

Military

EMBEDDED SYSTEMS

INCLUDING **DEFENSE TECH WIRE**

John McHale

Year-end budget uncertainty

Field Intelligence

RX for heart-healthy networks

Mil Tech Insider

VICTORY = COTS integration revolution

Legacy Software Migration

Migrating systems of systems
Gordon Hunt, RTI

Nov/Dec 2012
Volume 8 | Number 8

MIL-EMBEDDED.COM



Delivering
smartphones
to the warfighter



Big-screen biometric apps, stand aside:
Off-the-shelf smartphones enable rapid suspect ID for warfighters, intelligence ops
Q&A with Paul Schuepp, President and CEO of Animetrics



Enterprise
software and
the DoD

Opensystems Media
PAID
U.S. POSTAGE
FIRST STD

ELECTRONIC SERVICE REQUESTED

30233 JEFFERSON, ST. CLAIR SHORES, MI 48082

www.opensystemsmedia.com

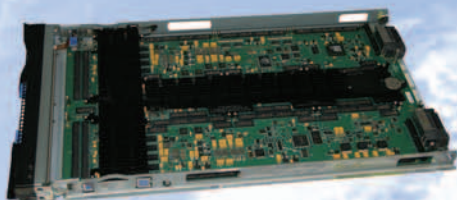
Annapolis Micro Systems

The FPGA Systems Performance Leader

High Performance Signal and Data Processing in Scalable FPGA Computing Fabric

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

***Direct Seamless Connections with no Data Reduction
Between External Sensors and FPGAs
Between FPGAs and Processors over IB or 10GE
Between FPGAs and Standard Output Modules
Between FPGAs and Storage Arrays***



Ultimate Modularity

**From 1 to 8 Virtex 4, 5 or 6 FPGA/Memory Modules
Input/Output Modules Include:**

**Quad 130 MSPS thru Quad 550 MSPS A/D
1.5 GSps thru 5.0 GSps A/D, Quad 600 MSps D/A,
Dual 1.5 GSps thru 4.0 GSps D/A
Infiniband, 10G, 40G or 100G Ethernet or SFPDP**

VME/VXS/VPX, IBM Blade, PCI-X/PCI Express, PMC/XMC, MicroTCA

**No Other FPGA Board Vendor Streams This Volume of Data
Real Time Straight Into the Heart of the Processing Elements
and Then Straight Back Out Again**

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

SynQor

Uninterruptible Power Supply



Sealed

Rugged

Smaller

Lighter

*More
Powerful*

- ▶ **Power 1U: 1250W/1500VA**
- ▶ **Weather-proof, shock-proof construction**
- ▶ **True on-line double conversion**
- ▶ **1U high rack mount (17" x 21.6" x 1.73")**
- ▶ **Low weight — 32 pounds**
- ▶ **Dual input (AC and DC)**
- ▶ **Battery run time >10 minutes @ full load**
- ▶ **Removable battery pack**
- ▶ **Full power operation: -20°C to +55°C**



Made in the United States of America.

1-978-849-0600 www.SynQor.com



SynQor[®]

ON THE COVER:

Top photo: During the Army's Nett Warrior demonstration, warfighters used smartphones and tactical radios together to transmit voice, video, and data over a secure network. Photo courtesy of the U.S. Army

Bottom Art: An aerial view of the Pentagon, photo by David B. Gleason



November/December 2012 | Volume 8 | Number 8

COLUMNS

Editor's Perspective

- 8 Year ends with more budget uncertainty
By John McHale

Field Intelligence

- 10 Software RX for heart-healthy networks
By Charlotte Adams

Mil Tech Insider

- 11 U.S. Army's VICTORY ushers in the next COTS integration revolution
By Steve Edwards

Legacy Software Migration

- 12 Easing legacy migration in Systems of Systems
By Gordon Hunt, RTI

DEPARTMENTS

- 14-15 Defense Tech Wire
By Sharon Hess

E-CAST

<http://ecast.opensystemsmedia.com>

Securing Android Against Cyber Attacks

December 6, 2012, 2:00 p.m. EST

Presented by Wind River

Watch archived E-casts on demand:
ecast.opensystemsmedia.com

WEB RESOURCES

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

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

Published by: 

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

© 2012 OpenSystems Media
© 2012 Military Embedded Systems
ISSN: Print 1557-3222

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



SPECIAL REPORT | Enterprise software for defense applications

- 16 Enterprise software and the DoD
By John McHale



MIL TECH TRENDS | Smartphone tech for mil applications

- 20 Smartphones on the battlefield
By John McHale
- 26 Big-screen biometric apps, stand aside:
Off-the-shelf smartphones enable rapid suspect ID for warfighters, intelligence ops
Q&A with Paul Schuepp, President and CEO of Animetrics

INDUSTRY SPOTLIGHT | Managing component obsolescence

- 32 Life cycle management: The COTS perspective
By Mark Grovak, Curtiss-Wright Controls Defense Solutions
- 36 Software compounds the challenges of military component obsolescence
By Colin Doyle and Stephen Denman, PTC
- 40 Obsolete components: What is the COTS life cycle costing you?
By Kaye Porter, GDCA
- 44 Managing the military component obsolescence paradox:
When new performance levels are needed after EOL
By RJ McLaren, Kontron America

 @military_cots

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

The image shows a black, rectangular environmental test chamber. It features a top handle and two large circular ports on the front face, each with a mesh screen. The side of the chamber is covered in a repeating pattern of text listing various MIL-STD-810F test methods, including Humidity, Radiated Emissions, Shock, and Temperature. The text is printed in white and black, creating a high-contrast, repeating pattern that covers the entire side of the unit. The background is a solid blue color.

X-ES systems are fully flight qualified to MIL-STD-810, MIL-STD-461, MIL-STD-704, and DO-160 specifications. We design, develop, manufacture, test, and support the systems and perform qualification under one roof in the U.S.



Extreme Engineering Solutions
608.833.1155 www.xes-inc.com

ADVERTISER INFORMATION

Page	Advertiser/Ad Title
33	ACCES I/O Products, Inc. – USB embedded I/O solutions – rugged, industrial strength USB
39	Aitech Defense Systems – Our technology investments protect yours
2	Annapolis Micro Systems, Inc. – High performance signal and data processing
30	Chassis Plans – Your configuration – one part number
29	Connect Tech, Inc. (CTI) – New COM Express Type 6 carrier boards
7	EADS North America – You make the mission critical systems
9	Elma Electronic – Small is the new big
35	Esterline Communication Systems – Eclipse electronic systems
17	Excalibur Systems, Inc. – Dragon – it's not a myth
23	Galleon Embedded Computing – Secure rugged storage
47	GE Intelligent Platforms, Inc. – You can't see them – but there are 300,000 people standing behind this display
31	Innovative Integration – Black beauty
27	Interface Concept – Switches and IP routers
34	Microhard Systems, Inc. – Wireless digital data link
42	Parvus Corporation – Qualified to perform
30	PC/104 Consortium – Maintaining and distributing PC/104 specifications
48	Pentek, Inc. – Got tough software radio design challenges?
38	Phoenix International – Solid or Spin ... we go both ways
43	Schroff Pentair – ATCA, μ TCA, VME and VPX systems ... faster
34	SDR Forum – SDR – WinComm
13	SIE Computing Solutions, Inc. – Rugged and ready when you are
3	SynQor – Uninterruptible power supply
18	Thermacore International, Inc. – Performance advantages in the world's hottest spots
25	WinSystems, Inc. – High performance Atom SBCs small and fanless
5	X-ES – Fully flight qualified
21	Z Microsystems, Inc. – Experience unprecedented clarity

Military

EMBEDDED SYSTEMS

OpenSystems media.

Military Embedded Systems Editorial/Production Staff

John McHale, Editorial Director
jmchale@opensystemsmedia.com

Sharon Hess, Managing Editor
sharon_hess@opensystemsmedia.com

Steph Sweet, Creative Director
ssweet@opensystemsmedia.com

Sales Group

Tom Varcie
Senior Account Manager
tvarcie@opensystemsmedia.com

Rebecca Barker
Strategic Account Manager
rbarker@opensystemsmedia.com

Eric Henry
Strategic Account Manager
ehenry@opensystemsmedia.com

Ann Jesse, Strategic Account Manager
ajesse@opensystemsmedia.com

Christine Long
Vice President, Online Business
clong@opensystemsmedia.com

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

Gerry Rhoades-Brown
Account Manager – Europe
gerry.rhoadesbrown@husonmedia.com

Regional Sales Managers
Barbara Quinlan, 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

Reprints and PDFs

republish@opensystemsmedia.com

OpenSystems Media Editorial/Production Staff



Mike Demler, Editorial Director
DSP-FPGA.com
EDA Digest
mdemler@opensystemsmedia.com

Joe Pavlat, Editorial Director
CompactPCI, AdvancedTCA,
& MicroTCA Systems
jpavlat@opensystemsmedia.com

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

Warren Webb, Editorial Director
Embedded Computing Design
Industrial Embedded Systems
wwebb@opensystemsmedia.com

Jennifer Hesse, Managing Editor
Embedded Computing Design
Industrial Embedded Systems
jhesse@opensystemsmedia.com

Sharon Hess, Managing Editor
VITA Technologies
sharon_hess@opensystemsmedia.com

Monique DeVoe, Assistant Managing Editor
PC/104 and Small Form Factors
DSP-FPGA.com
mdevoe@opensystemsmedia.com

Brandon Lewis, Associate Editor
CompactPCI, AdvancedTCA,
& MicroTCA Systems
blewis@opensystemsmedia.com

Curt Schwaderer, Technology Editor

Steph Sweet, Creative Director

David Diomede, Art Director

Joann Toth, Senior Designer

Konrad Witte, Senior Web Developer

Matt Jones, Web Developer

Editorial/Business Office

Patrick Hopper, Publisher
Tel: 586-415-6500
phopper@opensystemsmedia.com

Subscriptions Updates
Karen Layman, Business Manager
www.opensystemsmedia.com/subscriptions
Tel: 586-415-6500 ■ Fax: 586-415-4882
30233 Jefferson, St. Clair Shores, MI 48082

Rosemary Kristoff, President
rkristoff@opensystemsmedia.com
Wayne Kristoff, CTO

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



You make the mission critical systems.

We make sure they work.

Our state-of-the-art test solutions and top-tier engineering expertise provide everything you require to ensure the exact operating condition of your system. We team with you to create the right solution, from COTS to fully customized. Our invaluable support ensures you have exactly what you need, when you need it. That is the EADS North America Test and Services difference.

- COTS Test Products
- Test Software
- Turnkey Solutions
- Custom Test Products
- Integration
- Life Cycle Support

To find out more, visit our website at www.ts.eads-na.com
or call 800-722-2528.

EADS
NORTH AMERICA

Year ends with more budget uncertainty

By John McHale, Editorial Director



This past year has been a stressful, nerve-racking one for many in the defense electronics community. Their main customer – the Department of Defense (DoD) – is making major cuts to its budget and the threat of sequestration promises to cut another \$600 billion in defense funding.

The latter would result in thousands and thousands of defense industry jobs being cut. Most would be at the prime contractor and system integrator levels, as the cuts from sequestration would hit major programs and platforms.

As I write this, the Administration, Senate, and House are not creating a lot of public confidence that they can avoid the fiscal cliff – not having a balanced budget by Jan. 1, 2013 – which then triggers automatic sequestration. For an understanding of the government's negotiations on the budget deficit, entitlements, and taxes, I highly recommend Bob Woodward's latest book, "The Price of Politics." It retells how the government avoided default last year and gives an understanding into the key issues the three bodies are negotiating today, as they are pretty much the same. Obama and the Senate Democrats are insisting on raising tax rates for the rich, while the Republican-led House refuses to budge unless there are major entitlement cuts to programs such as Medicare and Medicaid.

I find the continued rhetoric on raising taxes for the richest Americans to be just ridiculous at this point. Even if they did, the revenue wouldn't be anywhere near what is needed to solve the deficit, yet the Democrats are pushing fiction by claiming it will make the difference. They refuse to cut anything without the rate increase.

A scene from Woodward's book captures this dynamic well. It is an exchange

between Republican Sen. Jon Kyl from Arizona and Gene Sperling, Director of the National Economic Council. During one negotiation, Kyl said to Sperling: "So you're saying to me that even though there are Medicare savings that you think are reasonable – that we could do – you won't do them unless we're going to raise taxes on somebody?" Sperling replied: "Well yeah. We can't agree to any of your stuff without any of our stuff."

■ ■ ■

"As I write this, the Administration, Senate, and House are not creating a lot of public confidence that they can avoid the fiscal cliff – not having a balanced budget by Jan. 1, 2013 – which then triggers automatic sequestration."

■ ■ ■

Despite this nonsense, my gut is telling me Congress will come up with some sort of deal to either avoid sequestration or push it off to the next Congress, and do it so they can get home for the holidays. So either I'm psychic or just hopeful. We'll probably know by the time you read this.

Much of our content in 2012 has touched on these issues and how they will not only affect the big boys at the primes, but the third party Commercial Off-the-Shelf (COTS) suppliers. The COTS folks are much more optimistic than those at the first or second tiers. They see the government looking to require more open standards and COTS

technology and fund nondevelopmental items. However, this same environment means the government will be at the whim of commercial market cycles more than ever.

Program managers working on smartphone technology (see page 20) and enterprise software (see page 16) are already facing the headaches of trying to get hardware and software certified to government standards before their device or operating system goes obsolete. They're having a hard time keeping up.

"The problem is a company like Apple can write a complete new operating system in less time than it takes the Defense Information Systems Agency (DISA) to generate a certification standard for the older operating system," says Bill Toti, VP at The HP NGEN Alliance, who also lends insight in our Special Report on enterprise software on page 16. "By the time they certified iOS 5 [for use in the Navy Marine Corps Intranet], it was already out of production and iOS 6 was being introduced. We keep chasing our tail because the current government process cannot adjust to a technical environment that moves at the speed of Moore's law. We could have gotten iPhones to the whole fleet two years ago if not for policy. Technology is easy, policy is hard."

Policy is hard, but covering the technology that supports our armed forces is a privilege. Thanks for reading and supporting *Military Embedded Systems* this past year. Have a wonderful holiday, and be sure to thank an airman, sailor, soldier, or Marine for their service if you get a chance this season. They deserve it. We will see you next with our Jan/Feb 2013 Radar Guide edition.

John McHale
jmchale@opensystemsmedia.com

Small is the New **BIG**!



We all know good things come in small packages.

Our Mini ATR design leverages Elma's proven COTS rugged construction techniques, yet delivers a smaller, lighter platform for space & weight constrained projects. It accommodates a wide range of embedded COTS architectures and payloads. It allows for DC and AC power variations, and custom I/O configurations.

One configuration combines a 3-slot OpenVPX™ backplane, and the option for a plug-in power supply and 2.5" storage tray. Elma will design the MIL-STD wiring and connectors specifically for your I/O needs. We can also help you with the payload — processors, audio/video, storage, you name it, we've got it. Elma is teamed with premier industry partners to provide the best solution for your application development needs.

Elma offers hundreds of system configurations using best in class products — from the backplane, to the SBC and storage, to high-end FPGA and GPGPU processors all integrated and tested from the one partner who pays attention to the smallest details.

ELMA
Your Solution Partner

Learn why the smallest details matter to Elma by visiting www.elma.com.
Or by contacting us at **510.656.3400** or **sales@elma.com**.

Software RX for heart-healthy networks

By Charlotte Adams

A GE Intelligent Platforms perspective on embedded military electronics trends



Internet Protocol (IP) switches and routers make up the heart of the Internet. Military network architects use this commercial technology for everything from base-to-base communications to tactical battlefield networks that connect soldiers, sensors, and weapons. But because the technology behind network equipment – even rugged, embedded products – is based on components developed for the commercial market, innovation is driven by demand for products like mobile devices, not by the wishes of niche customers like the U.S. military. Luckily for them, however, there's more to a switch than just hardware. At the end of the day, it's software that gives switches their character and determines their level of flexibility, security, and longevity.

Software brains

What differentiates one network device from another and makes some devices suitable for a wide range of applications is not the hardware nuts and bolts but the more adaptable software inside.

Switch management software controls the configuration, interoperability, addressing, monitoring, protection, supportability, and overall performance of the hardware. Ideally, the software is flexible and customizable enough to cover all corners, easy to use, secure, and backed by the latest tools and expertise. But that's a tall order in today's computing market.

Bridging two worlds

The military seeks to exploit COTS hardware and software and commercial standards to reduce costs and deployment time. But the specialized nature of military applications, sensitivity of the information, and the sheer number and diversity of the nodes mean that this customer often needs standards modified in order to get the job done.

In an intelligence application, for example, the military might want to harden a data link that collects video feeds from a reconnaissance drone. This might involve modifying a standard protocol slightly – in some small portion of the network – to make the link harder to hack. But this can introduce interoperability issues with other network equipment. Or a user with a large amount of time-critical data, implementing link aggregation on the network, might not tolerate any bandwidth reduction caused by the failure of a single link. But link aggregation methodology can be customized so that a network bandwidth reduction triggers a complete failover to backup link aggregations, maintaining bandwidth.

Addressing these issues at the hardware level can be costly and time consuming. And such one-of-a-kind requirements are obviously difficult to satisfy using commercial chips. In addition, the network equipment and network management software

Figure 1 | The NETernity GBX460 fully managed rugged 6U OpenVPX data plane switch module features GE's OpenWare switch management software.



might be supplied by multiple vendors, making any modification a complex and often unrewarding process.

Flexibility, the key

Network equipment that incorporates agile and flexible management software from a vendor who understands both commercial and military network applications can bridge the gap between the military and commercial worlds. It also presents a single face to the user for both hardware and software issues and requirements. OpenWare, a Linux-based switch management environment developed by GE Intelligent Platforms, provides the flexibility and depth of support required to serve both niche and commercial markets (Figure 1). The open source foundation to GE switch products also gives access to the wealth of tools and protocols maintained by Linux developers worldwide. This software, in turn, can be customized to meet application requirements.

Security

Switches can provide security features such as mandatory access control, denial of service protection, integrity checks, and filtering of traffic from untrusted domains. Access control can target switch ports, allowing the network administrator to limit dynamic connections and log switch violations. And dynamic address resolution protocol protection guards against spoofing attacks that could bring down the network.

Switches also can offer backup protection. The software can allow users to take one or multiple "snapshots" of a configuration, save them, and later recapture the desired configuration if it becomes necessary during switch debugging or if a switch is reassigned to a different mission, network, or geographic location.

Obsolescence

Switch management software can even combat obsolescence. If the software is tunable enough, a new switch can be programmed to mimic an out-of-production unit in a way that is transparent to other nodes and even to higher-level software and tools. Drop-in replacements of switching hardware can extend the life of military networks and significantly reduce maintenance costs.

defense.ge-ip.com

U.S. Army's VICTORY ushers in the next COTS integration revolution

By Steve Edwards
An industry perspective from Curtiss-Wright Controls Defense Solutions



Bringing state-of-the-art commercial silicon performance to deployed systems for rugged military environments can involve conflicting goals. Designers want the highest performance, but also need to design to the limits of the available space, weight, and power constraints. And the market realities of price and affordability can't be ignored. Applications and processor performance continue to expand in terms of complexity and compute power, but the space available inside of ground combat vehicles is not becoming any larger. In fact, space is always a premium, with electronic components competing for limited room with such other critical resources as ammunition storage. Limited space plus higher-performance electronics equal greater challenges for thermal management. Adding more subsystems, without a shared digital network connecting them, fosters redundancy, which eats up even more of the already limited available space.

The U.S. Army's Vehicular Integration for C4ISR/EW Interoperability (VICTORY) initiative takes aim at these problems by defining an approach for commonality through GbE networking, standard connectors, and well-defined electrical interfaces. In the U.K., the GVA initiative is doing similar work. Today, there is a groundswell of activity to bring the benefits of a digital backbone, to foster interoperability and commonality and shared data to make the warfighter more effective while reducing functional redundancies; such redundancies include the multiple GPS units that result from the proliferation of "stovepipe" systems. Even better, in an era of constrained defense budgets, these initiatives also promise to help drive affordability. Here's how.

Learning from the commercial world

In 2007, Steve Jobs, giving his annual Macworld keynote speech, said, "Today, we're introducing *three* revolutionary new products. The first one is a widescreen iPod with touch controls. The second is a revolutionary new mobile phone. And the third is a breakthrough Internet communications device." He then went on to clarify, "An iPod, a phone, an Internet mobile communicator. An iPod, a phone, an Internet mobile communicator ... These are *not* three separate devices! And we are calling it *iPhone!*"

What Apple had done was recognize that advances in silicon – such as low-power ARM processors – could enable the integration of multiple functions into a single compact unit. Similarly, VICTORY can help create a revolution in subsystem design for performance-hungry but space-constrained ground vehicles. Using adjacent market technologies such as ARM processors designed for the automotive market and network switches from the telecommunications market – to develop small, lightweight, rugged processor units that cost-effectively deliver multiple

Figure 1 | Curtiss-Wright Controls Defense Solutions' Digital Beachhead, an ARM-based, VICTORY-compliant unit



functionalities – eliminates redundant GPS units; it also eliminates redundant video displays, keyboards, and so on, because data, previously stovepiped, is shared over the common digital network. And this revolution doesn't end inside the vehicle. VICTORY encourages interoperability across ground vehicle platforms. The result with VICTORY: real-time exploitation of shared data ... mitigated SWaP constraints ... reduced costs.

One example of a VICTORY-compliant technology is Curtiss-Wright's Digital Beachhead, a compact subsystem that brings digital networking and advanced processing services to ground combat vehicles (Figure 1). This integrated VICTORY backbone solution features GbE switching and routing, along with a VICTORY data bus, and management and shared services (such as shared GPS data) to quickly and easily integrate the VICTORY architecture into any vehicle. Its high-speed network architecture enables resource sharing, eliminates redundancy, and reduces weight and power. An integrated Vehicle Management computer with HUMS/CBM+ system health services is provided.

VICTORY points the way

Innovation comes from constraints. The need for more processing power, communications, and functionality will only increase over time. With those demands comes more heat to dissipate. Where will the space for these systems come from inside the already overburdened vehicles? The solution for addressing these constraints is probably already in your pocket. COTS has always been about leveraging best-of-breed ideas from adjacent markets. With VICTORY-compliant systems that leverage best-of-breed hardware and software, it's possible to deliver optimal performance and functionality in an extremely low-power and small-footprint package at previously unattained price points.

Steve Edwards
Chief Technology Officer
Curtiss-Wright Controls Defense Solutions
Steve.Edwards@curtisswright.com
www.cwcdefense.com

Easing legacy migration in Systems of Systems

By Gordon Hunt



Historically, the military acquires systems – each to meet specific requirements. Because of this acquisition approach, legacy migration is a concern during a program's operations and maintenance phase.

Today, the acquisitions environment is changing in response to many pressures. The most obvious change is the reduction in spending on new systems. And, there are also pressures for the acquisition process to be agile and responsive to the asymmetric threat. The net effect is the next generation of systems will not be developed as new systems. Instead, acquisition officials look to gain efficiencies by reusing existing capabilities in new combinations to achieve new expanded capabilities, resulting in a System of Systems (SoS).

Benefits of Systems of Systems

The ability to assemble legacy capabilities is a force multiplier, and the extended capabilities of a System of Systems provide increased effectiveness beyond the individual systems and technologies. From the operator's perspective, Systems of Systems allow the use of costly weapon systems at their full kinematic ranges. From the combatant commander's perspective, a System of Systems is a means to a reduced "troop to task" ratio, meaning a reduction in the number of troops required to accomplish a task. Most significantly, from the taxpayer's perspective, Systems of Systems allow us to pay once for a capability, not repeatedly, which significantly reduces the largest portion of total ownership cost – operations and support.

Challenges of Systems of Systems

Creating a System of Systems from legacy systems or applications is fundamentally different from creating a system to requirements. Because the different components of a System of Systems have their own ownership, architecture, and original requirements, traditional

architectural approaches to legacy migration are insufficient. The traditional concerns of legacy migration and application portability are still present in the assembly of a System of Systems, but now with the additional challenge of multisystem interoperability introduced by a System of Systems.

The infrastructure of an application must support technical and syntactic interoperability. The infrastructure of a System of Systems must also support semantic interoperability. To support semantic interoperability, a software infrastructure must have three main characteristics: First, that it is based solely on open standards; second, it has an open data model that is rigorously defined, rigorously described, and fully discoverable; third, the primary nonfunctional requirement of a System of Systems software infrastructure is flexibility.



Because the different components of a System of Systems have their own ownership, architecture, and original requirements, traditional architectural approaches to legacy migration are insufficient.



Open standards

The appropriate software infrastructure will leverage open standards that support interoperability. Examples of standards that support technical interoperability are IEEE 422, ARINC 1553, and POSIX. Examples of standards that support syntactic interoperability are DDS, MPEG, and XML. Examples of standards that support semantic interoperability are SQL and DDS.

Data model

The software infrastructure provides a semantic bridge between systems; therefore, it must be semantically aware. Semantically aware software infrastructure uses an extensible data model that

captures semantics. This model must include the system's entities, the relationships between the entities to establish context, and explicit definitions of the system's observable and measurable phenomena (such as attitude, distance, location, position, and so on). This explicit definition must include the reference frame, units, and precision to concretely establish the context of the data to be exchanged. It must be rigorously defined, described, and discoverable.

Flexibility via super patterns

Finally, the software infrastructure must be flexible, because there is no one technology that is sufficient for the range of behaviors necessary for System of Systems-level software infrastructure. This flexibility is achieved by using architectural "super patterns" of distributed systems. The super patterns for organization, topology, state management, and communication patterns allow the other patterns to be constructed. The super pattern for organization is the traditional client server pattern. The super pattern for communication is the "event driven pub/sub" pattern. The topology super pattern is the "peer-to-peer" pattern. The state management super pattern is the "delegate to logical central repository" pattern.

Building the software infrastructure on these super patterns allows the software infrastructure to construct all of the other interaction patterns that legacy applications might have used.

Next evolution of systems migration is here

The next evolution of legacy migration enables the construction of Systems of Systems. A sophisticated software infrastructure, such as RTI Connext, is constructed specifically for this purpose.

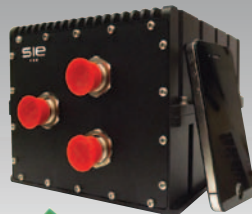
Gordon Hunt is Chief Applications Engineer at RTI. He can be contacted at gordon@rti.com.

sie-cs.com

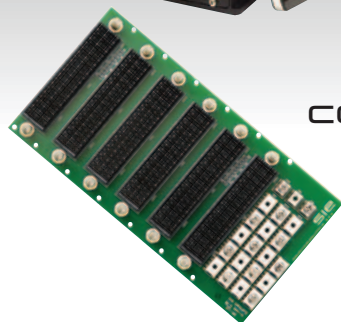
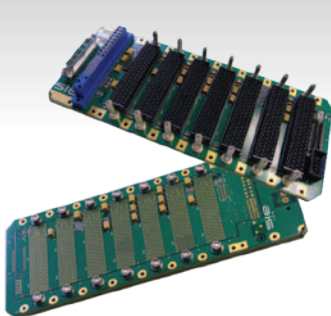


rugged & ready when you are

Open VPX [configured and ready to ship]



enclosures
backplanes
system integration
& custom solutions
VME
VPX
CompactPCI
Open VPX...



sie

COMPUTING SOLUTIONS • • •

MISSION-CRITICAL

PERFORMANCE-CRITICAL

SIE Computing Solutions | 10 Mupac Drive | Brockton, MA 02301 | 508-588-6110



NSA director admonishes U.S. to lead the pack in steeling cybersecurity

Once the office water-cooler discussion veers toward the global economy, the first considerations typically brought up are new job creation, unemployment rates, and outsourcing jobs (and to where). However, cybersecurity also plays a vital role.

Specifically, the global economy will benefit as cybersecurity is steeled, and the U.S. needs to lead the pack in developing solutions to solve cybersecurity challenges, asserted

U.S. Army Gen. Keith Alexander, NSA director, according to a DoD report on the recent U.S. Chamber of Commerce Cybersecurity Summit. (Alexander additionally heads the Central Security Service and U.S. Cyber Command.)

"We're the nation that developed the Internet; we ought to be the first to secure it," remarked Alexander (Figure 1).

Cybersecurity is not just a case of survival of the fittest. Cyberattacks have been perpetrated against entities one might think of as highly secured, such as L3, Google, Symantec, Sony, Visa, and government and military agencies, stated Alexander. Additionally, disruptive attacks are one of the biggest perils, he said, mentioning the attacks against Lithuania, Latvia, Georgia, and Estonia.

"Distributed denial of service attacks ... are gaining in momentum, intensity, and frequency," he added.

The other huge peril of cyberattacks is that of intellectual property theft, according to Alexander. The NSA director adduced companies such as Apple – whose worth catapulted from \$5.7 billion to \$148 billion between 2002 and 2012 – and Amazon – whose worth skyrocketed from \$851 million in 2002 to \$12.83 billion today. His point: to illustrate the criticality of IP protection via cybersecurity to foster such commerce growth.

Hence, the answer to the cybersecurity challenge, Alexander said, lies in training and education, and use of a defensible architecture like cloud computing, "so ... the Defense Department and the [intelligence] community moving to a thin, virtual client approach makes a lot of sense." He also recommended collaboration of industry, government, and the military regarding cyberspace issues, the DoD report concluded.



Figure 1 | As the Internet's creator, the U.S. needs to be first in developing solutions for effective cybersecurity, said U.S. Army Gen. Keith Alexander, NSA director

Navy's commercial air services program gets ... more services

The U.S. Navy's commercial air services program will soon benefit from a nearly \$50 million contract modification granted to Airborne Tactical Advantage Co., LLC, calling for the company to provide "services" to the program. Specifically, the program renders contractor-operated and -owned Type IV supersonic and Type III high subsonic aircraft to various customers of the Navy fleet, in an effort to provide diverse airborne threat simulation abilities. This gives aircrew, along with aircraft and shipboard weapon systems operators, necessary training for electronic attack operations and Electronic Warfare (EW). Forty-five percent of the work takes place in Jacksonville, FL and Newport News, VA, and another 35 percent is slated for Ft. Mugu, CA. The final 20 percent is planned for unspecified locale(s) outside the U.S., and all work under the modification is anticipated for completion next October.

USAF F-22s to undergo some rework

The USAF recently awarded Lockheed Martin Corp. a \$22 million contract covering F-22 heavy maintenance sustainment, modifications, modernization and structural retrofit plan, depot throughput, contractor field teams, signature analysis system reduction, and common configuration (Figure 2). Work under the contract will take place in Palmdale, CA and at Hill Air Force Base in Utah, by the end of next year. AFLCMC/WWUK, Wright-Patterson AFB in Ohio is the contracting activity. Meanwhile, the F-22 continues to fly unfriendly skies at speeds in excess of 1.5 Mach, sans any gas-guzzling afterburner usage (i.e., it boasts "supercruise" capability). This supersonic ability makes F-22s more versatile than other present-day fighter planes, which are required to utilize an afterburner for supersonic operation.



Figure 2 | Lockheed Martin recently received a \$22 million contract providing modifications and modernization for the USAF's F-22s. Pictured: an F-22A Raptor, photo courtesy of the USAF, by Master Sgt. Jeremy T. Lock

Navy orders new and remanufactured aircraft

In light of thinning DoD budgets, remanufacturing and reworking military technologies are a critical part of DoD spending these days. Consequently, the U.S. Navy recently issued contract modifications to Bell Helicopter Textron Inc. and Sikorsky Aircraft Corp. along those lines. But the Navy didn't forget about new aircraft too.

Bell Helicopter Textron: UH-1Y/AH-1Z

The Bell Helicopter Textron \$391 million "firm-fixed-price modification to definitize a previously awarded advance acquisition undefinitized contract action," according to the DoD website, stipulates that the company renders long lead parts for lot 9 and also components necessary to manufacture 15 new UH-1Y aircraft (Figure 3). Also provided by the modification are seven new iterations and a triad of remanufactured versions of the AH-1Z aircraft. Sixty percent of the work happens in Fort Worth, TX, and 40 percent transpires in Amarillo, TX. Fulfillment is anticipated in July 2015.

AH-1Z and UH-1Y helicopters can transport 2,000 to 4,000 pounds more than their two-blade predecessors, the Marine Corps' UH-1N and AH-1W.

Notably, the UH-1Y and AH-1Z aircraft share a parts commonality of 85 percent, easing maintenance and training.

Sikorsky Aircraft: VH-3D/VH-60N

The \$22 million Sikorsky contract modification follows suit somewhat, focusing on "special progressive aircraft rework of two fiscal 2013 VH-60N aircraft," According to a DoD report. The



Figure 3 | The Navy has issued contract mods to Bell Helicopter Textron Inc. and Sikorsky Aircraft Corp. covering new and/or remanufactured UH-1Y, AH-1Z, VH-3D, and VH-60N aircraft. Pictured: a UH-1Y Huey, photo courtesy of the U.S. Navy, by Mass Communication Specialist 1st Class Rebekah Adler

modification additionally covers "the associated vendor repairable and component overhaul for the VH-60N (Night Hawk helicopter) and the VH-3D aircrafts." Work is to be completed in Stratford, CT, in September 2013.

Spawned from the U.S. Navy's SH-60 Seahawk and the U.S. Army's UH-60 Black Hawk, the VH-60N serves as executive transportation. First deployed in 1989, the VH-60N replaced the VH-1N.

Meanwhile, the all-weather, twin-engine VH-3D helicopter also serves as executive transportation, specifically for the U.S. President, and is flown by HMX-1 (aka Marine Helicopter Squadron One).

New Army mobile chargers give the power back

What good is having a laptop, tablet computer, or smartphone if its battery has gone dead? While an uncharged mobile device battery can greatly frustrate highly impatient consumers, it could be a matter of life and death to a soldier crossing the "Desert of Death" in Afghanistan, for example, who would not have a traditional electric grid available for recharging mobile devices. Additionally, often local grids in faraway locales are unreliable because their provided AC power experiences wide voltage fluctuations.



Figure 4 | U.S. Army engineers, under RDECOM's CERDEC, are designing mobile device battery chargers for when the grid is nowhere in sight – or when local AC voltage fluctuations are prohibitive. U.S. Army photo courtesy of Tom Faulkner, RDECOM

Accordingly, U.S. Army engineers tasked with incarnating the U.S. Army Research, Development, and Engineering Command's (RDECOM's) vision, under the CERDEC umbrella, are working to design mobile device battery chargers when the grid is nowhere in sight or proves itself unreliable. The new chargers are powered by various military standard batteries, and can charge several devices at the same time (Figure 4). So far, the team has made prototypes of USB chargers capable of 2-port, 4-port, and 8-port support, in addition to an AC/USB adapter.

The 8-port charger for smartphones tips the scale at 2.5 ounces, powers as many as eight phones at once, and works with military batteries such as the BB-2557, BA-5390, BA-5590, and BB-2590. A smartphone battery can be recharged 37 times by a single BB-2590, fully charged.

The original 2-port iteration is for tablets and smartphones and weighs 1.8 ounces. A subsequent 2-port version features an AC adapter capability too, is able to charge two smartphones plus a laptop, and weighs 5.9 ounces.

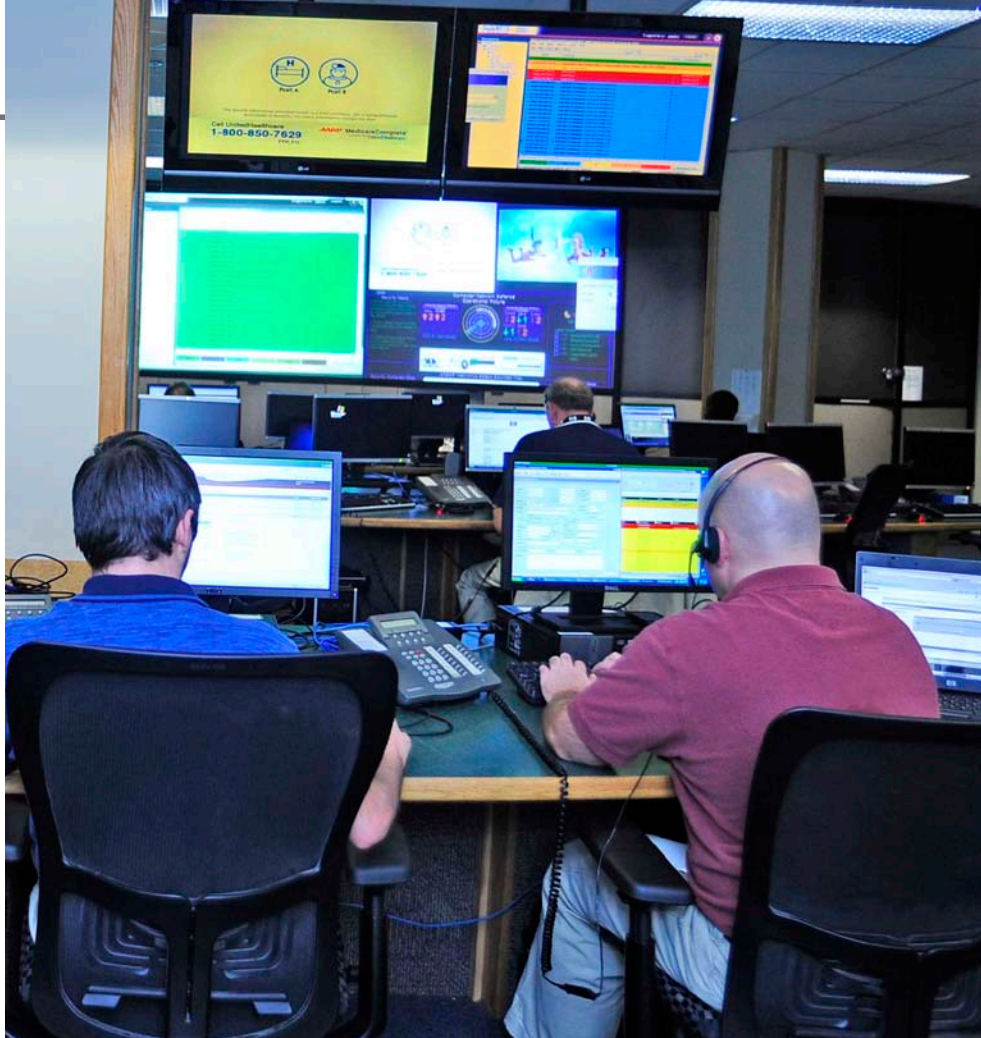
Twenty of the 2-port chargers have been delivered to troops serving in Afghanistan, while both 2- and 4-port chargers were deployed this year to U.S. Africa Command. The CERDEC team continues to work on design for a 150 W charger suited up with an AC adapter to recharge every laptop now commercially available.

Army engineers say that the prototypes were developed in a mere week and a half, RDECOM reports.

Enterprise software and the DoD

By John McHale, Editorial Director

Enterprise software management is becoming more pervasive throughout the U.S. Department of Defense because of its cost advantages and the inherent security advantages of having one network based on common standards. Meanwhile, the world's largest enterprise network – the Navy Marine Corps Intranet (NMCI) – is going through a transition.



The Navy Marine Corps Intranet is the largest enterprise network in the world, serving about 700,000 sailors and Marines and more than a million mailboxes.

Information technology leaders within the Department of Defense (DoD) are moving toward a network-centric enterprise infrastructure to reduce overall costs, consolidate personnel, improve training, and enhance security. They are doing this by leveraging and licensing Commercial Off-the-Shelf (COTS) hardware and software solutions and making them affordable and available across large networks.

The DoD's biggest success has been the Navy Marine Corps Intranet (NMCI), which has been a huge success, especially regarding security because it "prevents more than 78 million foreign network connection attempts per month, detects an average of 800 new viruses per month, and blocks approximately 35 million spam messages per month," according to the Navy Chief Information Officer (CIO) website. NMCI will be transitioning to the Next Generation Enterprise Network in 2014. Another effort enabling the enterprise for U.S. military forces is the DoD Enterprise

Software Initiative (ESI), which is sponsored by the DoD Chief Information Officer to "save time and money on commercial software, IT hardware, and services," according to www.esi.mil. "To date, DoD ESI has achieved a cost avoidance of over \$4 billion off prices established on the GSA Federal Supply Schedule."

"The use of enterprise licenses makes great sense for DoD," says Paul Capasso, VP of Strategic Programs at Telos. "Not only are there procurement cost savings, you also reduce costs in the operations and maintenance of the product through easier deployment of the software and help desk support. Maintaining multiple versions of a software product only adds complexity to the network and increases your security vulnerability. A joint enterprise email initiative is already taking shape within DoD. The Defense Information Systems Agency (DISA), who originally partnered with the Army to stand up this capability, has expanded this initiative to cover both

U.S. European Command and the Joint Staff. This initiative was expected to save the Army alone \$75 to \$100 million per year. This enterprise initiative provides the foundation for future Joint Information Environment (JIE) capabilities to come."

"The government is looking for standards and open architectures so they can start buying COTS software to manage with commercial APIs and create a higher service oriented architecture," says Jim Davis, Chief Technology Officer at WBEM Solutions, which is a software company that specializes in standards-based enterprise and data center management. "Until recently, there were not many standards to take advantage of, but now there are a few that are good enough that are also being promoted by well known standards groups such as Distributed Management Task Force (DMTF) and the Storage Network Industry Association (SNIA). Management Initiatives include the Storage Management Initiative (SMI)

from the SNIA, Systems Management Architecture for Server Hardware (SMASH), Desktop and mobile Architecture for System Hardware (DASH) and Common Diagnostic Model (CDM) from the DMTF. All of these initiatives are based on Web-Based Enterprise Management (WBEM), which includes the Common Information Model (CIM). As many organizations move to cloud-based solutions, these standards provide the instrumentation for the cloud.

"Government users like how standards enable them to build solutions from multiple vendors," Davis continues. "Some management initiatives provide solutions for a specified management domain such as storage, systems, desktops while other management initiatives may apply to all domains, such as diagnostics or power management."

"There are mechanisms and vehicles to pool buying power such as DoD ESI," says Rinaldi Pisani, VP/GM Cyber Application Solutions. "What they do is set up blanket purchase agreements with discounts for different products. The discounted price makes procuring the software quite easy. Telos holds DoD ESI licenses for its Automated Message Handling System (AMHS) and Xacta IA Manager, which is a Web-based application to automate a variety of certification and accreditation processes. It follows the NIST Risk Management Framework (RMF) to help identify risk to the system. The Marine Corps has standardized on this solution. Telos also offers Xacta Flux for vulnerability analysis, and Xacta CyberCOP (Common Operating Picture) for situational awareness, network performance, and security."

Security and the enterprise

"The fact that the DoD enterprise consists of a conglomerate of independent networks complicates the security paradigm required to protect it. Protecting data is the bedrock of cybersecurity," Capasso says. "Complexity and insecurity breed distrust. In simplest terms, moving to a JIE is all about reducing complexity and ensuring trust between the sender and receiver. The difference between good and bad information can be a matter of life and death to the warfighter."

There is a huge requirement for securing the data where it resides, Pisani says. "Software assurance is gaining mind-share and moving up the ranks of priority for DoD and government leadership. Historically, the focus has been perimeter defense and firewalls. Now they are paying more and more attention to the interior database layer because that's where the breaches are happening. The question they are answering now is how to treat the intrusions once they get past the firewalls. We established the Application Software Assurance Center of Excellence (ASACoE) at Maxwell AFB-Gunter Annex in Montgomery, AL,

to help manage this type of security. The center has conducted software assurance assessments on more than 1,000 applications."

NMCI to NGEN

The Navy Marine Corps Intranet, considered to be the largest enterprise computer network in the world, is currently in a transitional period to a new operational contract called the Next Generation Enterprise Network (NGEN). According to the Navy, all the services currently provided by NMCI will be transitioned to the NGEN, which is being competed for by two teams and



DRAGON
it's not a myth.

- Rugged PC/104 enclosure
- Data acquisition
- Monitoring • Recording
- MIL-STD-1553/1760
- AS5652 (MMSI) • H009
- ARINC-429/575 • ARINC-708
- CANBus • A/D • D/A
- Serial • Discrete
- User configurable
- COTS • Expandable
- Extreme environments
- Accepts third party cards

www.mil-1553.com

CAMELOT | MACC | LANC

is part of the Navy Enterprise Networks program under the Program Executive Office for Enterprise Information Systems. HP's NGEN team includes AT&T and Northrop Grumman. The other team is led by CSC and includes Harris, General Dynamics Information Technology, Verizon, and Dell.

"NGEN will have exactly the same network as NMCI. It is the service that is being competed," says Bill Toti, VP at The HP NGEN Alliance. "The Navy and Marine Corps bought the network from HP under the Continuation of Service Contract (CoSC). During the CoSC bridge, HP is the services provider for the Navy and Marine Corps. Now they are competing the service aspect under NGEN, which will provide the government with secure enterprise capabilities at a lower price. However, there is a slight difference between the Navy and Marine Corps management of NGEN. The government owns the network for both, but the Marine Corps

operates their network with contractor support. In other words, they refer to it as government owned and operated but contractor supported. The Navy, on the other hand, does not have the people to run it nor do they want to have active duty sailors operating the network. Therefore, it will be government owned and contractor operated.

"The fact that the Navy is competing NGEN will force the price down," Toti continues. "However, when it comes to moving toward what other large organizations are doing with the enterprise – such as more cloud operations – NGEN will be a step in the opposite direction. NMCI was a first-generation cloud solution and it used the cloud business model; in other words, you pay for what you use and the Navy paid by seat and will in the future. For the Navy, buying the infrastructure is neither good nor bad. For instance, a cloud model may not be the best choice for operational forces due to increased latency over long

distances and an increased risk of losing communication lines. However, for business services, which are more than half of the operations, it works just fine."

The NMCI success

"When NMCI was first implemented, there were about 2,000 disparate networks ... managed at varying degrees from a technical and security posture," says Drew Newman, Chief Information Officer for Department of Defense operations at HP and Chief Engineer for NMCI at HP Enterprise Services in Plano, TX. "The Navy didn't completely understand how many disparate networks and sometimes even where they were located. An early value add of NMCI was eliminating them and creating one common network platform with a common set of policies. Through NMCI we serve about 700,000 sailors and Marines and more than a million mailboxes. Geographically, that spans the continental U.S., Hawaii, Japan, and Guam. There are also some claimants and commands in the Navy that still retain



Performance advantages
in the world's hottest spots.

Mission-critical thermal solutions since 1970.

When the heat is on, for land, sea or air, military and aerospace engineers turn to innovative, reliable Thermacore thermal solutions to protect the mission-critical components of today and tomorrow. Through partnerships with military systems engineers, Thermacore continually discovers new ways to blend novel concepts and new materials with proven technologies.

AS9100 • ISO 9001 • ISO 14001 • DDTC/ITAR

For four decades, advanced military systems have relied on our thermal management solutions.

Find out why. Visit our Thermacore Design Center at www.thermacore.com/design



their legacy network connectivity only where they have applications that reside for a particular purpose. We allow them to reach back for that application access.

"Through the current structure we offer HP computers as standard, as well as Dell and some specialized tablets such as Panasonic Toughbooks," he continues. "We maintain a catalog for users to buy from for use off the network. Going forward, during the CoSC they can still buy them through us or bring a request and we can put an item on the catalog. It covers computers, printers, peripherals, equipment for classrooms, etc. So far we've rolled out 65,000 Windows 7 machines with 4 Gigs of RAM at a minimum. Specific security postures are enforced at the network layer and in how the machines are configured. We use ... two-factor authentication – something you have and something you know. Which in this case is a Common Access Card (CAC) plus user ID and password for enabling network entry. There is cryptographic log on and we also encrypt the disk for data at rest protection."

Mobility and NMCI

"Progress is being made on the mobilization of the network," Newman says.

"When it comes to introducing a mobile device – whether it is a smartphone or tablet – we lay out the use case for mobility. We determine what are they going to use it for – sending and receiving email, getting data, reading something, etc., and then map use cases to the different capabilities. We will have an iPad solution ready in mid December this year with a small limited deployment for capability for iOS devices. We've also implemented a limited deployment hosted virtual desktop. This occurs in the data center as a cloud and users can access it from their desktop at home or anywhere remotely. It is represented in a window on their mobile device. All the processing happens in the data center and no data remains on their remote device."

"One disadvantage to having a large network is that no COTS product is designed to operate on a network this big," Toti says. "From email to routers to network security to fill in the blank, almost everybody's product needs to be reengineered to work on a network this big. COTS equipment is typically designed for large commercial enterprises with 30,000 users, not a million users." **MES**

Enterprise company listing

Apple – Cupertino, CA
www.apple.com

AT&T – Dallas, TX
www.att.com

Blue Coat Systems – Sunnyvale, CA
www.bluecoat.com

Black Duck Software – Burlington, MA
www.blackducksoftware.com

Blue River Information Technology – Arlington, VA
www.blueriverit.com

CSC – Falls Church, VA
www.csc.com

Dell – Round Rock, TX
www.dell.com

EasyConnex – San Mateo, CA
www.easyconnex.com

IBM – Armonk, NY
www.ibm.com

General Dynamics Information Systems – Fairfax, VA
www.gd-ais.com

Harris Corp. – Melbourne, FL
www.harris.com

HP Enterprise Services – Plano, TX
www.hp.com

McAfee – Santa Clara, CA
www.mcafee.com

Microsoft – Redmond, WA
www.microsoft.com

Northrop Grumman Information Systems – Falls Church, VA
www.is.northropgrumman.com

Raytheon Trusted Computer Solutions – Herndon, VA
www.trustedcs.com

SafeNet – Belcamp, MD
www.safenet-inc.com

Symantec – Mountain View, CA
www.symantec.com

Telos – Ashburn, VA
www.telos.com

Thales E-Security – Plantation, FL
www.thales-esecurity.com

Verizon – New York, NY
www.verizon.com

VMware – Palo Alto, CA
www.vmware.com

WBEM Solutions – Pinehurst, NC
www.wbemsolutions.com

Virtual training over the enterprise

Virtual training over the enterprise

Engineers at EasyConnex are combining the best of gaming technology with enterprise management to create a virtual training environment that not only provides organizational culture and job training but also gives management the metrics to measure decision making in new corporate hires and military recruits.

"EasyConnex was founded on a concept called *gamification*, which refers to the technology and fundamentals behind games such as EA SPORTS titles and ultimate simulation games like Halo," says Leo Fang, President and CEO of EasyConnex. "We bring that realistic simulation and its application tools to an enterprise platform to help train employees over the enterprise. The tool creates a simulation scenario that replicates with a good deal of realism the environment they would be working in – military or corporate. Most games have goals and objectives [that] transition well to learning and training areas for military and corporate organizations. Game algorithms provide instantaneous feedback to the manager and through social collaboration can enable team building."

EasyConnex's tools also provide detailed metrics. "Within the enterprise space, the metrics aspect of our solution can gather a great deal of data, not just basics, such as how long users are spending on the system, etc.," Fang says. "We can actually track how people make decisions. You are not teaching values so much as you are learning about an employee. The tool is not a one-way street to tell new recruits how they should think, but lets management see how by their actions how they think and react."

Smartphones on the battlefield

By John McHale, Editorial Director

Military planners want warfighters to have the same capability that civilian consumers get from their commercial smartphones and are testing different devices. However, they still have to overcome security hurdles and the short development cycles in the commercial market before full-scale deployment can happen.



The H2 SCORPION handheld from DRS Tactical Systems provides a rugged package for a commercial smartphone with sled mating system mates that enable expansion for extended battery life, SAASM GPS, RFID, IR cameras, and more.

The typical civilian smartphone – whether it is an iPhone 5, Samsung Galaxy III, or even a BlackBerry – is easier to use and has more processing capability than any handheld device that soldiers, Marines, sailors, or airmen use in combat environments today. Modern cell phones have amazing technology, but are not seen as rugged or secure enough for military use on the battlefield. That is until recently. Different programs are in development in the Services to leverage commercial smartphones for battlefield use. One Army initiative – the Nett Warrior program, run by PEO Soldier – expects field these devices as early as 2014.

“No defense company in the world can beat the reliability and performance these small devices deliver,” says Jason Regnier, Acting Program Manager for the Nett Warrior program at Ft. Belvoir, VA.

“It is money well spent. What is enabling their use in part from a policy was a relaxing of the requirements about the environments they would be used in. For example, they don’t have to survive a nuclear blast anymore. We are still looking at more ruggedized devices for underwater use and the like, but right now we are focused on commercial devices due to the tremendous cost savings and they are meeting all of our objectives so far.”

“Smartphone development within the DoD is a testing environment,” says Brett Kitchens, Senior Director, DoD Strategic Programs, U.S. Federal Government Markets at Motorola. “PEO Soldier wants a smartphone device at the edge running secret-level security, but it is not a program of record yet today. I think the efforts will move quickly. Some

brigades are already testing different smartphone equipment and software. Eventually there will most likely be a pool of devices for the services to choose from based on their mission needs and user preference.”

Nett Warrior

Right now Nett Warrior – an integrated, dismounted situational awareness and mission command system – is in the operational testing phase and begins fielding in 2014, Regnier says. However, the Army is in a hurry to get this technology out earlier and is fielding Motorola Atrix Android-enabled smartphones with certain brigades this year to improve situational awareness. They are still secure with strong encryption, but not certified by NSA for secret data. It is not under a program of record, but is more of an experimental requirement.

The Nett Warrior program is currently using Rifleman Radios from General Dynamics C4 Systems during demonstrations to interface with various smartphone devices running the Android operating system, Regnier says. The Rifleman Radio is an interim solution until the Army finishes developing the Nett Warrior tactical radio, he says. General Dynamics C4 Systems also is developing the Nett Warrior radio, which will weigh less than 2 lbs., communicate using the Soldier Radio Waveform (SRW), and enable access to the U.S. government's classified networks at the secret or sensitive but unclassified levels, according to a General Dynamics release. The Low Rate Initial Production order is for 2,052 radios, scheduled to begin delivery early in 2013.

"For the smartphones, we are looking at commercial devices that have a dual or quad processor design, are low power, are unlocked so we can remove their

software and install the government code, and have a bright, easily readable display," Regnier says. "The WiFi and Bluetooth functions are turned off on these phones and only connect through the tactical radio. Each device functions essentially as a mini computer with a dual- or quad-core processor.

"One common frustration with using these commercial devices is that just when you have one modified and the proper software added, the company stops selling them," Regnier continues. "An example of this was a Samsung Note device we looked at that had a large, bright screen that the warfighters liked, but we were too late as Samsung has already stopped selling them and moved on to the next one. The commercial development cycle goes even faster than we thought it would. For Nett Warrior to make it through each year, I will have to look at what the

next smartphone will be to keep up with what the commercial cell phone guys are doing. For example, many cell phone companies are moving to Organic Light Emitting Diode (OLED) displays, which will be brighter but easily detectable at night. We need to make it dark so the enemy can't detect it and make the displays compatible with night vision goggles.

"The key will be to eventually have software that will work across multiple platforms even if the physical devices go obsolete," Regnier continues. "If you do it right and follow the coding it will work. But for us there are only certain phones that will work because the manufacturers do not unlock all the phones in the same way. We need the devices unlocked so we can remove their code and upload our certified software. The reason is we have to have secret capability in the end user device."

EXPERIENCE UNPRECEDENTED CLARITY

NEXT GENERATION DISPLAY SOLUTIONS FOR C4ISR



Advanced VEGA Rugged Displays with Real-Time Video Enhancement

The VEGA Display Series from Z Microsystems features an adaptable architecture that can satisfy a complete range of rugged COTS needs. Tough, lightweight, element-resistant, and with built-in image enhancement algorithms, VEGA displays can handle multiple inputs from a wide range of video sources. A choice of touch screens with easy on-screen controls offers viewers on-demand access to multiple video feeds in Picture-in-Picture (PIP), QuadView, Dual-View and full screen formats. With an armored shell manufactured from CNC machined aircraft grade aluminum and low profile fold and lock transportation handles these displays are FIELD-READY.



Call 858.831.7000 or visit www.zmicro.com/rtev

Securing smartphone communications

"The first hurdle for smartphone acceptance in the military is the security aspect, and industry and the government have got to prove it. But we think we have [gotten] it solved," Kitchens says. "We anchor the data at rest, which then goes through the chip as encrypted packet and users will have the keys to secure. Also if you pull the data out without the key, you kill it. The NSA is looking at certifying the security solutions and there will be different paths to agency certification of devices. They will also need criteria for mobility. It will be up to the authorities to take the risk, and right now 256 encryption looks good enough as it has not been broken, and 256 B is even tougher." Motorola secure smartphones include their AME 1000, which is based on the ES400 device for enterprise applications (Figure 1).

"Warfighters see the value of what you can do with a smartphone, but before it gets into the field en masse, the devices really need to be secured," says Tim Skutt, MILS Solution Architect at Wind River. "Right now smartphone use is kind of in a middle ground, going through limited experiments, not in widespread deployment yet. Wind River's secure Android offering has a holistic approach that supports integration of security enhancements tailored to the use case, as well as unique commercial Android capabilities, into security enhanced devices. We have five pillars that we are implementing when developing Android solutions – attack detection and prevention; device integrity; isolation; infrastructure security; data protection and system protection, which includes the ability to sanitize remotely."

Trusted Handheld Platform

"Enabling top-secret security in a COTS phone is a difficult challenge," says Gordon Jones, INTEGRITY Secure Virtualization at Green Hills Software. "Certifying a COTS phone for use can be done, but by the time the phone is certified, it may be obsolete before you can deploy it to the troops. What is needed is a way to keep the security

Figure 1 | Motorola's ES400 is the basis for their AME 1000 Secure Mobile Telephony Solution targeted at secure government users.

portable across architectures that also meets the commercial release process." Green Hills is participating in a Marine Corps effort called the Trusted Handheld Platform that is looking to advance the development of commercial mobile device technology for the DoD by enabling a capability to access multiple security domains, Jones says.

The program has four requirements, with the first seeking an isolation technology such as a separation kernel or security kernel, he continues. This will isolate the software components, control the intra-domain access, and also isolate the other resources on the devices. Second, it must be multipersonality, so the devices support multiple personalities on a single handset. Another requirement is that it use commercial standards and not be a custom government design. The fourth requirement is that it have a common product line architecture across multiple platforms, Jones says.

"Green Hills engineers are applying their separation kernel – INTEGRITY – and running multiple versions of Android on top of it and controlling the device," Jones says. "This guarantees separation time and space for the applications on top and also runs a complete virtual machine monitor. There will be applications running inside of Android, and since Android is a large and complex piece of code, the level of assurance for any code running inside of Android is low so isolation is required. What we do is isolate Android from the rest of the system. For instance, one Android could be connected to the Secure Internet Protocol Router (SIPR) network and one will be connected to the Non-secure Internet Protocol Router (NIPR) network, but they will be isolated from one another on top of the INTEGRITY kernel."



This dual domain phone would have an IT persona and a private persona – both isolated from each other on top of a trusted environment that would have an NSA-certified separation kernel like INTEGRITY, Jones says. A dual domain smartphone for the warfighter could operate in a classified and unclassified network as well as separate personal and work data. Having only one physical device also enables the warfighter to save on size, weight, and power, he adds.

"For protection of data at rest when implementing the INTEGRITY kernel on a device with Android as a guest, we insert a virtual self-encrypting drive that guarantees that every piece of data written to memory is encrypted by INTEGRITY in a trusted partition before being written to memory in the phone," Jones says. Therefore, as data moves in and out of Android unknown to Android, it is encrypted by the architecture when in motion or at rest and cannot be compromised.

Secure networks and tactical app stores

Engineers at Lockheed Martin are enabling the use of commercial tablets and smartphones by developing a secure 4G tactical cellular network they call



SECURE RUGGED STORAGE

- Up to 4TB Capacity
- High Performance
- Ultra Small
- Rugged

AES-256 Encryption
Removable Data Cartridge

Servers, NAS, Serial FPD and
Ethernet Data Recorders



Tel.: +1 (281) 769-8211
sales@galleonec.com
www.galleonec.com

 **galleon**
embedded computing

MONAX, says David Weber, Business Development Manager, C4ISR Systems at Lockheed Martin Information Systems & Global Solutions in Philadelphia. The network can be set up in places where there are no cell towers and, within hours, a private, secure cellular network is operational (Figure 2). No matter the smartphone or tablet device used for voice, video, and data transmission, users will still be able to access the network if they have the proper clearance, Weber says. Once connected, their device accesses a VPN tunnel that is encrypted, he adds.

"Once you get into the network, there are multiple layers of security via the Mobile Device Management (MDM) feature, which enables users to set secure access policies," Weber says. "The system can also be Common Access Card (CAC) enabled. For data at rest protection, the system can be remotely zeroed out through the MDM feature. Tactical radio users also can access MONAX by just entering the VPN tunnel, he adds.

"We have a MONAX application store that is very minimal because we don't build apps, but we will have the capability to download apps or purchase them from other vendors," Weber says. "Five apps that come with the MONAX solution are VOIP, tactical app, chat, map app, and an NSA app. The apps are developed for or rehosted on a smartphone, then approved and made available to warfighters in the app store. You can download popular apps, but we recommend you turn that capability off. If the customer wants to, we can enable it, but it can be risky as it opens up to the 'dirty' Internet."

The system consists of a portable MONAX Lynx sleeve that connects touch-screen smartphones and tablets to a MONAX XG Base Station infrastructure located on the ground or on airborne platforms, according to a Lockheed Martin MONAX brochure. Currently the Marine Corps uses MONAX in military exercises and it is also used for humanitarian disaster relief, Weber says. The Coast Guard is using MONAX with iPads

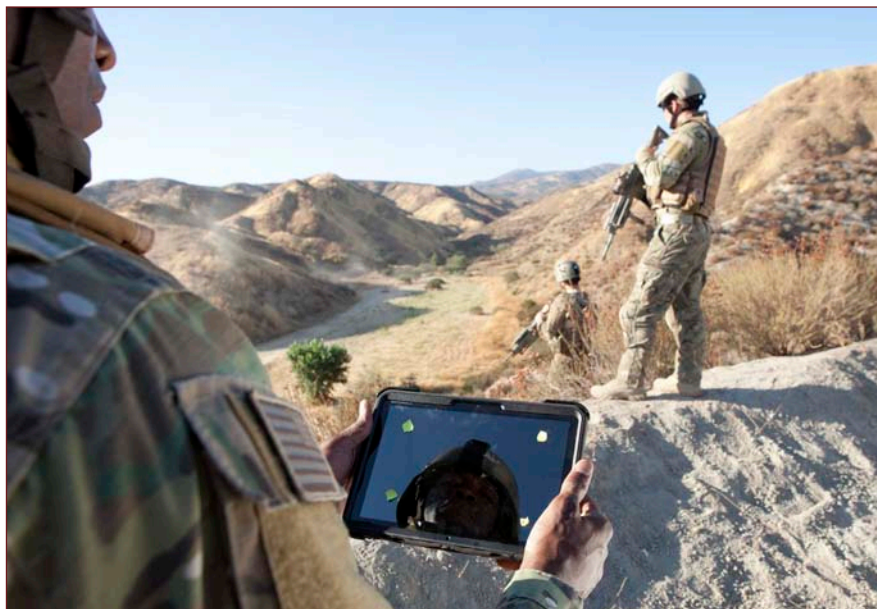


Figure 2 | The MONAX network from Lockheed Martin can be set up in places where there are no cell towers and, within hours, a private, secure cellular network is operational.

in all their medical clinics across the U.S., he adds.

Ruggedizing the smartphone

While commercial smartphones have state-of-the-art processing capability, they are not what the military would traditionally call "rugged," but have features and interfaces with which warfighters are comfortable. The Army did run a program for rugged handheld development called the Joint Battle Command-Platform (JBCP) Handheld System, which has since been moved under Nett Warrior. It is no longer an active program, but the Army is still looking at the ruggedization developments.

DRS Tactical Systems' first rugged handheld offering came out of that program and was called the SCORPION H1. "Although we met the initial requirement, it became clear it didn't meet with user expectations," says Bill Guyan, VP at DRS Tactical Systems. "Warfighters have the same expectations – in terms of ease of use – that they get from their personal smartphone: lightweight, small enough to fit in a pocket, and an efficient touch screen with good visibility and graphics. So for the next version – the H2 – we went a bit outside the box. We ruggedized a commercial handheld instead of building it from the ground up."

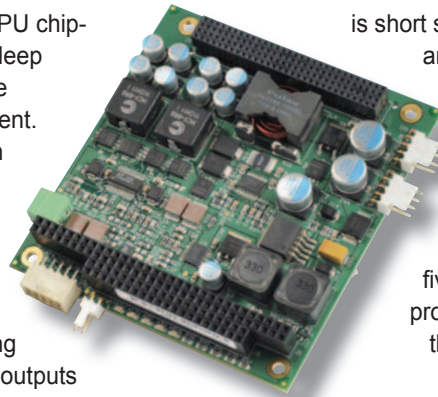
The H2's appeal is its modularity that enables warfighters to customize it for their mission. Its sled mating system mates through a connector that allows for expansion sleds for extended battery life, USB hub, SAASM GPS, information assurance, RFID, IR camera, dead reckoning, a cold weather module chemical/biological detection, or a combination based on customer specifics. If the phone is damaged or a newer model is available, it also can be easily swapped in and out of the housing. The 3G/4G-ready H2 features the Google Android 2.3.5 (Gingerbread) preinstalled and is Android 4.0 (Ice Cream Sandwich) ready. It uses a Qualcomm Snapdragon S3 Processor and has 1 GB of RAM. It weighs 8 ounces and has about 8 hours of battery life and can be charged while interacting with tactical radios.

The General Dynamics Itronix GD300 rugged smartphone also came out of the JBCP, says a General Dynamics spokesperson. The device meets MIL-STD-810G and is resistant to dust, rain, shock and vibration, and humidity. It has GPS capability, can be worn on the arm or chest, and weighs less than 10 ounces. The GD300 also can interface to a tactical radio network for secure communications. **MES**

ATX-compatible DC/DC Power Supply offers Wide Input Range and -40° to +85°C Operation

WinSystems' PPM-DC-ATX is a PC/104-Plus DC/DC power supply for PC/104, EPIC, and EBX single board computers (SBCs) that support ATX power controls. It features a wide voltage input range from 10 to 50 volts, which allows the unit to operate with 12, 24, or 48 volt battery-operated or distributed DC power systems. It generates five regulated DC output voltages from one common DC input, plus supports the software controlled shutdown and power monitoring for SBCs

with advanced CPU chip-sets employing sleep modes and active power management. Also, the unit can operate in a +85°C ambient temperature environment using normal convection cooling and no fan. The outputs are +5V@10A, +3.3V@10A, +12V@3A, -12V@500mA, and +5V_{STBY}@2A. Each output



is short short circuit protected and current limited. A minimum load is not needed to bring the supply into regulation. When power is applied to the board, five LEDs will illuminate providing a visual status that power is available.

WinSystems, Inc. (817) 274-7553
WinSystems.com/PPM-DC-ATXM

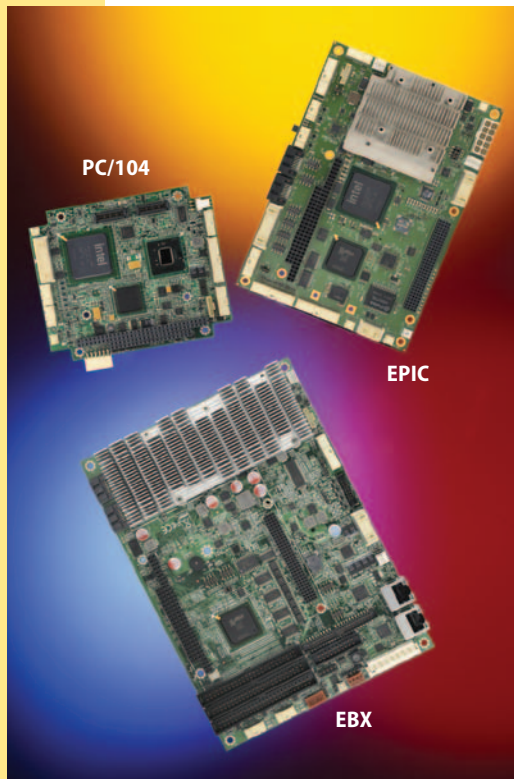
High-Performance Atom™ SBCs Small & Fanless

For your next design, select rugged WinSystems' single board computers powered with single- or dual-core Intel® Atom™ processors.

- ▶ Long-life Intel® Atom™ CPUs
- ▶ Simultaneous VGA and LVDS video
- ▶ Gigabit Ethernet port(s)
- ▶ Eight USB 2.0 ports
- ▶ Four serial ports
- ▶ PC/104 expansion
- ▶ SATA and CompactFlash
- ▶ Digital I/O with Event Sense
- ▶ -40° to +85°C Operation
- ▶ Outstanding Tech Support
- ▶ Industry Standard Platforms: EPIC, EBX, PC/104, and SUMIT-ISM™
- ▶ Software Support: Windows®, Windows Embedded, Linux, and x86 RTOS

Our SBCs are the right choice for security and military applications.

Go to WinSystems' SBC Guide at www.WinSystems.com/SBCsM



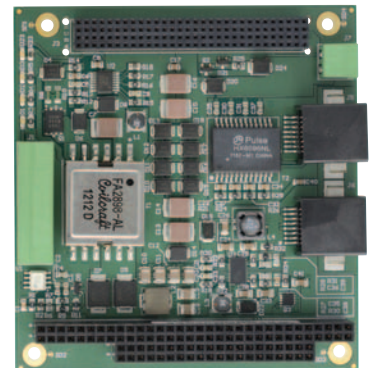
Call 817-274-7553 or
Visit WinSystems.com/AtomM
Ask about our eval program



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

PD Power Supply PC/104 Module for PoE Applications

WinSystems' PPM-PS397-POE-1 is an isolated 25W, 802.3af-compliant, Power over Ethernet (PoE) module. It powers a PC/104-Plus single board computer stack from DC power extracted from the CAT5 cable. It is designed for use in areas where other power is unavailable and to reduce the wiring costs for installations.



The PPM-PS397-POE-1 accepts 42-57VDC and converts it to three isolated outputs: +5VDC@5.0A, +12VDC@1.0A, and -12VDC@0.8A. Each output is short circuit protected and current limited. A minimum load is not needed to bring the supply into regulation.

WinSystems also offers this board configured for PC/104 and standalone systems.

No fans or heat sinks are required to meet its extended operating temperature range of -40° to +85°C.

WinSystems, Inc. (817) 274-7553
WinSystems.com/PPM-PS397-POE-M

Big-screen biometric apps, stand aside: Off-the-shelf smartphones enable rapid suspect ID for warfighters, intelligence ops

By Sharon Hess, Managing Editor



INTERVIEW

Editor's note: It sounds like something straight out of "Covert Affairs" or the "The Bourne Identity," but this time it's got a twist. Face biometric and facial recognition software hits up databases for their best shot at a face match, but it's not on the big screen nor at the local CIA or other intelligence agency office. Instead, biometric face recognition software is right in the operator's hands – via an off-the-shelf iPhone or Android-based smartphones – giving warfighters and intelligence operatives in the field the chance to autonomously identify suspects or persons of interest within seconds or minutes. Editor Sharon Hess recently caught up with Animetrics President and CEO Paul Schuepp to find out more. Edited excerpts follow.

MIL EMBEDDED: *Can you tell me a bit about Animetrics, how long in business, number of employees, and your technology focus?*

SCHUEPP: Animetrics is a small firm in Conway, New Hampshire, and we also have an office in Columbia, Maryland, kind of closer to the customer down there. We employ about 15 people, most of which are engineers and scientists. We specialize in face recognition and face biometrics software. We have been in business for nine years, and most of our work [is] with the Department of Defense and the intelligence agencies. And we're doing more now with public safety and law enforcement.

MIL EMBEDDED: *Your press release mentioned integrating your face biometrics and facial recognition software into smartphones for military use. Has that already started?*

SCHUEPP: Yes, it has been happening for a couple of years now, but deployments are slow going because there is so much testing that goes on, and the agencies are trying to get their hands around [how] to use it best. But we have apps that run on the iPhone and on Android platforms.

There are really two main apps: MobileID, which is a one-to-many search lookup of a face when you take a picture from the device itself. And then the other one is CredentialME, which is a one-to-one verification application where you could use your face for authorization to continue in another app, kind of like a password.

MIL EMBEDDED: *How can your face recognition software be used by the military and intelligence communities?*

SCHUEPP: Realistically, the intelligence agencies and military are most interested in using the face biometric software in conjunction with other biometrics, to try to resolve identity [questions arising] from [those serving] in theater.

MIL EMBEDDED: *Which other biometrics would they use them with?*

SCHUEPP: Fingerprinting, of course, has been around for a long time and there are several mobile devices today that have that on them. The other one is iris [scanning]. Iris is a very strong biometric, strong in the sense that it is very accurate, but, of course, it is also very controlled. You have to get very close to the person to be able to use it and [need] special lighting. But those are the biometrics of choice. But if you could use all three, including face biometrics, you're in really good shape relative to seeing if that person matches the database or authenticating that person on a watch list.

MIL EMBEDDED: *What about retina scanning?*

SCHUEPP: They really don't do retina scanning. Retinal was one of the original technologies that used an infrared. They didn't like infrared because it could be potentially harmful to your eye. But the iris scanning is very safe, and it is basically looking in your eye with a light just like an eye doctor does, and it recognizes the pattern of the iris.

MIL EMBEDDED: *What's the advantage of the face biometric technology then, particularly when it's on a smartphone?*

SCHUEPP: The face biometric is a very good tool for trying to find out who the person is that you are confronted with. And you can be a little bit away from them by using the camera, and not have to be awfully close. Face biometric software on a smartphone is not intrusive: Nothing touches the person like [doing] a finger[print], and that is one of the desirable attributes. You can be 6 to 10 feet away, take a picture, and look up that person to see if they are in the database that you are checking.

MIL EMBEDDED: *So anyone using your software on a smartphone would just take a photo like they would with any ordinary cell phone?*

SCHUEPP: Yeah, exactly. So now here's the military's appeal: [The military has] basically a portable networking system. They are able to use the same kind of phone that you and I use, like the iPhone or an Android[-based mobile device] to communicate with. But it is on a secure DoD special cellular system, and they use that now to access their central databases for a lot of information. So one of those is getting to a biometric database. As you can imagine, there are a lot of people, perhaps millions, on a watch list that the military and also the intelligence community are on the lookout for, once you think about what is going on in Afghanistan and other parts of the world.

MIL EMBEDDED: *How does the face biometric software on the smartphone match up the faces after you take the photo?*

SCHUEPP: There is a definite process. On the face recognition side, a photo is taken. Basically, you have to have a digital image, and that digital image is internally scanned by the computer to find a face. That is the first step, and that's a whole algorithm in itself, a technology in itself, called "face detection." Once [the software] finds the face, then it finds more attributes about the face and basically reduces that face, that photo, to a vector of numbers. The numbers are determined by the algorithms, the technology that represents things like texture of the face. We also recognize the 3D nature of the face so from the 2-dimensional image, the facial pose is determined. [Face biometric software] actually can perceive through a process called "computational anatomy" to create the 3D model. And our software also recognizes the varied lighting on the face.

So those are the three major components: the geometry; the texture, which is all the colors in your skin; and then the lighting. Those variables will all reduce to a set of numbers, and they call that a "face biometric template." And that template is used to compare to other templates that are previously stored in a large database, and then the statistical process [starts]. That takes that probe, that picture you just took, that template that is created, and determines how close it is to any of the other templates that are in that database. And if your statistical score is high enough, then it is deemed to be either a match or something that could be a match.

MIL EMBEDDED: *OK. So once someone takes a photo of a suspect with a biometric software-enabled smartphone, how long do the results take?*

SCHUEPP: Well, that is the exciting part. The systems that are being built now are set up to be very fast – we're talking minutes to get back the result, maybe even seconds but usually minutes. Before this, the warfighter would have to send in a picture and he would have to wait a couple of days to get back the results from headquarters. Back in the States, the BIMA (Biometric Identity Management Agency, part of the Army Provost Marshal General) agency's main location is in Clarksburg, West Virginia, and it had a long turnaround time. So the purpose of these systems being built now is to really improve that turnaround time to be very fast.

MIL EMBEDDED: *What kind of transmission were they using with the old way that took two days?*

SCHUEPP: It was a digital photo, but it was just protocol and sometimes I'm not even sure I understand why it took so long. But the systems were disconnected, and that is all being streamlined now. Of course, there was always the expedited way of doing things that the military can handle quite well. But as the normal everyday business, the way they had it set up wasn't practical but now that's changing.

MIL EMBEDDED: *When using your system with or without the iris scanning and the fingerprinting, the process is completely automated?*

SCHUEPP: Yes. We call it "lights-out face recognition." No people are involved except for the operator taking the picture.

MIL EMBEDDED: *What's the percentage of identification accuracy when using face biometric software like yours on a smartphone or mobile device?*

SCHUEPP: We test that all the time and in the face recognition business, there is a degree of variability, because the face is very uncontrolled compared to a finger or an iris. If you have a perfect facial image with good lighting on it and the person is



INTERFACE CONCEPT

ADVANCED ELECTRONIC SOLUTIONS

SWITCHES & IP ROUTERS

More than 30 models... VPX, VME, cPCI

ComEth 4410a




OpenVPX

- Data/control Planes 3U VPX switch
- Six 4-lanes ports (PCIe x4 Gen2)
- Up to ten Giga Ethernet Ports

SBCs PREMIUM

Intel® & Freescale® processors

QorIQ™



OpenVPX

- P5020, or
- P3041

Intel® Core™ i7



OpenVPX

- 2nd or 3rd Gen
- Dual or Quad Core
- with a Kintex™ 7
- and its personality module



www.interfaceconcept.com
+33 (0)2 98 573 030

looking at you frontal, you can [achieve] statistics of 99.9 percent identification rates.

But when the facial image varies from that, in other words you get poor lighting or lower resolution or especially an angulated face looking away from you, now the identification rate drops dramatically. But I am happy to say it is much better than it used to be. At Animetrics, our face biometric software is able, as long as two eyes can be seen, to identify angled faces at about a 92 percent identification rate.

MIL EMBEDDED: *Is there a specific smartphone camera requirement though when using biometric face software?*

SCHUEPP: There are some minimum requirements. Technically, when you take a picture of someone, [the software likes] to see 65 to 100 pixels between the eye centers. So what that means is if you have a 2 megapixel camera, you have to be within about 6 feet. I am not even sure you could buy a 2 megapixel camera anymore. But the iPhone 5 now [has an 8 megapixel camera]. With that, you could take a picture and be 25 feet away from a face, no problem, and get good resolution to get an ID.

There is a trade-off though: The higher resolution you use, the more data has to be transmitted, and sometimes that will make your response a little slower. The 2 megapixel camera would be much faster – it would be like seconds because of the less data in transit, depending on your network speed.

MIL EMBEDDED: *For an 8 [megapixel] photo, how long would transmission take?*

SCHUEPP: If you have a 4G network like AT&T or Verizon, it would only take 1.5 seconds, but if you're in a 3G network or 2G network, it is going to take several seconds.

MIL EMBEDDED: *Let's move on to how the face biometrics-enabled smartphone accesses the database after a photo is taken. Is it a database that the military or intelligence community has and maintains, or is it just a database on the phone itself?*

SCHUEPP: A little bit of both. There is no secret to the fact that the DoD has the large database, and they keep track of basically people who are outside of the U.S.; there are no U.S. civilians in the database – that is a separate system. That is the kind of system you have for the FBI, for people who are wanted, etc. But the military has a large database. BIMA, which I previously mentioned, maintains these very large databases with people of interest to the military.

The other process that happens is database access by a [system or] systems distributed by different military control centers in the field offices. We call them a forward operating base, and those forward operating bases have access to those databases. That's what can be accessed by mobile devices such as the Android smartphones.

MIL EMBEDDED: *Is there any range of distance for database access, for example, could someone in Afghanistan use this to access these databases you have referred to in the States?*

SCHUEPP: They could access them if they are authorized to. Everything is set up on the secure, secret networks that the military uses. They are very, very secure beyond your imagination, and so if the Marines or if Special Forces are authorized to use them, then they can. But to me, [this kind of access] is almost like having a weapon: They really have to be authorized for use.

MIL EMBEDDED: *Are you referring to SIPRNet and NIPRNet?*

SCHUEPP: That is exactly the type of networks they would be used on.

MIL EMBEDDED: *Your press release also said something about this being used in conjunction with a cloud system?*

SCHUEPP: Yes. Everything we've built is based on a cloud architecture, which allows your capability to expand, to be able to have capacity of very large databases, and have capacity to support thousands of people sending in pictures/photos at once while expecting a good response time.

MIL EMBEDDED: *So the military is putting some of its databases in the cloud?*

SCHUEPP: The military is, definitely. The DoD is definitely going with a cloud architecture. They have been building that now, and all their information systems are starting to go cloud.

MIL EMBEDDED: *What role does the cloud play in accessing the biometric information?*

SCHUEPP: The cloud has two purposes: the database and the processing. The good thing about the database: It provides for high capacity and redundancy. To build a real cloud system, you have all kinds of backup and redundancy should something break. So it protects your data.

On the processing side, you can enable tens or hundreds of computer nodes to support your processing, so you can get very high throughput and with high capacity.

MIL EMBEDDED: *Do all of your customers use the cloud?*

SCHUEPP: We have customers who are not cloud based and they operate fine. It's all about what the requirements are for what they are trying to do. For example, we have a system installed that runs a jail management system. It uses face recognition to keep track of the prisoners. So that was designed so that you'd be able to handle 100,000 prisoners. The department, in this case the sheriff's department, that purchased the jail management system bought a certain-sized capacity computer system and their face recognition system works fine. Now if they are going to expand, that jail system expands, it doubles, they are going to have to supply more computer power and more storage. And they are going to have to create the specifications, the throughput and capacity needs. They are going to have to design that. If they had it on a cloud system, they could just turn it on like you and I turn the water on, like just give me more.

MIL EMBEDDED: *Some of your face biometrics applications are described as a "localized" application on mobile devices. Are they localized to the phone?*

SCHUEPP: Yes. We are calling that an "embedded system." We are now able to do face matching and have a database actually on the device itself, not necessarily in the cloud, or it could be in both. So if you lose your communications or you don't want to use your communications, we now have the technology that can do that locally right on the device itself.

MIL EMBEDDED: *So how does the localized database update?*

SCHUEPP: Your face database will get updated when you synchronize. It is kind of similar from a conceptual point of view to when you update your mail with Google or Microsoft Outlook. You have your email on your computer locally and then when you plug into the network, it automatically synchronizes and updates your main Gmail system somewhere out there. Same concept.

MIL EMBEDDED: *What are the pros and cons of using a localized database?*

SCHUEPP: The disadvantage is that you might not have access to the entire database. But one advantage is that localized is faster; the other advantage is, if you don't have comms at all because you're off the grid – as you can imagine soldiers often are – they can still have the same functionality for their mission.

MIL EMBEDDED: *Are these COTS smartphones that are used with face biometric software? Can I use it on my iPhone that I am using right now?*

SCHUEPP: Yep you could. But we don't have it available as a consumer app to download. We sell it separately, directly to enterprises or directly to government agencies. The reason

is that it accesses a face recognition system [that accesses] a database of faces, like the Department of Motor Vehicles or the FBI most wanted list or sex offender lists. So those are usually government-owned databases. So it's not necessarily available to the consumer.

But the new wave of the future is for the military is to use more COTS, like Android, Motorola [smartphones], and so on. And in some cases, we're seeing that law enforcement and the military are using Apple phones now and iPads.

MIL EMBEDDED: *What about the Raptor ID smartphone mentioned in your PR?*

SCHUEPP: We [have entered into] a partnership with Raptor ID, and they make a military ruggedized Android device [RaptorOne], which has three biometrics on it – the face, the fingerprinting, and the iris scanning – but it is also very rugged to the point where if a tank rolled over it, it wouldn't break. It is purpose-built for the military's use in the field.

MIL EMBEDDED: *So that's a proprietary smartphone?*

SCHUEPP: Yes. But it's only proprietary in a sense like anything is proprietary: It's their device. But what makes it not proprietary is that it uses Android and that it runs on a standard mobile phone network like GSM cellular. And the military has its own protocols of cellular networks, and that will be available with that device from Raptor. **[Editor's note: For more info on Raptor ID's RaptorOne ruggedized biometric smartphone, go to: www.raptor-id.com/products/raptorone.]**



NEW COM Express® Type 6 Carrier Boards

Connect Tech Inc.
Embedded Computing Experts

- PMC/XMC & Mini-PCIe Expansion
- Type 6 & Type 2 Compatibility
- COM Express® Basic Size (95 x 125mm)
- 1U Rack Mount Designs
- -40°C to +85°C

Supports most current processors including 3rd Generation Intel® Core™ i7 and Type 6 COM Express® features including USB 3.0 and DisplayPort

www.connecttech.com • sales@connecttech.com • 519.836.1291

SCHUEPP: There are several projects involved with different military agencies doing just that. I'm not at liberty to disclose who they are and how they are using them, but the general sense, as I have kind of already explained, is that I don't know that any are deployed today as a program of record. In other words, it's in production. In most cases, they are being used as prototypes and are still under test at this stage.

SCHUEPP: We are looking forward to a lot of things as we go into 2013. The face biometric software will become recognized as a necessary instrument and tool for use in intelligence. It is going to be the way to keep people safe, safer than using guns actually. If you know who people are, then you know how to

In the future five years from now, three years from now, what is needed is for the military to deploy this technology and use it. And that's easily said but not easily done. Let's face it, the Army, the Navy, all those guys – very large organizations, a lot of data, large systems – take a lot of coordination, a lot of program management to get systems in play and to complete testing and training. **MES**

603-447-5600 | www.animetrics.com



**CHASSIS
PLANS**
Systems Engineered to Perform®



PC/104 CONSORTIUM

Maintaining & Distributing PC/104 Specifications

- PC/104-Express & PCIe/104
- PC/104, PC/104-Plus & PCI-104
- EBX & EBX Express
- EPIC & EPIC Express



All specifications are FREE for download

Choose PC/104...

- Backward Compatible
- Forward Looking
- Latest PC Technologies

Visit us to learn about PC/104, search for products and more!

WWW.PC104.ORG

Black Beauty



OpenVPX

VPXI-ePC

Racehorse Performance with our
4U 1/2 Rack OpenVPX Windows/Linux Computer
featuring an i7 CPU and Four Expansion Slots

Features

- i7 w/8 GB RAM, Gb Ethernet, 4x USB, Displayport, 256GB SSD+3 SSD drives
- Supports all Innovative XMC and VPX modules
- PCI Express and SRIO planes interconnect all I/O cards
- Integrated timing and triggering with synchronized, multi-card sampling
- Ultra-low phase noise sample clock from 0.125 to 1 GHz
- 10MHz, 0.5 ppm stable clock reference, GPS optional



FrameWork Logic



**Innovative
Integration**
a subsidiary of ISI

... real time solutions!

805.578.4260 phone • www.innovative-dsp.com

Life cycle management: The COTS perspective

By Mark Grovak

Application stability and predictability are essential for deployed COTS-based mission-critical military systems, which tend to have an in-service life long far longer than the typical commercial production period of some of the system's key components. To ensure that a system design can be supported for the full duration of the long life cycles demanded by these programs, system designers need to be familiar with the their life cycle management plan options, both from their COTS vendor partners and services they can develop themselves internally. Key life cycle management services include ongoing review of product configuration changes and component obsolescence, a quarterly Bill of Materials (BOM) health check, and a longevity of repair plan. A closer examination of the volume production phase, the post-production phase, and component storage and handling is vital when deciding which road to obsolescence management best meets a company's life cycle management needs.



U.S. Marine Corps photo by Sgt. Jesse J. Johnson

A comprehensive life cycle management strategy is the key to safeguarding programs and mitigating the challenges associated with COTS technology deployed in long-term mission-critical systems. In addition to reducing risk, life cycle management services cut costs by ensuring timely purchase and banking of End-Of-Life (EOL) components and greatly reducing the logistical burden. Without these services, the system designer must maintain ongoing visibility at a piece/part level with multiple OEMs, some of whom might not have had a process for providing proprietary data about component life cycles. Today, leading suppliers enable many of these services to be accessed via a dedicated website that provides 24/7 delivery of life cycle management information such as product health reports and baseline configuration data packages. Even better, Web-based life cycle

management services enable system designers to easily and quickly access, approve, or reject engineering change proposals via the Internet.

The wide range of life cycle services to consider includes updates and reporting on product configuration changes and component obsolescence issues. System designers also need control over product configuration changes and visibility into component obsolescence issues. Variant creation enables assembly and release of a unique production build package. Working with their vendors, system designers can develop plans to ensure longevity of supply that extends the product build capability beyond the standard production period. Similarly, a longevity of repair plan extends the product repair capability beyond the standard repair period. Component storage and handling provides the option of storing

selected components at the COTS vendor's facility for future builds or repairs.

Configuration changes and component obsolescence issues during a product's volume production phase need to be well understood. Program authorities must be able to determine the timing of a lock-down on a specific configuration or know when to migrate to a newer one. Having the ability to approve or reject a COTS vendor's engineering change proposals could be critical to meet specific program requirements and to avoid costly requalification activities. Life cycle management services that are of great value during the volume production phase include visibility service and control service. And the post-production phase and component storage and handling are key considerations as well when implementing an effective life cycle management strategy (Table 1).

Key stages and elements of life cycle management

Volume production phase	Post-production phase	Component storage and handling
Visibility services Class I Engineering Change Orders (ECOs) Class II Engineering Change Orders (ECOs) Quarterly Bill of Materials (BOM) report Component obsolescence Risk mitigation strategies Control Service Approve/Reject ECOs Quarterly BOM report Last time buy info Risk mitigation strategies	Longevity of Supply (LOS) Approve/Reject ECOs Quarterly BOM report Current and predicted obsolescence Component LTB info Risk mitigation strategies Product baseline configuration data Revision and ECO history Longevity of Repair (LOR) Approve/Reject ECOs Quarterly BOM report Product baseline configuration data Revision and ECO history	Segregation of components in secure warehouse Annual inspection and count

Table 1 | Effective life cycle management services encompass the volume production phase, post-production phase, and component storage and handling.

The volume production phase

Visibility services expose both Major (Class I) and Minor (Class II) Engineering Change Orders (ECOs) that are applied to the product by the COTS vendor during the active service period. Included in a visibility service process is a quarterly Bill of Materials (BOM) health check that highlights current component obsolescence (at the integrated circuit, or IC level) and identifies risk mitigation strategies.

A control service provides system designers with control over their product's configuration, including the authority to approve or reject all Major (Class I) and Minor (Class II) ECOs that are proposed by the COTS vendor during the contracted service period. Included in control service is a quarterly BOM health analysis report that details current and predicted component obsolescence (at the integrated circuit, or IC level), provides component Last-Time Buy (LTB) information, and identifies risk mitigation strategies. Such a service can also provide a product baseline configuration data package and a complete revision and ECO history.

The post-production phase

The natural course of events is that the volume production phase of a product will eventually end because of a high level of component obsolescence or diminishing customer demand. Before this happens, the COTS vendor should announce a LTB opportunity for a product. Two life cycle management services that should be in place to support the post-production phase of a product's life include a Longevity of Supply (LOS) service and a Longevity of Repair (LOR) service.

USB Embedded I/O Solutions

Rugged, Industrial Strength USB



16-Bit Multifunction Analog I/O, Up to 140-Channels 500kHz



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



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

USB/104® Embedded OEM Series

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

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

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



USB 2.0

Saving Space, The Final Frontier



ACCES I/O PRODUCTS, INC.
 The source for all your I/O needs
 To learn more about our Embedded USB/104® I/O boards visit <http://aces.io>
 or call 800 326 1649. Come visit us at 10623 Roselle Street San Diego CA 92121






USB PC/104 USB/104 Systems

LOS service

The LOS service is ideal for system designers who have a long production run and who are not in a position to requalify a new configuration or take immediate advantage of newer products via technology insertion. An effective LOS plan secures the continued manufacturing capability for a given product and ensures that the tools, test equipment, and expertise will be in place for continued builds and repairs after the last order date has expired. It provides system designers with continued control over a product's configuration, including the authority to approve or reject all Major (Class I) and Minor (Class II) ECOs that are proposed by the COTS vendor during the contracted service period. LOS should include a quarterly BOM health analysis report that details current and predicted component obsolescence (at the integrated circuit, or IC level), component LTB information, and risk mitigation strategy identification. LOS should also provide a product baseline

configuration data package and complete revision and ECO history.

When used properly, LOS guides system designers to purchase obsolete components to meet build requirements, as detailed in the quarterly BOM health analysis reports. The COTS vendor should assign new part numbers to identify customer-owned inventory and update the manufacturing BOM via an engineering change order.

LOR service

LOR is an ideal option for system designers who have a long in-service horizon and want to repair fielded circuit card assemblies past their COTS vendor's standard repair horizon. LOR service secures the continued repair capability for a given product and ensures the tools, test equipment, and expertise will be in place for continued repairs after the established last repair date. It provides system designers with continued control over a product's

configuration, including the authority to approve or reject all Major (Class I) and Minor (Class II) ECOs that are proposed by the COTS vendor during the contracted service period. A quarterly BOM health analysis should report current and predicted component obsolescence (at the integrated circuit, or IC level), provide component LTB information, and identify appropriate risk mitigation strategies. The LOR service also should provide a product baseline configuration data package and complete revision and ECO history. As in the LOS service, the quarterly BOM health analysis reports will provide guidance to the system designer for purchasing obsolete components to meet repair requirements.

Component storage and handling

Another key element for an effective life cycle management plan is component storage and handling. It can be very efficient and helpful for components to be stored for the system designer at the COTS vendor's facility. Storing the



microhard SYSTEMS INC.

Wireless Digital Data Link

Bidirectional Digital Data Link:

- Miniature Size (1.25" x 2" x 0.5")
- Starting at only 25 grams!
- Up to 12 Mbps data rates
- Extended temperature (-40°C to +85°C)
- Long distance range
- Enhanced sensitivity
- Strong interference rejection
- Simultaneous Ethernet & serial data

Frequencies available from 300 MHz to 6 GHz

Contact us: 403.248.0028 - info@microhardcorp.com



SDR - WinnComm
Wireless Innovation Forum Conference
on Wireless Communications Technologies
and Software Defined Radio

8-10 January 2013
Wardman Park Marriott, Washington, DC

Join us in Washington, DC, to **network** with customers, competitors, suppliers and the research community and **keep up to date** on the latest innovations in radio technologies. The **ONLY event of its kind** devoted to the advancement of radio technologies from research through deployment, **SDR-WinnComm features:**

- Top-notch **keynotes** from industry leaders
- 3 days of **technical presentations** and **tutorials**
- **Workshops** on LTE, DSA, and Public Safety
- **Product Expo and Tech Showcase**
- **Concurrent Technical Interchange Meeting**

Platinum Sponsors: GENERAL DYNAMICS C4 Systems, HARRIS, indra, OIS, SELEX ELSPR
Gold Sponsors: PENTEK, GENERAL DYNAMICS C4 Systems
Media Sponsor: Military EMBEDDED SYSTEMS

Conference.WirelessInnovation.org

inventory of components at the COTS vendor's site can facilitate timely builds and repairs. Proper storage and handling should include segregating the system designer's inventory in a secure area of the COTS vendor's warehouse. These valuable components should be kept in nitrogen-purged, evacuated bags to protect components from moisture, oxidation, and electrostatic discharge, and there should be a plan for periodic bag inspection to ensure they remain intact. And, at least once annually, the bags should be opened so that a physical count of the material can be performed to ensure that all inventory is accounted for.

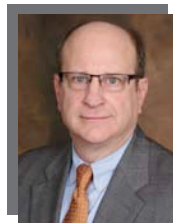
An example of a comprehensive life cycle management service is Curtiss-Wright's Continuum Life cycle Services. It is an interactive, Web-based system that provides the information the customer needs to make informed decisions. This service can be tailored to the needs of each individual program and is designed to identify and reduce the risks of COTS component obsolescence, provide control over product configuration changes

when required, and extend the availability of product builds and repairs to meet program demands. It includes ongoing reports to provide actionable advanced data that enables decisions to be made in a timely fashion. In the event that a silicon vendor announces a last-time buy, this keeps the system designer informed so that the organizations can work together to conduct the appropriate purchases to enable long-term repair to systems and guarantee repair for the program's specified timeframe.

Winning the battle against obsolescence

Winning the fight against obsolescence, while obtaining the full performance and economic benefits of using COTS electronics, requires a comprehensive life cycle management plan. A successful strategy should include an ongoing review of product configuration changes and component obsolescence, a quarterly BOM health check, and a longevity of repair plan. The result, especially if your life cycle management plan is put in place at the front-end of your program development cycle, will be application

stability and predictability. Early adoption of these services is economic, in that it enables the costs to be more effectively amortized over the program's overall budget. Proactive life cycle management, especially in today's budget environment, enables deployed systems to stay in service, an increasingly attractive option compared to the high cost of system redesign. **MES**



Mark Grovak is the Avionics Business Development Manager at Curtiss-Wright Controls Defense Solutions, respon-

sible for its avionics strategy. He has been involved in logistics support as a U.S. Navy Supply Corps officer and in establishing and managing repair depots. Contact him at Mgrovak@curtisswright.com.

Curtiss-Wright
Controls Defense Solutions
613-254-5112
www.cwcdefense.com

Esterline
Communication Systems

ECLIPSE ELECTRONIC SYSTEMS

DIGITAL SDR RECEIVERS	RF DISTRIBUTION MODULES	GPS TIME/FREQUENCY MODULES	INTEGRATED HW SUITES
--------------------------	----------------------------	-------------------------------	-------------------------



NOWHERE TO HIDE.....
20 YEARS OF FORCE PROTECTION

SUPPORTING SOFTWARE DEFINED SIGINT ARCHITECTURES OF THE FUTURE

WWW.ESTERLINE.COM/SIGINT - TEL: (972) 699-8580

PG OFF OWEN CHEVERTON/UK MOD CROWN COPYRIGHT, 2012

Software compounds the challenges of military component obsolescence

By Colin Doyle and Stephen Denman

Component obsolescence in military embedded applications will become one of the epic challenges of this century as software overtakes hardware as the primary means of innovation on and off the battlefield.



U.S. Navy photo by Mass Communication Specialist 3rd Class Raul Moreno Jr.

Component obsolescence in military systems and products is a well-known challenge, but it has developed a relatively new twist: the rapid increase in volume of embedded software. While software has been embedded in military electronic components to some extent for decades, that trend has accelerated to a fever pitch in the past decade; more and more of the critical functionality of our systems and products depends on software. Figure 1 illustrates the dramatic increase in embedded software as measured in source lines of code in U.S. military fighter aircraft over the past several decades. Similarly shaped curves can be found in most other complex military systems and products, including all other aircraft, naval vessels, ground vehicles, C4ISR systems, and off-battlefield supporting systems.

In fact, many in the aerospace and defense industry would claim that software has long since overtaken hardware as the primary source of innovation. Software, like hardware, is not immune to issues that require upgrading or replacement of those components. However, unlike hardware, those issues tend to be of a different nature and thus require different treatment.

Hardware is like people – Software is like wine

One of the biggest differences between hardware and software components is that hardware tends to degrade with time and usage, while software remains unchanged. Given the same inputs, the software will generate the same results every time. Hardware, on the other hand, will eventually break down or stop

performing to specification because of wear, corrosion, and/or fatigue cracking as it reaches or exceeds its operating life.

That is not to say that software does not contain flaws; it is just that such flaws are latent in the software when it is produced, rather than introduced over time through usage. Software is not “manufactured” in the same sense as hardware. Once a software component is developed, it can be replicated at essentially zero cost and with zero defects introduced by the automated replication process. The reliability of software components tends to exhibit a “bathtub” shape, where initial usage reveals many of these latent defects, which are then addressed through software updates, followed by a relatively long period of low defect rates, and then a growth in issues as the original design assumptions and constraints that were the basis for the software component are invalidated as the operational environment changes. Like wine, software components tend to improve with time, as more of the latent defects are discovered and addressed.

Given software does not have the tolerancing issues associated with hardware manufacturing, nor does software wear out through usage, the traditional hardware obsolescence measures such as Mean Time Between Failure (MTBF) do not have much relevance for software. So if software just gets better with age, how does it compound the military component obsolescence challenge? To answer that, we need to understand what can cause software to become obsolete.

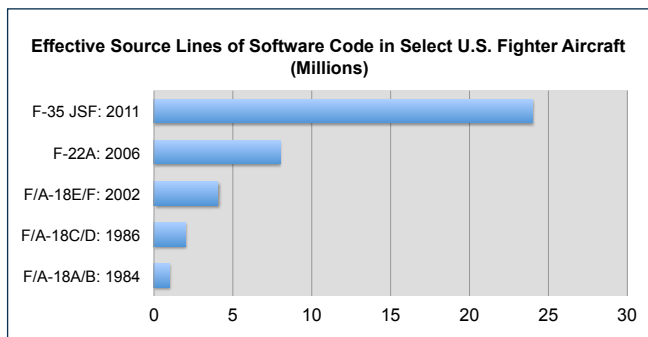


Figure 1 | Effective source lines of software code in select U.S. fighter aircraft from 1984 to 2011

Root causes of software obsolescence

There are three main reasons why a software component can become obsolete:

- › Changes in the environment the software must run in (compatibility)
- › Exposure of latent defects
- › Changes in the role and function the software must perform

Software is merely a sequence of coded instructions that governs the behavior of the hardware platform on which it executes. Software components rely on the underlying electronic component to provide the correct interfaces and behave as specified. Thus, a major factor in software obsolescence is the change in the underlying hardware platform because of electronic component obsolescence. Electronic component obsolescence is a well known problem, because of the rapid change in underlying technologies, and the relatively low volume of military procurements as compared to commercial applications. Whenever the underlying electronic components that software interacts with or runs upon change, the software must also be reevaluated and possibly upgraded or replaced as well.

A classic example of this is the Ariane 5 flight 501 in 1996, which ended in the destruction of the rocket 40 seconds after launch. The root cause of the failure was the reuse of an inertial reference system from the Ariane 4 without proper evaluation of the constraints and assumptions behind that subsystem in the context of the Ariane 5 design. The inertial reference system was reused as it was supposedly a validated and proven design. However, that system was designed for a rocket with less power and significantly less horizontal acceleration in its launch profile than the Ariane 5. A conversion of a floating point value into a 16-bit integer triggered an overflow error, causing the flight control system to crash.

Obviously, when defects are found in software components, they must be addressed. Depending on the nature of the software component and its associated hardware environment, performing such updates in the field can be as easy as downloading the update over a network connection, or as expensive as replacing an entire electronic component. The larger cost with software components is the development effort required to analyze the defect, update the design and implementation,

and revalidate the component before releasing it. This cost is often larger because the opportunity for an update often leads to the third reason: changes to the role and functionality of the software component.

As mentioned earlier, software is increasingly the source of product innovation. It is a key system integration technology, and the lives of many systems are extended through software upgrades. In the current military procurement environment, where “just-in-time” approaches to spares procurement are becoming more common, any software update opportunity typically involves enhancements to extend the life of systems or extend capabilities, as well as address defects. As hardware platforms become more powerful, more and more functionality is allocated by systems engineers to software, to save weight, reduce cost, and increase flexibility. It is these properties that have led to the drastic growth in the amount and complexity of software in military systems.

Software engineering: Not just plug and play

With components other than electronics and software, dealing with obsolescence is primarily an issue of finding an alternate manufacturing source for the component. With software, as mentioned, manufacturing is not the issue; component obsolescence requires reengineering that software, whether it is to resolve a defect or to extend and enhance its functionality.

As mentioned earlier, one of the factors that contributes to software obsolescence is changes to the context that the software must operate in – both the platform and signals it interacts with and the goals and roles of the system that the software enables. This context needs to be taken into account when reengineering software components, and too often it is not properly addressed.

Rapid growth in software complexity, the need to update software components within a systems engineering context, and the intangible nature of software all contribute to the challenge of updating and maintaining software components. The same high-level language abstractions that support development of more complex software also increase the challenge of isolating defects and determining the impact of proposed changes.

Traditionally, technical data packages for software component maintenance have focused on the source code as the artifact most closely related to the final software component, with less emphasis on the rest of the software artifacts, and little cohesiveness across the artifacts. Without full traceability between requirements, design, implementation, and verification artifacts, it is too easy to miss subtle dependencies that need to be taken into account. Tactical “patching” of software component source code can lead to monolithic, hard-to-maintain software. A more cohesive, holistic approach to software components needs to be taken to properly manage their complexity. Such an approach is known as Application Life cycle Management (ALM). ALM manages all the artifacts and activities required to define, design, implement, and verify software components (and the relationships between those artifacts and activities).

Conquering the epic challenge

While the growth in embedded software is a challenge, it is also a great opportunity, particularly with the current military procurement environment, where both cost containment and strategic advantage are demanded. Software development principles, practices, and tooling are maturing and continually improving. The following recommendations can go a long way toward taming the software challenge of component obsolescence:

1. Take a systems engineering approach to electronic and software component development, with deliberate planning and architecting of modular components that support reuse across different systems, with well defined interfaces between components to manage the complexity. Ensure that requirements and key design decisions that drive component definition are captured and managed for the service life of the systems using those components.
2. Implement a holistic ALM approach to software component development, with full traceability across all artifacts and activities and consistent processes managing all aspects of development. Invest in tooling to automate and enforce ALM practices; look for systems that provide a single process engine for managing all artifacts,

with strong ties to systems engineering and hardware engineering such as PLM systems. Manage the entire tool chain, including the build and release management system, to ensure predictable results when maintaining or updating software components.

3. Use iterative and incremental development practices to shorten feedback cycles and improve predictability and quality of component releases. Involve all disciplines, hardware as well as software, in component updates to ensure that any dependencies between components are understood and fully addressed. Implement proactive variant management to maximize reuse of components and control sources of variation such as changing roles or technologies.

With these recommendations in place, military system designers can use software to create differentiation between variants rather than hardware, with potentially lower costs and less weight and power consumption. Manufacturers are finding that designing products based on a generic hardware platform that is capable of supporting all product line variant functionality while using software to create the individual variants offers numerous advantages. **MES**




Colin Doyle is a Senior Product Manager within the ALM Segment of PTC. Colin has three decades of experience in systems engineering and software development, in fields as diverse as avionics, remote sensing, satellite communications, medical devices, precision laser systems, enterprise content management, and Application Life cycle Management. He has extensive expertise in software change and configuration management, agile and lean software development, and regulatory compliance issues. Colin has a B.A.Sc. from the University of Toronto in Engineering Science and an MBA from Wilfrid Laurier University. He can be reached at cdoyle@ptc.com.



Stephen Denman is on the ALM Solutions Marketing team at PTC, focusing on systems engineering and integral product/software life cycle management. He has worked in software and systems engineering since 1982, in areas including weapons systems, C4ISR, flight systems, embedded software development, information technology, application development, CAD/CAM/CAE, and product/software life cycle management. Steve has BSEE and MSEE degrees from Texas A&M University. He can be reached at sdenman@ptc.com.

Solid or Spin...


we go both ways



Ruggedized VPX Drive Storage Module

Whatever your drive mount criteria, everyone knows the reputation, value and endurance of Phoenix products. The new VP1-250X, compatible with both solid state or rotating drives, has direct point-to-point connectivity or uses the PCI Express interface with the on-board SATA controller. It is available in conduction cooled (shown), conduction with REDi covers (VITA 48) and air cooled (shown) configurations.


We Put the State of Art to Work



PHOENIX
INTERNATIONAL

www.phoenixint.com • 714-283-4800

PHOENIX INTERNATIONAL IS AS 9100 REV C / ISO 9001: 2008 CERTIFIED



PTC

781-370-5000

www.ptc.com

 @PTC

 @PTC_Integrity

 @PTC_Windchill

Our technology investments protect yours.

VME

CompactPCI

VPX



Whatever direction you choose, Aitech has the map!

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

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

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

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

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

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

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



Aitech 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



Obsolete components: What is the COTS life cycle costing you?

By Kaye Porter

Now more than ever, long-lasting embedded systems require proactive obsolescence management. Because of growing legislative and environmental requirements and shrinking budgets, program managers and sustainment teams are forced to take another look at COTS end-of-life-cycle costs – and how to avoid them. A proactive obsolescence management solution is the key.



When looking at supporting legacy systems, obsolescence management typically falls into two categories: acquisition, and logistical planning and sourcing. However, “product support, vital to both acquisition and logistics, has been treated as the stepchild of both functions”[1]. With the need for obsolescence management invisible until the clock has run out, reactive obsolescence mitigation now falls to engineering teams ... who then face the costs of recertification and working without access to critical IP.

A 2011 study published by the Air Force Science and Technology Board and sponsored by the National Research Council (NRC) estimated that 65 percent or more of Weapon System Sustainment (WSS) comes from supporting the system, meaning most of the program costs come after the system is initially rolled out. The Air Force requirement on the Weapons System Sustainment program alone continues to grow, and is currently projected to top

\$14.3 billion, nearly 32 percent of the Air Force O&M FY2012 budget[2]. Figure 1 depicts the USAF’s FY2012 WSS budget.

In this climate, the need for collaborative, proactive obsolescence management has never been more critical to support the modern warfighter.

Additionally, with the growing budget cuts and the National Defense Authorization Act for FY2012 (NDAA for FY2012) anti-counterfeiting laws, the defense industry more than ever requires proactive obsolescence management solutions, to ensure predictable costs and counterfeit mitigation throughout a system’s life cycle.

The COTS waterfall effect

In 2003, Senator Joseph A. Lieberman reported that “DoD and intelligence agencies will need to be first adopters of the most advanced integrated circuits, and will be increasingly dependent on such chips for a defense and

intelligence edge.”[3] In the time since his report, the embedded industry has seen the evolution of this prediction, not only in defense industry technology and the need for interoperability, but also in the growing challenges DMSMS teams face when it comes to sustaining long-lasting technology.

From its beginning in the 1950s, the semiconductor industry relied heavily on innovation funded by the U.S. defense industry while consumer markets remained relatively small. Today, the semiconductor industry has grown to \$300 billion annually, while supporting a \$1.3 trillion electronics supply chain[4]. However, as the consumer and commercial markets have expanded, the influence of the public sector versus the private sector has reversed, leaving the United States military accounting for less than 2 percent of the total semiconductor market[5].

This reduced presence offers less control when DoD programs find themselves

Air Force Weapon System Sustainment Budget for FY2012

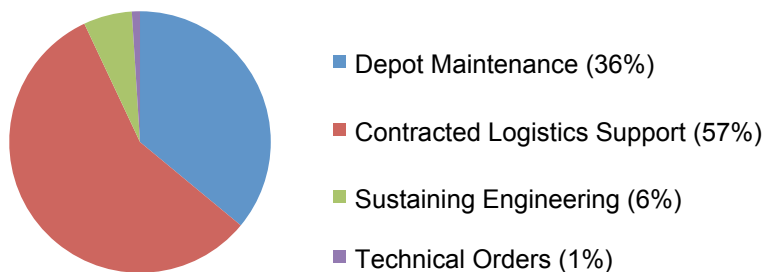


Figure 1 | USAF FY2012 WSS budget – Note: This does not include depot-level repair and consumable supplies – an additional \$2.6 billion. These costs in total bring the WSS overall sustainment spending in FY2012 to \$14.3 billion, nearly 32 percent of the Air Force O&M budget. Source: National Academy of Sciences, Examination of the U.S. Air Force's Aircraft Sustainment Needs in the Future and Its Strategy to Meet Those Needs (2011) pg. 74

hit by the shorter commercial life cycles and sourcing challenges when new disruptive technology is introduced to the market. In this environment, a "reactive" approach to obsolescence, such as waiting for an EOL or Product Change Notice (PCN), becomes both dangerous and expensive. The impact of components on an entire system is illustrated clearly in programs like the F-22 Raptor, which avionics systems required four technology refresh cycles before beginning production – and before it was ultimately shut down in December 2011.

NDAAs for FY2012 effects on End-of-Life

This treadmill of advancing technology is nothing new to experienced defense industry engineers. New systems are introduced, they are easy to support for a number of years before parts become scarce, procurement teams jump through hoops to get parts wherever they can, and only after all other options are exhausted, program managers call the engineers to design out electronic component obsolescence. And then the next list of parts becomes scarce, and the treadmill relentlessly continues.

But until recently, sourcing legacy components wasn't examined closely enough to give absolute confidence in 100 percent parts authenticity. Components could be sourced from any number of independent distributors globally, or even from eBay. The "heyday" of component sourcing and brokers ended in 2007, when NAVAIR asked the Bureau of Industry and Security's Office of Technology to conduct an assessment of

counterfeit/defective electronics within the DoD supply chain. The resulting report spurred a chain of events, leading to the 2012 National Defense Authorization Act, Section 818 – and an increased scrutiny of anyone dealing with obsolete components within the DoD supply chain.

The legislation goes beyond simple scrutiny, making it a crime punishable by a fine of up to \$2,000,000 for individuals and \$5,000,000 for companies involved in their first offense – and up to life in prison for an individual whose conduct, in violation of the statute, results in a death. With such serious consequences, OEMs and contractors are reexamining how they sustain legacy embedded systems.

Groups such as the Aerospace Industries Association (AIA), SAE International, and the Independent Distributors of Electronics Association (IDEA) are partnering with industry experts to develop new testing standards and best practices. New technology such as RFID tagging, DNA marking, and component encryption will be available moving forward. However, the details and definitions of "counterfeit," "suspect counterfeit," and "fraudulent" – and what counts as reasonable due diligence – are still being ironed out.

In the meantime, OEMs and defense primes are left in an uncomfortable void when it comes to sustaining legacy systems. Some defense projects could see up to 70 percent of their components go EOL before they're even out of the design phase; consequently, risks and

due-diligence costs of continuing to support longer-lasting technology by sourcing components from the broker market are being heavily weighed by manufacturers throughout the entire defense supply chain.

Before the legislation, many OEMs saw unfunded sustainment of older products as a "best endeavors" offer for their military customers. Now everyone is taking a renewed focus on mitigating their "best endeavors" risk of sourcing parts from independent brokers.

The reactive obsolescence management cycle

Proactive obsolescence management on the embedded board and component level is imperative at the beginning of new projects, to ensure that legacy systems won't be shut down. While OEMs often notify customers of major changes and EOL notices, teams who aren't direct customers and source through distributors might not see the notifications in time to take action. The typical 3- to 6-month Last-Time-Buy (LTB) notification provides limited proactive visibility for components on which long-lasting systems rely. Because of this, program managers (and engineers!) face unpleasant surprises when notified of a last-time-buy situation from logistics teams. Even with access to critical IP, including Bills of Materials (BOMs), engineering teams are often left to mitigate obsolescence on a reactive, part-by-part component level, sometimes with a complex substitute part or complete redesign.

In reaction to these unpleasant surprises, logistics teams will make a "lifetime buy" to secure authentic parts and materials to support the military system. While certainly guaranteeing a degree of product security, a lifetime buy only works if both the repair needs and application life cycle can be accurately forecasted, and if funding can be secured. If underestimated, the program will be left little option but to radically reengineer the system. If overestimated, the program is at risk for overstocking components and parts for a system no longer in use.

In the cases where the system's life cycle was underestimated, obsolescence

management solutions then fall to engineering teams, who are working to comply under current legislation, struggling under budget constraints, lacking access to original IP, and fighting sliding repair and service timelines. The Defense Microelectronics Activity (DMEA) currently estimates that a single incident of obsolescence can run up to \$2.4 million and 64 weeks to resolve. One way to estimate reactive cost impacts on an embedded board is by counting ASICs. Each obsolete ASIC could cost up to \$1.5 million per

component, not including recertification fees, and costs of downtime and repair.

When a project reaches redesign, program managers can find themselves looking at anywhere between \$80,000 and \$2 million and between 42 weeks and 64 weeks (NRE cost metrics from DMSMS), not including testing and recertifying the entire system. In an environment of budget cuts and Performance Based Logistics (PBLs), these ballooning costs can be a system's death sentence.

Visibility is critical

When a global product integrator discovered the \$15-\$30 ASIC components they relied on to support an in-flight navigation system were no longer available, it created an abrupt transition of focus for the program. Facing component shortages and without a lifetime buy option, follow-on support became impossible without either a single component redesign or a "proactive" \$3.3 million system redesign, neither of which was budgeted for on a \$750 board.

Unless a defense contractor has visibility into the OEM's life cycle and supply chain, these surprises aren't the exception, they're everyday occurrences. Obsolescence management requires collaboration across the supply chain, between acquisition, logistics, and engineering teams. To meet anti-counterfeit requirements from the NDAA for FY2012 and the current budget environment, OEMs and systems integrators need to ensure proactive processes and solutions are in place (Figure 2).

Proactive solutions require collaboration across departments:

- › **Life cycle analysis** – including BOM analysis, upcoming regulation investigation, and component presourcing.
- › **Proactive visibility** – maintaining direct contact with Original Equipment Manufacturers (OEMs) and Original Component Manufacturers (OCMs) across the supply chain, signing up for LTB notifications and PCNs, especially if components are not sourced from the original manufacturer.
- › **Up-to-date processes** – including how components are verified, steps to prove traceability, supplier audit notes, and listed trusted suppliers for EOL components.
- › **Proactive funding requests** – taking into account upcoming strategic maintenance schedules and the fact that sustainment requires ongoing engineering. Project managers who have planned early for sustainment will have more access to timely and lower-cost solutions, before there is a problem.



QUALIFIED TO PERFORM.

Cisco Technology - Ruggedized

As a Cisco Solution Technology Integrator, Parvus repackages the best in COTS Cisco IP networking technology into ultra-rugged routing and switching C4ISR subsystems optimized for SWaP, hardened for extreme shock/vibration/thermal conditions, and qualified to military standards.

Parvus

DuraMAR 5915 

- Rugged Cisco IOS Mobile Router
- Integrated Gigabit Ethernet Switch
- Designed for MIL-STD-810G, 461F
- Size, Weight & Power (SWaP) Optimized

www.parvus.com | 800.483.3152 | sales@parvus.com | facebook.com/ParvusCorp

Established legacy sourcing and manufacturing experience offers visibility into the life cycle of an entire embedded system and saves project resources. Ideally, an onsite sustainment team has these solutions outlined during the design phase, to prevent reactive obsolescence management. However, that isn't always the case, and an experienced extended service provider can help close critical gaps anywhere within a program's life cycle.

Mitigating obsolescence

In the end, it is critical to acknowledge obsolescence isn't an event that might happen once in an application's life cycle; rather, it's inevitable for long-life systems. To support an application through its end-of-life, programs require ongoing planning and life-cycle analysis to determine tasks, accountability, procedures, and maintenance schedules. Working with an extended service provider such as GDCA provides necessary visibility, extended manufacturing, out-of-warranty repair, and authentication for when critical system components are no longer available. **MES**

Proactive Obsolescence Management Architecture

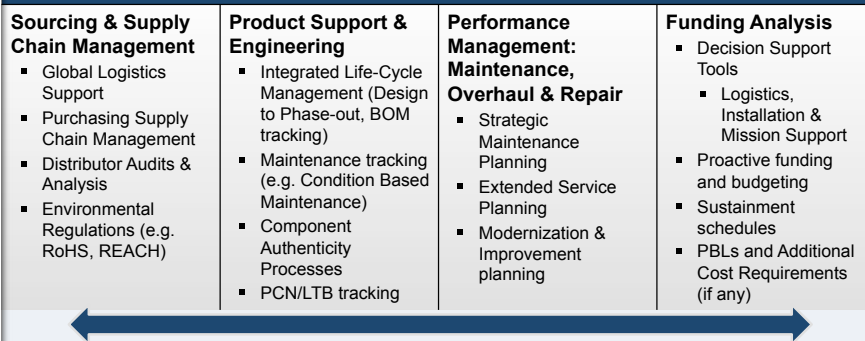


Figure 2 | A proactive obsolescence management architecture is key.

References:

1. 2009 DoD Weapon System Acquisition Reform Product Assessment. Washington D.C. Office of the Secretary of Defense.
2. Department of the Air Force, FY 2012 Budget Estimates, Operations and Maintenance, Vol. II.
3. J. Lieberman, "White Paper: National Security Aspects of the Global Migration of the U.S. Semiconductor Industry," Ranking Member Airland Subcommittee United States Senate Armed Services Committee (2003).
4. Maggie Hershey, SEMI North America Public Policy, "Semiconductor Equipment and Materials" (PowerPoint presentation, February 11, 2011).
5. George Scalise, Nanoelectronics and the Economy (Semiconductor Industry Association, PowerPoint presentation, December 3, 2010).

Kaye Porter is Marketing Manager at GDCA. Her current focus is bringing collaboration and awareness to the embedded industry on the latest in anti-counterfeiting and long-term product support. She can be reached at kporter@gdca.com.



GDCA | 925-456-9900 | www.gdca.com



ATCA, μ TCA, VME AND VPX SYSTEMS...FASTER.

Propel your project success with Schroff® Systems and Subracks EXPRESS. We provide VITA and PICMG compliant product solutions faster and at a competitive price. Protect your application with standard or customized electro-mechanical and system products – shipped in as few as two weeks and backed by our global network and more than 60 years of engineering experience. See our complete offering online.



Schroff®

RAPID DELIVERY

VITA and PICMG compliant solutions.

WWW.SCHROFF.US

Managing the military component obsolescence paradox: When new performance levels are needed after EOL

By RJ McLaren

Long-term delivery assurance, replace or upgrade programs, or shifting architectures are each an effective means of adding longevity to established legacy systems, and primarily depend on evolving performance demands. Competitive design options allow proactivity in managing obsolescence of critical applications – while focusing on improving performance.



U.S. Navy photo by Mass Communication Specialist Seaman Declan Barnes

Obsolescence management can be a tough challenge for military systems designers, but is always an essential consideration in plotting a successful product life-cycle policy. When critical components are no longer available and new performance features are continually required, other assurances are necessary in order to preserve program integrity. Adequate preparation for effective product life-cycle management, for example, ensures predictable product consistency and longevity. At a minimum, it gives mil/aero customers the ability to plan for the normal lifetime of a product.

Yet despite a manufacturer's best efforts, there might be a need to modify a product. This might be the result of a component prematurely becoming obsolete, an enhancement

that is desired by the market, or a correction to a problem. Because there might be the need to modify a product or end its lifetime prematurely, product life-cycle management can help designers respond efficiently and effectively to unexpected changes in a product's life.

Early notification, planning, and options are all imperative to determining the best design path to mitigate obsolescence. Updating components might migrate the system out of obsolescence; however, it might be more imperative to address requirements for integrating new technologies at the same time. Issues such as Size, Weight, and Power (SWaP), system performance improvements, connectivity, scalability, reliability, and enhanced ruggedness might need to drive the process.

Essentials of early notification

Product Marketing Information (PMI) ideally provides one-year notification (and a minimum six-month notice) that a component is being designated as EOL. Designers may elect for a last-time buy to support the product through its program life cycle, in which case the manufacturer can take steps to secure product as required. Included in the PMI are options, including recommendations for additional boards or components that will address the performance requirement.

Designers may choose to stay with an upgrade path supported for initial long life and then further extended through the enhanced next-generation components recommended via the PMI. However, when these upgrade paths are no longer appropriate given new

performance demands on the application in question, designers may choose to work with the manufacturer for an alternative solution, which might be best handled by a platform change.

Options and planning make all the difference

Planning product lifetimes starts as early as the development phase, dependent upon choices that affect the basic overall product life cycle (Figure 1). Components are selected based on features, market acceptance, and the approval of the vendor with the intent of ensuring long-term supply. As products mature, they are manufactured only for existing customers or for new designs that do not last longer than the product life cycle. The mature phase is usually two to three years, but will continue as long as there is sufficient demand or until component obsolescence makes it impossible to build the product.

Typically, a product of equal performance and features is available as a replacement for the product at EOL status. These parallel replacement product versions are developed as a part of a normal product redesign cycle to take advantage of newer or more economical technology. When a particular product family member enters EOL, other higher-performance products are available (or planned) within the product family and can be used as an upgrade replacement. Alternatively, many product families have members that are quite similar in performance and features, but differ in form factor. If the mechanical integration issues can be easily overcome, alternative replacements might even be a desirable path to capture new technology or other benefits, such as a reduction in size.

In these scenarios, SWaP might need to be decreased in a particular integrated system in order to decrease SWaP levels within the overall system. This approach is common when OEMs are working to manage obsolescence of existing platforms while introducing other systems elsewhere in the platform. Shipboard and ground vehicle applications are common areas for these design issues, with designers working to pack more functionality into a finite space that can only be extended

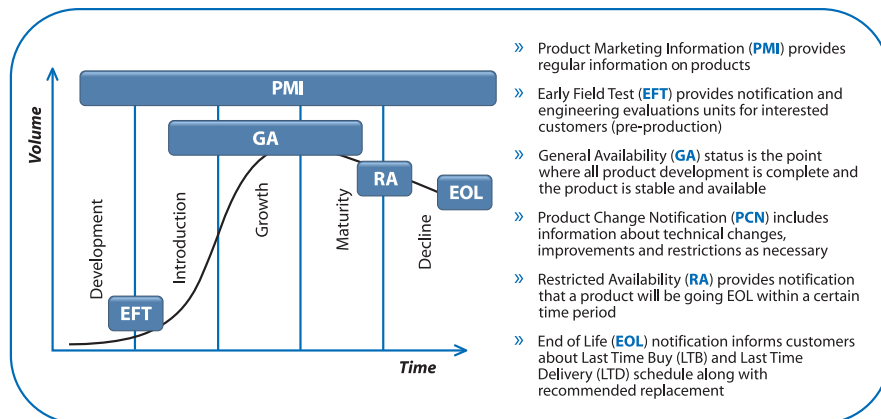


Figure 1 | Military and aerospace product life cycle

by reducing the footprint of existing systems. As combat environments evolve, SWaP reduction can improve troop safety simply by enabling a more streamlined deployment with long-deployed systems.

Managing obsolescence with architecture upgrades

A deeper level of upgrade might be considered, for example, if there is a need to increase performance based on new software capabilities established since the system's initial design or deployment. Additional features might now be required, such as higher CPU performance or increased memory. In this scenario, physical requirements might be flexible enough to allow a form factor change as warranted. For instance, an existing VME system that needs to incorporate higher-bandwidth technologies might need to evolve to VPX, but that requires changes to be made in the backplane and all system cards; this is significantly different from a simple CPU card upgrade and often requires greater design expertise.

The VPX architecture represents a dramatic shift from VME communication protocols, with signals moving across Serial RapidIO, Gigabit Ethernet, or PCI Express instead of the PCI or VMEbus. New High-Performance Embedded Computing (HPEC) platforms that are VPX-based supercomputer-like systems are gaining ground as a suitable option – providing massive processing power for compute-intensive DSP-based systems and allowing high-speed socket-based communication between blades by using multiple switched fabric interconnects within the backplane.

VPX replaces the bus with a network-based protocol, which typically demands application software retooling, and in turn drives military designers to consider 3U CompactPCI as a viable upgrade alternative for 6U VME-based systems. Its reduced form factor meets SWaP goals, and CompactPCI provides a well-established parallel bus standard, which provides a cost-effective modular computing platform that more closely resembles VME in terms of how application software recognizes the hardware.

Migrating to x86 can be a viable performance option

The cost of an architectural redesign might be too high, or specialized I/O boards might be difficult to replace. In these cases, designers can manage obsolescence by migrating to a new processor architecture that enables lower power and higher performance. For example, a VME design could transition from a PowerPC architecture to x86 by integrating current components that support the latest Intel processors. In this example, designing systems around 6U VME boards allows the final system to span different CPU architectures, which helps reduce risk and development time. This is essential as upgraded designs typically need to be put in place quickly with minimum risk to the overall system or application.

Further, designers can shift easily from 6U VME implementation to x86 in the 3U CompactPCI and 3U VPX platforms. Many designers are taking the opportunity to upgrade the backplane in the migration process, gaining bandwidth and performance features by moving to CompactPCI and VPX. In making this

transition, users can go from 2.5 Gbps data transfer for VME to 4.2 Gbps for CompactPCI or up to 10 Gbps for VPX. This represents a change in design thinking; although they cannot put as much hardware on each card (6U to 3U form factor change), designers have more space at the overall system level resulting from moving to a smaller form factor. Processors with faster clock rates and increased power-to-performance ratios mean they can pack the same performance in a much smaller volume.

Overall though, Intel x86 architecture is form factor-agnostic and applies readily to any number of the military's favorite platforms. The end result for military designers is that they can boost performance in a standards-based, multicore platform that is able to meet highly demanding signal- and data-processing requirements, an ideal fit for applications onboard submarines, naval ships, aircraft systems, and ground vehicles. For example, today's products based on third generation Intel Core processors enhance available small form factor solutions and provide up to 20 percent greater computing power and up to 40 percent increased performance per watt compared to designs based on previous generations.

Today's new x86-based embedded computing platforms combined with FPGAs enable another new realm of applications – providing highly adaptable feature options for designs that have previously been restricted due to lack of interface or I/O support (Figure 2). By understanding the collective advantages of this approach, designers can reduce Bill of Materials (BOM) costs and maintain long-term availability with legacy interfaces and dedicated hardware-based I/O. Most importantly for legacy systems facing upgrade or redesign, there is now a bridge to tap into the latest processor enhancements such as graphics media acceleration, hyperthreading, and virtualization for greater success in matching exacting requirements. The FPGA solution allows the designer the ability to replace legacy or obsolete I/O and still maintain

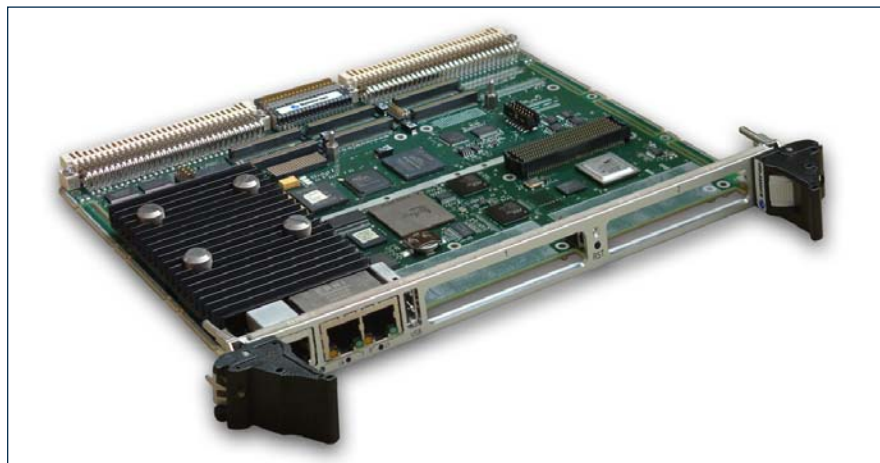


Figure 2 | With boards such as Kontron's VM6250, designers can readily migrate legacy or obsolete VME I/O to future-proof FPGA I/O, managing obsolescence by adding long-term flexibility to a design's features and performance options.

system integrity. This might require some initial software development if an existing IP core solution is not available. This is a significant advancement in bridging newer technologies with older systems implemented in the military market.

Budget, performance most vital in determining design path

Defense budgets are tight and the pressure is on. System deployments are being extended years longer than originally anticipated even while performance expectations are higher than ever. Designers of today's systems are challenged with getting creative – understanding evolving standardized platforms and finding the best embedded computing options to keep military applications and systems performing up to and beyond battlefield expectations.

Performance and reliability are essential: Older systems must be migrated and consistently enhanced to meet increasing levels of sophisticated data sharing, ruggedness, and performance. Designers approach obsolescence from several perspectives, each of which impacts their platform choice. Each approach might not be exclusively appropriate for a certain application or deployed environment, and designers will find it necessary to make trade-offs between performance, development time, cost, and legacy compatibility.

Based on costs and DoD budget requirements, many large, legacy military programs consider remaining in VME the most viable option – replacing legacy VME chassis, I/O cards, and software with products that now offer improved availability, performance, and features based on x86 architectures. In turn, many embedded computing suppliers are competing with this mandate, developing high-performance VPX and CompactPCI systems in parallel that deliver a range of compatible options designed for pure performance and reliability. Most importantly, system designers have a growing slate of competitive design options that allow them to be proactive in managing obsolescence of critical applications – while improving performance. **MES**



RJ McLaren
is Manager of Product Management for Military and Commercial Aerospace Products at Kontron America. He is responsible for product and business development for rugged systems along with Kontron's industry standard MicroTCA, CompactPCI, VME, and VPX product lines in North America. Contact him at rj.mclaren@us.kontron.com.

Kontron America
858-677-0877
www.kontron.com

You can't see them – but there are 300,000 people standing behind this display

What you can see is GE's Intelligent Vehicle Display, available with a 10" or 15" screen. By combining it with a powerful on board processor, memory and extensive I/O and networking capabilities, it can make a significant contribution to reducing in-vehicle size, weight and power.

What you can't see are the people behind it. Every GE product comes with a guarantee of exemplary customer support – the kind of support it takes to enable you to turn products into solutions more quickly and at lower cost, speeding your time to market and helping you achieve competitive advantage.

At GE Intelligent Platforms, we can offer you the best of both worlds: the agility and responsiveness of a small company, backed by the resources and strength in depth of one of the world's most dependable companies.

Add the GE team to your team, and experience the GE difference.

defense.ge-ip.com



imagination at work

Got Tough Software Radio Design Challenges?



Unleash The New Virtex-7 Onyx Boards!

Pentek's Virtex-7 Onyx™ boards deliver unprecedented levels of performance in wideband communications, SIGINT, radar and beamforming. These high-speed, multichannel modules include:

- A/D sampling rates from 10 MHz to 3.6 GHz
- D/A sampling rates up to 1.25 GHz
- Multi-bandwidth DUCs & DDCs
- Gen3 PCIe with peak speeds to 8 GB/sec
- 4 GB SDRAM for capture & delay
- Intelligent chaining DMA engines
- Multichannel, multiboard synchronization
- ReadyFlow® Board Support Libraries
- GateFlow® FPGA Design Kit & Installed IP
- OpenVPX, XMC, PCIe, cPCI, rugged, conduction cooled
- Complete documentation & lifetime support

With more than twice the resources of previous Virtex generations plus advanced power reduction techniques, the Virtex-7 family delivers the industry's most advanced FPGA technology.

Call 201-818-5900 or go to www.pentek.com/go/mesonyx for your FREE online *Putting FPGAs to Work in Software Radio Handbook*, technical datasheets and price quotations.



PENTEK
Setting the Standard for Digital Signal Processing

