@military_cots

Military EMBEDDED SYSTEMS

MIL-EMBEDDED.COM

July/August 2016 | Volume 12 | Number 5

RUGGED DISPLAYS EMBRACE COMMERCIAL TECH

P 20

P 16

Counterfeit components: The stakes are rising
By Rich Fitzgerald, Avnet

Cyber hardening networks and sensors

P 40

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

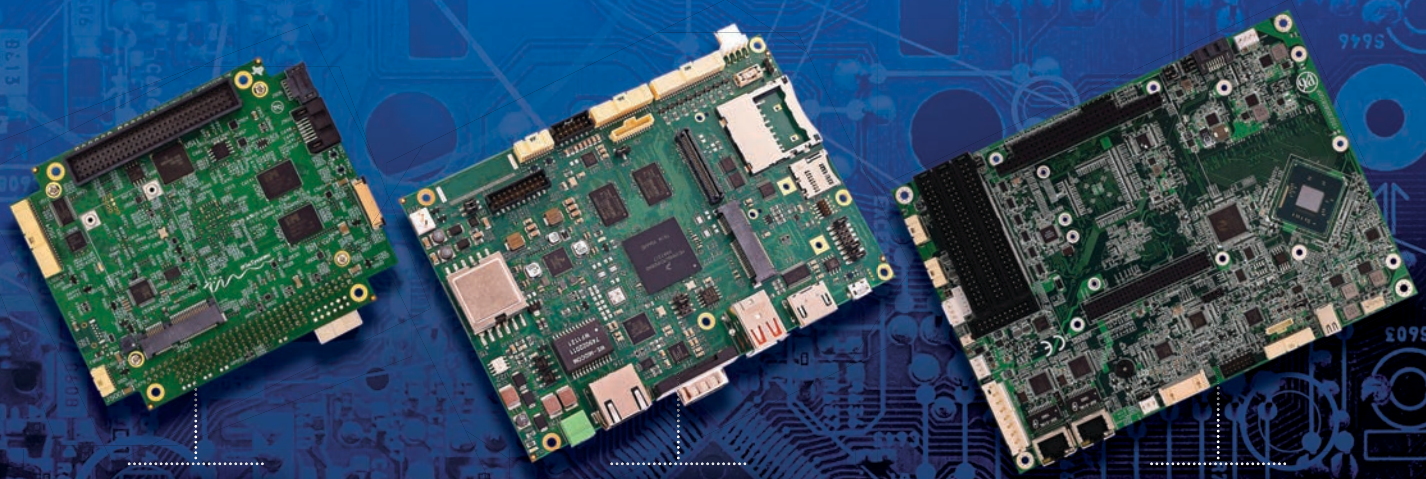
Chassis
4, 6 or 12 Slot
Up to 14G

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

DELIVERING MISSION-CRITICAL DATA CONNECTIVITY



PPM-C407 Fanless
E3800 PC/104 SBC Computer

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

EBC-C413 EBX Industrial
INTEL® BAYTRAIL™
Single Board Computer

SCADA | ENERGY | IOT | TRANSPORTATION | AUTOMATION

Single Board Computers

COM Express Solutions

Power Supplies

I/O Modules

Panel PCs

We live on the sensory edge of what's happening, where the flood of critical data originates. Whatever your application data requirements may be, WinSystems has a full line of embedded computers, I/O cards, cables and accessories designed to acquire and facilitate the flow of essential data. Our rugged, reliable and resilient single board computers are capable of processing a vast array of mission-critical data to support application solutions for an ever expanding world of embedded systems.

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

---

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

Ask about our product evaluation!

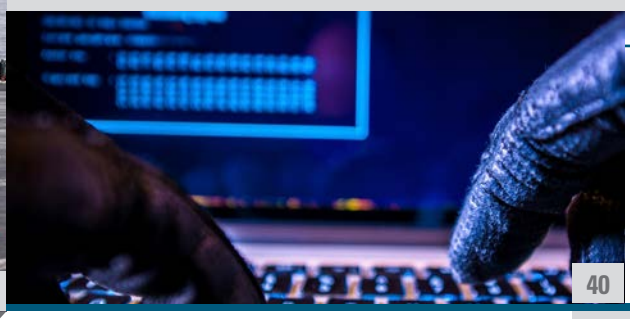
WinSystems®
The Embedded Systems Authority

Volume 12
Number 5

Military EMBEDDED SYSTEMS

July/August 2016

www.mil-embedded.com



E-CASTS

http://ecast.opensystemsmedia.com

Streamline your Software-Defined Radio with Model-Based Design

Presented by MathWorks
http://ecast.opensystemsmedia.com/659

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

ON THE COVER:

Top image: A soldier assigned to the North Carolina Army National Guard's 514th Military Police Company searches a vehicle, June 16, 2016, at Military Ocean Terminal Sunny Point, N.C., during Operation Vigilant Seahawk, an exercise designed to improve communication and coordination with state and federal partners during disaster response and recovery operations. North Carolina Army National Guard photo by Sgt. Odaliska Almonte.

Bottom image: The U.S. Department of Defense (DoD) is currently in the process of "hardening" its networks, sensors, and systems against cyberattacks. This includes real-time operational systems such as aircraft, unmanned aerial vehicles (UAVs), and ships, which all must undergo cyber hardening to enhance mission resiliency against system manipulation, hijacking, or destruction.

Will COTS suppliers find profits in commercial UAV applications?

By John McHale, Editorial Director

Suppliers of commercial off-the-shelf (COTS) hardware and software have had much success in the military unmanned aerial vehicle (UAV) market, especially in the areas of sensor payloads and signal-processing designs, where they excel. UAVs continue to be a profitable arena for these vendors, but as unmanned aircraft technology spreads to commercial markets such as agriculture, construction, retail delivery, disaster relief, and the like, will they find similar success in these nondefense applications, all of which promise to dwarf the value of the military UAV market?

On paper, COTS companies would appear to have the upper hand when it comes to supplying embedded electronics for payloads, as well as hardware and software in avionics systems. If nothing else, they've been doing it longer than anyone else and have a proven pedigree.

However, COTS suppliers will have to adjust to each commercial industry's various standards and form factors – and make that investment on their own dime. While self-funding is nothing new to COTS vendors, especially with Department of Defense budget cuts the last few years, it will likely be viewed as risky by some in management.

COTS suppliers I talked to in our McHale Report roundtable after the Xponential show this Spring in New Orleans – formerly known as the Unmanned Systems show – had mixed emotions when it came to potential commercial UAV opportunities.

"I am not sure anyone can project the level of success for military and commercial suppliers at this time," said Chip Downing, senior director business development, Aerospace and Defense, Wind River Systems. "What we do know is that suppliers of unmanned systems are experiencing a virtuous cycle of growth and innovation – both commercial and military systems are benefiting from rapid market growth based upon innovation of IoT [Internet of Things] and business-intelligence solutions. This growth is based upon open standards and COTS platforms, allowing the innovation to focus on the high-value IoT intelligence gathering and analysis, not the individual building blocks of the UAV or IoT solution stack. COTS platforms enable the fastest integration of the latest advancements in technology, while paving the way for rapid insertion of future innovation."

Some see it as a given that as commercial markets begin to figure out how they can leverage unmanned aircraft, they will need to rely on experienced military suppliers.

"There will undoubtedly be larger suppliers with military unmanned experience that enter into the commercial space," said Mark Littlefield, head vertical product manager, Defense, Kontron. "Certain commercial applications will need the full support of help with certifications, long-term product availability, design stability/scalability, safety standards adherence, small-form-factor features, I/O and multicore integration, ruggedization, and thermal management, which means they need to engage with experienced COTS suppliers."

Mike Southworth, product marketing executive, Curtiss-Wright Defense Solutions, says his company "is already seeing more and more interest from nonmilitary unmanned-vehicle platform customers for our small-form-factor processors and Ethernet networking technologies. We have high expectations that these programs will yield a healthy market for defense COTS companies like Curtiss-Wright. On the other hand, the miniature consumer-drone space will almost assuredly continue to be dominated by offshore manufacturers."

Even if they do find success in nondefense markets, COTS suppliers will often find it limited to applications that have requirements similar to military programs.

"COTS companies will still do OK, but the opportunities will be limited to applications that are used in industrial applications, police, fire, disaster recovery, etc.," said Scott Unzen, market development, Omnetics Connector Corp. "There will be a large development in consumer markets that will not use defense COTS companies because they will be driven by price and not by high-reliability components."

Unzen is right: At the end of the day the commercial applications will not want to pay defense prices for their systems, especially as the cost of the platforms come down when they are mass-produced for commercial markets. Many UAV producers do not have the manufacturing capability in place to produce components at the commercial-level volumes to enable the price reductions necessary for play in commercial arenas. Defense COTS companies would be taking a big risk, one they might not be able to back up.

The next few years will be telling, as civilian aviation authorities continue to evolve their rules to accommodate unmanned aircraft in the civilian airspace and as UAV developers design more sophisticated sense-and-avoid technology so the aircraft can operate more safely in civilian airspace alongside passenger aircraft.

"Over the last ten years, we have seen many airframes come to market and be successful – the next ten years will define how we use these airborne platforms in our personal and business lives," Downing noted.

For more on our roundtable, visit http://bit.ly/29LquCh.

ADVERTISER INFORMATION

Page	Advertiser/Ad Title
47	**Abaco Systems** – We innovate, we deliver, you succeed.
27	**ACCES I/O Products, Inc.** – PCI Express mini card, mPCIe embedded I/O solutions
19	**Acromag** – PCIe-based next generation AcroPack I/O modules
2	**Annapolis Micro Systems, Inc.** – WildStar OpenVPX Ecosystem
15	**Astronics/Ballard Technology** – Versatile COTS avionics computers
37	**Diamond Systems Corporation** – PC/104 SBC with on-board data acquisition
29	**EIZO Rugged Solutions (formerly Tech Source Inc.)** – Flexible rugged COTS
39	**Equipto Electronics Corp** – New Ka shield rack protects to 40 GHz
21	**Interface Concept** – Rugged HPEC boards for your OpenVPX systems
39	**Kimdu Corporation** – Protocol converters
17	**LCR Embedded Systems** – Rugged chassis, backplanes, and integrated systems engineered for your application
35	**MPL AG** – Rugged flexible COTS solutions from MPL
48	**Pentek, Inc.** – Capture. Record. Real-time. Every time.
35	**Phoenix International** – Airborne, shipboard, ground mobile, data recording, and data storage
26	**TE Connectivity** – Remote sensing's not just changing channels
30	**Technologic Systems** – Made in the desert, proven in the field
23	**Themis Computer** – Layer 2/3 enterprise non-blocking GigE smart switch for demanding SWAP-C environments
43	**Vector Electronics & Technology, Inc.** – VME/ VXS/ cPCI chassis, backplanes, and accessories
3	**WinSystems, Inc.** – Delivering mission-critical data connectivity
39	**Z Microsystems, Inc.** – ZX1C lightweight server

EVENTS

IEEE AUTOTESTCON 2016
September 12-15, 2016
Anaheim, CA
www.ieee-autotest.com

2016 AUSA Annual Meeting and Exposition
October 3-5, 2016
Washington, DC
http://ausameetings.org/2016annualmeeting/

Military EMBEDDED SYSTEMS

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

VITA EDITORIAL DIRECTOR Jerry Gipper jgipper@opensystemsmedia.com
PICMG EDITORIAL DIRECTOR Joe Pavlat jpavlat@opensystemsmedia.com
MANAGING EDITOR Jennifer Hesse jhesse@opensystemsmedia.com

SALES

SALES MANAGER Tom Varcie tvarcie@opensystemsmedia.com (586) 415-6500
STRATEGIC ACCOUNT MANAGER Rebecca Barker rbarker@opensystemsmedia.com (281) 724-8021
STRATEGIC ACCOUNT MANAGER Bill Barron bbarron@opensystemsmedia.com (516) 376-9838
STRATEGIC ACCOUNT MANAGER Eric Henry ehenry@opensystemsmedia.com (541) 760-5361
STRATEGIC ACCOUNT MANAGER Kathleen Wackowski kwackowski@opensystemsmedia.com (978) 888-7367
SOUTHERN CALIFORNIA REGIONAL SALES MANAGER Len Pettek lpettek@opensystemsmedia.com (805) 231-9582
SOUTHWEST REGIONAL SALES MANAGER Barbara Quinlan bquinlan@opensystemsmedia.com (480) 236-8818
NORTHERN CALIFORNIA REGIONAL SALES MANAGER Twyla Sulesky tsulesky@opensystemsmedia.com (408) 779-0005
ASIA-PACIFIC SALES ACCOUNT MANAGER Elvi Lee elvi@aceforum.com.tw
EUROPE SALES ACCOUNT MANAGER James Rhoades-Brown james.rhoadesbrown@husonmedia.com

OpenSystems media®
WWW.OPENSYSTEMSMEDIA.COM

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

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

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

REPRINTS

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

New game for GUIs

By Charlotte Adams

An Abaco Systems perspective on embedded military electronics trends

Those of us who recall DOS and other command interfaces appreciate the invention of graphical user interfaces (GUIs): Graphical controls and displays make us more efficient and productive because they are intuitive, with little or no learning required. GUIs make life easier, whether one is writing code or playing games.

Why? As the saying goes, a picture is worth a thousand words. But it's actually worth a lot more when it comes to operating controls. Fast readers can proofread material at about 200 words – or about 900 bytes – a minute. By the same token, a video gamer manipulating images on a 1920 by 1080-pixel screen at 60 frames per second can comprehend about 22 gigabytes a minute. So moving controls via graphical versus textual information wins by a factor of more than 22 million.

People can assimilate a vast amount of sensory data almost instantaneously. Think of cars weaving in and out of high-speed traffic at night, which happens every day with relatively few accidents. However, if you blindfolded those drivers and gave them verbal commands about when to floor it, when to slam on the brakes, and where to turn, it would be a disaster scenario.

Challenges to visualization

It's much easier to write code if each step in the process can be verified and tested visually rather than textually. If you know what the data should look like at certain points in the program, but the visualizations indicate the contrary, you can stop and fix the problems before they multiply. With GUIs, algorithms can be instrumented, simulated, and demonstrated as they are coded, reducing debug time. Yet although many GUI kits are available on the market, GUIs are not considered essential in the embedded world.

Programmers may not see the GUI cost/benefit since embedded software, such as a missile-tracking system or a radar-processing application, may not require graphics support. The target processor, for example, may not even feature a graphics chip. In addition, GUIs can drain processor cycles and create bottlenecks, both definitely unacceptable. Moreover, GUIs typically involve a lot of code, and the kits can entail extensive learning curves, as programmers familiarize themselves with hundreds or even thousands of application program interfaces (APIs).

What's more, conventional GUIs – which emerged from the nondeterministic world – are difficult to adapt to the needs of embedded processing. For one thing, GUI software typically is intended for event-driven programming models in which many programming loops "sleep" in the background until triggered by an action such as a mouse click or a key press.

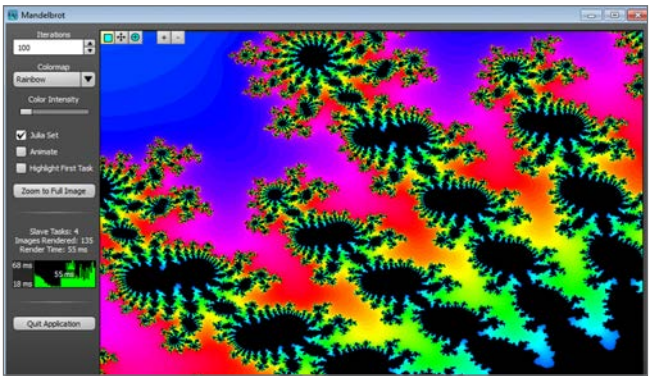


Figure 1 | Abaco's DataView is designed for displaying data and adding controls to signal- and image-processing applications as well as to any system-control or communications application.

The order in which components will execute will vary unpredictably, according to user inputs. This versatility is ideal for something like word processing. In contrast, real-time embedded processing applications, which require highly predictable performance, typically rely on a sequential programming model, where every step in the program is determined in advance and executes according to a rigorous schedule.

Developers of embedded software have been reluctant to develop GUIs because conventional GUIs increase development and maintenance costs, consume cycles, and appear to be unnecessary.

What if?

What if the embedded software world could reap the benefits of GUIs without incurring the costs? For starters, this would require easy-to-use GUI development kits that could quickly create no-frills interfaces. The GUIs also would need to be decoupled from the target code, so that visualizations could be run remotely, as needed.

Since these GUIs would be smaller and simpler than the systems found in the nonembedded world – no need for pull-down menus or pop-up dialog boxes – the kits would involve fewer APIs. The GUI would focus on the bare necessities of inputting and visualizing data. Application overhead would be limited to sending and receiving data when necessary over the TCP connections typically built into modern boards. Abaco Systems recently introduced AXIS DataView, a multiplatform, multi-operating system tool, which has only five APIs and is external to the application source code. (Figure 1.)

If GUIs can be set up quickly and allow developers to minimize coding and debug time, that is a winning scenario all around.

www.abaco.com

High-speed ADC/DAC and FPGAs drive the design of next-generation SATCOM systems

By Denis Smetana
An industry perspective from Curtiss-Wright Defense Solutions

Many military satellite communications (SATCOM) systems operate in the very-high-frequency S-band (2 to 4 GHz) and C-band (4 to 8 GHz) range. Accurate sampling of satellite communications requires frequency rates that are at least twice, but preferably 2.5 to 3 times, the speed of the carrier frequency.

Until recently this proved beyond the capability of most conventional digital converter technology. For that reason, embedded systems designed to handle S-band and C-band transmission rates have typically required analog conversion techniques, such as frequency mixing, to convert the received signal to a lower fixed intermediate frequency (IF) to bring the signals within range of standard digital converter technology. The analog conversion requirement adds cost, complexity, and power requirements to these systems, none of which is desirable for deployed embedded systems.

A better solution would be to directly sample the signals using an analog-to-digital converter (ADC). In addition to eliminating the need for a front-end mixer, this direct sampling approach would also enable the full communications bandwidth to be processed digitally using digital signal processing (DSP) techniques.

Another challenge for embedded SATCOM systems is the large amount of processing required to fully process the generation and reception of SATCOM signals. Historically this has been addressed with expensive custom application-specific integrated circuits (ASICs) that can handle the system's algorithms at the needed throughput. The good news is that as field-programmable gate arrays (FPGAs) have continued to grow in capability, SATCOM processing can now be performed using several FPGAs. This does require, though, that there is sufficient interconnect bandwidth (100 to 200 Gbps) to pass the data between the FPGA processing units. In addition to their lower cost compared to ASICs, FPGAs also provide reconfigurability, which simplifies and lowers the cost of upgrading the SATCOM system over time with new algorithms without having to change the system's hardware.

Combining the advantages of multigigabit, ultrawideband sampling ADCs and DACs with today's high-performance FPGAs now enables system designers to develop new classes of embedded SATCOM systems – for land-based stations or for simulation of space-based stations – that can sample and process S-band and C-band signals while eliminating the need to downconvert the signals using analog conversion.

Making this development possible is the recent availability of open-standards modules that contain 12 Gsps and 25 Gsps ADCs and DACs, developed by Tektronix Component Solutions; these modules deliver the bandwidth required to directly

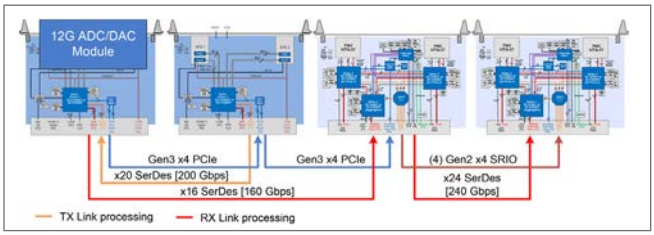


Figure 1 | An example of a fully digital SATCOM system designed to handle very-high-frequency S-band signals.

sample both S-band and C-band signals. When integrated with FPGA-based OpenVPX modules, these devices enable the development of scalable SATCOM high-performance embedded computing (HPEC) systems that feature a reconfigurable architecture supporting updates via firmware. OpenVPX modules based on these devices may also be combined with other general-purpose processor modules, switch cards, or recorders to provide even more capability.

An example of a fully digital SATCOM system designed to handle S-band signals was recently developed by a leading SATCOM provider. (Figure 1.) The system uses the Curtiss-Wright CHAMP-WB-DRFM OpenVPX module, which combines both 12 Gsps ADCs and DACs and a Xilinx Virtex-7 FPGA. Because of the high amount of processing required, additional FPGA modules were used to pass data between the modules. The DRFM module provides 20 serializer/deserializers (SerDes) directly connected to the OpenVPX backplane from the FPGA. Since the SerDes can each run at rates up to 10.3 Gbps, they provided 200 Gbps of available bandwidth. An additional FPGA module with three onboard Virtex-7 FPGAs and 40 SerDes was directly connected to the backplane. The FPGA board's SerDes, also running at 10.3 Gbps, provided 400 Gbps of available bandwidth. To provide more bandwidth, a rear transition module (RTM) was used to split the RX and the TX links into separate connections, enabling the Virtex FPGAs to use Xilinx's simplex Aurora protocol in a unidirectional mode, so that each SerDes TX/RX pair did not have to go to the same module. Because the RX links can come from one card while the TX links go to a different card, the amount of SerDes bandwidth was effectively doubled when daisy-chaining the modules together.

The same concept may be applied to other wideband communication systems that use S-band or C-band frequency signals. The technique can also be applied to even higher rate signaling, where it enables downconversion that can't be completely eliminated to at least be greatly simplified.

Denis Smetana, Senior Product Manager,
FPGA Products, Curtiss-Wright
www.cwcdefense.com

Hunting vulns by adding swarms of bugs to source code

By Sally Cole, Senior Editor

In a new twist on hunting vulnerabilities within source code, researchers are adding huge swarms of bugs to test the limits of bug-finding tools.

Software that sniffs out potentially dangerous bugs within computer programs tends to be extremely expensive, and yet there has been no solid way to determine for sure how many bugs go undetected. In response, a group of researchers from New York University (NYU), MIT Lincoln Laboratory, and Northeastern University developed a radically different approach to tackle the problem by intentionally adding hundreds of thousands of bugs to the source code to control the number of bugs within a program, rather than attempting to find and remediate them.

The group's approach is called "LAVA," short for Large-Scale Automated Vulnerability Addition, and tests the limits of bug-finding tools. It does this by inserting known quantities of novel vulnerabilities that are synthetic yet possess many of the same attributes as computer bugs in the wild.

This automated system was able to generate hundreds of thousands of unstudied, highly realistic vulnerabilities that are inexpensive, span the execution lifetime of a program, are embedded within a normal control and data flow, and manifest only for a small fraction of inputs to avoid shutting down the entire program.

The researchers needed to create novel bugs – and lots of them – to explore the strengths and weaknesses of bug-finding software. Previously identified vulnerabilities would have tripped current bug finders and skewed the results. (Figure 1.)

Just how big a problem is finding bugs within source code? Big. Moreover, the group discovered that many popular bug finders detected only two percent of the vulnerabilities created by LAVA.

"Although the two percent detection rate is definitely surprising – generally when I've asked people they expected something more in the range of 10 to 20 percent – I think the right way to think about it is not that these tools are very bad, but that finding bugs within code is inherently an extremely difficult problem," explains Brendan Dolan-Gavitt, an assistant professor of computer science and engineering at NYU's Tandon School of Engineering, and co-creator of LAVA. "We've seen cases where a bug might go undetected within some incredibly widely used software for decades."

The motivation behind LAVA came from realizing that "people creating bug-finding tools didn't really have a good way to tell how effective they were," Dolan-Gavitt says. "Someone would create a new tool and test it out, and if it found a few bugs that other systems hadn't caught, it was declared a success. This isn't a very rigorous way of evaluating the effectiveness of a detector. And standardized test suites were both rare and extremely expensive to create."

Tim Leek, who initially came up with the idea for LAVA at MIT Lincoln Laboratory, was involved in the creation of one of these test suites, and it took about six months to come up with a corpus of just 14 well-annotated and well-understood bugs. "So this really demonstrates that we need a better way of producing these test corpora," notes Dolan-Gavitt.

How can the U.S. military tap LAVA? "The military often uses commercial and open-source bug-finding software to evaluate new software systems. When choosing one of these bug-finding systems, they need to do due diligence by evaluating their effectiveness, and that's exactly what LAVA is designed to do," Dolan-Gavitt says. "Traditional ways of evaluating bug detectors, such as manually adding bugs or using databases of historical bugs, are very costly or too easy to game. I think LAVA could help bring down the costs of doing such evaluations, which will also force vendors to up their game."

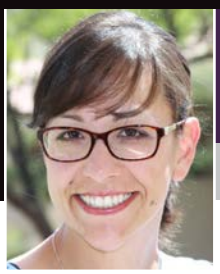
Figure 1 | Image courtesy of NYU.

Another area being explored for LAVA is cybersecurity training. "Right now, one of the primary methods of training cybersecurity experts in both the military and industry is through 'Capture the Flag' (CTF) competitions," he adds. "Basically, the competition organizers set up some deliberately weak systems and software, then people compete to see who can break in. But these competitions are a lot of work to put together, so LAVA might be able to help by adding new exploitable bugs for a CTF."

The group plans to launch its own open competition this summer to give developers and other researchers a chance to request a LAVA-bugged version of a piece of software, attempt to find the bugs, and receive a score based on their accuracy.

It's important to note that plenty of other bug-finding tools exist that the group hasn't been able to evaluate yet, both due to lack of time and the high cost of obtaining them. "We hope that when we open things up to a general competition, vendors will want to take part and do their own public evaluations," says Dolan-Gavitt.

For more information, visit: www.ieee-security.org/TC/SP2016/papers/0824a110.pdf.



DEFENSE TECH WIRE

NEWS | TRENDS | DOD SPENDS | CONTRACTS | TECHNOLOGY UPDATES

By Mariana Iriarte, Associate Editor

NEWS

U.S. Navy's first network-enabled weapon achieves initial operational capability

U.S. Navy officials announced that the service's first air-to-ground network-enabled weapon, Joint Standoff Weapon (JSOW) C-1, completed operational testing against land and sea targets, thereby achieving Initial Operational Capability (IOC).

The JSOW C-1 – a Raytheon-built weapon – is integrated with Link 16 network radio and also uses terminal infrared (IR) seeker GPS/INS for guidance. Navy officials say that the weapon will be launched in F/A-18E/F and F-35A/C aircraft. "JSOW C-1 provides the ability to engage our enemies at longer ranges and the flexibility to engage in direct attack even if enemy air defenses deny our aircraft access," says Cmdr. Sam Messer, Navy JSOW program manager.

Figure 1 | JSOW C-1 impacts target during test. Photo courtesy U.S. Navy.

CPI to provide research efforts in vacuum electronics for DARPA program

Officials at the Microsystems Technology Office, a division of the Defense Advanced Research Projects Agency (DARPA), selected the Microwave Power Products Division of Communications & Power Industries LLC (CPI) for the first phase of the High Power Amplifier Using Vacuum Electronics for Overmatch Capability (HAVOC) program to research revolutionary approaches to vacuum electronics.

Under the contract, researchers will develop and demonstrate a high-power, wide-bandwidth vacuum electron device (VED) that is compatible with mobile and airborne platforms. The HAVOC program aims to develop VED technology to minimize output power and bandwidth tradeoffs, consequently enabling both high-output power and wide bandwidths. The first phase of the contract is valued at an estimated $5.8 million; if all phases and options are exercised, the total ceiling value is estimated at $13 million.

Company officials restructure ThalesRaytheonSystems joint venture

Thales and Raytheon officials say they restructured their joint venture company, ThalesRaytheonSystems, to focus only on NATO agencies and NATO member nations for delivery of the Air Command and Control System (ACCS), Theatre Missile Defense, and Ballistic Missile Defense.

Representatives of both companies concluded the transaction to transition the stakeholder positions each held in the ThalesRaytheonSystems joint venture. Company structure transitions are effective immediately.

Moving forward, the parent companies will retain their ground-based radar systems and non-ACCS-related air command-and-control systems currently within the joint venture portfolio. Raytheon made a $90 million cash payment to Thales and will be recording a tax-free gain of about $150 million in its second-quarter financial results.

U.S. Navy's MQ-4C Triton demonstrates new capabilities during flight test

The U.S. Navy's MQ-4C Triton aircraft completed two flight tests demonstrating the ability of the unmanned aerial system (UAS) to extend its time on station as well as display interoperability between platforms.

During one demonstration, an MQ-4C Triton and P-8A Poseidon exchanged full-motion video for the first time via a Common Data Link. The flight test validated the Triton's capability to increase situational awareness for the P-8A crew by tracking a target with its electro-optical/IR camera.

The MQ-4C Triton also completed a heavyweight flight test, which officials say will enable the UAS to expand its estimated flight time before needing to refuel or return to base. U.S. Navy officials say that testing will continue on the Triton in preparation for its first scheduled deployment in 2018.

Figure 2 | The MQ-4C Triton standing by for flight tests at a naval station. Photo courtesy U.S. Navy.

University and Navy officials sign education agreement with cybersecurity focus

Naval Air Warfare Center Training Systems Division (NAWCTSD) and University of South Florida (USF) representatives have entered into an Educational Partnership Agreement that will focus in the areas of cybersecurity and cyberwarfare modeling, simulation, training, and human performance (MST&HP). The agreement will leverage the combined resources of both organizations for students wishing to pursue science, technology, engineering, and mathematics (STEM) education.

USF will provide strategic vision and guidance facilitating education and information sharing on cybersecurity through its Florida Center for Cybersecurity (FC2). Created by the 2013 Florida Legislature and under the USF leadership, FC2 is "charged with securing Florida's place as the national leader in cybersecurity through education; innovative, interdisciplinary research; and community outreach."

NAWCTSD, as an executive member of Team Orlando and with the assistance of other members, will provide MST&HP experience and resources to help make USF/FC2's vision a reality. Team Orlando is a modeling, simulation, and training company; through FC2's cybersecurity working group, Team Orlando and FC2 will facilitate the sharing of cyber training and technologies, lessons learned, and initiatives.

Figure 3 | Sri Sridharan, managing director and chief operating officer for FC2 at the University of South Florida (right), and Navy Capt. Erik Etz (left) sign the educational partnership agreement. Photo courtesy U.S. Navy.

Loitering, airborne ISR goal of Raytheon-UVision teaming

Raytheon Co. and UVision officials have signed a teaming agreement to work together to develop small, loitering airborne solutions. As part of the agreement, Raytheon engineers will adapt UVision's Hero-30 remotely operated lethal loitering airborne system for U.S. military requirements.

The Hero-30 is a man-packed, canister-launched airborne loitering system that Raytheon will modify for lethal target engagement as well as traditional airborne intelligence, surveillance, and reconnaissance (ISR) missions. The adapted system will meet the U.S. Army's requirement for Lethal Miniature Aerial Missile Systems (LMAMS)

The Hero-30 derivative potentially may fulfill conventional small-unit and special-operations requirements. Previous user evaluations have determined Hero-30 to be flexible and simple enough for use in small-unit operations.

SDR tech drives military mobile computing market growth

Increased requirements for software-defined radio (SDR) technology will contribute to the growth of the global military mobile computing systems market over the next five years, according to analysts at Technavio in Elmhurst, Illinois. They forecast the market to grow at a compound annual growth rate (CAGR) of more than 7 percent by 2020.

Factors driving the demand for SDR technology include the increasing need for tactical communications, interoperability, real-time data communications, modernization programs, and reduced size, weight, and power (SWaP) benefits. Another trend gaining momentum in this market is demand for solutions that enable network-centric warfare, according to Technavio analysts.

BAE Systems, General Dynamics, Harris, Rockwell Collins, and Thales are the key players in this market, according to the Technavio report, titled "Global Military Mobile Computing Systems Market 2016-2020." The Asia-Pacific (APAC) region will be the fastest-growing region in the military mobile computing systems market and is forecasted to grow at a CAGR of more than 11 percent by 2020, the report says.

X-57 designation given to NASA electric research plane

NASA officials announced a new X-designated test aircraft, the X-57, which will be nicknamed "Maxwell." The X-57 is an electric research plane with 14 electric motors turning propellers that will be integrated into a uniquely designed wing. NASA officials will test new propulsion technology with this aircraft.

Following a request from NASA, the U.S. Air Force assigned the aircraft with the X-57 number designation. NASA researchers working directly with the airplane also chose to name the aircraft "Maxwell" to honor James Clerk Maxwell, the 19th-century Scottish physicist.

As many as five larger transport-scale X-planes also are planned as part of this initiative. Its goals – like the X-57 – include demonstrating advanced technologies to reduce fuel use, emissions, and noise.

Figure 4 | This artist's concept of NASA's X-57 Maxwell aircraft shows the plane's specially designed wing and 14 electric motors. Photo courtesy of NASA Langley/Advanced Concepts Lab, AMA, Inc.

Counterfeit mitigation: The small-company challenge

By Shmuel Yankelewitz

It's an unfortunate fact of life that anything of value can – and probably will – be faked at some point. While exciting stories of forged multimillion-dollar paintings and violins might make the news from time to time, the far more pedestrian fact is that counterfeiting of small electronic components is an unfortunately thriving business, and one of enormous potential consequence when lives depend on complex electronic equipment operating as anticipated. It is of absolutely vital importance to major defense contractors and the companies that supply them, not to mention to the warfighters who rely on this equipment, that counterfeit components not make their way into the field under any circumstances.

Unfortunately for the typical small company, the process of counterfeit mitigation can be complicated and daunting, with a steep and perilous learning curve. Without a deep understanding of the landscape of counterfeit components nor the resources to respond, a small company can be very significantly impacted should such parts pass through their receiving inspection, assembly, and testing process and subsequently ship to their customers. Bleeding-edge mitigation technologies like DNA marking are often discussed but are not yet well established; such advanced technologies are also often extremely difficult for small companies to implement.

The good news, however, is that resources do exist to enable small companies to develop effective internal processes and systems to address this problem, and to ensure that they are not "caught out" by counterfeit components.

Background: Internal and external requirements

Counterfeit-mitigation requirements typically flow down from customer's purchase-order quality clauses, which can include requirements to comply with SAE Standard AS5553 – which covers high-reliability parts for space, defense, and aviation – a customer's internal counterfeit-mitigation requirements, or both. The AS5553 standard itself mandates practices and documentation of activities having to do with supply chain, inventory management, procurement, receiving inspection, and receiving; it also covers the all-important issue of appropriate responses when suspect components are discovered.

In addition to the flow-down requirements of the AS5553 standard, any deal with a large defense contractor will also contain recursive flow-down clauses, under which the requirements imposed upon the prime contractor by its (usually government) customers will flow down to its subcontractors, who are also obliged to flow them down to their suppliers.

The challenges for small companies

The most daunting challenges for small companies implementing counterfeit component mitigation revolve around limited resources and understanding of how to implement the practical requirements of the AS5553 standard. While there do exist what amount to free-to-join "crowdsourced" supplier organizations that deal with counterfeit components, some organizations charge hefty membership dues, which may be onerous for a small firm. Moreover, small firms who themselves may deal with "mom-and-pop" shops may face resistance when passing along counterfeit-mitigation flowdown requirements to these shops. Adding to the pressure, many small manufacturers have to deal with part obsolescence or hard-to-find parts under the tight scheduling pressures so prevalent in aerospace and defense (A&D). They therefore may be compelled to engage with unfamiliar nonfranchised distributors, or distributors who are not directly under contract with the original components manufacturers themselves.

It's important to state here that nonfranchised distributors are a vital and legitimate part of any supply chain, particularly in A&D, where customers may approach companies that require support for equipment that is decades old, and where manufacturers of the original components might not even exist anymore. In such situations, no distributor can possibly be expected to have a direct paper trail back to the original manufacturer. Many such components are often bought in somewhat randomly mixed lots, sometimes from first- and second-tier defense companies trying to get rid of old inventory. Without nonfranchised distributors, decades-old legacy equipment would never be able to continue to function and add value for perpetually cash-strapped A&D programs.

Other challenges facing small companies in this arena include the significant expense in requalifying parts once suspect components have successfully been quarantined. One of the biggest hurdles can be a broad organizational lack of familiarity with the nature of counterfeit-component mitigation.

How to avoid the bite of the counterfeit bug

Any counterfeit-mitigation program must begin with identifying the largest areas of risk, which typically resides with parts that are scarce or expensive. Examples include, but are not limited to, integrated circuits (ICs), central processing units (CPUs), memory chips, capacitors, resistors, and connectors of all types, which offer the greatest chance of "getting away with it" for counterfeit suppliers and the greatest potential payoff.

The second area companies can focus on is the documentation of a counterfeit-mitigation procedure that mirrors the AS5553 standard. This internal documentation, while following the AS5553 standard, must specifically identify high-risk components used by the company, clearly delineate how to qualify and deal with nonfranchised suppliers, and clearly specify the actions required when a suspect part is discovered. The procedure must also address flow-down requirements and supply-chain training where required.

In addition to this, small companies should obtain copies of their distributors' own internal procedures for counterfeit mitigation, as well as visit and audit their distributors where necessary. If a company's customers include large prime contractors, these big companies can also be a valuable resource for counterfeit-mitigation procedures and policies. The big primes, of course, have a vested interest in ensuring that counterfeit components do not slip into anyone's production. They are usually very open to sharing their experiences and documentation with any of their suppliers looking to implement counterfeit mitigation. Prime defense customers are also often amenable to sharing lists of their approved nonfranchised distributors. Because of their sheer size, large prime contractors have the necessary resources to qualify, track, and maintain the approval status of nonfranchised distributors; small companies who count them among their customers should not hesitate to take advantage of these resources.

The fourth leg of the process consists of education and training: Here, as well, it starts with customers. Most large- and medium-sized defense contractors have high-end training programs for counterfeit mitigation, including videos, workbooks, and training manuals and are eager to share them with their suppliers.

Supply-chain education and management is a critical part of counterfeit mitigation, and the purchasing department must be engaged in the counterfeit-mitigation process. Purchasing may consider a policy of not purchasing from a nonfranchised distributors unless there is no other way of obtaining a certain part. If a nonfranchised distributor is the only option to obtain a hard-to-find component, a company may consider creating a stringent multilevel approval process where the customer must provide final approval – with the company not to proceed until this approval is secured.

When a company has completed its counterfeit-mitigation procedure, it must also make sure to train not just the employees responsible for receiving inspection but

also the entire production staff, who may be fitting small components onto larger ones, soldering parts together, or otherwise engaging in activities that require an intimate familiarity with the components themselves. (Figure 1.) Anything from a slight change in component colors, shape, date stamps or other markings, or even an indistinct or messy supplier logo would stand out more clearly to production-floor staff, who see and handle components dozens of times a day. Anti-counterfeit vigilance must be encouraged and rewarded among all employees, given the stakes should counterfeit materials slip through and actually ship to a customer.

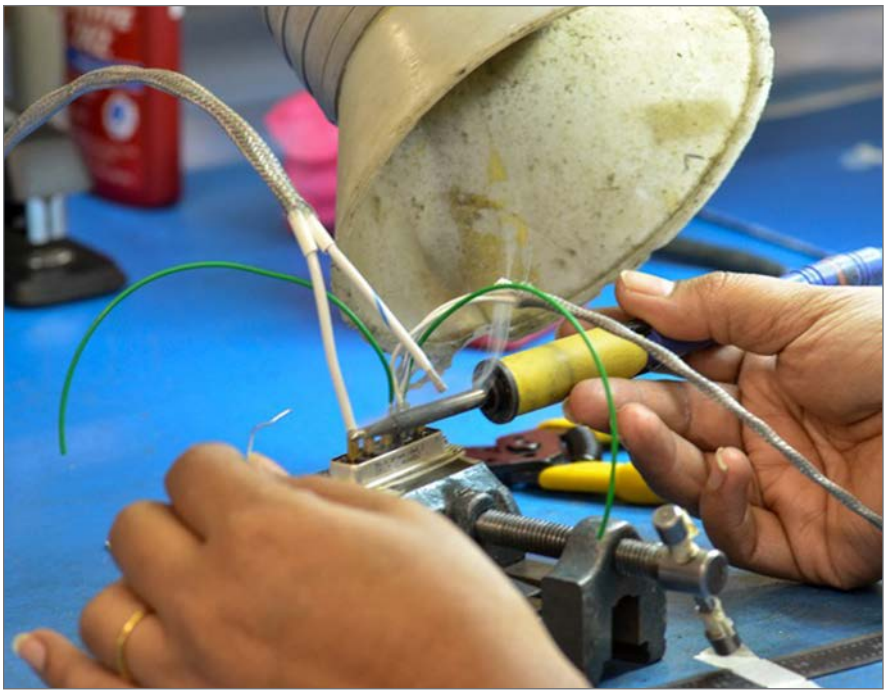


Figure 1 | Production-floor staff see and handle components dozens of times a day. They are often the first to notice anything from a slight change in component colors, shape, date stamps or other markings, or even an indistinct or messy supplier logo. Photo courtesy LCR Embedded Systems.

Industry resource organizations

There exist many organizations that are dedicated to counterfeit-component mitigation and which offer networking between members, standards, and best practices. Among them are the Government-Industry Data Exchange Program (GIDEP) – www.gidep.org – a free-to-join organization of suppliers, distributors, and customers created to share information among its membership to help alert the industry to many types of problems, not just counterfeit components. In a way, GIDEP is a crowd-sourced supplier knowledge base and a valuable resource for any company, large or small. A company can receive alerts on particular companies or components, and is also expected to inform GIDEP when they have encountered counterfeit components themselves. Through these means, knowledge can spread rapidly within the A&D community, making it even more difficult for counterfeit components to find their way into the field. Membership is available to government organizations, contractors, and suppliers in the U.S. and Canada. Corporate quality professionals should join GIDEP and report every counterfeit-component finding in their organization; this activity should be formally included as part of any company's counterfeit-mitigation process.

Electronic Resellers Association International (ERAI) – www.erai.com – is a global organization that monitors, investigates, and reports issues affecting the global electronics parts supply chain, including the challenges surrounding counterfeit mitigation. Via reporting by its membership – in a similar way to GIDEP – ERAI maintains a global knowledge base and alert system focused on counterfeit and nonconforming component mitigation. However, it is not free to join, and membership costs vary depending on the size of the member company and the level of information companies wish to access. While anyone can submit a report, only members can access them or receive alerts.

Section G.1 of the AS5553 standard also provides a full list of other government organizations that may need to be notified in order to facilitate criminal prosecution. In short, the consequences of counterfeit components finding their way onto the field are so potentially grave for contractors of all sizes, not to mention for the men and women who depend on their products, that companies will definitely find a great deal of resources and guidance at their disposal as they attempt to implement counterfeit-mitigation programs.

Counterfeits on the production floor

A company has come across suspected counterfeit components – what should it do next? The company must follow its own internal procedure for segregating and containing the suspected nonconforming parts, but any procedures should include the following:

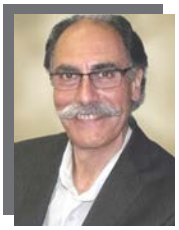
1. Segregate and quarantine the parts. Remove any parts in stores and on the floor, look for date codes, and identify all lots of potential parts in products that were already shipped to the customer.
2. Confirm the finding of counterfeiting.
3. Contact the part supplier. Notify the source of the suspect components that have been discovered. Tell them why the company believes that the parts may not be what they purport to be; such reasons could be and often are visual ones – the wrong-color components; a sloppy silkscreen, date stamp, or other information; marking stamps that do not conform to a known format,

and the like. Allow the part supplier to investigate the issue; if unsatisfied with the investigation, proceed to contact the part manufacturer.

4. Contact the part manufacturer. Let the manufacturer know that the company believes it is holding parts supposedly manufactured by them that are suspected of being counterfeit. Send the manufacturer samples of the suspect parts, and ask them to confirm the findings. If the manufacturer confirms the findings of counterfeiting, proceed with customer notification.
5. Notify the customer. Companies of course dislike being in the unenviable position of having to notify their customers that they may have accepted or even fielded counterfeit parts. As unpleasant as this will be, companies can take heart in the fact that their customers will ultimately appreciate any reliability and transparency regarding counterfeit information; this then enables customers to take their own internal and external steps to mitigate the problem.
6. Notify GIDEP and ERAI, which amount to crowdsourced knowledge bases for all members of the A&D industry. Without openly shared information, such knowledge bases would rapidly cease to be useful, so companies must take the time and responsibility to pass on their findings.

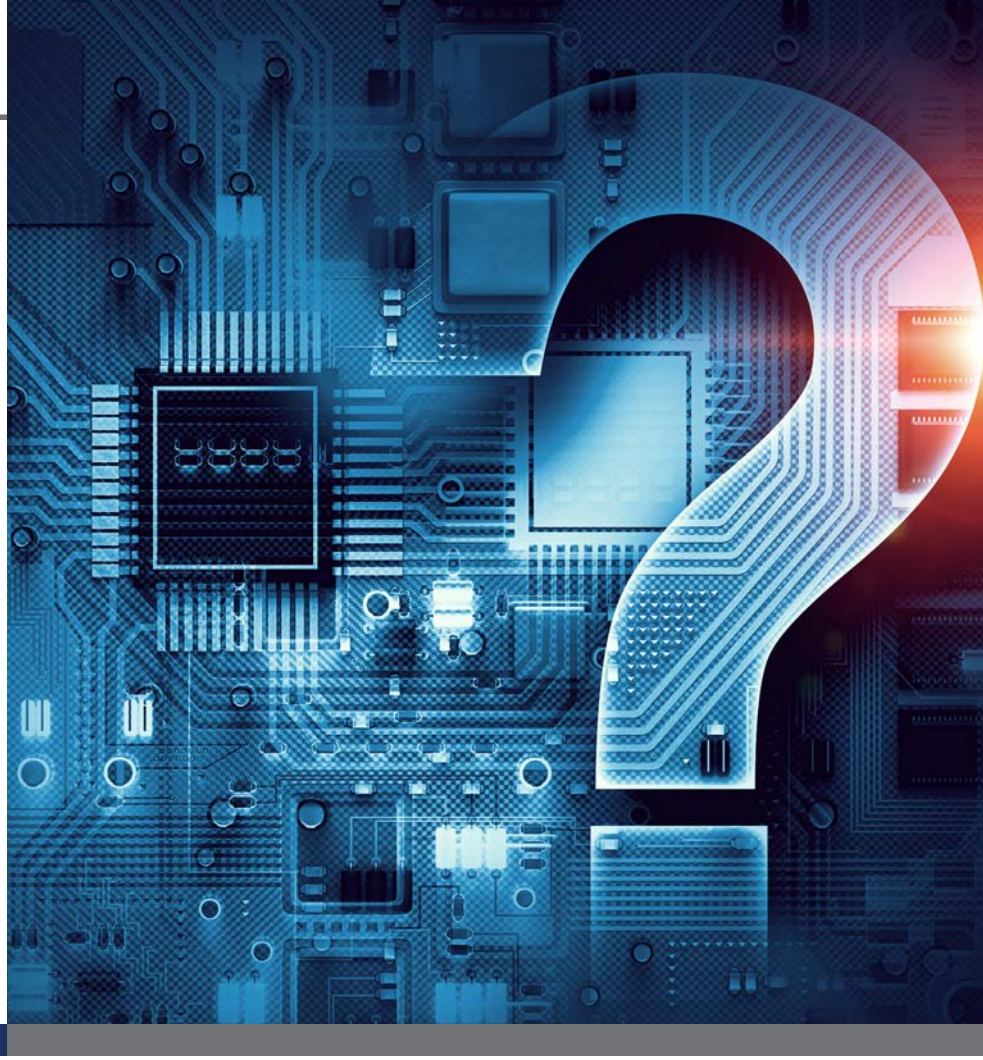
Going forward

It's all about preparedness and vigilance. As a company adheres scrupulously to well-documented counterfeit-mitigation procedures, it will begin to build a reputation for trustworthiness and transparency in the industry, and will gain reliability with customers that will stand it in excellent stead in the future. Counterfeit mitigation takes time and energy to put in place but once it is incorporated and part of an organization's culture, a company has created the most powerful tool to ensure the safety and reliability of its equipment and products – and ultimately the safety of the warfighter. **MES**



Shmuel Yankelewitz *is the Chief Operating Officer for LCR Embedded Systems. He obtained his MS in electrical engineering and MBA from Drexel University before joining Litton Special Devices in 1991. In 1994, he joined LCR Electronics Inc. and has remained with LCR Embedded Systems as Chief Operating Officer and Partner/Owner. A member of IEEE, he is experienced in strategic planning, organizational structure, operations and material management, manufacturing, engineering, and production. Readers may reach the author at syankelewitz@lcrembedded.com.*

LCR Embedded Systems
www.lcrembeddedsystems.com



Counterfeit components: The stakes are rising

By Rich Fitzgerald

One of the greatest risks to the welfare of not only U.S. service members, but all citizens around the world, is the proliferation of counterfeit electronic components into the military and aerospace supply chain. With the growing adoption of Internet of Things (IoT) technologies within practically every conceivable market segment, this risk is growing by orders of magnitude. Every person in the component supply chain should be doing their best to put an end to the counterfeit scourge before we find ourselves face to face with a systems failure or breach, driven either by greed or maliciousness, that could cause irreparable harm. All segments in the supply chain of things must take responsibility to eliminate this challenge.

In December 2015, three Chinese nationals were arrested in the state of Connecticut and charged with theft of sophisticated military-grade semiconductors. The trio had conspired to replace 22 military-grade Xilinx semiconductors in inventory for the U.S. Navy with fake components that would "look the same" but were "not ok for function." Fortunately, the naval official with whom they were attempting to conduct this illicit transaction was actually an undercover agent with the Department of Justice (DoJ).

The DoJ had been tracking the trio's criminal activity since 2012, when they received a tip from an employee of a manufacturer of counterfeit integrated circuit (IC)-detection equipment who met one of the defendants at a trade show and was troubled by the "suspicious and unusual questions" he was asking about the detection equipment. Had this individual not followed his gut and reported the peculiar activity, there is no telling how deep this counterfeit ring could have penetrated into the naval supply chain, or how many lives may have been lost as a result of the installation of those malfunctioning chips into critical defense systems.

True crime

Despite the billions of dollars in economic loss reportedly tied to the sale of counterfeit electronic components each year, the level of awareness and willingness to "get involved" demonstrated by that detection-equipment representative remains regrettably rare.

Perhaps it is because the losses are generally deemed part of the "cost of doing business," like pilferage in a candy store. This thinking, however, is not just short-sighted, but dangerous, and getting more so every day.

According to Interpol, the world's largest international police organization, "a clear link has been established between the trafficking of illicit goods and transnational

organized crime." These criminal enterprises use the profits they "earn" from the sale of counterfeit products to fund other nefarious activities such as drug trafficking, human smuggling, and arms dealing. These are not hapless con men selling cut-rate components out of the back of a truck. We are talking about seriously ruthless and highly organized criminals.

Of course, many say that any professional purchaser would be able to tell if a parts broker was really a front for organized crime. Well, as the saying goes, the devil wears many masks, and when it comes to disguises, counterfeiters can be masters of deceit. For example, in 2004, counterfeiters set up an entire bogus company using the NEC brand. They carried NEC business cards, signed production and supply orders, and even developed their own line of consumer electronic products marketed as NEC merchandise. Although most of the fake NEC products were finished goods, as opposed to board-level components, it is easy to see how one could be fooled into thinking they were dealing directly with legitimate NEC sales representatives.

This is why buyers must constantly be on alert, especially when sourcing from online parts brokers or from suppliers in regions that do not have the same rigid intellectual-property protections and enforcement that we take for granted in the U.S. Any organization that is honestly committed to maintaining the integrity of the electronics supply chain will take the time to scrutinize an unknown source, insist on documentation of a part's lineage, and always test parts before installing them in a design. This is as crucial for members of the commercial supply chain as it is for those in the military/aerospace sector. The industry cannot protect the high-reliability supply chain without protecting and securing the commercial supply chain as well.

Bad to the bone

Further complicating the counterfeit dilemma is the fact that economic gain is not always the primary motive for parts tampering. We are hearing more and more about the risk of malicious counterfeits making their way into the supply chain. Unlike "traditional" counterfeit parts that are reclaimed, remarked, reengineered, or otherwise fraudulently represented, malicious counterfeits are intentionally altered during the IC design process to insert malignant functionality – hardware Trojan horses, kill switches, etc. – into the code before it is manufactured. This tainted code may be triggered to launch a cyberattack in order to intercept classified intelligence, compromise critical infrastructure capabilities, or disable weapons systems. What makes these devices so insidious and difficult to identify is that they typically function as they should and are likely to be produced and sold by the original manufacturer; hidden within, however, is malicious functionality that

is unlikely to be detected via standard inspection and testing protocols.

So while in the past hackers labored to exploit security gaps that might exist in corporate IT and homeland-security networks or strategic weapons systems, today the gaps they are exploiting are instead in the integrity and security of the supply chain. For the most part, current anti-counterfeit defenses often prove inadequate against these back-door threats, as the vast majority of the safeguards within the supply chain are predicated on the assumption that profit is the end game of these perpetrators; therefore, detection strategies focus on the identification of parts that have been reclaimed, remarked, re-engineered or otherwise fraudulently represented.

With widespread adoption of IoT-enabling technologies increasing the connectivity between the systems in which these components are deployed, the potential for extensive economic and health and safety losses due to deliberately corrupted components increases by orders of magnitude.

Efforts to better protect ICs from tampering during the design and manufacturing process, such as the Department of Defense's Trusted Foundry initiative and the European Commission's Project UNIQUE have made great progress toward the development of an integrated approach to protect hardware systems against counterfeiting, cloning, reverse engineering, tampering, and insertion of malicious components. However, these are small steps in a very long and arduous journey.

One step forward, two steps back

DoD initiatives, including the Defense Federal Acquisition Regulation Supplement (DFARS) Case 2014-D005, for the detection and avoidance of counterfeit or suspect counterfeit electronic parts in the defense supply chain, have also made some inroads. Like all too many bureaucratic programs, execution often falls short of expectations. In fact, according to a February 2016 report from the United States Government Accountability Office (GAO), a significantly lower number of counterfeit parts reports have been submitted to the Government-Industry Data Exchange Program (GIDEP) since the DoD implemented the landmark section 818 of the National Defense Authorization Act (NDAA). The report cites insufficient "department-level oversight to ensure that all defense agencies are reporting in GIDEP," as a major flaw in the current process.

FEDERAL GOVERNMENT STATUTORY GOALS
23 percent of prime contracts for small businesses
5 percent of prime and subcontracts for women-owned small businesses
5 percent of prime contracts and subcontracts for Small Disadvantaged Businesses
3 percent of prime contracts and subcontracts for HUBZone small businesses
3 percent of prime and subcontracts for service-disabled veteran-owned small businesses

Source: Small Business Administration, www.sba.gov

Table 1 | Federal government statutory goals.

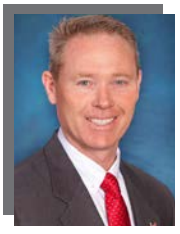
The GAO recommends that the DoD more actively "oversee its defense agencies' reporting efforts, develop standard processes for when to report a part as suspect counterfeit, establish guidance for when to limit access to GIDEP reports, and clarify criteria to contractors for their detection systems."

While there is no doubt that rules without enforcement are generally ineffective, the solution may not lie in the establishment of even more regulation. In fact, ill-advised government policy is at least partially responsible for the poor results from the DFARS rule to date; specifically, the practice of "goaling," which, according to the Small Business Administration, is designed to "ensure that small businesses get their fair share of work with the federal government." (See Table 1 for a sampling of the statutory goals established by federal executive agencies.)

Small and minority-owned businesses play an important role in the U.S. economy; this is not to suggest that these enterprises should be precluded from participating in government contracts. However, there is much pressure placed on these small businesses, which the DoD must address for these companies to be successful at supporting the government.

No more excuses

If there is one thing that will guarantee that counterfeit components continue to infiltrate the electronics supply chain, it is inertia. Whether due to a fatalistic belief that nothing can really stop these criminal networks or as a result of overwhelming scheduling and budget pressures, too many members of the supply chain continue to engage in risky sourcing behaviors without consideration for the long-term consequences. Until that changes, nothing else will. **MES**



Rich Fitzgerald *is vice president, business operations, of Avnet Embedded. Rich was an officer in the U.S. Marines for more than 12 years and has previously served as the COO of Qual-Pro Corp. and the CEO of Team Precision Public Company Limited; he also has held multiple manufacturing and operational excellence positions with Intel Corp. Rich has a bachelor's degree in business management from the University of Maryland – Robert H. Smith School of Business.*

Avnet
www.avnet.com

Acromag
THE LEADER IN INDUSTRIAL I/O

PCIe-Based Next Generation AcroPack™ I/O Modules

For the next 25 years

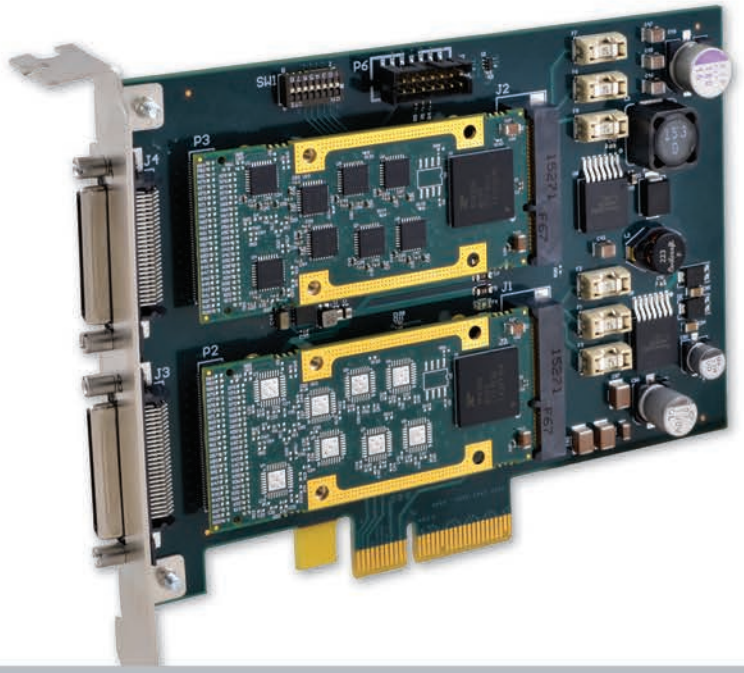
Acromag.com/AcroPacks

AcroPack™ mezzanine modules deliver maximum I/O density when used with AcroPack carrier cards for PCIe or VPX-based systems. Combining different AcroPack module types on one carrier allows for a simplified modular approach to system assembly.

Designed for COTS applications, these general purpose I/O modules deliver high-speed and high-resolution A/D and D/A, digital I/O, serial communication, and re-configurable FPGA functions.

Key Features Include:

- Mix and Match 100,000 I/O combinations in a single slot
- Create your own custom I/O combination
- VPX and PCIe carriers
- Linux®, Windows®, and VxWorks® support
- Sample software and diagnostics
- Solid Down connector I/O interface (no flimsy ribbon I/O cables)
- -40 to 85°C standard operating temperature
- A/D, D/A, Serial, Digital I/O and FPGA



Embedded I/O Solutions

FPGA Modules
Acromag.com/FPGAs

I/O Modules
Acromag.com/EmbeddedIO

VME SBCs
Acromag.com/Boards

SFF Embedded Computers
Acromag.com/ARCX

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

MADE IN USA ISO9001 AS9100

Rugged, smart displays enhance warfighter performance

By Mariana Iriarte, Associate Editor

Designers of rugged military displays are looking to leverage innovations from the commercial world such as touch screens and 4K technology to enhance situational awareness for the warfighter. The challenge is finding ways for displays with the commercial capabilities to meet strict military requirements for harsh environments.

Systel's FPC5106, a 10.6-inch LCD display with up to 28 programmable function buttons. Photo courtesy of Systel, Inc.

A rugged display may seem like a small part of the overall battlefield-equipment picture, but it has become a critical part of any air, sea, or ground platform as the main tool for delivering intelligence surveillance, and reconnaissance data to warfighters, helping them make faster, smarter decisions. Rugged displays that users will see in the next few years will start to leverage some of the innovation seen today in the commercial market such as touch-screen technology and 4K capability.

Displays are essentially evolving: This means that "you're starting to see more smart displays that are more computer-based display terminals," says Ross Hudman, sales and marketing manager at Digital Systems Engineering in Scottsdale, Arizona. "These displays have memory, have storage devices, so they are now combining a computer and a display. I would say that's a trend specifically more for land vehicles."

For example, "There's definitely going to be a transition to the way flat panels and LCD displays are used," says John Wade, founder and CEO of Z-Micro in San Diego, California. "We're seeing organic LEDs just starting to emerge in the commercial market and those are going to transition to the military," Wade says. "Even further out, maybe ten years out, we're going to start seeing flexible displays. So we'll start possibly seeing displays that can be rolled and unrolled just like something out of Star Trek. It's amazing how reality emulates science fiction."

A rugged touch

The big challenge will be how military designers adopt new technologies, such as infrared touch screens, says Benjamin K. Sharfi, founder and CEO of General Microsystems in Los Angeles, California. "To me, that's where you will see the next leap, moving from existing architecture technologies that we have, to the next generation. Even it if shatters slightly, you can still see it and use the touch screen. In infrared displays, sensors are embedded all around the display and it detects the breaking of the beam at a specific point or multiple points, so you can still use multitouch capabilities."

With touch-screen technologies, system engineers must take into account that "the military is often wearing gloves," says Roy Keeler, president of MilDef America in Washington, D.C. "And you can't use capacitive screens, so one of the trends that we see is using resistive-type screens that allow you to put pressure on the screen and move the cursor to an area of interest on the screen," Keeler says.

The military is craving and asking for what the commercial world has been enjoying: "Most of the commercial market now is using multitouch capacitive-type screens

Figure 1 | The MilDef DS11 10.1-inch tablet has an IP65 rating. Photo courtesy of MilDef.

on their PDAs and on their handheld devices. That's the stuff that allows us to do our pinching and swiping on our phones," Keeler comments. That technology is seen with MilDef's DS11 tablet, which has a 10-inch capacitive multitouch display and comes with an Intel i7 CPU. (Figure 1.)

Displays like Systel's FPC5106 (see lead image) has "customizable function buttons and is multitouch screen-resistive.

RUGGED DISPLAYS THAT USERS WILL SEE IN THE NEXT FEW YEARS WILL START TO LEVERAGE SOME OF THE INNOVATION SEEN TODAY IN THE COMMERCIAL MARKET SUCH AS TOUCH-SCREEN TECHNOLOGY AND 4K CAPABILITY.

That's something that we get asked for – that the touchscreen capabilities are multi-touch-resistive so that they will work with gloves as well as styluses because that can be an issue in certain environments," says Aneesh Kothari, marketing manager at Systel in Sugar Land, Texas.

Network-centric displays

The future of displays always includes the extension of video. "A game-changing technology," Hudman says, "will be wireless video. These network-centric ideas of having everything communicate over Ethernet. It's in the early stages, but I think in ten years it will be there."

Even virtual displays are making the race to be used soon, on the wearables side of technology: "Virtual display might be something that a warfighter would wear, which would overlay battle data on top of the existing environment," Kothari says. "As they're moving around in a battle situation, they have data right there."

As with every smart technology on a network, cybersecurity will be a requirement. "Historically, we would have a lot of what we would call dumb displays. As we move into more smart displays where they have a computer, you have to make sure that all the data is on there is encrypted and secure," says Hudman.

Digital Systems Engineering's LCD rugged monitor, which carries the IP67 rating, displays 1080p high-definition video during operations and has HDMI and DVI inputs. (Figure 2.)

Smarter displays, smarter warfighter

No longer are screens one-dimensional; the idea is to have "smart all-in-one displays, versus just monitors. A lot of rackmount applications may just want an LCD monitor and will plug that into a rackmount server and that is how it's powered," says Kothari. "Other applications – like vetronics applications, where it is panel-mounted, almost like tablets, but they are military, rugged, kind of small 10-inch displays – have to be an all-in-one display, that has to be smart with a touch screen and with some power behind it. All that included and [the display] still come in a small form factor because you don't have a huge rackmount-type area to put in with motherboards, servers, and CPUs." Moreover, says Z-Micro's Wade, "With the emergence of new high-resolution displays, our customers are looking for higher pixel density. That factors into 4K displays but also smaller displays with greater resolution."

While most of this technology is still years away, one thing is certain, Kothari continues: "Today's generation is so comfortable with [the technology], I don't think from that perspective, it'll be a hard adoption. Now, of course, from a logistics perspective, and actually placing that and having that as part of the infrastructure, that's very different and that's where the trick is."

Passing the test

No matter how amazing the features on new smart displays, they still must pass a series of tests and meet certain extreme requirements in order be qualified for battle.

Testing on these displays ranges from subjecting them to gunfire vibration to submerging them in water to brutal blunt-force challenges. Testing also varies between platforms, depending upon whether the end use is in an aircraft, onboard a ship, or on the ground with troops. Innovations are now emerging that bring modern-day smart display to the military services.

Engineers consider the platform before testing rugged displays because – depending on whether it's land-based, sea-based, or air-based – "what we find for each of those is that the requirements vary depending on the type of platform [the display] will be mounted upon," MilDef's Keeler says.

Warfighter mobility moves to the cloud

Mobility for the warfighter is no longer driven by size, weight, and power (SWaP) benefits, but by the data that resides in the cloud. As technology matures, the warfighter will only need a secure network to move from platform to platform and stay connected to the mission at all times.

"Let's take the special operations forces, they're looking at actually having computer identity modules that are about the size of a credit card that you can actually plug into a device, be it your handheld communications device, your PDA, or your laptop," explains Roy Keeler, president of MilDef America in Washington, D.C. "You can just take that with you and go to another location, go to another platform, plug it in, and all your protocols are loaded, all your identity is loaded, and you're on the network with that particular platform."

The physical aspects of each electronic component are now irrelevant. The difference now is that "every vehicle that is equipped with electronics has its own unique signature. What it does, based on the person and his credentials, is it gets you behind a system," says Benjamin K. Sharfi, founder and CEO of General Microsystems in Los Angeles, California. "So every commander has his own credential media that he logs in with, and an entirely different profile code. Their mobility is in the cloud now. It's not like the old days when you had to move your applications to different areas. Your application resides in a cloud and that's what makes this serviceability, upgradability, and maintenance extremely economical."

Figure 2 | Digital Systems Engineering's ultra-thin High Definition Rugged Monitor (HDRM) displays up to 1080p HD video during operations. Photo courtesy of Digital Systems Engineering.

When it comes to shipboard applications, typically, the weight is not the primary driver; it's more ruggedization, Wade says. "There are requirements to meet higher shock levels. The 901D grade-A shock, for instance, is very specific to our shipboard customers."

General Micro System's SD19 rugged smart display is one example where engineers completed the MIL-S-901D shock testing. "With the Navy, it is completely different. Vibration is really not an issue, but imagine you're taking a torpedo. The display has to be able to take a tremendous amount of peak shock and it has to be able to withstand and continue to be operational," Sharfi says.

In this case, Sharfi explains, the SD19 display (Figure 3) "was slammed over and over again by a 400-pound hammer from five feet in the air. The noise of the strike was deafening and its impact shook the ground, but throughout the test the SD19 remained not only intact but completely operational."

Testing displays for aircraft

"Conversely, for our aircraft customers, there's flight-safety requirements that we have to meet and electromagnetic interference (EMI) requirements that are quite stringent," Wade says. The

Figure 3 | The SD19 RuggedView smart display has a hardened 4:3 aspect-ratio touch screen and an LCD. Photo courtesy of General Micro Systems.

standard MIL-STD-461 tests for electromagnetic compatibility – with the latest revision being MIL-STD-461G – and it is one of the "requirements to follow that will ascertain there is no interference or susceptibility to radios.

"Aircraft applications have stringent requirements due to the radios and the electronics that are part of airborne assets. So there's an additional effort involved for the EMI for airborne platforms," Wade continues.

Requirements even change within each specific asset; for example, "you have slightly different requirements where usually, depending on the type of aircraft, whether it is fixed-wing or rotary-wing, the shock and vibration requirements change," says Keeler.

Meeting MIL-STD-810F

Rugged displays that undergo these tests will enable the warfighter to have a system that will last through routine use as well survive any harsh environment.

MIL-STD-810F "covers anything from shock, vibration, temperature, fungus, humidity, blowing dust – all of those," Hudman says. "It comes down to making a product that is fully sealed, and won't take in dust and water. It comes down to a product that is designed so that all the components stay intact and operable after shock and vibration.

"Just recently, for the combat rescue helicopter, our nine-inch HD display was put through general and gunfire vibration. The profile we were subjected to imitated a component that was on the drive shaft of the helicopter," Hudman explains. "The most stringent profile found within the procedure of the MIL-STD 810F: We literally put our display through it, mounted it to the test fixture, and it shook it so hard that there were audible tones that you could hear throughout the building, so loud that you had to cover your ears."

Another type of testing that displays undergo is the boot-kick test, in which the display is supposed to withstand a kick of a soldier's boot. However, Hudman states, "at the end of the day, you always have glass in front of the display and those will never withstand a severe blunt-force shock."

Testing displays for shipboard environments is not as harsh a process as it is for other environments. It is "slightly less rugged than you would have on either a ground vehicle or an aircraft," Keeler explains. "In ships you need to have an IP67 type of enclosure, which keeps out water and dust." A display needs to be submerged in water for at least three minutes in order to have the IP67 rating. **MES**

Moving virtual systems into the field

By Dave Lippincott

Implementing servers for harsh field-environment applications can be a complex task. Whether the location is a Navy ship, a desert tent, or a shelter in the Arctic, users need a ruggedized server that can function in a harsh environment. Users can achieve reliable system implementation by both focusing on design issues from the very beginning of the process and working with an established provider of ruggedized servers.

Data-center services are often needed in harsh field-environment conditions including extreme heat or extreme cold. In this photo, combat rescue officers and pararescue officers arrive to deliver supplies during Ice Exercise 2016 on Ice Camp Sargo, a temporary station on an ice floe in the Arctic Ocean, March 15, 2016. The U.S. Navy and other U.S. and partner-nation organizations conducted the five-week exercise to research, test, and evaluate operational capabilities in the region. Navy photo by Petty Officer 2nd Class Zachary Yanez.

Servers are increasingly moving beyond the traditional data center – many users now require data-center services in the field, which can often mean harsh environments. An example of this necessity is the military requirement to move users to zero or thin clients with access to servers running virtualized applications. Virtualized systems in the data center have become commonplace and are becoming even more popular as users realize that there are cost savings, performance improvements, and maintenance benefits to be had from virtualization software. Data centers are designed to support large installations of servers supporting many applications and are environmentally controlled with state-of-the-art cooling and clean 24/7 power sources.

Driving the military conversion to secure thin- and zero-client computing has been the U.S. Army's 72-page document, "U.S. Army Thin/Zero Client Computing Reference Architecture, Version 1.0, 14 Mar 2013," which promotes the conversion away from desktop and laptop computers to centralized servers and thin-/zero-client architectures.

Moving the server out of the data center into the real world – one that is hot, humid, salty, sandy, and full of vibration and shock – is a challenge and requires a system designed for the environment. Organizations will be required to look beyond the standard commercial data-center server in a 1-4 U sheet-metal enclosure – they need a better-designed system.

Virtualization in the field

The military is actively switching to zero and thin clients in the field connected to servers running virtualization suites such as VMware. Along with virtual servers used to support multiple applications, there is also a need for servers to support network function virtualization (NFV) in the field. NFV enables a smaller amount of hardware by eliminating specialized routers and switches by moving the software into a server. Software can then provide specialized network functions like routing and security and can also be easily upgraded in the future.

Developing requirements for a ruggedized server can be a confusing task for those used to specifying standard computer equipment for a data center. The server must be able to survive the field environment as well as withstand the trip to the field, as the trip to the remote location can be as hazardous as operating in the actual location.

The key features to look for when defining a system are the overall design and packaging, shock and vibration specifications, cooling, and overall performance. Since the system is designed to be a server, the same electronics components used in high-end data center servers are required, with the only difference that they are more robustly packaged. A typical 1-4 U server designed

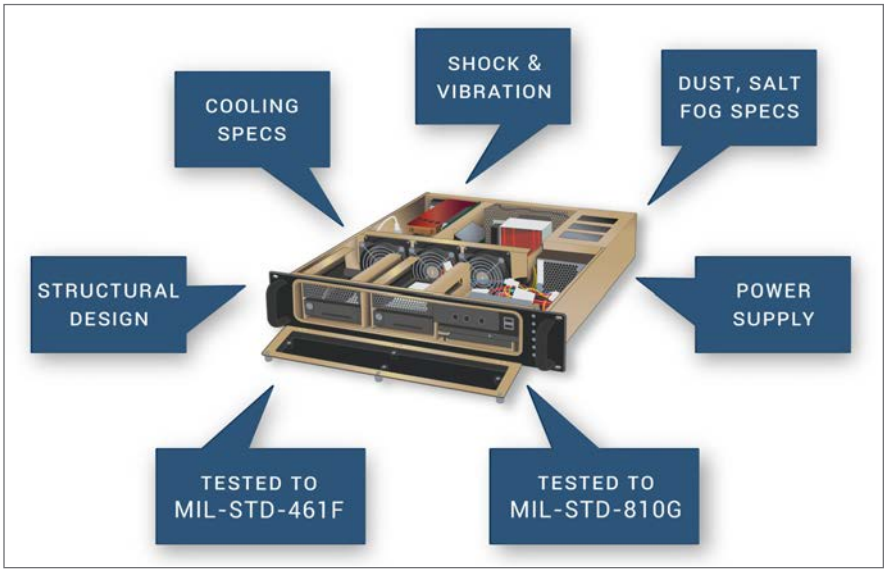


Figure 1 | Major system and test requirements for a ruggedized server.

for rugged military use would support multiple Xeon processors, 32 to 256 Gbytes or more of memory, rotating or solid-state disks in a RAID configuration, and multiple network connections. The key for a well-designed system: How to protect these components in severe environment.

System specifications for harsh environments

A multitude of specifications can be used to specify system design and testing, but the most commonly used is MIL-STD-810G. Although this standard was developed with military applications in mind, it provides a good baseline for specifications needed for any extended environmental environment. MIL-STD-810G addresses a broad range of environmental conditions that include low pressure for altitude testing, exposure to high and low temperatures plus temperature shock (both operating and in storage), rain (including windblown and freezing rain), humidity, fungus, salt fog for corrosion testing, sand and dust exposure, explosive atmosphere, acceleration, shock and transport shock, and vibration. The standard describes environmental-management and engineering processes that can be of enormous value to generate confidence in the environmental worthiness and overall durability of a system design.

For applications that require electromagnetic interference (EMI) protection, MIL-STD-461F describes how to test equipment for electromagnetic compatibility. While MIL-STD-461F compliance is technically not required outside the U.S. military, many civilian organizations also use this document. Even if the potential application does not require MIL-STD-461F, if a device complies with, or is very close to complying to, MIL-STD-461F, then it is certain to comply with the FCC Part 15 and EMC standards of other countries. It is simpler to run one test than to run a separate test for each EMI-compliance requirement.

Features of a rugged server

When considering a new server for a ruggedized application, whether for a military or industrial environment, there are several items to look for: In the basic metalwork, the chassis construction should be good quality. Use of high-quality 5052-H32 aircraft-grade aluminum for its strength and lower weight is a good choice. In addition, a solid front-panel design milled from a solid block for strength is another example of a good design practice. Another aspect: The front panel and any access panel on the system should be sealed with an EMI/environmental gasket. Finally, all hardware should be high-quality stainless steel that is self-locking to provide the best shock, vibration, and corrosion resistance. (Figure 1.)

Also of concern is air flow and cooling. Since the system will probably not be in a well-controlled environment, the ability to cool and provide clean air at the proper air flow rate is required. The system should have long-life, high-reliability, high-velocity fans with an intelligent fan controller designed to determine air flow requirements based on load and external temperature. Just as important as the fan is the need for clean inlet air since there will be dirt and dust in the environment. The use of air filters on all air inlets is required with an EMI filter to eliminate any electromagnetic interference, in compliance with MIL-STD-461F.

In addition to the packaging and cooling design issues, another key factor is the power-supply design. In some instances there is normal input power available to power the server, but in many cases generator power is the only power available. A rugged server design will have redundant power supplies with a wide range of input power requirements. Normally the range will be 100 to 240 volts AC/50 to 60 Hz with auto switching, but most designs will allow for special input voltages, such as 28 VDC, and additional frequencies as required. The input of the power supply will be robust enough to handle line transients and short power drops.

Shown in Figure 2: To illustrate server effectiveness for military applications, a standard Chassis Plans 4U ruggedized server was placed on a barge for the Navy MIL-S-901D barge test. The test consisted of placing 60 pounds of explosives 20 feet from the

Figure 2 | Navy barge test of 4U rugged server. Effect of 60 pounds of explosives 20 feet from barge and 24 feet deep in the water. (Photo courtesy Chassis Plans.)

Figure 3 | Pictured is a shock-mounted 6U transit case from Chassis Plans that supports a 2U military-grade server with two multicore XEON processors, multiple PCIe expansion slots, a RAID storage unit with as much as 48 TB of disk storage, a UPS/power conditioner for assured operation in power-poor environments, and a military-grade rackmount keyboard/LCD display. (Photo courtesy Chassis Plans).

barge at a depth of 24 feet. Four explosions were detonated at various distances from the barge. The server was operational during all four tests and no repairs or modifications were required.

Once the system design specification is complete, consideration has to be given to ease of setup and shipping. In most field applications, the system must be set up and operational quickly using simple tools and without expensive assembly. This demands design features such as captive screws for all accessible panels as well as all electronics installed at the factory.

In order to ensure that the equipment survives shipping, the system design must provide support for the electronics as well as the subsystems. Typically, disk drives will be shock-mounted and, if possible, the system itself will be shock-mounted in the shipping container or transit case. The example shown in Figure 3 shows a system installed in a transit case designed for shipping electronics equipment. An additional advantage of this type of container is that it allows the equipment to be operated while in the transit case and the containers can be stacked for larger installations. By using aircraft-grade aluminum for the design, the weight is minimized; a fully loaded transit case can be handled by just two people.

Although procurement for a standard commercial-grade server is simpler, total cost of ownership for a rugged application will be higher because of reduced reliability. Operating a ruggedized server is the same as a commercial server since the same administration and virtualized application software is used for both. **MES**

David Lippincott *is founder and chief technology officer at Chassis Plans, which provides custom industrial and military computer designs. Chassis Plans is also providing the rugged computers for the persistent surveillance aerostats for the 2016 Summer Olympics to be held in Rio de Janeiro, Brazil. Mr. Lippincott can be reached at davidl@chassisplans.com.*

Chassis Plans • www.chassisplans.com

Clock-throttling isn't the answer: Innovative thermal design supports real-time military application needs

By Rick Neil

Extended-temperature environments – like those often encountered by Army vehicles outfitted with the latest generation of the Warfighter Information Network –Tactical (WIN-T) – are a challenge for designers of today's powerful processors. U.S. Army photo by SSG John Briggs, 22 SBCT.

The extended temperature requirements of many military applications often mean slowing down the clock of a hot CPU. Clock-throttling of today's powerful processors works against military users' needs for high performance, but reliability and size/weight requirements of typical systems leave them few other valid choices. Instead, innovative cooling-system design offers the full advantage of high-performance processors without running over the device's recommended temperature range.

Multicore processor architectures offer high-performance computing platforms that are optimized for the size, weight, and power (SWaP) requirements of defense and electronic warfare (EW) programs. The challenge, however, lies in designing a conduction-cooled platform that maximizes processor performance and does not compromise system reliability in extended-temperature environments.

Processor clock-throttling – a feature of modern processors that reduces the operating frequency of the processor in response to over-temperature conditions – has become an accepted design practice when operating over the industrial temperature range of -40 °C to +85 °C. However, for military customers of mission-critical, real-time applications, this approach may be unacceptable when lives are at risk, such as in systems using gunfire-control systems, EW countermeasures platforms, or radar high-power attach-mode operating systems.

Rugged system designs that employ clock-throttling are typically a patchwork application of external temperature sensors, thermal gap-pads, heat sinks, and metal cooling plates that provide a near-non-clock-throttling solution that yields a temperature delta of 20 °C to 25 °C between the rugged system's processor core and the system's cold plate (the system's conduction-cooling interface). The challenge is to design a thermal management solution that minimizes clock-throttling but prevents the processor from operating at temperatures beyond its rated temperature limits. Qualitatively, this is not a bad thermal solution, but quantitatively it is not optimal.

A better option is a top-down, conduction-cooled, true non-clock-throttling design with a thermal delta of 10 °C between the rugged system's processor core and cold plate over the industrial temperature range of 40 °C to +85 °C. This design enables military applications to take full advantage

of high-performance processors without operating beyond specified system temperature limits or diminishing system reliability.

The thermal delta design challenge

To minimize clock-throttling while staying within the operational temperature limits of the processor, most system designers employ a disjointed amalgam of thermal gap-pad, heat sinks, cold plates, and thermal sensors under software thermal-management control. These approaches are integral to any good thermal-management solution, but taken separately, each of these design elements have limits to minimizing the thermal delta at the interface between the base of the conduction-cooled system and the processor's die. Bottom line: the thermal delta is where the rubber hits the road.

Given that the maximum temperature at the base of a conduction-cooled system (thermal mounting interface) is 85 °C by specification, designers must produce a thermal-management solution that minimizes the thermal delta at the interface between the base of the conduction-cooled system and the processor's die. For example, a design that produces a thermal delta of 20 °C to 25 °C when operating in environmental conditions of extreme heat, with a processor that has a maximum die temperature of 105 °C, will be forced to de-rate or throttle the operating frequency of the processor in order to maintain die temperatures within manufacture's specification. Throttling will be required because for constant power dissipation, the thermal delta is constant. In other words, the thermal delta "tracks" linearly over the industrial temperature range of -40 °C to +85 °C. Therefore, if the base temperature of a conduction-cooled system under review is at +85 °C and the thermal delta for the system is 20 °C to 25 °C (up from the base temperature), then the processor will operate at 105 °C.

Processor clock-throttling in Intel Core i7 processors

Intel refers to the collective operation of sensors, microcontroller, and clock control as the Adaptive Thermal Monitor. When enabled, an autonomous controller within the processor dynamically adjusts or "throttles" the operating frequency of the processor to keep the processor die temperature at or below the maximum operating temperature. The clock-throttling feature can be disabled in Intel Core i7 processors via settings in the BIOS, but that enables the processor to free-run up to temperatures beyond the processor's guaranteed operational limits. To address this, an Intel Core i7 processor whose clock-throttling feature has been disabled will shut down at a highly elevated temperature of approximately +130 °C. This behavior is designed to protect the processor from catastrophic failure and damage due to a poorly designed system.

One important goal of a rugged, conduction-cooled system is to minimize the thermal delta between the base of the conduction-cooled system and the processor's die. On the other hand, if the thermal delta could be constrained to only 10 °C, the processor die temperature will be 95 °C when the base of the system is at the maximum industrial temperature of 85 °C. Over constant power operation, the CPU would not reach the maximum die temperature of 105 °C. (Note: Most modern processors are "cavity down" and the top of the CPU package is actually the back side of the CPU die. Therefore, Tcase and Tjunction (die) are treated the same.)

A new approach for minimizing the thermal delta

Another approach employs a corrugated alloy slug with an extremely low thermal resistance to act as a heat spreader at the processor die instead of the typical use of thermal gap-pads to conduct heat from the CPU to the system's interface to the cold plate. Once the heat is spread over a much larger area, a liquid silver compound in a sealed chamber transfers the heat from the spreader to the system's enclosure. This approach yields a temperature delta of 10 °C or less from the CPU core to the cold plate, compared with more than 25 °C for typical approaches. This approach also requires that all printed circuit boards (PCBs) be designed with multiple power and ground planes, with specific thermal-management techniques for optimizing the heat flow from the CPU and other

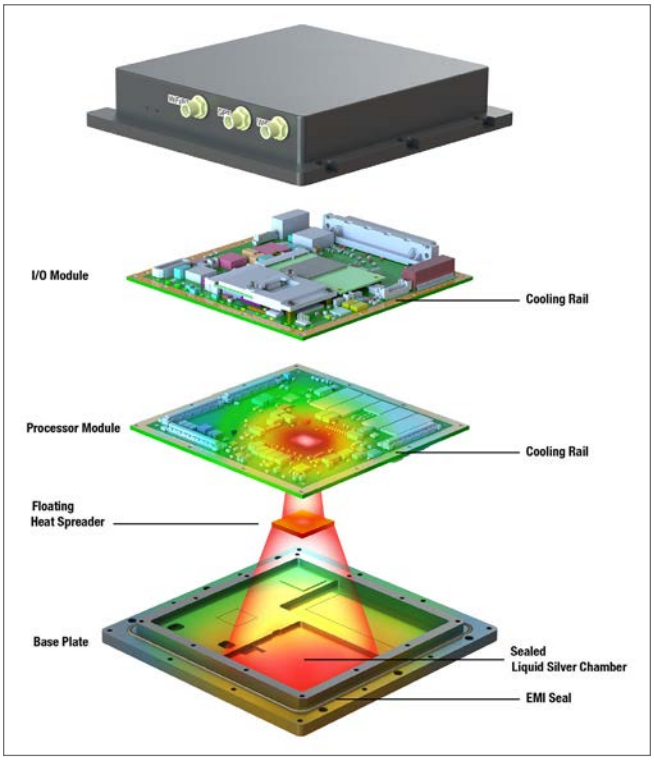


Figure 1 | An illustration of General Micro Systems' conduction-cooling system design.

high-power dissipation devices to the system's base. The base is the "base plate" as shown in Figure 1. In addition, internal and external thermal sensors that are monitored by layers of thermal-management software provide protection in the case of power spikes at unexpected processor loads. This multi-faceted approach enables systems using Intel processors with a TjMax of 105 °C to operate in an industrial temperature environment (-40 °C to +85 °C) at full operational load without throttling the processor.

Controlled experiment

We performed experiments on two configurations of rugged systems, one with the corrugated alloy design shown in the illustration, and the second without this technology, but with a carefully designed application of heat sinks and thermal gap-pads. In both experiments, throttling was disabled in BIOS settings and the onboard Intel Core i7 processors were loaded to 100 percent performance via third-party, off-the-shelf software. A typical profile for a formal thermal cycle as conducted in a controlled thermal chamber is illustrated in Figure 2.

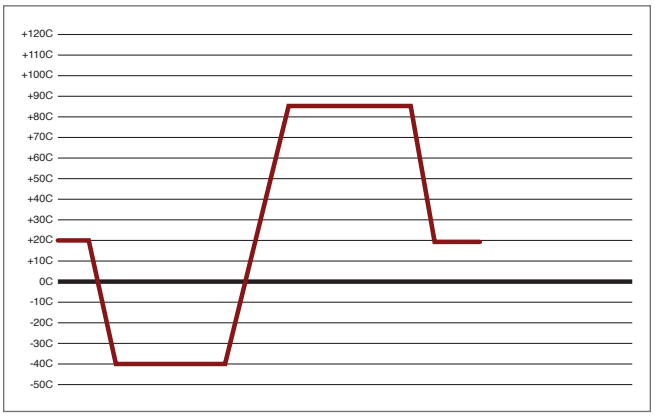


Figure 2 | A typical profile for a formal thermal cycle, illustrating the temperature of the base of a rugged system as measured by precision thermal couples. The flat part of the curves represent steady-state soak (dwell) times.

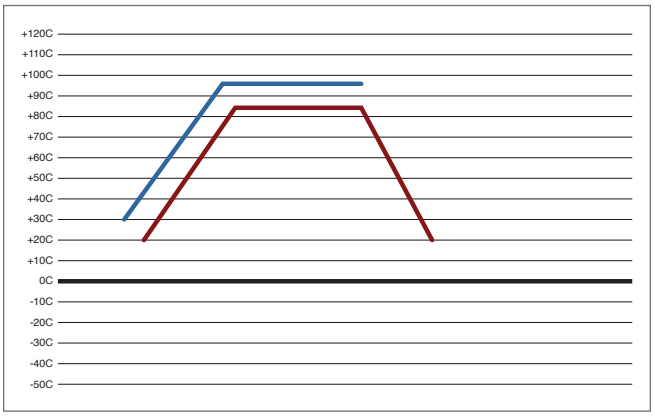


Figure 3 | An illustration of a 10 °C delta between the base and processor as measured on a military embedded system using General Micro Systems' conduction-cooled technology. The red line is a measure of the temperature of the system's base, while the blue line is a measure of the system's processor.

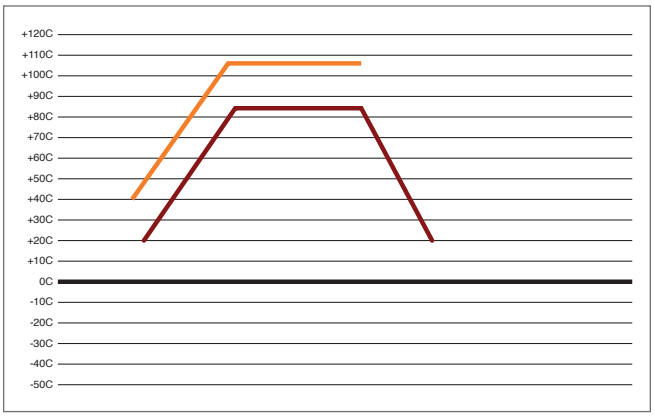


Figure 4 | An illustration of a 20 °C delta between the base and processor in a system using traditional heat sinks and thermal gap-pads. The red line is a measure of the temperature of the system's base, while the orange line is a measure of the system's processor.

For the newly designed system, the processor temperature tracked linearly at approximately 10 °C above the base temperature of the system (as illustrated in Figure 3) over the rising temperature cycle as shown.

In the second, conventional, configuration, the processor temperature tracked linearly at approximately 20 °C above the base temperature of the system, as illustrated in Figure 4. If throttling were enabled in the BIOS settings, this system would clock-throttle.

The application of the conduction-cool technology kept the processor temperature below the specified maximum when operating at 100 percent processor load and at a system base temperature of +85 °C while throttling was disabled.

It's clear that clock-throttling at maximum processor performance need not be an accepted design practice. A well-designed conduction-cooled system that minimizes the thermal delta at the interface between the base of the conduction-cooled system and the processor die maximizes processor performance without clock throttling. Moreover, this thermal performance meets the high-performance, high-reliability, and minimum-SWaP demands of military customers. **MES**

Rick Neil *is a senior hardware design and production engineer at General Micro Systems, responsible for the GMS flagship SB1002-MD and SB1002-MDv3 rugged computing systems. He has 25-plus years of military and commercial design experience at Xerox, TRW Space Systems, Rainbow Technologies, Hughes Electronics, Lockheed Martin, SAIC, and SCE. Rick holds a BS in electrical engineering with an emphasis in computer architecture from the California State Polytechnic University, Pomona. Contact the author at rneil@gms4sbc.com.*

General Micro Systems • www.gms4sbc.com

The commercial high-performance computing (HPC) market can be a good source of tools for designing innovative high-performance embedded computing (HPEC) systems.

Turbocharge HPEC system design with HPC development tools

By Tammy Carter

As parallel programming grows in importance and popularity, the critical challenge has become how to intelligently manage, develop, and debug the increasingly complex code. Traditional tools such as trace analysis, serial debuggers, and the venerable "printf" statement just aren't up to the task. Although some commercial off-the-shelf (COTS) vendors and customers in the embedded-defense space have attempted to develop their own parallel programming tools, the task has proved difficult and the resulting tools are far from full-featured. What's more, using proprietary development tools can add risk to a program's cost and schedule. The good news: A better source of tools for designing cutting-edge high-performance embedded computing (HPEC) systems already exists in an adjacent market – the commercial high-performance computing (HPC) market. Sourcing proven and powerful tools from the HPC community, long supported by an expansive user base, can greatly speed delivery time while decreasing costs and program risk.

The largest cost of developing a HPEC system for aerospace and defense applications is not the hardware, but rather the software. Research consistently shows at least 50 percent of programming time is typically spent debugging. The right tools can make all the difference. Using a comprehensive system debugger can help slash development time, reduce schedule creep, and eliminate cost overruns. Profilers can also be of great utility for HPEC system development because they help optimize and benchmark code and can perform regression testing. Another important tool for HPEC development is a cluster manager to help organize all of the nodes in the system. Taken together, debuggers, profilers, and cluster managers have become critical tools for creating a fully tested, validated, and benchmarked HPEC development environment.

The importance of these development tools has greatly increased in parallel with the availability of the latest generation of multicore central processing units (CPUs), graphics-processing units (GPUs), and field-programmable gate arrays (FPGAs). As the newest generation of devices has become the building blocks of choice for demanding embedded intelligence, surveillance, and reconnaissance (ISR) systems, the process of developing and debugging these systems has also become increasingly more complicated. This situation occurs because system designers tasked with taking full advantage of the processing power

COMMERCIAL AND MILITARY SUPERCOMPUTER SYSTEM DEVELOPERS FACE MANY OF THE SAME CONCERNS, INCLUDING FLOATING-POINT PERFORMANCE, THROUGHPUT, LATENCY, AND A PREFERENCE FOR STANDARD SOFTWARE APIs.

of next-generation devices to develop embedded HPEC "supercomputers" have found that their code must be executed in parallel across many nodes. High-speed serial coding techniques have proved inefficient when compared to programming the multiple independent and concurrent activities required to process the complex algorithms typically used in the radar, image, and signal processing jobs that HPEC systems perform.

HPC tools to the rescue

Over the past decade, the HPC market has evolved a mature and feature-rich set of software development tools that include math libraries, communications APIs, testing tools, and cluster managers. What makes these resources so appealing for the COTS market is the fact that the supercomputers used in commercial HPC applications, such as ultra-high-speed financial transactions and weather simulation, are built with the same hardware building blocks (processors, general processing units (GPUs), and fabrics) now used in the HPEC world. For example, the University of Texas's Stampede supercomputer is built with Intel Xeon processors and NVIDIA Tesla GPUs, also fundamental components of military HPEC systems. Commercial and military supercomputer system developers face many of the same concerns, including floating-point performance, throughput, latency, and a preference for standard software APIs.

For the HPEC system developer, cluster managers, debuggers, and profilers are the software equivalent of an oscilloscope, spectrum analyzer, and logic/network analyzer. As critical as the latter are for hardware development, these software tools are equally important for developing today's complex parallel HPEC systems.

Cluster managers handle system configuration

An HPC cluster manager saves time and money by easing the setup and maintenance of the system configuration. It also eases the strain on developer resources and scheduling by providing a simple method for sharing the lab-development system. Later, during the production phase, the cluster manager helps ensure quality and customer satisfaction by enabling exact duplication of the software images. A cluster-management system provides all the tools needed to build, manage, operate, and maintain a cluster in an HPEC system.

An example of a leading cluster manager, well-proven in the HPC market, is Bright Computing's Bright Cluster Manager. Using an intelligent cluster-management installation tool like Bright Cluster Manager for HPC enables the cluster to be installed, from bare boards to a full development system, in a matter of minutes. It can configure all of the system resources such as custom kernels, disks, and networks. Since the cluster manager supports image-based provisioning, kernel images can be maintained for different board types in the system, including GPUs, which makes adding, deleting, or moving a board to another slot as simple as a mouse-click.

Cluster managers also support developers loading their own kernel images to a single board or a combination of boards. This ability enables multiple developers to work on separate groups of processors on the system – a limited resource – simultaneously. The separate kernel images allow the developers to always start their work session at a known point, eliminating any doubt regarding the state the system was left in by a previous user. This image-based provisioning architecture can also guarantee that the same version(s) of software is loaded on all the boards, of all processing types, for full system testing and delivery, thereby eliminating the headache of reprogramming boards. The revision control also empowers the user to track changes to the software images using standardized methods, and effortlessly roll nodes back to a previous revision if needed.

The health and monitoring features – including temperature, CPU loading, and disk space – in the cluster manager provide a visual status of the entire system. It also logs and displays the boot-up messages for all of the boards and conveys any errors or warnings from the system logs. This feature removes the need to connect a terminal to serial ports to debug and configure the compute nodes, saving time that may have been spent searching for the right serial cable, a serial-to-USB adapter, or the driver for the adapter (especially if the user is on a network that can't access the outside world). This total management of the system supports the complete life cycle, enabling a seamless transition from lab development to flight readiness through manufacturing and delivery.

Debugger and profiler

Use of a high-end debugger and profiler sourced from the HPC community enables bugs to be addressed in a much more timely and efficient manner. An example of a leading solution, used by more than 70 percent of the world's supercomputers and taught in universities worldwide, is the Allinea Forge tool suite, which combines Allinea Software's debugger DDT and a profiler, MAP. Forge combines debugging, profiling, editing, and building – including integrated version control – with all the tools sharing the same easy-to-use interface.

Debuggers with advanced capabilities, like Allinea DDT, help developers quickly discover the root causes of software defects, such as an uninitialized variable. Without the debugger, weeks or months of effort might be spent trying to solve the same problem in a deployed system. Unlike other debuggers, DDT visualizes data across multiple processes, enabling developers to quickly spot unexpected

data points and generate statistical summaries of data structures. (Figure 1.)

Another valuable time-saving feature of advanced debuggers is their ability to automatically record debugging sessions, with comments, directly into online logbooks. This feature enables developers to exactly repeat the same test setup to eliminate transcription errors or omissions. Debuggers can log variables and events in the background without affecting system timing. This enables the system to collect data for however long it takes for the problem to occur. This capability can be invaluable for catching seemingly random, nonrepeatable bugs. When integrated with common version-control tools, debuggers can highlight any recently changed code to help pinpoint any new errors.

One challenge for HPEC developers is that solving problems spanning multiple processors is much more difficult than working with serially executed code. That's why, for HPEC system development, the debugger being used must have the ability to debug and control threads and processes, both individually and collectively. This type of debugger enables the creation of groups of processes based on variable or expression values, current code location, or process state. It also enables the developer to set breakpoints, step, and play individual or predefined groups of threads. In addition, parallel stacks can be displayed, providing a scalable view of all the stacks of every process and thread. This narrows down problems for any level of concurrency, from a handful of processes and threads to the entire system.

With these tools, finding and fixing deadlocks, live locks, race conditions, message synchronization, and other unexpected problems becomes much less daunting for the developer. One concern, though, is that if the debugger requires too much overhead to deliver all the desired advanced features, the system's timing can be negatively affected. To avoid that penalty, the debugger being used must be able to work interactively with many processes within certain time constraints.

Map it!

A rough rule of thumb for system development is that an application will spend 60 to 70 percent of the time performing computations and 10 to 20 percent handling communications. A profiler, such as Allinea's MAP, can point to computation and communication imbalances, including those performance issues caused by MPI or pthread synchronization issues. (Figure 2.) Profilers also perform equally well in finding and solving memory and I/O bottlenecks, which can otherwise cause developers some frustrating late nights in the lab.

Sometimes, even if the application code is up and running, it might not be meeting the timeline or may require some fine tuning to optimize performance. The conventional approach at this juncture is to insert timers into the code, run the code, analyze the results, and then change the code. This process might be followed by any number of iterations until results are satisfactory. Part of the problem is that by simply inserting and then removing a timer, errors can be easily and inadvertently introduced into the code. Using a profiler enables code to be compiled without having to be instrumented, and eliminates the need to record arcane compilation settings as well.

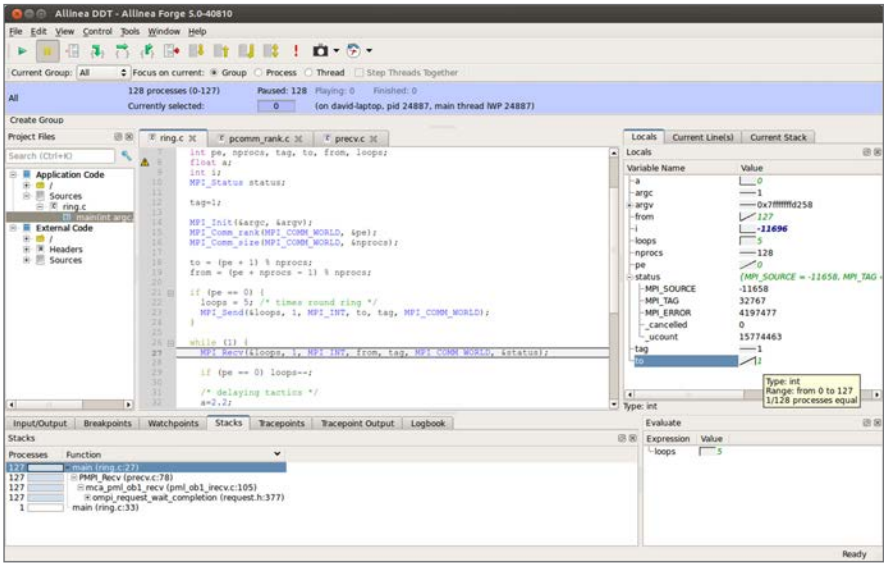


Figure 1 | Allinea DDT debugger running 128 processes.

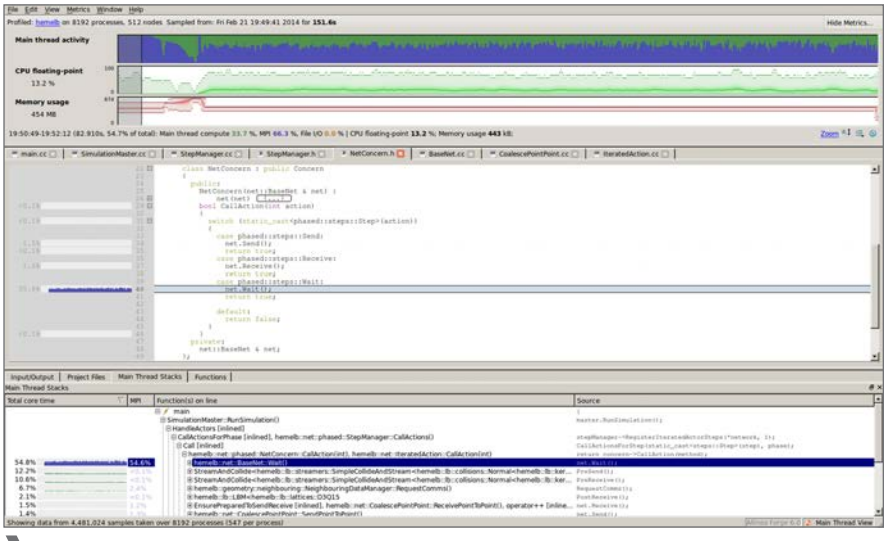


Figure 2 | MAP profiler pinpoints code-optimization opportunities.

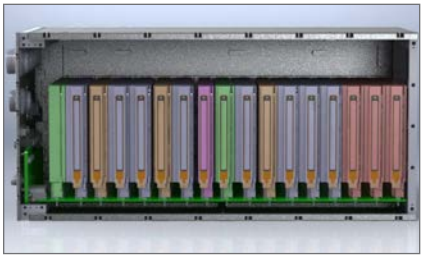


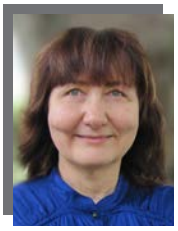
Figure 3 | Example of a 3U OpenVPX HPEC system.

Bringing HPC development tools to COTS HPEC

Leveraging the expansive, mature ecosystem of development tools used in the commercial HPC development community, with its vastly larger installed user base, provides HPEC system developers with proven, full-featured tools that embrace a system-level perspective. Instead of focusing on individual boards in the chassis, a higher-level approach is much more effective for setting up HPEC systems, maintaining them, and partitioning code across multiple nodes. To simplify the process of transferring proven HPC tools into the COTS HPEC environment, Curtiss-Wright has introduced the OpenHPEC Accelerator Suite. It features Bright Computing's cluster manager and Allinea Software's debugger and profiler solutions, brought over directly from the HPC domain. The tool suite supports 40 GB Ethernet, InfiniBand, and PCIe Gen 1/2/3 fabrics, as well as multiple versions of MPI for communications. This integrated HPEC development environment is tested, validated, and benchmarked. (Figure 3.)

The right tools

As the demand for larger-scale, higher-performance deployed HPEC systems increases, access to the best development tools will only become more critical. By leveraging tools such as debuggers, profilers, and cluster managers – tools that are already matured and proven in the commercial supercomputer market – HPEC system developers will derive significant productivity advantages that lower costs and cut development schedules. Even better, these tools provide a superior alternative to expensive proprietary options. **MES**



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

Curtiss-Wright • www.curtisswrightds.com

Optical and electrical high-speed communication in HPEC systems

By Thierry Wastiaux

Aircraft such as this Hawkeye E-2D surveillance and early-warning aircraft use technologies that generate huge amounts of data that must be processed and transmitted. Photo courtesy Northrop Grumman.

Throughout the defense field, demand for high-volume/high-speed data transfer for high-performance embedded computing (HPEC) is growing rapidly. Systems such as software-defined radio (SDR) use advanced, complex waveforms, all of which need fast sampling and generate huge amounts of data to be transferred. Other tools, such as active electronically scaled array (AESA) radar systems, generate huge amounts of data to be processed and transmitted.

High-speed transmission via boards and backplanes is starting to bump up against some physical limitations. Typical high-speed challenges include impedance mismatch, crosstalk noise, power and ground noise, and electromagnetic interference (EMI)/electromagnetic compatibility (EMC) performance. Impedance mismatches can occur due to line-width changes, vias, connectors, and cables.

Designers and manufacturers of printed circuit boards (PCBs) must monitor manufacturing tolerances carefully and ensure that such parameters as effective dielectric constant and surface-roughness variation are tightly controlled. Crosstalk noise is due to electromagnetic coupling between signal lines, via-to-via coupling, and digital/RF coupling. Power and ground noise control and tight requirements on the power distribution network (PDN) are essential to provide clean power to field-programmable gate arrays (FPGAs) and application-specific integrated circuits (ASICs). In particular, an imperfect power and ground delivery system results in simultaneous switching output (SSO) noise that propagates through the PDN. Moreover, most of the above effects produce EM radiation.

In order to design electronic boards with high-speed buses, designers can perform pre-layout signal-integrity analysis through software simulation using design-automation tools. Such a tool allows the user to define all the constraints for designing PCBs, including material, size of the stack, tracks and vias, anti-pads, stubs, and spacing between the tracks. Post-layout signal-integrity verification must then be performed. Electromagnetic simulation of the designed PCB enables extraction of the "scattering parameters" in order to verify compliance with VITA 68, which defines a VPX compliance channel. To improve impedance control and limit signal reflections, backdrilling techniques on the PCB can eliminate unwanted stubs; this process, however, makes the manufacturing process of the boards more complex.

Signal-integrity engineers today find that traditional electrical backplanes allow a data rate of as fast as 25 Gbps per differential link, provided that state-of-the-art techniques are used. The backplane connector remains one of the important limitation factors to reach this level. The industry is now under enormous pressure to develop new technologies, improve the performance of electrical transceivers, and define new standards and protocols to allow ever-higher throughput with lower energy consumption and smaller footprint.

One attempt to overcome these challenges is to use the fiber-optic technologies originally developed for telecom applications. These technologies are now brought to HPEC by designing

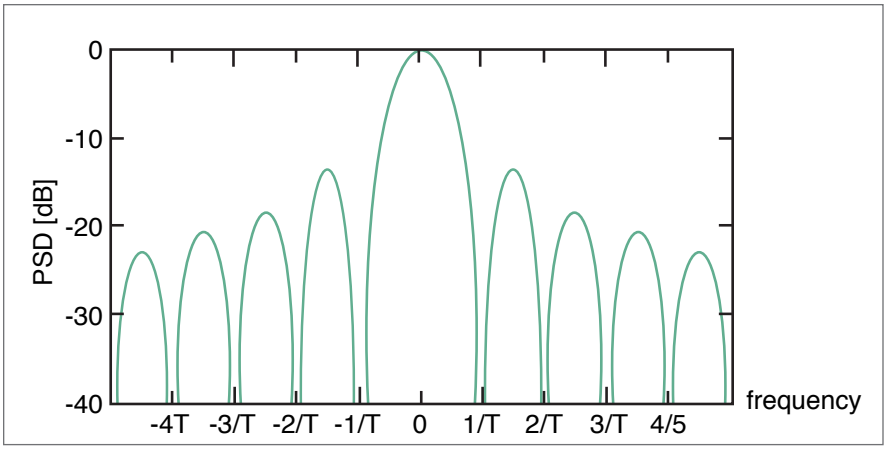


Figure 1 | NRZ power spectral density.

rugged versions of the standard components that can operate safely in a wide temperature range. In this vein, VITA has approved the 66.1 standard covering fiber-optic connectors, and is currently working on finalizing the 66.4 standard, a variant covering half-width interconnects. Reflex Photonics and Samtec are among the companies currently designing small, low-power, rugged transceivers for use in HPEC designs.

These optical solutions are suitable for use in connecting the thousands of transmit/receive modules of the active antennas used in an AESA radar platform to the signal-processing system and more generally for connecting sensors generating important flows of data.

These optical fiber solutions are clearly one of the ways to dramatically push the limits of high-speed data transfer through VPX backplanes. Moreover, they are the most readily available to designers today, even when higher cost and need for rugged packaging is considered.

Signal-integrity engineers are now working on new technologies to try to push the data-rate limits on boards and electrical backplanes and further explore whether higher throughput could be achieved on classical differential links.

The current protocols largely use the NRZ (Non Return to Zero) modulation technology. Many protocols – for example, PCIe, 1000BASE-T, 1000BASE-KX, 10GBASE-KX4, 10GBASE-KR, and Aurora – are based on the NRZ simple modulation for their physical layer. Figure 1 tracks the power spectral density of NRZ, "T" being the NRZ symbol period, with one symbol corresponding to one bit.

As serial data rates go beyond 20/25 Gbit/s per link – and to try to reach 40/50 Gbit/s – signal impairments caused by increasing bandwidth means that the high-speed serial data industry must shift its approach. Simple, baseband, NRZ signal modulation techniques are being left behind in favor of more bandwidth-efficient PAM4 (four-level pulse amplitude modulation).

PAM4 – which cuts the bandwidth in half by transmitting two bits in each symbol – must be distinguished from its symbol rate, referred to as Bd (baud). For example, a 56 Gbit/s PAM4 signal is transmitted at 28 GBd.

The only high-speed serial PAM4 standard that has been released so far is IEEE 802.3bj 100 Gigabit Ethernet (GbE), 100GBASE-KP4. To reach 100 Gbit/s total data rate, it combines four lanes at 13.6 GBd. The success of PAM2-NRZ has meant limited adoption of 100GBASE-KP4, but does provide a solid basis for the future of the emerging PAM4 standards.

Electrical PAM4 specifications will consist of multilane, low voltage, balanced differential pairs with embedded clocking and either transmitter or receiver equalization, or both. The increased impact of signal-to-noise ratio on PAM4 signals calls for forward error correction (FEC), which enables the maximum uncorrected bit-error rate (BER) to be increased to 10-6 for electrical signaling to achieve the data-rate targets, albeit at the price of some hardware complexity.

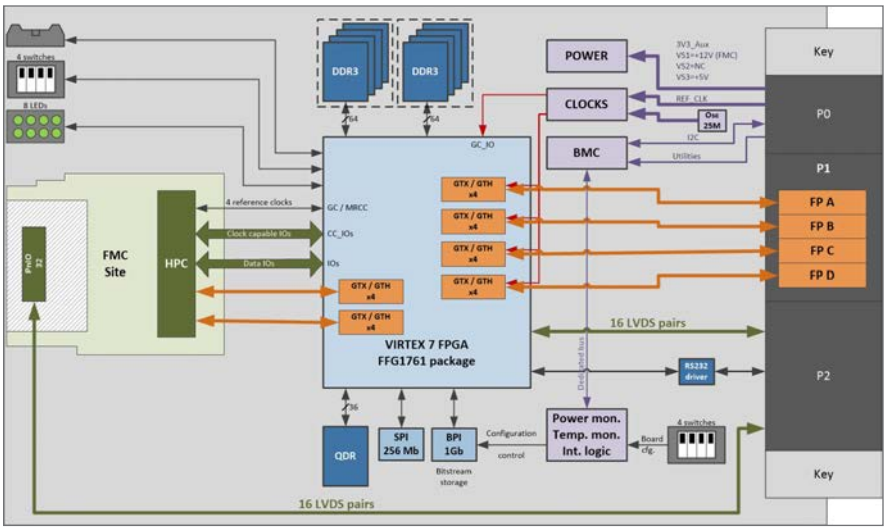


Figure 2 | IC-FEP-VPX3c block diagram.

Interface Concept is using high-speed fiber-optic technologies for two purposes. One target allows the connection of many optical fibers to a VITA 57.4 FMC carried by Virtex-7 and UltraScale/UltraScale+ front-end processing boards. The IC-OPT-FMCa board can thus connect 12 Tx/Rx optical fibers to the high-speed transceivers of the last generation of FPGAs. This configuration offers a bandwidth of 480 Gbps on a small mezzanine board. Thanks to the backwards compatibility of the VITA 57 standard, this FMC can bring high-speed connectivity to VITA 57.1 as well as VITA 57.4 FPGA carrier boards. In the case of VITA 57.1, a maximum of ten fibers only can be connected depending on the number of high speed transceivers in front of the high-speed serializer/deserializer (SerDes) pins of the FMC connector. On the IC-FEP-VPX3c, eight fibers can be connected to two Quad Virtex-7 transceivers, as seen in Figure 2. In the second instance, designers are looking to overcome the throughput limitations of the VPX connectors and backplanes by implementing the solutions defined by the VITA 66 standard. As an example, a version of the Interface Concept UltraScale VPX 3U board features a VITA 66.1 connector for 24 optical fibers connected to six quad GTH transceivers on the FPGA and replacing the P2 VPX connector.

Simply put, when going well beyond 10 Gbit/s per differential link in a VPX chassis, the best short-term approach lies in using optical technologies. Looking farther out, it is clear that designers are reaching the limits of copper and that PAM4 modulation will be the basis of a believable path towards competitive 50 Gbit/s differential links. **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

Spotlights

RUGGED

RUGGED 1U
LIGHTWEIGHT SERVER

WITH CARBON FIBER ELEMENTS

- 13 - 15lbs total weight (depending on configuration)
- Support for 2 Intel® Xeon® Processors
- Up to 2TB RAM
- EMI: CE102, RE102, RS101, CS101 Functional Shock: MIL-STD810G Vibration: DO-160E

zmicro.com

zmicro | RUGGED COMPUTING SOLUTIONS

AVIONICS

Protocol Converters

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

KIMDU TECHNOLOGIES

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

RADAR

New Ka Shield Rack Protects to 40 GHz

- Equipto Electronics "Ka Shield" Rack Enclosure far exceeds the toughest standard for EMI/RFI defense, with certified performance to 40 GHz ... TEMPEST requirement NSA 94-106
- Custom sized
- Line filters/wave guides
- Honeycomb air filters
- Many options
- RoHS Compliant

EQUIPTO Electronics Corp.

Equipto Electronics Corp.
800-204-RACK (7225)
sales@equiptoelec.com
www.EquiptoElec.com

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

Intel Xeon cores power high performance and low SWaP complex sensor solutions

By Curtiss-Wright Defense Solutions

As the flexibility and power of modern sensor systems – like those used in radar and imaging – has grown, so has the complexity of their software control. This white paper will discuss how updated processors can address the challenges of controlling today's more complex sensor systems.

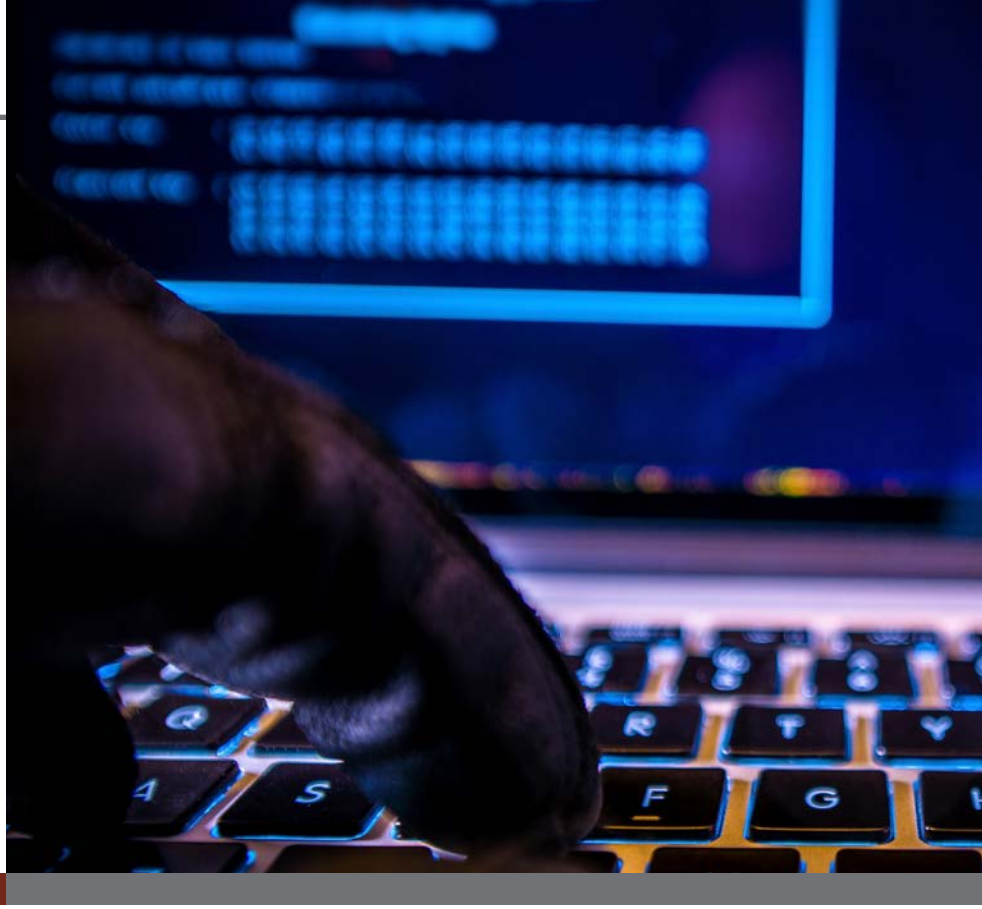
http://mil-embedded.com/white-papers/white-complex-sensor-solutions/

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

"Cyber hardening" DoD networks, sensors, and systems for mission resiliency

By Sally Cole, Senior Editor

BAE Systems, Lockheed Martin, and Raytheon are all leveraging automation and analytics to "cyber harden" military networks, sensors, and systems.



The U.S. Department of Defense (DoD) is currently in the process of "hardening" its networks, sensors, and systems against cyberattacks. This includes real-time operational systems such as aircraft, unmanned aerial vehicles (UAVs), and ships, which all must undergo cyber hardening to enhance mission resiliency against system manipulation, hijacking, or destruction.

What is cyber hardening?

Lockheed Martin defines cyber hardening as a broad concept that addresses securing various threats and challenges across multiple domains. Cyber hardening involves "assessing platforms, mission systems, network systems, and other at-risk solutions, and then applying multiple cyber models to help clients defend their networks, mitigate threats, protect their platforms, and continuously assess their systems – both from an internal and external perspective," explains Doug Booth, business development director for Lockheed Martin Cyber Solutions.

Raytheon is taking its cue from the DoD's definition, and Brian Stites, cyber hardening campaign program manager for Raytheon Intelligence, Information, and Services, describes cyber mission resiliency as "the confidence and assurance for systems to function as expected, and for forces to accomplish their missions within a contested environment in the face of sophisticated, capable adversaries."

The ultimate goal of DoD's cyber mission resiliency is to reduce the consequences of attacks. "An important aspect of resiliency is 'cyber hardening' or reducing the attack surface of a system and increasing the difficulty of system access and exploitation," Stites adds.

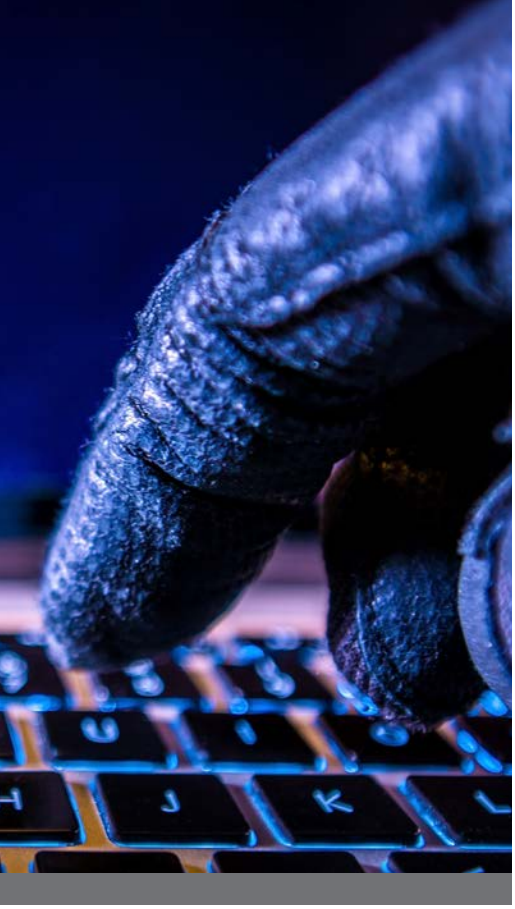
Raytheon applies a four-step methodology to harden systems. The first step involves an architectural review to seek out security flaws that an attacker could exploit to disrupt normal operation. Once these flaws are identified, they're prioritized from moderate to critical, based on how much damage they can inflict. Next, layered risk-management techniques – such as fixing vulnerable software, adding security tools, tightening policies, adding hardware and or training customer personnel – are applied. Finally, tests are run to ensure that the mitigation is effective and hasn't introduced new flaws.

The use of penetration testing by "red teams" is an incredibly valuable aspect of security assessments. "Large-scale enterprise and platform systems are increasingly based on a mix of government off-the-shelf/commercial off-the-shelf (GOTS/COTS) software, which increases the cyberattack surface," says Kevin M. McNeill, vice president and chief scientist of Intelligence and Security for BAE Systems.

"Tapping into the attacker's viewpoint and understanding their approaches for analyzing the attack surfaces of these complex systems can help to identify vulnerabilities that may be hidden within COTS environments," McNeill adds. "Any system that uses COTS has an ever-changing attack surface that requires frequent, thorough testing."

Automation and analytics

Artificial intelligence and automated systems are both being tapped for cyber hardening. Cyberattackers are increasingly using more complex attack patterns, "leveraging speed via scripts and automation, and exploiting insider access with social-engineering



attacks such as spear phishing or password guessing," says McNeill.

BAE Systems is working with its customers to enhance defense-in-depth strategies with solid system-administration practices – also known as cyber hygiene – supported with automation and analytics. "It's difficult for customers to scale up their staff to mitigate evolving attack techniques," notes McNeill. "Adding more expert cyberanalysts or system administrators to protect their networks would be ideal, but it isn't always feasible. There's a shortage of skilled personnel, and competition for them is high. For our government customers, competing with the private sector for skilled staff isn't easy."

One cost-efficient way to maneuver around the shortage in skilled personnel is to defend against attacks by leveraging automation tools and analytics as force multipliers for cybersecurity, which significantly raises the costs involved for attackers. "This approach requires robust and scalable governance methods, which is an active area of cyber research for BAE Systems," McNeill says.

Automation has become a critical tool in recognizing and responding to threats. Raytheon, for example, uses what it calls electronic armor to prevent adversaries from digitally penetrating and potentially disrupting missions on vehicles and other systems from anywhere around the world. "This technology is capable of detecting system penetrations regardless of the source," Stites says. "Electronic armor takes a snapshot of what a system looks like when it's secure. If that picture changes, even the slightest, it triggers a warning that the system may be compromised and it allows the vehicle to ignore malicious commands."

BAE Systems recently unveiled an automated cyberthreat intelligence solution developed in partnership with Fujitsu that "actively transforms raw cyberthreat data into actionable intelligence," McNeill says. "We view cybersecurity as an intelligence problem rather than simply a problem of compliance, patching, and configuration management."

For this collaboration, the two companies leveraged their cyberthreat intelligence (CTI) expertise and model-based software-engineering technologies to create and demonstrate an automated CTI-sharing system based on secured threat information expression (STIX) and trust automated exchange of indicator information (TAXII) standards.

"Think of STIX as a universal 'cyber language' for cyberthreats," McNeill explains. "Our models can translate the ones and zeros of STIX data to answer valuable cyber-intelligence questions regarding specific threats. For example, analysts can flag distinct patterns in the data – akin to a cyberattacker's fingerprints – to give us key information about the kind of threat we're looking at, when it was identified, where it originated, how the attacker attempted to enter a network, and eventually even who is likely behind the threat. This solution saves analysts valuable time."

This demonstration system is enabling "active bidirectional exchange of CTI between partners and allied organizations, and also provides an innovative model-based data protection framework that enforces sharing policies and ensures removal of private and other sensitive data from the shared CTI," he continues. "Its CTI management framework prototype provides cognitive assistance to cyberanalysts through graph-based analytics."

> "WITH A LOW COST OF ENTRY INTO THE CYBER DOMAIN, THE U.S. MILITARY FACES NEW ADVERSARIES ON A DAILY BASIS."
> – DOUG BOOTH, BUSINESS DEVELOPMENT DIRECTOR FOR LOCKHEED MARTIN CYBER SOLUTIONS

Automated systems appear to be the next evolution in cyberdefense. "Not only are they cost-effective … they're cyberdefense force multipliers," McNeill notes. "Think of automated systems as a mechanism for 'crowdsourcing cybersecurity.' As a best practice, BAE Systems harnesses all of the data surrounding cyberattack strings, etc. that target our own network." Once BAE Systems identifies and neutralizes these threats to their own network, they can share this cyberthreat data with customers and industry partners. "Collaboration through crowdsourcing is one way we'll all share the rewards of a safer cyberspace at a reduced cost," adds McNeill. "That's why real-time information sharing is the logical first step toward developing a holistic cyberdefense strategy."

Cyber hardening challenges

The DoD faces myriad cyber hardening challenges. Among the worst aspects: protecting such a wide variety of platforms, the age of the technology involved, use of COTS, and the ever-increasing threat of global attackers.

"With a low cost of entry into the cyberdomain, the U.S. military faces new adversaries on a daily basis," says Lockheed Martin's Booth. "The variety of systems and platforms that must be defended are a challenge. The size, scale, and complexity of these

systems – combined with the need to keep them operational and protected – are also a challenge. Legacy hardware and software pose yet another problem."

COTS systems tend to be designed for interoperability and functionality, but the DoD is finding that any associated cost savings must be balanced with mission assurance. One big problem is that COTS systems "typically don't include a requirement to harden systems," points out Raytheon's Stites. "Any cyber hardening must be added after the initial design review or even after a system becomes operational, during the modernization lifecycle."

And many existing platforms never had a requirement in the first place for cyber hardening of systems. "As these systems go through modernization, the systems are being upgraded, but these upgrades are required to be hardened, networked digital systems," Stites adds. "These programs didn't necessarily include budgets for additional protections and evaluations."

Increased adoption of COTS, cloud, and mobility technologies across the DoD "provides many benefits and enables cost reductions over GOTS and special-purpose systems," says McNeill. "But security aspects of technology adoption are a top priority, and the cybersecurity of specialized embedded systems used within weapons platforms must also be assessed."

For example, a significant cyber hardening challenge for the U.S. Army is that it's operating "a large, complex, and heterogeneous network of federated systems that are deployed globally, often in areas with limited infrastructure," McNeill adds. "It doesn't lend itself well to many commercial cybersecurity tools or methods, so the DoD must assess each solution individually to ensure it enhances cybersecurity without degrading critical mission functions."

DDoS attacks escalating

Distributed-denial-of-service (DDoS) attacks are an escalating annoyance and constant threat for the DoD. To deal with them, BAE Systems encourages network defenders to leverage automation by blocking IP addresses, shifting services, and changing routes.

"While automation can support rapid recognition and response to DDoS attacks, it should also be used to restore normal operations just as quickly," McNeill says. "Rapid-strike DDoS attacks can force countermeasures that may remain in place for hours or days beyond the attack, degrading mission functions. This extends the adversaries' effects rather than minimizing them. So BAE Systems is focusing on providing cyber resilience to enable missions to continue in the midst of cyberattacks."

Quantum impact

Quantum computing has the potential to greatly disrupt cybersecurity, but exactly how or when remains uncertain. "Quantum computing is a very broad term, but can prove a major threat in relation to impacts on DoD military networks and communication," says Doug Booth, business development director for Lockheed Martin Cyber Solutions.

While right now much of the focus on quantum computing centers on its potential to break existing cryptography, Kevin M. McNeill, vice president and chief scientist of Intelligence and Security for BAE Systems, points out that "some of the most promising applications will leverage quantum entanglement for secure communications."

Current research into using quantum entanglement points to future applications that will enable "communicating more securely, over greater distances, than any existing technology," McNeill adds. "It has the potential to provide communications globally, in real time, without the threat of eavesdropping or hacking. At this early stage, no methods exist to detect that communication is occurring. Such a capability denies adversaries the use of traffic analysis or endpoint geolocation, which could be a profound advantage."

DDoS attacks are an information technology (IT) issue, but operational technology (OT) can also be attacked. "DDoS is a cyber hardening concern," notes Stites. "Industrial-control systems, safety systems, utility systems manufacturing equipment, cameras, and many other devices controlled remotely via the Internet are susceptible to attack. So DDoS concerns are a top driver of innovation to protect the boundary between IT and OT."

IoT cybersecurity

The Internet of Things (IoT) will bring its own special bag of big challenges because every "connected thing" that has an IP address is vulnerable to attacks.

IoT, like all new paradigms, has the potential to break established approaches. "For many of BAE Systems' customers, there's an increased focus on more specialized computing platforms with respect to cybersecurity," McNeill says. "IoT is becoming pervasive and impacts infrastructure used by the government. The DoD's IoT devices rely on limited resources – CPU, memory, connectivity – and are often difficult to update. This requires a more surgical cybersecurity approach, so we're encouraging them to augment existing practices with automation and analytics. We're also working on cyber models to support this and to enable governance of IoT networks and devices."

Security standards are still largely in the works for IoT devices, and they must be "followed as we already do within IT environments," points out Stites. "Raytheon has analytics and visualization tools to create knowledge and better controls from the massive amounts of information generated by IoT data. Another technique we use is to remove software glitches from open-source operating systems Linux and Android – to essentially create newer and more secure versions of those systems to use in all manner of devices."

From Lockheed Martin's perspective, IoT is "just another challenge in the cyberdefense world," Booth says. "Using our Cyber Kill Chain methodology, IoT is treated as just another entry point or level of access." **MES**

ISO 9001:2008 & AS9100C CERTIFIED

ITAR REGISTERED

VECTOR

ELECTRONICS & TECHNOLOGY, INC.

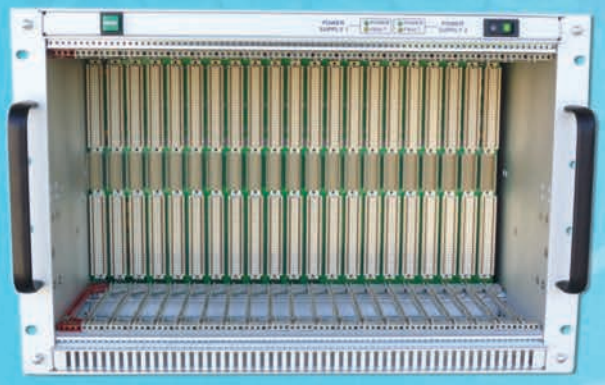
A FINE TECHNOLOGY GROUP

Since 1947

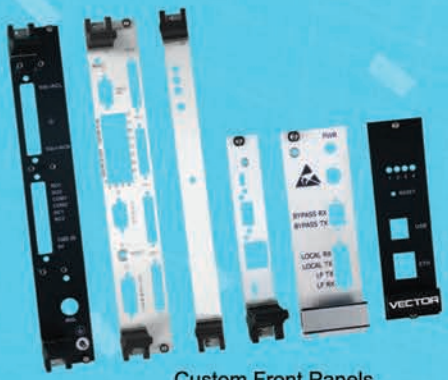
MADE IN THE USA

VME / VXS / cPCI ®

Chassis, Backplanes & Accessories



Chassis and Rack Accessories

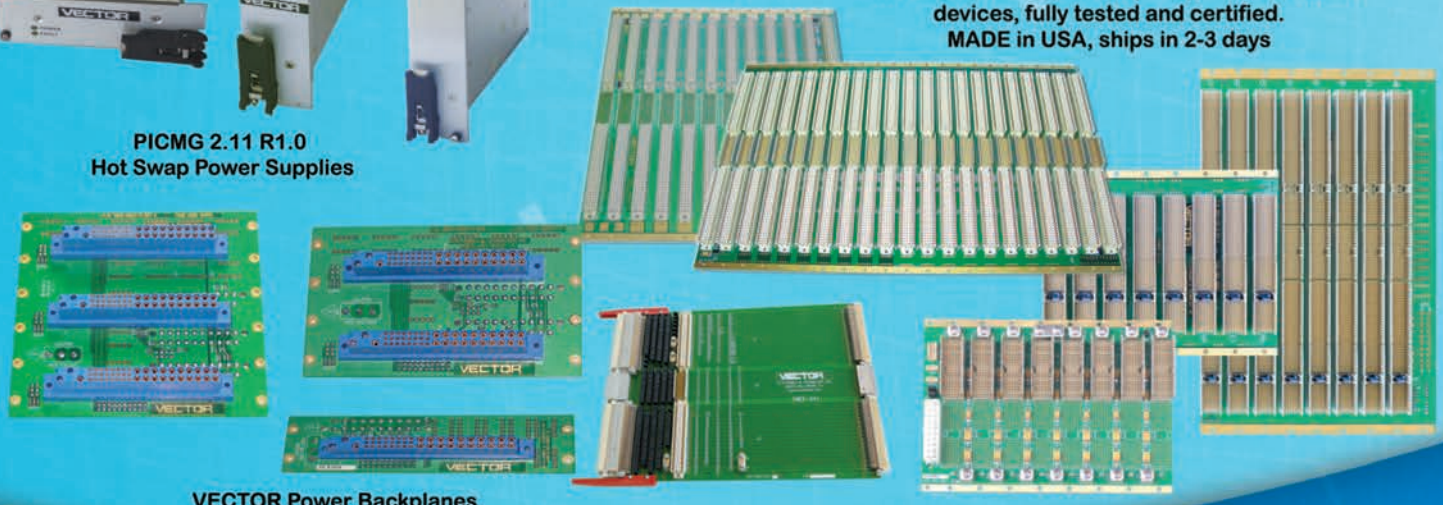


Custom Front Panels

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

MADE IN U.S.A.

(800)423-5659

WWW.VECTORELECT.COM

VISIT OUR NEW WEBSITE!

System for air-to-air and air-to-ground operations

Weighing in at 5.2 pounds, the L-3 Communications Tactical Airborne Navigation (TACAN) device is a remotely controlled aviation-navigation system that can track as many as four ground stations simultaneously in range, and two in bearing, with a tracking velocity of as fast as 1,800 knots. TACAN+ employs software-controlled antenna switching, enabling the aircraft to be configured for dual antennas if needed. The TACAN+ system can be used for air-to-air and air-to-ground operations and meets MIL-STD-291C and NATO STANAG-5034 standards.

Engineers designed the system with an eye to rugged military environments; thus it also meets MIL-STD-810G, MIL-STD-704, and MIL-461E requirements, as well as DO-160F helicopter vibration levels. The TACAN+ system features lightning-protected circuitry and is subjected to Highly Accelerated Stress Screening (HASS) and Highly Accelerated Life Testing (HALT) to achieve system reliability. It has multiple input/output buses to update flight management or inertial systems simultaneously, is compatible with a variety of cockpit displays including the L-3 GH-Series of Electronic Standby Systems, and has real-time identity verification on four channels. The system's 500-watt transceiver features a maintenance port for servicing.

L-3 Communications | www.l-3avionics.com | www.mil-embedded.com/p373505

Software for users looking to achieve RTCA DO-178B certification

The Presagis VAPS XT-178 is a safety-critical software package for creating embedded display graphics for avionics applications intended for RTCA DO-178B certification. It is a commercial off-the-shelf (COTS) object-oriented DO-178B qualified HMI tool that retains the core features of the VAPS XT HMI tool and adds on to that to enable end users to claim credit towards their certification requirements. Because the package is an XML-based HMI tool, VAPS XT-178 allows the user to create custom widgets, save them, and re-use them from project to project. VAPS XT-178 can be used to certify ARINC 661 and non-ARINC 661 applications.

VAPS XT-178, according to Presagis, shortens the time required for developing certifiable embedded software products by reducing the effort required within the software design, coding, and testing phases of the graphics display development life cycle. The end user may utilize the documents and test cases provided with the product in order to obtain credit for the tool qualification as part of the total system certification.

Presagis | www.presagis.com | www.mil-embedded.com/p373628

Radio design supports up to 4 Mbps

FreeWave Technologies' ZumLink Family represents a class of wireless Internet of Things (IoT) communication solutions offering a radio design that supports a link rate of as fast as 4 Mbps, as well as the ability to support third-party applications. These capabilities provide customers with increased bandwidth, lower power consumption, and possibilities for collecting, protecting, transporting, and controlling data from the network endpoints all the way back to the server. ZumLink features four platforms within its 900 Series, consisting of two radio modules, a board-level embeddable, and a fully enclosed device, all four of which operate in the 900 MHz unlicensed frequency range.

ZumLink offers several options for users, including Z9-PE enclosed with one Ethernet and two serial ports; Z9-T radio module with TTL interfaces; Z9-C radio module with RS232; and Z9-PC board level device with two Ethernet and two serial ports. Freewave also offers standards and user-defined hop sets; sense-before-transmit protocol; throughput of as fast as 2 Mbps at the 4 Mbps link rate; multiple link rates, channel sizes and modulations; frequency hopping and single-channel use; and user-channel masking. The core design can support a wireless application server and sports a built-in spectrum analyzer. It also consumes 30 percent lower power than traditional designs.

FreeWave | www.freewave.com | www.mil-embedded.com/p373629

Embedded rugged system offers three-in-one platform

The EB7001 embedded computer from Systel is an extreme-duty system designed for military operations, oil-field services, original equipment manufacturers (OEMs), and other rugged industrial environments. The EB7001 is a rugged small-form-factor three-in-one platform (encoder, decoder, and storage). It uses a single i7 4700 quad-core central processing unit (CPU) for critical computing and features up to 1.25 GB of solid-state drive (SSD) storage and quad HDSDI encoding. PCIe/104 expansion bus GB/E, serial and DIO cards may be installed to further expand the system, according to Systel. The removable SSD enables secure storage of mission data.

System features also include dual 3G-SDI or quad HD/SD-SDI/Composite (NTSC/PAL) H.264 encoder with full KLV COT metadata, Intel HD4600 graphics for decoding, two optional removable 1 TB SSDs, PCIe/104 expansion, IP66 water ingress, compliance with MIL-STD 461E and MIL-STD-810G shock and vibration standards, and operating temperature ranges between -40 °C and +55 °C. The encoder is an option that can be replaced by a selectable PCIe/104 boards for various I/O functions. An array of optional cards allows the user to customize the EB7001 for many different types of computing applications.

Systel | www.systelusa.com | www.mil-embedded.com/p373630

Spectrum monitoring for distributed networks in hostile environments

The RFeye Node 20-6 from CRFS is a spectrum-monitoring system designed for remote deployment in distributed networks, both indoors and outdoors, including in hostile environments. The system is packaged in a compact, rugged, and weatherproof housing that has been optimized to meet size, weight, and power (SWaP) requirements. The Node's architecture is capable of supporting multiple concurrent tasks and missions, including International Telecommunications Union (ITU)-compliant measurements. Timing and synchronization features enable correlation of data between multiple nodes for accurate direction-finding and geolocation of target signals using angle of arrival (AOA), time difference of arrival (TDOA), and power on arrival (POA) techniques.

The Node 20-6 is available with optional onboard solid-state drive for logging of very large data sets. Frequency ranges from 10 MHz to 6 GHz for real-time spectrum monitoring, with up to 20 MHz instantaneous bandwidth. Features of the system include 15 W of typical power, an embedded Linux system, RFeye system software, GbE, wireless modem and GPS, USB disk or internal SSD option, and power over Ethernet or local power supply unit (PSU). A ruggedized version carries optional IP67 covers.

CRFS | www.crfs.com | www.mil-embedded.com/p373632

All-in-one VPX-1 for compact system design

iVeia's VPX-1 is a compact plug-in module that aims to simplify overall VPX system design. The system comes with a new 64-bit ARM quad-core processor architecture, 16-nm high-density FPGA fabric, flexible high-speed backplane options – such as PCIe Gen/ Gen4 and 10 GigE – and modular high-performance I/O. Using iVeia's Mini-Flex modular I/O system, the VPX-1 can be configured to support the I/O of a number of different applications, including dual-channel 16-bit 250 MSPS ADC, quad 14-bit 125 MSPS ADC, low-power 14-bit 125 MSPS ADC, modulating 1 GSPS DAC, dual-channel 12-bit 1.5 GSPS ADC, high-bandwidth 12-bit 3.0 GSPS ADC, and camera link adapter.

The module is based on the Xilinx Zynq UltraScale+ MPSoC. Its processing system includes quad-core ARM Cortex-A53 MPCore processors, and has up to 600K UltraScale+ logic cells as well as more than 3,000 digital signal processor (DSP) slices in a 16-nm programmable logic fabric. The system is VITA 46 and VITA 65 compliant. 2 GB by 64 of DDR4 are dedicated to the processor, while two 512 MB by 16 banks of FPGA DDR memory are dedicated to the fabric, and ten 16 Gb/s high-performance serializer/deserializers (SERDES) support 10 GigE, PCIe Gen4, SATA 3.0, and other interfaces.

iVeia | www.iveia.com | www.mil-embedded.com/p373631

CONNECTING WITH MIL EMBEDDED

By Mil-Embedded.com Editorial Staff

www.mil-embedded.com

CHARITIES | MARKET PULSE | WHITE PAPER | BLOG | VIDEO | SOCIAL MEDIA | E-CAST

CHARITY

Tragedy Assistance Program for Survivors

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

This issue we are featuring the Tragedy Assistance Program for Survivors (TAPS), a 501(c)(3) nonprofit corporation that helps those who are grieving the death of a military service member. It provides a national peer-support network and connection to grief resources at no cost to surviving family members and loved ones.

The idea for TAPS arose in 1992, when eight soldiers were killed in a C-12 plane crash in Alaska; among the grieving family members was Bonnie Carroll, a retired Air Force reserve major and the widow of Army Brigadier General Tom Carroll. Ms. Carroll founded TAPS in 1994, after conducting two years of research examining the resources available to support bereaved military families and benchmarking best practices at other peer-based support organizations. The peer-support network offered at TAPS is the heart of the organization and represents the recognition of the connections made when communicating with those that have shared the same experiences.

Since its inception, says the organization, TAPS has assisted more than 60,000 surviving family members, casualty officers, and caregivers. It holds annual national and regional Military Survivor Seminars and sponsors Good Grief camps and campouts for children at locations across the country. The 24/7 Resource Line is staffed day and night to offer help and compassion to those grieving fallen military members, while survivors can avail themselves of published resource guides and the quarterly TAPS Magazine.

For more information, visit: http://www.taps.org.

E-CAST

Cybersecurity spotlight: Looking under the hood at data breaches and hardening techniques

Sponsored by Intel Security, RTI, ThingWorx

Networked embedded systems and applications dependent on the Internet of Things (IoT) enable services that change the way the world lives, learns, works, and plays. However, purpose-built attacks and data breaches on these environments are becoming commonplace.

In this e-cast, join us as experts in cybersecurity characterize common data-breach and attack techniques. The panel discusses tools, processes, and approaches to seal up vulnerabilities and harden software environments against hostile incursions.

View archived e-cast: ecast.opensystemsmedia.com/612

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

WHITE PAPER

AXIS software development tools

By Abaco Systems

The AXIS modular architecture can help engineers cut development time, reduce project costs, and shorten time to market. Its benefits reach from the initial stages of system design all the way through hardware and software changes at the later stages of the application life cycle.

AXIS allows its users to optimize communications between processors, enabling processing resources to be used more efficiently. It provides enhanced flexibility of transports, including InfiniBand, RoCE, TCP, UDP, Posix shared memory, KNEM shared memory, and GPU IPC. The architecture also supports multiple processor architectures (Power PC/Power Architecture, Intel, ARM) and operating systems (Windows, Linux, VxWorks).

AXIS also creates a layer of abstraction between the application and the hardware and operating system, which can give the user added portability and scalability.

Read the white paper: http://mil-embedded.com/white-papers/white-software-development-tools/

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

Let's face it: what's probably top of your mind is how to ensure your program stands the best chance of success: getting to deployment faster, at lower cost and with less risk. That's what your customers are demanding.

At Abaco Systems, that's our business. We could talk forever about how everything we do is based on industry standards and modular, open architectures – but that's not so important. It's just a starting point for our innovation. What's important is that you work with a company with the experience to back up our promises, and that's entirely committed to your success.

That company is Abaco Systems.

WE INNOVATE. WE DELIVER. YOU SUCCEED.

Find out more at abaco.com
or follow us @AbacoSys

abaco SYSTEMS

Capture. Record. Real-Time. **Every Time.**

Intelligently record wideband signals continuously...for hours

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

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

TALON

Eight SSD QuickPac™ canister, removable in seconds!

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

PENTEK
Setting the Standard for Digital Signal Processing

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