@military_cots

Military EMBEDDED SYSTEMS

MIL-EMBEDDED.COM

Nov/Dec 2017 | Volume 13 | Number 8

John McHale
Open standards, COTS, and AUSA 7

Special Report
Miniaturizing EW for guided weapons 14

Mil Tech Trends
Mission-critical power systems 28

University Update
Internet of Battlefield Things 44

PROGRAMMABILITY, CONNECTIVITY REQUIREMENTS DRIVE DIGITAL POWER SUPPLY DESIGN FOR MILITARY USE

P 18

P 40

Increasing data-transfer performance in VPX systems
By Thierry Wastiaux, Interface Concept

Ensuring navigation in GPS-denied environments

P 12

Volume 13
Number 8

Military EMBEDDED SYSTEMS

www.mil-embedded.com

November/December 2017

PERSPECTIVES
Executive Interview
12 Ensuring navigation in GPS-denied environments
Interview with Troy Brunk, vice president and general manager of Communication, Navigation & Electronic Warfare Solutions for Rockwell Collins Government Systems
By Sally Cole, Senior Editor

SPECIAL REPORT
Secure Navigation Technology for Precision Guided Munitions
14 Miniaturizing electronic warfare microelectronics to advance precision-guided weapon technologies
By Charlie Hudnall and Philip Fulmer, Mercury Systems

MIL TECH TRENDS
Military Power Supplies
18 Programmability, connectivity requirements drive digital power supply design for military use
By Mariana Iriarte, Technology Editor

24 Capacitive load switching sources in military systems: How to extend relay switching life and reliability
By Mike Baldwin, TE Connectivity

28 Mission-critical power start-up demands perfect performance every time
By David Berry, Vicor Corp.

32 Battlefield servers demand design for heat, spares, and application portability
By Chris A. Ciufo, General Micro Systems

INDUSTRY SPOTLIGHT
Open Standards for Embedded Military Systems
36 Truly rugged and proven reliable: VITA 47 and beyond
By Aaron Frank and Ivan Straznicky, Curtiss-Wright Defense Solutions

40 Increasing data-transfer performance in VPX systems
By Thierry Wastiaux, Interface Concept

COLUMNS
Editor's Perspective
7 Open standards, COTS, and AUSA
By John McHale

Field Intelligence
8 Making COTS great again
By Charlotte Adams

Mil Tech Insider
9 Getting up to speed on NSA-approved two-layer commercial encryption
By Paul Davis

University Update
44 Next-gen 'Internet of Battlefield Things' on the way
By Sally Cole

DEPARTMENTS
10 **Defense Tech Wire**
By Mariana Iriarte

43 **Editor's Choice Products**

46 **Connecting with Mil Embedded**
By Mil-Embedded.com Editorial Staff

EVENT
Embedded Tech Trends 2018
January 22-23, 2018 | Austin, TX
www.embeddedtechtrends.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

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

Published by:
OpenSystems media

ISSN: Print 1557-3222

ON THE COVER:
Top image: A preflight inspection is performed on an MQ-1 Predator unmanned aerial vehicle. (U.S. Navy photo/Mass Communication Specialist 2nd Class Brian T. Glunt)
Bottom image: Global militaries are leveraging multiple technologies and creating augmented solutions to ensure navigation in GPS-denied environments. Illustration courtesy Rockwell Collins.

ADVERTISER INFORMATION

Page	Advertiser/Ad Title
47	**Abaco Systems** – Now COTS means COTS
38	**ACCES I/O Products, Inc.** – PCI Express mini card; mPCIe embedded I/O solutions
21	**Acromag** – Acromag redefines SWaP-C with our new AcroPack I/O platform
35	**Advantech** – Enabling an intelligent planet
30	**AIM** – Modules - Software - Systems
5	**Aitech** – Aitech. Leading the space race
34	**Alphi Technology Corporation** – Mission critical I/O solutions
2	**Annapolis Micro Systems, Inc.** – Keep your FPGA system integration on target and above water
3	**Behlman Electronics** – When it comes to VPX, one company has the most flavors
22	**Crystal Group, Inc.** – Introducing the new FORCE to fight and win
27	**Data Device Corporation** – Your solution provider for … reliable power supplies
23	**Dolphin Interconnect Solutions** – Build next gen systems with PCIe networks
20	**Ecrin Systems** – µOnyx SFF mission computer
45	**embedded world Exhibition & Conference** – … it's a smarter world
42	**Evans Capacitor** – Advanced capacitors for demanding applications
17	**North Atlantic Industries** – Rugged power supplies from NAI
33	**Omnetics Connector Corp.** – Durable, reliable, and rugged connectors for your application
48	**Pentek, Inc.** – Capture. Record. Real-time. Every time.
39	**Phoenix International** – Airborne, shipboard, ground mobile data recording and data storage
31	**Pico Electronics** – .18" ht. Size does matter!
39	**Star Communications, Inc.** – Signal processing receivers; computing accelerators
16	**Themis Computer** – Reliable composable computing

E-CASTS

Reducing SWaP in RF & Microwave Designs for EW, SIGINT, and Radar Applications
Presented by Evans Capacitor and National Instruments
ecast.opensystemsmedia.com/756

Cyber Security: It Starts with the Embedded System
Presented by LDRA, Rogue Wave Software, Wind River, and WinSystems
ecast.opensystemsmedia.com/753

Military EMBEDDED SYSTEMS

GROUP EDITORIAL DIRECTOR John McHale jmchale@opensystemsmedia.com
ASSISTANT MANAGING EDITOR Lisa Daigle ldaigle@opensystemsmedia.com
SENIOR EDITOR Sally Cole scole@opensystemsmedia.com
TECHNOLOGY EDITOR Mariana Iriarte miriarte@opensystemsmedia.com
DIRECTOR OF E-CAST LEAD GENERATION AND AUDIENCE ENGAGEMENT Joy Gilmore jgilmore@opensystemsmedia.com
CREATIVE DIRECTOR Steph Sweet ssweet@opensystemsmedia.com
SENIOR WEB DEVELOPER Konrad Witte kwitte@opensystemsmedia.com
WEB DEVELOPER Paul Nelson pnelson@opensystemsmedia.com
CONTRIBUTING DESIGNER Joann Toth jtoth@opensystemsmedia.com
EMAIL MARKETING SPECIALIST Drew Kaufman dkaufman@opensystemsmedia.com

VITA EDITORIAL DIRECTOR Jerry Gipper jgipper@opensystemsmedia.com

SALES

SALES MANAGER Tom Varcie tvarcie@opensystemsmedia.com (586) 415-6500
MARKETING MANAGER Eric Henry ehenry@opensystemsmedia.com (541) 760-5361
STRATEGIC ACCOUNT MANAGER Rebecca Barker rbarker@opensystemsmedia.com (281) 724-8021
STRATEGIC ACCOUNT MANAGER Bill Barron bbarron@opensystemsmedia.com (516) 376-9838
STRATEGIC ACCOUNT MANAGER Kathleen Wackowski kwackowski@opensystemsmedia.com (978) 888-7367
SOUTHERN CAL REGIONAL SALES MANAGER Len Pettek lpettek@opensystemsmedia.com (805) 231-9582
SOUTHWEST REGIONAL SALES MANAGER Barbara Quinlan bquinlan@opensystemsmedia.com (480) 236-8818
NORTHERN CAL STRATEGIC ACCOUNT MANAGER Sean Raman sraman@opensystemsmedia.com (510) 378-8288
ASIA-PACIFIC SALES ACCOUNT MANAGER Helen Lai helen@twoway-com.com
BUSINESS DEVELOPMENT EUROPE Rory Dear rdear@opensystemsmedia.com +44 (0)7921337498

OpenSystems media®
WWW.OPENSYSTEMSMEDIA.COM

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

CORPORATE OFFICE
1505 N. Hayden Rd. #105 • Scottsdale, AZ 85257 • Tel: (480) 967-5581

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

Open standards, COTS, and AUSA

By John McHale, Editorial Director

When it comes to U.S. military trade shows, nothing usually tops the Association of the U.S. Army's (AUSA's) annual meeting for determining the mood of the Department of Defense (DoD) – and of the course the U.S. Army – regarding electronics procurement. Last month's event did not disappoint: Attendees and exhibitors from the warfighter to the components supplier showed enthusiasm for new technologies and the DoD's increased demand for open architectures and open standards.

I quizzed a few exhibitors on what the vibe was at the event regarding new technology and the market for commercial off-the-shelf (COTS) procurement in the COTS Confidential section of October's McHale Report newsletter (Read here: http://bit.ly/2hkbVv8). The response was consistently positive.

"The 'buzz' is that after the past eight years, and for 99 percent of the exhibitors, the defense market is back," stated Doug Patterson, vice president, Military & Aerospace Sector, at Aitech Defense Systems. "There's clearly optimism that there's a need for advanced technology. Any negativity seemed to come from companies that didn't take the opportunity in the past decade to position themselves with new, innovative technology to hit the ground running."

The Army, especially, is embracing COTS and open architectures, said John Ormsby, Business Development, Curtiss-Wright Defense Solutions. "The Army's requirements align well with the 'sweet spots' where COTS excels, such as reducing government risk and NRE [nonrecurring engineering costs] and delivering capabilities to the warfighter faster."

The enthusiasm for COTS and new tech was evident across all applications, noted Greg Powers, Global Market Leader, Aerospace & Defense Performance Solutions Division, W.L. Gore & Associates, Inc., in the discussion. "It seems all segments, depending on where your interests and expertise lie, are humming with activity for COTS vendors and people are eager to engage. This is because COTS-based, multiplatform open architecture has asserted itself as the mantra of the agencies and industry participants.

"Many of the COTS-based applications establish pedigree via select industry standards groups, such as Society of Aerospace Engineers (SAE), for items such as rugged 10 Gb Ethernet cable, or VITA Standards Organization (VSO), for VPX-based rugged embedded computers," Powers continued. "These industry groups have really taken the reins on the standardization of cutting-edge technologies with intimate oversight from various branch R&D arms, including CERDEC [U.S. Army Materiel Command's Communications-Electronics Research, Development and Engineering Center], AFRL [Air Force Research Laboratory], and NAVAIR [Naval Air Systems Command]. Joint approaches by the agencies are also becoming commonplace, furthering commonality. We are fortunate that technology and innovation are well funded at present."

The increased participation of U.S. military organizations such as CERDEC and NAVAIR is overwhelming evidence of their investment in open standards. "They buy in from the beginning and it gets more people at the military and system integrator level interested in supporting a standard," says Jerry Gipper, executive director of VITA. Key initiatives VITA works on with the government include the Sensor Open Systems Architecture (SOSA), which enables reuse of key sensor components across multiple platforms and services; and Hardware Open Systems Technologies (HOST), which will essentially create a three-tier VPX standard that will have open architecture characteristics on the top two tiers, with the bottom tier being proprietary and containing the secret sauce for U.S. military end users.

Also in the air at the event: The fact that open standards are becoming the necessary coin for doing business with the DoD on electronics platforms.

"We have received requests for proposal from the end users where lack of open standards could prevent a company from proposing," David Vos, Lockheed Martin Fellow, told me in a discussion we had recently on the release of the VITA 48.8 standard. This new standard describes an open standard for the design requirements for an Air Flow Through (AFT) cooled plug-in module having 3U and 6U form factors while retaining the VPX connector layout. It's the first standard to address AFT in 3U form factors, meeting a crucial need to reduce size, weight, and power. The standard's working group within VITA was sponsored by Lockheed Martin, Abaco Systems, and Curtiss-Wright, which chaired the working group.

"Prior to the development of the ANSI/VITA 48.8 standard, we were always challenged balancing the high-performance processing requirements our customers needed to effectively execute their mission," Vos said in a Curtiss-Wright release on VITA 48.8.

As I've said many times in this space, the DoD is not going back to the past, where they funded everything from the ground up. That practice is economically unsound, even with military budgets increasing. Open standards enable commonality and reuse across multiple platforms, translating to lower life cycle costs. Those who embrace this concept are primed to do well in the coming years.

For more on open standards, please see our Industry Spotlight section, starting on page 36.

Making COTS great again

By Charlotte Adams

An Abaco Systems perspective on embedded military electronics trends

Is it possible to produce commercial off-the-shelf (COTS) embedded computers that come closer to the original concept's promise of faster and more affordable procurements? A COTS version 2.0?

First step: Admit that military COTS is not all it's cracked up to be – it's better than mil-spec but by no means perfect. Second step: Retool the development process to focus on flexible, modular, adaptable, and reusable platforms rather than one-off products.

COTS works well on the consumer side because manufacturers choose the options they will offer in this extremely competitive market and consumers vote with their pocketbooks. But in the mil-aero world this model doesn't work well. Every military customer wants something different from the others and suppliers must comply. So COTS products quickly become custom products, driving up development costs and time to market. Rigorous environmental testing eats up additional time. By the time the equipment reaches the field, it may well already be obsolete.

Here's an example of what's wrong with COTS today. Say a computer has been designed for one customer with a fixed configuration of boards and chips, I/O interfaces and connectors, backplane, enclosure, software, and all the rest. But the next customer wants an I/O interface that is not native to the design. Changing this small but crucial feature means a new development project, involving an extra I/O interface and connector, additional bus logic, and potentially board and backplane redesign. This single change could add months to the delivery schedule and tens of thousands of dollars to development cost.

What if?

What if there was a way to meet customers' unique requirements with off-the-shelf products that could be assembled from standard, prequalified modules on a short schedule at a reasonable price? What if these products could then be supported through changes and upgrades at lower life cycle cost? It would be too good to be true if we were just talking about chips and boards. But if we include factors such as granular I/O implementation and a stable connector configuration and enclosure form factor, the picture brightens. At this higher level of integration, customer-specific COTS solutions become possible.

One of the most critical challenges and relentless cost drivers of embedded computer design results from the military's installed stable of elderly platforms. Upgrades that feature 10 Gigabit Ethernet and USB 3.0 have to talk to legacy equipment that uses RS232 and MIL-STD-1553. The use of these older systems means that the connector configuration, together with associated backplane, bus logic, and board design parameters, must be flexible enough to accommodate the old interfaces along with the new.

Figure 1 | The MCS1000 and GVC2000 two-slot 3U VPX systems are configurable and feature modular I/O.

Suppliers understand this and are developing modular and granular data bus interface implementations for both operational and data bus test uses.

An example is Abaco Systems' Lightning configurable computing family, intended for military air and ground vehicles. Its first two members, the MCS1000 and GVC2000, are two-slot, 3U VPX systems aimed at various mission/display processing profiles (Figure 1). Every product in this Lightning lineup will feature modular I/O – 25 data bus "tiles" to choose from, with up to four to a carrier card – standard connector configuration, stable enclosure envelope, and prequalification to military environmental specs, with Gigabit Ethernet, USB 2.0 and 3.0, and serial ports prepackaged in the tile carrier card.

If suppliers can design an array of small-form-factor I/O interfaces, and if the bus software logic is partitioned from the physical protocol implementation, the modules can be mixed and matched without costly hardware and software ripple effects. That in turn opens the door to precise, flexible, and affordable implementation of unique customer requirements.

Building blocks

If the right elements are in place – I/O interfaces are prefabricated in profusion, a wide range of compute cards is available, the enclosure envelope is stable, and the elements are prequalified – unique combinations become a matter of assembly rather than design. Such prefabricated platforms could themselves become modules in larger systems or across different air or ground vehicles, multiplying initial procurement and life cycle savings.

Further, the stability of the chassis envelope, power supply, and connector set – together with the potential reusability of the backplane and I/O panel – inherent in this approach promises to reduce the design work, development cost, and time to market of future iterations going forward.

www.abaco.com

Getting up to speed on NSA-approved two-layer commercial encryption

By Paul Davis

An industry perspective from Curtiss-Wright Defense Solutions

The National Security Agency/Central Security Service (NSA/CSS) created the Commercial Solutions for Classified (CSfC) Program to enable the use of commercial data protection in layered solutions to protect classified National Security Systems (NSS) data. Thanks to CSfC, system designers can now deploy a commercial off-the-shelf (COTS) solution with encrypted data protection in a matter of months and at a fraction of the cost, compared to the multiple years and millions of dollars typically required to achieve certification for more sensitive Type 1 products. Type 1 products, certified by the NSA to cryptographically secure classified U.S. Government information, use approved NSA algorithms. These products are typically designed and certified by the NSA through a rigorous and often very lengthy process.

As an alternative, CSfC defines an approach for protecting critical data using two-layer commercial encryption technologies. In many cases, system integrators considering a Type 1 approach may be pleasantly surprised to find that their application can instead use the significantly faster and less costly two-layered COTS approach.

System designers: Getting started with CSfC

Any COTS product vendor can develop products for use in a CSfC solution. To achieve NSA approval and placement on the CSfC Components List the COTS- based encryption components must undergo Common Criteria (CC) evaluation by the National Information Assurance Partnership (NIAP). Once that CC process is formally underway, the COTS vendor must establish a Memorandum of Agreement (MOA) with the NSA.

What is NIAP?

NIAP was created by the NSA and National Institute of Science and Technology (NIST) to evaluate commercial solutions proposed for inclusion in CSfC solutions. NIAP ensures that commercial products meet NSA standards for security by testing the products against stringent security profiles in certified labs. It oversees U.S. implementation of the Common Criteria validation of commercial IT products for use in national-security systems.

What is Common Criteria?

Common Criteria (ISO-15408) is a technically demanding, international set of guidelines for security certification that is required by the U.S. and 27 national governments worldwide. Common Criteria certification provides assurance that the process of specification, implementation, and evaluation of technology products has been conducted in a rigorous, standard, and repeatable manner. In partnership with NIST, NIAP approves Common Criteria Testing Laboratories to conduct security evaluations in private-sector operations across the U.S. Upon successful completion of the Common Criteria evaluation by the lab, the test results are then validated by NIAP and a Common Criteria certification is posted. NSA CSfC review and approval are the next steps. Then the approved product can be added to the NSA's CSfC Components List and proposed in a layered CSfC solution by an integrator. Selecting a preapproved device from the CSfC Components List enables system architects to rapidly design a COTS encryption solution and begin their system development, saving significant development cost and time while also greatly reducing their program risk.

What is the CSfC component list?

This list enables system integrators to identify products that are in evaluation or are already certified products that can be used in a data-protection solution. System integrators must apply to the NSA identifying the proposed product from the Component List and the application details. This approach enables system integrators to begin evaluating their data-security architecture and greatly reduces program risk and schedule. The NSA publishes Capability Packages (CP) which provide the solution guidance for different applications (such as Data-at-Rest).

Figure 1 | The DTS1 network attached storage device supports two encryption layers in one product.

A COTS solution for CSfC Data-at-Rest protection

As an example, Curtiss-Wright Defense Solutions recently commenced the Common Criteria certification process for its Data Transport System (DTS1) network attached storage (NAS) storage device. The small form-factor data recorder uses two layers of commercially available CNSA (formerly Suite B) cryptographic algorithms. It also uses the NSA's Data-At-Rest Capability Package as a design template and is based on the hardware and software full disk encryption (HS) solution approach. (Figure 1.)

Thanks to CSfC, COTS products using software and hardware encryption layers will be able to ease and speed the ability of system designers to protect Top Secret data with an NSA-approved cost-effective alternative to Type 1 encryption. This progress will result in more critical data being protected, sooner.

***Paul Davis** is Director of Product Management, Data Solutions, for Curtiss-Wright Defense Solutions.*

Curtiss-Wright Defense Solutions
www.curtisswrightds.com

DEFENSE TECH WIRE

NEWS | TRENDS | DOD SPENDS | CONTRACTS | TECHNOLOGY UPDATES

By Mariana Iriarte, Associate Editor

NEWS

Flight data recorder will go up with NASA's Dream Chaser to ISS

Data-storage firm Ampex Data Systems – a wholly owned subsidiary of communications provider Delta Information Systems – garnered a contract from space-component maker Sierra Nevada Corp. to provide a rugged flight multifunction data recorder (MDR) for the Sierra Nevada spacecraft cargo system.

The MDR that will fly on the Dream Chaser, the Model TS540, is a radiation-tolerant enhanced solid-state recorder that will be used for onboard recording during the craft's journey to and from the International Space Station (ISS). Under the NASA deal, Sierra Nevada will run six uncrewed cargo delivery flights to the ISS between 2020 and 2024.

Ampex documents describe the TS540 as a standardized, rugged, pluggable processing module that integrates the CPU with memory and I/O interfaces such as mini-PCI Express, XMC, USB, Ethernet, and serial ports.

Figure 1 | The multifunction data recorder (MDR) will fly on the Dream Chaser. Photo courtesy NASA.

DARPA awards contract for hypersonic Advanced Full Range Engine

Aerojet Rocketdyne signed an agreement with the Defense Advanced Research Projects Agency (DARPA) to develop and ground-test a propulsion system under DARPA's Advanced Full Range Engine (AFRE) program.

The primary goal of the AFRE program is development and initial demonstration of a reusable hydrocarbon propulsion system able to operate in a reliable and affordable manner over the full range of speeds between takeoff and hypersonic cruise. Such engines are being designed to enable responsive hypersonic aircraft for a variety of military missions.

"Through the AFRE program, we aim to mature the design and component technologies and bring them together to conduct a full system-level Turbine Based Combined Cycle ground-test demonstration," states Eileen Drake, Aerojet Rocketdyne CEO and president.

Air Force PRECOG effort to leverage probabilistic reasoning tools for satellites

The U.S. Air Force selected Charles River Analytics to build probabilistic reasoning tools for the Probabilistic Reasoning for Enhanced Course of Action Generation system (PRECOG) program. The 27-month contract is valued close to $750,000.

Charles River will use Figaro, its open-source probabilistic programming language for probabilistic modeling, in creating these tools. The company is also partnering on the PRECOG effort with Paul Szymanski of the Space Strategies Center and Professors Rina Dechter and Alexander Ihler of the University of California at Irvine.

The goal of PRECOG, say Air Force officials, is to advance decision-making algorithms, enabling efficient courses of action selection on board satellites.

NATO exercise tests air, missile defense under Aegis Combat System

The U.S. Navy and Missile Defense Agency – in concert with Lockheed Martin and naval forces from eight NATO nations – concluded a series of ballistic missile defense tests in the Atlantic Ocean during an exercise it called Formidable Shield 2017 (FS-17).

In one of the events, a U.S. Navy ship operating with the 4.0.3 Aegis Combat System conducted a simulated engagement of a live short-range ballistic missile (SRBM) target using remote track data provided by a Spanish F-100 class ship.

In the same event, another U.S. Navy ship, operating with the Baseline 9.C1 integrated air and missile defense capability, launched SM-2 missiles against cruise missile targets while simultaneously tracking the SRBM.

Figure 2 | Arleigh Burke-class guided-missile destroyer USS Donald Cook (DDG 75) as it was underway participating in exercise Formidable Shield 2017. Photo courtesy of the U.S. Navy/Mass Communication Specialist Seaman Apprentice Raymond Maddocks.

Navy's COBRA mine detection system achieves IOC

U.S. Navy officials announced that its AN/DVS-1 Coastal Battlefield Reconnaissance and Analysis (COBRA) airborne mine detection system recently achieved Initial Operational Capability (IOC).

The system – which can be integrated with the U.S. Navy's MQ-8 Fire Scout unmanned aircraft system (UAS) – detects and localizes minefields and obstacles when flown over a beach zone area. The Block I version of COBRA completed the first phase of initial operational test and evaluation (IOT&E) on board the MQ-8B Fire Scout UAS.

Part of the littoral combat ship's (LCS) suite of mine countermeasures (MCM) systems, COBRA is in low-rate initial production. It completed a series of developmental tests at Eglin Air Force Base, Florida and Webster Field, Maryland, over the past year. COBRA's next test will be an underway period on board an LCS equipped with a full MCM mission package. During the at-sea trial, COBRA will fly various missions over beaches while demonstrating system suitability for operating from the LCS.

Figure 3 | The Block I version of COBRA completed the first phase of initial operational test and evaluation on board the MQ-8B Fire Scout unmanned aircraft system. Photo courtesy of the U.S. Navy.

M1 Abrams tank fleets will get additional display systems

Military specialized display maker Palomar Display Products has been awarded a firm fixed-price contract totaling $5.3 million to deliver optically coupled military display systems for M1 Abrams tank fleets in the U.S. and allied nations.

The display systems have been designed, tested, and qualified for the M1 Abrams tank and will be installed on tanks delivered to the U.S. and some of its international customers. All deliveries under this contract will take place through 2018.

In addition, Palomar's indefinite quantity/indefinite delivery sole-source contract with the U.S. Army has been increased by $9.3 million, according to a company release, for a new maximum award ceiling of $37.9 million.

Army invites companies to sign on to VICTORY C4ISR/EW interoperability drive

The U.S. Army issued a special notice inviting nonmembers to join the Vehicular Integration for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance/Electronic Warfare interoperability (VICTORY) standards program.

Officials of the Army Contracting Command are inviting companies that are not already involved to attend the next meeting of the VICTORY standards body, to be held December 13 and 14 at the Detroit Arsenal in Warren, Michigan. The VICTORY group intends to hold working group discussions, engage industry partners and government agencies, and ultimately update participants on how to build C4ISR/EW [command, control, communications, computers, intelligence, surveillance, and reconnaissance/electronic warfare] and related mission equipment on military ground platforms.

Registration is required for the event; the registration period is open until November 27, 2017. Details for this F2F TIM [Face-to-Face Technical Interchange Meetings (TIMs)] are posted on the VICTORY public site.

USAF signs $131 million contract for additional laser guided bomb kits

Lockheed Martin signed a $131 million contract with the U.S. Air Force for follow-on production of Paveway II Plus Laser Guided Bomb (LGB) kits.

The Paveway II Plus kit includes an enhanced guidance package that Lockheed Martin officials says improves accuracy over legacy LGBs. Paveway II Plus – cleared for use on U.S. Air Force, U.S. Navy, and international aircraft authorized to carry and release LGBs – is qualified for full and unrestricted operational employment in GBU-10, -12, and -16 (1,000-pound) configurations.

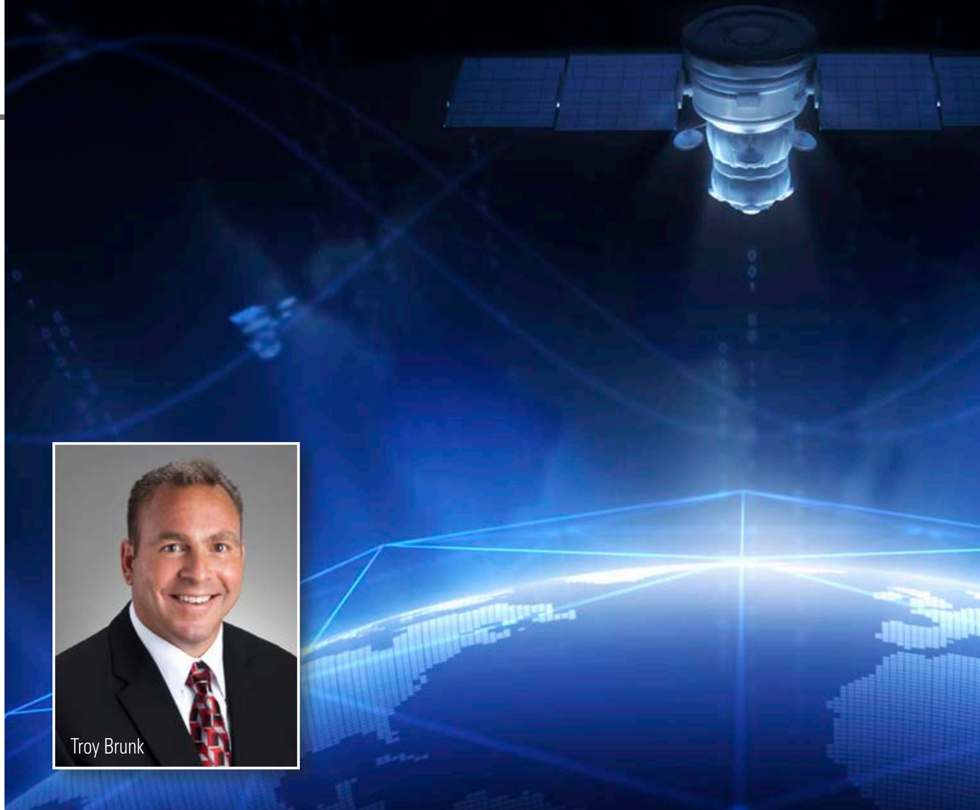
The company says that production of the guidance kits and air foil groups for GBU-10 (2,000-pound) and GBU-12 (500-pound) LGBs will begin in the first quarter of 2018.

Figure 4 | An F-15E Strike Eagle flies with a Lockheed Martin Paveway II Plus GBU-12 (500-lb) LGB (left) in flight exercises. Photo courtesy of the U.S. Air Force.

EXECUTIVE INTERVIEW

Ensuring navigation in GPS-denied environments

By Sally Cole, Senior Editor



Troy Brunk

Illustration: Rockwell Collins

Global militaries are leveraging multiple technologies and creating augmented solutions to ensure navigation in GPS-denied environments. In this Q&A with Troy Brunk, vice president and general manager of Communication, Navigation & Electronic Warfare Solutions for Rockwell Collins Government Systems, he discusses this trend, the history of GPS technology, improvements in Galileo Global Navigation Satellite System (GNSS) solutions, leveraging M-code, and more. Edited excerpts follow.

MIL-EMBEDDED: ***Can you please provide a brief history of GPS and GNSS technology? Rockwell Collins made the first GPS receiver, correct?***

BRUNK: Rockwell Collins built its own GPS receiver and became the first company to receive the signal that was sent from the world's first GPS satellite in 1977. Soon after, [the company] won the Navstar GPS user equipment contract. Since then, Rockwell Collins has continued to pioneer advancement in military GPS. In 1994, a secure, military-grade Precision Lightweight GPS Receiver (PLGR) was first fielded that provided warfighters a tactical navigational advantage on the battlefield. In 2012, [the company] began work on the Military GPS User Equipment (MGUE) program to develop an M-Code [Military-Code] receiver, which operates using a more powerful signal that's resistant to cyber threats. And in 2014, Rockwell Collins developed a prototype to track a satellite in the GNSS that was being created by the European Union to provide global coverage for its nations.

MIL-EMBEDDED: ***What's being done to ensure navigation in GPS-denied environments?***

BRUNK: The U.S. and other militaries are pursuing augmented solutions, including improved antijam and antispoof for GPS as well as the integration of non-GPS sensors and infrastructure to enable the delivery of Positioning, Navigation, and Timing (PNT) information in unfriendly environments. [To solve the GPS-denied problem we] also leverage the latest technologies in areas such as networked navigation, optical/radar tracking, pseudolites ["pseudo-satellites," most often small transceivers that are used to create a local, ground-based Global Positioning System (GPS) alternative], and map matching.

This year we delivered our latest-generation Digital GPS Anti-Jam Receiver, DIGAR, to the U.S. Air Force Special Operations Command. This provides airborne antijamming capabilities with [more than] 10,000 times the resistance over the previous model. (Figure 1.)

MIL-EMBEDDED: ***How are reduced size, weight, and power (SWaP) requirements impacting GPS designs? Any tradeoffs with smaller tech?***

BRUNK: The primary tradeoff is very low-SWaP applications will have reduced options to augment GPS for operation in unfriendly environments.

MIL-EMBEDDED: ***How is GNSS being improved? What are the biggest tech requests for Rockwell Collins when it comes to receivers for GNSS?***

BRUNK: Improved assurance (access and integrity) is being requested more from our markets. We have several technologies available to provide significant assurance

improvements. These include GNSS software enhancements, antijam antenna technologies, alternative (non-GNSS) navigation sensors, and alternative infrastructure technologies like pseudolites.

MIL-EMBEDDED: ***What are the key capabilities of your NavHub system and how does it leverage M-Code?***

BRUNK: NavHub is an augmented GNSS that allows multiconstellation GNSS as well as inertial sensors to provide improved assurance. Key capabilities of NavHub would include positioning for M-Code, GPS-denied navigation and timing on ground vehicles, and I/O compatibility with legacy GPS solutions.

MIL-EMBEDDED: ***GNSS is vulnerable to low-power signals. In mission-critical battlefield situations where navigation must work, what alternatives are being used? And are they being combined with GPS as backup?***

BRUNK: Several augmentations to GPS are being investigated and implemented to enable continuous delivery of high-assurance PNT. Rockwell Collins works to deliver solutions so warfighters can navigate with confidence in demanding combat environments and that of course involves making sure alternatives exist as a backup.

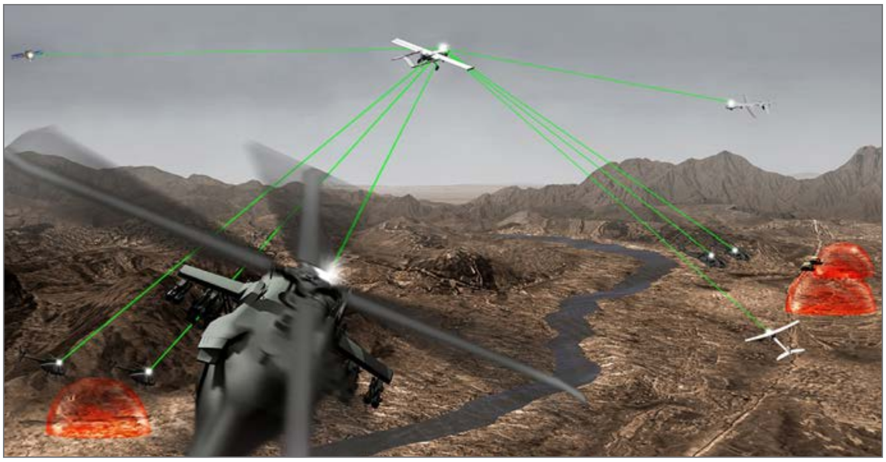


Figure 1 | The U.S. Air Force Special Operations Command uses the Rockwell Collins DIGAR for airborne antijamming capabilities. Graphic courtesy Rockwell Collins.

MIL-EMBEDDED: ***How big of a problem is jamming/spoofing, and what can you do about it?***

BRUNK: Recent innovations have significantly advanced technology to improve the antijam and antispoof performance of our GPS receivers. These include proprietary GNSS software enhancements, advanced antijam antenna technologies, and integration of non-GNSS sensors.

MIL-EMBEDDED: ***In terms of secure GPS technology, how do you leverage encryption in your systems?***

BRUNK: Military GPS signals are inherently encrypted and we implement the proper processing capability to take full advantage of that encryption. The new military M-Code is an encrypted code being rolled out by the U.S. military as the next generation of GPS, and Rockwell Collins has extensive work underway to transition our products to it for improved security and performance.

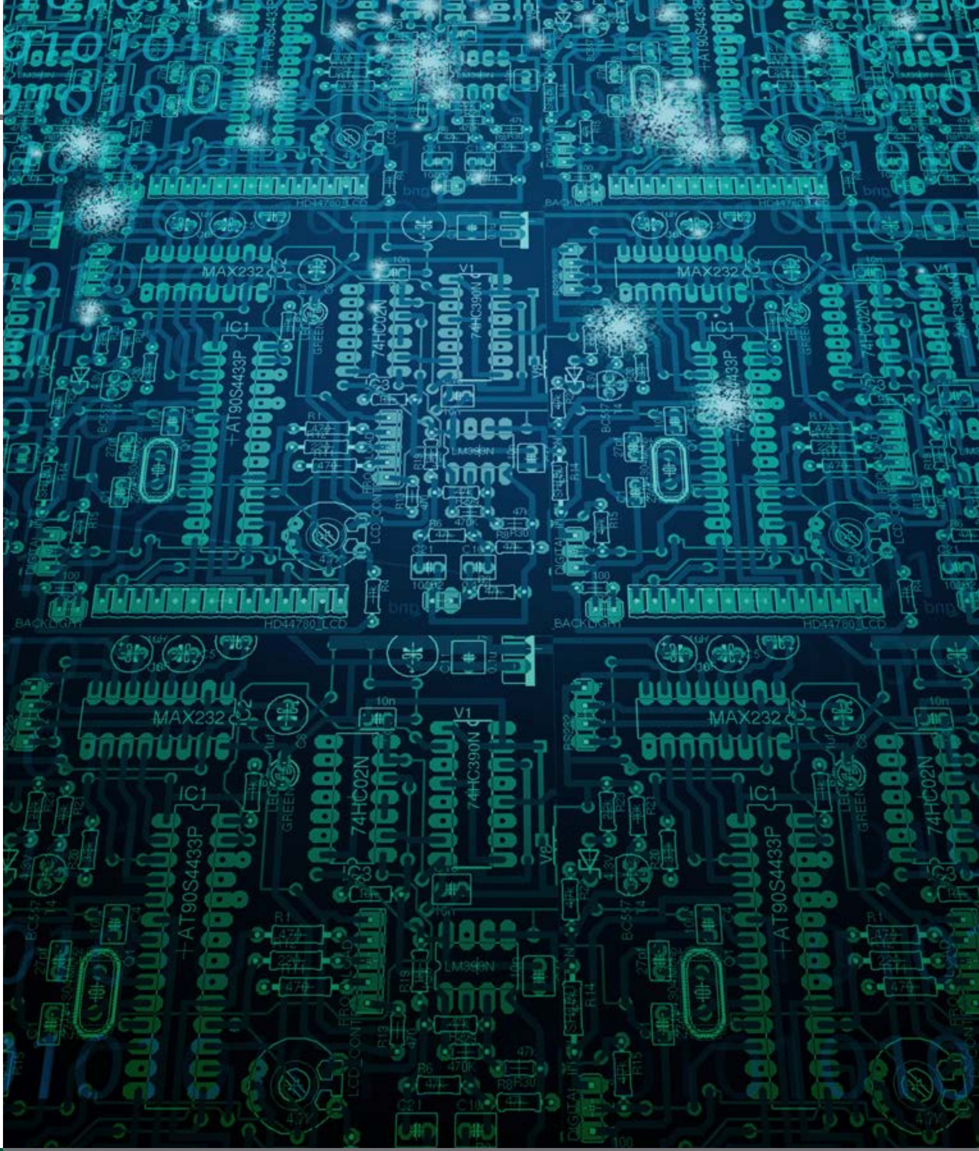
MIL-EMBEDDED: ***In the future, what disruptive technology/innovation do you expect to be a game-changer in the GPS/GNSS/navigation world?***

BRUNK: We believe size and cost reductions in technologies that enable high-assurance PNT at higher and higher levels of performance will enable more platforms to have more reliable PNT across more of their missions. Non-GNSS sensor technologies continue to advance in SWaP improvements, sensor fusion techniques continue to improve, and alternative sensors that can navigate with alternative infrastructure or without infrastructure continue to develop and provide viable navigation capability. **MES**

Troy Brunk is vice president and general manager of Communication, Navigation & Electronic Warfare Solutions for Rockwell Collins Government Systems. In this role, he is responsible for a major segment of the company's defense business including navigation products, communications systems, software defined radios, data links, electronic warfare, and range/training solutions. He was named to the position in September 2016. Since joining the company in 1992, Troy has held various management positions of increasing responsibility, most recently as vice president and general manager of Airborne Solutions for Rockwell Collins Government Systems. He has also held positions including programs manager for the Multifunction Information Distribution System (MIDS), programs manager for the Joint Tactical Radio System (JTRS) Ground Mobile Radio program, senior director of Processing and Head Down Display Products, and senior director of Airborne Communication Products. Troy earned his Bachelor of Science degree in industrial engineering and an MBA from The University of Iowa. He serves on the Industrial Advisory Board for The University of Iowa's Department of Mechanical and Industrial Engineering and supports local youth activities.

Special Report

SECURE NAVIGATION TECHNOLOGY FOR PRECISION GUIDED MUNITIONS



Miniaturizing electronic warfare microelectronics to advance precision-guided weapon technologies

By Charlie Hudnall and Philip Fulmer

Electronic warfare (EW) technologies are normally deployed in ground, naval, and airborne platforms to maintain a strategic and tactical advantage in the modern battlefield. As the threat environment evolves, there is an increasing need to integrate sophisticated EW capability into precision-guided weapons (PGW). These platforms present the most demanding size, weight, and power (SWaP) challenges for the defense microelectronics industry today. Recent technology developments have yielded high-performance, miniaturized and ruggedized RF components and modules for these SWaP-constrained EW systems.

Electronic warfare technologies, normally deployed in ground, naval, and airborne platforms, provide a strategic and tactical advantage in the modern battlefield. At the same time, modern military forces continue to transition from conventional weapons to precision-guided munitions and missiles with enhanced strike capabilities. In response, adversaries are turning to electronic attack technologies to disrupt the navigation and guidance systems of precision guided weapons (PGW), thereby reducing their efficacy to that of conventional weapons used in the first half of the 20th century. To counter this emerging electronic-attack threat, electronic protection microelectronics from ground, naval, and air platforms must be adapted and greatly miniaturized in a form factor sufficiently compact and ruggedized for PGW. Achieving this goal requires a fundamental shift in perspective on digital RF memory (DRFM) design methodology to embed EW technology in the extremely space-constrained environment allocated for microelectronics in modern PGW.

These highly miniaturized modules, small enough to fit in the palm of a hand, are ideal for applications where conventional DRFM capabilities are too large for consideration in missiles and precision-guided munitions.

Rethinking RF in DRFMs

The analog componentry of a typical DRFM design occupies the majority of the allocated design space; a miniature DRFM can only be realized with significant attention to shrinking the analog circuitry while simultaneously delivering the enhanced ruggedization needed to withstand the harshest expected operating conditions. Operating conditions can vary widely based on the munition and its specific profile. The DRFM

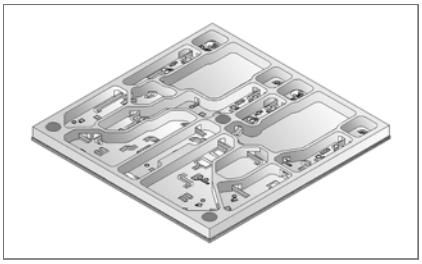


Figure 1 | RF MCM allowing simultaneous miniaturization and ruggedization of analog circuitry for DRFM applications. Illustration courtesy Mercury Systems.

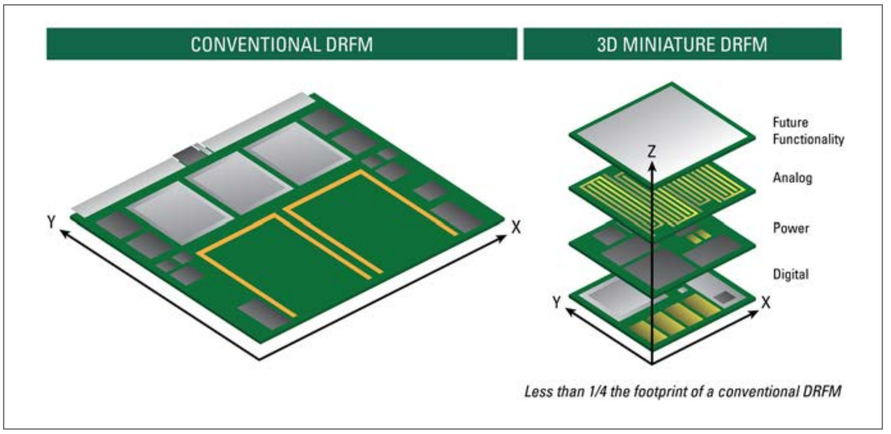


Figure 2 | Conventional DRFM device (left) with analog and digital components on the same two-dimensional plane, compared to miniaturized DRFM (right) using three-dimensional stacking of modular boards. Illustration courtesy Mercury Systems.

module must be designed to withstand any combination of high-frequency mechanical vibration, rapid acceleration during launch, extremes in thermal shock, and exposure to moisture, salt water, or corrosive environments. Addressing one of these challenges alone is a complex task; addressing all of them simultaneously requires the DRFM architect to completely rethink the approach to analog circuitry design. An appropriately designed multichip module (MCM) is a practical example of how both of these requirements can be achieved simultaneously. An example of such a MCM device, where miniaturization by a factor of more than three has been achieved, is shown in Figure 1.

On the bottom of the RF MCM device is a ball grid array (BGA) where solder balls carry power and required signals through the selected printed circuit board (PCB). The PCB material was carefully chosen to balance mechanical integrity and heat dissipation given the severe space constraints of the application. Where possible, bare die components were selected to maximize circuit miniaturization. However, this choice has consequences in terms of increased cost and reduced manufacturability. The latter can be largely overcome using engineering resources highly skilled in design-for-manufacturability principles. Even in the best-case scenario, however, not all components can be integrated as bare die. Hybrid manufacturing techniques are required to produce high-reliability MCM devices.

Ruggedizing digital components

The digital processing components of DRFM modules are far fewer in number and present fewer opportunities for miniaturization than the RF circuitry. The dimensions of the digital processing elements are restricted by the available packaging of commercial components. One area in which designers can take advantage of three-dimensional packaging techniques is by reducing the two-dimensional footprint of a planar array of DRAM modules, up to 75 percent in high-speed DDR4 memory modules. When embedded into a single BGA device, the resulting package delivers proven reliability benefits in extreme environmental conditions. Advanced three-dimensional packaging technologies using through-silicon vias offer the promise of further SWaP enhancements, but the technology has not yet achieved maturity levels sufficient to address the demanding thermal and mechanical requirements of the military market.

DRFM design for use case

Designers of DRFM modules used in less space-constrained environments view their design space as a two-dimensional plane, often with little attention paid to the third dimension. A miniaturized DRFM for a PGW, however, has such severe space constraints that all available volume must be considered as viable design space. Vertical stacking and interconnection of multiple printed circuit boards enables near complete utilization of all physical space available, as shown in Figure 2. However, in such cramped quarters, designers must now consider board-to-board signal interaction while ensuring sufficient mechanical integrity for the overall electronics package.

As DRFM microelectronic components are allocated to individual printed circuit boards for vertical stacking, the concept of modularity becomes important. Maximum space efficiency is achieved if components serving a common functionality are used on the same board. For example, all digital components have been placed on a single board in Figure 2 while the analog circuitry is colocated on a separate board. Modularity, however, offers other benefits. The separation of digital processing from the noise-sensitive RF circuitry naturally enables higher performance of the entire sensor chain. Additionally, if performance-limiting components – such as analog-to-digital converters (ADCs) or a field-programmable gate array (FPGA) – are updated by the manufacturer, modularity enables rapid upgrade cycles while reusing boards not affected by the design change. Furthermore, modularity enables early detection and resolution of manufacturing anomalies that would otherwise go undetected until final test of the fully assembled DRFM.

Space constraints and mission profiles will determine what trade-offs need to be made in the design to optimize overall system performance. For example, higher dynamic range can be realized, if required for the mission, by slightly enlarging the form factor of the stacked DRFM module; the resulting larger form factor is then better suited to address the heat dissipation requirement associated with the higher power levels required to enable the increased dynamic range.

Unlike conventional DRFM modules, which are expected to have lifetimes of many years, DRFM modules custom-engineered for PGW are in operational use for minutes and destroyed with a successful mission. Because of this extremely short operating life, DRFMs for PGW can operate at very high power levels – far beyond that of a conventionally designed and operated DRFM – thereby delivering effective electronic protection capability during the weapon's short flight. This high-power requirement complicates the overall system power supply requirements, as the digital circuitry requires a low operating voltage. The DRFM system power supply therefore must operate at high current and low voltage, with very low noise levels.

21st-century precision-guided weapons

The microelectronics content of weapons systems must continue to increase, both in RF performance and in processing complexity, to address the evolution of the modern threat environment. Miniaturization and ruggedization of microelectronics is no longer sufficient; microelectronics must be purpose-built for real-life use case scenarios with an eye towards modularity and overall system optimization.

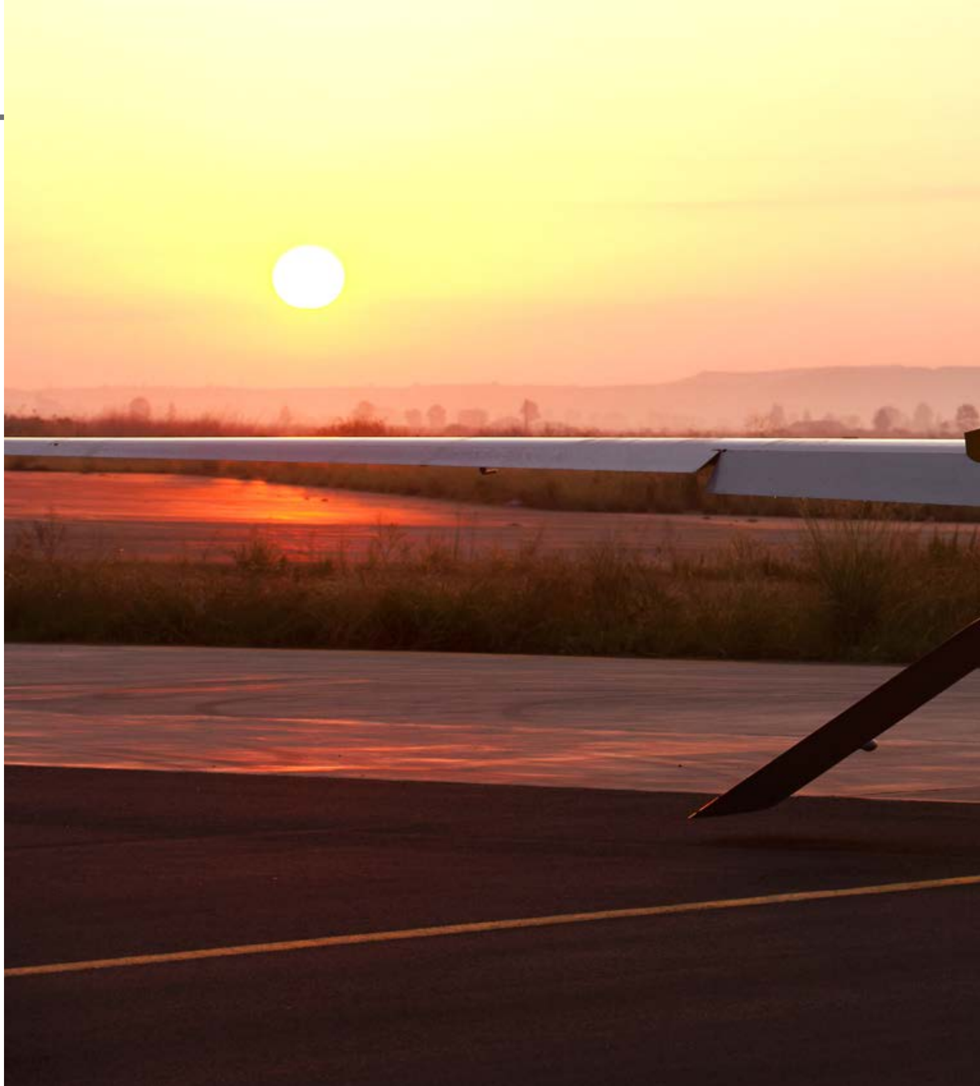
Maintaining a strategic and tactical advantage requires the defense community to continue embracing commercial technology advances while deploying innovative and upgradeable microelectronics platforms. **MES**

Charlie Hudnall *is vice president and general manager of the Embedded Sensor Processing group and Chief Technologist of the Advanced Microelectronics Systems group at Mercury Systems in Huntsville, Alabama. Charlie has a Bachelor of Science degree from Mississippi State University in Computer Engineering and a master's degree in electrical engineering from Southern Methodist University. He can be contacted at chudnall@mrcy.com.*

Philip Fulmer *is director of product marketing for the Advanced Microelectronics Solutions group at Mercury Systems in San Jose, California. Philip has a Bachelor of Science degree in Chemistry from the University of Scranton and a master's degree in Material Science and Engineering from the University of Texas at Austin. He can be contacted at philip.fulmer@mrcy.com.*

Mercury Systems
www.mrcy.com


Rugged Power Supplies from NAI
Widest Input Voltage Range
High Power Density
VITA Compliant
BIT Communications



Programmability, connectivity requirements drive digital power supply design for military use

By Mariana Iriarte, Technology Editor

A preflight inspection is performed on an MQ-1 Predator unmanned aerial vehicle. (U.S. Navy photo/Mass Communication Specialist 2nd Class Brian T. Glunt)

Flexibility and programmability along with improved efficiencies and reduced footprints flavor requirements for military power supplies today from unmanned aircraft to ground vehicles to Navy warships.

Regardless of platform – air, ground, or sea – designers of power suppliers for military electronics applications find commonality driving many of their designs as the end user wants devices that can be used across multiple platforms and meet multiple power requirements regardless of the end application.

Users want solutions that "comply with different military power requirements" so they apply them to multiple applications, says Jeremy Ferrell, manager of Standard Product Engineering for VPT Inc. in Roanoke, Virginia. This puts pressure on designers to design that flexibility from the ground up.

For example, VPT's "VXR series was designed around being very flexible and meeting many different military and commercial aviation requirements, including MIL-STD-704, MIL-STD-1275 and DO-160," Ferrell says. (Figure 1). This device enables the user "to attach the heatsink on either side, giving more flexibility to the end user's system design," he adds.

Programmability and cyber

Like many other electronics endeavors within the Department of Defense (DoD) space, users want increased flexibility to extend to programmability and connectivity.

Figure 1 | The VXR100-2800S DC/DC converter is designed for a range of applications, from military ground vehicles to commercial and military aircraft. Photo courtesy of VPT, Inc.

"We are seeing more programmable features being requested for all power products, including power supplies, solid-state power controllers, and motor controllers," says John Santini, vice president of power engineering at Data Device Corp. (DDC – Bohemia, New York). "The military recognizes the total cost of ownership, including the logistics of support, so we see a strong desire for reuse and a push for additional features and specifications to allow a part to be used in multiple applications."

With better programmability also comes the request for more connectivity.

"Connectivity has rapidly become the norm for power products," Santini says. "While simple serial data links such as RS-232 and RS-485 have been popular for years, we are seeing faster and more complex protocols being requested, such as CAN, 1553, Firewire, Ethernet, and EtherCAT."

However, increasing connectivity also provides cyber risks. Power supplies are no different than other electronics in terms of cyber protection in today's world. Nearly every piece of electronics – hardware and software – is considered from a cyber threat perspective in the DoD.

The reality is that "countering cybersecurity threats is an important element in any military platform," adds Leo Carbonneau, field application engineer at Milpower Source in Belmont, New Hampshire. "The vast majority of power conversion products are not connected to a network, and therefore do not require specific cybersecurity tools."

That does not mean that cybersecurity is not a huge issue right now. What it does mean is that companies are "addressing TEMPEST requirements to prevent against unintended electrical emissions can be an important communications security [COMSEC] step," Carbonneau clarifies. "A handful of customers do address TEMPEST requirements."

[Editor's note: TEMPEST is a National Security Agency specification and NATO certification referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations. The NSA's TEMPEST spec covers the methods used both to spy upon others and how to shield equipment against this kind of spying. The protection efforts are also known as emission security (EMSEC), which is a subset of communications security (COMSEC).]

Reliability is everything

When it comes to power supplies, reliability overarches all requirements. The power supply is critically important, since without power, any system is unusable.

"Military customers are seeking a truly rugged military power conversion solution," Carbonneau says. "MIL-STD-461 EMI-qualified solutions [for addressing] conducted emissions is a primary concern. It is not uncommon for customers, before bench testing, to verify meeting all output specifications to first run an EMI [electromagnetic interference] conducted scan as this has been the most problematic."

The military is very specific about what it needs for mission-critical systems and users "should be aware that all power conversion solutions do not address EMI adequately for military environments, which may result in the need for an external filter, which may adversely impact the power supply operation," Carbonneau adds.

"Every power conversion solution is not equal; companies sourcing a power supply for use in a military environment should pay close attention to product qualification and design attributes evident between a commercial and a true military grade power conversion solution," he continues.

Commercial/industrial versus military reliability

The military power supply market encompasses multiple applications, so much so that "The military power supply market tends to track the military market in general. Military power supplies usually need to operate over more stringent environmental conditions," Santini says.

Compared to their commercial off-the-shelf (COTS) counterparts, "[Military] specifications are usually more restrictive since their mission is typically critical," Santini. "Commercial and industrial supplies are usually optimized for a given percentage of the market, while most military power supplies have to work – and be reliable – under all expected environmental conditions."

For example, Carbonneau observes, "In the commercial market, operating temperature range is less strenuous, mechanical requirements are minimal, and low cost is the primary objective Most commercial power supplies are designed and manufactured in China, often using overstressed questionable components. In the military market, components need to be of a much higher quality, operating temperature is much wider, mechanical requirements are strenuous, weight is important, obsolescence is to be avoided, and component traceability is important."

WHEN IT COMES TO POWER SUPPLIES, RELIABILITY OVERARCHES ALL REQUIREMENTS. THE POWER SUPPLY IS CRITICALLY IMPORTANT, SINCE WITHOUT POWER, ANY SYSTEM IS UNUSABLE.

"The Senate Armed Services Committee delivered a clear message to the defense community regarding the selection of power supply products for use in military systems," Carbonneau says, pointing to the National Defense Authorization Act For Fiscal Year 2018.

"In the 'Commercial off-the-shelf power supplies' section, on page 199 of the document, the committee communicated two key points pertaining to the selection of power supplies for military applications," Carbonneau notes. "First, it noted that COTS parts (e.g., products not designed to MIL standards) introduce unnecessary risk and are a primary source of failures in military systems. The committee went on to request that program managers and acquisition professionals prioritize the design and qualification of the power supply products selected for use in military applications."

So, while commercial users do not need worry about many of these requirements, they like the military still has to contend with reduced size, weight, and power (SWaP) restrictions, which some may argue is the the biggest trend across all military electronics applications, even more so than cyber.

SWaP then and now

Historically, changes to power supply technology have been evolutionary rather than revolutionary, Santini points out. "The major disruptions have been the power switches that drive them."

The history of power supplies show that the "earliest solid-state switches were germanium," Santini says. "Then germanium was displaced by silicon, bipolar transistors gave way to FETs [field-effect transistors], while most recently the introduction of silicon carbide (SiC) and gallium nitride (GaN) parts is proving to be the next step. These changes have pushed switching frequencies up, and as switching frequencies go up, size and weight go down. Lower saturation losses and faster switching times reduce power losses, pushing efficiency up. Dissipating less power helps make the power supply smaller."

Cutting-edge technology has proven to help meet the constant SWaP challenge. For example, says Santini, "[SiC] and [GaN] nitride parts are enabling switching times a fraction of the parts of just a few years ago. Output rectifier diodes are being implemented as synchronous switches in more and more designs."

Santini points to DDC's 60 W DC-DC Converter, "a legacy triple output 60 W design, which will soon be upgraded to a GAN-driven design." It is currently a 60 W DC-DC Converter (Figure 2), however, "raising the frequency to 450 kHz could increase the output power rating to over 200 W."

Moreover, "Control methodology has also played a part in this evolution," Santini adds. "The availability of small, fast microcontrollers has enabled overall control to improve. Early uses were typically for monitoring and housekeeping, and later for cycle-by-cycle control."

The end result: Fully digital power supplies that enable the programmability and connectivity that users are asking for. "Today, many power supplies are fully under digital control," Santini notes. "As topologies, magnetics, and other passive components are developed to take advantage of these new parts, you can expect size and weight to continue to shrink, as efficiency continues to rise."

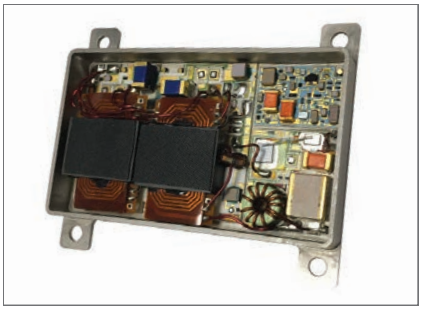


Figure 2 | Data Device Corp. (DDC) 60 W DC-DC Converter. Photo courtesy of DDC.

This evolution has moved the industry toward small-form-factor power supplies, primarily VPX, Carbonneau says: "The VPX standard makes available compatible cards from different manufacturers, all based on a standard connector and mechanical design. This minimizes the packaging design, including the backplane, and can take advantage of off-the-shelf modules."

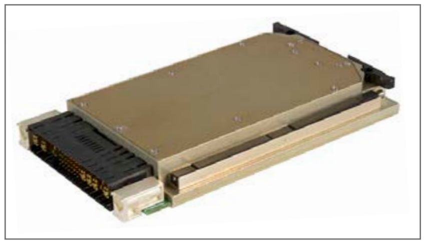
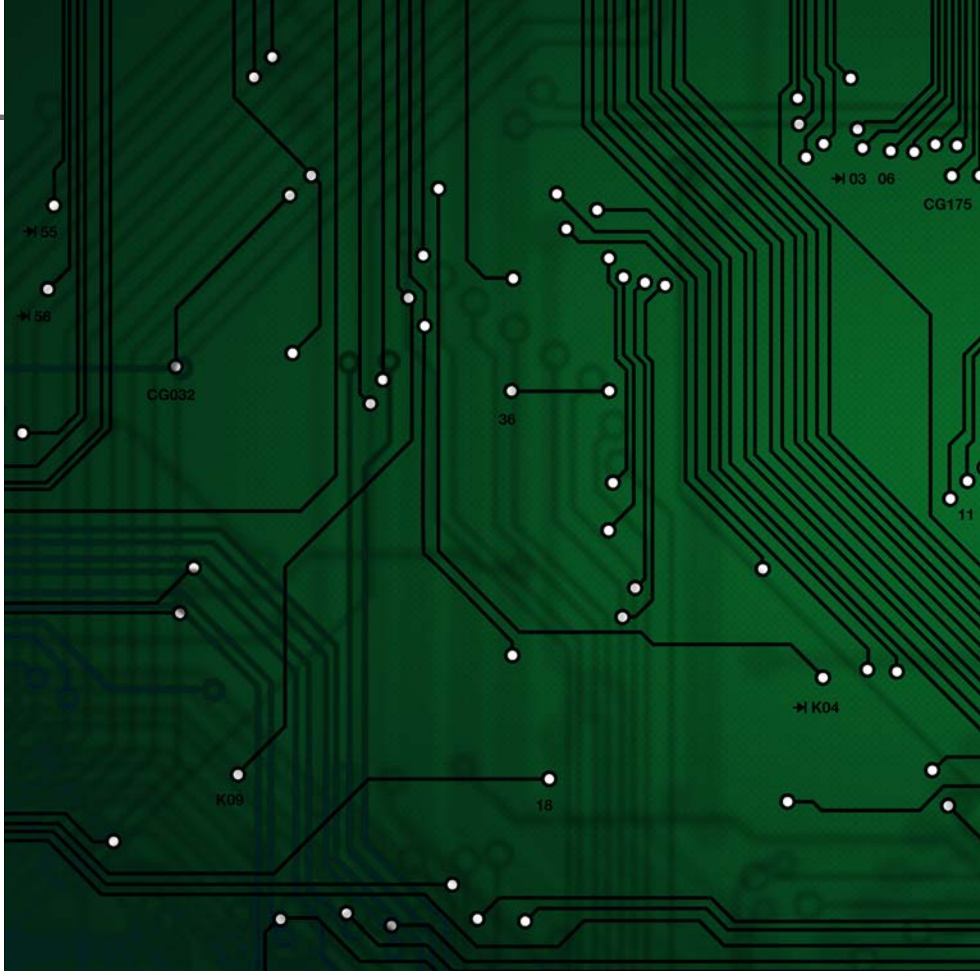


Figure 3 | Milpower 4065 VPX VITA 62 3U power supply. Photo courtesy of Milpower.

Milpower's 4065 VPX VITA 62 3U power supply (Figure 3) "is wedgelock conduction-cooled, providing six outputs at 600 W with an input voltage range of 18Vdc to 48Vdc over the full operating temperature range of -55 °C to +85 °C," as Carbonneau describes the product.

"While a standard is being sought, this should not be confused with COTS solutions. The ability of a VPX power conversion solution to perform consistently in a military environment is critical," Carbonneau adds. **MES**



Capacitive load switching sources in military systems: How to extend relay switching life and reliability

By Mike Baldwin

With high-performance electromechanical relays continuing to play an important part in military and aerospace applications, it is important for engineers to capture all the electrical requirements. A critical area is extending relay switching life under capacitive transient high inrush current conditions by complying with manufacturers' relay product performance specifications. Capacitors generate high current surges that can adversely affect circuit performance in such applications. These transients, while very brief in nature, can dramatically exceed the steady-state ratings for the contacts in a high-performance electromechanical relay.

When capacitive loads are properly identified and contained by the customer within the relay capabilities, a higher degree of application-relay compatibility can be achieved. Adapting the relay circuit design with current inrush reduction components can mean substantial reduction of capacitive transient high current loads and can increase relay contact life and ensure a relay utilized within its rated product performance specifications will meet the load switching requirements of the end application.

Capacitive inrush contact damage

Occasionally in military and aerospace relay switching applications, surprising sources of capacitive inrush can appear. One example would be the rapid heating and cooling of the material used in the relay, likely due to a very high current pulse of very short time duration, which exceeded the product's performance specification. Such overage can lead the contacts' material to fuse and separate, resulting in erratic operation.

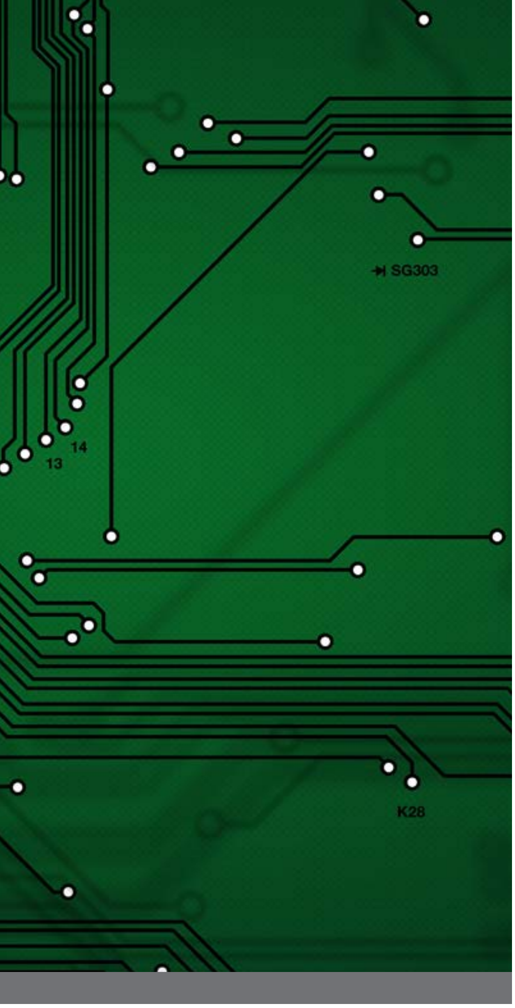
Capacitance comes from where?

While very large electrolytic capacitors lead the engineer to expect high current surges, there are often other, less easy to identify, capacitive sources in circuits. Capacitors are passive devices that resist instantaneous voltage changes while allowing instantaneous current changes that quickly absorb and release large amounts of energy as current surges.

One seldom-recognized source of high capacitance and inrush current is the EMI [electromagnetic interference] filtering common in DC/DC switching power converters for military and aerospace applications. (Figure 1.) From the rapid ON-OFF switching of the converter, large, discontinuous current changes are induced that require substantial filtering to reduce conducted high-frequency EMI noise. The popular solution is the use of low pass filters on the input and output of the DC/DC converter.

NTC current limiter devices

There is a class of resistive devices that can offer substantial current surge limiting. The specialized resistor is known as an NTC, or Negative Temperature Coefficient thermistor. It offers high initial resistance that drops quickly to a much lower value



as the device temperature increases from current flow.

At room temperature, the high initial nominal resistance limits the inrush current peak by quickly absorbing the energy and dissipating it over a thermal time constant. The resistance of the current limiter NTC drops by a factor of 30 to 50 times from its initial value. After removal of the power source, the NTC devices used in the following experiments return to room temperature in approximately five minutes, according to the thermal time constant curves in the following graphic (Figure 2).

NTC testing: repetitive cycling effects

NTC devices internally self-heat over a relatively short thermal time constant while dramatically reducing their internal resistance. Rapid pulsing of the NTC showed how sensitive and rapid was the response to self-heating temperature. When the 5 ohm NTC was tested with four pulse events in less than three seconds, the initial peak current level increased from 5.4 A to 8.5 A, an increase of 57 percent. The thermal time constants of NTC devices are often addressed by using them only during the initial inrush current pulse level, and then allow cooling, which in effect "resets" the NTC for the next high-current switching event.

Load-testing NTC current limiters

It was decided to set up the test to represent the input and output EMI filters and the input and output DC/DC converter capacitors and inductors. The total capacitive load measured was 717.6 uF for the development board since effectively all the filtering capacitors are in parallel. The procedure to test the development board involved supplying DC coil drive voltage through selected switches to provide the ability under load switching conditions to disable/enable each value of NTC device.

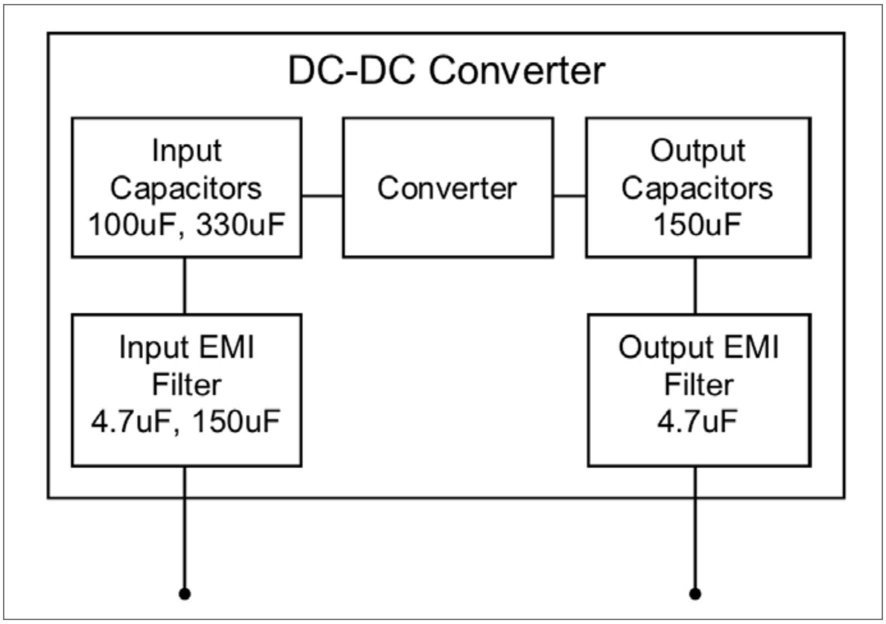


Figure 1 | Block diagram of a typical DC/DC converter

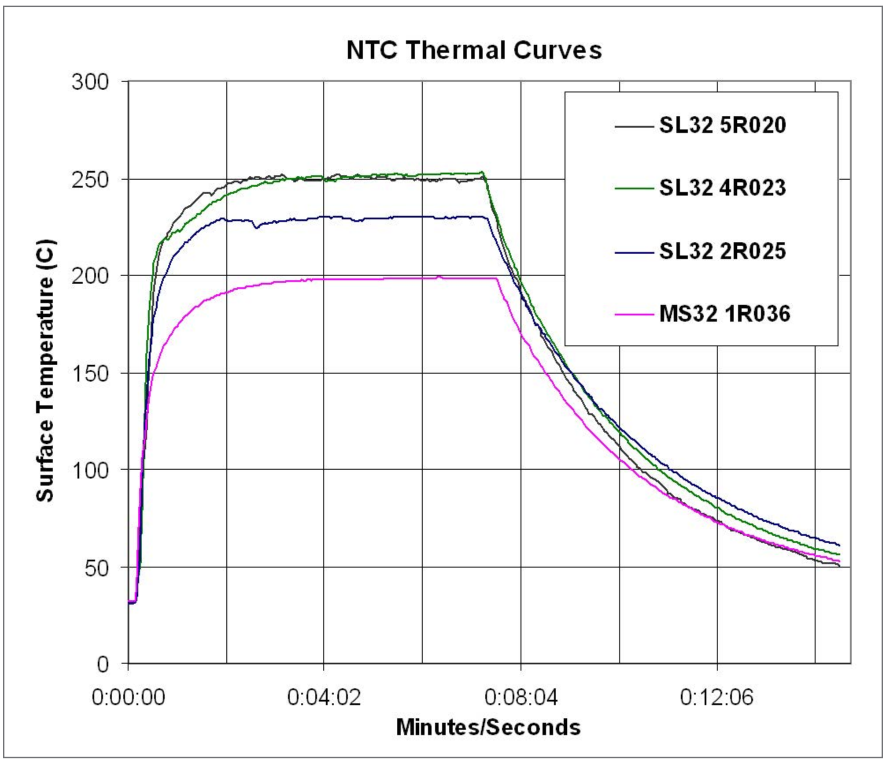


Figure 2 | NTC thermal time constants.

NTC load-testing life configuration

To test the NTC devices, it was determined that the development board required a resistive load on the output. The purpose of the resistive load was to simulate a 300 watt DC/DC converter supplying power to an application. Experimental efforts determined that NTC temperature rise and subsequent changes to internal resistance could be managed by controlling the cycling rate and duty cycle of the switched current pulses during relay life testing. (Figure 3.)

The NTC switch subassembly has a time-delay subassembly and shunt relay that operated approximately 20 milliseconds after the start of each pulsed coil event, effectively opening the current path through load. This resulted in the relay combinations carrying the step current but not breaking the current path.

The procedure to life test the relays involved supplying 26.5 Vdc coil drive voltage individually switched to six relays. The 26.5 Vdc load supply voltage went to the load enable FCA-325 3PDT 25 A relay. Then it was routed through the NTC Off/On FCA-125 SPDT 25 A relay to individually insert the NTC device or test with no NTC in circuit. The connection of a 3.0 ohm noninductive load resistor powered from a 26.5 Vdc source provided a nominal load of 9 A, or about 239 watts, for switching.

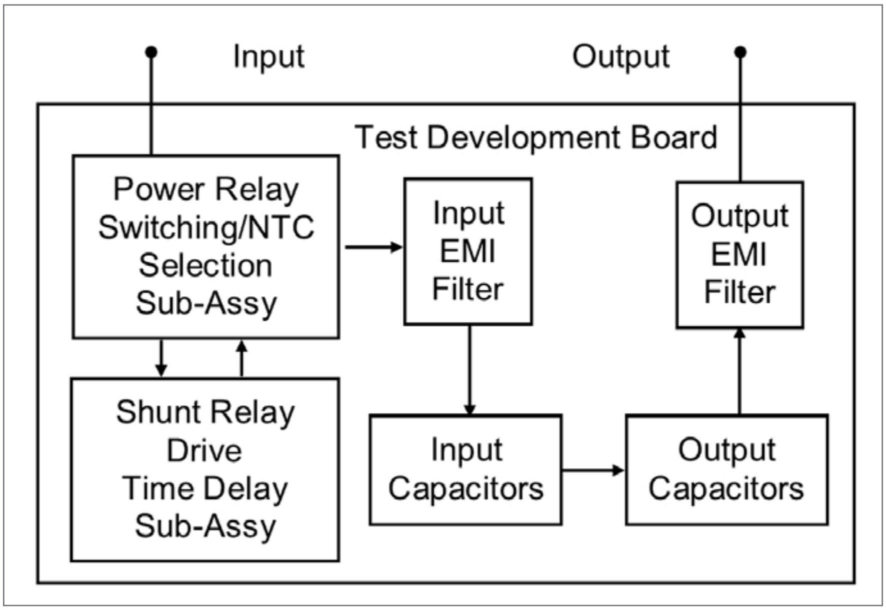


Figure 3 | Block diagram: Testing development board.

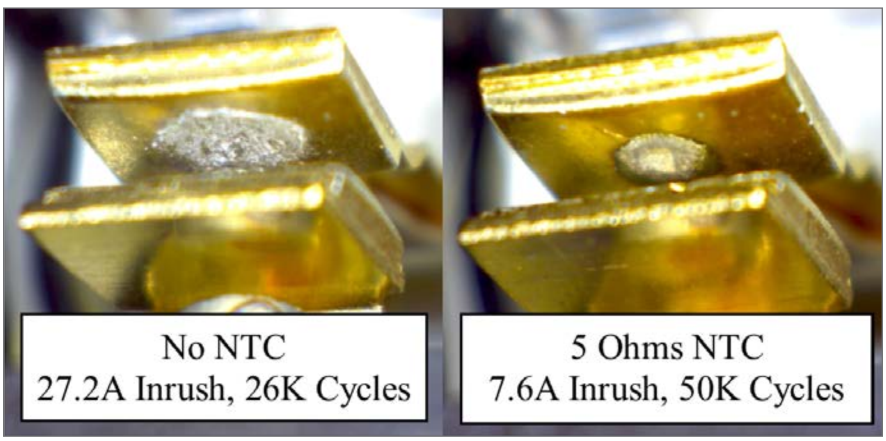


Figure 4 | Contacts evaluation: (left) Without NTC, (right) with 5 ohms NTC.

NTC load testing life results

No NTC: The first relay life test was performed with no NTC device in circuit. The relay was cycled at a rate of 20 cycles/minute and showed a sharp, high current transient at the start of the switched event. The pulse reached a peak of 26.8 A with a duration of 680 microseconds as part of the 20.2 ms of make/carry-only current time. The current level stabilized at a steady-state level of 9.2 A. The non-NTC load test was terminated early at approximately 26,000 cycles of the planned 50,000 cycles. This was due to contact "sticking" or tack welding that repeated several times and supported the thesis that unlimited capacitive inrush switching is often the primary cause of contacts sticking.

5 ohms NTC: Individually, each NTC value was used during relay life testing with the highest nominal resistance NTC of 5 Ohms having the greatest peak current inrush reduction. The peak current level started at 4.80 amps, a reduction of over 82 percent from life testing without any NTC in circuit. The peak current pulse length duration was measured at 3.84 ms, which then decayed to the step current of 3.20 A. The make/carry-only pulse length was measured at 18.20 ms at the start of the testing.

Test measurements were recorded again at an intermediate period and the conclusion of the 50,000 switching cycles and then compared to the initial readings. Due to the thermal characteristics of the NTC devices, slight increases in the operating temperature substantially affected the peak current level as it increased over 58 percent, to 7.60 A. It was confirmed that the step current level increased by 38 percent, to 4.40 A.

NTC life testing summary

Peak inrush and steady-state step current levels waveforms were analyzed for any substantial trends. As expected, the rapid cycling of the NTC/relay combination did elevate the respective peak and step current levels over time; however, even the lowest NTC value kept the inrush below the maximum relay contact ratings.

The testing showed that the peak inrush current had the largest gain of 36 percent for one ohm NTC, increasing to 58 percent when 5 ohms NTC was in circuit. The step current increase was much more modest and ranged from 6 percent to a maximum of 38 percent. The NTC external case temperatures were compared during the testing and had a very slight 6 to 7 °F, or 8 to 10 percent rise, above ambient. The slight change in NTC temperature confirmed that it would affect the peak and step current levels during relay life test cycling.

Contacts evaluation, post-NTC life testing

At the conclusion of life testing, each of the five relays were removed from the NTC/relay switching board and electrically tested to confirm that each met post-life test parameter limits. Review of the normally open and moveable contacts in the first relay illustrated substantial contacts material erosion and transfer as expected. This relay switched the full capacitive load without any NTC current limiting with testing stopped at 26K cycles, well short of the 50K cycles due to repeated contacts tack welding. There were visual signs of contact material adhesion and breakaway on the moveable contact that contributed to tack welding and likely mechanical binding of the moving contact surfaces.

Quite a different visual story was told when the relays with NTCs in circuit were opened and analyzed. The relay switching the load through 1 ohm NTC had material transfer reduced by an estimated 40 to 50 percent and substantially reduced the "cone and crater" affect. Moving through the tests, the relay switched through the highest resistance NTC, 5 ohms, had slight buildup of material on the normally open contacts and smaller corresponding crater on the moveable contacts. (Figure 4.)

Going forward

User applications often involve capacitive loads from common EMI filtering sources. By using NTC devices within their thermal time constant limitations, they were confirmed to substantially reduce the magnitude of the inrush currents and resulting contact material erosion. Experiments demonstrated that the inrush current reduction and reduced contact erosion extended the relay contacts' switching life when capacitive loads are present by helping the user remain within the relay's rated product-performance specifications. These improvements can lead to enhanced reliability of the equipment in military and aerospace applications. **MES**

Michael Baldwin *joined TE Connectivity, CII Products, in 1986 and is currently product applications engineer for the high-performance, aerospace, and high-reliability space relay products. He is a summa cum laude graduate of Western Carolina University, with a Bachelor of Science degree in electronic engineering technology and a Master of Science degree in technology; Mike also received A.A.S. degrees in electronic technology and business administration from Asheville-Buncombe Technical Community College. Readers may contact the author at baldwinm@te.com.*

TE Connectivity • www.te.com

Mission-critical power start-up demands perfect performance every time

By David Berry

Design of a mission-critical, rapid-start, isolated power system needs to be flawless. These systems, leveraged in mission-critical military applications, need to start in milliseconds – every time.

Photo of F-16 courtesy of Robert DeRobertis.

The purpose of the power supply in an electronic system is to provide a regulated voltage and/or current to a load. Attention is given to the performance of the power system in its response to rapidly changing loads and to rapidly changing voltages demanded by the load. The input voltage and start-up time of the power system is given much less consideration because it is generally assumed that the power source to the system is always present.

However, there are systems where the power source isn't present and the system must be active within milliseconds (ms) of application of input power. These systems typically require isolation from the power source to keep grounds isolated or to meet military specifications such as MIL-STD-704, which defines a standardized power interface between a military aircraft and its equipment.

For example, in many missile-launch systems, the target information isn't programmed into the missile until moments before launch. There are several systems that need to be active within the missile before target information is loaded; the power system is only one of these systems, and it needs to be the first system that is active to drive all the others. Therefore, the power system must get it right every time.

Designing mission-critical power systems

There are a few critical areas of consideration when designing an isolated power system that must start within 10 ms from application of input voltage. The input dv/dt should not exceed the ratings of the power components, the input capacitance cannot cause the sourcing components to exceed their ratings, and the output capacitance value should be selected such that the system does not go into current limit or exhibit instability.

The input section of many DC/DC converters includes an LC filter. If this LC filter is hit with a step voltage – that is, application of DC to the power system – the LC filter can ring up to a voltage level that can damage the internal circuitry of the power component. A common specification for maximum input dv/dt is 10 volts/microsecond. A mechanical switch or field-effect transistor (FET) that closes too quickly can easily exceed a 10-volt/microsecond rise time. An input filter with current limiting would keep the input to the DC/DC converter within its input dv/dt specifications.

Figure 1 shows the power system block diagram and Figure 2 shows the block diagram of the internals of a typical input filter. The input to a regulating DC/DC converter typically needs an input capacitor because it needs to see low source impedance and insure converter stability over line and load changes. This capacitor needs to

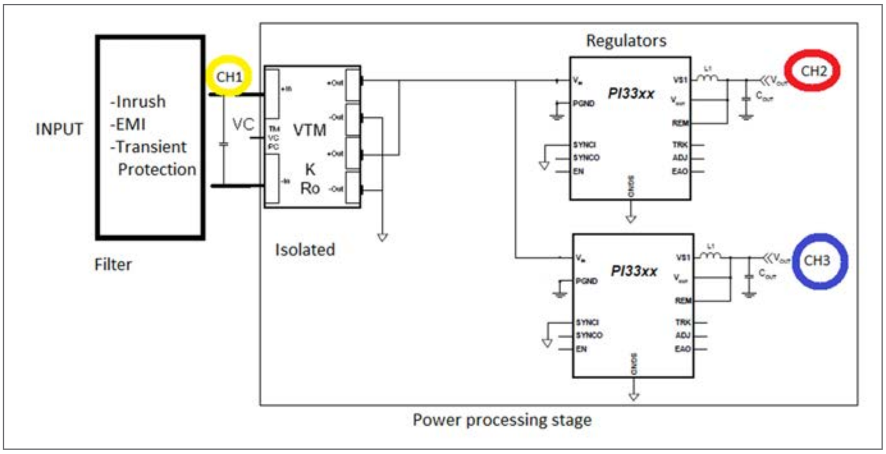


Figure 1 | Power system block diagram

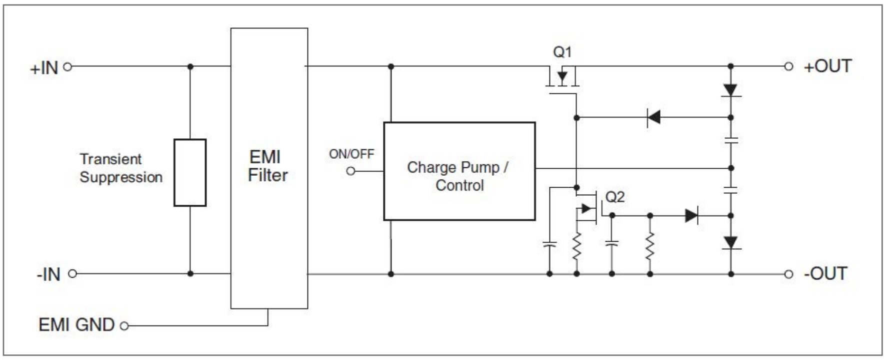


Figure 2 | Internal workings of a typical input filter.

be charged slowly as to not exceed the maximum dv/dt, but fast enough to help achieve the less than 10 ms start-up time of the power system. Starting at the application of system input voltage, Q1 in Figure 1, is off. At the undervoltage turn-on level the Charge Pump/Control block in Figure 1 will begin to enhance Q1 and raise the output voltage of the filter. This output voltage rise is controlled to not exceed the input dv/dt of the converter as well as control current drawn from the source.

Capacitance: important factor in rapid power start-up

To aid in achieving a less than 10 ms start time the filter must charge its output C as fast as possible. Selecting the lowest value of this output capacitor is best when designing for a fast turn-on time. Using an unregulated isolator at the output of the filter would be best because these require little to no input capacitance, they don't regulate, and thus don't affect the control loop. A good input filter will also include EMI and transient protection to meet MIL-STD-461 standards for EMI and MIL-STD-704 and MIL-STD-1275 for input transients.

If an isolator is used at the output of the filter and the filter output rise time is controlled, then the output of the isolator will be controlled. The isolator's output mirrors the input by the voltage ratio of the converter. This will keep the downstream regulators shown in Figure 1 within their input dv/dt specification range. The regulation stage does need input capacitance for source impedance requirements and stability, so this needs to be taken into account when determining capacitance seen by the filter. The isolator will reflect its output capacitance to its input and this will be seen by the input filter.

The capacitance reflection is the isolator's output/input voltage ratio squared, multiplied by the isolator's output capacitance. If the output/input voltage ratio is 1/2, and the isolator's output capacitance is 47µF then the reflected capacitance to the filter is 1/2 squared, times 47µF or 11.75µF. The performance of the isolator is critical in this application. The isolator needs to have very little inductance as part of its power train. The low values for inductance enables current to flow rapidly from input to output while maintaining a fixed input to output voltage ratio. Some isolators have power train internal inductances in the nH range.

The input filter also keeps the source from exceeding its maximum current ratings. As an example, during a high dv/dt event such as a hot plug, mechanical switch, or FET switch closing, the filter will shield any capacitance from seeing this high dv/dt. The power system source always has a maximum current rating due to source capability, connectors and traces that go to the power supply. If these components see higher current levels they can fail or become weakened and turn into latent failures. In power systems that require less than 10 ms start-up, the input voltage to the supply must come up quickly as this timing is part of the 10 ms start-up. A quick start-up into capacitance will result in high inrush current. The filter helps to reduce this inrush. Many filters have inrush ratings in Amps per output µF. If the rating is 0.007A/µF and you have 47µF at the filter's output then the inrush current is 0.007A*47µF or 0.329A.

In many applications, the power supply will have its own output capacitance as well as load capacitance. This capacitance is charged by the output voltage of the converters. When designing for a less than 10 ms start time the output voltage rise across the output capacitance must not cause the converter to exceed its current maximum, resulting in shut down or output voltage dip due to current limit. If the converter shuts down and restarts then the start-up time is lengthened. If the converter goes into current limit then the output voltage drops, resulting in a longer rise time and extension of the start-up period.

Taking this into account, it is best to design using the smallest amount of output capacitance possible. The output current charging the output capacitance is determined by the equation: I = C* dv/dt, where I is the converter output current, C is the output capacitance, and dv/dt is the converter output voltage rise time. If the load is active during the rise time, then this needs to be added to the current supplied by the converter. In either case, the current should not exceed current maximum. If the current does exceed the maximum, then another converter in parallel can be added to boost the current rating of this output.

The output capacitance of the converter helps keep the converter output ripple low and helps keep the converter stable during operation. Using a converter with a high switching frequency will help with keeping the output capacitance low. The high switching frequency will allow the design to use low values of inductance and capacitance to maintain output ripple as low as 30 mV to the load. Typical switching frequencies are in the 500 KHz to 1 MHz range.

When designing a power system for less than 10 ms start-up as shown in Figure 1, there will be several components that must become active and stay within each component's power, voltage, and current ratings. When the system input voltage is applied, the filter controller must wake up and begin controlling the filter's output voltage, keeping the source current below its maximum, and keeping the downstream converters within their maximum input dv/dt. When the downstream converters reach their undervoltage turn-on level, their internal controllers must wake up and effectively control their output voltages, charging the output capacitance, and in many cases the load current demand.

These wake-up times are cascaded; the resultant wake-up time has to be less than 10 ms. Figure 3 shows the performance

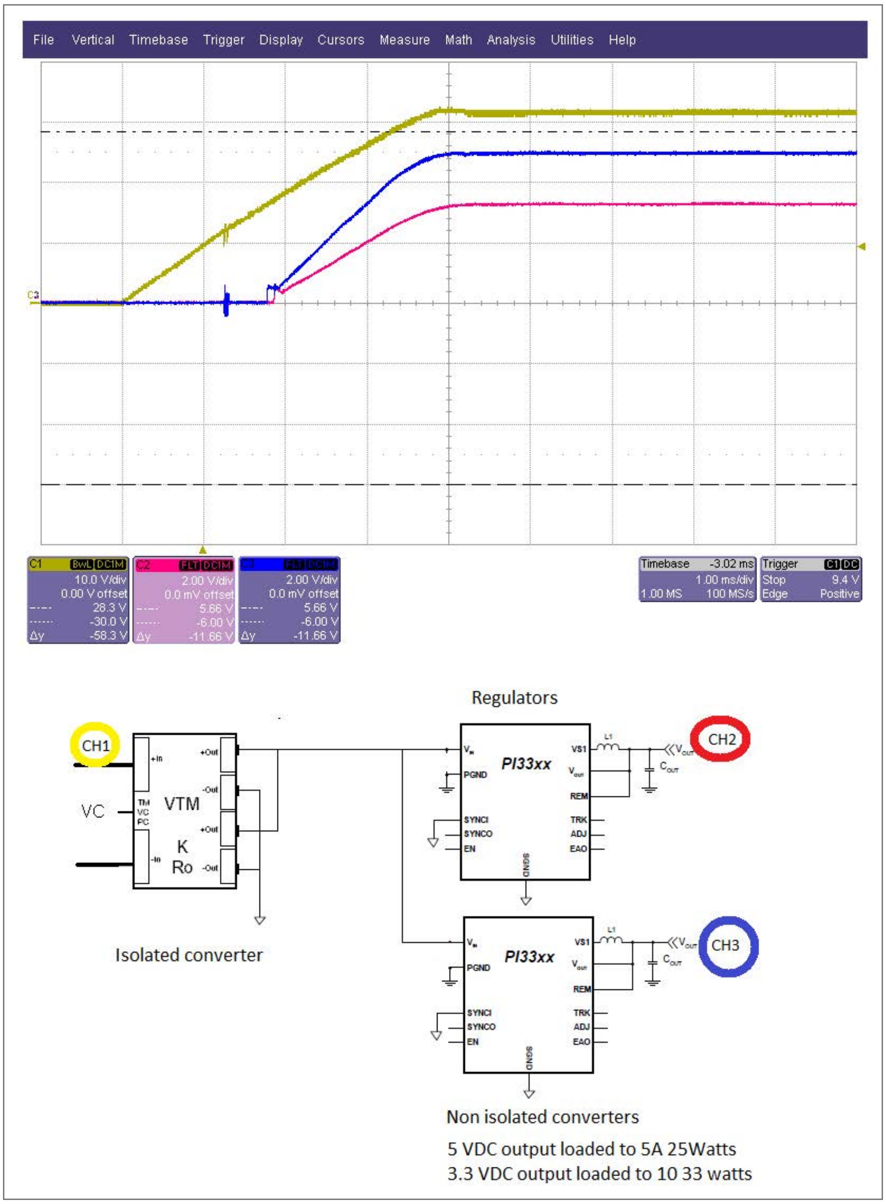


Figure 3 | A power system configured for a start-up time of less than 10 ms.

of a power system configured for a less than 10 ms start-up time. The system is configured with an isolator and two nonisolated regulators. The isolator enables the system to have a separate ground between input and output. The regulators are starting into a load of 25 watts and 33 watts, while the start time from application of input voltage is measured to be around 4 ms. This system is very scalable, simply by adding power components in parallel or using components with higher power levels. Adding components in parallel also enables redundant operation.

Designing an isolated power system with less than a 10 ms start-up time is achievable and reliable when using the right components. Those with high efficiency and small size makes them perfect for many military applications. **MES**

David Berry has a Bachelor of Science degree in electrical engineering from Union College in Schenectady, New York. He was a former magnetics designer specializing in impedance matching transformers; he now works for Vicor Corp. as a principal applications engineer. He has been working in component power design for 20 years.

Vicor Corp. • www.vicorpower.com

Battlefield servers demand design for heat, spares, and application portability

By Chris A. Ciufo

Freezing conditions at 40,000 feet; scorching heat in the Middle East. These are the world's battlefields for rugged servers.

Photo credit: Edric Thompson, U.S. Army/CERDEC.

Today's battlefield environments range from land to sea to air, but even in these diverse domains, three key design elements are necessary to keep battlefield servers operational where lives are at stake.

First, high-performance servers require innovative heat management to achieve maximum system performance without CPU throttling, even in the hottest desert conditions or in cramped, sealed environments. Second, reliability is critical, making line replacement units (LRUs) a key element that must be considered at the early design stage. Finally, application code reuse requires a modular approach so that the same application software is portable across many different server types based upon the installation as a way of saving money.

Heat is a server killer

On land, battlefield servers are commonly deployed in fixed-building platforms such as CONUS [Continental United States]; in tents or trailers used for quasi-fixed, behind-front-lines operations centers; or in mobile vehicles such as Humvees, MRAPs [mine-resistant ambush-protected vehicles], or Strykers. But heat is a killer for servers, especially in today's desert battlefields. Commercial temperature components operate at 0 °C to 70 °C and their performance suffers (or results in failure) when they get too hot. When Intel processors get close to their maximum 100 °C temperature, the CPU throttles, slowing down the clock to lower the workload and the device temperature. When this happens, the server slows down, its performance suffers, and under battlefield conditions, the slowdown could result in loss of life.

In buildings, tents, and trailers, servers are typically air-cooled (via convection) rackmount equipment, 19 inches wide and stacked with other gear such as RAID [redundant array of independent disks] drives, power supplies, Ethernet switches,

Figure 1 | A modern air-conditioned server room is dramatically different than a battlefield tent. (Image via Wiki Commons, courtesy of CSIRO.)

and sometimes rackmount radios. Convection servers use fans and pure commercial-temperature components. These are often the same equipment used in enterprise installations, which work in an air-conditioned server room (Figure 1) but not in burned-out battlefield command post buildings or mobile operations tents. In these locations, large, portable air conditioners are required to keep servers operating without overheating.

When rackmount servers operate without air conditioners, throttling can only be avoided with efficient air flow across the system and by effectively moving heat from components such as the processors onto the heat sinks. An effective approach is to use two hot-swappable fan tray assemblies that each contain six independently controlled fans. At 10,000 rpm per fan, hundreds of CFM [cubic feet per minute] are available to the entire 19-inch chassis to keep the system cool. To get the air to the heat sinks requires a very large assembly – as much as the full surface of a 6U VPX motherboard – plus vertical fins (Figure 2).

An additional approach uses one set of fans to push air across the heat sink assembly, while a second set pulls air out of another part of the system, intermixing cooler inlet air to counterbalance the warmer air moving across the heat sink. Individual fan control can be used to monitor multiple in-system temperature sensors so air flow can be tuned for maximum cooling.

In vehicles, servers might be rackmounted and installed in suitcase-like transit cases, but increasingly they are conduction-cooled small-form-factor (SFF) sealed chassis that are more robust and purpose-built to handle Xeon-class workloads. These systems may require new cooling technologies, such as the use of a viscous metallic

Figure 2 | Close-up of dual-processor server heat sink. This OpenVPX-based motherboard in the GMS S2U "King Cobra" server is engineered with wider fins for cooler inlet air, and narrow fins for more cooling when the air is warmer.

bath in which the processor's contact slug sits, creating a very low thermal path from the hot processor package to the final air-cooled heat sink. The result is less than a 10-degree heat rise from the hot die to the heat sink (Figure 3). This efficient thermal path means that more than 90 percent of the heat from the processor makes it to the heat sink and into the air stream, which makes it useful for an air-cooled server on a battlefield without air conditioning. For conduction-cooled battlefield servers, this technology moves heat directly to the box's mounting cold plate.

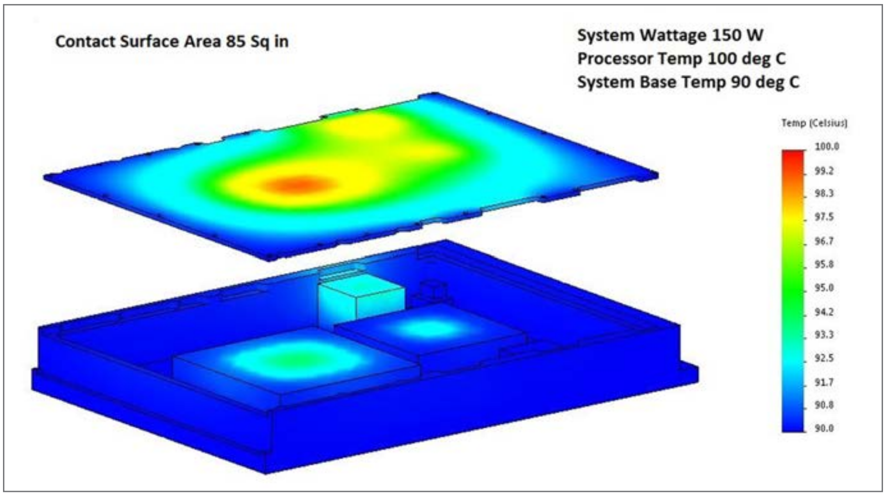


Figure 3 | A heat sink can maintain less than 10-degree heat rise between the hot CPU and the cooling plate.

Spares can be a logistical nightmare

Battlefield servers have unique requirements in other areas besides environmental. One is reliability: For rackmount servers, the ability to quickly replace a module due to failure or for an upgrade drives the need for modularity and hot-swap line replacement units (LRUs). Every module of the system – from power supply and fan assemblies to VPX-based motherboard and drive assemblies – must be replaceable in seconds. This is the downfall of typical commercial off-the-shelf (COTS) 1U or 2U servers: If there's a failure, the entire server must be replaced.

One of the biggest users of commercial rackmount servers is the U.S. Navy because the air-conditioned shipboard environment is typically tolerant of commercial equipment. Ships stockpile large volumes of new, brand-name servers that are constantly deployed as spares for the servers that are widely deployed on the ship.

In contrast, battlefield-rugged servers bring higher mean time between failures (MTBF) and can operate longer in environments that experience extreme heat, moisture, shock, and vibration, while remaining competitive with commercial server costs. A modular design for these purpose-built servers enables anything in the system to be swapped out on the battlefield, underway on board the ship, or in the air on a reconnaissance mission. This is particularly important in a submarine, for example, where carrying a few replacement modules is far more practical than hauling around a large quantity of spare servers.

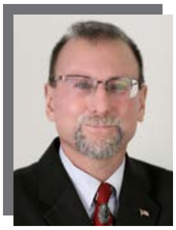
Application code reuse across platforms

Many large defense contractors have multiplatform systems, such as a command module with moving maps, sensor fusion, and database retrieval that overlays data on the unfolding mission scenario. This command system may reside in an air transport rack (ATR) or vetronics chassis mounted in an armored vehicle or widebody aircraft, could be in an air-cooled rack on a ship, or may need to be shoehorned into an SFF system on a multimission ground vehicle.

The same application software must be portable across many different server types, so the customer merely chooses the format of the server based upon the installation. That choice requires rugged servers to be code-compatible within the same processor family using a computer-on-module (COM) engine that houses the processor or processors subsystem, such as an Intel Xeon E5, Xeon D, or future processor types. The engine is the same, whether used in a VPX server blade, a SFF conduction-cooled chassis, an air-cooled 19-inch rackmount, or even sandwiched into a smart-panel PC display.

Purpose-built battlefield servers

Battlefield servers are being designed into a wide range of demanding defense applications. These include forward-deployed operations centers mobile tatical command posts; vehicle-mounted network infrastructure for semipermanent battlefield operations; shipboard systems; widebody command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) and electronic warfare platforms; and airborne command infrastructure that links to onboard and SATCOM [satellite communication] networks. For each of these diverse domains, a modular, purpose-built design approach ensures operational success for systems where lives are at stake. Key design considerations include innovative approaches for heat dissipation, modular spares to ensure system reliability, and application portability for multiplatform systems. **MES**



Chris A. Ciufo is chief technology officer and VP of product marketing at General Micro Systems, Inc. Ciufo is a veteran of the semiconductor, COTS, and defense industries, where he has held engineering, marketing, and executive-level positions. He has published more than 100 technology-related articles. He holds a bachelor's degree in EE/materials science and participates in defense industry organizations and consortia.

General Micro Systems • www.gms4sbc.com

Truly rugged and proven reliable: VITA 47 and beyond

By Aaron Frank and Ivan Straznicky

Composite photo courtesy Curtiss-Wright.

All vendors of commercial off-the-shelf (COTS) hardware intended for use in harsh defense and aerospace environments insist that their products are reliable as well as rugged. But without a consistent baseline for comparison, it's almost impossible for system integrators to objectively confirm whether one COTS product is more reliable than another. The VITA 47 standard gives system integrators just such a baseline as it is an American National Standards Institute (ANSI) standard.

ANSI/VITA 47 – introduced in 2005 – defines a set of rigorous environmental, design, and construction, safety, and quality requirements for plug-in COTS hardware that is intended for use in mobile defense and aerospace applications. VITA 47 provides system integrators with a common standard they can use to ensure that the COTS modules they are evaluating provide the functionality needed and that they meet environmental and durability requirements.

The VITA 47 standard outlines requirements for the following environmental factors:

- Temperature, including operating temperature, nonoperating temperature, and high levels of repeated thermal cycling
- Shock and vibration, including operating conditions and bench handling
- Humidity, altitude, and rapid decompression
- Fungus and corrosion resistance

VITA 47 also includes the following design, construction, safety, and quality requirements:

- Workmanship, including soldering to IPC Class 3, conformal coating to IPC Class B, and printed wiring board (PWB) fabrication to IPC Class 3
- Safety, including material restrictions to avoid hazardous or restricted materials, flammability to EN (European standards) or UL (U.S. and Canadian standards) specifications, and toxicity limits
- Quality to the ISO 9001 standard

The requirements defined in the VITA 47 standard are divided into levels within classes, with increasingly stringent test demands at each level. System integrators who require their embedded systems to perform optimally in extreme conditions should seek COTS products that have passed the highest levels in the VITA 47 standard.

Look for long-term reliability

COTS products that pass the highest levels in the VITA 47 standard are proven to meet the most challenging environmental requirements, including operating temperature,

THE IDEAL APPROACH IS TO COMBINE VITA 47 TESTING WITH A COMPREHENSIVE SET OF RELIABILITY ANALYSES, TESTS, AND PROCEDURES DEVELOPED OVER THE COURSE OF KNOWLEDGE GAINED BY DESIGNING, BUILDING, AND TESTING COTS PRODUCTS.

nonoperating temperature, and temperature cycling. For the popular conduction-cooled format, the VITA 47 levels are defined as ECC1 to ECC4 (Table 1).

For system integrators that need to assess the long-term reliability of COTS products, temperature (thermal) cycling tests prove particularly important. Even so, while evidence that a given COTS product has been tested to and passed the VITA 47 ECC4 level can provide a system integrator with confidence in the long-term reliability of the product, it doesn't necessarily provide an indication of expected life span. One of the best ways to determine the expected lifespan of electronics is to develop a "life profile" for the product and then evaluate what that profile means in terms of the VITA 47 thermal cycling requirement.

A life profile estimates the numbers of cycles of various environmental scenarios the electronics is likely to experience – the number of hot days, cold days, and days with ground operations, for example. For airborne systems, it's also important to consider the temperature ranges when the platform transitions from the ground to a high-altitude environment and back again. The total number of cycles can then be translated into accelerated thermal cycling tests with the corresponding number of cycles and temperature extremes.

As an example, a survey of temperature cycling requirements across 11 defense programs that required 10 to 30 years

Environmental Class	Cooling Method	Operating Temperature Class (4.1)	Nonoperating Temperature Class (4.2)	Temperature Cycling Class (4.3)	Vibration Class (4.4)	Operating Shock (4.5)
ECC1	Conduction cooled (Reference VITA 48.2, VITA 46, IEEE 1101.2)	CC1 (0 to +55C)	C1 (-40 to +85C)	C1 (-40 to +85C)	V3 (0.1g2/Hz)	OS2 (40g)
ECC2		CC2 (-40 to +55C)	C2 (-40 to +85C)	C2 (-40 to +85C)		
ECC3		CC3 (-40 to +70C)	C3 (-50 to +100C)	C3 (-50 to +100C)		
ECC4		CC4 (-40 to +85C)	C4 (-55 to +105C)	C4 (-55 to +105C)		

Figure 1 | VITA 47 test profile for conduction-cooled modules.

of service life in harsh environments revealed that the electronics had to sustain an average of 23 cycles of -55 °C to +105 °C per year. The VITA 47 C4 test is much more stringent: It requires that electronics be able to sustain performance after 500 cycles of -55 °C to +105 °C. This means that, in this case, the VITA 47 ECC4 thermal cycling requirement represents approximately 21.7 years of service life in an average defense program in a harsh environment.

Going beyond VITA 47

While the VITA 47 standard is an important measure for evaluating product ruggedness and reliability, even the most demanding thermal cycling tests won't deliver the ultimate proof of reliability. The ideal approach is to combine VITA 47 testing with a comprehensive set of reliability analyses, tests, and procedures developed over the course of knowledge gained by designing, building, and testing COTS products.

Best practices dictate that companies should run VITA 47 tests on their standard production modules, verifying compliance with the VITA 47 shock, vibration, and operational temperature requirement as part of a standard qualification process. Such compliance testing involves pushing the equipment to the worst case of VITA 47 expectations.

VITA 47 has proven to be one of the key tools for discovering new ways to deliver the highest levels of ruggedness and proven, long-term reliability. Testing process and research efforts, for example, led to the discovery that lead-free soldered assemblies can be just as reliable, if not more so, than tin-lead soldered assemblies. In addition, it was found that lead-free solder may present opportunities for even better reliability in the future. With tin-lead technologies, smaller solder balls and lower standoff height for components tend to reduce thermal cycling reliability. With lead-free solder, smaller solder joints can actually improve reliability. Such knowledge garnered through testing and research enables the continued miniaturization of components while increasing functionality density, all without negatively affecting reliability.

Another example is seen in improvements for PWB interconnect reliability. All PWBs are not created equal: The more complex the PWB, the smaller the interconnects on the board. The smaller the interconnects, the easier they break. PWB designers and manufacturers must understand the physics behind how electronics behave in harsh conditions over time to ensure that interconnects won't open or crack.

By studying the physics of failure at the lowest levels, a COTS vendor can understand how to design, analyze, test, and manufacture PWBs with highly reliable interconnects, even on extremely complex high-density interconnect designs.

The results of reliability tests have revealed how to best implement microvias on a PWB. Detailed knowledge about the tradeoffs between the density of interconnects and the reliability of interconnects enables the COTS vendor to optimize microvia density and reliability on a board in a way that goes beyond what is typically provided by other vendors.

Moreover, combining VITA 47 testing with detailed debugging and deep-dive root cause analysis enables designers to identify and eliminate failures before they can cause consequences in the field. Catching and correcting design flaws that might otherwise not be exposed before deployment in an embedded system is an important benefit of extensive analysis and testing.

Look for advanced reliability testing

System integrators evaluating COTS products for use in defense and aerospace systems should take a hard look at each vendor's reliability design, analysis, and testing procedures. Only vendors that commit significant resources, expertise, and time to understanding the physics of failure and systematically incorporating the resulting knowledge into their products can offer consistent reliability. The VITA 47 standard gives system integrators a baseline by which to objectively compare the reliability of COTS products from various vendors. Products that have passed the highest levels of the VITA 47 standard provide the highest level of reliability in the most extreme environments. **MES**

Aaron Frank *is the Senior Product Manager, Intel SBC, for Curtiss-Wright. Frank is responsible for a wide range of COTS products using Intel processing and video graphics/GPU technologies in many industry-standard module formats (VME, VPX, etc). Previous to this role, Aaron held the product manager role for networking products. Aaron has a Bachelor of Science degree in electrical engineering from the University of Waterloo (Ontario, Canada). Readers may reach him at aaron.frank@curtisswright.com.*

Ivan Straznicky *is a principal mechanical engineer for Curtiss-Wright, where his responsibilities include advanced thermal and packaging technologies. Ivan has more than 20 years of experience in the military/aerospace industry in manufacturing and mechanical engineering and management. He received his bachelor's degree in mechanical engineering from McGill University (Montreal, Canada) and is a Certified Advanced Technology Manager. He can be contacted at ivan.straznicky@curtisswright.com.*

Curtiss-Wright Defense Solutions
www.curtisswrightds.com

Increasing data-transfer performance in VPX systems

By Thierry Wastiaux

The combination of digital simulation and high-performance calculation is radically transforming industry and research. It is now possible to develop products and services without spending precious time and dollars on replicating work already done. This is certainly the case in the military and aeronautics fields, particularly in the area of building size, weight, and power (SWaP)-constrained embedded computing architectures for use in electronic warfare and radar applications.

Developing a high-performance embedded computing (HPEC) capability requests a strong knowledge of the technologies involved, particularly concerning high-speed data transfers. It goes without saying that high-performance data connectivity is a must-have piece of getting computing resources like processors or field-programmable gate arrays (FPGAs) to work together.

In today's embedded systems for defense and aerospace applications, the VITA 65 OpenVPX standard appears to be the best protocol to supply the needed connectivity and to pack maximum processing power in size, weight, and power (SWaP)-constrained HPEC architectures.

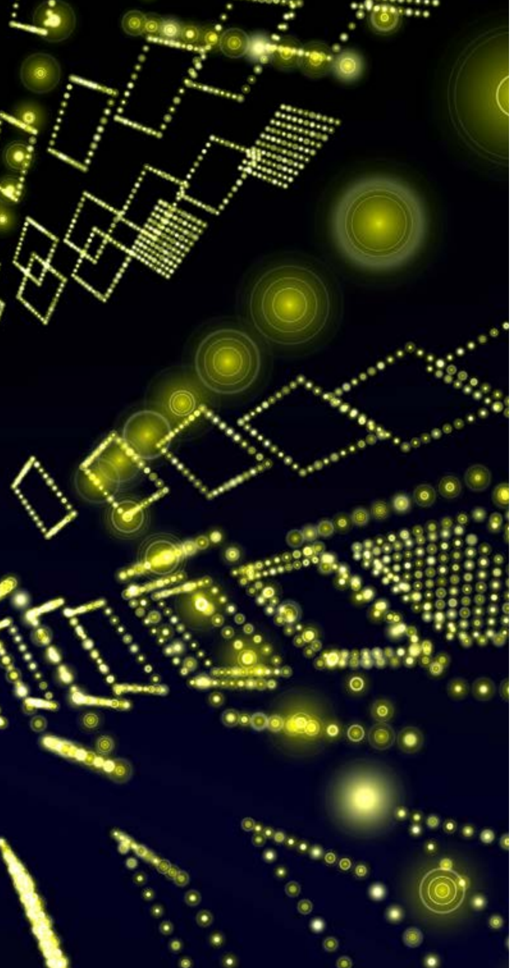
For data transfers, VPX defines the concept of the data plane separated from the control plane. To get the best from this VPX standard, some conditions have to be met: The most robust and high-throughput protocols must be chosen to operate the data plane. In addition, the processors must be relieved of the tasks of transferring data from memory to memory through the use of direct memory access engines.

State-of-the-art protocols for the data plane

The interconnect used in VPX HPEC systems must be robust, fast, flexible, and very power-efficient. The designer must consider the size of the targeted computing system in terms of the number of computing payloads. It is now well accepted by the market that PCI Express – in its Gen 2 or Gen 3 implementations – and 10GBASE-KR are currently the best protocols of choice to build HPEC VPX systems.

For PCIe, CRC [cyclic redundancy check] control at the link layer as well as retransmission hardware mechanisms can give users added robustness. Permanent effort sponsored by Intel has led to a steady speed and performance increase. The maximum theoretical bandwidth per lane is 7.88 Gbps in Gen3 thanks to the reduced overhead enabled by the 128B/130B encoding, which has particularly low-power consumption; this means a throughput of 31.5 Gbps on a PCIex4 link. The semiconductor industry has developed PCIe switch components. They usually include direct memory access engines for fast data transfers. These switches may be distributed on the different boards of a system or set in a centralized switch for both control plane and data plane.

In the PCIe architecture, each Intel processor is the root complex in its PCIe domain, enumerating all the end points. Enabling parallel processing in HPEC systems



means that designers must develop software to enable seamless communication between processors.

This approach has been successfully implemented in high-performing VPX 3U systems and appears well-suited for the design of small to medium VPX 6U systems where space is very limited. For example, in radar or electronic warfare (EW) applications, such an approach enables integration of the front-end processing FPGA modules that are directly connected to the different sensors. We can see that for small to medium-sized VPX 6U systems with just a few processor boards, PCIe is clearly the right choice. However, when more processing power is required with more computer boards, the PCIe approach becomes cumbersome due to the requirement of many point-to-point links between the boards.

The IEEE 802.3 standard for Ethernet has standardized 10GBASE-R and 40GBASE-R, with their physical layer (PHY) implementations for backplane communication based on 64B/66B code, 10GBASE-KR, and 40GBASE-KR4. The 64B/66B code of the physical coding

Figure 1 | The Cometh4510a (left) and 4590a (right) switches can be used for 6U and 3U architectures, respectively. Photos courtesy of Interface Concept.

sublayer (PCS) allows robust error detection, and its encoding ensures that sufficient transitions are present in the PHY bit stream to make clock recovery possible at the receiver. The physical medium dependent (PMD) sublayer of 10GBASE-KR enables transmission on one lane at 10.325 Gbps. The PMD sublayer of 40GBASE-KR4 enables transmission on four lanes at the same rate.

With 10GBASE-KR, systems designers are driven back to a central-switching approach, which becomes necessary when building large VPX HPEC systems with many processor and application boards.

The 6U VPX Cometh4510a, with its 48 10GBASE-KR data plane ports and 16 1000BASE-KX control plane ports (along with its additional optical front ports in addition), can be used as the backbone of a large central switched 6U VPX architecture. In large 3U VPX systems, designers can consider the Cometh4590a, which offers generous bandwidth and as many as 29 10GBASE-KR ports. (Figure 1.)

Even if these data plane protocols are sufficient for building the high-performance embedded systems that the market requires, the industry is looking for even faster protocols.

Increasing the throughput to 25 Gbps on a differential pair

Standards-making bodies are currently examining how to increase the high-density backplane serial throughput to 25 Gbps per differential pair. As an example, the IEEE 803.2 Ethernet Working Group has begun discussions on a 100 Gigabit backplane Ethernet standard with four lanes, each of them running at 25 Gbps.

A white paper on the subject from TE Connectivity ("A comparison of 25 Gbps NRZ & PAM-4 Modulation used in Legacy & Premium Backplane Channels 2012") sets out that backplane performance levels are essentially categorized by their insertion loss, return loss and insertion loss-to-crosstalk ratio) on a defined channel. This channel is specified using a backplane system with two daughterboards connected to a backplane, the length of the differential pairs and the connectors having been carefully specified.

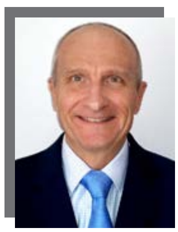
Per the white paper, two receiver architectures are to be considered: The first architecture is based on a conventional analog signal-processing approach. The second architecture uses a digital processing signal-based receiver. In both architectures, transmitter minimization, charge transfer efficiency transfer functions, sampling points, and the coefficients of the equalizer in the receiver to maximize the signal-to-noise ratio (SNR) are considered. In the simulations, the SNR margin is computed, being the difference between the SNR at the decision point of the receiver and the SNR required to achieve the target probability of symbol error.

The TE simulations found that one of the main sources of SNR margin degradation is due to channel reflections. The right design of connectors and the suppression of any stub on the PCB (backdrilling) thus become essential.

It also appears clearly that PAM-4 signaling offers better SNR margins than nonreturn-to-zero (NRZ) signaling. In addition, a lower symbol rate enables advanced equalization in DSP-based receiver architectures. But the simulations also reveal that PAM-4 signaling by itself is not sufficient for operation in legacy 10GBASE-KR-compliant backplanes: Megtron6 or improved FR4 as defined by the IEEE 802.3ap Backplane Ethernet Task Force and improved connectors must be used.

The development and the standardization of these new electrical technologies on the backplane will take some time. Meanwhile the VPX systems designers looking for fast data transfers beyond the 10 Gbps on a differential pair, can use optical links as standardized in the VITA 66.x norm for optical backplanes. As an example, the MIL-STD-compliant LightCONEX product from Reflex Photonics will be able to include a 12-lane transmit and a 12-lane receive at 10 Gbps linked directly into a 66.4 space, supporting extended temperatures. Such an approach avoids having optical cables running over the boards between the soldered transceivers and the VITA 66.X connectors with the inherent vibration issues possibly leading to wear points.

In the evolution of VPX towards higher throughputs on differential pairs, designers will have to build new high-quality backplane links using low-loss dielectrics, smooth copper, and low-reflection and low-crosstalk connectors. Board design will be even more demanding in term of impedance control with the systematic use of backdrilling. PAM-4 will probably be used as it improves the SNR margin. High levels of equalization will also be mandatory. In the meantime, PCIe and 10GBASE-KR protocols and optical VITA 66.x links remain good options for designers when more throughput is needed. **MES**



Thierry Wastiaux is senior vice president of sales at Interface Concept, a European manufacturer of electronic embedded systems for defense, aerospace, telecom, and industrial markets. He has 25 years of experience in the telecom and embedded systems market, having held positions in operations, business development, and executive management. Prior to joining Interface Concept, he was responsible for the operations of the Mobile Communication Group and the Wireless Transmission Business Unit at Alcatel-Lucent. He holds an M.Sc. from France's Ecole Polytechnique. Readers may contact Thierry at twastiaux@interfaceconcept.com.

Interface Concept
www.interfaceconcept.com

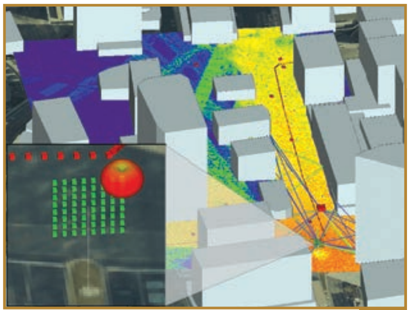
OpenSlice enables shared data between operating systems, platforms

Vortex OpenSplice from PrismTech, an ADLINK company, is a commercial and open source implementation of the Object Management Group's Data Distribution Service (OMG DDS) standard. Vortex OpenSplice enables data to be shared and integrated across a wide spectrum of operating systems and platforms. It provides a full implementation of the OMG DDS latest rev1.4 (DCPS profiles) and the OMG-DDSI/RTPS v2.2 interoperable wire-protocol standards. It is targeted for use with server-class (desktops, racks, etc.) platforms as well as more specialized real-time embedded environments and operating systems (e.g., a single-board computer running VxWorks).

The DDS API standard guarantees source code portability across different vendor implementations, while the DDSI standard ensures on the wire interoperability across DDS implementations from different vendors. The Vortex OpenSplice is data-centric, which enables applications to be designed around a data model, which PrismTech says adds safety to the model; the data-centric nature also promotes time and space decoupling, leading to systems that are easier to integrate, evolve, and reuse. The tool's real-time capabilities are able to deliver information to the right place at the right time.

PrismTech, an ADLINK Company | www.prismtech.com | www.mil-embedded.com/p374484

Wireless Insite software carries 5G and MIMO technology



Engineers at Remcom designed the company's Wireless Insite software with added 5G and multiple input multiple output (MIMO) capabilities. The tools are intended for use in radar-antenna design applications by industries including defense, biomedical, automotive, and energy generation.

Wireless InSite's MIMO capability enables the user to accurately predict path data between each transmitting and receiving element and reveals key channel characteristics in a timely manner. With optimizations that minimize runtime and memory constraints, Wireless InSite is able to simulate large arrays present in Massive MIMO systems. The tool's MIMO array builder contains the option to create 1-D, 2-D, and 3-D antenna arrays. Users have control over their model and can define unique antenna patterns and orientations for each element. All data is accessible, enabling results to be visualized within the context of the scene, as a 2-D plot, or exported to a file. Post-processing options include received power, complex channel matrix or H-matrix, complex impulse response, times of arrival, directions of arrival, and directions of departure for multipath.

Remcom | www.remcom.com | www.mil-embedded.com/p374486

Secure wireless communications for mobile devices

PacStar's Secure Wireless Command Post (Wi-Fi) is a small modular communications package that enables SIPR [secret internet protocol router] wireless and mobility access for smartphones, tablets, and laptops for classified networks in deployed, expeditionary, and tactical environments. The architecture – which follows the NSA Commercial Solutions for Classified (CSfC) Campus WLAN Capability Package v2.0 – enables end-user devices to use built-in commercial Wi-Fi on mobile devices to provide one layer of the required two-layer NSA encryption requirements. Combined with a single VPN client, end-user devices are able to transmit classified information over Wi-Fi.

The Secure Wireless Command Post (Wi-Fi) is based on the PacStar 400-Series small-form-factor platform. The PacStar 400-Series modular platform is designed to maximize capabilities with the smallest size, weight, and power (SWaP) footprint possible and is customizable and configurable to meet other NSA CSfC capability packages including MA CP (with LTE or other radio types) and MSC CP. It can also be configured to optimally serve a wide range of team sizes, and can also be customized with additional software and NFV solutions to ensure interoperability with existing customer infrastructure. PacStar Secure Wireless Command Post is managed by PacStar IQ-Core Crypto Manager, which the company says can simplify system CSfC setup, configuration, certificate authority requests, and VPN management.

Pacstar | www.pacstar.com | www.mil-embedded.com/p374485

Next-gen 'Internet of Battlefield Things' on the way

By Sally Cole, Senior Editor

In the not-too-distant future, humans and smart technology may merge to function as a cohesive network, providing warfighters with "extrasensory" perception in terms of battlespace situational awareness, prediction powers, and risk assessment.

What would the ability to network computers, sensors, cameras, data, weapons, soldiers, smart wearables, and media analytics together mean for the military? A $25 million initiative, funded by the Army Research Lab and led by researchers at the University of Illinois at Urbana-Champaign, is currently underway to find out and to lay the scientific foundations for what it calls the Internet of Battlefield Things (IoBT).

Today, there are already many examples of the military connecting "things," such as ships, planes, soldiers, and operating bases. But researchers believe the network can be greatly expanded to leverage advancements in unmanned systems and machine intelligence to achieve superior defense capabilities.

The idea of "interconnecting military 'things' at a global scale dates back at least to the 1990s, with concepts such as the Global Information Grid and Network Centric Warfare," says Tarek Abdelzaher, a professor of computer science at Illinois and the academic lead of the Army Research Lab's Alliance for IoBT Research on Evolving Intelligent Goal-driven Networks (IoBT REIGN). "What's new is that we're no longer talking about merely interconnecting these assets. The IoBT is more about building intelligent battlefield services that benefit from this connectivity and keep people out of harm's way."

One goal is "to execute missions with fewer soldiers and more machines, because the cost of life cannot be compared to the cost of hardware," he says. "This leads to fundamental research questions in machine intelligence and autonomy."

In the future, you should expect every battlefield "thing" within the IoBT realm to have a little bit of a brain or some smarts, not just a radio. As you might imagine, this ushers in "new research questions about understanding and managing the aggregate behavior of heterogeneous intelligent things when their 'brains' start interacting," says Abdelzaher. Among the questions: "How can we make them collaborate to achieve mission goals? How do we do this without micromanaging them – because we simply won't have time to do so? How do we specify human-commander intent to them in ways they can understand so they can adapt to unexpected situations in ways that meet the spirit of the mission? These are the issues surrounding IoBTs, even more so than the interconnection fabric. Within 10 years, we want to solve these hard challenges to reduce the loss of life in military operations."

What are the biggest challenges ahead for the IoBT? Security and robustness are definitely right up there: "We're talking about withstanding attacks by determined, highly intelligent adversaries," Abdelzaher elaborates. "Tomorrow's adversaries will be technologically sophisticated, so this means warfare between two advanced technologies. Any distributed capabilities we build out of IoBT assets will need to know how to deal with disruptions and reconfigure themselves after failures. They will need real-time reflexes that allow them to adapt, react, and regroup – without human help. The system must continue to function safely and successfully even after some parts have been damaged, disconnected, captured, or compromised by the enemy."

Connecting the IoBT with artificial intelligence (AI) is one of the "key centerpieces of the problem," he says. "If we simply add a lot of new gadgets to the battlefield and connect them, it increases the cognitive load on the warfighter. Someone will need to configure all of those 'things' and troubleshoot them when some device fails or disconnects, which will be normal in an adverse environment such as a battlefield."

Ever connect a laptop to a projector or use video conferencing technology? As Abdelzaher points out, it's fairly rare to have these experiences go smoothly. "Someone always has a setup problem," he notes.

But failures on the battlefield are highly undesirable while you're being shot at, so "machines will need to figure it out, and AI is the core. The more 'things' you interconnect, the more intelligence you need," Abdelzaher adds.

The researchers' goal is to create a cyber network of "things" that are capable of adapting as a mission changes or evolves. This means that the system will need to be able to analyze its available resources and reassemble itself in response to changing requirements. Systems must also be "self-aware" and able to reason about their goals, state, vulnerabilities, and other characteristics to meet commanders' intent.

So what types of technologies are being considered for connecting AI, which involves a lot of compute power, with IoBT at the edge of the network? Is software-defined networking (SDN) among them? "I think SDN is a promising technology," Abdelzaher says. "We're doing basic research, so many technology solutions are on the table and we want to understand their strengths, weaknesses, and domains of applicability, where each can really shine."

AI's role once it's connected to the IoBT: The IoBT system will feature cognitive abilities and be able to fuse data from sensors and technology with data provided by humans. And the system will need to function in a continuous state of learning at multiple time scales, such as learning from previous actions while acting in the present and anticipating future moves. The goal is to have systems that can provide commanders with the most relevant information at any given moment.

"When people imagine autonomous interconnected machines, dark sci-fi movies often come to mind. But the prospect really has a lot of promise for humanity," Abdelzaher says. "One of my friends, a civilian, was once driving over a bridge during an air raid in a war zone when an enemy jet appeared. The jet circled the bridge a couple of times until my friend finished crossing, then detonated the bridge. The human pilot in that jet clearly made a determination to spare the civilian's life. Can we build smarter weapons that can adapt similarly to avoid loss of civilian life? In fact, can we use smarter techniques to attain the ultimate goal of zero collateral damage sometime in the future? With sufficient AI and networking of sensors and weapons, I think it's possible."

This effort to understand and exploit the unique capabilities of networked battlefield systems is an interdisciplinary problem that brings together researchers from cyber-physical computing, information theory, security, formal methods, machine learning, networking, control, and cognitive science.

IoT devices tend to be vulnerable to cyberattacks, but according to the IoBT REIGN researchers, their work for battlefield applications may to lead to wider advances in making future civilian IoT technologies more secure and robust when it comes to cyberattacks.

"While commercial IoT provides some of this capability, they aren't challenged in the same manner as on the battlefield," says Stephen Russell, the Army Research Lab's Battlefield Information Processing Branch chief and the government lead for the Alliance. "The 'B' in the IoBT is our key focus."

The Army Research Lab's Alliance for IoBT REIGN also includes collaborators from the Army Research Lab; Carnegie Mellon University; University of California, Berkeley; University of California, Los Angeles; University of Massachusetts; University of Southern California; and scientific research institute SRI International. The project's $25 million funding covers the first five years of a potential 10-year effort.

Editor's note: *IoT security is a huge concern, mainly because many sensors or devices come with default passwords and known vulnerabilities that can be easily found on the internet, as well as without a way to patch or push security updates to them. But a group of U.S. senators recently introduced a bill, The Internet of Things Cybersecurity Improvement Act of 2017, which aims to change this. It essentially sets a fairly low bar establishing basic security best practices so that IoT devices sold to the federal government – including the military – will be required to eliminate default passwords and known vulnerabilities, and also include a way to push security patches or updates to them.*

CHARITY

Boys & Girls Clubs of America STEM Centers of Innovation for Military Families

BOYS & GIRLS CLUBS OF AMERICA

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

This issue we are highlighting the nonprofit organization Boys & Girls Clubs of America (BGCA), which is opening four new STEM Centers of Innovation for military families.

The new centers – built in partnership with Raytheon Co. – are Boys & Girls Clubs of Tucson, Arizona, serving families of the Davis-Monthan Air Force Base; Boys & Girls Clubs of Hawaii, Ewa Beach, Hawaii, serving families of U.S. Army Garrison Hawaii, Joint Base Pearl Harbor-Hickam, Marine Corps Base Hawaii; Hill Air Force Base Youth Program, Utah; and Kirtland Air Force Base Youth Program, New Mexico.

In 2016, according to BGCA officials, thousands of students from military families engaged with interactive modules and hands-on STEM [science, technology, engineering, and mathematics] activities at the six already built STEM Centers of Innovation across the U.S. and one abroad. Each center is equipped with 3-D printers, runs robotics and other educational workshops, and supplies high-definition video production and videoconferencing equipment.

"Military families make tremendous sacrifices for our country, but those sacrifices should never include their children missing opportunities to explore the endless possibilities available to them," states Jim Clark, president and CEO of Boys & Girls Clubs of America. "We're proud to offer a safe, familiar space for military youth across the country and abroad, and with these four new STEM Centers of Innovation from Raytheon, we'll be able to continue to build even more confidence and curiosity among these amazing kids to forge passions in STEM that will positively impact their future."

For more information, please visit www.bcga.org.

E-CAST

Enabling Multifunctional Electronic Warfare Systems

Sponsored by Annapolis Micro Systems, National Instruments, NordiaSoft

Traditionally, the electronic warfare (EW) market has been populated with customized systems and stovepipe technology based on closed architectures. As adversarial threats become more sophisticated, the pressure has mounted on designers to create multifunctional EW systems that can adapt and respond effectively in real time, marrying functions such as signals intelligence (SIGINT), electronic intelligence (ELINT), and even radar functions in one box.

This e-cast of industry experts will discuss how modern RF and signal processing components are enabling multifunctional EW capability.

View archived e-cast: ecast.opensystemsmedia.com/754

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

WHITE PAPER

Mission-ready systems deliver on promise of COTS

Sponsored by Abaco Systems

The promise of COTS espoused by former defense secretary William Perry more than 20 years ago is becoming a reality at Abaco Systems. The Lightning platform is a revolutionary response to a problem that has thus far proven to be intractable by the defense industry: how to substantially reduce the lead times for custom systems, giving them an availability that is much closer to "off-the-shelf."

In this white paper, learn about the systems based on the Lightning architecture, which are modular, scalable, and upgradable for lower cost. The systems use Abaco's micromezzanine technology to make configuring an application's precise I/O requirement easier.

Read this white paper: http://www.embedded-computing.com/military-white-papers/mission-ready-systems-delivering-on-the-promise-of-cots-abaco

Read more white papers:
http://mil-embedded.com/white-papers