

DECEMBER 2020

Military & Aerospace Electronics®

RELEVANT. TRUSTED.
ENABLING TECHNOLOGIES.

30 years of Military & Aerospace Electronics

Massive changes
seen in three decades
of magazine's
publication. **PAGE 2**

Military data storage

Rugged data
storage systems for
aerospace and defense
applications are moving
to new data interfaces
for unparalleled speed
and capacity. **PAGE 22**

militaryaerospace.com

TRUSTED COMPUTING AND CYBER SECURITY

*Military holds the line
against determined
hackers seeking to break
into critical computing
systems. **PAGE 14***



Breakthrough Performance... *Weight No More!*

Wideband RF Signal Recorders | Rugged ½ ATR | Built for SWaP

Designed for harsh environments and weighing only 18 pounds, the new Talon RTX SFF series captures real-time RF bandwidths of a gigahertz or more. Complete with a removable QuickPac™ drive pack holding terabytes of data, these units offer flexible I/O options and sustained real-time recording rates up to 4 GB/sec!

The RTX SFF series is the latest in our COTS Talon recording systems that deliver the industry's highest levels of performance in the harshest, space-constrained environments. You'll get high dynamic range, exceptional recording speeds and ample storage capacity for extended missions—all in this compact solution.

- **Sealed, rugged, ½ ATR chassis** for MIL-STD 810 and 461
- **Multi-channel recording**, A/Ds from 200 MS/s to 6.4 GS/s
- **Easily removable 61 TB SSD QuickPac** drive pack
- **Ideal for UAVs, military vehicles, aircraft pods** and more
- **Operating temperature** from -40°C to +60°C
- **sFPDP and Ethernet** models available

All this plus FREE lifetime applications support!



Model RTX 2589 with removable QuickPac drive



Download the FREE Development
Tactics & Techniques for SFF
Recorders White Paper

www.pentek.com/go/masff

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

Worldwide Distribution & Support, Copyright © 2019 Pentek, Inc. Pentek, Talon and QuickPac are trademarks of Pentek, Inc. Other trademarks are properties of their respective owners.



2 TRENDS

4 NEWS

9 IN BRIEF

14 SPECIAL REPORT The essentials of trusted computing and cyber security

U.S. military and government information security experts try to hold the line against determined hackers seeking to break into critical computing systems from foreign governments and non-state bad actors.

22 TECHNOLOGY FOCUS Speed and security for military data storage

Rugged data storage systems for aerospace and defense applications are moving to new data interfaces for unparalleled speed and capacity, while trusted computing and information security are driving trends.

26 RF & MICROWAVE

29 UNMANNED VEHICLES

32 ELECTRO-OPTICS WATCH

35 PRODUCT APPLICATIONS

37 NEW PRODUCTS

COVER STORY

FOLLOW US



FACEBOOK.com
/MilitaryAerospaceElectronics



TWITTER
@MilAero



LINKEDIN.com
/showcase/military-&-aerospace-electronics

Military & Aerospace Electronics® (ISSN 1046-9079, print; 2688-366X, digital / USPS 005-901) is published 12 times a year by Endeavor Business Media, LLC, 1233 Janesville Avenue, Fort Atkinson WI 53538. Periodicals postage paid at Fort Atkinson, WI 53538 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 3257, Northbrook, IL 60065-3257. Military & Aerospace Electronics is a registered trademark. © Endeavor Business Media, LLC 2020. All rights reserved. Reproduction in whole or in part without permission is prohibited. We make portions of our subscriber list available to carefully screened companies that offer products and services that may be important for your work. If you do not want to receive those offers and/or information via direct mail, please let us know by contacting us at List Services Military & Aerospace Electronics, 61 Spit Brook Rd., Suite 501, Nashua, NH 03060. Printed in the USA. GST No. 126813153. Publications Mail Agreement no. 875376.

PICO

Transformers & Inductors SURFACE MOUNT (and thru-hole)



AS9100D
CERTIFIED
TUV

Size Does matter!
Low Profile
From .18" Height
1.2 Grams Weight

Reliability:

MIL PRF27/MIL PRF21308
Manufacturing Approved DSCC

Quality:

AS9100C Qualified Facility

US Manufactured
Military and Commercial Aircraft
Supplier for over 50 Years

For all your TRANSFORMER & INDUCTOR requirements

- Audio • Pulse
- DC-DC • MultiPlex
- Power & EMI

See Pico's full Catalog immediately on
our new website
www.picoelectronics.com

800 431-1064

Fax 914-738-8225

E Mail: info@picoelectronics.com

PICO Electronics, Inc.

143 Sparks Ave. Pelham, N.Y. 10803-1837



Delivery - Stock to one week



Thirty years together with Military & Aerospace Electronics.

With this issue, we at Military & Aerospace Electronics finish our 30th year in publication. Our first regular monthly issue was January 1990, and we've come so far as we round-out December 2020. During the past three decades we've seen Global Positioning System (GPS) receivers evolve from an expensive rarity to something embedded in every smart phone.

We've seen development of the first U.S. Navy Arleigh Burke-class destroyer, development and deployment of the first F-22 Raptor jet fighter and F-35 Lightning II joint strike fighter, the first Virginia-class fast-attack submarine, the first Stryker armored combat vehicle ... the list goes on and on.

We've moved from closed-systems proprietary federated electronic architectures in avionics, vetronics, and shipboard electronics systems to industry-standard open-systems electronic designs built for rapid technology insertion and systems upgrades. We've seen military satellite designs evolve from massive things the sizes of school buses to quick-build packages the sizes of shoe boxes.

We've seen many generations of industry-standard embedded computing boards, chassis, and systems, as well as a continuing parade of embedded computing designers and manufacturers. So much has changed. So little is the same.

I started on this magazine in fall 1989, and helped prepare its prototype and first issues. In the publication's lifetime I've missed just 11 issues, during a short stint at Jane's Information Group, before I came back to where I belong. People ask me how long I've been with Military & Aerospace Electronics. I reply — only half-jokingly — longer than any other human being, living or dead.

I try to think about just how long is 30 years. It doesn't really seem so long, until I consider it's the same amount of time between introduction of the British Sopwith Camel single-seat biplane fighter aircraft on the Western Front of World War I and the first supersonic flight of the Bell X-1 piloted by Chuck Yeager. It's less than the time it took for rocket technology to evolve from the German V-2 — the first guided ballistic missile during World War II — to landing the Apollo 11 astronauts on the moon.

With that in mind I try to imagine where military electronics technology will be in another 30 years. I expect that laser weapons will be commonplace on jet fighter aircraft. Hypersonic weapons will be so commonplace by then that we'll hardly remember when missiles were merely supersonic. Artificial intelligence (AI) will be handling the lion's share of sensor processing and exploitation. Human beings and AI computers will work together to

develop future generations of combat aircraft, submarines, surface warships, and combat vehicles.

The leading-edge unmanned aircraft of today will look clunky and awkward compared to the UAVs we'll see routinely over the next three decades. The sophisticated systems-on-chip we see today will seem unbelievable big compared to what we'll see in 30 years. By then most likely we'll see a full networked computer system about the size of a grain of sand.

We'll see advanced tiny computers implanted in warfighters that can be reprogrammed wirelessly in real time. Think of a deployed Special Forces team receiving data for a new mission — complete with orders, plans, images, maps, and communications channels — while en-route.

By then 5G wireless communications will seem hopelessly slow, as humans, unmanned systems, and smart vehicles will team quickly for missions and targeting in plans can be put together in minutes, rather than hours or weeks.

Much of that future I may not be here to see. Still, as I look back over the past 30 years, I marvel at the changes I've seen, and at the new technologies that have been developed. I wish I could predict how the future will unfold. I expect, though, that I'll be as surprised as everyone else. ←

Largest Selection of High Power Amplifiers



Class AB High Power Amplifiers with Available Heatsinks

Pasternack brings you a broad offering of ready-to-ship high power amplifiers covering RF, microwave and mmWave bands:

- Saturated output power up to 200W
- Numerous heatsink options for high reliability
- Feature-rich: Class AB operation, temperature and power monitoring, TTL logic controls
- High efficiency, low distortion
- Latest GaN and GaAs pHEMT semiconductor technology
- Uniquely qualified for military radio, radar and communication systems, and test & measurement

In-Stock and Shipped Same Day

USA & Canada +1 (866) 727-8376
International +1 (949) 261-1920
pasternack.com

PE PASTERNAK®
an INFINIT® brand

Intelligence researchers want smart-radio technology able to detect and characterize suspicious signals and other RF anomalies.

Industry eyes smart radio technology, RF signal processing, to ensure data security

BY John Keller

WASHINGTON — U.S. intelligence experts are asking industry to develop to develop smart radio techniques that automatically detect and characterize suspicious signals and other RF anomalies in complex RF environments.

Officials of the Intelligence Advanced Research Projects Agency (IARPA) contracting office in Washington have released a broad agency announcement (IARPA-BAA-20-03) for the Securing Compartmented Information with Smart Radio Systems (SCISRS) program.

U.S. intelligence and military experts require information and data that is generated, stored, used, transmitted, and received in secure facilities and “in

the wild,” IARPA officials say. Vigilance is necessary concerning the security of this kind of data regardless of where the data are being used.

The U.S. government has made significant investments in infrastructure to provide high confidence in data security in facilities under the control of the data owner, yet in environments where there is potentially much less control, data security becomes more challenging, IARPA officials explain.

One possible indicator of attempted data breach is unexpected RF transmissions. The goal of the SCISRS program is to develop smart radio techniques to detect and characterize these suspicious signals and other RF anom-

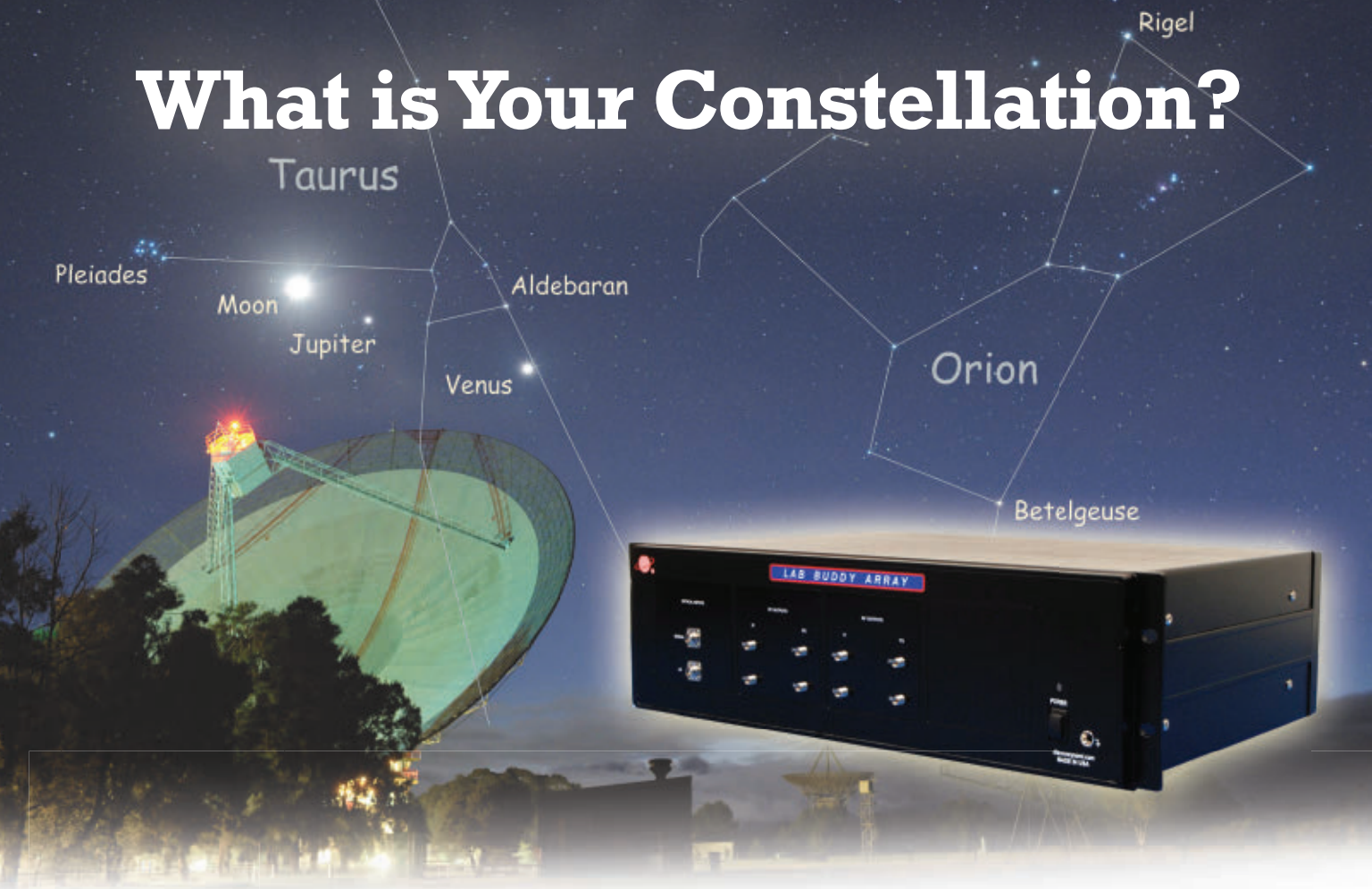
alies automatically in complex RF environments.

These anomalies can be low-probability-of-intercept signals, altered or mimicked signals, abnormal, or unintended emanations. IARPA experts are looking for solutions that are scalable, computationally efficient, and adaptable to a range of radio hardware.

Devising a solution involved RF signal processing won't be easy, IARPA experts warn. RF frequencies of interest may range over several orders of magnitude and the data collection rates may approach terabytes per second — about 1 million times higher than the data rate for high-definition video.

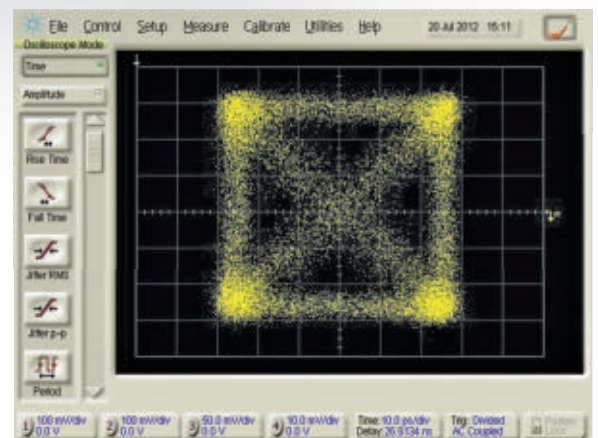
Leveraging technological advances

What is Your Constellation?

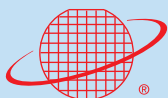


Configurable Coherent Optical Receiver Lab Buddy

- Dual or Quad Linear Balanced Receivers with Optical Hybrid (Single Polarization/Dual Polarization)
- Automatic (AGC) or Manual Gain Control
- User-adjustable RF Bandwidth for Optimum Signal to Noise Ratio (SNR)
- Plug and Play
- Versatile for your Multiple Coherent Applications :
Telcom, Datacom, Spacecom & Avionics Platforms
- Industry Standard Firmware
- Easy to use Graphical User Interface (GUI)
- IoT Compatible



Live 25 Gbaud QPSK Constellation using
Coherent Receiver Lab Buddy



Discovery Semiconductors, Inc.
We Chip the Future®

www.discoverysemi.com

119 Silvia Street, Ewing, NJ 08628 U.S.A.



in software defined radios (SDRs) and computational methods may help solve these problems. Laptop computers and tablet-sized software-defined radios today can handle RF signal processing that used to require a closet full of radio equipment. Wideband A/D converters, meanwhile, can convert a wide

swath of the spectrum efficiently into a large effective number of bits (ENoB) with precise linearity and low noise.

In addition machine learning image recognition algorithms have become so efficient they can match video rates even with modest data processing. Moreover, the increasing ability

of high-performance computing to accommodate the demands of machine learning techniques and digital signal processing may offer the potential to match 5G RF data rates.

The SCISRS program seeks to use off-the-shelf technologies for a wide variety of RF collection hardware that can detect and characterize various kinds of signals in environments cluttered with noise and interference.

Contractors chosen for the SCISRS program must be able to develop detection and characterization systems that work with a different architecture to be specified in each phase of the program.

IARPA will establish two test beds of RF emitters to handle anomalous signals. Contractors will install standardized collection hardware and provide an application programming interface (API) to control the hardware and format raw data for analysis.

Contractors must be able to demonstrate how they command and control the hardware for automatic detection and characterization of ambient signals.

The SCISRS program will have three phases, in which the level of difficulty and variety of anomalies will increase. The first phase focuses on RF baseline characterization and detection and characterization of LPI anomalies. The second phase focuses on altered and mimicked signal anomalies, and the third phase will focus on unintended emissions.

Companies interested were asked to upload proposals by 13 Nov. 2020 to the IARPA Distribution and Evaluation System (IDEAS) online at <https://iarpa-ideas.gov>. ←

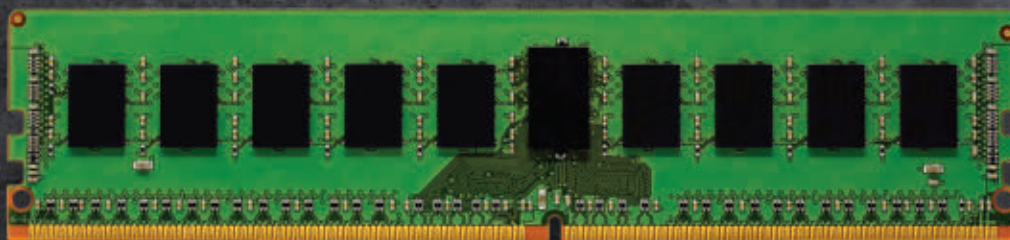


Our customers depend on us to deliver the best quality, highest reliability and lowest risk rugged embedded platforms. Count on us to meet your toughest program demands — be it land, sea or air, we are your trusted embedded computing partner.

Elma Electronic Inc.

elma.com

Email questions or concerns to IARPA at dni-IARPA-BAA-20-03@iarpa.gov. More information is online at <https://beta.sam.gov/opp/f2e9128015684101b2021e04d37516c7/view>.



Up to 85% space savings vs. standard DIMM modules

Rugged: Soldered-down – no DIMM connector

Actual Size
(15mm x 20mm)

POWERFUL & DENSE

A full sized 16GB module packaged into a postage stamp multi-chip package (MCP)

DENSITY
DDR4 MCP, 4GB, 8GB, 16GB

EXTENDED TEMPERATURE
Commercial, Industrial & Military
Temperatures

SPACE SAVING
Up to 85% space savings compared
to standard memory modules

MILITARY/DAS & BEYOND
Shock & Vibration, RAD
Tolerant Options

COMPLIANCES
ITAR & AS9100

CHALLENGING ENVIRONMENTS
Thermal, Electrical, Humidity
Optimized for Extreme Conditions



Scan this code for in-depth product features and specifications or visit
www.vikingtechnology.com/products/memory/parallel-cell-mcp

vikingmemory
TECHNOLOGY

Copyright © 2020 Viking Technology. All Rights Reserved

For sales information, please email us at
sales@vikingtechnology.com, or visit our website for
additional information.



Air Force Researchers want to move enabling technologies for machine autonomy quickly from the laboratory to flight testing.

Air Force focuses on maturing artificial intelligence (AI) and machine learning

BY John Keller

WRIGHT-PATTERSON AFB, Ohio — U.S. Air Force Researchers are ready to kick-off a potential \$98 million project to fast and efficient ways to move enabling technologies for machine autonomy from the laboratory to flight testing.

Officials of the Air Force Research Laboratory at Wright-Patterson Air Force Base, Ohio, have issued a presolicitation (FA8650-21-S-1017) for the Soaring Otter program to speed development and deployment of machine autonomy enabling technologies like artificial intelligence (AI), machine learning, neural networks, neuromorphic computing, and data exploitation.

The Air Force increasingly is employing machine autonomy to solve complex problems related to global persistent awareness, resilient

information sharing, and rapid decision making, researchers say. Enabling technologies include autonomy algorithms, hardware, and software to support autonomy.

Although these new computing solutions bring new capabilities, but they also confront systems designers with challenges like how best to develop applications and integrate them into military applications like target identification and recognition; positioning, navigation and timing (PNT); and unmanned aerial vehicle (UAV) route planning.

The problem revolves around how to integrate and test these new solutions with acceptable costs and risks; there is need for a well-defined progression from lab prototype, through realistic

system integration lab testing, and finally through field and flight testing.

The Soaring Otter project seeks to capitalize on the latest advancements in autonomy and machine learning in six areas: autonomy development and testing; evaluation of autonomy capabilities; computing approaches; new application areas; open-systems architectures for autonomy; and autonomy technology integration and testing.

Autonomy development and testing seeks to solve autonomy problems with machine learning, neural networks, and AI by maturing existing technologies, and determining early what is necessary to switch these autonomy technologies to the warfighter.

Evaluation of autonomy capabilities seeks to provide neutral third-party eval-

uation of algorithms from government, academia, and industry.

Novel computing approaches focuses on compact computing solutions for the warfighter operating on the edge of the battlefield. New application spaces, meanwhile, seek to determine where autonomy can bring the greatest benefit in intelligence, surveillance, and reconnaissance (ISR) applications.

Open-systems architectures for autonomy will be fundamental elements of future autonomous systems. Autonomy technology integration and testing, finally, seeks new ways of integrating new autonomy technologies into larger systems for laboratory, field, and flight testing.

A formal solicitation for the Soaring Otter program is expected in January 2021. The program should last for five years, and will be conducted at the top-secret level.

Email technical questions to the Air Force's Kelly Miller at kelly.miller.9@us.af.mil, or contracting questions to Jennifer Skalski at jennifer.skalski@us.af.mil. ←

More information is online at <https://beta.sam.gov/opp/78550e0901a84d7fa1d4d595570e2913/view>.

Army field-tests augmented reality battlefield goggle for situational awareness

The U.S. Army has finished the first field test of its do-it-all goggle in the ruggedized military version that soldiers could see by next year. Soldiers and Marines ran the Integrated Visual Augmentation System (IVAS) through a company-sized 72-hour training mission at Fort Pickett, Va., at the end of October. IVAS consists of a heads-up display to enable warfighters to experience augmented reality to enhance mobility and situational awareness and will enable soldiers to train in simulated environments with the same equipment they use to fight. The exercise included one of the more difficult dismounted operations — a nighttime trench-clearing exercise. To make that challenging movement more realistic, soldiers weren't limited to the IVAS goggle for targeting, night vision, thermal sights, and navigation capabilities. They also had micro-drones that they

Continued on page 11

Defense, aerospace and government services experience you can rely on when you need it most.

An experienced financial team knows dedication is in the details.

When faced with economic challenges, Regions Commercial Banking aligns dynamic companies with highly responsive, industry-focused, relationship-oriented local teams. We listen first, and then provide efficient solutions tailored to help meet your company's strategic and financial objectives. From risk management solutions to capital-raising services, our team focuses on the details of today while delivering on your vision for tomorrow.

regions.com/defense

Greg Jones
Defense, Aerospace & Government Services Group Head
 704.941.6633 | greg.jones@regions.com




Industry Expertise | Corporate Banking | Capital Markets & Advisory Services | Comprehensive Financing Solutions

Securities activities and Merger and Acquisition advisory services are provided by Regions Securities LLC, 1180 W. Peachtree St. NW, Suite 1400, Atlanta, GA 30309, 404-279-7400. Member FINRA and SIPC.

Banking products and services, including lending, financial risk management, and treasury and payment solutions, are offered by Regions Bank.

Deposit products are offered by Regions Bank, Member FDIC.

 © 2020 Regions Bank. All rights reserved. Regions Securities is a registered service mark of Regions Bank and is used under license for the corporate and investment banking services of subsidiaries of Regions Financial Corporation. Regions, the Regions logo and Regions Securities are registered trademarks of Regions Bank and are used by its affiliates under license. The LifeGreen color is a trademark of Regions Bank.

Rice University eyes nonsurgical brain interfaces for weapons and computer control

BY John Keller

ARLINGTON, Va. — U.S. military researchers are moving forward with a project to develop non-invasive or minimally invasive neural interfaces to connect the brains of warfighters to computers or other digital devices to enable fast, effective, and intuitive hands-free interaction with military systems.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., announced a \$9.8 million order Rice University in Houston for the Next-Generation Nonsurgical Neurotechnology (N3) program.

Rice University was one of six organizations awarded N3 contracts in May 2019 to develop non-surgical wearable interfaces to connect human brains with computers for tasks like control of active cyber defense systems and swarms of unmanned aerial vehicles, or teaming with computer systems to multitask during complex missions.

Rice University has been working on a minutely invasive, bidirectional system for recording from and writing to the brain. An interface records by using diffuse optical tomography to infer neural activity by measuring light scattering in neural tissue. It writes with a magneto-genetic approach to make neurons sensitive to magnetic fields.

This contract asks Rice researchers to continue with their work in developing a high resolution neural interface that does not require surgery.

Neural interfaces could enable warfighters to multitask more efficiently, and interact with autonomous and



U.S. military researchers are asking Rice University to help warfighters control computers and weapons with their brains.

semi-autonomous systems — particularly future systems equipped with artificial intelligence (AI), researchers say.

The original N3 contractors, in addition to Rice University, are Battelle Memorial Institute in Columbus, Ohio; Carnegie Mellon University in Pittsburgh; Johns Hopkins University Applied Physics Laboratory in Laurel, Md.; Palo Alto Research Center (PARC) in Palo Alto, Calif.; and Teledyne Technologies in Thousand Oaks, Calif.

The DARPA N3 project seeks to develop a nonsurgical neural interface system to broaden the applicability of neural interfaces to the able-bodied warfighter.

Until now, neural interfaces that connect human brains to computers and other digital equipment have been surgically invasive and used primarily to help restore functions and skills to injured warfighters. The N3 project, however, seeks to enable neural recording and stimulation with sub-millimeter spatial resolution in healthy warfighters.

The problem with human-machine neural interfaces today is how surgi-

cally invasive they are. State-of-the-art high-resolution single-neuron or neural-ensemble neural interfaces are invasive, and require surgical implantation of metal or silicon-based electrodes into brain tissue or on the surface of the brain.

The burden of surgery and associated risks are too high for this approach on able-bodied individuals. The N3 program aims to overcome these issues by developing a nonsurgical neural interface that is safe for human use, and that has high spatiotemporal resolution and low latency to enable function on par with current microelectrode technology.

DARPA wants the interface to be bidirectional and integrate technology for neural recording (read out) and neural stimulation (write in), and should be agnostic to military systems that would use it.

This neural interface either will be completely external to the body or will include a non surgically delivered nanotransducer that will serve as a signal transducing intermediary between neurons and the external recording and stimulating device.

The major technological challenge of the DARPA N3 project is to interact with neural tissue through the skull while maintaining high spatial and temporal resolution, using either a non-invasive interface or minutely invasive interface, DARPA officials say.

Non-invasive interfaces will involve sensors and stimulators that do not breach the skin. Minutely invasive

approaches, meanwhile, will permit nonsurgical delivery of a nanotransducer delivered to neurons of interest.

Transducers should be small enough so as not to cause tissue damage or impede the natural neuronal circuit, and will be external to the skull. Non-invasive and minutely invasive approaches will be necessary to overcome issues with signal scattering, attenuation, and signal-to-noise ratio.

The N3 program includes a computational and processing unit that must provide decoded neural signals for control in a military application. It must also provide the capability to encode signals from a military application and deliver sensory feedback to the brain.

The N3 program will provide funding at least through 2023 to deliver a nonsurgical neural interface system and is divided into three sequential phases: a one-year base effort, and two 18-month option periods. ◀

On this order Rice University experts will do the work in Houston and Waco, Texas; New York City; New Haven, Conn.; and Durham, N.C., and should be finished by May 2022. For more information contact Rice University online at <https://news.rice.edu>, or DARPA at www.darpa.mil.

Continued from page 9

could launch and view through the goggle, conducting their own short-range reconnaissance of an obstacle before taking on the opposing force.

Future Navy attack submarines to have long-range sonar, fly-by-wire control

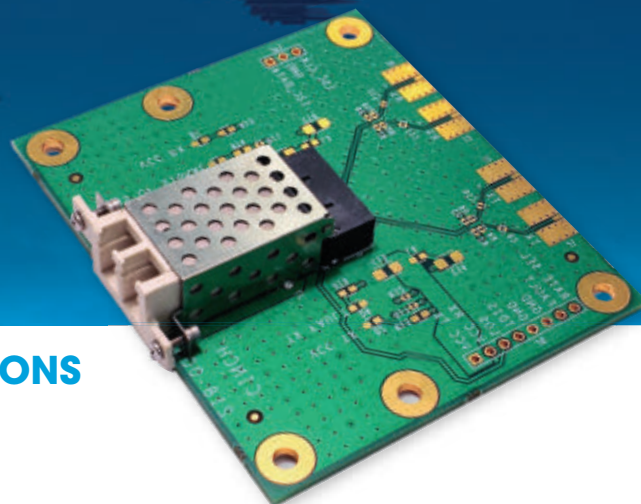
The U.S. Navy's future fast attack submarines will be bigger, faster, more autonomous, networked, and stealthier than the existing Virginia-class attack boats because greater size will allow for more advanced quieting technologies. Set to emerge in the 2030s, a SSN(X) class of attack submarines may be closer in size to the Navy's much larger future Columbia-class ballistic missile submarines. Yet another area of innovation likely to figure prominently in the development of a new generation of attack submarines is fly-by-wire navigational controls such as those built into the Virginia

Continued on page 12



OPTICAL HARSH ENVIRONMENT SOLUTIONS STRATOS FRONT LOADER TRANSCEIVERS

- Rugged Mil/Aero Construction
- Half the size of a standard SFP
- Pluggable connector allows swapping for different data rates, wavelength & fiber type options, without solder removal



belfuse.com/cinch

Draper to develop guidance technologies for submarine-launched hypersonic weapons

BY John Keller

WASHINGTON — U.S. Navy strategic weapons experts are asking the Charles Stark Draper Laboratory in Cambridge, Mass., for guidance systems research for submarine-launched ballistic missiles and hypersonic weapons.

Officials of the U.S. Navy Strategic Systems Programs in Washington have announced a \$133.5 million order to Draper to provide research into enabling technologies for guidance systems for the Common Missile Compartment for future U.S. Columbia-class ballistic missile submarines and United Kingdom Dreadnought-class missile submarines.

Draper also will provide specialized technical knowledge and support for hypersonic guidance, navigation, and control application; and support Navy guidance, navigation and control sys-



Draper will develop guidance technology to help Navy submarines launch future hypersonic weapons.

tems for hypersonic flight experiments.

The U.S. Navy is pursuing a Prompt Global Strike project to develop systems to deliver precision-guided conventional weapons anywhere in the world within one hour of launch — similar to a nuclear intercontinental ballistic missile (ICBM).

Prompt Global Strike hypersonic

munitions are expected to be carried aboard the future Columbia-class ballistic missile submarine, as well as aboard the United Kingdom Dreadnought-class missile submarine, the U.S. Virginia-class fast attack submarine, the U.S. Zumwalt-class land-attack destroyer, as well as from other platforms.

Prompt Global Strike hypersonic weapons could enable the U.S. to respond quickly to emerging enemy threats, either with conventional or nuclear weapons payloads. ←

On this order Draper will do the work in Cambridge, Mass., and in El Segundo, Calif., and should be finished by September 2021. For more information contact Draper online at www.draper.com, or the Navy Strategic Systems Programs office at www.ssp.navy.mil.

Continued from page 11

class Block III boats; instead of using mechanically operated hydraulic controls, the Fly-by-Wire system uses a joystick, digital moving maps and various adaptations of computer automation to navigate the boat. This means that computer systems can control the depth and speed of the submarine, while a human remains in a command and control role. The SSN(X)'s large-aperture bow sonar is passive and active; it can listen while remaining silent, yet can send an active ping, analyze the return signal, and render an enemy object to include its contours, speed and distance.

Descartes Labs to provide sensor fusion for targeting with artificial intelligence (AI)

The U.S. Air Force Research Laboratory has awarded a \$2.2 million contract to Descartes Labs Inc. in Santa Fe, N.M., to generate real-time analytics with a focus on developing moving target indication data. Air Force researchers will gain access to Descartes Labs geospatial analytics technology, which uses artificial intelligence (AI) and computer vision to process and fuse sensor data like satellite imagery for tactical use. Descartes Labs officials say their company's analytics expertise will help

the Air Force generate moving targeting indication data for detecting, pinpointing, and attacking ground and airborne targets. Descartes Labs won this contract through the Air Force Research Lab's Space Technology Advanced Research program, which launched last year to develop enabling technologies for space-based capabilities, including on-orbit servicing, debris management, and ground systems.

Navy awards \$9.4 billion contract to start building next-gen missile submarines

The U.S. Navy has awarded a \$9.4

billion contract for General Dynamics Electric Boat to start work on the first two Columbia-class ballistic missile submarines — work considered so critical to the Pentagon that Congress granted it an exception in the two-month continuing resolution passed in October. Getting the work started is critical because today's Ohio-class ballistic missile submarines are to be replaced in the 2030s, and will begin retiring at the end of this decade. The 12 Columbia subs eventually will carry 70 percent of the nation's nuclear weapons, so any gap between the Ohio retirements and new Columbias could hurt the nuclear triad. Construction is to begin this month and continue on a tight delivery schedule of 2028.

Navy officials have warned for the past year that any schedule slippage would ripple across the entire submarine fleet, so getting the Columbia boats in the water is more important than other shipbuilding programs. Columbia's program manager points out the Navy hasn't designed and built a new class of ballistic missile submarines since the 1970s, but has wrapped up its design efforts with plenty of time to test new technologies on land first.

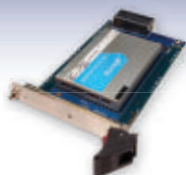
Mercury Systems named to 100 fastest-growing companies list

Mercury Systems Inc. in Andover, Mass., has been named to Fortune magazine's 2020 list of 100 fastest-growing companies. Mercury

specializes in trusted computing, secure mission-critical technologies, high-performance embedded computing, and RF and microwave technologies for a broad range of aerospace and defense programs. The annual Fortune list of 100 fastest-growing companies ranks public companies with market capitalization of \$250 million or more, based on revenue growth rate, EPS growth rate and three-year annualized total return. Mercury designs embedded computing and RF and microwave products. Embedded computing specialist Mercury achieved a ranking of #50 on the list and was the highest-ranked aerospace and defense company. Other companies on the list include Alphabet, Amazon, and Netflix. ◀

RUGGED RELIABLE SECURE DATA STORAGE*

AS 9100D / ISO 9001:2015 CERTIFIED



RPC24 SSD/HDD Magazine Based Disk Array

- 24 SSDs or HDDs in 2U of rack height
- No single point of failure
- MIL-STD-810G and MIL-STD-461E Certified



Open VPX NVMe Express (NVMe) Data Storage Module

- Capacities to 30TB per module
- Transfer rates to 3.5GB/s read, 3.1GB/s write
- Streamlined protocol and very low latency



Phalanx II SFF Network Attached Storage (NAS)

- Two SSDs, fixed or removable, to 32TB
- -40° C to +71° C operational temperature
- MIL-STD-810G, 461F, 704F/1275D

Open VPX Serial ATA (SATA) Data Storage Module

- SLC or MLC Solid State Disk
- 80,000 feet operational altitude
- Vita48 REDI conduction cooled



*** Supports AES-256 and FIPS140-2 encryption**



PHOENIX
INTERNATIONAL

www.phenxint.com 714-283-4800



The essentials of trusted computing and cyber security

U.S. military and government information security experts try to hold the line against determined hackers seeking to break into critical computing systems from foreign governments and non-state bad actors.

BY **Jamie Whitney**

We live in a digital world that depends increasingly on technology and the systems that keeps the digital world connected. It also is incumbent on the military and the intelligence community to keep malicious actors at bay from the homeland's connected infrastructure.

The cyber domain comprises civilian comforts like home appliances, video games, and streaming video services like Netflix and Hulu. However, comforts take a back seat to keeping our connected power grids,

hospitals, logistics, satellite communications, and even our own representative democracy.

Last month, the American people participated in a nationwide general election that was protected from outside actors by the U.S. Cyber Command and National Security Agency (NSA).

"We're looking at the spectrum of all of our adversaries, Russia, China, Iran, and ransomware actors," said Dave Imbordino, the NSA election security lead ahead of the 3 November election during the 2020 DEF CON computer

Photo (above): Personnel with the 175th Cyberspace Operations Group conduct cyber operations at Warfield Air National Guard Base in Middle River, Md.

hacking conference. "There's more people in the game. They're learning from each other. Influence is a cheap game to get into now with social media. It doesn't cost a lot of money. You can try to launder your narratives online through different media outlets. That's something we're laser-focused on as well."

RUGGEDIZED CONNECTIVITY SOLUTIONS KEEP NETWORKS OPERATING – ANYTIME...ANYWHERE.



SAME-DAY
SHIPPING



CUSTOM
CAPABILITIES



GLOBAL
CONNECTIVITY

Available for Same-Day Shipping!



OPERATING IN A HARSH ENVIRONMENT?

Are you operating in a harsh environment where cabling and interconnectivity components must withstand temperature extremes, moisture, corrosive materials, shock and vibration? To address these challenges L-com delivers connectivity solutions to keep your networks operating – ***anytime...anywhere.***

- **Weatherproof and Waterproof**
- **Resilient to Temperature Extremes**
- **EMI and RFI Resistant**
- **Shock, Vibration, Corrosive Materials Protection**

Our ruggedized connectivity solutions are in stock and available for same-day shipping.

Learn more at:
www.L-com.com/ruggedized-solutions
+1 (800) 341-5266

L-comTM
an INFINIT[®] brand



Real-time cyber attacks are displayed on screen at the 275th Cyberspace Squadron's operations floor in Middle River, Md.

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA) in a 12 November statement, the 2020 election was “The most secure in American history,” and that “There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised.”

Beyond the ballot box

Of course, the purview of the military and intelligence cyber security apparatus extends well beyond the protection of homeland infrastructure. The

military and aerospace industry needs to build rugged systems that work in extreme environments that not only enable our warfighters to complete missions, but also to deny intelligence — including proprietary, secret technologies alongside traditional military intelligence — to adversaries.

Because militaries around the world always are looking for an advantage over current and future foes, keeping that edge can make the difference between success and failure. As soon as the first computers were put to use in war rooms and operation centers, there was an interest in adversaries accessing them to control or compromise the technology.

Now, with increasingly connected equipment, malicious actors do not need to be in the same hemisphere — much less the same country — to try and compromise systems or acquire intellectual property and trade secrets.

According to the U.S. Department of Defense (DOD), some of the main actors in malicious cyber activities include China, Russia, Iran, and North Korea.

Of the quartet, China appears to have the most robust ability. The U.S. Department of Justice (DOJ) estimates that more than 90 percent of economic espionage cases involve China, as well as two thirds of trade secret theft.

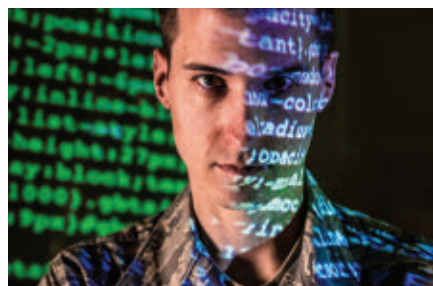
China pledged in 2015 not to use espionage to further its economic interests, but this year the DOJ announced indictments related to China's malicious cyber activity — including allegations of stealing terabytes of data that included COVID-19 research.

There are non-state actors, including terrorist groups that use cyberspace to disseminate propaganda, recruit extremists, and raise funds for operations. More run-of-the mill criminals use ransomware to extort public and private institutions.

A new approach

In the fall of 2018, the DOD announced the new National Cyber Strategy for the first time in 15 years. The strategy, according to the DOD, is founded on four pillars: protecting the American people, the homeland and the American way of life; promoting American prosperity; preserving peace through strength; and advancing American influence.

In its summary of the 2018 National Cyber Strategy, the DOD says “it is now undeniable that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. New threats to commercial and military uses of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks



An Air Force cyber-warfare specialist serving with the 175th Cyberspace Operations Group of the Maryland Air National Guard works at Warfield Air National Guard Base, in Middle River, Md.

against our critical defense, government, and economic infrastructure must be anticipated.”

For example, if an adversary were able to shut down a power grid, life in the homeland would be turned upside down. Hospitals would have to rely on generators to keep ventilators running, medicines at proper temperature, and monitoring equipment running. Water plants would be shut down and potable water from the tap would be compromised. Traffic controls would be taken off line, and cellular phone towers likely would be overwhelmed. In short: chaos.

In addition, if the power generation station were damaged with the attack, that chaos would be extended from hours to days and weeks.

In 2003, a software bug in the alarm system of an energy provider in Ohio caused a power surge and resulted in the loss of power for approximately 45 million people in the northeast United States and southeast Canada. The outage lasted from two hours to four days, depending on the location.

The summary also notes that “investments will prioritize developing resilient, survivable, federated networks and information ecosystems from the tactical level up to strategic planning. Investments will also prioritize capabilities to gain and exploit information, deny competitors those same advantages, and enable us to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks.”

Keeping confidentiality

Embedded computing safety and security experts at Green Hills Software in Santa Barbara, Calif., were awarded Evaluation Assurance Level (EAL) 6+ security level by the NSA in 2008 for the company’s INTEGRITY-178B real-time operating system (RTOS). EAL 6+ is the highest level awarded by the agency.

Richard Jaenicke, director of marketing for Green Hills, says that “The INTEGRITY-178 tuMP RTOS is a security-hardened OS that provides a Multiple Independent Levels of Security (MILS) environment. That MILS environment provides foundational security policies: data isolation between applications; control of information flow between applications; resource sanitization before switching applications; and fault isolation so a failure in one application will not affect any other part of the system. All of those controls are non-bypassable, evaluable, always invoked, and tamperproof (NEAT).”

Jaenicke says that trusted military systems adhere to the “CIA” triad: confidentiality, integrity, and availability.



The PacStar Secure Wireless Command Post enables wireless access to classified networks, using virtualized cyber security software on rugged tactical servers.

“So, if you’re trying to break confidentiality, you’re trying to steal secrets — otherwise known as espionage — or you’re breaking integrity, in which you’d change the data or the behavior in the system and thereby influencing your military decisions and actions,” Jaenicke explains. “Then you attack the availability — denial of service attacks or crashing the computer.

“Even in a real-time system, you’re just delaying it enough that it doesn’t need its real-time deadline causes that actions to happen,” Jaenicke continues. “So I think that’s that those

RUGGEDIZED MULTI-FIBER SOLUTION



Q-MTITAN™ ARINC 846: 12 FIBER OPTICAL CONTACT FOR QUADRAX CAVITY

Radiall provides connectivity solutions for applications requiring high density, high data rates and reliability. The Q-MTitan is qualified in several connectors, such as MIL-DTL-38999, to maintain excellent optical performance even in harsh environments:

- Temperature range: -55 °C to +125 °C
- Durability: 500 mating cycles
- Vibration: 41.7 Grms

<https://www.radiall.com>

Radiall  SIMPLIFICATION
IS OUR INNOVATION



An Air Force cyber transport technician connects fiber optic cables to switches at the network control center on Holloman Air Force Base, N.M.

are the basic ones. And then if you train ones that are a little bit more complex and put a couple of them together, you end up with things ultimately taking over physical control of a system so that you can fire a weapon or crash a vehicle or create some other kinetic effect.”

Information security

In addition to compromising the efficacy of military systems, state and non-state actors also are interested in obtaining useful information. The 2018 National Defense Strategy says

that non-state actors can even be viewed as something relatively “positive” in regard to cyber security.

“There is a positive side to this as well, as our partners in sustaining security also are more than just nation-states: multilateral organizations, non-governmental organizations, corporations, and strategic influencers provide opportunities for collaboration and partnership,” notes the summary. “Terrorism remains a persistent condition driven by ideology and unstable political and economic structures, despite the defeat of ISIS’s physical caliphate.”

Embedded computer expert Steve Edwards, director of product management at the Curtiss-Wright Corp. Defense Solutions division in Ashburn, Va., notes that hackers want to compromise, augment, or recreate the system.

“You’re listening in to see what you want to do with information,” Edwards says. “You might be trying to disrupt, or you might be trying to just learn about the system so that you recreate it down the road or come up with

countermeasures.”

End goals and uses for hackers depend on what sort of access they have, points out Charlie Kawasaki, chief technical officer for Pacific Star Communications Inc. (PacStar) tactical communications company Portland, Ore. Curtiss-Wright Defense Solutions acquired PacStar in September.

“With encryption, the threats to data at rest, you have to have access [to the system],” Kawasaki says. “It’s a gold mine. Where the threats for ‘data in transit’ come into play, you’re trying to capture information and decrypt it in a situation where it’s flying around with radio waves.”

Breaking in

With connected systems, malicious actors have myriad ways to try and access information or capabilities.

“One is if they can introduce malicious code somehow,” says Curtiss-Wright’s Edwards. “There are insider threats; there’s other ways to introduce malicious code. Maintenance operations would be another way, or network connectivity.”

Curtiss-Wright data storage senior product manager Steve Petric says that by using relatively low-risk, high-reward emails to trick authorized users into passing along their legitimate credentials — known as “phishing” — adversaries can sneak their way past past data security.

“That’s an incredibly successful attack,” Petric says. “The DOD is under those types of threats too. If you’re trying to use a denial-of-use, you can do that over the airwaves.”

Green Hills Software’s Jaenicke says other entry points for would-be spies comes from malware in maintenance computers, or “you can even have malicious code in from the beginning or



The 2020 general election and its security was on the minds of cyber experts at U.S. Cyber Command and the National Security Agency.

malicious hardware because of supply chain attacks.”

Beyond the DOD, phishing and similar attacks can impact businesses and disrupt the supply chain. As the United States defense apparatus embraces commercial solutions to military problems, the DOD recognizes that protecting the private sector is instrumental to maintaining military superiority.

“New commercial technology will change society and, ultimately, the character of war,” DOD experts say in their summary of the 2018 National Defense Strategy document. “The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed. Maintaining the Department’s technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base.”

Objectives and options

The DOD National Defense Strategy lists 11 main objectives. They are:

- Defending the homeland from attack;
- Sustaining Joint Force military advantages, both globally and in key regions;
- Deterring adversaries from aggression against our vital interests;
- Enabling U.S. interagency counterparts to advance U.S. influence and interests;
- Maintaining favorable regional balances of power in the Indo-Pacific, Europe, the Middle East, and the Western Hemisphere;
- Defending allies from military aggression and bolstering partners



Members of the Connecticut National Guard's Joint Cyber Response Team, assist the City of Hartford, Conn., information technology team following a ransomware attack.

- against coercion, and fairly sharing responsibilities for common defense;
- Dissuading, preventing, or deterring state adversaries and non-state actors from acquiring, proliferating, or using weapons of mass destruction;
- Preventing terrorists from directing or supporting external operations against the United States homeland and our citizens, allies, and partners overseas;
- Ensuring common domains remain open and free;
- Continuously delivering performance with affordability and speed as we change
- Departmental mindset, culture, and management systems; and
- Establishing an unmatched twenty-first century National Security Innovation Base that effectively supports Department operations and sustains security and solvency.

Cyber security is instrumental in achieving all of those goals. So how does the mil-aero industry help protect the cyber domain? Robust software, isolating sectors, and deterrence.



The Curtiss-Wright Data Transport TS1 is one of the embedded industry's first commercial off-the-shelf (COTS) data-at-rest network attached storage solution that supports two layers of full disk encryption in one device.



An Air Force cyber expert helps monitor malicious network activity during exercise Tacet Venari at Ramstein Air Base, Germany.

Alion Science and Technology Corp. in McLean, Va., provides solutions to U.S. defense, civilian, and intelligence agencies. The company's senior vice president and general manager of its cyber network solutions group, Katie Selbe, notes that speed is paramount to stopping malicious actors.

"Engagements in cyberspace take place at machine speed," Selbe says. "There are too many attacks for humans to detect and react to in a timely manner. Therefore, countering machine speed attacks requires use of software analytics that differentiate between normal traffic and attacks in fractions

of a second. Alion is a leader in creating software analytics, large data environments (BDP) to deploy these analytics, and complex applications to make sense of this data. Alion also provides the experienced researchers to conduct forensics on adversary software, attack vectors and who create counters to this rapidly evolving threat."

System segments

Green Hill's Jaenicke explains that because of the speed afforded to digital attacks, isolating system segments is key to stopping the spread of malicious code or preventing further damage or loss of data.

"If you have a sufficiently motivated, talented, and well-funded group of attackers, they're probably going to find a way in. You need to isolate them and restrict the effects of it," Jaenicke says. "The key is to make sure that they don't get very far and that you isolate them and restrict the effects of it. There are broader parts of the solution where you'd like to know that this happened so that you can shut that down, repair

any damage, assess any losses. But the way our software will provide the isolation and limit the damage, even if you didn't ever notice that the attack."

With Green Hills Software's INTEGRITY-178 real-time software, Jaenicke says that the operating system provides a MILS environment.

"That means if a cyber-attack manages to corrupt an application, such as one connected to external communication, that application cannot corrupt any other application or access its data," Jaenicke explains. "Because every application is isolated from the rest of the system except for predefined communications patterns, every application executes in a "zero trust" environment. The level of trust in INTEGRITY-178 that comes from the breadth and depth of that certification enables INTEGRITY-178 to host multi-level security (MLS) applications such as cross-domain solutions (CDS)."

If and when a hacker gets into a secured system, another countermeasure is to ensure all of the data is encrypted.

"What we have realized is there's a growing need and market in this space for secured encryption — certifiable inscription solutions," informs Curtiss-Wright's Petric. "A lot of our customers are debating which way to go. We see ourselves at data at rest, we push ourselves to be the best in that market place."

"From the processing board space — encryption is a big deal, especially encrypting of the application," says Curtiss-Wright's Edwards. "I would add to that making sure your card boots into a known good state — that might mean running only signed software."

PacStar's Kawasaki says that "If you can't trust your computer, all bets are off. But where PacStar comes in is, we



The Curtiss-Wright Unattended Network Storage (UNS) system is for deployed vehicles requiring Type 1 encryption, high throughput, and massive storage.

assume that we can trust the computer because we use suppliers and hardware [that are trustworthy]. So, once you have that trust in the underlying hardware, then what you need to do is you need to deploy a wide variety of security technologies in order to make sure that the computer can accomplish its goals without the application layer or the security layer software ... So what we what we do in PacStar is we take this trustworthy hardware and we work with the industry-leading cybersecurity companies to validate that their software meets government requirements to integrate it into complete solutions. And then we make it available in military ready, tactical ready environments where now you can deploy the best of enterprise class cybersecurity technologies, entrusted hardware configured and validated to security duty requirements.”

Curtiss-Wright Defense Solutions its Data Transport System (DTS1) network-attached data storage device for harsh-environment applications like high-altitude unmanned aerial vehicles (UAVs) that must operate at altitudes as high as 40,000 feet.

The DTS1 is a commercial off-the-shelf (COTS) data-at-rest storage solution that supports two layers of full disk encryption in one device.

The data storage system has been tested and validated for operation in extended temperatures from -45 to 85 degrees Celsius per MIL-STD-810G. It is a Common Criteria-certified solution endorsed by the U.S. National Security Agency NSA and approved by NATO with two certified encryption layers.

The DTS1 has two layers of AES 256-bit encryption, making protection of Top-Secret data more cost effective and low risk than traditional NSA Type 1 device development.

WHO'S WHO IN CYBER SECURITY AND TRUSTED COMPUTING

Abaco Systems
Huntsville, Ala.
www.abaco.com

Alion Science and Technology Corp.
McLean, Va.
www.alionscience.com/

Carbon Black
Waltham, Mass.
www.carbonblack.com

CrowdStrike Holdings, Inc.
Sunnyvale, Calif.
<https://www.crowdstrike.com>

Curtiss-Wright Defense Solutions
Ashburn, Va.
<https://www.curtisswrightds.com>

Cybereason
Boston
www.cybereason.com

Cybersecurity and Infrastructure Security Agency (CISA)
Arlington, Va.
www.cisa.gov

Duo Security Inc.
Ann Arbor, Mich.
<https://duo.com>

Gray Analytics
Huntsville, Ala.
www.grayanalytics.com

Green Hills Software
Santa Barbara, Calif.
<https://www.ghs.com/>

KnowBe4 Inc.
Clearwater, Fla.
www.knowbe4.com

LogRhythm Inc.
Boulder, Colo.
www.ndm.net/logrhythm

Lookout
San Francisco
www.lookout.com

Mercury Systems
Andover, Mass.
www.mrcy.com

PacStar
Portland, Ore.
<https://pacstar.com/>

Ping Identity Corp.
Denver
www.pingidentity.com

Symantec
Cambridge, Mass.
www.symantec.com

United States Cyber Command
Fort Meade, Md.
www.cybercom.mil

Webroot Inc.
Broomfield, Colo.
www.webroot.com

PacStar offers its scalable Secure Wireless Command Post to provide, as the name suggests, secure access to Wi-Fi on forward bases.

“So, you can use if you use a laptop, you can use a mobile device, you fire it up, you connect to Wi-Fi, you turn on the client and voila, you have access to classified networks,” says PacStar’s Kawasaki. “It allows the organizations to instead of stringing 17,000 feet of cable all over the place in order to get a command post set up, they just drop off our [Secure Wireless Command Post] and five minutes later, you’ve got you’ve got wireless access for all the people in the command post.”

Deterring adversaries

Beyond isolation and encryption, PacStar’s Kawasaki notes that deterrence starts with physical deterrence — keeping bad guys off of the base and out of server rooms or kept from accessing

technology. However, if adversaries get past physical means, robust encryption and isolation, nefarious actors can deter even the most motivated hacker.

“Limiting the effect always has some level of deterrence because then it changes the cost benefit calculation,” says Green Hills’ Jaenicke. “And waging that attack, if you have to put a ton of effort in and you get very little out of it, that’s a form of deterrence. The operating system can play part of that creates a secure environment. A more general solution could be thinking about ... a large network of satellites. It creates a mess if one of the satellites is compromised, [but] it is a lot more different than if you only have one or two big satellites and one of those becomes compromised. You’ve lost a lot of capability. So, the having the having more resilience in your systems means that you’ll have a smaller effect. And therefore, it creates some deterrence.” ◀

Speed and security for military data storage

Rugged data storage systems for aerospace and defense applications are moving to new data interfaces for unparalleled speed and capacity, while trusted computing and information security are driving trends.

BY John Keller

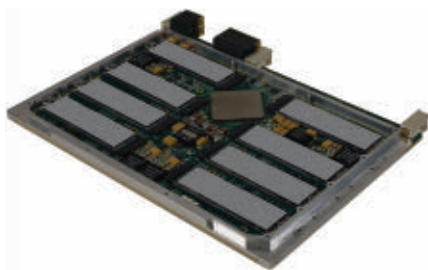
Demands on rugged data storage for aerospace and defense applications never have been higher, driven by the proliferation of sensors, tactical cloud computing, high-speed networking, and the need for real-time actionable intelligence.

In response, the embedded-computing and data-storage industries are responding with a wide variety of open-systems architectures, trusted computing and cyber security for data at rest and for data in motion, every-increasing capacities and speeds of data storage, power and thermal management, packaging for low size, weight, power consumption, and cost (SWaP), and cutting-edge data storage interfaces to optimize today's military embedded computing systems.

Storage capacity and speed

"Among the trends we are seeing is the increased number of sensors going inside of unmanned vehicles and manned planes driving faster data throughput and higher capacities," says Steve Petric, senior product manager of data solutions at the Curtiss-Wright Corp. Defense Solutions division in Dayton, Ohio. "This is driven by the need for more sensors, collecting more data, and increasing data-storage capacities in the same amount space — or even smaller."

One technological innovation that helps increase read and write speeds to



Curtiss-Wright is releasing the 6U VPX Storage Blade Air Cooled module that based on PCI Express NVMe technology, is aligned with the CMOSS and SOSA open-systems standards, and comes in capacities from 16 to 128 terabytes.

data storage media is Non-Volatile Memory Express, better-known as NVMe. This approach enables data storage media such as solid-state drives to access processors via the PCI Express databus. It also enables host hardware and software to capitalize on levels of parallelism possible in modern solid-state drives.

"We have been seeing NVMe with PCI Express," Petric says. "The type of data is moving from SATA to NVMe, and it's starting to get more adoption and traction in the defense market." SATA — short for Serial AT Attachment — is a computer bus interface that connects host bus adapters to data storage devices like hard disk drives, optical drives, and solid-state drives.

"The need for higher amounts of storage continues to evolve as sensors and cameras become faster and improve in resolution," says Brian Rine-

hart, systems and compliance engineering manager at rugged computer expert Crystal Group Inc. in Hiawatha, Iowa. "We can get more and more data storage in smaller and smaller products."

NVMe can increase data read and write speeds over SATA by four to five times — sometimes even more. As an example, SATA reaches its upper-speed limits at about 600 megabytes per second, while NVMe can sustain read and write performance of more than 3 to 3.5 gigabytes per second.

One principle behind NVMe is switching from serial to parallel data interfaces to increase data throughput. "As access times are shorter, those serial interfaces become saturated," says Crystal's Rinehart. "Then we start running parallel serial interfaces, which is the principle behind NVMe. the pipe just gets larger and larger, and the pipe between processing and storage comes immaterial."

Stuffing higher storage capacities into the same- or smaller-sized devices is a primary market driver, says Aneesh Kothari, vice president of marketing at rugged computing expert Systel Inc. in Sugar Land, Texas.

"From where we sit, the drivers are higher capacities in the same form factors and higher speeds so you can move from typical SATA drives to PCI Express and NVMe," Kothari says. "Designers can use that enhanced speed to move

from Gigabit Ethernet to 25-to-40-Gigabit Ethernet."

Driving these higher data-storage speeds revolve around drastically increasing numbers of sensors that aerospace and defense designers envision. "What's driving this is the idea that all these platforms are being so sensed, and you can collect massive amounts of data every second," Kothari says. You can ingest that data at close to real-time speeds; you have so much data coming in to capture and store, and use hot-swap drives to keep up. More speed and higher capacities may require fewer hot swaps during a mission."

The advantages of NVMe in capacity and speed are obvious, but systems designers also must consider technology and cost tradeoffs as they decide what kinds of data storage systems



The Phalanx II Rugged Network Attached Storage (NAS) file server from Phoenix International has removable solid state disks, is SWaP-optimized for military manned and unmanned aircraft, ocean vessels, and ground vehicles.

they need.

"Last year one of the big buzzes was the NVMe interface, which seemed to be the next big thing, but I have not seen the level of people going to that technology that I had expected," says Amos Deacon III, president of rugged data storage expert Phoenix International in Orange, Calif.

"The implementation of that technology is slower than I expected — a little bit because of the pandemic, but also because the technology is impeded by the existing storage infrastructures like SATA and Serial Attached SCSI (SAS). The capacities of NVMe drives are increasing like crazy; there are 15-to-16-terabyte NVMe drives now, but they are still pricey."

It's not only price that causes some systems designers to shy-away from NVMe; there are thermal-management issues to consider, as well.

"One of the issues with NVMe is they are very power-hungry," Phoenix's Deacon says. "They draw a lot of current, and that is challenging for an embedded computing environment. Because of the heat generated in a lot of applications, they have to throttle-back the system speed. Some systems can't run

The only Type 1 Data@Rest encryptor approved for both manned and unmanned operations.



ProtecD@R® Multi-Platform Encryptor (KG-204)

NOW
NSA
CERTIFIED

The **ProtecD@R® Multi-Platform (KG-204)** provides **NSA Certified** high speed encryption to protect stored data classified Top Secret and below.

MIL-STD ruggedized, the KG-204 includes standard interfaces and is operating system/ host agnostic for easy embedment into manned/unmanned platforms, integration into storage systems or stand alone desktop use.

Hard drives encrypted by ProtecD@R can be transported quickly and easily – expediting time from data collection to analysis.

How much risk are you willing to take?





The RPC24 rugged high-performance Fibre/SAS/iSCSI Host Channel, SAS Solid State/Hard Disk Drive RAID Storage Array from Phoenix International has a rugged, cable-less, passive midplane-based high-density 2U chassis for data storage capacity.

at PCI Gen 3 speeds; they have to go to Gen 2 because we can't get the system cool enough."

One customer of Phoenix decided the heat issues of NVMe were too challenging, and instead decided to go with SATA, despite its noticeably slower read-and-write speeds, Deacon says. "We had to find alternatives, and our customer stuck with SATA because we know it works."

Overall, however, Deacon says the future is still bright for NVMe. "In the future that's where we're going; we already are seeing low-power NVMe devices, and I think NVMe will overcome the temperature issues. It's started to happen now."

Future availability of thermally and power-efficient NVMe data storage systems couldn't come quickly enough for some designers. "The tradeoff is in your thermals," says Systel's Kothari. "The faster you go, and the more capacity you have, the hotter the system runs. You can have the fastest, fattest drives possible, but if it overheats, it really doesn't do you any good. If that heat is not accounted for, the heat can become a single point of failure."

Encryption and security

Encryption for data storage comes

in several different levels of security, spelled-out in standards from international authorities; the U.S. Department of Defense's National Security Agency (NSA) at Fort Mead, Md.; and the U.S. Department of Commerce National Institute of Standards and Technology (NIST) in Gaithersburg, Md.

Perhaps the most accessible commercial encryption standards are the Security Requirements for Cryptographic Modules standard, outlined in Federal Information Processing Standard (FIPS) 140-2; and the Advanced Encryption Standards (AES), outlined in FIPS 197. These commercial-level encryption standards are administered by NIST.

FIPS 140-2 is a U.S. government computer security standard to coordinate the requirements and standards for approving cryptographic modules that maintain the confidentiality and integrity of encrypted information.

The AES, meanwhile, specifies a FIPS-approved cryptographic algorithm that is a symmetric block cipher that can encrypt and decrypt information. It can use cryptographic keys of 128, 192, and 256 bits (AES 256) to encrypt and decrypt data in blocks of 128 bits.

The Opal Storage Specification from the non-profit Trusted Computing Group (TCG) in Beaverton, Ore., is a set of security specifications to apply hardware-based encryption to storage

devices. Storage devices that comply with TCG Opal can provide enhanced performance, security, and management, compared with software-based encryption. All security functions happen within the device itself.

Another encryption approach is the Common Criteria for Information Technology Security Evaluation, administered by the NSA's National Information Assurance Partnership (NIAP). Common Criteria is a technically demanding international set of guidelines for security certification recognized by the U.S. and 27 other governments worldwide for protecting sensitive stored data. It provides assurance that the process of specification, implementation, and evaluation happens in a rigorous, standard, and repeatable manner.

Common Criteria certification also is one of the first steps toward implementing the NSA's Commercial Solutions for Classified (CSfC) two-layer encryption for protecting classified information in aerospace and defense applications.

CSfC is intended to be a cost-effective way to use layered commercial encryption technologies in trusted data storage. The NSA has established the CSfC program as an alternative to the agency's more-stringent and more expensive Type 1 encryption.

NSA officials developed the CSfC program to deliver secure solutions using commercial encryption to get trusted data solutions to industry quickly. It works on the assumption that properly configured, layered solutions can provide adequate protection of classified data.

The most demanding encryption available for trusted data storage is NSA Type 1, which is an encryption device or system certified by the NSA for use in securing classified military or other



The VP1-250-eSSD 3U Open VPX NVMe solid-state disk data storage module from Phoenix International can hold as much as 3.2 terabytes of data.

government information. It's expensive and time-consuming to implement, and Type 1-certified encryptors are available only from a handful of certified providers.

Secure data storage needs more than just encryption to safeguard information properly. Security experts particularly are interested in denying an adversary physical access to data drives if systems fall into the wrong hands.

Anti-tamper technology is intended to prevent not only unauthorized access to stored data, but also to keep an adversary from reverse-engineering data drives or storage systems.

Demand for security

It used to be that data encryption and trusted computing capability in data storage was a nice-to-have option instead of a necessity. Today that's no longer the case. "Security and encryption are part of every conversation we are having," says Curtiss-Wright's Petric. "People ask if we have NSA Type 1, CSfC, or something else."

Curtiss-Wright offers the Unattended Network Storage (UNS) system — a rugged network-attached storage (NAS) device — that works with the KG 204 NSA Type 1 encryptor from General Dynamics Mission Systems in Fairfax,



The ADSR-4003 data storage system from Curtiss-Wright Defense Solutions supports DARv3 and IRIG-104 Chapter 10, two widely used flight test recording formats.

WHO'S WHO IN RUGGED DATA STORAGE

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

Barracuda Networks
Campbell, Calif.
www.barracudanetworks.com

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

CP Technologies LLC
San Diego
<https://cp-techusa.com>

CRU Data Security Group LLC
Vancouver, Wash.
www.cru-inc.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 America Inc.
San Diego
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

Systel Inc.
Sugar Land, Texas
<http://www.systelinc.com>

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

Virtium LLC
Rancho Santa Margarita, Calif.
www.virtium.com

ZMicro
San Diego
<https://zmicro.com>

Va. "Type 1 is much more expensive, and the general contention is the up-front costs of a Type 1 are much more than a CSfC solutions. Overall, the cost at the end is CSfC is cheaper."

In addition to encryption, user authentication, key management, and the ability to destroy data quickly also are driving concerns in military data storage, says Crystal Group's Rinehart.

Key management describes a piece of information used together with an algorithm to transform plain text into encrypted text to encrypt and decrypt data. "Registering those keys is important," Rinehart says. "You need to rotate the keys so they don't become stagnant, and revoke those keys when they become obsolete or at risk."

Although the U.S. military and prime defense contractors do not always require top-level and expensive data

storage encryption, at least some level of government-approved encryption is becoming the norm. "The number-one thing we see is some level of FIPS certification, in the drives themselves or in the transport of that device," Rinehart says.

Systel's Kothari says he agrees that some level of security is essential in today's aerospace and defense data storage. "We need to be able to store that data securely, whether it is for off-platform missions or during the mission for exploitation," he says. "That includes if you are swapping drives out, taking that data and sending it downstream somewhere, taking the data back to your base. We need to take that data off the platform securely and take it to a place where you can do something with it. You have to ensure the data is not corrupted and is secure." ◀



Air Force wants directional RF communications for tactical airborne networking

BY John Keller

ROME, N.Y. — U.S. Air Force researchers are asking industry for enabling technologies that involve next-generation, highly directional, networked aerial layer communications for tactical airborne networking.

Officials of the Air Force Research Laboratory Information Directorate in Rome, N.Y., are re-issuing a broad agency announcement (FA875020S7003) for the Next-Generation Airborne Directional Networking program.

Directional networking focuses a substantial amount of radiated energy on an intended receiver to resist interference and increase link capacity. It also reduces stray energy radiated in

directions other than the intended receiver to reduce interference and reduce the possibility of enemy intercept or eavesdropping.

Some experts confuse directional airborne tactical networking with land-based mobile ad-hoc networks (MANETs), yet these two communications modes are dramatically different.

Compared with MANET technology, airborne tactical networking involves entirely vehicle-based systems. This removes power consumption and equipment constraints otherwise imposed by battery-operated handheld devices like MANETs use.

Although less severe than handheld

Photo (above): The Air Force wants industry to develop secure directional wireless networking for high-performance military aircraft.

operation, airborne platforms still present size, weight, power consumption, and cost (SWAP-C) challenges as well as entirely different vibration and environmental requirements.

The different loss characteristics of airborne tactical networking enable greater range than MANETs, and enable any participant in the network to be directly. This increases the likelihood of challenges from interference. Different altitudes and environmental con-

ditions effect propagation of signals.

Jet fighters and other high-performance aircraft also move much faster than land vehicles, which also may require the ability to compensate for Doppler effects, propagation times, and synchronization. Jets also may need apertures and RF electronics able to switch and point rapidly.

Other issues of airborne networking include topology management and scheduling; network discovery while maintaining a low probability of detection; ad-hoc network join/leave; directional routing and media access control; survivable airborne communication technologies; modular and open-architecture systems; intelligent information services; flexible directional apertures; and multifunction RF systems.

From industry, Air Force researchers want white papers for research, development, integration, test, evaluation, and delivery of technologies for next-generation, highly-directional, networked aerial layer communications.

Those submitting good white papers may be invited to submit formal proposals. Researchers will accept white papers until 29 Sept. 2023, although companies have a better chance of acceptance if they submit white papers earlier.

Companies may submit white papers for first consideration by 4 July 2021, and by 3 July 2022. This solicitation originally was issued in November 2019. Companies interested should email white papers to the Air Force's Richard Butler at richard.butler.10@us.af.mil. ←

Email business or contractual questions to Amber Buckley at Amber.Buckley@us.af.mil. More information is online at <https://beta.sam.gov/opp/08a732e7306c438bb1a90f2565a2f406/view>.

Pentagon outlines new electromagnetic spectrum strategy

The U.S. Department of Defense (DOD) has announced release of the DOD Electromagnetic Spectrum Superiority Strategy. The strategy results from the need for freedom of action in the electromagnetic spectrum, at the time, place, and parameters of DOD's choosing. The modern electromagnetic operational environment is increasingly complex and is congested, contested, and constrained. It incorporates an electromagnetic enterprise focus on superiority in congested and contested space as well as the need to test, train, and operate in congested and constrained peacetime environments.

U.S. Army shows ability to control electronic warfare (EW) sensors remotely

The U.S. Army has demonstrated the ability to control electronic warfare (EW) sensors remotely through an over-the-air data link and feed the information back to a central battle-management tool. Previously, sensors connected to the Electronic Warfare Planning and Management Tool (EWPMT) through a wired link. This tool is a command-and-control planner that enables users to visualize the potential effects of EW in the field and chart courses of action to maintain effective jamming.

Wilkinson power divider for RF beam shaping introduced by Broadwave

BroadWave Technologies Inc. in Greenwood, Ind., is introducing the model 152-085-004 Wilkinson power divider for beam shaping anten-

nas, antenna systems, radar systems, and test and measurement applications. The model 152-085-004 has a five-Watt average power rating, and is a 50-Ohm four-way power divider with an 800-to-2700 MHz frequency range. This unit for antenna systems features 25-decibel typical isolation, 1.50:1 maximum voltage standing wave ratio (VSWR) and 1.2-decibel maximum insertion loss above theoretical loss. Available connector types are BNC, F, N, SMA and TNC or mixed connector types for unique applications. For more information contact BroadWave Technologies online at www.broadwavetechnologies.com.

Oscilloscopes with high-speed display technology introduced by Saelig

Electronics distributor Saelig Company Inc. in Fairport, N.Y., is introducing the Teledyne LeCroy T3DSO2000A oscilloscopes in two-channel and four-channel versions with analog bandwidths from 100 to 500 MHz. Each model offers a maximum sample rate of 2 gigasamples per second and a maximum memory depth of 200 Mpts in half-channel mode. The T3DSO2000A series uses high-speed display technology for signal clarity, fidelity, and performance. The system noise floor also is lower than similar products in the industry. This scope series provides a minimum vertical input range of 1mV/div, a digital trigger with high sensitivity and low jitter, and a waveform capture rate of 500,000 wfms/sec in sequence mode. For more information contact Saelig online at www.saelig.com. ←



Raytheon to provide 16 new AN/APG-79(V)4 radar systems for F/A-18C/D combat jets

BY John Keller

PATUXENT RIVER NAS, Md. — Radar experts at Raytheon Technologies Corp. will provide the U.S. Marine Corps with 16 AN/APG-79(V)4 active electronically scanned array (AESA) airborne radar systems under terms of a \$53.4 million contract.

Officials of the U.S. Naval Air Systems Command at Patuxent River Naval Air Station, Md., are asking the Raytheon Intelligence & Space segment in El Segundo, Calif., for replacement AESA radar systems for the Marine Corps F/A-18C/D Hornet carrier-based jet fighter-bomber.

The AN/APG-79(V)4 is a scaled-down version of the AN/APG-79 AESA radar for the U.S. Navy Boeing F/A-18E/F fighter-bomber and EA-18G Growler carrier-based electronic warfare jet. It provides aircrew situational awareness, near-instantaneous track updates, and multi-target tracking capability.

The order includes software, obsolescence management, engineering support, and technical, financial, and administrative data necessary for retrofit integration into the Marine Corps

F/A-18C/D aircraft.

AN/APG-79(V)4 radar is 90 percent compatible with the larger AN/APG-79 radar, and is designed to fit into the F/A-18C/D combat jet as part of a modernization program. It provides extended detection range, simultaneous air-to-air and air-to-ground mode capabilities, high resolution synthetic aperture radar (SAR) mapping, and high reliability.

The APG-79 radar has an open-systems architecture and rugged commercial-off-the-shelf (R-COTS) parts. Its array has solid-state transmit and receive modules for enhanced reliability, as well as an advanced receiver/exciter, ruggedized R-COTS processor, and power supplies.

The APG-79 AESA radar uses transmit/receive (TR) modules populated with gallium arsenide (GaAs) monolithic microwave integrated circuits (MMICs). Presumably these are some of the electronic modules that Boeing experts will modify with updated electronics to mitigate obsolescence issues.

The radar's active electronic beam scanning helps steer the radar beam

Photo (above): Raytheon will provide replacement AESA radar systems for the Marine Corps F/A-18C/D Hornet carrier-based jet fighter-bomber.

at nearly the speed of light to optimize situational awareness and air-to-air and air-to-surface capability, Raytheon officials say. The agile beam enables the multimode radar to interleave in near-real time, so that pilot and crew can use both modes simultaneously.

The first flight of a C/D Hornet fitted with this AESA radar was in January 2015, and the Marine Corps chose the AN/APG-79(V)4 radar in January 2019 to upgrade its legacy F/A-18C/D aircraft fleet. The radar enables the Hornet jet to fire several missiles at once and guide them to different targets that are widely spaced in azimuth, elevation, or range. ◀

On this order Raytheon will do the work in Forest, Miss.; El Segundo, Calif.; Andover, Mass.; and Dallas, and should be finished by June 2022. For more information contact Raytheon Intelligence & Space online at www.rtx.com, or Naval Air Systems Command at www.navair.navy.mil.



Northrop Grumman will upgrade the flight computers on the Navy E-2D Hawkeye to enable teaming with nearby manned and unmanned aircraft.

Northrop Grumman to enable E-2D aircraft to team with manned and unmanned aircraft

BY John Keller

PATUXENT RIVER NAS, Md. — U.S. Navy researchers are asking Northrop Grumman Corp. for design and software upgrades for the E-2D carrier-based early warning aircraft to enable the E-2D to work together with unmanned aerial vehicles (UAVs) as teams.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., are asking the Northrop Grumman Corp. Aeronautics Systems segment in Melbourne, Fla., for upgrades to the E-2D mission computer and displays software to support a laboratory demonstration involving manned/unmanned teaming (MUM-T) experiments.

MUM-T describes synchronized use of human warfighters, manned and unmanned aircraft, robotics, and sensors to achieve enhanced situational awareness, lethality, and survivability.

MUM-T involves a standardized systems architecture and communications protocol that enables the sharing of live and still images gathered from UAV sensor payloads.

MUM-T enables manned aircraft to connect with UAVs to enhance decision-making and mission effectiveness, and offer new levels of interoperability among ground forces, manned aircraft, and UAVs.

This contract with Northrop Grum-

man will last for six months, and the amount of the upcoming contract has yet to be negotiated.

The Navy Northrop Grumman E-2D is a tactical airborne early warning (AEW) aircraft designed to operate from aircraft carriers. The twin-engine turboprop aircraft has a distinctive antenna, and provides the carrier battle group with wide-area radar surveillance for enemy monitoring and combat air traffic control.

Its large saucer-like radar antenna mounted to the top of the aircraft, as well as other advanced avionics, enables it to detect hostile aircraft and missiles at extremely long ranges and

vector Navy aircraft to intercept.

Northrop Grumman officials call the E-2D reconnaissance aircraft a “digital quarterback” to sweep ahead of Navy aircraft carrier strike groups, manage missions, and keep U.S. network-centric carrier battle groups out of harm’s way. The aircraft provides battle management, theater air and missile defense, and multi-sensor fusion capabilities.

Compared with its E-2C predecessor, the E-2D has a new radar with mechanical and electronic scanning capabilities; glass cockpit; advanced

identification friend or foe (IFF) system; new mission computer and tactical workstations; electronic support measures enhancements; and modernized communications and data link suite, Northrop Grumman officials say.

The plane is nearly 58 feet long, has an 80-foot wingspan, can fly faster than 300 knots, and can fly to altitudes as high as 37,000 feet. It carries a crew of five: two pilots and three mission systems operators. The co-pilot also can act as a fourth mission systems operator.

Navy officials say they hope to pro-

cure 73 of these aircraft by 2022. These plans started going to the fleet in 2015.

Northrop Grumman is the sole designer of the E-2D, and is the only source with the knowledge, experience, and technical expertise to do this project, Navy officials say. Companies interested in subcontracting should email Northrop Grumman’s Vicky Harper-Hall at Vicky.harper-hall@ngc.com. ←

For more information contact Northrop Grumman Aeronautics Systems online at www.northropgrumman.com/who-we-are/business-sectors/aeronautics-systems.

Army eyes tanks, maneuver and unmanned systems for future conflicts

U.S. Army leaders want the first casualties of the next war to be unmanned systems, not a human being, yet no amount of high technology will allow a bloodless victory. Instead of devising some futuristic all-new force, experts are reviving battle-tested Cold War concepts — like battle tanks, infantry teamwork, and robust division-level formations — and updating them with a large dash of unmanned systems. Guerrilla warfare in Afghanistan and Iraq helped the Army beef-up its brigades to operate largely independently, with higher echelons such as divisions and corps in a supporting role. For future large-scale wars, the Army wants to strengthen the division, restoring the brigade-strength artillery and reconnaissance (“divisional cavalry”) elements eliminated in the 2000s. This combination of long-range firepower and scout forces in the air and on ground — will enable division commanders to fight and maneuver over

distances much larger than what their subordinate brigades can cover.

Marine Corps could add ASW logistical support to hold enemy subs at risk

Naval campaign planning for anti-submarine warfare (ASW) must include not only the Navy’s warfare communities, but also that of the U.S. Marine Corps. Nearly two years ago former Marine Corps Commandant Gen. Robert Neller, said, “We’re going to have to fight to get to the fight,” and, “I think we’re going to need more submarines” in a fight against a peer adversary. U.S. ASW capabilities in the air, on the surface, and under the sea rely on a brittle layer of logistical support. As Chinese and Russian undersea warfare capabilities continue to improve, logistics and other supporting operations for U.S. ASW forces will grow in importance. By offering forward logistics and support, as well as sensor and strike capabilities, Marine expeditionary advanced bases could make a significant contribution to undersea warfare campaigns.

Army ground combat center developing tactics and maneuver for the next war

The focus of the U.S. Army is ground combat and the way the Army fights is through fire and maneuver, so it makes sense that the job of figuring out where technological advances, doctrine, and tactics, meet would be at the epicenter of innovations in ground combat — the Maneuver Center of Excellence (MCOE) in Columbus, Ga. The era in which the Army operates today is similar to the 1970s, post-Vietnam, when the Army was coming out of a long counter-insurgency campaign and had combat-experienced leaders in the formation, says Maj. Gen. Patrick Donahoe, commander of MCOE. As early as 2013, Army captains prepared for tactics in counter-insurgency operations at the MCOE, and headed out on deployments just five or six months later. Since then, however, Army leaders have looked at regions like Crimea and areas around China to determine what they’ll need for the next deployment. ←

Amplifier for RF airborne data links in unmanned aircraft introduced by Comtech PST

BY John Keller

Comtech PST Corp. in Melville, N.Y., is introducing the model BME2969-75 solid-state power amplifier module for airborne data links and full-motion video in unmanned aerial vehicles (UAVs), fixed-wing aircraft, and helicopters.

Intended as a replacement in the traveling wave tube (TWT) market, the model BME2969-75 covers the 2000 to 6000 MHz band providing 75 Watts of linear power in a small, lightweight, ruggedized form factor.

This solid-state power amplifier for manned and unmanned aircraft features built-in protection and monitor-

ing circuits, low-voltage prime power input, and high efficiency.

The unit will self-protect under fault conditions and automatically return to normal operation when fault conditions are removed. The solid-state power amplifier module withstands and operates in rugged and hostile environments.

The model BME2969-75 offers programmable power control in 0.1 decibel steps; high power density; dual band operation; forward and reverse power monitoring; open, short, and high voltage standing wave ratio (VSWR) load monitoring and protection; tem-

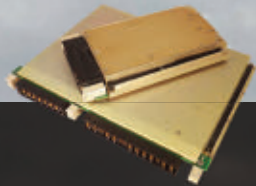
perature and current monitoring and protection; and mean time between failures of more than 20,000 hours.

The solid-state power amplifier for airborne data links offers 100 Watts of power output; RF Power Output of 100 Watts; RF Linear Power of 75 Watts; RF input of -10 to 0 dBm; gain of 59 decibel \pm 3dB; power control of + 1.0 decibel; RF input overdrive of 16 dBm; modulation format of AM, FM, CW, digital, and pulse; and input VSWR of 2.0:1. ◀

For more information contact Comtech PST online at www.comtechpst.com.

SUPERIOR MILITARY-GRADE POWER CONVERSION SOLUTIONS

STANDARD • TAILORED • CUSTOM



AC/DC | DC/DC | DC/AC | HOLDUP UNITS | VPX VITA 62 | GCU | PDU | UPS

With over 40 years experience focused exclusively on military power conversion and countless solutions fielded around the globe, Milpower Source is ready to support your unique specification, delivery and budget challenges. No matter the requirement – form-fit-function replacement, system upgrades or new designs – we've got you covered. Our superior solutions feature:

- Discrete Components (No Bricks!)
- Thermal-first Design
- Compliance with Relevant MIL-STDs
- Operation Through Transients and Surges
- Wide Input and Operating Temperature Ranges
- No Derating Through Full Temperature Range

MILPOWER
SOURCE

Speak directly with one of our design engineers today to identify the best solution for your power conversion requirement:
(603) 267-8865 | sales@milpower.com | www.milpower.com



Near-infrared LED illuminator for surveillance introduced by Opto Diode

BY John Keller

CAMARILLO, Calif. — Opto Diode Corp. in Camarillo, Calif., is introducing the OD-663-850 gallium aluminum arsenide (GaAlAs) near-infrared LED illuminator with ultra-high-power output for surveillance and night-vision applications.

The device has a uniform optical beam with a peak emission wavelength of 850 nanometers.

Other features include total power output from a minimum of 300 milliwatts to a typical output of 425 milliwatts, with typical forward voltage from

4.8 volts to a maximum of 5.4 volts.

The spectral bandwidth is 40 nanometers with a half-intensity beam angle of 120 degrees for surveillance and night-vision uses. Reverse breakdown voltage ranges from a minimum of 5 volts to a typical rating of 30 volts; rise and fall times are 100 nanoseconds, respectively.

Housed in a standard, a two-lead TO-66 electrically-isolated package, the OD-663-850 is for high-power near-infrared illumination tasks. With power

dissipation at 2.2 Watts, the device features a continuous forward current of 400 milliamps, peak forward current of 1 amp, and reverse voltage of 5 volts.

The lead soldering temperature 1/16 of an inch from the case for 10 seconds is 260 degrees Celsius. Storage and operating temperatures range from 40 to 100 C with a maximum junction temperature of 100 C. ←

For more information contact Opto Diode online at <https://optodiode.com>.

DARPA eyes sensors to detect COVID-19 airborne pathogens in seconds or minutes

BY John Keller

ARLINGTON, Va. — U.S. military researchers are asking industry to develop technologies for sensors able to detect low concentrations of airborne viruses in room-size spaces within seconds to minutes to help detect the presence of pathogens like the COVID-19 coronavirus and prevent its spread.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., issued a solicitation on Monday (DARPA-PA-20-01-04) for the SenSARS program.

The COVID-19 coronavirus pan-

demic has highlighted the need for improved environmental sensing of pathogens. Sensing SARS-CoV-2 virus in the air with high sensitivity could provide a new mechanism for public health monitoring to enable safe conditions for work, travel, and school.

The SenSARS project aims to identify SARS-CoV-2 signatures suitable for rapid indoor air monitoring and use these signatures to develop and demonstrate a technology readiness level (TRL) 4 prototype sensor.

Recent developments in radio fre-

quency vibrometry, improvements in terahertz sources and sensors, improvements in mass spectrometric techniques, emerging immunosensing techniques, electrochemical detection methods, and advances in signal analysis using machine learning approaches potentially could help monitor for SARS-CoV-2 airborne pathogens.

These approaches have the potential to enable sample agnostic detection of low viral concentrations within seconds to minutes for real-time aerosol detection. Improvements in portability



**AN ELITE
TEAM...
NEEDS ELITE
EQUIPMENT**



**FOR THE HIGHEST LEVELS OF
IT SECURITY AND FLEXIBILITY,
CHOOSE THE KVM EXPERTS**

Computer system reliability and maximum cyber security are crucial in any military control room. So it's essential you choose a KVM system you can trust completely.

KVM solutions from G&D prove their quality every day in vital operations, constantly building on our worldwide reputation for technical excellence, reliability and safety. They improve working conditions for both personnel and equipment, enabling quicker and better decisions to be made.

Talk to the KVM experts. Talk to G&D.

KVM extenders
switches
matrix systems

**G&D NORTH
AMERICA**

G&D North America Inc.
www.gd-northamerica.com
sales@gd-northamerica.com
Phone +1-818-748-3383



SenSARS seeks to identify SARS-CoV-2 signatures in rapid indoor air monitoring in a technology readiness level (TRL) 4 prototype sensor.

of traditional methods of detection — immunoassays and nucleic acid-based assays — out of the lab setting may enable onsite confirmation of results.

Most SARS-CoV-2 detection systems require collecting a sample and sending it to a lab, which can take hours or days, which is too slow for atmospheric sampling.

On the other hand, current air-breath-

ing environmental sensors using optical techniques offer fast detection times but limited ability to discriminate between benign and pathogenic material, such as the SARS-CoV-2 virus.

In general, current methods are not suitable for room-sized, indoor environmental monitoring and lack practical combinations of sensitivity, precision, acceptable false positive

rates, and speed. Today's methods also scale poorly because of costs and size, weight, and power requirements.

The SenSARS program will have two phases. The nine-month phase one focuses on determining environmental SARS-CoV-2 signature feasibility, and the nine-month phase two option seeks to refine signatures and produce and demonstrate a TRL 4 prototype sensor. Selection for the Phase 2 option depends on Phase 1 results and funding availability.

DARPA researchers are interested in technologies that are extensible to other pathogens beyond SARS-CoV-2; adaptable enough to detect new pathogens within 1 week to a month after discovery; and can save samples for additional analysis. ◀

Companies interested were asked upload proposals by 1 Dec. 2020. Email questions or concerns to SenSARS@darpa.mil. More information is online at <https://beta.sam.gov/opp/a84f1af107334afcbf39d885d8f668a3/view>.

3D image sensor using lasers introduced by Teledyne Imaging

BROMONT, Quebec — Teledyne Imaging, a Teledyne Technologies company in Bromont, Quebec, is introducing the Z-Trak2 3D image sensor for in-line height measurements for inspection, detection, identification, and guidance in electronics, semiconductor, automotive, and factory automation applications.

Z-Trak2 is a 5-Gigabit Ethernet 3D profile sensor that delivers scan speeds as fast as 45,000 profiles per second and features built-in HDR and reflection compensation algorithms to handle surfaces with varying degrees of reflectivity in one scan for precision in semiconductor manufacturing.

The Z-Trak2 family's S-2K and V-2K series fea-

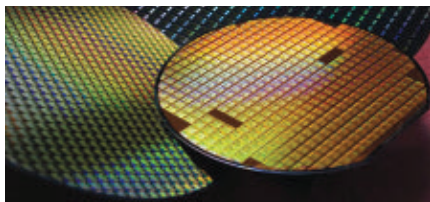


ture scanning speeds of 45,000 profiles per second and 10,000 profiles per second respectively.

Offering 2,000 points per profile, all Z-Trak2 models are factory calibrated and offered with either blue or red eye-safe lasers to suit various surface properties and operating environments.

All sensors are housed in IP67 enclosures for harsh environments and come bundled with Teledyne Imaging's Sherlock 8 — a point-and-click, rapid application development software package. ◀

For more information contact Teledyne Imaging online at www.teledyneimaging.com.



INTEGRATED CIRCUITS

Globalfoundries to provide trusted microelectronics for military applications

Officials of the U.S. Defense Microelectronics Activity (DMEA) in McClellan, Calif., needed a company to provide leading-edge current and legacy microelectronics and trusted processes for the U.S. Department of Defense (DOD) and other federal agencies. They found their solution from Globalfoundries U.S. 2 LLC in Hopewell Junction, N.Y.

DMEA has announced a \$400 million order to Globalfoundries for access to leading-edge current and legacy microelectronics and trusted processes for DOD and other federal agencies.

DMEA officials are turning to Globalfoundries because of an increase in interest for leading-edge microelectronics technology and lifetime orders for end-of-life technology. This contract modification brings to total value of the original Globalfoundries contract to \$1.1 billion.

The DMEA State of the Art Trusted Foundry Services project seeks to give DOD and other government agencies access to a wide range of microelectronics services that will ensure the confidentiality and integrity of specialized devices for military applications.

The globalization of the integrated circuit industry in recent years has made this function difficult, DMEA officials say.

The DOD Trusted Foundry program seeks to ensure that mission-critical national defense systems can obtain classified and unclassified microelectronics components like application-specific integrated circuits (ASICs) from sources like Globalfoundries that can protect the confidentiality and integrity of these devices.

This program involves design, aggregation, mask manufacturing, wafer fabrication, post-processing, packaging and assembly, test, and broker services.

From Globalfoundries, DOD officials require leading-edge and state-of-the-art semiconductor process technologies, including military temperature ranges and radiation hardness requirements.

The DOD needs Globalfoundries to fabricate at least 1,200 8-inch ASIC wafers per year, as well as crucial microprocessors, field-programmable gate arrays (FPGAs), and other microelectronics components.

Globalfoundries maintains a secret facility security clearance for manufacturing or assembly work, and otherwise will protect all trusted designs and devices with a cleared group of employees with personnel security clearances.

Globalfoundries will maintain its expertise in leading-edge and state-of-the-art complementary metal—oxide—semiconductor (CMOS) technologies, as well as in silicon germanium BiCMOS technologies. The company also will develop the ability to produce trusted microprocessors, graphics processors, digital signal processors, analog-to-digital converters, photonics, micro-electro-mechanical systems (MEMS), and other advanced microelectronics.

The company will continue its ability to conduct dedicated prototype runs, production runs, obtain trusted masks, and provide complete ASIC services, including design, fabrication, packaging, and test.

On this contract modification Globalfoundries will do the work in Burlington, Vt.; as well as in East Fishkill and Malta, N.Y., and should be finished in March 2021.

For more information contact Globalfoundries online at www.globalfoundries.com, or the Defense Microelectronics Activity at www.dmea.osd.mil/default.aspx?area=Homepage.

SENSORS

Three U.S. contractors to develop miniature ASIC technology for next-gen GPS receivers

U.S. Air Force navigation and guidance experts are choosing three U.S. defense contractors to develop

and build enabling technologies for M-Code capable handheld and vehicle-mount Global Positioning System (GPS) satellite navigation receivers.

Officials of the Space and Missile Systems Center of the Air Force Space Command at Los Angeles Air Force Base, Calif., have announced contracts collectively worth \$552.6 million for the Military GPS Users Equipment Miniature Serial Interface Increment 2 Application Specific Integrated Circuit (MGUE Inc 2 MSI ASIC) project.

The MGUE increment 2 MSI ASIC project is to be a small-size and -power consumption form factor to include a next-generation application-specific integrated circuit (ASIC) for secure GPS land navigation.

The three contracts are going to the Raytheon Technologies Corp. Intelligence & Space segment in El Segundo, Calif.; the L3Harris Technologies Interstate Electronics segment in Anaheim, Calif.; and the Raytheon Technologies Collins Aerospace segment in Cedar Rapids, Iowa.

The three companies will develop ASICs for the MGUE MSI GPS receiver card to accommodate low size, weight, and power consumption (SWaP) for ground embedded users, aviation, and precision-guided munitions, Air Force officials say.

The next-gen ASIC should provide significant performance improvements and extend production life over its predecessors, negate obsolescence issues of the current 90-nanometer and 45-nanometers increment 1 ASICs. The three companies chosen will complete receiver development, including formal qualification testing, verification, and security approval.



The joint-service MGUE program developed an updated set of military GPS receivers that provide accurate and reliable positioning, navigation, and timing service where previous receiver performance was compromised or unavailable.

The program addressed the increasing threat of enemy electronic warfare jamming of U.S. and allied GPS signals, as well as to deny the enemy the use of U.S. GPS signals. Orbiting GPS IIR-M and IIF satellites are part of the MGUE program, as are GPS III satellites that are in development.

Prototype GPS receiver electronic circuit cards built for the MGUE helped add new features into GPS receiver designs. The MGUE also developed M-Code signals, which are transmitted from modernized GPS satellites. These signals retain all legacy GPS receiver capabilities, yet offers high-power signals with the ability to resist jamming and interference.

M-Code signals also add security features to prevent their use by the enemy, and offer improved message formats and signal modulation for faster and more accurate performance.

Raytheon Intelligence & Space (formerly Raytheon Space and Airborne Systems), Collins Aerospace, and L3Harris Interstate Electronics were involved in the MGUE increment MSI program.

On this contract the three companies will do the work in Cedar Rapids, Iowa, Anaheim, Calif., and El Segundo, Calif., and should be finished by September 2025.

For more information contact Raytheon Intelligence & Space online at www.rtx.com/Our-Company/Our-Businesses/RIS, L3Harris Interstate Electronics at www.l3harris.com/all-capabilities/navigation-solutions, or Raytheon Collins Aerospace at www.rtx.com/Our-Company/Our-Businesses/ca.

UNMANNED SURFACE VESSELS

Liquid Robotics to build unmanned surface vessels for ocean persistent surveillance

U.S. Navy researchers needed long-endurance unmanned surface vessels (USVs) and sensor payloads for ocean persistent surveillance in classified and unclassified missions. They found their solution from Liquid Robotics Inc., a Boe-

ing company in Sunnyvale, Calif.

Officials of the Naval Information Warfare Center-Pacific in San Diego have announced their intention to award sole-source purchase orders to Liquid Robotics to buy the company's Wave Glider USVs, which for military applications are branded as the Sensor Hosting Autonomous Remote Craft (SHARC).

These USVs will have mission-specific sensors and payloads to demonstrate mission capability. Liquid Robotics will provide prototype systems, spares, maintenance, software licensing, and engineering support for missions in the maritime environment.

The value of upcoming contracts will be about \$12.5 million. The exact value has yet to be negotiated.

The Liquid Robotics Wave Glider is an autonomous unmanned surface vessel powered by wave and solar energy. It has two components — a surface vehicle about the size of a surfboard, and a tethered submersible with moving wings that dangles underneath the surface vessel to harvest wave energy for forward propulsion. It can travel as fast as 3 knots.

The Wave Glider USV can operate individually or in fleets to deliver real-time data and act as a data communications relay for as long as one year with no fuel.

Wave Glider instruments, working together, can provide fleets of networked wave-powered ocean robots for military, oil and gas, commercial, and science applications.

Key to the Wave Glider is its ability to harvest energy from ocean waves to provide essentially limitless propulsion to provide persistent surveillance at sea. Wave Gliders run on wave and solar energy for propulsion, communications, navigation, and computing.

Wave Gliders operate at the surface of the ocean and can travel across great expanses for

a year at a time without returning to port. They can monitor coastlines and connect the subsea world to shore, air, and space. They can survive and operate through some of the ocean's most severe conditions, such as hurricanes.

The Wave Glider harvests power from the up-and-down motion of the waves by converting this energy into forward thrust. The Wave Glider is equipped with computers for navigation, communications, and ocean sensors.

Wave Glider sensors can measure weather, sea conditions, water quality and chemistry, bottom topography, and currents. Acoustic microphones and arrays enable real time communications from subsea to space and can detect passing ships and capture vocalizations of whales and monitor other mammals.

Military applications of the Wave Glider and SHARC include anti-submarine warfare (ASW), countermine operations, coastal and border security, drug and human trafficking interdiction, and maritime domain awareness.

Users can operate the Wave Glider autonomously or control the USV virtually via any secure Internet connected device. The system can store data onboard or transmit it in real time via satellite or by cellular phone networks depending on the distance to shore.

The Wave Glider's software operating environment is called Regulus, and is based on Linux and Java. The system uses the Liquid Robotics Adaptable, Modular Power System (AMPS) to provide scalable power to support the most power-hungry sensors. The onboard battery storage scales from 0.9 to 4.5 kilowatt hours.

The Wave Glider and SHARC vessels have low observability and detectability. It cannot be detected by radar or infrared sensors, and is acoustically silent. Wave Glider can carry or tow a range of sensors, including acoustic Doppler current profiler (ADCP) sensors, weather stations, fluorometers, hydrophones, cameras, and water quality-sensors.

For more information contact Liquid Robotics online at www.liquid-robotics.com, or the Naval Information Warfare Center-Pacific at www.public.navy.mil/navwar/NIWC-Pacific/Pages/default.aspx. ←



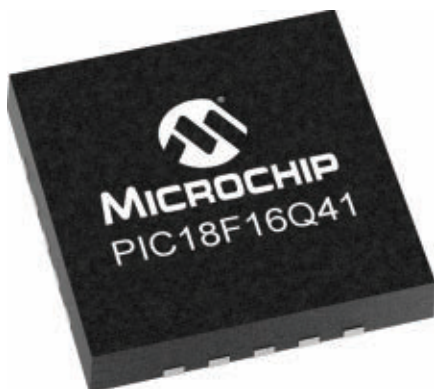


new PRODUCTS

INTEGRATED CIRCUITS

Microcontrollers with integrated data conversion introduced by Microchip

Microchip Technology Inc. in Chandler, Ariz., is introducing the PIC18-Q41 and AVR DB microcontrollers for large-scale artificial intelligence (AI) at-the-edge and sensor-based Internet of Things (IoT) applications. The PIC18-Q41 and AVR DB microcontrollers integrate data conversion to provide analog functionality and digital control capability, and combine advanced analog peripherals and multi-voltage operation with inter-peripheral connections for increased system integration and reduced signal acquisition times. The PIC18-Q41 microcontroller has a configurable operational amplifier, A/D converter, and D/A converter. It comes in compact 14- and 20-pin packages, and makes a good companion to Microchip's 32-bit microcontrollers and other controllers that require analog integration. The AVR DB microcontroller simplifies the challenges of mixed-signal IoT systems, often include several power domains, and can reduce costs by integrating true bi-directional level shifters. This feature lowers cost in applications like automotive, appliances, HVAC, and liquid measurement. The addition of three independent and configurable Op Amps, a 12-bit differential A/D converter, 10-bit D/A converter, three zero cross detectors, and core-independent peripherals makes the AVR DB microcontroller suitable for applications that involve analog sig-



nal conditioning and processing functions. For more information contact Microchip online at www.microchip.com.

RUGGED COMPUTERS

Rugged laptop computer for military and public safety offered by Getac

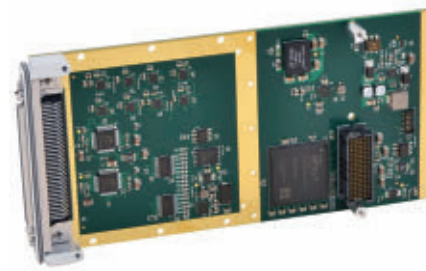
Rugged computer specialist Getac Technology Corp. in Irvine, Calif., is introducing the latest generation of the V110 rugged laptop computer for use in harsh environments in military, law enforcement, emergency medical response, field-utility installation and repair, and manufacturing applications. The next-gen V110 combines the functionality of a laptop with the convenience of a tablet via a proprietary hinge design that enables users to shuttle between tablet and laptop mode in one step. The V110's water- and shock-proof keyboard is 56 percent larger than that of a typical 10.1-inch rugged laptop. It also has 88 standard-sized, red-backlit, island-style independent keys. Other outstanding standard features of the latest V110 include a more powerful Quad-Core processor, a revolutionary 11.6-inch Getac LumiBond 2.0 wide screen indoor, outdoor, direct-sunlight display, a high-speed, rugged-mount PCI Express solid-state drive, and dual hot-swappable batteries. Other configurable I/O data capture-and-sharing options for the rugged laptop computer include Getac's KeyWedge bar code reader utility for generating clear readings from bar codes obscured by grease or debris, plus an RFID reader, USB3.1 Gen 2 Type C connections, and an 8-megapixel rear camera. For more information contact Getac online at www.getac.com.

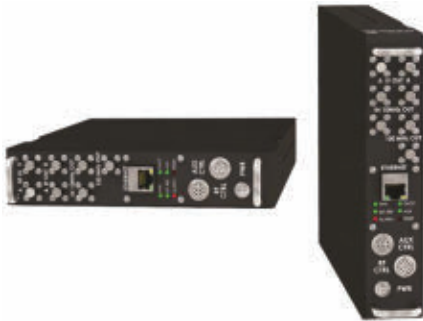


BOARD PRODUCTS

Rugged XMC I/O module for COTS embedded computing introduced by Acromag

Acromag in Wixom, Mich., is introducing the XMC730 XMC multi-function embedded computing I/O module for commercial off-the shelf (COTS) aerospace and defense applications. The XMC730 performs analog input, analog output, digital I/O, and counter/timer functions with high-performance direct memory access (DMA) to solve size, weight, and power consumption (SWaP) challenges. Three models provide front 68-pin SCSI-2 I/O connection or rear P16 and P4 I/O connectors, and perform high-speed and high-resolution A/D and D/A conversion, as well as digital I/O and counter/timer functions. A conduction-cooled version is available. The embedded computing module complies with ANSI/VITA 42.0 specification for XMC module mechanicals and connectors., complies with ANSI/VITA 42.3 for XMC modules with PCI Express interface, and conforms to PCI Express base specification, revision 2.1. The module operates in temperatures from 0 to 70 degrees Celsius, stores in temperatures from -55 to 100 C, in humidity from 5 to 95 percent, and withstands the effects of shock per VITA 47 Class OS1. The rugged module has DMA transfer support to move data between module memory and PCI Express bus, and has software development tools for VxWorks, Linux® and Windows environments. For more information contact Acromag online at www.acromag.com.





RF AND MICROWAVE

Microwave tuners for SIGINT and RF testing introduced by Mercury Systems

Mercury Systems Inc. in Andover, Mass., is introducing the TAC-3290 family of adaptive microwave tuners that brings broadband RF to aerospace, defense, and public safety users operating in harsh environments. The TAC-3290 deliver multi-mission operation to applications like signals intelligence

(SIGINT) and radio frequency (RF) testing. The compact and rugged design brings fast data processing to tactical operations in harsh environments while the flexible architecture increases digitizer compatibility eliminating complex and expensive system upgrades. "By replacing racks of application-specific equipment with a flexible solution small enough to fit in a backpack, the TAC-3290 delivers agile RF capabilities to signal capture and processing systems in the field," says Neal Austin, vice president and general manager of mixed-signal technology at Mercury Systems. The TAC-3290 series brings rackmount converter technology to a small form factor. Typical frequency converters receive signals in a pre-determined bandwidth, yet applications like SIGINT and spectrum management must operate on a wide range of varying signals. The TAC-3290 series resolves this mismatch

by enabling the converters to adapt in real time to match the signals of interest. For more information contact Mercury Systems online at www.mrcy.com.

CABLING AND CONNECTORS

Rugged and flexible VNA test cables introduced by Fairview Microwave

Fairview Microwave Inc. in Lewisville, Texas, is introducing vector network analyzer (VNA) test cables for demanding test and laboratory applications like semiconductor probe testing, precise benchtop testing, and production testing that requires a flexible-yet-durable cable solution. The high-frequency VNA test cables display electrical properties such as phase stability of plus-or-minus 6 degrees at 50 GHz and plus-or-minus 8 degrees at 70 GHz, as well as a voltage standing wave ratio (VSWR) of 1.3:1 at 50 GHz and 1.4:1 at 70 GHz. The 50 GHz assem-

PRODUCT & LITERATURE SHOWCASE

Better Decisions, Faster

Situational Awareness, Control, and Decision Support



Proven Solutions for Government, Military, Medical and Corporate Applications

We offer video signal distribution and display solutions for mission-critical applications, encompassing baseband and IP video, KVM control, display processing from desktop multiviewing to wide-area video walls, visual data recording, content management and third-party device control.



RGB SPECTRUM

rgb.com/contact

ADVERTISERS INDEX

ADVERTISER	PAGE
Annapolis Micro Systems Inc.....	C3
Cinch Connectivity Solutions.....	11
Discovery Semiconductors Inc.....	5
Elma Electronic Inc.....	6
General Dynamics Mission Systems.....	23
General Micro Systems Inc.....	C4
Guntermann & Drunck GmbH.....	33
L-Com.....	15
Milpower Source.....	31
Pasternack Enterprises.....	3
Pentek.....	C2
Phoenix International.....	13
Pico Electronics Inc.....	1
Radiall AEP Inc.....	17
Regions Financial Corporation.....	9
RGB Spectrum.....	38
Viking Technology.....	7

**Military
& Aerospace**
Electronics

Visit us for must
have industry insights
and articles.

www.militaryaerospace.com

**Military
& Aerospace**
Electronics

SUBSCRIPTION INQUIRIES

Phone: 1-877-382-9187 / International Callers: +1-847-559-7598

E-mail: MAEM@omeda.com

Web: www.mae-subscribe.com

VICE PRESIDENT/GROUP PUBLISHER Paul Andrews

203 423-3963 / pandrews@endeavorb2b.com

EDITOR-IN-CHIEF John Keller

603 891-9117 / jkeller@endeavorb2b.com

ASSOCIATE EDITOR Jamie Whitney

603 891-9135 / jwhitney@endeavorb2b.com

CONTRIBUTING EDITOR WESTERN BUREAU J. R. Wilson

702 434-3903 / jrwilson@endeavorb2b.com

EDITORIAL ART DIRECTOR Kermit Mulkins

PRODUCTION MANAGER Sheila Ward

AUDIENCE DEVELOPMENT MANAGER Debbie Bouley

603 891-9372 / dbouley@endeavorb2b.com

MARKETING MANAGER Adrienne Adler

603 891-9420 / aadler@endeavorb2b.com



www.endeavorbusinessmedia.com

EDITORIAL OFFICES

Endeavor Business Media, LLC

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

Keith Gregory, Sales Manager

508 1/2 Ocean Park Ave., Bradley Beach, NJ 07720

732 897-9550 / Cell 917 993-3741

kgregory@endeavorb2b.com

WESTERN CANADA & WEST OF MISSISSIPPI

Maureen Elmaleh, Sales Manager

7475 Miller Street, Arvada, CO 80005

303 975-6381 / Cell 212 920-5051

melmaleh@endeavorb2b.com

REPRINTS Jessica Stremmel

717 505-9701 x2205 / Jessica.stremmel@theygsgroup.com

DIRECTOR LIST RENTAL Kelli Berry

918 831-9782 / kberry@endeavorb2b.com

**For assistance with marketing strategy or ad creation,
please contact Marketing Solutions**

Kaci Wheeler

918 832-9377 / kwheeler@endeavorb2b.com

ENDEAVOR BUSINESS MEDIA, LLC

CHIEF EXECUTIVE OFFICER Chris Ferrell

CHIEF REVENUE OFFICER, CHIEF MARKETING OFFICER June Griffin

CHIEF FINANCIAL OFFICER William Nurthen

CHIEF OPERATING OFFICER Patrick Rains

CHIEF ADMINISTRATIVE AND LEGAL OFFICER Tracy Kane

CHIEF TECHNOLOGY OFFICER Eric Kammerzelt

EVP, TECHNOLOGY GROUP Lester Craft





blies are terminated with 2.4-millimeter connectors, while the 70 GHz versions use 1.85-millimeter connectors. The braided, stainless steel armoring surrounding the coax provides a rugged-but-flexible cable with a flex life exceeding 100,000 cycles. These VNA test cables are terminated with rugged stainless-steel connectors that provide as many as 5,000 mating cycles when attached with proper care. The flexibility of these cables makes it safe and easy to use with a device under test (DUT). A swept right-angle 2.4-millimeter and 1.85-millimeter connector option enables these cables to fit into tight spaces and reduce the length of cable in many applications. For more information contact Fairview Microwave online at www.fairview-microwave.com.

ANTENNAS

Horn antennas for public safety and industrial applications introduced by KP

KP Performance Antennas in Edmonton, Alberta, is introducing ProLine 5 GHz horn antennas for public safety, mining, industrial, and wireless internet service provider (WISP) applications. KP's ProLine 5 GHz horn antennas consists of three high-performance models with gains and patterns that are stable over a wide bandwidth. They are engineered to suppress

side-lobes and back-lobes and excel at rejecting interference. Featuring quick-connect waveguide technology with tool-less installation and adjustable polarization, these horn antennas are available in 30, 45, and 60-degree beam widths with frequencies from 4.9 to 6.4 GHz. These compact antennas deliver 19, 16, and 13.8 dBi gain depending on model, and are for filling in gaps in coverage, and reducing interference in noisy environments. For more information contact KP Performance Antennas online at www.kpperformance.com.

VISION SYSTEMS

CoaXPress frame grabbers for small vision systems introduced by BitFlow

BitFlow Inc. in Woburn, Mass., is introducing a single-link version of the company's Claxon series of high-performance CoaXPress CXP-12 frame grabbers for aerospace, scientific, robotics, and high-speed linescan inspection applications. The frame grabbers transfers image data from a CoaXPress (CXP)-interfaced camera to the host memory at speeds as fast as 12.5 gigabits per second, and provides developers of small, complex vision systems with a deterministic zero-latency pipeline. The frame grabber takes advantage of a half-size PCI Express expansion bus and StreamSync DMA to deliver the sustained bandwidth necessary to support acquisition from one of the new generation single-link CXP-12 cameras. Cameras are plug-and-play with automatic link speed and camera parameter detection. The Claxon CXP1 has an uplink interface as fast as 41.6 megabits per second, and further simplifies integration by supplying 13 Watts of safe Power over CoaXPress (PoCXP) — all on one coaxial cable using micro-BNC connectors. Unlike USB3, Camera Link, or other interfaces that rely on passive cable lengths of a few meters or less, the Claxon CXP1 frame grabber supports a 40-meter maximum cable length without the use

of a repeater that could jeopardize signal integrity. Fanless passive cooling ensures extended use of the frame grabber without maintenance. Drivers for third-party applications are available, such as LabView, VisionPro, and HALCON. For more information contact BitFlow online at www.bitflow.com.

EMBEDDED COMPUTING

Rugged GPGPU-based embedded computing system introduced by Aitech

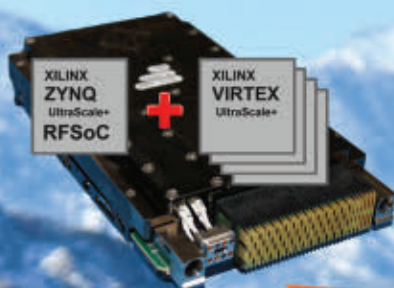
Aitech Defense Systems in Chatsworth, Calif., is introducing the upgraded and qualified version of the A178 rugged general-purpose graphics processing (GPGPU) AI embedded supercomputer for intense data processing in extreme environments. The A178 operates reliably in mobile, remote, military, and autonomous systems, and is for applications like training simulation, situational awareness, artificial intelligence (AI), image and video processing, and moving maps. One of the smallest of Aitech's small-form-factor (SFF) embedded computing systems, the A178 uses the NVIDIA Jetson AGX Xavier system-on-module that features the Volta GPU with 512 CUDA cores and 64 Tensor cores to reach 32 TOPS INT8 and 11 TFLOPS FP16. Upgrades help meet the demand for standalone and compact GPGPU-based systems that are rugged and SWaP-C-optimized. The low-power unit offers energy efficiency, while providing all the power necessary for AI-based local processing. The advanced computation abilities of the system include two dedicated NVIDIA Deep-Learning Accelerator (NVDLA) engines that provide an interface for deep learning applications. The system can accommodate as many as three expansion modules, such as an HD-SDI frame grabber, composite frame grabber, or NVMe solid-state drive. For more information contact Aitech online at <https://aitechsystems.com>. ←



THE MOST FLEXIBLE COTS RFSoC SOLUTIONS

SOSA™

MADE IN
U. S. A.



XILINX
ZYNQ
UltraScale+
RFSoc

2
PACKAGE
OPTIONS

Processing-Intensive
3U/6U or PCIe

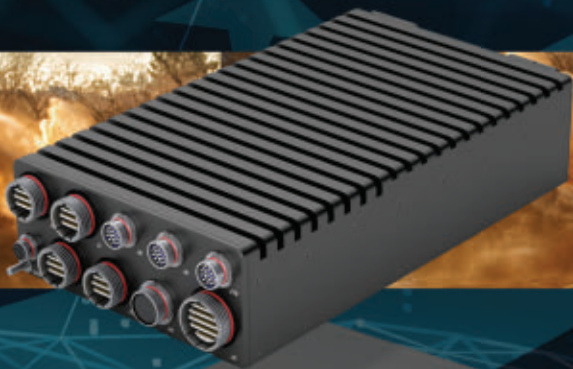
SWaP-Optimized
 $\frac{1}{3}$ of 3U Size



GENERAL MICRO SYSTEMS, INC.

ADVANCED SERVERS

ONE COMPANY FOR ALL YOUR SERVER NEEDS



RUGGED SERVERS



INDUSTRIAL SERVERS



COMMERCIAL SERVERS



MADE IN U.S.A.

GMS

GENERAL MICRO SYSTEMS, INC.

TRUSTED AND DEPLOYED SINCE 1979

(800) 307-4863 / GMS4SBC.COM