@military_cots

Military EMBEDDED SYSTEMS

MIL-EMBEDDED.COM

July/August 2015 | Volume 11 | Number 5

RUGGED COMPUTING FOR WEARERS OF CAMOUFLAGE

P 22

P 34

An interview with Gerry Janicki, Senior Director at Meggitt Defense Systems

Mitigating counterfeits in the supply chain

P 18

Great things do come in small packages.

www.acromag.com/ARCX

Customize your own rugged, small form factor embedded computer.

Acromag ARCX

Small Form Factor Embedded Computer

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

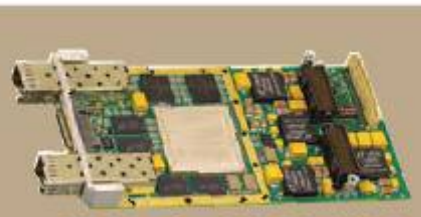
PMC/XMC/Mini PCIe/mSATA slots for specialized I/O, memory, and FPGA modules.

MIL-DTL-38999 connector front panel has options for a custom I/O power filter.

The front panel can be also be modified for customer-specified secondary connectors.

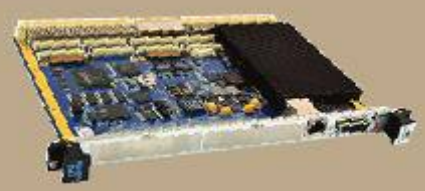
- 4th Gen Intel® Core™ CPU
- Shock and vibration-tested (MIL-STD-810G)
- MIL-STD-38999 high-density connectors
- IP67 sealed against dirt and water
- Customized expansion options
- SWaP-optimized
- Advanced thermal management
- 7-year product life expectancy

Embedded Computing & I/O Solutions



FPGAs for PMC & XMC
acromag.com/fpgas

Industry Pack & PMC Mezzanine I/O
acromag.com/embeddedio



VME & VPX SBC
acromag.com/boards

COM Express Type 6 System
acromag.com/comexpress

MADE IN USA ISO9001 AS9100

www.acromag.com • solutions@acromag.com • 877-295-7084

Acromag® THE LEADER IN INDUSTRIAL I/O

Annapolis Micro Systems

The FPGA Systems Performance Leader

WILDSTAR OpenVPX Ecosystem

FPGA Processing Boards
1 to 3
Altera Stratix V or
Xilinx Virtex 6 or 7
FPGAs per Slot

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

1 to 40 Gbit Ethernet
SDR to FDR Infiniband

Open VPX Storage
Up to 8 TBytes Per Slot
4 - 8 GBytes Per Second

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

Open VPX Switch
1 to 40 Gbit Ethernet
SDR to FDR Infiniband

Chassis
4, 6 or 12 Slot
Up to 14G

Annapolis Micro Systems

High Performance Signal and Data Processing in Scalable COTS FPGA Computing Fabric

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

Volume 11
Number 5

Military EMBEDDED SYSTEMS

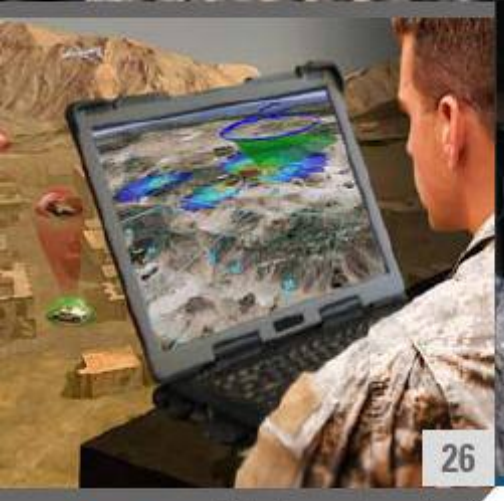
July/August 2015

www.mil-embedded.com


14


18


22


26


30

SPECIAL REPORT

Mitigation of Counterfeit Parts

MIL TECH TRENDS

Rugged Computing

INDUSTRY SPOTLIGHT

Secure Cloud Computing

COLUMNS

DEPARTMENTS

EVENT

MILCOM 2015
October 26-28
Tampa, FL • www.milcom.org

WEB RESOURCES

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

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

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

@military_cots

Published by:
OpenSystems media.

ISSN: Print 1557-3222

ENVIROINK

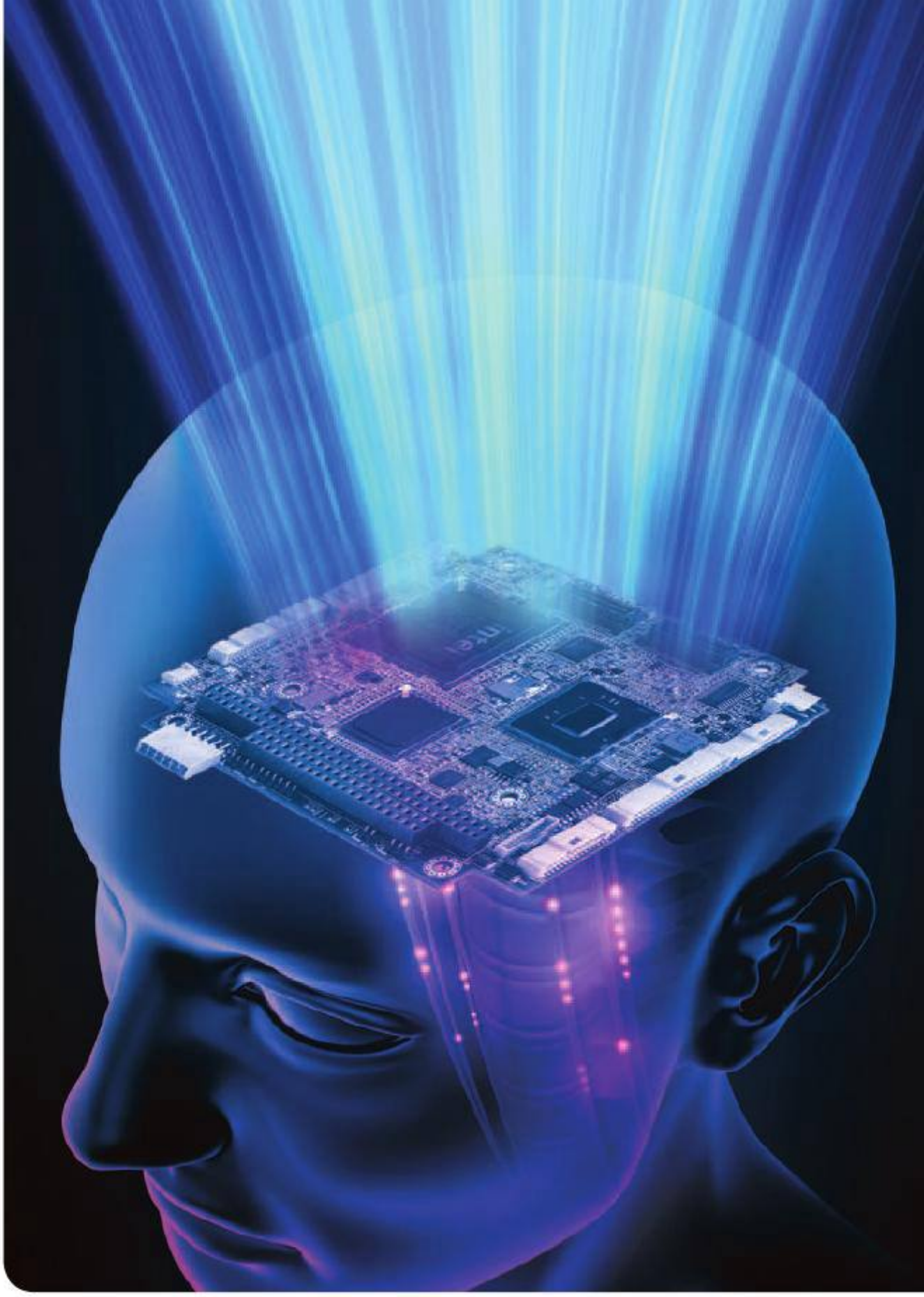
ON THE COVER:
Top image: DRS Technologies' Mounted Family of Computer Systems (MFoCS) provides modular computing capabilities for ground vehicles and weapons platforms across the joint services. (Photo courtesy of DRS Technologies)
Bottom image: Electronics-part counterfeiting is estimated to cost U.S. semiconductor makers around $7.5 billion each year. Working within a trusted supply chain that uses authorized manufacturers is the best way to lessen the risk of counterfeit parts.

EPIC Single Board Computers
Rugged, Stackable Form Factor
Fanless -40° to +85°C Operation

Small Form Factor Computers
Intel® Atom™ E3800 and i.MX6 CPUs
Fanless -40° to +85°C Operation

PC/104 Single Board Computers
Rugged, Stackable Form Factor
I/O Modules and Power Supplies

Single Board Computers
COM Express Solutions
Power Supplies
I/O Modules
Panel PCs



Thinking beyond the board

Sometimes our off the shelf products are not the perfect fit. Our application engineers and in house design talent are ready to develop customized solutions for your system requirements. Our stock products are accessible to use as building blocks for your next project. Calling WinSystems connects you directly with an Application Engineer who is ready to discuss customization options for firmware, operating systems, configurations and complete designs.

Team your engineers with ours to move your product from concept to reality faster.

715 Stadium Drive | Arlington, Texas 76011
Phone: 817-274-7553 | Fax: 817-548-1358
info@winsystems.com

Call 817-274-7553 or visit www.winsystems.com.
Ask about our product evaluation!

Take a peek at our NEW Website!

WinSystems®
The Embedded Systems Authority

Military EMBEDDED SYSTEMS

OpenSystems media.

MES Editorial/Production Staff

John McHale, Group Editorial Director
jmchale@opensystemsmedia.com

Lisa Daigle, Assistant Managing Editor
ldaigle@opensystemsmedia.com

Sally Cole, Senior Editor
scole@opensystemsmedia.com

Mariana Iriarte, Associate Editor
miriarte@opensystemsmedia.com

Steph Sweet, Creative Director
ssweet@opensystemsmedia.com

Konrad Witte, Senior Web Developer
kwitte@opensystemsmedia.com

Sales Group

Tom Varcie, Sales Manager
tvarcie@opensystemsmedia.com
(586) 415-6500

Rebecca Barker, Strategic Account Manager
rbarker@opensystemsmedia.com
(281) 724-8021

Eric Henry, Strategic Account Manager
ehenry@opensystemsmedia.com
(541) 760-5361

Twyla Sulesky, Strategic Account Manager
tsulesky@opensystemsmedia.com
(408) 779-0005

Kathleen Wackowski, Strategic Account Manager
kwackowski@opensystemsmedia.com
(978) 888-7367

Asia-Pacific Sales

Elvi Lee, Account Manager
elvi@aceforum.com.tw

Regional Sales Managers

Barbara Quinlan, Southwest
bquinlan@opensystemsmedia.com
(480) 236-8818

Denis Seger, Southern California
dseger@opensystemsmedia.com
(760) 518-5222

Sydele Starr, Northern California
sstarr@opensystemsmedia.com
(775) 299-4148

Europe Sales

James Rhoades-Brown
james.rhoadesbrown@husonmedia.com

Reprints and PDFs

Wyndell Hamilton, Wright's Media
whamilton@wrightsmedia.com, (281) 419-5725

OpenSystems Media Editorial/Creative Staff

Embedded Computing Design | Military Embedded Systems | Signal Processing Design | Industrial Embedded Systems | PC/104 and small form factors | PICMG Systems & Technology | VITA Technologies

John McHale, Group Editorial Director
Military Embedded Systems
PC/104 and Small Form Factors
PICMG Systems & Technology
VITA Technologies

Lisa Daigle, Assistant Managing Editor
Military Embedded Systems
PC/104 and Small Form Factors

Sally Cole, Senior Editor
Military Embedded Systems

Mariana Iriarte, Associate Editor
Military Embedded Systems
PC/104 and Small Form Factors

Jerry Gipper, Editorial Director
VITA Technologies
jgipper@opensystemsmedia.com

Curt Schwaderer, Editorial Director
Embedded Computing Design
cschwaderer@opensystemsmedia.com

Joe Pavlat, Editorial Director
PICMG Systems & Technology
jpavlat@opensystemsmedia.com

Joy Gilmore, E-cast Manager
jgilmore@opensystemsmedia.com

Rich Nass, Embedded Computing Brand Director
Embedded Computing Design
rnass@opensystemsmedia.com

Monique DeVoe, Managing Editor
Embedded Computing Design, DSP-FPGA.com
mdevoe@opensystemsmedia.com

Brandon Lewis, Assistant Managing Editor
PICMG Systems & Technology
Embedded Computing Design
Industrial Embedded Systems
blewis@opensystemsmedia.com

Jennifer Hesse, Managing Editor
VITA Technologies
jhesse@opensystemsmedia.com

Rory Dear, Technical Contributor
Embedded Computing Design
rdear@opensystemsmedia.com

Konrad Witte
Senior Web Developer

Steph Sweet, Creative Director

David Diomede, Creative Services Director

Joann Toth, Contributing Designer

Chris Rassiccia, Creative Projects

Corporate

www.opensystemsmedia.com

Patrick Hopper, Publisher
phopper@opensystemsmedia.com

Rosemary Kristoff, President
rkristoff@opensystemsmedia.com

John McHale, Executive Vice President
jmchale@opensystemsmedia.com

Rich Nass, Executive Vice President
rnass@opensystemsmedia.com

Wayne Kristoff, CTO

Emily Verhoeks, Financial Assistant

Headquarters – ARIZONA:
16626 E. Avenue of the Fountains, Ste. 201
Fountain Hills, AZ 85268
Tel: (480) 967-5581

MICHIGAN:
30233 Jefferson • St. Clair Shores, MI 48082

Subscriptions

www.opensystemsmedia.com/subscriptions

subscriptions@opensystemsmedia.com

DNA marking of ICs still causing discontent

By John McHale, Editorial Director

The Defense Logistics Agency (DLA) caused quite a stir among authorized integrated circuit (IC) suppliers and original component manufacturers (OCMs) in 2013 when – in an effort to mitigate counterfeits – it essentially required them to mark their Federal Supply Class (FSC) 5962 IC parts with plant deoxyribonucleic acid (DNA) to tag them as authentic. I wrote about the controversy in this space in our December issue with a column titled: "DNA marking for counterfeit parts: problem solver or money pit," that had comments from the DLA and from authorized suppliers affected by the mandate.

Since that time, DLA has stopped requiring the authorized suppliers to mark their parts with the stamp from Applied DNA Sciences in Stony Brook, New York, and are now doing all DNA marking themselves at their facility in Columbus, Ohio. According to Applied DNA Science's website, the facility opened in December of 2014, "with all new orders for microcircuits flowing directly to the DLA lab."

Despite the change, the authorized suppliers are still adamant that the DNA marking is a big waste of taxpayer money that was implemented just so the DLA could save money by going through brokers, which they claim actually increases the risk of counterfeit parts getting into the DLA supply chain. As I wrote then, accusations of wasteful spending in an era of budget cuts are worth a closer look.

"There is no longer any requirement for the OCMs to spend money foolishly to mark parts which are not counterfeit, it has reduced the part cost to DLA significantly, and has also reduced the lead time for the parts, all good things for the warfighter and the taxpayer," Lee Mathiesen, Operations Manager at Lansdale Semiconductor in Phoenix, Arizona, told me. "Currently, it appears that DLA is doing DNA marking internally for all 5962 product they procure, but by removing the product from the individual packaging when it has been procured from the authorized chain, it is not value added. They already know the product is not counterfeit; all they are accomplishing is inducing another handling point, which induces failures."

Essentially, what DLA does is bring "the product in, remove it from its individual device packaging, do some validation testing, and place DNA marks of the product," Mathiesen added. "I believe most manufacturers will not warrant the product with a DNA mark just because the product is no longer in the 'as-shipped' condition – it has been altered."

Dan Deisz, Director of Design and Technology at Rochester Electronics in Newburyport, Massachusetts, has a similar take: "What simultaneously happened was that all the authorized suppliers backed out because they said they wouldn't use the DNA marking and brokers recognized an opportunity to be in a sole-source position where they could increase prices with the DLA. In six quarters after mandating DNA marking, their costs doubled for FSC 5962 product, as they flipped from buying 80 percent of the 5962 products from authorized suppliers to buying 80 percent of the same products from brokers. They are now unwinding that. However, it's a slow switchback due to various purchase agreements and red tape."

It's also backing off what they told me – back in 2013 – was the main reason for using the DNA marking: DLA spokeswoman Michelle McCaskill said then that "DLA believes the costs will decrease over time and be relatively insignificant as greater adoption of the technology and increased competition occurs."

The unwinding of the broker approach seems to show that the increased competition did not mitigate the associated risk. "Some prime contractors and government program managers will not take product from DLA any more because they don't trust the parts they are getting," Deisz says.

During my conversations with the folks at Applied DNA Sciences, they made it clear that their technology does not stop counterfeits, but merely is a traceability tool. However, the authorized suppliers say that it falls short in that regard as well.

"DNA has been touted as a traceability tool and that traceability paperwork is enough, but there is no standard for what traceability paperwork means," Deisz says. "I can show you a traceable part that with unreliable handling can be degraded. Traceability documents do not tell you how something was handled outside of the authorized channel, the only auditable way to procure semiconductors."

"DLA puts the same DNA mark on all products, whether received from the OCM or a Qualified Suppliers List of Distributors (QSLD) broker," Mathiesen says. "They claim they do this so they have traceability to the product. So if the parts all get the same DNA mark no matter where or when it was procured, how does this make the parts traceable? Authenticity does not equal quality or reliability; every manufacturer has authentic product in their scrap bins that do not meet the quality or reliability that they advertise for their products.

"I don't blame Applied DNA Sciences for this," Mathiesen continues. "It is the irresponsible implementation on the part of DLA. DNA marking has been and continues to be a waste of taxpayer money. If you put out an irrational directive, and all of your authorized suppliers say 'no thank you, we choose not to do business with you,' shouldn't you look at your directive and the unintended consequences?"

Sonar processing: Back to basics

By Charlotte Adams

A GE Intelligent Platforms perspective on embedded military electronics trends

Like the rest of the world, the oceans and the vast spaces beneath them are growing more dangerous. International adversaries are projecting power more aggressively with fighting ships and submarines. Smaller, quieter vessels are being employed, and reverberation-rich littoral waters are now key to protecting shorelines. Sonars and sonar processing need to keep up with the threat.

Oddly, however, the reverse may be happening in some cases. Cost pressures as well as knowledge gaps are thought to be driving some countries to adopt simpler, single-sensor sonar systems in lieu of more capable towed or hull-mounted arrays with hundreds or thousands of individual sensors. Single-sensor sonars lack the resolution, beam-steering agility, and target-detection capability of multiple-sensor systems.

Single-sensor systems have a cost advantage over more complex, multiple-channel systems. The processing hardware and software are likewise more affordable, but are they cost-effective? If signal detection is the goal, the simpler, cheaper systems clearly leave something to be desired.

A single-sensor sonar is relatively less capable than its multiple-sensor counterpart of picking a signal out of the noise environment. Real signals are additive, whereas noise is not. That means that the more sensors you have, the better probability there will be of detecting a relevant signal.

Processing systems

If the decision is made to adopt a multiple-sensor solution, the next step is to choose a processing architecture. Submarines boast very limited real estate, so users ideally would want to squeeze as many processing channels as possible into the smallest hardware footprint at the lowest cost per channel.

Users can choose backplane solutions such as VME or VPX, in which data acquisition (DAQ) and data processing cards are housed in the same chassis, interconnected by a bus or fabric topology. Alternatively, users can opt for more distributed systems in which data-acquisition and data-processing functions are more physically distinct, but where front-end acquisition modules offer greater channel density and analog-to-digital (A/D) or digital-to-analog (D/A) throughput. Both architectures are supported by subsystem vendors.

There are merits to both approaches. The first consolidates front- and back-end processing in a single, convenient package, using standardized commercial off-the-shelf (COTS) embedded technologies that are well supported and understood. DAQ cards can be combined with single-board computers with Intel or PowerPC architectures, together with multiprocessor digital signal processing cards equipped with field-programmable gate arrays (FPGAs) and general-purpose processors. Newer cards and chassis can be added as applications grow.

The distributed approach, on the other hand, enables front-end data acquisition, alignment, and digitization tasks to be maximized by dedicated, high-density resources yet to be sectioned off from the processing tasks as a "black box" capability. These front-end DAQ boxes – which can be ganged together and synchronized for greater channel count – can then "serve" digitized data via high-speed networks to inexpensive, general-purpose commercial desktop computers rather than embedded cards.

Unlike bus boards, standalone DAQ elements require no processors, operating systems, drivers, and programming. They are simply network-attached devices that are controlled over Ethernet via TCP/IP or UDP commands. This approach allows easier growth of front-end capability while reducing the buildup of components such as power supplies, integrated circuits, and chassis, associated with multiples of VME or VPX systems.

Figure 1 | GE's daqNet is a complete, integrated, high-channel-count data-acquisition and control-node solution designed to significantly reduce integration effort.

An example of the second approach is the GE Intelligent Platforms daqNet (Figure 1), a 1U-format acoustic front-end system that features 192 analog channels, digital control channels, and redundant Gigabit Ethernet ports, with analog-to-digital sampling/conversion frequencies of 625 kHz/channel at 24-bit resolution (maximum).

Two-way street

Sensor processing is a two-way street, however. If the sonar system is active as well as passive, transmit as well as receive processing chains are required. This reality means implementing D/A channels as embedded cards or dedicated resources.

Whatever the choice of processing architecture, there's an argument for going back to basics. If the objective of a sonar acquisition is to maximize the resolution, agility, speed, reliability, and overall target detection capability of the military platform – and to get the most complete picture possible of the operating environment – a multiple-sensor system is something to be considered.

www.gedefense.com

Rapid Manufacturing with a Polite Disregard for Tradition

Tech-driven injection molding, CNC machining and 3D printing for those who need parts *tomorrow*

Request your free **Digital Manufacturing For Dummies** at **go.protolabs.com/MY5GJ**

ISO 9001:2008 Certified | ITAR Registered
Major Credit Cards Accepted |

Proto Labs uses proprietary software and a massive compute cluster to accelerate manufacturing of prototypes and production parts for every industry.

Got a project? Get 1 to 10,000+ plastic, metal or liquid silicone rubber parts in as fast as 1 day.

proto labs®
Real Parts. Really Fast.™

JLTV: The VICTORY vanguard

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

Later this autumn, the Department of Defense (DoD) decision is expected on which of the three competing designs for the U.S. Army/ U.S. Marine Corps new Joint Light Tactical Vehicle (JLTV) program will go into production. The JLTV program promises to be a significant milestone in the DoD's long-stated efforts to bring commercial off-the-shelf (COTS)-based open architecture interoperability to ground vehicle designs. The new light-wheeled vehicle will serve as the replacement for the High Mobility Multipurpose Wheeled Vehicle (HMMWV), popularly known as the Humvee. The venerable Humvee, manufactured by AM General, has been in service since 1984. Three competing prime contractors – Lockheed Martin, Oshkosh Defense, and AM General – each have a JLTV design under consideration.

The next-generation JLTV is greatly anticipated, not only for the impressive size of the program, but also for the technological innovations that it will bring to the battlefield. On the technology front, JLTV will feature a number of important design enhancements over the Humvee, including improved protection, performance, and payload capability. In addition to these features JLTV also has the distinction of being the first high volume implementation of the in-vehicle networking standards that derived from the U.S. Army's Vehicle Integration for C4ISR/EW [Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance/Electronic Warfare] Interoperability (VICTORY) initiative.

Kicked off in late 2011, the VICTORY initiative was started by PEO C3T (Program Executive Office for Command, Control and Communications-Tactical), and the resulting consortium, a combination of DoD and industry participants, is backed by PEO Ground Combat Systems (PEO GCS) and PEO Combat Support & Combat Service Support (PEO CS&CSS). In the words of the VICTORY program, the initiative "was started as a way to correct the problems created by the 'bolt-on' approach to fielding equipment on U.S. Army vehicles. Implementation of VICTORY enables tactical wheeled vehicles and ground-combat systems to recover lost space while reducing weight and saving power. Additionally, implementation allows platform systems to share information and provide an integrated picture to the crews. Finally, implementation provides an open architecture that will enable platforms to accept future technologies without the need for significant redesign."

VICTORY provides a common ground-vehicle infrastructure that eases the integration of new technologies while improving size, weight, and power (SWaP) by eliminating many redundant components. VICTORY also uses open network interfaces, open data formats, and open protocols to enable the integration and sharing of network, processing and display resources. Thanks to the VICTORY architecture, platforms will be better able to share data. It will simplify testing and training, while reducing overall life-cycle costs for maintaining the platforms. To achieve its goals, the VICTORY architecture encourages the

Figure 1 | The Curtiss-Wright DuraDBH-672 Digital Beachhead GbE switch and vetronics computer system extends the capabilities found in original VICTORY-compliant systems into a smaller form factor.

use of COTS open-system standards. In 2012, Curtiss-Wright Defense Solutions introduced the first COTS system to deliver an integrated VICTORY solution with a rugged subsystem that featured GigE switching and routing, along with VICTORY databus, management and shared services. This "Digital Beachhead" enabled integration of the new VICTORY architecture into any vehicle.

Over the last several years, while the JLTV program went through a 33-month engineering and manufacturing development (EMD) phase, the number and range of VICTORY-compliant subsystems and modules has increased, offering system designers a greater spectrum of choices for functionality sets in SWaP-C (SWaP plus cost) -constrained environments. An example of this new generation of VICTORY subsystems is the recently introduced DuraDBH-672 Digital Beachhead, a rugged COTS Gigabit Ethernet (GbE) switch and vetronics computer system with optionally integrated Rockwell Collins military GPS receiver (Figure 1). It extends many of the capabilities introduced in the original VICTORY-compliant system into a smaller form factor that is optimized for SWaP-C. The unit features 16 ports of fully managed Layer 2 GbE switching and static Layer 3 routing together with a low-power multicore ARM-based Freescale i.MX6 processor that can handle general-purpose processing requirements or optional VICTORY Data Bus Management and Shared Processor Services. It can also support the U.S. Army TARDEC's libVICTORY API to serve as a VICTORY Infrastructure Switch and Shared Processing Unit.

By consolidating what have traditionally been standalone line-replaceable units (LRUs), each dedicated to processing and network switching, into a single multifunction system solution, VICTORY subsystems enable ground-vehicle-system architects to significantly reduce integration SWaP and complexity. With its importance and high profile, the JLTV program should help to accelerate the adoption of COTS VICTORY solutions. At the vanguard of bringing the VICTORY architecture into ground vehicles, JLTV will serve as a model, helping to showcase the benefits of adopting a common network fabric for the C4ISR architecture and consolidating modern computing and networking architectures for SWaP optimization.

Mike Southworth
Product Marketing Manager, Curtiss-Wright Defense Solutions
Curtiss-Wright Defense Solutions • www.cwcdefense.com

DEFENSE TECH WIRE

NEWS | TRENDS | DOD SPENDS | CONTRACTS | TECHNOLOGY UPDATES

By Mariana Iriarte, Associate Editor

NEWS

I-Master radar is integrated into Scorpion jet

Thales and Textron AirLand have announced the integration of Thales' I-Master radar into the Textron AirLand's Scorpion Jet. The addition of the I-Master radar compliments the intelligence, surveillance, and reconnaissance (ISR) sensor suite that includes electro-optical/infrared (EO/IR) capability.

The I-Master radar, combined with an EO/IR camera, adds target tracking along with long-range, wide-area surveillance capability. These two payloads can be simultaneously operated. The Thales radar enables high-fidelity imagery for locating and classifying static and dynamic targets over land and sea. It provides operators with Ground Moving Target Indication, Synthetic Aperture Radar performance, and Maritime Moving Target Indication.

Figure 1 | Textron AirLand's Scorpion flight test with Thales I-Master. Photo courtesy of Textron AirLand.

Industry partnership augments JSTARS Recapitalization program

The U.S. Air Force's JSTARS (Joint Surveillance Target Attack Radar System) Recapitalization program is set to have a low-risk, affordable solution delivered by a team comprised of Raytheon, Bombardier, and Lockheed Martin. The team, led by Lockheed Martin, will provide the JSTARS program – the Air Force's surveillance and targeting aircraft system – with upgraded capabilities and an open system architecture that will enable the government to own the technical baseline for future upgrades and reduce life cycle cost.

Within the team, Lockheed Martin will be the lead systems integrator, while Raytheon brings its ground surveillance; intelligence, surveillance, and reconnaissance (ISR) systems; mission systems integration; and previous JSTARS communications experience to the team. Bombardier will leverage its ultra-long-range business jet platform for JSTARS by enabling onboard radar to see deeper into valleys and survey the battle space for extended periods of time without refueling.

MIDS Joint Tactical Radio Systems contract won by Data Link Solutions

Space and Naval Warfare Systems Command (SPAWAR) officials chose Data Link Solutions (DLS) for the production, development, and sustainment of Multifunctional Information Distribution System Joint Tactical Radio Systems (MIDS JTRS) terminals. The indefinite-delivery/indefinite-quantity contract has a maximum potential of $478.6 million. MIDS JTRS enables the command center to communicate with its forces by voice, video, and data links over a line-of-sight, jam-resistant channel across ground, air, and naval assets. It transforms a MIDS terminal into a four-channel JTRS radio maintaining current Link 16 and Tactical Air Navigation (TACAN) functionality.

The terms of the contract designated $1 million from the 2015 operations and maintenance fiscal year to the first task order concurrent with the contract award, which meets the minimum order requirement.

Data obtained from electromagnetic railgun

At the U.S. Army's Dugway Proving Ground in Utah, General Atomics Electromagnetic Systems (GA-EMS) engineers launched projectiles with onboard electronics from the GA-EMS Blitzer electromagnetic railgun. According to officials, the projectiles performed their intended functions during four consecutive tests. A railgun is a weapon that uses electromagnetic forces rather than explosives or propellant to achieve a high level of kinetic energy for the projectile. For several kilometers following launch, the electronics onboard the projectile measured in-bore accelerations and projectile dynamics, with the data link continuing to operate after the projectiles impacted the desert floor. Projectiles were exposed to the full electromagnetic environment of the railgun launch.

This test marks a milestone for railgun weapon systems, in which flight dynamics data have been measured and downlinked from an aerodynamic projectile fired from a railgun on an open test range, says Nick Bucci, vice president of Missile Defense Systems for the General Atomics GA Electromagnetic Systems Group.

Figure 2 | Projectiles from the Blitzer electromagnetic railgun, test-launched with an approximate acceleration of 30,000 times that of gravity. Photo courtesy of General Atomics.

Ballistic missile defense radar may be used by allies in forward-based mode

The U.S. government has authorized a number of U.S. allies and security partners to potentially procure – via Foreign Military Sales – the AN/TPY-2 ballistic missile defense radar made by Raytheon for use in forward-based mode.

In forward-based mode, the AN/TPY-2 is located near hostile territory and acquires ballistic missiles while they are in the boost (ascent) phase of flight shortly after they are launched. The radar then tracks, discriminates the missile, and passes critical information required by decision makers and missile-defense warfare systems via a command-and-control battle-management network. The terminal-mode AN/TPY-2 ballistic missile defense radar has already been approved for export as the fire control radar of the Terminal High Altitude Area Defense (THAAD) system. AN/TPY-2 is a high resolution, transportable, rapidly deployable X-band radar that can provide long-range acquisition, precision track, and discrimination of all classes of ballistic missiles.

Figure 3 | The AN/TPY-2 is used to guard civilians and infrastructure in the U.S., deployed warfighters, allied nations, and security partners from ballistic-missile threats. Photo courtesy of Raytheon.

WIN-T Increment 2 communications network moved to full rate production for the U.S. Army

The Warfighter Information Network – Tactical (WIN-T) Increment 2, a General Dynamics design system for the U.S. Army, moved to full rate production. WIN-T Increment 2 gives commanders and soldiers the ability to communicate and share intelligence while on patrol. The U.S. Undersecretary of Defense for Acquisition issued an Acquisition Decision Memorandum authorizing the Army to proceed to full-rate production and to field the mobile tactical communications network to the remaining Army units that are projected to receive the WIN-T Increment system, through 2028.

Mine Resistant Ambush Protected (MRAP), High Mobility Multi-purpose Wheeled Vehicles (HMMWV, also known as Humvees), and Stryker armored vehicles have integrated the WIN-T Increment 2 system. To date, four division headquarters and 12 brigade combat teams have the system in place. In Afghanistan, the system served Army units supporting the Security Force Assistance Brigades by replacing fixed communications infrastructure that had been dismantled when the U.S. military closed its operating bases. WIN-T also provided a "communications grid" for humanitarian operations in West Africa last summer during the height of the Ebola epidemic.

Small UAV market to hit $1.61 billion in 2015

Analysts at Visiongain have released a new study that shows the small unmanned aerial vehicle (UAV) market will hit $1.61 billion in 2015 and will continue to grow over the next ten years, despite regulatory hurdles restricting growth in the short term.

The demand for these platforms will vary from country to country and by design type, according to the Visongain analysts, in a report titled "Small Unmanned Aerial Vehicle (UAV) Market Forecast 2015-2025." They say that homeland security and military UAS applications are expected to grow, especially as payloads evolve to enable collection of a wide variety of data such as chemical, biological, radiological, and nuclear (CBRN) threats; facial recognition; and military intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) sensors.

"The small UAV market will register high levels of growth over the next ten years, producing year-on-year growth," says James Bingham, the Visiongain analyst responsible for this study. "The wide variety of applications in which small UAVs can be deployed is growing every day, as this growth platform finds new uses. The demand for small UAVs will be significant, with a wide and varied geographical spread. This growth is forecast to vary country-by-country and by design type. Understanding these dynamics – particularly the variations and intricacies the market produces – will be crucial to those seeking to invest in the small UAV market."

Open-systems architecture flown on NASA Global Hawk unmanned aircraft

A NASA Global Hawk unmanned aircraft flew with a new Open Mission Systems (OMS) architecture, implemented by Northrop Grumman engineers, to enable designers and users to quickly and cost-effectively adapt new capabilities onto un-manned aircraft systems (UASs).

This initial OMS flight, which took place at NASA Armstrong Flight Research Center at Edwards Air Force Base, California, confirmed the ability for ground operators to send OMS payload commands and then receive OMS subsystem status re-sponses via a Ku SATCOM Beyond-Line-Of-Sight (BLOS) communications link between the aircraft and an operations center. A prior OMS Critical Abstraction Layer (CAL) was adapted to an OMS Open Computing Environment (OCE) on the NASA unmanned aircraft using a production RQ-4 Global Hawk air-borne database computer.

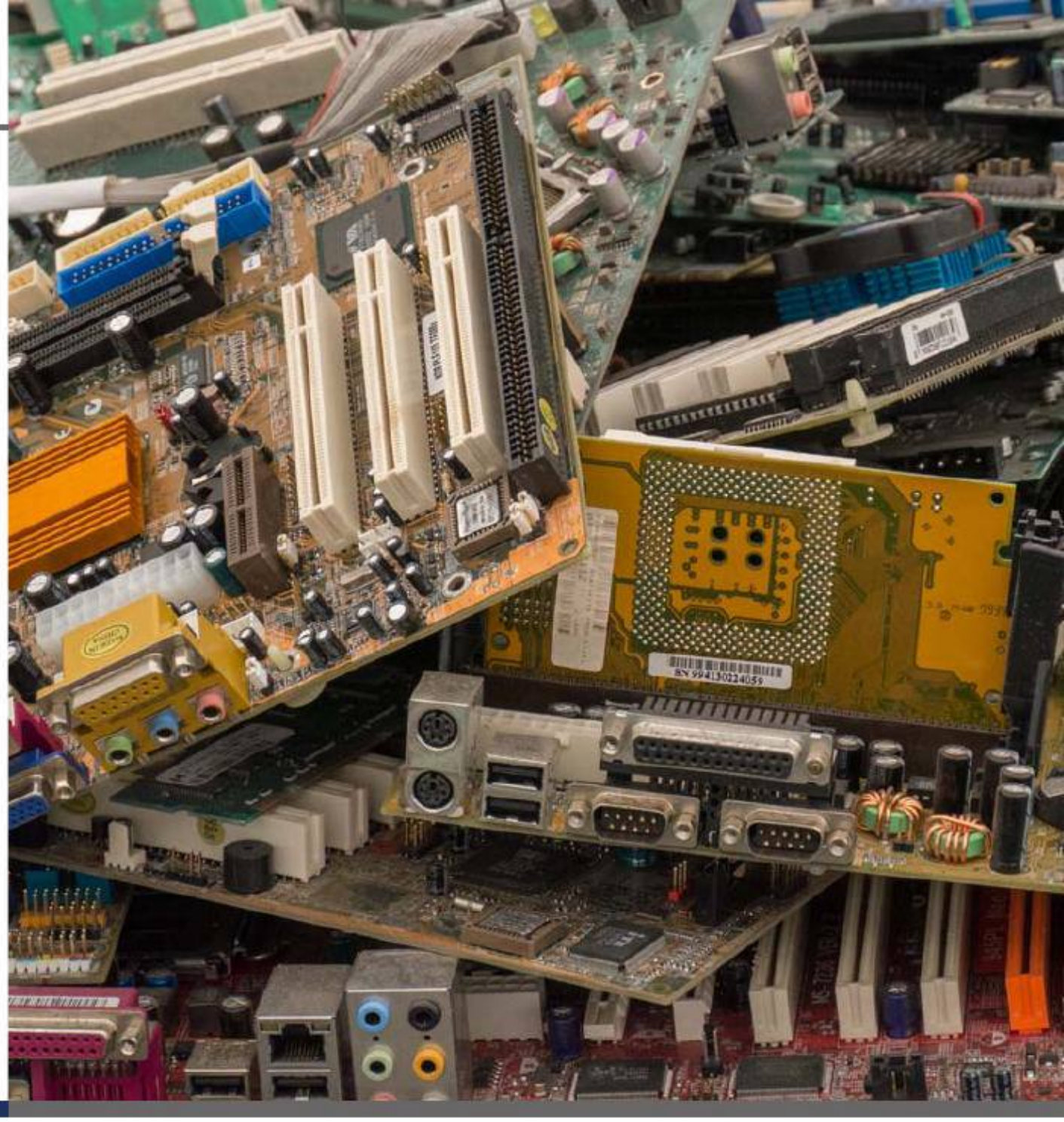
Figure 4 | NASA Global Hawk flies with OMS architecture. Photo courtesy of Northrop Grumman.

MITIGATION OF
COUNTERFEIT PARTS

Counterfeit IC threat evolves with spread of clone parts

By John McHale, Editorial Director

The better government and industry get at detecting counterfeit parts, the better counterfeiters get at fooling detection techniques, especially today with remanufactured or cloned parts adding to the threat. They are an imminent threat as they can permeate military systems, from fighter jets to nuclear submarines, and cause catastrophic failures.



Counterfeit components that find their way into the military supply chain could contaminate jet-fighter avionics, radar systems, and nuclear submarines potentially causing cause loss of life. They look exactly like legitimate integrated circuits (ICs), but have not gone through the rigorous testing and qualification process for use in military systems.

The U.S. government has taken measures against the threat, including passing the National Defense Authorization Act (NDAA) rule on the Detection and Avoidance of Counterfeit Electronic Parts. Millions of dollars are being spent by the military and industry to mitigate this threat, but counterfeits continue to proliferate on the open market and are only a click away on the Internet – all with the potential to affect every area of life that depends on technology.

"Counterfeits threaten every area of the electronics industry, from high-reliability industry applications such as defense and aerospace, medical, automotive, energy and telecom down to the entire commercial sector," says Tom Sharpe, Vice President of SMT Corp. (Sandy Hook, New Jersey; www.smtcorp.com). "[It] is getting much worse as counterfeiters are not only still producing traditional counterfeits – original component manufacturer (OCM) devices which have been modified/altered and misrepresented to appear as new and unused OCM devices – they are now creating ever-increasing amounts of advanced counterfeits or clones," he continues. "In other words, they are creating their own parts which unfortunately, are very similar physically and electrically to the real OCM parts, which makes it easier for them to defeat the inspection process. Clones, essentially, are a growing competitor in the open market to authorized supplier sales."

"The counterfeiters are continuously improving their ability to counterfeit product," says Dan Deisz, Director of Design and Technology at Rochester Electronics (Newburyport, Massachusetts; www.rocelec.com). "No longer is it the case of them banging parts together then washing them over a bucket in a river as portrayed in many media reports. That impression of counterfeiters is still out there, but the reality is that these folks have made real investments and are doing a far better job of not only how they pull parts off of boards and how they re-mark products for what we look for. They are carrying it one step further by cloning product and trying to make money off of their silicon instead of off the OCM's product."

Much like cybercriminals, counterfeiters continuously evolve their techniques to sidestep every new detection method.

"Escalation in detection capability and awareness within the electronics industry over the past several years has predictably inspired the counterfeiters to get better at what they do," Sharpe explains. "SMT first detected highly advanced clone devices back in 2012 and they have continued to proliferate. We had to refocus our labs on understanding what this new component threat looks like and how to reliably detect it. To do so, SMT has invested heavily in additional high-end inspection equipment, training, significant

Figure 1 | Counterfeit parts that make their way into a fighter jet like the F-16 could cause catastrophic failure of the aircraft. (U.S. Air Force photo/Staff Sgt. Nick Wilson)

electrical testing capability, and qualified component engineers."

Defining counterfeits

Lee Mathiesen, Operations Manager at Lansdale Semiconductor (Tempe, Arizona; www.lansdale.com), says that "there are three kinds of counterfeits:

1) The wrong part in the right package refurbished to "look" like the part. These don't work when put in the system, so the only real loss is the procurement cost.
2) Product pulled from electronic waste (Ewaste) that is the correct function, but is refurbished and marked to reflect a different date code, part number, screening level, etc. These are dangerous because they may work at room temperature, at least for a short time. They always fail at the worst possible moment, however, and may cause a loss of the system and mission.
3) Parts that are new, and look and act just like the originals, but they may be tainted to fail or disrupt operation. These include the clones that have been surfacing lately, which raises the question: What organization of counterfeiters can afford to reverse engineer and fabricate these parts? How can they expect to compete with the OCM manufacturer who has amortized the engineering cost over hundreds of thousands of parts? Who is paying for the overhead? A nation-state perhaps?"

Traditional counterfeits still out there

Although industry is vigilant in its search for clones, the old threat of traditional counterfeits still exist and must be guarded against (Figure 2).

"Traditional counterfeits are not going away anytime soon," Sharpe says. "China continues to turn a blind eye to the rights of intellectual property (IP) holders and instead provides a host country to a billion-dollar black-market industry for the creation of counterfeit electronics. They will continue to produce large quantities of crudely refurbished used parts as long as there is a market who continues buying it."

Government response to the threat

Authorized suppliers are adept at policing themselves, but they can only do so much. Only the U.S. government can enforce the laws and prosecute the counterfeiters.

"The government writes new laws, and has been chasing down and prosecuting more traffickers of counterfeits, and has been seeking heavier penalties," Mathiesen says. "We will see just how much the justice system believes that knowingly selling counterfeit parts to the Department of Defense (DoD) is really an act of sabotage on a DoD weapon system. The most recent prosecution is of a man named Peter Picone, who comes up for sentencing next month. The severity of his sentence should tell us a lot about what the judges will do in the future with these saboteurs." *[Editor's note: Picone reportedly acquired ICs from China and then sold them to the military for use on U.S. Navy nuclear submarines, but before they were installed they were discovered.]*

"The DoD and major DoD original equipment manufacturers (OEMs) are much better than others at being vigilant and taking the necessary precautions to combat counterfeits," Deisz says. "The only time it gets squishy is when you go to contract manufacturers (CMs) and they are incentivized to reduce price. You can't be sure of what shortcuts the CMs might take to meet those price goals. DoD OEMs do far better jobs at filtering and limiting choices as far as who they buy from, but unfortunately they still don't look everywhere for authorized solutions.

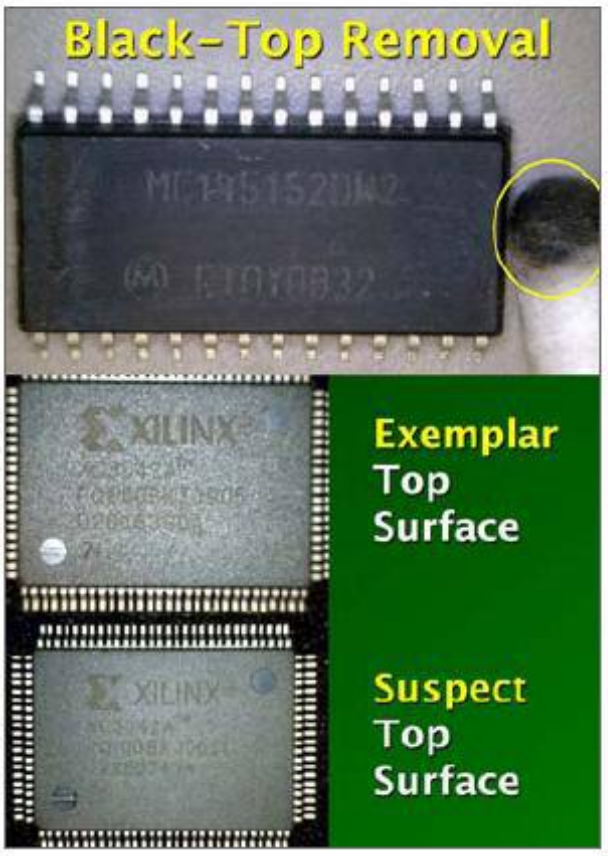


Figure 2 | Pictured are traditional counterfeit ICs. (Photo courtesy of Tom Sharpe.)

"There is still a part within the DoD where there is a wicked back and forth on how to manage obsolescence in the supply chain," Deisz states. The OEMs more or less "design in" obsolescence up front and nothing has changed regardless of product price and how much time they allow up front for design. However, the DoD wants more flexibility in who they buy from and with price as they continue to deal with budget-cut pressures, which creates the risk that counterfeits may find their way into a DoD system.

"We always assume it is the older technology systems where spare parts have become obsolete, but that is not necessarily true," Mathiesen says. "Probably more than 50 percent of the counterfeit product found is parts that are still in production at either the OCM or an authorized aftermarket manufacturer. Counterfeits are not a manufacturing problem, they are a procurement problem. If you don't want to buy counterfeit product, simply don't buy them."

"The Counterfeit Components Avoidance Program (CCAP)-101 program is designed to accept only new and unused components as the OCM shipped them," says Leon Hamiter, Consulting Engineer at Components Technology Institute Inc. in Huntsville, Alabama, which offers the CCAP-101, www.cti-us.com). "We don't even allow re-tinning of the leads. If you do that you have essentially destroyed the part as originally supplied."

Defeating the threat

Defeating the counterfeit threat will rely on new technology for detection, cooperation with the authorities, and an ability to keep the counterfeiters from learning about new detection methods.

"We continue to work with the government on the advanced counterfeit challenge, and share information at the right levels," Sharpe says. "One of the biggest problems with defeating traditional counterfeits has been that each time a new detection method was publicized, the counterfeiters were able to learn what wasn't working and improve upon it seemingly overnight. This public sharing of detection methods needs to end with the highly advanced counterfeits of today – otherwise we will continue to educate the bad guys.

"For example, a new SAE test standard, AS6171, getting released by the end of this year or shortly after, has already been defeated by clones, as it is designed to detect traditional counterfeits," he adds.

Don't tell the enemy

During World War II, the Allies kept the fact they broke Germany's Enigma code a secret at all costs, knowing that if the enemy found out, they could change their codes and the war could go on much longer, costing potentially millions of lives. Many in the semiconductor industry believe that they need to take the same approach with counterfeit detection techniques and stop publicizing their methods, because the counterfeiters are watching and learning.

"The continuously advancing clone threat will not be defeated by published inspection standards but instead through closely-guarded new detection technologies," Sharpe says. "Over the past three years, Battelle Labs in Columbus, Ohio, has done just that by developing the "Battelle Barricade" system specifically to counter the advanced counterfeit threat. I believe this highly-advanced detection system and others like it will become part of standard mitigation processes in the years to come."

Barricade enables "nondestructive authentication of electronic components from both trusted and untrusted sources, enabling separation of cloned or counterfeit components from authentic ones at a dramatically lower cost than alternative methods," according to a Battelle release (www.batelle.com).

The system, which is made up of electronic component signal-acquisition hardware and software, is installed at user sites. The validation process for Barricade consists of placing the IC into a "chip socket in the Barricade hardware to receive confirmation of authenticity or detection of counterfeit or cloned components within seconds," according to the release. The system, applicable to both analog and digital devices, determines authenticity based

on electrical signatures and a classification algorithm that creates identity signatures for each class of chips in a given class of authentic devices. Only a few authentic chips are necessary to enroll an entire class of chips into the system. Battelle officials say that the process can be performed at any point in the supply chain to reduce the risk of counterfeit components as well as to address new regulations that may arise for anticounterfeiting.

Trusted sources and proper testing

So what is the best approach for DoD OEMs and government agencies?

"Using authorized suppliers wherever possible is the best answer to the counterfeit threat," Sharpe says. "Authorized suppliers such as Avnet, Arrow, etc., and aftermarket ones like Rochester Electronics and Lansdale Semiconductor are your best bets to mitigate this growing threat. Clones have made it much more important now than it was five years ago to work with the authorized part of the supply chain wherever possible for components."

"There are two approaches for dealing with counterfeits: prevention or detection when they do not have positive traceability to the OCM," Hamiter says. "For prevention you need the samples to be of consistent production with same lot or date code and no signs of being reclaimed or remarked. Samples are x-ray inspected and decaped to verify consistent internal construction to see if the markings are consistent to the external markings. When the date on a die shows it to be newer than the external date code, assigned by the OCM makes it a clear counterfeit.

"A typical counterfeit analysis practice starts by looking for markings inside the package on the die. This requires a microscope with adequate magnification to see the die markings and if the wire bonds of die harvesting and repackaging," he continues. "There are also tests that can be done to see if the packaging material has the proper ESD characteristics. If it does not then you should assume it has been tampered with and declare it counterfeit as there may be ESD damage."

"Part of the insidious nature of clones is that they work at room temperature but not in extreme hot and cold environments," Deisz says. "If a user doesn't have the methodology to test beyond room temperature, they won't discover it doesn't work till it gets in the field. Brokers don't necessarily have this advantage or capability, yet claim they never see cloned counterfeit technology. How can they know?"

"Buy authorized. Whether it be from the OCM, their authorized distributor, or the authorized aftermarket manufacturer," Mathiesen says. "There is no 100-percent guarantee that any amount of nondestructive testing will catch every type of counterfeit product, and 100-percent destructive testing leaves you with nothing to use in your system. If you procure product from the authorized chain, the odds of obtaining a counterfeit product fall nearly to zero. If you buy product from the broker market, the odds of buying a counterfeit increase dramatically. If you absolutely cannot get the product through the authorized chain, it may be time to redesign the system." **MES**

Mitigating the risk of counterfeit electronics in the supply chain

By Ed Smith

Counterfeit parts are a serious business. The top four most-counterfeited components alone affect $281.5 billion worth of semiconductor markets, and it's estimated that electronics-part counterfeiting costs U.S. semiconductor manufacturers around $7.5 billion per year. The best way to mitigate this risk is to work within a trusted supply chain that depends on authorized manufacturers.

Electronics-part counterfeiting is estimated to cost U.S. semiconductor makers around $7.5 billion each year. Working within a trusted supply chain that uses authorized manufacturers is the best way to lessen the risk of counterfeit parts.

Were counterfeit components to make it into production, they would pose much more than a financial risk: product failure, grounded airplanes, national security, injuries, and even lost lives. U.S. Department of Defense (DoD) officials recognize these dangers and on May 6, 2014, published regulations that require defense contractors and their suppliers to take clear measures to detect and avoid using counterfeit electronics parts. Failing to follow these regulations is costly: Noncompliance can result in $5 million in penalties and losing the ability to do business with DoD in the future.

Many counterfeit components are caught before they enter a production cycle, as detailed in the 2013 Semiconductor Industry Association Report, which lists stories of counterfeit components that were caught prior to being used in manufacturing. These included counterfeit semiconductors intended for use in radiation detectors that emergency responders would use in cases of a nuclear power accident and counterfeit semiconductors intended for use in nuclear submarines. The impact of a product failure in these cases would be devastating.

How to mitigate this risk? First by understanding it, knowing how and where to look for counterfeits, and then by looking for reliable sourcing through authorized distribution.

Where to look for counterfeits?

Traditionally, the defense and aerospace markets have been popular targets for counterfeit semiconductors largely because of the prevalence of discontinued parts. After all, with the acceleration of component lifecycles and the length of defense contracts, defense and aerospace products typically have much longer manufacturing lifecycles than many of their components. With the weight of millions of dollars of production lines on their shoulders, this can leave a manufacturer actively looking for passive, discrete, electromechanical, and other components on the open market if they are not working with an authorized distributor.

Another change in the counterfeit risk is the large (and growing) shift away from using defense-specific components to commercial ones. There was once a large market for defense-specific and custom electronic components, but that is no longer the case as it has become cost-prohibitive to design defense-specific electronics components and integrated circuits in low volumes. Therefore, most defense and aerospace products today mostly contain higher-volume commercial components. The average defense OEM may rely on components from as many as 35 different commercial sources to create a single product. According to research and advisory firm IHS isuppli, these commercial components represent 80 percent of the counterfeits found in the defense supply chain today (Table 1). Using an authorized distributor greatly reduces this risk and simplifies the supply chain.

The detection challenge

One of the biggest challenges in detecting counterfeits is to find the right tests. Often, once a test is in place, a skilled counterfeiter has found a way to work around it.

As more outsourcing has moved offshore, the ease of accessing intellectual property and potential profit from counterfeits have led to sophisticated counterfeiting techniques. It has become virtually impossible to detect a counterfeit component simply by looking at it. Casings are nearly identical to the components that are being copied. Many times, the only way to know the difference is by either opening the parts (and thereby destroying them) or using sophisticated detection technology.

Our industry has adopted some very interesting detection technology to protect integrated circuits (ICs) from counterfeiting, including electronic-fingerprinting technology, electronic signatures, and algorithmic-authenticity detection. These methods are mostly focused on the four types of ICs (analog, memory, microprocessor, and programmable logic) that comprise more than 50 percent of the counterfeit market. The focus on these methods is coming more from component manufacturers who want to protect their revenue.

This makes sense: After all, if you are at the bank and someone tries to deposit a $50 or $100 bill, the teller is likely to bring out a light pen and check its authenticity. But who checks a $1 or a $5 bill? The cost of accepting a counterfeit $1 bill is not very high, in the end.

Rank	Commodity Type	% of Reported Incidents
1	Analog IC	25.2%
2	Microprocessor IC	13.4%
3	Memory IC	13.1%
4	Programmable Logic IC	8.3%
5	Transistor	7.6%

Source: IHS Parts Management 2012

Table 1 | Just four types of integrated circuits accounted for more than 50 percent of counterfeit semiconductors in 2011, according to a 2012 IHS report.

However, this risk analogy doesn't carry over to electronic components. While high-end ICs represent the bulk of counterfeit components, 42 percent of counterfeit electronic components are lower-value components, according to IHS isuppli. It is not unlikely that these low-dollar parts would enter the supply chain. While the dollar impact of a counterfeit $500 IC may be greater than that of a $5 component, the actual cost of product failure is the same. As a result, vigilance against counterfeiting must be the same, and detection testing alone is not going to be enough. In this case, authorized distribution is required.

Mitigating risk by using authorized distributors

The 2014 DoD regulations on counterfeit semiconductors require defense contractors to mitigate the risk of counterfeits – the only way to do this is to focus on plugging the leaks in the supply chain. The best way to ensure a clean supply chain is to source only from original component manufacturers or their authorized distributors and resellers. According to a 2012 report by the Senate Armed Services Committee, an "overwhelming majority" of the more than one million counterfeit parts identified in an investigation of the DoD's supply chain were sourced from the open market. In addition, an audit of the U.S. Missile Defense Agency's independent distribution sources determined that 60 percent of the suppliers were a "moderate to high risk for providing counterfeit parts."

WHILE THE DOLLAR IMPACT OF A COUNTERFEIT $500 IC MAY BE GREATER THAN THAT OF A $5 COMPONENT, THE ACTUAL COST OF PRODUCT FAILURE IS THE SAME.

That is not to say that every open-market source deals in counterfeit product. Many independent distributors have legitimate businesses serving the components' aftermarket. However, there are also those companies that intentionally engage in the manufacture and sale of counterfeit, remarked, and substandard parts; unfortunately, these bad apples can spoil the whole bunch.

Buyers must keep in mind that gray-market products typically change hands and regions many times before they land in a broker's stock. With each transaction and

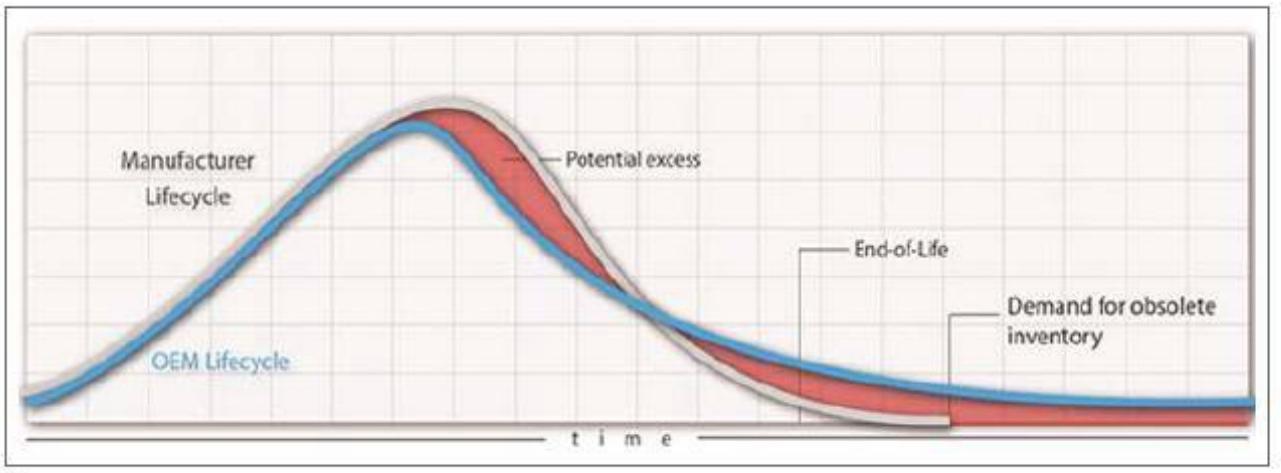


Figure 1 | The danger that sourced components may be counterfeit comes at the height of use and again during the "end-of-life" downswing. Graph courtesy of Avnet.

every shipment, the opportunity for the parts to be tampered with, repackaged, or relabeled is high. Without a verifiable paper trail, the ultimate seller generally cannot guarantee the authenticity or quality of the product. In contrast, an authorized distributor can provide buyers with certificates of compliance and origin.

Planning for obsolescence

For OEMs with long-field-life products, the best approach is to plan for obsolescence. OEMs should work closely with their authorized distributor partners to proactively manage their bill of materials. Avnet, for example, offers tools such as the BOM Optimizer that enables users to identify parts with potential obsolescence issues, prioritize those that could cause the greatest disruption, and develop cost-effective solutions. Designers should also pay attention to the market analysts whose sole purpose is to follow market and technology trends and communicate regularly with component manufacturers about component transitions.

When a supplier issues an end-of-life notice, an authorized distributor should offer customers a range of options, including lifetime buys, to assure ongoing supply. The distributor should also be able to recommend certified, reliable, and reputable aftermarket manufacturers who are authorized by the original component manufacturers to produce legacy components using original wafers and die (Figure 1).

Even with all of these measures, there is only one thing that will truly stop counterfeit components from infiltrating the electronics supply chain: buyer behavior. Defense OEMs cannot afford to engage in risky sourcing behaviors. They can lose their customers, have to pay substantial fines, and endanger lives.

Buyers need to remember that they don't just need parts: They need quality, reliable, factory-original parts, certified by an authorized distributor. There is a critical difference. **MES**

__Ed Smith__ was promoted to president of Avnet Electronics Marketing Americas in February 2009. Smith began his career at industrial distribution company W.W. Grainger. He then spent eight years at Avnet, where he held various sales and operational positions, including district manager in Los Angeles and Phoenix and director of sales for Avnet's Industrial Marketing Group. He left Avnet for the opportunity to serve as president and chief executive officer of SMTEK International, an electronics manufacturing services provider, and served on its board of directors. Smith subsequently returned to Avnet in 2004 to accept the post of senior vice president of sales for Avnet Electronics Marketing Americas. Readers may reach him at EdSmith-Comments@Avnet.com and may follow Avnet's Twitter feed at @avnetdesignwire.

Avnet • www.avnet.com

Rugged computing for wearers of camouflage

By Sally Cole, Senior Editor

Makers of rugged computing systems are working to deliver the best of all worlds: rugged-designed military products that enable mission-critical reliance and reliability, while balancing it with the best technology, at a low cost with commercial off-the-shelf (COTS) components, and in the shortest possible timelag behind the commercial market.

DRS Technologies' Mounted Family of Computer Systems (MFoCS) provides modular computing capabilities for ground vehicles and weapons platforms across the joint services. (Photo courtesy of DRS Technologies)

There's some confusion within the marketplace about what exactly the term "rugged computing" means because there's a lot of "rugged-washing" of products going on. The definition of rugged means something much different to wearers of camouflage than it does to the rest of the world.

In the case of most of DRS Technologies' (Fort Lauderdale, Florida; www.drs.com) systems, for example, there's a mission-critical capability to rugged computing. "In other words: it can't fail. It must be as reliable as the tanks, the weapons, and the radios soldiers rely on," explains Bill Guyan, vice president of business development for DRS Technologies. "It's grown into a mission-critical aspect of how we fight. We fight in a networked way and rely on our soldiers' ability to know where other soldiers are and their ability to track blue dots and red dots … and to fight that way."

Soldiers depend on rugged computers to work wherever they are and whatever the conditions may be – whether it's -40 °F or in intense desert heat, raining, snowing, and even if it suffers a hard drop and impact.

Keeping up with commercial technology

There's a persistent need for the military to try to stay closely linked to the commercial technology roadmap so soldiers always have the latest and most rugged gear in the field and don't get left behind. "This is challenging because commercial technology changes rapidly, and the need to keep up and spin military versions of these products shortly after the commercial versions first appear is a real trick," Guyan says.

To accomplish this, DRS Technologies leverages long-standing relationships with suppliers of key commercial components; for example, suppliers of processor boards, hard drive suppliers, or touch-screen LCDs. "By understanding their technology roadmaps and partnering with them, we're able to shadow their development and launch of next-generation products so that our military version comes out not long afterward," Guyan adds. "These, by the way, use many of the same common components to provide cost benefits that come with the volumes of the commercial market."

In a perfect world, commercial products would go straight to the battlefield. "But, given the mission-critical nature of the role they fill, we can't risk temperature extremes, water, mud, a dropped system, or electromagnetic interference hindering or compromising a mission," Guyan says.

COTS components: pros and cons

As commercial-off-the-shelf components are increasingly tapped for rugged computing systems, their pros and cons should be carefully considered.

"To be cost-effective today, you need to use COTS components, but the question is: How do you use them? Many in this business sell 'rugged' solutions by putting commercial boards into a box that's waterproof," Guyan says.

DRS Technologies designs products by first gaining a solid understanding of its customers' requirements, then looks to the market to find the best technology and price point, while also considering the performance levels available for the components. Then they design from the component level up through the electronics, housings, connectors, and displays to ensure that as a system-level design it's reliable, despite relying on commercial components. "We use an Intel processor in our computers, for example, and have a long history of delivering systems that work forever," Guyan notes.

Rugged design isn't so much about the processor as how the heat coming out of it is handled. What kind of a board do you put the processor on? What kind of isolation do you use in the boards and processor? How do you seal the unit? These are just a handful of aspects involved in rugged system design.

"You just can't take off-the-shelf components and stick them into a waterproof box and call it 'rugged' without running into reliability problems," Guyan says. "Our products may not typically be the least expensive, but they're reliable and the most widely fielded by militaries around the world because of it."

In 2013, DRS Technologies was awarded a three-year contract worth $455 million for a modular family of computers and display systems that will form the heart of next-generation network computing technology for the U.S. Army.

COTS and rugged wearable systems

Black Diamond Advanced Technology (Chandler, Arizona; www.bdatech.com), a maker of rugged wearable products whose primary application is within the joint fires realm for systems fielded alongside Joint Terminal Attack Controllers (JTAC), developed its newest product – the APEx Predator – to take advantage of COTS technology (Figure 1).

It's similar in capability to Black Diamond Advanced Technology's earlier Modular Tactical System (MTS), which has an integrated processor. "The APEx Predator makes use of the processor in the smartphone, tablet, or laptop, or whatever computing device you want to use," says Michael Stimpson, vice president of Black Diamond Advanced Technology. "And it maintains the power-management features of the MTS and the peripheral data and I/O distribution."

The APEx Predator was designed for a variety of end-user mission sets; its power requirements and computing capabilities are extremely scalable. This design enables the APEx Predator to be useful beyond C41 and JTAC missions, which makes it more appealing to assaulters.

Black Diamond Advanced Technology's customers are "used to smartphones, which are intuitive, easy to use, and seem to do everything they could want," Stimpson adds. "One aspect often forgotten is that a large network is required to

Figure 1 | Black Diamond Advanced Technology's APEx Predator system uses the processor in the smartphone, tablet, laptop, or any computing device the soldier is using.

support these smartphones. Nonetheless, customers like these commercial devices and form factor and want to be able to use it in the battlefield. This trend has been going on in the battlefield for a couple of years now, and military technology has finally reached the point where those devices can be used."

COTS reliability is, however, a concern in the field. "The drawback with COTS devices is that they aren't designed around the needs of the warfighter and are often not as robust as MIL-SPEC hardware," points out Verne Patterson, who supports business development for Black Diamond Advanced Technology. "Our design approach allows the user to achieve high reliability and the capability they require for missions that can take advantage of slightly less rugged commercial tablets or phones."

The company's in-house-built MTS has been around for a few years and, while people "usually want the new, smaller 'hotness,' it's been a 50-50 split choosing between MTS and the newer APEx Predator," Patterson says. "Both MTS and APEx have their strengths and weaknesses and are designed to become tools in a toolbox used and configured for each mission set."

The U.S. Air Force Battlefield Airmen Special Projects Office recently awarded Black Diamond Advanced Technology a $48.1 million five-year contract and placed an initial order for 22 APEx Predator systems.

Beating the heat

Heat is a tough design challenge the industry has been grappling with for more than 30 years. One of the biggest rugged-electronics design goals is to be passively cooled while maintaining a tolerant skin-temperature level, according to Black Diamond Advanced Technology's Patterson. "It all comes down to knowing how much can be stuffed into a particular size box. Developers need to be able to achieve that goal without increasing power requirements," he adds.

Although components do not tend to generate as much heat as in the past, it's "still a design challenge to make a box operate properly in the hot desert when you have a fully sealed processor without a fan to assist with cooling," DRS Technologies' Guyan points out. The heat that components generate is linked to the power they use, so generating less heat means batteries are typically lasting longer in systems.

This applies to tablets as well: For its line of Toughbooks and Toughpads, Panasonic Systems Communication Co. (Newark, New Jersey; business.panasonic.com) "combines heat piping with a sealed-fan method to keep the system cool and running longer," says James Poole, director of Department of Defense (DoD) sales for Panasonic Systems Communications. The fan is sealed to prevent dust or moisture from penetrating the device and causing a failure. Moreover, a magnesium alloy is also used to help disperse heat to prevent hotspots.

As part of its efforts to deal with heat, DRS Technologies uses LED backlights in displays now because "they're more reliable and don't generate heat like the old-style tubes," explains Guyan. "But in the past, heat generated by backlights on the display helped keep the system warm in cold-weather environments. We've had instances of designing products with new components and found that they don't keep enough heat inside the box to operate in colder climates. So the design challenge is sometimes inverted, and we've had to find ways to keep heat in the box to make it operate equally well in Alaska as it might in the deserts of the Middle East."

Grappling with power problems

The industry continues to wrestle with power problems, partly because it's "changed its complexion," as Guyan puts it. "Sometimes we want to keep heat in the box because it warms components; sometimes we want to let it out so the system can continue to operate without throttling down its processor power or eventually shutting itself off," Guyan elaborates. "It's a tough challenge and not one that most people know how to do well. Few with any COTS products deal with that challenge at all."

Black Diamond Advanced Technology views power-management capabilities as a key aspect of its wearable systems and factors it into designs. "Every ounce counts and carrying multiple batteries for computers, radios, GPS, and other components within the kit becomes extremely burdensome, Stimpson says.

"In response to this challenge, we distribute power from a single external battery to all connected peripherals on our MTS and APEx systems. Our Radio Power Wedge, which weighs only 3 ounces, powers handheld radios and VDL receivers," he continues. "It attaches where the battery would usually go and acts as a battery eliminator by drawing power from the main system battery. If desired, the radio battery can be attached to the bottom of the Wedge for trickle charging." (Figure 2.)

Future of tablet computing on the battlefield

As tablets become more desirable on the battlefield, one key design trend is a push toward smaller form factors.

Panasonic is currently seeing interest within the realm of military tablets "centered on Windows-based systems and operating systems, to carry over security protocols from the desktop-based world," Poole notes. "This coincides with another trend: enhanced security, primarily in the form of encrypted hard drives." (See Figure 3.)

Figure 2 | Black Diamond Advanced Technology's Radio Power Wedge is designed to power handheld radios and VDL receivers.

Figure 3 | Panasonic's Toughpad FZ-G1 is a thin, lightweight, rugged 10-inch Windows tablet with a 4th-gen Intel Core i5 vPro processor and a user-removable battery providing as much as 10 hours of continuous use and optional bridge battery.

With enterprise-grade tablets built for real mobility and military applications, users are demanding devices capable of withstanding six-foot drops and extreme temperatures. "Other key considerations are a removable hard drive in the event of a security issue, and 'hot-swap' replaceable batteries," Poole adds.

In the future, Poole expects tablets to expand in appeal and reach, particularly once more applications are developed, in terms of user interface, touchpoints, drop-down menus, etc. "As these applications are built or migrate over to the tablet world, tablet computing will make gains in popularity, and even lighter, thinner, more rugged systems will evolve … perhaps with detachable keyboards," he predicts. **MES**

Our technology investments protect yours.

Whatever direction you choose, Aitech has the map!

Established platform parallel bus protocols like VMEbus and CompactPCI still have their place in today's and tomorrow's harsh environment, real-time/hard-deadline embedded sub-system applications...especially when these products are upgraded and maintained to keep pace with the newest, fastest processor and memory technologies.

While there are some applications where high speed serial fabrics like VPX are ideal, there are others where VMEbus or CompactPCI still rule the roost.

One company continues to actively invest in maintaining – and **not** obsolescing – their military and space embedded computing products with a proactive 12-year minimum COTS Lifecycle+™ Program.

And one company continues to also invest in delivering the very best of the newest embedded COTS computing platforms with the new, serial fabric protocols.

And one company actively invests in technology insertion at the board level, creating backplane, pin-compatible products with the latest, next generation memory and processor technologies "on-board".

And that same company still delivers their legacy bus products at full speed **and** full capability and full mil temp range (-55 to +85°C) with those latest technologies.

The one company to do all that? Aitech. Check our website to learn more about our technology roadmaps and how they protect your investments.

Aitech

Embedded Computing *without* Compromise

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

30+

VPX in high-performance embedded computing

By Thierry Wastiaux

Taking advantage of the latest technologies deployed in the commercial high-performance embedded computing environments allow designers to build OpenVPX systems that pack the impressive computing power of tens of GFLOPS while meeting the space and weight limits required in the embedded military and aerospace fields.

Concepts developed in the supercomputing field can be extremely useful in the military domain, particularly in high-end signal intelligence (SIGINT), radar, and electronic warfare applications. Photo courtesy of the Department of Defense PEO IEW&S.

In the science field, high-performance massively parallel computing is used in computationally intensive applications such quantum mechanics, weather forecasting, molecular dynamic simulations, aircraft and spacecraft aerodynamics and other physical simulations. The concepts developed in the supercomputing field can be extremely useful in the military domain where it is highly strategic to pack more computing power into smaller sizes. This is particularly true in high-end signal intelligence (SIGINT), radar, electronic warfare (EW), search, and track applications that have very demanding computing requirements. In high-performance embedded computing systems (HPEC), the speed and the flexibility of the interconnect has become a key factor. The VITA 65 OpenVPX standard clearly appears to be the best standard to bring this connectivity while also enabling maximum processing power in small form factor parallel computing architectures.

Bringing the best from the supercomputing world and adapting it to the military and aerospace domain is clearly a challenge.

Processors and FPGAs for HPEC

The choice of the best possible processors and FPGAs to design powerful DSP boards is the first key element on the road to powerful HPEC architectures. These boards have to propose the best ratios in terms of number of operations per second and per watt. The last generations of Intel Core I7 and Xeon DE processors offer an excellent balance between processing power and energy consumption. Moreover FPGAs are known for offering the best ratio of GOPS/W. On integer operations and for parallel computing, they can run ten times faster than a processor which is extremely useful in image processing or signal processing applications. The Xilinx 7 series of Xilinx is one of the best FPGAs for these functions.

In terms of communication capabilities, Intel Core I7 processors feature many native PCI Express (PCIe) links offering tremendous data connectivity. Additionally, Intel Xeon DE processors have integrated 10/40 Gigabit Ethernet ports. Xilinx Virtex-7 FPGAs feature smartly designed transceivers reaching a data rate per lane of as much as 13 Gb/s with an aggregate bidirectional transceiver bandwidth of as high as 2.7 Tb/s. Tightly coupling processors to FPGAs enable the design of very dense and powerful processing boards that are the foundation of HPEC systems.

Small and distributed HPEC systems

Enabling supercomputing in an embedded system depends on the size of the targeted computing system. The interconnect of these systems has to be robust,

fast, flexible and very power efficient. Intel has invested massively in the specification and the implementation of the packet high data rate, point-to-point link PCIe protocol. CRC control at the link layer as well as retransmission hardware mechanisms enable robustness and the permanent investment to increase speed has led to very high throughputs.

The maximum theoretical bandwidth per lane is 7.88 Gb/s in Gen3 thanks to the reduced overhead allowed by the 128B/130B encoding. That is a throughput of 31.5 Gb/s on a PCIex4 link. By putting in parallel, various numbers of lanes, high flexibility can be enabled in the system design. Thanks to hardware implemented low power management features, PCIe is a particularly power efficient standard.

Due to the point-to-point nature of the protocol, the industry has designed

"THE CHOICE OF THE BEST POSSIBLE PROCESSORS AND FPGAS TO DESIGN POWERFUL DSP BOARDS IS THE FIRST KEY ELEMENT ON THE ROAD TO POWERFUL HPEC ARCHITECTURES. THESE BOARDS HAVE TO PROPOSE THE BEST RATIOS IN TERMS OF NUMBER OF OPERATIONS PER SECOND AND PER WATT."

many switch components that have DMA engines for fast data transfers. The switches can be distributed on the different boards in the systems or set in a centralized switch slot, switching both Control Plane and Data Plane. The Cometh4410a VPX 3U switch from Interface Concept is an example of this kind of implementation, but is limited due to the low number of ports it offers. Thus, PCIe appears as a leading candidate to become the defacto standard interconnect for HPEC systems.

In the PCIe architecture, each Intel processor is the root complex in its PCIe domain enumerating all the end points. Enabling parallel processing in HPEC systems means developing software allowing seamless communication between processors.

Interface Concept has developed a software package, called Multiware, that is able to transparently configure the hardware and the DMA engines of the switches and enables DMA transfers, message passing, and synchronization between the nodes of a HPEC system. In radar or EW HPEC systems this approach enables the inclusion of front-end processing FPGA modules that are directly connected to multiple sensors.

Enabling HPEC systems

PCIe is a point-to-point link protocol and when more parallel processing power is required with a high-speed dataplane over 10 GbE, the PCIe protocol becomes more complex to use. Reaching 10 Gb/s therefore cannot be achieved on only one lane in PCIe Gen3 and a PCIe Fat Pipe Gen3 cannot reach 40 Gb/s.

However, the IEEE 802.3 Standard for Ethernet Sections 4 and 6 from 2012 specifies new standards including 10 GBASE-R and 40 GBASE-R with their physical layer implementations for backplane communication based on 64B/66B code, 10 GBASE-KR, and 40 GBASE-KR4. The 64B/66B code of the Physical Coding Sublayer (PCS) enables robust error detection. Its encoding ensures that sufficient transitions are present in the PHY bit stream to make clock recovery possible at the receiver. The Physical Medium Dependent Sublayer (PMD) of 10 GBASE-KR allows transmission on one lane at 10.325 Gb/s, while the PMD sublayer of 40 GBASE-KR4 allows transmission on four lanes at the same rate.

The use of 10 GBASE-R and 40 BASE-KR4 brings back simplicity by enabling centralized switched architectures. The Cometh4510a is an example of a 10/40 GbE switch corresponding to the OpenVPX Switch Profile MOD6-SWH-16U16F-12.4.5-4. Its dataplane uses the last generation of Marvell Prestera CX platforms, while the control plane uses the well proven Ethernet packet processors of the Cometh4340a switch family. It features 16 ports 1000 BASE-KX on the control plane and 16 40 GBASE-KR4 ports or 48 10 GBASE-KR ports on the dataplane, thus offering a huge switching bandwidth.

A multicore PowerPC management processor running the Switchware package

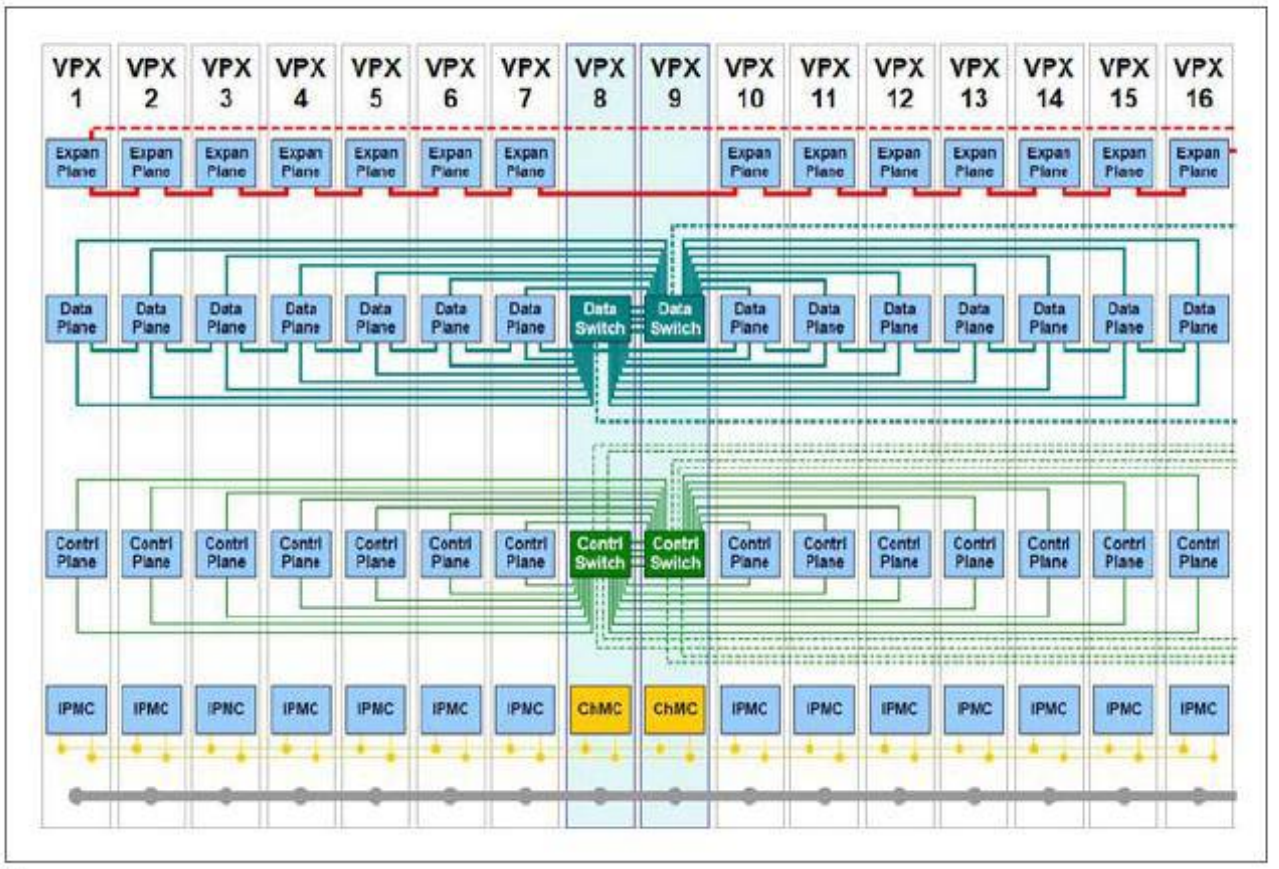


Figure 1 | Example of a 14 payloads architecture with redundancy switching.

offers two out-of-band 1000 BASE-T ports and allows traffic-log recording on NAND flash. In addition, a custom mezzanine can bring either two 10 GBASE-T ports at the front and two 10 GBASE-KX4 ports on P6, or four 10 GBASE-T ports at the front.

The 10/40 GbE switch is the keystone for building HPEC systems, enabling gathering in parallel as many as 48 DSP boards in 10 GbE and up to 16 DSP boards in 40 GbE. An example of possible cluster architecture is seen in Figure 1 with redundancy switching.

Designing HPEC clusters under extended temperature range is a challenge in terms of both heat density and signal integrity. Developing dense multicore DSP boards with communication data rates on differential pairs at more than 10 Gb/s requires the use of the last generation of electromagnetic simulation tools to control the impedance of links through the board and also of specific lab equipment for ensuring signal integrity.

New manufacturing processes insuring impedance control on multilayer PCBs must be well-mastered. Heat management also requires the right simulation tools to ensure efficient heat extraction. **MES**

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

Interface Concept
www.interfaceconcept.com

RUGGED COMPUTING

Application-ready platform choices expand rugged application possibilities

By RJ McLaren

Defense OEMs must find a way to cost-effectively meet mounting data throughput and processing needs with commercial off-the-shelf (COTS) platforms in smaller form factors. Application-ready systems that have been ruggedized for reliability in extreme military settings instill confidence with high availability by effectively addressing the significant power densities generated at the board, chassis, and system levels.

Ruggedized systems are intended for use in extreme military settings: A soldier from the 1st Brigade Combat Team, 101st Airborne Division (Air Assault) trains on a Warfighter Information Network-Tactical (WIN-T) Increment 2 Tactical Communications Node system at Fort Campbell, Kentucky, in March 2014. Photo credit: Claire Heininger, PEO C3T.

A growing number of military applications can benefit from employing capabilities similar to high-performance commercial PCs, which can be seen in data recorder systems that now utilize high-bandwidth 10 gigabit Ethernet (GbE) connectivity, giving military personnel the ability to load/upload and offload data quickly. Yet the task of making these systems rugged enough for military use is not without difficulty, and part of the problem is that high-speed signals such as USB 3.0, 10 GbE, and optical interconnects are not easily ruggedized. Ruggedizing for military environmental conditions, space constraints, and overall signal integrity is much more challenging than commercial connector solutions are built to handle. The equation is made even more complex when you consider that rugged computing that supports reliable signal integrity must also incorporate robust software implementation, smaller form factors, optimized BIOS, and trusted removable storage in sealed enclosures.

To satisfy all these demands, rugged computing must incorporate a multidiscipline approach in order to be effective. While there is no single option that fits all applications, there are a range of trusted COTS-based platforms that have a proven track record in military deployments. Helping further is the notion that most platforms can also act as modular building blocks to streamline development resources and timelines. For example, VME – still a predominant bus architecture – has evolved to the point where it now supports the latest x86 and field-programmable gate array (FPGA) processor architectures. Moreover, embedded computing platforms based on computers-on-module (COMs) are available as prevalidated systems, allowing developers to add integrated video processing and display features; compute performance is readily optimized for graphics-heavy imaging and sensor data processing applications without affecting rugged operation. In addition, prevalidated, microprocessor-based VPX platforms can deliver high-performance parallel processing using mainstream protocol such as PCIe Gen 3 and 10 GbE.

Using a modular platform approach enables developers to maintain compatibility and interoperability for many types of rugged applications ranging from ground vehicle systems and shipborne computing to manned airborne and unmanned aerial vehicle (UAV) payloads.

VME still stands strong

While industry experts have long predicted VME's demise, it's not dead yet and remains a popular bus and board architecture standard. Still highly reliable for mission-critical embedded systems, VME also enjoys a huge installed base of systems, supported by a broad and experienced ecosystem of suppliers. As a result, many legacy military programs will choose to keep VME when upgrading or refreshing established systems. In the current budget-conscious defense environment, it would be rare for a large program to make an architecture change, based on the high cost of replacing existing VME chassis, I/O cards, and software.

Even though continual enhancements to bandwidth, connectors, and I/O options have kept the familiar VME in the running, performance limitations on throughput are coming to light. Because of these issues, defense contractors are always looking for cost-effective solutions to maintain this trusted technology investment. Today, VME-based platforms are innovating by using FPGA technology that enables PCI-to-VME bridging, making VME more immune to silicon obsolescence. Also keeping VME-based systems relevant is suppliers' ability to offer effective processor migration for both PowerPC and x86, along with new integrated health-management capabilities.

VPX is application-ready and high bandwidth

3U Open VPX-based High Performance Embedded Computing (HPEC) platforms, in both air- and conduction-cooled options, capably support military systems operating within harsh environmental conditions. These types of systems are developed to be completely application-ready while supporting server class applications. A small 3U footprint and rugged technologies enable server consolidation that can simplify logistics, installation, and maintenance of complex military systems. Airflow temperature is controlled on each slot, while payload boards can be held in standby mode to meet low-energy surveillance requirements. Server-class silicon means that military field operations can readily utilize data center features such as libraries, middleware, and other technologies that have been optimized for rugged application conditions. Virtualization helps future-proof the VPX platform investment, allowing a single application to be easily adapted to hardware evolution needs such as CPU count, memory, form factor, and I/O availability. These application-ready systems combine dual ports of integrated 10 GbE and integrated I/Os (PCIe, USB, SATA, and other general purpose I/Os) into a single system for maximum efficiency.

It's important to note this platform also offers central health and power-management capabilities. For developers, this adds value in meeting sensor data processing requirements in space-constrained systems.

COMs-based platforms deliver small-footprint, application-ready advantages

The basics of COMs-based design enable modules to be switched out without affecting carrier-board customization; these attributes also ensure long life cycle support for customized military and space systems. The carrier-board design maximizes system capabilities while minimizing overall size so that the resulting system balances performance and footprint for applications that routinely require limited physical space. These same platforms integrate the latest x86 processors so that system performance can also evolve with processor-architecture advancements by swapping out modules. This reality means that

total cost of ownership is managed for long-term value as future upgrades are simplified, while developers avoid costly and time-consuming design requalification.

One such system is the Kontron COBALT, a rugged small-form-factor system based on COMs (Figure 1). COBALT's IP67 chassis operates in harsh conditions including extreme temperatures, shock, vibration, and electromagnetic interference (EMI). Sealed IP67 systems are expressly developed to support highly-rugged applications such as vehicle- or helicopter-based computing. The device's integrated video processing, display, and other features are designed not to affect rugged design considerations. For instance, its onboard Rapid Shutdown circuit design protects systems by enabling survivability from extreme episodes such as high-energy electromagnetic pulse (EMP).

Figure 1 | The Kontron COBALT, which uses a 3rd-generation Intel dual core-based COM Express Type 6 module is targeted at harsh and operationally demanding military and aerospace applications.

Effective thermal management by design

Why are application-ready systems so effective in managing thermal issues? All of the required system functionality is implemented in a chassis that has been pre-certified for ruggedized operation rather than simply listed as "designed to meet." Developers can incorporate a chassis that is manufactured to meet MIL-E-5400 Class 1 thermal performance, MIL-901D shock or MIL-STD-810F vibration requirements, in turn assuring the system's ability to withstand specified these same environmental extremes. Since robust design components are built in, it reduces the need for additional development resources, all housed in a sealed and temperature-controlled enclosure that offers ultimate protection for its internal computing elements and electronics.

A case in point are select small-form-factor COMs-based platforms that provide extended thermal characteristics "by design." These platforms employ a reengineered COM optimized for proven performance in extended temperature applications. They also bring up a common myth in systems packaging: the assumption that radiation plays a marginal role in cooling electronic equipment. While this statement remains true for higher-power systems requiring high levels of power dissipation, defense-system developers must pay closer attention to the effects of radiative cooling in passively cooled convection systems operating within low power requirements. As smaller, lower-power systems carve out and expand

Advantages of flexible I/O in COMs-based systems

Many current computers-on-module (COMs)-based rugged box level platforms are application-ready, contributing to their overall value in defense systems. These scalable building blocks simplify the design process by offering modular solutions that extend performance and feature application possibilities. Offering integrated mezzanine options, these solutions give designers a configurable platform capable of meeting a broad range of I/O and network-communications requirements. The mezzanine approach enables the development of new systems without significant modification to an original base design, thereby protecting and maximizing technology investments. For example, consider the COM Express Type 6 pinout as a foundation, which permits future design alternatives by reallocating legacy PCI pins for digital display interfaces and additional PCI Express lanes. Extra PCI Express lanes can be routed to serial-based mezzanine card slots such as mPCIe and XMC. The resulting expansion slots provide a performance jump compared to earlier pinout configurations. This pinout structure also enables developers to integrate an enhanced fourth-generation graphics architecture, essential in supporting prolific high-definition surveillance and imaging applications.

Putting flexible I/O into an application perspective can be shown in the restrictive quarters of a Navy submarine: This intense computing environment is well-suited for rugged COMs-based computing platforms. Very different from the limited capabilities of submarines depicted in films of the past, today's subs are marvels of technology that use state-of-the-art visualization, imaging, and networking technologies. Rugged small-form-factor COMs platforms that deliver versatile I/O enable data to be shared throughout the sub via wired and wireless networks, prioritizing information effectively to improve situational awareness and enable the best possible decision-making from military leadership. With increasingly more powerful graphics display and processing features, multiple displays of information can be accessed and displayed, for example, for real-time review, longer-term storage, or urgent distribution for immediate action. These same platforms also are able to serve up the performance for intense number-crunching operations and combat applications such as sonar, GPS and navigation, power, targeting, weapons, and more. COMs-based platforms make much of this additional computing power possible, continually bringing mission-critical capabilities to shipboard and other defense systems in very small spaces.

their niche in military electronics, radiation can impose significant restrictions on where they can be deployed. Systems that offer a passive convection alternative can deliver both scalability and excellent power dissipation in a sealed system. By integrating cooling capabilities into the size, weight, and power (SWaP) protocol, packaging engineers then have access to more sophisticated SWaP plus cooling) considerations early in the development process.

Achieving rugged design versatility

While no single rugged computing platform fits every need for modern military and aerospace networking and imaging applications, application-ready systems can provide a head start in a number of design scenarios. Designers can select from multiple "ruggedized" and proven options depending upon requirements, time frame, budgets, time to market, and anticipated future needs. Design success depends on selecting the right platform for the job, one that ensures confidence in mission-critical military operations. VME may be the best fit to meet legacy requirements via new FPGA functionality, whereas VPX offers some of the most rugged performance options in higher bandwidth systems. Moreover, systems that demand more flexible, scalable features can capitalize on the inherent value of COMs to enable a full complement of I/O options, reduce precious SWaP, and trim costs. In addition, many of these platforms also offer the ability to use and re-use prevalidated designs, giving a significant competitive advantage in meeting design requirements while reducing development resources and avoiding additional customization costs.

Reducing design risk and enabling increased design versatility is essential to the evolving, modern battlefield that continues to call for increased computational performance and communication bandwidth improvements. Enabling a small-footprint, low-power, and cost-saving answer for rugged applications, platforms that feature efficient thermal design support additional development flexibility while delivering essential fanless operation in severe environments. Designers looking for sustainable, long-term design that meets specified deployment life cycles will find a number of application-ready embedded computing platforms designed to support extreme rugged reliability, both now and when the need arises for future power or performance advances in the same small footprint. **MES**

RJ McLaren *is the Portfolio Manager for the Avionics, Defense and Transportation business unit at Kontron. He is responsible for product and business development for rugged systems along with Kontron's industry-standard COMe, AMC, CompactPCI, VME, and VPX product lines. He can be contacted at rj.mclaren@us.kontron.com.*

Kontron • www.kontron.com

Cooling electronics in modern military ground and air platforms must balance reliability and cost

By John McHale, Editorial Director

INTERVIEW

In this Q&A with Gerry Janicki, Senior Director at Meggitt Defense Systems in Irvine, California, he discusses design trends in military-electronics thermal management, challenges and requirements in air and ground platforms, and how modular hybrid cooling is solving current thermal challenges while reducing total lifecycle cost.

Please provide a brief description of your responsibility within Meggitt Defense Systems, your group's role within the company, and an example or two of where Meggitt's thermal management systems are used within the military.

JANICKI: I'm responsible for leading the Thermal Management System (TMS) and Environmental Control System (ECS) Programs and Business Development activities for Meggitt Defense Systems, as well as the Business Area Team, which all TMS and ECS Programs report into. I work closely with engineering to develop new products, codirect internal research and development (IRAD) investments, and am also responsible for the development of ECS business and program strategies, market forecasts and assessments, bid and proposal planning and execution, new-program starts, and developing new products and programs.

Meggitt has been developing affordable and reliable global and local thermal-management solutions for military ground and aircraft platforms and systems for over 40 years.

Your expertise is in the thermal management of military electronic systems. What factors are driving thermal-management designs today in these systems?

JANICKI: Thermal management has become a mission-critical function and subsystem in support of key electronics in combat vehicles and higher energy weapons. Good thermal management is benign, while poor thermal mismanagement can ruin your day.

The current and planned exponential growth in military platforms electronics is driving cooling requirements from several kW to several hundred kW. Network-centric warfare is driving the development of higher-functional-density electronics that need to be implemented on both new and legacy platforms.

To balance global and local cooling requirements, these systems need to be simple, modular, and flexible to cost effectively support commercial-off-the-shelf (COTS) electronics on legacy and future military platforms. Optimized solutions such as hybrid refrigerated (active and passive) forced liquid cooling of COTS electronics still represents a high-value solution for future military platforms. Modular hybrid cooling provides the best balance of cooling efficiency, power, reliability, and total system thermal management. The limitation of size, weight, and power (SWaP) has led to the development of these efficient hybrid thermal management systems.

What are the most popular cooling methods for military electronics today and why?

JANICKI: Forced air-cooling and forced (passive) liquid cooling are challenged by tomorrow's environmental and reduced SWaP; that's why more applications are using active (refrigerated) forced liquid cooling.

Fluids have a higher heat capacity than gases and are much more efficient at conduction-based heat transfer in many military operational environments. Thermal-management systems leveraging active liquid cooling, with COTS conduction cards in a rugged liquid flow through enclosure, represent a low-risk evolutionary solution for current and future military platforms

What are the current challenges and requirements you are seeing regarding thermal management in aircraft systems?

JANICKI: Military aircraft requirements focus on flight envelope, SWaP, dynamic loads, operating temperatures, storage temperatures, reliability, maintainability, and cost. Air density is also important, as it changes with altitude, which affects the thermal-management formula and the performance of equipment like fans.

The same for ground systems?

JANICKI: Military ground-vehicle requirements focus on SWaP, shock and vibration loads, operational and storage temperatures, reliability, maintainability, and cost.

Ground vehicles are additionally challenged because they have to have their vapor system on all the time, like an air conditioner running all the time in a car. The electronics need to have their own power sources.

What about naval platforms?

JANICKI: For naval systems, thermal management is not as big an issue, as these platforms have access to large heat sinks called oceans.

What types of thermal-management challenges do high-energy laser weapons present and how far along is the industry toward solving them?

JANICKI: The most challenging application and the majority of applications are driven by upgrades to legacy platforms and the introductions of high-energy weapons such as high-energy lasers and rail guns. There are multiple advanced laser weapon programs trying to field a 100-200 kW weapon. We are supporting some of this and also the electromagnet rail gun being developed for the Navy. Many of these systems still have a way to go to be called a product.

What new types of cooling methods are being explored today that we may see in future military systems?

JANICKI: There are many efficient ways to directly cool electronics, and every few years a recycled technology or technology du jour from a laboratory, university, or company grabs the attention of designers. Some of these include liquid immersion, impingement cooling, direct refrigeration, and nanoparticle liquid conduction cooling, none of which are ready for prime time on military platforms because after you remove the heat from the chip/board/line-replaceable unit, that heat has to go somewhere using a platform subsystem.

Many military ground-platform upgrades have had tough power-management challenges when adding new electronics and capability because the vehicles were designed from the ground up to meet today's SWaP requirements. Do you see next-gen platforms taking this into account or will we face the same power-management problems with the newer platforms?

JANICKI: The greatest constraint in ground-vehicle upgrade programs – such as on the HWMMV (commonly called the Humvee) or Bradley Fighting Vehicle – is power. On next-generation platforms such as the Joint Light Tactical Vehicle (JLTV), the designers are taking that into consideration, using larger generators on the engines from the get-go, while most existing platforms try to force-fit larger generators that are still not enough for current and projected loads. Even with the new systems' additional power, that number has to evolve every two to three years as you add high-performance radars and other processing-intensive equipment and communications electronics. These improvements impact all subsystems and total system thermal management. These platforms need to not only prepare for it today, but need to think ahead, for example, with a separate auxiliary-power unit to adapt to changing additional electric loads in the future.

Where will additional power resources come from in aircraft systems?

JANICKI: In modern aircraft, the engines being developed today provide about four times the amount of power compared to legacy platforms, but they produce a lot less or no bleed air as in the past. Now, engine-based generators, ram air-turbine-driven generators, and even batteries are being added to aid in electrical support and storage, as well as thermal batteries to combat extreme thermal requirements for next-generation high-energy weapons. Even if these generators are approaching 95 percent efficiencies, you still have an additional 50 kW of heat to deal with on a 1 mW generator. This situation gets much worse with the very inefficient high-energy weapons projected to be used on these platforms: Adding a 150-kW inefficient laser to the platform heat load can add more than double the generators' wasted heat energy – all of this also needs to be managed. Much more work has to be done to improve efficiencies with high-energy weapons.

It's not just the high-energy weapons that are creating challenges, increases in commercial processor clock speeds will as well. According to a new report from IPC.org on the printed circuit board (PCB) industry, clock speeds will be hitting 25 GHz and higher by 2019.

Designers are using high-performance commercial processors to drive performance while saving costs, but then they see those costs go back up as they have to innovate to overcome the thermal challenges in military platforms. How do you balance that?

JANICKI: It comes down to managing the total life cycle costs. SWaP-C (SWaP plus cost), myopically applied, can significantly drive a solution in the wrong direction. Electronics obsolescence and support need to be balanced against system reliability and what the cost of the program will be down the road if something goes wrong, as opposed to saving money on the front end to meet a reduced cost need.

Any thermal-management system may add additional thermal loads, power draw, space claim, added weight, thermal inertia, and operational-based thermal impacts. It all comes down to what balance works best for your program and how you can best reduce the total life cycle costs while still meeting thermal and performance requirements. **MES**

Gerald Janicki *currently serves as Senior Director for Meggitt Defense Systems, where he is responsible for leading the Thermal Management System (TMS) and Environmental Control System (ECS) programs and business development activities, as well as the Business Area Team which all TMS and ECS Programs report into. He has more than 34 years of experience in the aerospace and defense industry. Prior to joining Meggitt Defense Systems, Janicki had several roles with Boeing, including Director of Strategic Development for the Phantom Works organization. He also was involved in the startup of several new high-technology corporations. Janicki has taught engineering at the University of California at Irvine. He has a BS in Materials Engineering from Rensselaer Polytechnic Institute and a MS in Engineering Management & Business Administration from West Coast University.*

Rugged Computing Spotlights

ISO 9001:2008 & AS9100C CERTIFIED

ITAR REGISTERED

VECTOR

ELECTRONICS & TECHNOLOGY, INC.

A FINE TECHNOLOGY GROUP

Since 1947

MADE IN THE USA

VME / VXS / cPCI ®

Chassis, Backplanes & Accessories

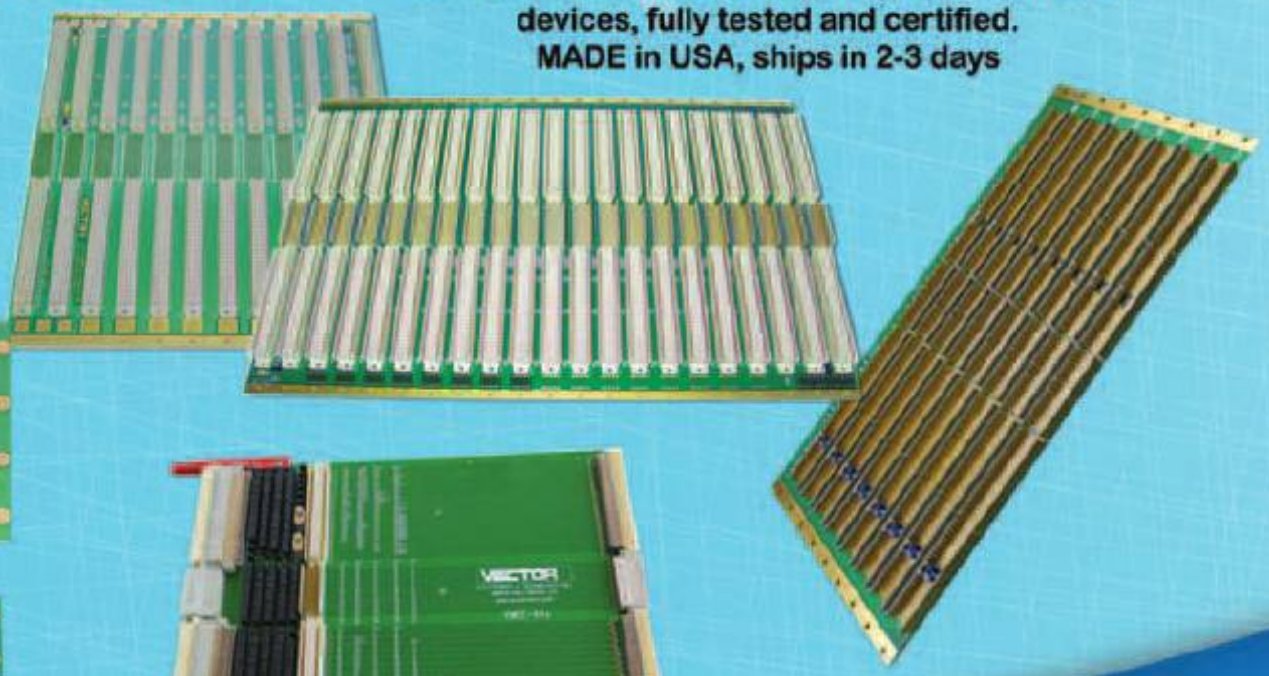
Chassis and Rack Accessories

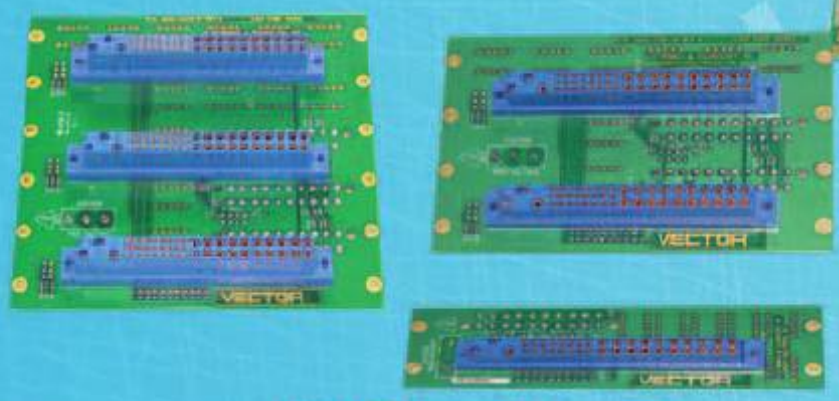
Custom Front Panels

PICMG 2.11 R1.0
Hot Swap Power Supplies

Mil-1-46058-C
Conformal Coating
Available for
all VECTOR backplanes

Hi-speed VITA ANSI/VITA 1.1-1997
monolithic backplanes (Hi Current VITA 1.7 compliant)
with Electronic Bus-Grant (EBG), Surface mount
devices, fully tested and certified.
MADE in USA, ships in 2-3 days





VECTOR Power Backplanes
PICMG 2.11 R1.0 Specification

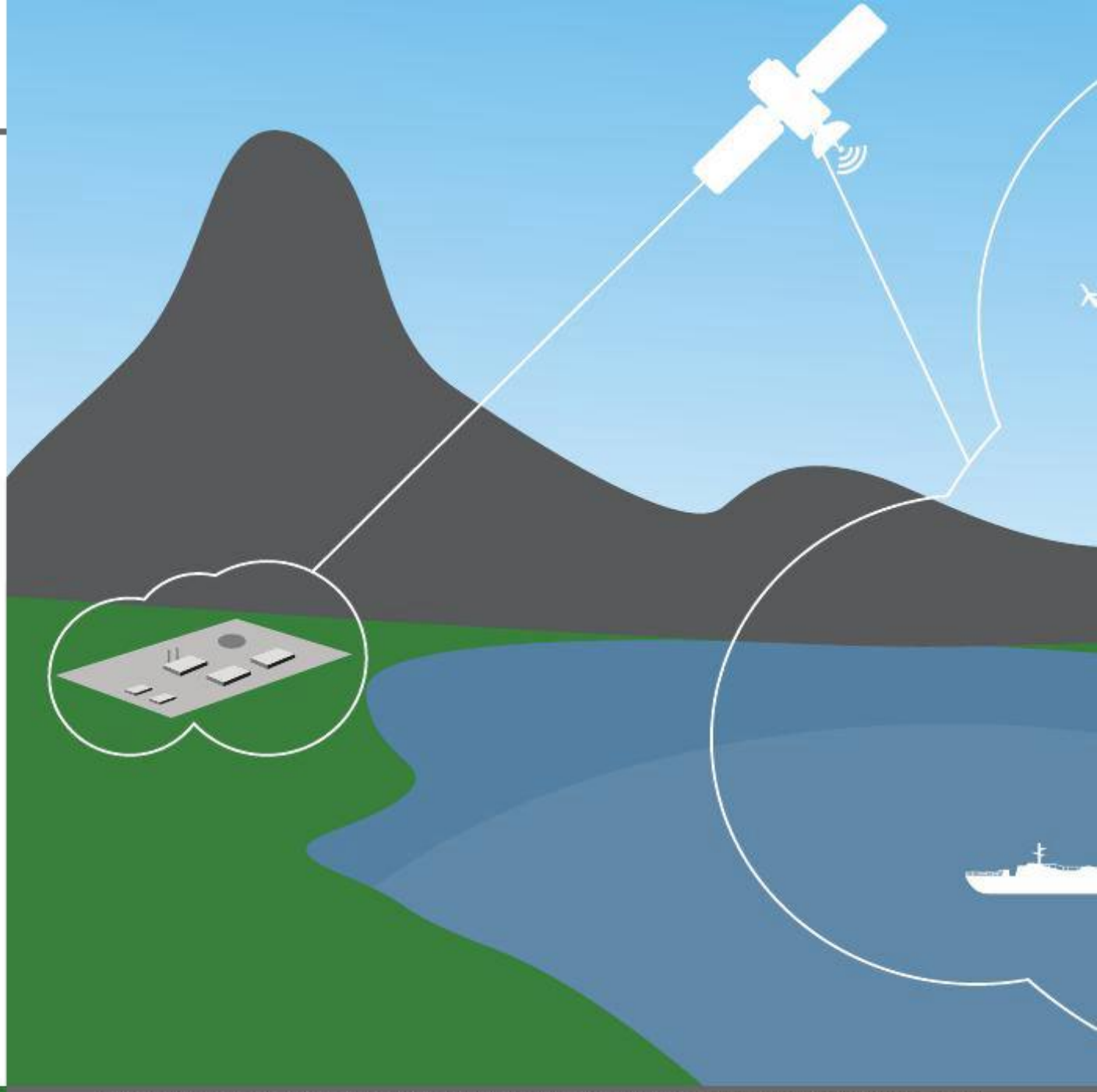
(800)423-5659

WWW.VECTORELECT.COM

MADE IN U.S.A.

The Internet of Things for the intelligence community

By Chip Downing



A fully functional, fully virtualized, self-repairing combat/tactical cloud is the foundation of next-generation intelligence systems.

The Internet of Things (IoT) is an initiative to integrate a wide variety of technical and commercial information-generating components to provide new business opportunities based upon device and system intelligence. This technology is the large-scale commercialization of technology that has been developed and proven by the U.S. Department of Defense (DoD) and the intelligence community (IC) over the past fifteen years. In much the same way that NASA and the early space program in the 1960s spurred innovations in chip technology, automation, propulsion, and miniaturization, solutions developed from the concept of network-centric operations (NCO) translate directly to the foundations of today's commercial IoT. Given that IoT concepts originated in the military/intelligence sector, does the commercialization of IoT provide new opportunities for this community itself? If so, how can vendors exploit these opportunities using commercial off-the-shelf (COTS) technologies?

Advanced sensor-to-cloud intelligence gathering allows today's security agencies to make decisions based on real-time analysis generated by integrating information from a wide range of sensors on a global basis. These systems provide a constant stream of data to agencies where it is analyzed and integrated with other data sources to enable comprehensive situational awareness of security-sensitive arenas.

This network-centric intelligence collection/analysis scenario sets the stage for how today's commercial IoT works (Figure 1). Whether in critical infrastructure, industrial control, or consumer wearables, these IoT systems use similar data-collection, distribution, feedback, and analytical technologies.

Challenges facing the intelligence community

The primary challenge for the military/IC sector is managing the ever-increasing volume of data generated by their system and open-source systems in an efficient and timely manner. Intelligence is based on a tasking, collection, processing, exploitation, and dissemination (TCPED) process, based primarily on a "send it back" model; unfortunately, a large portion of the "collection" in this model goes to archive, unanalyzed. There has been a large growth in the use and adaptation of automated data processing/decision support tools to fix this TCPED logjam, but the growth of data-generating resources, and increasing demand for speed of action, has shown the current architecture to be losing the battle of efficient and reliable information management.

There exist several specific areas where advances based on IoT concepts and technology could positively affect the current system. The first is TCPED architecture. The current reliance on centralized data-processing systems has proven to be incapable of keeping up with the growing sources of collection and data. "Virtualization" would allow the traditional sources and locations of networks, data fusion, and decision support to

capability would significantly accelerate the observe, orient, decide, and act (OODA) loop over today's standards. The key elements of this new NCO architecture are:

- **Intelligence ubiquity:** Every device, sensor, and system contributing to and enabling the Tactical Cloud Forward are available to the mission/operations commanders.
- **Multiple cloud availability:** Connections back to national and commercial cloud systems will be used when available, but a forward-unit, operationally capable subset of all the attributes and capabilities will provide a sustainable operational capability and allow for "graceful degradation" regardless of area of responsibility (AOR) threat level.

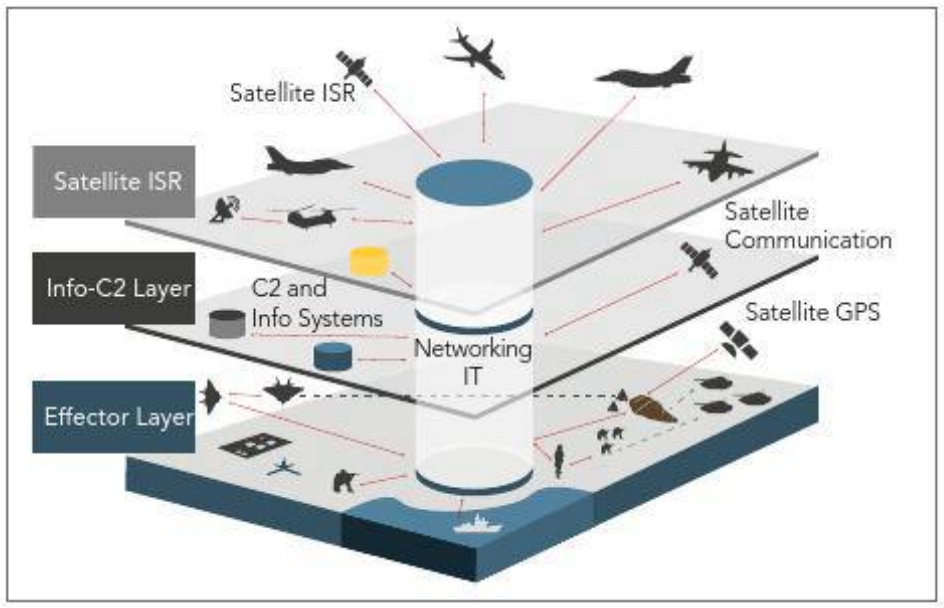


Figure 1 | Network-centric operations.

expand to include many if not all of the sensors, systems and devices deployed forward.

Another area is beyond line-of-sight (BLOS) communication. The TCPED and command-and-control (C2) process reliance on bandwidth/throughput-constrained satellites and other BLOS communications platforms is the Achilles' heel to IC/military operations. A decentralized operational functionality needs to be implemented to diversify the risks of this powerful but communications chokepoint. Lastly, look at the multilevel security (MLS) management area, which covers the need for supporting multiple services, agencies, coalition partners, and new operations partners with automated connectivity, discovery, and security separation of multiple levels of IoT data and intelligence at the user-specific access level without human intervention. This functionality extends to private/personal systems from commercial and government systems, increasing the level of access and collaboration while maintaining data protection and access profile management.

If the challenges in these areas can be solved, there is an opportunity to multiply our force capabilities exponentially. Our global military and intelligence assets are now deployed in many hot spots around the world. Moreover, our technology has matured to the point to where we can finally push data, data fusion, and decision support forward into a new soldier-enabling architecture where NCO-enabled personnel can access a real-time common operating picture (COP) and command data immediately from a Tactical Cloud Forward to solve immediate engagement challenges and identify/react to emerging opportunities faster. Such

- **Single cloud view:** Access to cloud services will appear as a single cloud architecture worldwide, with a fully functional cloud ("overcast cloud") capable of gracefully breaking into "broken" and even "scattered" clouds but retaining basic multisensor/system fusion, data distribution, and access, adapting to the assets available at any given moment.
- **Multilevel security:** The access to all cloud and systems services will have a natural, embedded, MLS method to autonomously filter data to warfighters and mission personnel, with automatic discovery and control to provide the most complete COP.
- **Self-repairing systems:** The flow of data must be self-repairing, able to reconfigure automatically and adapt to new sensor and systems availability, while maintaining and updating prioritization processing as information channels morph into new improved/degraded scenarios.
- **Open standards/open architectures:** All components of this architecture must be based upon open standards and open architectures; this ability enables the rapid insertion of new capabilities and the modification/adaptation of existing ones in order to support new and modified mission scenarios.
- **Platform consolidation:** The use of consolidation platforms using common core processing platforms with rapid, dynamic insertion capabilities is mandatory.
- **Secure remote management:** Edge-management systems and control systems must have secure remote management for reconfiguration to new environments and responding to changes in the threat landscape.
- **End-to-end security:** An end-to-end security architecture must be designed, deployed, and maintained. This security architecture must include both hardware and software as a combined, complementary solution and include both legacy (brownfield) and new system (greenfield) platforms.
- **Platform simulation:** A systems simulation/virtualization model of each hardware element will enable exhaustive testing, including scenario, reconfiguration, and degradation testing, on the overall system at any time. These simulation models can be made available prior to the availability of the actual hardware, allowing for security and robustness testing and design changes in advance of hardware readiness, accelerating time to deployment and boosting overall security robustness.

A fully functional, fully virtualized, self-repairing combat/tactical cloud is the foundation of next-generation intelligence systems. Currently, each military service/coalition partner has its own infrastructure. Transitioning to a combat cloud infrastructure would offer huge operational advantages, with greater ability to export both data and assets in the field for joint operations, providing all connected entities a real-time COP.

Transforming legacy systems into the combat cloud

Next-generation TCPED and Tactical Cloud Forward systems must be based upon advanced network servers to both provide high availability and enable new approaches to controlling and provisioning network systems by delivering full network function virtualization (NFV). NFV offers the operator the ability to dynamically configure the network infrastructure through sophisticated management protocols such as OpenStack, which gives operators the option to optimize for different network situations and demands, such as giving priority to certain data flows, or protecting parts of the network from cyberattacks (Figure 2).

Along with NFV capabilities, new technologies such as multicore silicon and virtualization can help create affordable solutions to these challenges. Virtualized systems enable the continued use of legacy software applications while combining them with new capabilities on new operating environments. The use of modern multicore technology can mitigate performance and separation risks in silicon, separating legacy and new environments on separate cores and networks to achieve the goals of affordability, performance, and mission-capability enhancement well beyond legacy single-core processors.

In the IoT era, consumers are realizing the benefits – and businesses are monetizing the intelligence – gained from technologies tested and proven in the intelligence community. This commercial investment is driving huge cost savings for next-generation security agency systems. With a trusted technology partner, the intelligence community can now reap the benefits of transforming its systems into the next generation of high-value network-enabled solutions, increasing the knowledge, speed, and utility of future security-agency systems. **MES**

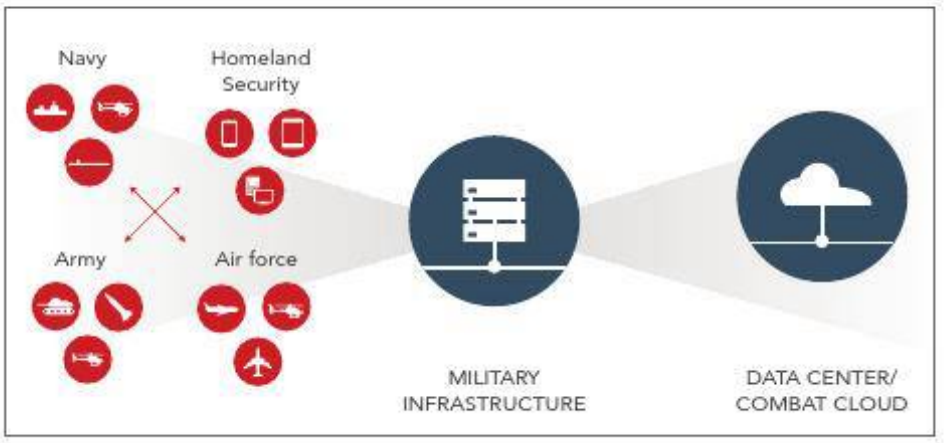


Figure 2 | Tactical Cloud Forward system.

__Chip Downing__ is the senior director of business development for aerospace and defense at Wind River Systems. He is a 20-year veteran of the embedded systems industry and a pioneer in safety certification for commercial real-time operating systems. Downing is also chair of the Future Airborne Capability Environment (FACE) Business Working Group Outreach Committee. Readers may reach him at chip.downing@windriver.com.

Wind River Systems • www.windriver.com

FACE-based tool for military avionics systems

Real-Time Innovations (RTI) engineers released the company's Transport Services Segment (TSS), a commercial off-the-shelf (COTS) connectivity software based on the new Technical Standard for Future Airborne Capability Environment (FACE) edition 2.1. It enables avionics-software developers and platform integrators to assemble technologies with COTS components that have already passed safety-certification credentials.

RTI's TSS technology is built on the Data Distribution Service (DDS) standard developed by the Object Management Group (OMG). This standard includes RTI Connext DDS Cert, which can be certifiable to DO-178C Design Assurance Level (DAL) A and can be used for resource-constrained applications. Additional features of RTI TSS include flexible communication due to the publish/subscribe paradigm, physical transport independence, and real-time Quality of Service (QoS). The system is also interoperable with non-FACE DDS applications, such as those that comply with the UAS Control Segment (UCS) architecture. The FACE TSS encompasses those APIs used for exchanging data between software components. To ease integration, the FACE standard also specifies that exchanged data must conform to a well-defined data model with unambiguous semantics. The RTI TSS includes a compiler that generates C++ data types and the TSS API from a FACE data model.

RTI | www.rti.com | www.mil-embedded.com/p372861

Digital communication system aimed at evolving security needs

In response to the world's constantly evolving transmission and communication security needs and to comply with the National Security Agency's (NSA) Cryptographic Modernization Initiative, Rockwell Collins' RT-1939 ARC-210 Generation5 is a military airborne transceiver/receiver that enables embedded, programmable INFOSEC capability within the ARC-210 communication system family. The RT-1939 has been redesigned to better meet the needs and conform to software defined radio (SDR) tenets and architectures and can help speed transfer of networked or point-to-point data, voice, and imagery. An additional connector has been added in the back of the radio to allow an Ethernet input.

The RT-1939 supplies full form, fit, function (F3), and integration replacement for existing ARC-210 RTs. In addition the communication system also features a frequency extension to cover 30-941 MHz, MIL-STD-188-220D and MIL-STD-2045-47001D networking; Joint Precision Approach Landing System (JPALS); MELP vocoder; Integrated Waveform (IW) for UHF SATCOM; and Soldier Radio Waveform (SRW). Additional features of the communications system include software that is reprogrammable in the field via Memory Loader/ Verifier Software (MLVS), and a support structure including logistics, training, test sets, PC-based loader, and controller.

Rockwell Collins | www.rockwellcollins.com | www.mil-embedded.com/p372862

OpenVPX 3U SBC a fast data processor for common algorithms

The AcQ Inducom "Medusa" VPX3424 is a 3U OpenVPX (VITA 65) single board computer (SBC), featuring the T4240 QorIQ processor from Freescale Semiconductor with as much as 12 GB of DDR3 RAM with ECC and a range of fast interconnects. The 12-core, 24-thread processor running as fast as 1.8 GHz is based on the e6500 core with AltiVec technology and offers performance capability as high as 173 GFlops. Using the T4240's built-in AltiVec technology accelerators, cryptographic engine, and high-speed serial interfaces, the VPX3424 is aimed at data-processing tasks for such common algorithms as FFTs, image analysis, networking, or wireless protocols. Further accelerators enable hardware-based parsing, scheduling (QoS), and queue management.

The VPX3424 has a user-programmable FPGA and OpenVPX user I/O pins, enabling support for application-specific interfaces or offload of specialized tasks to the FPGA. A conduction-cooled, ruggedized REDI (VITA 48) variant of the VPX3424 is available as part of the upcoming AcQ Inducom OpenVPX-based small form factor system (VITA 75), a modular and extendable platform for a range of embedded applications. AcQ Inducom offers a range of boards for this system using the OpenVPX (VITA 65) architecture. It can also be downsized with the T4160 (eight core-16 thread) and the T4080 (four core-eight thread), all pin-compatible.

AcQ Inducom | www.acq.nl | www.mil-embedded.com/p372863

Flight display replaces several instruments

The iSFD, or integrated secondary flight display, system from Meggitt Avionics is an update of the company's SFD. The updated system, aimed at use in commercial and military fixed- and rotary-wing aircraft, displays critical flight information – attitude, altitude and airspeed – replacing two or three electromechanical cockpit standby instruments with a single 3-ATI-size display unit. The active matrix liquid crystal display (AMLCD) has an LED backlight and is compatible with other updated AMLCD primary flight displays.

Within the iSFD itself are solid-state sensors plus a microprocessor system measuring aircraft pitch, bank attitudes, and air data. Air data is measured using the internal air data module (ADM); alternatively, if measured air data are available from an aircraft multifunction probe (MFP) or air data computer (ADC), the iSFD can receive and process the available digitally transmitted air data. If digital magnetic heading data is available, the iSFD will also display aircraft magnetic heading. Its small size – a display area of 61 x 61 mm – and light weight – the entire system weighs 3.3 pounds – are meant to facilitate installation in aircraft. As the system has no International Traffic in Arms Regulations (ITAR) components, it is available for export.

Meggitt Avionics | www.meggitt-avionics.co.uk | www.mil-embedded.com/p372866

Digital tuner for space-constrained applications

With a frequency range of 2 to 6,200 MHz, the Polaris SI-9150/D4 multichannel wideband digital tuner from DRS Technologies can intercept a wide range of signals of interest, providing a wideband 85 MHz digitized bandpass from each of its up to four channels. Its small size (3 by 5 by 2.51 inches), power consumption of 30 W (max.), and ruggedized construction are aimed at a range of manportable, vehicle-mounted, airborne, shipboard, and unmanned aerial vehicle (UAV) platforms.

The SI-9150/D4 four-channel tuner can operate its wideband channels independently, providing 340 MHz of instantaneous coverage, or phase-coherently, which is applicable for direction-finding or beamforming applications. Phase-coherent channel operations enable a designated master channel to share its local oscillator signals with one, two, or three slave channels. Amplitude tracking measures less than ±0.3 dB per 5 °C and less than ±0.1 dB per hour, while phase tracking between RF channels measures less than ±2.0 degrees per 5 °C and less than ±2.0 degrees per hour. The SI-9150/D4 features dual 10 Gbps Ethernet interfaces for streaming time-stamped VITA-49 IF data packets at full rate or user-selectable fractional decimation rates of selected bandwidth, which enables users to focus on specific spectrums of interest.

DRS Technologies | www.drs.com | www.mil-embedded.com/p372865

Central control for crew communications

The Telephonics NetCom-V system provides crew intercommunications and radio management for a wide range of tactical vehicles, including airborne, ground vehicle, and marine applications. The system – which consists of a single line-replaceable unit (LRU), or crew station, that can be expanded for system growth with as many as 20 operators, 60 radios, and 16 VoIP channels – facilitates audio distribution throughout the vehicle and interfaces with all communication assets and crew headsets. Two operators can use each crew station independently; each operator can select any or all connected radios or internal private communication nets for monitoring or transmission via manually controlled knobs.

NetCom-V is intended to enhance crew and personnel safety while increasing overall mission situational awareness. The system features interoperability via IP protocol suite, in addition to a wireless intercom with flexible encryption solutions. Its adaptive-noise-cancellation feature eliminates noise at the audio input, which gives the operator cleaner communication, with a direct interface to all available military vehicle headsets. In addition, the communications system uses a Department of Defense (DoD)-patented spatial audio, which can increase sound intelligibility. Users control the system via a remote Windows-based GUI. Operators can keep track of dismounted crew and personnel with the system's simultaneous voice, data, and location finders.

Telephonics | www.telephonics.com | www.mil-embedded.com/p372864

What distinguishes programming language "Ada" from its competition?

By Sally Cole, Senior Editor

Once considered a DoD-only programming language, "Ada" continues to evolve and is increasingly being taught in universities around the globe for high-integrity applications that demand safety, security, and reliability. The language, around since the early 1980s, is now undergoing a revival of sorts in industry and in academia.

Ada originated as a competitive design sponsored by the Department of Defense (DoD) during an attempt to find a common and modern language that – at the time – could take advantage of the many software-engineering advances of the late 1960s and 1970s. Back then, most of the programming languages were from the 1950s and 1960s and few had "checking" capabilities.

Initially, Ada's application area was military and defense systems because that was its original sponsor, but has gradually shifted more generally to systems in which either safety or security – or both – or reliability were critical. Again, the focus is to take advantage of Ada's language checking and security-oriented features.

As the language evolved, it has changed to reflect technological advances. "A full mid-1990s revision added full object orientation to the language, while a 2005 revision added support for interfacing with Java, which was quickly gaining traction at the time," says Ben Brosgol, senior software engineer at AdaCore, a provider of software solutions for the Ada programming language.

"More recently, in 2012, Ada added full support for contract-based programming, which allows you to add information that better documents what your program is doing and can be enforced with either the profiler or by run-time checks. Other languages have degrees of support for contract-based programming, but aren't really part of the language standards and require extra tools. With Ada, it's built into the language."

Ada gaining popularity

Over the last couple of decades Ada has been perceived to be close to a dead language only used in critical defense applications and not very interesting to incoming college students who spent much of their high school years learning C or C++.

While languages such as C, C++, and Java may receive more attention by sheer volume, one simple explanation is that "Ada has never made significant inroads into the enterprise software realm," says Brosgol.

The key aspect that distinguishes Ada from other languages is the degree of checking that's enforced by the language. "In languages like C or even C++, much is left to the option of the programmer and it's assumed that you know what you're doing…and if you don't you'll find out in the debugger. The idea behind Ada is that the compiler does many of the checks that in other languages take place only during run time. Ada boasts strong 'typing': if you have a data object and it should be used only as an integer, it's not useable as some other type."

Compared with C, Ada "offers more in terms of language features, as well as checking," says Brosgol, "including generic templates for reusability as a mechanism for concurrency, and abstraction – exploiting the various benefits of research work from the 1960s and 1970s."

Enthusiasm for Ada in universities

To help promote academic awareness of Ada, AdaCore launched the GNAT Academic Program (GAP) and is providing at least 200 members with access to AdaCore tools and support. "We try to encourage universities and professors to teach Ada, although it's still not a major language in terms of their curriculum," Brosgol notes.

Learning Ada "involves not just learning the language but also syntax – a set of problem-solving skills in terms of how to think about solving problems, how you design before you code. It's a different mindset," he adds. "We're finding that students who learn Ada turn out to be more efficient programmers than those who don't learn it, and they're landing jobs not only in Ada but also in other languages and fields."

SPARK, a subset of Ada, is also attracting academic attention because it enables mathematically proving program properties. "Students are learning how to build reliable software, as opposed to building it and debugging it until it works."

More than 18 months ago faculty and students from Vermont Technical College in Randolph Center, Vermont, launched a CubeSat satellite into a 500-kilometer Earth orbit as part of NASA's Educational Launch of Nano-satellites (ELaNa) IV program that relied on Ada. "We specifically chose to write the control program for our CubeSat in SPARK/Ada because it offers increased reliability over the C language software used in almost all CubeSats to date," says Prof. Carl Brandon, the project leader from Vermont Technical College. "Using Ada makes complete sense because it is so much more reliable than C code."

E-CAST

Managing avionics safety certification for unmanned aircraft

Presented by dSPACE and RTI

For the U.S. military, unmanned aircraft platforms have been a force multiplier, a term often used to describe something that gives one side a game-changing tactical edge over the other side. Now, however, the Federal Aviation Administration (FAA) is opening the nation's airspace to unmanned aircraft systems (UASs); these systems must now comply with FAA safety standards for technology, such as DO-178 B and C for flight-critical software and DO-254 for hardware. In this e-cast, learn from industry experts as they discuss the challenges found in and solutions for managing avionics safety certification for UASs.

GO TO E-CAST:
ECAST.OPENSYSTEMSMEDIA.COM/563

ADVERTISER INFORMATION

Page	Advertiser/Ad Title
16	**ACCES I/O Products, Inc.** – USB embedded I/O solutions, rugged, industrial strength USB
2	**Acromag** – Great things do come in small packages
36	**ADL Embedded Solutions Inc.** – ADLMES-8200 rugged modular enclosure systems
25	**Aitech Defense Systems** – Our technology investments protect yours
36	**Amphenol PCD** – We know harsh environments
3	**Annapolis Micro Systems, Inc.** – WildStar OpenVPX ecosystem
19	**Astronics/Ballard Technology** – Small size, big performance
6	**Behlman Electronics** – Improved VME and VPX power performance
20	**Creative Electronic Systems** – Optimizing SWaP is our passion
11	**Data Device Corporation** – Your solution provider for connectivity/power/control
29	**Diamond Systems Corporation** – Rugged Gigabit Ethernet switches
28	**Elma Electronic** – Reduce, save, improve
47	**GE Intelligent Platforms, Inc.** – RUGGED Capability without compromise
45	**IBI Systems, Inc.** – For full line of rugged systems
21	**Interface Concept** – Build your own VPX system!
36	**Intersil Corporation** – Rugged transceivers that outperform RS-485 & RS-422 standards
17	**Kimdu Corporation** – Advanced technology … personal touch
40	**MPL AG** – Rugged, flexible COTS solutions from MPL
6	**Orbit Electronics Group and Orbit Power Group** – 135+ VME and VPX solutions
48	**Pentek, Inc.** – Critical recording in any arena
40	**Phoenix International** – Airborne, shipboard, ground mobile data recording and data storage
9	**Proto Labs** – Rapid manufacturing with a polite disregard for tradition
10	**Sealevel Systems, Inc.** – Deliver high-speed data with accuracy every time
41	**Technologic Systems** – Superior embedded solutions
36	**TEN TECH LLC** – Mechanical engineering design & analysis
33	**Themis Computer** – Scale up and scale out: RES high-density (HD) servers
27	**VadaTech Inc.** – Rugged ATCA & MTCA
37	**Vector Electronics & Technology, Inc.** – VME/VXS/cPCI Chassis, backplanes, and accessories
39	**VEROTEC Electronics Packaging** – Verotec Integrated Packaging/TecSYS development platforms
36	**VersaLogic Corp.** – PC/104 "Bay Trail" single board computer
5	**WinSystems, Inc.** – Thinking beyond the board

CONNECTING WITH MIL EMBEDDED

By Mil-Embedded.com Editorial Staff

CHARITY

The Navy-Marine Corps Relief Society

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

This month we're featuring The Navy-Marine Corps Relief Society (NMCRS), a foundation that strives to provide – together with the Navy and Marine Corps – financial, educational, and other needed assistance to active-duty and retired sailors and Marines, their eligible family members, and survivors. The organization offers financial aid to active and retired sailors and Marines (and eligible family) in the form of interest-free loans or grants in case of urgent need; NMCRS volunteers also offer financial counseling to help clients improve their personal financial skills and show them how to work toward individual financial responsibility.

The society administers its own Education Assistance Program, which offers interest-free loans and grants for undergraduate/post-secondary education at an accredited two- or four-year educational, technical, or vocational institution in the United States. This financial assistance is available for children of active-duty, retired, or deceased sailors and Marines; spouses of active-duty sailors and Marines stationed outside the U.S. are also eligible for tuition assistance.

Medical help – including help with care and education after childbirth – is available through the Visiting Nurse program, while the Combat Casualty Assistance program will send a visiting nurse to consult clients who have served with the Navy or Marine Corps during recent overseas operations, regardless of current military status.

The MMCRS was started in 1904, with initial funding drawn from the 1903 Army-Navy football game. In its first year, the society gave $9,500 to families of enlisted men and widows; in 2014, according to the society, $48.5 million in interest-free loans and outright grants was given to sailors, Marines, and family members.

For more information, visit www.nmcrs.org

WHITE PAPER

Advantages and benefits of OpenRFM

By Mercury Systems

OpenRFM is a standards-based, modular open architecture that proposes design, test, and control practices for interfacing radio-frequency (RF) and digital subsystems in an embedded computing architecture. This white paper discusses OpenRFM's ability to integrate RF and microwave elements within electronic warfare, radar, and signals intelligence sensor processing chains by way of standardizing electromechanical and thermal interfaces, software, and control-plane protocols. The goal of OpenRFM is to help defense contractors, designers, and the Department of Defense refresh existing applications and develop future applications faster and at a lower cost.

Read the white paper:
Link: http://mil-embedded.com/white-papers/white-paper-advantages-benefits-openrfmtm/

Check out our other white papers:
http://whitepapers.opensystemsmedia.com

RUGGED

CAPABILITY WITHOUT COMPROMISE.

You need embedded solutions that work where you work. Brilliant enough to exceed your performance expectations. Rugged enough to take a beating in the process. Now you can have it all... from a team that knows how to make things work smarter and tougher.

GE Rugged.
Embedded brilliance.

gedefense.com

Critical Recording in Any Arena

When You Can't Afford to Miss a Beat!

Introducing Pentek's expanded line of Talon® COTS, rugged, portable and lab-based recorders. Built to capture wideband SIGINT, radar and communication signals right out-of-the-box:

- Analog RF/IF, 10 GbE, LVDS, sFPDP solutions
- Real-time sustained recording to 4 GB/sec
- Recording and playback operation
- Analog signal bandwidths to 1.6 GHz
- Shock and vibration resistant Solid State Drives
- GPS time and position stamping
- Hot-swappable storage to Windows® NTFS RAIDs
- Remote operation & multi-system synchronization
- SystemFlow® API & GUI with Signal Analyzer
- Complete documentation & lifetime support

Pentek's rugged turn-key recorders are built and tested for fast, reliable and secure operation in your environment.

Call 201-818-5900 or go to www.pentek.com/go/mestalon for your FREE *High-Speed Recording Systems Handbook* and *Talon Recording Systems Catalog*.

TALON

PENTEK

Setting the Standard for Digital Signal Processing

Pentek, Inc., One Park Way, Upper Saddle River, NJ 07458 • Phone: 201.818.5900 • Fax: 201.818.5904 • e-mail:info@pentek.com • www.pentek.com

Signal Processing Design

Resource Guide

Articles on
Hard Floating-Point FPGAs • OpenCL Programming • FMCW Radar Design • General-Purpose Processors for HPEC

Products include
Application Specific • Chipsets and ICs • Design • Hardware • Services • Standards and Systems

SIGNAL PROCESSING DESIGN

signal-processing.mil-embedded.com