

DECEMBER 2015

Military & Aerospace Electronics®

ENABLING TECHNOLOGIES
FOR NATIONAL DEFENSE

COTS parts

COTS parts are on the rise in military C4ISR applications. PAGE 4

Rugged data storage

Solid-state disks dominate, with requirements emerging for data security, network storage. PAGE 12

militaryaerospace.com

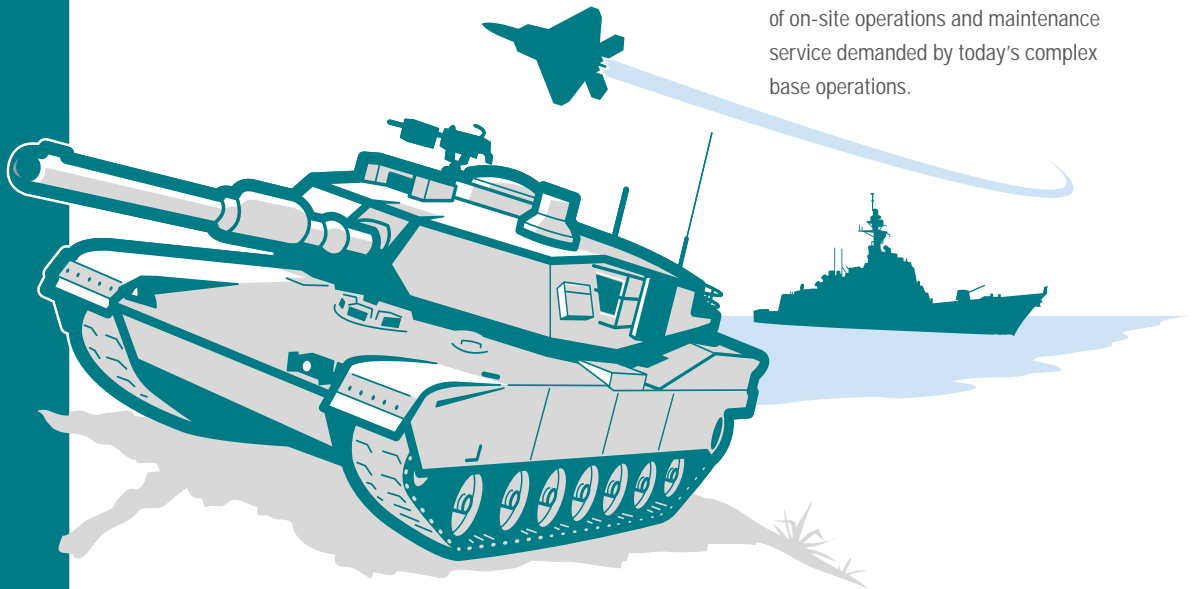
Cyber warfare

Cyber warfare capabilities grow to meet dangerous new cyber threats. PAGE 5

PennWell®

What don't we do for the US Military?

While we don't drive the armored vehicles or pilot the jet fighters, EMCOR has plenty of boots on the ground to keep our troops and their facilities safer, more efficient, and ever ready. Below is just a sample of how we help the military accomplish its missions...



It's all about support—24/7/365 our people are on call for virtually every type of on-site operations and maintenance service demanded by today's complex base operations.

EMCOR Government Services takes many forms—our people support key facilities for the Army, Navy, Air Force, Marines, U.S. Coast Guard, and U.S. Customs and Border Protection and more.

High-tech, high-performance facilities deserve a higher caliber of preventive maintenance and repair—we are proud to provide vital services and Base Operations Support nationally.

MISSIONS ACCOMPLISHED



FEDERAL AGENCIES



U.S. MILITARY



NATIONAL SECURITY



SPACE



WASHINGTON, D.C.



HEALTHCARE SUPPORT



EMCOR
Government Services

WHAT CAN WE ACCOMPLISH FOR YOU?

emcor_info@emcor.net

866.890.7794

emcorgovservices.com



2 TRENDS

3 NEWS

3 IN BRIEF



COVER STORY:

5 SPECIAL REPORT

Cyber security expands to meet demands

Defensive and offensive cyber warfare capabilities are growing to meet dangerous new cyber threats from national adversaries and shadowy terrorist groups, as military command structure evolves to meet tomorrow's cyber challenges.



12 TECHNOLOGY FOCUS

Data storage faces network-centric future

Rugged data storage is dominated today by solid-state disks, yet there is still room for rotating hard disks, with emerging requirements for data security and sharing storage devices on networks.



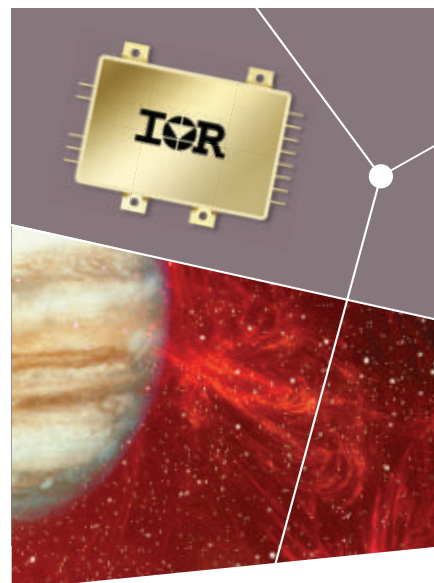
18 RF & MICROWAVE

20 UNMANNED VEHICLES

22 ELECTRO-OPTICS WATCH

24 PRODUCT APPLICATIONS

26 NEW PRODUCTS



LSO Series – Space Grade DC-DC Converter with OVP

Features:

- › Input current telemetry
- › 18 to 40V DC input
- › RAD-Hard with TID >100Krad/s and SEE immunity to LET = 83MeV-cm²/mg
- › 30W low voltage single and dual outputs
- › Efficiency up to 81%
- › Latch-off output overvoltage protection (OVP)
- › Design analysis including WCA available
- › Industry's standard package: 3.50"L x 2.50"W x 4.75"H

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

IOR HiRel
An Infineon Technologies Company

Military & Aerospace Electronics® (ISSN 1046-9079), Volume 26, No. 12. Military & Aerospace Electronics is published 12 times a year, monthly by PennWell® Corporation, 1421 S. Sheridan, Tulsa, OK 74112. Periodicals postage paid at Tulsa, OK 74112 and at additional mailing offices. SUBSCRIPTION PRICES: USA \$175 1yr., \$309 2 yr., \$440 3 yr.; Canada \$270 1 yr., \$465 2 yr., \$600 3 yr.; International \$325 1 yr., \$620 2 yr., \$810 3 yr. POSTMASTER: Send address corrections to Military & Aerospace Electronics, P.O. Box 3425, Northbrook, IL 60065-3425. Military & Aerospace Electronics is a registered trademark. © PennWell Corporation 2015. All rights reserved. Reproduction in whole or in part without permission is prohibited. Permission, however, is granted for employees of corporations licensed under the Annual Authorization Service offered by the Copyright Clearance Center Inc. (CCC), 222 Rosewood Drive, Danvers, Mass. 01923, or by calling CCC's Customer Relations Department at 978-750-8400 prior to copying. 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 via direct mail, please let us know by contacting us at List Services Military & Aerospace Electronics, 98 Spit Brook Rd LL-1, Nashua, NH 03062-5737. Printed in the USA. GST No. 126813153. Publications Mail Agreement no. 875376.



Remembering Amos Deacon Jr., 1934 to 2015

We lost someone whom many of us in the military electronics industry have known and done business with for a long time: Amos Deacon Jr., founder of rugged data storage specialist Phoenix International Systems Inc. in Orange, Calif. He lost his battle with cancer on 19 Nov. 2015 at his home in California. He was 82.

It was with a rare blend of business acumen, blunt honesty, human compassion, and wry humor that Deacon practiced his craft among us in the aerospace and defense electronics industry for more than half a century.

He was born in Dunedin Isle, Fla., in a house on stilts in the Gulf of Mexico, and grew up in Central Florida and Pennsylvania. After graduating in 1951 as class valedictorian at Paradise High School in Pennsylvania, he attended the U.S. Naval Academy in Annapolis, Md., and Lafayette College in Easton, Pa.

In 1962, he was hired by the Hughes Aircraft Co. and moved his young family to Orange, Calif. He completed the MBA program at the University of Southern California (USC) in Los Angeles where he was named to Beta Gamma Sigma, the highest honor of the USC School of Business. According to his family, his entrepreneurial spirit led him to much success as the founder and

CEO of various enterprises, most significantly as a pioneer in the mini computer industry with the establishment of MDB Systems in Orange, Calif., and Phoenix International.

In recent years, Deacon turned over day-to-day operations of Phoenix International to his son, Amos Deacon III, so he could start military light vehicle manufacturer All Terrain Vehicle (ATV) Corp. in Orange, Calif. ATV and Phoenix International were at the same location, one behind the other. For many years, Deacon was a fixture in the Phoenix International booth at military and aerospace embedded computing shows around the country. He could talk chapter-and-verse about ruggedized data storage systems that were his company's stock in trade, yet had an eye for the big picture in the embedded computing business.

I remember visiting Deacon at an electronics show in the mid '90s, as the U.S. defense industry was nosing over after the end of the Reagan military buildup of the 1980s. Although he could recite the established public relations line with the best of them, he gave me the straight scoop.

"What's the buzz at the show," I asked him. After an appropriate pause he gave me a knowing smile, looked over his glasses, and said, "John, there is no buzz." Indeed there

wasn't buzz at that show, despite all my efforts to find some.

What stays in my mind most about Amos Deacon Jr. was a phone call I had with him a month or two before the Twin Towers terrorist attack on 9/11. My dad had been to Africa where he was stricken with a paralyzing disease. I spent several agonizing days in Atlanta waiting for a long-delayed commercial flight from Johannesburg that brought my paralyzed father and exhausted mother back to the U.S. I arranged for an air ambulance to get him from Atlanta to Los Angeles where UCLA Medical Center was waiting for him. I left Atlanta on a commercial flight, and arrived in L.A. at about 3 a.m. to meet my dad, mom, and sister at UCLA.

There was little, if any, sleep that night, and I needed to speak to Deacon that morning on other business. The stress and lack of sleep must have come through in my voice when I spoke to him from the waiting room at UCLA Medical Center.

He asked me what was wrong and I explained the story. Knowing that he was just one county away from me in Southern California, he didn't hesitate. "John, if you need anything... and I mean ANYTHING... you call ME." I never forgot that, and I never will. Amos Deacon Jr. was a good man. I know we'll miss him. **J**

IN BRIEF

GE Intelligent Platforms to be renamed Abaco Systems

Embedded computing specialist GE Intelligent Platforms is changing its name to Abaco Systems as a result of the company's acquisition last September by New York-based private equity firm Veritas Capital. Re-branding the company's embedded computing products and systems to the Abaco Systems name begins immediately, as company officials work to close the acquisition and transfer ownership from General Electric Co. to Veritas Capital. General Electric officials announced in September that they are selling the General Electric embedded computing business based in Huntsville, Ala., known as GE Intelligent Platforms, to Veritas Capital. The embedded systems business has been part of GE largely since 2006 when GE acquired leading embedded computing companies Radstone Technology PLC and SBS Technologies. Earlier GE had acquired embedded computing companies VMIC in 2001 and RAMiX in 2003. **I**

FOR MORE INFORMATION visit **GE Intelligent Platforms** online at www.geautomation.com, or **Veritas Capital** at www.veritascapital.com.

Marines choose SAIC and BAE Systems to develop new amphibious armored combat vehicle

BY JOHN KELLER

QUANTICO, Va. — U.S. Marine Corps amphibious warfare experts are choosing BAE Systems and Science Applications International Corp. (SAIC) to develop advanced versions of a new amphibious armored combat vehicle and accompanying electronics to replace an aging fleet of amphibious assault vehicles (AAVs).

Officials of the Marine Corps Systems Command at Quantico Marine Base, Va., announced contracts to SAIC and BAE Systems to build 13 advanced prototypes of Amphibious Combat Vehicles (ACVs) in a program called ACV 1.1. The Marines will choose one of these companies in 2018 for full-scale ACV production.

The ACV will be a wheeled armored combat vehicle able to move Marine infantry warfighters from ships offshore to fight their way onto invasion beaches. Marine Corps leaders have reasonable costs in mind for the ACV project after having cancelled the expensive expeditionary fighting vehicle (EFV) program in 2011.

Both companies are basing their ACV designs on foreign-built armored personnel carriers. BAE Systems is basing its ACV design on the Superav 8x8 amphibious armored personnel carrier developed by the Italian company Iveco Defence Ve-



SAIC is basing its ACV design on the Terrex 8X8 armored personnel carrier, above, from ST Engineering in Singapore.

hicles. SAIC, meanwhile, is basing its ACV design on the Terrex 8X8 armored personnel carrier from ST Engineering in Singapore.

The BAE Systems contract is for \$121.5 million, while the SAIC contract is for \$103.8 million. Each contract has options to build three additional Amphibious Combat Vehicles that include different configurations and weapons systems for separate missions.

Each contract has options to build 60 low-rate initial production vehicles and 148 full-rate production vehicles.

Companies that competed for the ACV contracts but that were not selected include General Dynamics Corp. and Lockheed Martin Corp. It wouldn't be a surprise to see General Dynamics or Lockheed Mar-

CONTINUED ON PAGE 4 **I**

MARINES CONTINUED FROM PAGE 3
tin protest the contracts to SAIC and BAE Systems.


The BAE Systems and SAIC teams are building ACV systems able to operate through enemy direct fire, indirect fire, and land mines with low-profile visual and infrared signatures, modular protection, and other armored vehicle technologies.

The vehicles will be able to swim to shore from as far as 12 miles out to sea, switch from operating in the water to ground operations without pause, and then maneuver with M1 Abrams main battle tanks in a mechanized task force. The ACV will be able to destroy relatively light enemy combat vehicles similar to itself.

The ACV will provide direct fire support for Marine infantry, and will be able to carry 17 Marines at speeds of at least eight knots at sea amid three-foot waves with waves as large as three feet.

On shore, the ACV will have high-ground clearance and a V-shaped hull to resist the effects of land mine blasts, and will be able to operate with a wheel blown off.

Each ACV will have a crew of three and an M2 .50-caliber machine gun in a remote weapons station, with the potential to install a stabilized dual-mount M2/Mark 19 grenade launcher turret.

On these contracts, SAIC will do its work in Charleston, S.C., and BAE Systems will do its work in York, Pa. Both companies should be finished by September 2017. 

FOR MORE INFORMATION visit SAIC online at www.saic.com, BAE Systems at www.baesystems.com, or Marine Corps Systems Command at www.marcorsyscom.marines.mil.

COTS components on the rise in communications and surveillance

BY JOHN KELLER

MOUNTAIN VIEW, Calif. — Use of commercial off-the-shelf (COTS)-based computing, data storage, security, networking, and collaboration tools is accelerating in U.S. Department of Defense (DOD) command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) applications, market analysts say.



Spending for COTS components in military C4ISR will increase over the next five years, analysts predict.

Spending for COTS components in military C4ISR will increase over the next five years, despite a flat market for military C4ISR applications overall, say analysts at market researcher Frost & Sullivan in Mountain View, Calif.

Cloud computing and big-data technologies will complement COTS-based smartphones, tablets, wireless networks, and productivity applications of all kinds through 2020.

The DOD's appetite for cloud computing as an enterprise network service will grow dramatically, despite lingering security concerns, analysts say.

A total of \$39.54 billion has been earmarked for 2016 DOD programs for C4ISR, electronic war-

fare, and information operations, as well as multipurpose technologies, Frost & Sullivan experts say. This is an increase of 8.8 percent from 2015. C4ISR spending will continue to grow at a compound annual growth rate of 1.4 percent during 2014 through 2020.

"Sharp procurement spikes without significant corresponding research reductions for ballistic missile defense, unmanned vehicles, and satellites resulted in a substantial uptick in requested 2016 C4ISR spending," says Brad Curran, Frost & Sullivan aerospace & defense senior industry analyst.

Combat systems integration, collaborative targeting, and improved surface ship self-defense are priorities for the U.S. DOD through 2020, analysts say.

"With C4ISR products and services likely to experience price and technology upgrade pressure from commercial process control, imagery, IT, as well as energy and power industries, market participants must quickly revise their strategies for success," Curran says. "Additionally, adequate emphasis on maintenance, spares, logistics, and training services will be essential for new sales."

In 2014, the top 10 firms held 40.9 percent of U.S. DOD C4ISR contract value. Future growth rates and margins will depend on the extent to which they adapt to emerging market requirements. 

FOR MORE INFORMATION visit Frost & Sullivan online at www.frost.com.

Cyber security expands to meet demands

Defensive and offensive cyber warfare capabilities are growing to meet dangerous new cyber threats from national adversaries and shadowy terrorist groups, as military command structure evolves to meet tomorrow's cyber challenges.

BY J.R. Wilson

Cyber not only is the global fifth domain of war, but it also is the newest and most difficult to define, track, keep ahead of, or defend against, as well as the easiest to enter. All this

makes crafting strategies and developing enabling technologies infinitely more difficult for next-generation cyber warfare than doing the same for the air, land, sea, and space domains.

The Strategic Information and Operations Center, the FBI's global watch and communications center, provides a platform for cyber security decision-making and the ability to synthesize intelligence.

Cyber's pervasiveness across air, land, sea, and space warfare elevates it to a level of discussion, development, threat, and counter-threat previously unseen in military and law enforcement planning. For the past 15 years, virtually every military, government, and industry entity has created dedicated cyber commands,



Members of the Vermont National Guard conduct a cyber security exercise for cyber defenders with a fellow Red Cell team member during a 2014 Cyber Shield exercise in Arkansas.

subcommands, offices, agencies, units, and departments — mandated by the inexorable digitization of every aspect of life on Earth.

“Beyond impacting data, systems, and networks, adversarial operations in the fifth domain have the potential to negatively affect operations in the other four domains,” notes Troy Johnson, director of the U.S. Navy Cybersecurity Division. “As a result, the Navy is committed to improving its cyber security. Toward this end, the Navy established Task Force Cyber Awakening [TFCA] in 2014 to improve cyber security after its network was compromised the previous year. The mission of the task force was to take a comprehensive look at the Navy’s cyber security and make changes to improve its defenses.

“TFCA established priorities for protecting the Navy based on recommendations from industry, the cyber security community, and stakeholders. Using these priorities, the task force evaluated hundreds of funding requests for addressing vulnerabilities, which resulted in \$300

million being set aside in 2016 for solutions that strengthened the Navy’s defenses and improved awareness of its cyber security posture.”

The Navy Cybersecurity Division was created by the Chief of Naval Operations in September 2015 to continue the transformation started by TFCA. The new division oversees the Navy’s approach to cyber security by developing strategy, ensuring compliance with cyber security policy, and advocating for cyber security requirements. One TFCA-identified funding priority is for control points that allow the Navy to isolate portions of the network after a breach is detected. Johnson compares it to watertight compartments on a ship, with cyber control points allowing the Navy to limit the impact of a compromise and keep adversaries from moving to other targets in the network.

Limiting connectivity

“These control points will also allow the Navy to selectively limit connectivity for parts of the network if increased cyber activity from

adversaries is expected, similar to how ships set different material conditions of readiness,” Johnson adds.

“The task force also formed a Navy-wide group to implement the CYBERSAFE Program, which is modeled after SUBSAFE, the rigorous submarine safety program begun after the loss of the Permit-class fast-attack submarine USS Thresher in 1963.

“CYBERSAFE will harden a critical subset of warfighting components, which could be certain computer systems or parts of the network. [It also] will apply more stringent requirements to these components before and after fielding to ensure they can better withstand attempted compromises. CYBERSAFE will also require changes in crew proficiency and culture to implement these requirements.”

The Navy also maintains technical solutions alone cannot provide complete protection. Key contributors to naval defense in the future include the cyber security, professional and general workforce.

“I still use the term ‘defense-in-depth’ — there is no single technology that provides holistic defense-in-depth,” says Ralph Havens, president of Infoblox Federal. “Infoblox specifically addresses DNS [Domain Name System] security on the network, that known hole where information can provide internal and external threat detection and prevention on that service as part of a much larger defense-in-depth effort on your network.

“Is the global enterprise more at risk tomorrow than it was yesterday? Certainly. With the evolution of our military capabilities, the pervasiveness of global growth has opened up the number of entry points. The more bandwidth, devices, and

