AUGUST 2016

Military & Aerospace Electronics

ENABLING TECHNOLOGIES FOR NATIONAL DEFENSE

The myth of stealth

Today's radar can find anything, stealth aircraft included. PAGE 2

Encryption and cybersecurity

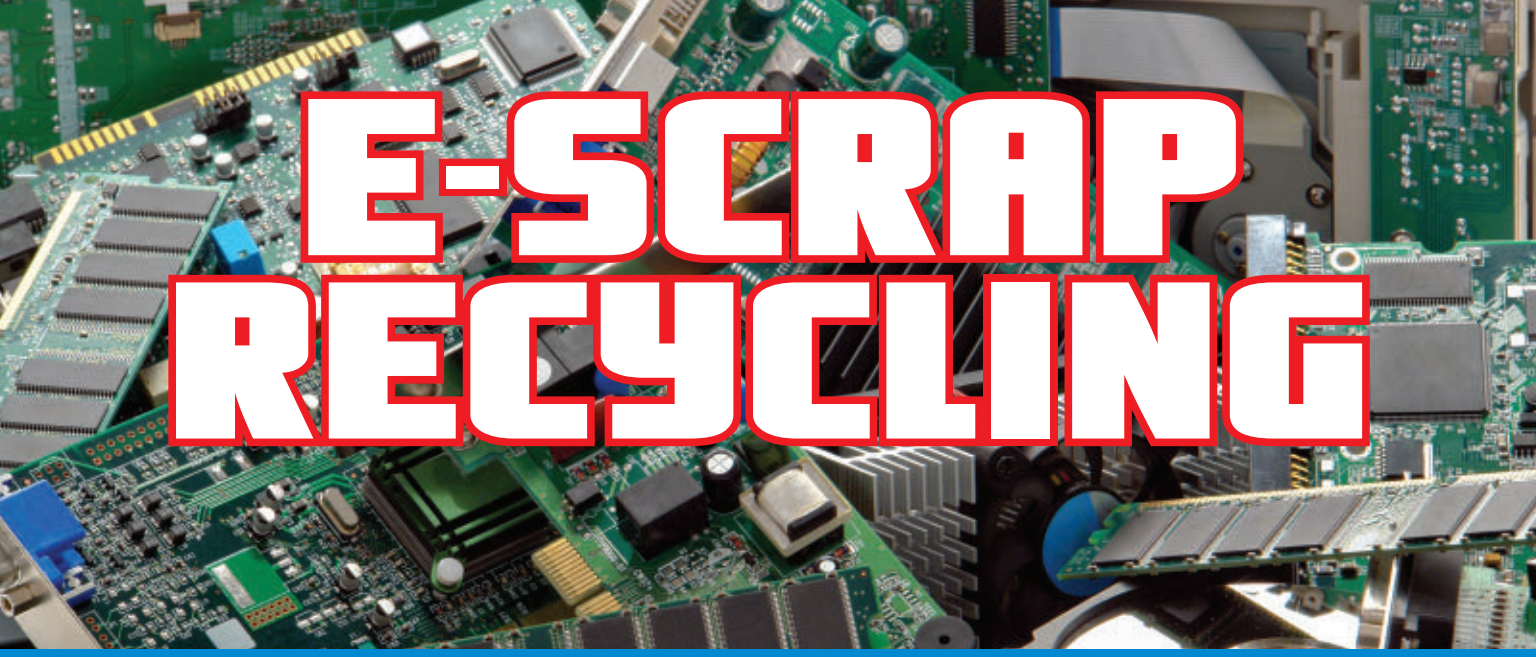
Designers capitalize on COTS technology to secure modern data. PAGE 18

militaryaerospace.com

Electronic warfare

Battle heating up for the electromagnetic spectrum. PAGE 10

PennWell®

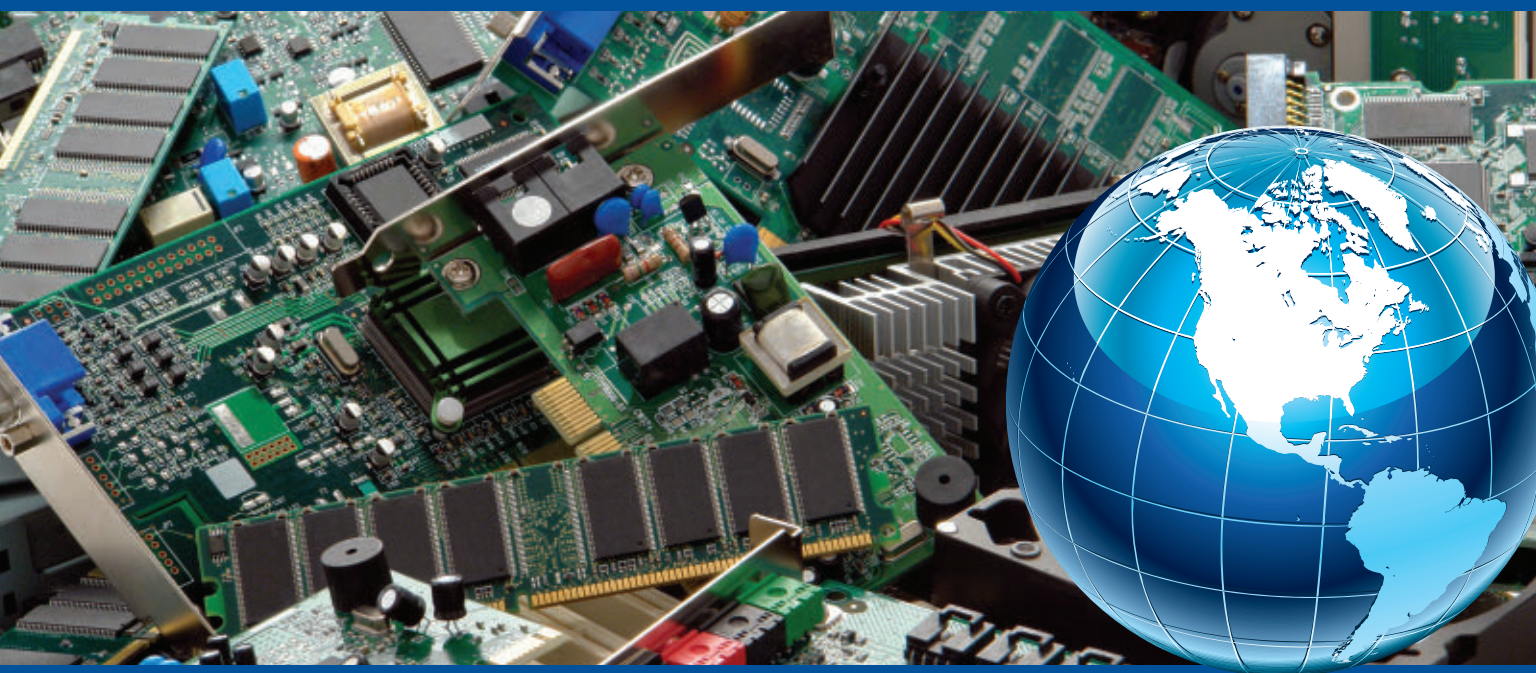


E-SCRAP RECYCLING

QML Inc.

Serving the globe

- Advances
- Hedging / Pre-Sales
- Freight Financed & Insured
- Now Offering Domestic Sampling

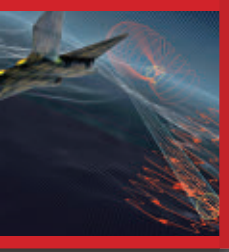


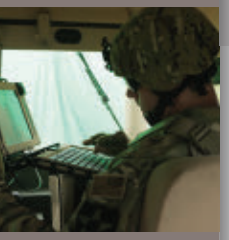
East Coast: **(401) 490-4555** West Coast: **(480) 459-0766**

272 Ferris Avenue • Rumford, RI 02916 • **www.qml.us**

AUGUST 2016
VOL. 27, NO. 8

Military & Aerospace Electronics





BY **JOHN KELLER**, EDITOR IN CHIEF

The siren song of radar-evading stealth aircraft

The U.S. military and its allies increasingly rely on so-called stealth technology to conceal manned and unmanned aircraft from enemy radar. We forget, however, that radar is adapting quickly, and it's only one of many ways to detect aircraft.

Stealth technology has been one of the most expensive and closely guarded military secrets since it first appeared in the mid-1980s, with aircraft like the now-obsolete F-117.

Stealth uses angles and coatings to compromise the effects of enemy radar. It attempts to deflect and absorb radio waves to fool enemy radar into thinking an aircraft is something other than what it really is.

Let's be clear: stealth technology — no matter how sophisticated — doesn't make an aircraft invisible to radar. It simply enables an aircraft to hide in radar clutter.

Today's radar systems are amazingly sensitive — so sensitive, in fact, that one of the biggest radar signal-processing challenges today isn't detecting targets, but filtering out unwanted signals. Today's radar systems can detect and track targets as small as insects and birds, so an aircraft of any size, any shape, and any material isn't really a big problem.

Weather radar is designed to track wind currents and concentrations of rain, and is becoming effective in helping predict severe weather events like thunderstorms and tornadoes. Rain isn't difficult for radar; it provides a nice return signal when its RF energy bounces off its water droplets.

Wind is something different; there's nothing in moving air itself that can provide a radar return. Instead, weather radar detects things blowing around in the wind — bugs, birds, leaves, and other solid objects that can reflect a radar signal. Ornithologists are using the signals from weather radar to track the annual bird migrations. If a radar can do this, rest assured it can detect even the smallest aircraft. The trick for radar designers is to know what they're looking for, and tune their radar systems and digital signal processing accordingly.

It follows, then, that stealth technology seeks to fool radar systems into filtering out their signals with the rest of the unwanted data. Once again, stealth aircraft aren't invisible to radar; they're just really sneaky about hiding in the radar clutter.

As radar systems become more sophisticated, as their digital signal processing algorithms become more advanced, and as signal-processing computers get faster, designing a stealth aircraft that can hide from radar will become prohibitively difficult and expensive to do.

We should think about this when we see reports about new stealth-detecting radar systems. Russia's powerful over-the-horizon Podsolnukh (Sunflower) radar reportedly is capable of detecting and tracking stealthy fifth-generation aircraft like the Lockheed Martin F-35 or any other fighter jet designed to avoid detection.

If these reports are true, the Russian Sunflower radar isn't magic; it's just one step ahead in the cat-and-mouse game we call electronic warfare (EW). Aircraft designers will adjust, as will radar designers. There's really no end in sight, but I would guess that eventually no aircraft will be able to hide from radar.

The problem gets worse if we stop fixating on radar as the only way to detect and track aircraft. There's more ways than radar to find a plane.

Think a sophisticated adversary trying to detect and track stealth aircraft is using only radar? I doubt it. They're also listening and looking with sophisticated acoustic and electro-optical sensors. Against these kinds of measures a so-called stealth aircraft is helpless — until he can fly silently and reflect no light whatsoever, and that's not happening any time soon.

Is there really such a thing as a stealth aircraft? That's getting harder and harder to accept.

RUGGED EMBEDDED INTEL 3U VPX SBCS

X-ES offers a portfolio of 3U VPX Intel® processor-based Single Board Computers featuring up to 16 GB of DDR4-2133 ECC SDRAM and a diverse array of I/O.

Integrated SecureCOTS™ technology with onboard, user-configurable FPGA modules supports hosting custom functions to protect data from being modified or observed and provides an ideal solution when stringent security capabilities are required.

Choose from our standard COTS products or work with our embedded computing experts to develop a custom solution to match your exact project requirements. Depend on X-ES embedded computing hardware in even the most extreme environments.

X-ES

Extreme Engineering Solutions

608.833.1155 www.xes-inc.com

MADE IN THE USA

Designed, manufactured, and supported in the USA

IN BRIEF

Bowhead to build aviation data management systems for Navy carriers

Naval Air Warfare Center Aircraft Division officials in Lakehurst, N.J., awarded a $9.7 million contract to Bowhead Manufacturing Technologies in Plano, Texas, to build four Aviation Data Management and Control System Block II, Phase 1 ship sets. The tactical data management system communicates real-time aviation and command-related data across the system's local area network and integrated shipboard network system, connecting the air department, ship divisions, and embarked staff who manage aircraft launch and recovery operations aboard surface warships.

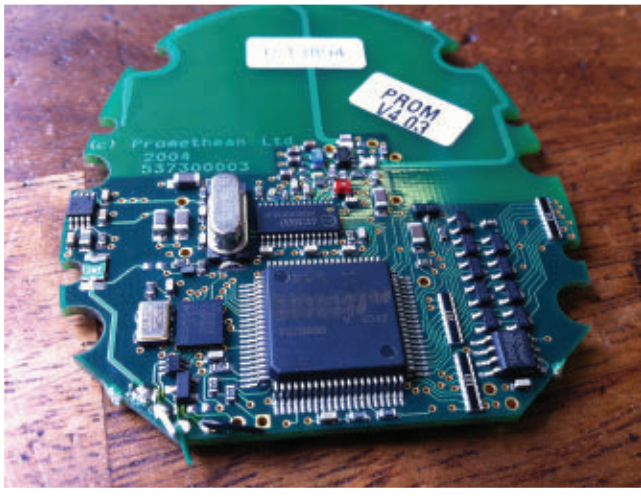
Lockheed Martin to build submarine-launched ballistic missiles

U.S. Navy strategic weapons experts are preparing to buy submarine-launched nuclear ballistic missiles capable of destroying city-sized targets virtually anywhere. Officials of the U.S. Navy Strategic Systems Program Office in Washington announced a $21.8 million contract to Lockheed Martin Space Systems in Sunnyvale, Calif., for long lead items to support the fiscal 2017 Trident II D5 missile production schedule. The Trident II D5 advanced submarine-launched

Northrop Grumman zeroes-in on technologies to protect military from counterfeit electronics

BY JOHN KELLER

ARLINGTON, Va. — Defense microelectronics experts at the Northrop Grumman Corp. Mission Systems segment in Linthicum, Md., are moving forward on a U.S. military research initiative to safeguard the military electronics supply chain from substandard used and counterfeit electronics.



Northrop Grumman microelectronics experts are moving closer to developing tools to combat the problem of counterfeit electronic parts.

Officials of the U.S. Defense Advanced Research projects Agency (DARPA) in Arlington, Va., announced a $7.3 million contract option for the second phase of the DARPA Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program.

In the program's second phase, Northrop Grumman engineers will continue work on a tool to verify the trustworthiness of protected electronic components without disrupting or harming the system into which they have been designed.

Used and counterfeit electronic components are widespread throughout the defense supply chain, DARPA officials say.

Suspect electronic components present a critical risk in military systems where a malfunction of a single part could lead to system failures that can put warfighter lives and missions at risk.

In the SHIELD program's first phase, Northrop Grumman experts worked to develop a 100-by-100-micron component, or dielet, that authenticates electronics components. The dielets have encryption engines and sensors to detect tampering that affix to electronic components like microchips.

The SHIELD program's goal is to provide 100 percent assurance against recycled components that are sold as new; unlicensed overproduction of authorized components; test rejects and substandard components sold as high quality; parts marked with falsely elevated reliability or newer date of manufacture; low-quality clones and copies

that may include hidden functionality; and components that are covertly repackaged for unauthorized applications, DARPA officials say.

SRI International in Menlo Park, Calif., and Charles Stark Draper Laboratory in Cambridge, Mass., joined Northrop Grumman on the DARPA SHIELD program's first phase. The three companies won SHIELD phase-one contracts in January 2015.

"SHIELD demands a tool that costs less than a penny per unit, yet makes counterfeiting too expensive and technically difficult to do," says Kerry Bernstein, the SHIELD program manager at DARPA.

"The dielet will be designed to be robust in operation, yet fragile in the face of tampering," Bernstein says. "What SHIELD is seeking is a very advanced piece of hardware that will offer an on-demand authentication method never before available to the supply chain."

Northrop Grumman, Draper, and SRI experts in phase one developed dielets that can be inserted into an electronic component's package at the manufacturing site or affixed to existing trusted components, without any alteration of the host component's design or reliability.

The companies designed dielets with no electrical connections to the host component, such that authenticity testing can be done anywhere with handheld or automated probes. After a scan, an inexpensive appliance like a smartphone will upload a serial number to a central, industry-owned server. The server sends an unencrypted challenge to the dielet, which sends back an encrypted answer and data from passive sensors (like light exposure) that could indicate tampering.

The contract option brings the total cumulative face value of the company's SHIELD contract to $19.6 million from $12.3 million.

On the second phase, Northrop Grumman will do the work in Linthicum, Md.; Albuquerque, N.M.; Santa Clara, Calif.; Reston, Va.; Lubbock, Texas; and Atlanta, and should be finished by January 2018.

FOR MORE INFORMATION
visit Northrop Grumman Mission Systems online at *www.northropgrumman.com*, and DARPA at *www.darpa.mil*.

IN BRIEF

atomic missile has a range of 4,000 to 7,000 miles, was first deployed in 1990, and is scheduled to remain in service until 2027.

BAE Systems investigates ability to grow tiny drones from chemicals

Scientists and engineers envision ways to grow small unmanned aerial vehicles (UAVs) in labs through chemistry, in a matter of weeks, rather than years. A new machine called a Chemputer could enable advanced chemical processes to grow aircraft and some of their complex electronic systems, as well as produce multifunctional parts for large manned aircraft. Engineers and scientists at BAE Systems and the University of Glasgow are working on this organic approach to manned and unmanned aircraft design.

Battelle to build armored SUVs with Special Forces vetronics

Unconventional warfare experts are developing armored sport utility vehicles (SUVs) with military-grade vetronics, communications, night vision, ballistic protection, mobility, and tires designed to survive small-arms fire. Military vehicles experts at U.S. Special Operations Command (SOCOM) at MacDill Air Force Base, Fla., are looking to Battelle Memorial Institute in Columbus, Ohio, for the five-year, potential $170 million Non-Standard Commercial Vehicles program.

Navy asks Boeing to upgrade networking and communications on Poseidon aircraft

BY JOHN KELLER

PATUXENT RIVER NAS, Md. — Military avionics experts at the Boeing Co. are making several improvements to the P-8A Poseidon maritime patrol aircraft avionics to upgrade the ability to detect, track, and attack enemy submarines and surface ships. These improvements, expected to become operational in 2020, also will enhance the Poseidon's signals intelligence (SIGINT) capabilities, as well as its ability to network its onboard subsystems and network with other military systems.

Officials of the U.S. Naval Air Systems Command at Patuxent River Naval Air Station, Md., announced a $71.6 million order to Boeing Defense, Space & Security in Seattle to build, integrate, and test several Poseidon Increment 3 Block I capabilities.

This order to Boeing is part of the third of three phases of planned improvements to the Poseidon aircraft, a ruggedized version of the Boeing 737 single-aisle jetliner hardened for long-range maritime patrol and anti-submarine warfare (ASW) missions.

Among the improvements involved in this order are Link 16 communications networking; the AGM-84N Harpoon II+ anti-ship missile; integrated broadcast system receiver and filtering; high-frequency (HF) radio upgrades; targeting improvements; and narrowband satellite communications (SATCOM) capability. These upgrades pertain not only to U.S. P-8A Poseidon aircraft, but also Poseidon planes operated by Australian military forces.

Link 16 is a U.S. and NATO military tactical data exchange network that enables military aircraft, ships, and ground forces to exchange their tactical picture in near real time. It supports text messages, imagery, and two channels of digital voice communications at 2.4 kilobits per second and 16 kilobits per second.

The Navy is asking Boeing to upgrade the P-8A Poseidon maritime patrol plane's ability to detect, track, and attack enemy submarines and surface ships.

Boeing AGM-84N Harpoon Block II+ is an anti-ship and land-attack missile with over-the-horizon range. It has a common datalink and new global positioning system (GPS) satellite navigation guidance. The Harpoon Block II+ is expected to be integrated aboard the Poseidon as the plane receives new networking capabilities.

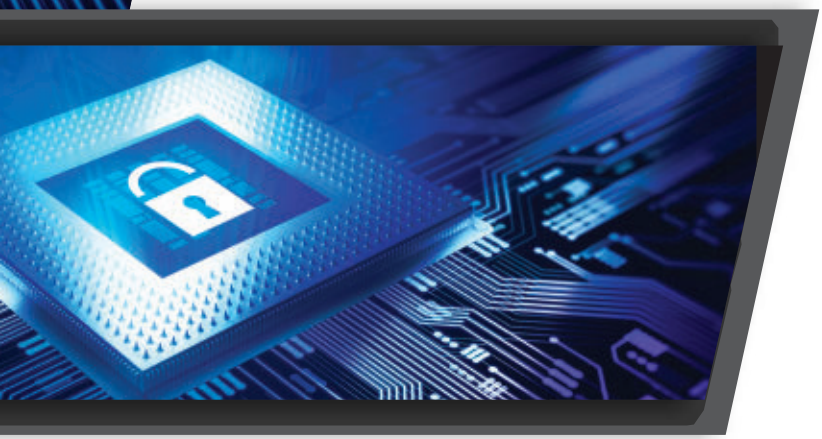
Planned Poseidon Increment 3 Block II upgrades are expected to improve the aircraft's radar abilities to identify, track, and attack threats on land and at sea with the Raytheon AN/APS-154 Advanced Airborne Sensor (AAS).

Boeing will do the work in Puget Sound, Wash.; Grand Rapids, Mich.; St. Louis; Patuxent River, Md.; Dallas; Oklahoma City; and El Paso, Texas, and should be finished by February 2019.

FOR MORE INFORMATION visit Boeing Defense, Space & Security online at *www.boeing.com/defense*.

Innovation **That's Secure.**

MERCURY IS THE FIRST COMMERCIAL-ITEM COMPANY TO DESIGN AND MANUFACTURE PROCESSING SOLUTIONS FOR THE WHOLE SENSOR PROCESSING CHAIN. OUR RUGGED OPEN SYSTEM ARCHITECTURE SOLUTIONS ARE DESIGNED AND MADE IN AMERICA, LEVERAGING PROVEN COMMERCIAL TECHNOLOGY SOURCED THROUGH TRUSTED SUPPLY CHAINS. FOR INFORMATION ASSURANCE, MERCURY IS THE BETTER ALTERNATIVE.



MERCURY SYSTEMS™

INNOVATION THAT MATTERS™

MADE IN AMERICA

Visit mrcy.com/secure and download our technical whitepaper: Secure Processing Solutions for the Defense and Intelligence Industry

Lockheed Martin to develop Special Ops mini-sub based on commercial technologies

BY JOHN KELLER

MacDILL AIR FORCE BASE, Fla. — Undersea warfare experts at Lockheed Martin are making another run at designing an affordable mini-submarine to transport Special Operations combat swimmers covertly while minimizing swim time to keep the divers from becoming too exhausted to carry out their missions.

Officials of the U.S. Special Operations Command (SOCOM) at MacDill Air Force Base, Fla., announced a $166 million contract to the Lockheed Martin Mission Systems and Training segment in Riviera Beach, Fla., for the Dry Combat Submersible (DCS) program. Lockheed Martin experts will design, build, test, and maintain a dry-environment diver lock-in/lock-out undersea-mobility capability by designing and procuring commercially classed submersibles for use by Special Forces in special operations environments.

The contract is necessary to fill a capability gap for surface-launched dry submersibles for use in harsh maritime environments. Lockheed Martin will capitalize on commercially available submersible technologies and international classing safety certification to keep costs down.

This project represents SOCOM's latest attempt at the expensive, time-consuming job of developing mini-submarines to transport Special Forces warfighters covertly underwater to operational areas.

SOCOM officials have been planning a submersible combat swimmer delivery system since cancelling the Joint Multi-Mission Submersibles program in 2010 because it was too expensive.

In April 2012, SOCOM awarded a contract to Lockheed Martin to prototype a medium-sized DCS undersea vehicle. Later that year, SOCOM awarded a potential $44.3 million contract to submarine maker General Dynamics Electric Boat in Groton, Conn., to prototype a lightweight DCS mini-submarine to deliver combat swimmers.

Lockheed Martin is attempting to design an affordable mini-submarine based on commercially available technologies to transport Special Forces combat swimmers

The medium-sized DCS was to be about 38 feet long with high endurance and high passenger and cargo capability that will be operated from specially configured commercial surface ships, and potentially from future submarine shelter systems. The lightweight DCS, meanwhile, was to be about 24 feet long with moderate endurance and moderate passenger and cargo capability to operate from specially configured commercial surface ships.

These SOCOM DCS projects sought to design and build prototype one-atmosphere, special operations dry combat submersibles of two different sizes to be free-swimming vehicles capable of delivering and extracting teams of combat swimmers.

Now SOCOM combat swimmer experts are working with Lockheed Martin to develop a more-affordable DCS version based on commercially available technologies, rather than developing Special Forces mini-submarines from scratch.

The DCS kind of mini-submarine is intended to operate from combat support surface ships or submarines. These DCS vessels are to deliver special operations warfighters to their mission areas ready to fight, rather than exhausted by long swims.

The light and medium DCS undersea vehicles were to move at speeds of at least five knots, at depths to 200 feet, with provisions for two pilots.

Those dry submersibles were to be sized to transport aboard C-5 or C-17 cargo jets, or in standard 40-foot surface ship containers. The DCS submersibles were to have military radios, military sonars, and high-power, silver-zinc batteries.

Lockheed Martin will receive $26.8 million up-front, and will try to earn the remainder of the contract value through successful research and demonstrations. Lockheed Martin was chosen for the job over 33 other companies that had expressed interest.

On this contract Lockheed Martin will do the work in Riviera Beach, Fla., and in the United Kingdom, and should be finished by January 2022.

FOR MORE INFORMATION visit Lockheed Martin online at *www.lockheedmartin.com/us/mst*.

Army Corps on lookout for data storage to replace obsolete subsystems

BY JOHN KELLER

HUNTSVILLE, Ala. — Information technology (IT) experts at the U.S. Army Corps of Engineers are on the lookout for new data storage subsystems to replace obsolete data storage items at all affected Army Corps of Engineer locations.

The Army Corps of Engineers in Huntsville, Ala., announced an $8 million contract to World Wide Technology Inc. in Maryland Heights, Md., to buy data storage hardware, software, and maintenance, to replace the Corps' obsolete data storage items.

The Army Corps of Engineers requires a wide variety of IT equipment, including data storage in its building and water-management activities.

The Army Corps of Engineers is working with World Wide Technology to replace the Corps' obsolete data storage systems.

The Corps builds and operates locks and dams; flood protection; military facilities; and restores ecosystems throughout the U.S. and the world. The organization has about 37,000 civilians and soldiers to deliver engineering services to customers in more than 130 countries worldwide.

On this contract World Wide Technology will do the work in Maryland Heights, Md., and should be finished by March 2017. World Wide prevailed over five other companies for this data-storage job.

FOR MORE INFORMATION visit World Wide Technology online at *www.wwt.com*, or the Army Corps of Engineers-Huntsville at *www.hnc.usace.army.mil*.

Today's battle for the electromagnetic spectrum

U.S. and allied military forces are working on new electronic warfare, cyber warfare, spectrum warfare, and information warfare systems to seize and hold control of communications, radar, and other important sensors.

BY **J.R. Wilson**

The BAE Systems electronic attack technology uses directed energy to attack, degrade, or neutralize an adversary.

Cyber warfare, information warfare, electronic warfare (EW), spectrum warfare, electromagnetic maneuver warfare. Those are only some of the names by which U.S. military experts describe their offensive and defensive use of the electromagnetic spectrum.

Some believe it all should be combined under just one term — Spectrum Warfare or Electromagnetic Maneuver Warfare. Its label, however, is not nearly so important as recognizing the new and rapidly evolving reality of this complex global environment, according to former Chief of Naval Operations retired Adm. Jonathan Greenert.

"The electromagnetic spectrum is an essential — and invisible — part of modern life [military and civilian]. Our military forces use wireless computer networks to coordinate operations and order supplies, use radars and sensors to locate each other and the enemy, and use electronic jammers to blind enemy radars or disrupt their communications," Greenert says. "With wireless routers or satellites part of almost every computer network, cyberspace, and the electromagnetic spectrum now form one continuous environment."

Spectrum warfare is just as important as any other traditional domain of war, Greenert insists. "This environment is so fundamental to naval operations — and so critical to our national interests — that we must treat it on par with our traditional domains of land, sea, air, and space," Greenert says. "In fact, future conflicts will not be won simply by using the electromagnetic spectrum and cyberspace; they will be won within the electromagnetic spectrum and cyberspace. This will require changes to our operating

RF Solutions From RF Engineers

Largest selection ✓

Expert technical support ✓

Same day shipping ✓

Armed with the world's largest selection of in-stock, ready to ship RF components, and the brains to back them up, Pasternack Applications Engineers stand ready to troubleshoot your technical issues and think creatively to deliver solutions for all your RF project needs. Whether you've hit a design snag, you're looking for a hard to find part or simply need it by tomorrow, our Applications Engineers are at your service. Call or visit us at pasternack.com to learn more.

866.727.8376
www.pasternack.com

PASTERNACK®
THE ENGINEER'S RF SOURCE

Small jammers that disrupt GPS signals are available at low cost that can fit in a car's cigarette lighter.

concepts, military systems, and — most importantly — a new way of thinking in our Navy."

Dino Mensa, chief engineer for electromagnetic spectrum dominance/electromagnetic maneuver warfare at the Naval Air Warfare Center-Weapons Division at Point Mugu, Calif., says the nature of that environment and the technologies being developed to operate safely within it will require multifunction and multimission systems.

"Increasingly, as we move forward, the lines between offense and defense are blurring," Mensa says. "To be effective in defense, you need to look to offensive capabilities to disrupt the enemy's ability to understand what is coming in. So we are moving away from a single box aboard a single platform to a more holistic mission look incorporating both offense and defense to get the job done. Still, there remain operational requirements differences between the services, he points out.

"My perception is the Navy is operating in the large, very capable multimission platform mode," Mensa says. He uses the F-35 Joint Strike Fighter (JSF) and the Next-Generation Jammer (NGJ) as multi-billion-dollar programs taking on the world. Other services, such as the U.S. Marine Corps, focus more on modular, reprogrammable, rapidly deployable, reconfigurable system payloads for specific missions; these mission-specific systems solve all EW issues.

Role of commercial technology

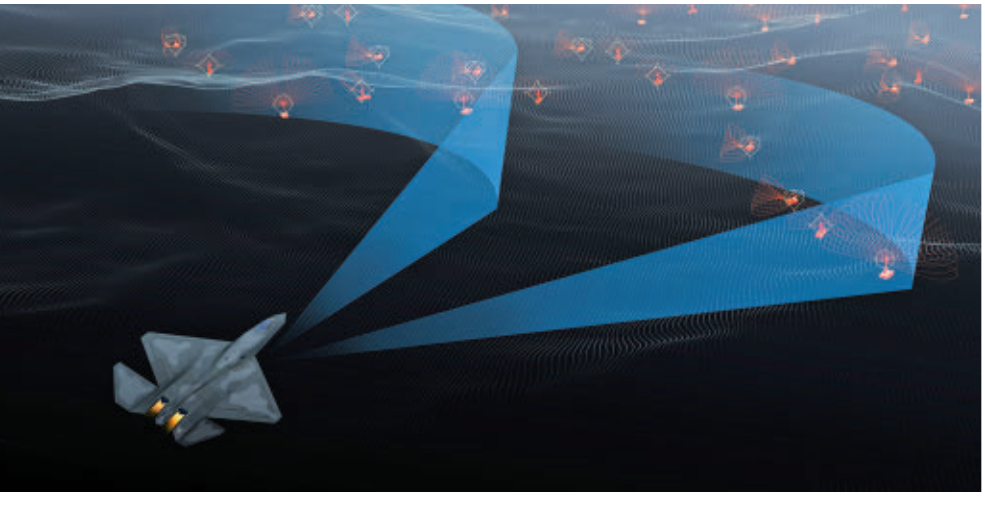
EW once largely was a U.S. domain, as evidenced by such archaic terms as information dominance. For the last 25 years or so, however, military-specific spectrum research has been dwarfed by the commercial telecommunications industry and the global proliferation of the now-ubiquitous smartphone. That followed and further spurred commercial dominance in the evolution of faster, smaller, cheaper computer processors, memory, displays, and cameras.

As a result, it became possible for any nation or terrorist group, regardless of size or military budget, to challenge the U.S. in various aspects of EW by developing or buying inexpensive GPS jammers. Without GPS, America would be in danger of losing the edge provided by its successful precision-guided munitions.

"Right now, we're at a major juncture in EW. The proliferation of commercial technology in the telecom world has really accelerated everybody's capabilities. In the 1990s and before, the U.S. was dominant in a lot of specialized EW technology. But with the growth of the commercial wireless market, a lot of other countries now have that technology," warns Joshua Niedzwiecki, director of sensor processing & exploitation at BAE Systems Electronic Systems segment in Nashua, N.H.

To counter that, Niedzwiecki adds, the U.S. Department of Defense (DOD) is seeking the help of the defense industry through their "third offset strategy," announced by the Pentagon in November 2014, "to identify and invest in innovative ways to sustain and advance America's military dominance for the 21st Century".

Historically, the first offset essentially was the threat of America's then-dominant nuclear force to counter the Soviet Union's overwhelming advantage in conventional forces in Europe. As the Soviets



The BAE Systems electronic support technology intercepts, identifies, and locates sources of radiated electromagnetic energy for threat recognition.

began to match U.S. nuclear power, a second offset strategy was devised, calling on the U.S. Defense Advanced Research Projects Agency (DARPA) to help integrate all promising new non-nuclear military technologies into a system-of-systems for joint-force deep attack.

Now the advantages of that strategy also are eroding in the face of several adversaries — from small regional states to near-peer and peer major powers to terrorist organizations with advanced capabilities — and easy access to advanced, commercially developed, technologies.

As a result, a host of new terms and innovations, many that seem to come straight from the pages of science fiction, are moving toward center stage in the next evolution of EW.

Cognitive EW

"Cognitive EW is one area in which we are involved in that. It really is merging a lot of advances in artificial intelligence (AI) and machine learning technology, allowing the use of massive amounts of data. DOD is looking at how to leverage that to give our weapons systems an advantage," says BAE Systems' Niedzwiecki. "One of the things my group does, focusing on processing and AI, with expertise in physics, signals processing, AI and machine learning, is research to make our sensors smarter across the board, including cognitive EW as part of the third offset strategy.

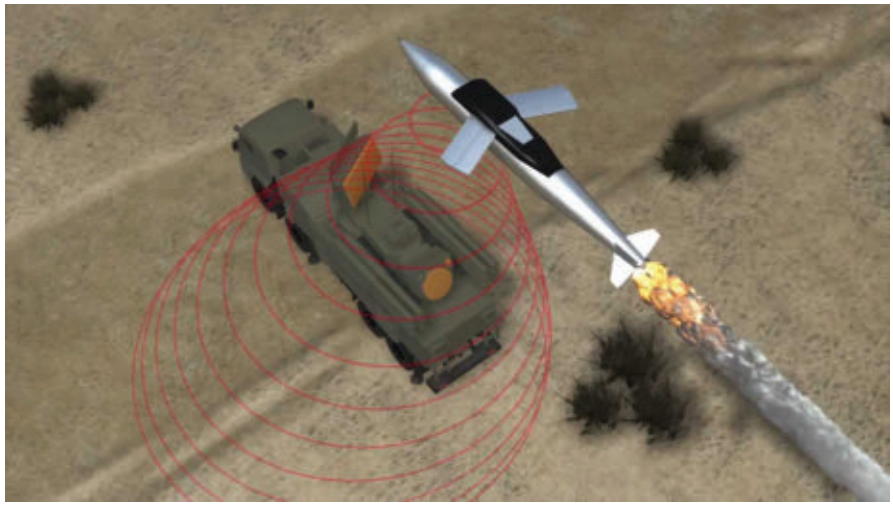
"As you go into an area the threat now, because they can change signal structure and quickly adapt frequencies, is you don't have a lot of prior knowledge to draw from," Niedzwiecki continues. "Cognitive EW is trying to be smarter, putting that intel into the sensor, and allowing the EW system to adapt, on the fly, in real time during the mission, based on what it is observing and how well it is performing. For example, if you see a radar threat with characteristics you've never seen before and try to jam it, cognitive EW measures how effective you are in keeping that radar from seeing you. And it remembers what works so you can use that same technology the next time you see it."

Larry Rexford, EW strategy & marketing manager at Rockwell

Collins in Cedar Rapids, Iowa, has been involved in electronic warfare for 35 years, the first 25 as an Air Force officer, including EW director in the Pentagon Requirements Directorate. In his estimation, the state-of-the-art in EW is the systems deployed on U.S. 5th generation fighters — Lockheed Martin's F-22 Raptor and F-35 Lightning II — and the data collection and processing capabilities of the Boeing RC-135 Rivet Joint reconnaissance aircraft.

Only the Air Force flies the F-22, however, and that aircraft no longer is in production. The oft-delayed F-35 has yet to achieve full operational capability and deployment.

"Internationally, coalition collection capabilities are not on par with the RC-135, except the U.K., which now has that platform, so [our allies] rely on support from the U.S. in that mission," Rexford says. For example, there are two vacant EW officer positions on the NATO staff. Outside of Tier 1 nations, such as the U.K. and Australia, which is buying the Growler [Boeing E/A-18G electronic attack aircraft], no one is really investing in this.



The U.S. Air Force is developing new antennas for manned and unmanned aircraft that disrupt enemy electronics with high-power microwaves.

Capabilities of adversaries

"In terms of potential adversaries, Russia integrated EW attack capabilities into air maneuver elements and were able to create huge advantages against Ukraine," Rexford continues. "By doing that, they disrupted communications and situational awareness to an extent the Ukrainian military could not act as quickly as Russia could pivot."

The Chinese also have advanced EW capabilities to confront U.S. forces. "You hear more about China in terms of cyber threats," Rexford says. "The Chinese always play a long game, geopolitically. I think they have developed airborne EW capability, but haven't employed it as the Russians did. I know they have collection capability and probably attack, but I don't know if they have integrated those into operations."

Rexford describes himself as a "traditionalist" in the warfighting domain. "You have to be able to sense, protect yourself in the electromagnetic spectrum, and attack to achieve effects — degrade, deny, even destroy. When you execute warfare in the electromagnetic spectrum effectively, you have effects in air, land, and naval applications. There are new requirements. On the collection side, spread spectrum signals — the new AESA radars and lower power radars such as maritime surveillance — are creating a requirements pull for wide instantaneous bandwidth capability.

"We're also seeing requirements for more autonomous capabilities. Cognitive and self-learning capabilities aren't fielded yet, but are popping up in some new programs," Rexford says. "If you are looking at an adversary using systems that can change frequencies, you're always trying to catch up. So we need to collect the signals, but also have cognitive, self-learning systems that can identify that and then, on the fly, check its own records to see what is the best way to adapt to those. On the attack side, you see a corresponding requirement to self-learn and self-apply."

DOD, with its third offset strategy, is responding to not only Russian EW integration successes and Chinese long-term electromagnetic strategies, but also to the proliferation of various types and levels of EW offensive and defensive capabilities to second and third tier nations and terrorist organizations.

Electronic warfare proliferation

In June, for example, the Air Force Life Cycle Management Center awarded a four-year, $118.5 million sole-source contract to Raytheon Missile Systems in Tucson, Ariz., for

an additional lot of Miniature Air-Launched Decoy Jammers (MALD-J), which are small unmanned aircraft that jam enemy radar while spoofing the characteristics of much larger U.S. and allied aircraft. The goal is to force enemy missile batteries to fire ground-to-air missiles at the wrong targets, thus clearing a path for real manned attack aircraft when those enemy missiles are depleted.

At West Point, Army cadets are being trained in the use of inexpensive "cyber rifles" to shoot down low-flying commercial unmanned aerial vehicles (UAVs), such as those Russia used against Ukraine. While current prototypes only are useful against specific UAVs, the Army Cyber Institute is working on handheld weapons for use against a wide range of UAVs — and possibly other close-by electronic targets.

The 2015 DOD Cyber Strategy is clear about the threat: "During a conflict, the Defense Department assumes that a potential adversary will seek to target U.S. or allied critical infrastructure and military networks to gain a strategic advantage."

In a recent online event hosted by Federal News Radio, Maj. Gen. Paul Nakasone, Commander of CYBERCOM's Cyber National Mission Force, explained the U.S. strategy to counter this growing threat: "We need to better integrate our forces into the planning and execution of operations across the Department of Defense, to build even stronger partnerships across the U.S. government, with allies and industry."

The lack of integration, Rexford maintains, is a key problem to the future of U.S. electronic warfare.

"You have to integrate and we haven't done that. So it's not an inability to create technology, it just goes back to the lack of advocacy, which reduces funding. That dynamic is starting to change because people in Congress are looking at what happened in Ukraine and are asking if we're protected against what the Russians did there, especially if they do the same thing in Poland, for example. So the capability exists, not just current but future generations, out to 2025."

A major part of Nakasone's partnership concept is finding ways to combine and adapt rapidly evolving commercial technologies to meet ever-changing and growing military requirements, preferably in ways it would be extremely difficult for potential adversaries to mimic or counter.

The role of unmanned systems

"I see a drive and need to move away from preplanned mission execution and toward smart unmanned platforms that can make decisions on the fly. Whether there would be a human in the loop would depend on the time scale of what needs to be done," the Naval Air Warfare Center's Mensa says. "There are revolutionary folks who say we need to go all autonomous, but the evolutionary camp says we're not ready to relinquish control. I think approaches are on the table."

Machine learning and cognitive artificial intelligence will be keys to the autonomous dream, Mensa says. "The first step is how do we capture what the EW experts do about attacking threats based on the waveform information we are seeing. That's the cognitive approach and machine learning is the enabler. We want to use as much of the electromagnetic spectrum as possible, so there is a hunger to open new areas of spectrum to operate in, to get away from contested environments, but also to provide more ambiguity as to where we're operating."

The only constant in future airborne EW technology is the lack of constant. The market faces rapid advances in commercial technology driven largely by the smartphone market, the continuation of Moore's Law, new materials and power systems, and faster, smaller, more capable processors. These factors are pushing the merging of electronic warfare, spectrum warfare, cyber warfare, and information warfare into becoming a full and central part of future combat.

"I do see the trend of evolving into a centerpiece," Mensa says. "Spectrum domination and the ability to project our will across swaths of spectrum is a means to an end to achieving commander's intent. So the role of EW becomes more and more central. I also see an increased focus on EW to protect and enable our kinetic capabilities — not just launch missiles, but make sure they reach their targets. EW is a key enabler in that fight."

For that enabler to become key, however, also requires major changes in how the U.S. government and the defense industry change how they develop, acquire, deploy, train, and employ future EW, relative to what U.S. adversaries are doing.

Military leaders share a concern that potential U.S. adversaries are able to observe, orient, decide, and act (OODA) more quickly than U.S. forces can. That means retooling to respond to warfighter needs

quickly, "and perhaps turn it around to a speed-to-fleet concept," Mensa says. "It's a challenge because we're used to working programs of record and toward milestones, but to meet the new threats, we need to respond much more quickly."

Worst-case scenarios

Military planners typically assume the worst possible scenarios. "At the Warfare Center, we assume the enemy is 20 feet tall because we have an incomplete knowledge of their capabilities and how integrated their overall warfighting capability may be. So we have to operate under the assumption they are our peers and keep pushing forward to tighten time cycles on new solutions and procedures," Mensa says.

"The assumption — and maybe the reality — is it takes us a lot longer to get a new technology ready for fielding. I'm hopeful we're addressing where it makes sense to be cautious and where it makes sense to rapidly field something. We cannot become too risk-averse. In a constrained fiscal environment, we tend to be so afraid to fail we don't take on challenges that might not work. And we cannot do that."

It is not just a matter of evolving new technologies to address new or more complex threats — something that would be impossible under current fiscal constraints. It also means protecting legacy systems such as Link 16 — a military tactical data exchange network used primarily by the U.S. and NATO aircraft, ships, and ground forces to connect in real time for text messages, images, and digital voice.

"One of the things we're looking at quite a bit is how do we take some of our legacy systems and upgrade them to be more capable," says Niedzwiecki of BAE Systems. "For example, Link 16 is a radio waveform designed and built in the 1970s but still the primary command and control and datalink system and a lot of what we're doing is designed to protect that."

The digital nature of today's military radios could be a key factor in upgrading Link 16 and other military radio networks. "Because our radios today are reprogrammable, we can better protect that investment," Niedzwiecki says. "If you want to design, build, and field an entire new radio system from scratch, that's a multi-billion-dollar effort due to all the interoperability, fielding onto platforms. So upgrading existing systems with better intel is one way to do that affordably."

Niedzwiecki also identifies evolving adaptive threats as one of the most significant challenges facing the U.S. Navy and Air Force, particularly in Eastern Europe and Asia.

Adaptive threats

"The operating environments differ, but what is consistent for any mission is it is all about keeping an expensive platform survivable, maintaining its capabilities, and allowing

Rockwell Collins is working on networked electronic warfare systems to cover warfighters on land, at sea, and in the air.

The Raytheon Miniature Air Launched Decoy Jammer (MALD-J), shown above, is a relatively simple air-launched unmanned aerial vehicle (UAV) designed to jam and spoof enemy radar.

it to operate with freedom of action and maneuver," Niedzwiecki continues. "EW is becoming more and more a common feature on all platforms, not just on dedicated systems."

Electronic warfare also may be an increasingly more important element of improving the survivability of planes, ships, and land vehicles.

"It's all about advancing capability to allow our platforms to operate in more highly contested environments where the spectrum is cluttered with a lot more friendly and enemy signals and being able to sort all that electromagnetic soup out and make sure our systems are able to communicate and sense and combat enemy radar," Niedzwiecki says.

Airborne EW traditionally has been the purview of manned aircraft. As such, plans to place EW capabilities on all future and legacy platforms means manned defense and attack will remain strong. Still, major advances in UAV types and capabilities during 15 years of war in Southwest Asia and plans to increase their presence aboard Navy ships means future adversaries will face thousands of small deep attack and swarming flying EW robots.

In contested environments, "large aircraft become aluminum confetti very quickly, so you have to stand off even though the collection range requirements haven't changed," says Rockwell Collins' Rexford. "The MALD-J, which was my program in the Pentagon, helps disrupt the enemy's integrated defense system and I think you will see more of those in the future. For sense and attack, I think you will see UAVs becoming more and more important."

Also of importance will be new hardware and software architectures for electronic warfare systems of the future. "Moore's Law is allowing for lower cost, more frequency-agile radars, but our processes in the U.S. are still tied to hardware moving to software," Rexford says. "Realistically, the only way to get at the problem of counter-counter is to have a similar technology cycle, integrated machine learning, and the ability to use and apply AI in a cognitive way that lets you detect, analyze and react on the fly."

The U.S. EW capability has suffered from decades of adversaries with little or minimal EW capabilities and incapable of challenging U.S. air superiority. Russia, China, and other potential future adversaries, however, used that time to close the gap and achieve near-peer capability in EW, such as Russia's integration of technologies — something the U.S. still has not accomplished.

Officials say American forces also still lack training in a near-peer EW environment, integrating spectrum maneuver with air and land forces. Which is another argument some put forward to support merging electronic warfare, cyber warfare, and information warfare under the unified rubric of spectrum warfare.

"As technology changes, the dynamic changes in warfare, as does the concept of operations and deployment," Rexford says. "One thing that has to change is the use of spectrum warfare to make it work. In the past, you dropped a bomb, saw a hole, and considered it a success. But in EW, if you deploy a weapon and a signal goes away, you don't know if you destroyed it or the enemy simply shut it down.

"We have to integrate spectrum warfare with maneuver warfare, train that way, update doctrine to capture that construct — all that has to be done to win the spectrum war in the future — and, ultimately, in a near-peer environment, the war itself," Rexford says. "If you don't win the spectrum war, you don't win the war. And that's not a good position to be in."

Cybersecurity and encryption for the masses

Aerospace and defense systems designers investigate fast and affordable ways to safeguard computers and communications from cyber attack by plugging vulnerabilities and layering COTS cybersecurity.

BY **John Keller**

The Data Transport System (DTS1) from Curtiss-Wright is a rugged network attached storage (NAS) file server for use in unmanned aerial vehicles (UAV), unmanned underwater vehicles (UUV), and intelligence surveillance reconnaissance (ISR) aircraft.

No one has to be told these days about the importance of data encryption and cybersecurity. Retail chains have had their computer hacked to compromise customer security. Financial institutions have lost thousands, if not millions, of dollars, and U.S. political parties have suffered e-mail hacks to reveal campaign secrets.

Consensus among experts says the problem will just get worse over time. One of the primary keys to cybersecurity for government and private industry is encryption. The problem, however, is that encryption historically has been expensive to obtain, and time-consuming to certify.

Some of that might be changing, as encryption approaches are emerging that are more affordable than traditional methods, and that can be tied into new systems and upgrades far more quickly than could be done in the past.

One of the more influential aspects of a new generation of timely and affordable encryption is the Common Criteria Recognition Arrangement (CCRA), an international agreement among 26 member countries that makes available different encryption approaches for business, military, and civil uses.

The U.S. arm of the CCRA is the U.S. Department of Defense (DOD) National Information Assurance Partnership at Fort Meade, Md. Other CCRA members include the United Kingdom, France, Germany, India, Japan, Israel, and Canada.

The technical basis of the organization is the Common Criteria for Information Technology Security Evaluation, which typically is known simply as the Common Criteria, or just CC. It offers products that licensed independent laboratories can evaluate for different security applications.

The Common Criteria represents a wide variety of mutually recognized encryption products for secure IT products. More on the Common Criteria and the CCRA is online at https://www.commoncriteriaportal.org/.

What's good enough?

Wide availability of cybersecurity and encryption products begs the question: if these encryption

schemes are so available and well-known, how secure can they really be?

For some applications these encryption products taken individually may be perfectly adequate. For others — especially for military, aerospace, homeland security, and other life- and mission-critical applications — just one might not be enough for reasonable assurance of security against malicious hackers or eavesdroppers.

Until recently the only other viable alternative for reliable and certifiable encryption and cybersecurity was the long-established Type I security available through sources approved by the U.S. National Security Agency (NSA) at Fort Meade, Md.

For a fair number of applications, however, NSA Type I encryption is just too expensive to consider — even such that some systems designers had to go without encryption and hope for the best. Sometimes taking such a risk has met with dire consequences.

One of these involved the so-called RQ-170 Incident in December 2011 when Iranian military forces commandeered a U.S. Lockheed Martin RQ-170 Sentinel stealth unmanned aerial vehicle (UAV) near Kashmar in northeastern Iran. An Iranian cyber warfare group took control of the U.S. UAV, landed it, and took it apart to discover its technical secrets.

From the lack of a reliably secure control data link, the U.S. may have lost technological secrets that would take years to overcome. This pivotal event caused a rethinking of encryption and cybersecurity in the Pentagon, defense industry, and other enclaves where security is essential.

The lessons learned from the RQ-170 Incident have given rise to several new initiatives to safeguard data flowing over networks, as well as data that resides on storage devices in unpowered computer systems.

Protecting UAV data links

On the UAV front, cybersecurity experts at Rockwell Collins in Cedar Rapids, Iowa, are working with specialists at other companies and government agencies to develop software that can repel hackers even over unsecured data links.

One effort, sponsored by the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., is called High- Assurance Cyber Military Systems (HACMS). The Air Vehicle team in the HACMS project involves Rockwell Collins in Cedar Rapids, Iowa, as well as the Boeing Co. Defense & Security Segment in St. Louis; Data61 in Canberra, Australia; Galois Inc. in Arlington, Va.; and University of Minnesota in Minneapolis.

The Rockwell Collins team is developing embedded computing software that can enable a UAV to keep operating safely despite offboard and onboard cyber attacks, Rockwell Collins officials say. The team has demonstrated prototype secure software on quadcopter UAVs, as well as on the Boeing Unmanned Little Bird helicopter, which was able to resist several cyber attacks launched by a team of advanced hackers.

"Our world is becoming more connected every day, and that includes the aviation industry," says Darren Cofer, fellow at Rockwell Collins. "Cybersecurity used to be a concern only for traditional

computing systems and networks. Now anything with embedded software can be vulnerable to cyber attack. As a result, we have to be vigilant about protecting critical systems like avionics."

Coffer explains that hackers have three approaches to attacking embedded computing systems: external interfaces; software bugs; and communications and software interfaces.

First, hackers can exploit weak external interfaces that have weak or no encryption. Second, they can exploit software bugs to create

Warfighters deployed in the field need the ability to safeguard data on the move and at rest from attempts to intercept or tamper with mission-critical information.

vulnerabilities. Third, they can use communications and software component interfaces in a way that software developers never intended.

Researchers involved in the DARPA HACMS program are concentrating on those three vulnerabilities to safeguard systems that are unencrypted from potential cyber attacks.

Layered COTS security

The RQ-170 Incident also has given rise to the NSA's Commercial Solutions for Classified program (CSfC) — a new way of delivering encryption and cybersecurity solutions that capitalize on industry developments.

The idea behind the NSA's CSfC program is to provide encryption and information assurance both quickly and affordably — and provide a viable alternative to expensive NSA Type I encryption for systems that might not be able to afford it or have the time to implement it.

NSA experts founded the CSfC program on the principle that

properly configured, layered solutions can provide adequate protection for classified data in a variety of different applications. This can enable aerospace and defense systems based on commercial off-the-shelf (COTS) hardware and software to communicate securely based on commercial standards in a solution that can be fielded in months, not years, NSA officials say. More on the NSA's CSfC program is online at https://www.nsa.gov/resources/everyone/csfc/.

The core approach of the CSfC program is to layer two or more commercially developed encryption and cybersecurity approaches to provide information security solutions that might not be entirely impregnable, but that are good enough for the applications at hand.

Military communications and computer developers describe the redundant practice of using two or more security approaches as "belt and suspenders," or "using the parking brake after putting the transmission in park."

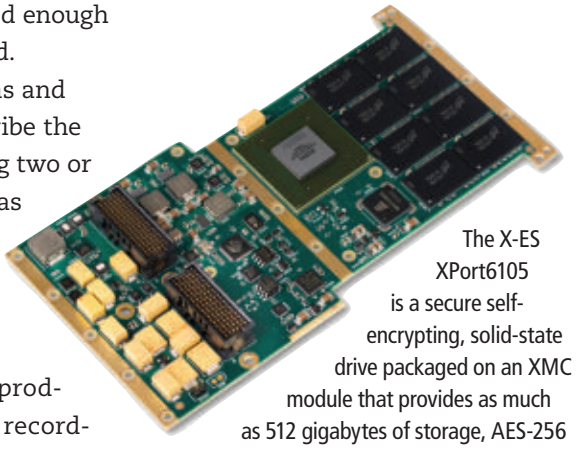
Paul Davis, director of product management for data recording and storage products at the Curtiss-Wright Corp. Defense Solutions segment in Ashburn, Va., describes the CSfC approach as overlaying two pieces of Swiss cheese.

"If you have two pieces of Swiss cheese, there are several holes," he explains. "If you rotate one piece 90 degrees, most of the holes are covered up. Any one piece might not be adequate to protect a system, but if you use two layers and cover most of the holes, it can be good enough for that application."

The CSfC approach couldn't come at a more important time. Not only are experts in the DOD and private business increasingly concerned about cybersecurity and encryption, but the need to safeguard data also is expanding exponentially with an explosion in the use of sensors, digital signal processing, and the so-called Internet of Things (IoT).

"It is definitely gaining more momentum," says David Jedynak, chief technology officer at Curtiss Wright Defense Solutions. "We can start with things on the Common Criteria list, and instead of doing this big Type I thing, we can take this commercial solution with that commercial solution and bring them together."

Where time to market is a big concern, this layered approach can



The X-ES XPort6105 is a secure self-encrypting, solid-state drive packaged on an XMC module that provides as much as 512 gigabytes of storage, AES-256 XTS encryption, and fast clear.

The Harris Corp. RF Communications segment in Rochester, N.Y., designs and manufactures the KGV-72 encryption device, shown above, which provides the ability to process classified messaging traffic.

make the difference between winning and not winning a contract. "The rationale is cost and time," Jedynak says. "A Type I development can be five to six years long, while a CSfC development is two to three years — sometimes only 18 months."

Curtiss-Wright is using CSfC two-layer approach to encryption and cybersecurity with a product to be launched in September called the Data Transport System 1 (DTS1) for protecting stored data at rest at times when computer systems are unpowered. It's part of the company's Trusted COTS (T-COTS) initiative.

"People want to protect data at rest, but are also concerned about having it encrypted and how people can break through that encryption if they have it in their possession. We are working to address and enhance our offerings in both areas," says Steven Edwards, director of secure embedded solutions at Curtiss-Wright. Company officials say they expect NSA certification for the DTS1 by the end of 2017.

Digital defenses

Most encryption approaches to cybersecurity represent efforts to keep potential digital intruders out. These and other conventional approaches are part of a mindset of building walls and guard towers around important data and data pathways.

What happens, then, when the hackers get in? Mark Testoni, president and CEO of SAP National Security Services (SAP NS2), a cybersecurity specialist in Rockville, Md., says security experts are starting to think about how to contain and otherwise deal with hackers after they've broken in, rather than simply preventing them from access to sensitive data.

"On the protection side, historically we have done a really good job of building perimeters around our systems," Testoni says. "We continue to do that, but most recently encryption has taken on a more important role with data on the move and data at rest."

Security experts have to face the fact that few, if any, defenses can be 100-percent effective. "Beyond perimeters, how do we look at our own systems, assuming people are going to get in," Testoni says. "We have to make a mental presumption that they are going to get in, and we have to figure out how to root them out."

Perhaps the primary opportunity today for cybersecurity providers is how to help companies look at their systems and network architectures, and help assimilate data on various activities going on in the network, Testoni says.

One approach to this is bringing in lots of metadata-level information to help establish a baseline for normal activity of the network and the network's users, Testoni says. The downside of this, however, is it requires a tremendous amount of compute power to research these behaviors and detect anomalies.

"We're starting to work on the importance of the digital DVR," Testoni says. "We look at and capture the data inside your system, and when you see deviations it can identify anomalies for further investigation."

Security experts at SAP NS2 are working on what Testoni calls HANA, short for High-Performance Analytic Appliance, that relies on a traditional database architecture. "You have core compute power, data storage, and hundreds of thousands if I/Os going back and forth," he says.

HANA seeks to place all data and computing is one place, not in storage, with petabytes of information available for analysis. "This is a real possible breakthrough," Testoni says.

Another way to deal with digital break-ins involves user behavior analytics (UBA), which looks at individual behavior on the network, based on documented normal behavior, Testoni says. "This isn't THE answer, but it's a piece of the answer," he says.

A third approach is to effect a cultural change that increases the vigilance of computer and network users to potential cyber threats such as those contained in what look like routine e-mails, such as dangerous attachments. Cyber defenses, detecting anomalies, and increasing individual vigilance "is a three-headed approach that will enable us to be successful," Testoni explains.

Lockheed Martin to upgrade TPQ-53 radar microelectronics

Military microelectronics experts at Lockheed Martin are upgrading electronic components in the AN/TPQ-53 fire-control radar to improve the system's abilities to track and locate hostile rocket, artillery, and mortar fires in high-clutter environments. Officials of the U.S. Defense Microelectronics Activity (DMEA) in McClellan Park, Calif., announced their intention to award a $4.1 million contract to Lockheed Martin Mission Systems and Training in Syracuse, N.Y., to make the AN/TPQ-53 upgrades. The Q-53 solid-state phased array radar detects, classifies, tracks, and determines the location of enemy indirect fire weapons like rockets, artillery shells, mortars, and even unmanned aerial vehicles (UAVs) in either 360- or 90-degree modes.

Northrop Grumman continues low-rate production of IED jammers

Electronic warfare (EW) experts at Northrop Grumman are continuing production of common open-architecture RF jammers for infantry, land vehicles, and fixed sites to protect U.S. and allied warfighters from radio-controlled explosives. The U.S. Naval Sea Systems Command in Washington announced a $103.4 million contract modification to

Army seeks to upgrade or replace Patriot missile-defense radar system

BY **John Keller**

PICATINNY ARSENAL, N.J. — U.S. Army missile experts want to upgrade or replace the radar systems on the Patriot air-defense missile system, and they are surveying industry to find companies able to do this.

Officials of the Army Contracting Command at Picatinny Arsenal, N.J., has issued a request for information (W15QKN16X06UY) for the Lower Tier Air and Missile Defense Sensor (LTAMDS) project to consider upgrades or replacements to the Patriot missile radar to improve its effectiveness against emerging threats and reduce maintenance costs.

The Army Raytheon Patriot surface-to-air missile (SAM) uses the Raytheon AN/MPQ-53 phased-array radar for high- to medium-altitude air defense against enemy aircraft and ballistic missiles. Army leaders want to keep Patriot in the field until at least 2040.

Army experts want new or upgraded Patriot radar systems that cost less than $50 million per installation. Solutions must be at least as mature as component and breadboard validation in relevant environments (Technology Readiness Level 5) by late 2017.

The Army Contracting Command is issuing this RFI on behalf of the Army Lower Tier Project Office (LTPO).

From industry, the Army wants descriptions of proposed solutions; expected per-unit costs of radar

The Army wants to upgrade or replace the search and fire-control radar for the Patriot air-defense missile, shown above, which has been fielded more than 20 years.

upgrades or replacements for 80 Patriot radars over 10 years; and expected test schedules. Army experts also are interested in technologies critical to a Patriot radar upgrade or replacement, including high-power amplifiers, low-noise amplifiers, limiters, low-noise oscillators, AC-DC and DC-DC power supplies, antennas, cooling systems, and prototypes.

Companies interested should e-mail unclassified responses to the Army's Gregory Smith at gregory.l.smith247.civ@mail.mil. Send classified responses by post or courier to PEO Missiles and Space, Attn: SFAE-MSL-LTG, Bldg. 5250, Martin Rd., Redstone Arsenal, AL 35898.

MORE INFORMATION IS online at https://www.fbo.gov/otices/35fb9706395f023d73813bc935d83300.

SRCTec to build lightweight counter-mortar radar in $85 million order

BY **John Keller**

ABERDEEN PROVING GROUND, Md. — U.S. Army air-defense experts are asking engineers at SRCTec LLC in Syracuse, N.Y., to build lightweight counter-mortar radar (LCMR) systems to help defend deployed warfighters from rocket, artillery, and mortar (RAM) attacks.

Officials of the Army Contracting Command at Aberdeen Proving Ground, Md., announced a three-year potential $85 million contract modification to SRCTec for LCMR systems, as well as vehicle mounts, spare parts, retrofit kits, and support services.

The LCMR family of counter-fire radars from SRCTec provides 360-degree surveillance and 3D rocket, artillery, and mortar location using a non-rotating, electronically steered antenna.

The SRCTec LCMR family consists of the AN/TPQ-49 and AN/TPQ-50. The TPQ-50 is the official Army program of record, while the TPQ-49 is designed for expeditionary forces, company officials say.

The radar systems detect and track several different rounds fired from separate locations, and send early-warning messages indicating a round is incoming. The radar also pinpoints the location of the incoming round's launcher for counter-fire from friendly artillery, mortars, or aircraft. Both systems are designed to cover 360 degrees over a nearly 200-square-mile area. The systems can be adapted to cover narrower sectors at longer ranges, if necessary.

The LCMR AN/TPQ-50 system detects incoming RAM from low-quadrant elevations, and provides a more accurate point of origin calculation from greater distances than its predecessors. The radar can be transported and operated on a vehicle such as a HMMWV, or rapidly emplaced in rugged terrain by installing it on a tripod. The LCMR AN/TPQ-49 radar can be assembled or disassembled by two soldiers in 20 minutes. It mounts on a tripod using lightweight antenna hardware. The relatively small system consumes low prime power, making it suitable for low-profile operation.

The U.S. Army is asking engineers at SRCTec to build lightweight counter-mortar radar (LCMR) systems to defend deployed warfighters from rocket, artillery, and mortar (RAM) attacks.

SRCTec originally won a potential $281.8 million contract in July 2013 to manufacture LCMR systems. On the contract modification, SRCTec will do the work at locations determined with each order and should be finished by July 2019.

FOR MORE INFORMATION visit SRCTec online at www.srcinc.com, or the Army Contracting Command-Aberdeen at http://acc.army.mil/contractingcenters/acc-apg.

Northrop Grumman Mission Systems in San Diego for low-rate initial production of the Joint Counter Radio-Controlled Improvised Explosive Device (RCIED) Electronic Warfare, Joint Crew (JCREW) Increment One Build One (I1B1). CREW systems provide combat troops protection against RCIEDs and are designed to provide protection for foot soldiers, vehicles, and permanent structures, Navy officials say. This integrated design makes the most of commonality across all capabilities, reduces life-cycle costs, and provides increased protection against worldwide threats.

General Dynamics to upgrade AN/MLQ-44A SIGINT vetronics systems

Military signals intelligence (SIGINT) experts at General Dynamics are ready to upgrade combat vehicle SIGINT vetronics system to enhance the system's ability to detect, identify, locate, and deter a wide range of signal emissions on the battlefield. Officials of the U.S. Army Contracting Command at Aberdeen Proving Ground, Md., announced plans to award a sole-source contract to General Dynamics Mission Systems in Scottsdale, Ariz., to upgrade 47 fielded AN/MLQ-44A Prophet-Enhanced SIGINT vetronics systems to the latest AN/MLQ-44B configuration. Prophet offers a near-real-time picture of the battlespace through SIGINT sensors and high-performance computing.

BAE Systems to build undersea navigation without GPS for UUVs

BAE Systems engineers are developing an experimental GPS-like undersea navigation system to enable manned submarines and unmanned underwater vehicles (UUVs) to navigate accurately with sonar beacons instead of inertial measurement units (IMUs) or global positioning system (GPS) satellite navigation. Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., have chosen the BAE Systems sensor processing and exploitation group in Merrimack, N.H., for the Positioning System for Deep Ocean Navigation (POSYDON) program. The DARPA POSYDON program aims to develop an undersea navigation system to enhance the U.S. Navy's ability to provide precise positioning throughout the ocean basins while remaining below the ocean's surface, BAE officials say. The value of the contract was not released. POSYDON seeks to develop undersea navigation capability that enables submerged UUVs and submarines to navigate over long periods and long ranges without surfacing for a GPS fix to fine-tune their positioning.

UUV networks needed for covert surveillance of global shipping

BY **John Keller**

WASHINGTON — U.S. intelligence experts are asking industry for ideas on developing networks of unmanned underwater vehicles (UUV) for covert surveillance of international ship traffic in important harbors, waterways, and choke points.

Officials of the U.S. Intelligence Advanced Projects Agency (IARPA) in Washington issued a sources-sought notice (IARPA-BAA-16-09) for the UnderWatch project, which seeks to use UUV networks to monitor ships and maneuver to inspect contacts of interest. IARPA is the research arm of the U.S. Director of National Intelligence.

The project will develop an undersea remote-sensing capability to observe a broad set of vessel types at long range, including container ships, cruise ships, commercial fishing traffic, recreational vessels, go-fast boats, and self-propelled semi-submersibles, IARPA officials say.

The world's oceans carry 90 percent of global trade and key waterways like the Strait of Hormuz and Strait of Malacca carry as much as 35 percent and 25 percent of the world's seaborne oil shipments, respectively, IARPA officials say.

While the sea lanes are a vital economic avenue, they are conduits for international terrorism, drug trafficking, illegal immigration, worldwide trafficking of women and children, illicit transfer of materials for weapons of mass destruction, and arms trafficking.

U.S. intelligence experts want to monitor global surface ship traffic using networks of unmanned underwater vehicles.

The ability to monitor vessel traffic secretly from below the ocean's surface, much the same as orbiting satellites monitor ground and air traffic, could help federal law enforcement detect, pinpoint, and characterize maritime threats before they become disasters. With this sources-sought notice, IARPA officials are trying to obtain information on industry's ability to perform research projects on persistent remote surveillance of the world's ocean traffic. It is not a request for proposals, yet may help IARPA compile a qualified bidders list.

IARPA officials are looking for information on the design of UUVs and UUV autonomy, communications, navigation, sensing, power, propulsion, and sensor payloads; and on UUV or manned submarine sensing for the automated detection of maritime contacts from underwater or above the surface.

Companies interested should e-mail non-classified responses to IARPA at dni-iarpacontracts@iarpa.gov.

MORE INFORMATION IS online at *https://www.fbo.gov/notices/0894ed051e29ac4a920a7312b08d5c16.*

DHS experts want to monitor the health of the agency's dogs working in harsh conditions.

DHS needs rugged dog-wearable electronics to monitor health of trained canines

BY **John Keller**

WASHINGTON — U.S. border-control authorities are trying to equip specially trained dogs with rugged wearable electronics to gather field intelligence and monitor the health of the canines when they work in harsh environments.

Officials of the U.S. Department of Homeland Security (DHS) in Washington have issued a solicitation (HSHQDC-16-R-00093) for the K9 Wearable Technologies project, which seeks to develop dog-wearable, intelligence-gathering sensors and health-monitoring devices.

Border-patrol dogs have become the best tool available to detect and apprehend persons attempting entry to organize, incite, and carry out acts of terrorism, DHS officials say. Dogs also are useful in helping agents to detect and seize illegal drugs and other contraband at border crossings.

With about 1,400 canine teams, the Customs and Border Protection Canine Program is one of the largest and most diverse law enforcement canine programs in the country, officials say.

Wearable health-monitoring sensors would be important because border-patrol dogs must work quickly, under pressure, in varied climates. Wearable technologies to diagnose illness and measure performance have become commonplace for human wearers. Now DHS wants to do the same for dogs.

Developing dog-wearable electronics, however, is easier said than done. Maintaining sufficient skin contact on dogs may be difficult, for example, and wearable devices could be uncomfortable or hinder the animal's performance.

Vest-worn devices, moreover, may overheat dogs, and sometimes the animals may destroy the wearable devices by chewing. Digital data storage also may be necessary for those times when the dog moves out of range of the handler. Battery life, of course, is a big concern.

To overcome these challenges, DHS experts are asking industry for ideas and technologies to help monitor the health and welfare of dogs without degrade the animal's mobility or performance. Specifically, DHS experts are interested in dog-wearable electronics that can record and transmit canine vital signs; retrieve, store, and analyze vital sign data; and maintain and update canine sensor components.

For the program's first phase, DHS officials envision separate contracts worth $50,000 to $200,000 that last for three to six months. Successful prototypes could yield longer contracts worth $200,000 to $800,000 over periods as long as two years. Contracts would involve proofs of concept, working prototypes, and initial production models.

Companies interested should e-mail responses no later next year than 7 June 2017 to DHS-Silicon-Valley@hq.dhs.gov. For questions or concerns, contact the DHS's Aaron Ford by e-mail at Aaron.Ford@hq.dhs.gov, or by phone at Aaron.Ford@hq.dhs.gov.

MORE INFORMATION IS online at *https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-16-R-00093/listing.html*.

Air Force kicks off airborne electro-optical sensor program for surveillance

BY **John Keller**

WRIGHT-PATTERSON AFB, Ohio — U.S. Air Force researchers are kicking off a new effort to advance electro-optical sensor technologies for intelligence, surveillance, reconnaissance (ISR), targeting, and situational awareness for manned and unmanned aircraft.

upcoming broad agency announcement (BAA-AFRL-RQKS-2016-0010) that will be released next September or October.

The objective of this contract is to conduct Research and Development to advance and mature the Air Force Research Laboratory's portfolio of electro-optical sensors and related technology for intelligence, surveillance, and reconnaissance (ISR), targeting, and situational awareness for manned, remotely piloted, and autonomous aircraft.

U.S. Air Force experts are ready to approach industry for electro-optical sensor technologies for intelligence, surveillance, reconnaissance (ISR), targeting, and situational awareness for manned and unmanned aircraft

Officials of the Air Force Research Laboratory's (AFRL's) sensors directorate at Wright-Patterson Air Force Base, Ohio, briefed industry on details of the Electro-Optical Combined Hyperspectral Imaging, Infrared Search and Track, and Long Range Imaging R&D (EO-CHIL) project.

The EO-CHIL project relates to an

FOR QUESTIONS OR concerns, contact the **Air Force's Richard Van Hook** by phone at 937-713-8589, or by e-mail at *afrl.ry.eo-chil@us.af.mil*.

G5IR long-range, electro-optical, target-detection system introduced by Sierra-Olympic

Sierra-Olympic Technologies in Hood River, Ore., is introducing the G5IR 550CZ-18 electro-optical, long-range, target-detection and surveillance system designed for all-weather security applications. The 550CZ-18 is an advanced midwave infrared (MWIR) imaging system featuring long-range target detection with recognition capabilities. The 18X continuous zoom lens provides 18 degrees of horizontal field of view (HFOV) at wide angle and 1-degree horizontal field of view at narrow angle. The thermal camera system can detect human-sized targets at 18 ranges farther than 11 miles in good conditions. The 640-by-512-pixel indium antimonide detector with a 15-micron pitch is optimized to operate in the 3-to-5-micron, medium-wave infrared spectrum, commonly considered the best waveband for imaging in marine and high-humidity environments. Other all-weather applications for the 550CZ-18 camera system include: border protection, vessel traffic monitoring, critical infrastructure protection, and airport perimeter surveillance.

FOR MORE INFORMATION visit **Sierra-Olympic Technologies** online at *www.sierraolympic.com*.

PRODUCT applications

TARGET DESIGNATORS

Navy chooses laser designators from B.E. Meyers for boat crews

U.S. Navy surface warfare specialists needed laser designators with infrared illumination capability to enable Navy Special Operations boat teams to illuminate targets in low-light conditions. They found their solution at B.E. Meyers & Co. Inc. in Redmond, Wash.

Officials of the Naval Surface Warfare Center Crane Division in Crane, Ind., announced their intention to negotiate a sole-source contract with B.E. Meyers for 15 of the company's DIAL-100G aiming laser.

The B.E. Meyers DIAL-100G (AN/PEQ-11A) is a high-power, multifunction aiming laser that combines an infrared pointer and illuminator and visible green laser.

The DIAL-100G (SKU: 432P) was designed for the crew-served weapons of Navy special operations boat teams to provide day and night target marking with infrared laser-in-laser technology, B.E. Meyers officials say.

These devices help Navy Special Operations sailors operate machine guns and other crew-served weapons in darkness and other low-light conditions.

The DIAL-100G provides illumination for infrared night-vision goggles and other infrared sensors, as well as a green laser dot to help aim weapons.

The DIAL-100G laser target designator and infrared illuminator weighs 13.5 ounces, measures 3.75 by 1.2 by 3 inches, and can illuminate targets with its green laser as far away as 1.5 miles. Its infrared illuminator can light-up targets as far away as three miles and provides a 55-degree field of view.

MORE INFORMATION IS online at https://www.fbo.gov/spg/DON/NAVSEA/N00164/N0016416T0126/listing.html. Also contact B.E. Meyers & Co. Inc. online at www.bemeyers.com, or Naval Surface Warfare Center-Crane at www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Crane.

WEAPON SIGHTS

N2 Imaging Systems to build Army's first clip-on thermal weapon sight designed for snipers

U.S. Army night-vision experts are asking electro-optical engineers at N2 Imaging Systems LLC in Irvine, Calif., to build the Army's first clip-on thermal weapon sight specifically developed and fielded for snipers.

Army Contracting Command officials at Aberdeen Proving Ground, Md., awarded an $81.1 million five-year contract to N2 Imaging Systems for the Army Family of Weapons Sights-Sniper.

N2 engineers will develop the new night-vision weapon sight for sniper rifles in three phases. First, N2 engineers will design, build, and test engineering and manufacturing development versions of the sniper night-vision weapon sights.

The second phase will involve delivery orders to design, build, and test low-rate initial production (LRIP) versions of the sights. The last phase will involve delivery orders to provide full-rate production versions of the sniper sights. If Army leaders exercise all options, they would ask N2 Imaging Systems to build as many as 5,375 night-vision sniper weapon sights.

N2 engineers will develop weapon sights for in-line mounting with the sniper's day sight to enhance the shooter's ability to fire accurately at targets in all light levels and limited

visibility scenarios, officials say.

A sniper, what the Army used to call a marksman, operates from hiding alone or with a partner and maintains constant visual contact with the enemy. When he has the opportunity, the sniper shoots important enemy targets and personnel from distances or from cover that the enemy cannot detect.

Snipers typically are trained to hit targets with special large-caliber rifles from long distances. In addition to accurate long-range shooting, military snipers are trained in detection, stalking, estimating range to target, camouflage, field craft, infiltration, special reconnaissance and observation, surveillance, and target acquisition.

In the past, snipers typically have been limited to operating in daylight because accurate long-range sniper weapon sights were not widely available. The Army is looking to N2 Imaging Systems to change all that.

N2 engineers will develop a night-vision sniper's weapon sight to enhance the sniper's ability to engage targets accurately in all light levels and in limited visibility. The company prevailed over two other bidders for this contract.

On this contract N2 will do the work in locations to be determined, and should be finished by June 2021.

FOR MORE INFORMATION visit **N2 Imaging Systems** online at *www.n2imaging.com*.

MOTION CONTROL

Navy chooses 6U VME synchro-resolver from North Atlantic Industries

U.S. Navy military aviation experts needed a 6U VME synchro/resolver-to-digital measurement motherboard to track rotating electronics subsystems. They found their solution from North Atlantic Industries (NAI) in Bohemia, N.Y.

Officials of Naval Air Systems Command at Patuxent River Naval Air Station, Md., announced their intention to award a sole-source contract to NAI for the company's 64SD1 VME-6U synchro/resolver-to-digital measurement motherboard.

Resolvers and synchros are transducers that convert the angular position and velocity of a rotating shaft to an electrical signal. A resolver-to-digital or synchro-to-digital converter converts these signals to a digital output corresponding to the shaft angle and velocity.

The specific application for the NAI 64SD1 was not specified in the Navy announcement. In July 2013, however, Naval Air Systems Command announced their intention to buy the NAI 64SD1 for the AN/UPX-29(V) Interrogator System Mode 5 shipboard identification-friend-or-foe (IFF) system aboard Navy Arleigh Burke-class guided missile destroyers.

The AN/UPX-24(V) interrogator set is manufactured by Northrop Grumman and integrates the NAI 64SD1. The AN/UPX-24(V) is the core identification-friend-or-foe (IFF) processor of the AN/UPX-29(V) shipboard interrogator system. It identifies aircraft and surface vessels equipped with selective identification feature (SIF) modes 1, 2, 3A, and C, and provides secure identification of cooperative mode 4 targets.

The IFF data from one AN/UPX-24(V) can be synchronized with as many as four individual radars, and provides the operator with synthetic IFF symbology for target recognition and tracking. The system is installed in Ticonderoga-class cruisers, Arleigh Burke-class destroyers, Wasp-class amphibious assault ships, San Antonio-class amphibious transport docks, and Nimitz-class aircraft carriers.

Navy officials say they plan to buy the boards from NAI sole-source because the company's 64SD1 is the only part that meets the form, fit, and function requirements and that works with existing software.

The NAI 64SD1 is a VME synchro/resolver measurement board that provides 16 synchro-to-digital converter channels, with accurate velocity outputs, that can be used in single-speed or two-speed modes.

The board provides wrap-around self-test, optional programmable reference supply, and is available for military or commercial applications.

The 64SD1 has 16-bit resolution, with optional 24 bits combined; plus-or-minus 1 arc-minute accuracy; continuous background built-in testing with reference and signal loss detection; self-calibration; 50 Hz to 10 kHz operation; tracking rate to 150 revolutions per second; programmable 2-speed ratios if 2 to 255; power-on self-test; and digital velocity outputs. ←

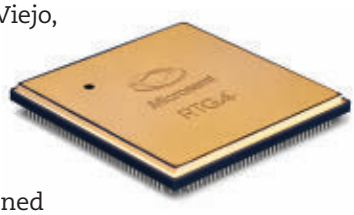
FOR MORE INFORMATION visit **North Atlantic Industries** online at *www.naii.com*.

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

MICROPROCESSORS

FPGA development devices for rad-hard space applications introduced by Microsemi

Microsemi Corp. in Aliso Viejo, Calif., is introducing the RTG4 PROTO field-programmable gate array (FPGA) as a development device for radiation-hardened space applications. The devices are developed to enable prototyping of space systems, and enable low-cost prototyping and design validation for radiation-tolerant, high-speed FPGAs. Microsemi's RTG4 PROTO FPGAs enable hardware timing verification, as well as power evaluation. As the devices use the same reprogrammable flash technology as flight units, they can be reprogrammed several times without being removed from the development board. Catering to the requirements of space system designers who must design for the harsh environment beyond Earth's atmosphere, the RTG4 PROTO FPGAs are electrically tested to ensure performance over full military temperature ranges and are offered in non-hermetic, ceramic packages. In addition to satellite applications, Microsemi's RTG4 FPGAs are for space-launch vehicles, planetary orbiters and landers, and deep-space probes. Target customers include designers, program managers, system architects, and component engineers serving the space market.

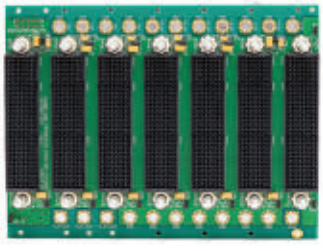


FOR MORE INFORMATION visit **Microsemi** online at *www.microsemi.com*.

BACKPLANES

3U OpenVPX backplanes for mission-critical systems introduced by Dawn VME

Dawn VME Products in Fremont, Calif., is introducing the VPX-598x series Gen3 3U OpenVPX backplanes for mission-critical embedded computing applications. Dawn's Gen3 3U OpenVPX backplanes are designed for signal integrity at speeds to 10.3 gigabaud (per VITA 68 backplane simulation models). Supporting PCI Express Gen 3 and 10-Gigabit Ethernet (XAUI) and advanced Gen3 bandwidth module configurations, Dawn Gen3 backplanes offer several connector choices, including a high-vibration option. Dawn uses VITA 68 S-parameter simulation models of signal paths across the backplane to insure compliance with signal integrity standards. In the simulation models, a signal integrity budget is established for the backplane portion of a system. These models permit simulation of the backplane with available OpenVPX modules and connectors. Using these simulations to guide the backplane designs, Dawn engineers use back drilling to remove stubs and then layout paths to eliminate impedance discontinuities. The goal is to optimize the path between any pair of transmitting and receiving chips in the systems.



FOR MORE INFORMATION visit **Dawn VME** online at *www.dawnvme.com*.

PROCESSOR BOARDS

PCI Express board based on Xilinx UltraScale FPGA introduced by BittWare

BittWare Inc. in Concord, N.H., is introducing the XUSP3R 3/4-length PCI Express board for a wide range of data center and networking applications, including cybersecurity, network processing, compute acceleration, and storage. The commercial off-the-shelf (COTS) board is based on the Xilinx UltraScale VU190 field-programmable gate array (FPGA), and offers as many as four Gen3 x8 PCI Express interfaces, along with four front-panel QSFP28 cages, supporting 16 lanes of 25 gigabits per second or four lanes of 100 gigabits per second — including 100 Gigabit Ethernet. Four DIMM sockets support memory configurations including as much as 256 gigabytes of DDR4 memory across four 72-bit-wide banks; alternatively, designers can populate each of those DIMMs sockets with BittWare's dual-bank QDR DIMMs, each providing 576 megabits of QDR-II+. An optional Hybrid Memory Cube (HMC) module with as much as 4 gigabytes also is

available which can be populated in addition to, and independent of, the DIMMs.

FOR MORE INFORMATION visit **BittWare** online at *www.bittware.com*.

EMBEDDED COMPUTING

Rugged embedded computer for unmanned systems introduced by Curtiss-Wright

The Curtiss-Wright Corp. Defense Solutions Division in Ashburn, Va., is introducing the Parvus DuraCOR 311 small-form-factor rugged commercial off-the-shelf (COTS) embedded computing subsystem for demanding applications like unmanned systems. The Parvus DuraCOR 311 mission computer combines 64-bit quad-core Intel Baytrail Atom modular mission processing capabilities with integrated Intel HD graphics. The mission computer weighs less than 1.5 pounds and is smaller than 40 cubic inches. The mission computer has a robust, flexible, and modular chassis suitable for civil and military unmanned aerial systems (UAS), helicopters, and military ground vehicles. The DuraCOR 311 are pre-validated through environmental, power, and EMI compliance testing per military standards and DO-160. The system is designed to meet MIL-STD-810G, MIL-STD-461F, MIL-STD-1275D, MIL-STD-704F, and RTCA/DO-160G environmental, power, and EMI standards. I/O interfaces include USB, Ethernet, serial, DIO, video, and audio. I/O expansion consists of three Mini-PCI Express expansion slots. The DuraCOR 311 also has mil-spec circular connectors and a dust and waterproof chassis.

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

RUGGED ETHERNET

Ethernet switch for networked embedded computing introduced by Abaco

Abaco Systems in Huntsville, Ala., is introducing a managed Ethernet switch for networked embedded computing applications with a 'power on to fully functional' elapsed time comparable to that of an unmanaged switch. The new Ethernet switch is based on the Abaco GBX411 3U OpenVPX Layer 2/3 rugged Ethernet switch, and is for mission-critical environments that demand superior quality of service, high reliability, and improved uptime through the ability to recover from partial network failure via redundancy and fail-over. Military and aerospace applications with the need to conserve power and minimize heat dissipation in delivering sensor-derived data, such as from IP cameras, cannot tolerate a delay of even a few seconds, Abaco officials say. Abaco engineers adapted the company's GBX411 3U OpenVPX Layer 2/3 rugged Ethernet switch to reduce the device's 'power on to fully functional' time from about 30 seconds to 15 seconds. Abaco's rugged GBX411 supports 24 Gigabit Ethernet and four 10 Gigabit Ethernet ports. The switch is qualified to several military standards.

FOR MORE INFORMATION visit **Abaco Systems** online at *www.abaco.com*.

ADVERTISERS INDEX

Military & Aerospace Electronics

GROUP PUBLISHER Alan Bergstein
603 891-9447 / alanb@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 ART DIRECTOR Cindy Chamberlin

PRODUCTION MANAGER Sheila Ward

SENIOR ILLUSTRATOR Chris Hipp

AUDIENCE DEVELOPMENT MANAGER Stephanie O'Shea
603 891-9119 / stephanieo@pennwell.com

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

MARKETING MANAGER Gillian Hinkle
603 891-9126/ gillianh@pennwell.com

PennWell®
www.pennwell.com

Editorial offices
PennWell Corporation,
Military & Aerospace Electronics
61 Spit Brook Road, Suite 401, Nashua, NH 03060
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 Jessica Stremmel
717 505-9701 x2205 / Jessica.stremmel@theygsgroup.com

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

For assistance with marketing strategy or ad creation, please contact PennWell Marketing Solutions
Paul Andrews, Vice President
240 595-2352 / pandrews@pennwell.com

Corporate Officers
CHAIRMAN Robert F. Biolchini
VICE CHAIRMAN Frank T. Lauinger
PRESIDENT AND CHIEF EXECUTIVE OFFICER Mark C. Wilmoth
EXECUTIVE VICE PRESIDENT, CORPORATE DEVELOPMENT AND STRATEGY Jayne A. Gilsinger
SENIOR VICE PRESIDENT, FINANCE AND CHIEF FINANCIAL OFFICER Brian Conway

Technology Group
SENIOR VICE PRESIDENT/PUBLISHING DIRECTOR Christine Shaw

SUBSCRIPTION INQUIRIES
Phone: 847 559-7330 • Fax: 847 763-9607
E-mail: mae@halldata.com
Web: www.mae-subscribe.com

BPA WORLDWIDE
AMERICAN BUSINESS MEDIA
The Association of Business Media Companies

Hyper-Unity™

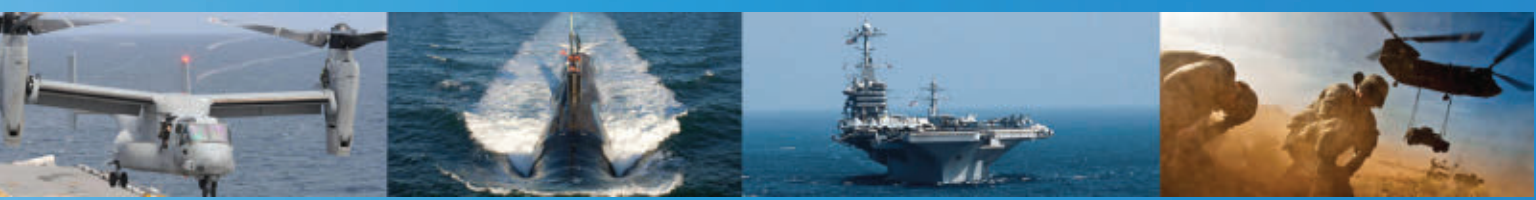
Rugged, Atlantis USX™ Powered, All-Flash Hyper-Converged Infrastructure Platform

Featuring Atlantis USX, Hyper-Unity is the first turn-key, Mil-Spec, SWAP-optimized, hyper-converged infrastructure platform, to deliver all-flash performance for virtualized applications, at less than half the cost of traditional storage or other hyper-converged platforms.

Atlantis USX-Powered All-Flash Performance
Rugged for Demanding Environments
Robust Resource Management
Rapid, Easy Deployment
Modular Scalability

- Superior resilience to shock, vibration, and temperature extremes
- Four-node base solution cluster – for high availability and performance
- Four RES-XR5-1U, eight drive servers with two E5-2600 v3/v4 Series Intel® Xeon® processors, twenty cores per socket, and up to 1 TB DDR4 ECC DIMMs
- Base cluster has 6 TB of SSD raw capacity from 12 to over 30 TB effective storage capacity
- Easy scale-out growth, by adding additional nodes to solution cluster (4-12 nodes)
- Base 1.5TB per node SSD capacity is expandable up to 16 TB per node today
- Integral high-speed, low-latency Mellanox Infiniband data network – 56Gb IB, 56/40GbE
- 1GbE resource management network for node configuration and out-of-band management
- Removable fans
- Single or redundant 36-72 VDC, 18 Amp
- Hot pluggable SSD slots (32 per base cluster)
- Operating temperature range: 0°C to 50°C
- Operating shock: 3 axis, 35g, 25ms
- Operating vibration: 4.76 Grms, 5Hz to 2000H (SSD)
- Operating humidity: 8% to 95% non-condensing
- MIL-STD-810G, MIL-S-901D, MIL-STD-167-1*

www.themis.com/hyper-unity



THEMIS

47200 Bayside Parkway, Fremont CA 94538 | 510-252-0870 | www.themis.com