NOVEMBER 2013

Military & Aerospace Electronics

ENABLING TECHNOLOGIES FOR NATIONAL DEFENSE

Secure cloud computing

Software tools aim for improvements in cost and efficiency. PAGE 20

Wearable computing

Commercial technology complicates Army plans for battlefield wearables. PAGE 28

militaryaerospace.com

Controlling unmanned vehicles

Designers eye common operating picture for drone command and control.

PAGE 12

PennWell

SWaP THIS!

TWO FULLY INDEPENDENT SYSTEMS IN ONE ULTRA-RUGGED BOX

NSA APPROVED SECURE ARCHITECTURE

SB1002-MD "GOLDEN EYES" FEATURES

TWO FULLY INDEPENDENT SYSTEMS (RED/BLACK) EACH WITH:

- *Up to 2.4GHz Quad Core i7 Haswell® processor w/ 6MB of L2 Cache*
- *Up to 32GB of 1600MHz DDR-3 memory with ECC*
- *Up to 512GB of sealed removable SSD drives*
- *Up to 512GB of fixed SSD for OS boot*
- *Two SAM™ sites for custom I/O (Wi-Fi/BT and GPS)*
- *Seven Gigabit Ethernet ports with TCP/IP Offloading Engine (TOE)*
- *Six USB 2.0 ports and two Serial Ports with RS-232/422/485 options*
- *Trusted Platform Module (TPM) and Trusted Execution Technology (TXT)*
- *Supports Intel Virtualization Technology (VT-x/VT-D2) for best performance*
- *Tamper proof hardware w/optional Secure Erase monitoring w/ status LED indicators*

• *Ultra-low SWaP only 5.4" x 6.5" x 2.75" @ 3.5 lbs. and as low as 60W total*

• *Operates from -40° C to +85° C without throttling CPU speed*

Many other standard configurations as well as custom builds available.

AS9100 REGISTERED FIRM

TRUSTED COMPUTING GROUP

PICMG

MEMBER VITA

All Rugged products are fully-sealed and Extended temp -40°C to +85°C. Compliant to MIL-STD-810F, 1275, 202, 901D, DO-160D and IP67. All GMS products are proudly designed and manufactured in the U.S.A. and are fully ITAR compliant. © 2013, General Micro Systems, Inc.

GMS COMPUTING ENGINES

GENERAL MICRO SYSTEMS, INC.

Powering the Embedded Market Since 1979

800-307-4863 gms4sbc.com

kontron

» Transforming the Landscape of Military Supercomputing «

High Performance Embedded Computing - From the IT Data Center to the Battlefield

» Mainstream IT Technology
» Balanced I/O and CPU power
» 3rd generation Intel® Core™ processors
» Delivers up to 10x more I/O data bandwith in a small footprint

StarVX

Get more information at:
kontron.com/starvx

Call: 1-888-294-4558 • info@us.kontron.com • kontron.com/starvx

The pulse of innovation

FORUM AEROSPACE INNOVATION

MONTRÉAL 2013 QC·CANADA

DECEMBER 2·3·4

Palais des congrès de Montréal

ORGANIZED BY AÉRO MONTRÉAL

IN COLLABORATION WITH CRIAQ

INNOVATION POWERS SUSTAINABILITY FOR THE AEROSPACE INDUSTRY

AS DESIGN, AS MANUFACTURED, AS USED, AS DISPOSED

DON'T MISS THE 4th EDITION OF THIS MAJOR INTERNATIONAL EVENT

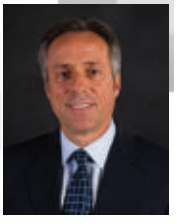
Taking place in Montréal, Québec, Canada

1,000 participants

200 companies from more than 15 countries

Learn about the vision of world leaders and dicover the most recent technological trends in the industry.

COME AND MEET 60 WORLD-CLASS SPEAKERS



GUY HACHEY
President & Chief Operating Officer,
Bombardier Aerospace

YANN BARBAUX
Chief Innovation Officer,
Airbus

PIERRE GUILLAUME
Chief Technology Officer,
SNECMA

DAVE WILLIAMS
Vice President Procurement,
Airbus Americas

ALAN EPSTEIN
Vice President, Technology and Environment,
Pratt & Whitney

DAVE CARTER
Vice President, Engineering and Technology,
UTC Aerospace Systems

AMY L. GOWDER
Vice President & General Manager,
Kelly Aviation Centers,
Lockheed Martin

SERGE BÉRENGER
Vice President, Strategy, Research and Technology
Safran Power / Hispano Suiza

RAPHAËL DUFLOS
Vice President and Chief Procurement Officer
Aerolia (EADS)

AN EXCEPTIONAL THREE-DAY PROGRAM :

- B2B technology meetings
- Networking events
- Conferences and workshops
- Technology Trade Show
- Industrial visits program

To register, visit : aeromontreal.ca/2013forum

PARTNERS

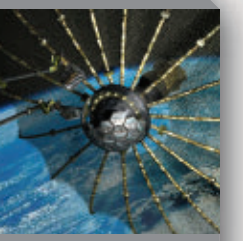
CGI EADS Bell Helicopter A Textron Company BOMBARDIER the evolution of mobility ÉTS Le génie pour l'industrie

HÉROUX DEVTEK Pratt & Whitney Canada A United Technologies Company POLYTECHNIQUE MONTRÉAL LE GÉNIE EN PREMIÈRE CLASSE NSERC CRSNG

McGill SAFRAN AEROSPACE · DEFENCE · SECURITY

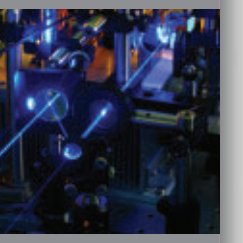
NOVEMBER 2013
VOL. 24, NO. 11

Military & Aerospace Electronics



COVER STORY

Image: Lockheed Martin



MILITARY & AEROSPACE ELECTRONICS ©2013 (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. 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**

BY **JOHN KELLER**, EDITOR IN CHIEF

The Army's future mission is vague, leaving industry with little direction

A variety of factors are gathering into a potential perfect storm that could threaten the U.S. Army's future mission, the continuing relevance of the oldest American military service, and how the defense industry can move forward to support the Army's needs.

Some of these factors are well-known: sequestration, dim prospects for budget growth, and substantial technology research and development that for most practical purposes has come nearly to a dead-stop.

Perhaps most serious, however, is how top military and civilian leadership define the Army's role moving into the future, the top threats the Army will evolve to meet, and the very relevance of a large standing Army in an era when large-scale, big-iron military land battles appear to be part of the past.

Here's where we are today: U.S. military forces are finishing their exit from Iraq, where they have operated for more than a decade. Their final exit from Afghanistan is but a few years off, or less. When operations on Southwest Asia are completed, where does the Army go from there?

The Army has had a clear set of missions since the U.S. entered World War II in 1941. Although the close of the Second World War in 1945 saw a rapid drawdown in U.S. military power, the strengthening Soviet Union was on everyone's mind.

Less than five years after World War II ended, North Korea invaded South Korea, which created another sudden and dire mission for the Army. That mission grew from containing North Korean forces to containing Communism around the world, which continued until the fall of the Berlin Wall in 1990. One year later, Iraq invaded Kuwait, which gave rise to Operation Desert Shield, and eventually the military ouster of Iraqi forces from Kuwait in Operation Desert Storm, in which the Army played a central role.

For the next decade, keeping an eye on a contained-but-restless Iraqi military, on ethnic strife in what then was Yugoslavia, and on other simmering hot spots throughout the world held the Army's attention and helped define its mission.

Today things are different. Counter-insurgency operations are nearing an end in Iraq and Afghanistan, Russia does not pose the immediate military threat that did its predecessors of the Soviet Union, and Europe has been relatively quiet.

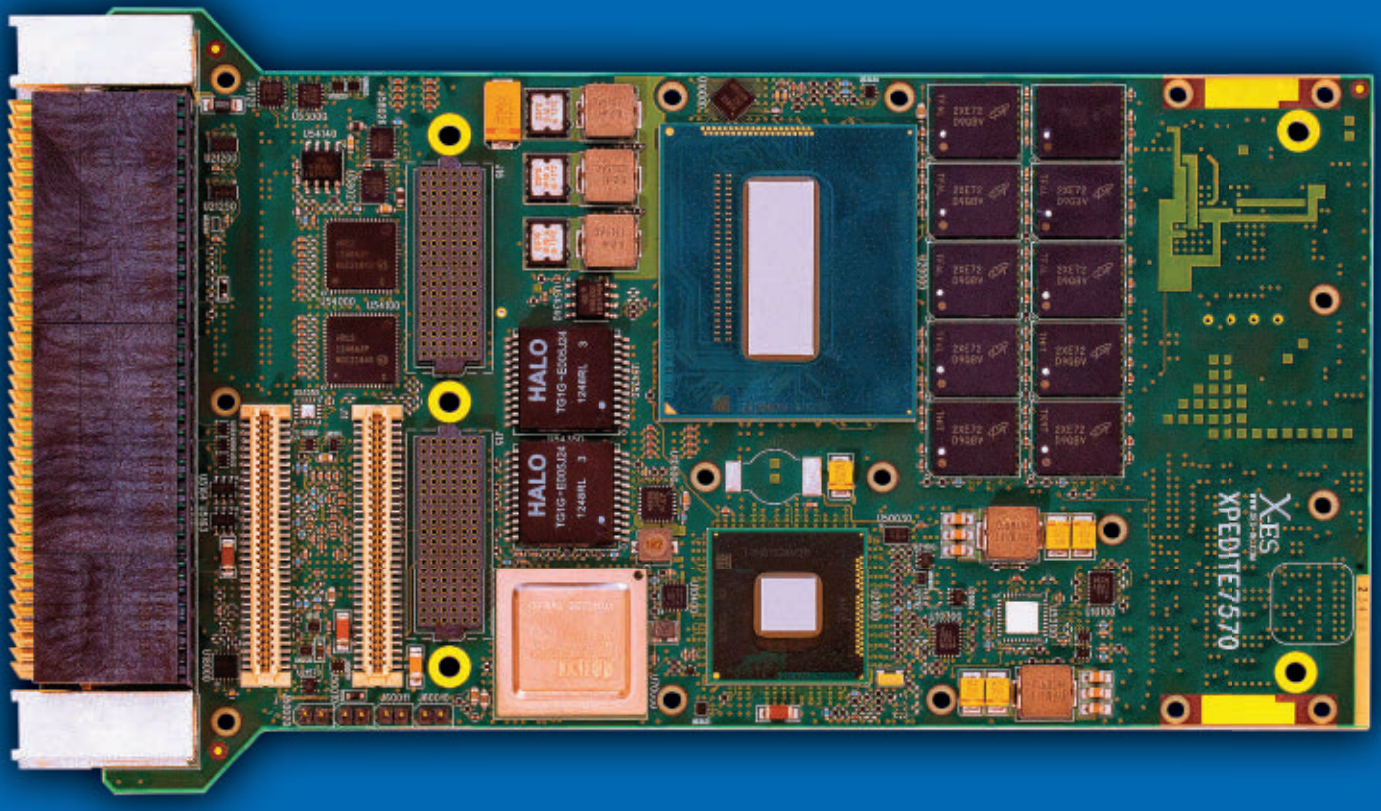
Still, trouble spots persist in areas like Syria and Iran, but with no open conflict yet involving U.S. Army forces. There is no immediate and dire threat in these areas, and hence no clear Army mission—at least not yet.

So how does the Army move forward? Counter-insurgency, certainly. Special Forces capability, of course. But what's the role of the large Army infrastructure involving large combat infantry units, main battle tanks, armored fighting vehicles, and other organizations designed for large ground conflicts?

I'm not sure there is a role, and I'm not convinced that the top Army leadership today knows what its role in the future will be, either. Maybe the Army is at a moment of transition, and leaders will get a handle on the Army's core mission sometime soon. With the civilian leadership vacuum we have in Washington, I'm not sure the Army will be able to do so. If Army leaders are unable to define the Army's long-term mission clearly, then the defense industry will have no idea how to proceed, other than to guess.

These factors were on display just below the surface last month at the Association of the U.S. Army (AUSA). What was striking in exhibits was a lack of direction in where we go from here. It was as though the industry were pointing out to the Army officers walking the aisles how far technology has led us to this moment, yet pleading for direction on where the industry should go from here.

4th Generation Intel® Core™ i7 from X-ES



VPX · cPCI · VME · XMC · COM Express · Custom

High-performance, rugged, and versatile 4th Generation Intel® Core™ i7 solutions from X-ES

X-ES

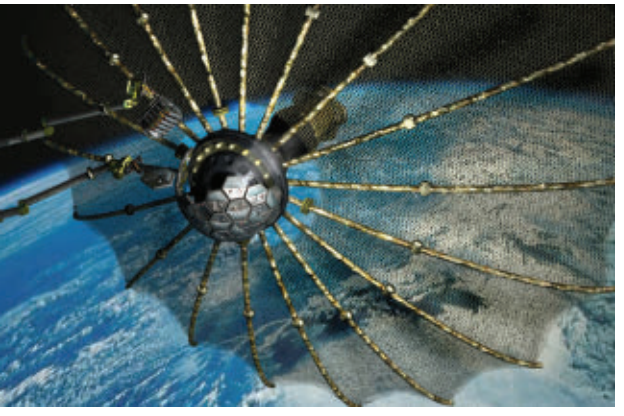
Extreme Engineering Solutions
608.833.1155 www.xes-inc.com

100% Designed, manufactured, and supported in the USA

Space scientists at NovaWurks to help DARPA reuse parts from orbiting dead satellites

BY JOHN KELLER

ARLINGTON, Va.—U.S. military researchers are looking to designers at NovaWurks, Inc. in Los Alamitos Calif., for advanced work in a project to reuse satellite antennas, apertures, and other components from decommissioned satellites.



NovaWurks will help DARPA with a project to reuse antennas, apertures, and other components from decommissioned satellites.

Spacecraft experts at the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., have awarded a potential $42.6 million contract for the second and third phases of the Phoenix program, which seeks to use still-good components from dead satellites parked in high-Earth orbit for building new satellites robotically while in orbit to reduce the costs of replacing failed satellites.

The contract has a base value $30.8 million, and four options collectively worth nearly $11.9 million.

NovaWurks won a $2.9 million contract for the first phase of the DARPA Phoenix program in early 2012. Also working on Phoenix phase 1 were experts at MacDonald, Dettwiler and Associates Ltd. in Richmond, British Columbia.

Phoenix seeks to demonstrate around-the-clock, globally persistent communication capability for warfighters more economically by robotically removing and re-using GEO-based space apertures and antennas from de-commissioned satellites in the graveyard or disposal orbit.

DARPA is asking NovaWurks to develop an integrated proximity awareness system (IPAS), rendezvous and proximity operations (RPO) technology suite, synergistic number of degrees of freedom (N-DOF) test facility support, virtual ground station operations, and payload orbital delivery system (PODS)-hosted launch.

The company vision of NovaWurks is to provide access to the exploration of space for everyone—not just space agencies, the govern-

CONTINUED ON PAGE 8 ➔

IN BRIEF

Crane Microwave to maintain B-1 electronic warfare components in $12.4 million contract

Electronic warfare (EW) experts at Crane Electronics Microwave Solutions in Chandler, Ariz., will maintain several kinds of electronic components and subassemblies in the AN/ALQ-161A defensive avionics system aboard the U.S. Air Force B-1B Lancer strategic jet bomber under terms of new $12.4 million contract. Officials of the Air Force Targeting & Electronic Warfare office at Robins Air Force Base, Ga., are asking Crane engineers to provide depot-level maintenance of nine shop-replaceable units in the ALQ-161A radio-frequency surveillance and electronic countermeasures (RFS/ECM) system on the B-1 bomber military aircraft. Crane staff will maintain ALQ-161A yttrium iron garnet (YIG) reject filters with drivers; YIG band pass filters; and digitally tuned oscillators. The AN/ALQ-161A Defensive Avionics System on the B-1B bomber identifies, acquires, and denies enemy radars and missiles. Built by AIL Systems Inc., the AN/ALQ-161A is an integrated RF countermeasures system. ←

POWER YOUR CRITICAL MISSION

A Full Range of Proven DC-DC Power Converters, EMI Filters and Accessories

Avionics & Military Features

- 1-120+ watts
- MIL-PRF-38534 Class H and Class K
- 100% hermetic
- -55°C to +125°C
- DLA SMDs available

Hi-Rel COTS Features

- 5-200+ watts
- Six-sided metal or potted packaging
- Rugged environmental screening
- -55°C to +100°C

Space Series

- 5-120+ watts
- Developed for TOR compliance
- TID: 100 krad (Si)
- SEE: 85 MeV
- -55°C to +125°C
- MIL-PRF-38534 Class H and Class K
- DLA SMDs available
- Engineering models typically ship from stock
- Other radiation levels and custom versions available

VPT

Power Your Critical Mission Today

www.vptpower.com

EFFICIENT & RELIABLE | 20 YEAR PROVEN HERITAGE | CERTIFIED QUALITY | SHIPS FROM STOCK

DARPA CONTINUED FROM PAGE 6

ment, or the military. The company seeks to enable the individual to capture instant, unaltered, affordable images of any location on the Earth at any time.

Through Phoenix, DARPA seeks to speed deployment of emerging technologies into on-orbit space systems at much lower cost than is possible today, DARPA officials say.

In the first phase of the Phoenix program, NovaWurks experts designed different tools for on-orbit salvage of satellite subsystems, and a prototype tool for ground tests together with Front End Robotics Enabling Near-term Demonstrations (FREND) robotic arm.

In the second phase, company experts will design an on-orbit salvage tool, as well as software for integration with the FREND control computer. The third phase calls for NovaWurks to deliver hardware and software for integration with the FREND arm and control computer.

The idea behind Phoenix is that building new satellites robotically in orbit using recycled components would be much less expensive than simply junking failed satellites, and building and launching new ones from scratch.

These satellites would operate in geosynchronous orbit, which matches the speed of the Earth's rotation and makes them operate in one spot above the planet's surface. Stationary orbits are extremely high, and repairing or retrieving failing spacecraft at these distances today is nearly impossible.

Government experts have established a graveyard orbit high above the Earth's surface for disposing of decommissioned spacecraft where they pose little risk of colliding with functioning satellites. The graveyard orbit is necessary because deorbiting these high-altitude satellites is dangerous and expensive.

Until now, the graveyard orbit has been a celestial junkyard filled with decommissioned satellites of no use to anyone. Even though they no longer function, however, these junked satellites often still have useful components like antennas and sensors.

DARPA officials want NovaWurks to develop technology able to launch orbiting robots that can salvage still-useful satellite components from the graveyard orbit and use them to build new satellites. Spacecraft in geosynchronous orbit are particularly useful for military and civil communications and persistent surveillance.

A previous DARPA solicitation requested industry proposals for satlets, a payload orbital delivery system (PODS) to orbit satlets quickly, and a separate on-orbit satellite servicing spacecraft with grasping mechanical arms and robotic tools to salvage spacecraft components and construct new satellites.

FOR MORE INFORMATION
visit **NovaWurks** online at *www.novawurks.com*, or **DARPA** at *www.darpa.mil*.

Slide show shows the evolution of the American soldier from beginning to future

SLIDE SHOW—The American soldier has come a long way since the beginning of the Republic 237 years ago. While uniforms for early soldiers were based on cost and utility, soldiers' clothing eventually considered ballistic protection, increasing storage space, protection from poison gas and other contaminants.

Today designers of soldier systems are considering future uniforms with wearable communications and displays, embedded computing, air-conditioned armor, and a variety of eye and skin protection.

Take a look at the evolution of the American soldier from the cocked hat and Brown Bess musket to head-mounted displays and superhero-like exoskeletons.

The Evolution of the American soldier slide show is on the *Military & Aerospace Electronics* website at www.militaryaerospace.com/articles/slideshow/2013/10/evolution-of-the-american-soldier.html.

This future Special Forces battle suit is only one part of the evolution of the American soldier depicted in the accompanying online slide show.

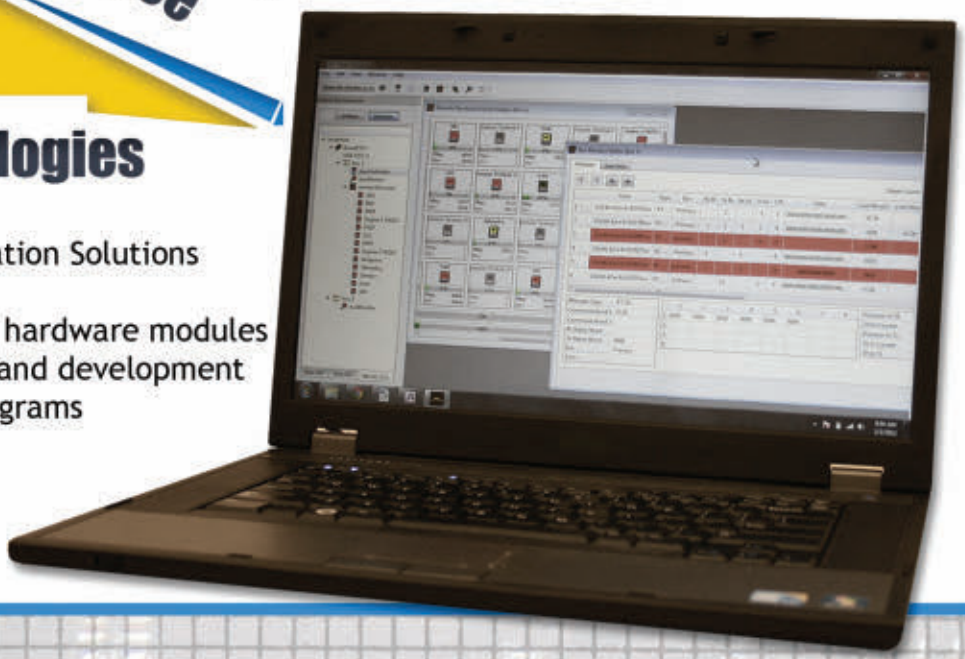
www.aviftech.com/software

Avionics Interface Technologies

TODAY'S SOLUTIONS
FOR TOMORROW'S DEMANDS

Complete Test & Simulation Solutions

Incorporating advanced hardware modules with intuitive software and development support for avionics programs



SOFTWARE TOOLS
Simple, Intuitive, & Effective

Flight Simulyzer™ Analyzer/Simulator software for MIL-STD-1553, ARINC 429, & ARINC 664

fcXplorer™ Analyzer/Simulator software for Fibre Channel & HS1760/MIL-STD-1760E

TEST INSTRUMENTATION

CUSTOM IP SOLUTIONS

RUGGED COTS MODULES

sales@aviftech.com

+1 402.763.9644


Reduce the clutter.
Print.
Works.
Recall the image.
Make your brand the one they remember.
Advertising works. After all, you're reading this. Print ads engage us in a focused, visual medium, making your brand and message easy to recall.
Keep your company's visibility where attention span is longer than a nanosecond. Then combine it with an online presence to maximize your market reach with the biggest impact you can.
Print Advertising works.
Print+Online
Photonics Consortium. Helping Photonics Companies Grow.

Lockheed Martin to upgrade communications software on Navy missile and attack submarines

BY JOHN KELLER

SAN DIEGO—U.S. Navy submarine communications experts needed a contractor to develop and maintain a common integrated communications architecture for voice and data communications systems aboard U.S. Navy fast-attack and ballistic-missile submarines. They found their solution from the Lockheed Martin Corp. Mission Systems & Training segment in San Diego.

Officials of the Space and Naval Warfare Systems Command (SPAWAR) in San Diego awarded a $12.7 million contract to Lockheed Martin for the Design and Maintenance of Common Submarine Radio Room (CSRR) Control and Management (C&M) Software program.

The Navy developed the CSRR as a replacement for the existing Ohio Class submarine Integrated Radio Room (IRR), and has installed CSRR equipment aboard Ohio-class ballistic-missile submarines, as well as on Virginia-, Seawolf-, and Los Angeles-class fast-attack submarines.

The CSRR integrates components of the Navy's Automated Digital Network System (ADNS), Digital Modular Radio (DMR), Extremely High Frequency/Follow-On Terminal (EHF/FOT), Global Broadcast Service (GBS), Super High Frequency (SHF), Submarine Single Messaging System (SubSMS), and ancillary equipment into a common architecture.

The system's control and management software manages these components to control, process, and disseminate command, control communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) information to provide the submarine fleet with secure and covert communications.

The technical approach to this effort is based on a common open-systems architecture, common software, common technical documentation, and one software support activity (SSA).

FOR MORE INFORMATION visit *www.lockheedmartin.com/us/mst.*

Flexible & integrated unmanned command & control

Unmanned vehicle technology advances deliver a common operating picture for enhanced decision-making and mission effectiveness.

BY **Courtney E. Howard**

The use of unmanned vehicles in aerospace and defense applications continues to grow, as militaries the world over seek to reap the benefits of unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and unmanned underwater vehicles (UUVs). The rapid advancement of key enabling technologies has helped to expand not only the use of unmanned vehicles, but also their role in the field.

UAVs continue to be the most dynamic growth sector of the world aerospace industry this decade, according to Teal Group market analysts in Fairfax, Va. Teal Group staff predict UAV spending to more than double over the next decade—from current worldwide UAV expenditures of $5.2 billion annually to $11.6 billion—amounting to more than $89 billion in the next 10 years.

Militaries are demanding not only more, but also more-capable unmanned vehicles and sophisticated command and control (C2) functionality.

Operation

Unmanned vehicle operators are amassing a growing list of desired features and characteristics, many of which center on ease of use and the ability to reduce operator workload.

"More sophisticated [unmanned vehicles] have built-in control and/or guidance systems to perform low-level human pilot duties, such as speed and flight path surveillance, and simple pre-scripted navigation functions," says Donald Palmer, chief technology officer at General Micro Systems (GMS) in Rancho Cucamonga, Calif. In addition to sophistication, unmanned vehicle customers seek security.

Unmanned system security is a high priority in aerospace and defense applications. "Secure communication links are vital for UAV operation, both to control the UAV based on mission objectives and to deliver data reliably to mission controllers on the ground. Encryption and decryption are inherent requirements, adding complexity and cost in the electronics," Palmer says.

"Most prominent and widely debated issues are associated with control compatibility with other UAV ground stations," says Val Zarov, director of program management at Curtiss-Wright Controls Defense Solutions in Ashburn, Va. "From a technology trend perspective, there is a significant movement toward utilization of open-architecture hardware and software. Advances in these areas will enable more generic/open-source ground command-and-control stations while protecting highly sensitive/classified data from unauthorized access."

Communications & security

AAI Corp. in Hunt Valley, Md., and ViaSat Inc. partnered to align AAI's advanced unmanned aircraft and C2 technologies with ViaSat integrated airborne and terrestrial satellite communications, as well as its Internet Protocol-based networking and security technology. AAI and ViaSat will work together to develop and advance beyond-line-of-sight (BLOS) satellite communications capabilities for current and next-generation AAI UAVs.

"The performance and affordability of tactical UAVs like our Shadow system make them an invaluable battlefield asset with a growing mission spectrum," says Steven Reid, senior vice president and general manager of AAI Unmanned Aircraft Systems. "Our private satellite network services can deliver the dedicated bandwidth needed to distribute tactical UAV video throughout the battlespace," says Paul Baca, vice president and general manager for ViaSat Global Mobile Broadband.

Interoperability

Aerospace and defense officials increasingly seek solutions to do more with less, such as operating several unmanned vehicles with one operator and one C2 system. Managing several drones is a unique challenge because each UAV type has proprietary control systems, says Nelson Paez, CEO of DreamHammer in Santa Monica, Calif. DreamHammer's commercial off-the-shelf (COTS) intelligent control device was designed to integrate unrelated unmanned vehicles from different manufacturers into one system.

"Ballista allows government or commercial customers to link together machines from numerous developers performing a variety of tasks," Paez says. "Some unmanned systems take as many as 200 people to manage one drone; Ballista enables one user to manage several drones simultaneously. Until now, there has been no way to tie [UAVs] together. A user who previously required extensive training to manage one drone or robot can now manage several drones or robots simultaneously—all to achieve one task or coordinated mission."

DreamHammer's Ballista COTS software works with all unmanned drones and robots and can be used to link several drones into one master system controlled by one person. Ballista, built on an open software platform, enables the autonomous and simultaneous control of several

The Lockheed Martin mobile Ground Control Station (mGCS) serves as the user interface for controlling and monitoring mini and small unmanned vehicle systems.

unmanned vehicles across all domains—space, air, sea, and land—and can be run from virtually any computer, including a tablet or smartphone. Radisys engineers, working with an aerospace and defense systems integrator, developed a universal ground-control system for UAVs built on Radisys ATCA technology. "Until recently, every type of unmanned aircraft had a specialized ground control station, as well as a unique version for each military branch, resulting in a proliferation of single-purpose equipment," says Jeff Sharpe, senior product line manager at Radisys in Hillsboro, Ore. "The integrator decided to develop a universal ground control station (UGCS) to satisfy U.S. joint services requirements, including simultaneous mission control of several unmanned aircraft." The UGCS architecture uses Radisys standards-based ATCA solutions, replicating the capabilities of its rackmount server with one ATCA blade, the Radisys ATCA-4300 compute processing module. Radisys engineers performed platform integration and thermal testing, and the integrator minimized up-front engineering costs by starting with a validated ATCA platform populated with available COTS components.

Many missions

The Hermes UGCS from Elbit Systems in Haifa, Israel, can control two concurrent missions when allocated two ground data terminals. Elbit engineers built the Hermes UGCS to enable the control of any type of UAV. The UGCS features side-by-side identical and redundant operator consoles with ruggedized COTS hardware and commercial software tools for mission planning, management, and control.

Piaggio Aero Industries in Italy

tested complete ground handling control of the company's new Piaggio Aero P.1HH HammerHead multirole UAV and mission management system (MMS) based on Selex ES Sky-ISTAR technology. Selex ES provides the vehicle control and management system (VCMS), the remote-piloting ground control station (GCS), and the UAV datalink and communications systems "to ensure safe operations during all flight activities, throughout the whole chain of UAV command and control," says a representative.

"The P.1HH UAV is able to perform command and control and data exploitation for several UAVs, operations in line-of-sight (LOS) and beyond-line-of-sight (BLOS) conditions, and flexible asset usage for the pilots and ground crew."

The MMS combines with the VCMS to manage the HammerHead UAV and mission-specific equipment. HammerHead's VCMS, controlled from the GCS via an airborne datalink system, commands the aerodynamic control surfaces and manages on-board equipment with a triple-redundancy Flight Control Computer and several remote Servo Interface Units, designed to achieve a high level of safety and mission reliability.

Common control

This past summer engineers from Lockheed Martin Corp. in Bethesda, Md., monitored and controlled several types of UAVs from one integrated command and control (C2) system during a U.S. Navy demonstration in support of the Unmanned Carrier Launched Airborne Surveillance and Strike System (UCLASS) and Common Control System programs.

"Lockheed Martin's system integrated with other Navy C2 and intelligence, surveillance, and reconnaissance (ISR) planning and execution systems, providing operators with a comprehensive mission picture and enabling the control of unmanned air vehicles and their on-board mission system sensors.

"This demonstration is an important step to fulfilling the Navy's requirement for a Common Control System that leverages several architectures from varied operational systems," says Rob Weiss, executive vice president of Advanced Strike

The MACE 3 unmanned ground vehicle (UGB) from MIRA features a UGV control system with tele-operational and autonomous modes.

and Intelligence and Reconnaissance Systems for Lockheed Martin Aeronautics. "A combined C2 and ISR capability will be essential as the Navy integrates UAV into its ISR enterprise."

During the demonstration, one operator managed several UAVs simultaneously using an open architecture framework integrated with DreamHammer's Ballista drone control software and Navy-compliant software protocols. The team also used new Navy Cloud capability to demonstrate control of ISR sensors and integrate the data into a complete mission picture, which was used to rapidly re-task and re-route the UAV assets.

The demonstration "underscores the critical role that common command and control systems can play in actual operations by highlighting the ability to enrich the overall ISR picture and increase the speed of decision making," says Jim Quinn, vice president of C4ISR Systems for Lockheed Martin Information Systems and Global Solutions. "An integrated battlespace picture emerges when we link the platforms, sensors, and information collected into one enterprise view that will enable the U.S. Navy to better achieve their C2 and ISR missions."

One for all

Lockheed Martin's Universal Ground Control Station (UGCS), an extension of the One System Ground Station (OSGCS) concept, enables interoperability of the U.S. Army's unmanned assets of dissimilar types from one common ground control station. It houses flight-critical hardware and software in a modular configuration.

The Mobile Ground Control Station (MGCS) from General Atomics is a UAS control center, enclosed in a either a 24-foot shelter or 30-foot trailer, used to control one GA-ASI aircraft.

VCS-4586 software, installed in every UGCS and in OSGCS shelters, is used to command and control the MQ-1C Gray Eagle, RQ-7B Shadow, MQ-5B Hunter, and LEMV Airship for the U.S. Army. Lockheed Martin CDL Systems' open, standards-based, and COTS software has been integrated into various unmanned vehicle platforms and designed on low-cost, interoperable, and open-architecture systems.

AAI's Expeditionary Ground Control Station (EGCS) delivers command and control capabilities in a small, modular configuration that includes ruggedized workstations for the aircraft and payload operators, as well as a remote interface box and miniature ground data terminal.

Man-portable, net-centric, and built on a scalable, open architecture, AAI's EGCS enables several unmanned platforms to be employed simultaneously and provides on-the-move C2 capabilities for mission flexibility. Customers include the U.S. Navy, Air Force, and Marine Corps.

Flexible & functional

Lockheed Martin Vehicle Control Station (VCS) software is helping control UAVs, UGVs, high-speed air and sea target-drones, and loiter munitions in a variety of roles. An integrated command, control, and information system for operating and monitoring unmanned vehicle systems, VCS supports the operation of several vehicles, sensors, payloads, data links, and other subsystems from as few as one operator workstation.

VCS provides increased autonomy by automatically managing basic piloting tasks. The automation of flight tasks enables operators to focus on their main objective: the mission, says a company representative.

VCS is built on an open-architecture framework and is hardware and operating system agnostic. VCS-4586's interactive map combines insight from real-time, geo-referenced positioning and directional information of all operational components, such as vehicles, sensors, payloads, data links, and other vehicle systems.

Air, land, and sea

Engineers at Micro Systems Inc. in Fort Walton Beach, Fla., designed the company's Unmanned Vehicle Command and Control (C2) Systems to be flexible and expandable, making them well suited for ground vehicles, sea surface vehicles, aerial target drones, and UAVs.

"We have fielded command and control systems that have been supporting missions for the U.S. Navy (System for Naval Target Control), U.S. Army (Target Tracking Control System/UHF or TTCSU), and several international defense organizations worldwide," says a representative. "Every command and control system we offer is readily adapted to a variety of unmanned vehicle applications and we offer a wide array of system configurations that include different form factors (i.e., portable or fixed site), number and type of controlled vehicles, and RF data links."

Micro Systems solutions can be configured to control as many as eight air vehicles and 16 sea surface and ground vehicles, with a simultaneous mix of vehicle types, as well as field expanded with no change to system software (plug and play).

"Our command and control systems are vehicle and data link independent, capable of controlling a mix of vehicles on several independent data links simultaneously," the representative adds. Systems are available with a variety of data link options, including: UHF FM, L-Band Direct Sequence Spread Spectrum (DSSS), 2.4-gigahertz ISM, Iridium Satellite (satellite to satellite or gateway to satellite), and custom data links.

The challenge of a secure military cloud

Reliable security and efficient resource allocation are central concerns as the military moves mission-critical information to the cloud.

BY **J.R. Wilson**

With all the changes brought by a global Internet and the subsequent transition of data to digital formats across all segments of society, security challenges have grown even faster, from cyber espionage and dedicated denial of service (DDoS) to cyber warfare.

In recent years, a new approach to data storage and sharing, generically called "the cloud", has begun to grow faster than security could match. On the positive side, that has brought less expensive operations, faster updates, easier sharing; on the negative, a plethora of new security issues.

While individuals typically use public clouds—such as those provided by Amazon.com, Google, and Apple—large entities with vast amounts of data have turned to private, "secure" clouds. The most concerned users, current and future, are government agencies, especially the military.

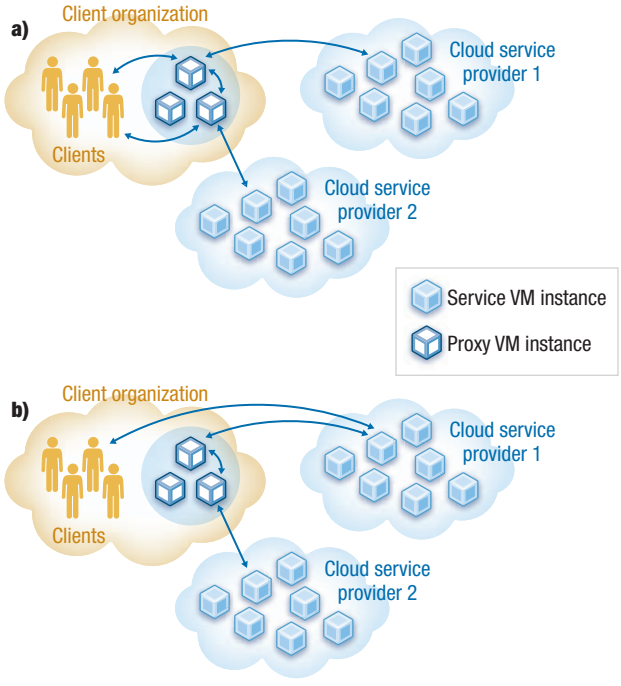


Figure 1: In the cloud computing paradigm, three layers are stacked, providing on-demand infrastructure, middleware, and software services. The cloud stack sits above the virtualization layer.

"The bulk of military data is just routine business information that is not particularly sensitive and could very easily go into a cloud that is considered commercially secure without a lot of headaches," says John Howie, chief operating officer of the Cloud Security Alliance (CSA) and a member of the IEEE Computer Society and its security-related programs. "That becomes very different when you start talking about highly classified data. There you will find some of the nature of the cloud, such as shared infrastructure, will get in the way of using current commercial cloud offerings.

"So cloud providers are building special environments for the military and others with top secret information, such as the U.S Department of Energy," Howie continues. "Those are more 'community' rather than public clouds. So you will see the government procure regular cloud offerings that meet FISA [Foreign Intelligence Surveillance Act] standards, but more specialized clouds being adopted by the military that meet an entirely different set of standards."

In February 2011, the Obama Administration issued a Federal Cloud Computing Strategy that essentially ordered federal entities—including military and intelligence services—to begin switching to cloud-based

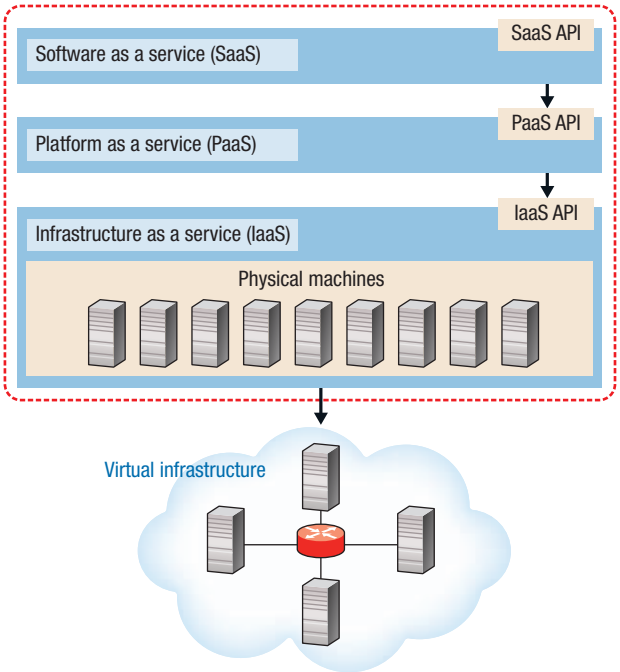


Figure 2: Conceptual cloud-based security overlay networks are composed primarily of cloud security and management units in addition to the customer network's protected endpoints. This generic architecture can be used to deploy any cloud-based security solution.

data storage and sharing. The strategy implemented a cloud first policy "intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments."

"Cloud computing has the potential to play a major part in addressing...inefficiencies and improving government service delivery. The cloud computing model can help agencies grappling with the need to provide reliable, innovative services despite a lack of resources," the new Strategy proclaimed.

"Cloud computing can be implemented using a variety of deployment models—private, community, public or a hybrid combination. Each agency will re-evaluate its technology sourcing strategy to include consideration and application of cloud computing solutions as part of the budget process."

The directive, released by U.S. Chief Information Officer Vivek Kundra, also predicted a whole-of-government shift to the cloud will accelerate an earlier effort, the Federal Data Center Consolidation Initiative,

intended to restructure the government's fragmented data center environment.

"Through the FDCCI, agencies have formulated detailed consolidation plans and technical roadmaps to eliminate a minimum of 800 data centers by 2015," the report noted. "Cloud computing can accelerate [those] efforts by reducing the number of applications hosted within government-owned data centers.

"For those that continue to be owned and operated directly by Federal agencies...environments will be more interoperable and portable, which will decrease data center consolidation and integration costs because it reduces unnecessary heterogeneity and complexity in the IT environment."

The strategy acknowledged such goals must be measured against a wide range of risk assessments, tailored by each agency according to its mission and requirements, no matter which deployment model is used. Of import to the U.S. Department of Defense (DOD) and its partners in industry and academia is adherence to Federal Information Security Management Act (FISMA) requirements, such as compliance with Federal Information Processing Standards, Authorization to Operate requirements, and monitoring and reporting vulnerability and security events.

"It is essential that the decision to apply a specific cloud computing model to support mission capability considers these requirements. Agencies have the responsibility to ensure that a safe, secure cloud solution is available to provide a prospective IT service and should carefully consider agency security needs across a number of dimensions," according to the Strategy. Those include:

- Data characteristics to assess which fundamental protections an application's data set requires;
- Privacy and confidentiality to protect against accidental and nefarious access to information;
- Integrity to ensure data are authorized, complete and accurate;
- Data controls and access policies to determine where data can be stored and who can access physical locations; and
- Governance to ensure that cloud

computing service providers are sufficiently transparent, have adequate security and management controls and provide the information necessary for the agency to appropriately and independently assess and monitor the efficacy of those controls.

Due to the special security needs of many government agencies—and a desire to create a system of cloud governance that will outlast individuals or administrations—the Strategy assigned specific roles and responsibilities to a number of federal agencies and organizations, including:

- National Institute of Standards and Technology (NIST) – Lead and collaborate with federal, state and local government agency CIOs, private sector experts and international bodies to identify and prioritize cloud computing standards and guidance;
- General Service Administration (GSA) – Develop government-wide procurement vehicles and cloud-based application solutions where needed;
- Department of Homeland Security (DHS) – Monitor operational security issues related to the cloud;
- Federal CIO Council – Drive government-wide adoption of clouds, identify next-generation cloud technologies and share best practices and reusable example analyses and templates; and
- Office of Management and Budget (OMB) – Coordinate activities across governance bodies, set overall cloud-related priorities and provide guidance to agencies.

"Cheaper processors, faster networks, and the rise of mobile devices are driving innovation faster than ever before. Cloud computing is a manifestation and core enabler of this transformation," the Strategy concluded.

Despite the widespread and rapid adoption of cloud computing across all sectors of society and government, there remains considerable confusion among new or non-users about what a cloud is and how it differs from traditional methods of data storage and sharing.

"A lot of people do tend to think of the cloud as some mythical place—but it really is a way of doing things, not a place. At the bottom of it is physical hardware—computers, hard drives, and so on. So the things that apply today regarding managing our own servers also apply to clouds," says Geoff Webb, director of Solution Strategy at NetIQ in Houston. "It's just as easy and possible for the IT service people handling a cloud to cause problems through mistakes as it is by your own IT department.

"A private cloud requires a fair degree of maturity in how it is managed—it is not for the faint of heart or inexperienced. If you have a lot of resources, but with varying demand on those, and someone with whom you can share those, then you both get more than if you each owned your own systems separately," Webb says. "But it requires knowledge, capability, trust in the people sharing the cloud and accepting the risk you both bring to it. I don't want to share resources—even

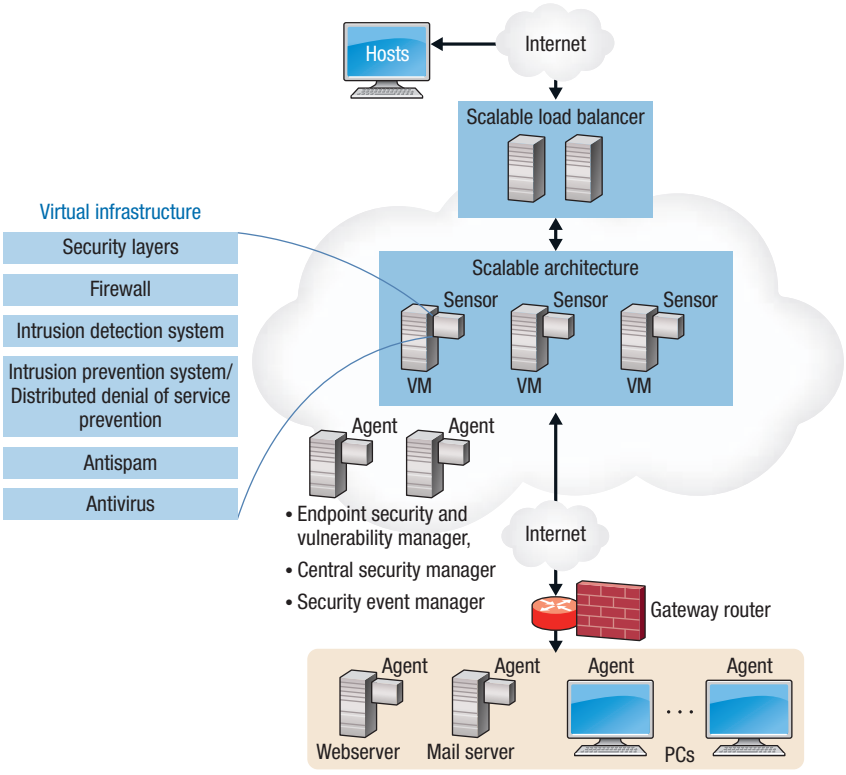


Figure 3: Client sends a request to cloud C1, which dynamically discovers the need to use services from clouds C2 and C3. C1 employs proxies to manage these interactions.

in a private cloud—for highly critical information."

Stelios Sidiroglou, a research scientist at MIT's Computer Science and Artificial Intelligence Laboratory in Cambridge, Mass., says defining cloud computing, especially a secure cloud, is harder than it should be.

"A lot of people have a very hard time understanding it. The cloud is similar to distributed computing we've had, but has a different name because of the different operations that have emerged in the past few years," he said. "And that is probably the source of a lot of confusion, because so many different services now have been attributed to the same concept—cloud computing.

"That confuses the issue of cloud security—are you just trying to secure one of those services or multiples or all? So first you have to identify what kind of cloud computing you're working on and focus on that," Sidiroglou continues. "You have to think about everything—the underlying hardware and operating systems and types of software being used."

NIST defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The core of cloud computing centers on three service models: software as a service (SaaS); platform as a service (PaaS); and infrastructure as a service (IaaS).

In addition, NIST has outlined five essential characteristics of cloud computing—on-demand service, broad network access, resource pooling, rapid elasticity and measured service—and four primary deployment models:

- Private cloud: Infrastructure operated solely for an individual organization, although it may be managed by a third party and exist either on- or off-premise.
- Community cloud: Infrastructure is shared by several organizations within a specific community with shared concerns (such as mission or security requirements); it may be managed by the organizations or a third party and may exist on- or off-premise.
- Public cloud: Infrastructure is available to the general public or a large industry group and is owned by an organization selling cloud services.
- Hybrid cloud: Infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

"We look at the cloud as a consumption model of the underlying technologies to support the mission," says Kyle Keller, cloud business director at EMC Corp. in Hopkinton, Mass. "We want to get to a point where we can set model and security at the application level and maintain control and visibility even if that software goes to another user and you don't maintain direct control.

"It's not so much secure cloud computing as secure computing

in general. Many of our customers want to move into the cloud, but don't have the best legacy security to begin with; cloud computing is an opportunity to do things differently. In the legacy arena, we looked at how to bolt security around the infrastructure. Now the technology is built in, so security controls in a virtualized space become foundational to the architecture from day one rather than something we build on after the fact."

The 2012 National Defense Authorization Act required the DOD Chief Information Officer to create a strategy for migrating defense data and government-provided services from Department-owned and operated data centers to cloud computing. That includes generally available private sector services that provide better capability at lower cost with the same or greater degree of security.

In July 2012, DOD Chief Information Officer Teresa M. Takai released a Defense Department Cloud Computing Strategy "to enable the Department to increase secure information sharing and collaboration, enhance mission effectiveness and decrease costs using cloud services. Active participation and commitment of all DOD components is critical to ensure consistency, optimize benefits and achieve the goal of this strategy."

That goal is to use cloud computing to secure information and provide IT services supporting the Department's mission, anywhere, anytime on any authorized device. It expanded beyond the earlier Federal Strategy in emphasizing the increasing danger of both state-sponsored and individual cyber threats, even as increasing budget constraints force transformations in IT structure and management. To that end, DOD created the Joint Information Environment (JIE) to deliver "faster, better informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location."

"The DOD Enterprise Cloud Environment is a key component to enable the Department to achieve JIE goals. The DOD Cloud Computing Strategy introduces an approach to move the Department from the current state of a duplicative, cumbersome and costly set of application silos to an end-state which is an agile, secure and cost-effective service

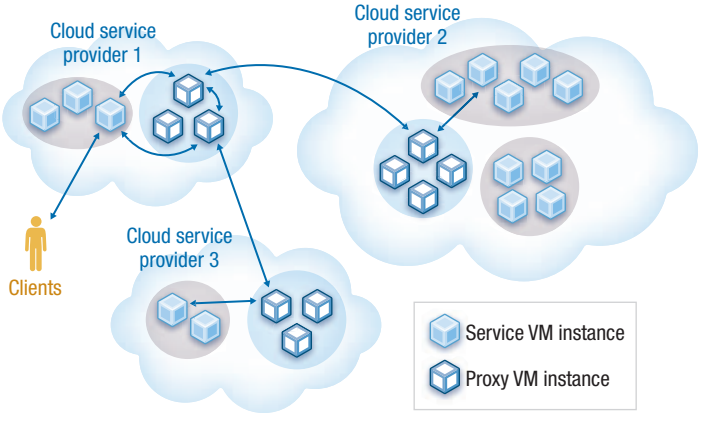


Figure 4: The proxy as a service scenario calls for cloud service providers to deploy proxies as an autonomous cloud systems and offer it as a service to their clients.

environment that can rapidly respond to changing mission needs," according to the report.

That effort is being leveraged with the Federal Risk and Authorization Management Program (FedRAMP) to establish a standard approach to assess and authorize cloud computing services and define requirements for the continuous auditing and monitoring of cloud computing providers.

"The DOD Enterprise Cloud Environment will include separate implementations and data exchanges on Non-secure Internet Protocol Router Network (NIPRNet), Secure Internet Protocol Router Network (SIPRNet) and Top Secret Sensitive Compartmentalized Information (TS SCI) security domains," the DOD Strategy reported.

"This environment will be closely aligned with intelligence community-led initiatives and support information-sharing with DOD traditional and non-traditional partners on the Joint Worldwide Intelligence Communications System (JWICS) and other networks. All cloud services must comply with Department IA [Information Assurance], cyber security, continuity and other policies."

Government-wide and DOD requirements to implement cloud computing as quickly as possible have put even more impetus on aerospace and defense industry and related academia to finalize their own adoption of cloud computing.

Many of the security concepts developed for pre-cloud systems remain viable, albeit with some tweaking. Even secure clouds typically are built with COTS software common to non-cloud systems, according to Howie—and if vulnerabilities exist in that software, they are likely to appear in the cloud, as well. To deal with those and other threats, many clouds now employ multiple levels of security—defense in depth—starting from the host's physical perimeter to the data itself.

"If there is vulnerability in one area, there will be layers elsewhere that will still protect the data and stop attacks or detect them," he said. "You can build a cloud that requires access to a closed network first, such as SIPRNET, then only someone able to access that secure network could access the cloud.

"Typically, if there is an attack, the problem is when the user—not the cloud provider—fails to take advantage of available security mechanisms. Ultimately, the cloud provider—even for private or secure clouds—is not in control of the ultimate security of the user's data. It is up to the customers to understand their responsibilities in using a cloud service. Security is actually a shared responsibility."

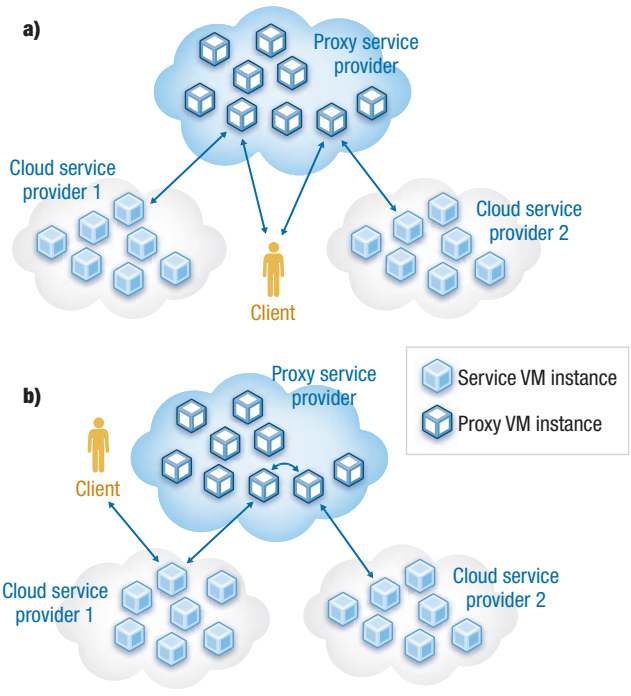


Figure 5: On-premises proxy calls for clients to deploy proxies within the infrastructure of their organization. (a) A client employs two proxies to interact with CSPs C1 and C2. (b) A client initiates a service request with C1, which then discovers the need for a service from C2.

Kevin Haley, director of security response at Symantec Corp. in New York, says there are similarities between the threats facing commercial users and aerospace and defense organizations. "The majority of threats are coming from profit-oriented groups, such as criminals. The real threat to government computing, and industry, involves espionage. If an attacker can steal secrets from a target's traditional systems or a cloud, he no doubt will," he said. "Attacking a cloud really isn't more difficult than attacking a standard data network—in some ways, it could be easier.

"If I can get your log-in details, I don't have to worry about whatever security system the cloud provider has implemented. So if your data is in the cloud, you not only have to worry about vetting your employees who have access, but also the cloud providers' employees."

Clouds also are vulnerable to the Stuxnet approach, a computer worm used in an indirect, but targeted, attack on Iran's nuclear facilities in 2010. "It's a technique we have seen quite a bit in recent years—if I can't directly attack my target, I can attack

the people who work for my target or someone who does business with my ultimate target," Haley said. "A lot of the focus tends to be on very high-level vulnerabilities, but as we focus on more high-tech hacking and solutions, we tend to lose sight of the simplest avenues, such as stealing log-in details."

Among efforts to secure DOD cloud computing is DARPA's Mission-oriented Resilient Clouds (MRC) program. "Where compelling incentives to do this exist, security implications of concentrating sensitive data and computation into computing clouds have yet to be fully addressed. The perimeter defense focus of traditional security solutions is not sufficient to secure existing enclaves. It could be further marginalized in cloud environments where there is a huge concentration of homogeneous hosts on high-speed networks without internal checks and with implicit trust among hosts within those limited perimeter defenses," according to DARPA.

"The MRC program aims to address some of these security challenges by developing technologies to detect, diagnose and respond to attacks in the cloud, effectively building a 'community health system' for the cloud. MRC also seeks technologies to enable cloud applications and infrastructure to continue functioning while under attack. To achieve these goals, the program will research development of innate distributed cloud defenses, construction of shared situational awareness and dynamic trust models, and introduction of manageable and taskable diversity into an otherwise homogeneous cloud, as well as development of mission-aware adaptive networking technologies."

As with many DARPA programs, MRC, launched in November 2011, involves research by a number of organizations, including MIT's SAIL.

"You can make systems more and more secure, but it's just an ongoing arms race and I don't see an end to that. You can set up systems that guarantee previous methods won't work in the future, but attackers are very versatile and will always come up with some way," says Martin C. Rinard, SAIL's MRC principal investigator. "If you have even a small vulnerability in some piece of hardware, it's hard to see how you could not at least mount a DDoS against it. The state-of-the-art in cloud security tends to evolve very quickly over time in the ongoing arms race. Our goal is to develop ongoing trends in how to analyze those.

There is an enormous amount of creative, high-level research underway to address issues current and future, known and still to be discovered. "You can expect to see very great changes in this environment in the next five years or so," Rinard says.

In the ancient manner of armor versus anti-armor, those seeking to secure the cloud face an endless challenge from ever more aggressive and technically sophisticated attackers.

"The cloud is very seductive, but I guarantee that in five years, we will look back and say there are a lot of good uses for clouds, but it doesn't solve all problems," Webb predicts. "Right now a very sensible discussion is underway as to what should or should not be in clouds and, even then, what should be in a public cloud and what in a private." ←

Rapid pace of commercial technology complicates Army plans for wearable computing

BY **John Keller**

Deploying wearable computers that can give the infantryman quick access to battlefield radio communications, messaging, targeting, situational awareness, video, and images is a top priority for the U.S. Army, but how to achieve this goal remains an elusive and moving target.

In the not-so-distant past, Army leaders were interested in equipping every foot soldier with a wearable computer—one that would be easy to use, easy to carry, and have the kinds of features the soldiers would be excited about using.

They considered purpose-built wearable computers designed from the ground-up to be rugged and reliable. Commercial technology didn't have the heft or muscle for what warfighters needed. Today, however, the military wearable computing landscape has flipped 180 degrees. Current requirements call for commercial-grade off-the-shelf smartphones, tablet computers, and hybrid combinations of both from commercial providers like Samsung.

The shift from purpose-built rugged to commercial-grade wearable computing is leaving experts at traditional rugged computing companies feeling confused, frustrated, and shut out of current military planning.

"It looks like the military wearable computer is definitely commercial, so there is no place for us," says Rich Barrett, senior director of engineering at Elbit Systems of America based in Fort Worth, Texas.

Nett Warrior

The Army's primary program involving wearable computing today is Nett Warrior, which is fielding Samsung Galaxy Note II smartphones for evaluation to Army Rangers and soldiers in the 10th Mountain Division at Fort Drum, N.Y. Warfighters are using these devices as chest-worn computers that display situational awareness information.

For this evaluation, the Army buys commercial-grade smartphones, wipes the memory clean, installs Nett Warrior software, and plugs the phone into the battlefield networks via the soldier-carried Rifleman software-defined radio.

This approach may bode well from a user standpoint, because many warfighters are familiar with the Android look and feel of the Galaxy Note II. The drawbacks, however, involve how potentially fragile and unreliable the phone may turn out to be under the environmental rigors of the battlefield.

Soldiers also may have a hard time with the smartphone's wired connection to the Rifleman radio.

COMPANY INFO

Argon Corp.
www.argoncorp.com

Azonix Corp.
www.axonix.com

Black Diamond Advanced Technology
www.bdatech.com

Crystal Group Inc.
www.crystalrugged.com

DRS Tactical Systems
www.drs-ts.com

Elbit systems of America LLC
www.elbitsystems-us.com

Eurotech
www.eurotech-inc.com

Getac
www.getac.com

Handheld USA Inc
www.handheldgroup.com

Honeywell Scanning and Mobility
www.honeywellaidc.com

InHand Electronics Inc.
www.inhand.com

L-3 Ruggedized Command & Control Solutions
www2.l-3com.com/rcc

MicroVision Inc.
www.microvision.com

Motorola Solutions
www.motorolasolutions.com

Panasonic Solutions Co.
www.panasonic.com/business/toughbook

Peratech Ltd.
www.eleksen.com

PFU Systems Inc.
www.pfusystems.com

Quantum3D
www.quantum3d.com

Raytheon Technical Services Company LLC
www.raytheon.com/businesses/rts

Secure Communication Systems Inc.
www.securecomm.com

Stealth Computer
www.stealth.com

Trimble
www.trimble.com

Two Technologies Inc.
www.2t.com

Tethering the two devices risks snagging the wire on trees, brush, and other battlefield obstacles, as well as presents a potential single point of failure if the wire or its connectors are damaged.

A problem facing Army proponents of wearable computers is a persistent disconnect between Army program officers and soldiers in the field—the ultimate end user of most envisioned wearable computing systems. Program office experts such as those at the Program Executive Office (PEO) Soldier at Fort Belvoir, Va., make a living defining requirements for soldier systems such as wearable computers, drawing up solicitations to industry, and ordering prototypes with the best capability at the most affordable price.

Satisfying customers

The problem with this system is soldiers in the field often don't like what the program offices come up with. One former Army program manager says that as much as 70 to 80 percent of program office-supervised new designs are rejected by the very soldiers they are intended to help. If warfighters don't like it, they won't use it, and there's little program offices can do about it.

Sometimes it can be a vicious cycle: Program offices set requirements and companies respond to them, only to have soldiers in the field turn thumbs-down on them. It's a difficult problem, and frustrating for the Army and industry alike.

It is this kind of conflict between program offices and end-users that the Army's semi-annual Network Integration Evaluation (NIE) experiments are designed to resolve. Still, these exercises happen only every other year, and commercial handheld computer technology moves much faster than that. It is this quick pace of commercial wearable computer technology that could continue to undermine Army plans for wearable computing before these plans can gain significant traction.

If Army leaders insist on tapping into commercially developed technology, they have to keep pace with commercial industry, and traditionally the Army's procurement structure is not good at this. ←

Navy asks Hydroid to build large and small unmanned submersibles in $36.3 million contract

U.S. Navy explosive ordnance disposal (EOD) experts needed unmanned underwater vehicles (UUVs) for ocean mine countermeasures, reconnaissance, and mapping. They found their solution from Hydroid Inc. in Pocasset, Mass. Officials of the Naval Surface Warfare Center Indian Head Explosive Ordnance Disposal Technology Division in Indian Head, Md., awarded a $36.3 million contract to Hydroid for UUVs that provide the military force with very shallow water and shallow water mine countermeasures as well as underwater object localization tools. Hydroid will provide an unspecified number of the MK 18 UUV family of systems (FOS), which consists of the MK 18 Mod 1 Swordfish—based on the Hydroid REMUS 100 UUV—and the MK 18 Mod 2 Kingfish—based on the Hydroid REMUS 600 UUV. The REMUS 100 UUV is 5.25 feet long, weighs about 80 pounds, and is 7.5 inches in diameter. It uses a rechargeable lithium-ion battery that lasts for 22 hours between rechargings, and the UUV can dive as deeply as 400 feet. The unmanned submersible is designed to travel at speeds from 3 to 5 knots.

DARPA program to launch long-range UAVs from small ships expands to five contractors

BY **John Keller**

ARLINGTON, Va. A U.S. military research program that seeks to develop a medium-altitude, long-endurance unmanned aerial vehicle (UAV) that can launch and recover from relatively small ships for long-term maritime surveillance has grown to five separate contractors.

UAV experts from Carter Aviation Technologies LLC in Wichita Falls, Texas; Northrop Grumman Corp. in Arlington, Va.; and Aurora Flight Sciences Corp. in Manassas, Va., are the latest companies to join the Tactically Exploited Reconnaissance Node (TERN) program of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va.

The DARPA TERN program seeks to overcome limitations of Navy shipboard aircraft surveillance. Helicopters are relatively limited in their maximum distances and flight times, for example, while fixed-wing manned and unmanned aircraft must operate from aircraft carriers or large land bases with long runways, although they can fly farther and longer than helicopters.

Carter Aviation Technologies, Northrop Grumman, and Aurora Flight Sciences join AeroVironment Inc. in Monrovia, Calif., and Maritime Applied Physics Corp. (MAPC) in Baltimore on the initial phase of the TERN program. Carter won a $2.2 million TERN contract on 6 Sept.; Northrop Grumman won a $2.9 million TERN contract on 6 Sept.; and Aurora won a $2.8 million on 17 Sept. AeroVironment and MAPC won their TERN contracts in August.

In the first phase of the TERN program, experts from the five companies will study designs for an operational TERN UAV, and plan for a prototype flight demonstration in 2017.

The number of companies developing technologies for UAVs that launch from small ships has grown to five.

Carter Aviation Technologies is an aerospace research and development firm that developed Slowed-Rotor/Compound (SR/C) technology that couples the speed, range, and efficiency of an airplane with the vertical takeoff and landing capability of a helicopter. Carter's SR/C technology is scalable from very small UAVs to large transport aircraft.

For the TERN program, Carter Aviation Technologies is offering a sea-based UAV with SR/C technology to enable long-range and long-endurance performance. Company officials expect significant challenges with recovering the UAV in heavy seas and bad weather.

Aurora Flight Sciences, meanwhile, produces the Centaur optionally piloted aircraft, Orion long-endurance UAV, and Skate small UAV that on first glance looks like a fly-

ing pizza box. Northrop Grumman is developing a carrier-based unmanned combat aerial vehicle.

The TERN program seeks to combine the strengths of aircraft bases on land and sea, by using small ships as mobile launch and recovery sites for medium-altitude long-endurance (MALE) fixed-wing UAVs, officials say.

The ultimate goal for a TERN UAV and launch system to enable persistent ISR and strike capabilities with payloads of 600 pounds while operating at ranges as long as 900 nautical miles from a host vessel.

The TERN system should be able to operate from several relatively small ship types in rough seas, including the 2,784-ton Independence-class littoral combat ship (LCS), which is 418 feet long and 104 feet wide, with a large aft-located flight deck. Other ships of interest are amphibious transport docks, dock landing ships, and Military Sealift Command cargo ships.

The program will produce a low-cost TERN prototype UAV to demonstrate launch, recovery, and enabling technologies.

DARPA plans to roll out TERN in three phases over three or four years, culminating in a full-scale launch and recovery demonstration. The first phase will include concept definition activities; the second phase will mature technology, with preliminary design; and the last phase will demonstrate a TERN prototype.

A second solicitation will be issued during the first phase of the program for TERN Phase II and III work.

From the TERN contractors, DARPA officials are interested in novel launch and recovery techniques; aircraft navigation; ship motion prediction; high lift devices; high stroke recovery or arrestment devices; and compact stowage arrangements. Other technologies of interest include automated maintenance systems; robotic deck handling; automated vehicle preflight checkout.

TERN envisions UAV systems for deep overland ISR and strike missions without forward basing or host nation help. Long radius of action enables access to remote geographic areas while long endurance enables persistent ISR and striking fleeting targets.

A relatively small ship deploying with two or more UAVs could offer high-tempo ISR and strike operations on an as-needed basis, DARPA officials say. The program does not involve helicopters or airships.

TERN aims to make it easier, quicker, and less expensive for the U.S. military to deploy ISR and strike aircraft almost anywhere in the world, DARPA officials say.

The TERN medium-altitude, long-endurance (MALE) UAV and automated launch-and-recovery system will be able to launch a 600-pound payload and fly as far as 600 to 900 nautical miles from its host vessel.

The TERN program envisions a capability "like having a falcon return to the arm of any person equipped to receive it, instead of to the same static perch every time," says Daniel Patt, the DARPA TERN program manager.

"About 98 percent of the world's land area lies within 900 nautical miles of ocean coastlines," Patt explains. "Enabling small ships to launch and retrieve long-endurance UAVs on demand would greatly expand our situational awareness and our ability to quickly and flexibly engage in hotspots over land or water."

FOR MORE INFORMATION visit **Carter Aviation Technologies** online at *www.cartercopters.com*, **Aurora Flight Sciences** at *www.aurora.aero*, **AeroVironment** at *www.avinc.com*, and **MAPC** at *www.mapcorp.com*.

PRODUCT applications

DATA COMMUNICATIONS

Navy chooses AN/SRQ-4 ship-to-helicopter data link radios from L3 for situational awareness

U.S. Navy helicopter avionics experts needed a digital data link to enable helicopters to share sensor information in real time with Navy and Coast Guard surface ships. They found their solution from L3 Communications-West in Salt Lake City.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., announced a $6.7 million contract modification to L3 to provide four Common Data Link Hawklink AN/SRQ-4 radio terminal sets for the Navy and one for the U.S. Coast Guard.

The AN/SRQ-4 is the shipboard element of a situational awareness system that links the MH-60R helicopter with surface warships in the area. It provides command and control (C2), sensor data transfer, data link operation, and built-in-test.

The system provides real-time use of aircraft sensors to extend situational awareness over the horizon by enabling surveillance helicopters to data-link radar, video, networking, and acoustic data to Navy Arleigh Burke-class destroyers, Ticonderoga-class cruisers, and Perry-class frigates. Its control systems run on modern open-systems architectures, L3 officials say.

The AN/SRQ-4 supports anti-submarine warfare (ASW) and anti-ship surveillance and targeting (ASST) missions; receives and distributes full-motion video; is IP-enabled and built to work with future network-centric applications; is compatible with the SAU7000 digital messaging interface; and has ruggedized construction and modules that are qualified to Navy shock and environmental standards.

The AN/SRQ-4 also has expanded CDL frequency range to support MH-60R helicopter operations; makes the most of link performance by auto-switching between open-loop pointing and closed-loop tracking, depending on the range between the helicopter and the ship; has a range of 100 nautical miles to the AN/ARQ-50 airborne terminal; and has built-in test.

FOR MORE INFORMATION contact **L3 Communications-West** online at *www2.l-3com.com/csw*, or **Naval Air Systems Command** at *www.navair.navy.mil*.

COMMUNICATIONS EQUIPMENT

Rockwell Collins to provide Navy with aircraft radio communications in $9.2 million contract

U.S. Navy aircraft radio communications experts needed electronic radios and related equipment for a variety of aircraft. They found their solution from Rockwell Collins in Cedar Rapids, Iowa.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., awarded Rockwell Collins a $9.2 million contract modification for AN/ARC-210(V) aircraft radios and related avionics communications equipment.

The AN/ARC-210 Gen V programmable digital communication system from Rockwell Collins provides two-way, multi-mode voice and data communications over frequencies from 30 to 512 MHz, covering UHF and VHF bands with AM, FM, and satellite communications capabilities.

The ARC-210 radio also includes embedded anti-jam waveforms, including Have Quick and SINCGARS, and other data link and secure communications features for battlefield interoperability and transfer of data, voice, and imagery. The radios communicate with other avionics over a MIL-STD-1553 data bus.

The ARC-210 aircraft radio provides VHF close air support radio communications on 30–88 MHz frequencies; navigation on 108–118 MHz; air traffic control on 118–137 MHz; land mobile communications on 137–156 MHz; and maritime communications on 156–174 MHz. The radios also provide aircraft with UHF military and homeland defense communications on 225–512 MHz frequencies; and public-safety communications on 806–824, 851–869, 869–902, and 935–941 frequencies.

The AN/ARC-210 Gen V programmable digital communication system conforms to software-defined radio (SDR) tenets and architectures, and transfers networked or point-to-point data, voice, and imagery.

Rockwell Collins engineers also have added a connector in the back of the radio to allow an Ethernet input for network-centric warfare. Rockwell Collins has supplied more than 30,000 AN/ARC-210 radios worldwide on over 180 different kinds of aircraft for multiband, multimode communications.

The ARC-210 also provides embedded, programmable information security per the U.S. National Security Agency (NSA) Cryptographic Modernization Initiative.

The contract modification to Rockwell Collins also calls for the company to provide the Navy with 40 C-12561A/ARC control radio sets; 80 MT-6567/ARC mounting bases; 40 MT-7006 ARC amplifier mounts; 40 AM-7526/ARC high-power amplifiers; 40 MX-11745/ARC low-noise amplifier (LNA) diplexers with high-power, radio-frequency switches; four C-12561A reprogramming kits with USB port connectors; and 80 RT-1990©/ARC receiver-transmitters.

Rockwell Collins will do the work in Cedar Rapids, Iowa, and should be finished in July 2014.

FOR MORE INFORMATION contact **Rockwell Collins** online at *www.rockwellcollins.com*.

CABLING AND CONNECTORS

Navy to buy serial adapters from Sealevel Systems for AN/PRC battlefield radio systems

U.S. Navy radio communications experts needed a special radio adapter to upgrade U.S. Marine Corps AN/PRC networking radios to send and receive Internet Protocol (IP) data such as GPS maps, images, coordinates, and IM-type communications. They found their solution from Sealevel Systems Inc. in Liberty, S.C.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., announced their intention to award a sole-source contract to Sealevel Systems for the company's ACC-188 USB synchronous serial radio adapter to upgrade fielded Harris and Thales AN/PRC tactical radios to send and receive battlefield data. The Sealevel cables operate with standard PDA-184 software developed by and available from DISA which is currently installed on fielded radios.

Communications such as the Harris Falcon III AN/PRC-152A wideband networking handheld

STATEMENT OF OWNERSHIP, MANAGEMENT, AND CIRCULATION

1. Publication title: Military & Aerospace Electronics
2. Publication number: 005-901. Filing date: 10/1/13.
4. Issue frequency: Monthly. **5. Number of issues published annually:** 12. **6. Annual subscription price:** $175.00.
7. Complete mailing address of known office of publication: PennWell Corporation, 1421 South Sheridan Road, Tulsa, Tulsa County, OK 74112. **7a. Contact person:** Traci Huntsman. **7b. Telephone:** 918.831.9435. **8. Complete mailing address of headquarters or general business office of publisher:** PennWell Corporation, 98 Spit Brook Road, Nashua, NH 03062. **9. Full names and complete mailing addresses of Publisher, Editor and Managing Editor:** Publisher: Ernesto Burden, 98 Spit Brook Road, Nashua, NH 03062. Editor: John Keller, 98 Spit Brook Road, Nashua, NH 03062. Managing Editor: John Keller, 98 Spit Brook Road, Nashua, NH 03062.
10. Owner: PennWell Corporation, 1421 South Sheridan Road, Tulsa, Tulsa County, OK 74112; Successors to the Estate of Helen B. Lauinger, 1421 South Sheridan Road, Tulsa, Tulsa County, OK 74112. **11. Known Bondholders, Mortgages, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities:** None. **12.** N/A. **13. Publication Title:** Military & Aerospace Electronics. **14. Issue Date for Circulation Data Below:** September 2013.

15. Extent and Nature of Circulation:

	Average # copies each issue during preceding 12 months:	No. copies of single issue published nearest to filing date:
a. Total # of copies	25,787	23,421
b. Legitimate paid and/or requested distribution		
1. Outside county paid/requested mail subscriptions stated on PS form 3541	23,121	21,524
2. In-county paid/requested mail subscriptions stated on PS form 3541	0	0
3. Sales through dealers and carriers, street vendors, counter sales, and other paid or requested distribution outside USPS®	35	19
4. Requested copies distributed by other mail classes through the USPS	0	0
c. Total paid and/or requested circulation	23,156	21,543
d. Nonrequested Distribution		
1. Outside county nonrequested copies stated on PS form 3541	1,599	1,616
2. In-county nonrequested copies stated on PS form 3541	0	0
3. Nonreqeusted copies distributed through the USPS by other classes of mail	0	0
4. Nonrequested copies distributed outside the mail	427	108
e. Total nonrequested distribution	2,026	1,724
f. Total Distribution	25,182	23,267
g. Copies not Distributed	605	154
h. Total	25,787	23,421
i. Percent Paid and/or Requested Circulation	91.95%	92.59%

16. N/A. 17. Publication of Statement of Ownership for a Requester Publication is required and will be printed in the November 2013 issue of this publication. 18. Signature and title of Editor, Publisher, Business Manager, or Owner: Traci Huntsman, Manager Corporate Assets and Postal Compliance. Date: 10/1/13.

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

radio; the Harris AN/PRC-117G Falcon III wideband tactical radio; the Thales AN/PRC-154 Rifleman radio; and the Thales AN/PRC-148 family of radios are software-defined communications systems that meet specifications of the Pentagon's Joint Tactical Radio System (JTRS).

These kinds of radios are for Marine Corps and Army infantry for voice and data communications, battlefield networking, and sending data like maps, photos, video, and GPS coordinates.

The Sealevel Systems ACC-188 USB synchronous serial radio adapter and DISA software upgrades tactical radios to send and receive IP data such as GPS maps, images, coordinates, and IM-type communications.

The ACC-188 operates with standard PDA-184 software developed by and available from DISA. The PDA-184 software provides a graphical user interface (GUI) that enables radio users to transmit and receive a variety of data types at relatively high speeds.

The ACC-188 enables interoperability among various radio brands and models, such as the Harris and Thales PRC radios. The ACC-188 is compatible with radios with synchronous communications ports using MIL-STD-188-184. The PDA-184 software is government-developed, government-owned by DISA.

The DISA PDA-184 software implements the MIL-STD-188-184 data waveform; facilitates high-speed data throughput; provides an easy-to-use Java-based GUI; and runs in Microsoft Windows 7 (32-bit), XP (32-bit) or 2000.

The ACC-188 cable and integrated assembly includes a printed circuit board packaged as a bump in the cable that provides a rugged, shielded product designed to withstand the effects of harsh environments. One end of the cable has a standard type-A USB connector to connect to computers and peripherals, while the other end has a connector specific to each brand or model of tactical radio.

FOR MORE INFORMATION contact **Sealevel Systems** online at *www.sealevel.com*, or **Naval Air Systems Command** at *www.navair.navy.mil*.

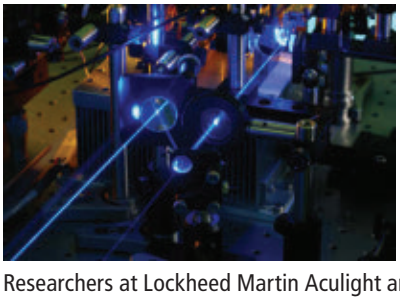
Lockheed Martin Aculight to develop 60-kilowatt laser to kill UAVs, rockets, and mortars

BY **John Keller**

HUNTSVILLE, Ala.—Laser weapons experts at Lockheed Martin Aculight in Bothell, Wash., will help the U.S. Army develop a 60-kilowatt fiber laser module for a truck-mounted laser weapon system intended to shoot down enemy unmanned aerial vehicles (UAVs), rockets, artillery rounds, and mortars.

Officials of the Army Space and Missile Defense Command in Huntsville, Ala., intend to award a sole-source contract to Aculight to develop the 60-kilowatt laser module for integration with the High Energy Laser Mobile Demonstrator (HEL MD)—a joint project of the Army and the Boeing Co. Directed Energy Systems segment in St. Louis.

The upcoming contract will ask Aculight experts to capitalize on technology developed under the U.S. military's Robust Electric Laser Initiative (RELI) such that they can increase laser weapons power from the 25 kilowatts demonstrated in the RELI program to 60 kilowatts. The HEL MD program is intended to develop a laser weapon to counter airborne threats with lasers of 50 to 100 kilowatts.



Researchers at Lockheed Martin Aculight are developing a 60-kilowatt fiber laser module for a truck-mounted laser weapon system to shoot down enemy unmanned aerial vehicles, rockets, artillery rounds, and mortars.

Aculight will build and integrate additional RELI 2-kilowatt fiber laser modules identical to those required for the RELI 25-kilowatt laboratory laser, to reach 60 kilowatts output power. Aculight experts will characterize the RELI beam combining fiber array and spectral beam combiner for the higher thermal loading imposed by the increased power.

The laser will be integrated into the HEL MD to support an upcoming demonstration. Army officials estimate it will be worth $23.8 million over three years. This project is a continuation of a succession of laser weapons research programs to ratchet-up the power of laser beams to make them strong enough for future generations of laser weapons.

The RELI program involves Raytheon Space Systems in El Segundo, Calif.; the Boeing Directed Energy Program in Albuquerque N.M., and Lockheed Martin Aculight. Partners on the RELI program are the Army and U.S. Air Force. The U.S. Navy also is expected to get involved.

FOR MORE INFORMATION visit **Lockheed Martin Aculight** at *www.lockheedmartin.com/us/products/aculight*.

Raytheon to develop new 3D electro-optical imaging sensors

Electro-optics experts at the Raytheon Co. Space and Airborne Systems segment in El Segundo, Calif., will help U.S. military researchers develop new avionics and vetronics electro-optic sensors for target identification and tracking under terms of a new $19.4 million contract. Raytheon will do the work as part of the second phase of the Military Imaging and Surveillance Technology – Long Range (MIST-LR) program, sponsored by the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va. The MIST-LR program focuses on long-range geometric and 3D imaging technology for characterizing targets.

Raytheon to provide midwave infrared sensor turrets military helicopters

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., awarded a $20 million order to the Raytheon Co. Space and Airborne Systems segment in El Segundo, Calif. to provide AN/AAQ-29A electro-optical forward-looking infrared (FLIR) sensor pods for CH-53K heavy-lift helicopters and HH-60 special operations helicopter. The lightweight, high-performance FLIR has a 480-by-640-pixel, 3-5 micron wavelength indium antimonide midwave infrared detector and a three-field-of-view telescope on a 12-inch turret. The FLIR pod helps helicopter pilots with low-level navigation to high altitude long-range targeting.

new PRODUCTS

To submit new products for consideration, contact John Keller at jkeller@pennwell.com.

EMBEDDED COMPUTING

Rugged 3U OpenVPX data recorder for radar, sonar, and imaging introduced by Curtiss-Wright

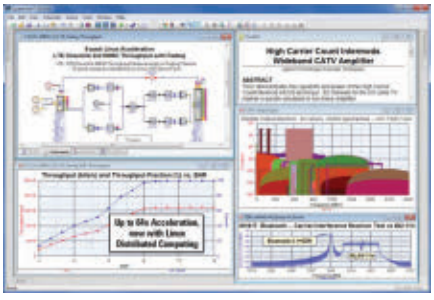
Curtiss-Wright Controls Defense Solutions in Ashburn, Va., is introducing the VR-1257 rugged 3U OpenVPX data recorder for demanding intelligence, surveillance, and reconnaissance (ISR) applications like radar, sonar, infrared imaging, and sensor data capture in aircraft, ground vehicles, and base stations. The small-form factor data storage engine captures high-volume continuously streaming data without interruption for high-throughput reliable data recording in a deployable 3U VPX COTS system. The VR-1257 enables system integrators to add data recording for lab development and rugged deployed environments. The VR-1257 is for harsh-environment air- and conduction-cooled applications. The rugged board has an Intel Core i7 processor and supports system expansion via an XMC/PMC mezzanine site. The mezzanine module interface provides eight lanes of Gen2 PCI Express to support a wide range of high-speed data fabrics such as sFPDP, Gigabit Ethernet, and 10 Gigabit Ethernet.

FOR MORE INFORMATION contact **Curtiss-Wright Defense Solutions** online at *www.cwcdefense.com*.

TEST AND MEASUREMENT

Agilent harnesses compute clusters for fast system-level validation and test

The Agilent Technologies SystemVue platform for communications and aerospace and defense systems design supports high-performance distributed computing. System architects of wireless, 4G smartphone, and radar applications can now verify next-generation system performance up to 64 times faster using Linux-based grid computing managers such as the IBM Platform Load Sharing Facility, according to a company representative. SystemVue 2013.08 introduces the W1712 Distributed Computing Eight-Pack, which integrates with enterprise grid managers and provides concurrent licensing for up to eight dataflow simulations (and necessary add-on libraries). Users are also able to control simulation jobs directly from the SystemVue interface. SystemVue 2013.08 is now available for download from www.agilent.com/find/eesof-systemvue-latest-downloads.



FOR MORE INFORMATION contact **Agilent Technologies Inc.** online at *www.agilent.com*.

POWER SUPPLIES

Fanless power supply for avionics, military, and missile uses introduced by Gaia

Gaia Converter in Le Haillan, France, is introducing the GPACK family of configurable integrated power supplies for avionics, aerospace, military, and missile applications. The GPACK is able to deliver as much as 800 watts without a fan in 24 to 28 volts DC. With input voltage ranges of 9 to 45 volts or 16 to 80 volts, the GPACK is an all-in-one, EMI, MIL-STD-461, DO-160, and transient MIL-STD-704 or MIL-STD-1275 reverse polarity protected, single- or multi-output power supply. The GPACK is configurable with as many as four independent output lines of 3.3, 5, 12, 15, and 28 volts. Each can deliver as much as 200 watts that can be serialized or parallelized and independently trimmed by the user.

FOR MORE INFORMATION contact **Gaia Converter** online at *www.gaia-converter.com*.

DATA STORAGE

Rugged VPX data storage modules for military embedded computing introduced by Elma

Elma Electronic in Fremont, Calif., is introducing the 533x family of dual-drive VPX data storage modules that provide more than 2 terabytes of data storage in one system

slot for military ground-based, shipboard, and aircraft applications. Target embedded computing applications include signals intelligence, engine control, and mission-critical information storage. The data-storage cards come with either solid state SLC, MLC, or 2.5-inch rotating drives. The high-capacity storage modules have a controller/carrier card configuration that enables system expansion to meet increasing storage needs. The 5330/1 boards have a 4-port PCI Express to SATA II 3-gigabit-per second controller that supports two on-board and two external SATA 3G drives or four external drives. This enables systems designers to implement the boards as part of a multi-slot storage array using Elma's 5332/3 series dual drive storage carriers.

FOR MORE INFORMATION contact **Elma** online at *www.elma.co.*

RUGGED COMPUTING

Rugged computer for planes, trains, building equipment introduced by MEN Micro

MEN Micro Inc. in Blue Bell, Pa., is

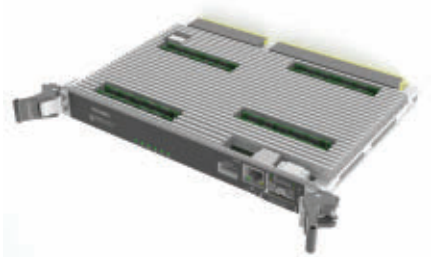
introducing h the BL50W maintenance-free box PC for wireless applications. Its compact, rugged structure is for a wide range of mobile environments including planes, trains, buses, construction, and agricultural machines. Equipped with four PCI Express Mini Card slots that control as many as eight SIM cards and a GPS interface, the BL50W can implement wireless functions such as WLAN, UMTS, GPS, GSM, HSDPA, EDGE, and LTE. The rugged computer also offers user-specific I/O, nine antenna slots, and conduction cooling. The box PC can operate as a content server or hot-spot server, and also can be used as a diagnostic interface or for fleet management as well as to implement vehicle-to-control center communications or for internet access in a train or airplane.

FOR MORE INFORMATION contact **MEN Micro** online at *www.menmicro.com.*

BOARD PRODUCTS

6U OpenVPX single-board computer for radar and other signal processing introduced by Mercury

Mercury Systems Inc. in Chelmsford, Mass., is introducing the Ensemble HDS6602 high-performance 6U OpenVPX single-board computer for complex radar and other massively intensive embedded computing applications. The dual Intel Xeon processor E5-2600 v2-based embedded computing module should be able to deliver peak symmetric multi-processing (SMP) performance of 608 billion floating point operations per second. The HDS6602 uses



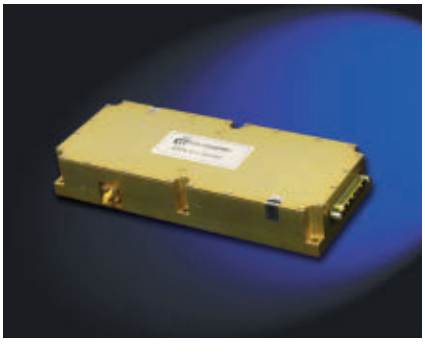
the Mellanox ConnectX-3 technology for InfiniBand or Ethernet as a high-performance interconnect in OpenVPX, and is powered by two 10-core Intel Xeon processors E5-2648L v2 (codenamed Ivy Bridge-EP) running at 1.9 GHz and supporting to 128 gigabytes of memory.

FOR MORE INFORMATION contact **Mercury Systems** online at *www.mrcy.com.*

RF AND MICROWAVE

High-power GaN RF amplifier introduced by Aethercomm

Aethercomm Inc. in San Marcos, Calif., is introducing the SSPA 6.000-18.000-50 high-power super -broadband gallium nitride (GaN) RF am-



plifier. The RF and microwave amplifier operates from 6 to 18 GHz, offers high power over a multi-decade bandwidth with power added efficiency, and operates at a base plate temperature -40 to 55 degrees Celsius. It is packaged in a modular housing that measures 8.5 by 3.5 by 1.38 inches.

FOR MORE INFORMATION contact **Aethercomm** at *www.aethercomm.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

RUGGED DEPLOYABLE

RAID DATA STORAGE

Drive Magazine Based High Performance Multi-Protocol Fibre Channel, SAS or iSCSI System **RPC24**

- ***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***

PHOENIX INTERNATIONAL

AS9100 Rev C/ISO 9001: 2008 Certified

www.phenxint.com 714-283-4800

A Codec Like No Other

Brilliant

Concurrent recording and streaming
Up to 1920x1200 resolution
Local and external storage
Event marking
H.264 *high* profile compression

The DSx™ 300 Delivers!

RGB SPECTRUM®
a visual communications company™

(510) 814-7000 www.rgb.com sales@rgb.com

ADVERTISERS INDEX

Military & Aerospace Electronics

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 **Justine Beauregard**
603 891-9410 / justineb@pennwell.com

PennWell®

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

WEST OF MISSISSIPPI **Jay Mendelson, Sales Manager**
4957 Chiles Drive, San Jose, CA 95136
408 221-2828 / FAX 650 941-5120 / 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

Military & Aerospace Subscription Services
PO Box 3425
Northbrook, IL 60065

BPA WORLDWIDE

AMERICAN BUSINESS MEDIA
The Association of Business Media Companies

Q+A

BIO:
NAME: Chris Kneizys
TITLE: President
CO.: Micro-Coax
ROLE: Provider of cable, assemblies, connectors, and EMI shielding solutions for communications, radar, missile guidance, satellites, aviation, and test systems.
CONTACT: www.micro-coax.com

Chris Kneizys

A specialist discusses custom technical solutions for signal transmissions in some of the most challenging and extreme environmental conditions.

Why are attentions turning to cables, cable assemblies, wiring harnesses, and connectors?

As electronic applications become more advanced, our space, military, and aviation customers are faced with the challenge of ensuring long-term reliability, while meeting or exceeding more stringent requirements for performance and durability under the most extreme conditions. An electronic system is only as strong as its weakest link.

Many customers are better understanding the "total cost of ownership" when it comes to cable assemblies. When you consider buying the cheapest product on the market, you must consider what is the long-term reliability of the product. For example: Will I need to buy two for every one needed by the system because of breakages during installation with a less-engineered product? Will I have to replace the cable more often in the life of the application using a less-engineered product? If I need technical support, will I get it or is it even available? What is the long-term liability, and are you putting your company in financial risk with a less-engineered product if it were to fail in the field? What will your end customer think of you if there is a failure in your product because the right cable assembly wasn't selected?

Quality and reliability are associated with consistency, which comes at a premium through effective process monitoring and tracking for repeatability of results.

Where are you seeing growth?

Despite the economic downturn, the space industry has demonstrated resilience, and forecasts call for about 10 percent growth per year for the next 10 years. Unmanned aerial vehicles (UAVs) make up the aerospace industry's most dynamic growth sector, catalyzed by the U.S. military. The area we see additional growth in is the civil aviation market and the application of ARACON shielding materials.

What advice would you offer?

First, space is considered to be among the harshest environments for electronic systems and components. Second, there is no option for failure; there is no chance for repair or recall. While quality (defined as meeting specifications) is most important, reliability (defined as quality over time) is the most important consideration. Select suppliers based on their understanding of the long-term reliability of the products they produce.

No one wants to be the engineer who purchased a more "affordable" cable assembly that caused an IED (improvised explosive device) jammer to malfunction or an ECM (electronic countermeasure) radar to be 20 percent less accurate three years after installation. If a customer is satisfied with the product's reliability/technical support and is compelled to reduce costs, please work with the suppliers who made the reliable components to drive a redesign that is both affordable and reliable. ←

Don't miss a word

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

Military & Aerospace Electronics

Mobile Your Way

Read it Anytime
Take it Anywhere
Share with Anyone

Take *Military & Aerospace Electronics* on the go and stay connected. From breaking news to videos to the mobile web, there's a way to connect from your mobile device.

Now Available

- iPhone
- iPad
- Mobile Site
- RSS
- Android

Scan the QR code at the right with a barcode-scanning app on your phone.

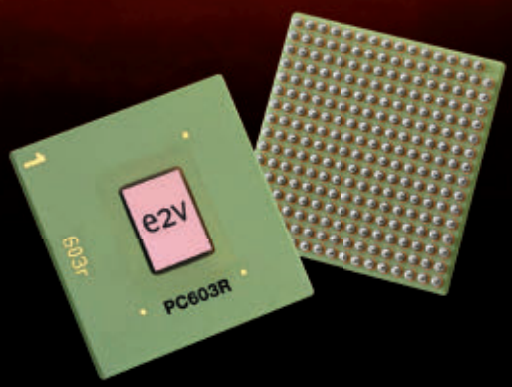
Download and go mobile with *Military & Aerospace Electronics* today.

http://www.militaryaerospace.com/mobile.html

e2v
aerospace and defense

Engineering excellence

Complex aerospace and defense equipment is at risk from the effects of unmanaged obsolescence before and after entering service. e2v aerospace and defense delivers secure continuity of supply with our Semiconductor Lifecycle Management program (SLiM™), a new standard in semiconductor obsolescence management. With extensive experience in die banking, repackaging and testing of product to military specifications, e2v aerospace and defense offers design, development and re-engineering services combined with the capability to store, test and package devices.



Semiconductor Lifecycle Management

Contact us at:

e2v-us.com | 408 737 0992