NOVEMBER 2014

Military & Aerospace Electronics

ENABLING TECHNOLOGIES FOR NATIONAL DEFENSE

Secure cloud computing

Technology is pushing even sensitive military computer data to the cloud. PAGE 20

Electronic flight bags

Commercial aviation moves forward on EFBs, while military lags behind. PAGE 32

militaryaerospace.com

Simulation & training

Industry gearing-up for fifth-generation tactical aircraft.

PAGE 12

PennWell

Critical Moments call for Critical Products

Coilcraft CPS has the battle-proven magnetics you need when the mission is on the line

Our critical-grade RF and Power inductors are built to withstand the most punishing conditions imaginable, including extreme temperatures, thermal shock, G-forces, EMI and vibration.

- Tin-lead (Sn-Pb) terminations for the best possible board adhesion. RoHS terminations also available.
- Extended temperature ranges (-55°C to +200°C)
- Vibration testing to 80 G / shock testing to 1000 G

We also offer comprehensive product testing and validation services in accordance with MIL-STD-981 and EEE-INST-002, as well as custom screening to your electrical and physical specifications.

Learn more about how our battle-tested components will keep your mission on target. Call or visit us online today!

Coilcraft CPS
CRITICAL PRODUCTS & SERVICES

800.981.0363 847.639.6400 www.coilcraft-cps.com

PICO

SPACE SAVING TECHNOLOGY
Transformers & Inductors from .18" ht.

Over 5,000 Standard Surface Mount and Thru-Hole Models

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

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

Multiplex Data Bus Pulse Transformers
Plug-In units meet the requirements of QPL-MIL-PRF 21038/27 Surface units are electrical equivalents of QPL-MIL-PRF 21038/27.

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

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

400Hz/800Hz Power Transformers
0.4 Watts to 150 Watts. Secondary Voltages 5V to 300V. Units manufactured to MIL-PRF-27 Grade 5, Class S (Class V, 155°C available).

ISO9001:2000 AS 9100 REV B

PICO Electronics, Inc.

143 Sparks Ave. Pelham, NY 10803 • ***Call Toll Free*** 800-431-1064 • ***Fax:*** 914-738-8225

VISA MasterCard

See PICO's full Catalog Immediately on the internet

www.picoelectronics.com

E-mail: info@picoelectronics.com

Stay on course.
Stay on schedule.

It's all in a day's work.

Your job is to make sure radar and satellite systems operate to designed performance. The Keysight FieldFox analyzer enables you to get the job done accurately and quickly. The compact 6.6 lbs., rugged package has three precise instruments in one: cable & antenna analyzer (CAT) + vector network analyzer (VNA) + spectrum analyzer. Now you can carry benchtop quality measurements – wherever you need to go.

FieldFox Combination Analyzers
Four models up to 26.5 GHz
MIL-PRF-28800F Class 2 rugged
Agrees with benchtop measurements
CAT + VNA + spectrum analyzer

Learn how to validate radar & satellite performance and more with our app notes at www.keysight.com/find/NoDownTime

USA: 800 829 4444
CAN: 877 894 4414

Scan to view video demo.

KEYSIGHT TECHNOLOGIES

Unlocking Measurement Insights

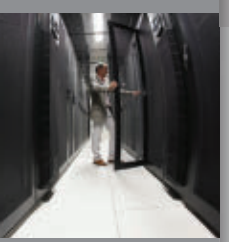
Agilent's Electronic Measurement Group has become **Keysight Technologies.**

NOVEMBER 2014
VOL. 25, NO. 11

Military & Aerospace Electronics

COVER STORY

Image courtesy CAE



MILITARY & AEROSPACE ELECTRONICS ©2014 (ISSN-1046-9079) is published monthly by PennWell Corp.,1421 S. Sheridan, Tulsa, OK 74112. Periodicals postage paid at Tulsa, OK 74101 and additional mailing offices. Editorial offices are located at 98 Spit Brook Road, Nashua, NH 03062-5737. Subscription Prices: Free to qualified subscribers in North America. Other subscribers in U.S.A: $175.00 one year; $309.00 two years; $440.00 three years. Other subscribers in Canada: $270.00 one year; $465.00 two years; $600.00 three years. All other international: $325.00 one year; $620.00 two years; $810.00 three years. Digital edition $70.00 yr. Call (847) 763-9540 for subscription information. We make portions of our subscriber list available to carefully screened companies that offer products and services that may be important for your work. If you do not want to receive those offers and/or information, please let us know by contacting us at List Services, Military & Aerospace Electronics, 98 Spit Brook Road, Nashua, NH 03062. **POSTMASTER:** Send change of address form to *MILITARY & AEROSPACE ELECTRONICS Subscription Services*, PO Box 3425, Northbrook, IL 60065. 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

Military struggling to maintain readiness and relevance

The U.S. military's mission in the Middle East is drawing to a close—with the exception of scattered and largely ineffective bombing raids to annoy the Islamic State of Iraq and Syria (ISIS). With this in mind, it's a legitimate question for U.S. military leaders and the defense industry that supports them to ask, where do we go from here?

The answer is unclear, as was evident at the Association of the U.S. Army (AUSA) conference last month in Washington. With pledges of "no boots on the ground" from the Obama Administration, the Army is in a particularly difficult place. With Army ground forces taken off the board, its leaders are struggling with what to do next.

In the long run, it's not just the Army that will suffer. An unclear military mission and insufficient resources are leading the U.S. military into a deepening malaise. In this environment, Army leaders are hanging their immediate future on two words: readiness and relevance. That's a far cry from what we've seen in the past.

Over the last century, the Army has answered the call for two world wars to confront totalitarian aggression in Europe; a long Cold War to contain communist expansion throughout the world; two hot wars to contain communism in Korea and Vietnam; and two separate wars to confront expansion in Iraq. Against that backdrop, the Army's mission is reduced to readiness and relevance... and so it goes for the other branches of the U.S. military.

When the son of talk show host Montel Williams, who served for 15 years in the U.S. Marine Corps and Navy, asks his father if he should follow in his father's footsteps and serve in the U.S. military, the elder Williams said no. Why? Because of the relative lack of support that military personnel and military veterans are receiving from their government these days, and the huge risks that military personnel are asked to face.

Risks, you ask? The White House is sending as many as 3,000 military personnel to Ebola-afflicted regions of West Africa, presumably to help contain this deadly contagion. Meanwhile, U.S. military veterans who served in Southwest Asia are finding it harder to find quality medical care than the illegal immigrants. No wonder Williams is discouraging his son from joining the military.

Junior Army officers must be asking themselves if they've chosen the right career. Meanwhile, Army contractors must be asking themselves if they're in the right business. Among the Army's industry contractors there's a third word to go along with readiness and relevance: desperation.

They're offering armored combat vehicles that no one is going to buy; computer and network gear that no one needs; and the ability to run computers and communications gear on obsolescent networking equipment that no one is going to use. Contractors are hoping that somewhere, somehow, some way, they'll find a buyer for something. Things eventually may change, but right now it looks pretty bleak.

No doubt, new Army procurement programs are in the offing.

The Joint Light Tactical Vehicle (JLTV) program may see a contractor selected within the next year. Meanwhile, there is some demand for inter- and intra-vehicular networking equipment to keep a shrinking number of Army vehicles up to date.

Yet rumors of a second round of sequestration threaten to deflate already dwindling military budgets even further. Bipartisan commissions warn that the military doesn't have the money to support its commitments, and the military services face unclear missions and unclear futures.

The Army's leadership may be struggling to maintain readiness and relevance, but I fear in this environment they may be able to do neither.

Go wide.

Keysight UXA Signal Analyzer

510 MHz real-time analysis bandwidth

>75 dBc full-band spurious-free dynamic range

-136 dBc/Hz phase noise at 1 GHz, 10 kHz offset

14.1" capacitive touchscreen with streamlined UI

Go deep.

The new UXA is the world's highest performing wideband signal analyzer. With real-time analysis bandwidth to 510 MHz and impressive phase noise, the UXA will give you the wide, deep views and performance headroom you need to troubleshoot hidden design problems. You can also simplify your measurement setup through an easy-to-use menu optimized for touch. Prove what your design can do. Get the UXA and see the real performance.

View our demo video and download an app note at www.keysight.com/find/newUXA

USA: 800 829 4444
CAN: 877 894 4414

Scan to view video demo.

KEYSIGHT TECHNOLOGIES

Unlocking Measurement Insights

Agilent's Electronic Measurement Group has become **Keysight Technologies.**

Navy wrapping up competition to develop helicopter-based EW to protect ships from missiles

BY JOHN KELLER

WASHINGTON—U.S. Navy surface-warfare experts will begin deciding this month on a contractor to design and build a helicopter-based, long-range electronic warfare (EW) system to counter existing and future advanced anti-ship missiles.

Advance Off-board Electronic Warfare will rely on helicopters as electronic warfare platforms.

Officials of the Naval Sea Systems Command in Washington are choosing a contractor for the preliminary design and low-rate initial production phase of the Advance Off-board Electronic Warfare (AOEW) program.

AOEW will provide long-endurance, off-board electronic countermeasures against current and future anti-ship missile threats with a long-duration EW active mission payload for the MH-60R and MH-60S ship-based maritime helicopters.

Navy officials first announced the AOEW program last April, and issued a formal solicitation in August. Companies must have top-secret facilities to be eligible to participate in the program.

The AOEW program intends to devise countermeasures for some of the world's most advanced radar-guided, anti-ship missiles, such as the Russian-made SS-N-22 Sunburn and SS-NX-26 Oniks.

The Sunburn can fly at three times the speed of sound and carries a 705-pound explosive warhead. The Oniks missile, meanwhile, can fly as fast as Mach 2.5, carries a 661-pound warhead, and may have the capability to maneuver on its terminal flight to its target, which could make defeating it difficult, if not impossible.

One of the goals of the AOEW program is to detect and jam incoming fast anti-ship missiles at standoff ranges to give on-board and off-board missile defenses a fighting chance at staving off the incoming weapon.

The AOEW competition—expected to attract bids from some of the nation's top-tier EW houses such as Raytheon Co. Northrop Grumman Corp., Lockheed Martin Corp., Exelis Inc., and BAE Systems—seeks to build an AOEW advanced mission payload that integrates not only with the MH-60R and MH-60S helicopters, but also with the Navy's AN/SLQ-32 shipboard EW system.

Although initial AOEW prototypes are to be installed on MH-60R and MH-60S helicopters, future deployable versions may be intended for long-range, long-endurance fixed-wing or helicopter unmanned aerial vehicles (UAVs), experts say.

The winning AOEW contractor will be asked to develop a modular open-systems architecture (MOSA) to enable the EW payload to adapt to evolving threats, hasten deployment, reduce development time and costs, and facilitate future system upgrades and technology insertion. ←

IN BRIEF

Mercury proposes standards for integrating RF and microwave components

Mercury Systems in Chelmsford, Mass., is proposing industry standards to streamline the integration of RF and digital subsystems in advanced sensor processing applications. The Mercury OpenRFM standards initiative aims at creating more affordable, flexible, and open standards-based solutions by addressing U.S. Department of Defense (DOD) procurement mandates including open systems architecture, interoperability, technology re-use, and affordability. OpenRFM describes a standards-based, modular open architecture that proposes design, test, and control practices for interfacing RF and digital subsystems in an embedded computing architecture such as OpenVPX. It enables the integration of RF and microwave elements within electronic warfare (EW) and signals intelligence (SIGINT) sensor processing chains by standardizing electromechanical and thermal interfaces, software, and control plane protocols. The aim is to help enable prime contractors and the DOD to develop and deploy or existing EW and SIGINT applications more efficiently and affordably.

Teal analysts name next-decade's top 11 defense electronics companies

BY JOHN KELLER

WASHINGTON—Eleven U.S. prime defense contractors will dominate the defense electronics market over the next decade, with the top three—Lockheed Martin, Raytheon, and Northrop Grumman—expected to take the lion's share of military electronics contracts through 2023. The total value of defense electronics contracts through 2023 is expected to be $373.4 billion.

F-35 contracts abound (U.S. Navy photo).

That's the prediction from market researcher Teal Group Corp. in Fairfax, Va. Teal analysts say the top U.S. defense electronics prime contractors over the next 10 years, in order of the anticipated value of their contracts over the period, are:

- Lockheed Martin Corp. in Bethesda, Md.;
- Raytheon Co. in Waltham, Mass.;
- Northrop Grumman Corp. in Falls Church, Va.;
- BAE Systems in London;
- General Dynamics Corp. in Falls Church, Va.;
- L-3 Communications in New York;
- Exelis Inc. in McLean, Va.;
- Boeing Co. in Chicago;
- DRS Technologies Inc. in Arlington, Va.;
- Telephonics Corp. in Farmingdale N.Y.; and
- FLIR Systems in Wilsonville, Ore.

Teal released portions of the annual Manufacturers Market Shares Overview at the Association of the U.S. Army (AUSA) conference.

Over the next decade, Lockheed Martin, Raytheon, and Northrop Grumman will dominate the defense electronics market, together earning slightly more than 40 percent of prime defense electronics contracts that will total $373.4 billion, analysts say.

Lockheed Martin will lead with $52.5 billion in total defense electronics prime contracts, based on leadership in command, control, communications, computers and intelligence (C4I), says David Rockwell, Teal Group's senior electronics analyst and author of the manufacturer market shares overview.

Lockheed Martin will have "dominant positions in electro-optics (EO) due to airborne fighter and attack helicopter targeting system markets, and in sonar due to A-RCI (Acoustics-Rapid COTS Insertion)," Rockwell says. Lockheed Martin also will hold a solid third in the radar market based on the naval AN/SPY-1 Aegis system, Rockwell says.

Raytheon will place second in the defense electronics prime contracting sweepstakes over the next 10 years with $51.6 billion, analysts say. Raytheon will place number one in radar, second in C4I and sonar, and third in EO.

One caveat to Teal's 10-year defense electronics forecast involves the F-35 Lightning II Joint Strike Fighter (JSF), on which Lockheed Martin, Raytheon, and Northrop Grumman have substantial electronics contracts.

Although Teal analysts predict high-volume series production of the F-35 over through 2023, "if JSF dies or production is seriously truncated, Raytheon will likely vault back into a dominant first place in electronics," Rockwell says.

Northrop Grumman will be in third place for defense electronics prime contracting over the next 10 years with an expected $47.9 billion in prime funding, Rockwell says. Northrop Grumman will have dominant positions in military electronic warfare (EW), EO, and radar contracting.

BAE Systems will follow in fourth with $15.8 billion in defense electronics prime contracts—$12.5 billion of that from electronic warfare, Teal analysts say.

In fifth place is expected to be General Dynamics with an expected $10.4 billion in defense electronics prime contracts, due almost entirely to C4I work.

In sixth place in defense electronics prime contracting over the next 10 years is expected to be L-3 Communications with $6.8 billion, followed by Exelis with $3.9 billion; Boeing with $3.1 billion; DRS Technologies at $3 billion; Telephonics with $2.1 billion; and FLIR Systems with $2 billion, Teal analysts say.

Many companies, especially outside the Big Three will earn considerable additional funding as subcontractors, Rockwell says.

Harness the Power of a MIL-SPEC COTS Test Platform

MTS-207 TEST SET
Tough enough for your harshest environments

ULTRA-RUGGED
Ideal for armament, avionics and data acquisition test

CONFIGURABLE
PXI architecture for ultimate customization and expansion

MILITARY AND AEROSPACE PROVEN
Globally deployed in 20 countries

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

VISIT MARVIN TEST SOLUTIONS AT AUTOTEST 2014, BOOTH 619.

MARVIN TEST SOLUTIONS | The Marvin Group

MARVINTEST.COM

Formerly Geotest - Marvin Test Systems

Progeny Systems to upgrade P-8A mission software to open-systems standards

BY JOHN KELLER

JOINT BASE MCGUIRE–DIX–LAKEHURST, N.J.—Aircraft software experts at Progeny Systems Corp. in Manassas, Va., are helping the U.S. Navy upgrade flight software to enable existing airborne mission computers to disseminate collected maritime airborne mission data in real time.

The U.S. Navy Boeing P-8 Poseidon is receiving real-time mission data dissemination capability.

Officials of the Naval Air Warfare Center Aircraft Division at Joint Base McGuire–Dix–Lakehurst, N.J., awarded a $9.6 million delivery order to Progeny Systems for work on the Maritime Airborne Service Oriented Architecture Integration program.

This initiative seeks to develop a maritime airborne service oriented engineering development model of the increment 3 architecture of the Navy Boeing P-8A Poseidon—a militarized version of the Boeing 727 passenger jet modified for maritime patrol and anti-submarine warfare.

Progeny's software model is necessary to support the P-8A network-ready and interoperability requirements, which include research and development for the source code and the Unified Modeling Language Model, Navy officials say.

The order is part of a contract originally awarded to Progeny in September 2013 for Maritime Airborne Service Oriented Architecture Integration work involving the P-8 maritime patrol aircraft. The original deal was a Small Business Innovation Research (SBIR) Phase III contract.

The Maritime Airborne Service Oriented Architecture Integration program seeks to upgrade flight software to enhance network connectivity. Most of today's Navy aircraft are unable to adapt to rapidly changing network-centric requirements due to limitations in their traditional siloed software architectures.

This traditionally developed software often involves closed, proprietary systems and subsystems that require extensive, expensive, and time-consuming engineering and re-engineering to gain access to systems and sensor data.

The service-oriented architecture (SOA) software design approach encourages openness through standardization, and enables reuse and rapid integration of information, Navy officials say.

SOA software design helps engineers upgrade existing software, enable users to run it securely, and make the software adaptable for future change that will be simple, straightforward, safe, and fast, Navy officials say.

Software experts at Progeny Systems seek to use SOA design principles and practices to develop an open-architecture system that will integrate The P-8A's legacy airborne mission-computing systems and sensors so as to provide near-real time dissemination of collected maritime airborne mission data.

The goal is to lay a foundation for a common software-integration architecture for maritime aircraft like the P-8 Poseidon that quickly can establish network-centric qualities and enable the rapid insertion of emerging technologies more economically than is possible today. ←

FOR MORE INFORMATION visit **Progeny Systems** online at *www.progeny.net*, or the **Naval Air Warfare Center Aircraft Division-Lakehurst** at *www.navair.navy.mil*.

Air Force Research Lab asks Leidos to redefine the state of the art in aircraft missile defense

Aircraft missile warning and defense technologies are getting a fresh look from Leidos to help advance the state of the art.

BY JOHN KELLER

WRIGHT-PATTERSON AFB, Ohio—Aerial missile defense experts at Leidos Inc. in Reston, Va., will attempt to advance the state of the art in aircraft missile warning and countermeasures under terms of a $49.4 million U.S. Air Force research contract.

Officials of the Air Force Research Laboratory at Wright-Patterson Air Force Base, Ohio, are asking Leidos experts to move missile-warning and -countermeasures technologies forward as part of the Air Force Threat Warning Countermeasures (TWCM) program.

The TWCM contract calls for Leidos experts to characterize and assess the vulnerabilities of missiles and sensors; simulate missile-detection sensors and enemy missiles; and evaluate potential advanced air-defense countermeasures.

Leidos researchers will investigate advanced integrated threat warning and countermeasure responses that include missile warning, laser warning, and hostile fire indication, Air Force officials say.

The company also will develop ways to detect and counter missile, laser, and hostile fire threats to U.S. military aircraft.

Threats to aircraft continue to evolve, which makes aircraft self-protection increasingly difficult, Air Force researchers explain.

Air crews need situational awareness that involves threat warning for missiles, lasers, and hostile fire as well as a means of defeating the threats through countermeasures, officials say.

The TWCM program is asking Leidos to test and evaluate new kinds of integrated threat warning and countermeasures that can include electro-optical, infrared, directional, and proactive countermeasures.

The goal is for Leidos engineers to integrate a broad spectrum of missile- and laser-warning sensors, mature electro-optical threat warning approaches, and develop cooperative aircraft self-protection techniques.

On this contract, Leidos engineers will do the work at Wright-Patterson Air Force Base in Dayton, Ohio, and should be finished by September 2020.

FOR MORE INFORMATION visit **Leidos Inc.** online at *www.leidos.com*.

The next generation of simulation-based training

Simulation and mission-rehearsal technologies are moving forward to accommodate fifth-generation fighter aircraft, as well as to embed in a variety of military systems to enhance training realism at affordable costs.

BY **Courtney E. Howard**

Readiness requires rehearsal. Aerospace and defense leaders throughout the world are focused on ensuring high levels of preparedness and the ability to respond quickly, efficiently, and effectively—no matter the threat, environment, or mission. To that end, organizations increasingly are investing in advanced simulation, training, and mission-rehearsal systems and solutions to help ensure a highly skilled and adaptable force.

Cost-benefit analysis

Aerospace and defense continues to be a strong market for simulation-based training, which delivers many benefits, says CAE Defense & Security Group President Gene Colabatistto in Saint-Laurent, Quebec. "Simulation offers a number of benefits, notably cost advantages, which simply cannot be ignored in a constrained budget environment.

"The increased cost of fuel, environmental impacts, and significant wear and tear on weapon systems all point to the greater use of simulation," Colabatistto continues. "Most importantly, simulation is the ideal tool for mission preparation and rehearsal, which is critical for ensuring readiness and doing so both safely and cost-effectively.

"The increased and more efficient use of simulation is part of the solution to lowering costs without sacrificing readiness or capability, and most defense forces are putting the increased use of synthetic training into practice," Colabatistto says. "The simulation industry offers a great value proposition; when you look at relevant statistics comparing the cost of simulation-based training against live training, it is pretty hard to beat."

The CAE Medallion-6000 shows a Canadian CH-149 Cormorant search-and-rescue helicopter approaching a Royal Canadian Navy frigate.

At the same time, Colabatistto admits that doing away with live training "is unrealistic and would be counter-productive to preparing defense and security forces for mission success." Nonetheless, he predicts that "the balance of live and virtual training will continue to shift more toward virtual" and "more integration between the live, virtual, and constructive domains" is needed.

Requests and requirements

Providers of simulation-based training and mission-rehearsal systems continue to advance technologies to meet a growing list of industry requirements and requests. Asymmetric warfare, challenging environments, modern threats, and next-generation vehicles and electronics all drive the need for more advanced, more realistic simulation and training solutions.

Fidelity tops the list of training system requirements. "Aerospace and defense customers continue to desire increasing realism—in other words, to make the virtual world look and feel just like the real world," Colabatistto says. "In order for defense customers to do more training and mission rehearsal in a virtual environment, that environment needs to be more immersive and realistic."

There are lots of pieces to the "immersive reality" puzzle, Colabatistto says. Some are in CAE's control; for some, the company leverages the technology curve of other industries, such as gaming or display technologies, he says.

CAE has had an internal research and development program over the past few years aimed at making synthetic environments dynamic, persistent, open, and scalable. "Defense and security customers say they want a fully correlated, interoperable, and persistent dynamic synthetic environment," Colabatistto says. "What they desire is the ability to plan for missions using 'what-if' analysis and decision-support tools, rehearse for missions in real-time, and then execute missions that will leave less room for surprise outcomes—and be able to do this in real time and in simulation. In other words, the synthetic environment needs to be more like the real world, which is constantly changing."

Networking and interoperability

More aerospace and defense customers seek networking capabilities and the interoperability of training systems, Colabatistto explains. "They understand that it is becoming increasingly important and cost-effective to have integrated, interoperable, and networked training

systems so that collective, joint, and even coalition training can be done in a virtual environment.

"Integration, interoperability, and networkability are much more difficult without open industry standards, so we believe defense customers will be continuing to demand non-proprietary systems moving forward," Colabatistto continues. "CAE is a strong proponent of standards, such as the Common Database (CDB), which can help accelerate the use of simulation and synthetic environments for not only training, but areas such as mission rehearsal and decision-support."

UAS operator training

The adoption, use, and value of unmanned aircraft systems (UAS) continue to grow throughout the global aerospace and defense community. UAS large and small are increasingly being called upon to perform myriad civil and military missions. The prevalence of unmanned vehicles is growing the need for effective operator training solutions.

Aerospace and defense is experiencing "a surge in demand for simulation-based training, especially in the UAS market channel," notes Greg Davis, director of Cloud Cap Technology product management and business development at UTC Aerospace Systems in Hood River, Ore. UAS programs benefit by certifying new flight crews in a low-risk simulated environment without putting their physical equipment at risk, he adds.

"The ability to inject aircraft faults and malfunctions tests the operator's decision-making process and crew resource management, while using standardized scenarios to maintain a consistent benchmark," Davis explains. "This is especially helpful for international customers by focusing on crew actions rather than instructor explanations, where a language barrier may reduce the effectiveness of the training. Additionally, simulators offer an economical alternative for trained crews to maintain proficiency."

UTC Aerospace's training center leverages Cloud Cap Technology hardware and software, 10 student trainee stations, and the ability for the instructor to run unique simulator instances for and evaluate the performance of each operator. International customers use UTC Aerospace's training program and integrated simulator] to reduce the development timeline and to refine operator tactics, techniques, and procedures prior to employing live systems.

"Recent requests from customers include increased simulator fidelity and portability," Davis says. "The primary goal is to conduct a mission beginning with the prelaunch checklist through aircraft recovery on a simulator based on their aircraft flight characteristics and performance. The simulator allows the ability to create unique scenarios to challenge both the air vehicle operator and payload operator under realistic conditions."

Industry will need to meet additional requirements for training and expanded use of simulators especially, if the U.S. Federal Aviation Administration (FAA) approves them as aviation training devices (ATD), Davis predicts. "Under current regulations, the FAA allows a limited number of simulator hours toward a student pilot's FAA certification or ratings. It's a realistic expectation that the FAA will allow simulator use in unmanned pilot certification similar to current regulations if/when they are written.

"A growing number of customers are using simulation to maintain operator proficiency and to rehearse mission profiles which complements its use as a training tool," Davis continues. "Civil operators such as airborne law enforcement or emergency responders find this extremely valuable since it allows them to focus their budgets on actual missions during flight operations."

Integrated instruction

Gamification and live, virtual, and constructive (LVC) are among the latest trends in simulation and training, says Bob Pescatore, director of business development at Cubic Corp. in San Diego. Cubic Advanced Learning Solutions (CALS) delivers gamification, which uses "immersive, 3D virtual environments to teach warfighters in settings and situations nearly identical to the ones in which they will perform in their particular role.

"Gamification or game-based training is a cost-effective means for large-scale training. Haptic devices measure force and movement to provide valuable feedback and stimulate muscle memory," Pescatore says. CALS won a contract to develop game-based courseware for the U.S. Navy's Littoral Combat Ship (LCS). "Sailors will meet requirements

CAE's full-mission simulators, such as the C-130J simulator for the U.S. Air Force above, are helping militaries increasingly use simulation-based training to maintain readiness more cost-effectively.

to become qualified and certified on their mission packages using CALS-produced, game-based courseware.

"Most military services are interested in live-virtual-constructive training, or LVC, because it promises to make training more affordable and in some cases more effective than training in live or virtual domains alone," Pescatore adds. "Regarding the vernacular LVC, Live refers to a human training in their real combat system (airplane, vehicle, and weapon). Virtual refers to a human training in a simulator. Constructive refers to computer generated entities or effects that support the live or virtual domains. As a provider of both air combat and ground combat training systems, Cubic is developing an LVC architecture designed to support integrated Air-Land-Sea combat training."

Modern aircraft and avionics

A growing number of fifth-generation aircraft—notably the Lockheed Martin F-35 Lightning II Joint Strike Fighter—is driving a need for LVC technology, Pescatore says. "Fifth-gen aircraft are expected to operate in a much denser threat environment than previous-generation aircraft. Creating a dense threat environment with live platforms, both air and ground, is expensive."

Most combat aircraft training occurs against similar-type aircraft that take turns replicating the enemy, Pescatore says. "The aircraft are expensive to operate, and are not always appropriate in this role. Blending virtual and constructive entities into a live training environment will increase the threat density at a much lower operating cost per threat.

"There simply are not enough live adversary assets available to train the growing 5th-gen fleet fully," Pescatore continues. "Of course, we expect there will always be some live adversary aircraft in LVC training augmented by virtual and live. A human adversary will always be important, as well as exercising live aircraft sensors and weapons."

A couple years ago, the U.S. Air Force Research Laboratory at Wright-Patterson Air Force Base, Ohio, conducted an LVC pilot project, in which Cubic was the lead systems integrator and architect. The project's objective was to prove the efficacy of using LVC for 5th-gen training and much was learned during that project, which culminated in a live flight demonstration, Pescatore says.

Next-generation air combat

U.S. Air Force officials at Luke Air Force Base, Ariz., opened its F-35 Lightning II Academic Training Center last month to provide state-of-the-art training for fighter pilots.

"F-35A training at Luke Air Force Base ensures the long-term viability of our mission of training the world's greatest fighter pilots, which Luke AFB has done for seven decades," says Gen. Robin Rand, Air Education and Training Command commander. "Luke is a part of the first command and its greatest contribution is the trained airmen we send to our combatant commanders executing the mission."

Valued at roughly $47 million, the Academic Training Center is an architecturally and technological advanced facility, reports Staff Sgt. Luther Mitchell Jr., 56th Fighter Wing Public Affairs. Now that construction is complete, Luke personnel are working with Lockheed Martin to install advanced equipment, including classified systems and simulators. Pilots will train in full mission simulators that replicate all F-35 sensors and weapons employment and provide half of the initial qualification

Keysight N5193A UXG Agile Signal Generator

Switch frequency, amplitude and phase in just 250 ns

Generate wide chirps that are 10% to 25% of carrier frequency

Use pulse descriptor words to generate long pulse trains and individually control pulse characteristics

The UXG is a powerful threat simulator that can create realistic electronic warfare signal scenarios. By blurring the lines between analog and vector technologies, the UXG offers fast switching, phase coherency, wide chirps, and per pulse control to generate increasingly complex simulations so you can get closer to reality. Compared to a typical LO, you can test enemy threats at a higher level of realism. And compared to a large threat simulation system, you can test much earlier in the validation process.

Simulate the worst. Protect the best.

View our demo video and download an app note at:
www.keysight.com/find/UXG4EW

USA: 800 829 4444
CAN: 877 894 4414

Scan to view video demo.

KEYSIGHT TECHNOLOGIES

Unlocking Measurement Insights

LASERS & PHOTONICS MARKETPLACE SEMINAR

February 9, 2015
Marriott Marquis
San Francisco, CA

THE LASERS & PHOTONICS MARKETPLACE SEMINAR is the only conference that analyzes the business of photonics and presents some of the most promising opportunities of the coming year. Three of the industry's leading resources—Laser Focus World, which delivers global coverage of the entire photonics industry; Industrial Laser Solutions, a primary source of information on industrial laser materials processing; and Strategies Unlimited, the world's foremost photonics market research company—combine their knowledge and expertise with other industry experts to produce an in-depth look at the business of lasers and photonics.

With presentations by **analysts, entrepreneurs, investors, and technology leaders,** you'll get detailed analysis and commentary on photonics-market trends, applications development, and the business outlook. If you wish to hear about laser sales and projections, about how to position and manage your business for success, about the hottest markets, and about emerging technologies and developments that will impact your business, then this conference is your best resource.

HELD IN CONJUNCTION WITH SPIE'S PHOTONICS WEST, the Lasers & Photonics Marketplace Seminar is a one-day event that analyzes the business of photonics. The annual seminar provides photonics industry decision-makers and stakeholders with market information and analysis, a look at emerging opportunities, and a forum for networking.

SPIE. PHOTONICS WEST

Strategy • Opportunity • Growth

REGISTER TODAY at marketplaceseminar.com

PennWell

flights, according to Lockheed Martin officials.

"At more than 145,000 square feet, this facility was designed to house a dozen full mission simulators and classrooms to train U.S. pilots and pilots from around the world," says Air Force Col. Kimberly Colloton, 60th commander, Army Corps of Engineers, Los Angeles district. The ATC is state-of-the-art in terms of what it will offer for training pilots on the latest in Air Force assets, she adds.

Luke will serve as an F-35A training site for 10 foreign countries on three continents. The first class of students is scheduled to begin training in the ATC in early May 2015.

Future functionality

Military training and simulation will continue to become more realistic and continue to improve readiness, says Cubic's Pescatore. "Many have complained that the defense industry lags the commercial sector when it comes to simulation, but we are seeing the gap close. To be fair, military training requirements in many cases must be stricter than commercial applications to ensure the simulation replicates the actual system in every way.

"An LVC environment must enable operators to train like they fight; otherwise it will be rejected by our customers. I envision that in the near future combat aviators will regularly climb into cockpits both on a flight line and in a simulator, join up in live-virtual airspace that is stitched together spanning 60 miles live and perhaps an additional 200 miles virtual, and counter a large formation of mixed live-virtual-constructive adversaries in a contested environment," Pescatore adds.

"The aviators in live cockpits will perceive the threat environment as if it were real, and not be able to distinguish live from constructive adversaries," Pescatore says. "Much like in Orson Scott Card's novel *Ender's Game*, live LVC participants will not easily recognize the difference between training and combat, other than the terrain and effects they see when they look out the window."

The future of computing is in the cloud

Military and commercial data networking experts are improving the reliability, security, and availability of cloud computing to facilitate use and reduce costs.

BY **J.R. Wilson**

Integrating traditional IT services into cloud computing is one of the biggest challenges facing military cloud users.

Cloud computing has been called the true future of computing, from personal to corporate to military, and a virtualization of resources, but also "a phenomenon that currently has as many definitions as there are squares on a chess-board."

The first confirmed reference to what might be called modern cloud computing was in a Compaq internal document in 1996, but the term did not enter the popular lexicon until a decade later, when Amazon.com introduced the Elastic Compute Cloud.

Two predecessor elements that eventually coalesced into cloud computing were online data storage—as opposed to backup services—and applications that run online rather than being installed on the user's computer, allowing them to be constantly updated and tweaked, behind the scenes.

With applications running online, the user's computer, operating system, RAM, or onboard hard drive are not significant factors, and the programs typically run faster. In addition, with the right access codes, they could be used from almost any computer anywhere in the world.

Cloud computing combines those online services, giving applications faster access to data, including multiple users sharing both simultaneously. Despite wide interest and implementation, however, when Cloud Computing Journal polled 25 global experts for their definitions, they got as many different responses, ranging from "elasticity" to "internet centric software" and including:

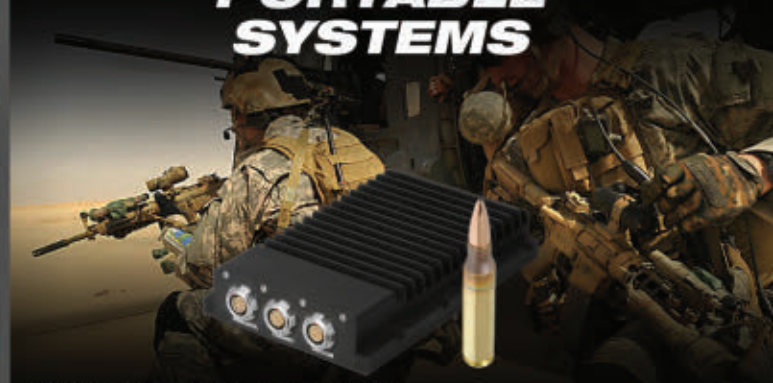
- realizing the earlier ideals of utility computing without the technical complexities or complicated deployment worries;
- using the Internet to enable people to access technology-enabled services must be massively scalable to qualify as true cloud computing;
- leveraging web-scale infrastructure (application and physical) in an on-demand way;
- shifting the infrastructural paradigm that enables the ascension of SaaS [software as a service];
- vast resource pools with on-

RUGGED C⁴ISR SYSTEMS
SINCE 1979

AIRBORNE SYSTEMS

"GOLDEN-EYES" SB1002-MD
Rugged, Dual, Fully Isolated Systems with Removable Drives
- Fully supports Multi-Domain, NSA-secure architecture
- Two fully independent systems (Red/Black) **each with:**
- Up to 2.4GHz Intel Quad Core i7 Haswell processor with 6MB of L2 Cache
- Up to 32GB of 1600MHz DDR3 memory with ECC
- Up to 1TB of sealed removable nDrive SSD drives and 1TB fixed for OS boot
- Ultra-low SWaP only 5.4" x 6.5" x 2.75" @ 6 lbs and as low as 40W total

PORTABLE SYSTEMS

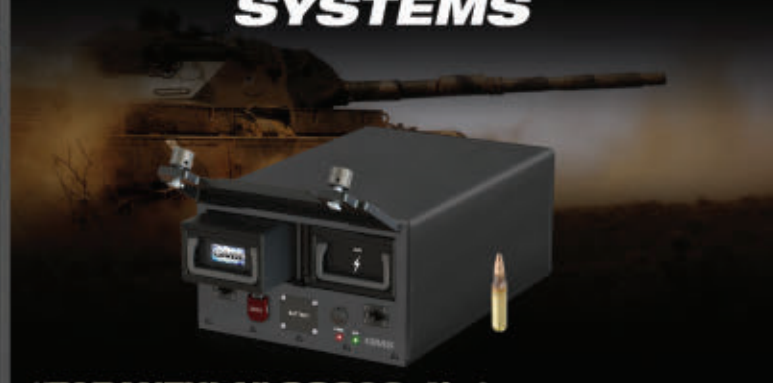


"MARLIN" SG502-LP
Fully Sealed, Rugged, Ultra-Low-Power System
- 2.0 GHz Intel Quad Core Atom processor with 2MB of L2 cache
- Up to 4GB of 1333MHz DDR3 SDRAM with ECC
- Up to 1TB fixed high speed SSD
- One Gigabit Ethernet port with Power over Ethernet (optional)
- Flexible high performance I/O configuration options
- Ultra-low SWaP only 6.0" x 3.75" x 1.0" @1.5 lbs and under 15W

VISION SYSTEMS

"RUGGEDVIEW"
Rugged, Touchscreen Smart Displays with Removable Drive(s)
- Ultra-rugged and lightweight, less than 2 inches thick!
- Up to 2.4GHz Intel Quad Core i7 Haswell processor with 6MB of L2 Cache
- Up to 32GB of 1600MHz DDR3 memory with ECC
- Available in 10", 15", 19" in 4:3 format
- Available in 12", 17", 24" in 16:9 format
- Available in 32", 55", 65" in 4K 16:9 format

VETRONIC SYSTEMS



"TARANTULA" SO302-4in1
Rugged, Secure Virtual Machine ,18 port Switch, RAID and APU
- Up to 2.4GHz Intel 10 Core Xeon Ivy Bridge-EP with Hyper-Threading
- Up to 128GB of DDR3 RAM with ECC up to 1600 MT/s
- Up to 6 Secure Virtual Machines and 18-port managed layer 2/3 switch
- Up to 16TB removable high-insertion cycle canister storage with hardware RAID controller
- Auxillary Power Supply (APU) for orderly system shutdown
- Ultra-low SWaP only 11.75" x 7.7.5" x 4.5" @ 18 lbs

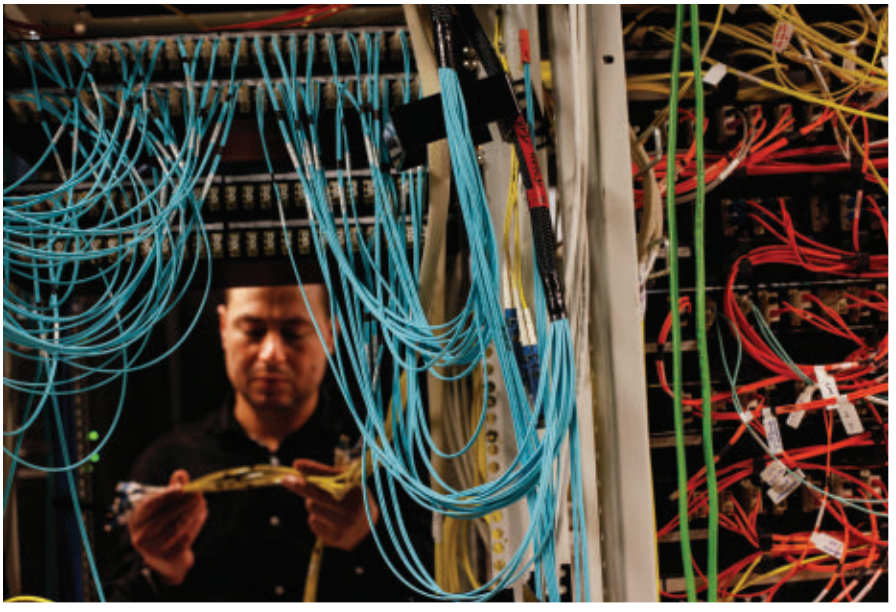
5.56mm M855A1 EPR shown for scale*

GMS COMPUTING ENGINES

GENERAL MICRO SYSTEMS, INC.
8358 Maple Place, Rancho Cucamonga, CA 91730 • (909) 980-4863 • (800) 307-4863

PROUDLY DESIGNED & MANUFACTURED IN THE U.S.A.

www.gms4sbc.com



Ubiquitous computing resources and data networking are some of the largest advantages of moving military information processing to the cloud.

demand resource allocation; and
- the user-friendly version of grid computing.

A matter of perspective

Defining cloud computing is as much a matter of the definer's perspective as it is the technologies and applications involved. Jay Mork, vice president and chief technology officer at General Dynamics Advanced Information Systems in Fairfax, Va., identifies three primary perspectives:

Technical—Moving back to data centers and mainframe computers, but changing it from a big integrated rack to a bunch of distributed computers, such as PCs stacked together to act like a mainframe at the data center, where all computing takes place. And the apps are broken up into pieces and layers rather than one application trying to do everything.

User—For the past 20 years, we've become used to having a PC, disk drive, and monitor. With the cloud, a lot of what had been on the desktop is elsewhere and all the user is interested in is the app. I may not even know where my data is and I don't even have to provide my own computers. So it makes the experience more about me than managing my computers.

Procurement—For people who have to buy and maintain IT infrastructure, the cloud completely changes how they do that. Instead of buying PCs from one company for everyone, they can lease the computer from someone, then lease the software. Mainly, it allows you to take a lot of cost out of the IT infrastructure. However, Mork adds, "there will always be different perspectives, but eventually we'll figure out what the elephant looks like."

Confusion over terminology is far less important to the military or aerospace companies as ensuring its secure and transformational implementation for the safe and efficient transport of passengers and cargo and the secure storage and exchange of information.

In 2011, the U.S. Chief Information Officer released the Federal Cloud Computing Strategy, reinforcing the government's plans to move information technology away from traditional workstations and toward cloud computing. But DARPA's Information Innovation Office said problems remain with regard to security when sensitive data and computations are moved into the cloud.

"The perimeter defense focus of traditional security solutions is not sufficient to secure existing enclaves," according to I2O. "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."

Privacy and security

That is true for anyone concerned about privacy or security, but is of special concern to intelligence agencies and military services gathering, manipulating, and sharing sensitive and classified data.

"The defense industry is applying commercial technology, largely to drive down costs," Mork explains. "A lot of the intel community is implementing their cloud services on top of Amazon Web Services and using COTS cloud technologies. The differences really come from the applications they install into the cloud. The military and defense contractors are now migrating a lot of their applications into the cloud, with the first of those adopting commercial technologies and practices.

"Down the road, as it gets deployed to the individual services

and used in more tactical systems, there will be requirements for real-time aspects," Mork continues. "There also is concern about security, including overlaying and mixing data. The defense industry has invested a lot in technologies around that and is rolling that back out to commercial uses, such as banking."

For the past 75 years, military and intelligence organizations have tried to enhance their system security, typically by keeping their computers, storage media, and work stations all contained within a secure facility with restricted access. Creation of the ARPAnet in the 1960s forced them to begin looking at security in an environment in which military, industrial, and academic labs exchanged data across numerous, widely dispersed computers, although most ARPAnet users still met the old restricted, single building security approach.

"The one big [enabler] that has really accelerated the deployment of the military cloud is the virtual desktop, which allows me to put the pixels on my screen and use my mouse and keyboard controls to reach back to the cloud without even knowing my computer is no longer on my desk. As soon as we demonstrated and proved that could be used for some really high-end applications, it completely changed the way people saw intel analysis, for example," Mork says.

"A lot of what the near-term things are looking at include new analytics and ways to exploit all the data we have, using the infrastructure for activity-based intel," Mork continues. "The cloud provides a different way to organize what you know and the relationships between things that are changing or developing in real time. Our guys are looking at immersive environments on how to recognize the data more quickly as it evolves. A lot of that is really applying existing technologies in new ways, so we don't yet know what we will be able to do."

When ARPAnet went public as the Internet—and more so with the World Wide Web's graphical user interface (GUI) being grafted onto it a few years later—the entire world

quickly became part of the new open, global communications and information-sharing system, with most of the original ARPAnet users still linked into it, which heightened security concerns by several orders of magnitude.

To help deal with that, the military created their own new systems, such as the Nonsecure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNet) and Navy/Marine Corps Intranet (NMCI). The old approach also was updated to the latest technology levels with the recent opening of the world's largest secured database facility, the National Security Agency's Intelligence Community Comprehensive National Cybersecurity Initiative Data Center, also known as the Utah Data Center.

Levels of security

As cloud computing became more secure in response to concerns from users outside the military and intelligence communities, its potential capabilities and advantages put pressure on the Defense Department to adopt the cloud—initially with data and processes requiring lower levels of security.

"Gaining information dominance is seen as a tactical advantage—and where we once talked about network-centric warfare, which migrated to network-enabled operations, we now hear network-dependent operations," says Rubin Dhillon, business development manager for military and aerospace network and communications solutions at GE Intelligent Platforms in Huntsville, Ala.

"The word 'dependent' is key," Dhillon says. "With every manned and unmanned military asset considered a sensor and every sensor connected and sharing data, military operations have completely changed in nature. Military forces depend on a reliable, high-bandwidth network and a constant feed of information.

Cloud computing security and reliability, however, remain concerns. "The reality is that no network is 100 percent reliable and no network will ever be completely secure," Dhillon

says. “Facing this reality, the U.S. Navy is focusing on how to operate in a denied environment and operating while compromised. In other words, how to maintain military operations when the communications network goes down and how to continue operations when—not ‘if’—an enemy hacks into the network infrastructure and cloud services that the Navy increasingly relies on.”

For all military services to explore the adoption of cloud computing makes sense, he adds, because pushing applications into the cloud, rather than relying on local resources, simplifies solutions to many of the deployment, security, redundancy, scalability, and flexibility issues that plague tactical information systems.

“The state-of-the-art changes quickly,” says Mork of General Dynamics. “Where we’re at right now is very similar to an Amazon cloud server—it’s privately held by customers in their own data centers and they are actively migrating users and data out to those clouds. The commercial world jumped onto this sooner and helped build it out. Defense is now doing that, but is taking more time to move data and apps. We’re in the process of migrating users into a virtual desktop environment, where they don’t need a desktop computer anymore.

“From an applications perspective, a lot of defense apps have not been broken into services and stacked into platforms for the cloud,” Mork continues. “From the user experience perspective, technology has advanced considerably from the dumb terminals of the 1970s; today the interface can be any device, because all they have to do is allow me to control access to my information. Looking forward, those devices will change from being a person doing that to devices, such as the thermostat in my house reaching back to a mainframe data center.”

While more and more mission-critical U.S. military applications move into the cloud, potential adversaries continue to develop weapons to take out satellites and other communications infrastructure, invest billions in cyberwarfare capabilities—and move forward as quickly as possible in cloud computing.

“Red Cloud Rising: Cloud Com-

puting in China" is a research report by Defense Group Inc. (DGI) in Vienna, Va. "In recent years, the Chinese government has prioritized the development of cloud computing technology, with the twin goals of expanding Chinese military and civilian access to cloud computing IT resources and creating an internationally competitive Chinese cloud computing service industry," the report says.

"Chinese language news sources indicate that China's primary foreign intelligence collection organization, the Ministry of State Security, has taken an oversight role in projects aimed at bringing foreign cloud computing investment to China," the report states.

Hardware-agnostic

As cloud computing evolves and becomes a standard part of aerospace and military operations, it also will become more hardware-agnostic. Increasing numbers of new technologies will be classified as "services" and software—with essentially unlimited resources in a "highly abstracted space"—will grow larger and more complex as programs are written to take advantage of the scales available. That also is expected to put an emphasis on modular software in which individual components will be modified without forcing a shutdown of the entire program.

One of the main challenges by 2020 will be the management of federated services, not only because applications will be based in the cloud, but also because several clouds will link to each other and to on-premise applications, says John Manley, director of Hewlett-Packard's Automated Infrastructure Lab.

Looking to that same point in cloud evolution, Massachusetts-based Forrester Research anticipates continued increases in processing power and technology advances not only will make cloud computing more predominant and less expensive, technologies currently limited to supercomputers also will move into the cloud and become part of the mainstream infrastructure.

As those elements coalesce, cloud computing is projected to lead to a new mindset and transition to lower-cost services and providers. That will accelerate as efforts such as the Open Compute Project move out of major commercial data centers into a broader range of smaller companies. Open Compute comprises engineers around the globe working to design and enable the delivery of highly efficient server, storage and data center hardware designs for scalable computing.

David Merrill, chief economist at Hitachi Data Systems, believes that will result in data center infrastructure and software automatically molding around the task rather than the task being manipulated to fit the system, with communications within the data center moving at hundreds of gigabits per second.

As with every aspect of the military's future plans, tight budgets, commercial developments and social trends are pushing the Defense Information Systems Agency and others to fine-tune cloud computing, command and control and mobile security. DISA's director, Air Force Lt. Gen. Ronnie D. Hawkins Jr., told the Joint Information Environment (JIE) Mission Partner Symposium in May 2014 that internal data security breaches, such as Edward Snowden and Bradley Manning, have mandated a reassessment of JIE's complexity as DOD shifts to a single security architecture that includes the Joint Regional Security staff.

The growing use of cloud computing in military and government applications is giving rise to new disciplines in computer networking test, measurement, and analytics.

"As we build out the JIE, an environment for the future, we can also help the services [with] capabilities to offload work to DISA, which would be able to free up their workforce," Hawkins reported. "We're able to put big data in the cloud, [but] it's not just about storing big data, but analyzing the data we put in there. We're creating enterprise-wide tools and, as a result, we're creating a more defensible architecture.

"Whatever type of handheld device you have, you can be assured that the information moved from point A to point B is the information

sent from the user to the receiver," Hawkins said. "We [also] are exploiting what is taking place as we build out the JIE within the Pacific Rim. The mobile networking system is the driver of the foundation."

In his keynote speech to the same symposium, Army Lt. Gen. Mark Bowman, the Joint Staff's Director of Command, Control, Communications and Computers/Cyber, said the U.S. military's 15,000-plus networks, 4 million desktops and laptops, and 1 million mobile devices have made cyber/networking operations and security essential to U.S. global warfighting capabilities at national and tactical levels and critical to overall national security.

Essential networking

"The JIE provides a framework that the DOD can gain and maintain a freedom of maneuver within cyberspace," Bowman said. "If we have tons of different applications on different types of networks without a common framework or architecture, we're not going to be able to figure out… what the anomalies are. All those disparate actions… provide gaps, seams and voids that are exploited by the bad guy every second of every day.

"We're now seeing the next generation of shared situational awareness in cyber capabilities that we have never seen before," Bowman said. "We will never go to battle again as an Army alone, as a nation alone. That's why it's so critical to get JIE right."

Army Gen. Keith B. Alexander, head of U.S. Cyber Command and the NSA, says the two agencies are working with DISA and the military services to implement JIE to upgrade operational concepts and command and control from DOD legacy IT architecture to a more defensible system. "I think the cloud architecture that's been pushed forward for the JIE and the intelligence community's IT environment is where our nation needs to be. A thin—or very minimalized—virtual cloud environment offers some great capabilities for the future," he told the National Press Club, adding such an environment would enable patching many computers with 100 percent accuracy at

network speed, allowing an entire network to be fixed in only minutes.

"You could remove humans from the loop in that [operation] and put them where you need them—protecting the networks. We can break down each system we see being scanned by an adversary and put it in a new place. You can jump networks, you can jump databases and you can jump your phone system, [making] it very difficult for adversaries to exploit them. [But] nobody sees it today. We don't have the shared situational awareness we need and this is going to be a key capability for the future."

While most experts believe the bulk of cloud computing research, development, test, and evaluation will fall to the commercial side, at least in the short-term, eventually military requirements will force the development of military solutions. Mork of General Dynamics says his company has been reaching out to industry, academia, and the government, looking for what COTS technologies can be exploited to address specific customer needs.

"We can find a lot of enabling technologies we can use, but to apply those to our customers' requirements domain and mission knowledge of what they do means a lot of military RDT&E will be invested," he says. "Cost, data integration, collaboration among users, the ability to rapidly address capabilities—if you follow a current acquisition process in the military, it takes five years just to think about what you want to do.

"But the threats are changing constantly," Mork adds. "What the cloud does is enable the military to rapidly take technologies and apply them to useful [applications]. Cloud technology allows that, but the acquisition side has to be set up in a way to enable that to happen. And we're seeing that already."

Flexible resources

Todd Stiefler, senior product manager for embedded services & software at GE Intelligent Platforms, says a key advantage of cloud computing is the ability to shrink or expand resources, on-the-fly, to meet real-time needs.

"If you make an investment in your own proprietary server room, you can't do anything more than that provides. With the cloud, you can expand to incorporate whatever is required," he says. "The intel community hosted their own computers and services, but now, using the cloud and putting more data together in one place, they can better share data among people with very proscribed and precise access.

"That will be the model for the military. The problem they are having, in a lot of areas, is missing the analytic insight today they can have with the cloud. The data is there, but the analytics are not—yet."

Many subject matter experts agree that the recent agreement between Amazon Web Services and the CIA has been a significant breakthrough in secure cloud computing. Under the agreement, Amazon has launched a secure cloud-computing system that will enable a revolution in how all 17 intelligence networks function and share information, accessing a variety of on-demand services and analytics from the CIA and NSA.

"The Amazon deal with the intel community is defining the state-of-the-art. DISA's initial mandate was to centralize the procurement and resale of cloud-based services to the military. There really was not a SOTA for military services and DISA will no longer be defining a SOTA for DOD or even acceptable standards. That makes it more of a free-for-all, but DOD is trading cohesiveness for a faster adoption of cloud services by the military," GE's Stiefler says.

Military private clouds will be self-contained, with key protected integration points between clouds, says Rob Smith, director of software engineering at Thales Canada Defense & Security in Ottawa, a primary integrator of software for the Canadian military.

"The different network security in the military environment, with the shared enterprise network, tactical and coalition networks, all of which will need to be integrated—those are problems that will need to be solved over time," Smith says. "The military cloud environment also will have employment differences—environments will be harsher, requiring more advanced equipment, especially when you move from the operational down to the tactical. And those will need to be easily scaled to meet the size of the operation.

"I don't think cloud computing is highly utilized or even understood within the military context as a lot of those try to get up to speed on how to modernize their current systems, such as the Army Private Cloud Initiative, and catching up with and adapting commercial technology," Smith continues. "So I would say infrastructure as a service, adapted to military environments, is the first state that needs to be happening now. Things like cloud encryption at all levels, VDI [Virtual Desktop

Infrastructure] and so on are following up, but the basic understanding needs to be in place first."

GE's Stiefler says running everything in the cloud also enables finding best-of-breed analytical solutions for all the services.

Cloud encryption

"Encryption technologies are getting better, and giving users greater confidence in cloud computing. The profusion of small, affordable sensors—from oil diagnostics in an MRAP to electro-optical sensing on a UAV—are not strictly an enabler, but they make cloud computing much more attractive. All those sensors create much more data across a wide range and run better and faster analytics in the cloud, which is much better than the traditional techniques of mining individual data on servers, then trying to combine it," Stiefler says.

"If you have different platforms and systems within them coming from different contractors, it can be difficult to get the data needed. There have been cases where a platform cannot access some data from its own sensors—it first has to be dealt with by the contractors that built them," Stiefler continues. "Users should be able to access their own data in a comprehensive way to make sense of it. Although it is not a requirement, you start to enable collaboration, data-sharing not only among geographically dispersed organizations but also between organizations within the same service that currently are not talking to each other."

Stiefler also raises a new advantage to cloud computing—making better use of human resources, in part an outgrowth of breaking down organizational stovepipes.

"A number of senior maintenance guys with decades of experience are retiring from the military—and from industry—at an alarming rate and, due to budget cuts, are being replaced with far less experienced personnel with less training," Stiefler says. "What you want to do is put the human resources you have in a central point to manage the entire fleet rather than scattering them among locations to deal only with data from this air wing or that ship.

"That also is true with intelligence analysts, where top experts in terrorist behavior can provide data across multiple battlespaces and use analytics to drive the most pressing problems and information," Stiefler continues. "Another problem area is remote monitoring and diagnostic solutions. It is very difficult to be predictive with the current system, so there is potential for cloud computing in satellites, especially national security platforms, which generate massive data, in terms of their sensors but also what is going on inside the satellite."

Stiefler also raises what many consider the most serious security risk across all domains—the insider.

"I think the risks from external hackers into military clouds have been overplayed," Stiefler maintains. "The industry is very good and there are fewer access points, although insider hacking becomes much greater for the next Snowden, who could access not only his own organization's data but that from a host of agencies sharing data and analytics. Those are being given a lot of consideration as they research their potential use of the cloud."

Increasing use of cloud computing will enable military data experts to trade in their laptop computers for electronic tablets while maintaining access to the same amount of information.

Cloud computing also enables users in the field to replace big laptops with small mobile devices.

"Maintenance guys can walk around with iPads instead of laptops and have access to more data and analytics without needing to key in an asset number; he can just stand next to the item and the system will know what it is and provide the needed data," Stiefler says.

SWAP of the cloud

"You could reduce a lot of SWaP by replacing local computing and data storage with cloud-based, that is positive; but there are concerns about the security of wireless systems. Wireless data transmission in military platforms can be a conversation stopper—even more so with the intel community. Technology advances could help advance the SOTA in cloud computing, especially the wireless transmission of data."

As to the future, while the military will be making advances related to its unique computing requirements and the cloud, it is likely the lag between the commercial state-of-the-art and defense SOTA will continue, which Stiefler says is "partially due to government bureaucracies, but also due to aversion to anything seen as challenging data security.

"All our machines today are generating information that is being collected into the cloud and analyzed there. By the end of the decade, I think we'll see industry has moved faster, but the military also will be more advanced and cloud computing will be major pillars for each of the services," he says, adding that should give the U.S. an extended lead over other nations. "My guess would be we're ahead of the game in thinking about it and have the best technology and some relatively visionary leaders within DOD who want to move this forward.

"I haven't seen anyone abroad really able to leverage net-centric technology to do military operations, which makes me skeptical of the ability of other nations to drive this kind of change," Stiefler continues. "I suspect those allies who would like to do all that are under-capitalized and looking to us to move military cloud computing forward and be able to interoperate with our systems."

Some years ago, General Electric coined a term that users and providers have picked and often link to cloud computing: The Industrial Internet. It is defined as the integration of complex physical machinery with networked sensors and software, drawing together fields such as machine learning, big data, the Internet of Things and machine-to-machine communication to ingest data from machines, analyze it (often in real-time) and use it to adjust operations.

"The idea of the Industrial Internet is that big industrial assets, from oil and gas to aircraft engines to MRI machines, as sensing becomes ubiquitous, will generate a tremendous amount of data. And if it is properly collected and processed by the right analytic, it can generate enormous benefits to the users," Stiefler says. "That includes increasing the operating time of those assets, the fuel burn and decreasing maintenance requirements. [The data generated will] enable analytics that provide value to the end user—information that was not available before.

"When we are able to collect data about military assets and predict, with a pretty good degree of accuracy, which platforms will have what maintenance issues when, it will be a big advantage to the military—fixing only those things that need maintenance rather than doing a full maintenance downtime for every platform. If you have weeks or months of predictive data on those platforms, you can better plan their use and availability. By avoiding unplanned downtime, you increase the efficiency of the whole enterprise."

Integrating IT services

Thales's Smith says the most difficult part of moving to the cloud is the infrastructure—integrating and operating classical information technology infrastructure services [ITIS].

"It's all about getting pre-architected infrastructure—full scalability, the system is elastic, requires less power, is smaller and more powerful, fully virtualized, abstracted from the hardware," Smith says. "When you take that approach you have a built-in backup, easier recovery, the ability to also reduce your desktop footprint. You can easily spin up the entire stack to be used in any context, such as integration

of the mobile layer. Getting the ITIS information under control at the first level is the low-hanging fruit, using cloud management for self-service and system response to user demands."

The military doesn't have the full virtualization, scalability, and ubiquitous access of services as the major commercial forerunners, such as Amazon.com and Google, Smith adds, but the requirements for cloud computing differ little from classical IT—data available as fast as possible, networking, data storage, data filtered and condensed to be presented in a usable form for the Common Operating Picture (COP) to influence their options and course of action.

"It's all about supporting the battle rhythm and ensuring the data is well integrated," he says. "The cloud simply provides a more integrated way to accomplish that, as an enabler for mobility and other military requirements. Conversion of infrastructure is key now, because it allows virtualization—storage, computing, even the network—of the entire system, including the configuration. Cloud management software is much more integrated and management is becoming easier, with self-service and automation becoming much more integrated for fielded soldiers."

Even as the military makes its first moves toward cloud computing, essentially playing catch-up with the large commercial trailblazers, users and providers are considering what capabilities can and should be part of future evolutions.

Those include encryption on the fly of all data and processes, at all levels; being able to provide services across the entire span of military communications; meeting higher security restrictions; combining encryption at all levels with context-aware identity and access management, specific to the environment, from tactical military in the battlespace to sensitive financial operations in commercial banking to interoperability for coalition operations.

"I think the heaviest investments will be on the industry side, with military R&D aimed at making it work within that environment. Generally, the military has not fully understood, deployed nor used cloud computing. We're looking at commercial technology and how to deploy those to military applications and get to the next level of development, so right now commercial developments and R&D are driving the technology," Smith says, but adds the size of U.S. defense spending, even at a time of tight budgets, means it is the only nation likely to drive even a part of commercial development.

"Cloud computing is definitely of interest and about to be pushed for military deployments in Europe, for example, but not as advanced as the U.S. military," Smith continues. "At the infrastructure level, classical ITIS, I think the U.S. military is a driving force, their program having started three or four years ago. But at the platform, services and true software architecture level, they remain behind major commercial users. With the consolidation of all their data centers, however, the U.S. military is a factor in infrastructure, but there, too, big commercial data centers have solved a lot of problems." ←

STATEMENT OF OWNERSHIP, MANAGEMENT, AND CIRCULATION

1. Publication title: Military & Aerospace Electronics. **2. Publication number:** 005-901 **3. Filing date:** October 1, 2014. **4. Issue frequency:** Monthly. **5. Number of issues published annually:** 12. **6. Annual subscription price:** $185.00. **7. Complete mailing address of known office of publication:** PennWell Corporation, 1421 South Sheridan Rd., Tulsa, OK 74112, Tulsa County. **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 Rd., Nashua, NH 03062. **9. Full names and complete mailing addresses of Publisher, Editor and Managing Editor:** Publisher: Ernesto Burden, 98 Spit Brook Rd., Nashua, NH 03062. Editor: John Keller, 98 Spit Brook Rd., Nashua, NH 03062. Managing Editor: John Keller, 98 Spit Brook Rd., Nashua, NH 03062. **10. Owner:** PennWell Corporation, 1421 So. Sheridan Rd., Tulsa, OK 74112, Tulsa County; Successors to the Estate of Helen B. Lauinger, 1421 So. Sheridan Rd., Tulsa, OK 74112, Tulsa County. **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:** September 2014.

15. Extent and Nature of Circulation:

	Average No. copies each issue during preceding 12 months:	No. copies of single issue published nearest to filing date:
a. Total number of copies	23,918	22,970
b. Legitimate paid and/or requested distribution		
1. Outside county paid/requested mail subscriptions stated on PS form 3541	21,415	20,517
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®	15	11
4. Requested copies distributed by other mail classes through the USPS®	0	0
c. Total paid and/or requested circulation	21,430	20,528
d. Non-requested distribution		
1. Outside county nonrequested copies stated on PS form 3541	1,513	1,670
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	589	563
e. Total nonrequested distribution	2,102	2,233
f. Total Distribution	23,532	22,761
g. Copies not Distributed	386	209
h. Total	23,918	22,970
i. Percent paid and/or requested circulation	91.07%	90.19%
16. Electronic Copy Circulation		
a. Requested and Paid Electronic Copies	0	0
b. Total requested and paid print copies + requested/paid electronic copies	21,430	20,528
c. Total requested copy distribution + requested/paid electronic copies	23,532	22,761
d. Percent paid and/or requested circulation	91.07%	90.19%

☑ I certify that 50% of all my distributed copies (electronic and print) are legitimate requests or paid copies.

17. Publication of Statement of Ownership: Will be printed in the November 2014 issue of this publication.

18. Signature and title of Editor, Publisher, Business Manager, or Owner: Traci Huntsman, Manager Corporate Assets and Postal Compliance. **Date:** 10/01/2014.

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).

Electronic flight bags becoming standard in civil aircraft cockpits; military adopts more slowly

BY **John Keller**

Commercial airlines and general-aviation pilots are moving forward on adopting electronic flight bags (EFBs) in efforts to replace stacks of paper documents in the cockpit with handy and easily stored electronic versions on e-readers and tablet computers.

Military aviation, meanwhile, slowly is beginning to adopt EFB technologies aboard large transport and patrol aircraft, and tactical military aviation like jet fighters have barely started any kind of transition to a paperless cockpit.

The EFB revolution, which is taking place primarily in civil aviation, is a broad attempt to transform traditionally paper documents such as aeronautical charts, weather information, checklists, and document libraries to electronic versions for easy perusal on handheld devices like e-readers and tablet computers.

Some EFBs, however, offer more than just electronic documents. Some offer interfaces with the aircraft, as well, and still offer the convenience, portability, and familiarity

COMPANY INFO

Airbus
www.airbus.com

AivlaSoft
www.aivlasoft.com

AOPA
www.aopa.org

Arconics Aviation
www.arconicsaviation.com

ARINC
www.arinc.com

ASG Inc.
www.asginc.net

Astronautics Corp. of America
www.astronautics.com

Avionics & Systems Integration Group (ASIG)
www.asigllc.com

Bergfeld Software
www.bergfeld-software.de

Boeing
www.boeing.com

Carlisle Interconnect Technologies
www.carlisleit.com

CAVU Companies
www.cavucompanies.com

CockpitApps.com
www.cockpitapps.com

DAC International
www.dacint.com

EDMO Distributors Inc.
www.edmo.com

Esterline CMC Electronics
www.esterline.com

Evoke Systems
www.evoke-systems.com

Exalit Ltd.
www.exalit.ch

Execaire Inc.
www.execaire.com

Flight Focus
www.flightfocus.net

Flightman
www.flightman.com

Global Airworks
www.airworksinc.com

Global NavSource
www.globalnavsource.com

Goodrich
www.goodrich.com

Honeywell
www.honeywell.com

IMS Flight Deck
www.imsco-us.com

Innovative Solutions & Support
www.innovative-ss.com

Jeppesen
www.jeppesen.com

L-3 Communications
www.l-3com.com

L-3 Communications Aviation Recorders
www.l-3ar.com

Lone Star Aviation Corp.
www.lonestaraviation.com

Lufthansa Systems
www.lhsystems.com

Midcoast Aviation
www.midcoastaviation services.com

navAero
www.navaero.com

Navtech
www.navtech.aero

On-Board Data Systems
www.obds.com

Optimization Technologies
www.optechsw.com

Otto Instrument Services
www.ottoinstrument.com

Ramco
www.ramcoaviation.com

Rockwell Collins
www.rockwellcollins.com

Sabre Airline Solutions
www.sabreairlinesolutions.com

SAT-WAY SA
www.sat-way.com

Seattle Avionics
www.seattleavionics.com

Shadin Avionics
www.shadin.com

SITA
www.sita.aero

Teledyne
www.teledynecontrols.com

Teledyne Controls
www.teledyne-controls.com

Universal Avionics Systems Corp.
www.uasc.com

UTC Aerospace
www.utcaerospacesystems efb.com

of well-known tablet computers like the Apple iPad, which is widely popular with EFB users.

EFBs come in three classes. Class 1 is the most simple of the three and simply involves electronic documents that store and display on e-readers like the Amazon Kindle or the iPad. These devices normally are stowed during takeoff and landing, and do not require an administrative process to remove them from the aircraft. Class 1 EFBs are not connected directly to aircraft systems.

Class 2 EFBs are something different. These devices are based on tablet computers like the iPad, but have mounting brackets and docking stations that connect them directly to aircraft systems while the aircraft are in flight or operating at airports.

While Class 2 EFBs offer the convenience of enabling the pilot to take them quickly out of the aircraft for use on the ground, they also have secure and encrypted wired or wireless connections to the aircraft systems to enable pilots to send and receive reports and forecasts during flight, and interface with aircraft navigation systems to display moving maps.

Class 3 EFBs, meanwhile, are permanent fixtures in the cockpit like other avionics instruments. They are hard-wired with secure links into aircraft navigation systems and flight computers, and offer expanded capabilities like automatic dependent surveillance-broadcast (ADS-B) cooperative surveillance.

Class 3 EFBs only can be removed from the aircraft by certified maintenance personnel, and each removal and installation must be documented in maintenance logs.

Overall, EFB technology is making the jobs of civil aircraft pilots a lot easier than before, as they can call up a wide variety of aeronautical maps, airport configuration drawings pointing out the locations of runways and taxiways, and up-to-the-minute aeronautical weather forecasts. All this is available in one handheld device, rather than in a bulky bag of pamphlets, books, and other documents.

Electronic documents displayed

CONTINUED ON PAGE 37 ➔

AeroVironment and Northrop Grumman develop long-endurance maritime UAV

Unmanned aircraft designers at AeroVironment in Monrovia, Calif., are moving forward on a program to develop a medium-altitude, long-endurance (MALE) unmanned aerial vehicle (UAV) that can launch and recover from small ships for long-term maritime surveillance. U.S. Defense Advanced Research Projects Agency (DARPA) officials in Arlington, Va., announced a $19 million contract modification to AeroVironment for the second phase of the Tactically Exploited Reconnaissance Node (TERN) maritime UAV program. AeroVironment joins the Northrop Grumman Aerospace Systems segment in El Segundo, Calif., for the second phase of the TERN maritime UAV program. The two companies won TERN Phase II contracts one day apart from one another. 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.

Air Force asks Northrop Grumman to stiffen Global Hawk UAV defenses against cyber attacks

BY **John Keller**

WRIGHT-PATTERSON AFB, Ohio—U.S. Air Force unmanned aerial vehicle (UAV) experts are asking Northrop Grumman Corp. to upgrade the Global Hawk UAV to resist computer hackers' attempts to commandeer the unmanned aircraft while in flight.

Officials of the Air Force Life Cycle Management Center at Wright-Patterson Air Force Base, Ohio, are awarding a $33.9 million contract modification to the Northrop Grumman Aerospace Systems segment in San Diego to retrofit satellite communications links in the Global Hawk UAV fleet. The contract modification calls for Northrop Grumman to upgrade communications security in International Maritime Satellite links to enable Global Hawk UAVs to improve their defenses against cyber attack.

Global Hawk, which can fly for more than 24 hours between refuelings, often relies on maritime satellite communications (SATCOM) links to enable ground controllers to maintain contact with the unmanned aircraft. The Air Force operates more than 40 Global Hawk unmanned aircraft.

Air Force officials want to stiffen the Global Hawk's maritime SATCOM links to prevent computer hackers from breaking through existing data security to take unauthorized control of the high-altitude, long-endurance (HALE) Global Hawk reconnaissance UAVs.

Northrop Grumman engineers are working to lessen the Global Hawk UAV's vulnerability to cyber hackers.

Recent studies have uncovered some flaws in satellite communications links that could enable cyber warfare attacks to disrupt military operations and ship and aircraft communications.

Global Hawk HALE UAV provides near-real-time intelligence, surveillance, and reconnaissance (ISR) over large areas. The Block 30 Global Hawk carries sophisticated imaging and electronic signals sensors on missions that can exceed 32 hours.

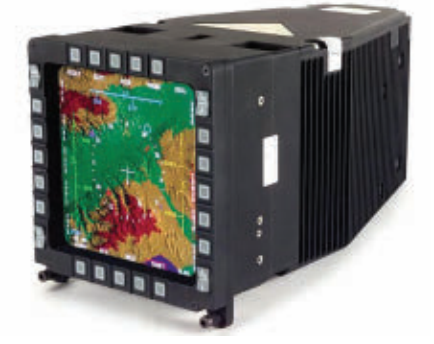
Under terms of the contract, Northrop Grumman will make maritime SATCOM security upgrades to Global Hawk unmanned aircraft, as well as to Global Hawk ground-control systems and spare parts.

Northrop Grumman will do the work in Palmdale, Calif., and should be finished by the end of 2016.

FOR MORE INFORMATION
visit **Northrop Grumman Aerospace Systems** online at *www.northropgrumman.com*.

Honeywell wins $15.7 million for cockpit displays on Hornet and Growler jets

PATUXENT RIVER NAS, Md.—U.S. Navy avionics experts needed a variety of cockpit displays for the Boeing F/A-18E/F Super Hornet jet fighter-bomber and the EA-18 Growler electronic warfare jets. They found their solution from the Honeywell International Inc. Aerospace segment in Albuquerque, N.M.



Honeywell is providing a variety of electro-optical cockpit displays for Navy carrier-based combat jets.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., announced a $15.7 million contract modification to Honeywell on Friday for 197 advanced multi-purpose displays (AMPD) for the Super Hornet and Growler aircraft.

The AMPD rugged display family consists of 5-by-5-inch forward avionics displays, 5-by-5-inch aft displays, and 8-by-10-inch avionics displays.

The order is for eighty 5-by-5-inch forward displays, seventy-five 5-by-5-inch aft displays, and seventy-five 8-by-10-inch displays. In this order, 52 forward displays, 48 aft displays, and twenty-four 8-by-10-inch displays are for the U.S. Navy, while 28 forward displays, 27 aft displays, and eighteen 8-by-10-inch displays are for the government of Australia.

The AMPD replaces obsolete cathode ray tube (CRT)-based displays in legacy aircraft, and uses state-of-the-art active matrix liquid crystal display (AMLCD) technology. The displays are full color, high density, and can be used during the day, at night, and with the night vision imaging system (NVIS).

Of the AMPD family, the 5-by-5-inch versions are for the F/A-18E/F/G models, and the 8-by-10-inch versions are for the F/A-18F/G aft cockpit. The 8-by-10-inch model includes a direct digital video input.

The displays provide symbology, raster, and hybrid display formats, and support mono and full-color modes.

On this contract modification, Honeywell will do the work in Albuquerque, N.M., and should be finished by February 2016.

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

FLIR thermal cameras for optical gas detection monitor gas pipelines from safe distances

FLIR Systems Inc. in Wilsonville, Ore., is introducing the FLIR G300a, G300pt, and A6604 thermal cameras for optical gas detection for monitoring gas pipelines and installations from safe distances. Each model contains a cooled indium antimonide (InSb) detector, which enhances the sensitivity of each camera to detect small gas emissions. The G300a and G300pt cameras have a resolution of 320 by 240 pixels, while the A6604 has a resolution of 640 by 512 pixels. Each camera can be controlled via Ethernet, or integrated into any TCP/IP network. They also are GEV/Genicam-compatible. The G300a and A6604 cameras require an additional housing while the G300pt comes with its own housing mounted on a pan/tilt mechanism. The housing can rotate the camera 360-degree continuously and tilt 90 degrees. The three FLIR cameras detect benzene, ethanol, ethylbenzene, heptane, hexane, isoprene, methanol, MEK, MIBK, octane, pentane, 1-pentene, toluene, xylene, butane, ethane, methane, propane, ethylene, and propylene.

FOR MORE INFORMATION visit **FLIR Systems** online at *www.flir.com*.

PRODUCT applications

RUGGED COMPUTERS

General Dynamics chooses rugged servers from Crystal for Prophet signals intelligence vetronics

Vetronics designers at General Dynamics C4 Systems in Scottsdale, Ariz., needed rugged computer servers for a combat vehicle signals intelligence (SIGINT) system. They found their solution from Crystal Group Inc. in Hiawatha, Iowa.

General Dynamics is using the RS112 1U rugged server from Crystal Group on a project to integrate and upgrade the U.S. Army Prophet program, which enables tactical commanders to detect, identify, locate, and deter a wide range of signal emissions on the battlefield.

The Prophet system is comprised of electronic components that are vehicle-mounted or soldier-transportable. Prophet offers a near-real-time picture of the battlespace through SIGINT sensors and high-performance computing.

The program is structured with the ability to incorporate new technologies as they become available, including Crystal Group's RS112 1U rugged server, Crystal officials say.

The Crystal Group server is relatively small, lightweight, and power-efficient, yet rugged enough to withstand the environmental rigors of vehicular electronics on the battlefield, where equipment is subject to high levels of shock and vibration, temperature extremes, dust, dirt, and other contaminants.

The RS112 meets MIL-STD 810, has a lightweight aluminum chassis, and is 20 inches deep. It has one expansion slot, two drive bays, and Intel Sandy Bridge or Ivy Bridge processor options, Crystal officials say. The rugged server is hard-mounted in Prophet vehicles or can be packaged in transit boxes that allow for quick installs.

FOR MORE INFORMATION visit **Crystal Group** online at *www.crystalrugged.com* and **General Dynamics C4 Systems** at *www.gdc4s.com*.

RUGGED COMPUTERS

GTS to provide Navy with shipboard computers

Global Technical Systems (GTS) in Virginia Beach, Va., will provide the U.S. Navy with air- and water-cooled, open-architecture, rugged computers under an $84.9 million contract.

Officials of the Naval Sea Systems Command in Washington are asking GTS to build the Common Processing System (CPS)—a shock-resistant, open-architecture computing system for Navy cruisers, destroyers, and other programs. The contract includes spare parts and engineering services. The CPS provides a common computing infrastructure for ship combat systems, including processing and memory, data storage, and I/O interfaces for csombat systems. The GTS team consists of Northrop Grumman, DRS Technologies, IBM, and GoAhead Software.

GTS engineers will build the CPS using commercial off-the-shelf (COTS) hardware and software, such as BladeCenter technology. Plug-in components are accessible, hot-swappable, and battle-ready protected by the GTS Advanced COTS Enclosure (ACE).The CPS consists of a rugged enclosure and three subsystems: the processing subsystem, the storage and extraction subsystem, and the I/O subsystem.

FOR MORE INFORMATION visit **Global Technical Systems** at *www.gtshq.com*.

CONTINUED FROM PAGE 33

on EFBs, meanwhile can be updated rapidly online, lowering the risk of pilots using out-of-date maps and airport drawings.

"At a very high level, the EFB is used to replace paper based systems to improve operational efficiency, where traditionally pilots operated with lots of paper, and these computers can replace that," explains Bill Baumgarten, business development manager for the cockpit data management group at EFB provider UTC Aerospace Systems in Charlotte, N.C.

Pilots often use their personal iPad tablet computers for Class 1 and Class 2 EFBs for their utility and mobility. "We are seeing the next evolution of the connectivity of that tablet computer to their environment," Baumgarten says. "They can be connected to the aircraft and to the outside world."

The transition to EFBs in military cockpits is lagging about five years behind civil aviation, says Gary Moore, military aftermarket business development representative at UTC Aerospace. The holdup, he says, stems primarily from military budgetary constraints rather than operational constraints.

Moore estimates that perhaps 35 to 40 percent of military pilots who fly large transport and patrol aircraft are using EFBs in a non-connected Class 1 fashion. In the future, Moore says he expects large military aircraft cockpits to adopt EFBs in a similar way that civil aviation has embraced these devices.

"They also understand the capability that connecting EFBs to the aircraft could give them," Moore says. Military pilots also have different needs from their EFB displays, such as compatibility with night-vision devices, Moore points out.

Tactical aircraft like jet fighter and attack aircraft, however, may be a different story. Moore says zero to 1 percent of tactical military pilots are using any kind of EFB capability in the cockpit today, and those only in a Class 1 capacity.

Fighter pilots need smaller-sized EFBs that could function not as an EFB, but instead as an "electronic knee board" that would strap to their thighs for quick reference. This need will require small tablets like the Apple iPad Mini, Moore says.

The technology exists today that is small enough to connect tactical military aircraft electronic knee boards to aircraft systems, but a lot of work needs to be done to find the best ways of integrating EFB technology into the small confines of the jet fighter cockpit. Eventually, however, this technology is expected to take hold in the tactical military aviation world.

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 Kristi Guillemette
603 891-9126/ kristig@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 & EASTERN CANADA & UK
Bob Collopy, Sales Manager
603 891-9398 / Cell 603 233-7698
FAX 603 686-7580 / bobc@pennwell.com

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

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

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

Corporate Officers
CHAIRMAN Frank T. Lauinger

PRESIDENT AND CEO Robert F. Biolchini

CHIEF FINANCIAL OFFICER Mark Wilmoth

Technology Group
SENIOR VICE PRESIDENT/PUBLISHING DIRECTOR
Christine Shaw

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

BPA WORLDWIDE

AMERICAN BUSINESS MEDIA
The Association of Business Media Companies

ADVERTISERS INDEX

new PRODUCTS

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

RUGGED COMPUTERS

Airborne servers offered by Kontron

Kontron in Poway, Calif., is introducing the ACE Flight 600 general-purpose airborne servers with an integrated 4G LTE modem for crew and passenger Web servers, flight maintenance or manifest servers, connectivity server, wireless content server, and in-flight entertainment (IFE) media servers. This embedded computing upgrade to the ACE Flight Server platform provides the airlines a 3X or greater increase in the amount of wireless content loaded during aircraft turnarounds when compared to the previous 3G modem version. The airborne server for Ethernet-based network installations on both linefit and retrofit aircraft integrates a dual core 1.5 GHz Intel Core i7 processor and 16 gigabytes of DDR3 memory with removable solid-state storage.

FOR MORE INFORMATION visit **Kontron online** at *www.kontron.com*.

CABLING

Flexible cables for military applications in harsh vibration introduced by Cicoil

Cicoil Corp. in Valencia, Calif., is introducing flexible cables for applications exposed to harsh vibration caused by propelling force, excessive turbulence, intense wind, driving rain, and rough seas. Cicoil uses a process of surrounding and encapsulating conductors in its shock absorbing Flexx-Sil rubber jacket that renders them unaffected by constant shaking, sudden influence, severe vibration, G-Forces, temperatures from -65 to 260 degrees Celsius, salt corrosion, submersion in water, humidity, chemicals, ozone, radiation, UV light, and the rigors of supersonic flight.

FOR MORE INFORMATION visit **Cicoil** online at *www.cicoil.com*.

RUGGED CONNECTORS

TTI introduces harsh-environment connectors from TE Connectivity

Electronics distributor TTI Inc. in Fort Worth, Texas, is introducing the DEUTSCH 369 connector series from TE Connectivity in Harrisburg, Pa., for harsh-environment aerospace applications like in-flight entertainment and power in civil aircraft. Designed to provide a high-reliability, lightweight, compact, and cost-efficient interconnect solution, the TE DEUTSCH 369 Series is particularly suited to harsh-environment applications that include high vibration and moisture. Sealed for use in areas with high moisture levels and

manufactured from high-performance composite materials, the interconnects conform to the smoke, toxicity, and flammability requirements of FAR 25.

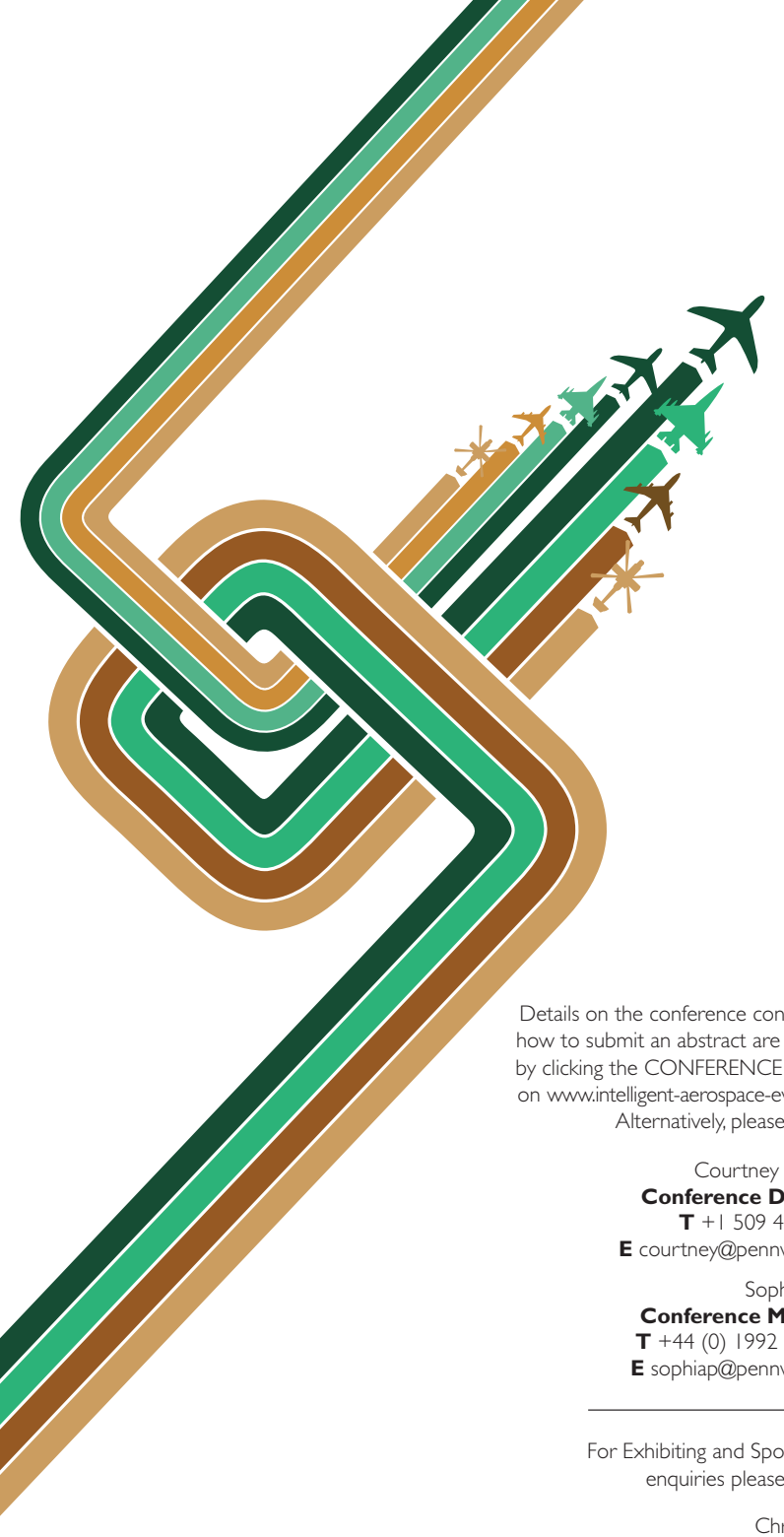
FOR MORE INFORMATION visit **TE Connectivity** at *www.deutsch.net*.

BACKPLANES

OpenVPX backplanes for ground and airborne applications introduced by Curtiss-Wright

The Curtiss-Wright Corp. Defense Solutions division in Ashburn, Va., is introducing three Hybricon central-switched Fabric40 OpenVPX backplanes and two Gen3 OpenVPX-optimized Fabric40 OpenVPX pass-through backplanes for demanding ground and airborne surveillance and electronic warfare applications. They deliver more than two times the embedded computing performance of previous-generation Serial RapidIO (SRIO) Gen-2-based systems and 4x the performance of 10 Gigabit Ethernet. The Gen3 OpenVPX backplanes support full-speed, bottleneck-free distribution of data over Gen3 PCI-Express 40 gigabits per second Ethernet or Infiniband fabrics. With signal integrity technology, these backplanes are for demanding defense and aerospace EW, SIGINT, and radar applications, such as the real-time detection and identification of signals of interest.

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



INTELLIGENT AEROSPACE™

CONFERENCE AND EXHIBITION
6 – 8 OCTOBER 2015
PTA • AMSTERDAM • THE NETHERLANDS
www.intelligent-aerospace-event.com

IMAGINATION **INNOVATION** INTEGRATION

CALL FOR PAPERS NOW OPEN

Submit an abstract for Intelligent Aerospace
Abstract submission deadline: 21 January 2015

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

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

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

Topics include:

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

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

Courtney Howard
Conference Director
T +1 509 413 1522
E courtney@pennwell.com

Sophia Perry
Conference Manager
T +44 (0) 1992 656 641
E sophiap@pennwell.com

For Exhibiting and Sponsorship enquiries please contact:

Chris Cope
Exhibit and Sponsorship Sales Manager
T +44 (0)1992 656 665
M +44 (0)7534 856 101
E chrisc@pennwell.com

Module and System-Level Solutions from X-ES

Intel® and Freescale™ Single Board Computers

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

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

High-Performance FPGA and I/O Modules

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

Secure Ethernet Switches and IP Routers

XPedite5205
Secure Gigabit Ethernet router XMC utilizing **Cisco™ IOS®**

XChange3018
3U VPX 10 Gigabit Ethernet managed switch and router

High-Capacity Power Supplies

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

Rugged, SWaP-Optimized, COTS-Based Systems

XPand4200
Sub-½ ATR, 6x 3U VPX slot system with removable SSDs

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

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

X-ES
Extreme Engineering Solutions
608.833.1155 www.xes-inc.com

Designed, manufactured, and supported in the USA