

# Military EMBEDDED SYSTEMS

VOLUME 5 NUMBER 8  
NOV/DEC 2009

INCLUDING:

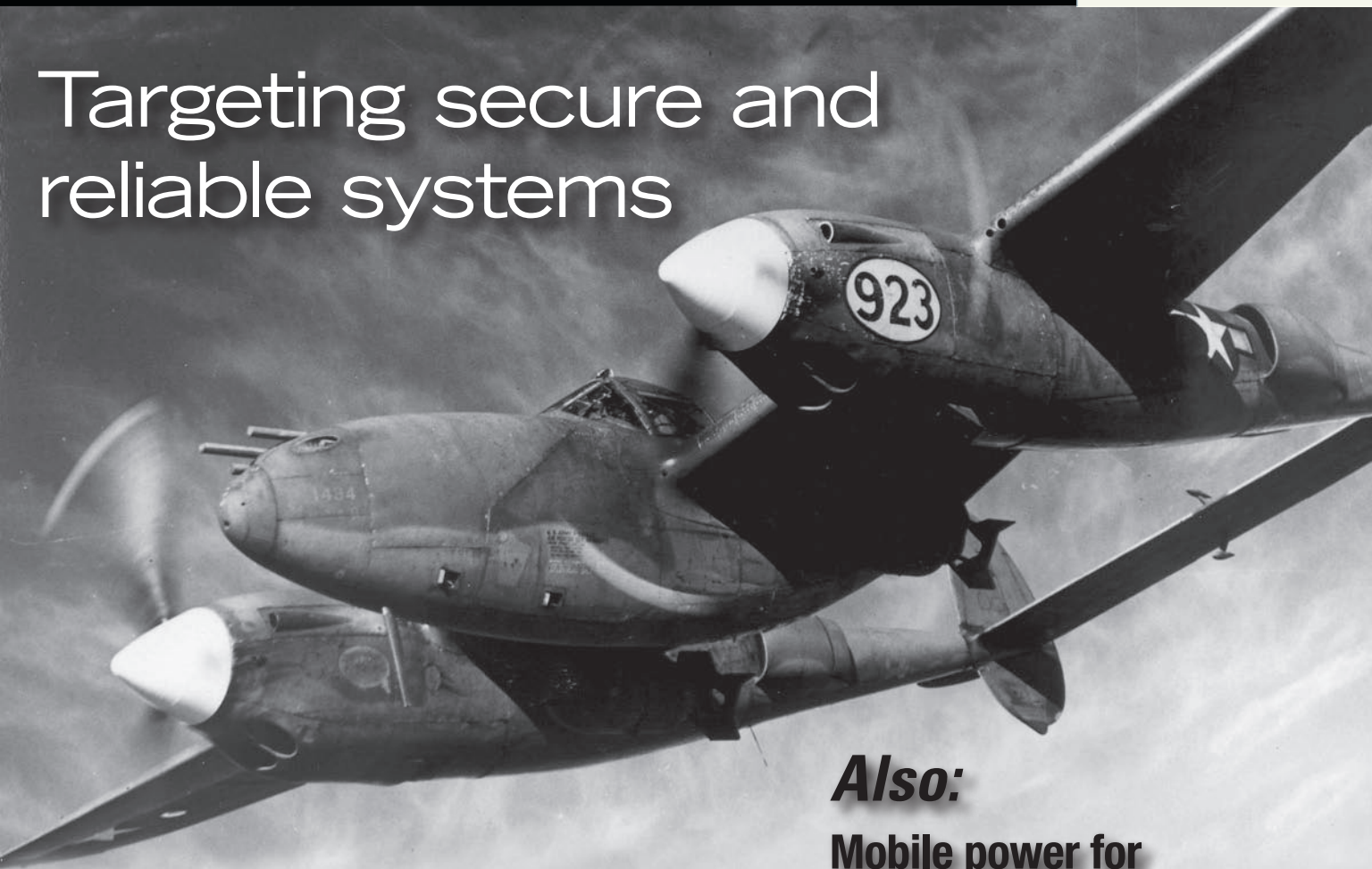
**Chris A. Ciuffo**  
C4ISR and the big picture

**Field Intelligence**  
Packet processors; mil networks

**Mil Tech Insider**  
High-voltage boosts modernization

**Legacy Software Migration**  
**Micro Focus**  
COBOL gets modern

Targeting secure and  
reliable systems



***Also:***

**Mobile power for  
tomorrow's battlefield**

**Static analysis:  
Beyond the compiler**



**Portability  
Versatility  
Longevity**

**Put a new tool in your pocket.**

### **USB - Powered Avionics Databus Interfaces**

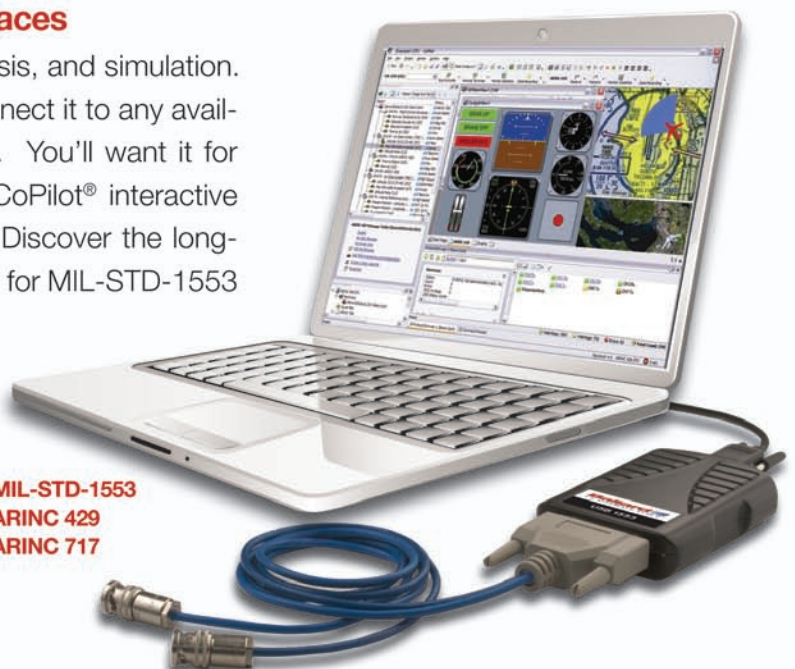
One small tool does it all – databus test, analysis, and simulation. Use it around the lab or in the field. Simply connect it to any available PC – it's fully powered by the USB port. You'll want it for all your interface applications. Add Ballard's CoPilot® interactive software for extra versatility and ease-of-use. Discover the long-lasting benefits of Ballard's new USB interfaces for MIL-STD-1553 and ARINC 429 and 717.

Call us today at 425.339.0281.

**Ballard** TECHNOLOGY  
The Avionics Databus Innovators  
AS9100 / ISO 9001 Registered

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

MIL-STD-1553  
ARINC 429  
ARINC 717







**POWER BY DESIGN**

## Custom power solutions designed to fit your specific needs

*Vicor Custom Power: Small company responsiveness, large company resources*

The sole focus of Vicor Custom Power is designing and manufacturing turnkey custom power systems that meet your specific needs. Vicor Custom Power maintains the flexibility of a small entrepreneurial company while taking advantage of Vicor's technical and business resources to deal effectively with your most challenging power requirements. Vicor has invested in the tools and resources to offer you full service solutions from prototype to mass production with the shortest lead times and the lowest risk.

### *General Capabilities:*

- Electrical and Mechanical Design
- Rapid Prototyping
- High Volume Production Capacity
- MIL-STDs Compliance
- Reliability / Certification Testing:

High Temperature Operational Life  
HALT (Highly Accelerated Life Test)  
Mechanical / Thermal Shock  
Vibration  
Humidity  
Acceleration

Altitude  
Explosive Atmosphere  
Temperature Cycling  
Burn In  
EMI  
Transient Immunity



Put Vicor Custom Power to work for you today, call 1-800-496-5570 to speak with a Vicor Custom Power engineer, or email [apps@vicorcustom.com](mailto:apps@vicorcustom.com)

**[vicorcustom.com](http://vicorcustom.com)**

**VICOR CUSTOM**  
POWER

# Military

## EMBEDDED SYSTEMS

November/December 2009 Volume 5 Number 8

### COLUMNS

#### Field Intelligence

- 8 **Packet processors to speed and protect military networks**

*By Duncan Young*

#### Mil Tech Insider

- 9 **High-voltage power distribution enhances platform modernization**

*By John Wemekamp*

#### Legacy Software Migration

- 12 **Application modernization provides link between historical systems and contemporary technology**

*By Bill Errico, Micro Focus*

#### Crosshairs Editorial

- 38 **C4ISR and the big picture**

*By Chris A. Ciufo*

### DEPARTMENTS

- 14-15 **Daily Briefing: News Snippets**

*By Sharon Schnakenburg-Hess*

- 37 **Editor's Choice Products**

#### Software: Static analysis:

##### Beyond the compiler

- 16 **How good is your compiler (at finding coding defects)?**

*By Wojciech Basalaj, Ph.D., PRQA*

#### Hardware: Designing in cool reprogrammability

- 20 **Releasing the full potential of FPGA-based designs**

*By Rob Evans, Altium Limited*

- 23 **Advanced cooling techniques beat the heat for rugged embedded COTS systems**

*By Ivan Straznický, Curtiss-Wright Controls Embedded Computing*

#### Technology: Battlefield power-up – It's all about the inverter

- 26 **On Board Vehicle Power (OBVP): Mobile power for tomorrow's battlefield**

*By Doug B. Mays, Diversified Technology*

#### Mil Tech Trends:

##### "Must be secure and reliable."

- 29 **Adding trust to an embedded system with a secure anchor point**

*By J. Ryan Kenny, CPU Tech*

- 32 **Protecting embedded systems from unauthorized software modifications**

*By André Weimerskirch, Ph.D. and Kai Schramm, Ph.D., escript Inc.*

- 34 **A new approach to testing embedded-LO converters**

*By David Ballo, Agilent Technologies*

#### ON THE COVER:

A P-38J "loaded for bear" dives on a bomb run. The P-38 was innovative and unusual for the 1940s as the twin counter-rotating props provided roll stability over single-prop fighters. First deployed during World War II to the Alaska theater (surprised?), the P-38 had an extended range that provided security to bombers deep into Germany. On the modern COTS-based battlefield, security is afforded by systems that behave in predictable ways and that can't be compromised due to cyber-attack or bad actors. See stories starting on page 29. (Image courtesy of Wikipedia Commons.)

Published by:  **OpenSystems media**

ISSN: Print 1557-3222

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

© 2009 OpenSystems Media © 2009 Military Embedded Systems

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

### EVENTS

[www.opensystemsmedia.com/events](http://www.opensystemsmedia.com/events)

#### Ethernet Technology Summit

February 24-25, 2010 • San Jose, CA

[www.ethernetsummit.com](http://www.ethernetsummit.com)

### 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>



# ***Annapolis Micro Systems***

## ***The FPGA Systems Performance Leader***

# **WILDSTAR 5 for IBM Blade**

## **The Perfect Blend of Processors and FPGAs**

**Fully Integrated into IBM Blade Management System**  
**Abundant Power and Cooling Ensure Maximum Performance**



**Made in the USA**

### **Ultimate Modularity**

**From 2 to 8 Virtex 5 FPGA/Memory Modules**

**Input / Output Modules Include:**

**Quad 130 MSps thru Quad 500 MSps A/D**

**1.5 GSps thru 2.2 GSps, Quad 600 MSps A/D**

**Dual 1.5 GSps thru 4.0 GSps D/A**

**Infiniband, 10 G Ethernet, FC4, SFPDP**

### ***Direct Seamless Connections with no Data Reduction***

***Between External Sensors and FPGAs***

***Between FPGAs and Processors over IB or 10GE Backplane***

***Between FPGAs and Standard Output Modules***

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

## ADVERTISER INFORMATION

Page	Advertiser/Ad title
21	<b>ACCES I/O Products, Inc.</b> – USB embedded I/O
5	<b>Annapolis Micro Systems, Inc.</b> – WILDSTAR 5
2	<b>Ballard Technology</b> – USB powered avionics
19	<b>CM Computer</b> – CM-SIXHEX
36	<b>CPU Technology, Inc.</b> – Acalis Secure Processor
27	<b>Curtiss-Wright Controls Embedded Computing</b> – Reduce your risk
13	<b>Excalibur Systems, Inc.</b> – Express yourself
39	<b>GE Fanuc Intelligent Platforms, Inc.</b> – Which of these platforms use GE Fanuc
7	<b>Kontron</b> – We do not build Navy ships
18	<b>Nallatech</b> – High performance FPGA solutions
25	<b>North Atlantic Industries</b> – MIL-STD power supplies
40	<b>Pentek, Inc.</b> – We've hatched the next generation of software
31	<b>Phoenix International</b> – Data storage
31	<b>TEWS Technologies LLC</b> – COTS I/O Solutions
12	<b>Themis Computer</b> – New Rugged Servers
24	<b>Tri-M Systems Inc.</b> – 100Mhz PC/104 Module
35	<b>Tri-M Systems Inc.</b> – PC/104 Can-Tainer
17	<b>Twin Oaks Computing, Inc.</b> – CoreDX
3	<b>Vicor</b> – Custom power solutions
28	<b>VPT Inc.</b> – Efficient, reliable power
10	<b>White Electronic Designs</b> – We've cleared the board

## E-LETTER

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

- 10 GbE in net-centric warfare: Why commercial network cards can't drive the application  
*By Rob Kraft, AdvancedIO Systems Inc.*
- Creating a simulated environment for UAS operator training  
*By Yannick Lefebvre, Presagis*
- Protecting today's military electronics systems with real-time hardware/software protection countermeasures  
*By Paul Bradley, DAFCA, Inc.*

OpenSystems media.

# Military EMBEDDED SYSTEMS

DSP-FPGA.com

VME<sub>and</sub>  
Critical Systems

PC/104<sub>and</sub>  
small form factors  
THE JOURNAL OF MODULAR EMBEDDED DESIGN

INDUSTRIAL  
EMBEDDED SYSTEMS

CompactPCI<sub>and</sub>  
AdvancedTCA Systems

Embedded COMPUTING  
DESIGN

## Military & Aerospace Group

**Chris Ciuffo**, Group Editorial Director  
cciufo@opensystemsmedia.com

**Hermann Strass**, European Representative  
hstrass@opensystemsmedia.com

**Sharon Schnakenburg-Hess**  
Assistant Managing Editor  
sschnakenburg@opensystemsmedia.com

**Konrad Witte**, Senior Web Developer

**Steph Sweet**, Creative Director

**Jennifer Hesse**, Assistant Managing Editor  
jhesse@opensystemsmedia.com

**Joann Toth**, Senior Designer

**David Diomede**, Art Director

**Terri Thorson**, Senior Editor (columns)  
tthorson@opensystemsmedia.com

**Phyllis Thompson**  
Circulation/Office Manager  
subscriptions@opensystemsmedia.com

**Monique DeVoe**, Copy Editor

## Sales Group

**Dennis Doyle**, Senior Account Manager  
ddoyle@opensystemsmedia.com

**Regional Sales Managers**  
**Ernest Godsey**, Central and Mountain States  
egodsey@opensystemsmedia.com

**Tom Varcie**, Senior Account Manager  
tvarcie@opensystemsmedia.com

**Barbara Quinlan**, Midwest/Southwest  
bquinlan@opensystemsmedia.com

**Rebecca Barker**, Strategic Account Manager  
rbarker@opensystemsmedia.com

**Denis Seger**, Southern California  
dseger@opensystemsmedia.com

**Andrea Stabile**  
Advertising/Marketing Coordinator  
astabile@opensystemsmedia.com

**Sydele Starr**, Northern California  
sstarr@opensystemsmedia.com

**Christine Long**, Digital Content Manager  
clong@opensystemsmedia.com

**Ron Taylor**, East Coast/Mid Atlantic  
rtaylor@opensystemsmedia.com

### International Sales

**Dan Aronovic**, Account Manager – Israel  
daronovic@opensystemsmedia.com

**Sam Fan**, Account Manager – Asia  
sfan@opensystemsmedia.com

## Reprints and PDFs

**Nan Holliday**  
800-259-0470  
republish@opensystemsmedia.com

## Editorial/Business Office

16626 E. Avenue of the Fountains, Ste. 203  
Fountain Hills, AZ 85268  
Tel: 480-967-5581 ■ Fax: 480-837-6466  
Website: [www.opensystemsmedia.com](http://www.opensystemsmedia.com)

**Vice President Editorial:** Rosemary Kristoff

**Vice President Marketing & Sales:**  
Patrick Hopper  
phopper@opensystemsmedia.com

**Publishers:** John Black, Michael Hopper,  
Wayne Kristoff

**Business Manager:** Karen Layman





## » We Do Not Build Navy Ships «

### Our Customers Do.

At the heart of the most advanced command and control systems deployed in Navy ships are Kontron Military Rugged COTS boards and systems. Keeping us safe with smart applications, military contractors look to Kontron for superior technology, performance and life cycle management expertise.



Electronic Warfare



Infrared Surveillance



Multifunction Radar



Towed  
Array Sonar

Missile Launchers

Bow mounted  
Sonar



### MILITARY RUGGED COTS

Call, Email or Visit today.

Call: 1-888-294-4558

Email: [info@us.kontron.com](mailto:info@us.kontron.com)

Visit: [www.kontron.com/military](http://www.kontron.com/military)

If it's embedded, it's Kontron.



By Duncan Young

# Packet processors to speed and protect military networks



Commercial network technology will be migrating deep into the digital battlefield to enhance performance, maintain service, and provide a more secure communications environment. Battlefield Network Enabled Capability (NEC) extends from individual soldiers, through Virtual Private Networks (VPNs) in chassis, vehicles, or shelters to the complete command infrastructure. The constant flow of information through shared network-based applications such as situational awareness, voice/data communications, and signals intelligence/surveillance is an essential element of today's sophisticated information-centric warfare environment. To meet the demands for growth, commercial networks employ packet processors to perform a broad range of tasks to manage networks, offload performance-sapping tasks such as encryption, and inspect payload content at 10 Gbps line speeds and more.

## Performance and network security

Just as commercial networks and the military's command and operations network infrastructure require continuous performance growth to meet users' expectations, so do battlefield networks. For example, network-centric applications such as sharing, analyzing, and annotating images from multiple sensors are very demanding of both network and computing resources. These applications can also extend across many tiers of battlefield command and multiple coalition partners with the resultant burden of varying security classifications between the many different systems and participants. The prevention of intrusion and the maintenance of network and data integrity are high priorities.

A common point of vulnerability is the IP address which, if unprotected, can lead to unauthorized access, denial of service attacks, or virus planting. IPsec, which is a mandatory part of IPv6 but only optional for IPv4, provides IP address protection through negotiated message transfers and

encryption. But IPsec is not yet universally implemented. Payload content can be further protected with additional levels of encryption that might vary in type with the data's sensitivity. However, the implementation of IPsec, payload security, and the trend for increased line speeds from 1 Gbps to 10 Gbps impose significant additional levels of processing that many subsystems and networks do not have. In addition, changing defense funding priorities means that many legacy fighting vehicles are now being modernized in preference to replacement, introducing many of the capabilities developed specifically for participation in the NEC environment.

## Packet processing

To meet the needs of network performance and security, packet processors can offload many of the protocol processing layers. And because of their performance potential, packet processors can perform many additional network management and security operations at line speeds. Packet processing provides the performance and capability for perimeter defense, encryption/decryption, virus checking, IP routing and address translation, and detection and prevention of service attacks within embedded computing subsystems, switches, and routers. However, packet processors are also able to analyze the payload content, even at Gbps line speeds, known as Deep Packet Inspection (DPI). DPI can determine the packet type such as voice or data, e-mail, or security threat and includes sophisticated pattern matching to identify packets that might require further processing before dispatch.

These requirements for packet processing have spawned a new generation of high-performance, multicore processing devices based on, for example, PowerPC (Freescale Semiconductor) and MIPS64 (Cavium Networks) cores. These Systems-on-Chip (SoCs) offer from 4 to 16 processor cores with GHz clock rates, on-chip pattern matching and security engines,

high-bandwidth memory interfaces, and flexible multi-GHz connectivity options to host processors and networks. GE Fanuc Intelligent Platforms has adopted Cavium Networks' OCTEON packet processing devices and software to power a range of commercial, standards-based telecommunications products. For military applications requiring extended environmental performance or conduction cooling, VPX (VITA 46) provides the ideal platform for implementations in either 3U or 6U formats. Depicted in Figure 1 is the NPA-58x4, a 4-port GbE AdvancedMC packet processor based on the Cavium OCTEON, transforming into reality the idea that efficient real estate, performance, and functionality could be achieved based on a 3U VPX military-grade product.



**Figure 1** | NPA-58x4 AdvancedMC module from GE Fanuc Intelligent Platforms

GbE is widely implemented and well supported by an ecosystem of multiple vendors of embedded computing equipment including SBCs, switches, routers, software, backplanes, and packaging standards suitable for use in military vehicles. These embedded systems will migrate through 10 GbE and 40 GbE for copper backplanes to the 100 GbE fiber standards of the future. Offloading protocol stacks, maintaining network integrity, and establishing secure zones, media gateways, and firewalls without compromising embedded system performance are key application areas that packet processing is set to benefit.

*To learn more, e-mail Duncan at [young.duncan1@btinternet.com](mailto:young.duncan1@btinternet.com).*



## High-voltage power distribution enhances platform modernization



By John Wemekamp



The new generation of ground-based vehicles has moved away from the traditional 28 VDC power generation and distribution systems to high-voltage systems of typically 610 VDC, achieving great savings in space, weight, cost, and efficiency. Although easier to implement on new vehicle designs, high-voltage technology and many of its component parts can also be introduced into existing vehicles to great effect – without the whole scale and potentially disruptive replacement of every 28 VDC powered electromechanical or electronic subsystem. Modernization programs aim to improve the warfighter's operational effectiveness and survivability.

The continued presence of North Atlantic Treaty Organization (NATO) partners in areas of conflict has, for many nations, shifted combat doctrine and drained budgetary resources away from new large-scale ground vehicle procurement programs. Instead, life extension and modernization of existing fleets of armored vehicles is proposed – providing enhanced crew survivability – to add more firepower, increase situational awareness by introducing more Network Enabled Capability (NEC), and reduce maintenance and life-cycle costs. The recent rounds of rationalization, typified by the manned ground vehicle elements of Future Combat Systems (FCS), will result in the migration of new technologies into a series of phased modernization and update cycles for the current armored vehicle fleets to meet these objectives.

### Mixed high- and low-voltage power systems

Significant weight, space, and efficiency gains will be achieved even by the partial adoption of new high-voltage power systems. Much of the new electrical technology is high-voltage based, whether power generation, distribution, all forms of motion control, driver control, or environmental controls. Modernization initiatives to infuse this technology into older vehicle types will result in two scenarios:

- Change out of the power-generation system to the new high-voltage standard plus the introduction of some new high-voltage subsystems along with the retention of legacy 28 VDC subsystems.
- Continue to generate power at 28 VDC but introduce some new technology subsystems requiring high voltage.

Both scenarios will utilize new power conversion technology between high voltage and 28 VDC or vice versa plus the inclusion of side-by-side distribution and switching systems.

Where and how this power conversion takes place will have a vital impact on a vehicle's weight and space available for other equipment. A large armored vehicle such as a Main Battle Tank (MBT) might require 100+ kW power generation capability. At 28 VDC, this equates to 3,500 A to be distributed around the vehicle, requiring heavy cables and massive switchgear.

Obviously, using a higher voltage reduces the current, allowing smaller, lighter cabling and switchgear. But crew safety also becomes a consideration, requiring additional physical protection of cables and connectors as well as the inclusion of ground fault detection circuit breakers.

### Motion control

Motion control is one of the greatest consumers of power in an armored vehicle. Its applications range from the operation of hatches, fans, and pumps, to the environmental control of work-spaces and electronic equipment, to a complete turret assembly. By providing a multi-axis stabilized platform for weapon, sensor, and crew systems, a typical turret system can require tens of kW per axis to control. The new generation of smart Servo Motor Controllers (SMCs) offers more opportunities for reducing weight and space. By providing high-power, three-phase synchronous output to the motor, an SMC can be directed to perform complex, preprogrammed movements by commands received via dual-redundant control buses such as CANbus or Ethernet.

Using solid-state switching and microprocessor technology, these SMCs offer increased reliability plus an inherent capability for sharing diagnostic and future prognostic results with other vetronics subsystems. Curtiss-Wright Controls Electronic Systems has played a major role in the development of equipment and installation technology for high-voltage ground vehicle power distribution, in addition to switching and motion control systems. Illustrating this breadth of expertise is a family of rugged, high-efficiency SMCs, packaged as Line Replaceable Units (LRUs) for vetronics applications, shown in Figure 1. Such an SMC can deliver two axis controls at up to 23 kW per axis in a package weighing only 22 lbs.



**Figure 1** | Curtiss-Wright Controls Electronic Systems' family of rugged, high-efficiency SMCs, packaged as LRUs for vetronics applications.

Inserting high-voltage power technology into existing vehicle fleets will undoubtedly create significant savings in weight, space, and efficiency. However, careful trade-offs will be needed to ensure the optimum savings and benefits, particularly as phased introductions of new technologies into each vehicle type are proposed. This will require a deep understanding of each vehicle's power infrastructure, its EMI characteristics, future upgrade plans, and crew safety requirements to create each optimal solution set.

To learn more, e-mail John at [john.wemekamp@curtisswright.com](mailto:john.wemekamp@curtisswright.com).





# We've cleared the board.

## It's your move.

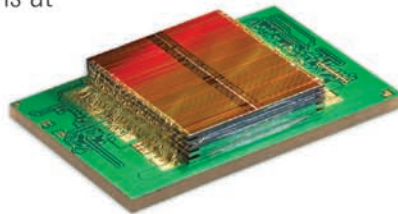
Space-saving system-in-a-package and multi-chip solutions from White Electronic Designs free up board space to make room for your big ideas.

Try our new DDR2 SDRAM that packs 1 GByte into a SnPb BGA package less than  $1/2$  in<sup>2</sup> ... or our new embedded SLC NAND flash BGA that has the performance of a solid state disk drive in a form factor that is one-fourth the volume of a comparable compact flash-based product.

WEDC lean microelectronic solutions are designed to solve component incompatibilities, reduce design complexity, and extend product life and environmental performance in military applications. We offer turnkey design, assembly and test of custom multi-chip solutions and a wide range of standard military off-the-shelf space-saving solutions.

Expand the possibilities; explore your options at [www.whiteedc.com/move](http://www.whiteedc.com/move).

602.437.1520 TEL | 602.437.9120 FAX



WHITE ELECTRONIC DESIGNS

[www.whiteedc.com](http://www.whiteedc.com)

Customer First. Quality Always.

# Legacy Software Migration

By Bill Errico



## Application modernization provides link between historical systems and contemporary technology

*During an era when battlefield technology is rapidly evolving, the DoD's goal is to ensure that the warfighter is equipped with best-of-class, mission-critical technology. Despite the need to stay ahead of the technology curve, the government's budget cycle can sometimes be out of sync with these objectives. Through application modernization, however, COBOL applications can be extended into new environments, enabling agencies to leverage the benefits of modern technologies such as Web and Service Oriented Architecture (SOA) enablement, and cloud computing.*

### Themis' New Rugged Servers Have Speed to Burn and Keep Their Cool.

#### New! 1RU RES Servers

- One or two Intel® Quad-Core 5500 Series Xeon® CPUs with Intel Nehalem Microarchitecture
- Up to 96GB ECC SDRAM
- Up to 3 removable and lockable 2.5" HDDs
- One PCI-E 2.0 x16 slot, optional SAS expansion
- 2RU RES Servers also available



RES-12XR3 server shown with optional filter door panels.

#### A New Era of Performance and Rugged Reliability

Themis' new family of XR3 Series of Rugged Enterprise Servers™ (RES) includes the latest Quad-Core Xeon processors and Nehalem Microarchitecture from Intel. These new Intel chips revolutionize server performance, and Themis' robust designs - only 20" depth - provide the reliability to keep mission critical applications running. Themis servers provide far greater reliability, improved life cycle management and substantially lower TCO than other COTS systems solutions.

#### Features in the RES-XR3 servers include:

- Dual redundant, hot-swappable power supplies
- Dual redundant DC power option
- Operating shock - 3 axis, 25G, 20ms
- Operating vibration - 3.0 Grms, 8Hz - 2000Hz
- Light weight, corrosion resistant, 20" depth chassis
- Optional air filter door panels

So when the environment gets tough and your data is critical, turn to the company that builds systems to perform in the harshest conditions. For Sun® Solaris™, Linux®, and Microsoft® Windows® environments. For more information on Themis' rugged new servers, please visit [www.themis.com](http://www.themis.com).

Themis rugged, mission-critical computers. Designed to take it.

(510) 252-0870.

## THEMIS

Transformational.

©2009, Themis Computer, Themis, the Themis logo, and Rugged Enterprise Servers are trademarks or registered trademarks of Themis Computer. All other trademarks are the property of their respective owners.

Despite the recent push toward modern programming languages like Java and C++, the majority of government agencies still rely on COBOL for their mission-critical applications. One of the primary reasons COBOL still exists is because many decades of time and millions of dollars are often invested in DoD applications. Aside from the fact that rewriting applications with a more modern programming language, or replacing them completely, puts operability of the applications at risk, COBOL still provides real value to the agencies and organizations it serves. Because of the programming language's longevity, the systems have evolved with defense agencies and continue to perform mission-critical tasks in support of the warfighter efficiently and reliably, providing every reason for the DoD to keep these historical systems alive.

#### Modernization enables Web capabilities

Integrating modern technologies with the 50-year-old COBOL programming language, however, is no simple feat. As network-centric warfare becomes more dependent on Web capabilities for enhanced availability and streamlined logistical processes, upgrading critical applications for Web compatibility is a must.

Application modernization fosters communication between historical systems and contemporary technologies, while preserving the unique value encompassed in existing IT systems. A compelling alternative to rewriting or replacing critical applications, modernization is often deployable in less than two months, enabling a rapid response to mission changes and quick realignment of current applications in compliance with constantly evolving security requirements



“ Integrating modern technologies with the 50-year-old COBOL programming language, however, is no simple feat. As network-centric warfare becomes more dependent on Web capabilities, ... upgrading critical applications for Web compatibility is a must. ”

and federal regulations. Modernization can also save agencies millions of dollars, and in many cases reduces operating costs by up to 80 percent. As the applications often reflect the investment of innumerable resources and years of code modified to meet the specific demands of individual agencies, changing the code can put operability in jeopardy. However, modernization eliminates the risk factor because it does not require the alteration of a single line of code. Instead of altering the code, the server emulates a mainframe execution environment, working with the target operating system to allocate memory for the historical application.

### The shift toward cloud computing

As agencies government-wide are starting to turn to modern technologies like cloud computing for enhanced availability and efficiency, defense agencies that rely on historical systems can be quick to follow through the use of modernization. Modernizing critical applications using Service Oriented Architecture (SOA) provides agencies otherwise bound to the mainframe environment the ability to leverage these modern technologies. Inserting an added layer of wrapper code that enables access to business functions, COBOL applications can now operate in a Web 2.0 environment, providing a responsive and rich Internet application, using unchanged code. The now-Web-based applications maintain the same functionality as when tied to the mainframe. Business regulations might have moved platforms with a Web 2.0 interface added, but quality assurance testing time is ultimately reduced because the application business logic remains untouched.

Security risks are often cited as the number one concern when upgrading systems for cloud computing compatibility. Government agencies concerned with a loss of

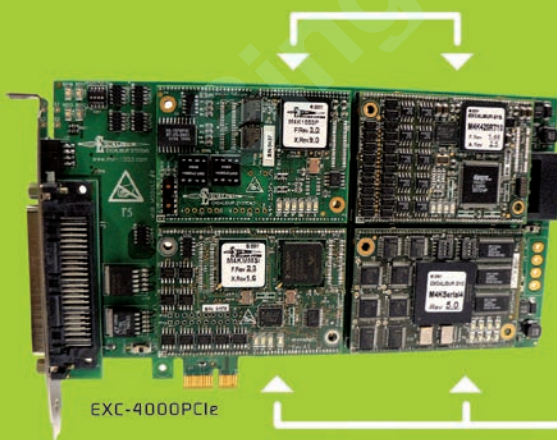
control over the environment in which the applications are executing can still leverage the benefits of cloud computing by taking practical steps toward the cloud, without making the full commitment. One solution is to transition applications to a private cloud, providing the same Web benefits from within the boundary of an agency's own firewall. A private cloud enables agencies to leverage benefits such as pay-as-you-go licensing and elasticity, from within their own data centers, at their own pace.

As government agencies continue to shift toward cloud computing, historical systems do not need to act as a barrier to defense agency modernization. Implementing modernization solutions allows defense agencies to leverage the benefits of modern technologies such as cloud computing, SOA, and Web-based technologies, ultimately providing the warfighter with more advanced battlefield technology at a faster time-to-deployment.

**Bill Errico** is vice president of federal sales and marketing at Micro Focus. He can be contacted at [Bill.Errico@microfocus.com](mailto:Bill.Errico@microfocus.com).

## express yourself

Excalibur's **NEW** PCI Express MagiCard



User upgradeable  
Multiprotocol  
9 Avionic Buses

up to four  
independent  
modules

MIL-STD-1553  
MIL-STD-1760  
MMSI/AS5652  
HOO9  
ARINC-429  
ARINC-708  
Discrete  
CAN Bus  
Serial

Extended temperature &  
ruggedization available.

Supported by **EXALT**



Systems • Data Recorders • Avionic Cards • Software  
Couplers • Terminators • Connectors • Cables

One Step Ahead

**www.mil-1553.com**



# Daily Briefing:

By Sharon Schnakenburg-Hess, Assistant Managing Editor

News Snippets

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

## 3U CompactPCI joins U.S. Army ranks

Following the trend of an increasing number of 3U (and sometimes even smaller) form factors enlisting for duty, prime Northrop Grumman recently marshaled yet another war for the U.S. Army's Small Tactical Airborne Radar (STARLite) synthetic aperture radar (Figure 1): BittWare's GT-3U-cPCI (GT3U) ruggedized 3U CompactPCI board. The agreement stipulates delivery of an unquantified "large production order" of the GT3U hybrid signal processing boards, which are powered by an onboard Altera Stratix II GX FPGA and a group of four onboard ADSP-TS201S TigerSHARC DSPs for flexibility. The boards will provide STARLite's "high-end" signal processing, which combines numerous radar images into a single high-res image, with the goals of target coordination and unprecedented situational awareness for ground-troop protection plus increased surveillance capabilities.



Figure 1 | STARLite synthetic aperture radar image of Fort Huachuca facilities, courtesy of Northrop Grumman

## RFID system spins 'military technology'

The phrase "military technology" often conjures mental images of warfighters' battlefield wares. However, the Marine Corps Base Camp Pendleton (MCBH) is giving the phrase a slightly different spin, thanks to a Web-based RFID tracking system by 3M, slated to enable Anchorage's Alaska National Guard and MCBH in more efficiently managing 40,000+ personnel records. The result: a projected accuracy increase plus a man-hour decrease equating to about \$1.5 million per year. The primary catalyst: 3M's File Tracking Software V3.0, proven at the recent Marine Corps Base Hawaii's pilot RFID project and used with 3M's D4 RFID tag. File Tracking Software V3.0 supports Windows Vista and offers Internet reporting and locating capabilities that render it usable on any Web-browser-enabled computer. Consequently, custom reports and item lists are easily generated, and personnel can be more rapidly reassigned or deployed.

## RATS welcome on the battlefield, by way of Android

While cell phone manufacturers and consumer gadgeteers were the first to appreciate Google's Android mobile operating system, defense industry pundits have been quite reluctant about its battlefield suitability. However, a combat-savvy incarnation of Android has emerged as the Raytheon Android Tactical System (RATS). RATS renders fast delivery of multimedia content such as full motion video and images to warfighters, via intelligence data dissemination utilizing RATS' Distributed Common Ground System (DCGS) Intelligence Backbone (DIB) system architecture. The benefit: DIB content viewing can take place immediately and can be searched by other mobile device users, enabling decision-making within seconds instead of hours. RATS "widget" applications in development are biometric collection including facial recognition, in addition to streaming video camera feeds and license plate reading, Raytheon reports. Rest assured, "some lightweight encryption" will be enabled, as will even more features, *Forbes* reports. (See *Raytheon Sends Android To Battlefield*, [www.forbes.com/2009/10/19/android-google-military-technology-wireless-raytheon.html](http://www.forbes.com/2009/10/19/android-google-military-technology-wireless-raytheon.html))

## First OpenVPX contract?

At the speed of light, it seems, the once-controversial OpenVPX Industry Working Group has very recently (and very peacefully) surrendered its recommended VPX system interoperability specification back into VITA/VSO's hands by way of VITA 65. And only a proverbial minute later ... Mercury Computer Systems, who spearheaded the OpenVPX (Figure 2) effort, has already announced "a multimillion-dollar system order from a leading defense supplier" for Mercury's OpenVPX wares. The unnamed defense supplier will utilize various technologies within Mercury's (OpenVPX) Ensemble 6000 Series for a global radar update. The deliverable: signal processing tucked inside a heterogenous environment within an overarching infrastructure of robust systems management. The pace: Fast. Mercury's support and services for complete subsystem development, validation, and qualification will comply with the defense supplier's Quick Reaction Capability (QRC) requirement: Integrated OpenVPX-based architecture delivery within 10 months (at most) and low-rate initial production in fewer than 16 months.



Figure 2 | Within days of the OpenVPX Industry Working Group sending its recommendations to VITA/VSO, Mercury announced a "multimillion-dollar system order from a leading defense supplier."



## U.S. Army signs a 'fitting' contract

The U.S. Army recently put pen to paper for a \$19 million Land Warrior maintenance contract with General Dynamics C4 Systems, which stipulates a year of "maintenance" for the presently-in-combat, modular, integrated Land Warrior fighting system ensembles (Figure 3). The team-leader-level ensembles include a small computer that heightens navigation and situational awareness capabilities, a helmet-mounted display, and a radio connectivity headset. Meanwhile, provided under the contract are logistics support and comprehensive engineering, in addition to maintaining returning-from-theater and training ensembles. The contract also affords two option years, which could boost the contract's value to \$50 million. The contract's inanimate beneficiaries are the U.S. Army's 300 kits for vehicle integration, along with 900 Land Warrior ensembles and associated Land Warrior equipment.



**Figure 3** | A Land Warrior fighting system ensemble, photo courtesy of General Dynamics C4 Systems

## Common thread woven among Navy subs

The 109-year-old U.S. Navy submarine force is nothing if not diverse, considering its lineup of SSBN fleet ballistic missile submarines, its SSGN guided-missile submarines, and its SSN attack submarines. But what is the common thread amongst all U.S. Navy subs? They will all soon sport the capability of two-way, real-time communications with surface ships, land-based assets, and aircraft – minus the requirement to emerge to periscope depth – as part of the U.S. Navy's Communications at Speed and Depth (CSD) program. Having successfully completed a recent CSD Preliminary Design Review (PDR), prime Lockheed Martin plans to reach *fait accompli* by providing a triad of types of two-way communications buoys plus associated submarine accoutrements and shore equipment. Two genres enable UHF and Iridium satellite transmission, while the third consists of an aircraft- and submarine-launchable acoustic-to-RF gateway system.

For consideration in Daily Briefings, submit your press releases at <http://submit.opensystemsmedia.com>. Submission does not guarantee inclusion.



**Figure 4** | U.S. Air Force officials at Germany's Ramstein Air Base recently said goodbye to their final C-130E Hercules, U.S. Air Force photo by Airman 1st Class Caleb Pierce

## C-130E says 'goodbye' ... and 'hello'

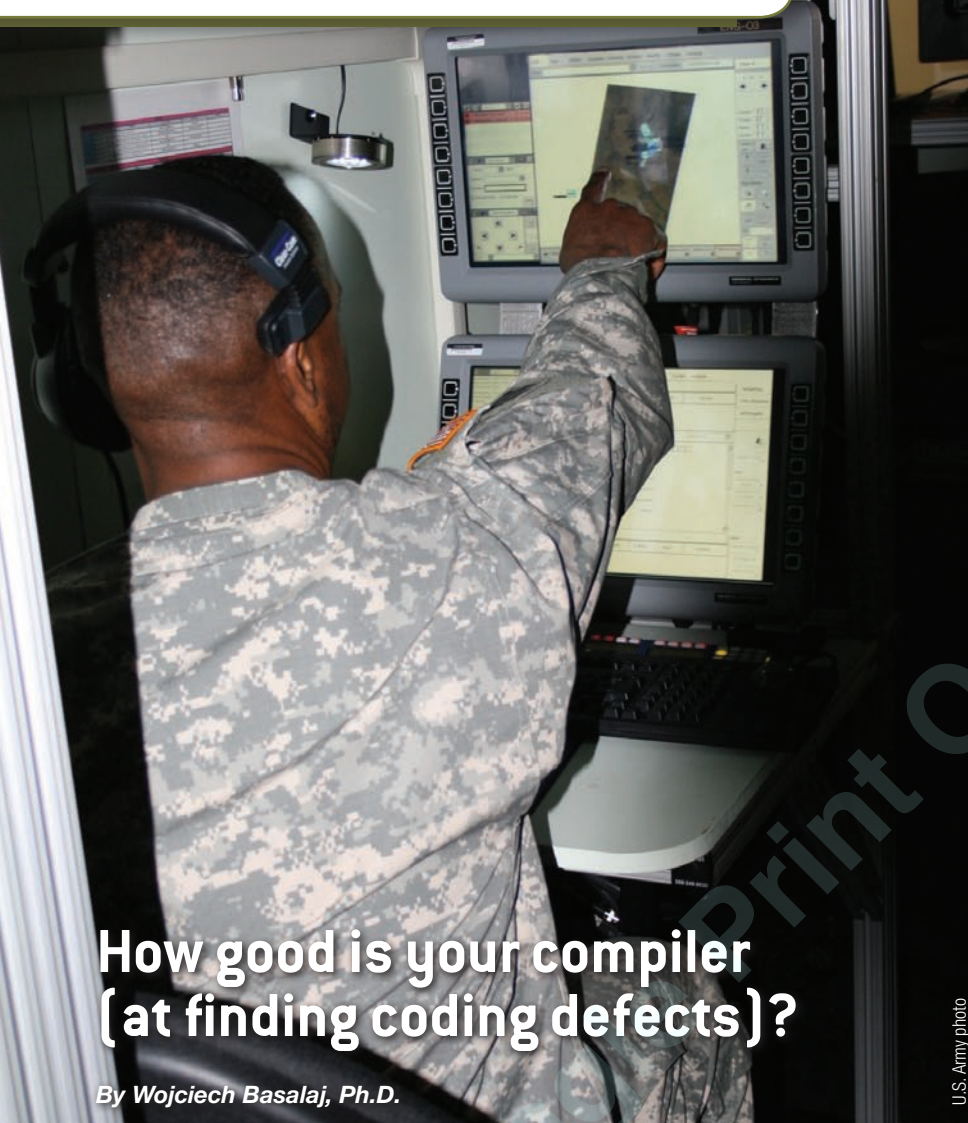
U.S. Air Force officials at Germany's Ramstein Air Base recently bid a fond farewell to their final C-130E Hercules (Figure 4). The C-130E then flew to its new home – the Powidz Air Base in Poland – per a Foreign Military Sales lease agreement between Poland and Air Force Materiel Command, signifying three primary milestones: 1) The C-130E's conclusion of about 40 USAF service years; 2) a new era for the Polish air force, which previously used the CASA C-295 twin turboprop as its primary aircraft for tactical transport (CASA C-295 can accommodate 70 passengers or 7.5 tons, while the more cargo-savvy C-130E can heft a 17-ton payload or 90 fully equipped passengers); and 3) the United States' transition to the updated and upgraded C-130J, featuring automation and computerization so advanced that the navigator and flight engineer positions have, consequently, been eliminated.

## Seeing the light ... in tunnels, behind walls

Did you see that? Odds are good that the answer is a resounding "no" when an object is located within a tunnel or behind a wall. However, the answer has now changed to "yes," courtesy of a phase II Department of Army contract with TiaLinx, Inc. The contract affords continued development of a V-band miniature antenna array to be integrated into TiaLinx's Eagle60 Ultra-wideband (UWB) Radio Frequency (RF) imaging systems. The systems utilize advanced mm-wave RF distributed sensors to enable users to even see movement of live objects within tunnels or behind walls (Figure 5), provide visual detection of landmines or unexploded ordnances, and render land, sea, and air surveillance in smog, rain, and fog.



**Figure 5** | A new V-band miniature antenna array means users can even see movement of live objects within tunnels or behind walls.



### How good is your compiler (at finding coding defects)?

By Wojciech Basalaj, Ph.D.

*Many believe that if source code compiles cleanly, with all warnings activated, then it is ready to move on to a verification stage such as test or code review. However, it is dangerous to assume that if the code has compiled cleanly, then any errors present must have resulted from the interpretation of the requirements and not their implementation. Wojciech empirically evaluates this assumption and proves that the range of warnings provided by any compiler is extremely limited when compared to those produced by a dedicated static analysis and Coding Standards Enforcement (CSE) tool.*

It is a commonly held view that if source code compiles cleanly, with all warnings turned on, then it is ready for verification such as test or code review. The danger with this assumption is that if the code has compiled cleanly, then any errors present must be in the interpretation of the requirements and not in their implementation. However, an empirical evaluation of this assumption ultimately shows that the range of warnings provided by any compiler is seriously limited when compared to those produced by a dedicated static analysis and Coding Standards Enforcement (CSE) tool.

The comparisons made herein use the GNU Common C++ “2” version 1.6.3, a real-world code base of around 42,000 lines of code. As this is a cross-platform library, it does not favor any particular compiler and can be used as a representative sample that any compiler might be expected to handle. Its modest size allows all compiler warnings to be manually reviewed for their accuracy, while ensuring at the same time that their diversity and amount is non-trivial.

The four compilers examined are GCC, Visual C++, C++Builder, and Intel C++ Compiler, along with a static analysis and CSE tool to show that if developers rely too heavily on their compiler to identify coding defects, they might find that their code isn’t maintainable, reusable, or portable. In addition, Visual C++ “Team edition” supplements its standard compiler warnings with a “code analysis” feature, the output of which is included in these results.

#### Warning outputs generated

In practice, every one of the defects missed by one of these four compilers has an impact on the quality of the code base, be that in its maintainability, portability, or reusability. That represents a significant threat when deploying the code, despite the fact that the majority of the sample source code passes the compilers’ architected checking parameters.

As these compilers are based on different front-ends, different warnings can be anticipated from each. Table 1 presents a side-by-side comparison of distinct warnings generated by each compiler, and by the static analysis tool, for the code base used in our comparison: GNU Common C++ “2”. The latest version of each compiler available at the time our results were compiled was used with the maximum warning level enabled. (The header row of Table 1 indicates the exact compiler versions and options used.) Rather than benchmarking these compilers relative to one another, their warning outputs were compared with a static analyzer for C++.

As indicated in the last row in the table, the CSE tool generates in excess of 400 warnings, while none of the compilers tested even manage to return 20. In fact, static analysis is empirically shown to identify 25 times more warnings than the best among all four compilers – Visual C++ with Code Analysis enabled (/analyze option). It is interesting to note that without this feature enabled, Visual C++ generates the fewest warnings among all the compilers tested.

The first column of data in Table 1 shows the percentage of warnings generated by each compiler that were also detected by the static analysis tool. Note that the degree of overlap is high, with an average



## Big Performance in a Small Package

Need a flexible, open-architecture communications infrastructure?

Concerned about data interoperability?

Struggling with constrained resources?

Save time and money by using a proven, interoperable communications middleware solution.

CoreDX provides a robust, quality-of-service enabled Data Distribution Service. Our implementation is perfect for embedded systems with constrained resources and a need for high-throughput, low-latency communications.

Integrate CoreDX today and launch your product.



Navy photo by Photographer's Mate 3rd Class Todd Frantom.

**Try the FREE CoreDX evaluation today!**

 **TWIN OAKS COMPUTING, INC.**  
 Innovative Software Solutions

[www.twinoakscomputing.com](http://www.twinoakscomputing.com)

	PR Static Analysis Tool	GNU GCC	Microsoft Visual C++	Microsoft Visual C++	CodeGear C++ Builder	Intel C++ Compiler
	2.5	4.3.2	2008	2008	2009	11.0.066
	all checks	-W -Wall -pedantic	/W4	/analyze /W4	All warnings	/W4
<b>Overlap</b>						
GCC warnings	88%					
VC++ /W4 warnings	100%					
VC++ /analyze warnings	73%					
C++Builder all warnings	92%					
Intel C++ /W4 warnings	67%					
ISO C++ conformance		17%	11%	11%	11%	11%
Portability problems		0%	0%	0%	6%	0%
Design problems		1%	2%	7%	3%	2%
Local standards		0%	0%	10%	0%	0%
Efficiency and use of C++		0%	0%	0%	0%	0%
Maintainability		3%	3%	3%	5%	4%
Coding style		2%	0%	0%	0%	3%
<b>Average overlap</b>	<b>84%</b>	<b>3.1%</b>	<b>2.4%</b>	<b>4.4%</b>	<b>3.6%</b>	<b>2.9%</b>
<b>Distinct warnings</b>	<b>412</b>	<b>8</b>	<b>7</b>	<b>16</b>	<b>12</b>	<b>13</b>

**Table 1 | Default detection comparison** – The basis of comparison and each percentage figure is the ratio between distinct warnings reported by a compiler and a static analysis tool within a given category. The header row details the exact compiler versions and options used to enable the maximum warning level.

84 percent of compiler warnings replicated by the CSE tool. This side of the comparison is only given for completeness, as developers would be expected to enable compiler warnings regardless of whether or not static analysis is performed.

The remaining rows of Table 1 show the other side of the comparison: How much of what is statically detectable do compilers flag? It is evident that compiler warnings steer clear of the “Efficiency and use of C++” category. This is expected, as compiler optimizations are performed in the back-end, typically silently. However, it is worth noting that dedicated CSE tools have a range of checks in this category focused on inefficient design, which cannot be corrected automatically, unlike low-level compiler optimizations.

### Common warnings missed

Portability is a common warning category missing from a compiler’s arsenal. Only C++Builder generated a single warning that can be classified as a portability issue, compared to 17 flagged by the static analysis tool. These represent those constructs that comply with the ISO C++ Language definition but can cause problems with different compiler implementations. It is not uncommon for compiler vendors to lock developers in by offering

extensions to ISO C++, and it is unsurprising that portability is not high on the agenda for them. This represents another aspect of portability concerns, conformance to ISO C++, which is addressed by a separate warning category in the static analysis tool.

To most compiler vendors, ISO C++ compliance boils down to accepting as much valid C++ code as possible, while sidestepping the issue of detecting non-conforming code – often their own language extensions. Detecting ISO C++ non-conformance is one of a CSE tool’s strengths, which is evident from Table 1. It is apparent that most compiler warnings can be classified as (code) “Design Problems” and “Maintainability,” with some so minor as to merit them being demoted to style issues. However, even for these focus areas, the coverage compared to the static analysis tool is far from comprehensive, standing at 7 percent for the best contender – Visual C++ with code analysis feature.

Other warning categories that compilers traditionally avoid include: naming conventions, code layout, complexity metric thresholds, and banning certain keywords (for example, throw) and functions (for example, malloc), with a notable

exception of a Visual C++ code analysis feature that has hardwired warnings for use of `_alloca`, `_snprintf`, and `TerminateThread` functions. As this is not as comprehensive as the static analysis tool's configurable check that allows any function to be specified, half a point was awarded, giving this compiler a score of 10 percent for Local (company specific) Standards enforcement. The primary benefit of enforcing the aforementioned areas is enhanced reusability of code, and it is apparent from Table 1 that this is virtually untapped by compilers.

Coding standard enforcement	Static analysis tool	GCC	Visual C++	VC++ / analyze	C++ Builder	Intel C++
HICPP violations detected	16399	3	33	42	40	63
JSF++ violations detected	33968	3	23	26	41	43
MISRA C++ violations detected	9082	25	70	72	76	67
Average overlap with static analysis tool		0.10%	0.35%	0.38%	0.40%	0.42%

Table 2 | Coding Standard Enforcement (CSE) comparison

When comparing the actual warning instances produced by each tool, it would not be particularly enlightening to tabulate raw warning counts, so common

C++ Coding Standards will serve as an objective basis of comparison instead. As can be seen from Table 2, none of the compilers offer any noticeable enforcement of High Integrity C++, JSF++, or MISRA C++, compared to the violations recorded by the CSE tool.

#### CSE tool: Most comprehensive/transferable route

It is a common misconception that compiler warnings are a sufficient means of statically analyzing source code. The range of warnings available from market-leading compilers is limited compared to a dedicated static analysis and CSE tool like PRQA's QA•C++. Moreover, the few checks that are available tend to be focused on code misbehavior and maintainability problems, with reusability and portability issues completely overlooked. A dedicated CSE tool offers comprehensive enforcement of all of these areas, while remaining compiler agnostic, so that code bases and development environments do not have to be tied down to a particular compiler and platform. ✚

**Dr. Wojciech Basalaj** has nine years of technical experience with PRQA in the Consulting Services Group and is the most senior Technical Consultant.

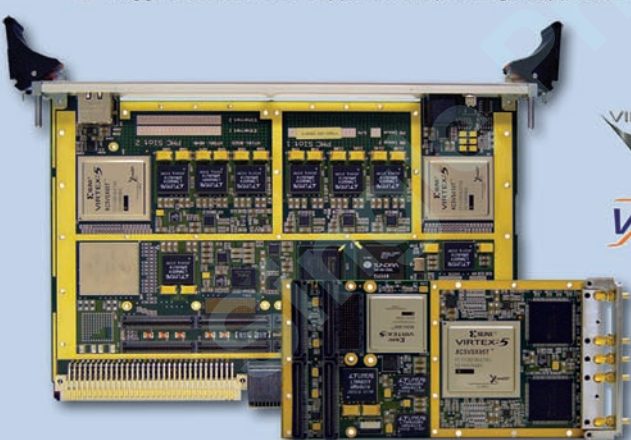
Wojciech graduated from King's College, London with a First Class BSc degree in Computer Science in 1997. As part of the course, he undertook a one-year industrial placement at Lucent Technologies Wireless in Winchester, UK. Wojciech obtained his Ph.D. in the field of Information Visualization at Trinity College, Cambridge. He can be contacted at [Wojciech\\_Basalaj@programmingresearch.com](mailto:Wojciech_Basalaj@programmingresearch.com).

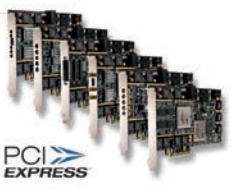
PRQA  
617-273-8448  
[www.programmingresearch.com](http://www.programmingresearch.com)

## HIGH PERFORMANCE FPGA SOLUTIONS


### RUGGED EMBEDDED VXS & XMC SOLUTIONS

- PowerPC & Dual FPGA VXS compute cards
- Analog & Digital I/O and FPGA processing XMC mezzanines
- Processing and I/O for SigInt Radar and SDR applications
- Rugged solutions to support multiple target applications






PCI EXPRESS AND  
PCI-104 SOLUTIONS




INTEL FRONT SIDE BUS (FSB)  
FPGA MODULES




FPGA MINIATURIZED  
MODULES

Nallatech Inc.  
Toll Free: 1-877-44-NALLA  
[contact@nallatech.com](mailto:contact@nallatech.com)  
[www.nallatech.com](http://www.nallatech.com)



## Nallatech

a subsidiary of  
Interconnect Systems Inc.



© 2009 Nallatech Inc. All Rights reserved. All trademarks or registered trademarks are the property of their respective owners.





## VPX, VME & cPCI True Military ATR Enclosures

### Fly first class with CM Computers

We are conscious that not all military integrators will require a top class ATR chassis like our new SixHex series, but we can ensure that our fortunate customers will enjoy the experience.

It has been demonstrated in the field that ATR enclosures are crucial to your end system reliability and performance. Therefore we have developed a superior product to guarantee that your payload electronics are matched with excellence.



CM-ATR-35/SIXHEX  
1/4 ATR, 7 Slot, 800W PSU

### The perfect Sealed COTS solution for advanced military electronic systems

Breaking all limitations previously understood by chassis designers, our fourth generation Six Heat Exchanger ATR series meets the demand for high power solutions that require exceptional thermal performance and truly flexible system integration.

The SixHex is manufactured incorporating US military standard components throughout.



### Product Highlights

- Contaminant-free enclosure
- Available in 1/4, 1/2 & 1 ATR size
- VPX, VME & cPCI ready
- Accepts Conduction & Air-cooled 6Us
- Flexible top & bottom I/O wiring
- Integrated Temperature Control Unit
- Six internal Heat Exchangers
- Up to 1.8 KW total Power Dissipation
- Up to 150 W per slot
- Dramatically increases payload MTBF
- 2 User defined PSU DC outputs
- 20°C less than heat exchanger ATRs
- 45°C less than conventional ATRs
- Stand alone low weight solution
- Customizable to specific requirements
- Mounting Tray with quick release system



All our chassis products are delivered Tested and Certified by independent authorized Labs per MIL-STD-461E & MIL-STD-810F for immediate deployment in US Navy & US Air Force military Fighters and Helicopters.

**CM Computer SixHex: Pure Power, Pure Dissipation, Pure Thermodynamics**

Visit [www.cmcomputer.com](http://www.cmcomputer.com) or contact us at [info@cmcomputer.com](mailto:info@cmcomputer.com) to request our Chassis Catalog



**CM Computer**  
True Military COTS Products



# Releasing the full potential of FPGA-based designs

By Rob Evans

*For all the power and flexibility FPGAs bring to embedded designs, the additional development process injects new levels of complexity and constraint into the design workflow. Unifying the conventional hardware-FPGA-software design processes to make full use of FPGA reprogrammability is one way forward.*

As FPGA technology barnstorms its way through the military electronics and systems and virtually all other sectors of the embedded electronics industry, applications exploiting the advantages of programmable logic are becoming a mainstay. Communications, airborne, and control systems in particular benefit from the design flexibility, field reconfiguration, and parallel processing capabilities of FPGAs, while the short design cycle and simpler verification process help to get applications into the field faster.

In spite of the FPGA's pervasiveness, though, very few applications are truly harnessing the FPGA's full potential for flexible design. This limitation results from the fact that FPGA development has simply been added to, or at best bolted on to, the traditional software-hardware workflow. This isolated FPGA development stage adds significant complexity to the overall design process.

To simplify the overall undertaking and restore design choices, the individual design processes – hardware design, software development, and programmable hardware design – need to be brought together so they can be tackled as a single task. If this is implemented at a fundamental level where all the processes

share a single pool of design data and common design environment, the dominant and unique advantage of FPGAs – reprogrammability – can be used to advance FPGA-based designs to the next level. Key to harnessing the full flexibility of FPGAs is an understanding of their evolution, design challenges, and what can be done to restore harmony among the three major FPGA-containing system design aspects: hardware, programmable hardware, and software.

### FPGAs evolve from glue logic to SoCs

Upon entering the embedded market, FPGAs were first regarded as a convenient and efficient host for implementing large sections of “dumb” glue logic for which development need not involve or interact with other elements of the design process.

However, FPGA devices, and how they are used, have significantly evolved from the concept of convenient containers for mass digital logic. High-capacity FPGAs now host entire SoC designs, where core functional elements such as processors, memory, and high-speed data processing are implemented in the programmable space. In military embedded systems where the relatively low production runs

struggle to justify a new ASIC start, FPGAs provided a viable, cost-effective path forward for harnessing the physical simplicity and reliability benefits of an SoC approach.

Compared to simple glue-logic designs, a major difference with SoC implementations is that software and hardware development are now fundamentally bound to, and dependent upon, the FPGA design. This is because FPGA devices and support peripherals are the center and core elements of the physical design, and the embedded application software is hosted within the FPGA space. As a result, any change in the FPGA domain will have a significant effect on the hardware and software domains.

### Restrained innovation

Regardless of the interdependence between design domains, the conventional development process for an FPGA-based product design still reflects a traditional approach by regarding each part of the design (hardware, software, and now embedded hardware) as separate, disconnected tasks.

A change in one domain tends to lead to a disruptive, time consuming redesign in the others. This means that major



decisions such as hardware-software partitioning must be made (and locked in) early in the design cycle – just as they were with traditional “non FPGA-based” embedded designs. In practice, physical hardware (FPGA devices and peripheral hardware) and then programmable hardware elements are locked down, in sequence, before meaningful software development can proceed.

Those initial decisions define the parameters and constraints for subsequent development processes, so the design options are increasingly limited through each sequential process. For example, the selected FPGA device (and hardware peripherals) will define a performance ceiling that includes identifying which embedded IP can be implemented. In turn, the embedded hardware design will define the functional capabilities available to the software. Or it could be as simple as the FPGA device only supporting soft processors supplied by that device vendor, which in turn defines the programming options available to the application software.

Additionally, pursuing concepts like fine tuning a design’s performance by moving software algorithms into embedded hardware, changing from an embedded to hardwired processor, or opting for a different FPGA device type will force a substantial redesign in all domains – hardware, programmable hardware, and software. For mil/aero systems development where hard deadlines are mandatory, the resulting design cycle disruption is untenable, so most engineers avoid tackling this type of design exploration at all costs. Yet invariably, high performance and design stability are also paramount, so investigating processor options and the potential benefits of soft-to-hard algorithm transfers is essential.

### Restoring unity

As mentioned, simply adding the FPGA development process on to the existing design workflow constrains the ability to harness its full flexibility potential. In applications where the low NRE costs and rapid design are of particular advantage, the barriers imposed by conventional design processes are diluting those attributes. Yet this is just where FPGAs should be exploited to maximum effect.

The first step to restoring design choices and fully harnessing FPGAs is to bring the design processes – hardware design, software development, and programmable hardware design – into one sphere (Figure 1). By using a single design system



**Figure 1** | The full potential of FPGAs can be harnessed when embedded hardware development, physical hardware design, and software development all exist in a single, fundamentally connected design environment.

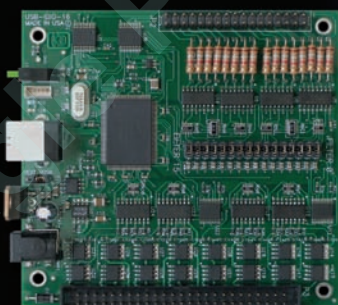
## USB Embedded I/O Solutions Stackable or Unstackable USB

### USB/104® Embedded OEM Series

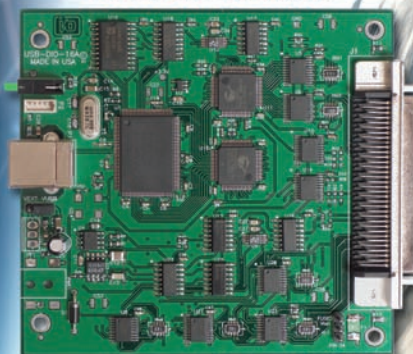
- Revolutionary USB/104® Form Factor for Embedded Applications
- USB Connector Features High Retention Design
- PC/104 Module Size and Mounting Compatibility
- Extended Temperature and Custom Options Available
- Choose From a Wide Variety of Analog, Digital, Serial, and Relay I/O



**16-Bit Analog  
Input 64-Channels  
500kHz**



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



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

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

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



**Saving Space,  
The Final Frontier**

**ACCES I/O PRODUCTS, INC.**  
The source for all your I/O needs

To learn more about our Embedded USB/104® I/O boards visit  
www.accesio.com  
or call 800 326 1649. Come visit us at  
10623 Roselle Street San Diego CA 92121



and application that draw from a single data model of the entire design, the design domains can interact and respond when design changes are made in an individual domain. In practice, each domain is using a subset of the same design and component library data. As a result, design changes such as moving functions between software and hardware or exploring alternative devices are simplified, since a change can easily (or even automatically) be reflected through all the domains.

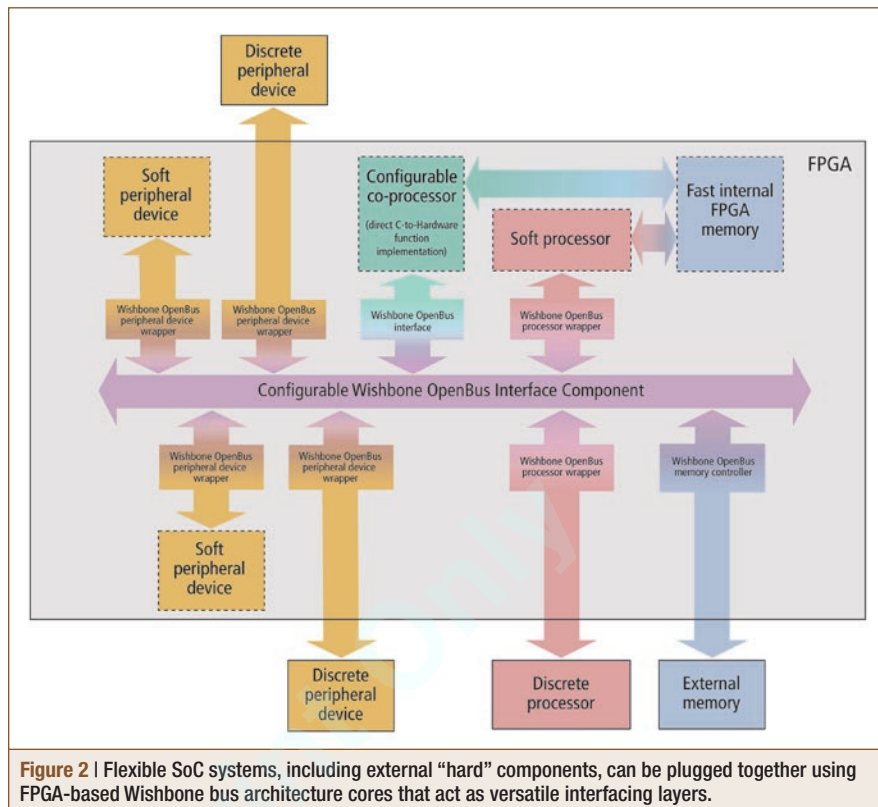
The design data and configuration files for the selected FPGA device, for example, are available to both the hardware and FPGA design domains, from the single pool of design data. If the FPGA device or its pin configuration is changed in the FPGA design space, that information is immediately available for implementation in the hardware design space. The action of exploring design options is more practical, while higher-level design functions like swapping pins between the hardware and FPGA design domains are simplified.

### Exploiting reprogrammability

In this singular design environment, developers can finally start to fully harness the flexibility of FPGAs. Take a typical situation where the most practical placement of physical hardware components creates extremely complex FPGA-to-peripheral connectivity, in part due to high-density BGA packaging. One answer is to bring the parts of that routing complexity inside the FPGA itself, by making strategic board connectivity paths via the FPGA's reassignable pins and internal routing.

Here, the FPGA's pin reassignment and internal routing capabilities are used to solve a board routing challenge, potentially reducing the board area and number of layer requirements. This concept, again, relies on the existence of a hardware-software-FPGA development environment that is connected at the platform level, as this is required to support intelligent and automated pin-swapping between the hardware-FPGA domains.

This unified design approach also opens up the possibility of implementing global software systems that raise the abstraction of the design process – such as schematic or graphically based embedded design



capture that is synchronized to both the hardware and software domains.

The natural extension of this design abstraction is to implement high-level embedded layers that effectively disconnect the soft elements of a design from the hardware on which it resides (Figure 2). These inserted layers “normalize” the interfaces between processors and hardware such as memory and peripherals, removing the need to deal with the low-level hardware complexity of I/O configurations and bus systems. Reconfiguring an FPGA design becomes a simpler, lower risk process, whether it's rebirthing legacy designs, configuring different production modes, reusing established IP, or performing post-production updates.

In practice, processors and peripherals can be supported by library-based FPGA cores based on the Wishbone bus architecture. The core abstracts a processor interface by effectively “wrapping” around the device, making it architecturally equivalent to other processors. It therefore allows a processor to be opportunistically changed without affecting the connected peripherals or forcing major redesign. Along with FPGA-based “soft”

devices, the concept can be extended to include hybrid hard-core processors, external processors, and off-chip discrete peripherals and memory devices.

### Next-generation FPGA design

The high-level unified embedded design approach outlined is made possible by capitalizing on the reprogrammable capability of the FPGA host. Any imposed layers and interfaces are automatically included in the FPGA's fabric, along with the functional design itself, enabling the hardware design to be dynamically explored without fatally disrupting the other parts of the design. ⊕



**Rob Evans** is a technical editor at Altium Limited. He has more than 20 years of experience in the electronics design and publishing industry, and studied Electronic Engineering at RMIT in Melbourne, Australia. Rob can be contacted at [rob.evans@altium.com](mailto:rob.evans@altium.com).

**Altium Limited**  
1-800-544-4186  
[www.altium.com](http://www.altium.com)



# Advanced cooling techniques beat the heat for rugged embedded COTS systems

By Ivan Straznicky

*Considering the environmentally intense environments faced by modern military electronics, the ability to meet the widest range of ruggedization and operating temperature requirements is an absolute must. And, when traditional Direct Forced Air (DFA) and conduction-cooling techniques are insufficient, designers are turning to more advanced approaches to save the day: Airflow Through (AFT) cooling, spray cooling, and Liquid Flow Through (LFT) cooling.*

Embedded COTS boards for deployed aerospace and defense applications have to be able to meet the widest range of operating temperature and ruggedization requirements. From air-cooled cards in relatively spacious racks aboard naval platforms, to conduction-cooled cards located in crowded corners of fighter jets, today's COTS boards need to perform on the tarmac of the desert at noon as well as in the cold environs of high-altitude flight.

With the increasing popularity of highly integrated small form factor 3U cards to deploy compute power in space-, weight-, and power-constrained platforms, embedded system designers are faced with an array of cooling approaches to address heat dissipation in rugged deployed COTS systems. When traditional Direct Forced Air (DFA) and conduction-cooling techniques aren't sufficient to handle cooling requirements (that is,  $-40^{\circ}\text{C}$  to  $+71^{\circ}\text{C}$  ambient), system designers must turn to advanced approaches such as Airflow Through (AFT) cooling, spray cooling, and Liquid Flow Through (LFT) cooling. Each of these cooling approaches has its particular advantages as well as design considerations to weigh before choosing which is the right one to adopt.

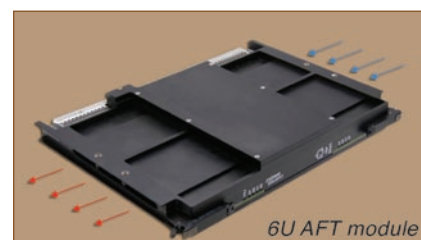
### Airflow Through cooling

One recent entry to the realm of higher-power cooling approaches for military COTS circuit cards is AFT cooling. Though relatively new to the military COTS cooling arsenal, AFT has been used by systems integrators for many years, most often in the form of an air-cooled duct featuring some metal finning. These ducts are called "compact core heat exchangers." In these applications, AFT is typically implemented by bonding two single-sided PWBs to either side of the heat exchanger. Unfortunately, that is not really viable for COTS because virtually all available military COTS cards are double-sided, with components resident on each side.

When applied to COTS cards, AFT can be implemented by placing the heat exchanger on the top of the primary side of the circuit card (see Figure 1). Mezzanine cards can then be placed on top of the heat exchanger. While similar to DFA cooling in that air is blown over the electronics to cool the card, there is no direct contact of the air with the electronics. This eliminates the risk of exposure to contaminants in the air that must be considered with DFA. For AFT to work properly, air seals must be provided at

the heat exchanger inlet and outlet of AFT cards. These are typically applied on the chassis side and need to be able to withstand hundreds of insertions and extractions. Additional features of AFT cards are retainers and injectors/ejectors, all of which are being standardized in VITA 48.5, the AFT standard, which is currently in draft form.

With AFT cards using similar airflow rates to DFA, it is possible to cool boards rated at up to 200 W. While AFT should be considered more of a mid-power cooling approach, it is superior to forced air and conduction cooling. The limits of AFT are related to the use of air for cooling, as they are with DFA as well. An asymptotic curve develops as



**Figure 1** | 6U AFT module with air heat exchanger mounted on primary side of military COTS circuit card. This module can cool  $>200\text{ W}$  with  $+55^{\circ}\text{C}$  inlet air.



# TRI-M SYSTEMS

proudly distributes

## TRI-M ENGINEERING

100MHz PC/104 Module



MZ104

Featuring the new edition ZF86  
FailSafe® Embedded PC-on-a-Chip  
Dual watchdog timers, Phoenix  
BIOS and FAILSAFE Boot ROM  
Extended temperature -40°C to 85°C

## TRI-M ENGINEERING

PC/104 VersaTainer



VT104

The VT104 VersaTainer is a rugged aluminum  
enclosure that can be used as either a PC/104,  
PC/104+ or EBX enclosure.  
The solid one-piece extruded body provides dual  
internal shock and vibration protection.

## TRI-M ENGINEERING

75 Watt High Efficiency PC/104



HE104-75W

75 Watt output  
+5V, +12V, -12V outputs  
6V to 40V Dc input range  
PC/104 compliant

www.tri-m.com

info@tri-m.com

1.800.665.5600

HEAD OFFICE: VANCOUVER

tel: 604.945.9565 fax: 604.945.9566

## Hardware: Designing in cool reprogrammability

the amount of air flowing over the heat exchanger increases. Compared to DFA, the decline in effectiveness is not as sharp because AFT employs an enclosed duct that can be made quite smooth. This duct and the smooth surface result in less flow bypass and lower pressure drops compared to those created by the natural ducts formed between two DFA cards, in which the components on the card surfaces present a rough route for the air to travel over.

### Spray cooling

A chassis-level implementation of spray cooling uses a mist of coolant directed at the circuit cards. When the coolant hits the circuit card hot spots, it vaporizes and then condenses within the chassis. Alternatively, the coolant can be sent to a remote heat exchanger where it is condensed further and pumped back into the chassis in a closed-loop system. Because spray cooling is able to cool very high power densities (such as processor die) to relatively low temperatures (such as -70 °C to +75 °C), it can enable the use of true commercial-grade circuit cards (0 to +70 °C) in rugged deployed applications. In comparison, rugged COTS cards are typically designed to -40 °C to +71°C or higher temperature ranges.

Spray cooling can also be used to mitigate cold startup issues. At the low end of the temperature range, the coolant can be heated to warm the electronics before they are turned on. One drawback to this approach, though, is that the commercial circuit cards need to be so-called "spray" ready. For example, any air cooled heat sinks on the cards need to be removed because the spray needs to be directed at the component or the die. Also, the circuit card must use materials, the thermal interface materials in particular, that are compatible with the type of coolant in the spray-cooled system.

Other drawbacks of spray cooling are the additional weight and volume that the apparatus adds to the chassis (roughly 50 percent) as well as the increased cost and complexity of the system. In addition, spray-cooling systems, unlike LFT cooling systems (to be discussed in the next section), are dependent on the physical orientation of the hardware because of unfavorable gravity force (and other body forces like acceleration) effects on the condensed liquid.

### Liquid Flow Through cooling

LFT is another relatively recent entrant into the ranks of military COTS cooling options, though it has been used for many years (if not decades) by system integrators in costly custom configurations. While similar to AFT, instead of an air-cooled heat exchanger LFT employs a liquid cooled heat exchanger, which in military COTS systems is typically placed on the primary side of the circuit card. The design of the heat exchanger will vary greatly depending on the heat density and heat distribution of the card to be cooled. As the liquid flows through the cores, it picks up the heat and then flows out at an end point. Liquids have much higher heat capacities than air [that is, 1-10 J/(cm<sup>3</sup>K) vs. ~10<sup>-3</sup> J/(cm<sup>3</sup>K)], allowing cooling of higher powers in narrower pitches. For example, LFT can efficiently cool boards with a 0.85" pitch for which AFT would need at least a 1.5" pitch. One design consideration for LFT, however, is that the liquid coolant requires an air heat exchanger at some point, which adds weight and volume to the system.

Two-level maintenance LFT systems have the additional requirement of Quick Disconnect (QD) liquid connectors that close the liquid loop between the chassis and the module. These QDs and other features of LFT for COTS systems are currently being standardized within VITA:

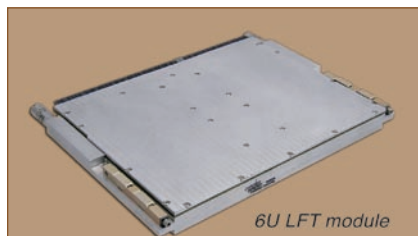
- VITA 48.3: Defines an approach where the liquid manifold is located in the chassis below the backplane
- VITA 48.4: Enables the liquid manifold to be placed above the backplane, which eases use of a standard ATR height chassis
- VITA 48.6: For use with LFT modules larger than 6U

Parker Hannifin and Curtiss-Wright Controls designed, manufactured, and tested an LFT module with some specific attributes in the cover that was able to cool more than 650 W (see Figure 2). This impressive result was achieved at +55 °C with a liquid coolant called PAO, a synthetic oil which has a relatively poor heat capacity. This project highlighted a particular benefit of LFT: the ability to use spreadsheet calculations to accurately predict thermal performance. This is not the case with air-cooling approaches,



“ While the need for higher-performance processing in smaller environments continues its inexorable rise, the military COTS industry is meeting the challenge with advanced cooling methods to stay ahead of the heat curve. ”

which typically require the use of Computational Fluid Dynamics (CFD) tools for accurate thermal predictions.



**Figure 2** | 6U LFT module with liquid heat exchanger mounted on primary side of military COTS circuit card. This module can cool >650 W with +55 °C inlet PAO coolant.

The design considerations for LFT include the risk of leakage from the QDs, as well as the resultant increase in weight, volume, and system complexity. LFT does, however, eliminate the orientation dependence of spray-cooling systems because it uses pumped, single-phase cooling.

#### Staying ahead of the heat curve

While the need for higher-performance processing in smaller environments continues its inexorable rise, the military COTS industry is meeting the challenge with advanced cooling methods to stay ahead of the heat curve. Going beyond air and conduction cooling requires more complexity and greater system challenges, such as utilizing relatively new cooling methods of AFT, spray, and LFT cooling. The open standards community is tackling these challenges to ensure that today's best computing technology is available to the warfighter in the most demanding and harshest environments. +



*Ivan Straznicky is a principal mechanical engineer for Curtiss-Wright Controls Embedded Computing, where his responsibilities include advanced thermal and packaging technologies. Ivan is currently the vice chair of the VITA Standards Organization and a key contributor to the following standards/specifications: ANSI/VITA 46, ANSI/VITA 47, VITA 48, and VITA 42. He has a degree in Mechanical Engineering from McGill University in Montreal, Canada. He can be contacted at [ivan.straznicky@curtisswright.com](mailto:ivan.straznicky@curtisswright.com).*

**Curtiss-Wright Controls Embedded Computing**  
613-599-9199  
[www.cwcembedded.com](http://www.cwcembedded.com)

# MIL-STD

## is the only thing standard about our power supplies.

### Any questions?

**Proudly made in the USA.**

### NAI Power Supplies. Designed to meet the most demanding needs... yours.

- Discrete component design facilitates rapid utilization of latest technologies
- Intelligent monitoring, control and communication
- Fully integrated EMI Filtering
- Key standards include:
  - MIL-STD-810      - MIL-STD-1399
  - MIL-STD-461      - MIL-STD-1275
  - MIL-STD-704      - MIL-STD-901
- Designed with Component Derating per NAVMAT guidelines
- Supported platforms include VME, cPCI and VPX

Intelligent COTS Solutions... for today's rugged systems.  
Visit [www.naii.com](http://www.naii.com) or call us at 631-567-1100 today.

**North Atlantic Industries**  
*Excellence in ALL we do*

[Embedded Boards](#) | 
 [Power Supplies](#) | 
 [Instruments](#)

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

# On Board Vehicle Power (OBVP): Mobile power for tomorrow's battlefield

By Doug B. Mays

*Current threats on our military forces have created a tremendous requirement for mobility as it relates to mission specifications. The development of On Board Vehicle Power (OBVP) systems not only increases warfighter mobility but also enables more effective power supply to current and emerging battlefield electronic systems by providing improved physical characteristics, in addition to more effective power disbursement than traditional "Tactical Quiet Generators," thanks to new OBVP inverter technology.*

The deployed U.S. soldier is given every technological advantage possible on the battlefield. U.S. warfighters have become more than rifle carriers, now utilizing a vast array of military systems active in any number of methods: From on-site radar and threat evaluation systems to UAV patrols to fighter-mounted thermographic and spectral imaging, these systems have provided the ability to not only outgun but completely control an occupied space.

A push is underway to make the U.S. military more agile, mobile, and lethal. To do so requires new weapons systems and next-generation computational systems. Many of these services and applications fall under the Army Brigade Combat Team (BCT) modernization strategy (formerly Future Combat Systems). Some of these most advantageous next-generation military applications involve high-density computational systems that can perform functions such as RF/spectrum scanning and analysis, dispersion analysis, locational detection, cryptanalysis, horizon bogey detection and threat prediction (as opposed to simple evaluation), and probability analysis directly on the battlefield, providing real-time information to on- and off-battlefield commanders. These applications are invaluable to the warfighter in the modern theater and are critical to maintaining situational awareness for the battlefield commander and dominance of active war space.

When talking of these next-generation battlefield systems, an often overlooked but critical question must be addressed: How does one power them? It is not possible to simply plug into an outlet in the middle of a desert. The move to these sophisticated battlefield applications will raise the demand for power exponentially.

Consequently, the rise in demand of power for these advanced deployed systems means an increase in the output of power required from generator systems. With traditional skid-mounted or trailer-towed fuel power technologies, the end result is reduced to nothing more than larger, heavier, and more fuel-hungry generators. This is in direct opposition to the nearly decade-old emphasis to create a faster, lighter, and more agile deployed force. However, new On Board Vehicle Power (OBVP) systems are providing a viable remedy with an improved physical design and new inverter technology for more effective power disbursement.

### **Traditionally deployed power systems: Designs no longer sufficient**

As mentioned, traditionally, theater-deployed systems are powered by trailer-towed or skid-mounted generators. Hitched directly to an HMMWV, these towed generators require ample diesel (fuel) to operate, reduce troop mobility and response times, and, when in operation at a site, are frequently giveaways to

the adversary as to the intentions and location of the camped troops. These "Tactical Quiet Generators" have been in use since the late 1980s and require the carrying of additional fuel to generate power. Skid-mounted units also drastically reduce the cargo capacity of the HMMWV, as they are typically carried in the rear cargo area of the vehicle.

In the past, commanders were dealing with defined combat lines and specific operational theaters and occupation directives. In the modern theater this is no longer the case, and power generators and techniques of the past cannot power the military and its systems of the future. While technology has improved, certain characteristics such as noise, lack of mobility, serviceability constraints, the need for extra vehicles to carry fuel and generators, and other logistical issues that are inherent to the design and use of these Tactical Quiet Generators have created battlefield nightmares for the operators (not to mention increased costs and the swelling of budgets for commanders to accommodate these logistical shortcomings). And all of these issues are in direct opposition to the current military push of "lighter, faster, stronger, smarter." They must be overcome to maintain Armed Forces dominance of an active theater.

To mitigate the shortcomings of present power technologies, a spur of developments in onboard vehicle power



mechanisms is occurring. The result: power systems that are compact, light-weight, and provide the military with the mobility desired while providing the robust power needed by next-generational computational systems.

Advances in the inverter technology used in OBVP systems, such as the increasing use of Insulated-Gate Bipolar Transistors (IGBTs) to create high-powered inverters, have spurred key developments in these modern power units. No longer is a simple conversion from the 28 VDC source to single-phase, 120 VAC/60 Hz enough. Mobility, serviceability, and space constraints must be considered as well. OBVP units do not require an external fuel source and can be mounted directly (in various mounting configurations – including wheel well, behind a seat, and so forth) to the HMMWV without decreasing needed cargo space, and can provide a wide range of output power to the end application.

#### OBVP systems: It's all in the inverter

These modern OBVP units are single- or three-phase AC power units for ruggedized environments that require mobility, portability, and durability. Power envelopes for these OBVP modules range from 2 kW to 30 kW. These units receive input voltages of 24-28 VDC from the vehicle's alternator. The OBVP unit contains control, pre-charge, and protection circuitry, phase power modules, and feedback monitoring and control. The OBVP inverter itself can be paired with other controllers and interfaces, allowing ease of operation by the user. In a nutshell, the unit takes DC power from the vehicle and inverts that to three-phase AC. Figure 1 contains a basic diagram of an OBVP unit and speed control interface.

There is typically a speed control mechanism connected via relays to the integrated OBVP unit and the alternator and engine complex of the HMMWV. These speed controllers can monitor and control throttle and RPMs as needed, and relay the information via a communications bus to an Interface and Indicator Unit (IIU). The IIU is where the operator controls the function of the OBVP inverter, either producing more or less power and monitoring states and so on. IIU can also have a Graphical User Interface (GUI) and easily understandable controls.

The speed control mechanism and IIU allow the operator to control the output

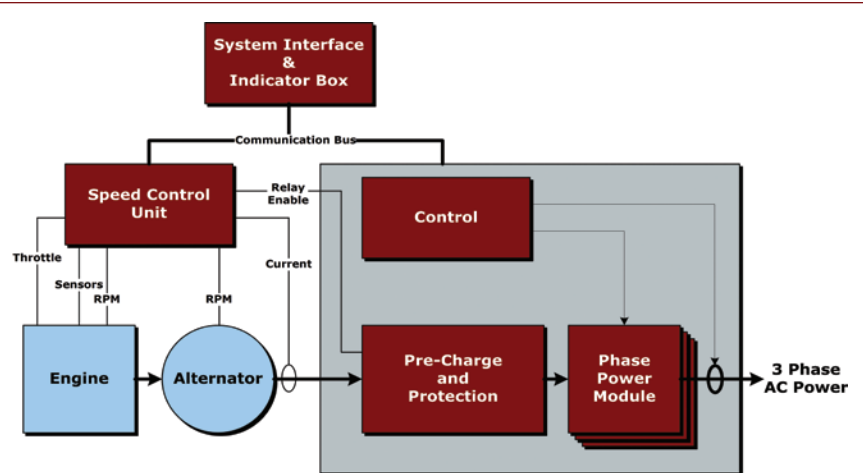


Figure 1 | Basic diagram of an OBVP unit and speed control interface

# REDUCE YOUR RISK

YOUR DATA RECORDER & STORAGE PARTNER

Photo courtesy of Lockheed Martin

Capitalize on Curtiss-Wright Controls Electronic Systems' 10 years of data recording and storage expertise to reduce your program risk and improve your time to market. The Vortex family of Data Recorders and Storage products can manage the critical data requirements of your instrumentation, mission, and SIGINT/ELINT applications. From the lab to your deployed system, the Vortex family of Data Recorders & Storage has a solution for you.

### Vortex Data Recorders



**Customer Programmable Recorders**  
Data Recorders for VPX, VXS, VME, CompactPCI



**Fixed Feature Recorders**  
Pre-programmed Recorders with industry standard interfaces including Serial FPDP, 1 or 10 Gigabit Ethernet and more



**SANbric**  
Rugged removable storage with 2.7 Terabyte capacity



**VPX3-FSM**  
3U VPX solid-state SATA Storage card with a NIST certified 256-bit AES data encryption capability

**CURTISS WRIGHT Controls**  
Electronic Systems

cwcelectronicssystem.com  
Tel: +1 (937) 610-5457  
data\_recorders@curtisswright.com

RECORDERS & STORAGE ABOVE & BEYOND

of the OBVP unit. While the unit receives 28 VDC input current from the HMMWV, the operator may select any of a range of output currents. If the system or application required the basic single-phase, 120 VAC/60 Hz output discussed earlier, three-phase 208 VAC, or 50 Hz or even 400 Hz frequencies, modern OBVP systems allow the operator to set the output of choice for the intended application with a variety of output waveform options.

As mentioned, the OBVP inverter is mounted onto the HMMWV in an area

that does not affect cargo capacity or function of the vehicle and allows instant availability to power in any area to which the HMMWV can maneuver. The modular methodology of not only the components but of the installation mechanisms means that the OBVP system can easily be removed from one HMMWV — returning the vehicle to its original configuration — and quickly and readily installed on other vehicle platforms as needed. (Figure 2 shows a side-mounted OBVP unit.) This provides the ability to provide critical power to areas of the battlefield including



**Figure 2** | Example of a side-mounted OBVP unit

those facing harsh environmental conditions, ensuring that critical systems are operational at all times.

### Realizing tactical goals with OBVP systems

As advances in battlefield technology force the requirements of higher power levels and more mobile power technologies, On Board Vehicle Power units will find their way into many deployments, providing an innovative physical design and improved power disbursement via advanced inverter technology. The military's focus on "faster, lighter, stronger" requires the use of new technology and next-generation computational and communication systems, and these systems and their deployments will all require newer mobile, rugged power solutions. Trailer-towed and skid-mounted power generators fail in these regards, as they add bulk, reduce mobility, and require external fuel (diesel) to operate, which further reduces the cargo of a military vehicle. Mobile vehicle power systems, like Diversified Technology's VPS10K, that draw power directly from the alternator and do not impede much-needed cargo space will be the go-to solution for the deployment of on-battlefield systems in the 21st century military. ✚



**Doug B. Mays** is a field application engineer for Diversified Technology, Inc. He can be contacted at [dmays@dtims.com](mailto:dmays@dtims.com).

**Diversified Technology**  
800-443-2667  
[www.dtruggedpower.com](http://www.dtruggedpower.com)  
[www.dtims.com](http://www.dtims.com)

## EFFICIENT, RELIABLE POWER FOR YOUR CRITICAL MISSION

### New Module Converts 270V Bus Power to 28V for Subsystems

Power your avionics or military subsystems more efficiently than ever with VPT's new VPTHVM-270 bus converter.

New design advances in this module reduce your power input requirements and improve thermal management for your power system.

- Greater than 91% efficient
- Up to 200W output power with a single output
- Power multiple VPT converters from a single module
- Can be used in parallel for higher power
- Wide input voltage range: 160 to 500 volts per MIL-STD-704
- Full operation over a wide -55°C to +100°C standard



Complete specifications, connection diagrams, technical video and catalog are available.

Contact VPT at:  
Web: [www.vpt-inc.com](http://www.vpt-inc.com)  
Phone: 425.353.3010  
E-mail: [vptsales@vpt-inc.com](mailto:vptsales@vpt-inc.com)

**VPT**  
a HESCO company  
Power Your Critical Mission Today.





U.S. Navy photo by Mass Communication Specialist 3rd Class Matthew Reinhardt

# Adding trust to an embedded system with a secure anchor point

By J. Ryan Kenny

*Keeping unwanted components and malware out of embedded systems requires monitoring of both the supply chain and systems in operation. The secure anchor point is a solution to the second half of this equation; it offers the capability to monitor systems in operation by becoming the "root of trust" in an embedded system.*

The integration of high-speed, low-cost embedded processing power has had revolutionary impacts on warfighter equipment. It is also slowly enabling the long-anticipated vision of net-centric warfare. However, integrating commercial technology without a complete history of its origin creates a whole host of new problems with "trust" among potential suppliers. Trust is the quality of a product or manufacturer whose identity and intentions can be assumed to a high degree of accuracy. Low levels of trust in the supply chain create significant issues in military operations; solving this problem revolves around improving the trust levels of either the supply chain or the embedded systems themselves.

One way to address the problem of trust in the electronic domain is the same way it is approached in the social world: relying on a handful of trusted sources to vouch for the authenticity of others, which can be called "secure anchor points." These can be official documents, badges, and personal references in the social world; the secure anchor point in a digital electronics system allows management functions and system monitors to validate the operational integrity of their networks and any persons who have access to their systems. Implementing the secure anchor point in a highly tamper-resistant secure processor raises both the trust and security level of the entire system. Our discussion examines the problems resulting from a lack of trust, how the secure anchor point is utilized, where it fits into the military's net-centric vision, and how to efficiently field the secure anchor point.

### Problems caused by lack of trust

When players (human or electronic) cannot be identified or trusted in a network or embedded system, vulnerabilities are created. One of the top trust problems today is in the electronics supply chain for commercial enterprise, government, and military electronic equipment. Multiple counterfeit parts have been found and reported. The unknown content of these components could lead to Trojan horse insertion, malicious circuits, or back doors that can allow unwanted and illegal access to individual, corporate, medical, financial, or government data and systems.

A survey sponsored by the U.S. Navy and the Commerce Department's Bureau of Industry and Security (BIS)[1] found more than 7,000 counterfeiting incidents in 2008, up more than 25 percent from 2007. Counterfeit electronics were defined as either "re-marked as higher grade," salvaged, or cheap copies. The impact of these counterfeits results in nonfunctional design, failure earlier than design-in, and inability to meet environmental conditions. Many of these were in military equipment, resulting in early failure of line replaceable units in tactical aircraft and vehicles.

### Utilizing a secure anchor point

Building more trustworthy systems does not mean rearchitecting them from the ground up or replacing every single system component without a known origin. This is too great a task for nearly all military systems and would not be cost-effective. Rather, system integrity and trusted operation can be improved simply by adding several roots of trust to the system, with out-of-band authentication and monitoring capabilities. These can be called secure anchor points.

The secure anchor point is a trusted processing node that can serve as the point of departure for authenticating other components and communication nodes in a system. Using virtualization technologies and applications developed specifically for the

hardware, trusted and secure applications can be run on the secure processor. There are several recommended features that lead to this trusted status:

- Trusted design and manufacture
- Secure boot code
- Resistance to tampering and reverse engineering
- Encrypted message passing and memory interfaces

As depicted in Figure 1, a secure processor hosts a set of activities that collects system bus information, processes the data, correlates the data streams to one another to look for unusual activity or component identities, and generates appropriate responses or tailored interrogations. This data is collected over various embedded system data lines, to include VME backplanes, PCIe and Serial RapidIO traces, or proprietary data formats. An FPGA or other commercially available bridging device is used to connect the secure processor to its data sources. An FPGA is preferred for two reasons: FPGA technology has progressed to allow a large number of data formats to be bridged within a single device; in addition, a block of Secure IP can be executed to support data encryption to further protect the functions of the secure processor.

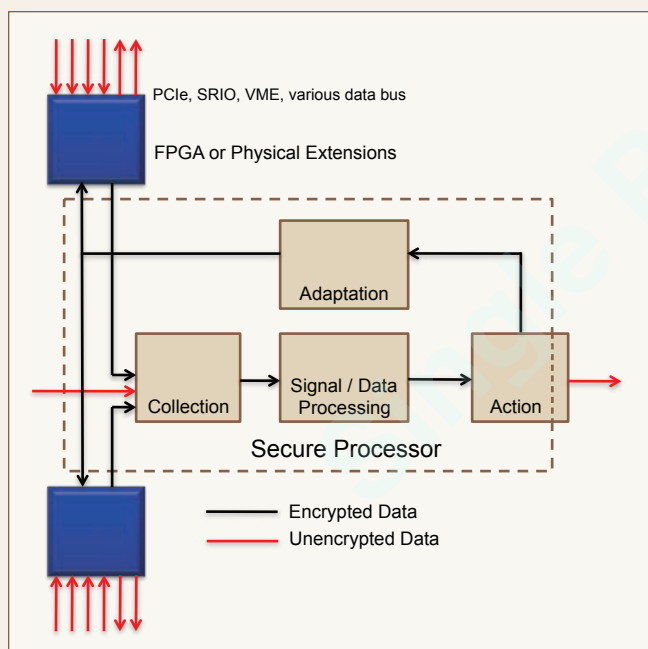


Figure 1 | Block diagram of a secure anchor point using a secure processor

One of the primary objectives of the secure anchor point is to control the "vulnerability point" of an embedded system. When an adversary attempts to reverse engineer, clone, or hack an embedded system, one of the first steps is to identify a single communications node that will allow clandestine control using malware or inserted code. The secure anchor point attempts to become that single communications node, making hacking extremely difficult or impossible through several layers of tamper resistance, encryption, and obfuscation. This is similar to the rationale of DoD Instruction 5200.39, which calls for military system developers to identify their Critical Program Information (CPI) and protect it.

“When an adversary attempts to reverse engineer, clone, or hack an embedded system, one of the first steps is to identify a single communications node that will allow clandestine control using malware or inserted code.”

#### Authenticating other network nodes

It is too daunting a task to implement in one step a distributed guarantee of trust across a net-centric military. Therefore, it is important to implement what Lynn Robert Carter of Carnegie Mellon University calls "asymmetric security"[2], or the capability of trusted agents to provide authenticated data and identity management to network participants.

The role of a secure anchor point in asymmetric security is to serve as the "referral" for other components or processors in a system. This referral will be based on the best available knowledge of threats, expected operating code, and known system elements. Because the secure anchor point is a secure processor, it can adapt to new threats over time without modifying the system through secure encrypted firmware updates. The verification and behavior monitoring information is provided through secure boot programming by the user. Secure anchor point interrogations enable strict inventory control and IP monitoring for highly sensitive or costly IP elements.

Controlled by system designers and/or administrators, the secure anchor point executes techniques like unique interrogations, hashes, serial ID queries, timing measurements, or other schemes. It then defines the response to any trust violations encountered from simple administrative warning notification to system shutdown or memory zeroization.

To make a secure anchor point application scalable across a net-centric operation, it is crucial to have a common set of building blocks and reference designs available. In this way, new anchor points can be added cost-effectively as enterprises expand, but they can still be modified and updated to monitor for recent and localized threats, counterfeit equipment, and out-of-bounds behavior.

#### Efficiently fielding the secure anchor point

The secure anchor point is designed to be extremely difficult to reverse engineer in both hardware and software. A secure processor such as CPU Tech's Acalis can serve as a secure anchor point because it was designed to resist cloning and reverse engineering and contains unique chip serialization (done in the IBM Trusted Foundry). These secure processors also have proprietary "watermark" characteristics as part of their manufacture that can be utilized for authentication both in the supply chain and while in operation. Adding an Acalis secure anchor point to a system requires adding labor hours in hardware design, software



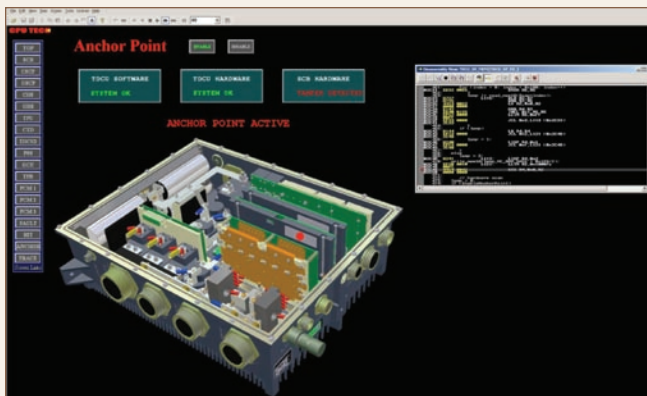


Figure 2 | Secure anchor point implemented on embedded hardware system

design, and IT infrastructure, but does not necessitate architectural changes or redesign to an existing system.

Figure 2 shows the implementation of a secure anchor point on existing hardware modeled by CPU Tech. High-fidelity hardware models are a great place to start in identifying the list of signals and components that should be monitored by the secure anchor point. Building the anchor point into the model offers the ability to identify threats and vulnerabilities, then implement a secure anchor point with a full range of response and system warning capabilities.

#### References:

- [1] Manufacturing and Technology News. "U.S. Government Finds Thousands of Counterfeit Electronics from China in Avionics Weapon Supply Chain." Nov. 17, 2008. [www.manufacturingnews.com/news/08/1117/counterfeitelectronics.html](http://www.manufacturingnews.com/news/08/1117/counterfeitelectronics.html)
- [2] Carter, Lynn Robert. "Computing Infrastructure Risk, Issue, Analysis, and Recommendation." Dec. 23, 2008. Carnegie Mellon University. Issued to White House call for inputs on Cyber Security Policy.



**J. Ryan Kenny** is a product manager at CPU Tech. He is responsible for developing security requirements and certification roadmaps for the Acalis line of secure embedded processors. He joined CPU Tech in February 2009 and has more than 10 years of experience in space and defense electronics in the U.S. Air Force and defense systems engineering. He graduated from the U.S. Air Force Academy and completed an MSEE and MBA from California State University Northridge and Santa Clara University, respectively. He can be contacted at [rkenny@cputech.com](mailto:rkenny@cputech.com).

CPU Tech  
925-224-9920  
[www.cputech.com](http://www.cputech.com)

### COTS I/O Solutions for:

IndustryPack®, PMC, CompactPCI, PCI  
with Outstanding Software Support.

- CPU Carriers
- IP and PMC Carriers
- Ethernet
- Communication
- CAN Bus
- Field Bus
- Digital I/O
- Analog I/O
- PC Card/CardBus
- Motion Control
- Memory
- User-programmable FPGA

- VxWorks
- Linux
- Windows
- LynxOS
- QNX
- OS-9

**TEWS TECHNOLOGIES**

[www.tews.com](http://www.tews.com)

**TEWS TECHNOLOGIES LLC:** 9190 Double Diamond Parkway, Suite 127 • Reno, NV 89521/USA  
Phone: +1 (775) 850 5830 • Fax: +1 (775) 201 0347 • E-mail: [usasales@tews.com](mailto:usasales@tews.com)

**TEWS TECHNOLOGIES GmbH:** Am Bahnhof 7 • 25469 Halstenbek/Germany  
Phone: +49 (0)4101-4058-0 • Fax: +49 (0)4101-4058-19 • E-mail: [info@tews.com](mailto:info@tews.com)

© 2008 TEWS TECHNOLOGIES GmbH, all rights reserved. IndustryPack is a registered trademark of SBS Technologies, Inc. All other trademarks mentioned are property of their respective owners.

## DATA STORAGE TECHNOLOGY

### RPC12 Ruggedized 3U Fibre Channel RAID System

Phoenix International designs and builds rugged COTS Data Storage Systems that plug and play in any application -- from Multi-Terabyte Fibre Channel RAID and Storage Area Network configurations to plug-in Solid State Disk Drive VME/cPCI Storage Modules.

**Low Operational Temperature**  
-20°C

**High Operational Temperature**  
+60°C

**Operational Altitude**  
to 45,000 feet

- Operational altitude to 45,000 feet
- Operational Temperature -20° to +60°C
- Redundant, hot swap components/FRUs
- 40Hz to 440Hz, 90/240 VAC Input Operation

**PHOENIX INTERNATIONAL**

See us at: [www.phenixint.com](http://www.phenixint.com) or contact us at: 714-283-4800 • [info@phenixint.com](mailto:info@phenixint.com)  
An AS 9100 / ISO 9001: 2000 Certified Service Disabled Veteran Owned Small Business

*We Put the State of the Art to Work*

# Protecting embedded systems from unauthorized software modifications

By André Weimerskirch, Ph.D. and Kai Schramm, Ph.D.

*Today's embedded avionics and other security-critical systems increasingly face the requirement for heightened security. Hence, a software downloading/flashing scheme utilizing digital signatures and the Rivest Shamir Adleman (RSA) and Elliptic Curve Cryptography (ECC) algorithms is helping to prevent unauthorized access and counterfeiting.*

More and more devices in our modern world are equipped with a multitude of embedded systems. An obvious example of this trend is the aviation industry, which uses a multitude of Electronic Control Units (ECUs) to control almost everything, such as air conditioning, the engine, and even the brake system[1]. ECUs typically allow downloading of updated program and data code via a boot loader. The authenticity of the software and a secure boot process must be ensured, since an increasing number of embedded devices are used in security-sensitive applications such as the engine control of an aircraft. Hence, any local or remote tampering of these devices must be prevented[1].

To prevent counterfeiting or unauthorized access, software – which is typically stored in reprogrammable flash memory – must be updated securely. During the boot process – where the software is typically signed at a secure back end server and then installed using a boot loader – the system must verify the authenticity of the new firmware by checking the digital signature. The new firmware must be executed by the device only if this verification is successful. A secure software download/flashing scheme based on digital signatures integrating the Rivest Shamir Adleman (RSA) algorithm and the Elliptic Curve Cryptography (ECC) signature algorithm is discussed as a means of granting this assurance[3].

### Authenticity via digital signatures

A digital signature provides integrity and authenticity; data that is digitally signed cannot be altered by a malicious third party without being detected by the receiver. Furthermore, the receiver can verify that the data was indeed signed by the claimed signer. Moreover, the signer is not able to deny that he is the legitimate creator of the signature (non-repudiation). Additionally, digital signatures are generated and verified with asymmetric cryptographic algorithms, such as the RSA algorithm or ECC.

A digital signature is computed as indicated in Figure 1. There is a pair of keys consisting of a private key  $SK$  and a public key  $PK$ . Only the signer has access to  $SK$ , whereas  $PK$  can be publicly

distributed. In general,  $SK$  is only known to the embedded system's manufacturer, for example, an OEM in the aviation industry, whereas  $PK$  is built into every embedded system. The program code  $x$  is first hashed to a short fixed length value  $y$ . Typically,  $y$  is computed by applying a hash function of the Secure Hash Algorithm (SHA)<sup>1</sup> family. Then a digital signature is computed over  $y$  using the private key  $SK$ . The signature can thereafter be verified using the public key  $PK$ . Hence, the software issuer (that is, the manufacturer of the embedded system) holds a private key  $SK$  for signing the software, and the ECU holds the corresponding public key  $PK$  for verifying it (see again Figure 1).

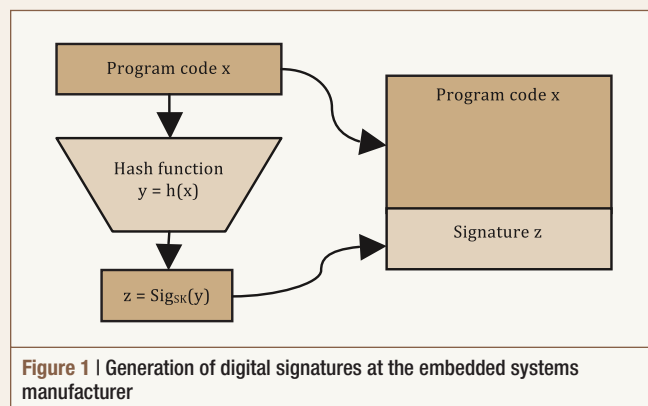


Figure 1 | Generation of digital signatures at the embedded systems manufacturer

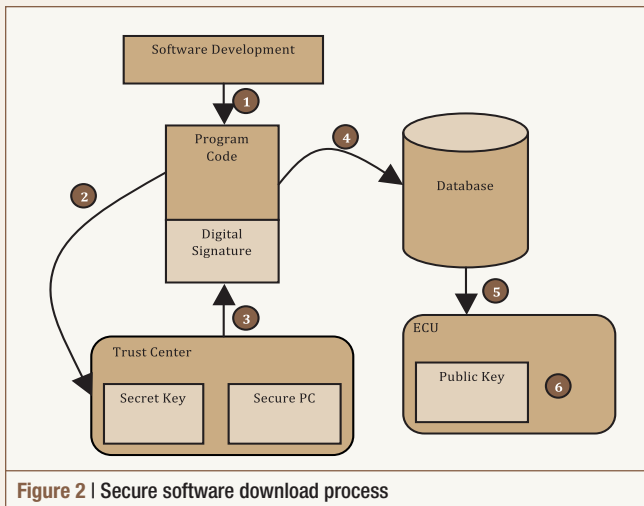
### Secure software downloads

Utilizing a secure software download process is key to upholding these required levels of information security in modern embedded systems. The secure software download process consists of several unique yet vital steps (see Figure 2):

- Step 1: The software is developed.
- Step 2: The program object code is passed to a trust center in a secure environment of the software issuer that signs the object code using its private key  $SK$ .

<sup>1</sup> The SHA hash functions are a set of cryptographic, one-way functions designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) as one of the U.S. Federal Information Processing Standards (FIPS).





**Figure 2 |** Secure software download process

- Step 3: The signature is then passed back and attached to the program object code.
- Step 4: The package of code and signature are now stored in a database that might hold versions for different embedded systems.
- Step 5: The appropriate program code is downloaded to an embedded system.
- Step 6: The appropriate program code is then verified with the corresponding public verification key *PK*.

In the context of this secure software download, RSA is an appropriate fit for signature verification. This is because it allows very fast signature verification and can be implemented in software without infringing patents. Some performance values of this implementation are displayed in Table 1.

It is sufficient to issue a single private/public key pair such that the private key *SK* is stored in the trust center and the public key *PK* in the embedded system. The trust center might be a PC disconnected from any computer network and a secure smart card that holds the secret key. The embedded system only needs to store the public key such that no secret information is stored in the system itself. However, this public key must be protected against manipulation (that is, it must be stored in secure memory that may be read but not overwritten[3]). Thus, safe storage receptacles include Read-Only Memory (ROM) or Write-Once Read Many (WORM) memory, which has to be initialized by the manufacturer during the production process[1].

### Secure software flashing

In the flash process, each block of software is optionally encrypted and the signature is computed beforehand. Next, an external programming device authenticates the boot loader (for example, by using a challenge-response mechanism). Then the

	Flash	RAM	Runtime/ Throughput
SHA-1 (hash function)	898 bytes	352 bytes	3,026 KBps
RSA 1024 signature verification	1,410 bytes	1,136 bytes	2 ms (short exponent 3)
AES-128 (encryption CBC)	2,343 bytes	236 bytes	661 KBps
ECC 160 (ECDSA signature generation)	4,244 bytes	932 bytes	35 ms
ECC 160 (ECDSA signature verification)	4,244 bytes	1,108 bytes	66 ms

**Table 1 |** Runtime of an RSA signature verification measured on an ARM MPCore @ 400 MHz compared to various cryptographic algorithms

external device passes block by block to the boot loader of the embedded system. The boot loader decrypts and stores each block and computes a hash over it[2]. Finally, after the boot loader has computed the hash value over the new flash program file, it performs digital signature verification. If the signature verification is successful, the downloaded file is accepted and activated. Otherwise, a safety procedure is activated and the boot loader awaits the download of a proper flash file.

### Digital signatures ensure peace of mind

Usually, a boot loader is built into the firmware to update the program. However, in most cases there are no mechanisms implemented to avoid downloading a manipulated program that alters the device's behavior in a manner not authorized by the manufacturer. The presented mechanisms are an efficient countermeasure to manipulation attacks. Such mechanisms have been successfully implemented in a variety of applications such as the automotive domain[3], the aeronautical domain, and even the mobile phone industry. We strongly suggest implementing the asymmetric cryptographic approach described – based on digital signatures. ✚

### References

- [1] Marko Wolf, André Weimerskirch, and Thomas Wollinger, "State-of-the-Art: Embedding Security in Vehicles," EURASIP Journal on Embedded Systems, Special Issue on Embedded Systems for Intelligent Vehicles, 2007.
- [2] Cullen Linn and Saumya Debray, "Obfuscation of Executable Code to Improve Resistance to Static Disassembly," ACM Conference on Computer and Communications Security (CCS), 2003.
- [3] Hersteller Initiative Software (HIS), "HIS Security Module Specification, Version 1.1," available at [www.automotive-his.de/download/HIS/Security/Module/Specification/20V1.1.pdf](http://www.automotive-his.de/download/HIS/Security/Module/Specification/20V1.1.pdf), July 2006.



**Dr. André Weimerskirch** is CEO and president of American-based escrypt Inc., where he is in charge of international activities. Previously, he held the position of CTO of escrypt GmbH. Prior to this, André worked with several research, development, and consulting companies including Accenture, Deutsche Post, Philips, and Sun. He studied Business Information Technology and Mathematics at Darmstadt Technical University before receiving his Master of Science in Computer Science at Worcester Polytechnic Institute, USA. He then received a Ph.D. from Ruhr-University of Bochum in Applied Data Security. He can be contacted at [aweimerskirch@escrypt.com](mailto:aweimerskirch@escrypt.com).



**Dr. Kai Schramm** is CTO of escrypt Inc. Previously, he worked for Renesas Technologies in the UK as a consultant. Kai has worked worldwide as a security researcher, consultant, and developer at the IBM Watson Research Center in Hawthorne, New York; the Infineon Technologies smart card department in Munich, Germany; and the Hitachi Central Research Laboratory in Tokyo, Japan. He studied Electrical Engineering and Computer Science at Purdue University in the USA and at the University of Bochum in Germany. He received a Ph.D. from the University of Bochum with a focus on Applied Data Security and Cryptography. Kai can be reached at [kschramm@escrypt.com](mailto:kschramm@escrypt.com).

escrypt Inc.  
734-418-2797  
[www.escrypt.com](http://www.escrypt.com)

# A new approach to testing embedded-LO converters

By David Ballo



U.S. Navy photo by Mass Communication Specialist 2nd Class John W. Ciccarelli Jr.

*Measuring mixers and converters when external Local Oscillators (LOs) can be supplied to the Device-Under-Test (DUT) is relatively easy, as is measurement when the DUT's internal LOs and the Vector Network Analyzer (VNA) can be locked to a common time base. However, DUTs with embedded LOs without access to the LO signal itself or its time base present unique challenges when it comes to measuring group delay. Consequently, modern VNAs are stepping in to ease the embedded-LO measurement process.*

Vector Network Analyzers (VNAs) provide fast and accurate S-parameter measurements of a variety of RF and microwave devices. While S-parameters have been traditionally used for non-frequency-translating devices such as filters, amplifiers, and antennas, in recent years, methods have been invented that extend S-parameter measurements to frequency-translating devices like mixers and converters. It is relatively easy to measure mixers and converters when external Local Oscillators (LOs) can be supplied to the Device-Under-Test (DUT), or when the DUT's internal LOs and the VNA can be locked to a common time base. However, for DUTs with embedded LOs without access to the LO signal itself or its time base, measuring group delay is particularly challenging. However, a new approach using modern VNAs is easing the embedded-LO converter testing process.

### Embedded LOs housed in satellite transponders

The most common types of converters with fully embedded LOs are satellite transponders. To characterize these transponders, a variety of key measurements

is needed. A VNA can be used to measure gain, gain flatness, phase and group delay linearity, port matches, intermodulation distortion, and noise figure. These parameters are tested under a variety of conditions – such as multiple frequency bands – over a wide range of temperatures and at several stages in their development, beginning at the circuit level. The parameter testing then continues at the module level and finally concludes at the systems level. With many parameters to characterize under many conditions, testing transponders becomes a time-consuming endeavor, producing large amounts of data.

### Using VNA-based systems for characterizing converters

Measuring conversion gain and vector input and output match of embedded-LO converters is easy with modern VNAs. With these instruments, the stimulus source and the measurement receivers can be tuned independently of each other, using the analyzer's frequency-offset mode of operation. Scalar transmission (gain) measurements are easy to set up and perform, and there is no need for access to the DUT's LOs.

However, to measure a converter's transmission phase and group delay, a reference mixer must be added to the setup. The reference mixer provides a signal to the reference receiver of the VNA at the same frequency as the DUT's output frequency. In this way, the phase difference between the reference and test signals can be measured, providing phase versus frequency information. Group delay can be easily calculated from this underlying phase information by performing a finite-frequency differentiation. The reference mixer is placed in the reference receiver path using front-panel access points available on most modern VNAs. The VNA can simplify the test setup by using the optional built-in second signal source to provide the LO signals. This arrangement is very fast, since the two sources and the receivers are synchronized with the VNA's internal hardware and software.

### Dealing with internal LOs

There are three different scenarios to extend this converter measurement technique for devices with internal LOs, each with a different level of noise (and, therefore, accuracy) resulting from the phase noise of the LOs.



### Common-LO scenario

The common-LO case gives the least amount of delay noise because the phase noise on the LO is present in both the reference (R1) and test (B) receivers. Since phase measurements are relative between the two receivers, the LO's phase noise is ratioed out of the measurement.

### Common-time-base configuration

For DUTs with inaccessible LOs but with time-base access, the reference mixer and DUT are driven by different LOs that are locked to a common time base (10 MHz, for example). This means their average frequency is the same, but the phase variations due to their inherent phase noise will be different. The two LOs are coherent in frequency, but not phase synchronous. Since the signals in the reference and test receivers are derived from different LOs, their phase noise does not cancel in a ratioed measurement between the R1 and B receivers, unlike what occurs with the phase-synchronous case. This results in increased delay noise, as shown in Figure 1.

Fortunately, there are methods that can be used to reduce the trace noise on non-phase-synchronous delay measurements. Usually, all these methods are used in some combination chosen by the user to balance measurement speed with measurement accuracy.

- When the DUT's LO, the reference mixer LO, and the VNA are all locked to a common time base, then narrowing the IF bandwidth results in less noise due to an improvement in the overall signal-to-noise ratio.

- Averaging is another tool that is commonly used: Both IF bandwidth reduction and trace averaging result in longer measurement times.
- Using the smoothing function enables a moving average filter to be applied to the trace. Smoothing does not slow down measurement times.

### Fully embedded-LO challenge

The most challenging scenario is the fully embedded-LO case, where access to the DUT's LO or its time base is unavailable. This is common with most satellite transponders, because size and weight limitations and the potential for unwanted spurious signals eliminate easy access to the LOs aboard the satellite. Therefore, it is not possible to make a connection to provide coherent frequency synchronization of the VNA and the transponder. This is why the VNA has historically not been used for these measurements, dramatically hindering efforts to improve the speed of transponder characterization. However, modern VNAs can circumvent the problem. This new VNA approach provides frequency and phase stability, allowing calibrated phase and group delay measurements.

### Establishing frequency and phase stability

To make the phase and group delay measurements for the embedded LO, the source providing the LO for the reference mixer must be set to a frequency that gives an output signal with a frequency that matches the transponder's output frequency.

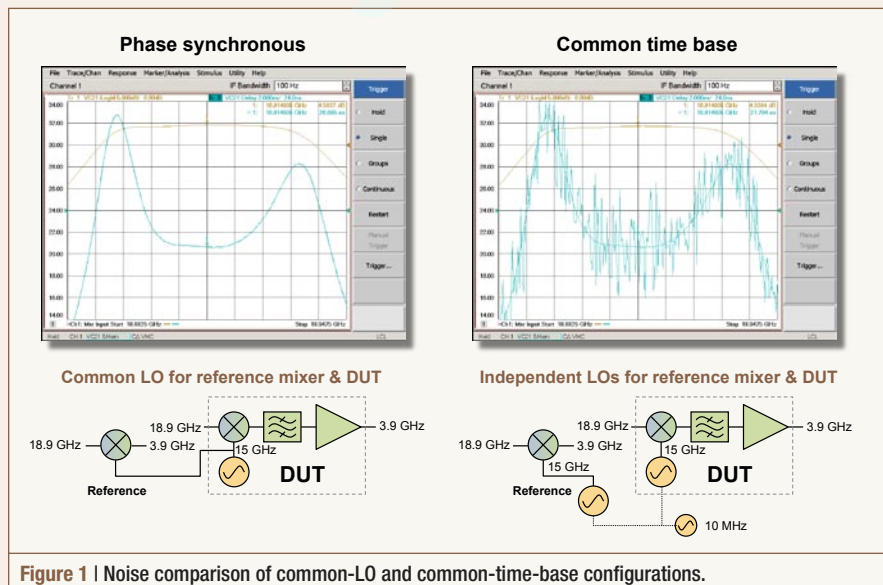


Figure 1 | Noise comparison of common-LO and common-time-base configurations.

## TRI-M ENGINEERING

### PC/104 Can-Tainer



Rugged anodized aluminum PC/104 enclosure designed for harsh environments.

Isolating shock mount and an internal stack vibration mount provides maximum protection from high frequency vibrations and low frequency G-forces.

### 108 Watt PC/104+ Power Supply



+3.3V, +5V, +12V & -12V DC output  
6V to 40V DC input range  
High Efficiency up to 95%  
PC/104 compliant  
Extended temperature: -40°C to +85°C

### 168 Watt Max with HPS-UPS firmware.



Total power: 168 Watt with ATX interface  
+3.3V, +5V, 12V outputs  
6V to 40V DC input range  
PC/104 size and mounting holes  
Built in temperature sensor

www.tri-m.com info@tri-m.com

1.800.665.5600

HEAD OFFICE: VANCOUVER

tel: 604.945.9565 fax: 604.945.9566

The frequency of the reference mixer's LO must be close enough to the DUT's LO so that relative phase drift during phase measurement is small. As long as the reference mixer's LO is close enough, the two IF signals will appear coherent just long enough to enable a good phase measurement. This condition is called "pseudo-coherent frequency locking," and it provides group delay measurements that are not significantly affected by the lack of a common physical LO connection, assuming the presence of the stable sources typically found in satellite transponders.

To establish the appropriate pseudo-coherent relationship between the DUT and the test instrument, modern VNAs such as Agilent's PNA-X break down the measurement of the transponder's effective LO into a coarse and fine measurement. This two-step approach achieves the needed frequency accuracy within a short time. Both the coarse and fine tuning can be done at each data point of the group delay measurement to create a coherent relationship between the instrument and the DUT.

Even when pseudo-frequency coherency has been established, there will be sweep-to-sweep variation in the absolute phase response due to the source-synthesis architecture of a VNA such as Agilent's PNA Series. However, the phase can be normalized at each sweep to an arbitrary trace point, which means that averaging can be used just as effectively as with the common-LO or common-time-base case.



**Acalis®**

**CPU TECH®**

Advanced, Built-In Tamper Protection  
 Highly Integrated with On-Chip DRAM  
 Fabricated at TAPO / IBM Trusted Foundry

**CPU TECH®**  
 Leading Solutions You Can Trust  
 WWW.CPU-TECH.COM

“ When adding in the time to measure conversion gain and match, VNA-based test systems can improve test times in excess of a factor of 100. ”

## Measurement results

Smoothing and averaging can be also be used to produce good results for embedded-LO measurements. Figure 2 shows that the results from an averaged and smoothed embedded-LO measurement, while slightly noisier, precisely overlay those from a measurement with the common-LO configuration.

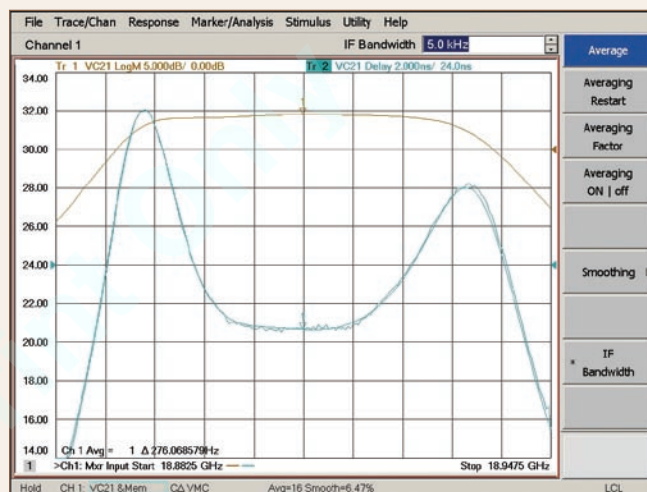


Figure 2 | The results of an embedded-LO delay measurement overlay those from the common-LO configuration, with a slight amount of additional noise.

## Measurement speed

The VNA approach to group delay measurements is much faster than using the traditional stepped signal source and spectrum analyzer approach. Using the embedded LO application, the measurement cycle time for 201 points is typically under one second. Assuming 10 averages are used, this translates to about 9 seconds per measurement. In comparison, a spectrum analyzer and signal source typically require many minutes to accomplish the same task. When adding in the time to measure conversion gain and match, VNA-based test systems can improve test times in excess of a factor of 100.

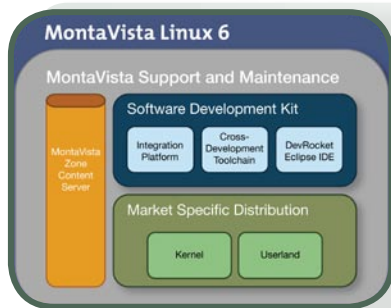


*David Ballo is an applications development engineer at Agilent Technologies' Component Test Division in Santa Rosa, California, where he has acquired 29 years of RF and microwave measurement experience.*

Agilent Technologies  
 800-829-4444  
 www.agilent.com

Find the full-length version of this article online at [www.mil-embedded.com/articles/id/?4144](http://www.mil-embedded.com/articles/id/?4144).





## Market-specific distros: MontaVista Linux 6

It's a case of where one-size-does-not-fit-all: MontaVista's Linux 6 (MVL6) product is now available in IC-specific flavors called *Market Specific Distributions* (MSDs). All built on a common Linux framework, the family of MSDs is designed specifically to take advantage of, and run efficiently on, various semiconductor vendors' hardware devices. Of course, this wouldn't be Linux if each MSD couldn't also be customized and optimized even further, depending upon the target application and actual end system. Announced in May 2009, MVL6 is being coded to support a staggering 40 MSDs!

Each flavor targets a specific SoC that utilizes a common semiconductor core such as the ARM11 or ARM9. What's particularly important to the SoC vendors — and to developers porting Linux to those processors or writing application code on top of the OS — is that driver development is available right inside the Linux MSD. The significance is that SoCs are differentiated not by the CPU (or MCU) inside but by the particular combination of system-specific peripherals in the device. MPEG4 decoders or vector processors, for example,

need the right drivers to meet power and performance objectives. This is all built into each custom MontaVista MSD. As of press time, new MSDs available include: Versatile ARM1176 and ARM926; Freescale MPC8377, MPC8349, MPC8548, and MPC8572; Intel x86 Pentium and Xeon; MIPS32 1004K, 24K, 34K, and 74K cores on Malta platform; and Xilinx ML 507 with the Virtex-5 EDK update.

**MontaVista • [www.mvista.com](http://www.mvista.com) • RSC# 42971**

## "Stable and stiff" compute blades

Targeting high-performance compute and connectivity density in demanding environments, Themis' CoolShell CS-3U blade servers provide thermal and kinetic management with a "stable and stiff" conduction-cooled processor module "shell." The CoolShell accommodates shock and events up to 25 g at 30 ms without external isolation. The 19" RETMA rack system includes a processor blade, I/O blade, and a media module.

The 3U blade servers specifically favor defense, rugged, and other nonbenign operating environments with one of two Intel Quad-Core Xeon 5440 CPUs, three dual-headed GPUs, and up to 64 GB of memory. The media module can house up to 1 TB of SATA and can be supplemented by up to five more 2.5" SDD/HDD drives in an optional module. I/O includes eight GbE ports (seven can be ordered with fiber instead). As expected, there's audio, PCIe expansion, and front-panel expansion. But most importantly, the unit can operate up to +50 °C. And the CPU module is protected from dust and dirt while maintaining adequate cooling and vibration resistance. A variety of server operating systems is available.

**Themis Computer • [www.themis.com](http://www.themis.com) • RSC# 42456**



## 48 V rugged and compact, low-noise DC-DC converters

Military and mobile systems are notorious for being low-voltage and high-current. But add in modern digital electronics operating at 3.3 V or 5 V, and you've got a mismatch that demands a DC-DC converter. Martek Power has a solution for low-power, battery-operated, portable, mixed signal, or Unmanned Aerial System (UAS) platforms: the 200UFR series of low noise, fully isolated DC-DC converters in 0.86" x 0.36" x 0.49" SIP packages. Outputs are 2 W with 1,500 VDC isolation. Even better, they operate over -40 °C to +85 °C — perfect for high-rel defense applications.

There are 14 members in the series in either single- or dual-output mode. All are low-ripple with short-circuit and over-current protection and remote on/off, and boast a full-load efficiency of up to 80 percent. Rated at 12, 24, or 48 VDC inputs, regulated output voltages available include:

3.3 V, 5 V, 12 V, 15 V, +5 V, +12 V, and +15 V. Maximum temperature coefficient is +0.02 % per °C, making the device very stable over a wide temperature range. As well, MTBF per MIL-HBD-217F is at least 1 million hours (+25 °C, ground benign).

**Martek Power • [www.martekpower.com](http://www.martekpower.com) • RSC# 43780**

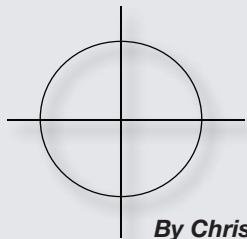
## Getac now offers Windows 7, gestures, and MIL-STD-810G

Panasonic's Toughbook series is the undisputed leader in rugged laptops, notebooks, and tablets for military applications. But upstarts like Getac are gaining ground with new features and attractive price points — things that matter in a tough economy, even to the DoD. The company's complete line of notebooks and tablets now supports Microsoft's brand-new Windows 7 operating system. Where applicable, Getac employs Resistive Multi-Touch technology to allow touch-screen gestures — even while wearing the thick and unwieldy gloves favored by soldiers and Marines. As well, the company has received product line certification to MIL-STD-810G, MIL-STD-461F, and IP65.

Certified by Microsoft, Multi-Touch allows keyboardless computing using the kind of gestures pioneered by Apple's iPhone such as single- and dual-touch maneuvers, "flick," and rotate. Resolutions up to 2,048 x 2,048 are supported with a 100 points-per-second report rate at under 32 ms response time. And, unlike older capacitive multi-touch technology (like that found on my own Wacom-enabled Toshiba TabletPC), the screen responds minutely and accurately to fat-finger gloves. As well, an independent lab has recently certified to several MIL SPECS Getac's A790, B300, and M230 (all notebooks); V100 (convertible notebook); E100 (Tablet); and PS535 (PDA). Tests included EMI, dust and moisture ingress, extreme temperature, and shock — including 78 consecutive drops from up to 6 feet.

**GETAC Technology Corporation • [www.getac.com](http://www.getac.com) • RSC# 43781**





By Chris A. Ciufo, Editor

## C4ISR and the big picture



On a per-line-item basis year after year, the majority of the DoD's technology budget has gone into digitizing the battlefield. As soon as a weapon or a platform became "smart," planners wanted it interconnected to everything else. To this day, programs that add COTS technology to help digitize the battlefield get preferential funding treatment – especially if they show immediate value to either save warfighters' lives or radically improve current mission objectives. Everything has computers, from the ordnance itself to the WWII-era towed Howitzers. Data is routed around the battlefield and beamed to TOCs or back to CONUS and stored on huge disks or in real-time local memory.

So we've got "data," but what the heck do we do with it all?

On one hand, we have the digital capabilities that technology offers. On the other, there are warfighting problems that need solutions. When battlefield data is used to solve problems and accentuate capabilities, everyone wins. Companies like GE Intelligent Platforms have recently been very successful winning C4ISR programs that marry small form factor systems to digital battlefield data to provide situational awareness and reconnaissance information. The M1A2 Abrams Evolutionary Design (AED) tank program awarded just shy of \$1.0 million to GE to prove that VPX Ethernet switch products and SBCs could connect new vetronics sensors with the Commander's Independent Thermal Viewer (CITV) and provide previously unavailable "sit rep" info using image processing and graphics overlays.

Not only that, at this year's Association of the U.S. Army (AUSA) meeting, GE demonstrated a 360-degree head-in capability that allows tankers to "see through" a vehicle using a helmet-mounted display and external sensors. This is similar to the previous Eagle Vision program demonstrated on the Bradley Fighting Vehicle by SBS (now GE), Sarnoff, and BAE. (It's also similar to the USAF's vision of the "glass canopy" where pilots can "look" down through an aircraft's floor and "see" targets or threats below.)

The GE system concept has evolved into the Distributed Aperture program, according to Frank Willis, director of product management and marketing for the military/aerospace group of GE Intelligent Platforms. Willis says that digital battlefield data collected at an "asset source" becomes locally consolidated by small form factor computers such as VPX, OpenVPX, and COM Express, and then "communicated across the battlefield." The key is local data consolidation and decision making to avoid fire-hosing information on low-bandwidth nets. This way, the data gets used by the asset that needs it the most before being passed along.

According to Larry Schaffer, VP of business development for applied image processing at GE, his company plans to capitalize on turning data into situational awareness using its 3U VPX/REDI-sized IPS5000 as an Army Appliqué-like upgrade that ties into fire control and on-vehicle sensors, and also aggregates heretofore unused "metadata." Vetronic platform targets are Abrams, Bradley,

Stryker, and the UK's Warrior. A smaller PC/104-based IPS500 uses even more COTS with sights set on Humvees, MRAP, and Joint Light Tactical Vehicle (JLTV) – a possible HMMWV replacement. Both GE systems contain video engines (input), visualization processors (rendering, post-processing), and storage – along with optional graphics processors for additional displays.

It's easy to see how data from new sensors can either feed into these types of GE systems or be sent to other assets to paint a "first person" view of the battlefield. For example, DRS Technologies was recently awarded a \$1.9 billion IDIQ contract from U.S. Army CECOM for Driver's Vision Enhancers (DVEs) that allow "seeing" through fog, smoke, and other battlefield obstacles on M1A2s, M2s, HMMWVs, and other ground vehicles. There's no reason DVE can't also send this data to Unmanned Aerial Systems (UASs) to augment a platform's local view to equally enhance situational awareness.

Along the same theme, General Dynamics C4 Systems (Scottsdale) recently delivered the first Prophet Enhanced tactical signals intelligence system to the U.S. Army. Here too, data from battlefield sensors are aggregated to present a battlefield threat picture. The networked ISR system, integrated into a BAE Panther rapid-deployment C2 vehicle, takes sensor data and allows tactical commanders to "see," "hear," and "respond" to battlespace data. According to *Jane's Defence Weekly*, the program is a follow-on to a fielded and secretive SIGINT program.

But using all this networked digital data doesn't depend only on hardware; software and data mining play big roles in reconstituting ISR information into new pictures. McObject, a COTS data management software company, has improved its eXtremeDB database product to parse and organize in-memory data in real-time, complete with hooks to embedded Java, Java ME, and Microsoft's .NET. In-memory data mining allows real-time microsecond information retrieval in deployed, harsh environment flash-based computers. As well, semantic fusion technology – an offshoot of artificial intelligence – coupled with natural language processing can combine battlefield data with human-created text data such as sit rep reports to paint a totally different picture of the battlefield.

The company Modus Operandi recently won a DARPA contract designed to exploit previously stovepiped information, such as Word or HTML documents. By overlaying sensor data with human text documents, such as "... at 20:00 hours there was single vehicle activity at the Northern border crossing ...", commanders will get a different view of the battlefield to aid in decision making. In this example, that single vehicle might've been previously tracked by a Predator, lost once it left the Area of Operations (AO), but now "found" again when it crossed a border checkpoint. By combining disparate databases, new intelligence is gained. This is just another example of how data, previously streamed onto the digital battlefield but unused, is being exploited using sophisticated COTS hardware and software.



CV90 Armored Vehicle DDG-1000 Multi-Mission Destroyer Roland Air Defense System  
HIMARS Artillery Rocket System B-2 Stealth Bomber F-35 Lightning II  
LHD Class Amphibious Assault Ship Expeditionary Fighting Vehicle Gripen Fighter  
Littoral Combat Ship A400M Transport NSSN Virginia Class Submarine  
F-117 Stealth Fighter MEADS Air Defense System EMB-145 Challenger 2 Tank  
M2/M3 Bradley C-5 Transport NH-90 ASW Helicopter AH-1W Helicopter  
Predator RQ-1 E-2C/D Early Warning Aircraft Neuron UCAV V-22 Osprey

# Which of these platforms use GE Fanuc hardware?

Fire Scout UAV F-15 Fighter SSN Astute Class Submarine Tornado Fighter  
Nimrod Aircraft RQ-4B Global Hawk AMX Fighter P-3C Maritime Patrol Aircraft  
C-17 Globemaster K1A1 Tank LPD 17 Landing Platform B-1B Bomber  
Taranis UCAV Avenger Air Defense System F-22 Raptor C-130 Transport  
Patriot Missile System 737 Wedgetail Arleigh Burke Class Destroyer  
E-3 AWACS M1A2 Abrams Tank AV-8B Harrier II Plus Eurofighter Typhoon  
F-16 Fighter Merlin ASW Helicopter Ticonderoga Class Cruiser T-6B Trainer  
EA-6B B-52H Long Range Multi-Role Bomber Barracuda UAV Demonstrator

---

ANSWER | GE Fanuc offers more COTS products than any other embedded company and we are part of  
ALL these platforms. To find out more, and join this growing list, visit [www.gefanucdefense.com](http://www.gefanucdefense.com)

---



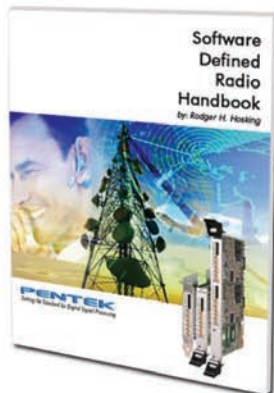
GE Fanuc  
Intelligent Platforms



**LIMITED TIME OFFER!**  
Save \$2,000 on the latest  
Software Radio Module

## We've Hatched the Next Generation of Software Radio Solutions

Pentek delivers board and system-level SDR products that include digital downconverters, upconverters and transceivers. Since all of these products are FPGA-based, Pentek offers powerful factory-installed IP cores plus the GateFlow FPGA Design Kit for custom development. These software radio solutions are perfect for applications in communications, SIGINT, radar, direction finding and many more.



And now the latest software radio module, Model 7156 with Dual 400 MHz A/Ds, 800 MHz D/As and Virtex-5 FPGAs, is now available in a bundled package offering you a \$2,000 savings!

Call 201-818-5900 or go to [www.pentek.com/go/messdreggB](http://www.pentek.com/go/messdreggB) for your FREE Software Defined Radio Handbook, technical data-sheets and to request pricing.

- New A/Ds: 200 MHz, 16-bit and 400 MHz, 14-bit
- XMC/PMC, PCI, PCIe, VME/VXS, cPCI
- Over 150 software radio modules
- Up to 512 channels of DDC per slot
- GateFlow FPGA resources
- FPGA-installed SDR IP cores
- Recording systems with rates up to 800 MB/sec

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

Pentek, Inc., One Park Way, Upper Saddle River, NJ 07458 Phone: 201.818.5900 Fax: 201.818.5904 e-mail: [info@pentek.com](mailto:info@pentek.com) [www.pentek.com](http://www.pentek.com)  
Worldwide Distribution & Support, Copyright © 2009, Pentek, Inc. Pentek and GateFlow are registered trademarks of Pentek, Inc.  
Other trademarks are properties of their respective owners. Prices are subject to change. Offer ends December 31, 2009. Offer applies to the Model 7156 only.

