

DECEMBER 2014

Military & Aerospace Electronics®

ENABLING TECHNOLOGIES
FOR NATIONAL DEFENSE

Rugged data storage

Data demands grow need for reliable and secure solid-state storage. **PAGE 16**

Rugged enclosures

Modular backplanes and enclosures aim at performance and time-to-market. **PAGE 22**

militaryaerospace.com

New frontier of cyber warfare

Defending sensitive U.S. military computer systems from malicious hackers.

PAGE 8

PennWell®



CONFERENCE AND EXHIBITION

6 – 8 OCTOBER 2015

PTA • AMSTERDAM • THE NETHERLANDS

www.intelligent-aerospace-event.com

IMAGINATION INNOVATION INTEGRATION

CALL FOR PAPERS NOW OPEN

Submit an abstract for Intelligent Aerospace

Abstract submission deadline: 21 January 2015

Details on the conference content and how to submit an abstract are available by clicking the CONFERENCE Nav tab on www.intelligent-aerospace-event.com

Alternatively, please contact:

Courtney Howard

Conference Director

T +1 509 413 1522

E courtney@pennwell.com

Sophia Perry

Conference Manager

T +44 (0) 1992 656 641

E sophiap@pennwell.com

For Exhibiting and Sponsorship enquiries please contact:

Chris Cope

Exhibit and Sponsorship

Sales Manager

T +44 (0) 1992 656 665

M +44 (0) 7534 856 101

E chriscc@pennwell.com

The advisory board of Intelligent Aerospace, is now accepting abstracts for its 2015 conference.

This new and exciting event provides an in-depth, high tech focus on cutting edge integrated hardware and software technologies found in all aspects of air travel and transport and how they interconnect - from ground operations and infrastructure to airborne platforms and electronics through space and satellite based systems.

Why not share your skills and expertise with your industry peers by submitting a paper for the Intelligent Aerospace conference.

Topics include:

- Airport Infrastructure and Operations
- Air Traffic Control and Airspace Management
- Commercial Aviation – Manned and Unmanned Platforms, Avionics, Electronics
- Military Aviation – Manned and Unmanned Platforms, Avionics, Payloads
- Rotorcraft Technologies – Helicopter, Tiltrotor, Vertical Lift Platforms and Systems
- Unmanned Aircraft Systems (UAS) – Platforms, Avionics, Ground Control, and Payloads
- Satellite Communications (SatCom) – Radiation-Hardened Platforms, Systems, Components
- Satellite Payloads – Commercial and Military, Meteorological Imaging, Weather Prediction

2 TRENDS

4 NEWS

4 IN BRIEF

8 SPECIAL REPORT

Cyber warfare ushers in fifth dimension of human conflict

The challenges of defending sensitive U.S. military computer systems and networks from malicious hackers, as well as devices offensive cyber strategies, are aims of newly created military cyber commands.

COVER STORY

16 TECHNOLOGY FOCUS

Data on demand

Aerospace and defense data demands grow the need for reliable, rugged, and secure solid-state information storage.

22 PRODUCT INTELLIGENCE

The challenge of efficiency in embedded power electronics.

24 UNMANNED VEHICLES

26 ELECTRO-OPTICS WATCH

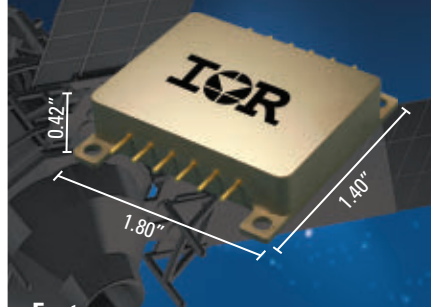
28 PRODUCT APPLICATIONS

31 NEW PRODUCTS

36 THE LAST WORD

Space DC-DC Converters with Two Regulated Outputs

D Series Hybrid DC-DC Converters



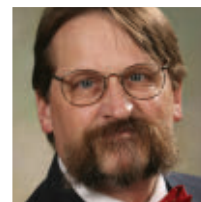
Features:

- Two outputs in one compact package with up to 5W per output
- Independently regulated outputs with excellent cross regulation
- Two low positive output voltages for digital loads or \pm outputs for analog circuitry
- Adaptable to all major satellite power buses
- Compliant with industry's standard de-rating requirements and NASA EEE-INST-002
- Small package, 55 grams maximum

For more information call 1.800.981.8699
or visit www.irf.com

International
IOR Rectifier
THE POWER MANAGEMENT LEADER

MILITARY & AEROSPACE ELECTRONICS ©2014 (ISSN-1046-9079) is published monthly by PennWell Corp., 1421 S. Sheridan, Tulsa, OK 74112. Periodicals postage paid at Tulsa, OK 74101 and additional mailing offices. Editorial offices are located at 98 Spit Brook Road, Nashua, NH 03062-5737. Subscription Prices: Free to qualified subscribers in North America. Other subscribers in U.S.A.: \$175.00 one year; \$309.00 two years; \$440.00 three years. Other subscribers in Canada: \$270.00 one year; \$465.00 two years; \$600.00 three years. All other international: \$325.00 one year; \$620.00 two years; \$810.00 three years. Digital edition \$70.00 yr. Call (847) 763-9540 for subscription information. We make portions of our subscriber list available to carefully screened companies that offer products and services that may be important for your work. If you do not want to receive those offers and/or information, please let us know by contacting us at List Services, Military & Aerospace Electronics, 98 Spit Brook Road, Nashua, NH 03062. POSTMASTER: Send change of address form to MILITARY & AEROSPACE ELECTRONICS Subscription Services, PO Box 3425, Northbrook, IL 60065. All rights reserved. No material may be reprinted without permission from the publisher. Back issues of Military & Aerospace electronics may be purchased at a cost of \$16.00 each in the U.S., \$22.00 Canada, and \$27.00 elsewhere. RETURN UNDELIVERABLE CANADIAN ADDRESSES TO: P.O. Box 122, Niagara Falls, ON L2E 6S4. Printed in the USA / GST NO. 126813153 / Publications Mail Agreement No. 875376



A once-proud class of U.S. Navy surface warships is quickly fading away

Throughout the Cold War, U.S. Navy frigates were essential pieces in the Navy's role of first line of defense. These relatively small, fast, and maneuverable surface warships were designed for the vital role of screening aircraft carriers from aircraft and missile attack, as well as protecting Marine Corps amphibious invasion forces and cargo ships from enemy submarines.

Next year, however, the American Navy is expected to be without its frigates for the first time since World War II, as the last of the Oliver Hazard Perry-class frigates (FFG 7) are decommissioned and stricken from the Navy's roster of active warships.

The Perry-class frigate is an icon of the Cold War. Its sleek silhouette was part of the outer screen of defenses for U.S. aircraft carriers and—for a brief time during the 1980s—for battleship surface-action groups when the nation's Iowa-class battleships briefly were put back into service for shore bombardment.

The Perry-class frigates performed the role of anti-air warfare and anti-submarine warfare to help protect sea lanes for commerce, as well as to screen the flanks of the carriers and the big-deck amphibious assault ships.

Notable surface actions of the Perry-class frigates included the near-sinking of the USS Stark (FFG 31) in 1987 after being struck by two Iraqi Exocet sea-skimming missiles. One year later the USS Samuel B. Roberts (FFG 58) hit an Iranian mine and nearly sank. Both vessels later were repaired and put back in service.



Even Hollywood movies added to the fame of the Perry-class frigates. The 1990 movie *The Hunt for Red October*, starring Sean Connery and Alec Baldwin, featured a cameo role for the USS Reuben James (FFG 57), when the ship launched a gun attack on the fictional Soviet missile submarine Red October.

In all, 51 Perry-class frigates were built and commissioned into the Navy surface fleet between 1977 and 1989. The first ship of the class, the USS Oliver Hazard Perry (FFG 7) was commissioned in 1977 and taken out

of service in 1977. The vessel was scrapped in 2006.

A changing world started putting the Perry-class frigates out of a job with the end of the Cold War. A fleet designed for blue-water operations started fading away with the Cold War, and ships designed specifically for near-shore operations along coastlines and near harbors increased in importance. Taking the places of the Perry-class frigates in the Navy's fleet are to be the littoral combat ships.

Today only 10 of the frigates remain in commission. The last ship of the class, the USS Ingraham (FFG 61) is scheduled to be decommissioned within the next two months. The last Perry-class frigate to serve in the fleet, the USS Kauffman (FFG 59) is scheduled for decommissioning in September 2015.

Although intended to replace the Perry-class frigates, the littoral combat ships will be built in nowhere near the same number as were the frigates. It's yet another symptom of the dwindling size of the U.S. Navy combat fleet.

There's less than one year left in the Navy's legacy of the Perry-class frigate. These vessels will be missed when they fade into history next year. ↙

Module and System-Level Solutions from X-ES

Intel® and Freescale™ Single Board Computers



XPedite7570
4th Gen Intel® Core™ i7-based 3U VPX
SBC with XMC/PMC



XCalibur1840
Freescale QorIQ T4240-based 6U VPX
SBC with dual XMC/PMC

High-Performance FPGA and I/O Modules



XPedite2400
Xilinx Virtex-7 FPGA-based XMC
with high-throughput DAC

Secure Ethernet Switches and IP Routers



XPedite5205
Secure Gigabit Ethernet router XMC
utilizing Cisco™ IOS®



XChange3018
3U VPX 10 Gigabit Ethernet managed
switch and router

High-Capacity Power Supplies



XPm2220
3U VPX 300W power supply with EMI
filtering for MIL-STD-704 & 1275

Rugged, SWaP-Optimized, COTS-Based Systems



XPand4200
Sub-1/2 ATR, 6x 3U VPX slot system
with removable SSDs



XPand6200
SFF 2x 3U VPX system with removable
SSD and integrated power supply



XPand6000
SFF Intel® Core™ i7 or Freescale
QorIQ-based system with XMC/PMC



Extreme Engineering Solutions
608.833.1155 www.xes-inc.com



Designed, manufactured, and supported in the USA

Nine years later, Marines have production of G/ATOR radar in sight

BY JOHN KELLER

QUANTICO, Va.—U.S. Marine Corps leaders are ordering prototypes of a long-delayed and expensive radar system designed to protect Marines on attack beaches from rockets, ar-



The long-delayed Marine Corps Ground/Air Task-Oriented Radar (G/ATOR) systems finally may be ready for production.

tillery, mortars, cruise missiles, unmanned aerial vehicles (UAVs), and other low observables.

Officials of the Marine Corps Systems Command at Quantico Marine Base, Va., announced a \$207.3 million contract modification to the Northrop Grumman Corp. Electronic Systems segment in Linthicum Heights, Md., for four prototype Ground/Air Task-Oriented Radar (G/ATOR) systems as a step toward full system production.

The contract modification, in addition to the four G/ATOR low-rate initial production systems, includes operating spares, contractor engineering services and support, devel-

opmental and operational test support, and transition to production, Marine Corps officials say.

G/ATOR is an expeditionary, three-dimensional, short-to-medium-range multi-role radar system designed to detect low-observable targets with low radar cross sections such as rockets, artillery, mortars, cruise missiles, and UAVs.

Marine Corps leaders are developing and fielding G/ATOR in three blocks for use by the Marine Air Ground Task Force across the range of military operations, officials say.

G/ATOR development began more than nine years ago with a \$7.9 million contract to Northrop Grumman Electronic Systems. The three-increment G/ATOR development involved short-range air surveillance, counter-battery fire and target acquisition, and sensor networking.

Northrop Grumman built G/ATOR for short-range air defense (SHO-RAD) and tactical air operations Center (TAOC) air surveillance missions, including IFF. The increment I design was to provide for growth to all following increments without equipment re-design and provide an open architecture to enable upgrades with following increments.

The second increment was to develop and produce systems based on the increment I baseline for

CONTINUED ON PAGE 6 →

IN BRIEF

Worldwide software-defined radio demand to reach \$27.3 billion by 2020

Worldwide demand for software-defined radio (SDR) systems and components will be worth nearly \$27.3 billion by 2020, increasing at a rate of 12.5 percent, predict analysts at market researcher MarketsandMarkets in Dallas. Americas and Europe represent the largest SDR market during the forecast period, while Asia-Pacific is the fastest growing region, with Japan leading the way, analysts say.

BAE Systems Australia to upgrade Nulka shipboard EW missile defense

Electronic warfare experts at BAE Systems Australia in Abbotsford, Australia will maintain, test, and upgrade a U.S. and Australian naval electronic warfare (EW) system designed to protect fast, maneuverable surface warships from radar-guided anti-ship missiles. Officials of the U.S. Naval Surface Warfare Center (NSWC) Crane Division in Crane, Ind., announced a potential \$9.2 million order to BAE Systems Australia for the support and advancement of the MK-53 Nulka electronic decoy cartridges and launchers. ←

Smart munitions to track and kill sources of RF jamming

BY JOHN KELLER

EGLIN AIR FORCE BASE, Fla.—The U.S. Air Force is developing special versions of two smart munitions that track and attack sources of electronic warfare (EW) jamming directed to throw the weapons off from their intended targets.



Researchers are developing a new warhead for the Joint Direct Attack Munition (JDAM), shown above, that homes-in on RF jammers.

Officials of the Air Force Research Laboratory at Eglin Air Force Base, Fla., have announced a \$9.8 million contract to Scientific Applications & Research Associates Inc. (SARA) in Cypress, Calif., for a Home-on-Jam demonstration of smart weapons already in the Air Force inventory.

The weapons involved in the demonstration are the GPU-31 Joint Direct Attack Munition (JDAM) and the GBU-39 Small-Diameter Bomb (SDB). SARA engineers will integrate the company's Home-on-Jam seeker into the JDAM and SDB-I smart munitions.

The goal is to support government-conducted flight tests to demonstrate the precision accuracy guidance capability against radio frequency threat targets in realistic conditions.

The JDAM and SDB smart munitions use radio waves to guide the

weapons to their targets, which an enemy can jam to prevent the munitions from hitting their intended targets. JDAM uses the Global Positioning System (GPS) satellite-nav-

igation system, while the SDB uses radar as well as electro-optical sensors for precision guidance.

In the presence of jamming,

CONTINUED ON PAGE 6 →

Tough Enough?



Hammer Tested for Your Demanding Applications.

Mission critical computers require a design team that can deliver. With over 30 years of experience and industry knowledge, Daisy's engineers design and produce a variety of complex, yet extremely rugged computing solutions for the military. Daisy's team can customize to any spec, including the Mil Standard 901D Grade A hammer test — and our solutions can withstand anything you throw at them.

**More Competitive. More Reliable.
More Affordable. Make It Daisy
& Make It Right.**

Visit d3inc.net/tough
to learn more.
717.932.9999

Make it  **Daisy**
DATA DISPLAYS

4556AA Series Military Shipboard PC
COTS Design, Mil standard 901D Grade A Shock tested, EMI Mil standard 461 and more. 19" LCD Panel PC with integrated touch screen. Used by the US Navy in the Smart Carrier program.

G/ATOR CONTINUED FROM PAGE 4

ground counter-battery and target acquisition. The third increment was to incorporate Mode 5/S IFF, electronic protection equipment and software, non-cooperative target recognition, sensor netting, an advanced radar environmental simulator, and a logistics integrated data environment (IDE).

The G/ATOR program was to showcase new component technologies, including the then-new VPX embedded computing fast switch-fabric interconnect. As part of the G/ATOR program's first increment, Northrop Grumman awarded a \$4.3 million contract in 2008 to Curtiss-Wright Corp. for VPX-based embedded computers for radar signal processing, to be delivered by 2010.

A fourth increment to G/ATOR was to incorporate an air traffic control (ATC) capability. That first con-

tract in September 2005 was to conclude in September 2009, and that's when problems cropped up.

By October 2009, the Pentagon reported a \$14 million cost overrun to G/ATOR, which was blamed on additional capability added during the previous four years, and to unexpected developments like the rising cost of gold, which made advanced electronic connectors for the military radar more expensive.

By mid-2012, nearly seven years after the program began, the Marine Corps awarded a contract to Northrop Grumman to begin the second increment of developing the Ground Weapons Locating Radar (GWLR) portion of G/ATOR. This 2012 GWLR work involved software installed on the first increment's hardware and operating system software, which Northrop Grumman engineers designed.

The GWLR portion uses active electronically scanned array (AESA) radar technology to enable the system to provide several different radar missions and adapt automatically to changing battlefield conditions. The GWLR is intended to increase detection range, accuracy, and deployability over other counter-battery radar systems.

Now, more than nine years after the initial contract, full-scale production of the G/ATOR system finally is in sight. Northrop Grumman will do the work in Linthicum Heights, Md.; East Syracuse, N.Y.; Stafford Springs, Conn.; San Diego; Big Lake, Minn.; Londonderry, N.H.; High Point, N.C.; Wallingford Center, Conn.; Camarillo, Calif.; and Woodbridge, Ill., and should be finished by October 2017. ←

FOR MORE INFORMATION visit www.northropgrumman.com.

SMART CONTINUED FROM PAGE 4

however, a Home-on-Jam seeker would follow the source of the RF jamming either to destroy the jammer or force an enemy to turn the jamming system off.

Home-on-Jam systems work in a similar way to the U.S. High-Speed Anti-Radiation Missile (HARM), which is designed to destroy enemy radar sites by homing in on the radar's RF emissions.

Home-on-Jam capability already is integrated on other weapons like the U.S. Advanced Medium-Range Air-to-Air Missile (AM-RAAM), which can home in directly on sources of radar jamming if the jamming is too powerful to allow the missiles to find and track their targets normally. Home-on-

Jam weapons use enemy jammers as beacons that announce the presence and location of the hostile transmitter.

The JDAM is a guidance kit that converts unguided dumb bombs into all-weather smart munitions with an inertial guidance system coupled to a GPS receiver. JDAM-equipped bombs have explosive payloads ranging from 500 to 2,000 pounds.

The SDB is a 250-pound precision-guided glide bomb that adds a tri-mode radar, infrared, and semi active laser seeker to the munition's original inertial and GPS guidance that works similarly to the JDAM. The SDB is intended to enable U.S. combat aircraft carry a higher number of bombs.

SARA engineers previously have

worked with the Air Force Research Lab to develop the Geolocation on GPS Jammers (GOGJ) system to locate GPS jammers with a low-cost solution. SARA's GOGJ system detects and precisely 3D geolocates several GPS jammers without prior knowledge of the threat and reports their locations to users on a map display.

The GOGJ seeker technology has been rendered into a flight-tested prototype for a home-on-GPS jammer mission. On this contract, SARA will do the work at White Sands Missile Range, N.M., and should be finished by October 2016. ←

FOR MORE INFORMATION visit **SARA** online at www.sara.com, or the **Air Force Research Lab** at www.wpafb.af.mil/AFRL.

Quarterly e-newsletter focuses on electronic warfare

BY JOHN KELLER

Electronic warfare is one of today's most pressing priorities of the U.S. Department of Defense (DOD). Properly done, electronic warfare—or just EW for short—can ensure that crucial U.S. and allied communications go through, and can deny this capability to hostile forces.

Still, EW technologies are evolving quickly, and represent important components of what is coming to be known as spectrum warfare—a combination of EW, optical warfare, and cyber warfare.

EW is a classic force-multiplier and is one of the few technology areas today in which the DOD budget is growing. EW capabilities are necessary on land, at sea, and in the air, and the military services have several major procurements in progress to bolster U.S. and allied capabilities.

It is for these reasons that Military & Aerospace Electronics is launching a quarterly Electronic Warfare Report e-newsletter for qualified subscribers. The e-newsletter publishes in January, April, August, and October.

The Electronic Warfare quarterly is a digest of the most important contracts, procurement opportunities, business developments, design-in case studies, budget prospects, news, and opinion related to military electronic warfare.

To subscribe to the quarterly Electronic Warfare report e-newsletter from Military



& Aerospace Electronics, go online to www.militaryaerospace.com/

newsletter and click on the fifth Yes box down just below the Electronic Warfare e-newsletter description. ←



AC does it

You need it right.
You want **Dawn**.

Dawn's Universal AC Input Vita 62 3U Power Supply

Dawn PSC-6236 universal **AC input VITA 62** compliant 3U power supply for air or conduction cooled OpenVPX systems. True 6 channel supply with up to 400 watts output. Mission critical wide temperature range at high power. Input 85 VAC to 264 VAC, 47 Hz to 400 Hz.

Can be special ordered to support high current single channel applications. **Embedded RuSH™** technology actively monitors voltage, current and temperature, and provides protective control.

DAWN
Dawn VME Products®

(510) 657-4444
dawnvme.com/vpx

Cyber warfare ushers in 5th dimension of human conflict

The challenges of defending sensitive U.S. military computer systems and networks from malicious hackers, as well as devices offensive cyber strategies, are aims of newly created military cyber commands.

BY J.R. Wilson

Throughout the history of warfare, new technologies have changed a given era's balance of power completely, often bringing down states and replacing them with those most adept at using the superior capability. For the first 12,000 years of recorded history, those advances were occasionally in force structure (i.e., Roman legions) or tactics, but predominantly in hardware (the English longbow, gun powder, aircraft, atomic weapons, satellites, unmanned aerial vehicles, etc.).

But the 21st Century saw the rise of a new threat, a "Fifth Domain of War" in addition to land, sea, air and space—cyber space. While cyber security, even cyber warfare, had its roots in the first significant use of military computers in World War II, it grew in significance with each succeeding decade.

As the 21st century dawned, nearly every aspect of human activity had become irrevocably intertwined with cyber space, from the public global Internet and its newer military counterparts to GPS precision location, navigation, and timing to



The 24th Air Force in 2013 opened a new facility in San Antonio, Texas, for Air Force cyber warriors. Air Force photo.

financial transactions and personal communications. That also raised the bar on ensuring the security of digital and cyber space elements and an accompanying increase in the volume, intensity and sophistication of computer and network hacking, malware and, ultimately, cyber weapons.

So far as is known outside classified sources, the leading use of cyber weapons to date has included the Stuxnet virus (of suspected—but never confirmed—U.S./Israeli origin) used to take down Iran's nuclear research computers; Russian confirmed and suspected cyber attacks on Estonia, Ukraine, Georgia, Latvia and Estonia; and Chinese incursions into U.S. military, government, and civilian infrastructure networks.

In May 2013, a cyber intrusion was confirmed into one of America's most sensitive physical infrastructure databases—the U.S. Army Corps of Engineers National Inventory of Dams. The NID database contains vulnerability details on some 8100 major dams across U.S. waterways, knowledge that could enable an adversary to conduct a

cyber attack that could open or lock flood gates to inundate areas behind or below the dam.

More direct cyber attacks, considered “tests”, have been mounted against small components of the national electric power grid. As naturally occurring blackouts in Canada, the U.S. Northeast and elsewhere in recent years have demonstrated, taking down even one key part of that infrastructure could lead to a cascade effect, blacking out far larger parts of North America. The growing sophistication of cyber capabilities—among nations and non-nation states—also is making it increasingly difficult to trace the origin of such attacks.

At one stage in 2010, more than three dozen separate cyber security-related proposals were introduced in Congress. The first decade of the 21st Century saw an explosion in the creation of cyber security agencies, departments, and offices throughout the U.S. government throughout the world.

This movement also elevated information technology (IT) from the “nerd” department responsible for



New!

Interpoint® 25 Watt DC-DC Converter

MFK Series™

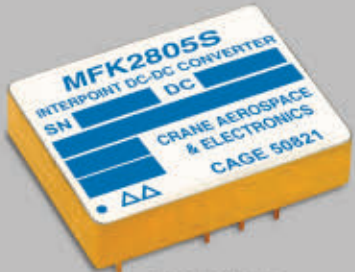



image size enhanced
actual size: 1.46 x 1.13 x 0.360 inches

- Wide input, 16 – 50 V
- Up to 42 W per cubic inch
- 11 outputs from 1.8 to 28 V
- Single and dual outputs
- High efficiency, up to 87%
- Magnetic feedback
- -55°C to +125°C operation



CRANE

AEROSPACE &
ELECTRONICS

Visit www.interpoint.com/mfk to download datasheet
To order call +1 425.882.3100 or email power@crane-eg.com

keeping an organization's phones and computers working to the heart of secure data and networking.

According to the 2013 Data Breach Investigations Report, 92 percent of cyber security breaches are of external origin: "Motive correlates very highly with country of origin. The majority of financially motivated incidents involved actors in either the U.S. or Eastern European countries (e.g., Romania, Bulgaria and the Russian Federation), while 96 percent of espionage cases were attributed to threat actors in China and the remaining 4 percent were unknown. This may mean that other threat groups perform their activities with greater stealth and subterfuge. But it also could mean that China is, in fact, the most active source of national and industrial espionage in the world today."

For the U.S. military, creation of the U.S. Cyber Command (CYBERCOM) in May 2010 as a sub-unified command subordinate to U.S. Strategic Command has been likened to the elevation of the Army Air Corps to a separate military service as the U.S. Air Force—the "Third Domain of War"—and within it, in 1982, creation of the Air Force Space Command (AFSPC) — the "Fourth Domain of War"—also as a component of STRATCOM. AFSPC also became the lead Major Command for Air Force cyber space operations in 2009, thus placing major components of three domains of war under the Air Force.

As the focus on cyber warfare and security grows, so does the need to ensure it is not confused with nor too tightly bound to older, established modes, such as Electronic Warfare.

"One area we are focusing on is moving beyond traditional IT, which is another skill set. That's an area we haven't considered as much in the past, so we are now reviewing that—how we do it now, how we'll do it in the future," says Troy Johnson, director of capability integration (N2/N6FX) for the Office of the Chief of Naval Operations (OPNAV) and Task Group Navy Cyber Security lead. "We're working it from both ends.

"The Task Force [Cyber Awakening] is cyber security on the inside, while the EW [electronic warfare] side is broken down into electronic attack, support and detects, so on the protection side we're working on hardening entry points through the spectrum, through electronic protect on the outside as well as inside the system, between the network components," Johnson says. "The computer and EW groups have grown up separately, but now are growing together, merging together."

U.S. Cyber Command

CYBERCOM's mission is to operate and defend sensitive U.S. Department of Defense (DOD) computer networks, conduct defensive and offensive cyber warfare operations, and establish cyber superiority—or the ability for the U.S. and its allies to operate freely in cyber space while denying cyber space to adversaries.

Similar to the structure of the joint Special Operations Command, CYBERCOM comprises specially created service components such as the Navy Fleet Cyber Command, Air Forces Cyber/24th Air Force, and Army Cyber Command. Their goal is to "make cyber space a suitable



Electronic warfare officers monitor a simulated test in the Central Control Facility at Eglin Air Force Base, Fla. Air Force photo.

place for military command and control," with a security focus on military operations.

CYBERCOM has three core missions: cyber support to U.S. and allied military commanders; defending DOD information networks; and defending the nation's critical infrastructure and key resources from enemy cyber attack.

"When I look at U.S. Cyber Command specifically, the Department of Defense is in the midst of a three-year journey that's going to create a cyber workforce of approximately over 6,000 individuals," CYBERCOM's commander, Adm. Michael Rogers, said in his keynote address to the 2014 International Cyber Symposium in Baltimore.

U.S. Air Force

The Air Force has created several cyber-related organizations, some tracing their origins back more than 60 years. For example, the 688th Cyberspace Wing stood up in 1953 as the Air Force Special



Communications Center, producing and disseminating intelligence data for the Air Force Security Service Agency.

That expanded to include EW in the 1960s, leading in 1975 to its designation as Air Force's first EW center. With the rise of what was known as Information Warfare in the early 1990s, the organization became the Air Force Information Warfare Center and, ultimately, the 688th Information Operations Wing, assigned to the 24th Air Force at Joint Base San Antonio in San Antonio, Texas.

Maj. Gen. James Kevin McLaughlin, commander of the 24th Air Force and Air Forces Cyber, has said the Air Force will add some 1,500 cyber positions during the next two years, even as the service undergoes an overall downsizing. They will focus on the Air Force's growing reliance on networks, data centers, mobile devices—even cloud computing—which already has led to malware infections, every 60 seconds, of more than 200 computers linked to numerous others that raise the reality

of widespread cyber-related issues.

In a mid-2013 special report on cyber security by the Center for Digital Government, McLaughlin said traditional borders and even combat lines between allied and adversary forces are irrelevant in cyber space.

"We are working to protect our

key cyber terrain through focused, deliberate operations," he said.

"Working together with our sister services and other partners is the only way to get the full picture of our adversaries' activities, thus the only way to posture ourselves ahead of those malicious efforts. We must



Great things do come in small packages.



Acromag ARCX Small Form Factor Embedded Computer

Made in the USA. AS9100 and ISO2001 quality.

- 4th Gen Intel® Core™ CPU
- Shock and vibration-tested (MIL-STD-810G)
- MIL-STD-38999 high-density connectors
- IP67 sealed against dirt and water
- Customized expansion options
- Single: 5.46"W x 3.29"H x 8.108"D
Double: 8.405"W x 3.29"H x 8.108"D

The ARCX rugged mission computer offers great flexibility to meet ever-changing requirements with unique expansion features.

PMC/XMC/Mini PCIe/mSATA slots for specialized I/O, memory, and FPGA modules.

MIL-DTL-38999 connector front panel has options for a custom I/O power filter.

The front panel can be also be modified for customer-specified secondary connectors.

Customize your own rugged, small form factor embedded computer. See all of your options at
www.acromag.com/ARCX



Visit us today to see our complete line of embedded computing solutions including: SFF systems, single board computers, FPGAs, I/O boards, carrier cards, and mass storage.

www.acromag.com • solutions@acromag.com • 877-295-7084

Acromag
THE LEADER IN INDUSTRIAL I/O



U.S. Army cyber warriors at Fort Sam Houston, Texas, look through information inside the Combined Air and Space Operations Center-Nellis during a recent Red Flag exercise. (Air Force photo.)

also adopt the mindset of protecting our most important assets and worry less about incursions that do not cause harm to systems or missions. We need to apply our resources efficiently and effectively to ensure we can accomplish our mission.”

McLaughlin has said all that has led to a shift of focus from network assurance to cyber elements key to mission assurance, with the 24th Air Force ultimately looking beyond core the Air Force networks to ways to ensure capabilities to joint commanders through a normalized and formalized cyber structure and the transition of the 67th Network Warfare Wing and the 688th Information Operations Wing to cyber space wings.

As Col. Alan Berry, AFCYBER chief of staff, said during his previous command of the Air Force 624th Operations Center—comparing cyber operations to the requirements of air operations to respond quickly

to inbound airborne threats—“In the Air Force, we’ve always operated at the ‘speed of need’. Everything in cyber is speed-of-need, every day.”

U.S. Navy

The Navy also has been refocusing and strengthening its cyberwar capabilities, as outlined in the U.S. Navy Information Dominance Roadmap—2013–2028 and further expanded by the August 2014 creation of Task Force Cyber Awakening (TFCA) within the Office of the Deputy Chief of Naval Operations for Information Dominance (N2/N6).

“This is not only an enterprise effort, but also critical warfighting,” Matthew H. Swartz, director—Communications & Networks Division (N2/N6F1) and TFCA lead, told a media roundtable on 31 October. “Cyber is not just a new warfighting effort for us, but also a critical enabler for our other warfighting domains and a new domain itself. In the last

decade, DOD—and specifically the Navy—has been forced to reassess our risk calculus for cyber, to understand from a risk perspective what we need to do to address this growing area. Because of that, we had to make sure we understood the risks of cyber as we move forward.

According to the National Intelligence Council’s Global Trends 2025: A Transformed World and Global Trends 2030: Alternative Worlds, “the future international system will be almost unrecognizable from previous decades owing to the rise of emerging powers, an increasingly globalized economy, an unprecedented transfer of relative wealth and economic power flowing to Asian states and the growing influence of several non-state actors. The U.S. will remain the single most powerful country in the late 2020s, but will be less dominant on the world stage and will see its relative strength—even in the military realm—decline.”

The Roadmap further outlined the problems facing the U.S. in cyber space: “The proliferation of advanced information technology could hinder U.S. efforts to maintain future access to the cyber space domain. The rapid pace of scientific breakthroughs in information technology will continue to accelerate. Joint Forces Command’s Joint Operating Environment postulates that such advances will change the very character of war. The emergence of space and cyber space as contested warfighting domains ... could impact or jeopardize the Navy’s success in high-threat operating environments.”

At the October media roundtable at the Pentagon, N2/N6 officials

outlined the year-long intent of Task Force Cyber Awakening, a cross-organizational effort to address those issues by extending the Navy's cyber security apparatus beyond traditional IT to combat systems, combat support and other information systems.

"The Navy must fight and win in the increasingly connected and contested cyber domain. TFCA will gain a holistic view of cyber security risk across the Navy and address the fragmented and uneven efforts across our platforms and systems," the CNO's office said.

Stood up in July 2014, TFCA is scheduled to conclude in August 2015, drawing on representation from across the entire Navy, including OPNAV and the CNO staff, significant fleet participation and the Marine Corps.

Lt. Cmdr. Hasan Abdul-Mutakallim, lead for Task Group Capabilities, noted the difficulties TFCA is seeking to identify and resolve: "We're trying to understand what kind of defenses we need in place to respond to ever-changing threats. The risk we have today may not be the risk we have tomorrow. And as risk changes in one area, we have to flex the profile we have in other areas to improve our cyber defenses as a whole. So whether the domain is CANES [Consolidated Afloat Networks and Enterprise Services] or NGEN [Next Generation Enterprise Network], what is the layered approach?"

U.S. Army

The Army Cyber Command/2nd Army was designated a new three-star operational-level Army force in October 2010, reporting directly to

the Department of the Army. The command comprised some 21,000 soldiers, DoA civilians and contractors around the globe—what ARCYBER describes as "an unprecedented unity of effort and synchronization of all Army forces operating within the cyber domain".

The Army has transformed existing cyber space forces (Network Enterprise Technology Command/9th Signal Command), portions of the 1st Information Operations Command and Intelligence and Security Command (INSCOM) into ARCYBER. Its personnel are responsible



With 16,535 unique models

we already have a proven DC-DC converter that meets your specs!

Contact our responsive support team at sales@mdipower.com or call 1 631 345 3100 to find exactly what you need...

MODULAR DEVICES, INC.
www.mdipower.com
 An ISO 9001:2008 registered company

for Global Information Grid Operations, Defensive cyber space Operations and, when directed, Offensive cyber space Operations. In addition, ARCYBER provides full spectrum cyber space operations and Intelligence support to CYBERCOM and in support of Army operations.

In addition to global cyber space operations, ARCYBER continues to develop the Global Network Enterprise Construct, to provide soldiers with a common set of applications and information resources, no matter where they are deployed. GNEC also supports the larger effort to transform the Army into a faster, more flexible organization.

"We're still building capability and are not yet where we should be; all commanders would like all cyber capabilities now," Lt. Gen. Edward C. Cardon, commander of ARCYBER, says. "Cyber is a team sport—everyone does it a little differently, but we all work together. The good news is there already are tools out there; they just need to be brought into use.

"I start off with defending the Army networks, then build cyber capability, support the COCOMs, support the reposturing of the force. What concerns me about cyber security is, if you have a really good network, with 100 people keeping it secure, and 97 do exactly what they are supposed to do, that would show up on a lot of charts as green. On my chart, it would show as black, because those three would be points of vulnerability."

Another problem Cardon identified is the failure of industry and the military, until recently, to build cyber security into their programs and devices.



The NexGen Cyber Innovation and Technology Center (NexGen) is for cyber research, and is the newest addition to Lockheed Martin's portfolio of research facilities.

"Going to the cloud and using hypervisors and gold images that give us clean computers and services, enabling us to better protect the data, will be a lot better than what we have now—separate networks secured in a variety of different ways. So overall, I think it will be a major improvement in cyber security," he says. "Right now, there is a clearly defined line between where DISA [Defense Information Systems Agency] stops and the Army starts. But in cloud computing, that line no longer exists.

"So how we manage the cloud will be a lot different from what we do today. No longer is it a question of a device, but what is around it, who manages it, how is its configuration managed. I'm a believer in big data cloud analytics, which I think will give us a lot of security, but I'm not a big advocate of clouds when you are in a remote place. We're on the edge of another huge explosion of technology and the way we do things today will be very different five years from now. Mobile devices

are driving this change."

A major problem, he adds, is not just ensuring the Army's top commanders are well-versed in cyber, but also expanding that knowledge to the larger Army.

"You have to protect your networks, determine how to use them and how to generate requirements for what we need to do down the road so we will be ready. The more competence, compliance and oversight we can put on this, the more useful cyber becomes," Cardon says. "It's really about what are the processes and procedures to do this. Up to this point, you see a lot of capabilities used at a very high level, but not so much at the tactical level. There probably are infantry men and women out there who can do this; you just need the right assessment tool to find them.

U.S. Coast Guard

As it assumed a greater responsibility for national security as part of the post-9/11 Department of Homeland Security, the Coast

Guard is developing and concentrating cyber resources to defend the nation's ports, terminals, ships, refineries and support systems—vital components of America's critical infrastructure, national security and economy.

"Cyber attacks on industrial control systems could kill or injure workers, damage equipment, expose the public and the environment to harmful pollutants and lead to extensive economic damage," according to the USCG's Office of Port and Facility Compliance Cyber Security website. "The loss of ship and cargo scheduling systems could substantially slow cargo operations in ports, leading to backups across the transportation system. A less overt cyber attack could facilitate the smuggling of people, weapons of mass destruction or other contraband into the country.

"In short, there are as many potential avenues for cyber damage in the maritime sector as there are cyber systems. While only some [of those] could credibly lead to a Transportation Security Incident, we must identify and prioritize those risks, take this threat seriously and work together to improve our defenses."

NATO and other allies

Article 5 of the NATO charter states that a military attack on one member would be considered an attack on all. At a NATO summit in September, the alliance extended that to include cyber attacks.

In addition, the NATO Coopera-

tive Cyber Defence Centre of Excellence, established in May 2008 in Tallinn, Estonia, is a NATO-accredited International Military Organization dealing with cyber security education, consultation, lessons learned and R&D. Although not part of NATO command nor force structure nor funded from the NATO budget, the Centre is directed and tasked via the Allied Command Transformation, with all products available to NATO nations unless restricted by the organization requesting that product.



Cyber Flag cyberspace force-on-force training fuses attack and defense across the full spectrum of military operations in a closed network environment

In June 2014, U.S. Army Maj. Gen. John Davis, Acting Deputy Assistant Secretary of Defense for Cyber Policy, says DOD has identified several allied nations where a "significant impact [or] existing threats" of active cyber attacks are higher than average. As a result, American and allied military officials are together to flesh out defensive measures against malware, overall network defense and various other TTPs to close "technological gaps" within those networks.

Davis says the primary focus of those efforts are U.S. allies in the Middle East and Asia-Pacific, which

are considered particularly vulnerable to cyber attacks from China, Russia and near-peer adversaries.

"There is growing understanding of the importance of cyber security, that any vulnerability is a threat. They say if you put a new computer on the network, it gets scanned within 5 seconds, so you really want to know your firewall is working. I think a lot of companies will look at cyber as an element of their products rather than an afterthought," says ARCYBER's Cardon.

"The speed of war, the speed of business and the speed of life have all dramatically accelerated. What used to take days now takes minutes or seconds ... The success of operations depends on security—and information security needs to be emphasized right alongside physical security," notes Air Forces Cyber's McLaughlin.

"Cyber and IT are now commanders' business, critical to the warfighter. It is a new domain in which

we have to fight and win with speed and agility, but the superiority we get in our other domains is contingent on our ability to provision and protect our cyber capabilities," Swartz concluded, noting the cyber threat is more mature than many of the organizations in place or standing up to deal with them.

"We have superiority in other warfighting domains, but some of that superiority is dependent on our ability to communicate information," Swartz added. "As that information flows, we need to make sure it and those connections are protected." ◀

Data on demand

Aerospace and defense data demands grow the need for reliable, rugged, and secure solid-state information storage.

BY Courtney E. Howard

The need for data storage is ubiquitous today—permeating both personal and professional lives—and will remain so into the foreseeable future. Data storage is particularly important in a majority of aerospace and defense applications, in which lives often can depend on ready and reliable information access.

Not just any kind of data storage will do for most aerospace and defense applications. Data solutions deployed in sensitive and classified missions, air and land vehicles, and extreme environments must meet a host of requirements. The prevalence of intelligence, surveillance, and reconnaissance (ISR) missions, among other data-intensive tasks, is driving greater demands for data storage.

Information extremes

Aerospace and defense systems designers want information storage solutions to meet requirements like high availability and reliability, encryption or other security features, compact size, high storage capacities, and the ability to withstand extreme temperatures and environments.

“Every program we bid on has a significant storage component,” says Ed Blackmond, director of software

services at embedded computing specialist Themis Computer in Fremont, Calif. “One example is infrastructure for tactical systems that must operate while in motion, as well as while standing. These systems are often configured in transit case racks and loaded onto trucks; they amount to small data centers that must operate in extremely rugged environments.

“Given the need to reduce space, weight, and power [SWaP], we are seeing tremendous interest in virtualized, hyper-converged environments where compute and storage resources share the same platforms,” Blackmond adds. “Rather than a dedicated storage server, these environments employ a virtual machine to aggregate storage from each system and provide shared access to this pool to other virtual machines implementing the application servers.

“As with any computing environment, storage requirements continually grow,” Blackmond says. “In these mobile data centers, reducing SWaP is of paramount importance—translating more and more into requirements for Flash, which also makes operation while moving possible.”

Every request Blackmond and

Astronics Ballard Technology designed the Rugged Toe Drive storage device for military use.


his colleagues receive includes virtualized, or private cloud, environments, Blackmond says. Customers often run large data-acquisition applications and feed data to “Big Data” processing using Hadoop and similar tools—all running in hyper-converged environments on a common set of hardware, he says.

“Along with the virtualization of compute [tasks], networking and storage are being virtualized,” Blackmond explains. “Customers increasingly want to simplify the systems they are deploying, using uniform hardware building blocks.” Hyper-converged building blocks are connected via a large network pipe with high bandwidth and low latency.

“Using emerging software-defined networking and software-defined storage capabilities,” Blackmond says, “customers can dynamically deploy new applications that can scale quickly by simply adding these hardware building blocks.” Because the hardware is uniform, they are much easier to manage when replacing or adding hardware, he says.



Overlapping applications



Military applications are surprisingly similar to those of a typical data center, Blackmond says. Reducing the weight of a system reduces the personnel required to load and unload equipment. Reducing system size enables more computing equipment to be loaded onto fewer trucks. Reducing the power requirements enables systems to run using fewer power resources. "All this translates into tremendous reductions in the total operating costs," he adds. "The military is able to do more with less."

Reduced SWaP through higher densities and hyper-convergence is the future of rugged data storage,

Blackmond predicts. "Sharing the resources for compute and data through virtualization allows significantly more to be done with significantly less. The savings are obvious in mobile tactical operations, but also apply to commercial applications."

"Ruggedization refers to more than kinetic issues. Thermal issues are also important," Blackmond says. "Powered by the open-source package Zabbix, [our Resource Manager] allows all the physical computing resource to be provisioned, monitored, and managed remotely" and includes the Open Stack Horizon dashboard for provisioning, monitoring, and management of virtual resources."

Growing needs, reduced sizes

Aerospace and defense professionals

are approaching Bill Schuh, vice president of sales at Astronics Ballard Technology in Everett, Wash., to meet ruggedized data storage needs related to mission systems, maintenance data, vehicle health monitoring, and crew reference data.

"Smaller size, less weight, and higher capacity are always in demand," Schuh says. "Our Rugged Toe Drive USB mass storage module is a portable storage device designed for the unique needs of the military market." It can be attached to a line-replaceable unit (LRU) via a MIL-SPEC 38999 connector and includes a captive cover to protect the connector when removed. A second cover provides access to a Micro-USB 3.0 port for connection to a host computer.

Data on the Rugged Toe Drive is

RUGGED DATA STORAGE



**Drive Magazine Based
High Performance
Multi-Protocol Fibre Channel,
SAS or iSCSI RAID System**

- **24 Solid State or Hard Disk Drives** in only 2U of panel height
- **Two Quickly Removable Storage Magazine**
 - each containing up to 12 HDDs or SSDs each
- **Fault Tolerant, Hot Swap Components**
 - no single point of failure
- **Sustained Read and Write Data Transfer Rates**
 - of over 5000 MB/sec and 3000 MB/sec respectively
- **MIL-STD-810G, MIL-STD-461E Certified**

**RPC 24
RUGGED
DEPLOYABLE**

PHOENIX
INTERNATIONAL



AS9100 Rev C/ISO 9001: 2008 Certified

www.phenxint.com 714-283-4800

Civil and defense data demands

Systems architects are introducing Ethernet into the design of new systems and even upgrades; they are looking for centralized storage, which is resulting in a big push for network attached storage (NAS), says Paul Davis, director of product management, Curtiss-Wright Defense Solutions in Dayton, Ohio.

Many aerospace and defense programs require that the storage device be removable, says Matt Young, product marketing manager at Curtiss-Wright Defense Solutions in Dayton, Ohio. "It needs to be removable, with high-insertion-cycle connectors, so they can take it back to a base station in the field to offload the data." The company's rugged, removable storage are typically located on a vehicle. On an aircraft, for example, they might be in the cockpit or in the back of the plane, assisting in data capture during the mission; after the mission, personnel want to remove that information storage device for post-mission data analysis.

Davis is seeing ever-increasing demand for securing data at rest. "We're seeing a lot of demand for encryption of the data at different levels, such as commercial encryption through FIPS 140-2 certification and NSA Type 1 at a higher level for top secret data in a deployed application."

"The increasing UAV market and number of vehicles being deployed are growing the need for encryption at various levels," Young clarifies. "With the

abundance of unmanned vehicles, we need to meet different encryption requirements. Unattended operation, where there's not an actual pilot in the plane, requires a whole different level of encryption. If no one is there physically, data needs to be much more secure. Whether on a manned or unmanned aircraft, the design approval authority (DAA) has to decide whether there's enough physical security. If it is not sufficient, they start to talk about encryption. If it's unattended, they are held at an even higher standard to protect the data; it depends, obviously, on the type of data."

SSD capacities

Many information storage requests are for solid-state disks, and capacities are continually increasing, Young says. "There are a lot more sensors out there gathering a lot more data at a lot higher speeds, producing much more data and requiring increased capacities."

High-definition (1080p) cameras are producing a lot of data, Davis adds. "Compression techniques reduce that amount, but they are streaming data constantly; there is this ever-increasing need for more and more storage."

Some aerospace and defense projects use Curtiss-Wright's CNS (compact network storage), a NAS box with a door; the company's FSM (flash storage module) removable storage plugs in behind the door. "We tune the CNS for the security level required for that

application," Davis says.

Curtiss-Wright personnel are working with Lockheed Martin engineers in Marietta, Ga., on the C-130J Super Hercules military transport aircraft program, for which the CNS and accompanying FSM were selected. The information storage system, used in conjunction with data processing on an Ethernet system in the back of the aircraft, is going through flight qualification testing now.

Rugged required

Engineers use information storage solutions from Curtiss-Wright Avionics & Electronics in Dublin, Ireland, for flight test applications and structural health and usage monitoring for crash recording.

"They all want rugged," says Stephen Willis, product marketing specialist, Curtiss-Wright Avionics & Electronics. "Crash recorders obviously have the most extreme ruggedness. Other recorder applications for flight test on commercial aircraft have to be rugged or else they won't survive the application."

"If you go even further, Curtiss-Wright data recorders are used in space applications," Willis says. "We've had [data recording] boxes go to and from the International Space Station, for example, and others being used in experimental tests coming back into orbit and the storage is the output of the mission essentially. The levels of ruggedization and seeing that data survives are critically important." ◀

encrypted at rest, so it remains secure during transport, Schuh says. Fast and secure erase functions can be initiated using a button on the device or remotely as part of a system-wide erase command.

The Toe Drive is well suited for mission-system data loading and mission data recording. It provides "a secure way to transfer critical mission data to mission and weapon systems," Schuh says. "Flight plans, targeting details, map data for 3D situational awareness systems, and other relevant mission data can be loaded to the drive, and the data remains secure during transport to the vehicle. When connected, data is loaded to the necessary systems. Autonomous vehicles, such as unmanned aerial vehicles (UAVs), can have a

higher dependency on loaded data."

Complete mission data, including avionics data and video, from a sortie can be recorded securely to the Toe Drive, Schuh says. On returning from the mission, the drive is easily removed for post-mission analysis and debrief. "With UAVs, data needed beyond the live stream can be recorded to conserve bandwidth. Mission data loading and recording can both be accomplished with a single drive using separate folders or drive partitions."

The Toe Drive provides a rugged medium for maintenance and health monitoring systems, recording performance data for fixed-wing aircraft, helicopter, and ground vehicle systems. The drive is resistant to high vibration and shock, as well as can be removed, switched out, or the

data transferred through an existing wireless link, Schuh says.

Detailed electronic maps, maintenance manuals, and other reference information also can be transferred aboard using the Toe Drive. "We see a trend toward recording more and more performance data, especially on the commercial side for health and usage monitoring systems (HUMS), given all the advantages that offers," Schuh observes.

Copious storage capacities

Virtually all aerospace and defense applications are driving greater demand for rugged information storage, says Brian Houston, vice president of engineering at Hitachi Data Systems Federal in Richmond, Va.

"In the defense space, where the



Empowering Microelectronic Solutions For Extreme Applications

- Ruggedized Motor Control Products
- Analog and Digital Controls Available
- CAN Bus Communication/Control Compatible
- 3 Phase Brushless DC Torque & Speed Controllers
- Controls & Bridges Driving Up To 1200V & 1000A
- MIL-PRF-38534 Class H and K Certified

20 YEARS OF MOTOR CONTROL AND DRIVE HERITAGE

MSK
M.S. KENNEDY CORP.
an Anaren Company

4707 Dey Road, Liverpool, New York 13088
Ph.: 315.701.6751 • Fax: 315.701.6752
www.mskennedy.com

Storage for surveillance

Information storage products from Phoenix International Systems in Orange, Calif., are used for “everything under the intelligence, surveillance, and reconnaissance (ISR) umbrella,” says Amos Deacon III, the company’s president. “Our products are typically used in data recording applications—a lot of that is surveillance. We’re seeing that on the [U.S. Air Force] Joint STARS program, for which we are still shipping RAID systems using solid-state disks replacing rotating media hard drives for the most recent upgrades to large, four-engine E-8C jet aircraft.”

The Joint STARS program has been around since Desert Storm; the ground surveillance platform uses synthetic aperture radar and software to uniquely and individually identify vehicles, including helicopters and potentially cruise missiles, Deacon explains. “It enables personnel to identify and track hundreds of vehicles of interest at one time. The [Northrop Grumman E-8C] aircraft is going through a retrofit technology refit where they are changing many systems on the aircraft, all the workstations, to more current technology—and we’re involved.”

With the advent of persistent surveillance, militaries are “putting up an aircraft that rather than being on station for hours is on station for days, commonly referred to as wide-area persistent surveillance,” Deacon says. “Along with radar data, they are using video at resolutions that aren’t

measured in megapixels, but gigapixels—and multiple streams of gigapixel video. That requires a lot of data storage.”

Phoenix personnel are working on a program with Lockheed Martin whereby multiple gigapixel streams need to be recorded—and stored. In this particular application, each of three streams of video data is collecting roughly 20 terabytes of information over an eight-hour mission. “Once the aircraft lands, you need to get that data off right away,” Deacon says. “In that application, they are using our magazine-based RAID product; it accommodates 12 disks in each magazine, which can be removed in seconds to a ground station for data mining, or whatever they need to do with that data.

“In that case, we’ve seen a very large increase in the capacity required, and that makes life difficult on an aircraft because the more storage capacity you have, of course, the more weight you have to put on the aircraft and the more space it is going to require,” Deacon adds. “We have seen requirements for much denser packaging of storage devices. It also is in an area of high altitude and high temperature, not to mention the shock and vibration. Hard disk drives don’t like to operate in that type of environment, so it is one of the things that are driving the use of solid-state disks. That’s where we see data storage requirements going, to solid-state disk, especially for airborne applications. ◀

U.S. Department of Defense (DOD) already manages stored data in volumes approaching the exabyte level, there is no question that high-resolution imagery, video, and other disparate forms of data collected from sensors on UAVs, satellites, and manned vehicles present the biggest storage challenge the DOD has ever faced,” Houston explains. “While the systems employed in theatre today and tomorrow will give the U.S. military an unprecedented intelligence advantage, the amount of imagery and data that needs to be stored and analyzed demonstrates an enormous challenge from both a budgetary and technical standpoint.

“In today’s cost-conscious environment, even the DOD isn’t impervious to budgetary shortfalls. In addition, from a technical standpoint, the military needs storage solutions that can not only store these massive data collects and empower intelligent analytics, but also be operated in the field without the risk of losing valuable data to the elements,” Houston says.

“Magnetic tapes are susceptible to outside influences like weather, moisture, and heat, which also contribute to the loss of data,” Houston continues. “Optical solutions, on the other hand, have enhanced durability to survive the extreme conditions associated with a rugged battlefield deployment or a natural disaster. Hitachi Digital Preservation Platform (HDPP) is impervious to dust, sand, heat, salt water, moisture, and even electromagnetic events.”

Digital data deluge

The explosion of digital information being created today and the proliferation of media formats pose a long-term storage challenge for the DOD

and all federal agencies, Houston says. Agencies are seeking a trusted, reliable data repository—one that preserves the integrity of your data and ensures accessibility for continued retrieval and use for an indefinite period of time, he says.

Optical storage will gain significant traction over the next several years, Houston predicts... but with a caveat: “There is no one-size-fits-all approach when it comes to storage environments. We closely partner with the DOD to ensure that the appropriate storage architectures are implemented, deployed, and scaled to meet the mission need of the agency, regardless of whatever legacy infrastructures are currently in place. Whether that’s virtualized storage platforms, rapid access flash drives, dynamically tiered solid-state disc arrays, or long-term optical preservation, the key is to ensure that the appropriate stakeholders are able to access the data whenever they need it and wherever they are located. This truly makes data actionable and able to assist meeting agency missions.”

Beyond being able to store massive amounts of new information generated daily, agencies need to make sense of it all, Houston says. “By definition, making sense of the data lies at the core of big data. From our standpoint, it’s absolutely critical that agencies deploy intelligent, nimble storage architectures to help leverage the power of big data.

“Flying a drone and collecting information is merely the first step in the data collection process,” Houston says. “In addition to sheer capacity, another critical consideration now and in the future has to do with performance. The images need to

be corrected, calibrated, processed, stored, and evaluated efficiently and effectively. The military must be able to store and manipulate this data efficiently and cost-effectively for the long term, so information collected on today’s battlefield will be readily available to the warfighters of the future. This is particularly important for ISR and other applications where intelligence is derived from the data itself; thus, the value of a



Each removable magazine in the Phoenix RPC24 RAID subsystem can fit 12 solid-state disks.

storage solution increases if it enables processing and analysis to be done more quickly. Doing so reduces the time from collection to action and improves the chances of mission success.”

Data preservation & optical options

The Hitachi Digital Preservation Platform (HDPP) is Hitachi Federal’s next-generation, long-term data preservation solution that leverages optical storage technology and allows federal agencies to preserve and archive mission-critical data indefinitely.

“HDPP meets the demands of the 21st century battlefield by enabling all branches of the armed forces to archive data in a manner that allows it to be accessed and searched, while scaling to meet the growing

storage needs of the military’s mission,” Houston says. As part of Hitachi Federal’s centrally managed, automated, and dynamically tiered storage architecture, HDPP ensures priority access to critical information from disparate sensors (UAVs, satellite, HUMINT) so data can be analyzed and compared to existing intelligence quickly and seamlessly.

Officials at the Naval Air Warfare Center’s Office of Innovation at China Lake Naval Air Weapons Station in Ridgecrest, Calif., have been implementing optical storage archiving solutions because of the sensitive and expensive nature of the data being collected, Houston says. “There is no room for error or data loss. Thus, the agency feels the need to utilize optical storage because the significant longevity and durability of the media.”

Current archiving methods are dominated by magnetic tape solutions, which require technology refreshment every four to six years; however, each refresh is expensive and data is susceptible to being lost in the migration, Houston says.

Magnetic tape is susceptible to conditions such as moisture, heat, and electromagnetic events. “These are unacceptable risks that could jeopardize the efficacy of military operations and put the lives of U.S. service members in danger. As an alternative, the military should employ optical storage solutions like HDPP that significantly reduce the need for regular data migrations and protect it from the elements,” Houston concludes. ◀

For more on data storage, turn to The Last Word on page 36.

Smaller, more modular backplanes and enclosures meeting performance and time-to-market demands

BY John Keller

Rugged embedded computing backplanes and enclosures for aerospace and defense applications are becoming smaller and more distributed in response to demands from systems integrators. In some cases, designs are evolving such that they use no backplane at all.

"The trend continues to be SWaP—reduced size, weight, and power," says J.C. Ramirez, product manager at ADL Embedded Solutions in San Diego. "We have mandates from our key customers asking us to figure out how to get 20 to 25 percent smaller and lighter in the next 12 to 18 months. That is the only way they can remain competitive in this space."

Among the most notable aerospace and defense applications driving down SWaP are unmanned aerial systems (UAS), other kinds of autonomous systems, ground vehicle-based explosives-detection sensors, image processing, hyperspectral imaging, situational awareness, and radio interfaces, industry experts say.

In backplanes and enclosures, trends point strongly to the use of 3U VPX architectures, but demand continues for new implementations of COM Express, PC/104, and small hybrid versions of the

standard 19-inch air transport rack (ATR), experts say.

"VPX is the predominant player in bus-based ruggedized solutions for military and aerospace," says Shan Morgan, president of Elma Americas in Fremont, Calif. "The market also is looking for more standardized pieces like COM Express in smaller boxes, as well as PC/104."

Although it is not new in the aerospace and defense embedded computing market, PC/104 continues to be a stalwart competitor for ever-smaller systems designs. "Just straight PC/104, there is a lot of things going on there, and it's driven by the fact that we need to get smaller and lighter," says ADL Embedded Solutions' Ramirez.

ADL designers are meeting demand for SWaP-constrained PC/104 embedded computing systems with single-board computers based on the high-performance Intel Core microprocessor architecture. "PC/104 is a very solid performer and will be so at least for the next five years," Ramirez says.

Market demand for distributed embedded computing systems connected over 10-Gigabit Ethernet also is helping drive down the size, weight, and power consumption

of embedded computing systems, experts say.

"People are looking to do more of a distributed load," says Jeff Porter, director of product development at Extreme Engineering Solutions Inc. (X-ES) in Middleton, Wis. "People used to put together a big, expensive system, but now they are getting smaller loads closer to the sensor."

Distributed architectures, in addition to the relatively small designs of 3U VPX, COM Express, and PC/104 also are easing the challenge of designing ruggedized embedded computing with conduction cooling that resist the effects of shock and vibration.

"We are seeing people who can distribute the heat load across the system," X-ES's Porter says. "People tend to distribute the load when their fabric and software allow them to do that. The modularity aspect in the smaller distributed architectures cost less to requalify the smaller systems than one massive system."

All this is not to suggest that the larger 6U-based backplane architectures are going away; far from it. "Some of the radar folks tend to be in that realm of the larger boxes," Porter says.

"There is a tremendous amount

COMPANY INFO

AbelConn LLC
New Hope, Minn.
www.abelconn.com

Aitech Defense systems Inc.
Chatsworth, Calif.
www.rugged.com

Ampro ADLINK Technology Inc.
San Jose, Calif.
www.adlinktech.com

Connect-Tek Inc.
Staten Island, N.Y.
www.connect-tek.com

Curtiss-Wright Controls Defense Solutions
Ashburn, Va.
www.cwcdefense.com

Dawn VME Products
Fremont, Calif.
www.dawnvme.com

EIC Solutions Inc.
Warminster, Pa.
www.eicsolutions.com

Electrorack Enclosure Products
Anaheim, Calif.
www.electrorack.com

Elma Electronic Inc.
Fremont, Calif.
www.elma.com

Equipto Electronics Corp.
Aurora, Ill.
www.equiptoelec.com

Extreme Engineering Solutions (X-ES)
Middleton, Wis.
www.xes-inc.com

GE Intelligent Platforms
Huntsville, Ala.
<http://defense.ge-ip.com>

General Micro Systems
Rancho Cucamonga, Calif.
www.gms4sbc.com

I-Bus Corp.
Santa Clara, Calif.
www.ibus.com

Kontron
Poway, Calif.
www.kontron.com

LCR Electronics Inc.
Norristown, Pa.
www.lcr-inc.com

Macrolink Inc.
Anaheim, Calif.
www.macrolink.com

Mercury Systems
Chelmsford, Mass.
www.mrcy.com

Optima Electronic Packaging Systems
Lawrenceville, Ga.
www.optimaeps.com

PCI Systems Inc.
Sunnyvale, Calif.
<http://pcisystems.squarespace.com>

Pentair Equipment Protection
Minneapolis
www.pentair-equipmentprotection.com

Pixus Technologies
Waterloo, Ontario
www.pixustechnologies.com

Rittal Corp.
Schaumburg, Ill.
www.rittal-corp.com

SIE Computing Solutions
Brockton, Mass.
<http://sie-cs.com>

Tracewell Systems
Westerville, Ohio
www.tracewellsystems.com

VadaTech Inc.
Henderson, Nev.
www.vadatech.com/

Vector Electronics & Technology Inc.
North Hollywood, Calif.
www.vectorelect.com

of legacy infrastructure out there," points out Elma's Morgan. "We had one customer who said he was no longer using the bus, but wanted a semi-custom VME backplane to keep the power and connections. They weren't passing signals slot-to-slot, but were using the box and connectors, and were connecting the cards directly. Everybody is familiar with the larger 6U VME system footprint and how it works."

For the future, however, ever-more-distributed architectures are leading to designs that don't use backplanes at all. "One of the trends in backplanes is fewer backplanes,"

Morgan explains.

"With today's chips, what used to be done on a backplane now can be done on a card," Morgan says. "Sometimes it is modules and carrier cards. Semi-passive backplanes and active carrier-card solutions interfacing from commercial silicon and modules are solving packaging and I/O problems on a module."

Distributed designs also are helping engineers solve more problems than just SWaP. "We are able to get the solution to market faster and cheaper without sacrificing the ruggedness and capability," Morgan continues. ◀

PICO

Surface Mount (and Plug In) Transformers and Inductors

See Pico's full Catalog immediately
www.picoelectronics.com

Low Profile from

.18" ht.



Audio Transformers

Impedance Levels 10 ohms to 250k ohms,
Power Levels to 3 Watts, Frequency Response
±3db 20Hz to 250Hz. All units manufactured and
tested to MIL-PRF-27. QPL Units available.

Power & EMI Inductors

Ideal for Noise, Spike and Power Filtering
Applications in Power Supplies, DC-DC
Converters and Switching Regulators

Pulse Transformers

10 Nanoseconds to 100 Microseconds.
ET Rating to 150 Volt Microsecond,
Manufactured and tested to MIL-PRF-21038.

Multiplex Data Bus Pulse Transformers

Plug-In units meet the requirements
of QPL-MIL-PRF 21038/27.
Surface units are electrical equivalents
of QPL-MIL-PRF 21038/27.

DC-DC Converter Transformers

Input voltages of 5V, 12V, 24V And 48V.
Standard Output Voltages to 300V (Special
voltages can be supplied). Can be used as self
saturating or linear switching applications. All
units manufactured and tested to MIL-PRF-27.

400Hz/800Hz Power Transformers

0.4 Watts to 150 Watts. Secondary Voltages 5V
to 300V. Units manufactured to MIL-PRF-27
Grade 5, Class S (Class V, 155°C available).

Delivery-Stock to one week
for sample quantities



800-431-1064

in NY call 914-738-1400
Fax 914-738-8225

PICO Electronics, Inc.

143 Sparks Ave. Pelham, N.Y. 10803

E Mail: info@picoelectronics.com

www.picoelectronics.com





UNMANNED vehicles

Army chooses 20 companies to develop explosives-detection for IEDs hidden in culverts

U.S. Army bomb-detection and -disposal researchers are choosing 20 companies to compete for future projects involving detecting and neutralizing improvised explosive devices (IEDs) hidden in and around roadside culverts. Officials of the Army Contracting Command at Adelphi, Md., announced contracts cumulatively worth as much as \$49.5 million to 20 companies representing a cross section of the robotics and sensor industries. The 20 companies receiving contracts are Advanced Reconnaissance Corp. in N.Y.; Applied Research Associates in N.M.; A-T Solutions in Va.; CyPhy Works in Mass.; Elbit Systems of America in Texas; L-3 Communication Systems-East in N.J.; NIITEK in Va.; Primal Innovation in Fla.; QinetiQ North America in Va.; Robo-Team NA in Md.; Advanced Technology Systems Co. in Va.; Applied Research Associates in N.M.; iRobot Corp. in Mass.; K2 Solutions in N.C.; Lockheed Martin Procerus Technologies L.C. in Orem, Utah; QinetiQ North America in Va.; Robo-Team NA Inc. in Md.; Stolar Research Corp. in N.M.; Science and Engineering Services in Md.; and Pearson Engineering Ltd. in England. ←

Navy chooses AAI Textron to provide mine-hunting unmanned boat for Littoral Combat Ship

BY John Keller

WASHINGTON—Unmanned surface vessel (USV) experts at AAI Corp. in Hunt Valley, Md., are building an unmanned boat designed to detect and pinpoint ocean mines that pose threats to Navy surface warships and other vessels.

Officials of the U.S. Naval Sea Systems Command in Washington announced a \$33.9 million contract to AAI for the Unmanned Influence Sweep System (UISS), which will help the Navy's Littoral Combat Ship (LCS) to perform its mine hunting mission.

The UISS is an integrated magnetic and acoustic minesweeping system that is part of the LCS mine warfare module. It will provide magnetic and acoustic influence minesweeping capability when deployed from the LCS.

The UISS will target acoustic, magnetic, and magnetic and acoustic combination mine types, and provide the LCS with a rapid, wide-area coverage mine-clearance capability to neutralize magnetic and acoustic influence mines.

UISS seeks to provide a high area coverage rate in a small, lightweight package with minimal impact on the host platform, Navy officials say.



AAI is developing an unmanned boat for the Navy's Littoral Combat Ship that will help with mine warfare operations.

The UISS surface vehicle will travel aboard the LCS and will be deployed as necessary to detect, pinpoint, and trigger explosive sea mines hidden under the surface to damage or destroy surface vessels.

The system consists of an unmanned surface vehicle that tows an acoustic and magnetic minesweep system that emits acoustic and magnetic signals that provide a false signature that triggers mines. The surface vessel while operating will be far enough away so it will not be damaged by a detonating mine, Navy officials say.

The UISS will use the Navy's Multiple Vehicle Communications System (MVCS) aboard the LCS, which handles communications between the LCS surface ship and different mission packages, including the UISS, which involve mine counter-

CONTINUED ON PAGE 25 →

Canadian military chooses iRobot UGVs to detect chemical agents, explosives, and radiation

BY John Keller

BEDFORD, Mass.—Leaders of the Canadian military needed unmanned ground vehicle (UGV) robots to alert uses to the presence of chemical warfare agents, toxic industrial chemicals, volatile gases, explosives, and radiation. They found their solution from iRobot Corp. in Bedford, Mass.

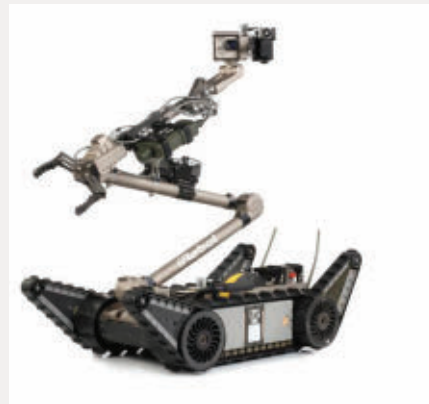
Officials of the Canadian Department of National Defence in Ottawa have awarded multi-year contracts to iRobot initially worth \$9.6 million for 20 iRobot 510 PackBot CBRN Recce UGVs with sensor suites that detect chemical, biological, radiological, and nuclear threats.

The CBRN sensors integrate five primary sensors are designed to

detect, alert and report on chemical warfare agents, toxic industrial chemicals, volatile gases, explosives, and radiation. The robot also has rear flippers to enhance mobility. The contract includes training and future product lifecycle support.

The iRobot 510 PackBot CBRN Recce UGV robot is a modular expansion to the company's 510 PackBot multi-mission robot that meets Canadian military requirements. The company will deliver the ground robots by April 2015.

The base 510 PackBot multi-mission platform is able to integrate additional sensors to assist with the identification and interrogation of CBRN threats. The robot also is for missions including explosive ord-



The Canadian military is using unmanned ground vehicles from iRobot like the one shown above for detecting hazardous agents.

nance disposal, reconnaissance, route clearance, and data collection in industrial settings. ◀

FOR MORE INFORMATION visit iRobot online at www.irobot.com, or the Canadian Department of National Defence at www.forces.gc.ca.

NAVY CONTINUED FROM PAGE 24
measures, anti-submarine warfare, and surface warfare.

For the MVCS, the Navy is using the AB3100H embedded computer from Ballard Technology, part of Astronics Corp., in Everett, Wash. The AB3100H rugged computer is part of the company's AB3000 line of small, lightweight embedded computers with the Intel E680T processor, MIL-STD-1553 and ARINC 429/708/717 interfaces, Ethernet, USB, video, audio, and PMC expansion.

The AB3000 series from Ballard comes with factory-installed PCI mezzanine card (PMC) modules that enable designers to add an Ethernet

switch, synchronous and asynchronous serial interfaces, and isolated double-throw relays.

AAI also designs the Common Unmanned Surface Vessel (CUSV) with unmanned maritime command and control station. The CUSV uses a modular architecture that accommodates platform reconfiguration and interchangeable payloads.

This common vessel is capable of executing mine warfare; anti-submarine warfare; communications relay; intelligence, surveillance and reconnaissance; anti-surface warfare; and UAS/UUV launch and recovery missions.

The UISS contract awarded to AAI has production options for as many as two production units per year for as many as six production units. AAI is part of Textron Systems Corp., and is in the process of rebranding from AAI to Textron Systems.

On this contract, AAI will do the work in Hunt Valley, Md.; Slidell, La.; Hauppauge, N.Y.; Columbia, Md.; and Lemont Furnace, Pa., and should be finished by March 2017. ◀

FOR MORE INFORMATION visit AAI Corp. online at www.textronssystem.com, or Naval Sea Systems Command at www.navsea.navy.mil.

► **Honeywell wins \$15.7 million to provide multi-function cockpit displays for Hornet and Growler jets**

U.S. Navy avionics experts needed a variety of cockpit displays for the Boeing F/A-18E/F Super Hornet jet fighter-bomber and the EA-18 Growler electronic warfare jets. They found their solution from the Honeywell International Inc. Aerospace segment in Albuquerque, N.M. Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., announced a \$15.7 million contract modification to Honeywell on Friday for 197 advanced multi-purpose displays (AMPD) for the Super Hornet and Growler aircraft. The AMPD rugged display family consists of 5-by-5-inch forward avionics displays; 5-by-5-inch aft displays, and 8-by-10-inch avionics displays. The order is for 80 5-by-5-inch forward displays, 75 5-by-5-inch aft displays, and 75 8-by-10-inch displays. In this order 52 forward displays, 48 aft displays, and 24 8-by-10-inch displays are for the U.S. Navy, while 28 forward displays, 27 aft displays, and 18 8-by-10-inch displays are for the government of Australia.

FOR MORE INFORMATION visit **Honeywell Aerospace** at <https://aerospace.honeywell.com>, or **Naval Air Systems Command** at www.navair.navy.mil.

► **Air Force orders LAIRCM laser missile defense systems for C-130 aircraft**
Missile-defense experts at

CONTINUED ON PAGE 33 ➔

Lockheed Martin tests laser weapons to protect aircraft from enemy fighters and missiles

BY **John Keller**

SUNNYVALE, Calif.—Aircraft laser weapons experts at the Lockheed Martin Corp. Space Systems segment in Sunnyvale, Calif., are conducting tests to validate the airworthiness of a prototype high-energy laser tail gun intended to protect combat aircraft from attacks from the rear.

Lockheed Martin has demonstrated the airworthiness of a beam-control turret being developed for the Aero-Adaptive/Aero-Optic Beam Control (ABC) program of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., to give 360-degree coverage for high-energy laser weapons operating on military aircraft, company officials announced.

A research aircraft equipped with the DARPA ABC-developed turret conducted eight flights in Michigan, in partnership with the U.S. Air Force Research Laboratory (AFRL) at Wright-Patterson Air Force Base, Ohio, and the University of Notre Dame in South Bend, Ind.

The ABC turret system is designed to enable high-energy lasers to engage enemy aircraft and missiles above, below, and behind the aircraft. Flow-control and optical-compensation technologies counteract the effects of turbulence caused by the protrusion of a turret from an aircraft's fuselage.



Laser weapons designers at Lockheed Martin are using a business jet as a test bed for a future laser weapon that could defend military aircraft from fighters and missiles.

All turret components meet U.S. Air Force and Federal Aviation Administration airworthiness requirements. Subsequent flight tests over the next year will demonstrate the turret in increasingly complex operations, officials say.

The company began developing the ABC laser turret early last year under terms of a \$9.5 million contract modification from DARPA for the ABC program's third phase to improve the performance of high-energy lasers on tactical aircraft against enemy aircraft or missiles in the aft field of regard.

It was this contract that called for Lockheed Martin flight test an active flow control turret mounted on a business jet to validate turret requirements, design, and predicted performance of ABC technology the company developed in the second phase of the program.

Lockheed Martin's work in the ABC program has included optimiz-

CONTINUED ON PAGE 33 ➔

Military spending for electro-optical technologies to reach \$8.38 billion this year

BY John Keller

AMSTERDAM—Worldwide military spending for military electro-optical and infrared systems will reach \$8.38 billion this year, with steady growth over the next decade, say analysts at market researcher ASD Media BV in Amsterdam.

Predictions for market growth by 2024 were not released in the announcement of the new ASD study, entitled "Military electro-optical infrared (EO/IR) Systems Market Forecast 2014-2024."

Established military markets generally will achieve lower rates of growth in comparison to emerging military powers whose investment will drive global spending, analysts say.

The increased affordability of EO/IR systems combined with their interoperability and mission critical functions will lead emerging military nations to integrate them into new procurement and military modernization programs.

The report encompasses the 20 largest military EO/IR national markets: the U.S.; Saudi Arabia; China; United Kingdom; Russia; Canada; India; Israel; France; Japan; Australia; Germany; Turkey; Brazil; Netherlands; South Korea; United Arab Emirates; Italy; Spain; and Greece. The report also covers the three main end use submarkets: ground, naval, and airborne.

The report also profiles 20 companies in military EO/IR technologies:

Airbus Group; BAE Systems PLC; Elbit Systems Ltd; Excelitas Technologies; Exelis Inc; Finmeccanica SpA; FLIR Systems Inc.; General Dynamics Corp.; Israel Aerospace Industries Ltd.; L-3 Communications Holdings;

Leidos; Lockheed Martin Corp.; Northrop Grumman Corp.; Rafael Advanced Defense Systems Ltd; Raytheon Co.; Rockwell Collins Inc.; Textron Inc.; Thales Group; Ultra Electronics Holdings PLC; and United Technologies Corp.

Technologies covered include imagery, infrared imaging, night-vision systems, and laser range finding systems for in-

telligence, surveillance and reconnaissance (ISR) and intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) capabilities of modern military forces.

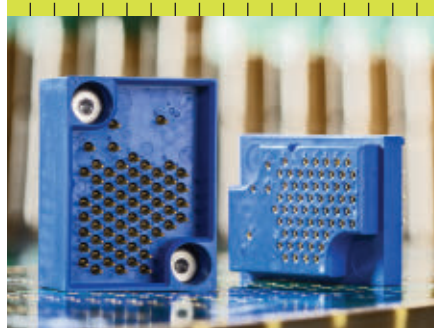
The report defines the military EO/IR systems market as powered systems that use visible and non-visible light to provide visual feedback to military personnel or are integrated with other military systems. It includes three broad applications of EO/IR systems on airborne, ground, or naval platforms.

Systems covered include multispectral day and night imaging sensors, night vision goggles (NVG), laser rangefinders (LRF), forward looking infrared (FLIR) systems and



Electro-optical sensor payloads for manned and unmanned aircraft like the one from Elbit Systems, shown above, will be staples in anticipated growth in the EO/IR market.

QUICK-TURN CUSTOM CONNECTORS



Courtesy of Siemens

Positronic leads the pack in providing high reliability, quick-turn custom connectors for a variety of industries. Whether you are faced with replacing an obsolete product, qualifying a second source or designing a connector perfectly tailored to your application - Positronic is your BEST VALUE choice! Contact us today at connectpositronic.com/contact.



Positronic®
global connector solutions

CONTINUED ON PAGE 33 ➔

PRODUCT applications

EMBEDDED COMPUTING

Navy chooses PCI Express cards from Ballard to connect MIL-STD-1553 systems to PCs

U.S. Navy aviation experts needed a way for PC computers to communicate with military avionics systems based on the MIL-STD-1553 databus. They found their solution from Ballard Technology Inc., part of Astronics Corp., in Everett, Wash.



Navy airborne weapons experts announced their intention to buy PCI Express 1553 interface cards and cables from Ballard. The value of the upcoming order has yet to be negotiated.

Officials of the Naval Air Warfare Center Weapons Division at China Lake Naval Weapons

Station in Ridgecrest, Calif., say they will buy the Ballard LE1553-5 PCI Express 1553 interface card, as well as the Ballard 16037 cables that connect PC computers to 1553 systems.

Navy officials say they will award a sole-source order to Ballard due to compatibility with existing software code and proprietary data. The purchase will involve four interface cards and eight cables.

The Ballard LE1553-5 is a personal computer expansion card for communicating with MIL-STD-1553 systems. These interfaces provide programmable data buffers and deep built-in memory.

The cards offer one to four dual-redundant MIL-STD-1553 channels, 16 I/O avionics level discretes, and IRIG time synchronization and generation. MIL-STD-1553 capability includes BC, RT, and monitor. Avionics discretes can be used as general-purpose I/O or linked in hardware to 1553 databus activity as triggers or syncs.

The cards support maximum data throughput on all 1553 interfaces, Ballard officials say. Each channel is independently configurable as bus controller, remote terminal, or bus monitor.

FOR MORE INFORMATION visit **Ballard Technology** online at www.ballardtech.com.



ENCLOSURES AND CHASSIS

Navy chooses VXI backplanes from Tracewell Systems for submarine communications routing

U.S. Navy undersea warfare experts needed embedded computing to route signals and information among various antennas and communications systems aboard Navy submarines. They found their solution from Tracewell Systems Inc. in Westerville, Ohio.

Officials of the Naval Undersea Warfare Systems Division in Newport, R.I., announced a \$144,612 contract to Tracewell for 80 high-performance 11-slot VXI backplanes for the Radio Frequency Distribution and Control Systems (RFDACS).

The RFDACS provides a means of routing signals and information between the various antenna systems and other submarine communication subsystems.

It replaces point-to-point wiring of radio frequency (RF) and control signals, and provides modular architecture for hardware and software for simplified expansion or modification of the system. The RFDACS(V)17 variant is installed on Los Angeles- and Virginia-class fast-attack submarines.

The Tracewell backplanes are components of RFDACS, which has undergone extensive environmental qualification testing (EQT) and

screening certification to the operational RFDACS Fleet equipment baseline, Tracewell Systems officials say.

Installed within a rugged main-frame, the backplane provides power distribution and signal interconnect for the precision VXI test instrumentation within the system, and provides signal and power distribution.

Optimized power and ground planes in the enclosure minimize voltage drop and ground shift, and designers have paid special attention to DC resistance and ground shift voltage, Tracewell officials say.

To meet high-current demands, power planes use high copper densities and increased surface area to minimize voltage drop. The low-inductance, high-density planes, and bulk decoupling capacitors located near all integrated circuits help reduce ground shift voltage caused by the inductance of IC pins and other connectors, company officials say.

FOR MORE INFORMATION visit **Tracewell Systems** online at www.tracewell.com.

EMBEDDED COMPUTING

BAE Systems chooses embedded computing from GE for training on Bradley Fighting Vehicle

Vetronics designers at the BAE Systems Platforms and Services segment in Santa Clara, Calif., needed rugged computers for embedded training capability on the U.S. Army BAE Systems M2A3 Bradley Fighting Vehicle. They found their solution from GE Intelligent Platforms in Huntsville, Ala.

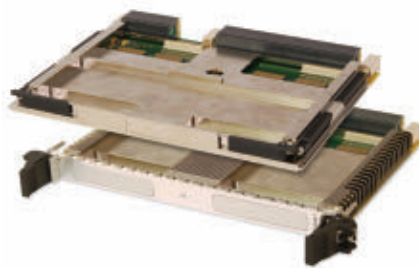
GE has received a \$2.6 million order from BAE Systems for the CRS-D5I-3VC1 rugged COTS system, which has GE's latest-generation 3U VPX COTS embedded computing boards for high-performance

embedded computing (HPEC) aboard the Bradley.

The CRS-D5I-3VC1 COTS rugged systems will be deployed as part of the Army's Common Embedded Training Unit (CETU) for in-vehicle training and simulation aboard the Bradley.

The GE CRS-D5I-3VC1 rugged embedded computing system offers small size, weight and power (SWaP) to provide the functionality necessary for embedded training on the Bradley vehicle.

Embedded training involves sim-



ulation, training, and mission-rehearsal capability that enables Bradley crews to practice tasks like driving, ammunition loading, target acquisition and tracking, and weapons firing inside the actual Bradley Fighting Vehicle.

Embedded training enables crews to practice on their vehicles, rather than traveling to large and expensive full-mission computer simulators that are located at a limited number of locations. Embedded training especially is useful for warfighters deployed overseas where simulation capability is limited.

The GE CRS-D5I-3VC1 is housed in a rugged, five-slot enclosure with a GE 3U VPX single board computer with an Intel Core i7 processor and a rugged graphics board based on the NVIDIA 384-core 'Kepler' graphics processing unit (GPU).

GPU technology enables

embedded computing designers to use massively parallel processing that enables complex applications like embedded simulation and training in small, power-efficient spaces.

FOR MORE INFORMATION visit **GE Intelligent Platforms** online at www.defense.ge-ip.com, or **BAE Systems Platforms and Services** at www.baesystems.com.

CONTRACT MANUFACTURING

Navy chooses contract manufacturer Sechan to build components for ship self-defense system

Electronics contract manufacturer Sechan Electronics Inc. in Lititz, Pa., will build hardware for the U.S. Navy's Ship Self-Defense System (SSDS) Mk2 under terms of a \$24.3 million contract.

Officials of the Naval Surface Warfare Center in Dahlgren, Va., are asking Sechan to build, assemble, configure, align, integrate, test, and ship SSDS hardware.

The SSDS helps crews of Navy surface warships detect, track, assess, and shoot down incoming subsonic and supersonic anti-ship missiles. It is designed to expedite the detect-to-engage sequence to defend against anti-ship cruise missiles.

SSDS links and automates standalone sensors and weapon systems to help ship crews respond to incoming anti-ship missile threats quickly enough to shoot them down before they hit their vessels.

The SSDS uses a fiber optic local area network to connect ship sensors and weapons to coordinate sensor integration; identify and evaluate potential threats; assess readiness of ship defenses; and execute specific tactical procedures.

The SSDS also helps the ship's



captain control his weapons such that his crew has a good chance at shooting down incoming cruise missiles. The system is for aircraft carriers and expeditionary ships on seven ship classes.

On this contract, announced on 23 Sept. 2014, Sechan will do the work in Lititz, Pa., and should be finished by September 2017.

FOR MORE INFORMATION visit Sechan Electronics online at www.sechan.com.

SATCOM

U.S. Special Operations Command picks ViaSat Small Tactical Terminals for infantry communications

U.S. Special Operations Command (SOCOM) needed small networking terminals to link ground vehicles, small boats, ships, helicopters, and unmanned aerial vehicles (UAVs). They found their solution from ViaSat Inc. in Carlsbad, Calif.

Officials of the SOCOM Directorate of Procurement announced plans this week to buy five of ViaSat's Small Tactical Terminals (STTs) for use as aircraft radio that supports two channel simultaneous operation. No other company has the same kind of technology, officials say.

ViaSat engineers developed the Link 16/Secure UHF Line-of-Sight (LOS) Small Tactical Terminal KOR-24 together with Harris Corp. to merge air and ground situational

awareness at the tactical edge.

Packaged in a small, lightweight, ruggedized form factor, the STT brings mobile network connectivity to tactical warfighters and disadvantaged platforms such as ground vehicles, small boats, ships, helicopters, and UAVs.

Interoperable with the Multifunction Information Distribution System (MIDS) Link 16 and UHF Data Radios, the STT enables users to exchange secure situational awareness information and critical data communications with allied air, land, and sea platforms over Link 16 or UHF to help maintain the tactical picture and avoid blue-on-blue engagements, ViaSat officials say.



The STT combines Link 16 technology from ViaSat with Harris UHF radio heritage to provide interoperability with MIDS Link 16 terminals, JTIDS, or UHF data radio systems deployed around the world. This device also supports all TADIL J network messages, including Network Enabled Weapon (NEW) messages.

Infantry warfighters and disadvantaged nodes can use the STT to deliver mission-critical connectivity and total battlefield visibility.

FOR MORE INFORMATION visit ViaSat online at www.viasat.com, or U.S. Special Operations Command at www.socom.mil.

RACKMOUNT SERVERS

NASA chooses image-generating rackmount visual servers for simulation from Concurrent Computer

Space researchers at the NASA Marshall Space Flight Center in Huntsville, Ala., needed real-time computers to help them develop flight sensors and emulators. They found their solution from Concurrent Computer Corp. in Duluth, Ga.

NASA-Marshall officials announced their intention to purchase ImaGen rackmount visual servers from Concurrent to help them build operation flight instrument (OFI) sensors, United Launch Alliance (ULA) emulators, and Integration Test Lab (ITL) emulators within the NASA-Marshall Integrated Avionics Test Facilities.

Because of the complexity of the real-time computing, the systems running the real-time operating system must be certified by Concurrent, the provider of the systems, NASA officials say.

The Concurrent family of ImaGen visual servers offers integrated high-performance image-generation for real-time simulation and modeling applications, company officials say. Powered by Concurrent RedHawk Linux, ImaGen is for interactive virtual reality, landscape, architectural, and aerial, ground, and marine simulation. ←

FOR MORE INFORMATION visit Concurrent Computer online at www.ccur.com, or NASA Marshall Space Flight Center at www.nasa.gov/centers/marshall.





DATA ACQUISITION

Interface to add military sensor data acquisition and distribution introduced by NAI

North Atlantic Industries (NAI) Inc. in Bohemia, N.Y., is introducing an enhanced Nano Interface Unit (NIU1) to add sensor data acquisition, distribution, and communication interfaces to military and aerospace embedded computers without chassis and backplane redesign. Enhancements to the NIU1 include SoC dual ARM Cortex-A9 processor for smaller size, lower power, higher bandwidth, shared memory, and lower latency in a small package, as well as processor software programming support for Wind River Linux, VxWorks, and Xilinx Petalinux. The compact, nano-sized



subsystem connects to existing Ethernet networks, making data available to any system on the network. Built on NAI's Custom-On-Standard Architecture (COSA), the NIU1A offers more than 40 intelligent I/O and communications functions.

FOR MORE INFORMATION visit North Atlantic Industries online at www.naii.com.

INTERCONNECT TECHNOLOGY

Circular connector with a small flange to fit heavy equipment vehicles introduced by Amphenol

Amphenol Industrial Products Group

in Sidney, N.Y., is introducing the ATC-09-9-1939PN 9-way AT circular series interconnect receptacle with a small flange to fit heavy equipment vehicles. The ATC-09-9-1939PN circular connector meets SAE J1939, a specification for communication and diagnostics among industrial vehicle components. Used as a diag-



nostic connector in demanding applications found on construction and farm equipment as well as in heavy-duty trucks, these round receptacles include a strain relief for the wires coming out of the back of each unit and a wave spring for higher vibration applications. The upgraded connectors have simple jam nut mounting for quick assembly and a smaller flange that saves space on mating panels.

FOR MORE INFORMATION visit Amphenol online at www.amphenol-industrial.com.

POWER ELECTRONICS

Isolated DC-DC converters for information and communications gear introduced by TDK-Lambda

TDK-Lambda Americas Inc. in San Diego is introducing the 300-watt TDK-Lambda iEH series of isolated DC-DC converters for information, communications, semiconductor



manufacturing, measuring, and industrial equipment. With digital non-linear adaptive control, these power electronics devices provide better dynamic performance, improved system stability and reduced component count, TDK officials say. Operating from a 48 volts DC nominal input, the iEH series can provide output voltages of 9.6 to 12 volts with currents to 33 amps. The converters are in the industry-standard eight-brick package and include a baseplate with mounting holes for use with an external heat sink. Optimization of components using digital control enables to 192 watts of output power with 200LFM airflow in an 85 degrees Celsius ambient.

FOR MORE INFORMATION

visit TDK-Lambda online at www.us.tdk-lambda.com.

RF AND MICROWAVE

High-power rackmount solid-state RF and microwave power amplifier introduced by Aethercomm

Aethercomm Inc. in Carlsbad, Calif., is introducing the SSPA 0.960-1.215-2000-RM high-efficiency, high-power and linear rackmount solid-state power amplifier for a variety of RF and microwave applications. The amplifier operates from 960 MHz to 1215 MHz, and is microprocessor controlled. The built in pre-distortion linearizer allows for low



level IMD's at high RF output power levels. The unit produces 800-1000 Watts PEP or 200+ watts CW. The LCD touch screen display allows the operator to control all functions including the desired RF power output, and ALC enable and disable. The rackmount unit is housed a 4U high



rack mounted enclosure that weighs less than 55 pounds.

FOR MORE INFORMATION

visit **Aethercomm** online at www.aethercomm.com.

MOTION SENSORS

Miniature inertial systems for stabilizing moving vehicular subsystems introduced by SBG

SBG Systems s.a.s. in Rueil-Malmaison, France, is introducing the Ellipse series of miniature inertial sensors for stabilizing or orientating vehicular subsystems while the vehicle is moving. These miniature but high performance sensors can be connected to SAASM receiver for accurate navigation and positioning even during GPS outages, company officials say. The devices are



designed to replace the SBG IG-500 series. This series of miniature inertial systems benefits from a design, sensors, capabilities, and algorithms. Weighing from 45 grams, Ellipse sensors are flexible. Ellipse sensors resist the effects of dust, water, and vibration. The series is IP68 and compliant with the MIL-STD-810 certification.

FOR MORE INFORMATION

visit **SBG Systems** online at www.sbg-systems.com.

TEST AND MEASUREMENT

Fast logic analysis system for high-end digital test and measurement introduced by Keysight

Keysight Technologies Inc. in Santa Rosa, Calif., is introducing the U4154B logic analysis test & measurement system for engineers who work on high-end digital designs, mobile, computing, DDR and LP-DDR memory and server applications. The state-mode logic analyzer from Keysight (formerly Agilent)



samples as quickly as 4 gigabits per second, and is for validating simultaneous read and write DDR4 traffic across all byte lanes captured from a DDR4 DIMM operating at data rates of more than 2.5 gigabits per second. The Keysight U4154B logic analysis system merges three modules to help memory design engineers accelerate turn-on and debugging of DDR2/3/4 and LPDDR2/3/4

memory systems. The system provides data capture, precise triggering and a portfolio of validation and performance tools. The instrument is driven by a 64-bit software application that enables users to take full advantage of all memory installed in their 64-bit operating systems.

FOR MORE INFORMATION visit

Keysight online at www.keysight.com.

CHASSIS AND ENCLOSURES

Weld-free, rugged electronics cabinets for extreme environments introduced by Optima Stantron

Optima Stantron in Lawrenceville, Ga., is introducing the MB-series weld-free, rugged electronics cabinets that offer increased



structural integrity to withstand a variety of demanding, extreme environments. The rugged enclosures are for use in places affected by harsh, corrosive conditions such as salt spray, as found in shipboard applications, as well as in rugged, mobile environments, such as air, ground, water, and test and measurement equipment. The modular MB-series is a set of flexible, customer-tailored cabinets designed to specific application requirements. Conforming to several MIL specifications, the cabinets incorporate a heavy-duty aluminum frame with horizontal and vertical extrusions that accommodate EMI gaskets and steel corner-key inserts. The MB-series can be fitted with optional hard-mount or shock-isolation

hardware for added resistance to environmental influences.

FOR MORE INFORMATION visit Optima online at www.optimastantron.com.

POWER ELECTRONICS

Power PRM for UAVs and other SWAP-constrained military applications introduced by Vicor

Vicor Corp. in Andover, Mass., is introducing the power pre-regulator module (PRM) for unmanned aerial vehicles (UAVs) and other military systems designs that focus on small size, weight, and power (SWAP). Target applications for this power electronics device included those involved with MIL-STD-704, high-voltage 270 volts DC aircraft systems, and high-density power supplies. The PRM regulator (MPRM-



48NF480M500A00) is based on Vicor's VI Chip platform, and provides power density of 106 Watts per cubic centimeter and efficiency of 97.7 percent, company officials say. The regulator delivers 500 watts output power in the same package size as Vicor's earlier generation 120 watts MIL-COTS PRMs. The regulator measures 32.5 by 22 by 6.73 millimeters, has an operating input range of 38 to 55 Vin, offers regulated 20-to-55-volt output range (adjustable), and is available in surface-mount and through-hole assembly options.

FOR MORE INFORMATION visit Vicor online at www.vicorpower.com.

Northrop Grumman Corp. will install laser-based aircraft missile-defense systems aboard 28 U.S. Air Force C-130 four-engine turboprop aircraft under terms of a \$28 million contract modification. Officials of the Air Force Life Cycle Management Center at Wright-Patterson Air Force Base, Ohio, are asking engineers at the Northrop Grumman Electronic Systems segment in Rolling Meadows, Ill., to install the electro-optical Large Aircraft Infrared Counter Measures (LAIRCM) aboard the aircraft. Northrop Grumman will provide LAIRCM C-130 group A kits and installations on 11 AC-130H gunships, 12 MC-130U gunships, and five EC-130J psychological operations aircraft under terms of the contract modification. LAIRCM automatically detects a missile launch, determines if it is a threat, and activates a high-intensity laser-based countermeasure system to track and defeat the missile, Northrop Grumman officials say. LAIRCM focuses high-intensity laser energy at the infrared seeker head of incoming missiles to blind the missile and force it off its target. The system is designed to protect large aircraft such as the C-130 from shoulder-fired infrared missiles like the U.S. Stinger when the aircraft is operating close to the ground, such as on take-off and landing, as well as during low-level operations. ◀

FOR MORE INFORMATION visit Northrop Grumman Electronic Systems online at www.northropgrumman.com, or the Air Force Life Cycle Management Center at www.wpafb.af.mil/aflcmc.

LOCKHEED CONTINUED FROM PAGE 26

ing flow control for pointing angles behind tactical aircraft, as well as exploring how to synchronize ABC flow-control technology with adaptive optics.

Lockheed Martin engineers are designing representative optical paths, a scaled turret, and flow control actuator system, as well as conducting wind-tunnel testing, and mounting a prototype aircraft laser-defense weapon to the test aircraft—the Airborne Aero Optical Laboratory Transonic Aircraft that belongs to the University of Notre Dame.

Adaptive optics involves manipulating the shapes of lenses and mirrors to enable high-energy laser weapons to compensate for the effects of atmospheric turbulence.

Lockheed Martin is doing the work on the third phase of the ABC program in Sunnyvale, Calif.; Fort Worth, Texas; and Orlando, Fla. Company officials should be finished with the program's third phase by fall 2015. ◀

FOR MORE INFORMATION visit Lockheed Martin Space Systems online at www.lockheedmartin.com/us/ssc, or DARPA at www.darpa.mil.

EO/IR CONTINUED FROM PAGE 27

infrared targeting pods.

The report excludes optics-based seeking systems and flare systems. The report also excludes unpowered EO/IR systems such as binoculars and will not include data storage of visual display systems for EO/IR platforms. ◀

FOR MORE INFORMATION contact ASD Media online at www.asdreports.com.



ST-9020 rugged computer system with 20" display, MIL STD shock & vibration qualified



DU-19/U rugged monitor

For full line of rugged systems contact:

IBI SYSTEMS, INC.
6842 NW 20TH AVE, FORT LAUDERDALE, FL 33309
PHONE: 954-978-9225, WEB: www.ibi-systems.com

have an open mind

*...and fill it with
info on epoxies*

Visit our resource
library for:

- white papers
- videos
- e-newsletters
- technical tips



Hackensack, NJ 07601 USA •
+1.201.343.8983 • main@masterbond.com

www.masterbond.com

SITUATIONAL AWARENESS

DISPLAY VIDEO & COMPUTER SIGNALS ON A SINGLE SCREEN



Combine up to 12
real-time visuals on
a single screen

Display any signal type,
including graphics, HD
and video

Position and scale
images any size,
anywhere

Pan and zoom
within images

SUPERVIEW® - ALWAYS THE BEST...NOW EVEN BETTER



SPECTRUM®
decision support systems™

(510) 814-7000 www.rgb.com

PUBLISHER Ernesto Burden
603 891-9137 / ernestob@pennwell.com

EDITOR-IN-CHIEF John Keller
603 891-9117 / jkeller@pennwell.com

EXECUTIVE EDITOR Courtney E. Howard
509 413-1522 / courtney@pennwell.com

CONTRIBUTING EDITOR
WESTERN BUREAU J. R. Wilson
702 434-3903 / jrwilson@pennwell.com

EDITORIAL GRAPHIC DESIGNER Cindy Chamberlin

PRODUCTION MANAGER Sheila Ward

SENIOR ILLUSTRATOR Chris Hipp

AUDIENCE DEVELOPMENT MANAGER Debbie Bouley
603 891-9372 / debbieb@pennwell.com

AD SERVICES MANAGER Glenda Van Duyne
918 831-9473 / glendav@pennwell.com

MARKETING MANAGER Kristi Guillemette
603 891-9126 / kristig@pennwell.com



Editorial offices
PennWell Corporation,
Military & Aerospace Electronics
98 Spit Brook Road LL-1, Nashua, NH 03062-5737
603 891-0123 • FAX 603 891-0514 • www.milaero.com

Sales offices
EASTERN US & EASTERN CANADA & UK
Bob Collopy, Sales Manager
603 891-9398 / Cell 603 233-7698
FAX 603 686-7580 / bobc@pennwell.com

WESTERN CANADA & WEST OF MISSISSIPPI
Jay Mendelson, Sales Manager
4957 Chiles Drive, San Jose, CA 95136
408 221-2828 / jaym@pennwell.com

REPRINTS Jeanine Pranses
717 505-9701 x344 / jeanine.pranses@theygsgroup.com

DIRECTOR LIST RENTAL Kelli Berry
918 831-9782 / kellib@pennwell.com

Corporate Officers
CHAIRMAN Frank T. Lauinger

PRESIDENT AND CEO Robert F. Biolchini

CHIEF FINANCIAL OFFICER Mark Wilmoth

Technology Group
SENIOR VICE PRESIDENT/PUBLISHING DIRECTOR
Christine Shaw

Subscription Inquiries
847 763-9540 • FAX 847 763-9607
e-mail: mae@halldata.com
web: https://pennwell.sub-forms.com/PNW20_MFcontact



Rugged flexible COTS Solutions from MPL
fully designed and produced in Switzerland



Highlights

- 10+ years availability
- 20+ years repairable
- Openframe up to IP67 enclosure
- OEM and customized solutions

Features

- up to 3rd. gen. i7 Core, ARM, Freescale
- temp. -40°C up to +85°C
- all fanless at full load
- Switches, Routers, Fiber, Firewall w. source code

info@mpl.ch **MPL** www.mpl.ch
High-tech • Made in Switzerland

MPL AG, Täfernstr. 20, CH-5405 Dättwil/Switzerland
Phone +41 56 483 34 34, Fax +41 56 493 30 20

ADVERTISERS INDEX

Acromag.....	11
Crane Aerospace & Electronics	9
Daisy Data Inc	5
Dawn VME Products	7
Extreme Engineering Solutions	3
IBI Systems Inc	34
Intelligent Aerospace Conference & Exhibition 2015.....	C2
International Rectifier	1
Lasers & Photonics Marketplace Seminar.....	C3
M S Kennedy Corporation.....	19
Marvin Test Solutions.....	C4
Master Bond Inc	34
Modular Devices Inc.....	13
MPL AG	35
Phoenix International	17
Pico Electronics Inc.....	23
Positronic Industries.....	27
RGB Spectrum	34

**BIO:****NAME:** Christian Heiter**TITLE:** Chief Technology Officer**CO.:** Hitachi Data Systems Federal**ROLE:** Provider of virtualization and cloud solutions to reduce complexity and increase efficiency of government data center initiatives, including big data analytics**CONTACT:** www.hdsfed.com

Christian Heiter

Hitachi Data Systems Federal executive discusses innovating with information, improving IT efficiency, meeting initiative and budget requirements, and gaining better insight from data.

Why is data storage a hot topic?

The solutions space is expanding. The problems [aerospace and defense organizations] are trying to solve are much broader. It's not just about how many bytes of storage or how many cycles per second to process; it's really how you combine them all together, and that way you can make much better business or operational mission decisions—and make them faster and with higher reliability—and that really allows us to be able to protect our people and fighting troops on the ground, as the case may be.

What challenges exist?

A huge problem is the amount of data that comes in off of even just a single mission. If we look of the life of data, it comes off of the sensor

platform over some kind of communications link to local ground station or somewhere around the world. Now we've got to go collect it, analyze it, and compare it to other data that could be sitting on local storage where the vehicle landed or geo located somewhere else, even hundreds of thousands of miles away.

How do we make better, more intelligent decisions? By trying to correlate all this information into a better answer or a better prediction of what might happen.

Our technology doesn't sit out at the edge; data is fed to our systems in the data centers for the much larger collection or aggregation of information. Not only do we aggregate it, but we can also disseminate it very cost effectively to other sites.

Because we are really focused on the storage economics, we have a tight design control making sure we are within a green power budget, to try to reduce the amount of power used; that helps with the overall

operational costs for a mission.

We try to look at the full data lifecycle; as it hits our data center, we try to make sure our customers have a better, much more reliable solution not only for the short term but the longer term operation expenses are reduced—so they can have a much better chance of meeting their budgetary requirements. As a taxpayer, I think we all would like that; I have a strong interest in being better for the overall economy and ecology of the world around us—anything we can do to save power can only help.

What advice would you offer?

The whole industry is looking at utilizing metadata differently. We built a set of tools that allows us to exploit metadata and manage it in a much more cost effective manner. We know we have these deep piles of data, all different types of storage; let's find new ways we can use the metadata to help us manage these huge piles of information more cost effectively and go out and find the data that's out there. Many people have pools of storage they don't even know what's in there; they think they know but they really can't find it. This is a big problem both in the commercial and the federal space. ◀



Don't miss a word

Access the rest of this conversation by visiting www.militaryaerospace.com/LastWord or scanning the QR code at left.



LASERS & PHOTONICS MARKETPLACE SEMINAR™

FEB 9 2015 | MARRIOTT MARQUIS, SAN FRANCISCO, CA



Charting Global Market and Business Strategies

THE LASERS & PHOTONICS MARKETPLACE SEMINAR is the only event anywhere in the world that focuses on the entire laser marketplace. It provides a comprehensive market perspective that is unobtainable elsewhere, with market data segmented by applications and laser technology from three of the photonics industry's leading resources: *Laser Focus World*, which delivers global coverage of the entire photonics industry; *Industrial Laser Solutions*, a primary source of information on industrial laser materials processing; and Strategies Unlimited, the world's foremost photonics market research company. In addition, industry experts present their views and analysis of photonics-market trends, applications development, and business outlook.

GLOBAL LASER MARKETS:
INSIGHTS AND FORECASTS
presented by



Allen Nogee,
Strategies Unlimited

EARLY BIRD DISCOUNT!

Register by December 19th
and SAVE \$200!

REGISTRATIONS FEES | Include all seminar sessions, full proceedings and all scheduled seminar meals.

BEFORE DECEMBER 19, 2014

Seminar \$1,095

Multiple Registrations* \$995

AFTER DECEMBER 19, 2014

Seminar \$1,295

Multiple Registrations* \$1,095

Register at: www.marketplaceseminar.com

WHO SHOULD ATTEND?

- Presidents, CEOs, and COOs
- Chief Technology Officers
- R&D Management
- Sales and Marketing Executives
- Business Development Directors
- Managing Directors
- Business/Technology Analysts



KEYNOTE:

The Ultrafast Future

Ursula Keller, PhD

Ultrafast Laser Physics Group,
ETH Zurich

Ultrafast--or ultra-short pulse--laser technology is dramatically impacting many areas of photonics, from basic science to industrial manufacturing and biomedicine. The design and performance of the lasers behind these applications will be critical for creating new applications and opening new market opportunities. Prof. Keller will provide a view of the ultrafast laser landscape and help the audience understand such important topics as power scaling of semiconductor lasers and diode-pumped solid-state lasers, and where such new capabilities might lead.

See the full agenda and register at: www.marketplaceseminar.com

Conference Sponsor:



Conference Sponsor:



Reception Sponsor:



Lunch Sponsor:



Wi-Fi Sponsor:



Media Sponsors: **LaserFocusWorld**

**INDUSTRIAL
LASER SOLUTIONS**
FOR MANUFACTURING

Strategies Unlimited

BioOptics
WORLD

Owned &
Produced by:



Held in
conjunction with:



Supported by:



Harness the Power of a MIL-SPEC COTS Test Platform



MTS-207 TEST SET

Tough enough for your harshest environments

ULTRA-RUGGED

Ideal for armament, avionics and data acquisition test

CONFIGURABLE

PXI architecture for ultimate customization and expansion

MILITARY AND AEROSPACE PROVEN

Globally deployed in 20 countries

See how the MTS-207 can help you deliver your solution on-time and on-budget. Read our solutions white paper, "Leveraging a MIL-SPEC COTS Test Platform," at marvintest.com/flightlinetestingsolutions.

VISIT MARVIN TEST SOLUTIONS AT AUTOTEST 2014, BOOTH 619.



Formerly Geotest - Marvin Test Systems

The
Marvin Group

MARVINTEST.COM