DECEMBER 2018

Military & Aerospace Electronics

RELEVANT. TRUSTED. ENABLING TECHNOLOGIES.

2018 Innovation Awards

Defense and aerospace electronics companies recognized for technology innovation and achievement. PAGE 6

Secure data storage

Designers and systems integrators struggle with keeping data secure in proliferating networked devices. PAGE 22

militaryaerospace.com

Military organizes for cyber warfare

U.S. warfighters work aggressively to protect military computers and networks. PAGE 16

PennWell

We didn't break the mold.
We shattered it.

RFSoC | Unparalleled Performance | Unbelievably Fast Integration

The combination of Pentek's new Quartz™ architecture, and the processing power packed into the new Zynq® UltraScale+™ RFSoC FPGA, smashes the boundaries of high-performance embedded computing.

Pre-loaded with a host of IP modules, this OpenVPX board is ready for out-of-the-box integration into high-performance systems. Optical streaming interfaces, a unique modular design and the Navigator™ development platform means fast, high-speed deployment.

- **Powerful Zynq Ultrascale+ FPGA** with built-in wideband A/Ds, D/As & ARM processors
- **Dual Optical 100 GigE** interfaces for extreme system connectivity
- **Robust Factory-installed IP** for DRFM,radar range gate engine, waveform and chirp generation, real-time data acquisition and more
- **QuartzXM™ eXpress Module** speeds migration to other form factors
- **Board Resources** include PCIe Gen.3 x8 and 18 GB DDR4 SDRAM
- **Navigator Design Suite** BSP and FPGA design kit for seamless integration with Xilinx Vivado®

All this plus FREE lifetime applications support!

Model 5950
Eight-Channel A/D
& D/A RFSoC in
3U VPX Conduction
Cooled

QUARTZ

NAVIGATOR
Design Suite

Unleash the Power of the RFSoC.
Download the FREE White Paper!
https:/www.pentek.com/go/marfsoc

PENTEK
Setting the Standard for Digital Signal Processing

Pentek, Inc., One Park Way, Upper Saddle River, NJ 07458
Phone: 201-818-5900 • Fax: 201-818-5904 • email: info@pentek.com • www.pentek.com

30 YEARS

DECEMBER 2018
VOL. 29, NO.12

Military & Aerospace Electronics

Military & Aerospace Electronics® (ISSN 1046-9079), Volume 29, No. 12. Military & Aerospace Electronics is published 12 times a year, monthly by PennWell® Corporation, 1421 S. Sheridan, Tulsa, OK 74112. Periodicals postage paid at Tulsa, OK 74112 and at additional mailing offices. SUBSCRIPTION PRICES: USA $185 1yr., $327 2 yr., $466 3 yr.; Canada $280 1 yr., $479 2 yr., $618 3 yr.; International $335 1 yr., $638 2 yr., $834 3 yr. POSTMASTER: Send address corrections to Military & Aerospace Electronics, P.O. Box 47570, Plymouth, MN 55447. Military & Aerospace Electronics is a registered trademark.

BY **JOHN KELLER**, EDITOR IN CHIEF

Western Pacific is becoming a dense concentration of unmanned surveillance assets

It's getting crowded in the Western Pacific.

Military rivalries along China's coast are transforming the region into a rare concentration of military unmanned vehicle technology, as global powers China and the United States, as well as regional powers like Japan and South Korea, step up their long-range surveillance capabilities in the air and at sea.

The South China Sea and East China Sea, north and south of Taiwan, represent serious global military flash points as China expands its military forces into international waters, builds modern aircraft carriers, boosts anti-aircraft and anti-ship defenses, and maintains its potential threats against Taiwan.

As a result, the U.S. is stepping-up its freedom-of-navigation operations at sea and in the air, with frequent military overflights of the region — including flights by strategic bombers like the B-1 and B-52, as well as by strategic reconnaissance planes like the P-8A Poseidon.

U.S. military forces also are keeping a close eye on the region with the Northrop Grumman RQ-4 Global Hawk and MQ-4C Triton long-range unmanned aerial vehicles (UAVs), as well as with manned surveillance aircraft like the Poseidon — a militarized Boeing 737 passenger jet modified for maritime patrol missions.

Although less visible, the U.S. Navy is deploying a variety of unmanned maritime vehicles, including unmanned submarines like the General Dynamics Knifefish, as well as unmanned underwater gliders that can cover vast distances with minimal onboard power.

Two years ago China's navy captured a U.S. unmanned underwater glider in the South China Sea. The UUV, which the Pentagon said was operating lawfully and was clearly marked as U.S. property, was collecting data about the salinity, temperature, and clarity of the water about 50 nautical miles northwest of Subic Bay, Philippines, when it was taken.

It's likely this unmanned underwater craft was gathering more information than just water salinity, temperature, and clarity, although the UUV's precision mission almost certainly is classified. It most likely had to do with helping keep the military balance in the region. China reportedly returned the UUV after examining it.

This is probably not the last incident of its kind, as use of unmanned surveillance equipment only can become more widespread. China, also, reportedly is increasing its military use of unmanned aircraft and submarines to keep tabs on the region.

As time goes on, moreover, it won't be just the U.S. and China operating unmanned reconnaissance assets in the Western Pacific. Japan and South Korea are about to get into the game, too.

In December 2014 the Republic of Korea placed a $657.4 million order with Northrop Grumman through the U.S. Air Force for four RQ-4B Block 30 Global Hawk long-range UAVs. It reportedly was the first sale of the unmanned aircraft to an allied nation in the Asia Pacific region under the Foreign Military Sales process. Deliveries could start as early as this year.

In addition, and just this month, the government of Japan placed a $489.9 million order with Northrop Grumman, also through the Air Force, for three RQ-4 Global Hawk Block 30i long-range surveillance UAVs. Global Hawk deliveries to Japan could start by 2022.

The Global Hawk is a serious UAV. It's big — 47.6 feet long, with a wingspan of 130.9 feet. It can fly as high as 60,000 feet, can carry surveillance sensor payloads as heavy as 3,000 pounds, and can fly for as long as 32 hours on one load of fuel. They also cost upwards of $150 million apiece.

With heavy iron like the Global Hawk deployed by several different nations in the region, the Western Pacific is bound to get more tense, more unstable, and more dangerous. Not to be a pessimist, but this is the kind of environment where things easily and quickly could get out of control. ←

You Engineer the Future.
We'll Supply the Components... Today!

Largest Selection ✓ Same-Day Shipping ✓ Expert Technical Support ✓

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
Pasternack.com

an INFINITE company

PASTERNACK®
THE ENGINEER'S RF SOURCE

Navy asks Lockheed Martin to build additional Trident II D5 submarine-launched nuclear missiles

Strategic weapons experts at Lockheed Martin Corp. will build additional UGM-133A Trident II D5 submarine-launched ballistic nuclear missiles and support deployed D5 atomic weapons under terms of two orders announced Friday collectively worth $90.4 million. Officials of the U.S. Navy Strategic Systems Programs (SSP) office in Washington are asking the Lockheed Martin Space Systems segment in Sunnyvale, Calif., to provide new procurement of Trident II (D5) missile production and D5 deployed systems support. One order is worth $41.3 million, and the second order is worth $49.1 million. Over the past eight months Lockheed Martin received contracts and orders collectively worth $139.3 million for Trident II D5 missiles and support. Over the same period the Charles Stark Draper Laboratory Inc. in Cambridge, Mass., won a $58.6 million order for Trident D5 MK 6 guidance system production.

Here's what you need to know about America's new defense Titan

Harris Corp. and L-3 Technologies are planning to come together in hopes of better competing against the much larger primes. Two years ago Harris completed its acquisition of Exelis Inc. On Oct. 14 Harris and L-3 said they would combine in an all-stock deal that would create a $33.5 billion defense electronics company. L-3 Technologies CEO Chris Kubasik said the deal would move the two companies closer to becoming an "innovative non-traditional 6th Prime," though the company would still fall well short of industry leaders Lockheed Martin, General Dynamics, Northrop Grumman, Raytheon,

Military researchers seek to counter threats from enemy hypersonic missiles and aircraft

BY **John Keller**

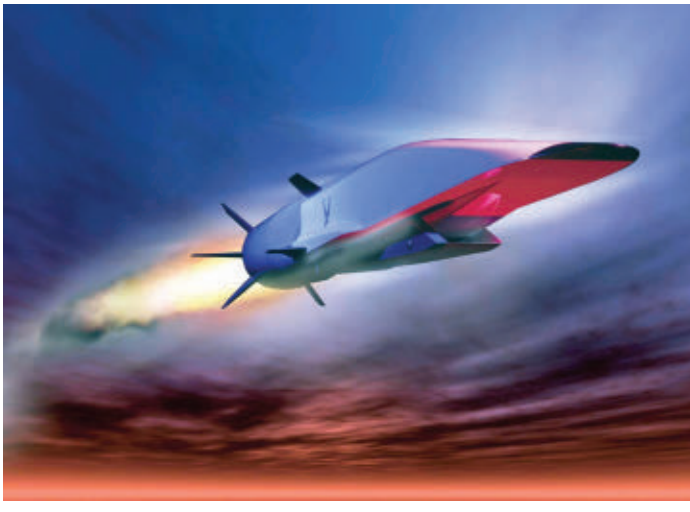
ARLINGTON, Va. — U.S. military researchers are kicking off a project to develop enabling technologies to counter the growing threat of enemy hypersonic missiles and aircraft.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., issued a broad agency announcement in November for the Glide Breaker program to counter enemy hypersonic vehicles — or those that can fly faster than five times the speed of sound.

Top U.S. military leaders over the past year have voiced their alarm about Chinese and Russian projects to develop hypersonic missiles and aircraft. Hypersonic missiles particularly would be useful to attack large U.S. surface warships like aircraft carriers.

The DARPA Glide Breaker project will develop an enabling technology critical for an advanced interceptor capable of defeating hypersonic vehicles, DARPA officials say. Key aspects of the project are classified, and only proposals addressing the classified aspects of Glide Breaker will be eligible for funding.

This effort asks the U.S. defense industry for innovative proposals in counter-hypersonics to advance U.S. means to counter hypersonic vehicles. It will develop and demonstrate an advanced interceptor able to engage enemy maneuvering hypersonic threats in the upper atmosphere.



Military researchers have turned their attention to defending against enemy hypersonic missiles and aircraft, which can travel as fast as five times the speed of sound.

DARPA officials will choose one contractor for Glide Breaker, which will carry out a system requirements review, preliminary design review, critical design review, and test readiness review to counter enemy hypersonics.

The winning contractor will develop requirements, define a design, manage risk, mature enabling technologies, develop requirements, develop a conceptual design, develop software, conduct trade studies, and analyze costs.

If the Glide Breaker program makes sufficient progress to warrant prototyping and other advanced development, DARPA may release additional solicitations next year. Companies interested should submit proposals no later than 21 Dec. 2018 to the DARPA BAA Website at https://baa.darpa.mil. Email questions or concerns to DARPA at HR001119S0008@darpa.mil. ←

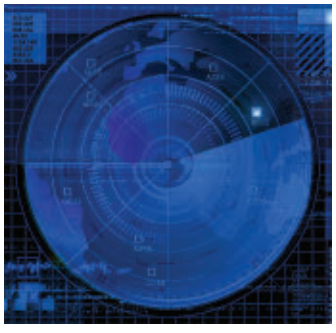
More information is online at https://www.fbo.gov/spg/ODA/DARPA/CMO/HR001119S0008/listing.html.

Northrop Grumman to blend radar and electro-optical sensors

BY **John Keller**

WRIGHT-PATTERSON AFB, Ohio — Military sensors experts at the Northrop Grumman Corp. Mission Systems segment in Linthicum, Md., will help U.S. Air Force researchers enhance the effectiveness of long-range surveillance radar by blending-in electro-optical technologies like visible-light, infrared, multispectral, and hyperspectral sensors.

Officials of the Air Force Research Laboratory at Wright-Patterson Air Force Base, Ohio, have announced a $16.5 million contract to Northrop Grumman for the Precision Real Time Engagement Combat Identification Sensor Exploitation (PRECISE) project.



Northrop Grumman is helping the U.S. Air Force enhance long-range surveillance radar by blending-in electro-optical sensor technologies.

PRECISE seeks not only to fuse several different RF and electro-optical sensors, but also to enhance current radar technologies through signal processing, alternative bandwidths, and similar approaches.

Radar has been used for decades, yet potential U.S. adversaries are looking for ways to reduce radar's effectiveness — especially at long ranges, Air Force researchers explain. PRECISE seeks to improve radar signal processing and fuse other sensors with radar to break ambiguities and improve confidence in declaring targets at long ranges.

The project primarily will develop enabling technologies that advance combat identification for warfighters, and will focus on radar-based identification of air and ground targets for reconnaissance and surveillance aircraft.

Promising enabling technologies developed in the PRECISE program may be integrated onto a surveillance aircraft for flight demonstration. ←

For more information contact ***Northrop Grumman Mission Systems*** *online at www.northropgrumman.com, or the* ***Air Force Research Laboratory*** *at www.wpafb.af.mil/afrl.*

and Boeing in annual sales. Each company focused on military electronics and communications. Both have been pushing to increase the amount of business they do directly with the Pentagon instead of subcontracting, with Harris focused on battlefield management, aircraft communications, and increasing its classified space work and L-3 making a range of sensors and night-vision equipment and developing unmanned vessels.

Army set sights on sophisticated vetronics and technology for future main battle tanks

Could there be a lightweight armored combat vehicle able to speed across bridges, deploy quickly from the air, detect enemies at very long ranges, control nearby robots and fire the most advanced weapons in the world–all while maintaining the unprecedented protection and survivability of an Abrams tank? Just what, exactly, should future light main battle tanks look like? "I believe that a complete replacement of the Abrams would not make sense, unless we had a breakthrough ... with much lighter armor which allows us to re-architect the vehicle," Col. Jim Schirmer, program manager for the Next Generation Combat Vehicle, said last month at the Association of the United States Army Annual Symposium in Washington. Newer lightweight armor composites, active protection systems, and next-generation vetronics may not evolve fast enough to address the most advanced emerging threats. The Next Generation Combat Vehicle (NGCV) program, which has been moved forward by nearly a decade, could likely evolve into a family of vehicles and will have unmanned technology. Any new tank will be engineered with additional space for automotive systems, people and ammunition. ←

2018 Military & Aerospace Electronics Innovators Awards

2018 Military & Aerospace Technology Innovation Awards announced for aerospace and defense achievement

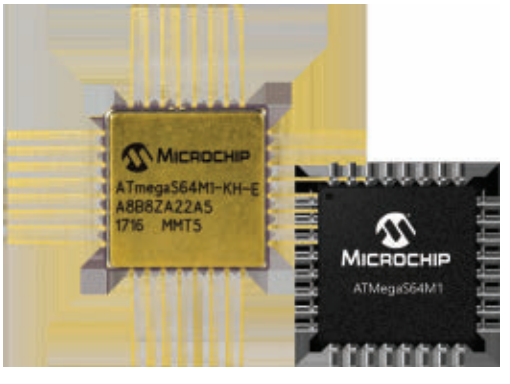
BY **Mil & Aero staff**

NASHUA, N.H. — *Military & Aerospace Electronics and Intelligent Aerospace today announced their 2018 Technology Innovation Awards to recognize companies offering substantial military, aerospace, and avionics design solutions.*

Awards are in three tiers — ranging from platinum, the highest, to the gold awards, and finally to the silver awards — and are based on the recommendations of an independent panel of industry judges.

PLATINUM

The **ATmegaS64M1 AVR microcontroller** (MCU) from **Microchip Technology Inc.** in Chandler, Ariz., brings the AVR core with CAN databus capabilities to the aerospace industry. It is designed for enhanced radiation, extended temperatures, and increased reliability in critical aerospace applications, and comes with CAN controller, power stage controller, A/D and D/A controller, and analog comparators.



The ATmegaS64M1 AVR microcontroller (MCU) from Microchip Technology Inc.

The **ADRV9008/9** from **Analog Devices** in Norwood, Mass., is an integrated, radio frequency (RF) agile transceiver offering dual transmitters and receivers, integrated synthesizers, and digital signal processing. With a turning range from 75 MHz to 6 GHz, it offers wide bandwidth and high performance in single-chip TDD solution for communications, aerospace and defense, and electronic test & measurement applications.

The **HSR40 high-speed network-attached storage** (NAS) data recorder from the **Curtiss-Wright Corp. Defense Solutions Division** in Ashburn, Va., offers 40 Gigabit Ethernet handling the incoming data, with dual Xeon D processors and two built-in 40 Gigabit Ethernet interfaces. The processors can absorb the incoming data and redirect it to the persistent storage media, using third-generation PCI Express. Data pipelines over the backplane to the PCI Express-based non-volatile memory express (NVMe) solid-sate drives. Drives are installed onto removable memory blades, each with a maximum capacity of 32 terabytes, allowing for quick offloading of data for post mission analysis.

The HSR40 high-speed network-attached storage (NAS) data recorder from the Curtiss-Wright Corp. Defense Solutions Division in Ashburn, Va.

The **LP360 rugged connector** from **Fischer Connectors** in St-Prex, Switzerland, is for dismounted soldier systems, to enable foot soldiers to share information in real time. It connects and powers electronic devices body-worn by soldiers, and is an integral part of the Fischer intelligent vest, based on a

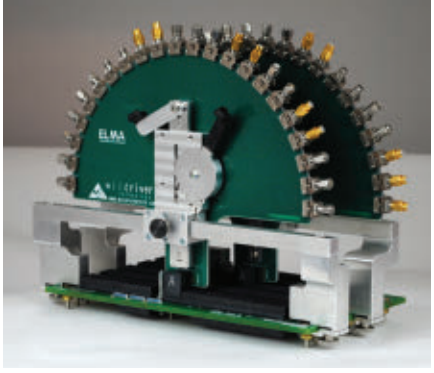
The LP360 rugged connector from Fischer Connectors in St-Prex, Switzerland.

shared data and power bus with wiring on the inside, one central battery for all, and connectors that work as a hub interface at strategically chosen locations.

The **ATS-6100 WFT wire fault test and measurement system** from **Astronics Test Systems Inc.** in East Aurora, N.Y., is designed to detect existing and potential wire faults and help extend the life of aging military or civil aircraft, ships, ground vehicles, and other high-vibration equipment where operational failure would be catastrophic. It detects hard and soft faults in a handheld, self-contained tablet, and eliminates the need to terminate the opposite end of the cable for testing, limiting human interaction and leaving cables undisturbed in the system.

The **S402-SW Tiger** from **General Micro Systems** in Rancho Cucamonga, Calif., is a mobile battlefield data center that provides server-class performance in a ruggedized, conduction-cooled system. Developed for the U.S. Army's Product Manager Mine Resistant Ambush Protected Vehicle Systems (PdM MRAP VS) the S402-LC/SW is sealed and operates in temperatures from -40 to 85 degrees Celsius with no fans required.

The **VPX Backplane Probe Card Test Fixture** from **Elma Electronic** in Fremont, Calif., enables characterization of differential VPX backplane channels between any two points on any 3U or 6U VPX backplane. It was designed for use on backplanes intended to support high speed signaling protocols such as PCI Express 2.1, InfiniBand DDR, Serial Rapid IO 2.2, PCI Express 3.0, Ethernet 10GBASE-KR, InfiniBand QDR, or InfiniBand FDR. The platform comprises three elements: a set of probe cards, a mechanical test fixture and a calibration card.



The VPX Backplane Probe Card Test Fixture from Elma Electronic in Fremont, Calif.

Simics from **Wind River Systems** in Alameda, Calif., is simulation software that provides the access, automation, and collaboration to enable agile and continuous development practices. By using virtual platforms and simulation, aerospace and defense software developers can decouple their work from physical hardware and its limitations during development. Software developers use Simics to simulate nearly anything from a single chip to complete systems and networks. Simics can run unmodified target software.

The TRRUST-Stor VPX Radiation-Tolerant Solid-State Drive from Mercury Systems in Andover, Mass.

The **TRRUST-Stor VPX Radiation-Tolerant Solid-State Drive** from **Mercury Systems** in Andover, Mass., is a commercial solid-state drive (SSD) engineered for harsh operating environments using SpaceVPX standards. Although designed for commercial satellite applications, the device also can adapt to other applications where radiation exposure may occur, including high-altitude aircraft, airborne weapons, and mission-critical ground computing systems. TRRUST-Stor VPX RT SSD includes advanced BuiltSECURE error-correction algorithms paired with large geometry industrial-grade single-level cell (SLC) NAND flash memory.

The **S1U-MD Cyclone 1U rack-mount multi-domain rugged computer system** from **General Micro Systems** (GMS) in Rancho Cucamonga, Calif., is two complete Intel Xeon-based rugged computer server subsystems, each with as many as 18 cores. The server subsystems are packaged together, but electrically isolated, including their separate power supplies and APUs. Cyclone is intended for military and aerospace Red/Black networks that also require storage-such as found on platforms with SIPR/NIPR networks.

The **Axon Miniature Data Acquisition Unit** from the **Curtiss-Wright Corp. Defense Solutions Division** in Ashburn, Va., is an ultra-compact and lightweight data acquisition system that works as a remote node or as a stand-alone chassis. Axon uses a 1-gigabit-per-second serial backplane to support high data rates. This design also enables designers to place off-the-shelf data acquisition modules in ultra-miniature "Axonite" housings and locate them remotely. It helps decrease the installation time and cost of the instrumentation while simultaneously reducing wiring weight.

GOLD

SystemLink from **National Instruments Corp.** in Austin, Texas, is software that enables engineering teams to connect, manage, and optimize automated test and measurement systems. SystemLink improves operational efficiency and system uptime by providing a centralized web application for automating

tasks such as systems deployment and management, test monitoring, and data analysis and reporting. SystemLink improves configuration compliance by discovering system settings and parameters and enabling remote configuration and diagnostics functions.

The **Gallium Nitride (GaN) field effect transistor** (FET) power supply solution from **Renesas Electronics Corp.** in Tokyo comprises the Intersil ISL70040SEH GaN FET driver and ISL70023SEH and ISL70024SEH GaN FETs to provide power to ferrite switch drivers, motor control driver circuits, heater control modules, embedded command modules, 100- and 28-volt power conditioning, and redundancy switching systems in satellites and launch vehicles.

The **CTA803 AC-DC power supply** from **Aegis Power Systems Inc.** in Murphy, N.C., is for low size, weight, and power (SWaP) applications for advanced military armored vehicles. It is housed in a water-tight enclosure and designed to meet MIL-STD-810F environmental standards, EMI requirements of MIL-STD-461F, and the 28-volt vehicle requirements of MIL-STD-1275E. It weighs 115 pounds and can accommodate U.S. Army counter-UAS technology needs.

The Gallium Nitride (GaN) field effect transistor (FET) power supply solution from Renesas Electronics Corp. in Tokyo.

The **SR429/4D NEXSYS ARINC 429 Multi-bit Decoder** from **Applied Avionics Inc.** in Fort Worth, Texas, can provide a binary decode of several data bits from one ARINC 429 data label. The SR429/4D is configurable with either 2x4 or 3x8 decode capabilities in less than 1 cubic inch of space. It offers configuration options for ARINC transmission speed, discrete output type, handling of SDI bits, and parity checking. Optionally, the SR429/4D can be configured with fail-sense circuitry that can simultaneously monitor the operation of the signal converter.

The **RACE0161 AV/Unmanned Driving Solution** from **Crystal Group Inc.** in Hiawatha, Iowa, is a high-performance, rugged embedded autonomous vehicle computer that harnesses modern commercial off-the-shelf (COTS) components stabilized in a rugged, compact enclosure constructed of aircraft-grade aluminum to streamline and speed the development and deployment of safe, robust, and reliable autonomous and unmanned vehicles and systems. A turnkey system, it helps overcome common challenges related to power and thermal management, size and weight, reliability, harsh elements and extreme environments, and an upgrade path to accommodate future needs and technologies.

The **D2D-34S ATR chassis** from **Atrenne Computing Solutions** in Brockton, Mass., supports the development-to-deployment program (D2D) life cycle, maximizing use of COTS components for development and demonstration with upgradeability for deployment, for reduced risk, reduced schedule, and reduced costs. This approach allows the product to use the same platform to support customers through their program life cycle.

The **QPD1025L 1800-Watt (P3dB) discrete gallium nitride on silicon carbide high electron mobility transistor power IC** from **Qorvo** in Greensboro, N.C., is for identification friend-or-foe (IFF) systems, avionics, and test instrumentation. It operates from 1.0 to 1.1 GHz., and input prematch within the package results in ease of external board match and saves board space. The device is in an industry standard air cavity package, and can support CW and pulsed operations.

The **ZM3 enterprise-class small-form-factor mission computer** from **Zmicro Inc.** in San Diego is for space-constrained applications such as manned and unmanned airborne intelligence, surveillance, and reconnaissance. It is equipped with an NVIDIA Quadro P6000 graphics processing unit (GPU) accelerator, and comes in a rugged design that's about the size of a shoebox and weighs nine pounds. This lightweight computer packs in a 16-Core Intel Xeon D processor, three PCI Express expansion slots, as many as two removable storage drives and double-wide COTS high-end graphics cards. It provides the capabilities of a rackmount server in a fraction of the size and weight.

The **OpenVPX CMOSS Convergence Development Platform** from **Elma Electronic Inc.** in Fremont, Calif., is a complete test environment that supports OpenVPX embedded computing application development where compliance with the hardware convergence requirements of the military CMOSS (C4ISR/EW Modular Open Suite of Standards) initiative is the goal. At the heart of the system is Elma's 12-slot CMOSS backplane, with 12 payloads and two power supply slots. The backplane features high-speed RF and optical I/O connectivity. The platform includes OpenVPX computer and networking modules, support for IEEE1588 precision timing, dual high-wattage pluggable VITA 62 compliant power supplies, and support for air- and conduction-cooled modules.

The **BuiltSAFE GS Software Multi-Core Graphics Renderer** from **Mercury Systems** in Andover, Mass., is for safety-critical applications, and enables advanced graphics on devices without a graphics processing unit (GPU), rendering purely in software, to eliminate the need for a GPU. This results in less hardware, less complexity, and lower certification costs for many applications. The high-performance safety-certifiable rendering engine is for applications ranging from avionics, to automotive

displays. Data items required to achieve the highest levels of safety certification are available.

The **VPX3-1260 3U VPX 8th Gen Intel Xeon E-2176M single-board computer** from **Curtiss-Wright Defense Solutions**, offers a leap in performance over previous generations of Core i7 and Xeon processors in the smallest 3U form factor. Leveraging Intel's first-ever six-core processor, the VPX3-1260 is designed to deliver more than 50 percent more processing power than previous for-core designs. The VPX3-1260 offers 10-Gigabit and 40-Gigabit Ethernet connectivity for fast data transfer and high network productivity. It has a local NVMe local solid-state drive, and is built to VITA 47 standards. It provides high non-throttling performance, and offers Intel's latest Trusted Computing features, such as Intel Boot Guard and UEFI Secure Boot, and offers Intel Software Guard Extensions (SGX) for secured run-time software enclaves.

The **Rugged Video Gateway Range product family** from **Curtiss-Wright Defense Solutions** provides a flexible building block for complex video management and integration. It's interoperable with the Curtiss-Wright RVG range enabling complex, scalable, solutions. For example, the format converter can combine in a video management system with the RVG-SD1 digital video switch and/or the RVG-SA1 analog video switch. Other elements are available for configuring a complete VMS — include rugged LCD touchscreen mission displays, and digital HD video recorders.

The **BuiltSECURE System-in-Package (SiP) Secure Processor** from **Mercury Systems** incorporates several types of devices — typically memory and a processor — in one package. Mercury's BuiltSECURE SiP technology incorporates several discrete components, such as FPGA, processor, passive devices, volatile memory, and nonvolatile memory, in addition to more specialized components. It can replicate the capabilities of a custom ASIC for embedded security, and supports analog-to-digital converters and digital-to-analog converters for applications where RF inputs must be digitized and processed. It can be deployed for ground platforms, aircraft, unmanned vehicles, naval vessels, and weapons that may inadvertently fall into the hands of an enemy who desires to reverse engineer the architecture to exploit this technology against our military forces.

The **EnsembleSeries LDS3517 3U AI OpenVPX blade with BuiltSECURE technology** from **Mercury Systems** is a 3U OpenVPX single-board computer powered by an eight-core Intel Xeon D processor with FPGA co-processing, Ethernet fabrics, and mezzanine site. It offers a PCI Express data and expansion plane for high speed I/O or module interconnect, dual 10 Gigabit Ethernet control plane interfaces, support for Linux and VxWorks operating systems, and a BuiltSECURE foundation for system security engineering support.

The **Apex rugged server** from **General Micro Systems** is for today's energy-conscious data center, where efficient server design pays big total cost of ownership dividends by balancing power consumption, performance, and shelf/floor space. Apex combines military reliability, security, and SWaP into a rackmount server. A 22-inch 2U short rack modular blade server system is designed for subsystem modularity, maximum performance at 8-gigabit-per-second speeds, flexible add-in, and add-on options — all based upon VPX interconnects. Apex can replace as much as 17U of equipment in a 2U height. Add-in I/O is available ranging from M.2 and XMC, to U.2 and PCI Express. An internal four-slot and external two-slot x16 PCI Express chassis support GPGPU deep learning and supercomputing modules from AMD and Nvidia, or FPGA and ASIC coprocessors.

SILVER

The Modest3D software suite from Modest Tree in Halifax, Nova Scotia, is designed for the rapid creation of 3D and virtual reality training solutions. It includes the Modest3D Editor and Modest3D Xplorer content development tools. Modest3D Editor helps create advanced 3D applications for task training. Modest3D Xplorer helps create immersive product presentations rapidly, as well as realistic virtual reality training without coding.

The RESmini XR6 rugged enterprise-class server from Mercury Systems is a tactical cloud that can host sensitive missions in theater and operate on almost any power source. It packages one Intel Xeon scalable processor socket with as many as 28 cores in a 15-pound subrack. An optional FAA-compliant UPS power case provides more than 100 minutes of autonomous operation. The SWaP-optimized RESmini meets military specifications and brings next-generation integrated enterprise-class server technology to mission-critical military, industrial, and commercial applications.

The **OpenVPX System Manager** from **Elma Electronic** monitors the health of an OpenVPX chassis and its boards, reports anomalies, and takes any necessary corrective action. It maintains an inventory of the components and sensors in the

chassis and receives event reports and failure notices from boards as well as any intelligent field replaceable units in the chassis. It negotiates power needs before powering up, and uses E-Keying to instruct the boards only to enable compatible links, reducing improper board insertions. Monitoring features include power management, cooling control, event sensor logging, electronic keying, and card hot-swap monitoring. A Web server interface provides a graphical representation of the chassis. Complete sensor information can be obtained with a mouse click on the image of the FRU to query.

The **Themis HDversa Computing Platform** from **Mercury Systems** has 12 module bays that accommodate seven to 12 single- and double-slot modules, which function in a plug-and-play fashion and can be mixed and matched according to application needs. It is designed for applications that require minimum size, weight, and power (SWaP) for standardized compute, storage, PCI Express expansion, networking, and management modules. Users can mix more than five module types, each sharing common attributes to enable users to plug and pull modules according to specific system needs.

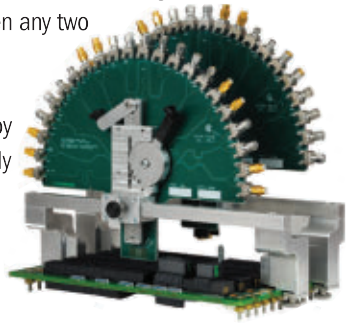
The **Qorvo QPM1002** from **Qorvo** in Greensboro, N.C., is a gallium nitride MMIC front-end module designed for X-Band radar applications within the 8.5-to-10.5 GHz range. The MMIC combines a T/R switch, low-noise amplifier, and a power amplifier. The receive path offers 25 dB gain with a low noise figure of 2.2 dB. The transmit path has a small signal gain of 33 dB, delivers 3 Watts of saturated power with a PAE of 32 percent, and has 25 dB of large signal gain. The FEM is robust up to 2 Watts of input power into the ANT port eliminating the need for a limiter. The QPM1002 is fabricated on Qorvo's QGaN25 0.25-micron GaN-on-SiC process. It is packaged in an over-mold encapsulated 5-by-5-millimeter QFN surface-mount package, and performs well in a high temperature environment.

Military & Aerospace Electronics 2018 Innovation Awards

PLATINUM

Precision VPX Backplane Channel Characterization for Optimal System Performance

Elma's VPX Backplane Probe Card Test Fixture enables electrical characterization of differential signal channels across card slots between any two points on 3U or 6U VPX backplanes. It is a development tool used by Elma to provide extremely precise signal measurements, repeatability, mechanical robustness and ease of use during critical VPX channel characterization for systems in high performance ISR applications.



ELMA
Your Solution Partner

www.elma.com

PLATINUM

1U Rugged Rack Mount Server with Two Fully Isolated Domain

The S1U-MD "Cyclone" is a unique ultra-rugged, 1U rack-mount, lightweight multi-domain server system is designed to provide two fully-independent and isolated high-performance Intel® Xeon® E5 v4 servers, 26 Ethernet ports, dual add-in PCIe cards, as well as two sets of four removable SAS/SATA/NVMe drives—all in 1U height.

GMS
COMPUTING ENGINES

www.gms4sbc.com

PLATINUM

Rugged, Fully Sealed, Intel® Xeon® E5 CPU Server with Removable Drive(s) and Switch

The S402-SW "Tiger" is a third-generation, fan-less (conduction-cooled) fully rugged, low cost Intel® Xeon® E5 server. It is designed to provide the highest level of server-class performance possible in a fully ruggedized, conduction-cooled system, operating up to -40° C to +85° C.

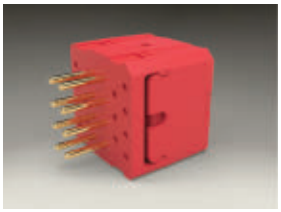
GMS
COMPUTING ENGINES

www.gms4sbc.com

GOLD

ARINC 429 Multi-Bit Binary Decoder, 1 Cubic Inch

The ARINC 429 Multi-Bit Binary Decoder (SR429/4D) can provide a full binary decode for up to three bits from a single ARINC 429 data label, providing a dedicated discrete output for each possible outcome of either a 2x4 or 3x8 truth table. The small form factor of the SR429/4D allows for configuration inside of a VIVISUN® lighted pushbutton switch or NEXSYS® Module. The product is designed, tested and qualified to applicable military standards and meets environmental requirements of DO-160.



Applied Avionics

www.appliedavionics.com/mae

GOLD

Atrenne's D2D-34S ATR Supports Lab Development AND Rugged Deployment

The D2D-34S ATR chassis from Atrenne Computing Solutions in Brockton, Mass. supports the development-to-deployment program (D2D) life cycle, maximizing use of COTS components for development and demonstration with upgradeability for deployment, for reduced risk, reduced schedule, and reduced costs. This approach allows the customer to use the same platform from lab and software development to the release in the final mission application.

Atrenne
A Celestica Company

www.atrenne.com

2018 Military & Aerospace Electronics Innovators Awards
GOLD HONOREE

THE MOST TRUSTED SERVER FOR UAV SYSTEMS.

Accelerate deployment of UAVs with Crystal Group Rugged Autonomous Computer Equipment. Crystal Group systems are compact, with impressive compute power, data-handling capabilities, and storage capacity in a rugged, reliable solution that withstands harsh conditions of land, air and sea that cause traditional systems to fail.

CRYSTAL

SERVERS | DISPLAYS | STORAGE | NETWORKING | EMBEDDED | crystalrugged.com

GOLD

Modular 2U Short Rack, Complete Server/Switch/NAS/ Flex VPX™/GPGPU expansion

The S2U "Apex" is a revolutionary 2U short rack (22-inch) modular blade server system designed for subsystem modularity, maximum performance at Gen 3 speeds (8 Gbps), flexible add-in, and add-on options—all based upon VPX interconnects with military system reliability.

GMS
COMPUTING ENGINES

www.gms4sbc.com

Military organizes for cyber warfare

U.S. warfighters work aggressively to protect computers and networks, just as they would do to protect territory, airspace, sea lanes, and access to space. **By J.R. Wilson**

Cyber warfare specialists serving with the Maryland Air National Guard's 175th Cyberspace Operations Group engage in weekend training at Warfield Air National Guard Base in Middle River, Md.

THE UBIQUITOUS USE of computers has elevated the significance of military signals intelligence (SIGINT), imagery intelligence, geospatial intelligence, measurement and signature intelligence, and technical intelligence to far greater significance than ever before.

That same explosion of technology also leads to the rapid evolution of two new classes of military conflict: electronic warfare (EW) and cyber warfare (CW). It is the Pentagon's responsibility to keep America and her allies at the cutting edge of offensive and defensive EW/CW — and to use all of its ISR capabilities to know and understand what EW/CW abilities that potential adversaries employ.

"One of the biggest challenges we have is just keeping up," admits Giorgio Bertoli, senior engineer at the Intelligence & Information Warfare Directorate (IIWD) within the Army Communications-Electronics Research, Development and Engineering Center (CERDEC) at Aberdeen Proving Ground, Md.

"The Internet is only 30 years old, yet look at how much it has grown in just that time," Bertoli says. "So there's no

The Right RF Parts.
Right Away.

We're RF On Demand, with over one million RF and microwave components in stock and ready to ship. You can count on us to stock the RF parts you need and reliably ship them when you need them. Add Fairview Microwave to your team and consider it done.

Fairviewmicrowave.com
1.800.715.4396

an INFINITE company

Fairview Microwave
RF COMPONENTS ON DEMAND. Done!

reason to believe the next 20 or 30 years will not be just as changeable — from the Internet of Things, to autonomous vehicles, and to wearable computing.

"Trying to keep up with those is a major challenge," Bertoli continues. "The Army is embracing this change and trying many ways to change their processes to improve their speed of capability enhancement, and their speed of acquisition. There is still a lot of work to be done, but we are aware of pending challenges and gearing-up to support those."

Personnel of the 780th Military Intelligence Brigade set up deployable cyber tools overlooking the mock city of Razish at the National Training Center at Fort Irwin, Calif.

SIGINT was born in January 1904, during the Russo-Japanese War, when a British cruiser intercepted a wireless transmission to mobilize the Russian fleet and passed it on to Japan, then a British ally. It was the first act of electronic warfare, defined by the military as any action involving the use of the electromagnetic (EM) spectrum or directed energy to control the spectrum, attack an enemy or impede enemy assaults by denying an opponent the advantage of, and ensure friendly unimpeded access to, the EM spectrum. EW can be applied from air, sea, land and space, and can target humans, communications, radar or other military and civilian assets.

Targeting computers

Cyber warfare represents the use or targeting of computers, online control systems, and networks through offensive and defensive acts of electronic espionage and sabotage. While it often is equated with EW, which is the subject of several programs and studies throughout U.S. Department of Defense (DOD), cyber warfare has been declared a domain of war with the 2010 creation of the joint U.S. Cyber Command, which brought together the individual cyber capabilities of the Army, Navy, Air Force and Marines.

China, which has touted its intention to become the world's dominant cyber warfare superpower, also has unified its cyber capabilities. Russia has employed cyber warfare at least twice in the past decade — in its 2008 military incursion into Georgia and in a 2014 cyber attack on Ukraine.

Israel also is considered one of the world's new breed of cyber super powers, based in part on its estimated 10 percent share of global computer and network security technology sales.

While not as active or public as the others, the United Kingdom in recent years has invested heavily in expanding its cyber capabilities to become the European center of cyber warfare technology.

Although less is known about the cyber warfare developments of Iran and North Korea, of those tightly closed societies are suspected in several cyber attacks — North Korea against U.S. corporations like Sony, and Iran in a host of attacks across Southwest Asia — especially against Saudi Arabia.

Some pundits have declared the world has entered into a new, multi-polar Cold War, with its own cyber warfare equivalent of the original Cold War's doctrine of Mutual Assured Destruction (MAD), in which the U.S. and Soviet Union refrained from the use of nuclear weapons because the other side would respond in kind. While this new, unofficial "digital equilibrium" has been followed by the five cyber warfare superpowers, Iran and North Korea have launched serious attacks, with Iran, in particular, seeking to cause real damage.

In the event of a direct conflict between any of the Five, however, each

nation's full cyber warfare capabilities likely will be employed, possibly as a first strike. That still may be avoided, especially as artificial intelligence (AI) comes into play, making cyber warfare far more precise and effective, says Richard Wittstruck, associate director, field-based experimentation and integration at CERDEC's Space and Terrestrial Communications Directorate (STCD).

Parallel attacks

"In field artillery, we can have single shots or volleys," Wittstruck explains. "In cyber, it's very rare to have a single-shot weapon; it's usually multiple parallel attacks in hopes one or more strikes hit the target. Artificial Intelligence (AI) will enable offense to do more of those attacks, but also allow defense to put up more barriers simultaneously. So you really will have machine-to-machine warfare. AI may become the nuclear deterrent element, because you know I can do it, I know you can do it, so we go to the negotiation table — digital MAD. Still, the general public needs a better understanding of cyber warfare.

"We keep speaking in geek-speak within the community, and until we can translate that into terms the average person can understand, it will be hard to help people understand cyber is not something foreign; it's just a new environment we operate in," Wittstruck says. "In some ways, it's a generational thing. Those who grew up in a digital world — born with a computer in the crib — are very comfortable talking about all these terms, but the digital dinosaur is almost still trying to learn how to spell cyber."

This holds true for the military, as well — even though each service has a cyber component in CYBERCOM, and DOD puts increasing levels of people and money into cyber research.

"A lot of the government side is a little helter-skelter on cyber," says Steve Edwards, director of secure embedded solutions at the Curtiss-Wright Corp. Defense Solutions Division in Ashburn, Va. "We don't do back office enterprise systems; we deal with hardware that gets deployed air-land-sea. There are lots of people involved and they're still trying to figure out how to have a cohesive strategy.

Everyone has his own opinion about what's important in cyber warfare, Edwards says. "Even with commands in the same service, you get different perspectives. Within each division, they are working on that. We've taken part in a couple of meetings on the Air Force side and the standardization push they're trying to make across the Air Force, but it's a slow process."

Under today's military structure, the individual service cyber commands focus on the needs of their warfighters. Some of the technologies and materiel are the same, but how they are applied can be different. CYBERCOM functions as an umbrella command, setting national policy and ensuring there is no duplication of effort.

"There also are areas of agreement and exchanges of people in terms of DOD working with other agencies, such as Homeland Security," says Army CERDEC's Wittstruck. "Cyber cuts across several different departments and there are interagency agreements and statutory authorities. Cyber is so prolific, every federal agency has a cyber component, which makes it a lot easier in a digital age to communicate and cooperate across those boundaries."

Problems with cooperation

Such cooperation becomes more problematic when sharing cyber warfare capabilities among allies. "Each country has its own internal effort, but we're still working on treaties and international law to develop a governance on cyberspace," Wittstruck says, adding that military authorities still don't have cyber warfare doctrine, training, leadership development, facilities, and policy completely nailed down.

In a digital world, where most technologies are readily available to anyone, coordinated, constant, and comprehensive countermeasures are mandatory.

"Cyber is the new IED [improvised explosive device], which began in the early '90s in Bosnia with explosives put in a pothole and covered with garbage," says CERDEC's Wittstruck. "It was prolific, effective, and random and anybody could do it who had the knowledge and access to materials. The same is true today with cyber, although they also need to be able to access a network."

Despite this, the military can search cyberspace constantly for abnormalities or alerts that something has changed. "The challenge is things can change very rapidly, so in a matter of milliseconds, you can go from having a good day to having a bad day," Wittstruck says.

"Once something does occur, it doesn't mean that's a combat loss; you just have to manage it, determine the effect on your fighting capability, and have a contingency plan on getting back." This is called a primary alternate contingency emergency (PACE) plan. "This is a combined arms fight," Wittstruck says. "Cyberspace is what some call the fifth domain and we bring many of those combined arms principals to bear on force effectiveness and planning."

Defensive cyber warfare can face a variety of attack types, depending on whether the enemy wants to deny, degrade, or disrupt computers and

networking — or any combination of the three. It also depends on the target — military enterprise, subnet, platform, individual warfighter or unit. Or they may target civilian infrastructure and just turn the lights on and off to tell civilians they are no longer in control and can be attacked at any time," Wittstruck says.

Difficult to trace

Modern military satellite surveillance covers most of the planet, making it virtually impossible to hide an attack by missiles, aircraft, ships or land forces, enabling the target to strike back against the attacker's home base. That is not the case with a cyber attack, however, which is extremely difficult to backtrack. Even if a cyber attacker can be traced, it can be impossible to tell if the attack came was the nation from which the attack was launched, a non-state group, or even individual operating from within that nation.

Sorting out cyber attackers is called cyber forensics, which has had exponential growth in recent years as the cyber threat has become more pronounced. Backtracking requires that the attack is still in progress. Once it ends, different methods must be employed. Still, without that critical link between the attacker and the target, determining the attacker's IP address is almost impossible with current technology.

More frustrating to cyber defenders is how cheaply perpetrators can launch cyber attacks; it doesn't require a lot of money or infrastructure, only the necessary skills and the ability to access the target.

How a cyber attacker gets to the target represents another line of investigation. Does the attacker have someone on the inside helping, or is it a high-level hacker who can penetrate network defenses without a care if the target knows about it or not. If the same person makes multiple attacks, he or she is likely to leave digital fingerprints reflecting the techniques they use, which may help identify and locate the attacker. For now, however, cyber forensics is unlikely to find a "smoking gun".

The effects of a cyber attack can last long after the attacker has disconnected. Shutting down a power grid, for example, could leave thousands, even millions, of people without electricity to heat or cool their homes, pump gas for cars and trucks, light homes and streets (an open invitation to looters, who also would not have to worry about alarms), get fresh water because the pumping stations are down, treat patients in hospitals The only remedy is for the power company to have the necessary remediation, redundancy, and repair capabilities in place; how quickly it performs those functions will make the difference between degradation, disruption and denial.

Even so, not everyone sees cyber as a potential 21st Century Pearl Harbor, as several government officials have warned.

Keeping the lid on

"Granted, there are thousands of attacks every day on various targets, a lot of them using automated systems churning away and looking for weaknesses or openings," says CERDEC's Bertoli. "For the most part, commercial service and security providers have made great strides and most of those activities are blocked at various places within the infrastructure."

For would-be cyber criminals, however, pulling off an attack is easier said than done. "Cyber attacks are not nearly as easy to pull off as you might assume," Bertoli says. "Going after a hard target requires some serious effort — you have to know what defenses the target has, for example. So while there

The Cyber Operations Center at Fort Gordon, Ga., is home to signal and military intelligence noncommissioned officers, who watch for and respond to network attacks from adversaries as varied as nation-states, terrorists and "hacktivists."

Cyber operations specialists from the Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion (Cyber), from Fort Gordon, Ga., provide offensive cyber operations as part of the Cyber-Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) program during the 1st Stryker Brigade Combat Team, 4th Infantry Division, National Training Center Rotation.

are threats we must take into consideration, it is unrealistic to believe one guy in his basement, acting alone, could bring down the Internet or any major infrastructure system."

Perhaps the notion of a Cyber Pearl Harbor is somewhat overblown. "Could an adversary mount a meaningful attack against a critical infrastructure component to cause harm? Absolutely," he says. "But could it cause the same kind of loss of life as a Pearl Harbor or 9/11? Probably not. Our power structure is pretty resilient and could recover from an attack fairly quickly. I would not put cyber in the same category as a Pearl Harbor or 9/11. I don't think anybody would really want to make that kind of cyber attack on its own, except perhaps a terrorist organization. So while some scenarios are pretty scary, I don't think they jump to that level."

To help prepare for and defend against cyber attacks, the U.S. military services have begun including cyber in military exercises, including some, such as the Army's Cyber Blitz, dedicated to cyber warfare. The Army has conducted three such exercises, each incorporating what was learned from previous efforts and the latest technologies.

Cyber Blitz 3 involved more than 700 participants from 25 organizations, including the Marines. The integrated campaign has matured through those exercises to improve how to go "from space to mud" in support of the tactical commander in a fight against a regional peer in kinetic and non-kinetic effects, such as cyber.

"Cyber Blitz was born as the result of the Cyber Center of Excellence and CERDEC, back in 2015, wanting to demonstrate and validate the concepts of that doctrine before it was updated to the Army writ large," says CERDEC's Wittstruck. "We established our first Cyber Blitz in 2016, in which a unit had to fight their way through a validated scenario, not just kinetic effects in which they were well versed, but also cyber attacks, GPS denial, spoofing They had to learn, sometimes on the fly, how to deal with that. The Army's cyber warriors don't operate in a vacuum, but in a combined arms fight. So we focused on a brigade fight working with partners."

Keeping in practice

Cyber Blitz 2019 will pivot to the Pacific and work with Pacific Command to determine what elements should be the subject of focus. Wittstruck predicts they will integrate cyber into some as yet unnamed element in that exercise.

Cyber defense is not exclusively an end user concern, it begins at the beginning, with the contractors who build the systems, subsystems and components that comprise a cyber or cyber-protected program.

"The threats are ubiquitous," notes David Sheets, senior principal security architect at Curtiss-Wright Defense Solutions. Defense contractors, he says, "have to understand the risks and make sure we have all the correct procedures and processes in place so we can tell our customers we have done the due diligence to assure they will have a secure system once they put all the boards and such together. That impacts our supply chain management, production flow, all of which have to go together to insure there are no kinks in the armor as you integrate these systems.

"Multiple people have been trying to wrap their heads around the intersection of cyber security and safety critical systems and how those work together," Sheets says. "I don't think anyone has a good answer to that yet — there is a lot of synergy in some areas, while in others, cyber may say one thing and safety something else." ←

Secure data storage for battlefield networking

Designers and systems integrators struggle with keeping data secure in proliferating networked devices, and blending systems with new and legacy information storage technologies.

BY **J.R. Wilson**

Information is the fuel that drives 21st Century military tactics, techniques, and procedures (TTPs) and the foundation on which all offensive and defense actions depend.

While the emphasis best known to the public is the collection of information, securing the collected data from the point of origin to eventual archiving is of equal, if not greater, importance. The increasingly rapid evolution of technology also is keeping security measures in a constant state of flux.

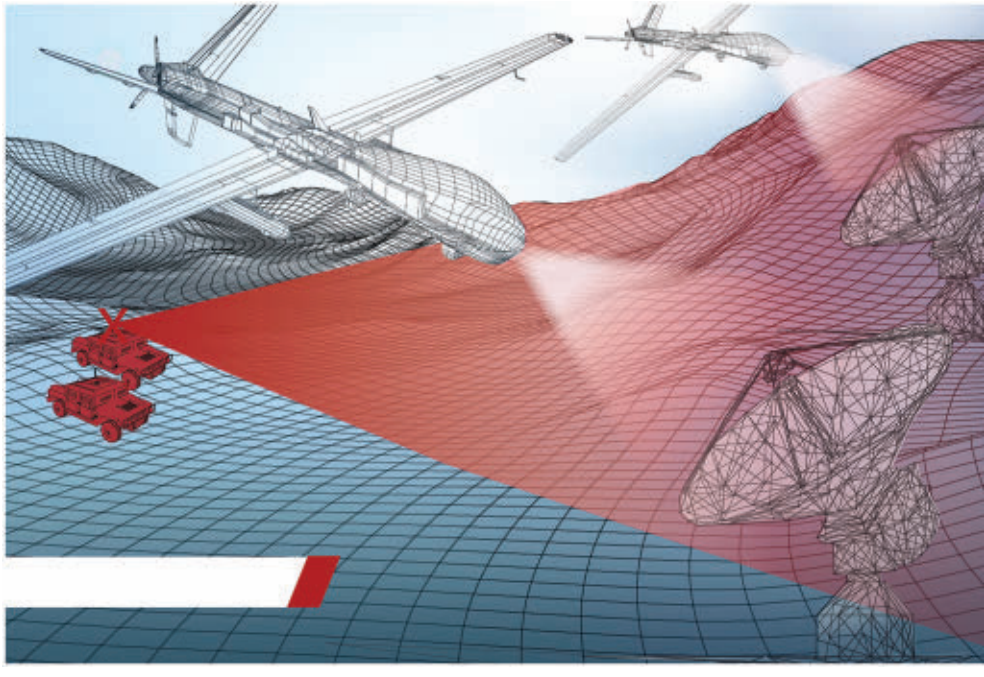
"With the emergence of so many technologies, it's hard to predict which technologies and security measures will be adopted — and some that are adopted may not last long," says Drew Castle, vice president of engineering at Chassis Plans LLC in San Diego.

"Estimates are there will be 40 billion interconnected devices by the end of next year," Castle continues. "Look at new technologies that are being developed by individuals at home and wonder how many will be adopted widely, what will trickle into the DOD [U.S. Department of Defense] space."

Military forces today rely on information technology more than ever before. "We are becoming more and more dependent on technology — and the more dependent we become, the higher the threat," Castle says. "We will be more rather than less vulnerable as we become more and more dependent on technology and susceptible to cyber threats and the destruction of that technology. And now you have lone actors who can take down networks and cause global problems at far less cost than a nuclear weapon."

Almost every military, government, academic, and industrial organization in the world today has at least an office, if not a full command, devoted to cyber and electronic security. Although that has placed a greater emphasis on security, especially at various levels of "data at rest", it also has been done largely on an independent basis.

"Our biggest question in terms of cyber and physical security is where is DOD going. There are huge numbers of briefings on it and we really want to understand how all those are going to join together in a uniform strategy for DOD



The battlefield of today is a monolithic data network, with data continually flowing from ground units, to aircraft, to satellites. This wouldn't be possible without secure data storage.

Priority

Source High-Reliability RF Cables

Need(s):

- ☑ Reliability
- ☑ J-STD Soldering
- ☑ Test Reports
- ☑ Lot Traceability

Tomorrow?

Pasternack

Complete Line of High-Reliability RF Cables Shipped Same-Day!

Our new portfolio of commercial-off-the-shelf (COTS), high-reliability RF cable assemblies are designed and processed to stand the test of time. These new cables are assembled using J-STD soldering processes and WHMA-A-620 workmanship. Inspection data, test data and material traceability are all included as part of the package. The combination of materials, processing and supporting data work together to create a dependable, fieldable cable assembly for applications where performance over time is critical and the cost of failure is high. Call or visit us at pasternack.com to learn more.

866.727.8376
Pasternack.com

an INFINITE company

PASTERNACK®
THE ENGINEER'S RF SOURCE

meeting their future cyber and physical security requirements for storage and networking," says Chassis Plans President Mike McCormack.

"I think that is still a work in progress. DOD is trying to understand what is the threat, how sophisticated is it, how can they counter and mitigate that, offensively and defensively, McCormack says. "The big question for us is what do we do in the next few years in terms of where DOD is going."

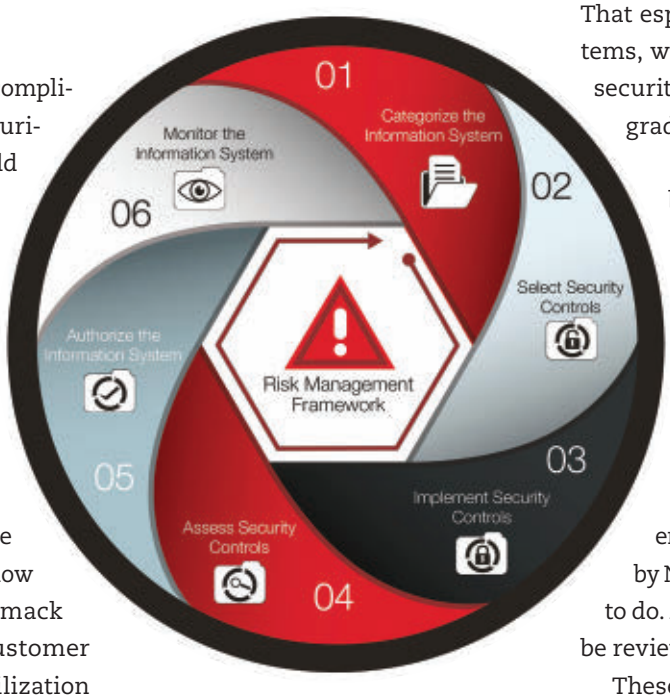
Complicated picture

That question is getting more complicated for those supplying security systems; contractors are told only the requirements — physical or software encryption or both — but not how or where the end system will be used.

"Depending on the mission and application, it goes into the ability to meet FIPS [Federal Information Processing Standard] compliance with your servers, depending on the customers perceived risk and how to mitigate that risk," McCormack says. "In most cases, the customer won't discuss with us the utilization of the data being stored, just ask what we can do to mitigate their risk. That may be FIPS compliance, potential outside corruption from an EMP [electromagnetic pulse] blast and so on."

Systems integrators are trying to keep information security risks to a minimum. "It really depends on what the customer wants us to do to mitigate the risk, whether physical security, tamper-proofing, or encryption levels. They give us the requirements and that's what we develop our products to meet," McCormack says.

Those requirements evolve not only with new missions but also in response to new developments in security and security-breaking capabilities. Requirements also reflect what the military perceives as the greatest threat to secure information storage at the time. Still, it must take into account every step along the way to creating and implementing security measures, with those requirements becoming pervasive across the network stream as well as in networked storage.



This chart outlines a process for designing trusted computing systems with secure data storage.

"I would say physical capture is the biggest threat, but a four-star general might say cyber security, being able to gain remote access," McCormack continues. "The threat is greater, including at the personal level, if you don't have the proper firewalls in place."

Third-party DOD information from a contractor to the military also has to have cyber security safeguards in place to comply with NIST 800, which are documents from the National Institute of Standards and Technology that describe government computer security policies, procedures and guidelines. "So the biggest concern at DOD is the cyber threat," McCormack says.

Dealing with legacy systems

What is certain is the demand for higher levels of security for military information storage only will increase as the ability of an ever-widening list of potential adversaries to penetrate legacy and current state-of-the-art grows. That especially is true for legacy systems, which tend to have proprietary security methodologies, making upgrades difficult.

"There is a level of encryption, but it is proprietary in most legacy systems, where now FIPS 140-2 is an industry standard with regard to encryption," says Amos Deacon III, president of Phoenix International in Orange, Calif. "Going back 10 or 20 years, companies developed their own proprietary encryption techniques, certified by NSA, but that is really expensive to do. And each future change has to be reviewed and re-certified."

These legacy systems can be difficult — if not impossible — to upgrade sufficiently to comply with modern data storage security standards. "For legacy systems, you're looking at a forklift upgrade," Deacon says. "If you have a system using hard disk drives that have been operating for more than five years, you have the output power and performance requirements of new technologies, in many cases, making it ineffective to try to continue using the older equipment and upgrade interfaces. You just put in a whole new system rather than a legacy tech refresh."

In a lot of those systems, the software was written for that specific

environment and equipment — which may have been out of production for many years. The solution is to move to new systems, many of them Linux-based, which enables the use of industry-standard encryption techniques.

Physical security

Although the bulk of today's data storage security is software-focused, physical security remains an important part of most security systems, especially active, online storage at fixed locations and inactive, offline archival storage.

"If you want secure data, that is security in terms of encryption, but also security of the physical drive, especially when it is removed from the deployed asset and returned to a lab," says Jason Wade, president of ZMicro in San Diego. "So you have to look at how you are cooling the drive, how it can be removed without degradation, and protection against the environment."

Sometimes the answer is combining technologies. "The state-of-the-art is really when you combine the technologies available in the marketplace," Wade says. "In just hard drives, there are numerous solutions with self-encrypted drives. The way you get a solution for the end user is to bring together a system that works in concert with the motherboard, the hard drive, and Opal 2 compliance. To provide the strongest level of security, you will put a layer on top of that using software encryption."

The Opal Security Subsystem Class is a hardware-based hard drive standard developed by the Trusted Computing Group (TCG) in Beaverton, Ore.,

Solid-state drives used in manned and unmanned airborne surveillance present a unique security challenge; if an aircraft is captured there may be no one available to physically destruct or initiate a process to eliminate the sensitive data.

to encrypt rotating media hard drives, solid-state, and optical drives. The benefits of hardware encryption include the ability to work with any operating system, transference of the encryption process' computational load to dedicated processors, reducing stress on the host CPU, and thwarting cold-boot attacks by storing the encryption/decryption keys in the hard drive controller rather than in system memory.

"We're in a sea-change with storage in terms of the advancement of NVMe-based storage modules," Wade says. "Moving forward, all hard drives will be NVMe-based and that will provide four times the read/write speed. And hard drives with Opal-2 compliance and encryption will become standard," he adds. "What will become more and more seamless is management of the drives, how they are erased, how the keys are managed. At a certain point, that will become inherent to all hard drives."

NVMe, which stands for non-volatile memory express, is a host controller interface and storage protocol created to accelerate the transfer of data between enterprise and client systems and solid-state drives (SSDs) over a computer's high-speed PCI Express bus.

Anti-tamper

The need for physical anti-tamper security was highlighted in 2001 when a U.S. Navy EP-3E ARIES II SIGINT aircraft collided with a Chinese J-8II interceptor jet and was forced to land on China's Hainan Island. The P-3 was dismantled by the Chinese military before being returned to the U.S. and an undisclosed amount of classified information was extracted from its computer systems.

"The encryption routines have progressed since then to the point that, while not impossible, it is a lot tougher to access data," says Phoenix's Deacon. "The use of solid-state storage devices also allows you to physically destroy the data in a much more complete and faster manner. The P-3 was using hard disk drives and there is no way to really quickly erase data on those drives short of destroying the media itself."

Security keys are the key ingredients of today's solid-state drives. "With solid-state, in addition to the encryption level, where you destroy the keys to the data, there are physical ways to erase the data much more quickly," Deacon says. "Even if you pull the power to that device, as soon as power is reapplied, the erasure procedure would continue, so the use of solid-state technology has allowed for an increase in the ability to secure data should it fall into a bad actor's hands. But anti-tamper also will have to be through software, to have the tamper evident and, proactively, to automatically sanitize the data or block the intrusion once it is detected."

Deacon agrees with McCormack that physical capture is a greater threat to classified data than remote access.

"You may not have the opportunity to press the button — software command or physical button — to destroy the data," Deacon says. "Then

Data security requires a system level approach including self-encrypting drives, host support for secure encryption key management, and physical security features that support robust transportability

you have to rely on the level of encryption. The level of computing power these days requires a higher level of encryption, typically AES-256 on a fixed 140-2 device. The beauty of AES-256 is the use of encryption keys, which are what allow you to access the system — and the combination of keys is massive."

It's extremely difficult to break in to one of today's secure hard drives. "To put it in perspective, breaking into a 256-bit key by brute force would take something like 50 supercomputers checking a billion AES keys per second

Built-in encryption solves helps safeguard sensitive mobile information since adversaries will be unable to access data on the drive without the authorization key.

and take literally thousands of years to hit every combination," Deacon says. "There's just not a computer technology currently capable of cracking that, which leaves only quantum computing, which isn't there yet. But network security needs physical and software preventative measures, from an enclosed system to a software infrastructure that denies unauthorized access, modification or destruction of the data."

Trusted supply chain

Another element of increasing concern is a trustworthy supply chain. The prime contractor and its major subcontractors may have the highest levels of physical and digital security in place, but still be vulnerable due to a third-level supplier's use of components made in China.

The People's Republic of China has become the world's leading producer of electronics, from the smallest connectors to major systems, such as satellites. It also has made no secret of its intention to become the world leader in cyber and electronic warfare. The U.S. military has protocols in place blocking the use of Chinese and Russian software and electronics to combat counterfeit parts and potential "back door" security holes.

"Part of the conversation today is how to reduce vulnerability, but a lot of things are made in China, including most processors. There are processes and procedures in place to verify component providers," says ZMicro's Wade. "What's at issue is the potential of vulnerabilities in hardware, which always needs to be addressed. And that brings you back to the system-level approach, with Opal drives and 256-level encryption and hardware that supports TPM tech."

Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor — a dedicated microcontroller that secures hardware by integrating cryptographic keys. The technical specification was written by the Trusted Computing Group. The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standardized the specification as ISO/IEC 11889 in 2009.

Sometimes it all comes down to the political situation at any given time. "China has now become an adversary in technology and political and economic power in the world, says Chassis Plans's McCormack. "DOD and the world in general are realizing we have to find other sources that are TEA [technology exchange agreement] compliant. But Taiwan is TEA compliant, but get a lot of their components from China," he says.

"Do you have processes in place to make sure you are not getting components that are counterfeit or have been tampered with in China? There will be a bigger drive to see that there is more TEA complaint board manufacturing in the U.S., in the DOD space and in U.S. manufacturing," he says.

On the near horizon is another advance that influences the data security of individuals, governments, corporations, and the military, yet its primary evolution is in the least secure environment of all — the home.

Networked vulnerabilities

"Who is driving the technology? Look at the Internet of Things, with totally interconnected homes and people who are remote working," McCormack warns. "Having everything connected is fantastic. But that also will be the biggest threat. It allows the exponential spread of viruses because security in the home, especially, does not protect against cyber attacks. If someone attacks my thermostat, which is connected to my computer, that allows access to my bank accounts."

"It's like building the interstate," he continues. "It improved transportation, but fatalities increased massively. Between 2005 and 2012, we saw a lot of ransomware attacks. Then we got smarter. Each home, office, and defense component must have more and more firewalls and security measures to isolate them within greater wide area networks."

The rapid and universal spread of new electronic and computing technologies has increased the vulnerability of today's deployed military to data interception, spoofing, and tampering.

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

COMPANY LIST

Aitech Defense Systems
Chatsworth, Calif.
www.rugged.com

Barracuda Networks
Campbell, Calif.
www.barracudanetworks.com

Cavium Networks
San Jose, Calif.
www.caviumnetworks.com

Chassis Plans LLC
San Diego
www.chassis-plans.com

Crystal Group
Hiawatha, Iowa
www.crystalrugged.com

Conduant
Longmont, Colo.
www.conduant.com

Curtiss-Wright Defense Solutions
Ashburn, Va.
www.conduant.com

DRS Tactical Systems Inc.
www.leonardodrs.com/products-and-services/leonardo-tactical-systems

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

Extreme Engineering Solutions
Verona, Wis.
www.xes-inc.com/about/contact/

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

Kaman Fuzing & Precision Products
Middletown, Conn.
www.kaman.com/fuzing-precision-products

Kontron
www.kontron.com

Mercury Systems
Andover, Mass.
www.mrcy.com

Pentek Inc.
Upper Saddle River, N.J.
www.pentek.com

Phoenix International
Orange, Calif.
www.phenxint.com

Trusted Computing Group
Beaverton, Ore.
https://trustedcomputinggroup.org

ZMicro
San Diego
https://zmicro.com

"That is a consideration that is holding back the deployment of some systems," says Phoenix's Deacon. "For example, the fusing of sensors, such as proposed for the Joint STARS recapitalization program, taking a number of independent sensors on-platform and sharing that data."

Necessary solutions might not be available for some time. "The technology to do that does not exist right now and potentially that won't be available for another 15 or 20 years," Deacon says. "So there is a risk of the cancellation of the JSTARS recap program for this fused sensor approach because being able to move that much data around in a real-time environment can't yet be done — and once you do get there, you run into security problems."

The Compact Network Storage 4-slot (CNS4) conduction cooled high-performance data recorder from Curtiss-Wright Defense Solutions offers scalable storage and encryption options for capturing critical data in a harsh environment.

Determining what security measures to implement in a given system often involves the end user deciding what capabilities are most important to the mission.

"There are tradeoffs you constantly have to make and evaluate," says ZMicro's Wade. "For example, if the customer requests 140-2 compliance, we can look at Opal 2 drives; if they are looking for it to be validated, that reduces the number of available drives. Yet if a customer identifies high-speed processing as a paramount factor, software encryption might not work, despite providing a greater level of security, but with a performance hit. But with the ever-increasing performance of today's processors, the level of that hit is open to question."

Readily available technology

Advancing technologies, many available to anyone to adapt to offensive applications, have made truly secure military information storage a critical component of military operations and procedures at all levels. But securing data takes more than hardware and software, it also has to address the human factor.

"It will include secure physical access, from passwords to more advanced restrictions," says Chassis Plans's McCormack. "Also people not bringing outside media into facilities where malware might get onto the system. You have to make sure the staff is trained on the threats that are out there; human beings are the weakest points of entry and make mistakes, so the training has to be there to understand security requirements, even in the smallest companies. You never know where a thumb drive has been or came from, so you have to make sure you keep physical media from coming into a facility."

As more sensors and platforms collect and process more and more data, transferring it over high-speed networks to real-time displays, short-term and archival storage, the greater the need for multiple layers of hardware- and software-based encryption and anti-tamper solutions.

As ZMicro's Wade notes, "Everything is a potential vulnerability if you're not paying attention to it." ←

Army to make AH-64E Apache attack helicopter more capable at sea and deadlier overall

The U.S. Army has released new details about its plans for improving the AH-64E Apache attack helicopter as part of the future Version 6 upgrade package. The updates will include a major boost in the Apache Guardian attack helicopter maritime capabilities, make it easier for them to team up with a much broader range of unmanned aircraft, and improve the helicopter's general ability to collect and share information, engage hostile targets, and avoid threats. The Army's Apache Attack Helicopter Project Office presentation shows that the service completed integrating the Version 4.5 capabilities into the AH-64E fleet in 2017 and plans to finish with the Version 6 updates by 2026. The Army first began receiving AH-64Es, previously known as the AH-64D Block III and also called the Apache Guardian, in 2011. The helicopter will remain the service's primary attack helicopter through at least 2048, though the gunship version of the Future Vertical Lift family of aircraft is supposed to reach initial operational capability in 2034.

Air Force scraps Boeing upgrade of AWACS radar signal processing

The U.S. Air Force terminated a Boeing Co. contract to update the radar on its flagship AWACS radar surveillance aircraft after the company encountered major delays in developing hardware and software, according to budget documents. Instead of continuing the $76 million contract with Boeing, "the Air Force determined the best approach for providing this critical capability would be to replace the legacy radar processor and its related components,"

Air Force eyes airborne communications node with artificial intelligence

BY **John Keller**

HANSCOM AIR FORCE BASE, Mass. — U.S. Air Force communications experts are looking for companies able to design an airborne communications node able to gather, process, and distribute important battlefield information.

Officials of the Special Programs Division of the Air Force Life Cycle Management Center's C3I&N Directorate at Hanscom Air Force Base, Mass., issued a request for information for the Multi-Domain Command and Control Mobile Node Capability project.

Air Force experts want to hear from companies able to design airborne communications nodes able to ingest data securely at high data rates via existing and future military airborne and satellite communications links.

This node should be able to perform artificial intelligence (AI) functions like data prioritization, data normalization, and semantic enrichment; enable AI products; and export relevant data and AI products. This communications node should be able to manage several different levels of security.

The idea is to gather, process, and disseminate important information to warfighters quickly to exploit enemy weaknesses on the ground, on the air, at sea, and in cyberspace. This communications node also should be able to mitigate enemy electronic warfare (EW) and cyber attacks against command-and-control communications.

Technical challenges include securely blending legacy and future command-and-control data links; managing incoming data quickly and securely; managing data availability, open artificial intelligence development environment, and security; disseminating data to specific users securely in a delay-tolerant network; developing autonomous operation; and manage size, weight, and power consumption (SWaP).

Air Force researchers are working on a new battlefield airborne communications node to gather, process, and distribute important information.

Air Force experts are looking for an airborne communications node matured at least to a developmental level (technology readiness level 4), with estimates of how long it would take to achieve a demonstrable system (technology level 6).

Companies interested were asked to email eight-page white papers by 5 Dec. 2018 to the Air Force's Gregory Ketcham at gregory.ketcham@us.af.mil. For questions or concerns contact Gregory Ketcham by phone at 781-225-0601, or by email at gregory.ketcham@us.af.mil.

More information is online at https://www.fbo.gov/spg/USAF/AFMC/ESC/FA87826-19-X-HNJK/listing.html.

Ball Aerospace to build first WSF-M microwave imaging weather satellite

BY **John Keller**

EL SEGUNDO, Calif. — Spacecraft designers at Ball Aerospace & Technologies Corp. in Boulder, Colo., are moving forward with a project to develop a next-generation weather satellite with a passive microwave imaging radiometer instrument to measure the direction and speed of ocean winds, as well as the intensity of global hurricanes.

Officials of the U.S. Air Force Space and Missile Systems Center at Los Angeles Air Force Base in El Segundo, Calif., announced a half-billion-dollar order to Ball Aerospace last month for the Weather System Follow-On-Microwave (WSF-M) satellite project.

The Air Force is awarding $255.4 million to Ball Aerospace to develop and build the WSF-M space vehicle 1. Ball originally won a $93.7 million contract last year to get started on the WSF-M project to design and build the WSF-M low-Earth-orbit satellite with a passive microwave imaging radiometer instrument and hosted government furnished energetic charged particles sensor to provide ocean surface vector wind and tropical cyclone intensity capabilities.

The WSF-M will be a next-generation polar-orbiting satellite to provide the kind of space-based terrestrial environmental sensing capabilities now provided by the Defense Meteorological Satellite Program (DMSP) and the Naval Research Laboratory's WindSat spacecraft.

The WSF-M system will have a space segment, launch segment, and ground segment. The space segment has a flight vehicle testbed, ground support equipment, and a satellite able to sense, sore, and transmit microwave raw sensor data to measure wind speed and direction at the ocean's surface — including the intensity of tropical cyclones like hurricanes and typhoons.

Ball Aerospace is developing the Weather System Follow-On-Microwave (WSF-M) satellite with a passive microwave imaging radiometer to measure winds at sea and the intensity of global hurricanes.

The WSF-M launch segment consists of launch vehicle, launch support facilities, and launch services. Its consists of a primary and backup ground services operations center, as well as the Air Force Satellite Control Network (AFSCN) Space Ground Link System (SGLS) and Unified S-Band (USB)-capable ground stations. The ground segment incorporates WSF-M mission software, including WSF-M command and control software and senor data processing software.

On this contract Ball Aerospace will do the work in Boulder, Colo., and should be finished by January 2023. ←

*For more information contact **Ball Aerospace** online at www.ball.com/aerospace, or the **Air Force Space and Missile Systems Center** at www.afspc.af.mil.*

Captain Hope Cronin, a service spokeswoman, said in an email. "Several companies responded to the Air Force's request for information, and a request for proposal is currently being developed." Boeing was on contract to provide improved radar digital signal processing "in a specific flight environment to meet a classified requirement," for its E-3 Sentry Airborne Warning and Control System surveillance aircraft, Cronin said. The E-3 Sentry airborne warning and control system (AWACS), which are modified 707-320 commercial planes, are recognized by their saucer-shaped, rotating radar domes that can spot and classify aircraft as far as 250 miles away.

Navy recognizes electromagnetic battlespace, convergence with cyber

A new U.S. Navy policy recognizes the electromagnetic spectrum as a warfighting domain on par with sea, land, air, space and cyber. The policy pushes an enterprise approach to all activities necessary for Navy electromagnetic spectrum (EMS) operations, including the department's roles and responsibilities for developing, implementing, managing, and evaluating electromagnetic battlespace programs, policies, procedures, and controls, according to the policy, which took effect on 5 Oct. The EMS enterprise includes all electronic systems, subsystems, devices, and equipment that depend on using the electromagnetic spectrum. The role of spectrum warfare and its potential convergence with cyber and electronic warfare (EW) has been a big topic in military circles over past several years, with strategists divided on how to manage the two battle domains. U.S. Army Cyber Command leadership anticipates the domain to possibly replace, cyber in warfare planning. ←

General Atomics to build year's worth of MQ-9 Reaper unmanned combat drones

BY **John Keller**

WRIGHT-PATTERSON AFB, Ohio — Unmanned aerial vehicle (UAV) experts at General Atomics will build additional MQ-9 Reaper unmanned aircraft for surveillance and attack under terms of a $263.4 million contract.

Officials of the U.S. Air Force Life Cycle Management Center at Wright-Patterson Air Force Base, Ohio, are asking the General Atomics Aeronautical Systems segment in Poway, Calif., to produce the MQ-9 Reaper combat drones in the fiscal 2018 production configuration.

The Reaper, a variation of the General Atomics MQ-1 Predator UAV, is designed for surveillance and attack missions using a suite of airborne sensors and the AGM-114 Hellfire air-to-ground missile. Last December Air Force officials started a project to integrate the Raytheon laser-guided small diameter bomb (SDB) on the Reaper.

The latest version of the combat UAV, the Reaper Block 5, has increased electrical power, secure communications, auto land, increased gross takeoff weight, weapons growth, and streamlined payload integration capabilities, compared with earlier Reaper Block 1 versions.

The Block 5 model has a high-capacity starter generator and upgraded electrical system with a backup generator that can support all flight-critical functions.

The MQ-9 Reaper armed drone has three independent power sources to accommodate new communications such as dual ARC-210 VHF/UHF radios with wingtip antennas for simultaneous communications among multiple air-to-air and air-to-ground parties; secure data links; and an increased data transmission capacity. The Reaper Block 5 can carry heavier payloads or additional fuel.

The turboprop-powered, multi-mission Reaper armed drone can fly for more than 27 hours without refueling at speeds to 240 knots at altitudes to 50,000 feet. The medium-endurance UAV can carry payloads as heavy as 3,850 pounds, including 3,000 pounds of external stores like Hellfire missiles and the Small Diameter Bomb.

The Reaper can carry as many as four Hellfire missiles, two GBU-12 Paveway II laser-guided bombs, or two 500-pound GBU-38 Joint Direct Attack Munitions (JDAMs). Twice as fast as Predator, the Reaper carries 500 percent more payload and has nine times the horsepower, General Atomics officials say.

The Reaper has a fault-tolerant flight control system, triple-redundant avionics system, and is powered by the Honeywell TPE331-10 turboprop engine, integrated with digital electronic engine control (DEEC) to improve engine performance and fuel efficiency at low altitudes.

The Reaper can carry electro-optical and infrared (EO/IR) sensors, Lynx multi-mode radar, multi-mode maritime surveillance radar, electronic support measures (ESM), laser designators, and a variety of weapons.

General Atomics will build additional MQ-9 Reaper unmanned aircraft for surveillance and attack under terms of a $263.4 million contract.

The sophisticated combat UAV has redundant flight-control surfaces; can fly remotely piloted or autonomously; has a MIL-STD-1760 stores management system; seven external payload stations; C-band line-of-sight data link control; Ku-band beyond line-of-sight and satellite communications data link control; more than 90 percent system operational availability; and can self-deploy or fly aboard C-130 utility aircraft.

This aircraft has been acquired by the U.S. Air Force, U.S. Navy, U.S. Department of Homeland Security (DHS), NASA, the United Kingdom Royal Air Force, the Italian Air Force, and soon others, company officials say. On this order General Atomics will do the work in Poway, Calif., and should be finished by November 2021. ←

For more information contact ***General Atomics Aeronautical Systems*** *online at www.ga-asi.com, or the* ***Air Force Life Cycle Management Center*** *at www.wpafb.af.mil/aflcmc.*

Raytheon BBN to tap into sea life to help detect and track enemy submarines and UUVs

BY **John Keller**

ARLINGTON, Va. — Marine scientists at Raytheon BBN Technologies Corp. in Cambridge, Mass., are investigating new ways of using sea life to detect and track potentially hostile manned submarines and unmanned underwater vehicles (UUVs) over vast areas of the world's oceans.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., announced a potential $6.4 million contract to Raytheon BBN last month for the Persistent Aquatic Living Sensors Bio-Acoustic Sonar System (PALS) program.

PALS seeks to capitalize on living things in the ocean to augment existing hardware-based maritime sonar to tap into the innate abilities of marine organisms to sense and respond to disturbances caused by submarines and UUVs. The DARPA PALS contract to Raytheon BBN is for $3.3 million, and has options to increase that to $6.4 million.

DARPA and BBN researchers will work together to apply those abilities to detect, characterize, and report on manned or unmanned underwater vehicles ranging from small autonomous vessels to large nuclear submarines.

Because marine organisms are ubiquitous, self-replicating, and largely self-sustaining, sensing systems that use marine organisms as their foundation would be discreet, cost-effective, and provide persistent undersea surveillance with a minimal logistical footprint, DARPA officials explain.

DARPA and BBN are trying to develop a two-stage system that first can sense and detect the presence of an underwater vehicle and respond with an output signal or other observable behavior; and second to develop a detector to observe, record, and interpret

Military researchers are looking into using sea life to help track the movements of submarines and unmanned underwater vehicles (UUVs)

the organisms' responses, and report analyzed results.

The complete PALS system also will seek to discriminate between target vehicles and other sources of stimuli, such as debris and other marine organisms, to limit false alarms.

The world's vast oceans and seas offer seemingly endless spaces where U.S. adversaries can maneuver undetected, DARPA officials say. The U.S. military deploys networks of manned and unmanned sensors to monitor adversary activity, but the scale of the task is daunting and hardware alone cannot meet every need.

Sea life, however, offers a potential new advantage, DARPA officials say. Marine organisms are attuned to their surroundings, and may be able to help monitor strategic waters such as straits and littoral regions for enemy submarines and UUVs.

DARPA and BBN scientists will study natural and modified organisms to determine which ones best could support sensors able to detect the movement of manned and unmanned underwater vehicles. The idea is to capture and interpret the responses of these marine organisms with networked hardware.

"The U.S. Navy's current approach to detecting and monitoring underwater vehicles is hardware-centric and resource-intensive," says Lori Adornato, the DARPA PALS program manager. "As a result, the capability is mostly used at the tactical level to protect high-value assets like aircraft carriers, and less so at the broader strategic level.

"If we can tap into the innate sensing capabilities of living organisms that are ubiquitous in the oceans, we can extend our ability to track adversary activity and do so discreetly, on a persistent basis, and with enough precision to characterize the size and type of adversary vehicles," Adornato says.

Sea life adapts and responds to its environment, DARPA officials explain, prompted by evolution to sense tactile, electrical, acoustic, magnetic, chemical, and optical stimuli. Raytheon BBN researchers will develop hardware, software, and algorithms to translate organism behavior into actionable information and then communicate it to military authorities. ←

*For more information contact **Raytheon BBN** online at www.raytheon.com/ourcompany/bbn, or **DARPA** at www.darpa.mil*

Vehicle-mounted laser weapon could help Marines knock down UAVs on the move

A battlefield laser weapon designed to destroy or disable enemy unmanned aerial vehicles (UAVs), already in use by the U.S. Army, is giving U.S. Marine Corps leaders a glimpse at how they might melt drones soon. The Compact Laser Weapon System, or CLWS, is already part of the Army's Mobile Expeditionary High Energy Laser program. The vehicle-mounted weapon is deployed on Stryker vehicle in Europe and has been part of field experiments. The Boeing creation is a 5-kilowatt laser that can shoot down UAVs, attack snipers, breaching obstacles, setting-off unexploded ordnance, denying enemy landing zones, and to defend ports or airfields. The laser can mount atop the Joint Light Tactical Vehicle (JLTV) or other light battlefield vehicles, or it can go on a tripod and hooked to a generator to knock down UAV threats at a medium-sized forward-operating base or on the perimeter of a larger installation.

Pentagon wants more money for directed-energy weapons for drone-swarm and missile defense

The U.S. military will request more money to develop lasers, microwave beams, and other directed-energy weapons to fight off missiles and drone swarms, the Pentagon's top weapons engineer says. "You're going to see, in upcoming budgets for missile defense, a renewed emphasis on laser scaling [meaning scaling up the power of laser weapons] across several technologies," says Michael Griffin, defense undersecretary for research and engineering. "In my opinion, we are no more than a few years away from having laser weapons of military utility," Griffin says. "In units of ones

Boeing to upgrade infrared search and track (IRST) for Navy jet fighter-bombers

U.S. Navy air combat experts are asking electro-optics engineers at the Boeing Co. and Lockheed Martin Corp. to upgrade infrared search and track (IRST) sensors for the F/A-18E/F Super Hornet jet fighter-bomber to enable the aircraft to detect, track, and attack enemy aircraft in a stealthy way without making its presence known.

Boeing and Lockheed Martin are upgrading the infrared search and track systems on Navy Super Hornet jet fighter-bombers.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., announced a maximum $131.6 million order Thursday to the Boeing Co. Defense, Space & Security segment in St. Louis to build and upgrade weapon-replaceable assemblies to optimize the Block I low-rate initial production F/A-18E/F IRST.

The order includes technical risk reduction related to an engineering change proposal, and asks Boeing experts to provide integration and tactics development.

The Super Hornet's IRST is a long-wave infrared detection system that can detect and lock weapons onto enemy aircraft without using radar. The system detects hot spots on aircraft — particularly their engine exhaust. The passive system does not emit RF energy like radar does, and can help conceal the presence of its aircraft.

The system for jet fighters, which Boeing is buying from the Lockheed Martin Missiles and Fire Control segment in Orlando, Fla., uses infrared search and track technology to detect and provide weapon-quality track solutions on potentially hostile aircraft.

The electro-optical IRST Block I, also called the IRST21 Sensor System, fits on the front of the Super Hornet's centerline fuel tank. Two years ago, Navy leaders approved a restructured program that foregoes full-rate production of Block I sensors and proceeds directly to the Block II system.

The IRST consists of a passive long-wave infrared receiver, a processor, inertial measurement unit, and environmental control unit. The infrared receiver, processor, and inertial measurement unit fit inside the sensor, which attaches to the front of the fuel tank mounted on the Super Hornet's BRU-32 bomb rack.

The Navy developed the IRST Block I using components from the F-15K/SG aircraft's infrared receiver, which is based on the IRST design of the now-retired Navy F-14 Tomcat jet fighter. IRST Block II will include improvements to the infrared receiver and updated processors.

At this stage, existing IRST Block I systems will support testing and tactics development. Navy leaders say they will begin the Block II operational tests in 2020. The Navy intends to produce 170 IRST systems.

Even amid electronic attack or heavy RF and infrared countermeasures, IRST

provides autonomous, tracking data that increases pilot reaction time, and enhances survivability by enabling first-look, first-shoot capability, Lockheed Martin officials say.

The IRST's stealth characteristics can enable Super Hornet pilots to make positive identification of enemy aircraft at long ranges, and enable them to fire their air-to-air missiles at maximum ranges.

Data from the IRST system can stand alone or fuse with other on-board sensor data situational awareness. Lockheed Martin also is developing an IRST pod for the F-15C and F-16 jet fighters.

On this order Boeing and Lockheed Martin will do the work in Orlando, Fla., and in St. Louis, and should be finished by April 2022. ←

For more information contact ***Boeing Defense, Space & Security*** *online at www.boeing.com/defense,* ***Naval Air Systems Command*** *at www.navair.navy.mil.*

DARPA eyes microelectronics optical interconnects for high-performance embedded computing boards

BY **John Keller**

ARLINGTON, Va. — U.S. military researchers are asking the microelectronics industry to find ways of using optical interconnects on high-performance embedded computing boards to enhance bandwidth, power efficiency, channel density, and link reach.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) have released a broad agency announcement for the Photonics in the Package for Extreme Scalability (PIPES) program.

PIPES seeks to enable disruptive system scalability by developing optical signaling technologies for digital microelectronics. The program will employ intimate integration of photonics with advanced integrated circuits to yield unprecedented system connectivity.

The project seeks to integrate photonic interconnects on state-of-the-art multichip modules for system prototyping; advance embedded optical signaling performance with emerging component technologies, photonic-electronic integration techniques, scalable architectures, and multiplexing concepts; develop low-loss optical packaging and reconfigurable switching technologies; and, establish a domestic ecosystem that gives military systems designers access to new capabilities for in-package photonic signaling.

The DARPA PIPES project aims to use optical interconnects on high-performance embedded computing boards to enhance bandwidth, power efficiency, channel density, and link reach.

Since the end of clock frequency scaling in the mid-2000s, the microelectronics industry progressively has embraced parallelism to sustain performance growth, DARPA researchers explain. Constraining the benefits of parallelism, however, is not computation at individual nodes, but

or twos, we can roll out tens of kilowatts. That is within a factor of two or three of being useful on a battlefield, airplane or ship" to take out enemy drone swarms, Griffin says. A space-based weapon that could destroy boost-phase missiles would require power in the megawatt class. One big question remains: whether missile-defense satellites will make it into the Missile Defense Review.

Medium-wave infrared (MWIR) camera for electro-optical imaging introduced by Sierra-Olympic

Sierra-Olympic Systems Inc. in Hood River, Ore., is introducing the Ventus 275 medium-wave infrared (MWIR), 640-by-512-by-15-micron imaging engine for security, surveillance, fixed monitoring, military, and unmanned vehicle applications. The compact MWIR camera core weighs about 2.5 pounds, and is designed for OEM integrators of surveillance system enclosures and other imaging gimbals. It has an f/5.5, 19–275 millimeters continuous zoom (CZ) optic. The Ventus 275 features include an indium antimonide focal plane array and a finely tuned athermalized and parfocal zoom lens with a 28.4–2-degree horizontal field of view (HFOV). The image processing engine provides advanced image enhancements including electronic image stabilization, automatic-and-manual gain control, adaptive contrast control and optional target tracking and detection. The electro-optical imaging device also features a shutter-based non-uniformity correction (NUC) and an environmentally-sealed front lens element. Several output interfaces include analog NTSC/PAL video, H.264/MJPEG IP video, and 14-bit Camera Link digital video. For more information contact **Sierra Olympic** online at https://www.sierraolympic.com/products/details/ventus-275. ←

by data movement between embedded computing nodes.

While short-reach connects is possible today between on-chip cores and within multi-chip modules using high-bandwidth electrical links, this interconnect performance rapidly degrades at the longer lengths of circuit boards and beyond because of unfavorable scaling with frequency and reach. This restricts off-chip I/O capacity, reduces system performance, and limits its scalability.

Granted, photonic transceiver modules can enable optical signaling with high bandwidth and minimal loss over long distances with optical fiber, yet optical I/O typically comes in pluggable modules on circuit boards, connected to MCM packages with electrical links whose power dissipation and density limit overall performance.

Instead, DARPA researchers are trying to find improvements by reducing signaling energy and latency, while increasing overall signaling capacity and component density. This is where the PIPES project comes in.

Developing efficient, high-bandwidth, package-level photonic signaling should have substantial influence on high-performance computing, on big-data applications that use machine learning, advanced sensors, and wireless interfaces.

While optical signaling is common today in such systems at the board and rack levels, it has not yet been integrated within component switch chips, central processing units (CPUs), and graphical processing units (GPUs).

The PIPES program revolves around three technical areas: photonically enabled multichip modules; photonics for massive parallelism; and interconnect fabrics to facilitate package-level photonic I/O in future systems.

PIPES is a 42-month program divided into three phases: demonstration of concepts, components, and function; integration and prototyping; and establishing scalability, complexity, and maturity.

Companies interested were asked to upload abstracts to the DARPA BAA Website by 20 Nov. 2018 at https://baa.darpa.mil, and to submit full proposals no later than 17 Jan. 2019 online at www.grants.gov/applicants/apply-for-grants.html.

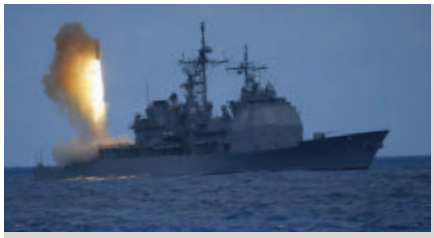
Email questions or concerns to Gordon Keeler, the PIPES program manager, at HR001119S0004@darpa.mil. ←

More information is online at https://www.fbo.gov/spg/ODA/DARPA/CMO/HR001119S0004/listing.html.

Lockheed Martin eyes satellite sensor payload providers for next-gen missile warning

Lockheed Martin Corp. has down-selected Raytheon and a Northrop Grumman–Ball Aerospace team to compete to provide the satellite sensor payload for the Air Force's next-generation missile warning satellite system. This competition will be part of the first-phase contract for the next-generation overhead persistent infrared (OPIR) Block O Geosynchronous Orbit (GEO) satellite, which will replace the service's current Space-Based Infrared System (SBIRS) expected to be phased out within the next five years. The award includes development scope through critical design review. A final down-select is expected at the end of the CDR phase in 2020. ←

PRODUCT applications



CONTRACT MANUFACTURING

DRS to provide electronics manufacturing on rugged shipboard computers

Electronics manufacturing experts at Leonardo DRS Laurel Technologies in Johnstown, Pa., will build shock-resistant open-architecture computing systems for U.S. Navy destroyers and cruisers under terms of an $8.6 million order.

Officials of the Naval Sea Systems Command in Washington are asking DRS Laurel to build 18 technical insertion (TI) 16 Common Processing System (CPS) water-cooled core computing system cabinets and six TI-16 CPS water-cooled advanced storage area network cabinets.

The CPS provides a common computing infrastructure for ship combat systems, including rugged computer processing, memory, data storage and extraction, and I/O interfaces for combat systems.

Other contract manufacturers for the Navy CPS include Global Technical Systems (GTS) in Virginia Beach, Va., as well as Northrop Grumman Corp., IBM Corp., and GoAhead Software, which has been acquired by Oracle Corp. in Redwood City, Calif.

CPS runs Navy combat system software applications in naval surface warship combat systems such as Aegis Modernization, Aegis new construction, Surface Electronic Warfare Improvement Program (SEWIP), and other Navy programs.

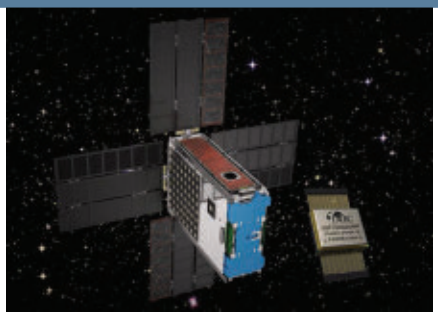
DRS engineers build the shipboard electronics CPS using commercial off-the-shelf (COTS) hardware and software such as BladeCenter technology that supplies common infrastructure for processing and network fabric.

The CPS consists of a rugged enclosure and three subsystems: the processing subsystem, the storage and extraction subsystem, and the I/O subsystem.

The processing subsystem provides the computing resources to execute combat system application programs on Navy surface ships. The storage and extraction subsystem provides data storage for CPS operating system (OS) image storage, program storage, data extraction, and database management. The I/O subsystem, meanwhile, interfaces the processing and storage hardware to various external elements.

Oracle provides for the Common Processing System open-standard middleware, designated SAFfire, for the CPS to support high-availability management of mission-critical combat system. SAF stands for Standards Availability Forum, an industry consortium of companies that develop open standards-based products. The overall CPS is designed with a shock-isolating enclosure that protects unhardened COTS components from the intense shock and vibration that can occur on Navy surface ships — including hits from missiles and torpedoes. The CPS comes in air- and water-cooled versions.

On this order DRS will do the work in Johnstown, Pa., and should be finished by December 2019. For more information contact DRS Laurel Technologies online at *www.leonardodrs.com/locations/drs-laurel-technologies-johnstown-pa,* or Naval Sea Systems Command at *www.navsea.navy.mil.* ←



SOLID-STATE MEMORY

Radiation-hardened memory from DDC picked for NASA BioSentinel space project

Space flight computer experts at the Space Dynamics Laboratory at Utah State University in North Logan, Utah, needed radiation-hardened high-density NAND Flash memory for the Pearl single-board computer they designed for the NASA BioSentinel CubeSat spacecraft. They found their solution from Data Device Corp. (DDC) in Bohemia, N.Y.

The Pearl single-board computer is to be used as the flight computer on the NASA BioSentinel CubeSat satellite space mission to study the effects of solar radiation on organisms.

The Pearl computer board, along with DDC's Flash memory, is baselined for use on several different upcoming missions for NASA and the U.S. Department of Defense (DOD).

BioSentinel CubeSat will deploy as part of the first flight of the Space Launch System (SLS) — the largest rocket ever developed, and will enable astronauts to explore destinations far into the solar system.

DDC's 192-gigabit NAND Flash provides the CubeSat spacecraft with compact high-density memory to enable the satellite's use of triple modular redundancy (TMR) error correction for operation without failure, DDC officials say.

The NAND Flash uses radiation-mitigation RAD-PAK technology that provides spot shielding against space radiation. RAD-PAK enables DDC to deliver the latest commercially available microelectronics in a space-qualified package, providing designers with high-performance space-grade solutions at affordable costs.

RAD-PAK-based space solutions offer a total dose immunity of 100 kilorads or higher, and have been qualified by NASA, ESA, JAXA. and

thousands of missions for over 20 years without flight failures.

DDC's hermetically sealed RAD-PAK NAND Flash devices come in a ceramic flat package with radiation-hardened shielding. They are based on as many as eight 32 Gb x8 NAND Flash die (256 Gb), and use single-level cell (SLC) Technology for fast read and write capabilities and boot times.

The BioSentinel mission is funded by the Advanced Exploration Systems program within the Human Exploration and Operations Mission Directorate at NASA headquarters in Washington.

Partner organizations include NASA Ames Research Center in Mountain View, Calif.; NASA Johnson Space Center in Houston; Loma Linda University Medical Center in Loma Linda, Calif.; and the University of Saskatchewan in Saskatoon, Saskatchewan.

For more information contact **DDC** online at *www.ddc-web.com*, or the **Space Dynamics Laboratory at Utah State University** at *www.sdl.usu.edu/solutions/hardware/pearl.*

WEAPONS FUZING

Air Force chooses Kaman to provide programmable fuzes for airborne weapons

U.S. Air Force airborne weapons experts needed special fuzes that enable aircraft pilots to program weapons in flight. They found their solution from the Kaman Corp. Fuzing & Precision Products segment in Orlando, Fla.

Officials of the Air Force Life Cycle Management Center at Eglin Air Force Base, Fla., announced a $52 million order to Kaman on Wednesday for 15,000 FMU-152 A/B Joint Programmable Fuzes (JPF).

The JPF enables air crew to program weapon settings in flight while weapons are mounted to the aircraft, and is for several different weapons, including general-purpose bombs and guided bombs that use JDAM or Paveway kits.

Aircraft that can use the JPF on their weapons include the F-15E jet fighter-bomber, F-16 jet fighter, F-22 fighter, A-10 ground-attack jet, B-1 and B-2 strategic bombers, B-52 bomber, and MQ-9 Reaper attack unmanned aerial vehicle (UAV).

Fuzing provides mechanical, electro-mechanical, and electronic safe/arm products for general-purpose and penetration bombs, missiles, and rockets.

Kaman is the sole source of the Joint Programmable Fuze (FMU-152 A/B) to the Air Force, and been the sole provider of the JPF to the Air Force

since 2002. Kaman also provides the JPF to 26 other nations. Kaman produces the JPF at facilities in Orlando, Fla., and in Middletown, Conn. The has projectile velocity measurement equipment, projectile impact media, high-speed photographic equipment, and lighting for night firing and tests to help in JPF production.

On this order Kaman will do the work in Orlando, Fla., and Middletown, Conn., and should be finished by June 1, 2020. For more information contact **Kaman Fuzing & Precision Products** online at *www.kaman.com/fuzing-precision-products/about-us.*

WIRELESS NETWORKING

Persistent Systems to provide mobile ad-hoc networking (MANET) for unmanned aircraft

Unmanned aircraft designer Insitu in Bingen, Wash., needed mobile ad-hoc networking (MANET) capability for the company's ScanEagle, ScanEagle2, ScanEagle3, Integrator, and RQ-21A Blackjack unmanned aerial vehicles (UAVs). They found their solution from Persistent Systems LLC in New York.

Persistent Systems and Insitu, a Boeing company, have entered into a five-year agreement for Insitu to incorporate Persistent's Wave Relay MANET technology into Insitu UAVs.

Installing Persistent's MANET radios on unmanned aircraft will enable Insitu UAVs to join land-, air-, and sea-based networks to enable warfighters to share voice and data, including imagery, video, and text.

The agreement between Persistent and Insitu enables Insitu to join the Wave Relay Ecosystem, an alliance of companies using Wave Relay MANET radios. This will enable Insitu's UAVs to work seamlessly with all other Wave Relay MANET-enabled products.

"Integrating the Wave Relay MANET into our products gives our systems a critical communication capability, enabling a wholly networked field solution," says Matt Bartow, Insitu's chief technology officer.

Ad-hoc networking enables warfighters operating in the same region to create RF networks on the fly to enable data networking, in areas where no communications infrastructure exists. Each Persistent Systems radio acts simultaneously as a transmitter, receiver, and network node — similar to a cell phone tower.

The Wave Relay MANET adapts quickly and continuously to fluctuations in terrain and other difficult environmental conditions to make the most of connectivity and communications performance.

The Wave Relay MANET's proprietary routing algorithm enables users to incorporate vast numbers of meshed communications devices into the network in which the devices themselves form the communication infrastructure.

Persistent Systems Wave Relay radios each use three antennas instead of one to boost communications range and power, as well as to mitigate the effects of multipath and other interference to keep data communications open and operating at high bandwidth.

For more information contact **Persistent Systems** online at *www.persistentsystems.com*, or **Insitu** at *www.insitu.com.* ←

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

TEST AND MEASUREMENT

Spectrum analyzer for aerospace and defense introduced by Rohde & Schwarz

Rohde & Schwarz in Munich is expanding the company's Spectrum Rider FPH family of handheld spectrum analyzers with three new base models providing frequency ranges from 5 kHz to 6 GHz, 13.6 GHz, and 26.5 GHz for everyday measurement tasks in aerospace and defense, mobile network testing and broadcasting. These test and measurement devices offer a capacitive touchscreen and a unique frequency upgrade concept via keycodes. Since upgrades require neither downtime nor recalibration, users can upgrade their base models. The Spectrum Rider FPH is a tool for verifying signal transmission over 5G, broadcast, radar and satellite communications links. Higher-frequency models enable the rugged Spectrum Rider FPH to perform measurement tasks in the field and lab. Weighing 5.5 pounds, the Spectrum Rider FPH spectrum analyzers have a battery that lasts more than six hours. For more information contact **Rohde & Schwarz** online at *www.rohde-schwarz.com.*

RACKMOUNT COMPUTERS

Rugged computer for vehicles, ships, and aircraft introduced by Chassis Plans

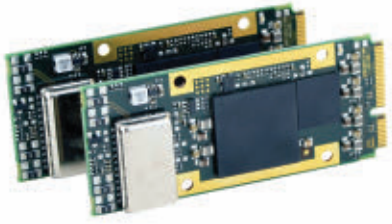
Chassis Plans LLC in San Diego is introducing the HPC M5U-22 rugged high-performance computer (HPC) for a wide range of ground, vehicle, shipboard, and aircraft installations. The HPC M5U-22 is based on a ruggedized 5U enclosure with operating specs that include altitudes to 12,000 feet, temperatures of 0 to 50 degrees Celsius, 5 to 95 percent noncondensing humidity, and resistance to vibration and shock. This system also offers a high-power redundant power supply and RAID options for additional hard drive redundancy. The heart of this computer system is a long-life system board using the Intel Xeon scalable microprocessors. It also provides four 3.5-inch drive bays, a slim-slot fed optical drive, two USB 2.0 ports, as much as one terabyte of RAM, and ability to run Windows 10, Windows 7 Pro, and other 32- and 64-bit operating systems. The

CP SysCool thermal management system extends the life of the computing system, reduces power consumption, and lowers overall system noise levels. The system also can support as many as 4x NVIDIA Tesla graphics processing units in one package. For more information contact **Chassis Plans** online at *www.chassis-plans.com.*

AVIONICS

Rugged Mini PCI Express MIL-STD-1553 avionics modules introduced by Acromag

Acromag in Wixom, Mich., is introducing two rugged AcroPack MIL-STD-1553 communication modules based on the Mini PCI Express card standard — the AP571 and AP572 — for commercial off-the-shelf (COTS) military and commercial avionics applications. These Mini PCI Express mezzanine modules deliver a SWaP-optimized solution for avionics test, simulation, and monitoring



applications. The AP571 provides single-function MIL-STD-1553 communications, while the AP572 provides full multi-function databus communications. Both models provide one dual redundant channel with four open/ground avionics level discrete I/O signals in addition to IRIG-B I/O and Trigger I/O. A high-performance system-on-chip (SoC) architecture has dual-core RISC processors tightly coupled to large programmable logic for host CPU offload and real-time functionality. With 128 megabytes global RAM on-board for data scheduling and buffering, the modules can operate dependably at full bus rates. A variety of carrier cards are available to host a mix of as many as four AcroPack I/O modules on PCI Express, VPX, or XMC embedded computing form factors. For more information contact **Acromag** online at *www.acromag.com.*

TEST AND MEASUREMENT

Oscilloscopes for optical network testing introduced by Keysight

Keysight Technologies Inc. in Santa Rosa, Calif., is introducing the Infiniium UXR-series of oscilloscopes for high-speed serial and optical networking test, measurement, and development. These models range from 13 to 110 GHz of analog bandwidth to enable designers create designs in any generation of DDR, USB, PCI Express, or other serial technologies, as well as PAM4, 5G, radar, satellite communications, and optical designs. These oscilloscopes deliver a low noise floor and high vertical resolution to ensure measurements.

Keysight also announced two additional solutions that, when paired with the company's Infiniium UXR-series oscilloscopes, offer an end-to-end solution from stimulus to analysis for PAM4 and 400G, 600G, as well as terabit coherent optical interconnect designs. These solutions include N4391B Optical Modulation Analyzer (OMA) — a compact, real-time oscilloscope-based OMA designed specifically for complex optical data transmission and terabit measurement challenges; and M8194A 120 gigasamples per second arbitrary waveform generator (AWG) — Keysight's fastest AWG delivers a level of stimulus performance for generating challenging formats such as 64 gigabaud 64QAM (quadrature amplitude modulation) and other wideband modulation schemes. For more information contact **Keysight** online at *www.keysight.com*.

RUGGED COMPUTERS

Small-form-factor rugged computer for signal processing introduced by X-ES

Extreme Engineering Solutions Inc. (X-ES) in Verona, Wis., is introducing the XPand6215 commercial-off-the-shelf (COTS) rugged computer system for a wide range of signal processing applications. Based on the Intel Xeon D-1500 family of processors and the Xilinx Kintex Ultrascale FPGA, the XPand6215 offers several high-speed fiber-optic interfaces on the front panel. With a compact design, the XPand6215 makes the most of processing and networking performance while minimizing size, weight, power, and power consumption (SWaP). It is a small-form-factor (SFF) system with one 3U VPX Intel Xeon D single-board computer hosting a 10 Gigabit Ethernet Switched Mezzanine Card (XMC) networking module and one 3U VPX Xilinx Kintex Ultrascale field-programmable gate array (FPGA) module with FireFly connectors. In the first slot, the XPedite7670 single-board computer has an Intel Xeon D-1500 processor that has as many as 16 Xeon-class cores in one, power-efficient system-on-chip. The XPedite7670 hosts an XPort3305 10 Gigabit Ethernet XMC module, which provides a 10GBASE-SR Ethernet port through a fiber-optic connector on the XPand6215 front panel. The system includes an integrated 28-volt DC power supply and MIL-STD-461 EMI filtering. For more information contact **X-ES** online at *www.xes-inc.com*.

PRODUCT & LITERATURE SHOWCASE

RF AND MICROWAVE

RF coaxial probes for RF and microwave test and measurement introduced by Pasternack

Pasternack Enterprises in Irvine, Calif., is introducing an extended line of RF coaxial probes that reach into the 40 GHz operating frequency range for use in RF and microwave components, high-speed communications, and networking.

The RF coaxial probes are for signal integrity test and measurement, chip evaluation, coplanar waveguide, Gigabit SERDES, substrate characterization, and test fixture applications. The probes include four models that deliver 10 dB maximum return loss over a frequency range of DC to 40 GHz. These probes come in GS and GSG configurations with a pitch of 800 or 1500 microns and a 2.92-millimeter interface. They are gold-plated and have compliant pogo pin contacts that allow for a wide range of probing angles. These RF coaxial probes can be used by hand, with or without a probe positioner, and can be cable mounted or mounted with Pasternack's multi-axis probe positioner. For more information contact **Pasternack** online at *www.pasternack.com.*

ADVERTISERS INDEX

Military & Aerospace Electronics

SUBSCRIPTION INQUIRIES
Phone: 1-800-869-6882 / International Callers: +1 512-982-4277
E-mail: MAEM@kmpsgroup.com
Web: www.mae-subscribe.com

GROUP PUBLISHER Alan Bergstein
603 891-9447 / alanb@pennwell.com

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

ASSOCIATE EDITOR Jamie Whitney
603 891-9135 / jamiew@pennwell.com

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

ART DIRECTOR Meg Fuschetti

PRODUCTION MANAGER Sheila Ward

SENIOR ILLUSTRATOR Chris Hipp

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

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

MARKETING MANAGER Adrienne Adler
603 891-9420 / aadler@pennwell.com

PennWell
www.pennwell.com

EDITORIAL OFFICES
PennWell Corporation,
Military & Aerospace Electronics
61 Spit Brook Road, Suite 501, Nashua, NH 03060
603 891-0123 / 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
Kaci Wheeler
918 832-9377 / kaciw@pennwell.com

CORPORATE OFFICERS
PRESIDENT AND CHIEF EXECUTIVE OFFICER Mark C. Wilmoth
EXECUTIVE VICE PRESIDENT, CORPORATE DEVELOPMENT AND STRATEGY Jayne A. Gilsinger
CHIEF OPERATIONS OFFICER, PENNWELL MEDIA Robert Brighouse

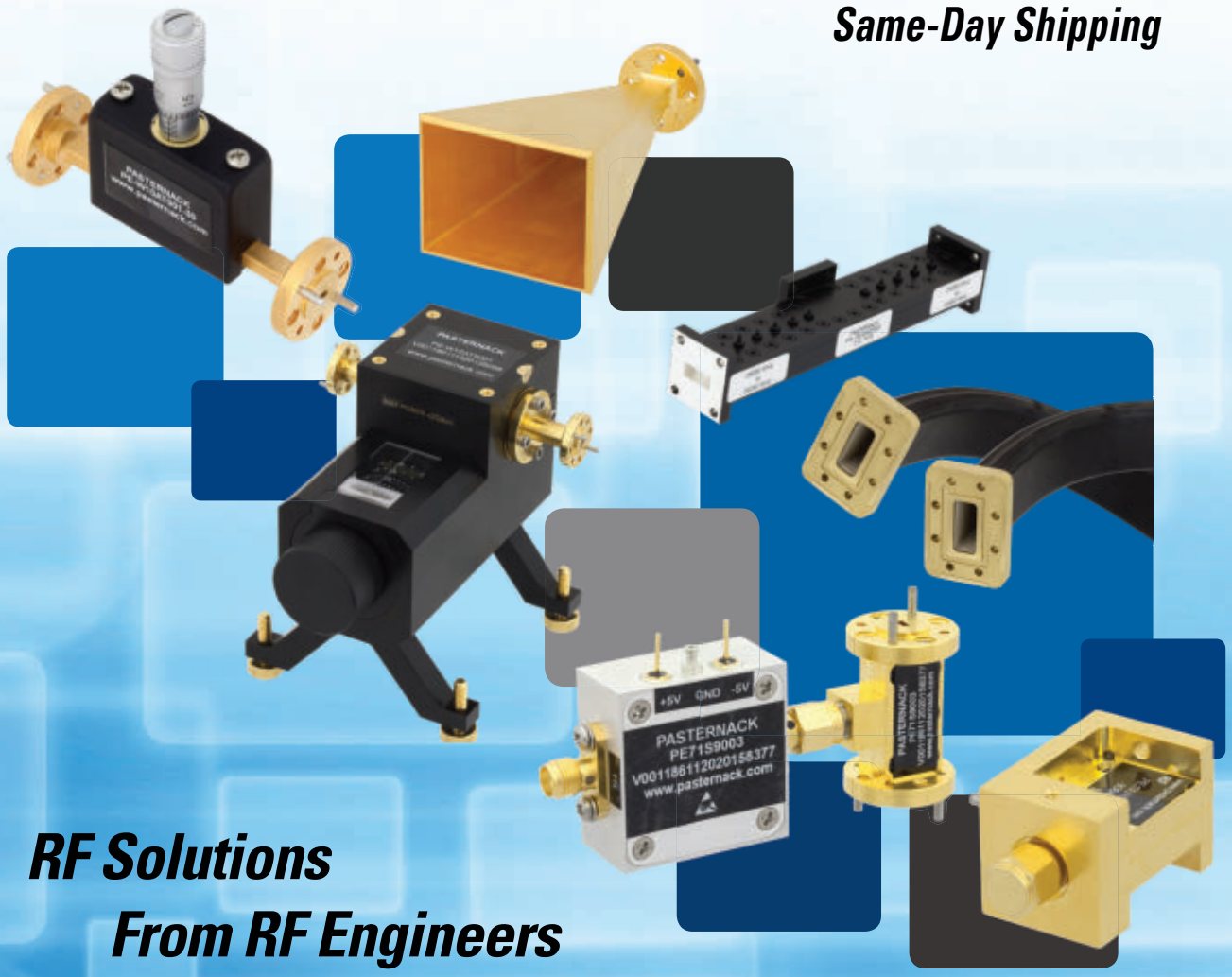
TECHNOLOGY GROUP
SENIOR VICE PRESIDENT/PUBLISHING DIRECTOR & CMO June Griffin

BPA WORLDWIDE Connectiv

Largest In-Stock Selection of

Waveguide Components

All Available for Same-Day Shipping



RF Solutions From RF Engineers

Pasternack's RF Engineering team has assembled the largest selection of in-stock and ready to ship waveguide components covering RF, microwave and millimeter-wave bands up to 110 GHz. With 20 different waveguide categories and over 500 designs including adapters, power amplifiers, detectors, bandpass filters, PIN diode switches, attenuators, horn antennas and more, Pasternack has the waveguide components you are looking for. Whether it's waveguide products or any of the other 40,000 in-stock components we carry, our Application Engineers stand ready to deliver solutions for all your RF project needs.

866.727.8376
visit pasternack.com today!

PASTERNACK®
THE ENGINEER'S RF SOURCE