MIL-EMBEDDED.COM

COTS and technology for the entire military life cycle

Military EMBEDDED SYSTEMS

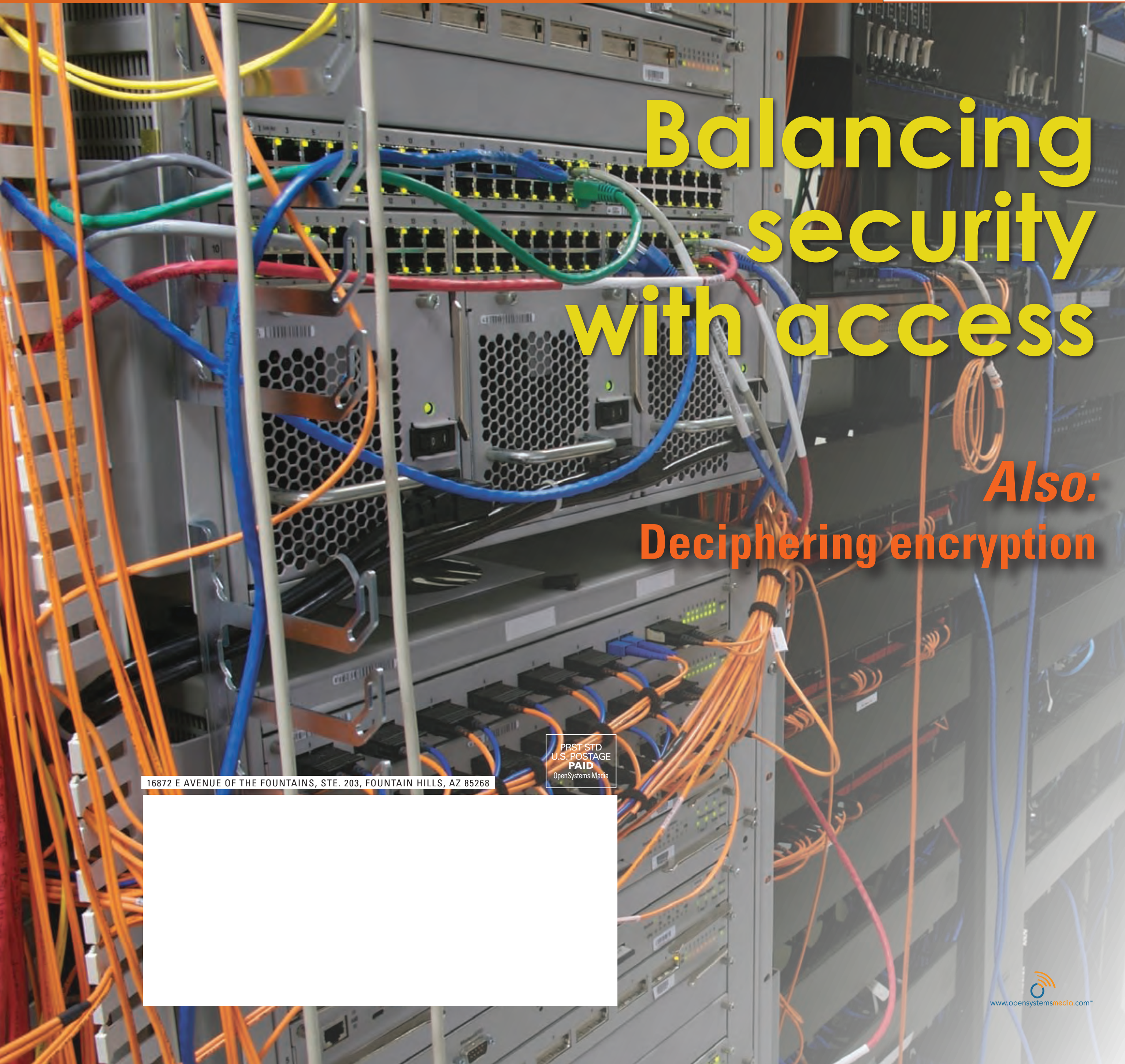
VOLUME 4 NUMBER 7
OCTOBER 2008

INCLUDING:

Chris A. Ciufo
Software as a product line

Joe Pavlat
Tom Swift would be amazed

Daily Briefing:
News Snippets



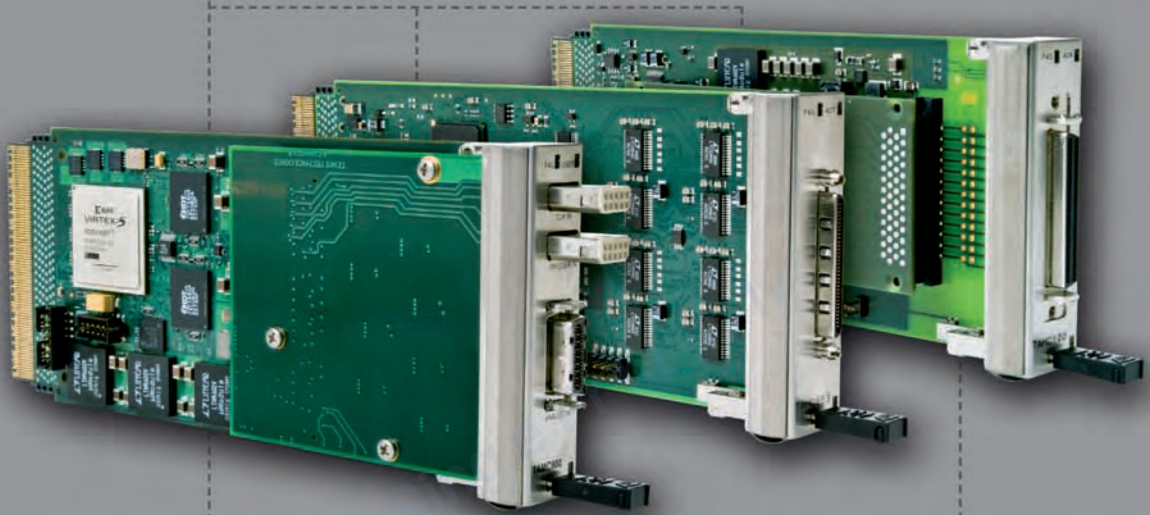
Balancing security with access

Also:

Deciphering encryption

16872 E AVENUE OF THE FOUNTAINS, STE. 203, FOUNTAIN HILLS, AZ 85268

www.opensystemsmedia.com™



Military EMBEDDED SYSTEMS

October 2008 Volume 4 Number 7

E-LETTERS

www.mil-embedded.com/eletter

Helicopter HMIs: Managing risk with automatic code generation, standards, and simulation
By Robert Kopersi wich, Presagis

Digital Molecular Matter: Realistic material damage for military training simulations using real-time Finite Element Analysis
By Steve Griffith, Objective Interface Systems

Back on track: JTRS JPEO assures open SCA and coalition use
Q&A with Dennis M. Bauman, JPEO, JTRS

Digital-Down Converter implementation, FPGAs offer new possibilities
By Bob Sgandurra and Rich Kuenzler, Pentek, Inc.

E-CASTS

www.opensystems-publishing.com/ecast

Virtualization: Operating systems and I/O
Nov. 11, 2008 • 2 p.m. EDT
Presented by: Freescale Semiconductor, LynuxWorks, and Wind River

Multicore: A look from three sides
Nov. 13, 2008 • 2 p.m. EDT
Presented by: Emerson Network Power, Freescale Semiconductor, and Wind River

EVENTS

www.opensystems-publishing.com/events

SDR '08 Technical Conference & Product Exposition
Oct. 26-29, 2008 • Washington, D.C.
www.sdrforum.org/SDR08

Embedded Systems Conference – Boston
Oct. 26-30, 2008 • Boston, MA
www.cmp-egevents.com/web/escb

MILCOM 2008
Nov. 17-19, 2008 • San Diego, CA
www.milcom.org

ON THE COVER:
A typical enterprise server farm contains copper and fiber LAN, MAN, and WAN connections to the Internet "cloud." Defense systems use mostly these same architectures to access the public Internet with unclassified data. But how secure are these COTS-based military systems? And where is the demarcation between widespread Internet access … and secure, classified battlefield networks? See articles starting on page 24.

WEB RESOURCES

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

Published by: OpenSystems media™

The MISSION WORKSTATION

A ruggedized multi-computer workstation for applications that demand the best.

- 4 completely independent computer systems in one 19" 6U rack mount enclosure
- Every Mission Workstation is screened to a ruggedized production acceptance test including fully powered 3G NAVMAT vibration test and environmental stress screening (ESS) test.
- Can be factory configured to be powered from DC or AC sources
- All hard drives are removable
- Temperature range of -10C to 60C
- Each of the 4 computers can be independently configured with Core 2 Dual or Core 2 Quad Intel processors
- Supports multiple operating system configurations
- Can be factory configured as 4 independent computer systems or one cluster computer
- Each individual computer has 2 PCI slots, 1 PCIx-16 slot, up to 8G RAM, 4 SATA ports, 2 Gigabit Ethernet ports, and up to 12 USB 2.0 ports

- Jacyl Technology is the OEM of the Mission Workstation, contact us for custom configurations

Jacyl Technology specializes in the design and production of custom and COTS electronic systems for severe environment applications.

JACYL TECHNOLOGY
Advancing Today's Technology into Tomorrow

www.jacyltechnology.com

Military EMBEDDED SYSTEMS

AN OPENSYSTEMS MEDIA PUBLICATION

Military and Aerospace Group

- DSP-FPGA.com/E-letter
- DSP-FPGA.com Resource Guide
- Military Embedded Systems/E-letter
- Military Embedded Systems Resource Guide
- PC/104 and Small Form Factors/E-letter
- PC/104 and Small Form Factors Resource Guide
- VME and Critical Systems/E-letter

Group Editorial Director	Chris A. Ciufo cciufo@opensystemsmedia.com
Senior Editor (columns)	Terri Thorson tthorson@opensystemsmedia.com
Associate Editor	Sharon Schnakenburg sschnakenburg@opensystemsmedia.com
Assistant Editor	Robin DiPerna
New Products Editor	Cliff Witte
European Representative	Hermann Strass hstrass@opensystemsmedia.com
Senior Web Developer	Konrad Witte
Web Content Specialist	Matt Avella
Creative Director	Steph Sweet
Art D rector	David Diomede
Circula ion/Office Manager	Phyllis Thompson subscriptions@opensystemsmedia.com
Reprints and PDFs	license@opensystemsmedia.com

OpenSystems media™

16872 E. Ave of the Fountains, Ste 203, 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

Communications Group

Editorial Director	Joe Pavlat
Managing Editor	Anne Fisher
Technology Editor	Curt Schwaderer
European Representative	Hermann Strass
Senior Designer	Joann Toth

Embedded and Test & Analysis Group

Editorial Director	Jerry Gipper
Editorial Director	Don Dingee
Senior Associate Editor	Jennifer Hesse
European Representative	Hermann Strass

ISSN: Print 1557-3222

Military Embedded Systems (USPS 019-288) is published eight times a year (January/February, March/April, May, June, July/August, September, October, November/December) by OpenSystems Media, 16872 E. Ave of the Fountains, Ste 203, Fountain Hills, AZ 85268. Subscriptions are free to persons interested in the design or promotion of *Military Embedded Systems.* For others inside the US and Canada, subscriptions are $28/year. For 1st class delivery outside the US and Canada, subscriptions are $50/year (advance payment in US funds required).

Canada: Publication agreement number 40048627. Return address WDS, Station A PO Box 54, Windsor, ON N9A 615

POSTMASTER: Send address changes to ***Military Embedded Systems***
16872 E. Ave of the Fountains, Ste 203, Fountain Hills, AZ 85268

DSP-FPGA.com VME and Critical Systems PC/104 and small form factors
Embedded COMPUTING DESIGN INDUSTRIAL EMBEDDED SYSTEMS CompactPCI and AdvancedTCA Systems

Industry Analysis

Tom Swift would be amazed

By Joe Pavlat

Many young boys, including myself, who were interested in science avidly read the books that were part of the long-running Tom Swift science fiction series. One of my favorites, “Tom Swift and his Photo Telephone,” was written in 1914. Science fiction, of course, became science fact.

The breadth and capability of communications are increasing at an exponential rate. About half of the world’s population now has access to a mobile phone, and millions of new subscribers are added weekly. Communication for the average person is becoming increasingly wireless, and the silicon, software, and infrastructure to support it are evolving quickly. It is now as easy to make a phone call to distant parts of the world as it is to call next door. While we take this in stride, it has broad implications for all of us.

Presentations at the recent Intel Developer Forum (IDF), held August 19-21 in San Francisco, certainly contained the usual amount of hype; however, technologies under development highlighted at IDF credibly predict an increasingly wireless world with seamless voice, video, and data communications that are always on. Wi-Fi, WiMAX, next-generation cellular technologies including Long Term Evolution (LTE), lower-power silicon, improved battery technologies, and even wireless device recharging via resonant RF coupling will enable more numerous and powerful services. In addition to laptops, cellular phones, and PDAs, Intel is planning for a host of low-cost mobile Internet devices that will increase Internet access across the world. They predict 15 billion new wireless network connections in the next 10 years. I believe it. Many of these devices move away from the data center and desktop, and this will produce significant ramifications for the embedded computer industry.

As well, this has many positive – and a few potentially negative – implications for military electronic systems designers and warfare planners. The obvious benefit is that the goal of “any data any time, to anyone, anywhere” will be enabled by these innovations. As we all know, virtually all silicon development is driven by commercial markets, and military designers must work with what is available. Some of the technology Intel presented, including advanced thermal design and heat dissipation techniques, will directly benefit the designs of equipment that must operate in extremely challenging environments.

But at the same time, an increasing reliance on radio transmission for all of this wonderful new stuff has the very real potential to create vulnerabilities that might be very hard to overcome. Hacking into secure networks will become an important *weapon* that will be developed by countries and armies. Due to the relatively low power used by wireless infrastructure, brute force jamming could be used to disrupt battlefield communications. Agile, frequency-hopping radio systems and redundant communications paths will ameliorate this somewhat, but sophisticated directed-energy weapons already under development will be able to permanently cripple critical systems. Major powers will have the ability to disable or interfere with satellite communications. This has major implications for remote awareness and management of battlefield conditions (and even the operation of unmanned aerial vehicles, upon which at least the U.S. military increasingly depends). And, because of the global and open nature of commercial consumer communications technology, protecting intellectual property will be difficult.

This is not just a concern for military planners. As we have seen during recent California earthquakes, disrupting civilian communications can have a significant impact on civil order, especially in major metropolitan areas. All is not gloom and doom, however, as continuous innovation will reduce some of these risks by keeping cyberwar a moving target.

I think I will go up to the attic and see what Tom Swift had to say.

To learn more, e-mail Joe at jpavlat@opensystemsmedia.com.

Legacy Software Migration

By Marianne Crowe

The importance of integrating software reuse into corporate culture

Corporations must systematically reuse code rather than throw away the investment and start from scratch.

Software reuse is a critical strategy for all software development groups. By reusing code while moving to the next-generation platform, corporations can leverage their existing software investment and lessen time to market. However, many companies are struggling to fully implement code reuse throughout their organization. In order to achieve efficient and methodical code reuse, organizations must integrate this goal into their culture.

Reusing code provides the greatest benefits to an organization if it is done systematically, rather than sporadically and opportunistically. However, there are many issues that can prevent systematic code reuse, both technical and non-technical.

Software reuse – Technical issues

On the technical side there are many differences between operating systems, such as the levels of task priorities offered by each OS, which make modifying code for a different platform tedious and cumbersome. This has brought the need for COTS porting tools that will automatically account for differences in operating systems to make the porting work quicker and easier.

In order to avoid porting issues altogether, organizations see the need for an abstraction solution to protect their code against future platform changes. However, developing an abstraction interface using native OS APIs will not give the portability and performance needed in an embedded application. Instead, a lower-level approach needs to be taken to ensure that the fundamental OS resources such as threads, semaphores, and mutex will behave the same across platforms and that performance is not impacted. Also, building and maintaining an in-house abstraction for multiple operating systems requires considerable time, money, and resources.

The developers must have detailed knowledge of each operating system and perform a lot of testing to verify portability across

different platforms, which results in high costs. This is why many companies are turning toward a COTS abstraction layer that is maintained, tested, and verified by a third party, rather than taking focus away from the organization's core competencies. Using common APIs (provided by the COTS OS abstraction) across platforms also lessens any potential learning curve when developing with new operating systems, thereby making code reuse easier to adopt.

> "Reusing code provides the greatest benefits … if it is done systematically …"

Just as reusing code on different operating systems has its own challenges, reusing code when moving to a different language presents difficulties as well. For example, many companies are now moving away from Ada to the more modern C language, due to a lack of programmers and support for Ada. These organizations are utilizing COTS language conversion tools for automatic conversion to avoid a rewrite.

Software reuse – Industry issues

On the non-technical side, while top-level executives and government agencies might see the benefits of code reuse, there is a lack of goal congruence with engineering groups and subcontractors. Many times these groups have psychological barriers to reusing code. They might mistakenly think that code reuse will cause their talents to no longer be necessary. However, by reusing their legacy code quickly and efficiently with COTS code reuse solutions, they are able to contribute their talents to new projects and product development, rather than being bogged down by wearisome porting work.

Organizations might also need to change productivity policies and benchmarks to effectively integrate code reuse into their culture. Rather than focus on how many new lines of code the developer contributed, they might need to reward shorter times for project completion. This will motivate developers to use COTS porting tools so that they can reuse as much as possible quicker to meet an earlier deadline. This will lead to more project completions, more new products, and ultimately more opportunities to get a larger market share in the organization's industry.

Many corporations are finding systematic code reuse difficult to implement due to both technical and non-technical issues, some of which have been mentioned here. However, software reuse remains a critical strategy for a corporation to decrease product development time and costs. For this reason, organizations are turning to COTS code reuse products such as those offered by MapuSoft Technologies (www.mapusoft.com) to lessen the software reuse effort.

__Marianne Crowe__ is director of marketing for MapuSoft Technologies, Inc., responsible for all marketing activities from concept to execution, both domestically and internationally. She holds a BS in Marketing with a concentration in e-Commerce from the University of South Alabama and is currently pursuing her MBA with a concentration in Marketing from Auburn University. She can be reached at marianne@mapusoft.com.

Daily Briefing: News Snippets

By Sharon Schnakenburg, Associate Editor

www.mil-embedded.com/dailybriefing

VME brings new life to Navy system

While some might say VME is a thing of the past, a recent U.S. Navy contract has VME in its future. The Navy's contract stipulates that Cornet Technology, Inc. develops Maritime Embedded Global Positioning System Adapters (MEGA) next-gen VME cards for the San Diego SPAWAR Systems Center. MEGA replaces end-of-life cards in the application module of the Navy's global positioning receiver system, and is part of the Navy's goal of upgrading its maritime GPS to reach Selective Availability Anti-Spoof Module (SAASM) compliance. SAASM is a component of the Space-based Positioning, Navigation, and Timing policy signed by President Bush in 2004. SAASM assures that U.S. enemies can't imitate true GPS signals or insert incorrect time or position information.

U.S. Navy photo by Photographer's Mate 1st Class Ken J. Riley

Organic approach *saves* USAF costs

U.S. Air Force photo by Staff Sgt. Tony R. Tolley

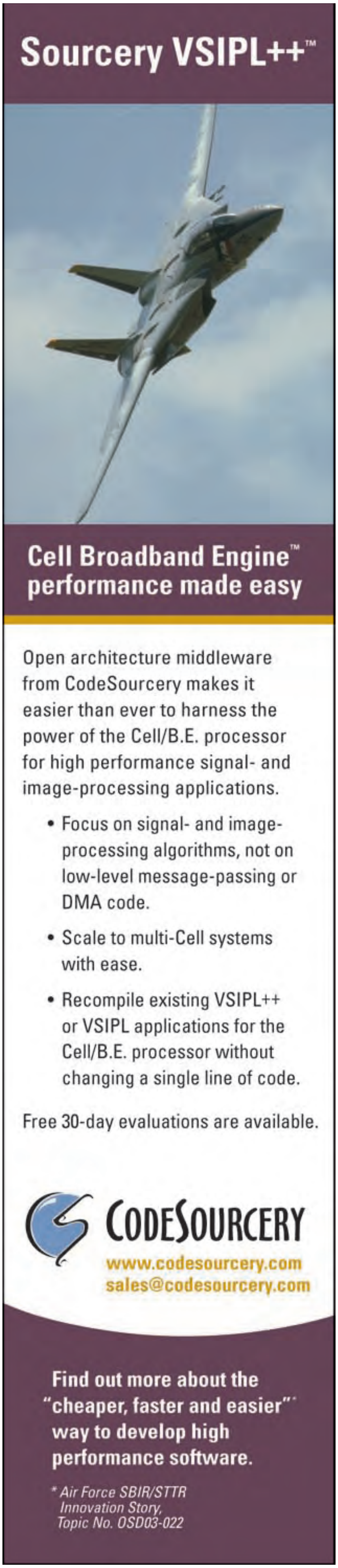
Though "going organic" typically means higher prices, the U.S. Air Force believes the approach will lower theirs. Case in point: Officials at the U.S. Air Force Warner Robins Air Logistics Center decided to form their own internal or "organic" teams – instead of outsourcing to contractors – to conduct a C130 avionics software update. However, the USAF did enlist software developer DDC-I for assistance including training, services, and foundational products for the upgrade. "[The USAF is] creating their own 'organic' software teams to save costs and reduce turnaround times," says DDC-I president/CEO Bob Morris. In addition, the contract specifies that DDC-I provides its OpenArbor object-oriented, mixed-language IDE for safety-critical apps to replace the USAF's legacy MIPS and 1750A Ada compilers.

U.S. Army stays ahead of the game

Photo courtesy of U.S. Army

While the ability to see the future is highly coveted, the U.S. Army is planning on the next best thing: One Tactical Engagement Simulation System (OneTESS). Enter AT&T Government Solutions, Inc., which recently chose Parvus as supplier of the simulation system's Vehicle Interface Control Unit (VICU). The VICU is based on Parvus' DuraCOR 810 COTS processor platform, designed for C4ISR apps and harsh mobile environments as specified by MIL-STD-810F. Meanwhile, OneTESS's operational capabilities are scheduled for FY08 use on vehicles including the Abrams M1A2 SEP and M109A6 SP and the Bradley M2/M3A3. Part of the Army's systems-of-systems, OneTESS will render realistic combat simulations for live participants, including Force-on-Target (FOT) and Force-on-Force (FOF) training to support tactical missions.

Continued on page 14



Continued from page 13

Boeing and Raytheon together again

Already onboard the Boeing-led industry team for the U.S. Navy's P-8A Poseidon, Raytheon recently joined Boeing's EP-X industry team. EP-X is a manned ISR and targeting aircraft slated to supersede the EP-3, a U.S. Navy SIGINT platform. Raytheon will provide EP-X's multi-intelligence integration and sensor integration, and play a major part in core mission systems. The EP-X $1.25 million "concept refinement contract" was awarded to Boeing earlier this year. Boeing expects to draw maintenance, logistics, support, relevant data, and training from P-8A Poseidon into the EP-X project. P-8A Poseidon is an ISR aircraft designed for anti-surface warfare and anti-submarine warfare.

VPX computing speeds up DARPA

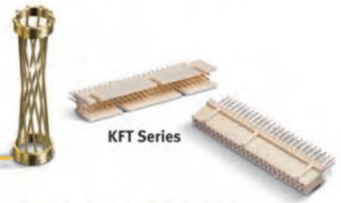
… or hastens one of DARPA's field intelligence programs anyway. Accordingly, prime Science Applications International Corporation (SAIC) recently chose Quantum3D, Inc.'s LibertyVPX High-Performance Embedded Computing (HPEC) system for subcontractor implementation for the DARPA Space-Time Adaptive Processing ("STAP Boy") contract. STAP Boy provides field environments with teraflop computing power, enabling fast, real-time, high-volume processing in order for soldiers and first responders to use space-time adaptive radar systems, high-resolution sensors, occupant tracking, and urban structure mapping during life-critical missions. LibertyVPX HPEC will provide STAP Boy's research and development program with Imagery Intelligence (IMINT), COMINT, SIGINT, and radar capabilities.

'Freedom' in the U.S. Navy

The U.S. Navy has long encompassed the value of freedom, but now it is embracing a more tangible form of *Freedom*: the first Littoral Combat Ship (LCS) in the nation. The 378-foot *Freedom* monohull ship, aka *LCS 1*, was recently delivered to the Navy for service and commissioning by an industry team led by Lockheed Martin. *Freedom* can displace 3,000 metric tons, travels faster than 40 knots, and is touted to lend the Navy increased dominance in seaside battles. Additionally, *LCS 1* will help the Navy overthrow maritime threats including surface warfare, anti-submarine warfare, and mine warfare. The combat vessel passed its sea trials in August and is slated for commissioning this November in Milwaukee, WI.

Photo courtesy of Lockheed Martin

HYPERTAC
HYPERTRONICS
EXTEND


KFT Series

Deciphering encryption: Choosing the best protection for your network

By Oren Barkai

U.S. Army photo by Staff Sgt. Kevin L. Moses Sr.

Over the past few centuries, military means and methods have evolved in line with technology. Communication networks have become a crucial component of the military's day-to-day operation and with that, the growing need for their protection. With encryption as the basis of network protection, Oren compares the two most common methods, namely IPSec and Layer 2 encryption, with Layer 2 as the clear winner.

Modern-day warfare dictates that network-centric communications technology must be as much at the core of a successful military campaign as a strong battle plan and disciplined soldiers.

Accordingly, a network-centric communications infrastructure must have flexibility, agility, scalability, redundancy, and the ability to assimilate information security in key network layers (Figure 1). Integrated management is also required to allow shared situational awareness for all staff levels. But above all, network-centric communications infrastructures must be secured and protected – a formidable challenge when faced with numerous and potentially lethal security threats.

Through common standards platforms such as FIPS, ITU-T, IEEE, IETF, and others, administrators of military communication systems around the world are able to share and exchange knowledge about the most common threats. These threats include interception, or the gaining of access by an unauthorized party to sensitive assets; interruption, or the rendering useless of an asset of the system; modification, or the tampering of an asset by an unauthorized person; and fabrication, or the insertion of new objects into the system by an unauthorized party.

One of the most frequently used and most effective solutions for combating these network security threats is encryption, which is defined by the Israel Ministry of Defense as: "Scrambling of data, entirely or in part, by modifying the data or how it is transferred, using mathematical equations or algorithms, whether by means of a key or not."[1]

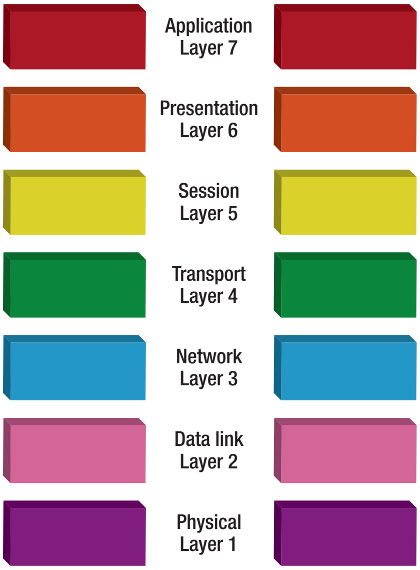


Figure 1

Defense against network threats comes at a price, and installing a proper encryption system can be costly. In certain cases, costs can reach as high as 10 percent of the total link costs. However, the challenge that many military network administrators face is not only managing encryption budgets and expenditures, but also finding an encryption platform that is highly effective and does not hold significant performance implications.

In the next sections, we will look at these performance implications, namely network complexity, jitter, and latency. We will also examine how Layer 2 solutions can overcome most of these drawbacks at a reasonable cost, and why they are a better alternative to the commonly used IPSec.

Encryption drawbacks: The ins and outs of network complexity

Network complexity has become a significant concern amongst network administrators as the use of modern IPSec encryption continues to grow. Reasons to note include:

- If IPSec Tunnel Mode is used, then a new IP header is created to mask the whole packet, meaning that the IP packet becomes larger and takes more time to pass through the route, thus process time increases. It also complicates the network as the operator needs to hold two sets of addresses (for encrypted packets and decrypted packets).
- Encryption usually works in point-to-point or point-to-multipoint connectivity. More links mean more encryption keys are required. This makes operations more complex and can cause human errors, leading to network malfunctions.

As an example, a voice over IP network requires that end-to-end latency is below 250 milliseconds (msec), a requirement that, in most cases, can be satisfied by design. In an example network, the longest span latency reaches a maximum of 200 msec. This is a characteristic latency between two remote nodes in a representative network.

However, if point-to-point encryption is introduced and there are several hops along the way, each hop represents twice the latency introduced by the encryptor. If an encryptor introduces 5 msec latency, it will only take seven hops before there is significant adverse impact on network performance.

Since maximum span reaches 200 msec and the span comprises seven hops, the combined latency becomes 270 msec (200 msec span latency + 5x14 encryptors latency = 270 msec). Being above the minimum required 250 msec latency level translates to rapid degradation of voice quality and ocasionally the rendering of inaudible conversations.

IPSec issues: Latency and jitter

The two other main drawbacks are latency and jitter. When using IPSec encryption as described in our previous example, packet size may change in a non-deterministic way. This change influences the network performance, mainly in terms of latency and jitter.

Figure 2 demonstrates that, apart from processing the information in the encryptor, the overall packet size of the new IPSec encrypted packet may vary. In this

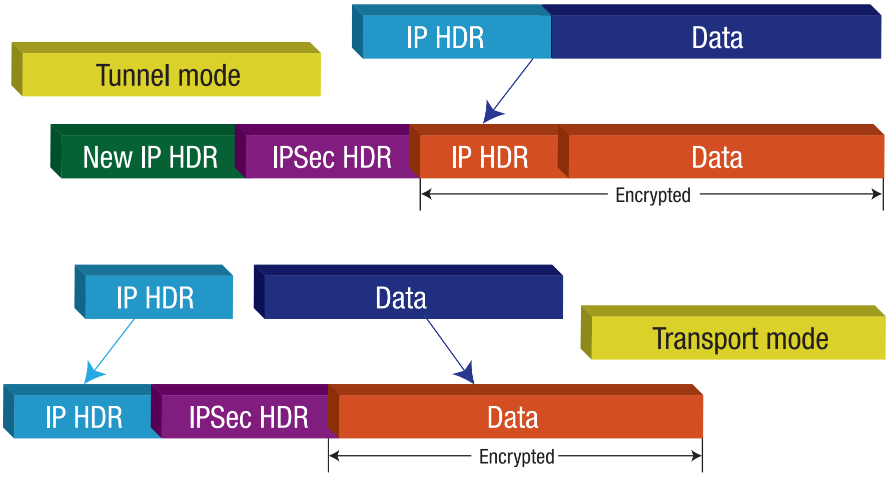


Figure 2

instance, not only does latency occur, but variations in packet size can also take place, introducing unnecessary jitter to the system.

Apart from jitter, let us assume that the network has 20 nodes (a small network), with each node connected to 3 other nodes. In this case, the routing tables comprise a maximum of 19 IP addresses at each node. Introduction of IPSec in tunnel mode means that an additional 19 or more (if we are using several keys between nodes) IP addresses will be required as we can also work in unprotected mode (for lower classified applications).

We therefore find ourselves faced with a serious and complex dilemma. If we use encryption, costs increase, performance suffers, and the network is saddled with numerous complexities, making it very difficult to manage. If we do not use encryption, costs are lower; however, the network is extremely vulnerable.

Analyzing possible solutions

It is commonly understood that military networks will not "function" without encryption as classified applications demand more and more network resources. Therefore, the solution is to find the best-performing and most cost-effective encryptor (Table 1). This system should include the following attributes:

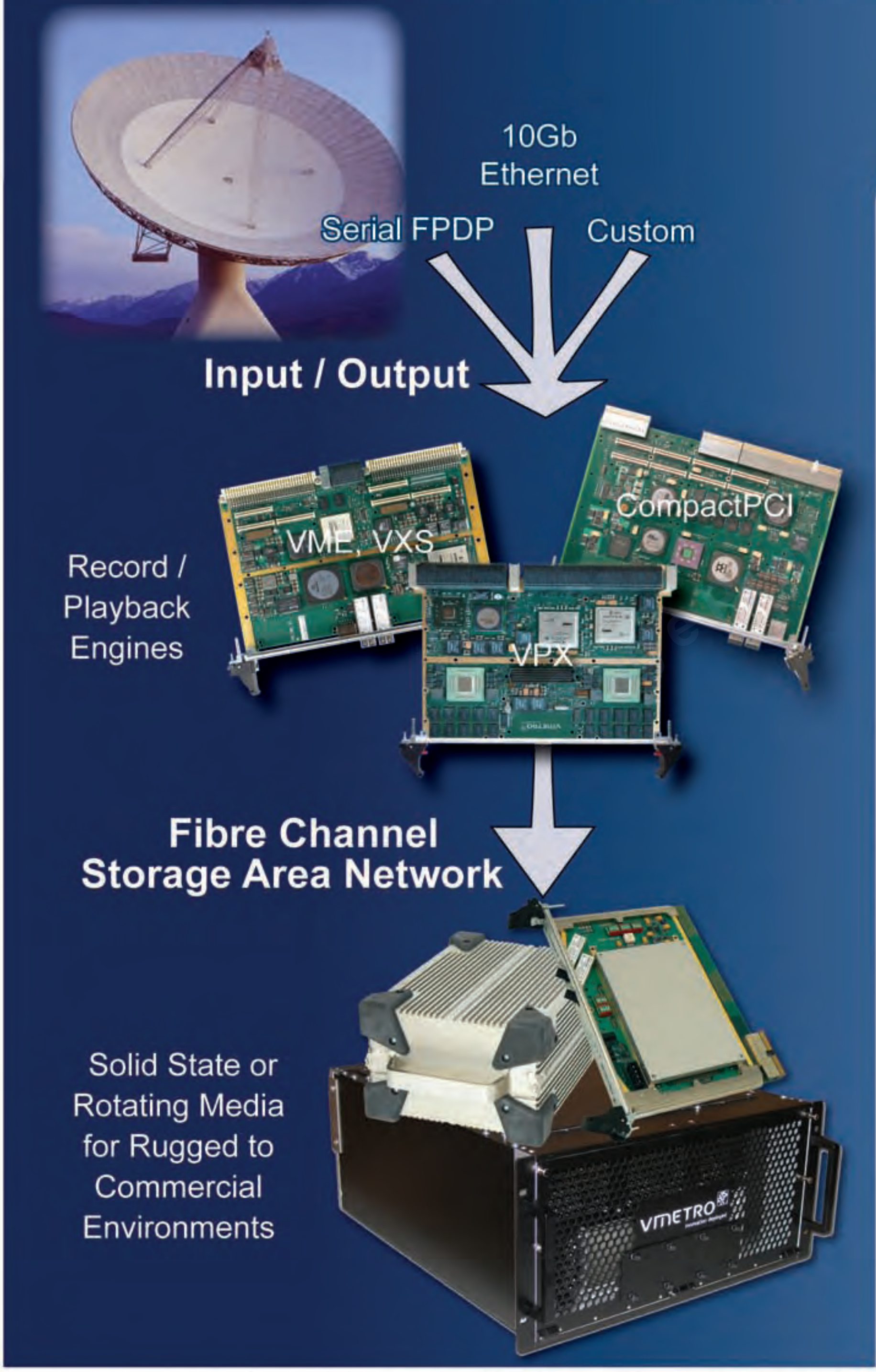
- High performance – minimum latency, maximum throughput possible
- Low in cost

Type of encryptor	Latency	Variation in latency (jitter)	Throughput	Network protection	Cost
None	Best (none)	Best (none)	Best (100%)	Worst (none)	Best (none)
Transmission encryptor (for example, Ethernet)	Excellent (under 1 msec)	Excellent (under 1 msec)	Good (small packets 80% and for mid-large packets 99%)	Very good	Medium-Low
IP encryptor (IPSec)	Good (under 5 msec)	Good (1-2 msec)	Good (usually around 90-99%)	Good (not covering Layer 2)	Medium-High
Application based encryption (such as Internet Explorer SSL module)	Not good (depends on platform and resources availability)	Not good (variation depends on non-deterministic platform behavior)	Not good (high variation)	Not good (covering only specific applications)	Excellent (may be free or very low cost)

Table 1

Hybricon Corporation 12 Willow Rd. Ayer, MA. 01432
info@hybricon.com
1 800 HYBRICON
Tel: 978 772-5422
Fax: 978 772-2963
Let Hybricon Put Your Mind At Ease
www.hybricon.com
When your boards are subjected to the most severe environments, trust Hybricon enclosures to safely package and protect them.
Hybricon®
Innovation • Quality • Service
0908DA

Rugged High-Speed Data Recording and Storage


10Gb Ethernet
Serial FPDP
Custom
Input / Output
VME, VXS
CompactPCI
VPX
Record / Playback Engines
Fibre Channel Storage Area Network
Solid State or Rotating Media for Rugged to Commercial Environments
VMETRO

Powerful

- Streaming data recording platforms with up to **800MB/s** per recording engine sustained recording performance
- Scalable Fibre Channel SAN architecture providing virtually limitless storage capacity

Flexible

- Customer programmable or application specific recording and playback systems
- VPX (VITA 46), VPX-REDI (VITA 48), VXS (VITA 41), VME and CompactPCI recording engines
- Solid state or rotating media options from rugged to commercial
- Access and control using web browser or XML-RPC
- Disk grouping and intelligent disk management

Recording Information: rec1

Disk Group	Recording	Size	First Stripe	Last Stripe	State	Avg. MB/s
dg1	rec1	[illegible]		851	Not Recorded	0.00

Record and Playback

Infinite operation	Specify Playback Start Offset (Bytes)	Specify Playback End Offset (Bytes)
□	0x	0x

Select operation:

Recording utilities:

Disk Speed Test
Integrity Check
View Data

Embedded Computing - Data Recording/Rugged Storage - Bus/Protocol Analyzers

For more information, please visit
http://www.vmetro.com/recorder
or call (281) 584-0728

VMETRO
innovation deployed

Request our New
2008 Color Catalog

VECTOR

ELECTRONICS & TECHNOLOGY, INC.

A FINE TECHNOLOGY GROUP

FORWARD THINKING

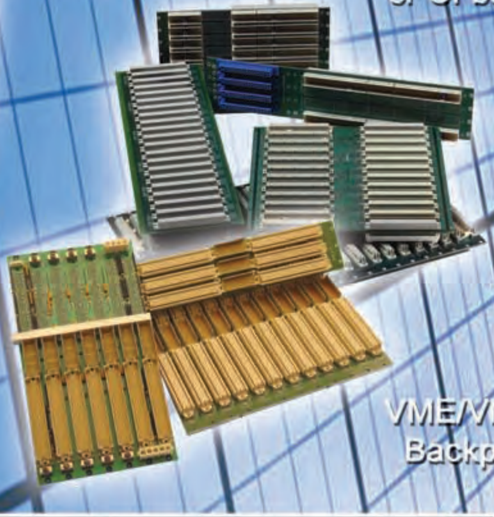
THE MOST EXPERIENCED IN
SYSTEM PACKAGING DESIGN.

Subracks

790 and 792 Ruggedized Enclosures

Model 2345 shown with optional dual AC, hot-swap power supplies, cPCI backplane 4RU, front air intake, and top exhaust

VME/VME64X/
cPCI® Rackmount
Enclosures



VME/VME64X
Backplanes

Made in U.S.A

(800)423-5659

WWW.VECTORELECT.COM

SHORT LEAD TIMES ● CUSTOM CONFIGURATIONS ● FACTORY SUPPORT

- Minimal network implication – no change in IP address
- Maximum protection to the network – as low as possible on the Open Systems Interconnection Basic Reference Model (OSI Model) seven layers model of International Organization for Standardization (ISO). See again Figure 1.

Let us examine several options to see how they fit these requirements.

Since not employing an encryption system is not a realistic option for today's defense networks, and considering the poor performance of application-based encryption, let us turn our attention to transmission versus IP encryptors.

IPSec technology is a Layer 3 technology, which protects all layers from Network to Application. IPSec is today's common civil solution for Internet traffic securing and business-sensitive traffic solutions. Transmission encryption, on the other hand, is a Layer 2 technology, which protects all layers from the Data Link layer all the way to the Application layer.

For the sake of establishing the preferred method, ECI Telecom has conducted several trials with both transmission and IP encryptors in order to review both options and compare performances. The trial setup was based on a point-to-point link with traffic generator at both sides and load testing using changeable packet/frame size. This method was used to compare how Layer 2 and Layer 3 encryptors behave. Figure 3 shows an illustration of the trial setup.

The traffic generator created traffic marked as "Cleartext" with variable packet/frame size. Both encryptors were tested at different times, and the reports of the traffic generator were noted.

As already stated, it is acceptable for an encryptor to reduce the amount of traffic passing through it (limiting throughput). However, it is advised that the throughput would be as close to the actual Cleartext traffic as possible to minimize the performance issues. The trials were repeated several times, and the average test results are shown in Figure 4.

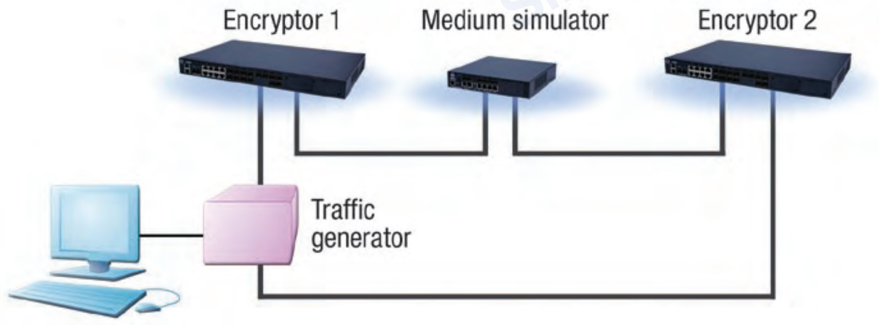


Figure 3

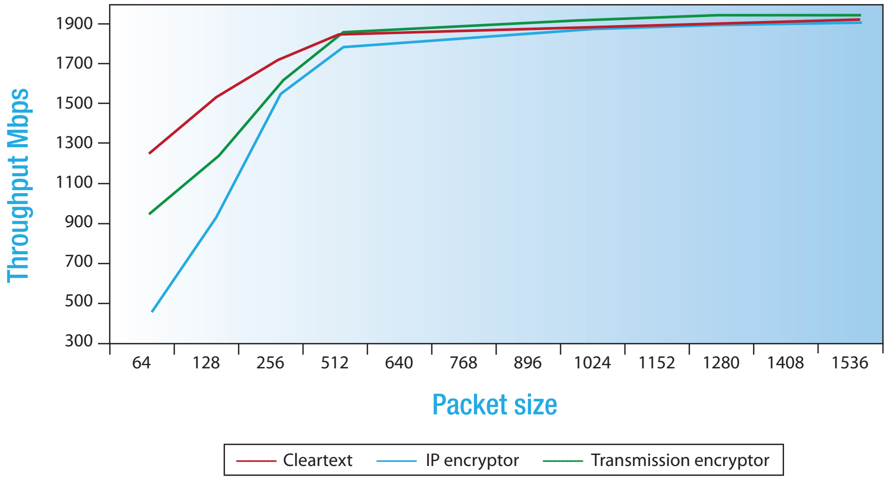


Figure 4

In parallel, ECI Telecom has also tested latency performance. For those tests, using the same test setup but measuring the latency of the link (passing through a Layer 2 encryptor and medium simulator), the medium simulator was set to 10 microseconds to eliminate influence on total link latency. The results of these trials are summarized in Table 2.

It is evident from the test results that even though IPSec encryption results in acceptable latency and jitter performance, Layer 2 encryption has superior influence on network performance. Layer 2 encryption has better network protection and results in simplified network operation.

Layer 2 is "number 1"

Extensive testing by ECI Telecom showed that Layer 3 encryptors perform with an average latency of almost 2 msec coupled with variation (jitter) of 13 percent, while Layer 2 encryption has an improved latency performance 30 times over, with twice the stability in variation.

These results indicate that Layer 2 is a superior, more effective approach for the majority of today's military networks, which operate large multi-hop complex communication infrastructures. This provides them with an ultimate solution to balance both cost and performance, while securing their networks in greater depth.

References:

1. www.mod.gov.il/pages/encryption/governing.asp

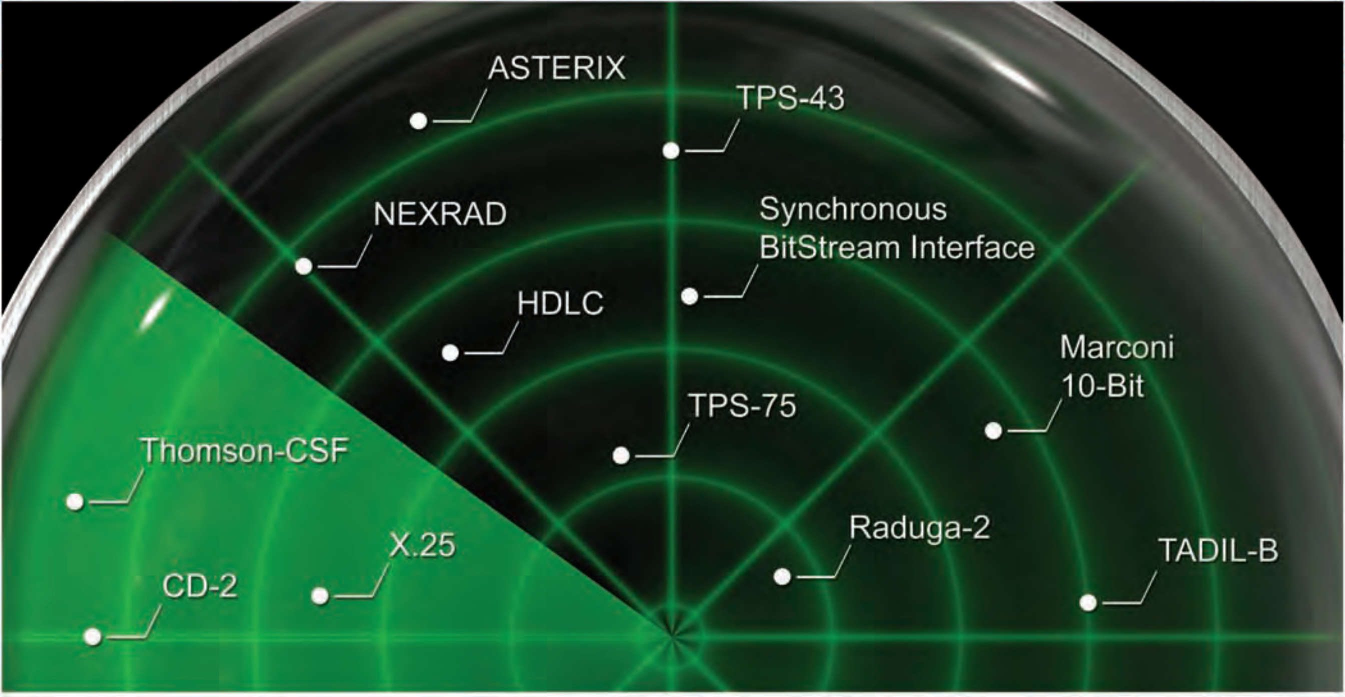
> "It is evident from the test results that even though IPSec encryption results in acceptable latency and jitter performance, Layer 2 encryption has superior influence on network performance."

__Oren Barkai__ is senior system architect, Government & Defense Solutions, at ECI Telecom. He holds an MBA from the Technion – Israel Institute of Technology and a B.Sc. in Electrical Enginerring from Tel Aviv University. He is a former Major in the Israeli Defense Forces Signals Corps, and brings with him a decade of experience in military networks and security. Oren can be reached at Oren.barkai@ecitele.com.

ECI Telecom
+972 3 9266555
www.ecitele.com

Encryptor type	Average latency (msec)	Latency deviation/Jitter (microseconds)	Comments
IPSec (Layer 3)	1.87	250	---
Transmission (Layer 2)	0.06	4	Variation of medium normalized and may be ignored

Table 2



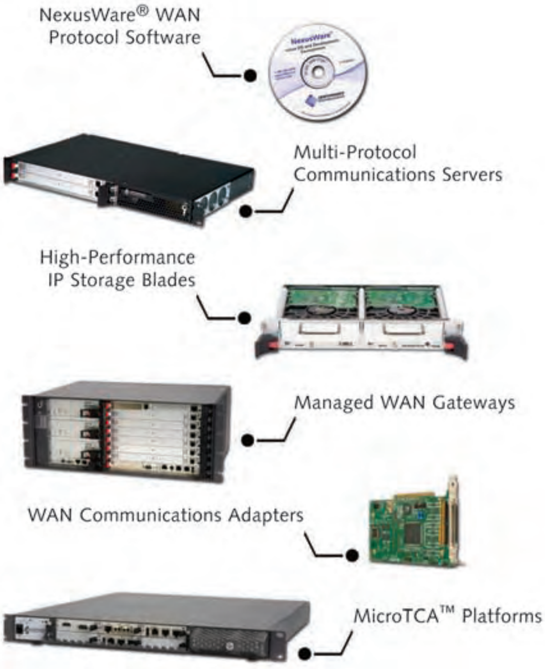
What's on your Radar?

Performance Technologies' NexusWare® WAN protocol software provides a seamless connection to a broad range of telecommunications, aerospace and defense, and commercial applications for both emerging and legacy networks.

With over 25 years experience developing highly reliable and scalable solutions, we can provide you with integrated hardware and software that can meet your product needs today and allow for future migration tomorrow.

Managed WAN Gateways, Radar Extraction, Recording Servers, and Lawful Intercept Platforms are a few of the many applications that utilize our broad software offering. Available on a suite of hardware platforms in PCI™, PCI Express®, CompactPCI®, MicroTCA™, and stand-alone form factors, our flexible WAN protocol solutions can easily accommodate a wide range of data and communication network requirements.

Explore the limitless possibilities for your programs by calling Performance Technologies today.


NexusWare® WAN Protocol Software
Multi-Protocol Communications Servers
High-Performance IP Storage Blades
Managed WAN Gateways
WAN Communications Adapters
MicroTCA™ Platforms

PERFORMANCE TECHNOLOGIES

Phone: 585.256.0200 • www.pt.com/radar5 • E-mail: info-request@pt.com

U.S. Air Force photo by Airman 1st Class Kelly L. LeGuillon

Finding the balance between network access and security

By Bob Fortna

Network access management solutions can deliver both collaboration and security to support the DoD's vision for net-centric operations and military transformation.

As the need for increased security grows within U.S. Department of Defense (DoD) communications networks, defense IT network managers face growing pressure to provide solutions that enable the right people to access the right information at the right time.

Secure network access is essential to modern military operations. The past decade has brought numerous technological advancements and a plethora of new handheld mobile computing devices that allow DoD personnel and contractors remote access to resources. This exploding "edge" of defense networks presents a whole new world of challenges when combined with increasingly sophisticated and coordinated security threats and wide ranges of security clearances of warfighters, defense personnel, and various partners.

How can defense IT managers field networks that protect sensitive data while ensuring the right people can access it quickly, securely, reliably, and remotely?

Greater access, greater threats

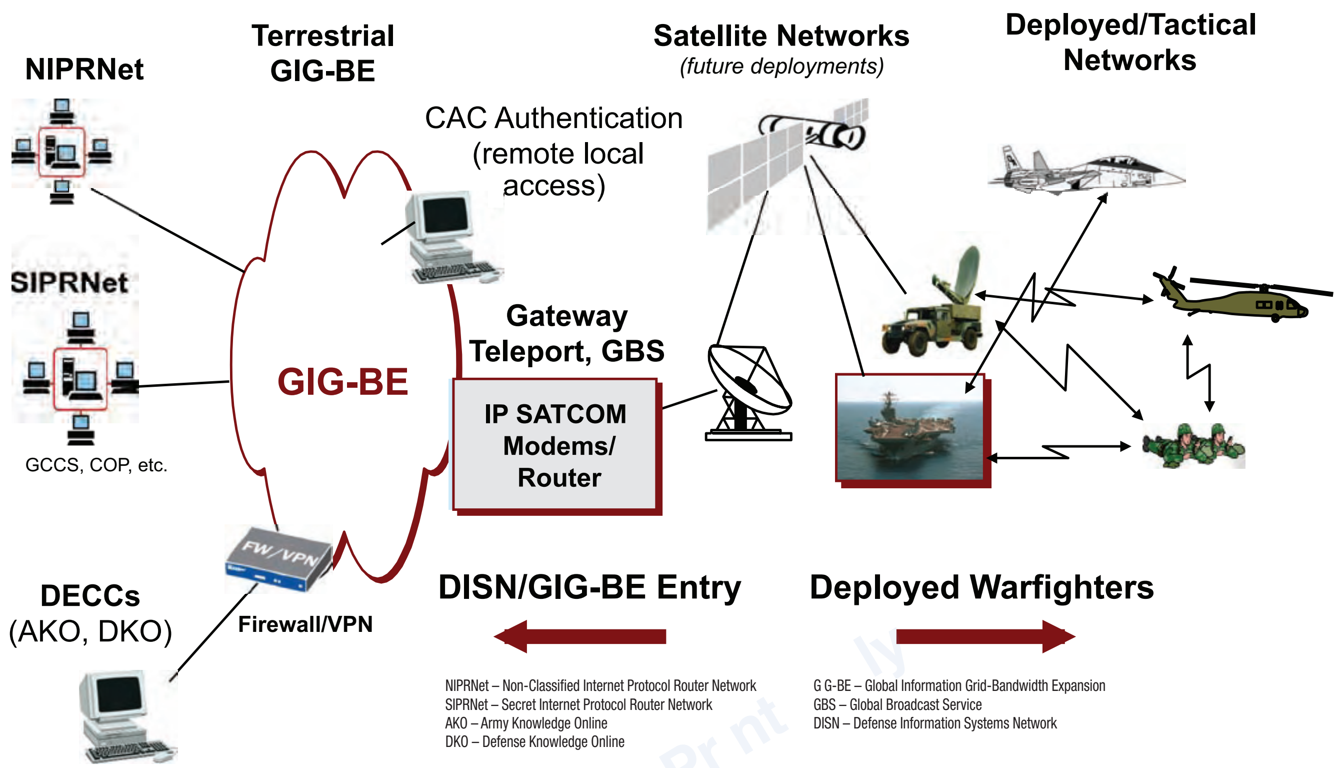
Technology that enables warfighters to communicate from virtually anywhere in the world has significantly improved battlespace operations and management, and opened doors for greater collaboration throughout the defense logistics and outsourcing chains. However, such expanded networks often weaken the traditional model of trusted internal users surrounded by physical network security.

Today's defense networks must support a dynamic and diverse user community, including warfighters, suppliers, partners, and remote workers who work from their office desktops, home laptops, or mobile devices in all manner of field conditions. Defense IT teams must therefore ensure the physical and informational security of an interconnected global network.

These security demands are exacerbated by an increasingly mixed workforce with varying clearances requiring access to unified networks, using increasingly sophisticated mobile devices. Network security is further threatened by the growing number and volume of mission-critical and collaborative applications. The adoption of new business applications, the "Webification" of existing applications, and increasing demands for converged networks transporting voice, data, and high-volume video and geospatial images are fueling the demand for higher-bandwidth defense networks.

Military personnel who share the same networks (and, in many cases, terminals) to access vital information face these challenges throughout their workday. As in the Defense Department's Global Information Grid (Figure 1) or other networks, defense personnel of various ranks and security levels must access a safe, global DoD network, regardless of where they are located, for a number of mission-critical applications. It is at this intersection of collaboration and security where network-wide visibility and control are necessary to manage changing risks.

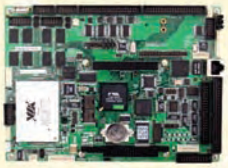
Communications Elements Of The GIG



NIPRNet – Non-Classified Internet Protocol Router Network
SIPRNet – Secret Internet Protocol Router Network
AKO – Army Knowledge Online
DKO – Defense Knowledge Online

G G-BE – Global Information Grid-Bandwidth Expansion
GBS – Global Broadcast Service
DISN – Defense Information Systems Network

Figure 1



The key to secured collaboration

When managing a global defense network, IT managers need to employ a holistic security approach that integrates authentication, data encryption, and data protection. Highly integrated security solutions that can proactively address security breaches without constant IT intervention are key in solving the DoD's security challenges. Three critical approaches to identity management and access control are essential:

Adopt an adaptive threat management strategy – You cannot control what you cannot see. An adaptive threat management strategy enables network-wide visibility and control to adapt to constantly evolving security risks. This allows network IT departments a network-wide view for monitoring, trending, and reporting security breaches.

An effective adaptive threat management solution will combine Secure Sockets Layer Virtual Private Network (SSL VPN) technologies with Intrusion Detection and Prevention (IDP) approaches, including deep packet inspection, anomaly detection, and application inspection. When enabled for high-performance throughput networks, an adaptive threat management approach results in numerous network security benefits such as proactive data protection, operational continuity, and reduced Total Cost of Ownership (TCO).

Adaptive threat management automatically responds to network attacks and isolates only offending users while others continue their communications unaffected. This results in fewer network disruptions, more efficient use of IT resources, and support for rigorous compliance requirements. It helps reduce the strain on IT resources and time by automatically taking action against users not complying with security policies by forcing them to remedy their actions and drop their traffic. Meanwhile, IT is instantly notified of the security violation.

Establish effective authentication policies – Endpoint security compliance is important because of the increasingly mobile military force and wide range of devices accessing the network. Ensuring that applications are only accessed by authenticated and authorized users is especially significant in situations where highly sensitive data can be compromised if accessed by inappropriate users or those with inadequate levels of security. The first step to solving this issue is to create policies that establish who is permitted access to certain information and under which conditions. These policies must apply regardless of the user's location and endpoint device, and must then be enforced through network access control technologies (for example, firewalls and user authentication applications).

Deploy appropriate technology "gatekeepers" – Network policing ensures appropriate authorization and protection. Since DoD personnel access the network from various locations, the network must employ technology that enforces authentication policies whether the network is being accessed from a secure office or a vulnerable wireless location. Deploying appropriate technology "gatekeepers" ensures authorization that protects against viruses and security breaches.

SSL VPN solutions are the most efficient way of obtaining user identity and establishing endpoint security, while allowing granular user access policy adherence and thus providing end-to-end, real-time network protection. Combined with firewalls and IDP solutions, defense IT managers can ensure global network protection that not only provides information such as IP addresses, but actually lends insight into who is navigating the network perimeter and which applications they can access.

> “Remote, wireless access to high-performance networks where security is paramount and collaboration is among trusted partners is now a hard requirement of defense systems.”

Example: CAC authentication

An example that illustrates the critical elements in a wireless communications environment is provided in the area of Common Access Card (CAC) authentication. CAC authentication is required to access defense networks, with strong data encryption required for wireless access (such as conforming to NIST FIPS 140-2 standards).

The Juniper Networks Unified Access Control (UAC) solution supports FIPS 140-2 encryption and CAC authentication for wireless devices. UAC also helps to enforce endpoint security policies such as the state of the user's personal firewall, anti-virus software, and operating system patches. The security health of the endpoint device is routinely and dynamically monitored by UAC, which forwards these findings to a downstream policy server. The policy server then determines the level of access granted to the wireless endpoint. For instance, unhealthy endpoints can be dynamically placed onto a quarantine network or simply denied access.

Such FIPS-compliant approaches to adaptive threat management are demonstrating their ability to secure wireless defense networks serving defense users and their partners. Such solutions will help meet increasing demands for secure, high-bandwidth collaboration networks for a variety of defense applications, from logistics and supply management to battlefield operations.

Redefining the secured perimeter

Defense IT and network managers need to create a responsive and trusted environment for delivering intelligence in support of military operations. Remote, wireless access to high-performance networks where security is paramount and collaboration is among trusted partners is now a hard requirement of defense systems. A comprehensive access management strategy, integrated with rigorous network security solutions, can enable responsive and trusted network environments to better serve and protect the warfighter and logistical partners.

These balanced approaches between access and security will enable significant improvements in trusted collaboration throughout defense networking systems – and between defense users and those in other federal agencies and international organizations.

Bob Fortna is vice president of the defense sector for Juniper Networks. Bob is an active participant in the Armed Forces Communications and Electronics Association (AFCEA) and currently serves on the AFCEA Executive Committee and board of directors. He can be contacted at bfortna@juniper.net.

Juniper Networks
571-203-1723
www.juniper.net

Case study: Vigilant and alert

Emergency notification system deployed for force protection at Baghdad's Camp Slayer

By Andy Anderson

***Editor's note:** Public photos of Camp Slayer are practically nonexistent due to security reasons. The camp is a sprawling complex east of Baghdad's airport and west of the main city, and comprises many of Saddam Hussein's former palaces, retreats, and recreational lakes. In this photo (left), Sgt. Phillip Nichols gets fitted for his new Improved Outer Tactical Vest at Camp Slayer on March 14, 2008. The up-armored vest is a grim reminder that life in Iraq for coalition forces is anything but recreational. Vests are worn most of the time, or donned quickly when an alert is sent. [Image courtesy of U.S. Army Central (USARCENT) Coalition Forces Land Component Command (CFLCC). Photo by Spc. Aaron Rose, U.S. Army.]*

Camp Slayer in Baghdad, Iraq, lies in what the U.S. Army refers to as a "theater of operations." This somewhat innocuous phrase obscures the volatile nature of an area that exists under a constant spectrum of wartime threats.

Multi-National Force-Iraq personnel living and working at Camp Slayer must constantly be on guard for unpredictable and random attacks by an adversary adept at

SUPER ★ TALENT®
THE BEST MEMORY

Reinventing Storage

Rugged, Reliable, Unparalleled

SATA / IDE SSD

Solid State Drives

SATA/ IDE SSD

- SATA I, SATA II, IDE and ZIF Interfaces
- 100% compatible with standard hard disk drives
- Form Factors in 1.3"/1.8"/2.5"/3.5"

Now up to 120MB/Sec!

- **Performance**
  Operating Temp: Industrial and Commercial Temperature available
  Access Time: 0.1ms
  Power Consumption: 85% less than Average HDD
- **Reliability**
  Shock: 1500G(operating)
  Vibration: 16G(operating)
  MTBF: >1,000,000
- **Endurance**
  Read: unlimited

DuraDrive - Ultra Rugged and Reliable SSDs
MasterDrive - Ultra Fast Commercial SSDs

"AWARD WINNING PRODUCT"

CeBIT
"Innovation of the year"
Award

DISKCON USA
Best of Show Award

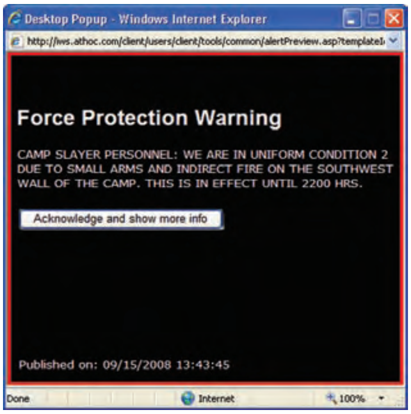
For more information, please contact :
oemsales@supertalent.com or 1.408.934.2578

ssd.supertalent.com

hit-and-run tactics. Vigilance is key. Being alerted to threats in time to take appropriate action means lives saved, injuries avoided, and facilities protected.

At Camp Slayer, the task of emergency notification is done by AtHoc's IWSAlerts. IWSAlerts is a network-centric, emergency notification system that rapidly communicates to personnel through a wide range of communication channels and delivery devices. The alerting system is deployed at Camp Slayer primarily for force protection purposes to notify of changes in the defensive posture of the camp.

When a threat has been identified, authorized personnel at the Area Defense Operations Center (ADOC) can trigger alerting scenarios using IWSAlerts, which manages the entire alerting process. Emergency alerts appear on computers as intrusive audio/visual desktop alerts. The alert notification system controls notification, scenarios, permissions, user contact information, and alert tracking. Typically, the alerts notify personnel to put on Kevlar helmets or individual body armor due to enemy activity in the area. The alert includes notifications directing personnel to take cover or remain indoors due to the threat of indirect fire, incoming mortar, or rocket rounds.


Desktop Popup - Windows Internet Explorer
http://iws.athoc.com/client/users/client/tools/common/alertPreview.asp?templateI
Acknowledge and show more info
Done
Internet
100%

Force Protection Warning

CAMP SLAYER PERSONNEL: WE ARE IN UNIFORM CONDITION 2 DUE TO SMALL ARMS AND INDIRECT FIRE ON THE SOUTHWEST WALL OF THE CAMP. THIS IS IN EFFECT UNTIL 2200 HRS.

Published on: 09/15/2008 13:43:45

The screenshot shows an example of an alert that is commonly sent out at the camp.

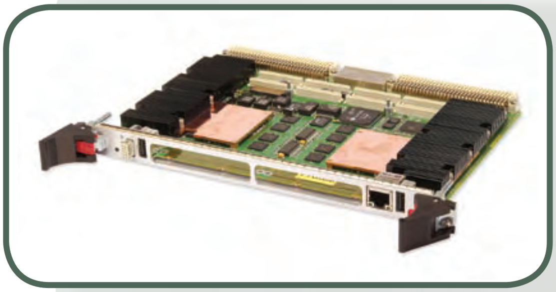
According to Captain Greg McCulley, former C2 Systems Branch Chief, Multi-National Force-Iraq, "The alerts can be tailored to include information about the threat and provide instructions for action based upon the alert recipient's role and location. Personnel receive alerts within seconds after the alert is triggered." The alert notification system is currently protecting several hundred troops. At peak times of hostile activity, alerts have been activated as often as three times a week.

This COTS-based alerting system was selected to be deployed at Camp Slayer because of its proven performance throughout numerous U.S. military commands, as well as for its speed of alert delivery and support of military-grade security requirements. Local network technicians and the vendor worked closely over a few weeks to install and configure the system and train the local operators. Army security specialists then rigorously tested the system over a two-week period for information assurance certification before deploying the COTS software on their secret SIPRNET network.

Leaders at all levels take personal responsibility for getting alerts out during high-threat conditions. The network-centric alerting system has done much to enhance the defensive posture of all the members of the multinational force posted at Camp Slayer. Keeping them informed of current threats is crucial to keeping them safe in a hostile environment. Iraq is no place to become complacent, and with a powerful emergency alerting system in place, troops are safer and the camp is better protected.

Andy Anderson, *Colonel, USAF (Ret.), is AtHoc's vice president of defense operations. He oversees AtHoc's continued expansion in the Department of Defense (DoD) and directs the company's defense-related business development activities. Prior to retiring from the Air Force, he served as director of logistics and communications for Headquarters Air Force Space Command. Andy has also held assignments at the Air Force Communications Command, Air Mobility Command, and Air Force Special Operations Command. He served as the director of staff for the Pentagon's communications directorate, and as the executive officer for the senior communications officer at NORAD and U.S. Space Command. He can be contacted at aanderson@athoc.com.*

AtHoc • 650-685-3000 • www.athoc.com

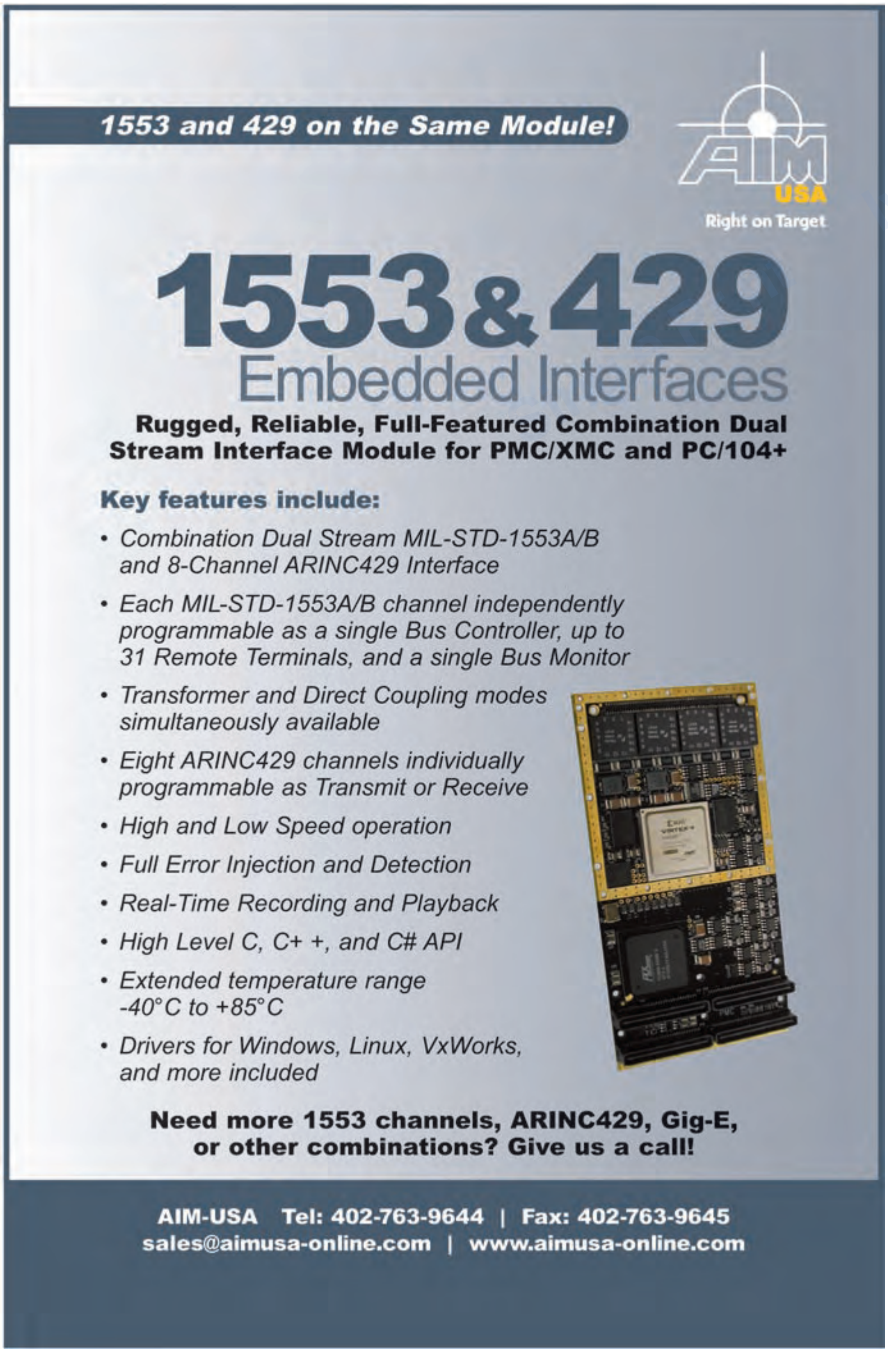


Over 20 percent power savings with PPC SBC

Everyone wants more: more cash, more horsepower, more leisure time. But when it comes to power consumption on SBCs … *less is more.* So GE Fanuc Intelligent Platforms began pressuring Freescale for lower-power versions of the company's MPC 8641/8641D PowerPCs. The result was the 27 percent lower-power MPC 8640/8640D. Mounted on GE Fanuc's 6U VME VG6, users can configure the SBC with one or two 8640s, as well as 8641s or 8641Ds (for legacy compatibility or configuration-managed programs).

Each CPU node can be equipped with 2 GB of DDR2 ECC memory, with an x8 PCI Express adapter between nodes. There's a total of five Ethernet ports (three Gbps; two 10/100 Mbps), two SATA ports, four serial ports, and six USB 2.0. extension slots provide for PMC/XMC. As well, GE Fanuc's DSP220 VXS and DS230 VPX boards can be equipped with MPC 8640/8640D processors.

GE Fanuc Intelligent Platforms • www.gefanucembedded.com • RSC# 39001



CWCEC's first packaged COTS subsystem

A handful of rugged COTS vendors has discovered the advantages of offering fully populated and configured subsystems: it proves credibility, it's easy to modify to suit the customer, and it hastens the customer's development cycle. The MPMC-9350i (Intel) and -9350p (PowerPC) Multi-Platform Mission Computer (MPMC) series from Curtiss-Wright Controls Embedded Computing (CWCEC) are the company's first *Packaged COTS* (PCOTS) mission computers. Housed in a conduction-cooled five-slot CompactPCI chassis, the MPMC is targeted for ground vehicles, helicopters, and UAVs.

The box is rugged, having passed DO-160E environmentals for Airborne equipment, plus shock, vibration, ESD, and all the other "ilities" we've come to expect from CWCEC. The 10.72" x 5.11" x 7.62" (L x W x H) box uses three PowerPC 7448 SBCs (DCP-124 and DCP-124P) or three Intel Core 2 Duo SBCs (DCP-1201 and 1201P) with more I/O than we have room to describe. A typical stack-up includes: a Slot 1 CompactPCI system controller with dual 1553 channels; Slot 2 with 32 ARINC-429 channels; Slots 3 and 5 for video; and Slot 4 reserved for the SBCs with PMC mezzanines. Though CWCEC's not the first to offer a prepackaged CompactPCI mission computer, their MPMC is surely the best equipped.

Curtiss-Wright Controls Embedded Computing
www.cwcembedded.com • RSC# 38999

It's harsh, but "contact me"

What fails first on your cell phone – the phone itself, or that flimsy little connector that recharges it? Although not as spiffy as multicore CPUs or safety-critical software, the lowly connector can become a critical failure point in any system. And when we're talking about the harshest environments on, below, or off the planet, durable high-temperature contacts become mission critical. With 100,000+ mating cycles, low insertion/extraction, and superior reliability, the HTT Series from Hypertronics is designed to withstand temperatures from -65 °C to a blistering +400 °C.

Target applications include *extremely harsh environments* such as rocket, jet and turbine engines, industrial machinery, oil and gas exploration, and of course, military. The patented wire basket hyperboloid design creates a 360-degree wiping action, resulting in multiple contact points and "extremely high immunity to shock and vibration." Suffice it to say, these HTT Series contacts are tough.

Hypertronics Corporation • www.hypertronics.com • RSC# 38997

Continued on page 34

Application instrumentation: Linux-based event recording for multiprocessors

Both Microsoft and Intel are on record as stating software is going to be the number one impediment to fully utilizing multicore processors in today's desktop systems. But rewind back a few years, and before there were multicore CPUs, there were multiprocessor defense systems. Vendors such as SKY Computers learned long ago how to write code, debug, and optimize software spread across dozens and hundreds of processing nodes. The concept of "instrumenting the application" is the basis for SKY's TimeTrac performance optimizing software for Linux-based multiprocessing systems. The dynamic tool is used for fine-tuning and debugging multiprocessor (and multicore) systems.

Originally designed as an in-house tool for SKY's programmers but now available as a COTS package, TimeTrac is also used to measure and optimize algorithm development, modifications, and ultimately system deployment. Through an easy-to-use viewer that minimally intrudes on the application code, key functions include: discovery of application loading and where the system is bogging down; visibility into race conditions; algorithm speedups; processor/node loading idenfication; communication and semaphore synchronization; and visibility into *infrequent* runtime problems. In true COTS fashion, the software is downloadable and can be ordered via PayPal.

SKY Computers • www.skytimetrac.com • RSC# 39000

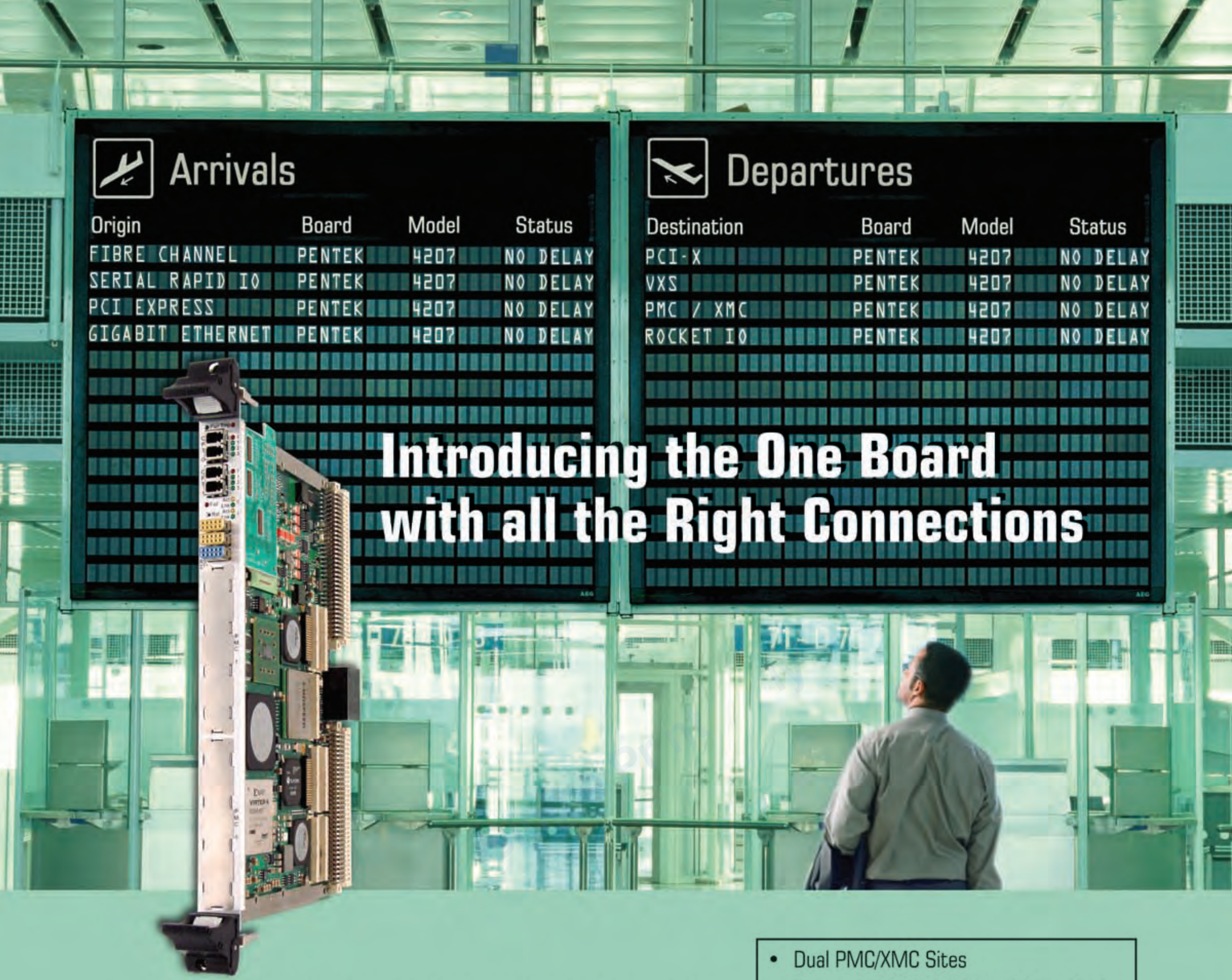
Panoramic IR camera does it all

C4ISR on the battlefield is often supplemented by less-than-stellar local surveillance to protect one's own bivouac. At best, single wide-angle optical or IR cameras provide limited Field Of View (FOV), leaving soldiers and Marines partially exposed. The IR Revolution 360 from HGH Infrared Systems is designed to present a 360-degree view with intrusion detection from up to 3 miles away. This single unit can often replace several single- or dual-head cameras set to pan, tilt, or zoom with a fixed FOV.

With an IR resolution of an equivalent 8-12 megapixels, "blobs" can be resolved as threats or merely wildlife. The completely passive camera emits no light and produces a complete 360-degree scan every second, providing near real-time detection and tracking. Data connection is via COTS Ethernet, making setup quick and simple via a point-and-click Windows interface (which doubles as a remote control). The French manufacturer, HGH Infrared Systems, is exclusively represented in America by IRCameras.

HGH Infrared Systems (via IRCameras)
www.ircameras.com
RSC# 37764

Continued on page 37


Arrivals
Origin Board Model Status
FIBRE CHANNEL PENTEK 4207 NO DELAY
SERIAL RAPID IO PENTEK 4207 NO DELAY
PCI EXPRESS PENTEK 4207 NO DELAY
GIGABIT ETHERNET PENTEK 4207 NO DELAY
Departures
Destination Board Model Status
PCI-X PENTEK 4207 NO DELAY
VXS PENTEK 4207 NO DELAY
PMC / XMC PENTEK 4207 NO DELAY
ROCKET IO PENTEK 4207 NO DELAY
Introducing the One Board
with all the Right Connections

Targeting high-performance I/O and processing applications, the Model 4207 delivers an on-time solution for your real-time application using the latest high-speed serial interfaces.

On board PowerPCs, FPGA, PMC/XMC sites, and extensive memory resources are connected to the industry's fastest interfaces including VXS, Gigabit Ethernet and dual Fibre Channel ports for high-speed recording.

All board resources and interfaces are joined through a configurable zero-latency crossbar switch using protocol-transparent gigabit serial data paths.

With so many connections to choose from, you are bound to find just what you need for your next system.

- Dual PMC/XMC Sites
- Freescale MPC8641D Dual Core AltiVec PowerPC Processor to 1.5 GHz
- XC4VFX60 or XC4VFX100 FPGA
- 4 GB DDR2 SDRAM
- PCI Express, Serial RapidIO™, RocketIO™
- Dual Gigabit Ethernet Ports
- Dual 4 Gbit Fibre Channel Interface
- Fabric-transparent Gigabit Crossbar Switch
- VXS, VME64x, Gigabit Ethernet-X
- Linux and VxWorks Support
- ReadyFlow® Board Support Libraries
- GateFlow® FPGA Design Resources

Call today to have it all!
201-818-5900 or go to
www.pentek.com/go/mesconnect for the
4207 brochure, technical datasheet
and to request pricing.

ISO 9001:2000
CERTIFIED QUALITY MANAGEMENT SYSTEM

PENTEK
Setting the Standard for Digital Signal Processing

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

- . Ultra DMA Mode 6 Support
- . Compliant Compact Specifications
- . No Seek Error No Noise
- . Low Power Consumption
- . Shock Resistant & Anti-vibration
- . No Latency Delay
- . RoHS
- . Form Factors in 1.8"/2.5"
- . SATA I,SATA II, IDE and ZIF Interface
- . SLC/MLC Flash IC Technology

Wide Temp.
-40 degree~+85 degree

The Flash Storage Leader

On Sale!

MLC 2.5"/1.8" SATA SSD
Capacity: 16GB~128GB

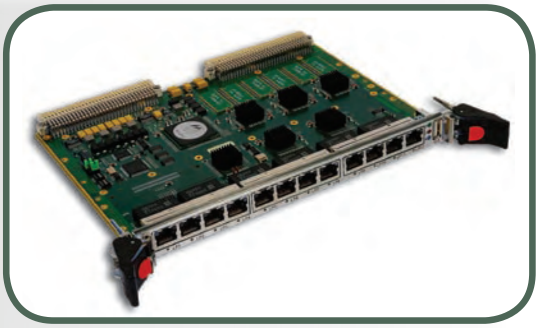
MLC 2.5"/1.8" SATA SSD
Capacity: 16GB~128GB
SATA Interface:22 Pins
Read: 114MB/Sec.
Write: 38MB/Sec.

SLC 2.5"/1.8" WIDE TEMP.
SATA/IDE SSD
Capacity: 8GB~64GB
SATA Interface:22 Pins
IDE Interface: 44pins
Read: 118MB/Sec.
Write: 63 MB/Sec.

PQI Corporation
Tel:(510)651-7281
Fax:(510)651-7240
For information, please contact:
dom@pqimemory.com
Learn more at: www.pqimemory.com

pqi

No Ethernet rack? Try this 24-port VME switch



If your defense system can accommodate a 19" rack, your choices for COTS Ethernet switches are abundant. But if you need to deploy your switch in really rough terrain, then VME is likely your form factor of choice. Now you can take your Ethernet and VME on the road with Concurrent Technologies' FP 210/024 24-port managed Ethernet switch. Designed for time-critical voice, video, and data, the Marvell Prestera 98DX240-based 6U card routes 12 ports to the front panel and 12 to P2. There's even an optional rear transition module with 12 RJ45s on it.

Consuming less than 20 W and available in wide temperature and conduction-cooled versions, each port is 10/100/1000 Mbps. Moreover, two of the front panel's ports can be rigged for optical Ethernet connections. The switch's core supports wire-speed and Layer 2 QoS switching and can learn and cache for up to 8192 MAC addresses. Four hardware priority queues are available per port, and the FP 210/024 supports port ID, MAC address, IEEE 802.1p, IEEE 802.1Q, IPv4, and IPv6.

Concurrent Technologies • www.gocct.com • RSC# 38998

Got an analog waveform to test?

The real world is analog; all this digital stuff is just a convenient way of examining or manipulating it – and even hard-core analog test engineers still need digital computers for analog signal analysis and development. One way to accomplish this is to use WaveEasy from Geotest. The analog waveform development software runs on the company's GX1110 or other third-party arbitrary waveform generators.

Sporting over 40 functions and operators for various waveform file formats, the tool is designed to interactively edit and create analog waveforms in WaveEasy, ASCII (txt, csv, prn), or NI-HWS formats. Line or freehand drawings can be used to create the waveform before mathematical functions turn curves and segments into algorithmic representations. Noise, filters, and other attributes can also be added. Once the waveform has been realized, it can be transferred from the EasyView development environment into ATEasy, LabVIEW, LabWindows/CVI, or Microsoft Visual Studio – or plugged into your favorite waveform generator. Operators include Add, Subtract, Multiply, Divide, and Exponent. There are also math and trig functions such as Ln and Log, COS/SIN/TAN, and various filter types.

Geotest-Marvin Test Systems
www.geotestinc.com
RSC# 38996

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.

Software as a product line offers the right benefits to long life-cycle military programs

By Chris A. Ciufo, Editor

It's only been in the past five years that Eclipse and Linux evolved from novelties and "Ridiculous!" by opponents, into *de facto* products in defense system development and deployment. They started out as grassroots movements to fulfill a need: In the case of Eclipse, it was to create a standard framework for development tools; in the case of Linux, it was to break the control of proprietary operating system companies. Today, you can't buy a mainstream COTS toolset that doesn't offer Eclipse plug-ins. And you'd be hard pressed not to find some Linux floating around in *every* military program – either during the IRAD stage or actually deployed in-system. The same will happen with *software as a product line,* a methodology that governs conception, creation, testing, deployment, and code sustainment.

> "[SPLE] methodology … governs conception, creation, testing, deployment, and code sustainment."

At September's Software Product Line Conference (SPLC) in Ireland, a panel session chaired by BigLever Software was held, addressing the emerging trend of Software Product Line Engineering (SPLE). Simply stated, SPLE is a methodology for creating software – requirements, code, test procedures, maintenance, and all related attributes. It's easiest to understand what *software as a product line* is *not*: It's not a one-off, shrink-wrapped implementation of software intended for single use or one product. According to John Carrillo, senior director of corporate and product strategy at Telelogic (an IBM company), it "takes into account how to manage the pieces and variability over the entire life cycle." More specifically, *product line* implies several members of a family, including future versions, variants, and as-yet-unimagined features.

This long view of software and the entire ecosystem that goes into creating it sounds like something written in a DoD operations manual or a MIL-SPEC SCD. In fact, the SPLE definition was born in the civilian software marketplace but is so military-sounding that it reads like our magazine's tagline: "COTS and technology for the entire military life cycle." Major defense prime contractors have already noticed this in a big way. Boeing is on record as endorsing this kind of methodology.

So too has Lockheed Martin's Maritime Systems and Sensors (MS2) division. The benefit of SPLE to MS2, according to James Cezo, principal member engineering staff, is "Reuse. This allows us a way to reuse existing assets and customize them for new customers and markets." To be sure, this is how Lockheed Martin (like most prime contractors) has always done business. A good portion of its defense systems are actually features located in software that's run on program-specific hardware. Software was effectively cloned, then dropped into a new program, hardware, and sensor. From there, it was modified to meet the program's ORD.

But *software as a product line* emphasizes a way to write the code for intentional reuse from the very start, maximizing reuse while reducing cost and providing an orderly way to manage variations from A, to B, to C. Effectively, says Bola Rotibi, principal analyst with Macehiter Ward-Dutton, the software can be written for the "whole world" using the SPLE methodology. Her IT-focused market analysis company thinks this is early days for this way of writing software, but it's likely growing into such a groundswell of best practices that it will become commonplace and second nature within only a few years. Her firm is conducting extensive research on the trends, publishing analyst reports, and planning to advise its clients on the best ways to recoup software reuse.

Ironically, there are no *formal* standards adopted yet for SPLE, though Telelogic and BigLever Software are collaborating to write some. The Software Engineering Institute is also working in this area, but BigLever and Telelogic are approaching the task like IBM did with Eclipse: first developing collaborative tools that solve real problems that people can use – instead of just a set of ideological specs. According to Charlie Krueger, founder of BigLever, the next steps are 1) standards; 2) best practices; and 3) an interoperable framework.

For sure, *software as a product line* is still at the *innovator stage;* however, I'm confident that the military community will find this so compelling that they'll provide some much-needed momentum to the effort. After all, writing software for the long haul is 100 percent in-phase with our way of military life-cycle thinking.

It says so, right on the cover of this magazine.

Chris A. Ciufo

Chris A. Ciufo
Group Editorial Director
cciufo@opensystemsmedia.com

For more information from BigLever on these concepts, check out the articles in the *Military Embedded Systems* archive at: www.mil-embedded.com/articles/search/index.php?op=cn&max=10&q=biglever.

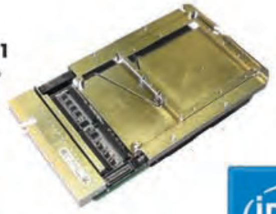
HIGH PERFORMANCE PROCESSING THAT KEEPS ITS COOL

Curtiss-Wright's rugged Intel® Core™2 Duo processor SBCs take performance per Watt to a whole new level. Our 6U VME S/DMV-1901 and 3U CompactPCI SCP/DCP-1201 compute engines raise the bar for dual core X86 processing performance in space, weight and power limited environments. When heat is the enemy and low power is the target, Curtiss-Wright's Intel® processor-based SBCs are the solution.

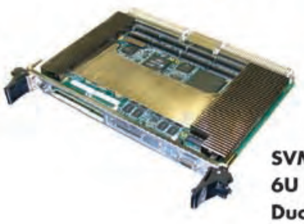
We ship the 1201 and 1901 with an optimized BIOS that lets users "park" one of its dual cores when unneeded to cut heat dissipation and lower power consumption. Going further, we enable optional processor downshifting, reducing the processor speeds down to 1 GHz, enabling high performance operation with even less power usage. Our Intel® Core™ microarchitecture boards' low-power mode performance goes beyond surprising. The 1201 runs as low as 18 Watts on a single core, and the 1901 can run under 30 Watts. Uniquely, Curtiss-Wright's VME 1901 provides support for 320 Mbytes/sec VME320 under Windows® XP Embedded. And our custom driver fully supports most VME320 modes for higher data bandwidths. There's more: To Windows, add VxWorks,™ LynxOS,® and Linux™ support. And there's Solaris™ 10 for applications requiring global security certification. But that's not the whole story. We've also optimized system expansion, too. With Intel® multi-core processors and exceptional memory bandwidth, the 1901 and 1201 deliver the industry's highest PMC/XMC expansion card data transfers in their given form-factor.

Whether, controlling software radios on UAVs or anti-submarine warfare avionics simulators on maritime patrol aircraft, Curtiss-Wright's Intel Core microarchitecture SBCs deliver awesome performance per Watt.

SCP/DCP-1201
3U CPCI Intel®
Core™2 Duo
Processor



intel
Embedded and
Communications
Alliance



SVME/DMV-1901
6U Intel® Core™2
Duo Processor

The SVME/DMV-1901 supports one 1.5 GHz Intel® Core™2 Duo processor. It acts as a dual CPU 6U VME320 board. The SCP/DCP-1201 is a multifunctional Intel Core 2 Duo processor 3U CompactPCI board. Add a SCSI, SATA, or USB hard drive and these boards become full-featured computing platforms.

CURTISS
WRIGHT Controls
Embedded Computing

Innovation In Motion.
cwcembedded.com

DUAL CORE x86 SBCs... ABOVE & BEYOND