

# Military

## EMBEDDED SYSTEMS

INCLUDING **DEFENSE TECH WIRE**

**John McHale**  
Remembering Ron Mastro

**Field Intelligence**  
Avionics data bus tackles SWaP

**Mil Tech Insider**  
Cheaper by the dozen (volts)

April/May 2013  
Volume 9 | Number 3

MIL-EMBEDDED.COM

Securing  
the cloud for  
DoD applications



Full speed ahead: FACE initiative fosters reuse,  
cuts costs and delivery time of military avionics systems  
Q&A with Jeff Howington, Vice Chairman of the FACE Steering Committee

Commonality and  
reduced SWaP drive  
vetronics designs





# Small Size Big Performance Perfect Fit



Models for horizontal  
or vertical mounting



## The Rugged AB3000 Avionics Computer

The AB3000 from Ballard Technology is small, lightweight and loaded with capabilities for easy integration into today's modern aircraft, UAVs, and ground mobile platforms. With an efficient Intel® E680T processor, MIL-STD-1553 and ARINC 429/708/717 interfaces, Ethernet, USB, video, audio, and PMC expansion, this rugged, conduction-cooled COTS device is ready to take on all of your toughest computing and interface problems.

**Performance and versatility in less space ... that's the AB3000.**

Visit our website or call 425.339.0281 for more information.

**Ballard**   
TECHNOLOGY  
AN ASTRONICS COMPANY

### Key Features...

#### Optimal SWaP

Minimal size, weight, and power

#### Next-Generation Intel Processor

With Hyper-Threading and virtualization

#### High I/O Density

2D/3D video, audio, avionics databus interfaces, serial, discretes, and more

#### Reliable Power

Conforming to vehicle and aircraft standards

#### Smooth Durable Housing

Easy hose down; salt fog resistant

[www.ballardtech.com/AB3000](http://www.ballardtech.com/AB3000)

AS9100 / ISO 9001 Registered



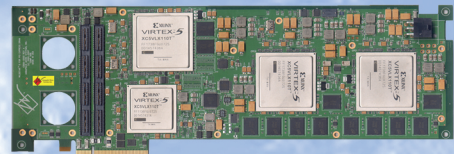
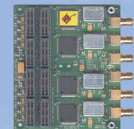
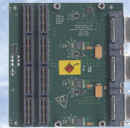
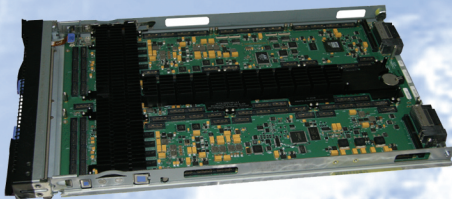
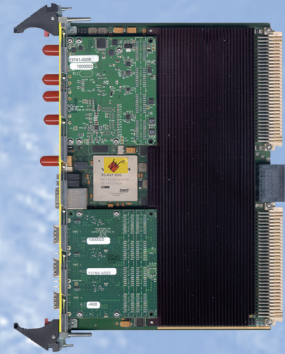
# **Annapolis Micro Systems**

## **The FPGA Systems Performance Leader**

### **High Performance Signal and Data Processing in Scalable FPGA Computing Fabric**

**GEOINT, Ground Stations, SDR, Radar, Sigint, COMINT,  
ELINT, DSP, Network Analysis, Encryption, Image  
Processing, Pattern Matching, Oil & Gas Exploration,  
Financial Algorithms, Genomic Algorithms**

***Direct Seamless Connections with no Data Reduction  
Between External Sensors and FPGAs  
Between FPGAs and Processors over IB or 10GE  
Between FPGAs and Standard Output Modules  
Between FPGAs and Storage Arrays***



#### **Ultimate Modularity**

**From 1 to 8 Virtex 4, 5 or 6 FPGA/Memory Modules  
Input/Output Modules Include:**

**Quad 130 MSPS thru Quad 550 MSPS A/D  
1.5 GSps thru 5.0 GSps A/D, Quad 600 MSps D/A,  
Dual 1.5 GSps thru 4.0 GSps D/A  
Infiniband, 10G, 40G or 100G Ethernet or SFPDP**

**VME/VXS/VPX, IBM Blade, PCI-X/PCI Express, PMC/XMC, MicroTCA**

**No Other FPGA Board Vendor Streams This Volume of Data  
Real Time Straight Into the Heart of the Processing Elements  
and Then Straight Back Out Again**

**190 Admiral Cochrane Drive, Suite 130, Annapolis, Maryland USA 21401  
wfinfo@annapmicro.com USA (410) 841-2514 www.annapmicro.com**



### ON THE COVER:

**Top photo:** DoD officials are turning toward cloud computing for its huge cost savings and operational efficiency benefits but are moving cautiously to assure they have plugged all the potential cyber security vulnerabilities inherent in something as nebulous as a virtual cloud.

**Bottom photo:** Commonality and reduced Size, Weight, and Power (SWaP) requirements are driving vetronics designs in platforms such as the Joint Light Tactical Vehicle (JLTV). Photo courtesy of Lockheed Martin



April/May 2013 | Volume 9 | Number 3

## COLUMNS

### Editor's Perspective

- 8 Remembering a friend and mentor  
*By John McHale*

### Field Intelligence

- 10 Avionics data bus technology meets the SWaP challenge  
*By Charlotte Adams*

### Mil Tech Insider

- 11 Mil system power is cheaper by the dozen (volts)  
*By Eran Strod*

## BONUS FEATURE: INTERVIEW

- 16 Full speed ahead:  
FACE initiative fosters reuse,  
cuts costs and delivery time of  
military avionics systems  
*Q&A with Jeff Howington, Vice Chairman  
of the FACE Steering Committee*

## DEPARTMENTS

- 12-14 **Defense Tech Wire**  
Connecting with Mil Embedded  
*By Sharon Hess*

- 44-45 **Editor's Choice Products**

## EVENT

### AUVSI's Unmanned Systems 2013

August 12-15 • Washington, D.C.

[www.auvsishow.org/auvs13/public/enter.aspx](http://www.auvsishow.org/auvs13/public/enter.aspx)

## 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>

Published by: **OpenSystems media.**

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

© 2013 OpenSystems Media  
© 2013 Military Embedded Systems  
ISSN: Print 1557-3222

**ENVIROINK**  
The inks used to print the body of this publication contain  
a minimum of 20% by weight, renewable resources.



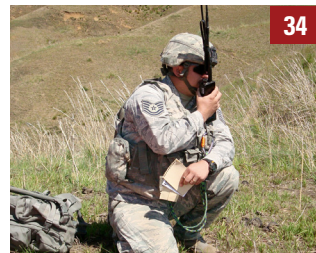
### SPECIAL REPORT | Vetronics

- 22 Commonality and reduced SWaP drive vetronics designs  
*By John McHale*



### MIL TECH TRENDS | Cyber security

- 28 Cloud security and the DoD  
*By John McHale*
- 34 Encryption and the migration to  
COTS technologies  
*By Rubin Dhillon, GE Intelligent Platforms  
and Jim Kelly, Juniper Networks*



### INDUSTRY SPOTLIGHT | Cloud computing

- 40 Deploy warfighter applications  
faster with open source  
Platform-as-a-Service  
*By David Egts, Red Hat*



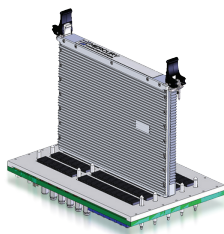
@military\_cots

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



# *Innovation* **That Cools.**

MERCURY OFFERS INDUSTRY-LEADING INNOVATIONS IN THERMAL MANAGEMENT FOR AIR-COOLED, CONDUCTION-COOLED AND VITA48 SUBSYSTEM CHASSIS. OUR SOLUTIONS, SUCH AS THE NEW AIR FLOW-BY™, TRANSFER MASSIVE AMOUNTS OF THERMAL ENERGY AT THE INDIVIDUAL COMPONENT, MODULE AND SUBSYSTEM LEVEL — WHILE STILL OVERCOMING THE MOST CHALLENGING SWaP REQUIREMENTS FOR THE OVERALL SOLUTION. NOW CUSTOMERS CAN TAKE FULL ADVANTAGE OF HIGH-POWER SENSOR PROCESSING TECHNOLOGIES.



## **Other Mercury Innovations**

*Big Data streaming analytics*  
*Electronic countermeasures*  
*High-density storage*  
*High-performance computing*  
*Mission security*  
*Open EW architecture*  
*Thermal management*



 **MERCURY**  
SYSTEMS™

INNOVATION THAT MATTERS™

Visit [mrcy.com/mes](http://mrcy.com/mes) to see how Mercury Systems' signal and image processing innovations help deliver unrivalled performance.



## Military Embedded Systems Editorial/Production Staff

John McHale, Editorial Director  
jmchale@opensystemsmedia.com  
Sharon Hess, Managing Editor  
sharon\_hess@opensystemsmedia.com

Steph Sweet, Creative Director  
ssweet@opensystemsmedia.com

## Sales Group

Tom Varcie  
Senior Account Manager  
tvarcie@opensystemsmedia.com  
Rebecca Barker, Strategic Account Manager  
rbarker@opensystemsmedia.com  
Eric Henry, Strategic Account Manager  
ehenry@opensystemsmedia.com  
Ann Jesse, Strategic Account Manager  
ajesse@opensystemsmedia.com  
Christine Long  
Vice President, Online Business  
clong@opensystemsmedia.com

### International Sales

Elvi Lee, Account Manager – Asia  
elvi@aceforum.com.tw  
Gerry Rhoades-Brown  
Account Manager – Europe  
gerry.rhoadesbrown@husonmedia.com

Christian Hoelscher  
Account Manager – Europe  
christian.hoelscher@husonmedia.com

Lauren Palmer  
Account Manager – Europe  
lauren.palmer@husonmedia.com

### Regional Sales Managers

Barbara Quinlan, Southwest  
bquinlan@opensystemsmedia.com  
Denis Seger, Southern California  
dseger@opensystemsmedia.com  
Sydele Starr, Northern California  
sstarr@opensystemsmedia.com  
Ron Taylor, East Coast/Mid Atlantic  
rtaylor@opensystemsmedia.com

## Reprints and PDFs

republish@opensystemsmedia.com

## OpenSystems Media Editorial/Production Staff



John McHale  
Editorial Director  
Military Embedded Systems  
jmchale@opensystemsmedia.com  
Sharon Hess  
Managing Editor  
Military Embedded Systems  
Embedded Computing Design  
Industrial Embedded Systems  
sharon\_hess@opensystemsmedia.com  
Jerry Gipper, Editorial Director  
VITA Technologies  
jgipper@opensystemsmedia.com  
Warren Webb, Editorial Director  
Embedded Computing Design  
Industrial Embedded Systems  
webb@opensystemsmedia.com  
Joe Pavlat, Editorial Director  
xTCA and CompactPCI Systems  
jpavlat@opensystemsmedia.com

Monique DeVoe  
Assistant Managing Editor  
VITA Technologies  
EDA Digest  
DSP-FPGA.com  
mdevoe@opensystemsmedia.com

Brandon Lewis  
Associate Editor  
xTCA and CompactPCI Systems  
PC/104 and Small Form Factors  
blewis@opensystemsmedia.com

Curt Schwaderer  
Technology Editor

Steph Sweet  
Creative Director

David Diomede, Art Director

Joann Toth, Senior Designer

Konrad Witte, Senior Web Developer

Matt Jones, Web Developer

## Editorial/Business Office

Patrick Hopper, Publisher  
Tel: 586-415-6500 ■ Fax: 586-415-4882  
phopper@opensystemsmedia.com  
Subscriptions Updates  
www.opensystemsmedia.com/subscriptions  
Karen Layman, Business Manager  
30233 Jefferson  
St. Clair Shores, MI 48082

Rosemary Kristoff, President  
rkristoff@opensystemsmedia.com  
Wayne Kristoff, CTO  
16626 E. Avenue of the Fountains, Ste. 201  
Fountain Hills, AZ 85268  
Tel: 480-967-5581 ■ Fax: 480-837-6466

Page	Advertiser/Ad Title
38	<b>ACCES I/O Products, Inc.</b> – USB embedded I/O solutions rugged, industrial strength USB
29	<b>Alphi Technology Corporation</b> – Looking for I/O for your mission computer?
19	<b>AMP Inc. Accelerated Memory Production</b> – High durability standards for the DDR3 ruggedized SO-DIMM
3	<b>Annapolis Micro Systems, Inc.</b> – High performance signal and data processing
27	<b>Avalon Defense Ltd.</b> – Protocol converters
27	<b>Avalon Defense Ltd.</b> – Low-cost MIL-STD-704 power supplies
2	<b>Ballard Technology</b> – The rugged AB3000 avionics computer
9	<b>D-TA Systems</b> – From DC to daylight ... Scan, detect, process, record and playback RF signals at will
25	<b>Excalibur Systems, Inc.</b> – Dragon – it's not a myth
47	<b>GE Intelligent Platforms, Inc.</b> – Enabling and securing the connected warfighter
23	<b>Interface Concept</b> – Switches and IP routers
15	<b>Kontron</b> – Streamline your next-gen technology upgrades
5	<b>Mercury Systems</b> – Innovation that cools
33	<b>North Atlantic Industries</b> – Up to 136 programmable discrete I/O channels ... on one rugged board
37	<b>Parvus Corporation</b> – Qualified to perform
48	<b>Pentek, Inc.</b> – Get tough software radio design challenges?
43	<b>Phoenix International</b> – Introducing RPC 24 – rugged, deployable, mission oriented data storage
39	<b>Proto Labs</b> – Others say they're fast ... But do they have the scale to deliver?
21	<b>SynQor</b> – Mil-COTS DC-DC power converters
20	<b>TeleCommunication Systems, Inc. (TCS)</b> – Toughest SSDs on the planet
7	<b>X-ES</b> – Searching for Intel Core i7 processor solutions?



# SEARCHING FOR Intel® Core™ i7 PROCESSOR SOLUTIONS?



## Your search is over!

CompactPCI • COM Express • VME • PrPMC/XMC • VPX • Custom

X-ES delivers the latest 3rd generation Intel® Core™ i7 processor solutions on the widest range of standard and custom form factors in the industry. With our proven record of meeting aggressive schedules, you can count on X-ES to deliver Intel Core i7 processor solutions on time, and with unparalleled customer support. **Call us today to learn more.**

**You need it, we have it! That's Extreme.**

# X-ES

**Extreme Engineering Solutions**  
608.833.1155 [www.xes-inc.com](http://www.xes-inc.com)

# Remembering a friend and mentor

By John McHale, Editorial Director



My girlfriend tells me that I'd light up like a Christmas tree whenever I'd see my friend and former boss, Ron Mastro, retired publisher of *Military & Aerospace Electronics* magazine. How could anyone not? The man had buckets of charisma and when he turned on his high beams, you couldn't help but smile. The laughs and smiles will stay with me even though I had to say goodbye to him this spring after he lost his battle with lung and brain cancer. Ron was a month shy of his 71st birthday.

For close to 15 years he led the magazine and its affiliated COTScon show – later called the Military & Aerospace Electronics Forum. A Navy veteran, Ron thrived in the military electronics market and took great pride that his little publishing niche covered an institution – the U.S. military – that he loved and respected. Though considered a bit of a maverick by his bosses, his leadership style generated loyalty as well as revenue, as he ran a profitable media franchise year after year for PennWell.

Ron's staff loved him because he treated them more like a family than a staff. He always preached that we keep disagreements in the family, solve them in the family. He was loyal to us and we were loyal to him. As a result, we had a close-knit core staff – publisher, sales rep, and two editors – who stayed together from the time I joined the magazine in 1996 until Ron retired in 2008. Very little turnover, and Ron was a big reason for that.

A born bon vivant and raconteur, he launched countless friendships every time he said, "Hi, I'm Ron Mastro." Ron told me he tried to get everyone to like him – whether it was a potential customer, a waitress, bellhop, valet, police officers, and so on. They didn't always like him back, as Ron was opinionated – especially about his Republican politics. He even held a small, elected office in

New York in the 1980s. Never shy, Ron said whatever was on his mind. He once joked with an executive during a budget meeting to "hurry it up, you're cutting into my nap time." Ron also had Irish diplomacy, in other words "the ability to tell a man to go to hell and make him look forward to the trip." He'd chew out a colleague, only to have the same guy call and thank him an hour later.

There are tons of stories like that about Ron, most of which I can't tell here because he flavored his speech with four-letter words befitting the sailor he was – a former Navy Asst. 1st Class Petty Officer serving on a Navy HSS-2 Sea King helicopter – later designated the SH-3A. Ron was a well-read storyteller with a colorful lack of a filter that endeared him to his friends and colleagues.



***"Ron was a human  
social network long before  
there was ever a LinkedIn  
or a Facebook."***



He was a human social network long before there was ever a LinkedIn or a Facebook. "I channeled Ron today," an introverted mutual friend told me after hearing Ron passed away. "I said hi to every stranger who crossed my path, asked how they were doing, asked their names. I connected with people and it felt good to be like Ron."

Ron was known for hugging his way out of the office and that's how he went through life too. Delivered devastating news that cancer had spread to his brain, Ron did what any of us would do and had a pity party. However, Ron's pity party was a cocktail party with wine, whiskey, and beer flowing for 30 of his



**Figure 1** | The laughs and smiles will stay with me even though I had to say goodbye to Ron Mastro, my friend and former boss, this spring after he lost his battle with lung and brain cancer.

closest friends in The Villages, a golf-cart retirement community in Florida. The Villages is advertised as "America's friendliest hometown" – the perfect place for Ron. He spent most of his last five years there trying to break 90 in golf, reading historical novels and the works of political columnists, and enjoying his children and grandchildren.

Fortunately for me, Ron retired near my parents and I was able to golf, drink wine, and spend time with him every few months. I can still see him now, drinking a whiskey on the rocks on his Florida porch or outside a hotel bar on the road, saying: "John, are you happy?" He meant happy in my job, my love life, or just that day. Well, I am happy. Happy and grateful I knew and loved a man like him. Through the years Ron was at times a boss, a second father, a mentor, and a golf buddy, but most of all he was my friend. One of the best I ever had and I miss him terribly.

Ron leaves his wife of nearly 49 years, Cheryl; daughters Deidre, Danielle, and Megan; and five grandchildren. The family has asked that donations be made to the Wounded Warrior Project foundation in Ron's name online at [www.woundedwarriorproject.org](http://www.woundedwarriorproject.org).

John McHale  
[jmchale@opensystemsmedia.com](mailto:jmchale@opensystemsmedia.com)



# From DC to Daylight.... Scan, Detect, Process, Record & Playback RF Signals at Will

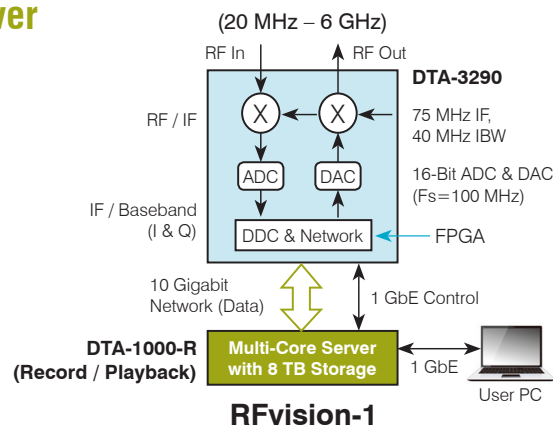
## RFvision-1 Wideband (40MHz) Scanning Transceiver



Shock-protected packaging

- 0.02 – 6 GHz frequency coverage
- 40 MHz instantaneous BW
- 16-Bit ADC & DAC
- FPGA based programmable DDC for complex baseband conversion
- Real-Time recording (over 11 hrs for 40 MHz BW)
- Optional RF playback of recorded & simulated signal
- Convenient & failsafe GUI for control and display

**DTA-3290 (1U)**  
**DTA-1000-R (1U)**



Click "RFvision-1 Wideband Scanning Transceiver" on our home page.

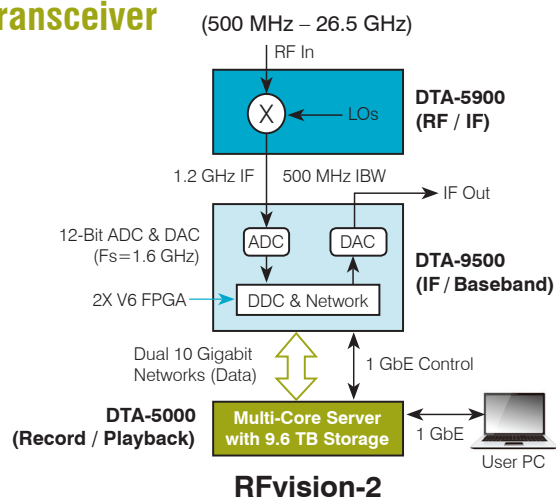
## RFvision-2 Ultra-Wideband (500 MHz) Scanning Transceiver



Shock-protected packaging

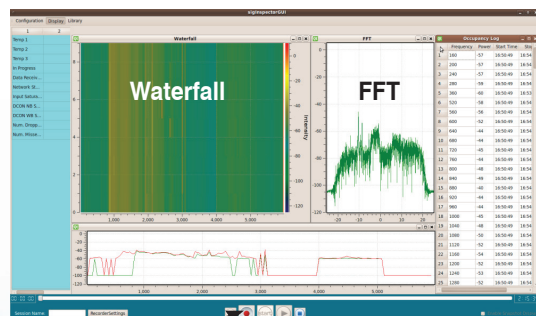
- 0.5 – 26.5 GHz frequency coverage
- 500 MHz instantaneous BW
- 12-Bit ADC & DAC
- FPGA based DDC for complex baseband conversion
- Real-Time recording for hours
- Optional IF playback of recorded & simulated signal
- Convenient & failsafe GUI for control and display

**DTA-5900 (1U)**  
**DTA-9500 (1U)**  
**DTA-5000 (3U)**



Click "RFvision-2 Ultra-Wideband Scanning Transceiver" on our home page.

## SigInspector™ GUI



- 'Plug & Play' solutions with D-TA's SigInspector™ GUI
- Rapid user development using D-TA's Software Development Kit (SDK) and support

**DTA**  
D-TA SYSTEMS INC.  
A Sensor Interface and Processing Company  
**www.d-ta.com**

sales@d-ta.com 1-877-382-3222

**SPECTRUM INTELLIGENCE FROM D-TA  
NOTHING ELSE COMES CLOSE!**

# Avionics data bus technology meets the SWaP challenge

By Charlotte Adams

*A GE Intelligent Platforms perspective on embedded military electronics trends*



In military avionics, SWaP is a major challenge. As major contractors refresh and redesign electronics systems, in light of less funding availability, they are asking their suppliers to create smaller, less expensive, subsystem solutions, such as data communications modules. These subsystem solutions, moreover, are expected to be priced and supported as Commercial Off-the-Shelf (COTS) products even though they were created as one-of-a-kind responses to unique requirements.

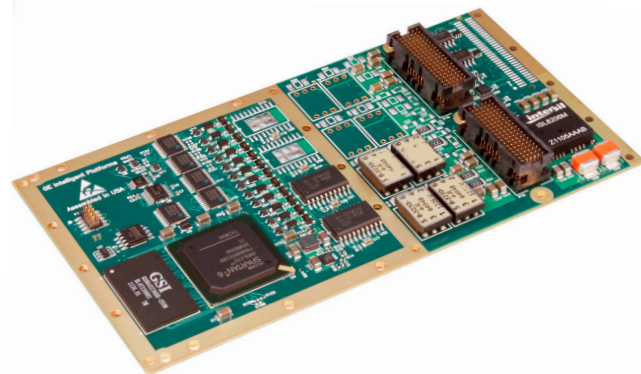
The resolution to the SWaP challenge and the custom/COTS paradox in data bus and other avionics technologies depends on the provider's flexibility, expertise, and the ability to roll new features into its "stable" of standard products, recovering the cost of development and supporting future development with standard product sales. This constant recycling of ideas keeps front-end innovation going, costs contained, customers happy, and the product line on a healthy growth curve.

## Shrinking bus board size and cost

Shrinking the size of a subsystem typically involves consolidating the cards by using smaller, higher-density components. A three-card data bus solution providing multiple channels of multiple bus protocols, for example, can be downsized into a single card by incorporating smaller, less power-hungry components and by implementing some bus elements in more efficient packages. This approach is often a win-win for the customer because – thanks to competitive pressures and the evolution of technology in the market – the new card is likely to cost less than the old ones. The new subsystem will use less power, as well. And the slimmed-down replacement allows the overarching system to be lighter and smaller – always virtues in avionics – or of equivalent size and weight but with more functions and features.

Shrinking the footprint of data bus and other avionics cards is possible, thanks to the trajectory of electronics technology. Moore's Law still holds sway over microelectronics: Components are increasing in density and decreasing in size at a rapid rate. FPGAs, for example, have undergone phenomenal growth in gate counts, while decreasing in size and power consumption. Bus card vendors are finding ways to shrink MIL-STD-1553 and ARINC 429 protocol implementations by incorporating some bus features in FPGAs or ASICs.

An FPGA can incorporate 1553 bus control logic that deciphers bit patterns and generates the proper responses, buffering, and processing for the 1553 bus controller, remote terminal, and monitor functions, as well as PCIe drivers and logic that enable the card to communicate with the host. As FPGA densities increase, more 1553 channels can be implemented on the device. A case in point is the RAR15-XMC, the latest



**Figure 1** | The GE Intelligent Platforms RAR15-XMC is a multiprotocol embeddable avionics module.

GE Intelligent Platforms avionics data bus card, which squeezes four dual-redundant MIL-STD-1553A channels, 10 ARINC 429 receive channels, and eight ARINC 429 transmit channels plus memory and protocol processing into approximately 8 square inches of board real estate (Figure 1). A spinoff from custom mil/aero projects that replaced two- or three-PMC card subsystems with a single XMC module that cut customer costs in half, the RAR15 is a standard, off-the-shelf, conduction-cooled product that implements key 1553 and 429 technology and protocol processing in a single FPGA.

While ASICs can be implemented in smaller sizes than FPGAs and can burn less power, the downside is that when ASICs go obsolete, it's more difficult to migrate the software in them to a new board. FPGAs, on the other hand, are more easily swappable from one generation to another, allowing as close to a drop-in replacement as possible.

Memory densities also have increased, allowing these chips to take up less space. And power circuitry is becoming smaller and more efficient. New data bus cards exploit hardware consolidation, miniaturization, and power savings trends to extract maximum performance for minimum footprint. Data bus card developers use all these opportunities to create customized solutions and then incorporate these advances into standard cards.

## Win-win situation for avionics

Data bus cards, like every other subsystem on an avionics platform, have to earn their way into an aircraft by meeting challenges such as size, weight, and power. By exploiting the trend toward ever smaller, lower-power-yet-denser electronics, designers are able to meet unique system demands while expanding their technology stables.

[defense.ge-ip.com](http://defense.ge-ip.com)



# Mil system power is cheaper by the dozen (volts)

By Eran Strod

An industry perspective from Curtiss-Wright Controls Defense Solutions



Today open standard VME and VPX boards come in three flavors of power: 3.3 V, 5 V, and 12 V. As a result, system designers have to daily confront the extra work and cost of designing custom power supplies when the different boards they select for their system design fall into some mix of the three voltage types. The problem resurfaces when it's time to upgrade the system, since an entirely new power supply with a different mix of voltage types might be required to support the technology refresh. However, there's a better way to solve this challenge – one that delivers some very real, easy-to-understand SWaP-C benefits.

## 50,000-foot view:

### Why homogenous 12 V works best

In recent years, some of the leading COTS vendors have standardized on 12 V as the single power type for all of their new Intel, Power Architecture, FPGA, and GPGPU-based VME and VPX modules. Eliminating the aforementioned mixed-voltage "Tower of Babel" will result in simpler, cleaner, and more easily scaled system designs. One fundamental advantage of standardizing on 12 V is that it is ideal for use in military platforms. 12 V is evenly divisible into the common 48 V telecommunications power supply de facto standard, which makes it easy to take advantage of the wide range of choices and cost efficiencies that flow out of the commercial telco market.

12 V also works natively with the most popular off-the-shelf AC/DC conversion modules found on military platforms. Reducing platform-to-backplane conversion increases power efficiency. Eliminating conversion saves power that would otherwise be wasted. Even better, it reduces space and weight in the system since a single standard 12 V backplane supply can be used to support all boards in the system. Eliminating the need to convert the platform vehicle

power source into separate DC power of 12 V, 3.3 V, and 5 V signals on the backplane enables the system designer to achieve greater efficiency and space savings in the chassis subsystem.



***"Eliminating conversion saves power that would otherwise be wasted.***

***Even better, it reduces space and weight in the system since a single standard 12 V backplane supply can be used to support all boards in the system."***



## System-level view: Pure 12 V benefits

These days, every system designer is tasked with simplifying their designs and supply chains to lower the overall hardware cost of ownership. The single 12 V approach eliminates the time, cost, and hassle of sourcing, maintaining, and storing multiple different power supplies or developing custom chassis supplies. And once a single voltage becomes the standard, it eases, speeds, and simplifies the development of system variants. In one real-world example, a 17-slot system designed to support 12 V boards requires three power slots for three distinct power supplies. If the design included a mix of 12 V and 3.5 V boards, two additional slots out of the 17 available would have to be dedicated to 3.5 V power supplies. Thus, the decision to standardize on 12 V comes from having a system-level view.

Let's say an SBC was based upon 5 V and a DSP module was based on 3.3 V power. The number of boards would drive the requirement for different amounts of each supply. This would

mean a specific power supply for each configuration of boards. A configuration that used two SBCs and one DSP board might need a different power supply than a configuration that used one SBC and two DSP boards. This drives up cost, increases complexity, and reduces the ability to adapt a platform architecture to multiple applications. Not so when all the boards standardize around 12 V. With commonality around 12 V, a single supply can accommodate many different mixes of boards.

Additionally, a 12 V HPEC system could leverage a single system design and leverage that box into many easily configurable variants to address many different applications. An example is the Curtiss-Wright HPEC platform, which offers Intel SBCs, PowerPC SBCs, DSP boards, GPGPU boards, FPGA boards, and VPX switches that can be mixed and matched to meet different application requirements. All of these boards operate principally off of 12 V so the integrator doesn't get into a trap of choosing a power supply with a certain amount of 3.3 V, 5 V, and 12 V power.

## Thwarting the mixed-voltage power dilemma

It's easy to remember: Power comes cheaper by the dozen volts. A homogenous 12 V plan frees the design from custom power supplies, saves slots, simplifies logistics, cuts system weight, and provides opportunities to leverage standard commercial telco power supplies. And because integrators are increasingly trying to leverage intellectual property from one program to others, in today's cost-conscious world, it might just be a matter of survival to operate 12 V lean and mean.

**Eran Strod**  
System Architect  
Curtiss-Wright Controls  
Defense Solutions  
[www.cwcdefense.com](http://www.cwcdefense.com)



# DEFENSE TECH WIRE

NEWS | TRENDS | DOD SPENDS | CONTRACTS | TECHNOLOGY UPDATES

By Sharon Hess, Managing Editor



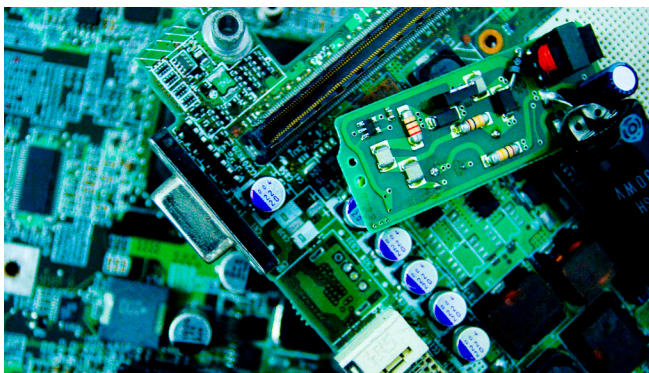
NEWS

## Could silicon become a thing of the past?

It's a foregone conclusion that computing will always be powered by a silicon backbone ... but, is that true? Believing that silicon transistors' improvement limits have nearly been reached, University of Nebraska-Lincoln (UNL) physicists and researchers have been developing a silicon alternative – a mere-atoms-thick ferroelectric oxide layer, touted to result in more storage capability for digital data than silicon, while utilizing less energy as compared to memory based on silicon. The goal is to make significantly more powerful, smaller electronics a reality.

The ferroelectric oxide layer research is based partly on the quantum tunneling phenomenon, where particles penetrate a barrier solely at the atomic or quantum level. Two electrodes have an ultra-thin barrier inserted between them, then electrons – stimulated by applied voltage – produce a current with resistance as they tunnel through the barrier. The ferroelectric oxide provides polarization directions, negative and positive, enabling polarization charge reversal that alters tunnel junction resistance by 100x. These capabilities are in contrast to present-day silicon, which demands more current and more real estate between regions in order to accommodate generated heat.

But don't look for ferroelectric oxide technology at your local Radio Shack just yet. The potentially silicon-replacing technology is only effective when temperatures are a chilly -100 °F or less.



**Figure 1** | Believing that silicon transistors' improvement limits have nearly been reached, University of Nebraska-Lincoln (UNL) physicists and researchers have been developing a silicon alternative – a mere-atoms-thick ferroelectric oxide layer. Stock photo



**Figure 2** | The U.S. Army and The Boeing Co. signed a triad of contracts for CH-47 (pictured) support and system development for the AH-64 Apache Block III. U.S. Army photo by Tech. Benjamin Faske

## Boeing and U.S. Army sign trio of contracts

The Boeing Co. and the U.S. Army Contracting Command located in Redstone Arsenal, AL, put pen to paper three times in one day for a triad of contracts, two of which are almost identical: A contract awarded to Boeing's Ridley Park, PA business for \$22 million for CH-47 helicopter fleet and project management office *deployed* field-service support, plus a nearly \$18 million (maximum value) contract mirrors the first contract exactly, except that it provides for *nondeployed* field-service support (Figure 2). Work under both contracts is anticipated for completion by the end of September, 2015. The third contract was awarded to Boeing's Mesa, AZ business for about \$41 million, covering incremental funding modification for system development for the AH-64 Apache Block III. Work occurs in Mesa, AZ, with completion expected in September 2014.

## Standard Missile-3 gets more support

The venerable Standard Missile-3 will soon gain more in-service engineering support, thanks to a recently awarded Missile Defense Agency contract modification for \$62 million to Raytheon Missile Systems Co. located in Tucson, AZ. The modification raises the contract's cumulative total from \$594 million to nearly \$657 million. Work under the contract modification commences in Tucson, AZ and continues through September 2015. The modification is incrementally funded by Research, Development, Test, and Evaluation (RDT&E) funds for fiscal 2013.

## USAF, Italy, Australia benefit from Lockheed mod

Luke Air Force Base's Pilot Training Center 1 will soon benefit from a recently exercised \$72 million (maximum) modification to the existing U.S. Navy LRIP Lot 6 advance acquisition contract already awarded to Lockheed Martin. The modification covers the training center's support equipment procurement for the F-35 Lightning II Conventional Take-Off and Landing air system program. The mod also covers supplier support tasks under the data quality integration management umbrella, plus products for sustainment data in support of the USAF in addition to the governments of Australia and Italy. The allocations of the contract are: USAF – about 76 percent or just over \$55 million; Australia – 9.5 percent or nearly \$7 million; and Italy – just over 14 percent, at about \$10 million. Work under the modification occurs through August 2014.





## VIDEO

### DARPA's voice-trained, animal-like robot eases soldiers' burdens

Soldiers on the ground are burdened with hundreds of pounds of equipment to lug through rough terrains and adverse weather conditions such as blistering heat. But that's where the DARPA/USMC-funded Legged Squad Support System (LS3) quadruped robot comes to the rescue, designed to interact with soldiers the same way a trained animal would, while carrying a robust 400 lb. equipment load. As the video-captured recent testing at Fort Pickett shows, the Boston Dynamics-developed robot will obey voice commands such as "power on" and "follow tight" and can also traverse rough terrain. As the video shows, when there is a rollover, the robot uses its enhanced roll recovery capability and carries on into a simulated urban environment without running into anything or anyone. LS3 also serves as a nocturnal mobile power source to recharge troops' batteries for their hand-held devices and radios. LS3 testing will be ongoing through Q2 2014.

Watch the video: <http://opsy.st/Y1d8AC>

More videos: [video.opensystemsmidia.com](http://video.opensystemsmidia.com)

## MARKET PULSE

### Counterfeit and substandard semiconductors: The solution to the threats

By George Karalias,  
Rochester Electronics

Counterfeit semiconductors are entering the worldwide supply chain in unprecedented numbers, and those numbers are increasing at an exponential rate. Also entering the world supply chain are substandard components that were originally viable but have been damaged through improper handling, storage, and shipping methods employed by unauthorized distributors. All of these components are causing production and maintenance failures that range all the way from inconvenient to deadly.

Added to the already overwhelming mix of components that just don't perform properly – or at all – are components armed with malicious "extras" that can destroy systems, cause malfunctions, or covertly gather proprietary information. Malicious insertion threatens national security. This white paper offers a solution to these threats and how to detect counterfeit parts.

Read this white paper: <http://opsy.st/YjPzH2>

More white papers: [whitepapers.opensystemsmidia.com](http://whitepapers.opensystemsmidia.com)



## SOCIAL MEDIA

## LinkedIn



John McHale (Military Embedded Systems) posted a link:

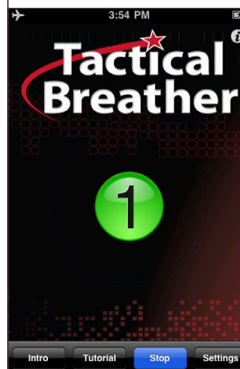
**FACE Edition 2.0 avionics standard approved and published**  
[mil-embedded.com](http://mil-embedded.com)

DAYTON, OH. Officials at the Open Group announced that the Future Airborne Capability Environment (FACE™), Edition 2.0, – has been unanimously approved and published by organization's Governing Board. The FACE standard...

Like • Comment • Share

Hear what our "Military Embedded Systems" editors and group connections are saying: [www.linkedin.com/groups/Military-Embedded-Systems-1864255?trk=myg\\_ugrp\\_ovr](http://www.linkedin.com/groups/Military-Embedded-Systems-1864255?trk=myg_ugrp_ovr)

## INNOVATION



### T2 mobile app aims to quell fight-or-flight reaction

To tame the intensity of in-combat fight-or-flight adrenaline responses, in addition to psychological stress reactions in the heat of battle, troops can now download the free Tactical Breather mobile app to their iPhone, iPad, iPod touch, and Android devices. Created by the National Center for Telehealth & Technology (T2), the app comprises techniques for training soldiers to exercise control of their concentration, emotions, heart rate, and other variables that commonly react to stressful scenarios. Partially based on the book "On Combat: The Psychology and Physiology of Deadly Conflict in War and Peace," by Lt. Col. Dave Grossman, the app won the Apps4Army (A4A) competition's 2nd place award for the "General Wellness" category. Download it at the iTunes app store, on Google play, or at the Amazon appstore for Android.

## E-CAST

### Quantum™ SA.45c Chip Scale Atomic Clock – Precision Timekeeping with Low Size, Weight, and Power (SWaP) for Military Applications

Presented by: Symmetricom

Ultra-precise timekeeping that can change the outcome of missions is now mandatory for mission-critical military applications. Atomic clocks in the past have offered the accuracy and precision required for these applications but could not be used due to their large form factors – which added to the overall weight of the system and total power consumed.

Watch this on-demand event: [ecast.opensystemsmidia.com](http://ecast.opensystemsmidia.com), then click on "See Archived E-casts and Events in-progress"

## BLOG

## CODE QUALITY:

## Dynamic and static analysis combined makes engineers and auditors happy



By Mark Pitchford, LDRA

*In the good old days, before writing software became “software engineering,” code development was a black art practiced by weird nerdy kids straight out of college. For them, coding was by no means a structured discipline. If you managed to get them to communicate, they might tell you that they were hacking code together and using ad hoc test data to see whether it did what it was supposed to do when they executed it.*

Whether they knew it or not, they were practicing dynamic analysis through system functional test. Unlike static analysis, dynamic analysis involves code execution by definition.

But what did this do beyond showing the basic functionality as roughly correct for whatever rudimentary test data was dreamed up? While better than nothing, likely no more than half of the code was exercised. Jack Ganssle, industry software guru, and chief consultant for The Ganssle Group, and industry editor, concurs: “Studies confirm that, without the use of code coverage analysis, testing typically exercises only 50 percent of the code. Given typical bug rates, that means 100K lines of code in a program will ship with 2,500 to 5,000 bugs. These bugs lead to many systems failures.”

Why? Because no matter how imaginative the tests, chances are that real life will throw some curve balls to try out the untested paths. And if something executes that wasn’t tested, you’re likely in for some surprises and potentially catastrophic failures.

Fast forward 30 or 40 years. Although such a homespun approach doesn’t cut it with complex military embedded applications, functional test remains at the core of what dynamic test can do. Carefully selected test data show that the branches and statements in the source code are exercised in accordance with specification, allowing us to not only show that the system is functionally correct, but also that we have exercised all of it. When used in tandem with static analysis, dynamic analysis provides the supporting evidence needed to prove that all of our other good works and best practices yield a safe, secure, and high-quality end product.

Unlike the hacking of years ago, today’s automated test tools precisely trace the execution route via techniques such as the use of instrumentation probes. These probes are essentially additional function calls that generate “I’ve been here”

messages from strategic points in the source code and allow coverage data to be collated. They allow dynamic tests to generate feedback on how comprehensive they are, so that we can successively build on each set of results until the desired level of coverage is reached.

In turn, this gives us flexibility in how much code is exercised at a time. Dynamic analysis of an entire system is possible, but there are always routes through the code that cannot be exercised by our system during normal operation – defensive code, for instance; perhaps a check for a division by zero.

At times like this, it’s good to also use “unit tests.” Unit tests encapsulate a subset of the system and allow parameters to be passed such that the defense mechanism code in our example is exercised. We even have the option of basing application dynamic analysis entirely on unit tests, collating code coverage data as each module is developed and removing any requirement to wait for a complete system.

Today’s military applications require support for architectural standards such as ARINC 653 or FACE to improve code portability and reusability. The provision of comprehensive coverage data by means of dynamic analysis provides evidence that code remains maintainable, safe, and secure even when ported to a different application, particularly when used in tandem with an effective static analysis regime.

Our nerdy friends of yesteryear weren’t easily impressed, but they would surely recognize what we are doing as an extension of their own test efforts. Who knows?! We might even get a grunt of approval for our system failure rates or maybe even high fives over the mounds of Coke cans and pizza boxes stacked around their computers!

*To become a guest blogger, email Editorial Director John McHale at [jmchale@opensystemsmedia.com](mailto:jmchale@opensystemsmedia.com).*



# » Streamline your Next-gen technology upgrades «

**Kontron uniquely suited for today's military tech refresh and upgrade programs**

- » Next Gen Processing Technology
- » Technology Migration
- » Legacy Platforms
- » Lifecycle & Obsolescence Management
- » Risk Management



## Gen3 PCIe & 10GbE

- » Maintain backwards compatibility with next gen higher I/O throughput and processor performance
- » Software usability across all product lines



**VX3042 & VX3044**  
3U VPX 3rd gen Intel® Core™ i7 dual/quad core Single Board Computer



**CP6004X-SA**  
6U CompactPCI® 3rd Gen Intel® Core™ i7 Processor Blade

Only Kontron supports native Gen3 PCIe & 10GETH

## PPC-to-x86 Seamless Migration

- » Pin compatible processor boards
- » Matching I/O ports for plug and play



**VM6250**  
6U VME Power PC with Altivec Computer



**VM6050**  
6U VME Intel® Core™ i7 Single Board Computer

← 100% pinout compatibility →



## Full speed ahead: FACE initiative fosters reuse, cuts costs and delivery time of military avionics systems

Q&A with Jeff Howington, Vice Chairman of the FACE Steering Committee



*The Future Airborne Capability Environment (FACE) Technical Standard aims to hasten delivery and cut costs of military avionics systems via a modular architecture, data models, standard interfaces, and conformance criteria that meld to enable reusable software components and a common operating environment. Our editors recently caught up with Jeff Howington of Rockwell Collins, a FACE Consortium founding member, to find out how the FACE approach will affect the U.S. Army's Common Avionics Architecture System (CAAS) program – and the industry at large.*

U.S. Air Force photo



**MIL EMBEDDED:** *The FACE Consortium approved and published its FACE 2.0 spec in March. How will it work, technically speaking, and how will it benefit mil avionics systems? (Also, what about the FACE 1.0 spec?)*

**HOWINGTON:** The intention of the Technical Standard for Future Airborne Capability Environment (FACE) Edition 2.0 is to reduce costs and speed delivery of military avionics systems. Most future expansion of aviation capability will come from the integration of systems controlled by software, so the FACE Consortium, an Open Group Managed Consortium, concentrated its efforts toward addressing avionics software development and deployment. One of the biggest cost drivers to conquer is the common practice of developing different software for different platforms that implement the same capability. By codifying a modular architecture, standard interfaces, data models, and conformance criteria into a common operating environment and reusable software components, we will have the means to share capabilities not only across platforms, but also across the military services and avionics vendors as well.

Edition 1.0 of the FACE Technical Standard was published on January 30, 2012 and laid the foundation by standardizing the modular architecture and interfaces. Edition 2.0 adds a data model, which provides an interoperable means of data exchange among FACE software components, further reducing the need to modify those components when they are integrated onto different platforms. Edition 2.0 is published by The Open Group at their web bookstore. [See <http://www.opengroup.org/bookstore/catalog/c137.htm>]

**MIL EMBEDDED:** *What is Rockwell Collins' role in the FACE Consortium, and how are systems integrators like Rockwell going to leverage the FACE approach?*

"One of the biggest cost drivers to conquer is the common practice of developing different software for different platforms that implement the same capability. By codifying a modular architecture, standard interfaces, data models, and conformance criteria into a common operating environment and reusable software components, we will have the means to share capabilities not only across platforms, but also across the military services and avionics vendors as well."

**HOWINGTON:** Rockwell Collins is one of the founding members of the FACE Consortium. Our company is active within the technical and business working groups, and we hold leadership positions in the steering committee and the data model sub-committee. Together with more than 50 other member organizations, we are working to create a successful technical standard and business strategy.

The FACE environment gives customers greater freedom to incorporate capabilities that reside in other platforms. Reusing already-proven and fielded capabilities benefits integrators like Rockwell Collins because it adds value to our underlying product – a complete functional hardware and software system. Imagine if your personal computer was the best and latest, but you couldn't run the word processing application that your colleagues use. At the very least, your training and the way you operate your computer are different and in the extreme case you cannot exchange files with others. Your office IT team will soon replace that computer, as it raised your cost of doing business. Our military customers are tackling similar cost issues. Rockwell Collins will leverage the FACE Technical Standard and associated business practices as one means to solve that problem.

**MIL EMBEDDED:** *Rockwell Collins already leverages their avionics systems used in business and commercial jets for use in military platforms. How will the FACE initiative affect this?*

**HOWINGTON:** Rockwell Collins first adopted modular open architecture concepts 15 years ago and today it powers how we leverage our civil avionics systems onto military platforms. Examples of this are the Rockwell Collins' next-generation avionics systems now aboard the Boeing 787, which we leveraged into the U.S. Air Force KC-46 tanker program, and the Rockwell Collins Pro Line Fusion business and regional jet avionics solution, which we leveraged into the Embraer KC-390 and the AgustaWestland AW609 aircraft. These reuse examples represent substantial cost reductions and schedule savings for our customers.

The good news for Rockwell Collins is that we already implement much of our avionics capabilities as reusable software components. These components can move readily within our system families. Since their design is close to the FACE Technical Standard, we are well prepared to meet these new requirements.

**MIL EMBEDDED:** *In which ways is the FACE initiative similar to the CAAS program started by Rockwell Collins and the Army to leverage COTS and common software architectures across Army helicopter platforms? How will the FACE concept affect CAAS, or will it?*

**HOWINGTON:** More than a dozen years ago, Rockwell Collins began working closely with U.S. Army Special Operations Aviation Command in the development of the Common Avionics Architecture System (CAAS). To meet the Army's demanding requirements, we adapted our Modular Open Systems Architecture technology fielded on the USAF's KC-135 Tanker aircraft. Today, CAAS flies on nearly 1,000 Army, Navy, Marine Corps, Coast Guard, and allied force rotary-wing aircraft. These aircraft include the MH-47G, CH-47F, and other Chinooks for the United States, Canada, Singapore, and Italy; the VH-60N, MH-60T, and MH-60L/M Black Hawks; the MH-65E; and the CH-53E. With the first CAAS implementations dating back to 2000, this architecture remains a trusted capability for our military rotorcraft customers.

The CAAS program and the FACE initiative have similar goals with respect to capability reuse. FACE intends to go further by establishing a standard for an architecture that supports portable, capability-specific software applications across military avionics systems, regardless of the avionics vendor. To work successfully, FACE applications must execute within a FACE computing environment on the installed computing hardware of the platform.

So the most immediate change you will see with CAAS is the inclusion of a FACE computing environment to support execution of FACE-conformant applications. The CAAS modular open architecture design closely aligns with the FACE Technical Standard and is requiring minimal modification to provide a FACE environment. CAAS will also continue to support the Army's existing software applications. This provides the crucial ability to preserve customers' existing technology investment, while extending their platforms to accept the latest capabilities well into the future.

**MIL EMBEDDED:** *How will the FACE approach enhance the military's use of DO-178B/DO-178C software and similar safety-certified code, even though military platforms typically don't*

*have to undergo FAA certification? What does the FACE "certification" process entail, and by whom are products approved, or is it all the "honor system"?*

**HOWINGTON:** Flight safety is very important to the FACE Consortium. Its goal is to complement the existing airworthiness processes, not to replace them. FACE certification indicates adherence to the Technical Standard for portability purposes.

The reason for this is that airworthiness processes prescribe significant efforts to prove that the functional logic residing within software components will work as intended in all conditions. But the FACE Technical Standard does not address how this logic is created. Instead, the modular architecture, standard interfaces, and data models are described and it is up to programmers and integrators to ensure safe designs are in place in the way their software operates within that framework. The benefit with portability is that if the finished software meets DO-178 criteria, the software supplier can reuse both the software and its certification artifacts in another system, saving time and cost.

The FACE conformance certification process provides a formal evaluation assuring that the software component adheres to the FACE Technical Standard. For example, part of the verification process will examine which Application Programming Interfaces (APIs) a FACE application uses. A truly conformant application will use only those APIs called out by the standard and no other.

Software portability comes only if everyone plays by the same rules in the standard, so no "sneak circuits" are allowed, so to speak. If the application passes the complete set of conformance tests and other defined required criteria, then it is considered FACE conformant and is marketable as such with an official certification logo. The FACE Conformance Certification Guide describes this process.

**MIL EMBEDDED:** *Describe the FACE business model and how much that business model will provide in long-term DoD savings, in light of present and possible DoD budget cuts.*

**HOWINGTON:** The FACE Business Guide suggests a number of potential software-centric business model options for avionics acquisitions. These are not often used in marketing defense avionics because currently, most purchases of avionics result in the delivery of embedded hardware with software bundled within. Adhering to the FACE Technical Standard allows for more software acquisitions independent from hardware.

One example for applying the FACE business model is the potential acquisition of Required Navigation Performance for Area Navigation Flight Management System (FMS) capability (RNP RNAV). Rockwell Collins has been able to reuse its civil RNP RNAV capability aboard military aircraft that use our avionics systems. If such a capability were to appear as an application that conforms to the FACE Technical Standard, not only could we apply it to Rockwell Collins' avionics systems, but to other aircraft as well if those aircraft provide a FACE Computing Environment. This will result in major cost and schedule savings by reducing if not eliminating software modifications when moving the capability from platform to platform, which in turn reduces integration costs and safety certification costs.

**MIL EMBEDDED:** *How does the FACE approach benefit embedded COTS suppliers? Do you foresee any possible challenges for COTS suppliers in implementing the standard? If so, what?*

**HOWINGTON:** The FACE Consortium is privileged to have several embedded Commercial Off-the-Shelf (COTS) suppliers as consortium members, including all of the largest real-time operating system vendors for avionics. These companies provide insights into the issues faced by COTS providers, including the important role that intellectual property protection plays in incentivizing their participation in the defense



marketplace. Many of the FACE documents and processes now incorporate these insights.

A number of COTS suppliers have announced products that are aligned with the FACE Technical Standard. Many have cited the value that it brings to their products and the expansion of their addressable market as a result. Many COTS suppliers tend to use open standards and by all accounts the transition for avionics-oriented suppliers has gone well. Because the FACE Technical Standard does not address how functional logic for avionics is created, or eliminate the flight-safety knowledge required, it does not readily open the market for just anyone. The avionics learning curve still remains, which applies not just for COTS providers, but everyone else as well.

**MIL EMBEDDED:** *Will there be a "store" where designers can download conformed code or products?*

**HOWINGTON:** Suppliers can make their conformant software products publically known through the FACE Library. The library consists of two major functions, the FACE Registry that lists the products and their searchable metadata, and the FACE Product Repositories, which contain the actual products. The product registry is the single-reference listing for certified FACE-conformant products, and products are listed there only after they receive their FACE certification. Multiple, independent repositories enable suppliers to configuration manage their products and ensure intellectual property protection.

Obtaining software from the FACE Library is a two-step process. Prospective customers first search the product registry for products that meet their requirements. The registry will contain information approved for public release about the products, such as names, capabilities provided, requirements for the hosting hardware, and the suppliers' contact information. Once a selection is made, the customer establishes contact with the supplier for purchasing

information. If purchased, the software is obtained from the appropriate product repository. FACE Product Repositories are owned and managed by contractor entities, government agencies, or other organizations that supply the software.

**MIL EMBEDDED:** *Which technology(ies) is/are needed to take the FACE concept to the next level, but not available now?*

**HOWINGTON:** The Consortium continually explores ways to improve avionics software, but we see beneficial results using current technologies. The next level is to promote FACE adoption and use.

**MIL EMBEDDED:** *What will FACE activities look like a year from now. What about 3 years from now? Ten or 20 years from now?*

## High Durability Standards for the DDR3 Ruggedized SO-DIMM

The new DDR3 Rg SO-DIMM 4GB standard offers a cost effective way to satisfy the need for high durability standards in applications such as transportation, medical, military and aviation. The modules are rated at -40° to +85° or -20° to +70° C temperature operation, providing critical durability in the harsh environments they are designed to operate in.

- JEDEC standard 1.5V  $\pm 0.075V$
- SSTL 1.5 interface
- VDDQ = 1.5V  $\pm 0.075V$
- Module rank = 2
- Non-ECC/64 bit wide
- Supports 667 MHz clock (1333 MT/s)
- Programmable CAS Latency 6, 7, 8, 9
- Burst Length: 4, 8
- Bidirectional differential data strobe
- Thermal Sensor with Integrated SPD
- FBGA DDR3 SDRAM
- Screw mounted for Ruggedized applications
- Module Height: 34.0mm, (1.34 in.)
- Made in USA

**amp inc**  
Memory and Storage solutions for today's world  
Accelerated Memory Production, Inc.



**For more information, call 800-778-7928**

Accelerated Memory Production, Inc.  
1317 E. Edinger Ave., Santa Ana, CA 92705  
714-460-9800 | 800-778-7928

**www.ampinc.biz**

**HOWINGTON:** When the FACE Consortium first formed in 2010, a conscious decision was made to focus on promoting military avionics software portability and reuse. That area alone is hard enough to get right and required strict focus to prevent distractions from moving us away from our end goal. In the short term, you will see us continue to focus on solidifying the FACE Technical Standard and the support for it in terms of standing up the FACE Library, a conformance certification program, development tools, test tools, and so forth. Over time however, we've seen interest from other adjacent markets that see value in our work. If interest is strong enough from the civil avionics market, we may look into how we can help there. Longer term, it's hard to say if we will take the FACE Consortium into different areas, or provide another team with our lessons learned and enable them to head off on their own.

The one constant that I believe will endure is the joint government industry consortium structure that has proven its worth throughout. We have averaged 130 people at our last two meetings from more than 50 consortium member organizations. More than 600 individuals are directly or indirectly involved in any number of activities, such as weekly teleconferences and the like.

We could not fault anyone for thinking that a crowd of that size would produce nothing of merit. Yet this team has succeeded in creating a workable software-centric avionics ecosystem as evidenced by industry product announcements and government program awards. We are on track to continue refining and improving the FACE concept. **MES**

*Jeff Howington is a member of the Rockwell Collins business development team within the company's Government Systems Airborne Solutions segment. He currently serves as Vice Chairman of the FACE Steering Committee.*

### About The Open Group FACE™ Consortium

Further information on the FACE Consortium can be found at [www.opengroup.org/face](http://www.opengroup.org/face). Contact [ogface-admin@opengroup.org](mailto:ogface-admin@opengroup.org) for specific inquiries. The FACE LinkedIn Group is located at [www.linkedin.com/groups?gid=4127663&trk=myg\\_ugrp\\_ovr](http://www.linkedin.com/groups?gid=4127663&trk=myg_ugrp_ovr)

## Toughest SSDs On The Planet

[WWW.TOUGHSSD.COM](http://WWW.TOUGHSSD.COM)



**TCS**

**Rugged Solid State Drives for Military,  
Aerospace and Industrial Applications**

**1-800-307-9488**  
[sctsales@telecomsys.com](mailto:sctsales@telecomsys.com)

©2013 TeleCommunication Systems (TCS). All rights reserved.



# SynQor

## Mil-COTS

### DC-DC Power Converters

- ▶ **Output power up to 800W**
- ▶ **High efficiency: up to 92%**
- ▶ **Full power from -55 to +100 °C**
- ▶ **Fixed switching frequency**
- ▶ **Vin ranges from 200V to 475V**
- ▶ **Built-in current sharing**
- ▶ **No minimum load requirement**



**New! 270Vin 800W Full-Brick**



Designed and manufactured in the USA  
1-978-849-0600 [www.SynQor.com](http://www.SynQor.com)

**SynQor**<sup>®</sup>  
Advancing the Power Curve<sup>®</sup>



## Commonality and reduced SWaP drive vetronics designs

By John McHale, Editorial Director

*Budget cuts and changing strategic priorities have slowed the military vetronics market to one that is flat for the foreseeable future. However, innovation in electronics design has not slowed, as military embedded system suppliers develop creative ways to introduce more commonality in components to navigate the budget-constrained environment and continue to meet reduced Size, Weight, and Power (SWaP) requirements.*



Commonality and reduced Size, Weight, and Power (SWaP) requirements are driving vetronics designs in platforms such as the Joint Light Tactical Vehicle (JLTV). Photo courtesy of Lockheed Martin

"To go up against [German Gen. Erwin] Rommell we need the best tank man we've got," said Karl Malden in the role of Gen. Omar Bradley in the movie "Patton." He was referring to the title character – Gen. George S. Patton – and foreshadowing his genius in tank warfare, which eventually led to allied victory in WW II. Good tank commanders are still needed today but not with nearly the strategic importance of 70 years ago. As the U.S. pulls back from two ground wars and occupations in Iraq and Afghanistan, its global military footprint will comprise more unmanned systems, cyber warfare, and electronic intelligence gathering than ground troops and vehicles. Less troops on the ground means fewer tanks going into battle with new tank and vehicle platforms likely to be put on hold for decades.

Special Forces programs, unmanned vehicle platforms, and C4ISR technology will dominate the near-term DoD funding priorities. Some of these programs – especially Special Forces – will require state-of-the-art vetronics technology, mostly through retrofits. Large Army tank deployments, funding of new tactical vehicle programs, and even new versions of HMMWVs [High Mobility Multipurpose Wheeled Vehicles] are likely to be put on hold or canceled all together.

"The vetronics market is effectively flat to declining, says Wayne Plucker, Industry Manager at Frost & Sullivan. "The Army is planning to reduce tank rebuild to minimum sustainment levels. The last of the new build, Strykers was produced last year. The Army is effectively done

building new ground vehicle platforms. The Ground Combat Vehicle and Joint Light Tactical Vehicle (JLTV) programs are likely to be delayed or stretched out. There will be necessary spending on refits for returning vehicles, but that will not have the market pickup that it once was estimated to have." Last fall Plucker says the value of the vetronics market was at about \$900.3 million. There was a small increase in vetronics funding, but it was less than initially estimated, as reduced spending was mandated within DoD, he says. "The move to standards will still be needed, but likely delayed or stretched out. Also the airpower and UAV asset use will probably have some effect on ground vehicles, but I think that will be mostly based on doing more with less and delaying deployments where possible. The principal growth will be in






the RDT&E budget, not in procurement. One funding area that will essentially remain fluid is Special Forces operations. The Special Operations Command (SOCOM) will still have the ability to buy what they want when they want. Their program spending is dynamic, while TACOM spending is more predictable."

"Sequestration has hit the large iron manufacturers the hardest as there are less vehicles being built," says Doug Patterson, Vice President of Military Business Development at Aitech in Chatsworth, CA. "Sequestration has hit us indirectly by adding uncertainty as to the direction of defense funding. Many integrators are holding on to their money until they get more direction. The vetronics market is slow as there are no new programs on the horizon, and

upgrades and refreshes will be more incremental in nature."

"Budget constraints drive commonality," which is advantageous on the front end but also on the back end of electronics systems as well, says Bill Guyan, Vice President at DRS Network and Imaging Systems in Melbourne, FL. "It is a big cost saver when it comes to supportability." Nearly every single component, equipment, and system comes with its own manual and requires uniquely trained personnel to field and install each device, which gets very expensive, he continues. "If the same component or computer can be used across multiple platforms, it will create huge savings on the back end. That is just at the hardware level." Software supportability costs can scale even



# INTERFACE CONCEPT

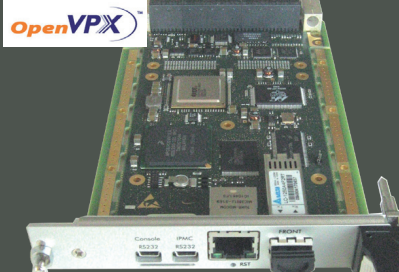
ADVANCED ELECTRONIC SOLUTIONS

---

## SWITCHES & IP ROUTERS

More than 30 models... VPX, VME, cPCI

### ComEth 4410a



OpenVPX™

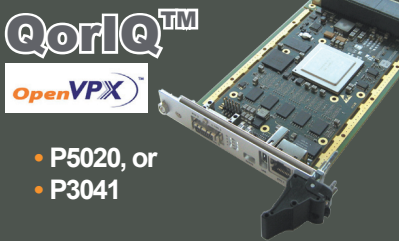
- Data/control Planes 3U VPX switch
- Six 4-lanes ports (PCIe x4 Gen2)
- Up to ten Giga Ethernet Ports

---

## SBCs PREMIUM

Intel® & Freescale® processors

### QorIQ™

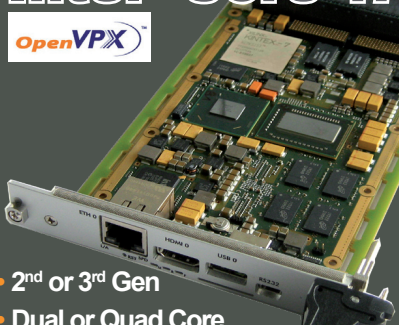


OpenVPX™

- P5020, or
- P3041


---

## Intel® Core™ i7



OpenVPX™

- 2nd or 3rd Gen
- Dual or Quad Core
- with a Kintex™ 7
- and its personality module



www.interfaceconcept.com

+33 (0)2 98 573 030

higher when maintaining software base-lines and enabling security for trusted computing, Guyan adds.

"Commonality reduces the training burden and greatly increases operational flexibility," says Andrew Shepherd, Product Manager at General Dynamics Canada in Ottawa, Ontario. "With common displays, a crew can move from one platform to another, interfacing with the vehicle's systems and C4ISR applications through this common display. In addition, leveraging the combined investments made by multiple customers helps to reduce through-life costs of the system and mitigates obsolescence risks by drawing on a larger supply base. [Another] trend is the recognition of the need for operational redundancy. Combat vehicles with a central computer, hosting various vehicle information and C4ISR systems while driving a number of displays, have a single point of failure. If the one central computer fails, the operational effectiveness of the platform is severely compromised. Networked smart displays enable any application to be run from any position and allow crews to share 360-degree situational awareness. These smart displays allow the driver to see what the gunner sees through his sights or all crew members to see a live UAV video feed."

"Themis is still investing its own money in development of goods and services for the vetronics market," says Bill Ripley, Director, Business Development, Tactical Systems at Themis Computers in Fremont, CA. "We feel that there is a lower likelihood of funding being eliminated for vetronics programs, both for new and recapitalized vehicles. The requirement won't go away, but the funding might slip to the right a bit. There is a real need in the Army and Marine Corps for vetronics systems, and because these systems lagged the aviation community, there are fewer "Plan B" options available. The world of military ground vehicles is changing at a very fast pace. The customer is demanding more and more integration, while trying to drive down the acquisition costs of the vehicles. An Army acquisition officer told me that compared to their aviation



**Figure 1** | A Canadian soldier receiving information on General Dynamics Canada Smart Display during Family of Land Combat Vehicles (FLCV) capability demonstrations.

counterparts, the vetronics community wants F-16 functionality at Cessna 150 prices. The vetronics market and integrated battlefields are requiring systems that don't cost very much and [can] be architected in such a way as to be able to deal with an evolving threat."

### VICTORY

Commonality across multiple platforms also is a cornerstone of the U.S. Army's Vehicular Integration for C4ISR/EW Interoperability (VICTORY) initiative. VICTORY provides interoperability at the subsystem level, enabling subsystems from different manufacturers to work together in one system and across multiple platforms via standard connectors and well-defined electrical interfaces.

"Commensurate with VICTORY, budget issues have forced prime contractors to try to find creative ways to still meet their requirements in this funding-constrained environment," says John Ormsby, Business Development Director for Ground Defense at Curtiss-Wright Controls Defense Solutions in Charlotte, NC. "As a result, programs like Stryker came out with a vehicle network requirement – which is what VICTORY was designed to help meet. We believe the market is driving toward this trend."

"The VICTORY architecture is being developed to facilitate the integration of C4ISR systems into ground vehicles," Shepherd says. "Historically, ground vehicles have adopted a bolt-on approach for C4ISR capability, which results in problems with size, weight, and power. VICTORY provides a framework architecture, standard specifications, and design guidelines to enable the integration of C4ISR systems directly into the platform. General Dynamics supports the development of the VICTORY standards and participated in both the Information Assurance and Networking working groups. In addition, our products are compliant with VICTORY standards. One example is our Smart Display product, which consolidates the interface to different systems, both classified and unclassified, onto a common display solution (Figure 1)."

"The activity in the VICTORY community has picked up, and remains at a high level," Ripley says. "The standard development has progressed quickly and in a focused manner, with few hiccups and false starts. There has been unprecedented cooperation between the government and industry, with players like Themis being able to bring good ideas to the table and have them



considered and even adopted. From our vantage point, more and more programs are requiring VICTORY compliance. The only unknown is what version of VICTORY will be the baseline for a particular program."

"VICTORY callouts and specifications are starting to show up in request for proposals," says David Jedynak, Chief Technical Officer for COTS Solutions at Curtiss-Wright Controls Defense Solutions. "We are starting to see VICTORY penetration into the tactical fleet such as the JLTV and the modernization of the Bradley and Abrams platforms. The biggest advantage of VICTORY is the integration capability: Vetronics and C4I systems were traditionally built separately, but now they can be integrated through VICTORY. The government wants to reduce the overall dollar per mile with each vehicle. This is the overall larger metric that takes account of a number of factors such as sustainability, fuel costs, and a number of other things. VICTORY enables this by leveraging commonality in the vetronics system that reduces the footprint and has a higher MTBF. Our main way of meeting minimal VICTORY requirements is through the Digital Beachhead (Figure 2), which meets the minimal requirements for VICTORY and has all the basic pieces – such as databus, switch management service interfaces, CAN buses for automotive interfaces, and a number of other pieces that help vehicle integrators easily drop in VICTORY functionality without going through a major overhaul of the vehicle electronics." The system also comes with an integrated Vehicle Management computer that has HUMS/CBM+ system health services.

#### Reducing SWaP

Whether a program calls out VICTORY requirements or not, nearly every program manager demands reductions in SWaP with their vetronics systems. Replacing a six-box vetronics system with a single-box solution containing modern processors not only enables SWaP, but also enhances C4ISR capability and the smaller footprint provides integrators with more room to store equipment or to just make the vehicle lighter.

**Figure 2** | The Digital Beachhead from Curtiss-Wright Controls Defense Solutions meets the minimal requirements for VICTORY and has all the basic pieces – such as databus, switch management service interfaces, and CAN buses for automotive interfaces to enable easy drop in VICTORY functionality.



## DRAGON

### it's not a myth.

- Rugged PC/104 enclosure
- Data acquisition
- Monitoring • Recording
- MIL-STD-1553/1760
- AS5652 (MMSI) • H009
- ARINC-429/575 • ARINC-708
- CANBus • A/D • D/A
- Serial • Discrete
- User configurable
- COTS • Expandable
- Extreme environments
- Accepts third party cards



[www.mil-1553.com](http://www.mil-1553.com)



CAMELOT | MACC | LANC

"Reduced SWaP also is enabled by grouping a number of components into one box – hosting functions that are independently running on one piece of hardware over network protocols," Jedynak says. "The system is taking on more of a network mindset where the physical block diagram and the functional block diagram cease to be dependent on one another. You can place 10 cards in 1 box and 10 in another; when building a distributed network concept, it doesn't matter how you've built it, rather that it is interoperable."

"Rugged smart displays meet this need by integrating more capability into a smaller package and replacing the need for separate computer modules, video distribution boxes, and video display screens while significantly reducing the cabling necessary to integrate the disparate components," Shepard says.

Engineers at DRS Tactical Systems are solving SWaP issues in Special Operations vehicles with their C4InSight solution, which includes a Data Distribution Unit (DDU) and Mission Command Software Suite (MCSS) that are interoperable with existing platform displays and computers. The DDU is half the size of the DRS JV-5 Block 2 Rugged Vehicle System that is used in Army vehicles, Guyan says. It can be deployed on a platform as a tactical router, as a battle management system computer, or as a hub to distribute video and voice data, he adds.

It was produced to meet the C4ISR management requirements of U.S. Special Operations Command (USSOCOM) Family of Special Operations Vehicles (FOSOV) and is consistent with VICTORY and USSOCOM's Mobile Distributed C4ISR Architecture (MDCA) objectives, according to DRS. The solution enables integrators to remove four or five different boxes off a space-constrained platform such as Army tracked combat vehicles and replace them with one box, improving the total power budget, as well as total size and weight availability as you are removing other equipment off the vehicle as well when you remove the boxes, Guyan says.

### Distributed architectures

"Vetronics integrators still want smaller SWaP, but still want levels of performance they are used to, so we are pushing the envelope," Patterson says. "The move toward a distributed architecture has not hit its stride yet as the integrators are still happy with [a] large central-computer-based architecture."

Several factors have driven the vetronics community to a distributed computing architecture such as "smaller bite-sized integration efforts, more common hardware, and inherent system redundancy," Ripley says. "Products that lend themselves to extensibility and a distributed architecture ultimately reduce schedule and development risk, as well as the cost to the customer. For example, our NanoSWITCH product can be as simple as a 'dumb' layer 2 switch, or extended to be a layer 3 switch/router. Its functionality is extensible in that a Single Board Computer (SBC) and optional CAN Bus and MIL-STD-1553 interfaces can be added to allow for Ethernet to vehicle or tactical data bus gateway functionality. The SBC can be used as a system controller, bus gateway, firewall, or security processor. A SAASM GPS also can be integrated in the switch to give Precision Time Protocol (PTP) control, synchronization, and orientation."

The VITA 74 SBC can turn a dumb vetronics display into a smart display by using a removable and replaceable conduction-cooled processor, which enables a display's expensive electronics to be gutted in minutes and reused with a touch screen or upgraded/repurposed by changing modules, he adds.

### VITA standards and vetronics

Standards from VITA such as 3U VPX and the VITA 74 small form factor specification are also enabling the SWaP advantages in military vetronics retrofits. There are opportunities for 3U VPX-based systems in those upgrades as they solve some of the SWaP challenges. For vetronics applications, Aitech offers their Corei7 Haswell C873 product, which is available in 3U CompactPCI and VPX formats (Figure 3).



**Figure 3** | Aitech's Corei7 Haswell C873 product is available in 3U CompactPCI and VPX formats.

"In the heavy vehicle area, there is an increase in 3U VPX adoption with 6U VPX typically being used only for ISR or EW gear," Jedynak says. "Mission management, battle command, and other various systems in the vehicle are all being run on 3U VPX systems. Tactical vehicles, on the other hand, are not embracing modular architectures as they have tighter SWaP-C requirements so it doesn't make sense. People are looking for a smaller form factor in these applications, but not necessarily open standard SFF boxes. We have designed a small form factor Intel solution that is compliant with the UK Generic Vehicle Architecture and can meet tactical vehicle needs."

"The VITA 74 systems have found favor in the vetronics marketplace because they offer a standards-based solutions at prices often 50 percent less than similar 6U VME/VPX or custom form factor solutions, without compromising environmental specification compliance," Ripley says. "Staying with the standards ensures that the customer could have multiple sources to choose from, which itself promotes innovation and drives down acquisition costs. VITA 74 makes it much easier to offer highly rugged, high-performance computing, storage, and switching subsystems for vetronics applications. The volumes associated with vetronics programs offered a much better incentive to the system manufacturers to build systems with increased capabilities at reduced costs, and the aviation community, as well as the commercial marketplace, will reap the benefits." **MES**



# Vetronics Product Spotlights

## Protocol Converters

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



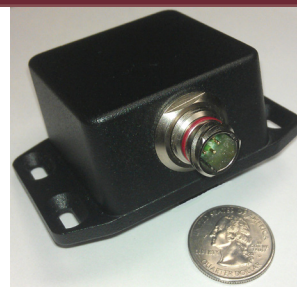
**Avalon Scientific**  
1-800-348-1765

[www.avalonscientific.com](http://www.avalonscientific.com)  
[sales@avalonscientific.com](mailto:sales@avalonscientific.com)

**AVALON**  
SCIENTIFIC

## Low-Cost MIL-STD-704 Power Supplies

- 50W now with more models to follow
- Semi-Custom and Custom are our specialties
  - Quick Turnaround
  - No NRE with minimum quantity order
- Low Cost



**Avalon Scientific**  
1-800-348-1765

[www.avalonscientific.com](http://www.avalonscientific.com)  
[sales@avalonscientific.com](mailto:sales@avalonscientific.com)

**AVALON**  
SCIENTIFIC

**E-cast**

## REGISTER NOW

for these and other free, on-demand webinars by accessing [ecast.opensystemsmedia.com](http://ecast.opensystemsmedia.com), then clicking on "See Archived E-casts and Events in-progress."

### Accelerating Safety and Security Certification with FACE™ COTS Solutions

**Presented by:** Esterel, GE Intelligent Platforms, RTI, Wind River

Complying with safety and security certification standards and requirements in any market is an expensive, tedious, and time-consuming task, but it saves lives in the friendly skies and can be a force multiplier on the battlefield. Meeting those requirements is often more efficient through open architecture designs and the use of common standards much the way the Future Airborne Capability Environment (FACE) Consortium is doing in the military avionics realm. New certification benchmarks such as DO-178C are also enhancing the safety compliance process. This E-cast of industry experts will discuss how designers can manage today's aerospace and defense software safety and certification requirement demands through improved modeling tools, common computing platforms, code analysis tools, and more.



### Radar and Electronic Warfare Drive Signal Processing Innovation

**Presented by:** Altera, Pentek, Inc., Mercury, Rohde & Schwarz

Radar and Electronic Warfare (EW) system designers are continually tasked with doubling and tripling performance in every new design or system upgrade, which places a tremendous demand on signal processing solutions for these applications. Military program managers want to track multiple targets simultaneously and track every signal coming in for all flavors of EW systems and radar from huge long-range surveillance radars to small Synthetic Aperture Radar (SAR) designs in UAV payloads. For these requirements they are turning toward commercially developed signal processing solutions and an open architecture approach for long-term refresh that leverages low-power components. This webcast of industry experts will discuss how EW and radar systems are leveraging commercially developed signal processing technology and more.

### Cloud security and the DoD

By John McHale, Editorial Director

*Cloud computing has demonstrated huge cost savings and operational efficiency benefits for the private sector and now Department of Defense (DoD) IT managers are exploring the concept for enterprise and tactical applications. However, DoD planners are moving much more cautiously to assure they have plugged all the potential cyber security vulnerabilities inherent in something as nebulous as a virtual cloud.*

Department of Defense (DoD) officials trying to keep the lights on in today's budget constrained environment love how cloud computing can reduce data center operational costs, bricks and mortar expenses, and staff overhead. Virtually storing data instead of physically in a hard drive is very appealing – especially to younger military personnel who have grown up with virtual technology such as the iPhone and the iCloud. However, military cloud services – just like military smartphones and tablets – will need to be much more secure.

The National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

“Back in the 2005 timeframe, Northrop Grumman had hundreds of data centers and consolidated them down to five data centers in 2011,” says Joe Cloyd, Director of Technology, Defense Cyber Security and Enterprise Services at Northrop Grumman ([www.northropgrumman.com](http://www.northropgrumman.com)). “In our next round

of consolidation we will go down to three enterprise data centers. The DoD will eventually do this as well, consolidating each respective network, and far down the road possibly rethinking a totally segregated approach to having multiple networks with duplication.”

“Many people initially think a cloud is inherently insecure as it is a single point of failure – the cloud goes and all your data goes with it,” says Todd Moore, Vice President of Product Management at SafeNet ([www.safenet.com](http://www.safenet.com)). “However, responsible cloud providers build in redundancy so when they write data to a cloud, they also write it to a disk at the same time. The virtual environment is encrypted and is also stored on a disk.”

“Securing the cloud is simple, as it is about providing assurance,” says Will Keegan, Technical Director, Software Security at LynuxWorks ([www.lynuxworks.com](http://www.lynuxworks.com)). “Users need to feel comfortable that when they log on remotely, every transaction they make will be secure. The complexities of public ISP cloud systems are too high to assure that data loss or leakages cannot occur. In a public cloud you have to assume all users are adversaries, and we rely on the ISP to protect other customers from stealing my data.”







Transforming "government data centers and applications into cloud computing environments, such as what Northrop Grumman is being asked to do on the Army Private Cloud contract, is often done on-site with security built in from the ground up," Cloyd says. "This includes the full spectrum of options from enterprise data centers to mobile cloud solutions focused on the tactical edge. We call it 'cloud transformation,' which is aiding a customer through various stages of maturity from unstructured chaos to a highly structured approach."

#### Mapping to NIST

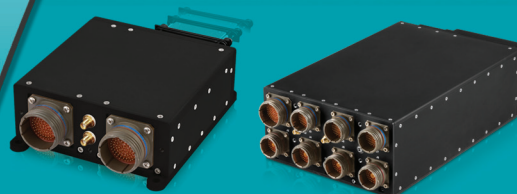
When it comes to securing the cloud from the ground up, many integrators rely on cloud computing characteristics and guidelines set forth by NIST. "When we think of the cloud we map everything back to the policies and procedures that the business and government communities pulled together under NIST," Moore says. There are four different types of cloud models: private, public, community, and hybrid as defined by NIST – with public and private being the most likely to be adopted by government users. A private cloud – owned and operated by a single organization or with a third party – is made up of multiple units and can be located on-site or off, according to NIST. A public cloud is open for use by the general public, is located on

## ALPHI TECHNOLOGY CORPORATION

Whatever your Form Factor, VME, PCI, cPCI, PCIe, PMC, Mini-PCI or proprietary, ALPHI provides the MIL-STD-1553 Solutions and COTS-I/O for your Mission Critical Systems.

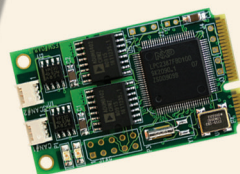
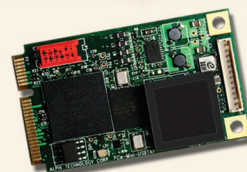
[www.Alphitech.com](http://www.Alphitech.com)  
**480.838.2428**

**Looking For I/O for  
Your Mission Computer?  
ALPHI PCI Express Mini I/O  
Solutions are the Answer!**



#### PCIe-Mini-1553/ARINC 429

- ◆ PCIe x1 Lane
- ◆ One Channel Dual Redundant 1553
- ◆ Two Independent ARINC 429 Receiver and one Transmitter

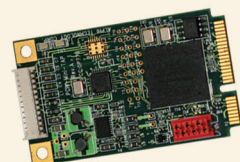
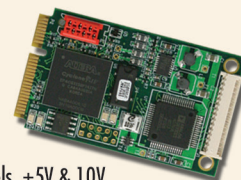


#### PCIe-Mini-CAN-USB

- ◆ 2 High Speed Isolated CAN to ISO 11898-2
- ◆ Supports 11-bit (CAN 2.0A) and 29-bit (CAN 2.0B Active) Identifiers
- ◆ Programmable Bit Rates 10 to 1000 kbps

#### PCIe-Mini-AD8200

- ◆ 8 Channels Simultaneously Sampled 16-bit A/D Converter
- ◆ Throughput Rate: 200 KSPS for all 8 Channels,  $\pm 5V$  &  $10V$

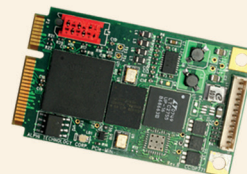


#### PCIe-Mini-DIO16

- ◆ 16 Digital I/O Channels
- ◆ 0-60V Voltage Range

#### PCIe-Mini-FastDAC-4

- ◆ 4 Channels 16-bit D/A, 2us
- ◆  $\pm 10V$  Output



**ALPHI offers custom modules as well.**



the premises of the cloud provider, and may be owned, managed, and operated by a business, academic, or government organization or a combination of them, according to the agency.

"If you want to have a cloud service, there are five essential characteristics you need to check off: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service," Cloyd says. "Each of these is fairly straightforward for commercial cloud networks, but when applied to the DoD, each has unique challenges. [For example], self-service is about the provisioning of authorized users or services. One unique risk associated with self-service authorized end users is the role of insider threats. The DoD-broad community has millions of users; the Army alone has 1.2 million core users. These are huge numbers and within such a large population insider risk is a real threat. A provider needs to provision its services with proper governance to prevent insider threats. Broad network access is one of the most interesting characteristics from a DoD perspective, as so much of the DoD is focused on rigid, tightly controlled networks such as service-specific portions of NIPRNet and SIPRNet rather than on open network access like the Internet at the other extreme. The key is for services to be available across the entire DoD, and this is largely possible today. The problem is as soon as access is broadened, it increases the attack surface, making the idea of a perimeter and a boundary much more nebulous."

The Army Knowledge Online (AKO) program "is a great example of a system that exhibits almost every one of the NIST cloud characteristics in that the NIPRNet version supports broad network access from anywhere in the world via the Internet, user accounts and resources are self-provisioned and support elasticity and spikes in usage, the infrastructure allows reallocating virtualized resources within or across its multiple data centers, and the system has been designed to support multitenancy and very detailed usage data for potential charge-back," Cloyd says. "With checks next to each of those essential characteristics, AKO could be poised as a great example of Software as a Service (SaaS)." SaaS is the capability provided to the consumer to use the provider's applications running on a cloud infrastructure, according to NIST. Other types of service include Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

"The DoD will likely set up a cloud for each classification level, as multilevel classification within a single cloud environment is just too much to tackle right now," Cloyd says. "Down the road, I hope they will move to having multiple classification levels in a cloud, as in the long-term if we do everything right with cloud computing, trusted multitenancy at different classified levels should be within reach."

### Data is key to the kingdom

Secure cloud computing is more than just the network; it is also important to focus on the identity and authentication management to make sure each piece of data in a cloud is being accessed by the proper individual. This is roughly akin

## Securing the physical platform

Engineers at LinuxWorks are enabling cloud security in hardware by providing assurance via a software separation kernel. "Too often people cut corners when leveraging their OS and they don't know what's in it," says Will Keegan, Technical Director, Software Security at LinuxWorks ([www.linuxworks.com](http://www.linuxworks.com)). "If assurance also can be applied dynamically at the hardware level, a whole new avenue for getting to a trustworthy solution is created."

"While the cloud is different from a hardware device in that it consists of more than one device, it is the same in that it is an integrated computing system, and the same rules of assurance apply," he continues. "However, they are not identical computing systems and they would require different assurance techniques. Users need to know the OS running on it is secure, know where it came from, know where the virtualization came from, whether it is authentic, etc. The first phase would be about securing the hardware platform and supervisory kernel that hosts the cloud services. The second phase would be securing the interfaces between cloud software service stacks."

"A layered approach is not needed, but it is a good approach that allows integrators to reuse existing components," Keegan continues. "A separation kernel can be used to ensure layers are protected from each other and have controlled nonbypassable interfaces. The separation kernel also isolates functions and controls the information flow between functions. It ensures a user cannot modify the functions or bypass the information flow enforcement. Separation kernels give integrators the opportunity to build systems that cannot be subverted, but integrators can certainly build flawed complex implementations with a separation kernel. Our separation kernel is secure by fully implementing a least privilege design both internally in the kernel design and externally in the user API. The internal structures of the kernel do the least amount of work with the least amount of privilege to reduce complexity and attack surface. The user API has no privilege to subvert the kernel or other apps and has full control to partition code and control information flow between partitions and devices."

"We already built the hypervisor in our separation kernel. Our next-gen technology lives outside the hypervisor and separation kernel," Keegan says. "We can call them MILS Cloud Components, which are critical security components that have the least privilege necessary to protect application-level services. They do not belong in the kernel because they would have too much privilege and add complexity that would expand the attack surface, and they do not belong in third party services because we do not trust third parties for controlling critical functions that other service providers and customers depend on. So we rely on a separation kernel vendor who knows the most about the integrated services and securing the physical platform to build trustworthy applications."





**Figure 1** | SafeNet engineers are working on key management schemes to enable multifactor authentication to help protect data in the cloud.

to needing an ID card and a retina scan to enter a building and also needing additional authentication factors to access a file in a drawer.

"So much client focus in the DoD is about the network," Cloyd says. "However, you cannot just focus on a network-based, umbrella approach to protect systems. Data is the key to the kingdom so you have to protect the application, as well as the traditional network boundaries. Identity and access management at the application are finally getting the attention that they deserve, but they are not new concepts. With a growing importance on stronger authentication, cloud providers need to increase the number of authentication factors they consider. The typical two-factor authentication approach – typically a Common Access Card (CAC) in DoD – is not enough; they need to add additional factors based on the risk associated with certain data. We are focusing on 'fine-grained entitlements' in applications and how to secure everything with a lot of fidelity at the application level and data level. This also includes new approaches and technologies to securing data at rest."

"There is a general government-focused trend to move to multifactor authentication," SafeNet's Moore says. "The government wants to move away from password-based protection to Public Key Infrastructure (PKI) protection. Things such as SIPRNet smart cards provide two-factor authentication and meet PKI standards. There is a large U.S. government Key Management Infrastructure (KMI) program that is focused on creating and delivering keys to government users ensuring that key rotation – the key life-cycle management – is up to date and efficient. The life of a key depends on the mission

requirements. It can last from 24 hours to 6 months to a year if necessary.

"Key management plays into cloud security," Moore continues. "Data encryption is a typical protection in laptop or mobile devices – encryption of the drive and on-device storage. Encryption also will be needed for data that is stored off-premise in a cloud. These virtual worlds are multitenancy environments with many users and servers involved, creating a need for more granular encryption than is provided at the device level. We will need to encrypt data at the object level – pictures, maps, files, and so on. Encrypting at the object level and tagging each object with situational awareness data require strong enterprise key management so data can be securely accessed anywhere from any device. The data just needs to be locked down at the most granular level with the lock being an encryption key management scheme that protects data at the object level.

"One of the biggest threats is the administrative threat, caused by vulnerabilities related to having a super user or super password that can access every file," he says. "Industry and government are moving away from super users due to leaks that have occurred. If that super user or super password is compromised, every piece of data in a system is vulnerable. At SafeNet we assume someone is bound to get in, so we work at encrypting each object so even when they get in they can't wreak havoc with the data. The more granular you drive the encryption, the less exposure your data will have to malicious attacks."

#### DDoS attacks

A cyber threat that targets clouds that is becoming more common and getting more attention in the media is the

Distributed Denial of Service (DDoS) attack, which messes with the shared infrastructure of a cloud, causing all the subscribers to be at risk. "Cloud organizations that host the services of other organizations and operate their data centers are providing public cloud services instead of private," says Ronen Kenig, Director of Security Solutions at Radware ([www.radware.com](http://www.radware.com)). "Public clouds are more likely to be attacked by threats such as DDoS. A public cloud, for example, would be a news site that might be hosting multiple user services on their cloud or business-oriented applications. Each client is then part of the cloud's shared infrastructure. Anything between the Internet and the servers is a shared infrastructure. If something happens to the shared infrastructure, all customers hosted in the cloud will be affected. If a firewall goes down, nobody can access the cloud. About 63 percent of DDoS attacks strike the shared infrastructure as it's the first thing the attack will hit.

"Prior to recent attacks on financial institutions in the U.S., there was not much awareness or knowledge of DDoS attacks and other cyber threats," Kenig says. "However, once the first bank became a victim, immediately all the other institutions started to learn more about the attacks, search for solutions, then deploy those solutions quickly. When I look at military

cloud security solutions, there are many vendors and partners providing tools and solutions, but not many providing availability security. DDoS attacks are hurting the availability of online services and many antivirus vendors and firewall vendors do not focus on the availability aspect."

Cloud providers find protecting the shared infrastructure can be challenging because it is an expensive up-front cost, he continues. "However, if a DDoS attack disrupts the shared infrastructure, every client in the cloud will be adversely affected. If a cloud provider can't protect the shared infrastructure, other customers will be reluctant to do business with them and they could become a joke in the industry. For large-volume attacks, Radware offers a new security service called Defense Pipe that basically is designed to protect the Internet pipe of a provider, no matter what security solution they use to protect their other data. With Defense Pipe, we divert traffic into a scrubbing center, where it can absorb very large volume to mitigate its effect and protect the cloud service. We activate the service when the Internet pipe is about to get saturated to better protect the cloud data center. All the effects of an attack can be blocked in the data center except those that are saturating the Internet pipe." **MES**

### Securing the supply chain

Long before the cloud is set up, malicious code or counterfeit parts can find their way into a system undetected, later wreaking havoc on networks. Two companies are looking to mitigate these supply chain risks at the hardware and software level: Sypris Electronics, LLC and GrammaTech respectively.

Engineers at Sypris Electronics are working to enable robust cloud security by providing security assurance in hardware at the silicon level. Sypris Electronics believes this is a paradigm shift in approaching security as "no one out there is really addressing security from the ground up," says Joel Stein, Senior Director, Information Security Systems and Cyber Defense & Network Assurance at Sypris Electronics ([www.sypris.com](http://www.sypris.com)). "If you can trust the hardware, then it makes it easier to trust the software running on top. We are looking at cloud-supported hardware authentication to enable machine-to-machine trust so when a user logs into a cloud, the machine itself can authenticate that user in addition to the network and software authentication processes he may go through," Stein says. "The Resilient Device Authentication System (RDAS) supports application services that control how a user may authenticate to hardware and how the hardware authenticates to the back end service. It does not require specialized hardware; you can buy an FPGA or work with us to design it in with your own board, or Apple, or Dell, etc. The whole purpose is to create an environment that can build a security as a service capability into cloud security. At the application layer, we are in the emerging technology demonstration phase of this solution.

Sypris engineers "create physically uncloneable functions in the silicon itself," Stein continues. "The electrical properties

are different from chip to chip, and we make use of that difference to create a function on the FPGA or ASIC itself that will use the variance between the hardware component electrical properties to uniquely identify each chip. We consider it a biometric for the chip itself. The resultant solution can be used as a trust anchor for the device it is embedded in, making it ideal for supply chain risk management applications as it prevents counterfeit components from being used in the hardware. If a counterfeit or malicious hardware component were to be used, the component would not be registered and would be recognized as not having the proper chip biometric, which means trust anchor would not be present and we would know something changed on the device or the component it was to be placed on."

Engineers in GrammaTech's research department in Ithaca, NY are working on finding security vulnerabilities in firmware for devices that might attach to computers such as printers, network interfaces, routers, fax machines, and so on. All these devices are running firmware that could contain malicious code that is mostly undetectable at this time, says Paul Anderson, VP of Engineering at GrammaTech. It could enable enemies to break into voice over IP telephone networks as the microphone is software-based, he continues. They can listen and record every conversation undetected. There is no easy way to get the code to test it effectively for security vulnerabilities, so DARPA has tasked GrammaTech to research ways to remove the code and to analyze it through static analysis and non-static analysis via their CodeSonar tool, Anderson says. Multiple companies are participating in the program, but no one is under contract yet, he adds.



# Up to 136 Programmable Discrete I/O Channels... on One Rugged Board!



Proudly made  
in the USA.

Only NAI delivers high density 0 - 60VDC discrete I/O with a multitude of valuable user programmable features.

- Senses broken input connection and if input is shorted to +V or to ground
- Handles high in-rush current loads (e.g. two #327 incandescent lamps in parallel)
- Supports "dual turn-on" (series channel output) applications
- Reads I/O voltage and output current for improved diagnostics (indicates if load is connected)
- Current shares by connecting multiple outputs in parallel, to sink/source up to 2A per channel/bank
- Continuous background built-in-test (BIT) during normal operation, status of channel health and operation feedback
- Programmable for Input (voltage or contact sensing) or Output (current source, sink or push-pull) per channel/bank

Discrete I/O... available on a  
board or in a rugged system.

The Single Source for Intelligent COTS I/O Solutions

Visit [www.naii.com/Discrete-I-O/F18](http://www.naii.com/Discrete-I-O/F18) or call us at 631-567-1100 today.



**Embedded Boards**

**Power Supplies**

**Instruments**

631-567-1100 • Fax: 631-567-1823 • [www.naii.com](http://www.naii.com)



# Encryption and the migration to COTS technologies

By Rubin Dhillon and Jim Kelly

*The network is becoming increasingly crucial to the world's armed forces. Unsurprisingly, it uses the same technologies that are proven in the commercial world, with much of the equipment sourced by the armed forces being of COTS origin. But the military needs a level of security – anti-tamper, information assurance, data destruction, encryption – way beyond what the commercial world requires. COTS solutions have emerged that leverage the innovations driving the commercial mobile data industry while addressing specific military security concerns such as encryption.*



U.S. Air Force photo



Armed forces around the world, and in particular the United States military, are striving for total information dominance over foreign adversaries. This new focus on information dominance has transformed the battle space, where all assets – unmanned aerial-, terrestrial-, and sea-based platforms; ground combat vehicles; precision guided weapons; handheld computers; and so on – are in constant communication and collaboration over a secure and reliable tactical network. This network is expanded through larger terrestrial networks and support systems in order to provide warfighters and commanders with the information needed for an accurate and real-time common operating environment.

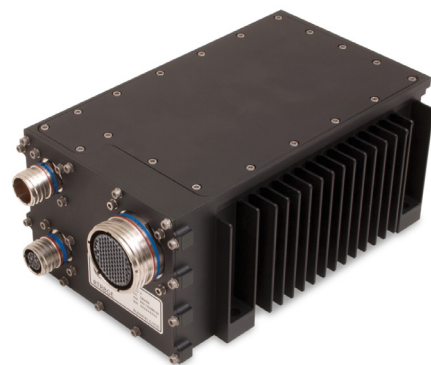
Encryption of all this classified information, both during transmission (“data in motion”) or while it is stored (“data at rest”) is critical to ensure both military operations success and personnel safety. However, a military organization has to be able to communicate securely with its government and potentially other governments, as well as with nonmilitary organizations that might be involved. Using COTS hardware, standard encryption algorithms, key exchange, digital signatures, and hashing enable the timely sharing of classified information.

#### Encryption transitions to COTS, GOTS

Historically, military critical infrastructure relied on platforms and technologies specifically designed, developed, and delivered for military use. However, initiatives to streamline procurement, improve deployment times, and reduce cost led to the adoption of architectures that increasingly rely on Commercial Off-the-Shelf (COTS) products and technologies or slight derivatives customized for military use – Government Off-the-Shelf (GOTS). This focus on commercially derived technologies is currently seeing renewed emphasis, with these COTS and GOTS platforms leveraging the most advanced and forward-looking technologies and architectures in the industry – for example, virtualization, mobility, cloud computing, and so on.

The migration to COTS/GOTS systems increases the importance and

**Figure 1** | GE's RTR8GE secure battlefield router uses a FIPS-certified version of Juniper Networks' Junos network operating system.



complication of the role encryption plays for the warfighter. How do governments ensure that they can trust these devices to handle their most sensitive data, and how can individual vendors or industry partnerships provide technologies and platforms that facilitate the approved encryption processes?

In the United States, military cryptography is traditionally developed and maintained by the National Security Agency (NSA). Not only does the NSA develop secret crypto algorithms designated as “Type 1” or “Type A” cryptos for classified U.S. government communications, but its responsibilities also include the approval of all military communications and computing devices that implement encryption. As the requirements for military communications have grown rapidly over the past few years, installation, deployment, performance, obsolescence, and maintenance issues and rising costs are becoming an increasing concern. In 2005, the NSA and the U.S. DoD launched the Cryptographic Modernization Program to combat these issues.

Perhaps the most remarkable development of the Cryptographic Modernization Program has been the acceptance and adoption of nonclassified, industry-developed cryptographic algorithms. These so-called “Suite B” cryptos are more conducive to the military’s COTS/GOTS systems strategy.

#### Cryptographic algorithms are open standards-based

Suite B encrypted systems are based on open standards cryptographic algorithms. Governments such as that of the United States publish guidelines and standards that outline which algorithms may be used for classified and nonclassified information. The Federal

Information Processing Standard FIPS 140-2 published by the National Institute of Standards and Technology (NIST) outlines the cryptography requirements for all devices used on a National Security System. Government/military agencies use the Common Criteria for Information Technology Security Evaluation (often referred to as simply *Common Criteria* or CC) international standard when they specify security requirements. Using a Common Criteria rating scale ranging from Evaluation Assurance Level (EAL) 1 through 7, the government can compare how rigorously particular devices have been tested to meet their security requirements. Implementing standard cryptographic algorithms and key exchange is not authorized on a National Security System until they have been tested and certified. Common Criteria evaluation and validation must be done by an accredited NSA/NIST testing laboratory.

It is important to point out that a higher EAL rating does not necessarily mean that one device is more secure than another – only that it has been tested more rigorously, suggesting a higher level of trust. Most hardware network devices carry an EAL rating between 1 and 4. GE’s RTR8GE rugged secure battlefield router, for example, runs a FIPS-certified version of Juniper Networks’ Junos network operating system and has achieved the Common Criteria EAL 4 rating, which states “methodically designed, tested, and reviewed” (Figure 1). Given the rapid growth in the number of devices going through the evaluation process and the time and cost involved in obtaining such a high rating, EAL 4 rated devices will likely be rare in the future. Most networking devices today only carry an EAL 2 rating, which designates that the solution was “structurally tested.”

### Encryption methodologies are evolving

The premise of public-key cryptography is that the mathematical problem that must be solved to decrypt the communication would take so long to

solve that by the time it was solved, the information would no longer be useful. Suite B uses Elliptical Curve Cryptography (ECC), which has the advantage of using much smaller keys with an equivalent level of security,

thereby reducing the computing power and bandwidth required. The efficiency of ECC enables a high level of security for the wide range of Internet Protocol (IP)-enabled devices available today.

### IPsec key creation and management

Each IPsec node pair is configured with a unique key that allows the pair to encrypt and decipher their communication. The distribution and management of these keys are critical in ensuring the security of encrypted communications. There are three kinds of key creation methods:

- › **Manual key:** Often used in small, static networks, this involves administrators manually configuring security at each end of the encrypted link.
- › **Autokey IKE:** Keys are generated by each end node automatically using the Internet Key Exchange (IKE) protocol. Authentication is achieved through pre-shared keys or with security certificates issued by a trusted Certificate Authority (CA).
- › **Diffie-Hellman (DH) exchange:** This methodology allows each node to produce a shared secret value. This secret value is not transferred over the communications link. There are 5 DH groups ranging from Group 1 (768-bit keys) through Group 5 (1,536-bit keys).

› **Sidebar 1** | IPsec key creation methods

### Common FIPS-approved cryptographic algorithms

There are many FIPS-approved cryptographic algorithms that are commonly implemented, including the following:

- › AES 128, 192, 256 for encryption/decryption
- › DSA with 1,024-bit keys for digital signature generation and verification
- › RSA with 1,024- or 2,048-bit keys for digital signature generation and verification
- › Triple-DES for encryption/decryption
- › SHA-1 for hashing
- › SHA-2 for hashing (SHA-256)
- › HMAC-SHA-1
- › HMAC-SHA-256
- › FIPS 186-2 RNG (with Change Notice)

### IPsec security protocols

IPsec uses two protocols to secure communications at the IP Layer. The Authentication Header Protocol verifies the authenticity/integrity of packet content and origin. This is achieved by calculating a checksum using a secret key and either the MD5 or SHA-1 hash functions.

The Encapsulating Security Payload (ESP) protocol encrypts either the entire IP packet or just the data payload depending on the configuration and architecture of the network.

These encryption algorithms are often used:

**Triple-DES or 3DES** is a block cipher. Therefore, it operates on fixed-size blocks of data. 3DES replaced the DES algorithm. The latter is no longer considered secure.

**AES-GCM** with key lengths of 128, 192, and 256 bits is also used as an integrity algorithm. AES-GCM is part of Suite B and is a symmetrical block cipher that encrypts/decrypts data in 128-bit data blocks.

**AES-CBC** (AES in Cipher Block Chaining mode) with key lengths of 128, 192, and 256 bits is part of Suite B. Similar to 3DES, it operates on fixed blocks of data. These data blocks are 128 bits wide. Cipher Block Chaining is used to hide identical blocks of data within the same packet, ensuring that all encrypted data blocks are unique.

› **Sidebar 2** | Common FIPS-approved cryptographic algorithms and IPsec security protocols explained



There is no question that Internet Protocol is rapidly becoming the dominant network protocol used throughout military communications networks, and while it is still common to find specialized military- and application-specific protocols in the tactical battlefield environment, these are being replaced. Therefore, Internet Protocol Security (IPSec) (see Sidebars 1 and 2), a set of open standard Internet Engineering Task Force (IETF) standards, is used throughout military networks to configure encryption and secure sensitive communications. IPSec with the approved, tested, and validated encryption algorithms and key management can meet the FIPS 140-2 and Common Criteria requirements for encryption over IP networks.

IPSec is a point-to-point architecture that manages key exchange, verifies the integrity of data packets, negotiates crypto algorithms, and authenticates between two end-nodes on a network. However, regardless of the key management methodologies or security protocols implemented, IPSec might not be ideal for tactical military networks, particularly as they grow in size and complexity. Key distribution and management will likely represent serious challenges, and application performance, dynamic routing, reliability, and management might all suffer.

A group-based network encryption has evolved that promises to address the limitations of traditional IPSec point-to-point architectures. The standards-based Group Encrypted Transport (GET) integrates routing and encryption together in the network and alleviates the need to set up individual point-to-point connections. Since policies and keys are managed from a central point, key distribution and management are greatly simplified. Group Encrypted Transport is well suited to battlefield networks, given their dynamic and mobile nature, with diverse devices transmitting and receiving sensitive data over a large geographic area. Military network architects will likely prefer

the flexibility afforded by GET over traditional IPsec tunneling.

### Encryption faces new challenges

Server virtualization and hypervisor technologies have grown to enable cloud computing in the commercial/data center world, and these technologies are now finding their way onto the battlefield. Government agencies, including the DoD, continue to embrace emerging technologies such as cloud computing. In fact, cloud computing

promises to address some of the DoD's most pressing issues such as improving deployment time for new warfighter applications and technology, enabling data sharing between joint forces and allies, and simplifying and streamlining network management – all while reducing costs.

The basic concept behind the implementation of cloud computing, virtual machines, and virtual networks is to replace hardware devices with software.



**QUALIFIED TO PERFORM.**

Effective tactical Communications on the Move (COTM) depends on proven, secure Mobile Ad Hoc Network (MANET) routing technologies. With Parvus' DuraMAR 5915, tactical radios and satcom gear now interface with a MIL-STD qualified, SWaP-optimized mobile router/switch subsystem integrating Cisco Systems IOS management, information assurance, and mobile IP routing capabilities.

**DuraMAR 5915** 

- Rugged Cisco IOS Secure Mobile Router
- Integrated Gigabit Ethernet Switch
- Data, Video and Voice Support
- Qualified to MIL-STD-810G, 461F
- Size, Weight & Power (SWaP) Optimized

 **Parvus**

[www.parvus.com](http://www.parvus.com) | 800.483.3152 | [sales@parvus.com](mailto:sales@parvus.com)



A single rugged multicore computing device installed in an unmanned platform, for example, could perform the function of mission computer, router, firewall, and sensor processor – an architecture that provides significant SWaP benefits, essentially replacing four individual devices.

However, this concept of a software-based appliance is challenged by the fact that government and DoD policies, procedures, certifications, and testing

methodologies primarily revolve around hardware devices. Foundations have been laid by the NSA that would allow use of software-based Suite B crypto “devices” running in virtual machines, but the evaluation process needs to catch up. Since the benefits of cloud computing and virtualization are so compelling, industry and the DoD are working closely to address these procedural issues and we will likely see this addressed within the next few years.

### Commercial users will follow

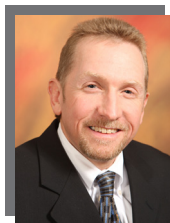
As the next phase of the Internet begins to develop with the Industrial Internet Revolution, the focus is shifting from communications between people to communication between machines, manufacturing plants, energy production facilities, logistics/shipping hubs and even aircraft engines. All these are transmitting, storing, and sharing data like never before. Other government agencies and Non-Governmental Organizations (NGOs) providing law enforcement and homeland security seek the benefits of cloud computing architectures to share critical and sensitive information as well.

However, many of these nonmilitary industries and applications are unprepared for the security implications that ubiquitous connectivity brings and therefore look to the military sector for the technology and procedures needed. Solutions that have a Common Criteria EAL rating are attractive in nonmilitary markets and, as the Industrial Internet grows, it is likely that more and more devices will embed the encryption algorithms, methodologies, and design principles that are common in military systems. It is safe to say that this will be an exciting arena to watch for many years to come. **MES**



**Rubin Dhillon** is Business Development Manager at GE Intelligent Platforms. He can be contacted at [rubinder.dhillon@ge.com](mailto:rubinder.dhillon@ge.com).

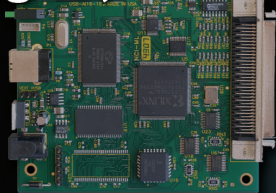
GE Intelligent Platforms  
[defense.ge-ip.com](http://defense.ge-ip.com)



**Jim Kelly** is Product Line Manager at Juniper Networks. He can be contacted at [jkelly@juniper.net](mailto:jkelly@juniper.net).

Juniper Networks  
[www.juniper.net](http://www.juniper.net)

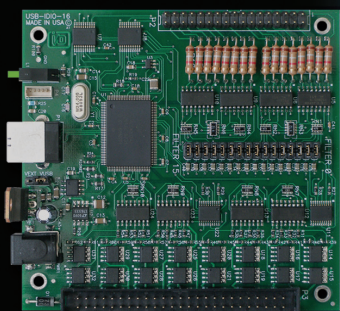
## USB Embedded I/O Solutions Rugged, Industrial Strength USB



**16-Bit Multifunction Analog I/O, Up to 140-Channels 500kHz**

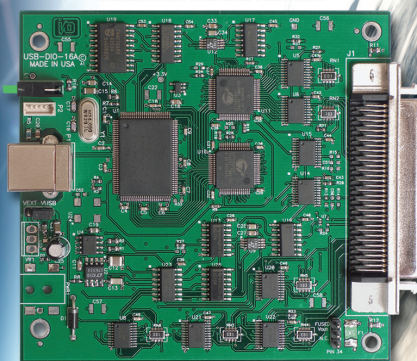
### USB/104® Embedded OEM Series

- Revolutionary USB/104® Form Factor for Embedded and OEM Applications
- USB Connector Features High Retention Design
- PC/104 Module Size and Mounting Compatibility
- Extended Temperature and Custom Options Available
- Choose From a Wide Variety of Analog, Digital, Serial, and Relay I/O



**Isolated Digital I/O 16 Inputs and 16 Solid-State Relay Outputs**

**Digital I/O, Sustained 16 MB/s With 80 MB/s Bursts**



**ACCES I/O Products' PC/104 size embedded USB boards for OEM data acquisition and control.**

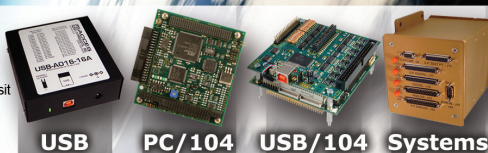
**OEM System SPACE Flexibility with dozens of USB/104® I/O modules to choose from and extended temperature options - Explore the Possibilities!**



**Saving Space, The Final Frontier**



The source for all your I/O needs  
To learn more about our Embedded USB/104® I/O boards 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**



Others say they're FAST...

But do they have the

**SCALE** to deliver?



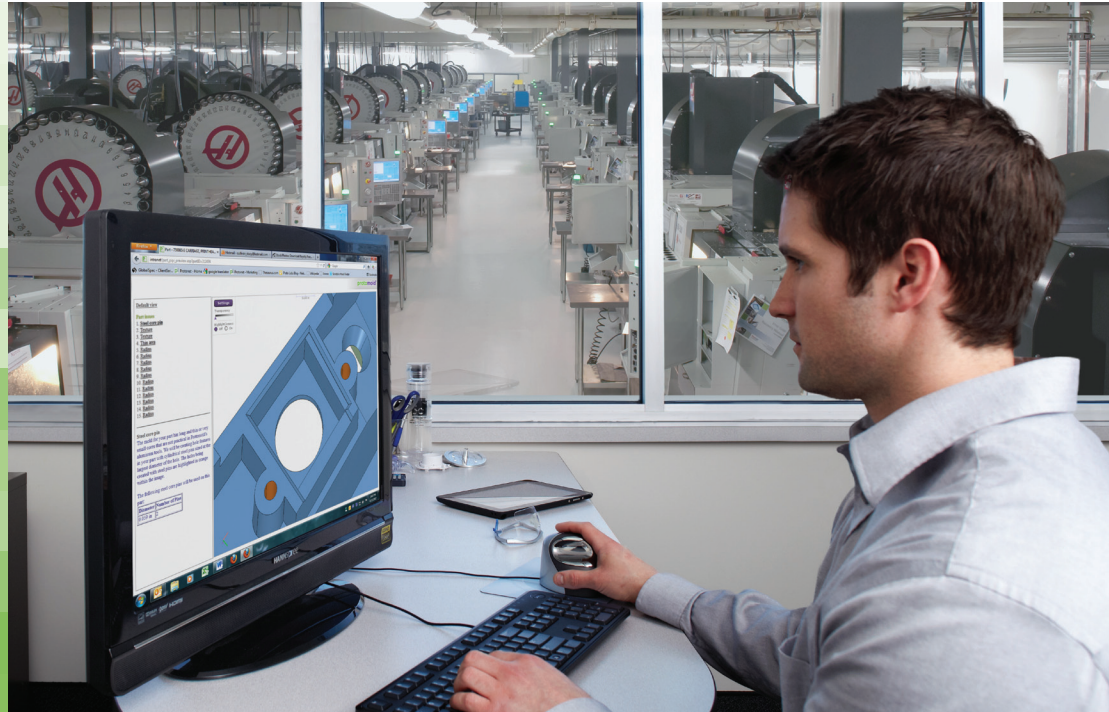
### Puzzled by resin choices?

Request your FREE Resin Puzzle—nine of the most common thermoplastics used in injection molding. Visit [www.protolabs.com/parts](http://www.protolabs.com/parts) to request your design aid. Enter code MY13B.



### Check out our virtual tour!

Visa/Mastercard Accepted  
© 2013 Proto Labs, Inc



**Proto Labs'** entire operation is optimized to deliver quick-turn CNC machined and injection molded parts in as fast as one business day. We manufacture parts every day for thousands of customers, many of whom come to us at the last minute with dozens of designs they need to test ASAP. Since 1999, we've produced tens of thousands of molds, and shipped tens of millions of parts to our customers all over the world.

Sure, it's our technology that allows us to make your parts faster than anyone else. We back it up with large-scale global manufacturing facilities with hundreds of CNC machines and injection molding presses on three separate continents.

Whether your project calls for a few machined parts or thousands of molded parts from 50 different designs—we have the scale to meet your needs. Every time!

Call 877.479.3680  
or visit [www.protolabs.com](http://www.protolabs.com)

ISO 9001:2008 Certified • ITAR Registered

**proto labs**<sup>®</sup>  
Real Parts. Really Fast.™

## Deploy warfighter applications faster with open source Platform-as-a-Service

By David Egts

*Up-and-coming Web startups are leapfrogging each other to market using Internet-hosted Platform-as-a-Service (PaaS) technologies. PaaS allows these startups to innovate rapidly by focusing more time on their mission and less time managing hardware and software. Can the warfighter benefit from PaaS too? Yes, if the warfighter controls the PaaS stack – and open source delivers that control.*



U.S. Army photo by Spc. Marcus Fichtl



Historically, warfighter applications are often monoliths from the power plug to the running application – they were often designed for a single purpose without reuse and interoperability in mind. The design variances of these monoliths have also prevented economies of scale in terms of technology and Certification and Accreditation (C&A) reuse. This lack of reuse can prevent applications from getting to the warfighter in a timely fashion and can also lead to cost and schedule overruns. By identifying areas of commonality that could be standardized, certifying those components once for reusability, and focusing more on the remaining differences, agencies can increase efficiency and save the time involved with regularly recertifying applications. Platform-as-a-Service (PaaS) is one solution that can alleviate these challenges by shrinking timelines and eliminating vendor lock-in. PaaS utilizes IT stacks that are consistent across multiple applications, including everything from the power plug to hardware to virtualization to operating system to application server. The IT stack can be certified once and reused many times with a significantly smaller amount of re-certification work. As such, developers can focus more on their application and get it into production sooner since it's running on a stack of hardware and software that someone else has already rigorously certified.

Figure 1 illustrates the difference between a developer-maintained stack versus a PaaS stack. Note how the developer's effort is diffused down the stack without PaaS. Instead of focusing on the application itself, effort needs to be expended to specify, acquire, integrate, deploy, certify, and maintain all

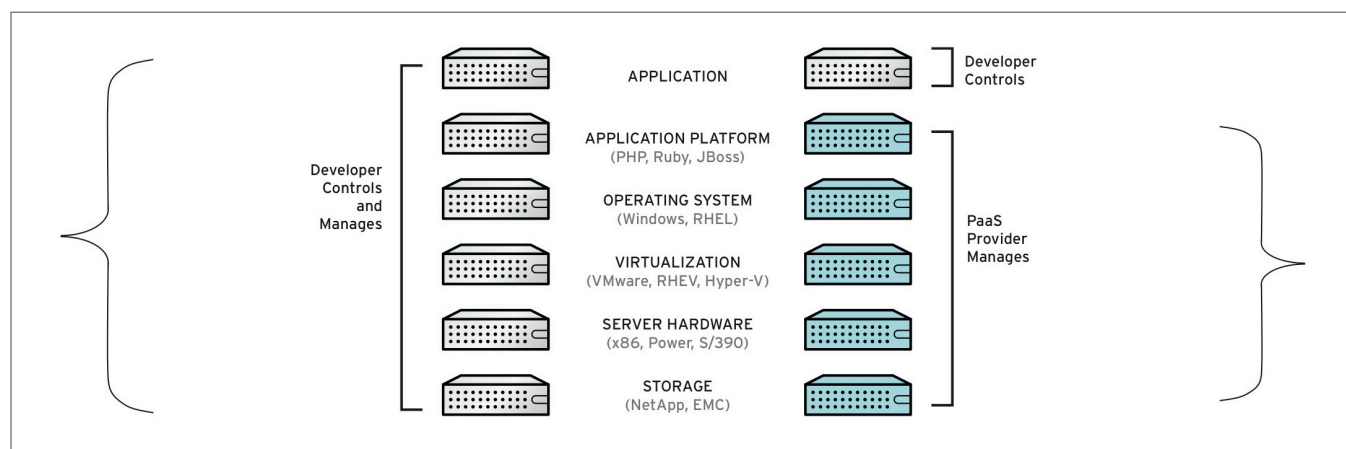


U.S. Army photo by Spc. Jeffrey Alexander

the components of the stack. Further, every application's developer may specify a different vendor for each of the components, requiring the end customer to be proficient in all. This erodes economies of scale in terms of training, operations and maintenance costs, and volume purchasing. With PaaS, the developer can dedicate more time to the application itself while letting the PaaS provider take advantage of economies of scale while maintaining and securing the infrastructure and platform hardware and software on the developer's behalf.

#### Proprietary PaaS is a nonstarter for the warfighter

One problem with PaaS, however, is that most Internet-hosted PaaS providers are proprietary. Many of these PaaS providers



**Figure 1** | Developer-maintained stack compared to PaaS stack

only support their proprietary languages and/or libraries, which only run on their back-end servers on the Internet. If a developer ever wants to move an application to another PaaS provider or move an application to on-premise servers, application porting is necessary. And in the case of embedded and/or classified systems, which may not have Internet connectivity, proprietary Internet-hosted PaaS is not an option. This is where open source PaaS can provide a solution. A PaaS stack that is open source from top to bottom can be run on a public cloud, a classified enclave, or a tactical vehicle and provide the same experience. The application written for one deployment model is also portable across all. Open source PaaS offers the deployment efficiencies of traditional PaaS with the platform deployment target choice of open source.

Figure 2 illustrates this difference between a hosted PaaS provider and an on-premise PaaS solution. Both offerings allow the developer to focus on their application, but only an on-premise PaaS solution can run in an end user's data center, classified enclave, tactical vehicle, airborne or undersea platform, and so on. When choosing a PaaS solution, one should ensure that applications written in a hosted PaaS environment can run on an on-premise PaaS environment with little to no modification. The best way to do this is to ensure maximum portability by ensuring the PaaS solution and applications are built upon open source software.

### Open source PaaS delivers agility with control

OpenShift is an autoscaling, open source PaaS for applications and includes hosted, on-premise, and community offerings (Figure 3). It was first released in developer preview in May 2011 to address the need for vendor-agnostic PaaS using open source principles and serves as a good example of the aforementioned PaaS concepts. It runs on top of Red Hat Enterprise Linux and each user-developed application runs as a PaaS "gear" inside a Linux container. By using Linux containers and not giving each application its own virtual machine, applications can be thinly and rapidly provisioned, which is ideal for massive scale as well as for small form factor embedded tactical

“ By choosing these cartridges, the developer leaves the maintenance and security of that code up to the centralized PaaS administrator. This provides economies of scale in that the PaaS administrator can apply a bug or security fix to a cartridge once and all developers' applications using that cartridge immediately benefit. ”

deployments. Even though the applications are multitenant and running on the same Linux operating system, the Linux containers are confined using Linux resource control groups called *cgroups*, as well as Common Criteria-certified and NSA-developed SELinux.

Once the application's gear is provisioned, a developer can then choose pre-canned PaaS "cartridges" of application frameworks, languages, and SQL and NoSQL databases. By choosing these cartridges, the developer leaves the maintenance and security of that code up to the centralized PaaS administrator. This provides economies of scale in that the PaaS administrator can apply a bug or security fix to a cartridge once and all developers' applications using that cartridge immediately benefit.

Once the cartridges are in place, the developer can then add mission-specific application code to the PaaS using git or an Eclipse IDE with a compatible PaaS plug-in. Once the code is pushed into the gear, it's up and running. After deployment, DevOps tools such as Maven and Jenkins can also be added for automated building and continuous integration. When the

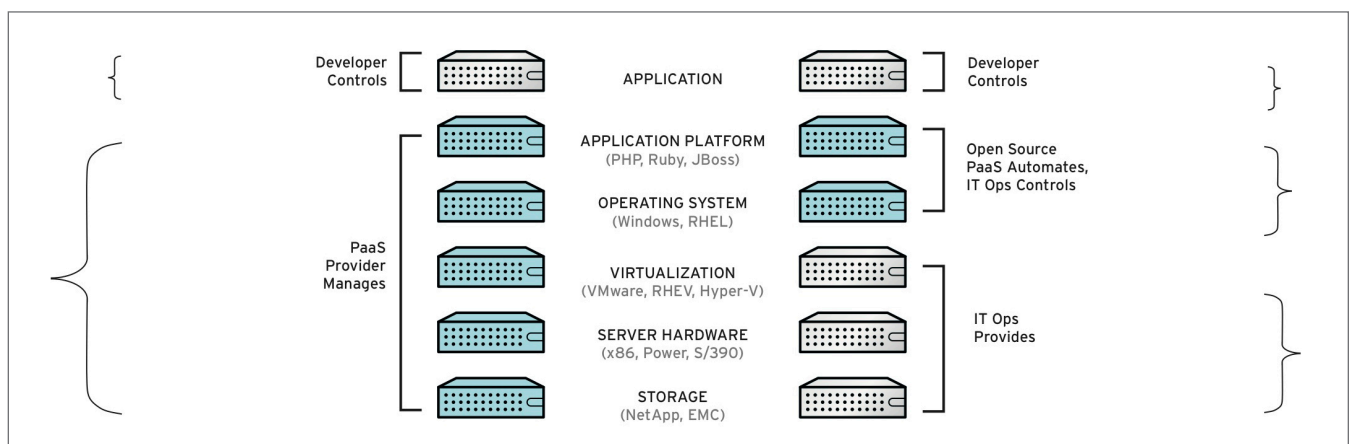


Figure 2 | Hosted PaaS compared to on-premise PaaS



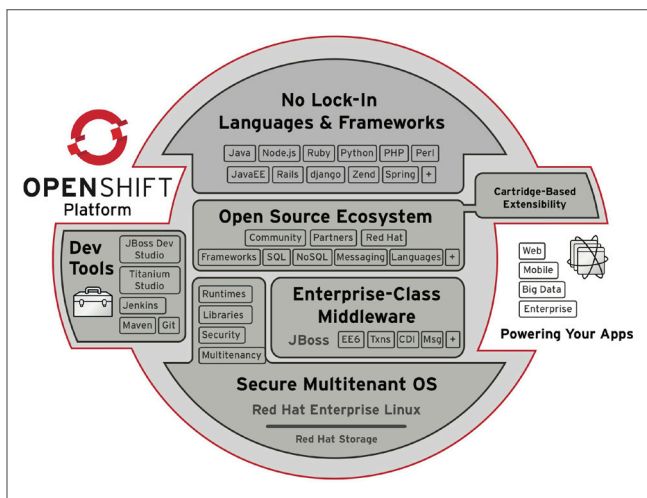


Figure 3 | OpenShift components

application has been put into production, and if it goes “viral” (in a good way), the PaaS even has an HA-Proxy Cartridge that can automatically spin up and spin down additional gears based upon server load. By being built on top of open source, any application written for the PaaS can run without it, so vendor lock-in is eliminated. Further, an application can be developed on the PaaS and then deployed without it, such as in a light-weight tactical or embedded environment.

## PaaS is the future

Agencies are being forced to do less with more. They need to identify areas of redundancy and consolidate efforts without compromising their missions. As proven in the private sector, PaaS provides the ability to rapidly deploy applications by focusing more on the mission and letting the PaaS provider economically provide a secure and stable platform upon which to build. For the warfighter, Internet-hosted PaaS is often a nonstarter. Applications need to run disconnected in either tactical and/or classified environments. Again, open source PaaS, such as Red Hat's OpenShift, for example, provides a way for the warfighter to take advantage of the economies of scale of PaaS with the control of open source.



**David Egts** is the Principal Architect for Red Hat's U.S. Public Sector organization, specializing in the application of open source enterprise infrastructure technologies within federal, state, and local government agencies, the Department of Defense, and educational institutions.

Contact him at [degts@redhat.com](mailto:degts@redhat.com) and follow him on Twitter @daveidgts.

Red Hat

703-748-2201 • [www.redhat.com](http://www.redhat.com)  
<http://openshift.redhat.com>

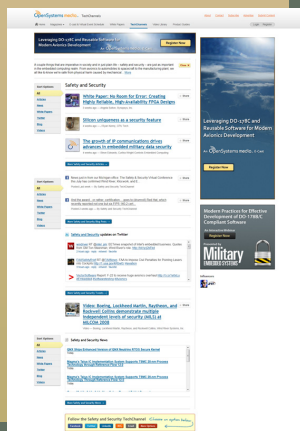
## Safety and Security TechChannel

Up-to-the minute, in-depth, focused info

OpenSystems Media is continuing innovation with TechChannels:

Microsites that explore leading-edge embedded topics in more detail. Combine contributed articles from industry experts with the best in staff-written material, and mix in instant information from:

- Latest news and videos
- Blogs
- White Papers
- E-casts
- Twitter
- Facebook
- LinkedIn



[tech.opensystemsmedia.com](http://tech.opensystemsmedia.com)

introducing **RPC24**  
**Rugged, Deployable, Mission Oriented Data Storage**

**Drive Magazine Based High Performance Multi-Protocol RAID System**

- **24 Solid State or Hard Disk Drives** in only 2U of panel height
- **Two Quickly Removable Storage Magazine** - 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 5000 MB/sec and 3000 MB/sec respectively
- **MIL-STD-810G, MIL-STD-461E Certified**

**PHOENIX**  
 INTERNATIONAL  
[www.phenxint.com](http://www.phenxint.com) 714-283-4800

AS9100 Rev C/ISO 9001: 2008 Certified



## Flight, mission, and radio management in one box

The CMA-4000 Flight and Displays Management System, developed by engineers at Esterline CMC Electronics in Montreal, leverages an open architecture design to include radio control management, mission management, and flight management functions in one 11 lb box. The CMC Electronics box can drive as many as two external MultiFunction Displays (MFDs), enabling graphics capability and integrated management of the CDU/MFD manmade machine interface. It also provides multiprocessor support for developing customer or independent software application designs.

Flexibility is built in via a variety of standard bus, analog, and discrete interfaces with a total of 284 pins at the rear connector. The maximum size of the 640 x 480 color display is 5" x 4". The display, which uses LED backlighting, also is sunlight readable and night vision goggle compatible.

The CMA-4000's basic configuration consists of one processor card with PMC, a graphics carrier card (with an optional graphic PMC), one I/O assembly, and two spare CompactPCI card slots. With the optional graphics PMC, the system can accommodate two video composite/S-video inputs and offers two RGB video outputs to drive multifunction displays. The CMA-4000's graphics engine rotates and scales video and superimposes graphics for display on MFDs in landscape or portrait mode.

**Esterline CMC Electronics | [www.cmcelectronics.ca](http://www.cmcelectronics.ca) | [www.mil-embedded.com/p371476](http://www.mil-embedded.com/p371476)**

## Military systems controlled by game-style unit

Engineers at Ultra Measurement Systems, Inc., in Wallingford, CT, have designed a rugged controller with a game-style form factor familiar to today's warfighters. The patented handheld Freedom of Movement Control Unit (FMCU) has been used by the Army and Marine Corps, Ground Based Operational Surveillance System (GBOSS), and in the Fire Scout unmanned helicopter system. Because of the controller's intuitive nature, warfighters can easily figure out what each switch or joystick does and be off and running. It was the first fully ruggedized game-style controller for military applications.

The controller – available in desert sand and black colors – now comes with a ruggedized, sunlight-readable Light Emitting Diode (LED) backlit Liquid Crystal Display (LCD) that is a modular design with a standard 5" screen with options for 6.4" and touch-screen displays. Non-line-of-sight operation also is supported. The device has sealed, ruggedized, mappable controls, two Hall effect mini joysticks, two single-detent triggers, a four-way switch, 10 momentary push buttons; two optional dead man switches are available. Custom switch modules may also be developed for mission-specific applications. It has a mounting bracket for fixed-position operation. The switch configuration may also be completely customized.

**Ultra Measurement Systems, Inc. | [www.ultra-msi.com](http://www.ultra-msi.com) | [www.mil-embedded.com/p371477](http://www.mil-embedded.com/p371477)**



## Secure data transfer for military flight applications

Engineers at Physical Optics Corp. (POC) in Torrance, CA, developed an in-flight data loading device/digital recorder, dubbed the Data Transfer System (DTS) with secure cryptographic features. It is an NSA-defined Suite B and FIPS 140-2-approved cryptographic solution that also supports NSA-approved Type 1 encryption if needed. Its main functions include uploading mission and map data, recording in-flight mission data, and recording maintenance data during flight and ground operation.

The DTS has four GbE ports that can operate at 500 Mbps per channel. It also uses three independent Removable Memory Units for data storage with a capacity of 128 GB each – which can expand to 512 GB. The RMUs function as the transportable storage medium for pre- and post-mission information exchanges between the mission planning system, maintenance ground station, and the airborne platform. They can be inserted to any slot and the data routing to the appropriate channel can be configured via software. The system includes zeroization functionality for all RMUs and internal nonvolatile memory. It supports the Built-in-Test (BIT) capability to isolate/detect about 95 percent of internal failures through PBIT, SBIT, IBIT, and MBIT functions. The DTS runs on 28 V and uses less than 40 W of power.

**Physical Optics Corp. (POC) | [www.poc.com](http://www.poc.com) | [www.mil-embedded.com/p371478](http://www.mil-embedded.com/p371478)**





## MEMS-based navigation device for unmanned systems

The AHRS-8 navigation sensor from Sparton Corp. in De Leon Springs, FL, is small enough to fit into Unmanned Aerial Vehicle (UAV) payloads and to provide stability and navigation capability in environments with high levels of electromagnetic noise. It offers 3D magnetic field measurement and 360 degree tilt-compensated heading, pitch, and roll information. The Micro Electro-Mechanical Systems (MEMS)-based attitude heading reference system provides in-sensor programmability via the NorthTek Development System, and integrates electromagnetic disturbance compensation for in-platform and transient disturbances.

The AHRS-8 uses AdaptNav II, which has adaptive algorithms to enable real-time optimization of navigation sensor performance in a variety of electromagnetic and dynamic operating environments. It has three-axis magnetic, three-axis acceleration, and three-axis gyro sensor technology. The device, which measures 1.66" by 1.11" by .43", has an operating range of -40 °C to +70 °C. It also has a user-selectable gyro and accelerometer dynamic range, power management capability via a sleep mode, and True North heading output via its built-in World Magnetic Model. It is pin-for-pin compatible with the Sparton DC-4 and GEDC-6 navigation devices.

Sparton Corp. | [www.spartonnavex.com](http://www.spartonnavex.com) | [www.mil-embedded.com/p371479](http://www.mil-embedded.com/p371479)

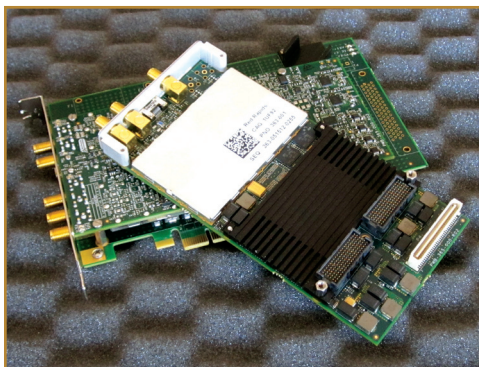
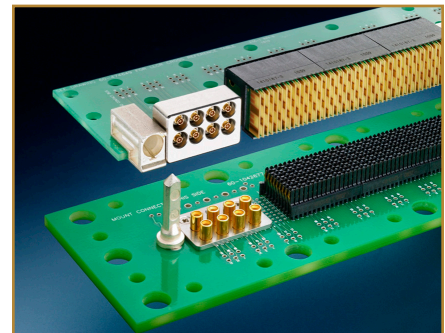
## RF connectors and VITA 67

New RF connector modules from TE Connectivity in Harrisburg, PA, are designed for rugged embedded computing applications that leverage the OpenVPX architecture. The Multiposition RF connector modules were developed to meet VITA 67.0, 67.1, and 67.2 standards that define the RF connector modules for implementation within OpenVPX. The TE modules offer a standardized microwave interface and also meet the requirements of C4ISR applications such as communication systems and ground base stations, avionics, ground-based radar systems, and other applications.

The devices work in high-reliability, high-density military applications that meet VITA 47's environmental, vibration, and corrosion resistance requirements.

VITA 67 standards enable the addition of RF capabilities in VITA 46 (VPX) board-to-board connections. The RF connector modules also are compatible with the VITA 65 (OpenVPX) specification, which defines standard profiles for various configurations at the backplane, chassis, module, and slot levels. RF modules are available with standard four positions (VITA 67.1) or eight positions (VITA 67.2) of high-frequency coaxial contacts for blind-mate daughtercard-to-backplane applications. The SMPM-based contacts are on a 0.240" centerline, and the module interface is designed to maintain excellent channel-to-channel isolation, over 100 dB at 30 GHz.

TE Connectivity | [www.te.com](http://www.te.com) | [www.mil-embedded.com/p371480](http://www.mil-embedded.com/p371480)



## Signal acquisition cards for SDR, radar pulse applications

Designers at Red Rapids in Richardson, TX, developed a product family called Signal Stream for general-purpose signal acquisition and generation for military applications such as Software-Defined Radio (SDR) and radar pulse receivers/transmitters as well as applications in the medical and industrial markets. Available in PCIe or XMC form factors, the devices integrate a set of software programmable features including selectable operating modes – continuous, snapshot, and periodic – time-stamped data samples, external or timed event triggers, data packing, and data sizing.

Signal Stream devices, which come in seven different models, configure their data path as a receiver for ADC channels and a transmitter for DAC channels.

Each type of channel may process raw sample data or data packets as defined by the VITA 49 specification. Each channel also can continuously stream data samples from the ADC to host memory, or from host memory to the DAC. Signal acquisition or generation may be started by software command, software trigger, external hardware trigger, or by a preset time of day. These same options are available to stop a collection or transmission. Its API has drivers for Windows, Linux, and VxWorks operating systems.

Red Rapids | [www.redrapids.com](http://www.redrapids.com) | [www.mil-embedded.com/p371481](http://www.mil-embedded.com/p371481)

# 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:

AdvancedTCA

Android

Avionics Certification

Automotive

Deep Packet Inspection

GUI Linux in Medical Devices

Internet of Things

M2M

Multicore

PCI Express

Radar

SDR

Static Analysis

Switched Fabrics

Test & Measurement

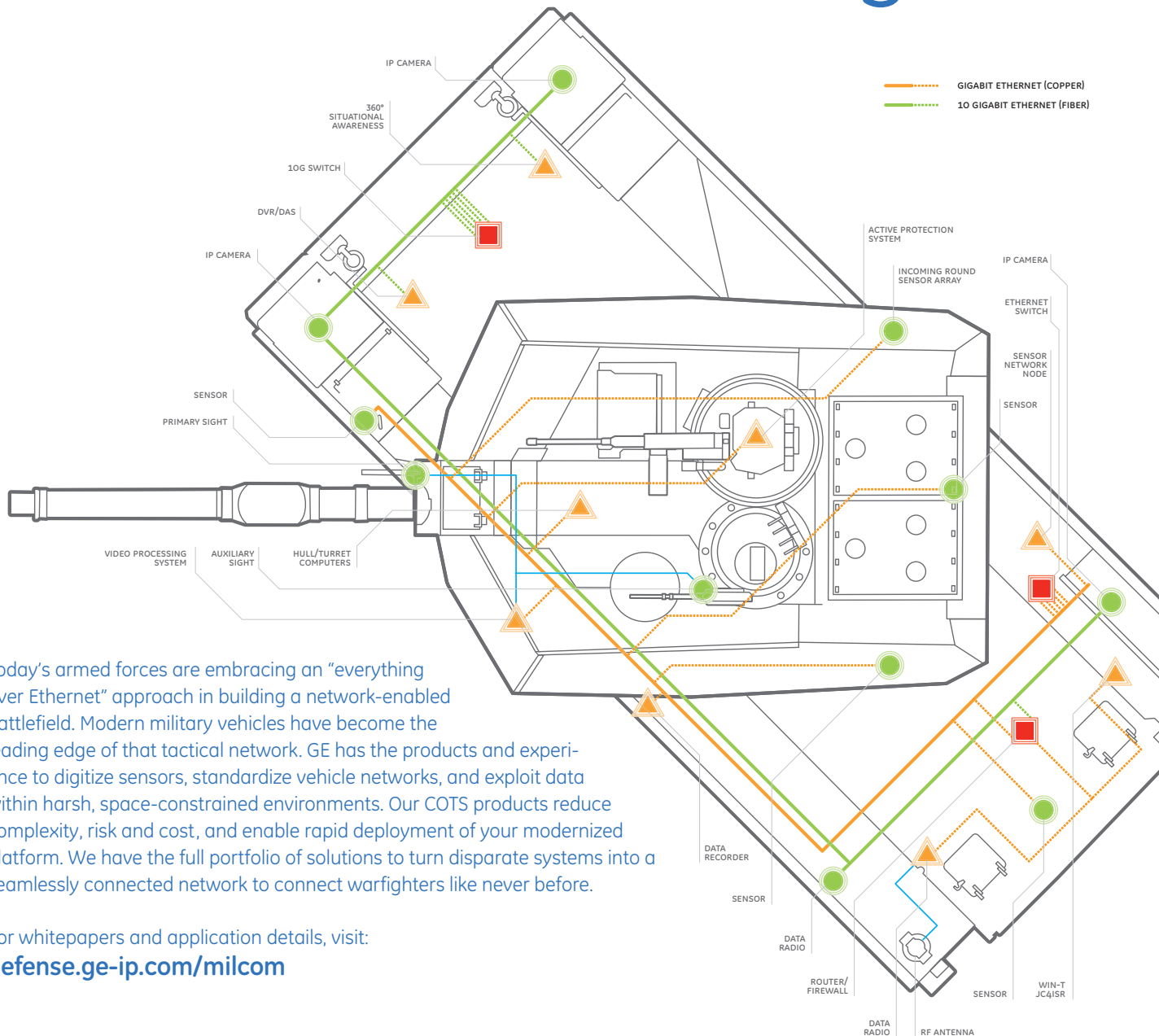
UAVs



OpenSystems media®



# Enabling and securing the connected warfighter



Today's armed forces are embracing an "everything over Ethernet" approach in building a network-enabled battlefield. Modern military vehicles have become the leading edge of that tactical network. GE has the products and experience to digitize sensors, standardize vehicle networks, and exploit data within harsh, space-constrained environments. Our COTS products reduce complexity, risk and cost, and enable rapid deployment of your modernized platform. We have the full portfolio of solutions to turn disparate systems into a seamlessly connected network to connect warfighters like never before.

For whitepapers and application details, visit:  
[defense.ge-ip.com/milcom](http://defense.ge-ip.com/milcom)



imagination at work

# Got Tough Software Radio Design Challenges?



## Unleash The New Virtex-7 Onyx Boards!

Pentek's Virtex-7 Onyx™ boards deliver unprecedented levels of performance in wideband communications, SIGINT, radar and beamforming. These high-speed, multichannel modules include:

- A/D sampling rates from 10 MHz to 3.6 GHz
- D/A sampling rates up to 1.25 GHz
- Multi-bandwidth DUCs & DDCs
- Gen3 PCIe with peak speeds to 8 GB/sec
- 4 GB SDRAM for capture & delay
- Intelligent chaining DMA engines
- Multichannel, multiboard synchronization
- ReadyFlow® Board Support Libraries
- GateFlow® FPGA Design Kit & Installed IP
- OpenVPX, XMC, PCIe, cPCI, rugged, conduction cooled
- Complete documentation & lifetime support

With more than twice the resources of previous Virtex generations plus advanced power reduction techniques, the Virtex-7 family delivers the industry's most advanced FPGA technology.

Call 201-818-5900 or go to [www.pentek.com/go/mesonyx](http://www.pentek.com/go/mesonyx) for your FREE online *Putting FPGAs to Work in Software Radio Handbook*, technical datasheets and price quotations.



**PENTEK**  
Setting the Standard for Digital Signal Processing

