for many embedded computing applications. With components that feature support for IEEE 1588 PTP, synchronization can be as simple as connecting to the network.

Andrew McCoubrey is the product marketing manager, switching and routing solutions, for Curtiss-Wright Defense Solutions.

www.curtisswrightds.com



DEFENSE TECH WIRE

NEWS | TRENDS | DOD SPENDS | CONTRACTS | TECHNOLOGY UPDATES

By Mariana Iriarte, Associate Editor



NEWS

Navy, Lockheed Martin test Aegis Combat System against ballistic missiles

The USS John Paul Jones – with support from the U.S. Navy, the Missile Defense Agency, and Lockheed Martin – successfully fired two Standard Missile-6 (SM-6) Dual I missiles against a medium-range ballistic missile target from the Aegis Combat System, according to Lockheed Martin officials.

During the recent test, the system detected, tracked, engaged, and launched both missiles to intercept a medium-range ballistic missile target. The test, called Flight Test Standard Missile-27 Event 2 (FTM-27 E2), demonstrated the system's updated software capabilities.

SM-6 offers over-the-horizon offensive and defensive capability by using the previously designed Standard Missile airframe and propulsion system to support anti-air warfare, anti-surface warfare, and sea-based terminal ballistic missile defense.



Figure 1 | A medium-range ballistic missile target is launched from the Pacific Missile Range Facility on Kauai, Hawaii. Photo courtesy of the Missile Defense Agency.

Northrop Grumman awarded \$265 million USAF airborne communications contract

Northrop Grumman has won a contract worth \$265 million from the U.S. Air Force to handle aircraft maintenance and logistics support of the Battlefield Airborne Communications Node (BACN) system. BACN is a high-altitude, airborne gateway that translates and distributes voice communications and other battlespace information from different incoming sources. The BACN system bridges the gaps between those systems and extends communications among disparate users and networks to provide improved situational awareness.

Under the terms of the contract – a base year contract with four option years – Northrop Grumman will support four BACN E-11A aircraft. The work is a continuation of an existing five-year maintenance contract set to terminate in January 2018.

L3 WESCAM tasked to deliver its imaging turrets in \$49 million contract

The U.S. Naval Surface Warfare Center, Crane Division (NSWC Crane) selected L3 WESCAM for an indefinite-delivery/indefinite-quantity (ID/IQ) contract to deliver its MXTM-10MS electro-optical and infrared (EO/IR) imaging turrets for the Military Sealift Command Situational Awareness System program. The contract is worth an estimated \$49 million.

NSWC Crane will integrate the systems into a larger overall solution in support of the situational-awareness system requirement for the Military Sealift Command Electro-Optical System (MSC-EOS) program.

In addition to MXTM-10MS systems, the ID/IQ can further be exercised for the purchase of ancillary equipment, product training courses, and customizable in-service support programs. The Canadian Commercial Corp. will execute the contract.

USMC awards General Dynamics \$105 million command and control contract

The U.S. Marine Corps has awarded General Dynamics Mission Systems a full-rate production contract for the Common Aviation Command and Control System (CAC2S) program, a command and control system that visually combines ground and aviation command and control data for greater situational awareness and faster decision-making.

The CAC2S contract is worth approximately \$105 million over four years.

CAC2S – which consolidates the existing functionality of the seven Marine Air Command and Control Systems into a single system – was developed using an open architecture approach, which General Dynamics Mission Systems officials say enables easier technology insertion, quicker capability enhancements, and more intuitive learning for users.

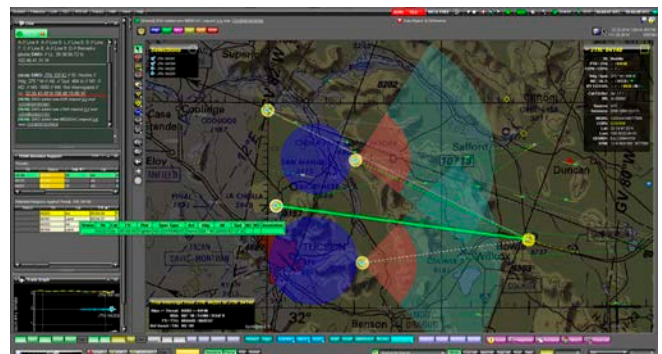


Figure 2 | Screenshot of the Common Aviation Command and Control System (CAC2S) courtesy of General Dynamics.

Teams selected for Phase 1 of DARPA's mobile force protection program

The Defense Advanced Research Projects Agency (DARPA) has selected three companies for Phase 1 of the agency's Mobile Force Protection (MFP) program, which aims to expedite the development of counter-small, unmanned aircraft systems (sUAS) capabilities and their near-term introduction to the field.

The three companies are Dynetics in Huntsville, Alabama; Saab Defense and Security USA in East Syracuse, N.Y.; and SRC in North Syracuse, N.Y. The MFP program is aiming for three phases of work punctuated by open-air demonstrations involving increasingly sophisticated threats and scenarios. The goal is for the technology demonstration system to show initial functionality at the end of Phase 1 and progressively improve, culminating in a full-capability demonstration on a moving vehicle or vessel by the end of Phase 3.

At the conclusion of each open-air demonstration, DARPA plans to offer the armed services and other U.S. government agencies the opportunity to fund extended field evaluations of the current technology demonstration system.



Figure 3 | DARPA's Mobile Force Protection (MFP) program seeks to develop defense systems and component technologies to improve real-time protection of ground and maritime convoys against various small unmanned aircraft system (sUAS) threats. Photo illustration courtesy of DARPA.

New nuclear missile design concepts to be matured by Lockheed Martin, Raytheon

U.S. Air Force officials selected Lockheed Martin and Raytheon to mature design concepts and prove developmental technologies for the Long Range Stand Off (LRSO) missile program.

Each company was awarded a contract of approximately \$900 million, with an approximate 54-month period of performance. Upon successful completion of the contracts, the Air Force Nuclear Weapons Center will choose a single contractor for the Engineering and Manufacturing Development and Production and Deployment phases of the program.

The new design will replace the aging AGM-86B Air Launched Cruise Missile with modernized weapon capabilities designed for its nuclear bomber fleet, to include the B-21, according to the Air Force.

Virtual training hub at Mayport supports east coast LCS crews

The U.S. Navy has installed several new virtual trainers to help instruct sailors in their homeport location while a formal training center is constructed on base as it works to support the growing group of littoral combat ship (LCS) crews being stationed on the U.S. east coast.

Two simulators and a virtual reality lab (VRL) recently opened in existing buildings at Mayport. Installation of these interim trainers was accomplished using seed money from the LCS Fleet Introduction and Sustainment Program Office (PMS 505), the LCS class in-service program management office within the Littoral Combat Ships Program Executive Office (PEO LCS).

The 18-seat VRL launched its first class in early August with the LCS Engineering Plant Technician (EPT) course, which trains the sailors with 626 individual lessons including those on ship familiarization, propulsion generation, common machinery maintenance, waterjets, and watch challenges. Seated in front of three-screen workstations, sailors wear headsets to communicate with their instructors as they control avatars to accomplish tasks and procedures just as they would on board an actual warship.

Point Mugu Sea Range adds system to aid in weapons test, development

The U.S. Navy's Point Mugu Sea Range (Ventura County, California) has adopted a new directed energy test atmospheric-based system that may turn out to revolutionize the Navy's ability to measure and predict weather conditions on the range, which is a critical factor in supporting the test and development of weapons systems.

The Integrated Atmospheric Characterization System (IACS) is a land-based survey tool that measures complex weather features and conditions that could affect laser propagation, such as optical turbulence, transmissivity, and water vapor levels.

IACS uses two LIDAR [light detection and ranging] systems to help measure and characterize atmospheric conditions, determine boundary heights, and serve as a so-called super ceilometer, providing finely resolved cloud base height and tilt measurements for test engineers and operators.



Figure 4 | IACS is a land-based survey tool that measures complex weather features and conditions that might affect laser propagation, such as optical turbulence, transmissivity, and water vapor levels. Photo courtesy of the U.S. Navy.

SDRs and designing for flexibility

By Brandon Malatest

The design of radio equipment for the military market has evolved significantly from the use of transistor-based circuits to specialized and powerful integrated circuits (ICs). Designs may be geared towards rigid, single-purpose platforms or towards flexible, application-agnostic systems with dedicated digital signal processors (DSPs), such as software-defined radio (SDR). The one thing all of these approaches have in common: difficulty in estimating and understanding the cost/performance trade-offs of new designs.



Master Corporal François Leclerc (left) and Corporal Frederic Morin – radio operators from 12e Régiment blindé du Canada – link radio communication channels prior to heading out on patrol during a sovereignty operation in Nunavut (northernmost territory of Canada) during early 2017. Photo courtesy of Canadian Armed Forces/P02 Belinda Groves, Task Force Imagery Technician.

As the complexity of wireless systems increases, so does the challenge of determining the most efficient design to meet current and potentially future needs while remaining cost effective. Nearly all new designs – including radar, electronic warfare, communications, and signals intelligence (SIGINT) – face this dilemma, where a marginal increase (or savings) in cost could have a disproportionate impact on the performance of the system.

These trade-offs are sometimes evaluated against commercially available solutions; this approach, however, typically results in overengineering of the system and incurring significant associated costs. It can also often result in a performance hit through suboptimal decisions based on the only available platforms.

SDR aims to address this trade-off issue, but even in these designs many compromises are necessary based on performance and costs. While it seems straightforward to design a product that exceeds performance requirements across all areas, this approach often results in unnecessary and extreme cost overrun.

Designing SDRs

When designing SDR platforms, there are typically six crucial elements that designers need to consider that can both drive the architecture and limit the utility of the platform (Figure 1). These elements include transmit and/or receive functionality, operating frequency, number of radio chains, instantaneous RF [radio frequency] bandwidth, FPGA/DSP [field-programmable gate array/digital signal processor] resources, and digital backhaul. In addition to these standard elements, some applications may have other requirements as well that need to be considered, including RF performance, latency, synchronization, and the like.

Not all SDR platforms provide receive and transmit functionality; the decision to proceed with either one or both is dictated by the end application. These different options can have a large or trivial impact on the overall cost of the system, depending on the architecture. For example, a platform that is modular in design will typically offer transmit as well as receive functionality, as the system will already have the resources required for both (that is, system clock, FPGA/DSP resources, digital backhaul, etc.).

In the past, radios were designed for a dedicated purpose on a dedicated frequency band (or bands). With SDR, this process is not as simple, and designers need to determine the upper and lower bounds of frequencies to support. Many times this frequency decision is driven by a specific application, such as VHF/UHF radios, while other times it is decided based on available integrated transceiver chips, such as the LMS7002M that operates from 100 kHz to 3.8 GHz. Finally, there are some that aim to extend the utility of the SDR by extending the operating frequency as much as possible while not exceeding a cost threshold.

www.mil-embedded.com

WHEN DESIGNING SDR PLATFORMS, THERE ARE
TYPICALLY SIX CRUCIAL ELEMENTS THAT DESIGNERS NEED
TO CONSIDER THAT CAN BOTH DRIVE THE ARCHITECTURE
AND LIMIT THE UTILITY OF THE PLATFORM. THESE ELEMENTS
INCLUDE TRANSMIT AND/OR RECEIVE FUNCTIONALITY,
OPERATING FREQUENCY, NUMBER OF RADIO CHAINS,
INSTANTANEOUS RF [RADIO FREQUENCY] BANDWIDTH, FPGA/
DSP [FIELD-PROGRAMMABLE GATE ARRAY/DIGITAL SIGNAL
PROCESSOR] RESOURCES, AND DIGITAL BACKHAUL.

to consider is the number of radio chains. This metric enables the user to not only receive/transmit on different frequency bands simultaneously, but it can also be necessary for multiple input/multiple output (MIMO), radar, and communication applications. These applications typically require phase coherency and/or additional radio capacity that a single channel cannot offer due to bandwidth limitations.

High instantaneous RF bandwidth is critical for some users and not as useful for others. Luckily, this specification is dictated by the converters on board (i.e., analog-to-digital and digital-to-analog converters). These converter devices provide different options for sample rates, which drives the maximum instantaneous RF bandwidth along with the overall costs of the system.

In a radio design, once the signal reaches the digital domain, one of the most important aspects to consider is the available DSP resources offered. Many SDRs utilize FPGA ICs in their design to offer flexibility for different design requirements and usually a migration path to upgrade the FPGA when more resources are required.

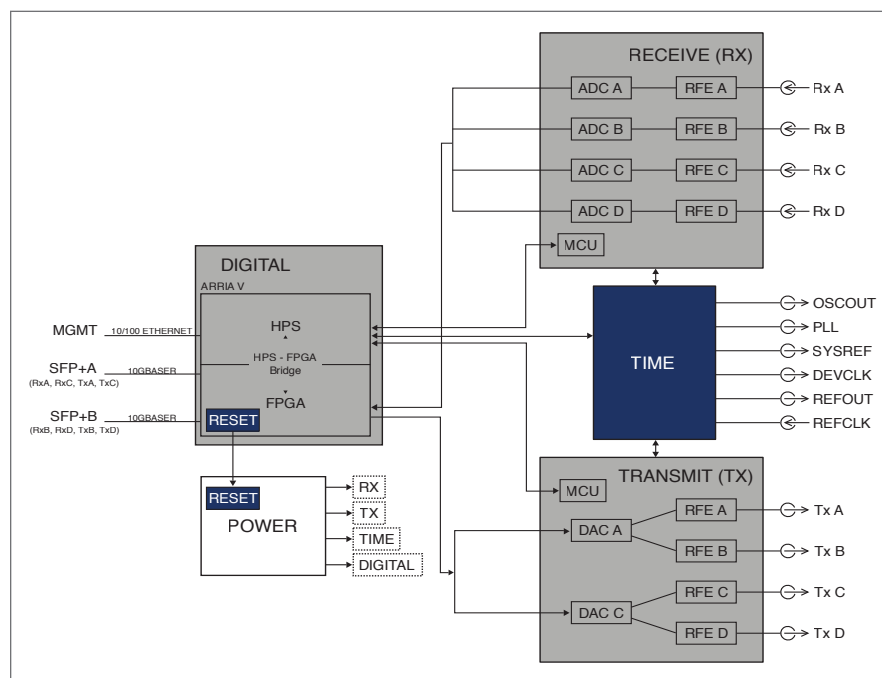


Figure 1 | SDR platforms typically incorporate six crucial elements: transmit and/or receive functionality, operating frequency, number of radio chains, instantaneous RF bandwidth, FPGA/DSP resources, and digital backhaul. Diagram courtesy Per Vices.

The other important characteristic to consider for the digital system design is the digital backhaul; how data will be sent and received to and from a host system. In some designs, this feature is tied to the instantaneous RF bandwidth since the data received is sometimes not processed onboard the unit and needs very high data-transfer rates to send to a host system. Typical digital backhauls include PCIe, 1G Ethernet, and 10G Ethernet.

To address the problem of estimating cost/performance trade-offs in the defense radio space, one approach provides designers with access to real-time cost estimates associated with different platform parameters. The "Build Your Own SDR" tool from Per Vices uses various algorithms to meet a variety of customer requirements. The tool's categories, parameters, and available range enable selection of the most performant system, if desired, or selection of only the bare criteria required for an application.

Decisions, decisions

Wireless systems designed and used by the defense market vary drastically, whether in communications and networking, radar, (counter) electronic warfare, or signals intelligence. Each of these systems require different specifications based on the application. For example, communication and networking equipment typically requires high bandwidth and encryption, while radar requires greater emphasis on the RF performance of the system, including noise figure, sensitivity, isolation, and dynamic range. These decisions driving the design of wireless systems are challenging. Such complexity in the military-radio market will only increase as new electronic components become available, users demand higher performance, and new technologies come on line. **MES**



Brandon Malatest graduated from the Honours Physics program at the University of Waterloo, where he spent the

majority of the time in experimental physics. Upon graduating, he started a career as a research analyst at one of the largest market research firms in Canada. He is now one of the co-founders and COO of Per Vices Corporation, a Canadian company headquartered in Toronto, Ontario, developing high-performance software-defined radio (SDR) platforms that are designed to meet and exceed requirements across multiple markets. Readers may reach the author at Brandon.m@pervices.com.

Per Vices Corporation
www.pervices.com

AIRBORNE, SHIPBOARD, GROUND MOBILE DATA RECORDING AND DATA STORAGE



**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



PHOENIX
INTERNATIONAL

www.phenixint.com 714-283-4800

Rugged flexible COTS Solutions from MPL

fully designed and produced in Switzerland

Highlights

- 10+ years availability
- 20+ years repairable
- Openframe up to IP67 enclosure
- OEM and customized solutions



Features

- up to i7 Quad Core, Xeon
- temp. -40°C up to +85°C
- all fanless at full load
- MIL-STD-810G/461F/1275D
- Switches, Routers, Fiber, Firewall w. source code



MPL AG 5405 Dättwil / Switzerland
Phone +41 56 483 34 34
U.S. Office
Phone +1 480-513-8979

MPL
High-Tech • Made in Switzerland
info@mpl.ch • www.mpl.ch

WHERE TECHNOLOGY EXPERTS GATHER



MARKET TRENDS, TECHNOLOGY UPDATES, INNOVATIVE PRODUCTS

Military Embedded Systems focuses on embedded electronics – hardware and software – for military applications through technical coverage of all parts of the design process. The website, Resource Guide, E-mags, and print editions provide insight on embedded tools and strategies such as software, hardware, systems, technology insertion, obsolescence management, and many other military-specific technical subjects.

Coverage includes the latest innovative products, technology, and market trends driving military embedded applications such as radar, sonar, unmanned system payloads, signals intelligence, electronic warfare, C4ISR, avionics, imaging, and more. Each issue provides readers with the information they need to stay connected to the pulse of embedded technology in the military and aerospace industries.

Military
EMBEDDED SYSTEMS
mil-embedded.com

Software-defined networking: On-the-fly agility, security

By Sally Cole, Senior Editor

When it comes to securing the Department of Defense's massive networks, software-defined networking (SDN) can help protect vulnerable legacy and custom-developed network infrastructure.

The U.S. Department of Defense (DoD) operates one of the largest and most complex networks on the planet, which poses unique security challenges.

During the Air Force Association's 2017 Air, Space, and Cyber Conference in September, Navy Admiral Michael S. Rogers, commander of the U.S. Cyber Command and director of the National Security Agency, pointed out four key areas that the DoD is focusing on defending: networks, platforms, weapons systems, and data.

Much of what goes on to protect the DoD's network is classified, but embedded systems are surely among its greatest security challenges. "DoD networks are global in scope and support absolutely critical operations," says Dr. Dennis Moreau, senior engineering architect, networking and security, for VMware in Palo Alto, California. "When they aren't working, people are at risk. And these networks contain many devices developed under contract, such as specialized signals processing and specialized communications ... across the board to embedded sensors, field-programmable gate arrays (FPGAs), and all sorts of new electronics 'at the edge.'"

One of the problems these enormous networks bring is that "when endpoints are idiosyncratic, custom-developed, or developed under contract, it's difficult to go find a patch for something that was built maybe 10 years ago, but has since become an absolutely essential part of the network infrastructure," Moreau adds.

The DoD's massive network has evolved over a long period of time, so this requires bringing together many unique endpoints. "If we consider the military network with embedded systems writ large, I'm not sure there is anything more complex – from a configuration-management, security-management perspective, sort of 'defense across asset evolution,'" Moreau says.

If you think it would be a complete nightmare to try to secure all of these networks and devices, you're right. "Its complexity is also due to the unique challenges that the military has with regard to staffing," Moreau points out. "Folks go in and get very good at something and then move on, because it's 'up or out' in terms of promotion."

Third parties or contractors provide a level of continuity, but their roles and contracts also change over time, so it can be difficult to get a clear, long-term definition of what their roles are, what their organizational entitlements are, and what normal behaviors are when you have all of these dynamics and very evolved systems with global reach in place. "You can see how situations in which contractors gain too much access and are able to do things that would otherwise seem extraordinary – like exfiltrating gigabytes worth of data – can happen within this kind of environment," Moreau notes.

What role can SDN play in network security?

Again, much of what the DoD is doing in terms of network security is secret or classified, but 2017 budgets for the Army, Navy, and the Defense Information Systems Agency (DISA) all include mentions of software-defined networking (SDN).

"We're seeing significant initiatives within the Defense Department to cultivate 'software-definedness,'" Moreau says. "One of the biggest is DISA's decision to move the inter-military branch networks to a software-defined basis."



SDN is essentially a stack architecture designed with security as its foundation, which separates the network-control plane from the data-forwarding plane and centralizes it within a controller that defines forwarding behavior through higher-level policy. Northbound application programming interfaces (APIs) sit atop the controller and present a network abstraction interface to the applications and management, while southbound APIs allow the controller to define switches' behavior at the bottom of the SDN stack. The key to SDN is the separation of data and control planes.

"DISA and individual military branches have been looking hard at the recognition that there really isn't a 'finish line' here because SDN is evolving," Moreau says. What this means is that they need an infrastructure that gives them a level of agility to respond to what they see as it's happening.

"The 'software-definedness' of the networking and 'plumbing' – even software-defined radio and systems that provide battlefield frontline connectivity – is all in recognition of the fact that what you need to do often isn't well defined before you need to do it, so you need the ability to be agile and to shape your infrastructure to accommodate whatever it is that you need to do," he continues.

All embedded technologies that were built under contract and may be old, or were custom-developed and don't have a consistent place to go for security patches, can be protected via SDN. "You can wrap a logical network right around those custom-developed capabilities – whether it's a device, a sensor, or a system – to give it state-of-the-art protection in terms of its network and intrusion prevention system (IPS) capabilities," Moreau explains.

SDN provides the flexibility of "potentially giving every custom system its own network, which can then be protected appropriately, without having to change the underlying system behind the scenes," he says. "You can give it its own protection policy, allowing you to decide what should and shouldn't go into and out of an application, placing the controls right on its boundary. So you can extend the secure operational lifetime of some of these older or custom technologies."

PICO

SURFACE MOUNT
(and thru-hole)
Transformers & Inductors

**Size
does
matter!**

from
low-
profile



.18"ht.

- **Audio Transformers**
- **Pulse Transformers**
- **DC-DC Converter Transformers**
- **MultiPlex Data Bus Transformers**
- **Power & EMI Inductors**

**AS9100C
CERTIFIED
TUV**

**VISIT OUR EXCITING
NEW WEBSITE
www.picoelectronics.com**

**See Pico's full Catalog immediately
www.picoelectronics.com**

800 431-1064
Fax 914-738-8225
E Mail: info@picoelectronics.com

PICO Electronics, Inc.
143 Sparks Ave. Pelham, N.Y. 10803-1837

Delivery - Stock to one week

For example, you can give an embedded radar system on a naval ship its own network, protection, and policy, so that those policies will be a concise set of policies, aligned to whatever changes occur on that system and vulnerabilities discovered over time. "No need to change the system that may have been built five to ten years ago," Moreau says. "Many aspects of 'software-definedness' that make security better in defense, military, and embedded scenarios are also being leveraged in the enterprise."

Another bonus is that compelling sustainable costs come from SDN because it allows the user to essentially host legacy capabilities on modern technologies. "Also, by reducing the complexity, the same system that can host Linux can also host Windows and very old Windows – and provide state-of-the-art protections to it by having modern firewalls, IPS, web application firewall (WAF), sandboxing ... sitting right in front of old versions of old applications on old operating systems," Moreau adds.

SDN visibility

One of SDN's biggest benefits is that it provides granular visibility when firewalls are placed on east-west traffic.

"Try doing this with hardware and you'll end up hairpinning the traffic out of the data center to some device on the outside and then back in. The latency, complexity, and selectiveness with which we have to do that really limits your visibility," Moreau explains. "But if I can put the firewall right on the logical boundary of the application, the virtual machine, or the embedded system, then my visibility is intrinsic and it scales with the number of workloads. More workloads, more protection, more visibility. Consequently, the ability to grope around for a victim and to move laterally within an environment once an initial infection occurs is no longer something that occurs in the dark."

There's still work to be done, because SDN needs effective analytics to pay attention to all of the new sensors' instances and boundaries within these environments and "to then make what we see to usable, again using the flexibility of the network to help to defend it," he says.

Going forward, SDN even enables advanced protections like moving target defense (MTD). "MTD is becoming more easily realizable because of things like 'software-definedness' and especially SDN, where we can proactively provision systems so that when we see something anomalous we can reprovision it," says Moreau says. "We can throw down a brand-new network, a brand-new machine, and provision an application on top of it from trustworthy sources, so that an infected one can be rolled off [for investigation] and a new one rolled in. All this can happen by using the dynamics you get from 'software-definedness' you get as a protection mechanism."

Putting SDN to work

If you simply take an existing network topology and implement it on "software-defined" technology and don't change the logical topology at all, you won't get the ability to wrap a network around those legacy or custom solutions or get the more granular protection, visibility, and additional flexibility it provides, Moreau says.

Taking advantage of SDN requires investing in the definition of granular security posture, the policy you want to place on the boundary of those applications and systems to get tighter "least-privileged protection, preventing ad hoc abuse of loose permissions and access controls," he adds.

It involves characterizing all of the systems, both legacy and current – to decide how they should and shouldn't behave (for example, decide what the firewall rules on its boundary should be; what the SNORT [a network-intrusion prevention system] rules on the IPS on its boundary should be; what the MSRI rules on the WAF should be to stop cross-site scripting).

THE McHALE REPORT



The McHale Report, by mil-embedded.com Editorial Director John McHale, covers technology and procurement trends in the defense electronics community.

ARCHIVED McHALE REPORTS AVAILABLE AT:
WWW.MIL-EMBEDDED.COM/MCHALE-REPORT

"This requires knowing what the system is supposed to do," Moreau cautions. "So you need to do that work and documentation so that it's current and maintained to be able to take advantage of the cost and capability advantages of SDN."

None of this happens by accident. "It takes effort and involves cost – but the cost is repaid in spades in terms of efficiencies, life cycle costs, and more effective protection," Moreau asserts.

Attacks on SDN controllers/hypervisors

Two of the security concerns people have expressed about SDN are that its controllers and hypervisors can be attacked. Know what stops that conversation almost immediately? "For decades, we've had hardware-based network protections and control and it doesn't seem to have stopped massive breaches," says Moreau says.

With software-defined controllers, if you find a flaw, when something isn't behaving the way you want, you can rapidly address it. "This isn't the case with a bunch of hardware devices scattered across the globe and synchronized in different ways, using an operating system designed exclusively to run, for instance, routers and firewalls. Those have a long history of having challenges with respect to security themselves," he explains. "No software artifact ever built was perfect. The question is: Does it have the resilience to have a vulnerability or exploit occur and the ability to continue operating with integrity? This is where 'software-definedness' comes into its own."

The same goes for hypervisors because no underlying processors are perfect. "We've seen issues, for example, in IOMMU [input-output memory management unit] addressing in TMP firmware, in control flow, in controllers using DMA, and on," Moreau notes. "The very same issues can cause problems with hardware ISPs and firewalls, or anything else used for isolation or protection. The big advantage is that, with SDN, we can do something about it."

Agility and resilience

SDN's ability to cultivate situational awareness comes in the form of "actionable context and flexible response – workloads that we can move, networks on which we can ratchet down security posture or adaptively change the isolation boundaries," says Moreau.

This agility "results in resilience that lets us do something about flaws when and if they come up," he continues. "So it's not a matter of getting to a point where there are no flaws in hypervisors, network controllers, or underlying hardware in firewalls – physical or virtual. It's all about being able to see when something is wrong and being able to effectively respond." Having the flexibility to correct problems and adapt to them while continuing to leverage the system to do what you need it to do is "what resilience is really about," Moreau concludes. **MES**



Great Things Do Come In Small Packages

- 4th Gen Intel® Core® i7 Haswell CPU
- Shock and vibration-tested (MIL-STD-810G)
- MIL-STD-38999 high-density connectors
- IP67 sealed against dirt and water
- PMC/XMC expansion
- SWaP-optimized
- Advanced thermal management
- Optional removable solid state drives with RAID support

The ARCX rugged mission computer offers great flexibility to meet ever-changing requirements with unique expansion features.

We have the I/O to meet your application requirements:

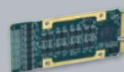
- FPGA
- Analog/Digital
- Counter/Timer
- Serial Communication
- Multifunction I/O
- 10-Gigabit Ethernet

Visit Acromag.com/ARCX TO LEARN MORE

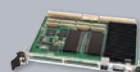
Embedded Computing & I/O Solutions



FPGA Modules



AcroPack® I/O Modules



VME SBCs



AcroExpress® VPX SBCs

www.acromag.com | solutions@acromag.com | 877-295-7088



Where did that software come from?

By Russell Doty

Where did the software on your embedded system come from? Can you prove it? Can you safely update systems in the field? Cryptography provides the tools for verifying the integrity and provenance of software and data. There is a process as to how users can verify the source of software, if it was tampered with in transit, and if it was modified after installation.

Military systems are subject to many attacks, including attacks on the software supply chain that provides software to the system. To ensure protection against these attacks, managers should ask three questions: What is the source of the software components? Has the software been tampered with or modified? Can they prove it?

Cryptography solves this problem through software signing and hashing, which work together to verify sources and files. Software signing uses a public-key/private-key pair to verify the source of a piece of software. Software is signed with a private key, and the public key is then used to verify that the software was signed with that specific private key. Whether the signer and the software can be trusted is a separate discussion; software signing verifies the source of the software and that it hasn't been tampered with after being signed.

Hashing is a technique for processing a file or set of data of any length and producing a single fixed-length checksum

that is unique to that file. Any changes to the file produce a completely new checksum – for example, changing one bit in a 10 GB file will produce a different checksum. The popular (although somewhat weak) sha1 hash produces a 40-character checksum, while the more secure sha256 hash produces a 64-character checksum. With a file and its checksum you can verify that the file has not been corrupted or tampered with in any way. Hashes run quickly, even on large files, making them an effective tool for file verification.

These techniques can be applied to any file. It doesn't matter if the file contains source code, executable images, data, or other files; any file or set of data can be used.

Can source be controlled?

The starting point for all software is source code, which is typically written and modified over a period of time by multiple people and released as multiple versions and updates of a product. The code is spread across hundreds or thousands of files and is constantly changing. Effective code management uses a version-controlled code repository such as git1 (see it at <https://git-scm.com/>).

A git repository is a database of patches, each with a unique identifier. In git, this unique identifier is the hash of the contents of the patch – the result is that each patch is identified by its contents. Any changes to the contents of a patch are immediately visible, since the patch no longer matches its identifier.

A git patch includes information on the previous patch it is applied to and the identity of the person submitting the patch. Similar to a blockchain, git patches incorporate sets of backpointers based on encryption, making it impossible for someone to change the history without detection. Patches may also be signed using the techniques previously described, thereby verifying who made the patch. This technique is a useful tool in any environment that requires verification of contributions.



A version-controlled software repository is the foundation of any secure software-supply chain, as it provides a history of all changes to the software and who made the changes. It also provides reliable ways to build specific versions of a software package.

Building verifiable provenance

Using software from known and trusted sources is important to maintaining the integrity of your embedded system. But how do you know that a piece of installable software actually comes from known source code?

Source code repositories, combined with automated build systems like Jenkins2 (see at <https://jenkins.io/>), enable the user to build an executable image from a known set of source files. After an image is built, it can be signed and hashed by the build system. This allows the user to know both the source of the software and the exact build that produced the software. Routine builds are signed with test keys, whereas production builds are signed with a release key, require special authorization and approval, and are often signed on a separate secure system. This enables the user to determine both the source of a piece of software and whether or not it is an official release.

All files making up a piece of software are combined into a single package for distribution, installation, and updates. A packaging system used in Linux is rpm3 (see <http://rpm.org/>). An rpm is a single file that contains a compressed archive of multiple files plus the commands for installing, configuring, updating, and removing its associated application. An rpm file also includes a manifest of all the files in the archive, including their names, version numbers, and checksums. This manifest information is included in an rpm database, which maintains information on all rpm-based software installed on a system.

Software often includes third-party components. When these third-party components are included in an rpm, the rpm metadata and checksum ensure that this is the software that the vendor included. Third-party components should be signed to ensure their integrity; if they are simply passed through from the other vendor, they should be signed by the other vendor.

Typically, rpm packages themselves are signed. The tooling to create and sign rpm packages is included in Linux and should be used by everyone developing software, including in-house developers. The rpm installer by default checks to see that a package is signed with a known key before allowing installation. Attempts to install unsigned software or software signed with an unknown key will fail unless they are overridden. The rpm installer also checks the integrity of the package: If the contents of the package have been modified, either through data corruption or malicious tampering, the installation will fail.

The operating system vendor will include its public key in the operating system (OS). This addition enables the user to be sure that software packages, updates, and security errata are in fact from the OS vendor and have not been tampered with by any outside party.

The user must add the software keys for each approved vendor to the system. Depending on the particular security requirements, the user may need to take steps to ensure the validity of vendor keys, especially when downloading software from mirrors or other intermediate sources like system integrators. Keys should be obtained directly from the vendor website. Some go so far as to hand-carry hard copy listings of the key from a known source.

Moreover, signed rpm packages allows the use of unsecured transports such as the Internet or a CD-ROM through the mail, as the rpm tooling enables verification of the source of the rpm and whether it has been corrupted or tampered with.

Life after installation

Checking software before and during installation is a good start, but it's important to continue maintenance after installation is complete. What can be done to verify a running system?

A powerful feature of rpm is that it allows the user to verify the integrity of files on a running system. The rpm database includes the checksum for all files contained in each rpm. System utilities enable the user to calculate the checksum for each file on the system,

WHAT IS THE SOURCE
OF THE SOFTWARE
COMPONENTS? HAS
THE SOFTWARE BEEN
TAMPERED WITH OR
MODIFIED? CAN THEY
PROVE IT?

compare this to the rpm database, and identify any files that have changed. The rpm database is a fast and efficient way to do this. Another way to accomplish this is to go back to the signed rpm packages and use the checksums directly from the rpm. While this way is slower and requires access to the original installation files, it is quite secure.

Major Linux distributions use these techniques to ensure that they are installing and running unmodified software from a known source. Knowing the origin of all software installed on systems and whether or not it has been changed is vital. This knowledge is a powerful starting point for establishing and maintaining system integrity as systems in the field are deployed and updated. **MES**



Russell Doty is a technology strategist and product manager at Red Hat, focused on systems manageability and security, addressing both

technical and usability issues, as well as delving into the special characteristics of the Internet of Things. Russell has extensive background in high-performance computing, visualization, and computer hardware from previous positions at Digital Equipment Corporation and Compaq. Recent open source projects include the OpenLMI system-management framework and the OpenSCAP security automation system. Readers may connect with Russell at rdoty@redhat.com.

Red Hat
www.redhat.com

The network-centric approach: Solving the challenges of real-time battlefield communications

By Barry McElroy



Cpl. Jesse Croswell, with 3-2 Stryker Brigade Combat Team, 7th Infantry Division, sets up new communication equipment in a Stryker combat vehicle at Joint Base Lewis-McChord in Washington. The new equipment gives units a reliable mobile communications platform and enhances a commander's ability to exercise mission command. (U.S. Army photo by Sgt. James J. Bunn, 5th Mobile Public Affairs Detachment.)

To meet the challenges of 21st-century wartime communications, a new approach to collecting and using intelligence called network-centric warfare can provide military operations with information superiority. However, real-time information collection only works with a battle-ready wireless communication system.

Wars in the 21st century are fought asymmetrically – modern soldiers now fight an enemy who is everywhere and nowhere at the same time, who has not been trained in battle formations or military strategy, who does not wear a uniform or use WoRm formulas to calculate where to fire.

Soldiers must be constantly on their guard and ready to fight – and this need for always-on preparedness has changed the way the military collects and uses intelligence, giving rise to what's called "network-centric warfare" to provide advantages on the battlefield.

A network-centric approach to warfare links all military assets to each other and to decision-makers via computer, radio, and data networks, enhancing the way military objectives are accomplished because of information superiority. According to David S. Alberts, who formerly worked in the office of the Assistant Secretary of Defense for Networks and Information Integration, "A robustly networked force improves information sharing. Information sharing and collaboration enhance the quality of information and shared situational awareness. Shared situational awareness enables self-synchronization. These, in turn, dramatically increase mission effectiveness."¹

A Department of Defense (DoD) text adds that while war will always be characterized by "fog, friction, complexity and irrationality," network-centric operations provide increased awareness and more informed decision-making: "... Having a better near-real-time picture of what is happening ... certainly reduces uncertainty in a meaningful way."²

Doing so requires a true military-grade network that must provide continuous communication to in-motion and stationary personnel, vehicles, and equipment, giving

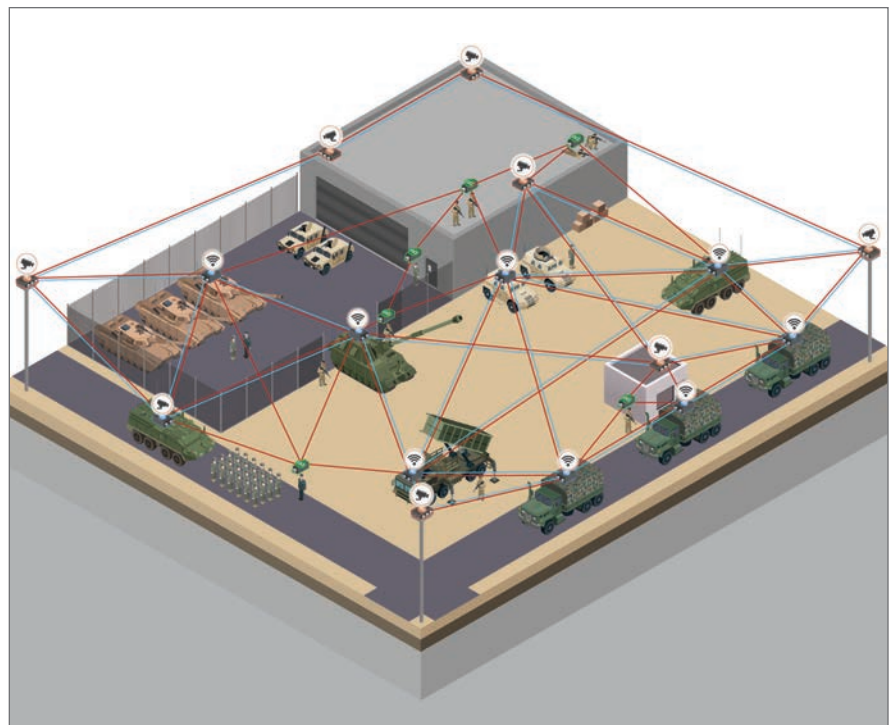


Figure 1 | A kinetic mesh wireless network instantaneously routes data between nodes via the best available traffic path and frequency. Illustration courtesy Rajant.

Solving battlefield communication challenges

A kinetic mesh wireless network combines wireless network nodes and networking software. Such a network uses multiple radio frequencies and any-node-to-any-node capabilities to instantaneously route data via the best available traffic path and frequency, with as fast as 300 Mbps transfer rates.

If a certain path becomes unavailable for any reason – due to antenna failure, for example – nodes on the network use an alternate route to deliver the data, eliminating any gaps in communication and enabling on-the-fly transmission of voice, video, and data to provide situational awareness, despite conditions that would cripple other networks. Routes are built automatically and are evaluated for quality and performance for every sent and received packet.

There is no central control node and no single points of failure. These self-healing, peer-to-peer networks support Wi-Fi, integrate easily with Ethernet-connected devices, and scale to hundreds of high-bandwidth nodes – in fact, the more nodes added, the more pathways are established and the more resilient a network becomes. The nodes are built to withstand hostile environments like battlefields. Each node serves as singular infrastructure, which enables everything within the network to be mobile: Wireless nodes can move, clients can move, network traffic can move – all in real time and without manual intervention.

A kinetic mesh network can be easily redeployed and expanded in multiple ways and still operate with the same level of reliability, even in the harshest conditions. Kinetic mesh eliminates the challenges of time-consuming, complicated deployments in the midst of battlefield pressures, challenging terrain, and changing operations. A soldier doesn't need extensive training to learn how to set up a radio, and a company no longer needs to lay new cable every time its headquarters moves, which requires personnel hours and taxpayer dollars.

commanders and troops always-connected, secure access to applications and information and improving situational awareness and mission effectiveness. There is no room for security breaches or outages of any kind when it can mean the difference between life and death, or a war won or lost.

Communications have sometimes been a weak link between the various moving parts of the armed forces, whether between ground, airborne, and seaborne forces, or between forces and nonaligned units such as foreign coalitions or sister services within the DoD. However, this situation has been changing over the course of the past decade as military operations and projects have begun using a network called kinetic mesh.

Not to be overlooked is the network's military-grade level of security (with some radios certified to "Secret and Below" interoperability). Kinetic mesh delivers end-to-end, 256-bit encryption. When encrypted information flows through the mesh and comes out another node, it stays encrypted all the way through, and is not decrypted until it is delivered to its destination, ensuring privacy. At each hop in the network, kinetic mesh provides a per-hop authentication for each packet. Metadata also is encrypted; an attacker cannot analyze the traffic and see which nodes are communicating with other devices – which, in a battlefield situation, could give away position.

Kinetic mesh in the field

Kinetic mesh has been a part of several military programs and projects. Two notable examples include C-RAM and Wolfhound. C-RAM is actually a "system of systems" that primarily uses radar to detect incoming projectiles (rockets, artillery, and mortars)

fired from hostile forces. An engagement weapon then attempts to intercept the projectile and destroy it in flight before it impacts.


There also is a warning component to C-RAM; once the radar has determined the trajectory of the projectile, it can determine what kind of shell or projectile it is, as well as its estimated point of impact, to determine the blast radius. It then can send an alert to the affected area, instructing all personnel to seek cover. A soldier has about 10 seconds to find cover before detonation if the projectile is not intercepted in flight – which can mean the difference between life and death.

The C-RAM program was an important countermeasure to enemy fire during the wars in Iraq, where the way the enemy fought made it impossible for troops to deploy counterfire, because there was simply no one at whom to fire. Instead, the enemy would set up crude stands with rockets on top and use a triggering device to deploy the rockets from afar. It was by no means a scientific method of warfare, but it was intermittently effective, killing or injuring soldiers and disabling military assets.

For the past six years it's been in use, kinetic mesh has provided the communications link between the radars and the command center, and between the warning towers and the command center. Before kinetic mesh radios were implemented, there was a much higher rate of interference between the various components and the radios, creating gaps in communications. With kinetic mesh radios, system availability rate has increased significantly – meaning that even more human lives will be saved in current and future field operations.

Wolfhound is a man-portable electronic warfare (EW) and cyber capability that has been used to support kinetic operations in Operation Enduring Freedom. The system includes three networked, man-packable wireless nodes capable of detecting, identifying, and direction-finding conventional communications. It targets Very High Frequency (VHF) or

PCI Express Mini Card mPCIe Embedded I/O Solutions



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

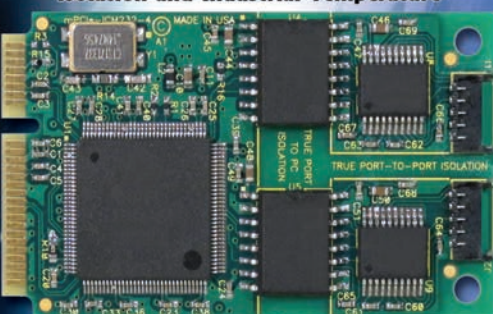
mPCIe Embedded OEM Series

- 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!**



**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 1649. Come visit us at
10623 Roselle Street San Diego CA 92121



USB PC/104 USB/104 Systems

BEFORE KINETIC MESH RADIOS WERE IMPLEMENTED, THERE WAS A MUCH HIGHER RATE OF INTERFERENCE BETWEEN THE VARIOUS COMPONENTS AND THE RADIOS, CREATING GAPS IN COMMUNICATIONS. WITH KINETIC MESH RADIOS, SYSTEM AVAILABILITY RATE HAS INCREASED SIGNIFICANTLY – MEANING THAT EVEN MORE HUMAN LIVES WILL BE SAVED IN CURRENT AND FUTURE FIELD OPERATIONS.

Ultra High Frequency (UHF), push-to-talk, handheld radio communications, and is a counter-IED [improvised explosive device] program.

IEDs were used extensively against U.S.-led forces in Iraq and were responsible for nearly 2,000 deaths between July 2003 and January 2009. Since Wolfhound's inception, however, the program has prevented the detonation of more than 1,000 would-be IEDs and is expected to save many more lives in the future.³

The need for real-time communications in modern warfare

As warfare becomes more unpredictable and asymmetrical, a network-centric approach will be ever more critical – without real-time communications enabling information superiority, all the artillery in the world won't make a difference. Kinetic mesh networks can provide the mobility, reliability, scalability, security, and high bandwidth needed to ensure mission-critical intelligence is sent and received in real time, breaking new ground in wartime communications and helping to save lives. **MES**

Notes

¹ http://www.dodccrp.org/files/Alberts_IAT.pdf

² <http://www.au.af.mil/au/awc/awcgate/ccrp/ncw.pdf>

³ <https://web.archive.org/web/20090113201909/http://icasualties.org/oif/IED.aspx>

Barry McElroy is vice president of Rajant. Before joining Rajant he served as a Detachment Commander for the U.S. Army's Special Operations for 17 years. He can be reached at bmcelroy@rajant.com.

Rajant • www.rajant.com

MISSION-CRITICAL I/O SOLUTIONS



Alphi Technology designs and manufactures board level products.

ALPHI TECHNOLOGY CORPORATION



PCIe-Mini-1553/ARINC 429



PCIe-Mini-CAN-USB



PCIe-Mini-AD8200



PCIe-Mini-FastDAC-4

Designed and manufactured in the USA. | 480.838.2428 | www.AlphiTech.com | sales@alphitech.com

Gaming tech: Shaping the reality of military training

By Mariana Iriarte, Associate Editor



Bohemia Interactive Solutions' (BISim) Virtual Battlespace 3 (VBS3) is part of the U.S. Army's current Game-For-Training program of record. VBS3's content library has hundreds of weapons, including machine guns, launchers, rifles, handguns, and ordnance, including grenades, IEDs, and mines. Photo courtesy of BISim.

Budget cuts, changing mission goals, and sequestration have all resulted in training shortages and shortfalls within the Department of Defense (DoD), yet effective warfighter training has never been more critical and the technology necessary for successful training more complex. Driving much of the innovation in military simulation and training is technology from the commercial gaming community, bringing much familiarity to the young warfighter, but unique challenges to system designers.

The U.S. military leadership still pushes the mantra "train like you fight," but the technology necessary to meet that goal is getting more sophisticated and more dependent on their relationship with the commercial gaming world and concepts such as virtual reality (VR), augmented

reality (AR), and mixed reality. This has become especially beneficial as many young recruits are digital natives and find this simulation technology intuitive.

Technologies like AR, VR, and mixed reality in military training today are not uncommon as "training and education theories evolve over the years," says Tony Prause, portfolio manager, U.S. Army and U.S. Marine Corps training programs, at Engility Corp.'s Chantilly, Virginia location.

More realistic simulation technology also enables more remote training and less use of expensive live platforms, thereby saving the DoD millions of dollars.

"What we're seeing around the world are two things: The first one is an ever-tightening of military budgets, so that's basically universal, and the second one is a reduction in the amount of real-world space where militaries can conduct training exercises," says

Pete Morrison, co-CEO of Bohemia Interactive Simulations (BISim) in Winter Park, Florida. "Both of these facts, or both of these items, will lead military organizations toward using simulation for training."

"The military faces many challenges as it relates to training," states Andre Balta, chief technology officer of Cubic Global Defense in Orlando, Florida. They continue to focus on increasing throughput while increasing the quality of training – whether through point of need training (distributed training) or accelerating learning through learning science, he adds.

Much of their current training leverages similar technology to the games they played in high school, improving skills, ranging from complex decision-making to simple daily maintenance tasks.

Even as many parties agree on the usefulness of VR and AR in military training,



there are not yet requirements in place to facilitate companies' proposing and fulfillment of such programs. "It's a challenge to identify what the training requirements are today, but even harder to do so in five years because you don't know what will change," Prause notes.

Despite the lack of requirements, commercial gaming technology has a foothold in military training. The recruit's go-to forms of entertainment are often video games, as they grew up with games like Call of Duty. "Today's sailors expect that same immersive training environment that not only includes the technical aspect – such as the systems the military uses – but also the scenario storyline," explains Eric Phipps, program manager, U.S. Navy training programs at Engility Corp.'s San Diego facility.

It's no surprise that "The entertainment industry, specifically around computer games, is huge," Morrison says. "The latest estimate is that by the end of this year [2017], computer games will be a \$100 billion industry."

The military-simulation industry is small compared to that, and "what we've seen over the last couple of years is that the technology in the entertainment domain has really outpaced the technology, especially in terms of graphics and physics, in the military-simulation world," he adds.

Military simulation leverages gaming concepts

Increasingly, gaming community advances are driving military-simulation designs. "More and more companies are leveraging the cultural and process elements that mainstream game studios use to create high-fidelity products at rapid rates," Balta says. "These 'cultural' changes contribute significantly to the evolution of the

training industry. These game engines – advanced, photorealistic, and cost-effective – also come with tool suites to generate content easily and readily. The defense industry benefits from all the best practices documented from the gaming industry."

The content is just as important as the technology, but it's more "of a holistic approach," Prause says. "For example, an Electrician's Mate (EM) or Electronics Technician (ET) in the Navy has to go through 'A school' and subsequently through different types of schools, including on-the-job training. Each of those different training scenarios are system-specific schools – and you have to take all that into account to build through that whole training life cycle," Prause says. "That's a challenge, but you have to take that bigger picture into account."

The entire solution set needs to be realistic enough for the military. "From an Engility standpoint, we have to create a full backstory for every training scenario," Phipps says. "During the crisis or scenario, orders have to be realistic. Coalition forces, geography, geopolitical boundaries, all of that has to be developed to provide the fidelity that sailors expect."

Mixing reality with a game

VR and AR are all part of the game with mixed reality sitting on the cutting edge. Morrison adds. "Mixed reality is where you have a headset with video cameras, which captures the real world, but we inject virtual elements.

"A pilot can sit in a mock-up of a cockpit, but that cockpit is created in the real world with all the dials and switches," Morrison explains. "But then when they look out the window through their headset, they're seeing the virtual world, which is generated by our software. This is called mixed reality, and the next frontier we're working on with the U.S. Navy."

The idea that the user's mind must create a fake reality, yet can feel, see, and touch the tools and systems make this type of training more effective – and it's simply mind-blowing.

This provides an ability to have a mixed reality solution, enabling interaction with the real world, vis-à-vis the cockpit controls or anything else an operator may want to do, explains Nick Gibbs, vice president and general manager, training solutions, for Rockwell Collins in Sterling, Virginia. "You could fire a weapon, it would be a real weapon and you could load and unload it while seeing your hands performing the task. You don't need any simulated behaviors for that."

Live, virtual, constructive (LVC) training – which integrates live and virtual constructs – also enables the military to bring together different domains from air to sea to land.

"An LVC environment is very scalable and repeatable. That's another benefit the Navy wants take advantage of," Phipps says. "They can train a single ship, crew, or aircraft, or scale up to just about any number of ships, crew, aircraft, and other forces. And

they can repeat the training as necessary, ensuring that the objectives and learning points have been achieved."

Eventually, the end result will align with the Navy's vision, which is "to eventually take the synthetic environment and blend it with a LVC environment that will be seamless between real and constructive forces," Phipps says.

Efficiency versus effectiveness

While adoption of a gaming-style type of training for today's digital natives sounds natural for the military concerns over effectiveness remain. "Now that you've given the training, how do you determine how successfully that individual is now trained, or that collections of individuals are now trained, in the task that they were supposed to obtain from the course or from the simulations?" Gibbs says.

"Right now, there's an effectiveness and an efficiency argument," Morrison states. "When we talk about effectiveness, we've proven that doing simulated exercises, and it doesn't matter what the domain is whether it's land, sea, or air, if you do a task in simulation before you do it in the real world, and that simulation is suitable for the training task of course, then you're going to essentially decrease the failure rates in the real world. You're going to be better at that task."

The mantra with this training is: practice makes perfect. "Our software gives them an opportunity to practice how to think," Morrison says. "They can operate collectively in the virtual environment and practice the things that they need to do in the real world. Through practice in the virtual environment, it reduces the amount of training that they have to do live, and it also can help save their lives in theater because they've done it many more times in simulation that they would've gotten to do it live."

In addition to practicing, AR and VR "increases the effectiveness, in particular the decision-making process," Praise says. "It reduces the cost of training and becomes very attractive for users, not just for the cost, but also because the access to the training is easier."



DDC® YOUR SOLUTION PROVIDER FOR...
CONNECTIVITY | POWER | CONTROL



STAY CONNECTED

Scalable, Multi-Protocol Connectivity
Compact Avionics Interface Computer

Applications Include:

- **Mission Interface Computer**
 - Interface with platform sensors & terminals
- **Embedded Tester/Simulator**
 - Simulate/analyze sensors pre- & post-flight
- **Data Concentrator**
 - Analyze, convert & consolidate multiple I/O types into single port

SWaP-C Optimized System

- Rugged Deployable Compact Enclosure
- High Computing Performance, with Low Power Consumption
- MIL-STD-810G Shock, Vibration, and 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, Video, WiFi, GPS, Power Control, Motor Control, and Motion Feedback
- 3 modes (Remote Access, Protocol Conversion, and Standalone)
- Expandable: (2) Mini-PCIe sites and (1) I/O Expansion Module

53
YEARS OF SERVICE






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

DATA DEVICE CORPORATION

The aftereffects of gaming tech in military training

Gaming technology is attempting to close the gap in the training deficiencies that the military is currently experiencing. For example, the U.S. Navy's Littoral Combat Ship (LCS) engineering casualties in late 2015 through 2016 forced military leadership to emphasize training.

In answer to that situation, "Cubic's Immersive Virtual Shipboard Environment (IVSE) developed for the U.S. Navy's Littoral Combat Ship is a game-based learning continuum using Unreal 4 Engine," Balta explains. "It is designed to meet the Navy's objective of 'Train to Qualify' (T2Q) and 'Train to Certify' (T2C). T2Q is the standard set as an individual measure of a sailor's proficiency to 'stand the watch' as soon as he/she reports aboard their ship, while T2C is a similar measure of proficiency for the 'watch team.'"

By using gaming technology "students are immersed in a high-fidelity 3-D replica of the actual ship within a virtual environment that contains all the spaces, compartments, systems, equipment, technical documents, instructions and tools necessary to qualify a student for their prospective watch station," Balta says. (See Figure 1 video/image).

"Training is conducted in the controlled virtual environment, enabling multiple students to learn simultaneously, independently, or in teams," Balta adds. "Training in the IVSE replicates on-the-job training just as sailors learn on board current ships of the fleet, without the 'underway' challenges of limited time and inconsistencies as sailors learn from various sources and senior personnel."

The use cases are not hard to find. "Since 2004, Games for Training has been a program of record within the U.S. Army, so that's essentially validation that there is forward recognition that gaming technology works, and that's an investment by the U.S. Army in gaming technology, probably to the tune of maybe \$50 to \$100 million dollars a year, so there's anecdotal evidence that given the level of investment, the U.S. military believes that it works," Morrison points out.



Figure 1 | Cubic's Immersive Virtual Shipboard Environment (IVSE) developed for the U.S. Navy's Littoral Combat Ship. Video/image courtesy Cubic via Surface Warfare Officers School.



Figure 2 | Rockwell Collins EP 8100 used for the Apache helicopter visual system. Photo courtesy of Rockwell Collins.

"We've had a case in the U.K. where, a soldier credited game-based training for saving one of his soldier's lives in Afghanistan," He adds. "They had a vehicle rollover event, and because they'd rehearsed that so many times in simulation, they knew exactly what to do in the real world when it happened."

From sea to land to air, "a great example is the joint-strike fighter, where it's a single-seat plane," Rockwell Collins' Gibbs says. "There is no second seat version for training. All of the pilot's training before first flight takes place in the simulator. We provide the helmet-worn display, the entire visual system along to Lockheed Martin for that training device."

Rockwell Collins' high-fidelity training system, the EP 8100, has "FPGA [field-programmable gate array] technology, so it provides even more enhanced capability," Gibbs adds. (Figure 2.)

The beauty of this type of training is that "users can create whatever scenario they need to train to in an immersive training environment," Phipps says. "For example, users can't always train in ballistic missile defense (BMD) against long-range high-altitude missiles in real life. It is expensive and there's a high-risk factor involved with this scenario. There is also a decision-training matrix involved including the ships being trained, the authorities in charge, and an intelligence background needed. A synthetic background is ideally suited for this. You can network multiple ships and train for a BMD scenario without the restrictions of battlespace." **MES**

How low-cost LRUs can support a Condition-Based Maintenance Plus environment

By John Rodwig



A Condition Based Maintenance Plus (CBM+) strategy can help designers in military programs increase reliability and availability, improve maintenance practices, and lower life cycle costs. Low-cost line replaceable units (LRUs) designed for condition monitoring and health assessment can be a large part of a CBM+ integrated strategy.

The Condition Based Maintenance Plus DoD Guidebook [published in March 2017 by the Department of Defense (DoD)] describes CBM+ as a “conscious effort to shift equipment maintenance from an unscheduled, reactive approach at the time of failure to a more proactive and predictive approach that is driven by condition sensing and integrated, analysis-based decisions.” CBM+ implementation is usually seen in high-priced equipment, or in equipment with the most critical failure-effect modes. According to the DoD guidebook, operations and support (O&S) costs account for 65 to 80 percent of a program’s total lifecycle cost. Lower-cost LRUs generally do not feature the condition monitoring required to feed sufficient prognostic data to CBM+ processing. Such LRUs simply provide post-fault visibility into the reactive maintenance system, thereby limiting their usefulness.

As CBM+ continues to gain traction, the benefits to the military will be increasingly dependent on the level of participation of the downstream subsystem diagnostics. A complete reliability-centered maintenance (RCM) analysis that would provide a full set of rules for predictive fault assessment is uncommon in smaller development contracts.

Even using lower-cost, lower-utility devices, it is possible to implement monitoring of critical device status using common components in a way that will enable products to be in a position to participate in CBM+. A well-instrumented LRU, even with less sophisticated health monitoring, can provide valuable insight into unit operation and move a device closer to proactive maintenance.

Architecting for condition monitoring

Figure 1 illustrates the CBM+ infrastructure areas. Compliant LRUs in this environment typically satisfy requirements in the areas of sensors, condition monitoring, health assessment, communications, and human interfaces. Design features that perform processing in these areas can be implemented with reasonably low recurring costs. Although the initial development cost is incrementally higher than most common go/no-go diagnostics, the high reuse, longer service life, and potentially lower average maintenance cost make a compelling business case.

Robust health assessment depends on detailed rules from RCM analysis, but at the LRU level, a reliability prediction, along with a failure modes and effects criticality



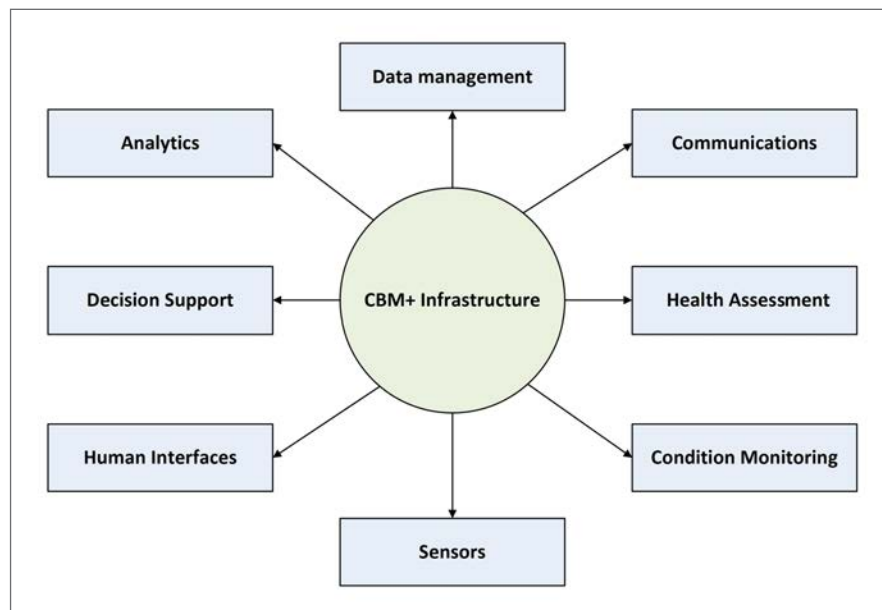
analysis (FMECA), provides enough information to develop meaningful health assessment algorithms. Such monitoring and analysis can uncover trends such as increased current flow, ripple on DC power lines, or a compromised heat map. If health assessment still proves too costly, maintaining a log for future analysis is a reasonable compromise. Valuable data can be extracted to determine if a unit back for repair experienced a shock, vibration, temperature, or input power event.

In a vehicular or avionics display unit (DU), for example, typical diagnostics include memory, communications port internal loopback, power fail, and possibly LED [light-emitting diode] driver voltage monitoring. If there is a single-board computer (SBC) that features diagnostics middleware, additional measured power, temperature, and power cycle count data may be available. Built-in test (BIT) options include power up, background, initiated, and possibly one or more operator-involved visual tests.

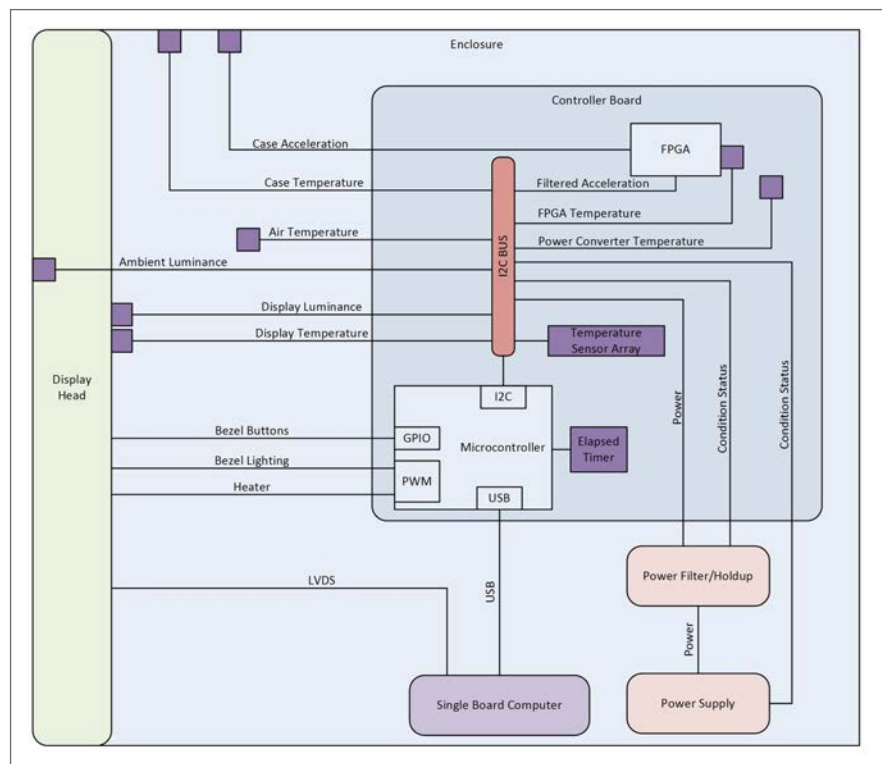
A DU architected for condition monitoring is shown in Figure 2. Temperature, power, acceleration, and light sensors measure and transmit key operating parameters to the microcontroller for subsequent health assessment processing.

› Temperature sensors

The low cost of thermal sensors enables the developer to use multiple sensors to gather temperature data from many locations to produce a high-resolution heat map. Candidate designs range from higher-priced sensors with built-in calibration and serial communication, down to very low-cost thermistors that require additional analog multiplexing to provide the signal to the MCU.



› **Figure 1** | CBM+ infrastructure areas.



› **Figure 2** | Display unit architected for condition monitoring (Image courtesy IEE).

The stylized depiction in Figure 3, the output of a thermal-simulation study, is illustrative of a typical thermal profile of a circuit card assembly. When validated with empirical data, the design engineer can readily select a few key locations for thermal measurements to support a real-time measurement of the circuit card thermal profile. With the aid of RCM+, this temperature sensor mapping can provide effective measurement of the card and support detection of the onset of failure conditions.

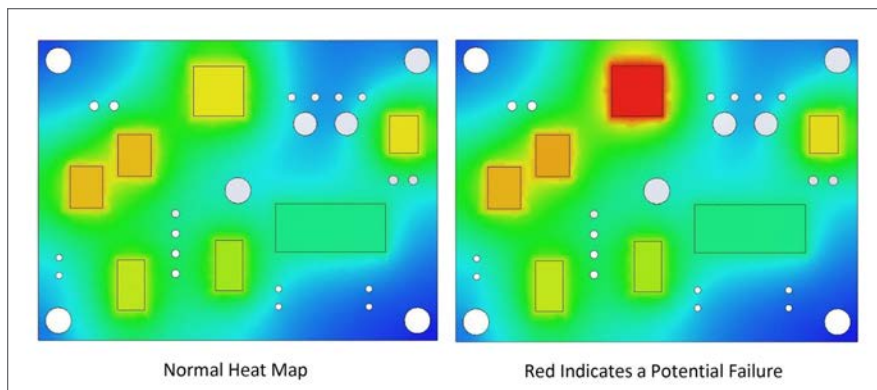


Figure 3 | Circuit board assembly heat map visualization and actual measurement (Image courtesy IEE)

➤ Power sensors

Voltage and current monitoring of primary and secondary power have been simplified with the availability of low-cost monolithic devices. Changes in voltage and current that do not correlate to temperature, CPU utilization, or other factors are an indication of the onset of a potential failure.

➤ Luminance sensors

The display unit can track the backlight intensity, ambient light intensity, backlight drive current and voltage, temperature, and elapsed time to piece together trend data on display degradation. Luminance detection may be used to increase fault detection in lieu of operator feedback. Although a display failure may be obvious to the operator, some system designs do not allow operator interaction to be part of fault detection and will not factor into BIT verticality analysis.

➤ Acceleration sensors

Accelerometers can detect shock and vibration events, and can warn that the LRU has been subjected to them, for failure prediction or post-failure root

RADAR & ELECTRONIC WARFARE

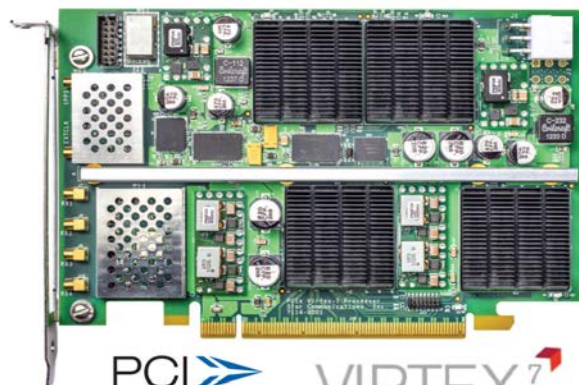
The Radar/Electronic Warfare monthly newsletter provides features, news, columns, and more covering radar and electronic warfare technology as well as hardware and software designs for systems in the defense and aerospace markets.



Subscribe to receive your copy of the newsletter:
http://url.opensystemsmmedia.com/radar_quarterly_subscribe
 Archived newsletters at: mil-embedded.com/radar-electronic-warfare



Star Communications, Inc.



PCI EXPRESS

VIRTEX⁷

- signal processing receivers
- computing accelerators

Small. 4.4 x 6.6 x 0.8 inches
 Powerful. >65 Teraops/sec
 Affordable. scalable 1-4 FPGAs
 Easy-to-use. installs in any PC or server

made in the U.S.A.

www.starcommva.com

cause analysis. Accelerometers produce large amounts of data, so their output should be processed through a field-programmable gate array (FPGA) or other data-acquisition preprocessor to facilitate storing only the acceleration events that meet threshold criteria. More sophisticated designs may incorporate enough power holdup capacity to detect removal and post-removal handling events during which the LRU is particularly vulnerable.

› Health monitoring

The integrated diagnostics engineer must determine what to do with all this data. The absence of complete systemwide RCM analyses leaves the health assessment processing to the supplier, who should perform sufficient failure analysis to provide basic rules for health monitoring. Many failure thresholds are specific to devices and require a large amount of specification details obtained from component data sheets. Although it may take time and effort to provide meaningful LRU machine health data into the CBM+ environment, health monitoring is a critical component for full participation.

› Communications

In our example, the display unit is responsible for providing pertinent operating parameters and health status data to the mission computer. The system is responsible for making the data accessible to all levels of the CBM+ environment.

› Human interfaces

The DU presents critical operating parameters and health assessment data to the operator for workaround actions during mission conduct. This data, in the more detailed form of the fault log, lets the maintenance operator use the CBM+ Communications infrastructure to accomplish effective troubleshooting and repair. The unit also enables the mission and maintenance operators to initiate diagnostics and visual tests that require operator feedback.

Sensors the key

Lower-cost LRUs can participate more fully in a CBM+ environment by implementing sensors, condition monitoring, health assessment, communications, and human interface functions. If all such units implement these functions to some degree, designers of even critical equipment used by the military will find a significant impact on total life cycle costs and reliability. **MES**



John Rodwig is a Director of Program Management at Industrial Electronic Engineers, Inc (IEE). He has more than 30 years of technical and management experience in defense and telecommunications, and coholds a patent for a radar scan converter. John earned a BS in electrical engineering from Tulane University and an MS in engineering management from California State University, Northridge. He can be reached at jrodwig@ieeinc.com.

IEE • ieeinc.com





Test and Development Chassis with Room to Maneuver

Elma's Type 39 E-Frame open access chassis is the optimal choice for your application development needs in VPX, VME and cPCI systems.

Elma - so much more.





Find out why Elma is the authority in embedded computing platforms, systems & components.
www.elma.com | 510.656.3400

Data-driven design for HMI development in avionics design

By Raymond Niacaris



F-22 cockpit. Photo courtesy U.S. Air Force.

Engineers and designers who work on glass cockpit displays continue to look for effective ways to interact with the inanimate objects they want to control. Using a data-driven approach similar to that used in video games, a structure can be created through which advanced human-machine interface (HMI) applications are deployed to meet the needs of avionics developers.

Data-driven models and model-based design are two terms that are cropping up more frequently in discussions among avionics engineers and designers, as well as in standards steering committees. All are focused on the most effective ways for humans to interact with the inanimate objects they wish to control. HMI can mean any method a human can use to interact with a device. Thus, a brake lever on a trolley car is a HMI device. For the purpose of this discussion, the definition of HMI will be limited to that of a pilot or an unmanned aerial system (UAS) ground station operator interacting with a glass display to effectively control and monitor an air vehicle.

The interaction between humans and aircraft systems requires complex actions and decision-making with split-second timing. For example, the space shuttle, with 3.5 million parts, used to be controlled by four or more astronauts, with a hierarchy of commander, pilot, and mission specialists. However, consider the F-22 Raptor fighter aircraft/weapons system: It has millions of parts and is heralded by many as one of the most complex systems developed by humans, yet it is controlled by a single individual – the pilot. It is important to note that this complex weapons system has glass multifunction displays (MFD) that control most of the systems' functions.

There are many ways to create a graphical display. Software developers can use a graphics set of application programming interfaces (APIs), such as Open GL, or a myriad of tools that enable the developer to create interactive dynamic graphics to communicate with users needing to control systems via interactive glass displays. Many of the tools employ an integrated development environment (IDE) that stores the animated control graphics in a native format and then uses a code generator to create a source code file that can be compiled into an executable file. In some cases, the code generators used will optimize the native format file. The file generated is

then compiled into an executable program, in many cases by an optimizing compiler that changes the executable even more. This would be a worst-case scenario in that most code generators have settings that allow the user to control the degree of optimization, which is also true of optimizing compilers.

The downside of this design approach is that it is often difficult, if not impossible, to baseline the ensuing code files and accurately track the effect of minor changes in these files. For example, if a simple shape is drawn in a frame and then is subsequently moved a few pixels to the left or right, that action could cause an optimizing code generator to create an entirely different output file, making that minor change impossible to baseline or track. The issue could be further exacerbated when the target display changes, which then calls for a change in the display layout, which needs to be redeveloped to accommodate the new target.



A data-driven approach

The gaming industry has long been faced with developing video games that need to run on a number of platforms. Faced with the number of game consoles that come and go, and the relatively short life cycle of many games the industry needed to develop a method that would let the game developers focus on the game play and environment of the game and not on constantly tweaking the game design to accommodate a given game console. The solution was to design to a gaming engine, for instance, to the "Unreal 4 engine." Any game console that supported the Unreal 4 engine would then, by definition, support the original game design. Game designers could now focus on the game design and playability and not worry about the target gaming platform.

Suppose the same approach was used in the design of a glass HMI display. A graphics engine would sit on the target platform (embedded display system) and would process data to create a dynamic graphical display and its associated behavior. The HMI designer would focus on the look and feel of the display and not be concerned with the target system. In fact, that display could be

used in an embedded cockpit, a flight simulator, or even a graphics tablet for training or marketing-related activities. The graphics engine would process a command stream downloaded to the target system as a file or array of data. Since it is pure data, there would be no need to compile or link it into an executable code base on the target system. The data would not change from display to display, thus creating a stable, consistent display system. Since the target-based engine is simply processing data, it would be a straightforward task to dynamically overlay this data with new data on the fly.

This approach means that the look and feel of the display could be altered while the target system is running and enables so-called man-in-the-loop HMI glass display design in real time. Stimulus and response times could be measured, altered, and evaluated in real time, saving many engineering design hours and rework.

A data-driven example

A good example of a data-driven architecture is the Aeronautical Radio, Inc. (ARINC) 661 specification, where the HMI is represented by a data format or model. In addition, the use case is very much like the gaming case described earlier, in that many different user applications (UA) can send commands to a common cockpit display system (CDS) and have those commands drive the CDS to communicate the status of the UA component, effectively providing control input to the UA. In theory, any UA written to the ARINC 661 specification can interface to an ARINC 661 CDS in much the same way that those earlier theoretical game developers write their game software to a gaming engine.

However, that is where the similarity ends. In the gaming world, the software game is defined once to the engine and then is spawned to many game consoles for execution. The opposite is true in an ARINC 661 system: A single CDS is communicating with many UAs in virtually all aircraft systems. (Figure 1.) Look at it this way: A single CDS can be used as the pilot-aircraft interface. Since a single CDS is controlled by many UAs, a clear definition of the communication constructs is an essential component of the ARINC 661 definition. In addition, a

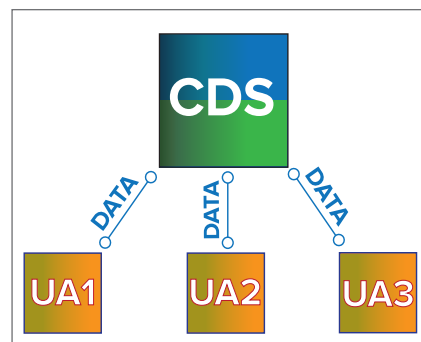


Figure 1 | Diagram of an ARINC 661 system, in which a single cockpit display system (CDS) is communicating with many user applications (UAs).

UA can be communicating and controlling its data representation on several CDSs simultaneously. This methodology is being deployed on many aircraft, most notably the Boeing 787 Dreamliner.

The IData Tool Suite from ENSCO Avionics is one mechanism designers can use to create and deploy advanced HMI applications – for example for use in a cockpit display – within a data-driven, model-based development environment. The user has a single design to target multiple desktop or embedded systems, and support multiple stages of a product life cycle. Through data-driven development, the tool can help designers reduce the time required to create, test, and deploy HMIs. IData's approach – which borrows from various industries that employ computer graphics – combines content-creation tools with a high-performance runtime engine processing an optimized data file. **MES**



Ray Niagaris has spent that last six years at ENSCO Avionics and the last 15 years working with HMI tools. He has more than 35 years of experience in real-time embedded systems and computer graphics. He holds degrees in electrical engineering and computer science from the Illinois Institute of Technology, has completed advanced studies in human factors and advanced product design, and has served on the faculty at the Illinois Institute of Design. Readers may reach Ray at niagaris.raymond@idatavs.com.

ENSCO, Inc.
www.ensco.com

Military MRO: Solving the maintenance skills shortage with augmented reality

By Kevin Deal



Maintaining sophisticated military equipment across land, sea, and air is a difficult enough challenge when the required resources are readily available. How can the military balance equipment availability with a reactive and compliant maintenance strategy and supply chain when the number of skilled engineers is limited? The use of augmented reality can help the military deliver maintenance expertise from and to anywhere in the world.

The market for virtual and augmented reality is growing: A January 2017 report from Digi-Capital predicts that the virtual reality/augmented reality (VR/AR) market will be worth \$120 billion by 2020. Virtual reality has been a hit in the consumer world; the defense sector is now starting to see the power of the technology, and its close relation augmented reality, in action.

VR/AR technologies have been used to simulate training exercises to speed up and reduce the costs associated with readying military personnel for deployment. For example, the Dismounted

Soldier Training System for the U.S. Army, deployed in 2012, was the first-ever fully immersive virtual simulation training system aimed at giving soldiers more training time before sending them to the battlefield. Only now are we seeing VR/AR implemented to fulfill a growing requirement for defense organizations: the globally pressing issue of effectively and flexibly deploying scarce and expensive maintenance personnel.

Growing asset complexity requires skilled engineers

Military assets continue to grow in complexity. Forces across the globe are beginning to take delivery of the F-35 Joint Strike Fighter, the most complex and capable military jet ever manufactured. Larger assets such as the Nimitz-class super aircraft carriers also pose significant maintenance challenges. The Navy estimates that the USS Theodore Roosevelt contains over 1,000 miles of electrical cable and an air-conditioning plant capable of sustaining 500 houses. At that huge size, it's no surprise that it took a full four years to complete the midlife refueling and complex overhaul (RCOH) of the carrier, from 2009 to 2013.

Increasing asset complexity, the decline in defense personnel numbers, and a definite lag in maintenance training means that having the right engineers in place to keep equipment available is becoming a difficult management task.

Supply loses out to demand from booming commercial aviation market

On one hand, the sophisticated equipment entering defense supply chains requires significantly longer lead times on training. Maintenance personnel are trained and qualified to perform specific repairs on specific equipment and – particularly on aerospace assets – nothing else. On the other hand, the military cannot compete with the booming commercial aviation industry, especially in the fast-growing Middle East and Asia-Pacific regions, where airline operators and maintenance, repair, and overhaul (MRO) outfits can headhunt military personnel with attractive salary offers, work hours, and safer environments.

The demand for maintenance is rapidly outpacing supply. In a 2014 report, the U.K. Military Aviation Authority reported that the RAF lacked 411 tradesmen for aircraft maintenance – a 12 percent shortfall in the number of trained engineers the Ministry of



Defense (MOD) required. Innovative solutions are needed to help bridge this gap.

Globalization's huge logistics footprint

Add to this shortfall in personnel the fact that military engagements are less predictable now than ever before. Insurgency-based threats can arise anywhere at any time, and counterterror warfare requires defense organizations to be prepared to respond as quickly as possible. Sending a fully effective defense force to a forward area requires maintenance expertise to be available close to the area of equipment operation. Maintenance personnel then need transport, food, and shelter, along with force protection. All of this quickly becomes an ever-growing logistics footprint.

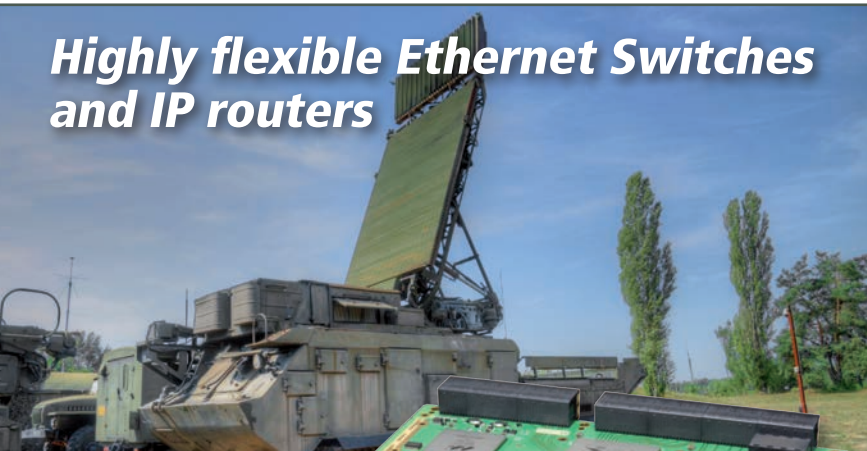
Of course, it's worth remembering that in wars of old – let's say during the Crimean War, fought from 1853 to 1856 – there were no logisticians involved. Major developments since then mean that across the three services of a mature defense organization such as the U.K. MOD, a full one in six personnel are now directly involved in logistics. In a modern air force organization, such as the U.S. Air Force or Royal Air Force, 95 percent of trades are nonpilot supporting roles.

Which option to choose?

When positioning maintenance personnel to maximize force readiness, defense organizations are faced with three options:

1. Strategically position maintenance engineers geographically: One option for defense forces is to deploy units and maintenance personnel in likely areas of conflict. With insurgency-type threats arising without notice in any given area, second-guessing these potential conflicts would require deployment of many maintenance troops and engineering equipment, not to mention life support in different locations. However, even deploying a small force involves a spiraling logistics footprint and cost involving equipment, fuel, food, ammunition, security, spare parts, and more, plus the transport infrastructure to rotate them. A small deployment soon becomes a long-term camp; witness the U.K. Ministry of Defense Camp Bastion in Afghanistan, which is estimated to have cost \$1 billion over its lifespan, supporting 28,000 troops, 4,032 contractors, and 3,080 vehicles.
2. Adopt a "fix when required" approach: Should defense forces risk leaving a vehicle, weapon, or plane sitting idle in a remote location and take the chance on flying a qualified engineer out to fix it on an as-required basis? With forces spread in remote locations, flying a skilled engineer out to the front line to repair stricken equipment can take time, which defense forces simply cannot afford. In many cases, it may be too dangerous to deploy a maintenance engineer in the field, leaving squads cut off without mission-critical equipment. In addition, until a maintenance assessment has been completed at the asset, it's not always obvious which engineer role, qualification, and equipment is needed to perform the repair.

Highly flexible Ethernet Switches and IP routers



Stay ahead with
IC proven solutions

Extensive range of 3U/6U
high-performance platforms
designed to meet your critical applications needs.



www.interfaceconcept.com

ELMA
Your Solution Partner

Please contact Elma Electronic Inc. for further information on these products
www.elma.com • sales@elma.com • 510-656-3400

3. The third way – augmented and virtual reality: Using remote guidance via a wearable or mobile device, engineer skills can be “augmented” as more qualified technicians provide expertise from any location in the world. Virtual reality simulation can even speed the training process itself. At the 2016 MRO Europe conference in Amsterdam, ICF International vice president Jonathan Berger predicted that virtual reality could shave one or two years off traditional maintenance engineer training programs. AR/VR will be of particular interest to the military in the coming years as the technology continues to mature. A one-to-many delivery of expertise from a central hub to remotely deployed engineers has the potential to drastically reduce training times, improve maintenance efficiency, and bring huge cost savings.

Augmented reality a solution for safety and scheduling

Current mobile solutions support collaboration and drive better data capture and compliance, but even these devices cannot solve the “right skills in the right place” issue. Maintenance personnel could of course contact senior technicians via cellphone, but there is no way of seeing or demonstrating how a task should be executed. Such uncertainty is unacceptable in many situations; after all, these are often decisions regarding airworthiness and safety. Integrating the latest technology with a configuration-controlled solution adds the necessary rigor to remote maintenance tasks.

Augmented reality company XMReality (Linköping, Sweden) has been working on remote guidance in the field, enabling junior engineers involved in a repair to instantly contact experts back at base. The company has designed an AR training and remote guidance solution for the Swedish Defence Materiel Administration (known by the Swedish acronym FMV).

Using remote guidance, a support technician can see the asset in real time and

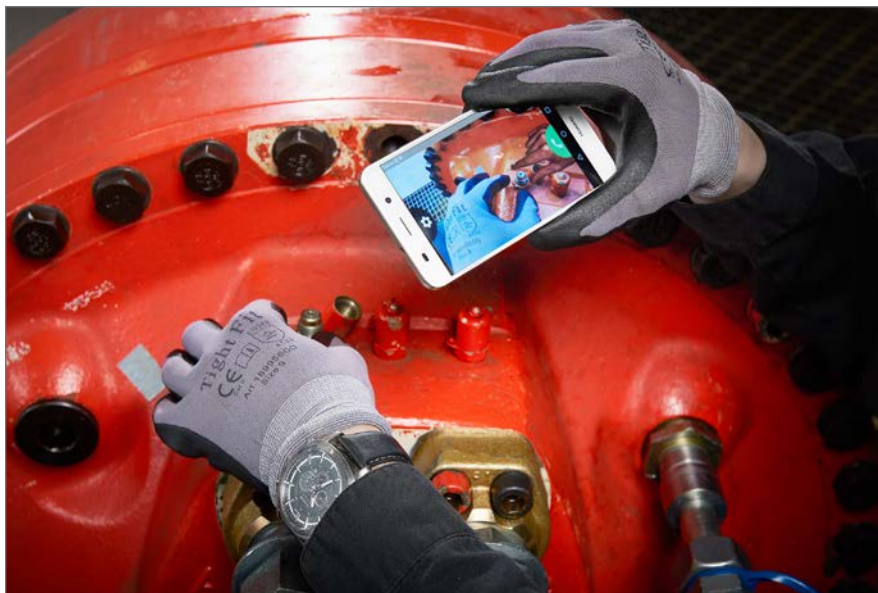


Figure 1 | The XMReality Remote Guidance tool allows for knowledge sharing, including training. The solution uses augmented reality (AR) to project an overlay on mobile devices such as smartphones, tablets, or laptops. Smart glasses can be used if both hands are needed to perform the task. Image courtesy XMReality.

guide the engineer through every step of the repair with augmented hands and tools – all without having to leave base. Using smartglasses, mobile devices, or tablets, engineers can see a real-time, interactive demonstration of the repair job right in front of their eyes. (Figure 1.) These skills can be leveraged anywhere at any time with the capability of modern mobile technology, helping improve first-time fix rates and decrease the chance of error.

What's next: keeping soldiers safe and missions on course

When these AR/VR technologies are integrated with a supporting enterprise asset management or MRO solution, the maintenance operator can quickly report and complete repair jobs, getting mission-critical equipment back up and running as soon as possible.

The next step will be to develop these solutions to the point where they can be feasibly used on the front line or in the bowels of an aircraft carrier, without compromising repair time, soldier safety, and mission success. Functionality must be tailored for ease of use in the field, keeping in mind the conditions a soldier or front-line engineer may be operating in – possibly kitted up in chemical, biological, radioactive, and nuclear equipment or huddled in the dark bilge of an at-sea submarine.

With augmented reality maximizing engineer and technician efficiency, defense forces will no longer have to suffer long waits and knowledge gaps when it comes to maintenance resource shortage. **MES**

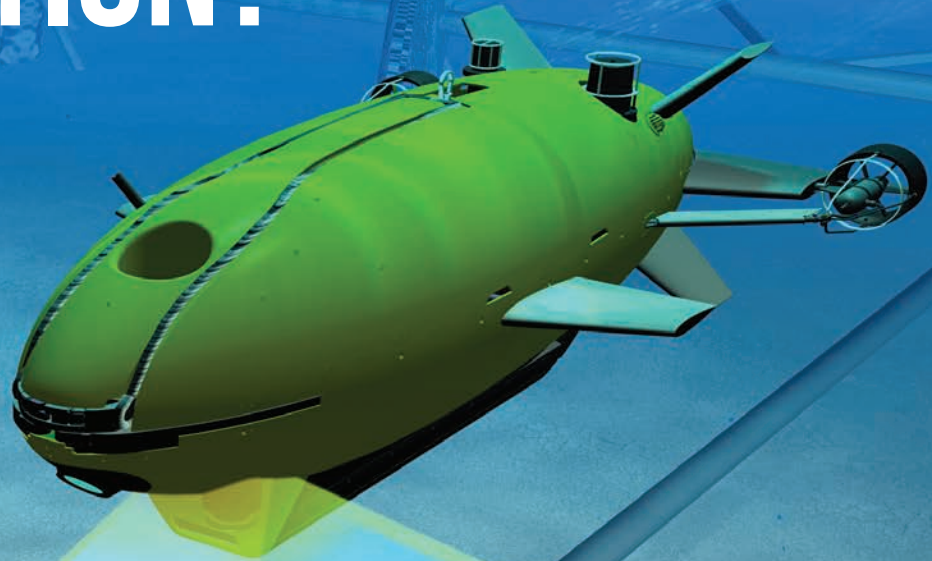


Kevin Deal is vice president for Aerospace and Defense/North America at IFS. He has been in the aerospace and defense IT business for over 25 years. Prior to joining IFS, Kevin held a number of roles, including Director of Mid-Americas and Federal at BroadVision and Director of National Sales at Cincom. Kevin was also a logistics war modeler and former director of the DoD's Supportability Investment Decision Analysis Center (SIDAC).

Readers may contact the author at kevin.deal@ifsworld.com.

IFS • www.ifsworld.com

LOOKING FOR THE LATEST INFORMATION?



TECHNICAL COVERAGE OF ALL PARTS OF THE DESIGN PROCESS



Military Embedded Systems magazine focuses on "whole life COTS" and the total military program life cycle, providing technical coverage that applies to every stage of a program, from front-end design to deployment. The website, Resource Guide, Internet editions, and print editions provide insight on embedded tools and strategies such as hardware, software, systems, technology insertion, end-of-life mitigation, component storage, and many other military-specific technical subjects.

Coverage areas include the latest, most innovative products and technology shifts that drive today's military embedded applications, such as SDR, avionics, radar, cybersecurity, C4ISR, standards, and more. Each issue provides readers with the information they need to stay up to date on the embedded technology used by the military and aerospace industries and the newest, most exciting technologies in the pipeline.

Military
EMBEDDED SYSTEMS
mil-embedded.com



Rackmount computer with SysCool thermal-management system

The U.S.-assembled M2U-20 from Chassis Plans is a revision-controlled mil-grade rackmount computer for use in rugged, computationally intense military applications that consumes limited rack space. It weighs 24 pounds (weight differs on configuration) and contains the proprietary SysCool thermal management system; SysCool, says the company, extends the life of the computing system, reduces power consumption, and lowers overall system noise levels. The M2U-20 is ISO 9001:2008-certified and ITAR-registered.

The computer has four central processing unit (CPU) options – single Intel Core i5 or i7, single Intel Xeon E3 series, single or dual Intel Xeon E5 series, and high-performance motherboard options – for applicability in airborne operations, land-based operations, seaborne operations, telemetry, diagnostics, simulation, imaging, persistent surveillance, unmanned aerial vehicles (UAVs), and automation. Additional features include three horizontal or several vertical plug-in card slots and a single or redundant power supply. Drive options include four 3.5-inch drives that are fixed or removable; four 2.5-inch removable drive sleds that are expandable to 10 times; and 12 2.5-inch removable drive sleds. All drives are shock-mounted. The system is also tested to or designed to meet the MIL-STD-810G environmental standard.

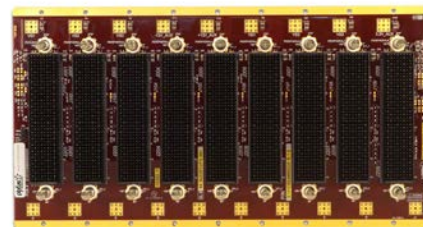
Chassis Plans | www.chassis-plans.com | www.mil-embedded.com/p374362

3U OpenVPX backplane design with data rate options up to 40 Gbps

Pixus Technologies' VPX30 backplanes are compliant with the latest VITA 65 interoperability specifications. The backplanes have data rate options as fast as 40 Gbps, with selectable rear I/O options. While the backplane was designed with five, six, seven, nine, 12, and 18 slots as a standard, other sizes are also available.

The 3U backplane design is customizable and modifiable upon request without nonrecurring engineering costs (NRE), with conformal coating optional; to customize, a minimum order placement is required. Pixus also has several off-the-shelf 3U and 6U VPX configurations. Other VPX derivations include VITA 46 (base VPX), VITA 66 for optical, and VITA 67 for radio frequency (RF). Pixus also provides accessories to use with the backplanes, such as VITA 62 power boards and RTM cables.

Pixus Technologies | www.pixustechnologies.com | www.mil-embedded.com/p374363



Frequency synthesizers built to meet airborne, shipboard standards

The 1018 series of frequency synthesizers from Cobham is designed to meet the phase noise, spurious, and harmonic specifications required for airborne, shipboard, and laboratory environments. The product line features a parallel control interface to facilitate pipelined hopping, which enables switching speeds of up to and over 250 μ s (typical) switching speed from any start frequency to any stop frequency in the full range. Smaller frequency steps typically achieve faster switching speed.

The family of synthesizers – which measures 2.6 by 2.6 by 0.6 inches and weighs just 0.25 lbs. – covers frequencies from <450 MHz to >18 GHz in 10 MHz steps. The power requirement for the synthesizers is typically +5 VDC \pm 10 percent, at 1.25 amps. The compact synthesizers have an SMA port for connection to an external 10 MHz reference oscillator while maintaining the frequency stability of the external reference. The output power is calibrated to remain within a \pm 2-dB window when the frequency synthesizer is operated within \pm 5 $^{\circ}$ C of the calibration temperature. The units are built to withstand operating temperatures of -40 $^{\circ}$ C to +70 $^{\circ}$ C and storage temperatures of -55 $^{\circ}$ C to +85 $^{\circ}$ C on aircraft, aboard ship, and in the lab.

Cobham | www.cobham.com | www.mil-embedded.com/p374434



Nanosecond Pulser product line for high-power microwave applications

The Nanosecond Pulser (NSP) product line from Eagle Harbor Technologies features pulse generators for low- and high-power applications. The turnkey precision pulse control system features a front-panel pulse control and outlet for DC power supply. The user can adjust independently the output voltage and pulse width and it also features a pulse repetition frequency option. Additional options include external pulse input, 1 MHz burst mode, and pulse-shaping output stage.

The NSP units are shipped with a floating output that cannot be grounded; the floating output significantly decreases electromagnetic interference (EMI) and improves measurements of output waveforms. While grounded units can be purchased, Eagle Harbor Technology recommends floating outputs unless an application specifically requires a grounded unit. The NSP product line can be used in applications such as dielectric barrier discharge, pseudospark, laser driver, high-power microwaves, drag reduction, light production, surface modification, medical devices, and fast capacitor charging.

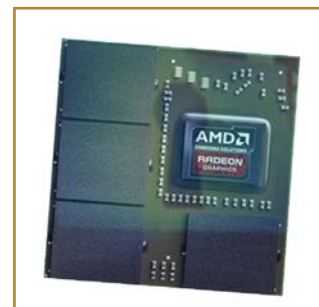
Eagle Harbor Technologies | www.eagleharbortech.com | www.mil-embedded.com/p374365

SecureCore aimed at GPU security

CoreAVI's SecureCore product is designed to secure information as it is passed through a graphics processing unit (GPU) for display. SecureCore is an option to CoreAVI's ArgusCore OpenGL drivers to address potential security vulnerabilities within the GPU/OpenGL management of data. This provides a high level of information assurance for systems that manage confidential and classified information alongside unclassified data rendering to one or more displays.

SecureCore protects rendering surfaces from access from unauthorized partitions and adds a memory clear function to video memory allocations to protect previous memory contents from unauthorized access. It is designed to use GPU hardware functions for memory management and virtualization to provide data security. Additional features include clearing video memory before allocating, accessibility to inspect source code, and ability to witness driver build. It supports RTOS including VxWorks, SYSGO PikeOS, Green Hills Integrity, DDCI-Deos, Lynx Software LynxOS, and Linux. It can be fully integrated with CoreAVI's ArgusCore (OpenGL) graphics drivers with HyperCore with no changes to APIs. It also supports use of TrueCore GPU health monitoring in dedicated partitions. SecureCore is available with the following safety certification packages: CertCore178TM (Avionics DO-178C/ED12-C Level A), CertCore26262TM (Automotive ISO 26262 ASIL D), and CertCore50128TM (Railway CENELEC EN-50128 SIL 4).

CoreAVI | www.coreavi.com | www.mil-embedded.com/p374366



SBC with Intel Xeon D-1500 multicore processor

The C876 is a 3U VPX single-board computer (SBC) for embedded and harsh-environment systems applications. The C876 has an Intel Xeon D-1500 (formerly Broadwell DE) silicon on chip (SoC) platform with as many as 12 cores. It features onboard I/O – including 10 Gb Ethernet, graphics, RS 232/422 serial/USB 3.0 and 2.0 ports – as well as other enhancements and Xeon-powered, integrated subsystems.

Other features include a 16 GB DDR4-2133 SDRAM with ECC, up to 64 GB of onboard SATA III flash disk, onboard graphics consisting of VGA via SMI750 on PCIe, dual 10GBase-KR and dual 1000BaseT Ethernet, eight-lane PCIe Gen 3 XMC slot, real-time clock, and temperature sensors. The 3U VPX SBC can be either conduction-cooled or air-cooled and is both vibration- and shock-resistant. The C876 includes Intel trusted execution technology and has dual redundant BIOS with auto-failover.

Aitech | www.rugged.com | www.mil-embedded.com/p374367



GaN MMIC power amps enable wide bandwidth spread

The CMPA2735030S and CMPA2735015S from Wolfspeed are gallium nitride (GaN) high-electron-mobility transistor (HEMT)-based monolithic microwave integrated circuits (MMICs) that contain a two-stage reactively matched amplifier design approach, which enables the user to achieve wide bandwidths. According to Wolfspeed, GaN MMICs are higher-performing in some applications compared to silicon or gallium arsenide, including having higher breakdown voltage, higher saturated electron drift velocity, higher thermal conductivity, and greater power density.

The group of power amps is suited for military radar applications involving L-Band, S-Band, X-Band, C-Band, and Ku-Band and are available in both 15 W and 30 W options. The MMICs operate in the 2.7 - 3.5 GHz range and carry an operating voltage of 50 V. The small signal gain is tested at between 30 and 32 dB, while the typical power added efficiency (PAE) is measured at 50 percent. Both can also be packaged in a 5 by 5 mm surface mount QFN-32 package or as bare die.

Wolfspeed | www.wolfspeed.com | www.mil-embedded.com/p374443

Oscilloscope enables Windows or standalone modes

Tektronix has introduced the 5 Series MSO [mixed-signal oscilloscope], which is intended to meet the design challenges of today's more complex embedded systems. The 5 Series MSO includes what the company terms calls FlexChannel technology, which enables a view of four, six, or eight analog channels and as many as 64 digital channels. Digital signals are sampled, triggered, and stored the same as analog signals. It also features an integrated protocol analysis and signal generator; a new 12-bit signal acquisition system; a large-area, high-def capacitive touch display; and a Direct Access user interface. Users can drive the oscilloscope using either a mouse or with the conventional front-panel controls.

The 5 Series MSO leverages a newly launched front-end amplifier that lowers noise about 4.5 dB from the previous generation's scopes. It also uses a 12-bit analog-to-digital converter (ADC) and a high-resolution mode that delivers as much as 16 bits of vertical resolution. In addition, the 5 Series MSO can run as either a dedicated scope or in an open Windows configuration; the user can switch between the two by adding or removing a solid-state drive (SSD) that has the Windows license/OS installed on it. When the SSD is installed, the instrument boots Windows; when it's removed, the instrument boots as a dedicated scope; either way, the tool's user interface is identical.

Tektronix | www.tek.com | www.mil-embedded.com/p374444



SSASM aimed to boost immunity from GPS spoofing, jamming

The SyncServer S650 SAASM Time and Frequency Instrument from Microsemi is designed for high security,

modern military electronics, and networks that require accurate and adaptable synchronization performance. The base timing I/O module has eight BNC connectors that come standard with the most popular timing I/O signals (including IRIG B, 10 MHz, 1PPS). Users who need additional flexibility can use the S650's FlexPort technology option, which enables six of the BNCs to output any supported signals (time codes, sine waves, or programmable rates), all configurable in real time via the secure web interface. Similar functionality is also applied to the two input BNCs. The FlexPort technology can allow up to 12 BNCs output in any combination of supported signal types.

For applications requiring superior low phase noise (LPN) 10 MHz signals, two different LPN modules are available; each LPN module features eight isolated 10 MHz LPN outputs. The GPS SAASM GB-GRAM MPE-S Type II PPS receiver enables accuracy of <20 ns RMS to UTC (UNSO). In addition, the hardware has been subjected to MIL-STD-810G testing, the operating temperature ranges from -20 °C to 65 °C, and the tool has a dual power-supply option. Users can upgrade to a high-performance oscillator, such as a Rubidium atomic clock, to keep the S650 accurate for long periods in the event of a GPS service disruption.

Microsemi | www.microsemi.com | www.mil-embedded.com/p374445

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

PICMG

Counterfeit parts

Data Security



DARPA's Electronics Resurgence Initiative addresses eventual saturation of Moore's Law

By Mariana Iriarte, Associate Editor



In an effort to address Moore's Law before engineers run out of time, Defense Advanced Research Project Agency (DARPA) officials recently launched the Electronics Resurgence Initiative (ERI). The initiative consists of six programs in which engineers from government, industry, and academia, will spend the next four years scrutinizing the three pillars of the program – materials and integration, circuit design, and systems architecture – to ensure that technological progress continues at the same rapid pace. Moore's Law – the prediction that the number of transistors in a dense integrated circuit doubles approximately every two years – has held true in the microelectronics world over the past five decades. Now, however, engineers realize that the fast clip of technological innovation will eventually outpace Moore's Law.

Before DARPA rolled out its ERI, Dr. Bill Chappell, director of DARPA's Microsystems Technology Office (MTO), and other DARPA representatives spent the summer of 2017 speaking with representatives from private commercial industry. The results of the research and investigation pushed MTO to launch ERI. DARPA officials realized the potential of working with industry alongside the Department of Defense (DoD) to innovate in the area of national security, Chappell says.

The growing complexity of systems has undoubtedly pushed DARPA and industry to think way ahead of the game: Because of the pace of innovation and style of corporate product development, says Chappell, it has become hard for the DoD to keep up with trends in design and manufacturing. The ERI wants to address the current issues with Moore's Law from design concept to physical products.

ERI builds on years of experience and past programs that also address the three pillars of materials, circuit design,

and systems architecture. For this specific initiative, DARPA is taking it a step further with its university-based program: Joint University Microelectronics Program (JUMP), which DARPA says intends to "build up a fundamental research base in fields underlying microelectronics technologies."

DARPA wants to ensure that this initiative is successful: The Broad Agency Announcements (BAA) posted calls for a \$75 million per year investment to overcome the current challenges and eventually create the autonomous, intelligent systems that are currently out of reach.

The systems architecture pillar will encompass the Software-Defined Hardware (SDH) and Domain-Specific System on a Chip (DDSoC) programs, both of which address the concerns around big data. SDH, especially, wants to find the most efficient way to get more data in a network, Chappell explains. In a similar vein, the DDSoC aims to revolutionize how systems recognize the type of data in use and reconfigure themselves as needed in the moment.

The Intelligent Design of Electronic Assets (IDEA) program and the Posh Open Source Hardware (POSH) program will fall under the circuit design umbrella, while the materials and integration pillar houses the Three Dimensional Monolithic System-on-a-Chip (3DSoC) program and the Foundations Required for Novel Compute (FRANC) program.

The following provides a small glimpse into each. For more information, visit the DARPA website (www.DARPA.mil).

➤ **Three Dimensional Monolithic System-on-a-Chip (3DSoC) program**
The aim is to develop design tools, materials, and fabrication techniques in order to build "microsystems on a single substrate with a third upward dimension, compared to

the usual flat, two-dimensional format for microelectronic chips," DARPA says.

- **The Foundations Required for Novel Compute (FRANC) program**
FRANC aims to transcend the traditional von Neumann architecture, which throttles performance because it cannot simultaneously perform both an instruction fetch and data operation. DARPA states that "those submitting research proposals for this program will need to show how they might overcome this 'memory bottleneck.'"
- **The Intelligent Design of Electronic Assets (IDEA) program**
IDEA wants to take the human out of the equation. The end goal will be to enable a nonexpert user to design complex electronic technologies.
- **The Posh Open Source Hardware (POSH) program**
Alongside IDEA, POSH wants to "deliver an open-source design and verification framework, including technologies, methods, and standards, which would enable cost-effective design of ultracomplex SoCs," according to DARPA.
- **Software Defined Hardware (SDH) program**
DARPA says that the goal of this program is to develop a "decision-assistance technology base for designing and manufacturing reconfigurable hardware and software that can run data-intensive algorithms."
- **Domain-Specific System on a Chip (DDSoC) program**
The program seeks to "develop multi-application systems through a single programmable framework," according to DARPA documents.

For more information on the ERI, visit the DARPA website at www.darpa.mil/news-events/2017-09-13.

U.S. Army Research Laboratory models predict cyber intrusions

By Sally Cole, Senior Editor



Researchers from the Army Research Laboratories (ARL) have found that the number of cyber intrusions into a system can be predicted, particularly if analysts are already observing activities on a company or government organization's computer network.

Cyber intrusions are difficult to prevent if an attacker wants access to that data badly enough, so it's helpful to know how often it is likely to occur before undertaking the work of designing network cybersecurity and resilience postures.

The empirical data for the ARL work came from a cyberdefense services provider, which was defending organizations during intrusions. The researchers were able to tap this information to find the correlation – or lack of one – between the number of successful intrusions and certain features observed for 41 different organizations.

To get at the answer, the researchers scrutinized security incident reports containing detailed information about malicious activities and computer security policy violations by users and operators; DNS traffic, collected with specialized and open source software for all organizations within the study; and other data sources describing a selected subset of features of each organization's network topography and cyber footprint.

Based on this data, they proposed four generalized linear models (GLMs) to predict the number of successful cyber intrusions into an organization's network, for which the rate of intrusions is a function of several observable characteristics of the organization. The researchers took this a step further by additionally analyzing regression results for a fit to the intrusion data.

What did they discover? "One of these models – the generalization of the Poisson regression model to the negative binomial GLM – predicts the response variable appreciably better than others," says Dr. Nandi O. Leslie, part of the ARL's Network Security Branch. Moreover, intrusion data shows "sufficient regularity in a statistical sense, and the construction of a practically useful predictive model is feasible."

One of the key research questions the group was exploring – that asking which of the initially conjectured predictor variables should be included in the model – brought some surprises, she adds.

"Several of the predictor variables that were recommended to the researchers by subject matter experts (SMEs) turned out to be lacking in influence or were even misleading," Leslie explains. For example, they felt "that the extent to which an organization is visible on the Internet, as measured by the number of records found related to that organization on the popular Google Scholar, would be a significant predictor of intrusion frequency." It turns out, however, that visibility alone isn't a useful predictor of successful intrusions.

Another variable that the SMEs expected to be influential – the number of hosts within an organization's network – also turned out to be less significant as a predictor for the GLMs than anticipated.

But, as you might expect, the researchers found that the number of violations of an organization's internal cybersecurity policies is a strong predictor of the number of intrusions. "This is rather intuitive," Leslie says. "If users such as employees of the organization lack the discipline or knowledge to comply with organizational cyber

Dr. Nandi O. Leslie is part of an Army Research Laboratory group that explored empirical data from successful cyber intrusions committed against a variety of organizations. Photo credit: Jhi Scott, U.S. Army photographer.



hygiene policies and if the organization is unable or unwilling to enforce its own policies, it's easy to expect that the organization's cyber defenses are poor and lead to more frequent intrusions."

Or maybe not quite so intuitive: "The frequency of accesses by the organization's networks to the domains domestic.net and foreign.net are strong predictors of intrusions," Leslie says.

What can the researchers' predictive models be used for? One option is to help managed security service providers, which are often hired by government and defense organizations to provide their cyberdefense services, estimate how many intrusions might be expected during a certain time period. This metric is important because the cost of doing business is influenced by the number of intrusions experienced by clients of managed security service providers.

These types of models can "contribute to our fundamental understanding of cyber situational awareness and ways to monitor, quantify, and manage cyber risk," according to the researchers.

Models of this nature "may offer clues toward enhancing the security posture and perhaps the design and operation of an organization's computing systems and networks," the researchers report. "If the model indicates that certain characteristics are associated with an increased number of intrusions, the organization might be able to find ways to modify those characteristics."

CHARITY



FourBlock

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 FourBlock, a 501(c)(3) non-profit organization that aims to act as the country's local network for leading veteran professionals.

Mike Abrams, who formerly served in the Marine Corps, founded FourBlock in a bid to equip post-9/11 student veterans to find meaningful careers and maximize their potential through an educational program and a nationwide network of alumni and partners. At the foundation of the FourBlock approach is a semester-long program – held in conjunction with a number of accredited colleges and universities around the U.S. – in which each FourBlock student group may engage with their educational instructors and executive mentors in order to open paths to the best careers possible.

The foundation operates campus programs in 12-plus geographical locations, including at Columbia University (New York), Auburn University (Alabama), University of Washington (Seattle, Washington), and Northwestern University and University of Chicago (Illinois). FourBlock has also worked with companies to introduce veterans to such companies as JPMorgan Chase, Citigroup, Accenture, Amazon, Facebook, GE, and Goldman Sachs.

According to the organization, the typical veteran that signs on with the FourBlock program is typically in their junior year of undergraduate studies or first year of their graduate studies. The typical cohort is roughly 75 percent former enlisted and 25 percent former officers, with the majority of them pursuing a bachelor's or MBA degree. About 60 percent of those in the programs are interested in finance, international affairs, and consulting careers, with the remainder interested in accounting, cybersecurity, engineering, intelligence, IT, journalism, and marketing.

For more information, please visit www.fourblock.org.

E-CAST

Solving real-time direction-finding and spectrum monitoring with software-defined radios

Sponsored by National Instruments

As the variety and complexity of communication systems in the modern RF battlefield increase, the need to quickly design, deploy, and field upgrade spectrum monitoring and direction-finding solutions becomes paramount. Software-defined radio (SDR) platforms for these applications need to cover wide frequency ranges, process high bandwidth data in real time, provide synchronization scalable across multiple channels, and support flexible development tools.

In this e-cast, National Instruments (NI) leads a discussion regarding the next generation of flexible and powerful commercial off-the-shelf (COTS) SDRs that enable direction-finding, spectrum monitoring, and radio functionality. Additional topics will include key RF system requirements, an overview of multiple software tool flows, and a demonstration of a reference direction-finding application.

View archived e-cast: ecast.opensystemsmedia.com/751

View more e-casts:

<http://opensystemsmedia.com/events/e-cast/schedule>

WHITE PAPER

DO-178C: Get on a high with your software development

Sponsored by LRDA

The DO-178 guidance document "Software Considerations in Airborne Systems and Equipment Certification" has been the driving force in the area of aerospace and flight safety since it was published in 1982. Following a rewriting in 1992 and an update in 2011 as DO-178C, its processes and procedures continue to be a technical challenge and an administrative headache.

In this white paper, learn about the automated tools – for performing analysis, test, and traceability – that can help developers meet the objectives of the DO-178C standard, including bidirectional traceability, test management, source code static analysis, and dynamic analysis of both source and object code.

Read this white paper:

<http://www.embedded-computing.com/military-white-papers/lrda-tool-suite-and-do-178c-technical-briefing-5>

Read more white papers:

<http://mil-embedded.com/white-papers>





NOW COTS MEANS COTS



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

Meet *Lightning*, Abaco's new mission ready system platform. It's designed specifically to deliver application-specific I/O – without penalty.

But that's not all that *Lightning* brings. It also significantly eases the design process because one *Lightning*-enabled mission computer is identical to the next in terms of size, form factor and pinout. Similarly with *Lightning*-enabled graphics computers.

And because *Lightning* mission ready systems are modular by design, upgrade is simple, straightforward – and cost-effective.

Sound too good to be true? Let us convince you. abaco.com/lightning

WE INNOVATE. WE DELIVER. **YOU SUCCEED.**

Now Available:
**2X Channel
Density**

Unfair Advantage.

2X HIGHER performance | **4X FASTER** development

Introducing Jade™ architecture and Navigator™ Design Suite, the next evolutionary standards in digital signal processing.

Pentek's new Jade architecture, based on the latest generation Xilinx® Kintex® Ultrascale™ FPGA, doubles the performance levels of previous products. Plus, Pentek's next generation Navigator FPGA Design Kit and BSP tool suite unleashes these resources to speed IP development and optimize applications.

- **Streamlined Jade architecture** boosts performance, reduces power and lowers cost
- **Superior analog and digital I/O** handle multi-channel wideband signals with highest dynamic range
- **Built-in IP functions** for DDCs, DUCs, triggering, synchronization, DMA engines and more
- **Board resources** include PCIe Gen3 x8 interface, sample clock synthesizer and 5 GB DDR4 SDRAM
- **Navigator Design Suite** BSP and FPGA Design Kit (FDK) for Xilinx Vivado® IP Integrator expedite development
- **Applications** include wideband phased array systems, communications transceivers, radar transponders, SIGINT and ELINT monitoring and EW countermeasures

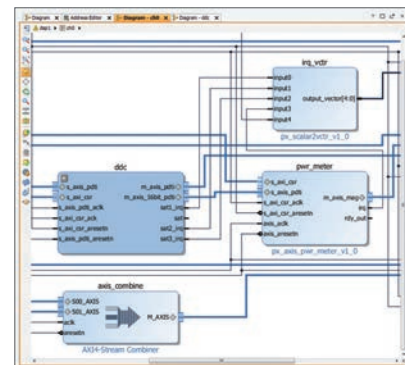
All this plus FREE lifetime applications support!



Jade Model 71131 XMC 8-channel module, also available in VPX, PCIe, cPCI and AMC with rugged options.



Kintex Ultrascale FPGA



Navigator FDK shown in IP Integrator.



See the Video!

www.pentek.com/go/mesjade or call 201-818-5900 for more information

