Daily Briefing: *News Snippets*

Military EMBEDDED SYSTEMS

VOLUME 7 NUMBER 3
MAY 2011

INCLUDING:

Chris A. Ciufo
Big bucks for better batteries

Field Intelligence
Enhancing platform protection

Mil Tech Insider
IP drives mil security

Legacy Software Migration
Spark Integration Technologies:
Comms framework eases integration

MIL-EMBEDDED.COM

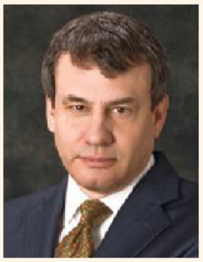
Silicon helps the fight for security

Page 26

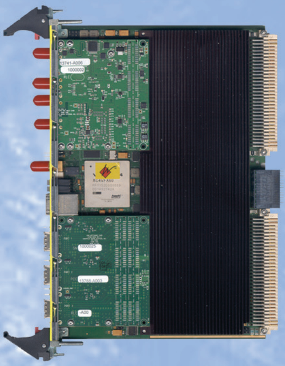
Also:

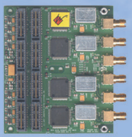
Xilinx is master of their domain; App store to follow?

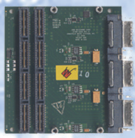
Page 38

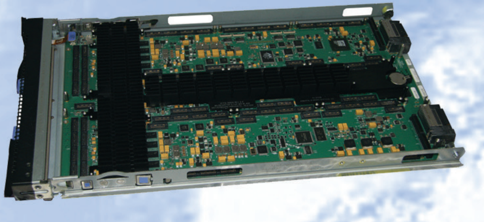


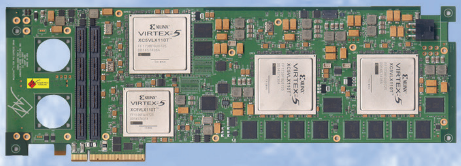
Exclusive Interview:
HP's Bill Toti on Navy's NMCI network
"Inside the enemy's OODA loop."
Page 22

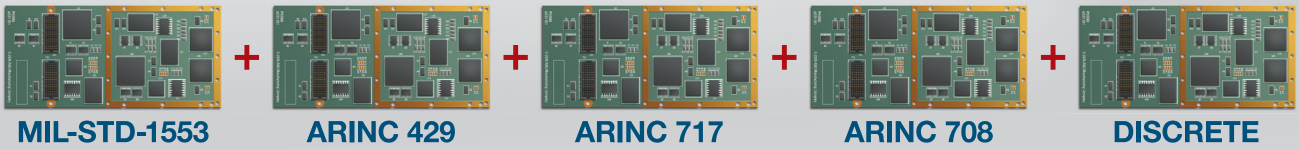












MIL-STD-1553
+
ARINC 429
+
ARINC 717
+
ARINC 708
+
DISCRETE

Military EMBEDDED SYSTEMS

May 2011 Volume 7 Number 3

COLUMNS

Field Intelligence

Mil Tech Insider

Legacy Software Migration

Crosshairs Editorial

DEPARTMENTS

ON THE COVER:
Our feature interview this month is with Bill Toti of HP, VP of Strategic Programs, U.S. Department of the Navy. Bill's job, in a nutshell, is to keep HP plugged into the Navy's NMCI network. But Bill's also a career Naval officer, having commanded a Los Angeles class nuclear submarine (SSN 697 *USS Indianapolis*) just like this one on the cover. Subs like this one have pummeled Libya with Tomahawk cruise missiles in recent weeks. Check out our exclusive interview with Bill and learn what an "OODA loop" is. Interview starts on page 22. (Image of *USS Tucson*, SSN 770, by Mass Communication Specialist 3rd Class Adam K. Thomas. Photo courtesy of U.S. Navy)

Published by: OpenSystems media

ISSN: Print 1557-3222

Software: Smartphone tech coming to a theater near you

Hardware: Fighting for security

Technology: Mil vetronics go rugged

Mil Tech Trends: FPGAs to go, anyone?

EVENTS

www.opensystemsmedia.com/events

ESC Chicago co-located with sensors expo & conference
June 6-8, 2011 • Chicago, IL
http://esc.eetimes.com/chicago/

Freescale Technology Forum (FTF)
June 20-23, 2011 • San Antonio, TX
www.freescale.com

AUVSI's Unmanned Systems North America 2011
Aug. 16-19, 2011 • Washington, DC
www.auvsi.org/auvsi/auvsi/Events/Default.aspx

WEB RESOURCES

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

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

» Who can solve my SWaP-C challenges? «

Kontron's expertise at the computing core, along with rugged system design, provides a complete solution to address the most complex space constraint, weight reduction, power consumption and thermal management hurdles.

Size
- Small Form Factor
- Semi & full custom

Weight
- Fanless cooling options
- Light Weight Materials

Power
- Compact PSU solutions for MIL & avionics environments

Cooling
- Expertise in heat dissipation and thermal management

+

One source to mitigate risk and reduce total cost of ownership

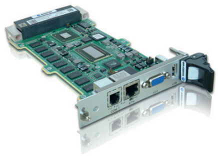
CRITICAL QUESTIONS ... ANSWERED

Reduced SWAP – High-performance Embedded Computer

Cobalt™

- Small Form Factor
- Intel® Core™2 Duo or Atom™ processor
- Custom I/O

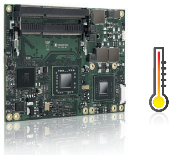
3U VPX CPU board
2nd generation Intel® Core™ i7 processor



VX3035

- Available in standard and rugged air-cooled, or rugged conduction-cooled
- Compliant to VITA46 (VPX), VITA65 (OpenVPX) and VITA48 (VPX REDI)

High-performance COM Express® hardened for extreme environments



ETXexpress®-PC-XT

- Intel® Core™2 Duo with Intel® GS45 and ICH9M SFF
- Operation: -40°C to +85°C

AP Labs is now a part of kontron

CONTACT US

☎ 1-888-294-4558 ✉ info@us.kontron.com kontron.com/military

intel Embedded Alliance Premier

If it's embedded, it's Kontron.

ADVERTISER INFORMATION

Page	Advertiser/Ad title
9	**Aitech Defense Systems** – NightHawk RCU Rugged Computer Unit
31	**Alphi Technology Corporation** – Looking for a MIL-STD-1553 solution
2	**Annapolis Micro Systems, Inc.** – High performance signal and data processing
3	**Ballard Technology** – Do more with less
23	**BittWare, Inc.** – Looking to maximize your FPGA processing power?
14	**CoreSolid Storage Solutions** – XDOM PCIe mini card
39	**CPU Technology, Inc.** – Security is not a feature
44	**Curtiss-Wright Controls Embedded Computing** – Defy size, weight and power
25	**D-TA Systems** – 10G series record and playback systems
36	**Elma Electronic** – The leader in profiles
20	**Elma Electronic – Systems** – Rugged ATCA system for mobile network communications
19	**Excalibur Systems, Inc.** – Dragon
7	**Extreme Engineering Solutions** – Designed with your application in mind
43	**GE Intelligent Platforms, Inc.** – More processor. More data. More intelligence.
33	**InnoDisk** – i-DIMM industrial DRAM module
5	**Kontron** – Who can solve my SWaP-C challenges?
28	**Kontron** – High-performance IPv4/IPv6 OpenVPX switch
21	**LCR Electronics** – Engineered for your application
41	**Microhard Systems, Inc.** – Wireless innovation
10, 11	**Microsemi** – We create space
15	**Nallatech** – One Stop SWaP
35	**North Atlantic Industries** – The only compact, rugged chassis offering 300 I/O pins and processing
37	**Octagon Systems** – Re-defining rugged
24	**Parvus Corporation** – Qualified to perform
41	**Phoenix International** – VC1-250-SSD conduction cooled SATA solid state disk
27	**Sealevel Systems, Inc.** – Rugged connectivity deploys incredible power
32	**VersaLogic Corp.** – VersaLogic Tiger, strength and performance!
29	**Wind River Aerospace & Defense Division** – Innovation
13	**WinSystems, Inc.** – 1 GHz PC/104 SBC supports networking and communications

OpenSystems media.

Military EMBEDDED SYSTEMS

@military_cots

DSP-FPGA.com | VME and Critical Systems | PC/104 and small form factors THE JOURNAL of MODULAR EMBEDDED DESIGN | INDUSTRIAL EMBEDDED SYSTEMS | CompactPCI Advanced & Micro TCA SYSTEMS | Embedded COMPUTING DESIGN

Military & Aerospace Group

Chris Ciufo, Group Editorial Director
cciufo@opensystemsmedia.com

Sharon Hess, Assistant Managing Editor
sharon_hess@opensystemsmedia.com

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

Monique DeVoe, Web Content Editor
mdevoe@opensystemsmedia.com

Christine Capuano
Web/Editorial Assistant

Brandon Lewis, Copy Editor

Hermann Strass
European Representative
hstrass@opensystemsmedia.com

Konrad Witte, Senior Web Developer

Steph Sweet, Creative Director

Joann Toth, Senior Designer

David Diomede, Art Director

Matt Jones, Web Developer

Phyllis Thompson
Circulation/Office Manager
subscriptions@opensystemsmedia.com

Sales Group

Dennis Doyle, Senior Account Manager
ddoyle@opensystemsmedia.com

Tom Varcie, Senior Account Manager
tvarcie@opensystemsmedia.com

Rebecca Barker
Strategic Account Manager
rbarker@opensystemsmedia.com

Christine Long
Online Manager
clong@opensystemsmedia.com

Laura Arsenault
Media Assistant
larsenault@opensystemsmedia.com

International Sales
Elvi Lee
Account Manager – Asia
elvi@aceforum.com.tw

Regional Sales Managers
Barbara Quinlan, Midwest/Southwest
bquinlan@opensystemsmedia.com

Denis Seger, Southern California
dseger@opensystemsmedia.com

Sydele Starr, Northern California
sstarr@opensystemsmedia.com

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

Ad Coordinator
Steph Sweet
ssweet@opensystemsmedia.com

Reprints and PDFs

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

Editorial/Business Office

16626 E. Avenue of the Fountains, Ste. 201
Fountain Hills, AZ 85268
Tel: 480-967-5581 ■ Fax: 480-837-6466
Website: www.opensystemsmedia.com

Publishers: John Black, Michael Hopper,
Wayne Kristoff

Vice President Editorial: Rosemary Kristoff

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

Business Manager: Karen Layman

XPEDITE7370
HALO
HALO
X-ES

Field Intelligence

Enhancing platform protection with a digital receiver/exciter

By Duncan Young

Controlling the electromagnetic spectrum using Electronic Countermeasures (ECM) is crucial for survival in the combat theater. Designers of military platforms such as aircraft, surface ships, and ground vehicles are faced with the dual challenge of using onboard radar systems for their own situational awareness and weapons systems control, while simultaneously using ECM to defeat or deceive hostile radar systems trying to detect them. Digital Receivers and Exciters (DRE) are replacing previous generations of purpose-built analog hardware with DSP engines and field upgradeable software/firmware. While this capability has previously been available in ground installations or on large airborne platforms such as the C-130, Size, Weight, and Power (SWaP) requirements have meant that smaller platforms such as single-seat fighters have been denied many of these capabilities, until now.

Electronic Countermeasures protect friendly assets

ECM can be used to deny or confuse any part of the electromagnetic spectrum to disrupt communications or to avoid detection by sensors such as radar. To deceive an enemy radar, incoming pulses are identified and analyzed to be retransmitted as false echoes that appear to come from a different position or from multiple targets. Specialized airborne ECM platforms such as the EC-130H or EP-3 can protect multiple types of friendly aircraft within a battle space under surveillance by many radar types and positions. However, these are large platforms, not typically space- or weight-constrained, often having controlled, pressurized environments. Consequently, state-of-the-art commercial equipment can be deployed to digitally process any radar threats and provide protection in real time. The development of highly capable yet rugged digital signal acquisition and processing capability is now enabling integrators to extend this protection capability to: combat aircraft, Unmanned Aerial Vehicles (UAVs), helicopters, or ground vehicles.

Replacing analog

Over time, jamming has developed from wideband denial and the use of chaff – both of which will confuse friendly and enemy radar alike – to much more sophisticated replication of timing and pulse shapes. The final Intermediate Frequency (IF) stage of an ECM receiver will generally use an analog discriminator to measure radar pulses, but long-term instability and drift with temperature of the analog filters require regular recalibration for reliable operation. For maximum deception, pulse shapes must be accurately reproduced, and replacing the analog discriminator with digital signal processing is now preferred. But to achieve this will typically require signal sampling at 1.5 GHz with 10-bit resolution, to give real 8-bit digitization and up to 500 MHz bandwidth for the accuracy needed. Sampling at this rate generates vast amounts of data that can be transferred to a separate processing engine, or can be stored and processed locally in Digital RF Memory (DRFM). In either case, processing power is vital to reducing the time it takes to retransmit false echoes, particularly when countering increasingly agile radar systems.

DRE elements

The basic elements of a generic DRE are a front-end analog-to-digital converter, large capacity DRFM typically with Gigabytes of memory, a programmable signal processing engine, and a digital-to-analog converter to produce the false echoes. By their very nature, ECM characteristics and algorithms are proprietary and highly classified; thus, integrators and end users look for reprogrammability of the processing engine so that algorithms can be upgraded as radars evolve, yet be easily erased for security. The signal-processing engine could use a general-purpose processor device, but an FPGA such as Xilinx's Virtex-6 offers more in much less space. The Virtex-6 SXT family offers up to 2,016 DSP slices for the massively parallel processing task of analyzing the incoming data at IF rates and the creation of false echoes to drive the digital-to-analog converter.

Embedding DREs using VPX

Open standards-based, integrated system architectures are well established as a means of saving vital SWaP. These architectures, often implemented using the rugged VPX (VITA 46) packaging standard, integrate many previously separate subsystems – such as fire control, missile warning, or DRE subsystems – into a platform's main computing system. The modularity and architecture of VPX with its high-speed serial data and control planes plus the choice of 3U or 6U module sizes provide an ideal basis for COTS vendors to offer easily integrated subsystems or functions to embed within such a larger system. Based on a single 3U VPX module, the SPR870A from GE Intelligent Platforms provides a complete DRE subsystem with a programmable SX475T Virtex-6 FPGA and PCI Express VPX data plane (Figure 1).

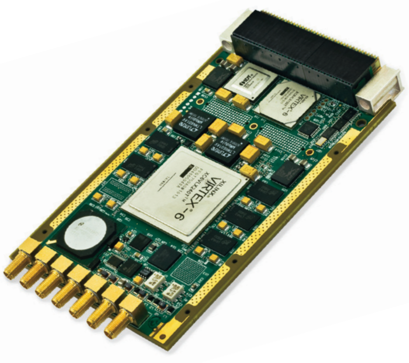


Figure 1 I The SPR870A based on a single 3U VPX module from GE Intelligent Platforms

In general, a DRE would be tailored to a specific radar type or frequency band. Hence, specialized ECM platforms will have many DREs to provide complete battle-space coverage. For rugged, small platforms, VPX with its PCI Express data plane offers a scalable solution, accommodating more than one DRE per VPX chassis for enhanced protection now and future growth as radar systems continue to evolve.

To learn more, e-mail Duncan at duncan_young1@sky.com.

NightHawk RCU™ Rugged Computer Unit

Light weight. Light years ahead. Hi-performance. Lo-SWaP. And OTS!

Harness improved processing and SWaP efficiency in the free-air-cooled Aitech NightHawk RCU™ Rugged Computing Unit – without sacrificing durability or versatility. The Remote Interface/Data Concentrator capabilities of this PC-based embedded unit are ideal for demanding applications in defense, aerospace, and rugged industrial environments, such as CBM, GPS, and RFID monitoring in manned or unmanned vehicles.

*Minimize weight...*at just 4.5 lbs., this space-saving unit delivers exceptionally efficient SWaP performance in a slim-profile 195-in.^{3} package.

*Expand I/O versatility...*with 18-36 vdc input, standard PC I/O interfaces, video-cam input, independent hi-def XGA and standard TV video outputs, plus extensive internal expansion support to add peripheral I/O interfaces for military/industrial embedded apps.

*Enhance your processing efficiency...*with a low-power Intel® Atom™ (Navy Pier) 1.6 GHz RISC microprocessor, 2 GB DDR2 SDRAM and 8 GB SSD memory, plus optional CompactFlash or 250 GB Solid State Disk (SSD) storage with room for customization.

*Take rugged to greater extremes...*with an environmentally sealed, extruded aluminum housing and innovative convection/radiation cooling design that dissipates more than 22 W at +55°C. With MIL-DTL 38999 connectors, the sealed NightHawk protects against windblown fine dust and sand particles, while numerous EMI/RFI features meet MIL-STD 461 emission and susceptibility limits, all in a shock-, vibration-, and corrosion-resistant design for harsh mechanical, climatic, chemical and electrical environments.

*Limitless applications...*maximize your options with the flexibility to configure the NightHawk RCU™ into the control unit you need it to be. Contact us today for detailed power and I/O specifications.

Aitech

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

Celebrating 25 Years of Success

Photography Courtesy of Lockheed Martin

We create space…
Microsemi

Mil Tech Insider

The growth of IP communications drives advances in embedded military data security

By Steve Edwards

The increasing volume of IP-based data sent over standard interfaces, such as situational awareness video and remote sensor data, is driving the embedded military market to recognize the need for advanced data network security. Increasing Ethernet connectivity between systems needs to be protected with advanced IP security techniques such as firewalls, Virtual Private Networks (VPNs), sophisticated cryptography, anti-spam, anti-malware, and anti-virus to ensure the integrity, confidentiality, and availability of individual systems. The challenge is how to best leverage COTS Ethernet security protocols and ease of connectivity while addressing the rigorous security needs of military applications.

Traditionally, military communications involved dedicated radio-based connectivity, such as Communications Security (COMSEC) and Transmission Security (TRANSEC). These dedicated systems – using proprietary military-specific systems – were generally considered more secure than traditional Ethernet networks, which with all of their advantages have also introduced Internet-based hacker tricks to the military space. The use of relatively low-end software to capture Unmanned Aerial Vehicle (UAV) video feeds in Iraq, widely reported in December 2009, is one example. However, network devices are providing a higher level of security as compared to software-based security.

Looking to COTS Internet security

While appreciative of the benefits that COTS Internet security offers, systems integrators and their end customers see potential risks. The good news is that some standard and sophisticated encryption algorithms and techniques proven in high-end commercial and financial Internet networks can be applied to embedded applications via software or with dedicated hardware.

Commercial Ethernet security technologies provide low-cost, fairly high-bandwidth communications, including Gigabit and 10 Gigabit interfaces. More importantly, they can be made transparent to the application, such that streaming video is “unaware” that video data is being encrypted or decrypted. Locating network security in the lower layers of the seven-layer Open Systems Interconnection (OSI) protocol model frees the upper layers, which are focused on the application rather than the communications, from security concerns while enabling the lower layers of network communications to handle security performance. Making applications security agnostic enables security methods to be added and changed independent of the application. Decoupling security from the application also enables multiple independent methods of security to be layered for added protection.

Multiple threats demand security techniques

No single security method can address all the types of vulnerabilities. For example, data encryption will not stop an attempt to access and scan the computer or a Denial of Service (DoS) attack. True protection requires multiple types of network security. Techniques beyond data encryption include Access Control Lists (ACLs) and firewalls, Network Address Translation (NAT), and deep packet inspection for anti-virus and anti-malware. Previously, the functions of communications and security were handled independently with data from a network switch or router being sent to a separate encryption box. Integrating these functions significantly reduces SWaP while increasing throughput and efficiency.

Simply processing an Ethernet stack presents a computational burden. Adding security processing contributes to that burden. With Ethernet, every single data packet must be inspected as a potential viral or spam threat. A single malicious packet breaching a firewall can be catastrophic. In 2003, the Sapphire worm infected 75,000 host computers in 10 minutes. Sapphire proliferated amazingly quickly, reaching a peak of more than 55 million malicious network scans per minute. Yet it was contained in a single 376-byte packet.

The good news is that network devices can deliver greater network security performance than software-based security. In addition, they support application transparency. The downside of software-based security is that these systems can usually only handle a single stream or single application’s network bandwidth at one time, while a hardware-based network switch with dedicated encryption capability can handle many applications and many gigabits of data traffic concurrently. Dedicated network hardware that combines network switching/routing with advanced security offloads the host processor while providing additional significant advantages. A dedicated network device can support hardware accelerated cryptography and provide dedicated pattern recognition engines for malware, Trojans, and viruses.

An example of a network device designed for military network security is Curtiss-Wright Controls Embedded Computing’s (CWCEC’s) VPX3-685 3U OpenVPX module. In addition to its switch and router functionality, the card provides a hardware accelerated Intrusion Detection System (IDS), secure firewalls and ACL, an IP security engine with hardware-accelerated crypto engine supporting multiple encryption algorithms, and a route and policy-based VPN. Each of the security functions on this 3U card addresses a specific network vulnerability. In a corporate network environment, each function might typically be deployed in a stand-alone box in a 19-inch rack.

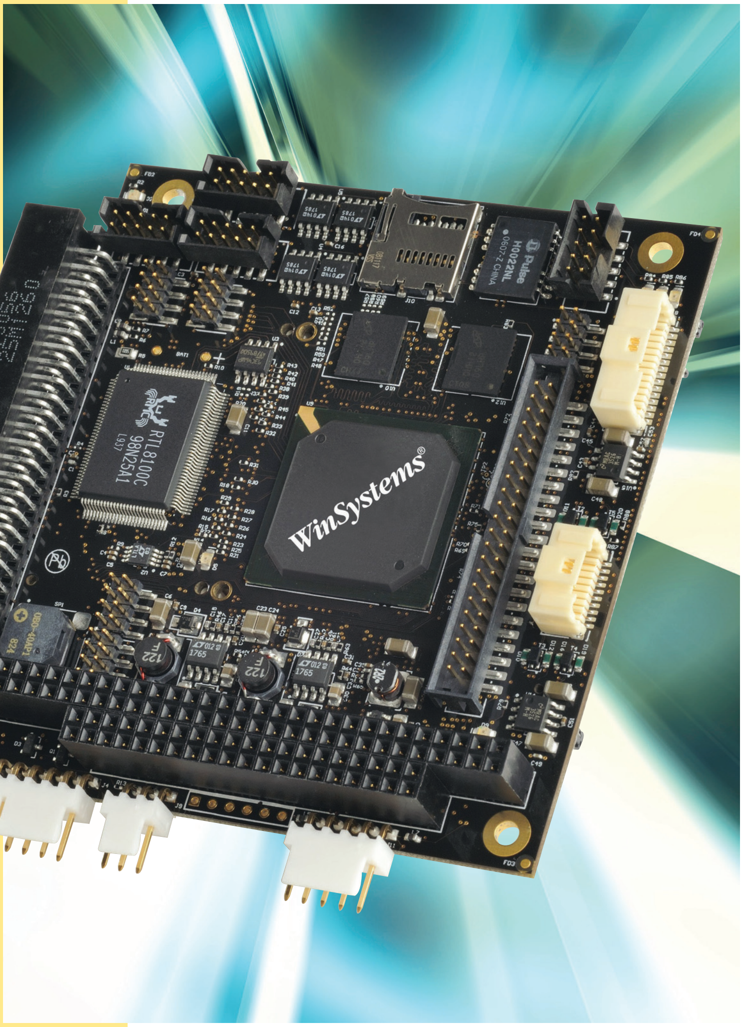
Protecting networks via Internet security tech

In 2009, there were more than 40,000 known and published network vulnerabilities. The challenge of keeping up with malicious network threats will only continue to grow. To secure critical military systems, embedded system designers must be able to adapt, leveraging the state of the art in today’s commercial and financial Internet security technologies. The threat will not diminish; it will only grow in complexity.

To learn more, e-mail Steve at Steve.Edwards@curtisswright.com.

1 GHz PC/104 SBC
Supports Networking and Communications

Hardened for harsh, rugged environments, the low power PCM-VDX-2 PC/104 single board computer is ideal for Mil/COTS applications. It is packed with serial, USB, and Ethernet ports, plus GPIO. With its diverse range of functions, most applications will not require additional I/O cards; however, it has Mini PCI and PC/104 connectors for specialty I/O expansion.



- Fanless, low power 1GHz Vortex86DX processor
- PC/104 Bus compliant form factor (90 x 96 mm)
- 512MB of soldered-down onboard DRAM
- 1MB of battery-backed SRAM
- CompactFlash socket
- Optional 512MB onboard SSD flashdisk
- Full-featured I/O includes:
  - Two 10/100 Mbps Ethernet ports
  - Four USB 2.0 ports
  - ESD protection on LAN, USB, and serial ports
  - Four serial RS-232/422/485 ports
  - 16 lines of general purpose I/O
  - PATA, LPT, PS/2 KYBD and Mouse controller
  - Mini PCI and PC/104 expansion connectors
  - WDT, RTC, status LEDs, and beeper
- Extended temperature -40°C to +85°C operation
- Runs Linux, DOS, and other x86-compatible operating systems
- Downloadable drivers available
- Responsive and knowledgeable technical support

Understanding long-term product availability is a critical issue for Mil/COTS customers, the PCM-VDX-2 is offered beyond 2017.

Contact us for additional product information and pricing. Our factory application engineers look forward to working with you.

Ask about our 30-day product evaluation.

Call 817-274-7553 or Visit
www.winsystems.com/PCM-VDX

WinSystems®
An Employee-Owned Company

715 Stadium Drive • Arlington, Texas 76011
Phone 817-274-7553 • FAX 817-548-1358
E-mail: info@winsystems.com

By Chad Trytten

Communications framework eases legacy stovepipe system integration

Warfighters need data to be fused into useful information providing integrated situational awareness. Accordingly, a communications framework can ease legacy system integration woes.

The DoD has overseen a rapid expansion in the use of next-generation technologies during the past decade, driven by two active wars and the rapid evolution of electronics and computing capabilities. However, the inability of these technologies to be integrated and communicate with existing legacy environments is hampering the competitive advantage these systems provide. Data acquisition systems such as persistent Intelligence, Surveillance, and Reconnaissance (ISR) and unmanned ground, aerial, surface, and underwater vehicles highlighted the problem. However, a multi-layer communications framework that adapts for use with new technologies is needed to simplify legacy system integration.

"One standard? Yes, if it's mine!"

Complex ISR, unmanned vehicle, and other rapidly fielded capabilities now play a major role in every military scenario. The United States built its technological advantage largely on the diversity and competitiveness of its supplier base. But now one of its greatest strengths has become its greatest liability. Systems provided by a broad base of suppliers use very different technologies. The costs and risks of integrating vastly different technologies are now escalating as innovation and military needs rapidly evolve.

The traditional approach to integration requires using singular standards to ensure certain systems can interoperate. However, this approach assumes that these conglomerates of systems can themselves be isolated. This is no longer true – interaction between different services and indeed between different countries in coalition warfare is now normal. Also, standards change, and often. Once a system is deployed, future versions will not be supported nor usable by that system. Another problem, often underestimated, is that standards have a tendency to represent a lowest common denominator and lag innovation. Vendors cannot easily adopt one standard where the specialty functions and closely held IP that differentiate each unmanned vehicle, ISR, or rapidly fielded capability are not supported.

An ideal scenario would allow all hardware and software, whether legacy or new, to leverage whichever standards they each require while operating within a Systems of Systems (SoS) framework economically, effectively, and sustainably. This would require independently produced systems to cooperate without significant custom modification. A mechanism is needed to integrate unrelated hardware and software components into one effective SoS, sharing information between highly disparate assets. Rather than enforce a single standard, it would embrace multiple, domain specific, incompatible standards.

Common messaging/standards

Products have been available for a while that enable independently developed technologies to share information through a standards-based messaging framework. Each of these products has its own requirements relative to which set of standards should be used, along with methods for conversion to these standards. In this approach, the legacy and new systems can exchange information in a neutral format that is consumable. But what if standards conversions could be point to point and managed systematically instead of converting all formats into a neutral format?

A highly adaptable approach utilizes dynamically loadable modules to implement support for each *layer* of technology in the operating environment – supporting each of the specific hardware, operating systems, programming languages, and network protocols to deal with specific conversion requirements. Semantic data definition is also separated in this environment to support multiple formats.

Decomposition of these four layers of the operating environment permits abstraction of implementation specifics for the system designer. It also simplifies the work of the application developer as software code can be automatically generated by developer tools independent from the data definition.

Info exchange or info integration?

A communications framework with supporting development and management tools can simplify the way information is exchanged between components of a distributed architecture. This is achieved using a unique combination of two key innovations. First, the information distribution layer uses a structured and detailed open-definition information model incorporating each interface to link the system together and provide a conversion mechanism for disparate system components. This is done by using a structured, user-definable information model of each component's interface. Then a distributed abstraction approach enables the distribution layer to operate across heterogeneous environments via a plug-in assembly that is entirely separate from the data type definitions in the information model. This approach is utilized by Spark's Distrix, which uses an object-oriented model for distributed programming with data distribution performed through an underlying publish/subscribe mechanism. However, Distrix does not force developers, specifically those developing procedural code for embedded systems, to use object-oriented concepts. In stark contrast to traditional integration and migration approaches, the user defines each system's standards in isolation. Semantic conflicts are handled separately, and the transport is automatically translated for use at each endpoint. This approach has been proven by the Office of the Secretary of Defense to significantly reduce time to deployment.

***Chad Trytten** is founder/CEO at Spark Integration Technologies. Contact him at chad.trytten@sparkintegration.com.*

Daily Briefing: News Snippets

By Sharon Hess, Assistant Managing Editor

www.mil-embedded.com/dailybriefing

BAE's hard body reaches 1 million strong

While there is no surefire way to prevent battlefield injuries, BAE Systems has perhaps developed the next best thing – and has the numbers to prove it: The company's hard armor inserts, which are tucked inside a warfighter's vest to safeguard vital organs and preserve lives, recently reached the "1 million manufactured" milestone. The Phoenix, Arizona based celebration was attended by U.S. Rep. Ed Pastor (D-Arizona), with a focus on BAE's USMC-, U.S. Army-, and Defense Logistics Agency-requested body armor including the Small Arms Protective Insert (SAPI) plate (Figure 1) worn on the side, back, and front torso. The company has additionally expanded to Next Generation (X) plates and SAPI derivatives such as Side SAPI, XSBI, and XSAPI, in addition to the SOLAR series, which adheres to requirements specified by the Special Operations Forces Equipment Advanced Requirements (SPEAR) as part of the Body Armor and Load Carrying System program.

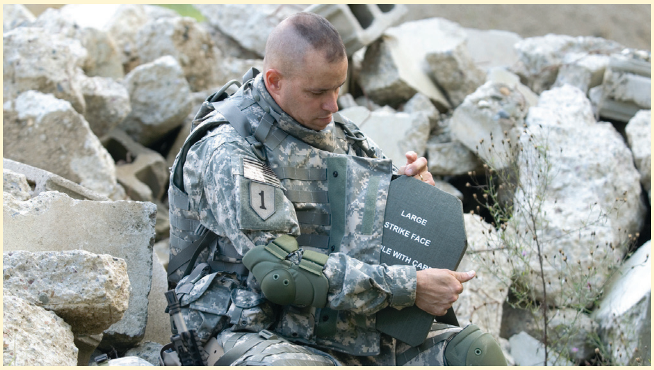


Figure 1 | BAE Systems recently celebrated the "1 million manufactured" milestone of its hard armor inserts such as this Small Arms Protective Insert (SAPI) plate. Photo courtesy of BAE Systems

Raytheon AIM-9X gets System Improvement Program sprucing

The U.S. Navy touts the AIM-9 Sidewinder as one of the most economical and successful – yet oldest – U.S.-weapons-inventory missiles; thus, a recent $19 million contract with Raytheon Missile Systems to engage the AIM-9X's System Improvement Program might not come as a complete surprise. Falling under the Foreign Military Sales program envelope, the contract consists of development, integration, and flight tests and "partners" six different entities: the U.S. Navy at $370,000, the USAF at $14 million, Korea at nearly $3 million, Saudi Arabia at about $1 million, Singapore at $720,000, and Turkey at $50,000, give or take. All this is certainly supporting evidence to the U.S. Navy's claim that the AIM-9 is the most ubiquitous air-to-air missile, presently residing in the arsenals of 40+ nations.

Lockheed Martin SEWIP: Domino effect

Often in life – and certainly in U.S. DoD contracts – one thing leads to another, like a proverbial game of dominos. Case in point: Lockheed Martin's $9.9 million Surface Electronic Warfare Improvement Program (SEWIP) Block 2 contract of November 2009 for AN/SLQ-32 EW system upgrades contained various contract options culminating at $167 million. The first $51 million option was activated in July 2010, and LM's Block 2 prelim design got the Navy's thumbs up. That then leads us to LM's recent Block 2 critical design review, which was deemed a success. So the next resultant "domino" is for LM to prep and present a duo of system prototypes by next year. The AN/SLQ-32 presently rides aboard U.S. Navy destroyers, aircraft carriers, cruisers, and other warships. SEWIP harnesses COTS electronics technologies.

USAF requests a new fuze

The USAF and Alliant Techsystems, Inc. recently penned a $35 million contract, stipulating that Alliant Techsystems renders a hard-target sensing "fuze" system to be utilized in conjunction with BLU-122, BLU-113, and BLU-109 (Figure 2) warheads and related guidance systems. And this fuze system is fierce, offering penetration survival of 5K to 15K pounds per square inch of reinforced concrete and/or multiple soil layers. Additionally, the fuze can be programmed to detonate at a specific time or inside a target's specified void. Safing, in-flight programmability, multidelay arming, and multimode function capability are also provided.

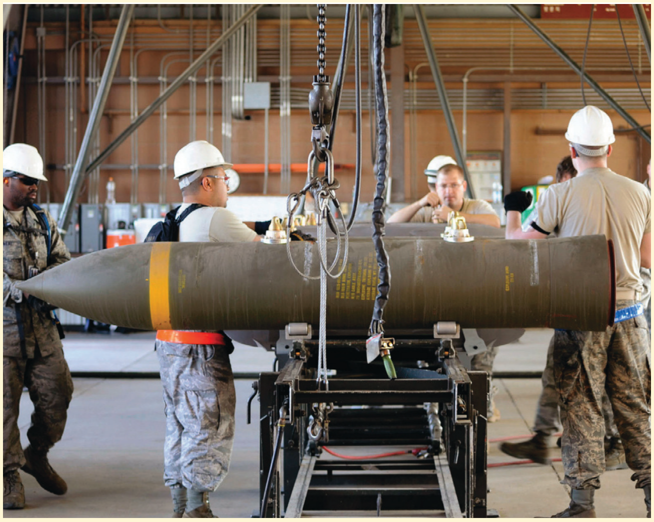


Figure 2 | A recent $35 million USAF/Alliant Techsystems, Inc. contract provides for a hard-target sensing fuze to be utilized with BLU-109 (pictured) and other BLU warheads. Photo courtesy of U.S. Air Force

Boeing begets Hellfire on an Avenger

Dealing with the U.S. Army's Hellfire is all in a day's work for The Boeing Company, which recently aided in testing Hellfire at Florida's Eglin AFB. Specifically, Boeing developed, manufactured, and installed the equipment needed to integrate the AGM-114 Hellfire missile and companion Hydra 2.75" rocket launchers mechanically onto an Avenger weapons system. During Boeing-supported testing, the missile was subsequently fired out of said updated Avenger system (Figure 3), under the Adaptive Force Protection System (AFPS) program umbrella. Though originally incarnated for air defense, Avenger is being evaluated for integration with ground-defense capabilities to increase system versatility. Avenger turrets have proven useful for mounting on vehicles such as the Mine Resistant Ambush Protected (MRAP). Avenger can also be utilized as an independent, fix-mounted weapon station.

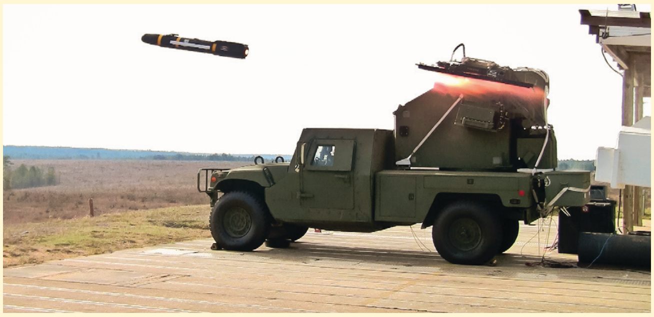


Figure 3 | Boeing recently supported the U.S. Army's initial test launch of a modified Avenger turret-fired AGM-114 Hellfire missile at Eglin AFB. Photo courtesy of U.S. Army

The soldiers' future is in their own hands

Handhelds are the wave of the military technology present and future, and a recent contract between the U.S. Army and General Dynamics C4 Systems reflects the trend. The $2.3 million contract specifies that General Dynamics renders a handheld prototype of battle command capability with more network connectivity than previously seen. The prototype also provides heightened situational awareness and more command and control functionality for Marines and dismounted soldiers, and falls under the U.S. Army's Joint Battle Command – Platform (JBC-P) handheld program. Though not described as a "smartphone," there are some similarities between smartphones and General Dynamics' answer to the call for a prototype: the GD300 computer. The GD300 tactical computer weighs a mere 8 ounces, renders real-time position and mapping information, and supports data, texting, video, or voice contact from far away or nearby. The rugged handheld also connects soldiers to mil software programs including the Tactical Intelligence Ground Reporting (TIGR) system and features an "apps-friendly operating system."

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

Figure 4 | APPTIS, Inc. and SAIC will render uninterrupted Defense Information Systems Network (DISN) Global Solutions (DGS) contract services, thanks to a couple of recent contract mods.

SAIC and APPTIS hang in at DISA

A couple of recent contract modifications keep the lifecycle-management gears turning at the Defense Information Systems Agency (DISA). The mods – granted to APPTIS, Inc. (formerly SETA Corp.) and Science Applications International Corp. (SAIC) – increase the two contracts' combined total by $635 million and add a duo of six-month options to the original IDIQ contracts. The impetus was DISA's need for uninterrupted Defense Information Systems Network (DISN) Global Solutions (DGS) contract services (Figure 4), including systems engineering, program management, software and hardware management, logistics, manufacturing, and test and evaluation, among others. The contract is thus now extended until March 31, 2012.

Letter to the Editor

Chris,

Nice reference to Radio Aware Routing (RAR) as No. 5 in your article: "2011: Top technologies for the warfighter" (www.mil-embedded.com/articles/id/?5051), in the *Military Embedded Systems* Jan/Feb issue:

> **"5. Cisco's Radio Aware Routing: Part of Cisco's Mobile Ready Net and offered on the company's 3200 and 5940 (3U CompactPCI, air- and conduction-cooled) deployed routers, the concept of ad hoc routing applies cognitive radio techniques to route data across whatever battlefield assets are available. Radio Aware Routing ... is part of RFC5578, PPP over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics."**

RFC 5578 is aimed at point-to-point radios. For broadcast-type radios (802.xx like), there are two new RAR protocols: R2CP and DLEP. R2CP was an industry collaborative effort, while DLEP is currently being worked with the MANET Working Group. Both are IETF submissions:

Radio-Router Control Protocol (R2CP)
www.tools.ietf.org/id/draft-dubois-r2cp-00.txt

Dynamic Link Exchange Protocol (DLEP)
www.ietf.org/id/draft-ietf-manet-dlep-00.txt

These complement RFC 5578 capabilities.

Regards, Bo Berry

U.S. Marines photo by Lt. Col. Deanna Bague

How to build a better smartphone:

Architecting with mobile virtualization for secure military communications

By Rob McCammon

OEMs and integrators can build cost-effective "superphones" – like the "ObamaBerry" or Jack Bauer's phone on the Fox TV show "24" – but for real military personnel and members of the intelligence community. To do this, a key consideration is understanding architectural options for melding standard commercial smartphone device hardware with mobile virtualization and open source software.

Military personnel and national security operatives are probably the most mobile workers in public service today, and depend on specialized and secure communications equipment to fulfill their missions at the office and in the field.

In the past, such secure communications devices – digital field radios, police/fire radio transceivers, and so on – emerged from highly proprietary design and acquisition cycles, resulting in systems that were hard to build, expensive to acquire, difficult to maintain, and impossible to upgrade. And they were yet another device for personnel to carry in addition to handsets and notebook computers.

Today, in lockstep with initiatives previously launched by the U.S. government, federal agency IT management and mobile device integrators and contractors are leaving behind the world of proprietary legacy systems and looking for COTS mobile solutions similar to those used by Jack Bauer on Fox TV's "24" or the "ObamaBerry."

The following sections explore using COTS hardware and software to create secure mobile communications devices. In particular, they focus on mobile security threats, lay out requirements for secure mobile devices, and present architectural options for integrating standard commercial smartphone device hardware with open source software and mobile virtualization. An Android proof-of-concept is also introduced.

Threats to mobile security

As mobile devices become increasingly similar to desktop and also data center computers, they suffer from the same maladies that plague corporate and government IT:

Vulnerabilities: Devices are subject to viruses, spyware, Trojan horses, and other malware. Application code bases and the middleware that supports them are large – tens of millions of line of code – and by definition untrustworthy and non-certifiable.

Buggy software: Mobile OSs and the software that runs on them are unavoidably buggy and thus are subject to a constant stream of *zero-day attacks,* which are exploits of application vulnerabilities unknown to the software developer. Open OSs supporting standard application development (such as RimOS and WindowsPhone) and open source OSs (such as Android or Linux) and applications that run on them emerge from commercial and community development of greatly varying quality and sensibilities – especially where security is concerned.

Brute force attacks: Mobile applications running on smartphones, including communications clients, are subject to Denial of Service (DoS) attacks on a per-process and system-wide level, for example. Of particular concern to government and other public entities are exploits that expose voice, text messaging, and other data streams to eavesdropping or other unauthorized third-party scrutiny. Another worry is the ability of unauthorized parties to interrupt mission-critical communications and spoof or forge participant identities and content.

A secure mobile communications device

Ideally, a secure mobile communications device such as a smartphone would be constructed from commercially available handsets and tablets that deploy off-the-shelf software platforms and applications running Android or Linux, for example. Devices need to support regular communications (voice, texting, social networking, and so on) and applications for "normal" conversations, but also enable secure exchanges (encrypted voice and secure texting/video transmission) among similarly equipped devices and/or infrastructure.

Ultimately, the scenarios of interest boil down to straightforward but difficult-to-meet requirements criteria. One requirement is that of secure communications, which refers to conventional applications including 3G voice, VoIP, Short and Multimedia Messaging Services (SMS/MMS), video, and so on, where clients run in secure contexts with options for encrypting data streams.

Open networks are also required. Using COTS hardware and software also predicates leveraging ubiquitous 3G, WiFi, and other public networks for private and secure communications. While GPRS, CDMA, 802.11, and so forth offer their own security regimes, those measures alone are insufficient to support secure and certified systems needs – they have been repeatedly demonstrated to be vulnerable to sniffing, spoofing, and other exploit techniques.

The requirement for off-the-shelf devices can also be difficult to meet. The vision for secure communications described herein builds on COTS hardware, but not necessarily mass-market handsets sourced through conventional operator and retail channels. Rather, secure communications devices represent collaboration of OEM handset manufacturers and third-party integrators and/or government contractors. Suppliers of aftermarket hardware encryption devices must also collaborate, such as vendors providing SD cards and/or encryption software running independently or leveraging existing capabilities in mobile chipsets. A concurrent requirement is that integration of these technologies still offers reasonable options for maintenance and upgrades, avoiding the expensive lock-in presented by legacy custom-built hardware and software.

Open software is also imperative. Smartphones and other devices suitable for the secure communications mission increasingly run open and/or open source OSs like Android, Linux, and so forth. As mentioned, a secure communications mobile device developer would be well advised to not replace those software platforms, but rather to augment or encapsulate them with secure and certifiable software.

Architectural options: Considering the candidates

Although this discussion emphasizes a COTS approach to secure mobile communications, it must also address the secure communications challenge holistically by considering several candidate architectures such as the following:

Point solutions

While requirements for mobile security are ubiquitous and system-wide, approaches to secure mobile communications tend toward single-function point solutions of limited scope in the software stack and communications stream. Such point solutions typically entail building and deploying secure and/or certified applications and middleware, encrypted data streams, and dedicated communications channels.

While constraining scope-of-effort is usually a good design and engineering practice, it ill serves modern mobile/wireless devices that are more like desktop computers than handheld radio sets. Unfortunately, these point solutions can still be compromised at an application level through cracking a saved or running application image, or by starving that application of compute resources (DoS).

Dedicated hardware

The most robust and secure method for isolating software is to run programs on separate pieces of hardware. Some mobile chipsets do feature unique companion processors to accelerate functions like graphics, video, audio, and in some cases, even encryption.

However, these dedicated coprocessors are configured as slave peripherals and do not provide sufficient context to run entire communications stacks and voice and messaging clients. In theory, more robust resources could be integrated on an SD card or other aftermarket interfaces, but then would lack means to transmit and receive secure data streams through an otherwise unsecured device without extensive modification to what should be a COTS OS and program stack.

Multicore architecture

High-end current-generation handsets and next-generation designs increasingly feature multicore application processors with two or more ARM processor cores. In theory, one or more cores could be dedicated to secure mobile communications, offering strong isolation from open OSs and open application environments.

In most cases, integrators or even OEMs would be hard-pressed to free up an entire CPU core for secure mobile communications processing, at least not without degrading overall device performance. (In a dual-core CPU, performance degradation could be up to 50 percent.) Moreover, even with a dedicated CPU core running secure communications loads, shared physical memory could still be subject to attack from the core(s) running an open application OS.

Virtualized architecture

A comprehensive and straightforward approach to architecting a secure mobile platform entails introducing mobile virtualization. This technology, like its data center cousin, runs over "bare metal" silicon to host an open application OS and software stack, or it could have one or more fully isolated secure cells (virtual machines) to host secure software in its own separate context. It could also have additional cells (as needed) to host selectively shared resources such as device drivers.

The benefits of a virtualized architecture are many:

- A very small trusted computing base (just the underlying microvisor) to ease certification and limit opportunities for exploits
- Deployment of existing off-the-shelf open OSs and software stacks in their own isolated cells
- Flexibility for integrators to instance new cells to meet the particular needs of a security regime and the technology to support it
- Capabilities-based security providing fully flexible dynamic protection management
- Defense against malware and security among cells through isolation and use of restricted intercell communications APIs – the visible open OS can become infected and fail without impacting secure communications software in other cells
- Fast Inter-Process Communication (IPC) mechanisms for high performance
- Resistance to DoS attacks through monitoring, prioritization, and load balancing among cells

Android proof-of-concept on the BeagleBoard

The mobile virtualization platform and security architecture depicted in Figure 1 builds upon a proof-of-concept announced by Open Kernel Labs last year. The OK:Android design for secure voice communications is based on Digi-Key's community-driven BeagleBoard running a Texas Instruments OMAP3530 system-on-chip. It is detailed in a white paper available at www.ok-labs.com/products/whitepapers-abstract-page.

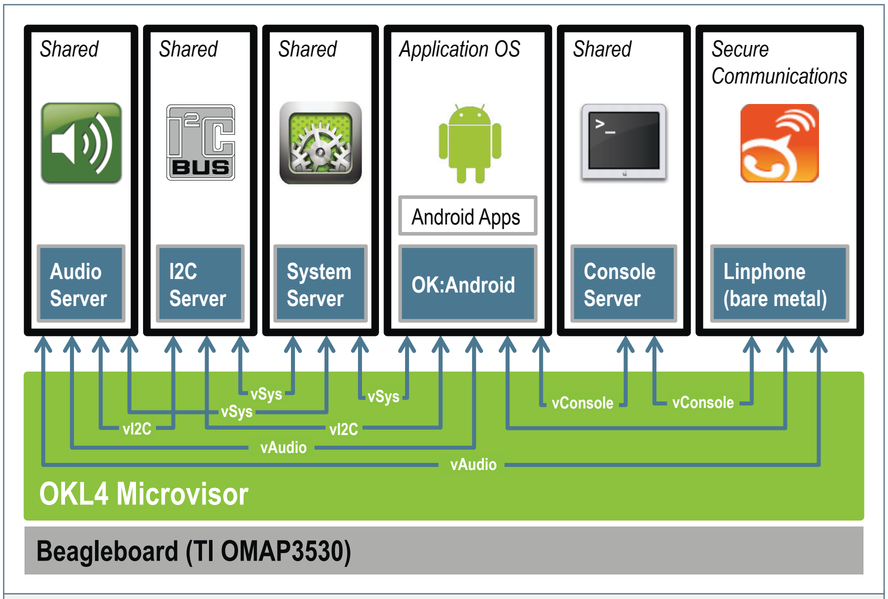


Figure 1 | SecureIT Mobile proof-of-concept for secure voice using Android

The secure voice design uses OKL4 to split up phone resources among multiple mobile hypervisor (or "microvisor") partitions, including one for OK:Android, one for secure communications, and one for shared server compartments. The latter includes shared server cells for audio, various peripherals, system functions such as clocks and power management, and a console for debugging. OKL4 can also facilitate secure video and texting in other instances.

From proof-of-concept to deployment

Previously, securing government apps, voice, and SMS required costly custom hardware and proprietary software stacks. This resulted in one-off handsets and radios, saddling government workers with yet another device to carry, locking in their employers to a single vendor, and presenting IT support staff with platforms that are difficult to maintain and impossible to upgrade. Today, several major government integrators and their partners are developing and deploying real-world secure mobile devices by building on mobile virtualization and off-the-shelf mobile hardware and software.

Rob McCammon *is Vice President of Product Management at Open Kernel Labs, where he is in charge of the OKL4 product line. During part of his 25 years of embedded industry experience, Rob was also Director of Advanced Technology Planning at Wind River Systems. He holds a Master of Management from Northwestern, and an MS in Computer Engineering from USC. He can be contacted at robm@ok-labs.com.*

Open Kernel Labs
312-924-1445 • www.ok-labs.com

Navy's NMCI network speeds warfighter's chance to get inside the adversary's OODA loop

An exclusive interview with HP's Bill Toti, Strategic VP and U.S. Navy Los Angeles class sub driver

EDITOR'S NOTE

More than any interview of recent memory, my time with HP's Bill Toti went by all too quickly. That's because this calm, unassuming man is chock-full of real-world experience. In war. In industry. And now, leading HP's efforts to secure a multibillion-dollar contract for the Navy's and Marines Corps' next-generation private network to replace NMCI. In the text that follows, Bill brings us up-to-speed on how NMCI is the world's second biggest network (behind the Internet), how it's secured and hardened from predators, and how it forms an integral backbone to help defeat America's adversaries. Bill is also a retired Navy captain who commanded nuclear submarines and "served time" at the Pentagon. Read on for a behind-the-scenes look at NMCI and its follow-on called "NGEN." (Edited excerpts follow.) – Chris A. Ciufo, Editor

MIL EMBEDDED: ***A lot of people might be surprised to see Hewlett Packard at AFCEA. What does Hewlett Packard do for the U.S. Armed Forces?***

TOTI: When I was in the Navy about 10 years ago, EDS won the contract to provide the Navy with its intranet called the *Navy Marine Corps Intranet* or *NMCI*. NMCI is a network that is connected to the Internet. HP ties in because it bought EDS, which was a $17 billion a year company. HP is a $135 billion a year company, so you know there's the capacity to do this. [NMCI] is now the largest network on the planet, other than the Internet. I don't think anybody would challenge the assertion that NMCI is the most secure, accessible network in the DoD. In fact, I've heard senior Navy leaders say exactly that recently.

MIL EMBEDDED: ***What makes NMCI the most secure?***

TOTI: [HP has been] very aggressive in how we monitor for and defend against intrusions. The defense department standards for cyber security evolve over time. The Navy has a single network, rather than a whole bunch of uncoordinated, disassociated base-centric or regionally centered networks like the other Services do. So the Navy's single network makes it easier for us to administer in ways that ensure compliance with DoD standards – and makes it easier to quickly deploy solutions as the threat changes.

The team not only made the network bigger by assimilating all the various elements of the early Navy networks into one large network, but the Navy HP team was also able to make it more secure. Usually when you make a network bigger, by definition you provide more points of entry – which makes it less secure. We did exactly the opposite. It is now more secure than ever. That's a huge accomplishment.

> "That's because the perfect decision made one moment too late is a failure. A good enough decision made on time is a success."

MIL EMBEDDED: ***How does Hewlett Packard differentiate itself from other network IT companies who might be feeding into SPAWAR or Naval IT infrastructure?***

TOTI: So first of all, Hewlett Packard is the biggest IT company on the planet – running the biggest network on the planet. It seems like a logical marriage to me, so that's issue one.

Issue two: It's Hewlett Packard Enterprise Services that runs the network, not the product side of HP. What that means is we take best of breed, and we are very honest in our assessment of components that ought to go into the network. When it makes sense to use a competitor's components in a network, that's what we do. We are nondenominational when it comes to selecting the solution, because we want to do the right thing for the customer, because we know that's the only way we'll get selected [to administer NMCI] the next time.

MIL EMBEDDED: ***Tell me more about HP's NMCI contract and how it came about.***

TOTI: The NMCI contract ran about 10 years – until just a couple months ago – and was very different from the contract we're in right now. The contract we're in now is called the *Continuity of Services Contract,* which is a follow-on to NMCI, which is transitioning into the next phase. It's called *Next Generation Enterprise Network* or *NGEN* for short. So, as originally conceived in the '90s when I was in the Pentagon, it was all the rage for the Services to say, "We ought to operate using the best business practices to the extent that we can." And I remember conversations at the Pentagon where someone would ask, "What company owns its IT?" Companies don't do that. They outsource IT.

Because IT was thought of as a business process application, the Department of the Navy treated it like a business decision. They said, "We could save money by having somebody else own the stuff." So [HP] used to do everything [on NMCI]. We owned and operated it.

MIL EMBEDDED: ***So that was the beginning of NMCI? How did it end?***

TOTI: A transition is beginning to take place under our current Continuity of Services Contract, and NGEN will be a new competition. It's not recompete. In fact, they're breaking up NMCI into four separate competitions. One is *transport,* which is kind of the cable – the fiber infrastructure upon which all the data is transported. Another is called *enterprise services,* which is the desktop environment that includes the end user for the large part, but also includes the servers and storage and things like that. And then the *software* and also *hardware,* and those are self-explanatory. This all falls under PEO EIS, which is a Naval Program Executive Office in northern Virginia. *[**Editor's note:** There's also an unrelated Army PEO of the same name.]*

MIL EMBEDDED: ***How many employees did HP have managing NMCI, and how big was the contract of record?***

TOTI: It's produced more than a billion dollars a year in revenue. There are thousands of employees who worked on the contract. You'd find contractor employees on every base.

MIL EMBEDDED: ***How many people in your own organization do you anticipate working on the NGEN capture team?***

TOTI: We always have dozens. You're talking about writing some fairly large proposals. We haven't seen an RFP yet, so we don't know what the requirements are going to be, but I've led multi-billion dollar pursuits in the past and we had 40 people writing. It takes a lot of money for a company to compete for something like this.

MIL EMBEDDED: ***Does NGEN have anything to do with the Naval open architecture concept of their embedded systems that talk on the network, such as CEC [Cooperative Engagement Capability]?***

TOTI: The short answer is that "open architecture" is a concept the Navy adopted probably a decade ago or more. And certainly, the Navy wants open architecture and as much IP ownership as they can have. So, that's all probably going to be part of the RFP engine going forward, but as I mentioned, I haven't seen an RFP yet. There will be other standards besides that to be incorporated in the RFP – I have no doubt.

MIL EMBEDDED: ***Tell me about some of the open standards one expects to see.***

TOTI: I know that TAA [Trade Agreements Act] is a big issue. Basically, it's a security construct that makes sure your components were not manufactured in a way that allows them to have spyware in them and things like that. Some of the cool really "Gucci" technology people want to order would have a hard time meeting the TAA certification standard. That becomes an issue at times when people ask for things they can't have, because our contract requires us to adhere to a standard the commercial world doesn't have to adhere to. We have even built our laptops to a mil-spec that most commercial companies don't have to worry about, to make them more tolerant to dust or heat.

MIL EMBEDDED: ***HP makes rugged laptops?***

You Tube *Military Embedded Systems* magazine certainly isn't the only media to interview Bill Toti. Check out this CBS "60 Minutes" Toti interview about the U.S. Navy's "Giant Shadow" exercise.

TOTI: We make rugged mil-spec standard laptops. We don't make extremely ruggedized. The NMCI contract requires some ruggedization, but not to [Panasonic] Toughbook standards, as a matter of routine. But our rugged laptops are certainly more rugged than something you'd get at Best Buy.

MIL EMBEDDED: ***Speaking of consumer tech, what are your thoughts about adding iPhones or Blackberries for access to NGEN secure military networks?***

TOTI: Companies like Apple really push the envelope of a concept called "design." It goes beyond mere engineering: It's the user interface and the form-fit-function. Throughout my industrial career, it's been a big mantra of mine to first think about high-level design: What is the user experience supposed to be? … whether we're talking about a FLIR pod that's on a helicopter or a Predator, or an IT system.

I don't see Apple's innovations as a threat. I see them as forging a need for us to figure out how to think innovatively like they do. We can build something with the look, feel, form, fit, and function of an iPhone with the right level of security. We just need the requirement and the funding to do that. *[**Editor's note:** These comments are incredibly prescient, because Steve Jobs publicly announced Apple's form-fit-function vision nearly two months after Bill's assertion, at the launch of the iPad 2.]*

MIL EMBEDDED: ***What about the risk tolerance factor?***

TOTI: The issue is whether there's a level of risk you're willing to tolerate for the convenience and accessibility of having [instant] access to information … not data, but information. Absolutely: There's a risk that someone is going to get into your information because you have a PDA. There's also a risk that the commander is not going to make the right decision because it took too long to get the information, which is a greater risk.

In modern warfare, the speed of the decision cycle – called the *Observe-Orient-Decide-Act loop* or *OODA loop* – is spiraling at ever-tightening timelines. So it's much more important that decision makers have information they need to make a timely decision than it is to worry about a manageable cyber threat. That's because the perfect decision made one moment too late is a failure. A good enough decision made on time is a success. The enemy has an OODA loop, too. All you have to do is make sure your OODA loop is inside of theirs.

MIL EMBEDDED: ***Interesting, spoken like a warfighter. So considering networks, many new things will come online.***

TOTI: That's true. It's an exciting opportunity, an exciting time.

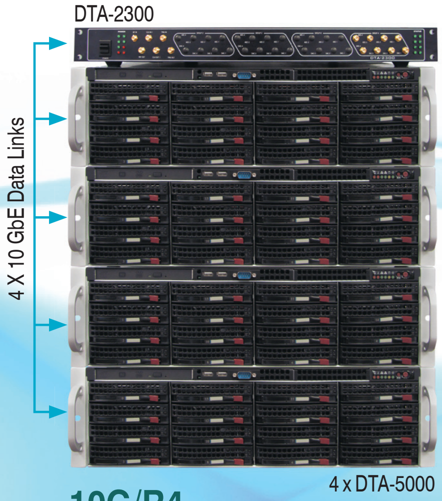
***Bill Toti** is Vice President for Strategic Programs, U.S. Department of the Navy at HP. He is responsible for overseeing HP's Naval Network Environment (NNE) 2016 initiatives, including the Next Generation Enterprise Network (NGEN). Bill has served in the U.S. Navy for 26 years. He can be contacted at william.toti@hp.com.*

HP Enterprise Services
1-800-566- 9337
www.hp.com

10G SERIES RECORD & PLAYBACK SYSTEMS

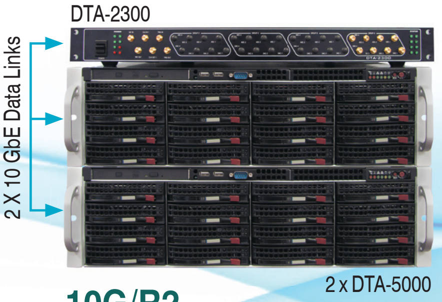
ULTRA-FAST, SCALABLE & 10 GIGABIT NETWORK POWERED

Synchronized (Phase-Coherent) Recording & Playback of Multiple Wideband Radio Signals



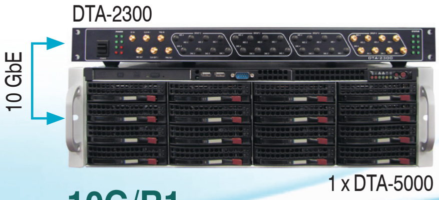
10G/R4

- 8 or 16 IF Inputs & Outputs
- 38.4 TBytes Storage Capacity
- 2.4 GBytes/s Sustained Record/Playback Rate
- Optional DTA-3200 (20MHz to 6GHz) tunable RF Front End



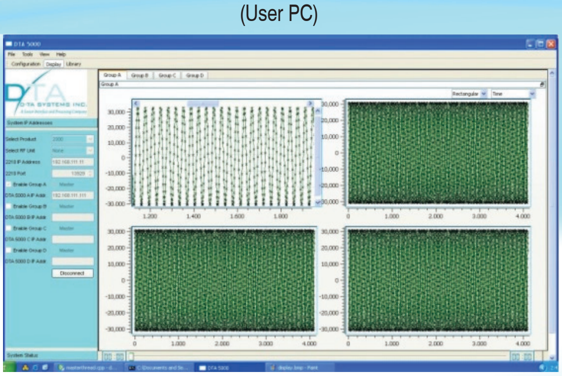
10G/R2

- 4 or 8 IF Inputs & Outputs
- 19.2 TBytes Storage Capacity
- 1.2 GBytes/s Sustained Record/Playback Rate
- Optional DTA-3200 (20MHz to 6GHz) tunable RF Front End



10G/R1

- 2 or 4 IF Inputs & Outputs
- 9.6 TBytes Storage Capacity
- 0.6 GBytes/s Sustained Record/Playback Rate
- Optional DTA-3200 (20MHz to 6GHz) tunable RF Front End



Comprehensive GUI for Failsafe Operation & Control of All System Components. Time, FFT and Waterfall Displays for Monitoring Data Quality During Record or Playback.

With 16-bit 130MHz ADCs & 500MHz DACs and programmable DDCs and DUCs, the 10G Series Systems offer high-precision and large IF Bandwidths. They are fully-integrated for immediate deployment.

1-877-382-3222
SALES@D-TA.COM

Download 10G Series Technical Presentation
WWW.D-TA.COM

NOTHING ELSE COMES CLOSE

D-TA SYSTEMS INC.
A Sensor Interface and Processing Company

SENSOR PROCESSORS THAT DRASTICALLY REDUCE DEPLOYMENT TIME AND COSTS

Silicon uniqueness as a security feature

By J. Ryan Kenny

Military developers have been investigating ways to measure and utilize chip-unique characteristics for security. Some of these techniques and capabilities are commercially available today, and open discussions are now taking place on how to use them to improve system security. But before making any decisions, it's imperative to gain understanding of the primary silicon uniqueness technology – the Physically Unclonable Function (PUF) – and its usage models.

One of the primary tenets of cryptography is the simple ability to calculate a large number for key and identity generation, but choosing a method such that factoring this number back to its constituent parts is nearly impossible. This is called a "one-way function." The ability to generate device-unique keys or identities based on physical world (hardware) randomness is an important new technology that is currently migrating from the "possible" phase to the "How do I use this?" phase.

The following discussion examines the state of this technology, and comes to a conclusion familiar to all practitioners of cryptography: The hard part is the implementation and the use case, not the algorithmic generation of the unique ID.

Survey of industry techniques

The primary silicon uniqueness technology available today in security products is often referred to as *Physically Unclonable Functions,* or *PUFs*.

A PUF is a physical function that is analogous to a one-way algorithm-based randomness function used in cryptography and key generation. More importantly, it is nearly impossible for would-be hackers to recreate the totality of the function in hardware for all inputs (thus the term *unclonable* in *PUF*).

Several methods have been proposed and implemented in PUF generation. The success of these methods is determined both by the entropy represented in the PUF value's response, and in the narrow band of determinism, or predictability, in the responses after repeating the same input.

Techniques for PUF randomness include chemically "doping" a material to create random responses to optical or chemical signals. This can be done in a lens, light filter, or chemical coating on a material. Intrinsic randomness looks at the physical properties of an object or material as part of its manufacturing or curing process. There are several more techniques being looked at for introducing intrinsic PUF randomness, and common areas for doing so include the initial states in silicon Static Random Access Memories (SRAMs), feed-back wired flip-flop chains, ring oscillator features (phase noise, interference signals, and so on), and electromagnetic properties of circuits. The chip-to-chip differences in any one of these these silicon measurements can generate random but deterministic responses, given the same inputs.

How secure are they?

The similarity between PUF circuits and cryptographic algorithms applies when assessing the security of PUFs: The strength of the PUF is part of the answer, but more important than the PUF itself is how it is used. Likewise, the implementation of algorithms and key handling is by far the largest security concern in the encryption market today.

There is no strong industry standard for measuring the algorithmic strength of a PUF circuit. However, there are numerous laboratory studies, government investigations, and proprietary benchmarks in play for measuring PUF success.

The basic theory of the "strength" of a PUF circuit is proportional to the entropy of the possible responses it generates ($S_{PUF,}$ or PUF entropy), and inversely proportional to the accuracy/diversity of the response to a single "challenge" (S_{RE}, or response entropy). This relationship is stated simply in Figure 1. PUF technology circuits typically have proprietary methods for transforming these low-entropy responses into unique key responses or identification codes.

$$\frac{S_{PUF}}{S_{RE}}$$

Figure 1 | Basic equation for PUF entropy and strength

Factored into this effectiveness is how the PUF circuit response varies with respect to temperature, usage, and other environmental factors like moisture. In addition, circuit characteristics like transistor voltage thresholds and response times begin to vary as the circuit ages and conducts high currents over prolonged periods of time. The determinism of the response can vary more as these events occur, making the described metric only effective under ideal conditions. Because PUF circuits are designed for security and information assurance, assumptions of "ideal conditions" are not usually realistic, and cannot be counted on when protecting critical information. Higher order use cases, therefore, must be able to address the environmental variability of existing PUF technologies.

Usage models for PUF circuits

There are several ways that PUF circuits are used as part of a security architecture. These map to various security needs that exist in commercial and sensitive military markets. The usage model is probably the most important factor in determining how to implement a PUF or other uniqueness technology in a military system.

Software and IP licensing and activation

The software and IP licensing and activation usage model focuses on the IP market and feature-based pricing in sophisticated electronic systems. This process has traditionally utilized protected license files or activation codes manually entered into a software interface. Traditional licensing relies on the protection of activation codes by other means (secure distribution, and so on).

The IP licensing usage model for unique ID technologies implements a PUF or other uniqueness circuit as an application-accessible function in the silicon device and OS driver. The IP licensing usage model can be accessed at any time to generate device-unique keys that verify a user's right to access or decrypt other IP in the system. As this is a commercial model for licensing purposes, there are typically few other protections for logging the number of challenges to the PUF circuit, identifying PUF circuit or system responses to unauthorized challenges, or specifying the appropriate interactions of multiple PUF circuits.

For cost and simplicity reasons, this model is implemented with the standard library approach in a circuit design, whereby user access to feature-based libraries is controlled by license and tracked to individual embedded devices using silicon uniqueness. This makes it appropriate and usable for FPGA fabrics, simple micro devices, and possibly mixed-signal circuits. It is less appropriate for large-scale ASIC circuits.

Inventory and counterfeiting control

The inventory and anti-counterfeiting usage model is aimed at higher-cost, lower-volume devices. The unique device ID is used in such a way that its personal identification is integrated into the operation and purpose of the device.

The uniqueness or PUF circuit is typically implemented in hardened logic in the device and is accessed only through prescribed hardware functions built around the PUF circuit. This usage

model is often used in a chip in place of a hard-coded unique identifier as an extra layer of protection against physical intrusion.

This usage model is aimed at providing a more secure “root of trust” for activities like digital hashing signatures, Web source authentication, and unauthorized change detection such as in the Trusted Platform Module. Such activities rely on the uniqueness of the device and its inherent signature key.

Critical Program Information protection

An important but not-often-described usage model for device uniqueness and PUF circuits is that of Critical Program Information (CPI) protection. This usage model protects the operation of the entire silicon device. The objective is to obfuscate to unauthorized users/developers all CPI operation, functions, and software instructions.

The primary difference in implementation of a PUF circuit for CPI protection is its limited-use model. Typically, the uniqueness or PUF circuit will have a single or dedicated purpose. The simplest and most effective use of this PUF circuit will be to authorize boot and initialization through uniquely sourced and encrypted boot images and software (see example in Figure 2). However, other individual PUF circuits may be used to further authorize access to memory managers, data peripherals, and additional pre-stored cryptographic keys.

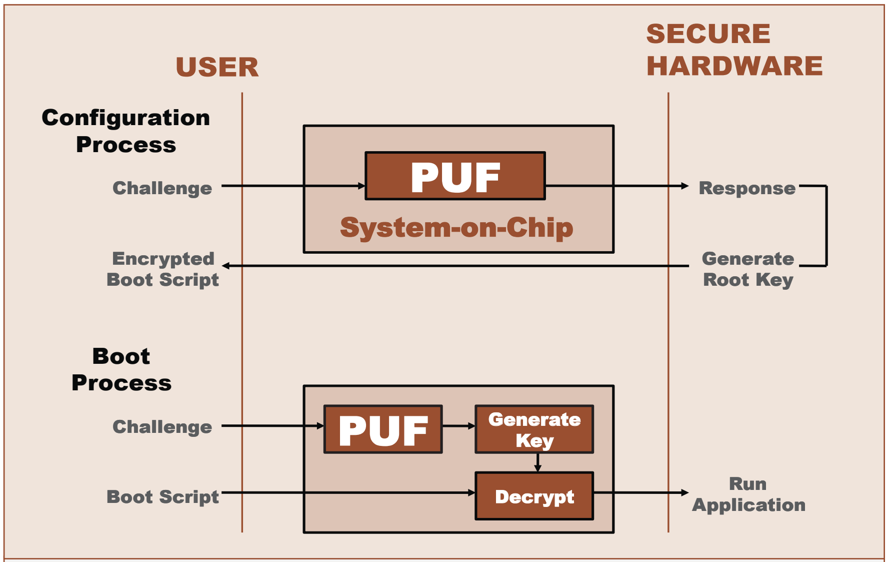


Figure 2 | Example use of PUF to initialize and authorize device boot

This usage model disallows access to the PUF circuitry and challenge mechanisms for any purpose but device enablement and boot. It necessitates specification and integration into a security architecture as part of an SoC design, with attention to all cross-circuit effects and side-channel vulnerabilities required for high-security processing.

Recommendation: Decide on a usage model first

When considering silicon-unique or PUF solutions, or answering the question of how effective these circuits are, a great deal depends on the implementation and how the device is designed to operate. While effectiveness of the PUF technology or circuit itself is also important, metrics on these circuits are not widely available, nor are there yet public guidelines on what might constitute “sufficient” security for IP licensing, anti-counterfeiting, or CPI protection.

Until metrics are offered or available, PUF circuits themselves can be considered relatively interchangeable, but their integration and implementations may not. A PUF technology can be designed and implemented for protecting proprietary information, but might have usage model limitations that might not make them suitable for the protection of critical military systems, depending on the scenario.

References:

[1] Intrinsic ID. “Conquering Copycats: The Key is Hardware Intrinsic Security,” Pim Tulys, August 2009, www.eetimes.com/electrical-engineers/education-training/tech-papers/4137648/Conquering-Copycats-The-Key-is-Hardware-Intrinsic-Security

***J. Ryan Kenny** is a product manager at CPU Tech. He is responsible for developing security requirements and certification road maps for the Acalis line of secure embedded processors. He joined CPU Tech in 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 M.S.E.E. and M.B.A. from California State University and Santa Clara University respectively. He can be contacted at r.kenny@cputech.com.*

CPU Tech
925-224-9920
www.cputech.com

INNOVATION IS THE FIRST UNMANNED AIRCRAFT THAT LANDS AT SEA.

Northrop Grumman X-47B
First tailless unmanned aircraft designed for
autonomous carrier-based capability.

Initial Flight
Edwards AFB: 29 minutes
February 4, 2011

How does the latest breakthrough in unmanned aircraft systems go from concept to carrier deck? With help from Wind River. Our VxWorks real-time operating system was chosen by the innovators at Northrop Grumman Corporation as the software platform for their Unmanned Combat Air System-Demonstration (UCAS-D) program and by GE Aviation as the foundation for the Common Core System, the backbone of the UCAS-D computers, networks, and interfacing electronics. Building upon VxWorks' proven reliability and unmatched performance, project engineers were able to rapidly create, deploy, and maintain safety-critical control systems—all while reducing development costs and maintaining schedule integrity. Proof that when innovators work together, the sky is hardly the limit.

Please visit **www.windriver.com/customers** to see
how Wind River customers have reached new heights.

WIND RIVER
INNOVATORS START HERE.

Case study: Dual-CPU PC/104 stack meets Marines vehicle OBC upgrade challenges

By Jonathan Miller

A recent military contract called for a compact, rugged, wide-temperature embedded system to be used in upgrading the U.S. Marine Corps already-vehicle-deployed Onboard Computers (OBCs). The challenge of upgrading the OBCs was met by integrating two CPU subsystems within a single PC/104 stack, while utilizing a new approach to conduction cooling.

U.S. Marines photo by Lance Cpl. Samantha H. Arrington

U.S. Marine Corps vehicles serve as the workhorses of U.S. global peacekeeping activities. The Onboard Computer (OBC) monitors the health of the vehicle's engine and drive train, to alert crew and maintenance staff to critical problems that might strand the vehicle during operation. If allowed to occur, such failures would present a mortal risk to the vehicle's occupants and, of course, to the vehicle itself.

Each vehicle's OBC gathers data through various onboard sensors, data acquisition subsystems, embedded computers, and remote user interfaces, and caches the data in local mass storage. Later, the OBC must rapidly transfer its collected data wirelessly to an off-board server, which aggregates and analyzes the diagnostic data collected throughout the fleet.

Accordingly, a large defense prime contractor recently required a compact, rugged, wide-temperature embedded system for upgrading a diagnostics Onboard Computer deployed on U.S. Marine Corps vehicles. As the following case study describes, the challenge was to upgrade the OBC's user interface, performance, communications, and internal storage, while meeting the stringent size, thermal, ruggedness, and other constraints of an existing enclosure (Figure 1). The solution involved integrating two independent CPU subsystems within one PC/104 stack, plus an innovative approach to conduction cooling.

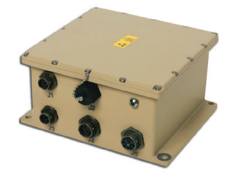


Figure 1 | The upgraded OBC embedded computer needed to fit within an existing sealed enclosure

Evolving system requirements

As initially envisioned, the required embedded system electronics upgrade would consist primarily of a PC/104 form factor SBC based on an 800 MHz National LX800 CPU – a custom PC/104 I/O module for interfacing via CAN to the vehicle's electronics – and a custom Uninterruptable Power Supply (UPS). These modules needed to fit within an existing 7" x 7" x 4" sealed enclosure. Additionally, the system was required to operate over the extended temperature range of -40 ºC to +71 ºC (measured at the enclosure's surface), and had to withstand MIL-STD-202G shock and vibration conditions.

During the defense contractor's design phase, it was determined that the anticipated architecture of initial upgrade design would not satisfy the diagnostic system's performance requirements. Consequently, a second embedded processor, dedicated to the tasks of wirelessly uploading data to the depot and managing the system's operator interface, was added to the architecture. The new dual-processor architecture also necessitated two additional Ethernet ports, through which the pair of CPUs would communicate with each other.

Based on the design team's estimate of CPU bandwidth needed for managing both the high-speed wireless data uploads and the OBC's operator interface, an Intel 1.6 GHz Atom Z5xx was designated to be the system's second processor.

This turn of events significantly complicated the diagnostic system's heat dissipation requirements because of the added power consumption of the new components (particularly the Atom CPU and its associated chipset), and because the number of boards in the PC/104 stack packed within the compact, sealed enclosure now needed to be doubled from two to four.

In short, the need for a second embedded processor appeared to be both a space and budget buster. The key challenges now would be:

- Fitting the expanded set of electronics into the small enclosure
- Meeting the application's operating temperature and shock/vibration requirements

After exploring various alternatives, the design team concluded that an all-COTS system upgrade could not provide a satisfactory solution for two main reasons. For one thing, too many boards would be needed in order to meet to the application's I/O and dual-CPU requirements, making it impossible to fit everything inside an existing enclosure.

Additionally, the conventional method of cooling PC/104-sized SBCs without forced air is to use a large, finned heat sink above the module, thermally attached to the CPU and chipset. However, this method would be unable to provide adequate cooling for reliable operation at the high end of the required external temperature range (+71 °C). A better thermal solution would be needed to maintain the CPU's junction temperature (Tj) below its specified maximum limit of +90 °C to prevent thermal runaway.

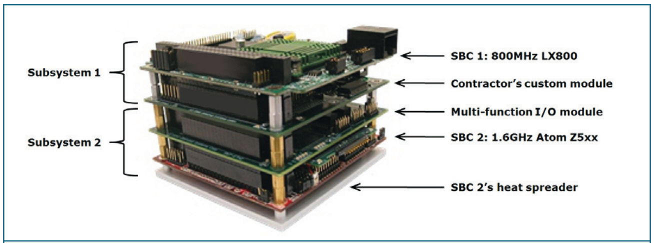


Figure 2 | The solution hinged on integrating dual SBC subsystems within a single PC/104-style stack, and removing heat from the Atom Z5xx processor/chipset via a large heat spreader.

Dual-SBC architecture

The solution to the contractor's dilemma turned out to be an innovative system architecture that solved both the size and heat-dissipation problems, while meeting the project's performance and cost targets. The approach involved physically combining the two subsystems into a single PC/104-style stack, while isolating them from each other functionally (see Figure 2).

In addition to the two PC/104-sized SBCs and the contractor's custom I/O module, the new architecture added a newly developed multifunction I/O module, which was to become a COTS offering from Diamond Systems. The new module integrated a collection of additional requirements of the contractor's application, including an 802.11a/b/g wireless radio, two 10/100 Mbps Ethernet ports, a SATA-interfaced 32 GB Solid-State Disk (SSD), and an SDVO-to-VGA video output converter.

Referring to Figure 2, SBC 1 gathers real-time data from various sensors and data acquisition components throughout the vehicle via the CAN interface residing on the contractor's custom module. SBC 2, meanwhile, manages the vehicle's operator interfaces, processes the vehicle data sent to it by SBC 1, caches it on the SATA SSD, and later rapidly uploads it via high-speed WiFi to the off-board server. While it might not be apparent from the photo, the PC/104 bus connector on the contractor's custom module (one down from the top) is implemented with a "non-stack-through" bus connector. Consequently, its PC/104 bus only connects upward to the stack-through pins of SBC 1's PC/104 bus, but not downward to the PC/104 bus of the modules below it. This creates the required functional isolation between Subsystem 1 and Subsystem 2.

So, the resulting four-module PC/104 stack satisfied all of the system's functional requirements. But without fans or exotic heat-extraction methods, how could a dual-processor stack situated within such a small, sealed enclosure be expected to operate reliably amid external environments of up to +71 ºC?

Conduction cooling meets PC/104

The heat dissipation challenge was addressed with the aid of the unusual conduction-cooled thermal design methodology of Diamond's Atom-based "Aurora" PC/104 form factor SBC. The SBC's main heat-generating chips – the Intel Atom Z530 along with its US15W chipset – are positioned on the bottom of the board, in contrast to the topside CPU and heat sink positioning generally used on PC/104 SBCs.

In this SBC's case, the underside processor and chipset are conduction cooled by means of a large, flat heat spreader. A layer of Z axis-compliant Thermal Interface Material (TIM) between the heat spreader and the underside IC packages ensures a low thermal resistance. In addition to efficiently cooling the SBC's hottest components, the board's bottom-mounted heat spreader also provides a

standardized pattern of four mounting holes, with which the entire PC/104 stack can be ruggedly bolted to a system chassis.

Although not employed previously on PC/104-expandable SBCs, conduction cooling is a common practice in COM-based designs. Figure 3 compares the effectiveness of Aurora's conduction cooling to that of the typical convection method used in the design of most PC/104-expandable SBCs. Lab tests confirmed that the SBC's conduction-cooling design successfully lowered CPU junction temperature (Tj) by more than 20 °C, compared with a conventional heat sink-based convection-cooling approach.

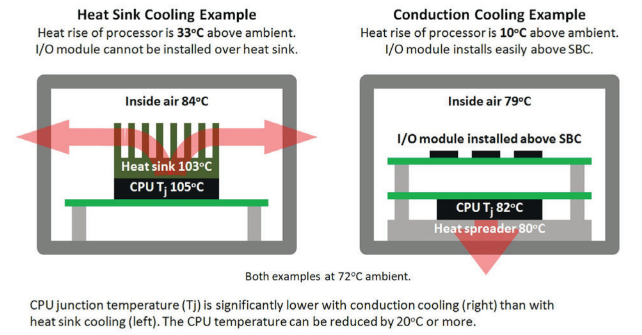

Heat Sink Cooling Example
Heat rise of processor is 33°C above ambient.
I/O module cannot be installed over heat sink.
Inside air 84°C
Heat sink 103°C
CPU Tj 105°C
Conduction Cooling Example
Heat rise of processor is 10°C above ambient.
I/O module installs easily above SBC.
Inside air 79°C
I/O module installed above SBC
CPU Tj 82°C
Heat spreader 80°C
Both examples at 72°C ambient.
CPU junction temperature (Tj) is significantly lower with conduction cooling (right) than with heat sink cooling (left). The CPU temperature can be reduced by 20°C or more.

Figure 3 | A comparison of typical topside, heat sink-based PC/104 CPU convection cooling and Aurora's bottom-side conduction cooling

Mission accomplished

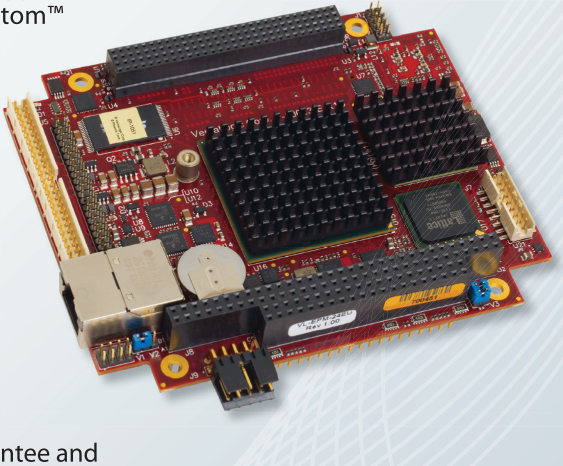
The contractor's objectives in upgrading the OBC's performance, communications, and storage capabilities – without an enclosure redesign – were successfully accomplished despite stringent size, thermal, ruggedness, and other constraints. The key elements of the solution involved:

- Fitting a dual-processor system architecture into a single PC/104-style module stack
- Developing a new PC/104-sized wired/wireless communications and SSD module product
- Applying conduction-cooling technology to the problem of removing heat from a PC/104-sized SBC's 1.6 GHz Intel Atom CPU and chipset

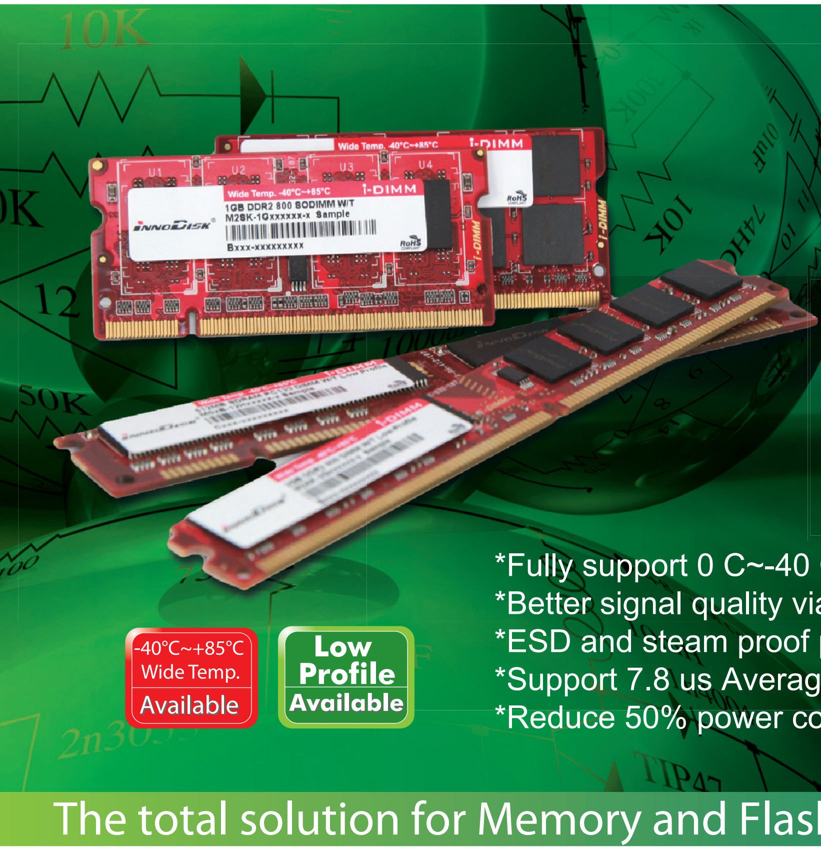
The end result is enhanced capability to monitor the engine and transmission health of a fleet of USMC ground vehicles, thus protecting the vehicles and their occupants. This success also demonstrates the continued viability of PC/104-style modules as a pragmatic solution to COTS development challenges.

Jonathan Miller is founder, president, and chief technology officer of Diamond Systems Corporation. He held various technical positions before launching Diamond Systems in 1989, and is Chairman Emeritus of the PC/104 Embedded Consortium. He holds a B.S. in Computer Science from the Massachusetts Institute of Technology. He can be contacted at jonathan@diamondsystems.com.

Diamond Systems Corporation
800-36-PC104 • www.diamondsystems.com



INNODISK®
Beyond your imagination



i-DIMM
INDUSTRIAL DRAM MODULE

-40°C~+85°C Wide Temp. Available

Low Profile Available

*Fully support 0 C~-40 C, and 85 C~95 C operation temperature.
*Better signal quality via 30um gold connector
*ESD and steam proof protection by PCB surface protection.
*Support 7.8 us Average periodic refresh interval (Auto-Refresh Rate)
*Reduce 50% power consumption on 85 C ~95 C

The total solution for Memory and Flash Storage

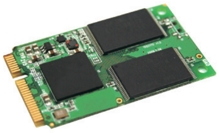
SSD Industrial Solid State Disk

2.5” SATA 20000H
- 256GB
- Read:230MB/sec. (max.)
- Write:190MB/sec.(max.)

1.8” SATA 10000-D
- 2GB~32GB
- Read:120MB/sec. (max.)
- Write:100MB/sec.(max.)

2.5” SATA 25000
- 16GB~128GB
- Read:250MB/sec. (max.)
- Write:200MB/sec. (max.)

EverGreen Series
Industrial Flash Storage

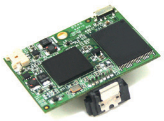


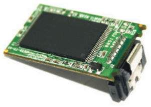
EverGreen 2.5” SATA SSD
- 16GB~128GB
- Read:220MB/sec. (max.)
- Write:150MB/sec. (max.)

EverGreen mSATA
- 8GB~64GB
- Read:220MB/sec. (max.)
- Write:150MB/sec. (max.)

EverGreen SATA Slim
- 8GB~64GB
- Read:220MB/sec. (max.)
- Write:150MB/sec. (max.)

D150 SATA Module

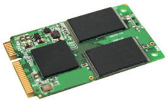




SATADOM®
D150Q Series

SATADOM®
D150S Series

SATA Slim D150



mSATA D150

CFast D150

Industrial SD card

- Compatible with SD 1.1/2.0 specification
- Support speed up to Class 10
- Support wear-leveling algorithm
- Built-in ECC function
- Support S.M.A.R.T function (New)

www.innodisk.com

InnoDisk USA Corporation
43130 Osgood Road, Fremont, CA 94539 TEL: 510-314-8393 FAX: 510-314-8394 Email:usasales@innodisk.com

U.S. Army photo by Sgt. Erica Knight

Designing and testing for reliability: Ruggedizing vetronics to survive

By Curtis Reichenfeld

When using COTS for ruggedized vetronics systems and subsystems, designing in cutting-edge technologies – such as metal matrix composite enclosures – and employing test methodologies including MEMA, RGT, and SRT will help ensure Size, Weight, Power, and Cost (SWaP-C) success.

A key challenge when ruggedizing COTS-based vetronics for military platforms is posed by the necessity of using available commercial and industrial components in most electronic systems. MIL-STD components (-55 °C to +125 °C) are either not available, or they are neither practical nor economical. As a result, subsystem designers must carefully analyze and test the thermal management features of the rugged system to ensure optimal performance and reliability in harsh combat environments before it is deployed. Making matters worse, more extreme operational temperatures than those specified in the past for military environments, such as those of the desert environments in Iraq and Afghanistan, are now commonly confronted.

Today's rugged military systems are typically designed for ambient operating environments ranging from -40 °C to +71 °C. The electronics, such as computer boards, integrated into contemporary ruggedized subsystems are specified to perform at -40 °C to +85 °C at the card edge. These thermal management challenges make it difficult to cool today's advanced electronics with a natural convection-cooled chassis, but a metal matrix composite enclosure is key in thermal management.

Moreover, to achieve Design For Reliability (DFR) with COTS, the subsystem needs to be designed to survive and perform over the extreme temperature range combined with intense shock and vibration. It also needs the necessary reliability and availability to perform the mission. To ensure these levels of reliability, subsystem integrators are going beyond their traditional responsibility to provide advanced testing and analysis of components from third-party suppliers to guarantee performance and quality.

To achieve DFR beyond thermal management requires a full range of techniques including component analysis, subsystem-level testing, Environmental Stress Screening (ESS), infant mortality testing of system-level components, the use of redundant elements, intelligent power, and health management. Thermal analysis and simulation are additional powerful tools that enable the system designer to discover potentially harmful hot spots and to redesign to improve overall system reliability.

The following discussion examines a new metal matrix composite enclosure designed to help the system continue reliable operation in extreme environments, in addition to a case study of a vetronics subsystem where RGT, SRT, and MEMA tests were performed.

Metal matrix composite enclosures beat the heat

On the cooling front, one promising approach for significantly extending the thermal management limits is the use of new enclosure designs that use proprietary advanced composite materials to both increase cooling and lower weight, a breakthrough for Size, Weight, and Power- (SWaP)-constrained applications. This new class of enclosure uses a mixture of metal matrix composite materials to provide 2-to-3x greater thermal conductivity than is available from aluminum alone (Figure 1). The technology comprises a unique thermally efficient composite core housed within a structural composite shell. This makes it possible to provide the cooling performance of copper without the 3x weight penalty, not to mention the higher cost. Recent test results of the composite enclosure technology using a baseplate-cooled 3U VPX or CompactPCI enclosure showed a 2.4x increase in thermal conductivity at the chassis level (2.4x decrease in sidewall temperature rise), along with a 10 percent weight decrease compared to aluminum construction. The ability to thermally manage higher-power circuit cards has become increasingly critical, as leading-edge multiprocessing and DSP system designs accelerate their use of new technologies such as multicore processor-based VPX board architectures.

This new enclosure technology offers the potential to enhance the weight and thermal performance of natural convection-cooled, forced air conduction-cooled, or liquid conduction-cooled chassis through superior heat spreading.

Design for reliability: A case study

A real-world example of the value of DFR recently occurred. The challenge

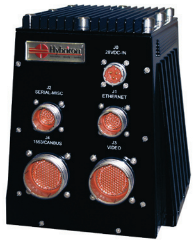


Figure 1 I Metal matrix composite enclosure

was to cool a vehicle and mission control subsystem on a military vehicle in a +71 °C ambient environment in dead air without fans or ventilation. Aggressive field and laboratory testing of the vehicle's subsystem resulted in a highly reliable product. The test methods used included qualification, Reliability Growth Testing (RGT), Statistical Reliability Testing (SRT), and hybrid MEMA SRT/RGT. The test technologies included traditional Single-Exciter Single-Axis (SESA) ElectroDynamic (ED) shakers, Multi-Exciter Multi-Axis (MEMA) ED shakers (Figure 2), and pneumatic repetitive shock. All the tests were performed using the procedures defined in MIL-STD-810G, with the exception of HALT, which exceeded the standards. A closer look at these testing methodologies is warranted.

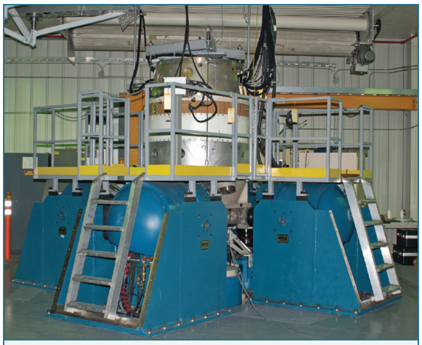


Figure 2 | Multi-Exciter Multi-Axis (MEMA) Electrodynamic shaker

RGT testing

RGT testing was used to determine temperature and voltage, the SESA random vibration, pneumatics and temperature, and SESA repetitive shock and temperature values. To assess its temperature and voltage, the subsystem underwent high then low temperature in its vehicle orientation. Temperatures were stepped, and for a given voltage, a full Acceptance Test Procedure (ATP) was performed. To determine the SESA random vibration, a unit was placed on an electrodynamic or hydraulic shaker and submitted to one complete life at an exaggeration factor of 3.5, followed by another run at 4.5. To determine the value for pneumatics and temperature, the unit underwent high Grms impacts from a pneumatic hammer. Stepped stress was applied at the operational low then high temperatures. An eight-hour endurance test was then run at 25 Grms, with half the time at the operational low temperature and the other half at the high temperature.

The SESA repetitive shock and temperature testing comprised multiple single-axis shocks in an attempt to determine if single-axis shock can provide similar results to multiple axis, or whether it is required to have a combination of multiple directions to uncover latent defects. The amplitude of the shock was increased in 20 *g* increments until failure occurred. Duration and shock pulse were not varied to maintain spectral consistency of the Shock Response Spectrum (SRS). In each axis, 50 shocks were applied at the low-temperature design level and 50 more at the high-temperature requirement for a combined environment input.

SRT testing

SESA random vibration and temperature is used to determine a reliability prediction within a desired statistical confidence level, based on the assumption that mechanical energy and thermal energy are the primary drivers of fatigue in a product. This testing comprised life testing at the design's high temperature for one axis, followed by another life test at the design's low temperature, with this sequence repeated for all three axes.

MEMA RGT/SRT hybrid testing

The subsystem also underwent a hybrid test that combined MEMA, RGT, and SRT. MEMA testing involved controlled random vibration excitation in multiple axes simultaneously. The shaker system used for this test had eight electrodynamic shakers that provided 6-DOF motion (three translational and three rotational).

Of the test technologies used, MEMA shaker technology produced the greatest ability to apply test results to reliability information. MEMA vibration testing was used to reduce laboratory test durations and increase laboratory test fidelity of the military ground vehicle. A MEMA shaker utilizes multiple single-axis actuators coupled into one shaker head, enabling simultaneous shaking of a test article in multiple degrees of freedom. This test method is inherently more realistic to field stresses and can reduce laboratory test durations by 66 percent. Testing the subsystem provided a realistic example of a complicated mission-essential LRU with extensive laboratory and field information; thus, MEMA testing could directly compare other methods of verification and validation.

Accelerated Life Test (ALT) via vibration stress is often used to provide qualitative and quantitative levels of confidence in the reliability and ruggedness of a product before it is deployed into the field. Choosing the appropriate test program can be difficult, depending upon the available cost and schedule to meet an acceptable risk threshold. MEMA testing promises to be a viable testing method to address cost sensitivity and schedule risks, and to provide high-failure mode and cause fidelity.

Demand for rapid deployment of the vehicle required that units be fielded in parallel with laboratory test efforts. Laboratory test methods were used to replicate all field defects. The design changes implemented as a result of the defects detected, in combination with ESS of the assembly, prevented any failures on the most recent version of the subsystem in the field. All described subsystem tests were performed by Curtiss-Wright Controls Electronic Systems.

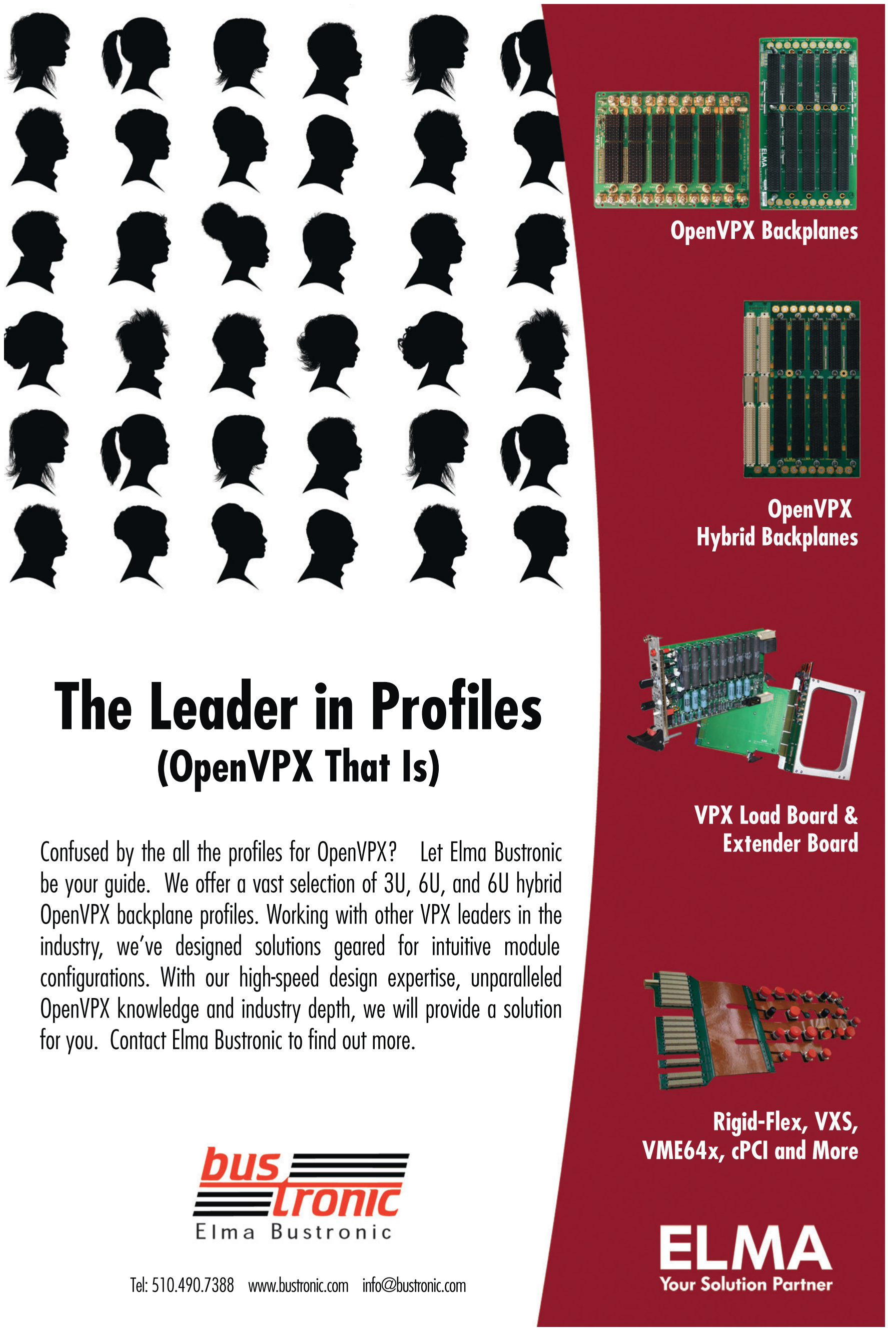
Keeping pace with new ruggedization trends

Designers of rugged vetronics systems must continuously adapt to emerging military system needs, understanding and anticipating the latest requirements for cooling and SWaP-C that continually drive advances in the approach to ruggedizing vetronics. One example of a trend that will drive new approaches to ruggedizing vetronics is the emergence of smaller military vehicles designed to hit price targets derived from the commercial automotive realm. To meet these needs, system integrators will have to come up with new approaches to ruggedize for smaller, more affordable vehicles. These new electronics developments such as new SWaP- and heat-efficient composite metal enclosures – combined with MEMA and RGT/SRT testing – will drive new ruggedization approaches and design for reliability.

***Editor's note:** Curtiss-Wright Controls has two separate and distinct divisions working on embedded technologies. This article was written by CWCEL (Curtiss-Wright Controls Electronic Systems).*

***Curtis J. Reichenfeld,** P.E., is the Chief Technical Officer at Curtiss-Wright Controls Electronic Systems. He has more than 25 years of experience in safety-critical hardware and software for military electronic systems. He can be contacted at creichenfeld@curtisswright.com.*

Curtiss-Wright Controls
Electronic Systems
661-257-4430
www.cwcelectronicsystems.com



GPS
LAN
Option
Power
ANT1
LNK / ACT
PWR
Display
Multi I/O
COM/CAN
ANT2
OCTAGON SYSTEMS
RMB-C2

Xilinx becomes master of their own domain; App Store to follow

An accidental interview with Brent Przybus, Director of Platform Marketing, Xilinx

Throughout 2011 Xilinx has been furiously announcing new targeted design platforms, tools, and high-density stacked chips. They've also not squelched rumors that they'll get into the SOC/ASSP business if the volume is right. I pulled aside their chief marketing guru Brent Przybus at a Xilinx press event where he casually provided the following information. Little did I know at the time that he was mapping out Xilinx's strategic plans: more IP via an App Store and FPGA-like devices propagating into higher-volume consumer markets. Edited excerpts follow.

– Chris A. Ciufo, Editor

What's new at Xilinx these days?

PRZYBUS: There's a difference in Xilinx's philosophy. Xilinx used to do technology for the sake of technology. But the reality is that customers are looking to do some pretty amazing things with an FPGA, and they're not going to tolerate technology simply replacing technology. They need solutions to problems, and that's really where the fundamental difference in our approach now comes in: If there's a problem, let's figure out how to build a complete solution for that customer so that he can solve that problem. By doing this, we can get FPGAs adopted in ways we wouldn't have been able to before.

So Xilinx is trying to expand out of its "comfort zone" markets, if you will?

PRZYBUS: Yes. A lot of our business partners are deeply immersed in a circle of markets that probably don't know Xilinx very well. A great example of this is the automotive industry and companies that work closely with major auto manufacturers. While quite a few of these companies know Xilinx when it comes to solutions, they have a better relationship with the vendors they have worked with for years. We now work with these vendors, showing them how to use FPGAs to build market-specific solutions known as *targeted platforms.*

How much more does Xilinx intend to get involved with customers than before?

PRZYBUS: It comes down to empowerment. We start by providing base platforms that include functionality that is common to most all applications. We show by example how best to take advantage of the many features in an FPGA. Avnet and other vendors take these base platforms and extend the functionality to include domain capability such as DSP. Finally, market-specific vendors take these base and domain platforms and extend them to build market-specific platforms: solutions to a given market problem. We provide the building blocks and step back, let the work happen, and the results show up.

> “Xilinx used to do technology for the sake of technology.”

The benefits are twofold. First, our core business: next-generation aerospace and defense, medical imaging, communications, and test and measurement – companies that know a lot about FPGAs learn how to take best advantage of new features and technology needed to build their systems. For them, the base or domain-level platforms provide what they need.

Second, for our new business targeting specific markets – automotive, consumer – we provide platforms to solve market problems using FPGAs in a way they wouldn't have thought of before. That's where the growth will also come from.

You'll have FPGA technology that customers can commoditize and drop into their end design?

PRZYBUS: Yeah, the platform approach enables a model that will be something like iTunes, where you have developers creating market-specific applications, linked to customers who can find these applications and drop them into their FPGA. It could be a commodity thing, yes.

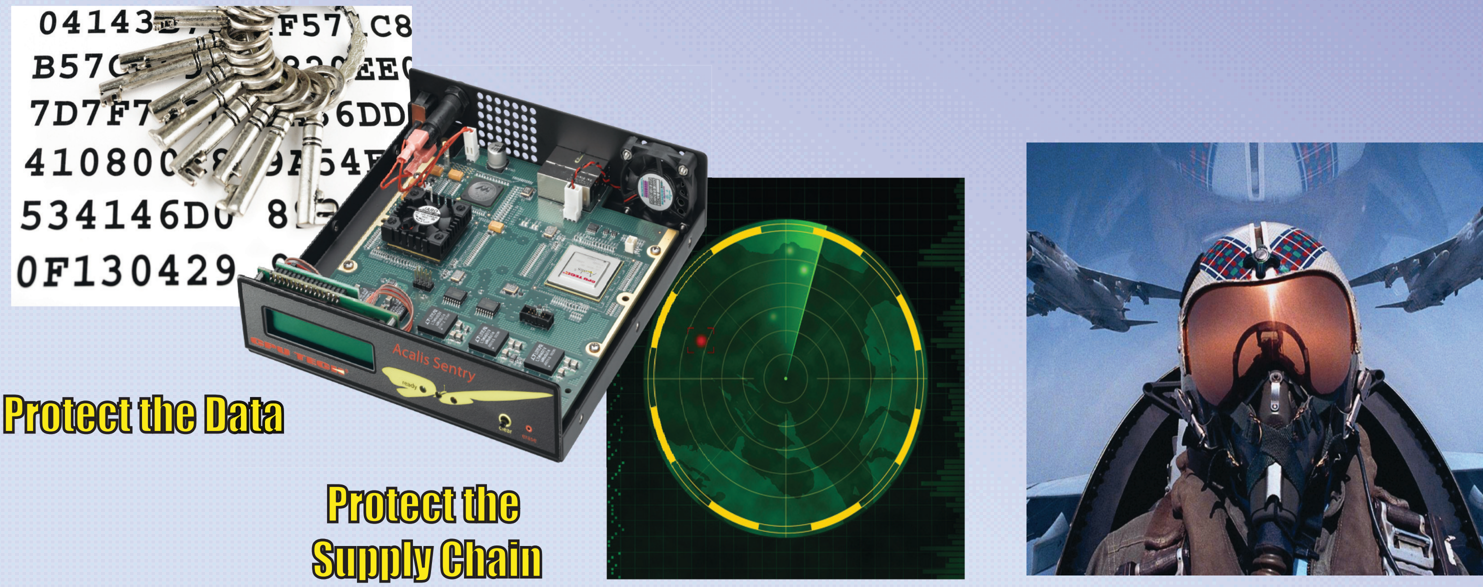
An App Store for FGPAs?

PRZYBUS: I think the analogy loosely works. We certainly have the enablers. The work we've been doing with ARM's AXI4 common interconnect, IEEE standards to support encryption, and IP-XACT enable what we call *plug-and-play FPGA design,* a key component of what you're talking about: the platform App Store of sorts. I don't believe customers will ever implement an entire design using content from the App Store; they will be able to replace possibly 50 percent of a design using these apps, though. In the end they have access to [something] they can easily use.

***Brent Przybus** is Director of Platform Marketing with responsibility for platform definition, global introductions, and marketing campaigns for the company's current and next-generation platforms. Contact him at brent.przybus@xilinx.com.*

Xilinx
408-879-4631 • www.xilinx.com

Security is not a Feature: It's the Mission



Protect the Data

Protect the Supply Chain

Protect the Technology

→

Protect the Warfighter

Acalis®

Secure Processor and Development Environment

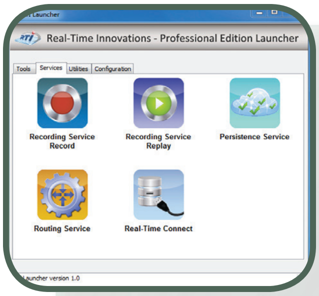
925-224-9920 www.cputech.com Available for Order

CPU TECH®

Leading Solutions You Can Trust

Editor's Choice Products

Editor's note: Military Embedded Systems *is "hip" to the whole Web 2.0 social networking revolution. While we don't know which of today's buzzy trends will last, we're going to start including links to vendors' social networks, when provided. You can also reach us on Twitter, Facebook, and LinkedIn … and that's just for this week. Next week there'll undoubtedly be more new sites.*



RTI bonds DDS with government researchers, on the cheap

The publish-subscribe Data Distribution Service (DDS) continues inroads into DoD distributed networks because of easy data and message passing between nodes. But the DDS concept isn't easy to understand, nor is it "cheap" for the typical shoestring budgets of government labs, SBIR winners, or universities. Real-Time Innovations (RTI) is changing that through the company's DDS Technology Network, a comprehensive training, tools, and software website designed to help researchers get up to speed quickly and inexpensively.

First off: Per-member prices range from $2,500 to $4,000, based upon the organization's size. For this price, members get a payload full of valuable stuff starting with a no-charge license to RTI's DDS software. Also included are tools, runtime services from the company's Professional and Elite toolkits, and a pile of source code. But perhaps most valuable in this program are the mentoring and training materials, ranging from access to DDS experts ("humans"!) in data-centric design, to distributed system security and safety, as well as tools for applications in control systems and unmanned vehicles. Other training includes workshops, phone and email support, community forums, and discounts for on-site training. According to RTI, more than 200 organizations have joined. Some "qualifying programs" receive no-cost DDS licenses for Windows and Linux environments.

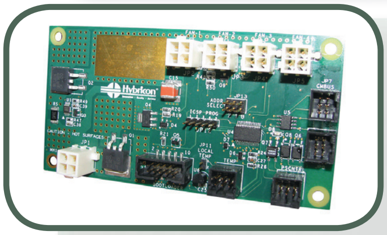
Real-Time Innovations • www.rti.com • www.mil-embedded.com/p47776

Better bus licenses

Even the newest, freshest military platform retains legacy interfaces such as MIL-STD-1553 or ARINC 429. That's because these tried-and-true communications links are rock solid and still used in familiar *older* equipment installed in *new* aircraft, ships, or ground vehicles. One of the leaders in 1553 and 429 hardware is Data Device Corporation (DDC), whose board- and chip-level hardware is arguably chosen more often than any other vendor. Yet DoD systems do not operate on hardware alone. That's why DDC offers a number of software packages for their hardware, including dataSIMS, BusTrACEr, Commercial Avionics Utilities, and a LabVIEW Support Package.

Still, software requires licenses, and DDC has just simplified theirs while making software available on more host platforms than ever before, including 32- and 64-bit versions of Windows Vista and Windows 7. License choices now comprise: a USB dongle license for host computers that move around (such as laptops or Tablet PCs). For dedicated host platforms that don't move, there's now a Node-Locked license. And finally, for network-based development sites, DDC offers a Network License version. The company has also extended the support contracts to 12- or 24-month periods. We're aware that a new license structure might not rock your world, but your program manager might thank you for bringing this to their attention.

Data Device Corporation • www.ddc-web.com • www.mil-embedded.com/p47777



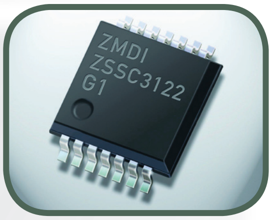
Among a chassis' biggest fans

We've got high-performance CPUs mixed up with barn-burning GPUs next to screaming 1 GbE controllers. All this energy ultimately boils up to one thing: heat. And in an air-cooled chassis (and even some conduction-cooled chassis with cold-wall convection), it's the lowly fan that feels the heat. Suppose Mr. Fan up and crapped out? Yeah: bye-bye $100,000 electronics package. So Curtiss-Wright Controls Electronic Systems thinks an intelligent fan controller is just smart money. Their Hybricon rugged intelligent fan controllers comply with PMBus-based chassis management systems and pass MIL-STD-461F, MIL-STD-810G, and MIL-STD-704F.

The variable speed control system can be configured for PWM or voltage regulator outputs with programmable speed, warning, and fault thresholds. Four fans (via tachometer input) and four temperatures can be monitored, and sophisticated BIT information is broadcast over the PMBus interface. Warning and fault indicators for both fan and temperature are broadcast and the controller itself can drive the fans, alleviating the need for a separate PSU (in 12, 24, and 28 VDC). The controller can also interoperate with other Hybricon controllers in a 16-fan configuration. Lastly, this little guy can really take the heat and operates over -40 °C to +85 °C, just like you'd expect from a Curtiss-Wright Controls product.

Curtiss-Wright Controls Electronic Systems • www.cwcelectronicsystems.com • www.mil-embedded.com/p47778

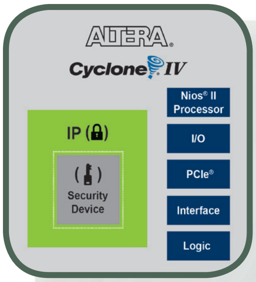
Harsh-duty touch sensor conditioner for battery apps



The human-machine interface in defense apps is critically important – especially when it comes to pushing buttons or scrolling pages. Designed for use in non-contact applications where harsh or explosive environments don't favor electric-spark buttons, virtual buttons on LCD and other screens are becoming the *de facto* way to control embedded computers. In low-power and battery-operated systems, it's the capacitive overlay that humans use to manipulate on-screen objects like buttons. But those touch screens require capacitive signal conditioners like the wide-dynamic range ZSSC3122 by ZMDI.

Primary specs boast 14-bit capacitive to digital conversion, with sensitivity, sensor offset, and temperature digitally corrected via algorithm. Designed to sip 60 microA over a voltage range of 1.8 V to 5.5 V, the conditioner interfaces to capacitive sensors from 2 to 10 pF with a sensitivity down to an astounding 120 atto-Farads (aF) per digital bit and accuracy up to 0.25 percent over -40 °C to +125 °C. Calibration for the device is digital and corrects first- and third-order nonlinearity errors, making it ideal for the high-humidity and -pressure applications found in military systems. Calibration coefficients are stored onboard in EEPROM. Designed to be interfaced to a microcontroller, the ZSSC3122 can also be used stand-alone in transducer and switch applications. Programming is accomplished via a PC with ZMDI development tools. If you've got a capacitive touch system, you need these controllers. Trust us.

Zentrum Mikroelektronik Dresden AG (ZMDI) • www.ZMDI.com • www.mil-embedded.com/p47783



Video surveillance chipset does "reality TV" in HD

So your iPhone 4 records in HD at 720p. So does the Cisco Flip camera (which, by the way, just went "obsolete" as we went to press). How hard can HD be? Suppose you want to integrate 1080p at 60 frames/s in a military camera or remote sensing surveillance application? Are you going to duct tape an iPhone to a Global Hawk? Altera and their buddies have a better idea: the HD WDR video surveillance chipset. This ASSP comprises an Altera Cyclone IV E FPGA loaded with image processing IP bolted to an image sensor, and it provides High Def Wide Dynamic Range plus logic security. Best of all is that Altera has done all the hard work for you, and the off-the-shelf combination comes complete with tools and software, too.

Starting with an AltaSens 1080p60 A3372E3-4T image sensor, 2200 x 1125 pixels by 16 bits/pixel is fed into the FPGA at 60 frames per second. Do the math and that's over 2 Gbps fire-hosed into the Cycle IV E FPGA. Now you see why an iPhone ain't gonna cut it, despite the glamour of the shabby-chic duct tape look. Inside the FPGA is Apical's HD WDR full Image Signal Processing (ISP) pipeline IP, which Altera has conveniently made available for license on their website. Other tools available for this package deal include evaluation IP prior to purchase, evaluation license, ISP core license, and Altera's Quartus II software. It goes without saying that once the video is inside the FPGA, other processing is possible such as image enhancement, edge detection, target identification, and transcoding. We are hugely impressed with the possibilities of this rugged, programmable, COTS chipset.

Altera • www.altera.com/surveillance • www.mil-embedded.com/p47780
AltaSens • www.altasens.com • www.mil-embedded.com/p47781 **Apical • www.apical-imaging.com • www.mil-embedded.com/p47782**

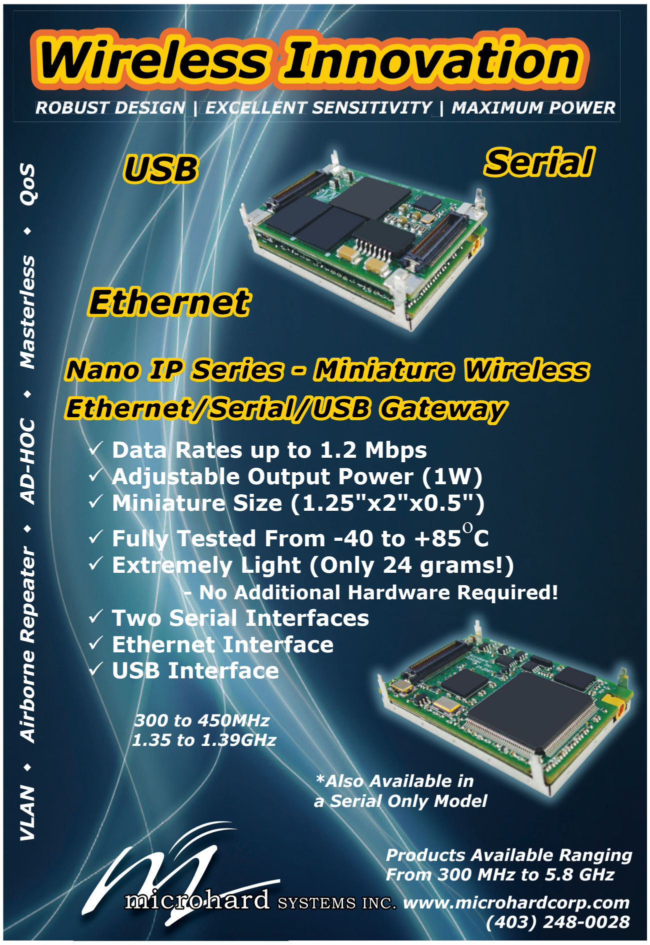
Board-level Micro and ATX Sandy Bridge servers pack big performance

When Intel's Sandy Bridge microarchitecture hit the Core processor family in January 2011, the personal computer market was rocked to its … core. The performance numbers were so sensational that all other desktop and laptop CPUs looked like last month's moldy meat. Sandy Bridge also spruced up Intel's Xeon server line – and the performance/power ratio went through the roof. TYAN, a name probably unfamiliar to our readers, added Xeon E3-1200 sockets to their entry-level servers. Those ATX and Micro ATX form factors might be ideal in many deployed, benign military applications.

Available in two flavors, the S5510 is a Micro ATX motherboard equipped with Xeon socket and an Intel C204 or lower-cost C202 chipset. Depending upon configuration, there are 3 or 4 PCI-E 2.0 x8 slots, 6 SATA ports, and either two or three 1 GbE ports. The ATX-sized S5512 comes in four different versions for rack-optimized server setups. Similar to the S5510, the '12 has up to 8 SAS ports, four 1 GbE ports, and a management port. Both server versions offer IPMI 2.0 support for out-of-band and remote management. We're sure some enterprising designer will stuff a Micro ATX server in a rugged chassis, blow some air across it for cooling, and end up with a server that's 30 percent of the price of a comparable VME or VPX setup. Go ahead: We dare ya.

TYAN (a subsidiary of MiTAC International Corporation) • www.tyan.com • www.mil-embedded.com/p47779

Editor's Choice Products are drawn from OSM's product database and press releases. Vendors may add their new products to our website at http://submit.opensystemsmedia.com and submit press releases at http://submit.opensystemsmedia.com. OSM reserves the right to publish products based on editors' discretion alone and does not guarantee publication of any product entries.



Crosshairs Editorial

Big bucks for better batteries sure to power future mil systems

By Chris A. Ciufo, Editor

Editor's note: *This is a follow-on to my* Crosshairs Editorial *column on portable power from the January/ February issue of* Military Embedded Systems *(see http://bit.ly/port_pwr).*

While Moore's Law evolved 1000x performance from the Pentium 4 to today's Core i7 in only a few years, batteries have changed little until now. New funding on batteries is finally trickle-charging research a few million dollars at a time to universities, federal labs, and COTS startups. As well, many established battery companies are spending their own capital developing better batteries for the digital smartphone and tablet markets, or for automobile applications such as GM's Volt, Nissan's Leaf, and other vehicle platforms. Money is being spent in both primary cells (disposable) and secondary rechargeable batteries. The DoD is also funding battery research directly and through DARPA.

Military batteries are primarily used in vehicle engines and portable communications equipment, though the DoD's future UASs and ground drones also require batteries for mission payload packages where, according to battery expert Contour Energy Systems, batteries power the motor, controls, radio, and imaging systems on micro UAVs. As well, too much of a soldier's mission walking weight comprises heavy military BA-5X90/U Li/SO_2 or Li/MnO_2 batteries to power SINGARS or satellite comms gear. High current drain and extended missions force soldiers, SEALS, and Marines to carry spare batteries instead of extra food, water, and ammo. That costs lives.

For vehicles, the U.S. Advanced Battery Consortium (USABC) has handed out funding the past several years such as the $1.41 million to Quallion LLC for their patented Matrix "series plus parallel cell" battery. USABC, funded by GM, Chrysler, Ford and the DOE, is keen on the Quallion's cell that's redundant and dissipates recharging heat very well. For defense, Matrix's redundancy means battle resilience and the ability to operate in extreme heat. USABC also handed out $15.6 million in March to another five companies with promising battery concepts, including Maxwell Technologies for their double energy density 30 W-h/kg advanced ultracapacitor, which isn't a battery at all but a big capacitor.

The DoD has also requested money for batteries, from zip in FY10 to $800,000 in FY11 for the "Fuel Cell Hybrid Battery Manufacturing for Defense Operations." Traditional lead-acid car batteries work fine in your Jeep Liberty until you do some serious off-road wheelin' and the acid leaks or the lead plates break. Worse, at 0 °C, the battery has lost 20 percent of its capacity; at -40 °C, it's lost 70 percent (source: Concorde; www.marine-electronics.net). A combined fuel cell/primary battery might offer the best of both worlds in high shock/vibration military vehicles. Congressman John Yarmuth of Kentucky agrees, and has requested for his state $5 million in DoD funding for advanced battery R&D for "novel battery and ultracapacitor materials discoveries" for military transportation. Improved energy density vehicle batteries would not only start the engine, they would help drive power-hungry electronics gear and supplement or replace onboard generators.

International Battery of Pennsylvania just won the first $730,441 of an estimated $6.7 million from the U.S. Army's TARDEC to develop a hybrid energy storage solution for tanks and Stryker vehicles. The Silent Watch program wants lightweight, rugged, no-heat batteries using lithium iron phosphate cells for energy and ultracapacitors for 50-100 Amps in a car-battery footprint.

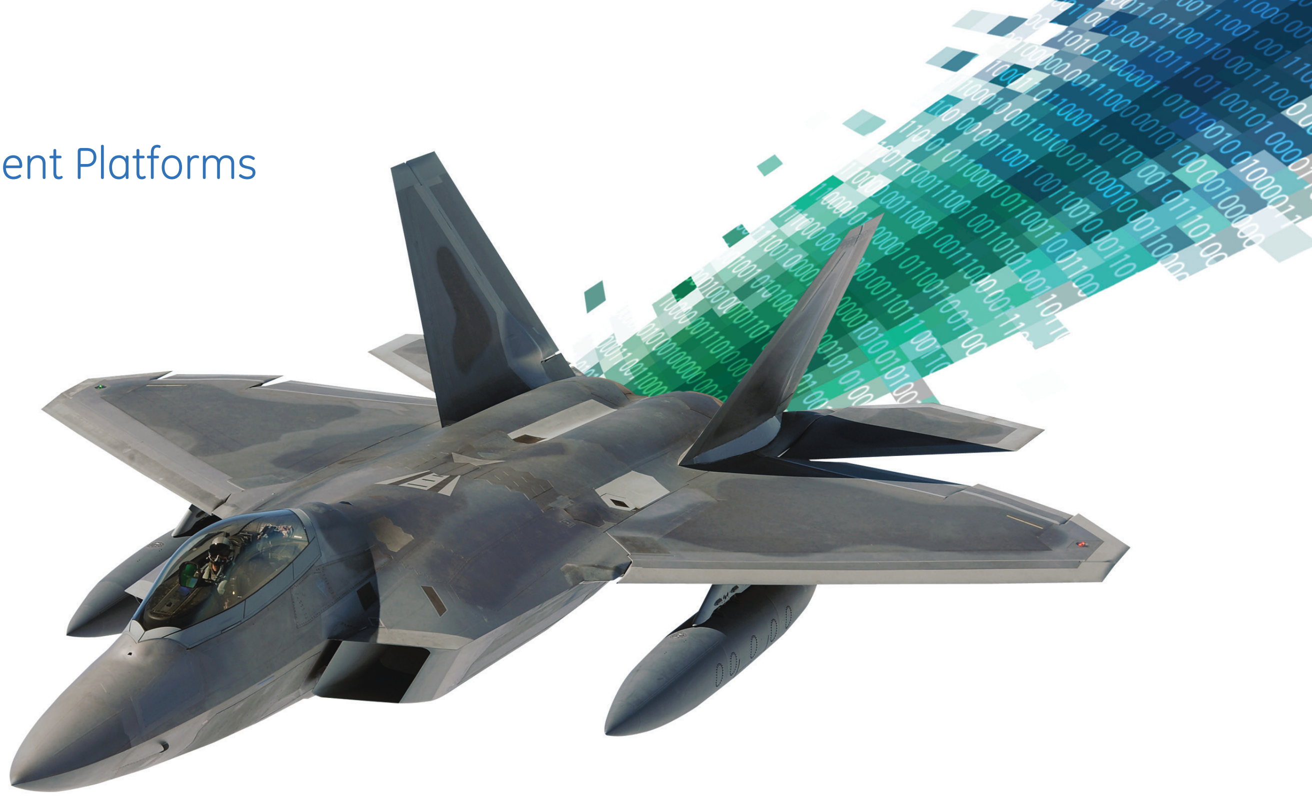
Meanwhile, the DoD started funding Battery Network (BATTNET) at $1.0 million per year in FY10 with Short Term Proposals at $100K per year for "sustained availability, quality, and affordability of batteries." The focus here is for digital electronics. The worry: exotic materials like Lithium that might come from unfriendly offshore sources. Elsewhere on the digital side, Contour Energy has invested in Fluorinated Carbon nanotube cathode materials to dramatically increase energy density, temperature range, charge cycles, and voltage. The Carbon nanotube design provides substantially more cathode surface area, a key measure of chemical energy production.

By introducing Fluorine atoms to the Carbon reaction in a typical military BA-5x90/U soldier's battery, double the volumetric energy or half the weight is possible. This means longer runtimes for digital gear within the same battery envelope. For now, Contour Energy is selling COTS button batteries of the CF/CRxxx type and gearing up for Li/CFx thin film, cell, and prismatic batteries.

Finally, there's one last type of novel battery attracting investment. Betavoltaic batteries work much like a photovoltaic solar cell: using high-energy particles to excite a current flow. Start-up City Labs has taken garden-variety Tritium – the mildly radioactive Hydrogen isotope used in luminescent watches – to blast electrons at a PN junction[1]. Electron-hole pairs are created, causing a nanocurrent to flow. They've achieved 25 to 50 nW/cm^2, which can be scaled three-dimensionally to about 50 microW/cm^3. Not enough to power a radio, but enough to power an FPGA backup SRAM or keep a crypto key alive for 20 years.

I've mentioned at least 10 different battery companies and nearly as many novel battery technologies that emerged in only the past couple of years. As funding flows from federal, state, and private sources, existing public companies are also boosting their battery R&D efforts. Whether for cars or fire control systems, lightweight, high-energy batteries will power the warfighter's future.

[1] Refer to my interview with City Labs at http://bit.ly/betavoltaic.



WinSystems®

Embedded PCs and Stackable I/O for Rugged, Harsh Applications

Embedded Solutions Catalog

Mil/COTS · STD Bus · Transportation · SBCs · Medical · EBX · Communications · EPIC · Industrial Controls · PC/104

About WinSystems

WinSystems builds strong business relationships with our customers by providing high-quality, cost-effective products along with extraordinary customer service.

Bob and Jerry
ESOP members

WinSystems is a leading provider of embedded products for use in industrial environments. Founded in 1981 by Jerry Winfield, we have grown to become an employee-owned company. Our facilities are located in a 55,000 square foot office campus which houses our design, manufacturing and support teams as well as our corporate headquarters. We are located in Arlington, Texas midway between Dallas and Fort Worth.

We are a business where the employees have stock ownership, longevity, and a stake in the success of the business and our customers. When you talk to a WinSystems' employee, you are talking to an owner.

An ESOP benefits our customers by having a very talented and motivated workforce that is responsible for developing and supporting our products.

When you buy from WinSystems, you are buying more than just a product. You are receiving our company's engineering and manufacturing expertise along with the support of our dedicated professionals. WinSystems sets itself apart from traditional corporations with our increased commitment and dedication to excellence found in every owner in the company. This provides a culture for a creative and responsive team where customers can have confidence that we are here today and here tomorrow.

Mew and Sye, members of
WinSystems ESOP team

Profit from our 29 years of proven experience with our wide selection of Single Board Computers (SBCs), I/O modules, memory devices, and hardware accessories. Our products feature extended temperature operation, low power requirements, and a two-year warranty. Combined with knowledgeable, award-winning technical support and long-term product availability, it makes WinSystems' products the right choice for reliable, x86-based embedded PCs.

WinSystems supports and promotes open hardware and software standards. We offer both stand-alone and bus-expandable SBCs with SUMIT, PC/104, PC/104-*Plus*, and Pico-I/O expansion; plus we continue to manufacture legacy STD bus products.

As you look through this catalog, you will find an overview of our diverse product lines. For the most current technical information, please be sure to visit our Website: http://www.winsystems.com.

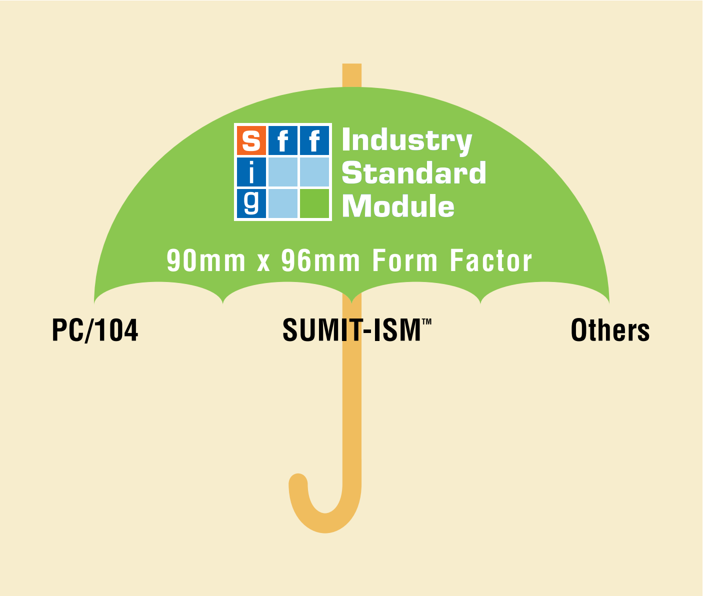
We, the employee-owners of WinSystems, look forward to working with you on your next project.

Service Responsiveness Knowledge Quality Trust

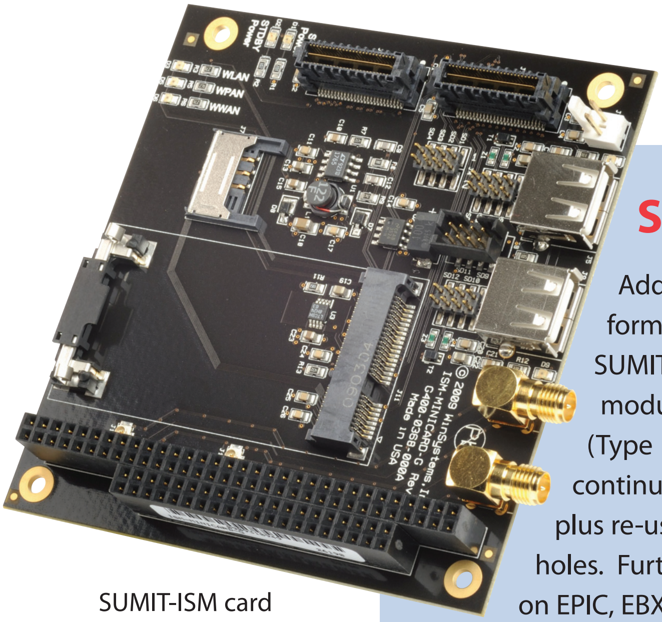
Table of Contents

Small Form Factor Boards

An Industry Standard Module (ISM) is defined as a 90mm x 96mm form factor board outline without bus expansion. It specifies the board size, four fixed mounting holes, and flexible "expansion zones" for additional circuitry or I/O and/or bus connectors. ISM is an umbrella concept to provide coherence to the many different boards that are available in this 90mm x 96mm footprint.



ISM modules are small, easy-to-use, and scalable as they provide a powerful set of building blocks for a variety of different applications. Depending upon the interconnect technology, they can be stacked "piggyback" on top of each other to expand or customize a system solution. This reduces cost and bulk while increasing mounting and packaging options. The best known stackable ISM implementation is PC/104; however, recently SUMIT and other connector configurations have been defined and are being produced as well.



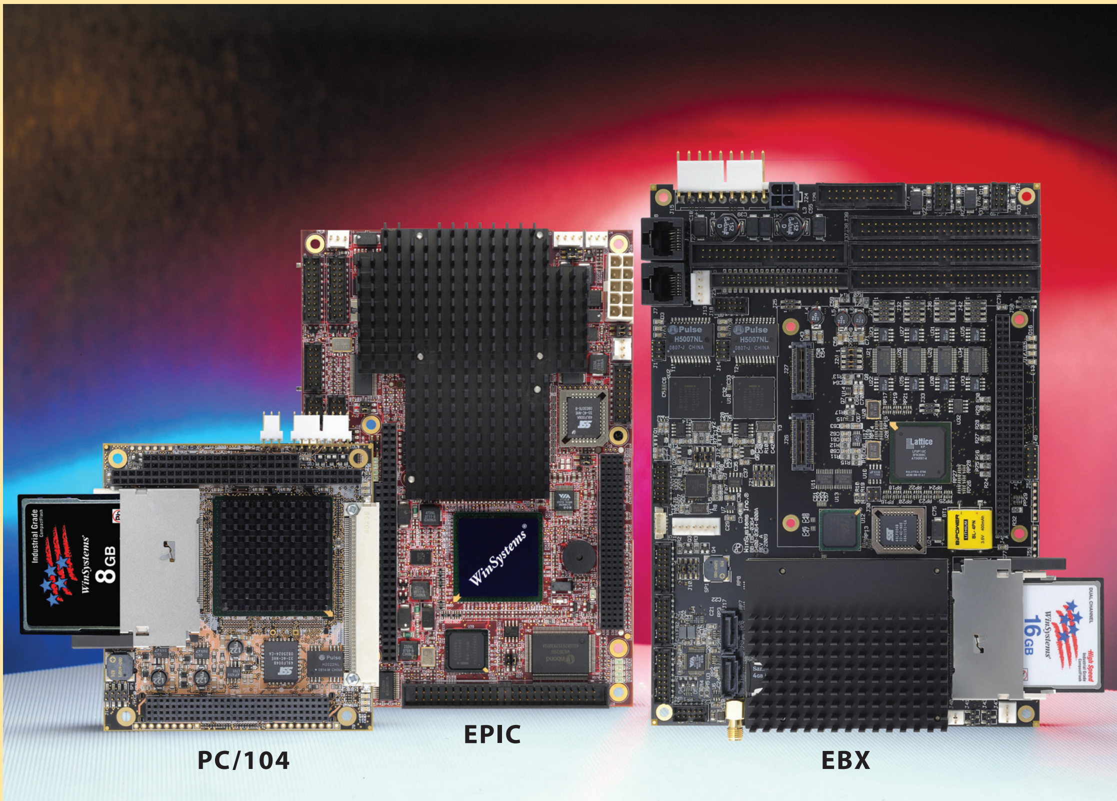
SUMIT-ISM card
with legacy
PC/104 connector

SUMIT + ISM = SUMIT-ISM

Adding SUMIT expansion (see page 12) on the ISM form factor creates SUMIT-ISM. It specifies where the SUMIT AB connectors are located on a 90mm x 96mm module. It also supports a legacy option for PC/104 (Type 1) or PCI-104 (Type 2) modules by allowing the continued use of their connectors in the existing locations plus re-using established physical dimensions and mounting holes. Furthermore, SUMIT-ISM expansion can be supported on EPIC, EBX, and other standard and custom form factors. SBCs using SUMIT-ISM modules allow a designer to build small, reliable, easy-to-use, cost-effective, and stackable systems since they provide a powerful building block for a variety of different applications.

Our Embedded PCs come in three sizes from an industry standard 3.6" x 3.8" module to a 8.0" x 5.75" EBX with SUMIT™ and PC/104 expansion.

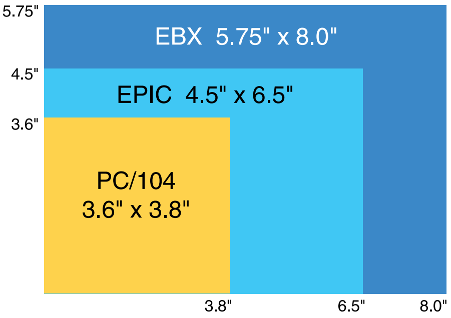
- x86 Compatible
- Compact & Modular
- Rugged & Reliable
- Easy to use
- Extended temperature
- Wide Selection of I/O
- SUMIT, Pico-I/O, and PC/104 Expandable
- 30-day Product Evaluation Program



Small size, low power, wide operating temperature, and PC-compatibility are the fundamental computer elements required for embedded designs. Our feature-rich SBCs meet these requirements and are ideal for space- and power-limited applications in harsh environments.

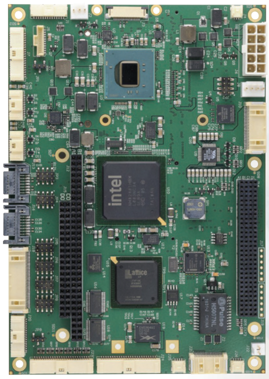
Designed to run x86 instruction set software, these SBCs are compatible with Linux and Microsoft's® Windows operating systems as well as the applications that run on them. They also support ROM-DOS and other PC-compatible x86 operating systems. PC software compatibility assures faster program development, debugging, and checkout of your application's software.

A comprehensive SBC selection guide is located on pages 8 and 9.



Size Comparison
PC/104 vs. EPIC vs. EBX

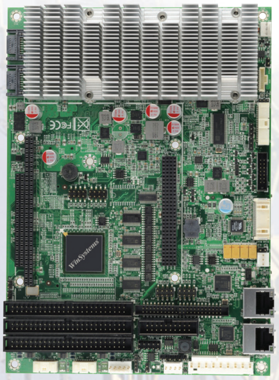
Single Board Computers



Intel® Atom™ EPIC SBC

- 1.66GHz N450 single core Atom
- 1.66GHz D510 dual core Atom
- 2 Gigabit Ethernet controllers
- CRT and LVDS flat panel support
- 8 USB 2.0 and 4 COM ports
- 2x SATA channels and CF socket
- 48 lines of DIO, LPT, HD Audio
- PC/104-*Plus* and miniPCIe connector
- Opt. battery-backed SRAM
- 4.5″ x 6.5″ EPIC-compliant

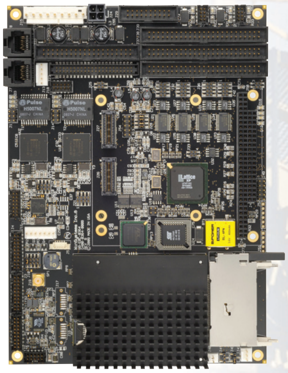
Model:
EPX-C380-D2-1
EPX-C380-S1-0
EPX-C380-S2-0



Intel® Atom™ EBX SBC

- 1.66GHz N455 single core Atom
- 1.80GHz D525 dual core Atom
- 2 Gigabit Ethernet controllers
- CRT and LVDS flat panel support
- 8 USB 2.0 and 4 COM ports
- 2x SATA and 1x PATA channel
- 48 lines of DIO and HD audio (7.1)
- LPT, PS/2 mouse & KYBD controller
- PC/104-*Plus* and miniPCI connector
- 5.75″ x 8.0″ EBX-compliant

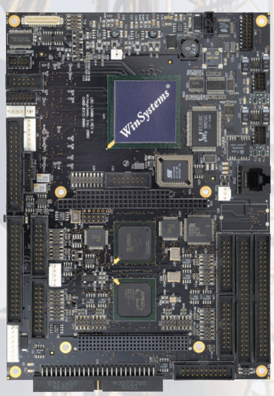
Model:
EBC-C384-D2-0
EBC-C384-S2-0



Fanless Intel® Atom™ SBC

- Intel® 1.1GHz or 1.6GHz Atom™
- CRT and LVDS flat panel support
- 2 Gigabit Ethernet controllers
- Wireless support with MiniPCIe
- 4 COM, 4 USB, and 48 DIO
- LPT port, KYBD, and mouse support
- SUMIT-ISM, PC/104, and Pico-I/O expansion modules supported
- CompactFlash socket
- 5.75″ x 8.00″ EBX-size board

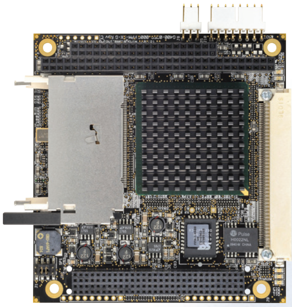
Model:
EBC-Z510-G, 1.1GHz
EBC-Z530-G, 1.6GHz



All-in-One Fanless SBC

- AMD LX800 CPU
- CRT and LVDS flat panel support
- 10/100 Mbps Ethernet controller
- 12 COM and 4 USB ports
- 48 bi-directional digital I/O lines
- IDE, FDC, keyboard, and mouse interfaces
- CompactFlash socket
- PC/104 expansion connectors
- OEM configurations available
- 5.75″ x 8.00″ EBX-size board
- -40° to +85°C operation

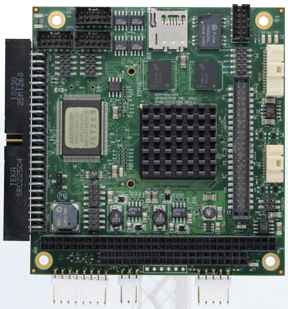
Model: LBC-LX800-G



Ethernet and Video PC/104-*Plus* SBC

- AMD LX800 SBC
- x86 software compatible
- Video with CRT resolutions 1920 x 1440 and panel resolutions 1600 x 1200
- Custom splash screen on start-up
- Up to 1GB of SDRAM
- 10/100 Mbps Ethernet controller
- 4 COM channels with FIFOs
- 2 USB 2.0 with overcurrent protection
- 16 digital I/O lines with event sense
- LPT, mouse, CF, audio and PATA interfaces
- WDT, RTC, status LEDs, and beeper
- PC/104-*Plus* compliant
- -40° to +85°C operation

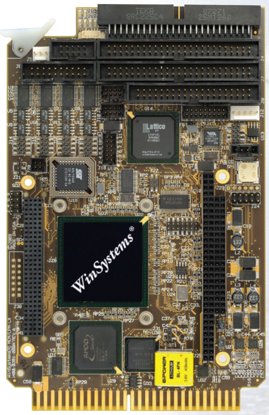
Model: PPM-LX800-G



PC/104 SBC with Dual Ethernet

- 500MHz or 1GHz Vortex86DX SBC
- 256MB or 512MB of soldered down SDRAM
- Optional 512MB SSD flash disk
- 1MB battery-backed SRAM
- CompactFlash socket
- 1 or 2 10/100 Mbps Ethernet ports
- 4 USB and 4 COM ports
- ESD protection on data lines
- 16 digital I/O lines with event sense
- PATA, LPT, PS/2 KYBD and mouse
- MiniPCI and PC/104 expansion
- WDT, RTC, status LEDs, and beeper
- -40° to +85°C operation

Module: PCM-VDX-1-256
PCM-VDX-2-512



SBC with Video, Ethernet, and I/O

- AMD LX800 0.9W CPU
- Up to 1 Gigabyte of SDRAM
- LCD and CRT supported
- Custom splash screen on start-up
- 10/100Mbps Ethernet controller
- 4 USB and 4 COM ports
- 48 digital I/O lines plus LPT
- Audio, CF, PATA, PS/2 KYBD and mouse interfaces
- PC/104-*Plus* expansion connectors
- STD Bus expansion
- -40° to +85° C operation

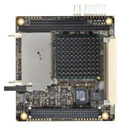
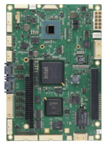
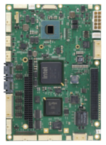
Model: LPM-LX800-G

WHEN TO USE AN SBC

- Need faster Time-to-Market
- Proven design by vendor increases reliability and reduces project risk
- Multiple vendors provide a variety of different sizes, functions, and price options
- Component-level design is too complex for in-house engineers
- Internal company resource limitations
- Lack of internal manufacturing expertise

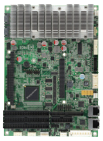
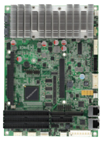
WinSystems' SBC Selection Guide

WinSystems' SBCs are designed for embedded applications and will operate without a rotational disk, keyboard, or a monitor over extended temperature ranges without the need of a fan. They are available in various physical sizes and CPUs to match your application's requirements.

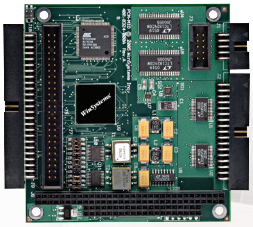
					
Part Number	PPM-LX800-G	PCM-VDX-2-512	PCM-VDX-1-256	EPX-C380-S2	EPX-C380-D2
Form Factor	PC/104-*Plus*	PC/104	PC/104	EPIC	EPIC
CPU Type	AMD LX800	Vortex 86DX	Vortex 86DX	Intel Atom N450	Intel Atom D510
Single/Dual Core	Single	Single	Single	Single	Dual
CPU Speed	500MHz	1GHz	500MHz	1.66GHz	1.66GHz
Chipset	CS5536	Integrated	Integrated	ICH8M	ICH8M
System Memory	Up to 1GB in a socket	512MB soldered down	256MB soldered down	Up to 2GB in a socket	Up to 2GB in a socket
Power Management	–	–	–	✓	✓
CompactFlash Socket	✓	✓	✓	✓	✓
VGA	✓	–	–	✓	✓
Flat Panel Support	Digital	–	–	LVDS	LVDS
Custom Splash Screen	✓	–	–	✓	✓
Simultaneous Video	✓	–	–	✓	✓
10/100/1000 Ethernet	–	–	–	2	2
10/100 Ethernet	1	2	1	–	–
USB 2.0 Ports	2	4	4	8	8
RS-232/422/485	2	4	2	4	4
RS-232 Only	2	–	2	–	–
Digital I/O	16	16	16	48	48
PATA Interface	1	1	1	CF only	CF only
SATA Interface	–	–	–	2	2
SUMIT Connector	–	–	–	–	–
PC/104 Connector	✓	✓	✓	✓	✓
PC/104-*Plus* Connector	✓	–	–	✓	✓
Mini PCIe Socket	–	–	–	✓	✓
Mini PCI Socket	–	✓	✓	–	–
Keyboard and Mouse I/F	PS/2 - USB	PS/2 - USB	PS/2 - USB	USB	USB
LPT	✓	✓	✓	✓	✓
Audio	AC97	–	–	HD (7.1)	HD (7.1)
Fanless	✓	✓	✓	✓	–
Ex. Temp. Operation	✓	✓	✓	✓	✓
Voltage Required	+5	+5	+5	+5	+5
RoHS Compliant	✓	✓	✓	✓	✓

Quick Start Kits Available

WinSystems' x86-compatible single board computers run Linux, Windows® embedded, ROM-DOS, and other compatible RTOSes along with their development tools. Each of our SBCs and I/O boards comes with software drivers. A Quick Start Kit is available to speed your development.

					
EBC-C384-S2	EBC-C384-D2	EBC-Z510-G	EBC-Z530-G	LBC-LX800-G	Part Number
EBX	EBX	EBX	EBX	LBC	Form Factor
Intel Atom N455	Intel Atom D525	Intel Atom Z510	Intel Atom Z530	AMD LX800	CPU Type
Single	Dual	Single	Single	Single	Single/Dual Core
1.66GHz	1.8GHz	1.1GHz	1.6GHz	500MHz	CPU Speed
ICH8M	ICH8M	US15W SCH	US15W SCH	CS5536	Chipset
Up to 4GB in 2 sockets	Up to 4GB in 2 sockets	512MB soldered	512MB soldered	Up to 1GB in a socket	System Memory
✓	✓	✓	✓	–	Power Management
✓	✓	✓	✓	✓	CompactFlash Socket
✓	✓	✓	✓	✓	VGA
LVDS	LVDS	LVDS	LVDS	Digital	Flat Panel Support
✓	✓	✓	✓	✓	Custom Splash Screen
✓	✓	✓	✓	✓	Simultaneous Video
2	2	2	2	–	10/100/1000 Ethernet
–	–	–	–	1	10/100 Ethernet
8	8	4	4	4	USB 2.0 Ports
4	4	4	4	12	RS-232/422/485
–	–	–	–	–	RS-232 Only
48	48	48	48	48	Digital I/O
CF only	CF only	1	1	1	PATA Interface
2	2	–	–	–	SATA Interface
–	–	AB	AB	–	SUMIT Connector
✓	✓	✓	✓	✓	PC/104 Connector
✓	✓	–	–	✓	PC/104-*Plus* Connector
–	–	✓	✓	–	Mini PCIe Socket
✓	✓	–	–	–	Mini PCI Socket
PS/2 - USB	PS/2 - USB	PS/2 - USB	PS/2 - USB	PS/2 - USB	Keyboard and Mouse I/F
✓	✓	✓	✓	✓	LPT
HD (7.1)	HD (7.1)	HD (7.1)	HD (7.1)	AC97	Audio
✓	–	✓	✓	✓	Fanless
✓	✓	✓	✓	✓	Ex. Temp. Operation
+5	+5	+5	+5	+5	Voltage Required
✓	✓	✓	✓	✓	RoHS Compliant

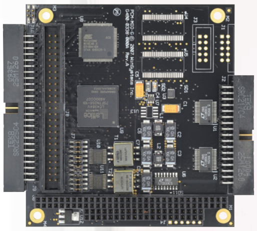
PC/104 I/O Modules



Multifunction Analog and Digital I/O

- Two, 16-bit A/D converters with 0-5V, 0-10V, ±5V, and ±10V
- Up to 16 SE and 8 DI channels
- Speed: 100K samples/sec
- Eight, 12-bit D/A converters
- 48 lines of digital I/O
- -40° to +85°C operation

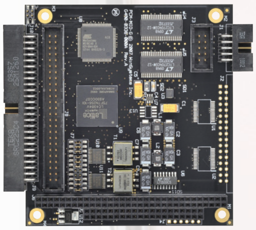
Model: PCM-MIO



Analog Input and Digital I/O Module

- Two, 16-bit A/D converters with 0-5V, 0-10V, ±5V, and ±10V
- Up to 16 SE and 8 DI channels
- Conversion speed: 100K samples/sec
- 48 lines of digital I/O
- -40° to +85°C operation
- No calibration required

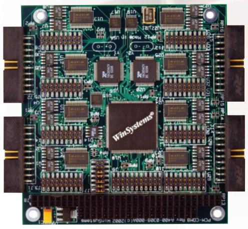
Model: PCM-MIO-AD



Analog Output and Digital I/O Module

- Eight, 12-bit D/A converters with 0-5V, 0-10V, ±5V, and ±10V
- No calibration required
- 48 lines of digital I/O
- 12 mA sink current per line
- Windows®, Linux, and C drivers
- -40° to +85°C operation

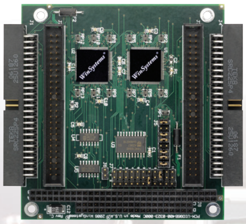
Model: PCM-MIO-DA



Octal Serial I/O

- Eight independent COM channels
- Two 16C554-compatible quad UARTs support RS-232/485/422 levels
- 128byte Rx and Tx FIFOs
- Data rates to 115,200bps
- All outputs short circuit protected
- +5V only operation
- -40° to +85°C operation

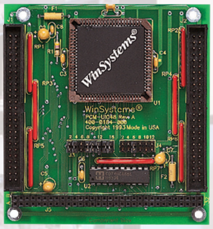
Model: PCM-COM8



96-Line I/O with Event Sense

- 96 lines as input, output, or output with readback
- 48 of the lines can generate interrupt requests that are edge selectable, latched and software enabled
- 12 mA sink current per line
- -40° to +85°C operation

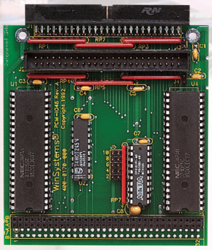
Model: PCM-UIO96A



48-Line I/O with Event Sense

- 48 lines as input, output, or output with readback
- 24 of the lines can generate interrupt requests that are edge selectable, latched and software enabled
- 12 mA sink current per line
- -40° to +85°C operation

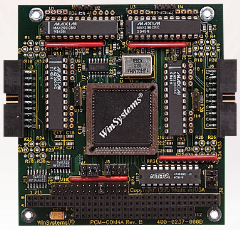
Model: PCM-UIO48A



Digital I/O

- 48 digital I/O lines
- Two 82C55A PPIs
- Dual 50-pin connectors
- Interfaces to two, Opto-22 (or equiv) module racks
- +5V only operation
- -40° to +85°C operation

Model: PCM-IO48

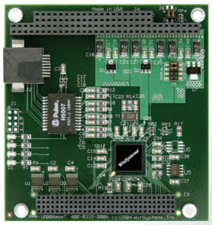


Quad Serial Module

- Four RS-232 COM ports
- Optional RS-422/485 on each channel
- 16C554 UART with 16-byte Tx and Rx FIFOs
- Data rates to 115,200bps
- +5V only operation
- -40° to +85°C operation

Model: PCM-COM4

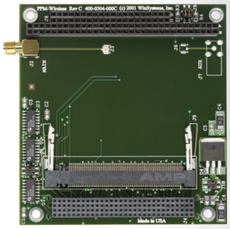
PC/104 I/O Modules



Gigabit Ethernet Controller

- Gigabit PCI Ethernet controller
- Auto-switching from 1Gbps down to 100 Mbps and 10 Mbps
- Full- and half-duplex operation
- IEEE 802.3ab Auto-Negotiation support
- RJ-45 connector on the board
- PC/104-*Plus* module
- -40° to +85°C operation

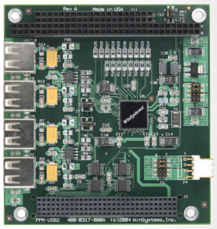
Model: PPM-GIGABIT



Wireless 802.11 Adapter

- IEEE 802.11 wireless adaptercard
- Supports 802.11 miniPCI modules
- Available with or without a card installed
- External antenna connector
- PC/104-*Plus* module
- -40° to +85°C operation

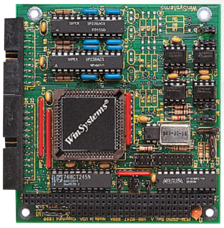
Model: PPM-WIRELESS



Four-channel USB 2.0 Module

- OHCI host and EHCI Host Compliant
- Root hub and four downstream facing ports onboard
- All downstream ports handle low-speed, full-speed, and high-speed transactions
- Each port with overcurrent and in-rush protection
- PC/104-*Plus* module
- -40° to +85°C operation

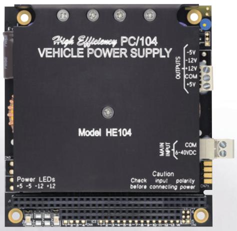
Model: PPM-USB2



Dual COM & LPT

- One LPT printer port
- Two RS-232 COM ports with RS-422/485 on each channel
- 16C552 UART with 16-byte Tx and Rx FIFOs
- Data rates to 115, 200bps
- +5V only operation
- -40° to +85°C operation

Model: PCM-DSPIO



High Efficiency Power Supply

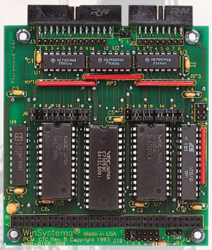
- 50W DC/DC power supply
- Input ranges: 6V to 40V
- Output: +5V @ 10A, +12V @ 2A
- Low output ripple
- Voltage status LEDs
- Quick disconnect connector
- -40° to +85°C operation
- Other models available

Model: PCM-HE104

CompactFlash Disk Adapter Module

- CF Type I or II interface to IDE
- Compatible with Windows and Linux
- On-card automatic power management
- Supports multiple drive operation
- Remote mounting configuration available
- -40° to +85°C operation

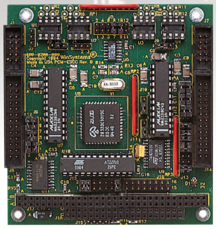
Model: PCM-CFlash2



Counter/Timer Module

- Six, 16-bit counter/timers
- Six programmable counter modes per channel
- Buffered Clock, Gate, and Out signals
- 82C59A interrupt controller
- -40° to +85°C operation

Model: PCM-CTC



Dual Synchronous Serial Controller

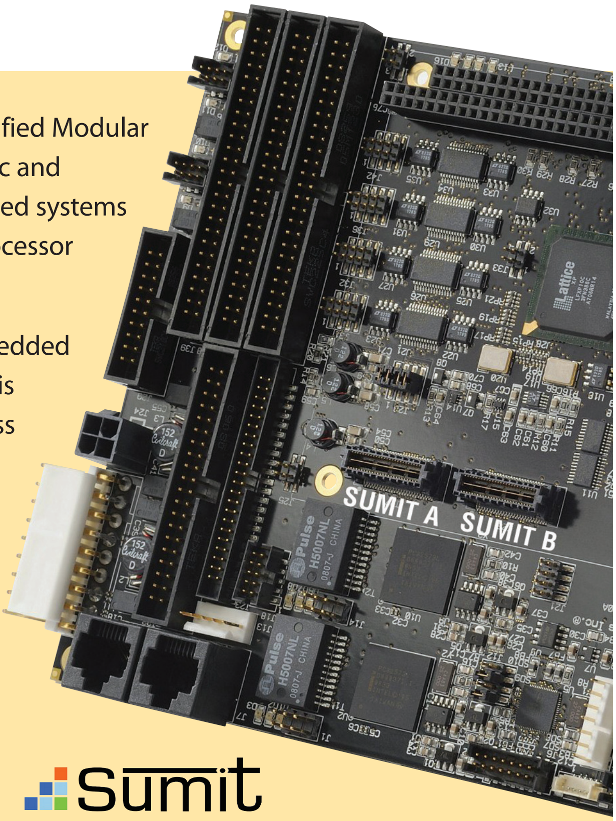
- Uses 85230 ESCC
- Two full-duplex, independent
- RS-232 channels with FIFO
- Supports Async, X.25, HDLC, SDLC, and BISYNC
- DMA supported
- -40° to +85°C operation
- +5V only operation

Model: PCM-ESCC

SUMIT I/O Modules

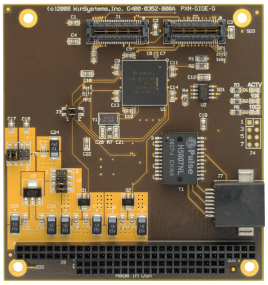
WinSystems' engineers co-designed SUMIT, a Stackable Unified Modular Interconnect Technology. SUMIT's architecture is I/O-centric and addresses the vast majority of peripherals used by embedded systems using a stacking architecture. It is both form factor and processor independent.

Pronounced "sum it," it is an interconnect standard for embedded systems that uses two, 52-pin, high-density connectors. This interconnect standard integrates the high-speed PCI Express and USB 2.0 serial bus technologies used by the latest generation chipsets, while also providing a bridge to legacy I/O technologies as well.



SUMIT A	SUMIT B
One PCI Express x1	One PCI Express x1 & x4 or Five PCI Express x1
Four USB	
LPC (Low Pin Count Bus)	
SPI/uWire	Power
SMBus/I²C Bus	Ground
ExpressCard	Control Signals

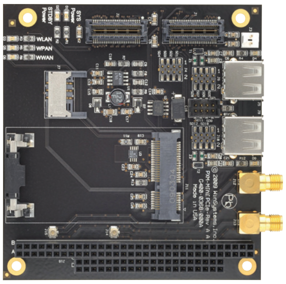
sumit



Gigabit Ethernet LAN SUMIT-ISM Module

- Uses 82573 Ethernet controller
- SUMIT x1 PCIe lane
- Gigabit Ethernet controller with automatic switching down to 100Mbps and 10Mbps
- 90 x 96mm Industry Standard Module
- SUMIT-AB and PC/104 connectors
- RJ-45 connector on board
- Standard Windows® and Linux drivers

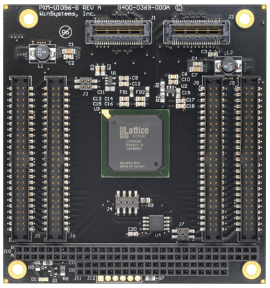
Model: PXM-GIGE



MiniPCIe and USB SUMIT-ISM Module

- SUMIT PCIe x1 interface
- MiniPCIe connector supports wireless, memory, and video modules
- Two USB pass through connectors with overcurrent protection
- PCIe x1 interface to SUMIT
- SUMIT-ISM: 90 x 96mm
- -40° to +85°C operation

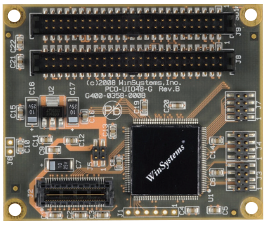
Model: PXM-MiniPCIe



96-Line Digital I/O SUMIT-ISM Module

- 96 lines programmable for input, output, or output with readback
- Event sense on change of status
- Direct interface to WinSystems' isolated termination boards
- PCIe x1 interface to SUMIT
- SUMIT-ISM: 90 x 96mm
- -40° to +85°C operation

Model: PXM-UIO96



48-Line Digital Pico-I/O Module

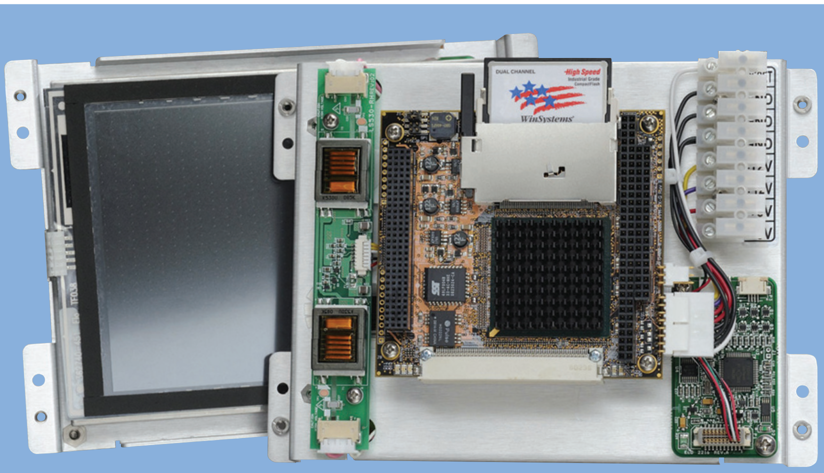
- 48 lines programmable for input, output, or output wih readback
- 24 Event sense lines
- TTL compatible I/O
- SUMIT LPC interface requires no BIOS modifications
- -40° to +85°C operation
- Pico-I/O compatible: 60 x 72mm

Model: PCO-UIO48

6.5-inch PC/104 Flat Panel Computer

This light-weight, integrated system combines a 6.5-inch flat panel display, PC/104-*Plus* SBC, and touchscreen into an industrial-grade, open-frame enclosure that is less than two inches thick.

Ready-to-mount in harsh environments; the PPC3-6.5's PC compatibility supports Linux and Windows® XP embedded operating systems, along with real-time x86 kernels. It operates over an extended temperature from -20° to +70°C.



Model: PPC3-6.5

- Includes a PC-compatible single board computer (SBC) mounted with PC/104 I/O module expansion capability
- Active Matrix color LCD with touchscreen
- Thin profile, small size
- Industrial-grade resistive touchscreen
- Easy to mount, open-frame design
- Gasket material supplied for better fit into application enclosure
- Extended temperature operation

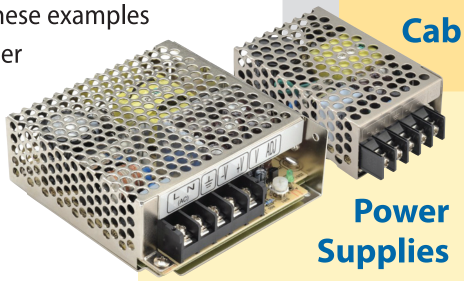
Accessories Complete Your Project

WinSystems offers accessories and quick start kits to help speed product development using our SBCs and I/O modules. This includes interface industrial cables, AC power supplies, applicable software drivers, batteries, SODIMMs and CompactFlash memory.

WinSystems' knowledgeable factory engineers will support you during your initial system configuration through production. Plus we can help configure customized designs for OEM projects. These examples include BIOS changes, special splash screens, jumper configurations, cabling, and flat panel support.

Contact us with your requirements;
call 817-274-7553 or e-mail info@winsystems.com

Cables and Batteries



Power Supplies

30-day product evaluations available.

Industrial CompactFlash Cards

-40°C to +85°C Operation

- 128MB to 16GB storage capacity
- Withstands 2000Gs shock / 16.3Gs vibration
- Up to 66MB/s (burst) with 37MB/s Read and 16MB/s Write (sustained) for high-speed cards
- Sophisticated error checking and wear leveling
- Spares and bad block management
- PC Card ATA and True IDE Mode compatible
- Low power consumption
- Dual 3.3V / 5V interface support
- Power loss protection
- Windows® XP Embedded and Linux operating system compatible
- -40°C to +85°C temperature operation
- 10-Year data retention
- Knowledgeable and responsive technical support
- In-stock availability and RoHS 6/6 compliant
- Custom programming services available
- Visit **www.IndustrialCompactFlash.com**

WinSystems' CompactFlash cards are designed for applications that require industrial-grade reliability, industry-standard compatibility, and IDE hard disk drive emulation for fast program and data storage. These rugged CompactFlash cards have higher reliability, longer endurance, lower-power consumption, and more powerful performance over their commercial-grade counterparts.

Fully operational from -40° to +85°C, these CompactFlash cards fit any computer, SBC, or instrument with a CompactFlash socket. WinSystems offers both standard and high-speed industrial CompactFlash cards. These cards are manufactured for use in harsh, rugged applications that are mission critical.

They are compatible with different operating systems such as Linux, Windows,® and other RTOSes without requiring special drivers. WinSystems offers in-stock CompactFlash product availability, plus free technical telephone support with a factory applications engineer.

	High Speed	Standard
Densities	1GB to 16GB	128MB to 8GB
Sustained READ	37MB/sec	8MB/sec
Sustained WRITE	16MB/sec	6MB/sec
Data Transfer Mode	True IDE	True IDE and ATA-2
	PIO Modes 0-6	PIO Modes 0-4
	MDMA Modes 0-4	DMA Modes 0-2
	UDMA Modes 0-4	
Endurance	2,000,000 program / erase cycles	2,000,000 program / erase cycles
Number of Read Cycles	Unlimited	Unlimited
Data retention	10 years	10 years
Shock	2000Gs (max)	2000Gs (max)
Vibration	16.3Gs rms (max)	16.3Gs rms (max)
Altitude	80,000 feet (max)	80,000 feet (max)
Dimensions	36.4 x 42.8 x 3.3 mm	36.4 x 42.8 x 3.3 mm
Temperature Range	-40° to +85°C	-40° to +85°C
Part Number	**CF-DC-G-xxG-I**	**CFLASH-G-xxxx-I**

WinSystems' Advantage

PC/104

SBCs

EBX

EPIC

DUAL CHANNEL
High Speed Industrial Grade CompactFlash
WinSystems
16GB
-40°C to +85°C
Industrial Grade CompactFlash
WinSystems
8GB
-40°C to +85°C

STD Bus

Panel PCs

Compact Flash

SUMIT

We are a stable leader in the industrial embedded PC market with many long-term and repeat customers. Our products are used in many transportation, medical, security, communications, industrial, defense, and power/energy applications. WinSystems' approach has been to handle the issues of designing and manufacturing the embedded PC hardware while allowing the customer to focus on developing their actual application hardware and software.

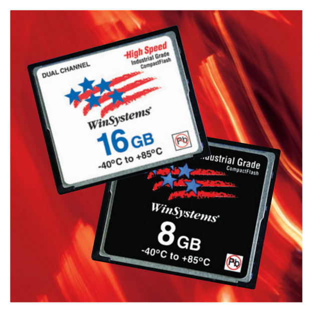
We understand that when a company selects a computer hardware vendor, they are selecting both an engineering and business partner rather than just a supplier. The continuing success or failure of their program or product is directly related to the success or failure of the business relationship. To that end, we focus not only on a board's technical specifications that are listed in a data sheet, but also on the manufacturing and non-technical factors of award-winning customer service and support. We look beyond just the "specman-ship" issues of a product to also focus on long-term availability, high reliability and customer satisfaction.

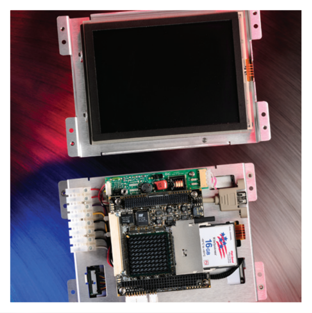
By choosing WinSystems, you are receiving our company's engineering and manufacturing expertise to deliver fully tested, high quality embedded PCs. Our engineers will assist you in analyzing, configuring and selecting the correct hardware that will work with your software development environment.

We look forward to the opportunity to demonstrate how our proven success in the industrial market can work for you.

WinSystems®
An Employee-Owned Company

Mil/COTS · STD Bus · Transportation · SBCs · Medical · EBX · Communications · EPIC · Industrial Controls · PC/104





WinSystems®
An Employee-Owned Company

715 Stadium Drive • Arlington, Texas 76011
Phone 817-274-7553 • FAX 817-548-1358
Web Site: www.winsystems.com
E-mail: info@winsystems.com