

READ THE DIGITAL EDITION

ANYTIME, ANYWHERE, ANYWAY YOU LIKE

At your desk or in the field, our digital edition makes it easier than ever to read important content wherever you go.

▶ **EASIER TO READ**

Flip through pages one at a time or enlarge them to go easy on your eyes.

▶ **WORKS ON ANY DEVICE**

The new responsive design lets you access it on your smartphone, tablet or desktop.

▶ **PUTS YOU IN CONTROL**

Interactive table of contents
Lets you choose exactly what you want to read.

Page View

Simply toggle between Page View or Reading View using the toggle button on the top right of page.

Digital Archive Library

Click the button on the top left of page to view all previous issues.

Download or Print

Share with your colleagues or save for yourself.



Military+Aerospace Electronics®

Subscribe at www.militaryaerospace.com/subscribe
and check out our digital edition today!

DECEMBER 2022

Military+Aerospace Electronics®



TRUSTED COMPUTING FOR NATIONAL DEFENSE

Cyber focuses on zero trust, as military seeks to safeguard technologies from cyber hackers and spoofers. PG. 12

THE MERCURY PROCESSING PLATFORM

mercury

TECHNOLOGICAL SUPERIORITY MEANS DECISION SUPERIORITY

The climate of continuous urgency in the geopolitical environment is escalating demand for faster, more powerful and secure aerospace and defense (A&D) systems. From data to decision, silicon to systems, customers entrust their mission-critical challenges to Mercury. Our trusted, secure, end-to-end processing platform leapfrogs incremental gains, bending the curve to power the most critical A&D missions on the planet and beyond.

mrcy.com/processing-platform

Innovation That Matters®





Features

12 SPECIAL REPORT

Trusted computing for national defense

Cyber security enters the realm of zero trust, as military forces seek to safeguard sensitive military technologies from enemy cyber hackers and spoofers.

21 TECHNOLOGY FOCUS

Data storage making the transition to network-based systems

Network-attached secure data storage architectures not only can help warfighters get broad access to mission-critical data, but also help to keep data safe from hackers and other cyber security threats.

D1 DIGITAL EXCLUSIVE

Commercial Aerospace

www.militaryaerospace.com/subscribe

Columns

2 TRENDS

4 NEWS

7 IN BRIEF

26 RF & MICROWAVE

30 UNMANNED VEHICLES

34 ELECTRO-OPTICS WATCH

38 PRODUCT APPLICATIONS


45 NEW PRODUCTS

FOLLOW US

Cover photo: ID 879913280 © gorodenkoff | gettyimages.com

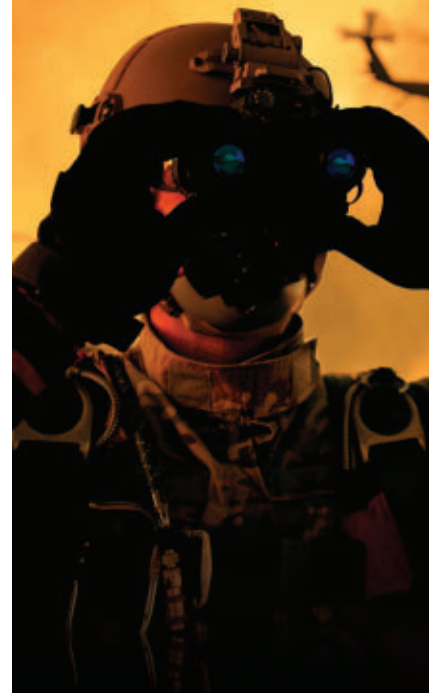
 **FACEBOOK.com**
/MilitaryAerospaceElectronics

 **TWITTER**
@MilAero

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



Military+Aerospace Electronics®



Aerospace & Defense professionals
rely on *Military + Aerospace
Electronics* magazine, website,
and newsletters for the latest
technology design trends and
the most important aerospace
and defense applications driving
technology innovation.

SUBSCRIBE TODAY!

www.militaryaerospace.com

Military & Aerospace Electronics® (ISSN 1046-9079, print; 2688-366X, digital / USPS 005-901) is published 12 times a year by Endeavor Business Media, LLC, 30 Burton Hills Blvd., Suite 185, Nashville, TN 37215 USA. Periodicals postage paid at Fort Atkinson, WI 53538 and at additional mailing offices. SUBSCRIPTION PRICES: USA \$171 1yr., \$280 2 yr.; Canada \$198 1 yr., \$320 2 yr.; International \$224 1 yr., \$360 2 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 2022. 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.

PHOTO: © MEYSAM AZARNESHIN - STOCKADOB.COM

Unmanned systems to take lead role in defending Marines on invasion beaches



BY **John Keller**
EDITOR IN CHIEF

Autonomous technologies and unmanned systems are set to play a leading role in how U.S. Marines operating on invasion beaches defend themselves from enemy warships that seek to thwart Marine Corps footholds in captured territory.

It comes down to the role of armed unmanned vehicles in the future Navy/Marine Expeditionary Ship Interdiction System (NMESIS), which aims to use shore-based long-range anti-ship missiles and unmanned vehicles to defend Marines from attacks by enemy surface warships.

The anti-ship weapons will be the Raytheon Naval Strike Missile (NSM), which has an imaging infrared seeker, an onboard target database, and navigates by Global Positioning System (GPS), inertial sensors, and terrain-reference systems.

The NSM can detect, recognize, and discriminate among targets independently, and is designed to strike enemy ships at or near the water line to inflict maximum structural damage. Raytheon is building the NSM in partnership with Kongsberg Gruppen in Kongsberg, Norway.

NMESIS will provide Marine Corps High Mobility Artillery Rocket System (HIMARS) battalions with NSM anti-ship capabilities. Launchers for the NSM anti-ship weapons will be unmanned remotely operated versions of the Oshkosh Defense Joint Light Tactical Vehicle (JLTV), each which will carry two NSMs.

The combination of the unmanned JLTV missile launchers and NSM anti-ship weapons will be called the Remotely Operated Ground Unit for Expeditionary Fires (ROGUE-Fires). Oshkosh Defense won a \$23.7 million Marine Corps Systems command contract last month to provide the ROGUE-Fires unmanned JLTV launchers. The NSM is a modernized version of the Norwegian Penguin anti-ship missile.

The remotely operated ROGUE-Fires vehicles will make the most of machine automation and unmanned systems technologies once they hit the beaches with the Marines.

Invasion beaches are busy places, where Marines are concerned primarily with fighting-off enemy attempts to throw them back into the sea, setting up communications and command posts, placing the Northrop Grumman Ground/Air Task-Oriented Radar (G/ATOR) for air defense, and supplying Marine infantry with fuel, food, and other supplies.

Each time a system like a ROGUE-Fires vehicle can operate unmanned frees a Marine from driving vehicles, and helps the Marine take-on more important responsibilities. To make ROGUE-Fires and NMESIS operations even more efficient, one Marine can operate several unmanned missile launchers to help hold enemy ships at bay.

The ROGUE Fires version of the JLTV lacks a crew cab and body, and is integrated with sensors and cameras, with a launcher mounted on top of the vehicle.

There are many possibilities for battlefield unmanned vehicles, ranging from logistics and warfighter resupply, to mobile communications center setup and relocation, to combat vehicle refueling, to battery recharging.

With unmanned applications like those in place, it's just a matter of time before combat functions start relying on machine automation technologies for efficiency on the leading edge of the battlefield.

Future applications won't involve just remote operation, either. We're on the cusp of a new era when artificial intelligence, machine learning, and other autonomous technologies start to take their places beside warfighters in the heat of battle. ◀



RF Custom Cable Assemblies

Fairview Microwave stocks and builds the industry's most comprehensive selection of custom RF cable assemblies. With over 250,000 possible combinations all available to ship the same day, Fairview Microwave RF custom cable assemblies in coaxial and twinaxial are the solution for your urgent needs. Whether you're looking for a common cable or something unique to your specifications, Fairview Microwave allows you to design your own custom RF cable assembly.

RF custom coaxial cable assemblies can be built from over 1,300 connector types and close to 125 different coaxi cables (including Twinax). Fairview Microwave can also provide you value-added services for your custom RF cable assemblies such as a suite of testing solutions, custom labeling, lead-free solder, custom booting/heat shrink options, plus more. If you're interested in designing your very own custom coaxial cable assemblies, please use our Cable Creator™ today!

Place your order by 6 PM CT, and have your cables or any other components shipped today.

In Stock & Shipped Same-Day

fairviewmicrowave.com
+1 (800) 715-4396

 **Fairview Microwave®**
an INFINIT[®] brand





NASA's Artemis I 'mega rocket' launches tech-filled Orion spacecraft to the moon

By Jamie Whitney

KENNEDY SPACE CENTER, Fla. — It was all systems go for the National Aeronautics and Space Administration (NASA) as officials announced the successful liftoff on 16 Nov. of the agency's Space Launch System (SLS).

NASA's SLS is the most powerful rocket in the world; it provides 8.8 million pounds of thrust, and launched the agency's Orion spacecraft. Lockheed Martin Space in Denver is the prime contractor for NASA and built the crew module, crew module adaptor, and launch-abort system.

The craft was sent to the moon as part of the Artemis program. The launch is the first leg of a mission in which Orion is planned to travel approximately 40,000 miles beyond the moon and return to Earth over the course of 25.5 days. This flight is a significant test prior to flying astronauts on the Artemis II mission.

The launch and following missions were enabled by technology from dozens of industry partners, including Wind River Systems in Alameda, Calif., and Honeywell in Phoenix.

Wind River's VxWorks real-time operating system was selected to aid the SLS's first stage of launch, inside the Orion Crew Vehicle for life support, communications, and Lunar orbit, plus associated science experiments.

▲ **The NASA Space Launch System, the most powerful rocket in the world, launched the Artemis 1 spacecraft to the moon in mid-November.**

In addition, Honeywell provided the full navigation and guidance system for the Artemis I launch vehicle. This allowed the spacecraft to know exactly where it's going, stay on course and return safely to Earth.

Honeywell technology is also helping control the thrust on rockets.

Early in this uncrewed mission, the spacecraft deployed series of 10 small science investigations and technology demonstrations, called CubeSats, from a ring that connected the upper stage to the spacecraft.

Orion's service module performed the first of a series of burns to keep Orion on course toward the moon approximately eight hours after launch. Mission controllers at NASA's Johnson Space Center in Houston will conduct additional checkouts and course corrections as needed.

Orion is expected to fly by the moon on Nov. 21, performing a close approach of the lunar surface on its way to a distant retrograde orbit, a highly stable orbit thousands of miles beyond the moon. ◀

"The Space Launch System rocket delivered the power and performance to send Orion on its way to the moon," said Mike Sarafin, Artemis I mission manager. "With the accomplishment of the first major milestone of the mission, Orion will now embark on the next phase to test its systems and prepare for future missions with astronauts."



Oshkosh to build unmanned combat vehicles as anti-ship missile launchers

BY John Keller

QUANTICO MARINE BASE, Va. – U.S. Marine Corps expeditionary warfare experts are asking Oshkosh Defense LLC in Oshkosh, Wis., to provide unmanned armored combat vehicles as mission launchers for a new Marine Corps land-based anti-ship missile system.

Officials of the Marine Corps Systems Command at Quantico Marine Base, Va., have announced a \$23.7 million contract to Oshkosh for Remotely Operated Ground Unit for Expeditionary Fires (ROGUE-Fires) carriers for use in the Navy/Marine Expeditionary Ship Interdiction System (NMESIS).

The ROGUE-Fires long-range anti-ship missile launchers will be based on unmanned remotely operated versions of the Oshkosh Joint Light Tactical Vehicle (JLTV), each which will carry two Naval Strike Missiles (NSM) to help protect Marine Corps infantry on invasion beaches.

NMESIS will provide the Marine Corps High Mobility Artillery Rocket System (HIMARS) battalions with anti-ship capabilities. NMESIS integrates a Naval Strike Missile (NSM) launcher unit, capable of launching two NSMs, onto a ROGUE-Fires carrier.

The NSM has an imaging infrared seeker, an onboard target database, and navigates by Global Positioning System (GPS), inertial sensors, and terrain-reference systems. It can detect, recognize, and discriminate among targets independently, and is designed

▲ **Oshkosh Defense will build unmanned versions of the company's Joint Light Tactical Vehicle (JLTV) to serve as anti-ship missile launchers to help defend invasion beaches.**

to strike enemy ships at or near the water line to inflict maximum structural damage.

Raytheon is building the NSM in partnership with Kongsberg Gruppen in Kongsberg, Norway. In addition to NMESIS, the missile is to equip the lit-

toral combat ship and FFG(X) future frigate with stand-off surface-to-surface weapons capability.

Raytheon and Kongsberg in their initial OTH-WS bid offered the Naval Strike Missile (NSM) — a fifth-generation long-range, precision-strike missile that offers strike capability against heavily defended land and sea targets. NSM is a modernized version of the Norwegian Penguin anti-ship missile.

Experts from the Marine Corps and Raytheon tested the NMESIS off the coast of California in April 2021. The ROGUE Fires vehicle is remotely operated using the teleoperator or leader-follower modes. It was built for the Marines to support anti-ship operations from the ground.

The ROGUE Fires version of the JLTV lacks a crew cab and body, and is integrated with sensors and cameras, with a launcher mounted on top of the vehicle. Marine Corps leaders say they plan eventually to launch future weapons from ROGUE Fires. ◀

On this contract Oshkosh will do the work in Alexandria, Va.; Gaithersburg, Md.; and Oshkosh, Wis., and should be finished by November 2023. For more information contact Oshkosh Defense online at <https://oshkoshdefense.com>, or Marine Corps Systems Command at www.marcorsyscom.marines.mil.



Northrop Grumman, Raytheon eye electro-optical sensors with built-in machine learning

BY John Keller

ARLINGTON, Va. — Two U.S. prime defense systems integrators are moving forward with a military research project to develop a new kind of camera and digital signal processing to enable intelligent electro-optical sensors for tactical military applications.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., have awarded orders collectively worth \$25 million to the Northrop Grumman Corp. Mission Systems segment in Linthicum Heights, Md., and to the Raytheon Intelligence & Space segment in El Segundo, Calif.,

◀ **the Fast Event-based Neuromorphic Camera and Electronics (FENCE) program will develop a new kind of camera and digital signal processing for intelligent electro-optical sensors.**

for the second phase of the Fast Event-based Neuromorphic Camera and Electronics (FENCE) program. DARPA FENCE seeks to develop and demonstrate a low-latency, low-power, event-based camera and a new class of digital signal processing and machine learning algorithms that use combined spatial and temporal information to enable intelligent sensors for tactical military applications.

In June 2021 Northrop Grumman won a \$15.8 million contract and Raytheon won an \$8.8 million contract for the first phase of the FENCE program.

Neuromorphic describes silicon circuits that mimic brain operation; it exhibits low latency, sparse output, and extreme energy efficiency. Neuromorphic cameras offer sparse output, and respond only to changes in the scene, with accompanying low latency and low power for small-format cameras in sparse scenes.

Event-based imaging sensors operate asynchronously, and only transmit data from pixels that have changed, so they produce 100 times less data in sparse scenes than traditional focal plane arrays (FPAs). This leads to 100x lower latency at 100x lower power.

Despite their inherent advantages, existing event-based cameras are not compatible with military applications because military images are cluttered and dynamic. The FENCE program seeks to develop an integrated event-based infrared focal plane array with embedded processing to overcome these challenges.

The FENCE program's primary focus is on developing an asynchronous read-out integrated circuit (ROIC) capable of very low latency and power operation, and a new, low-latency event-based infrared sensor with in-pixel processing.

The project also will develop a low-power processing layer that integrates with the ROIC to identify relevant spatial and temporal signals. The ROIC and the processing layer together will enable an integrated FENCE sensor that can operate on less power than 1.5 Watts.

On these orders Northrop Grumman will do the work in Linthicum Heights, Maryland; Baltimore; San Diego; and Palo Alto, Calif. Raytheon will do its work in Goleta and El Segundo, Calif.; Cambridge and Tewksbury, Mass.; McKinney, Texas; and New York. The companies should be finished by June 2024. ◀

For more information contact Northrop Grumman Mission Systems online at www.northropgrumman.com, Raytheon Intelligence & Space at www.raytheon-intelligenceandspace.com, or DARPA at [Paste link here](#).

United Airlines wants people who drive to fly on electric planes instead

Cars aren't the only polluters. If we want to save the planet, every part of how we travel has to change, and that includes airplanes. Whether or not that method of clean travel will catch on though is another thing. But as CNBC reports, United Airlines thinks electric planes will be the next generation of air travel, but mainly for short, regional flights. "Initially we want to fly on routes that are 200 miles or less," Mike Leskinen, president of United Airlines Ventures, the carrier's in-house venture capital arm, said, during a video interview at CNBC's ESG Impact Virtual Conference earlier this month. As the technology improves, aircraft will have a range of 250 miles or 300 miles, Leskinen said. In October United Airlines announced a \$15 million investment in Brazil-based Eve Air Mobility. In addition, United has also signed a conditional purchase agreement for 200 four-seat electric aircraft plus 200 options, expecting the first deliveries as early as 2026. This continues United's investment in the Urban Air Mobility (UAM) market, also called "flying taxis" – or eVTOLs (electric vertical take-off and landing vehicle).

How Joby and Delta are making flying taxis a reality

The world has long dreamed of a day when flying cars become part of daily life. And despite many attempts, that day hasn't arrived. But we might not have to wait much longer. Advances in battery and electric propulsion technology have enabled entirely new types of aircraft to take to the skies. Startups Joby, Archer, Vertical, Lilium, and more are developing eVTOLs, electric vertical takeoff and landing aircraft, with the vision of making air taxis a reality. Joby's aircraft is designed to fly fast, quiet and sustainable trips in and around cities. The aircraft has flown more than 1,000 test flights, demonstrating its range, speed, altitude and low noise profile. The company was the first eVTOL company to be granted a G-1 (Stage 4) Certification Basis for its aircraft by the FAA and recently received its Part 135 Air Carrier Certification. In 2022, Delta also continued to invest in digital identity technology in these and other airports, which allows customers to move through the airport using facial matching, eliminating the need to show a boarding pass or government ID and thereby expediting their journeys.



BlackHorse Solutions and Georgia Tech seek new cyber security anti-hacker measures

BY John Keller

ARLINGTON, Va. – U.S. military researchers are asking BlackHorse Solutions Inc., a Parsons Company in Herndon, Va., to develop ways to detect, manage, and defeat cyber hackers and help build-in cyber security as part of the computer design process.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., has announced a \$11.7 million contract to BlackHorse Solutions for the Signature Management Using Operational Knowledge and Environments (SMOKE) project.

SMOKE seeks also to measure the risk of cyber threats in real-time; and find new ways for red-team ethical hackers to maintain their evasiveness as they help train cyber security experts root-out malicious cyber behavior.

BlackHorse Solutions joins Georgia Tech Research Corp. in Atlanta on the DARPA SMOKE trusted computing project. BlackHorse won its contract in September, while Georgia Tech won a \$22.7 million contract in October.

Cyber security experts from BlackHorse Solutions and Georgia Tech will develop data-driven tools to automate the planning and execution of threat-emulated cyber infrastructure necessary for military network security assessments.

Military computer networks are under persistent threat from malicious cyber hackers, so network security experts must be able to assess their cyber vulnerabilities and defenses by using red team ethical hackers and blue team cyber defenders.

◀ **The DARPA Signature Management Using Operational Knowledge and Environments (SMOKE) project seeks to develop ways to detect, manage, and defeat cyber hackers and help build-in cyber security as part of the computer design process.**

The ability to emulate sophisticated threats, evade detection, and reduce signatures requires a significant amount of time and expertise. Today, furthermore, the demand for network security assessments is greater than the supply.

SMOKE seeks to develop tools to automate the deployment of automated cyber threats that will enable red teams to increase the effectiveness of cyber security assessments. These tools also could provide red teams with longer cyber security assessment because of their ability to remain hidden.

DARPA researchers want industry to develop tools that enable automated and scalable emulated cyber threats. SMOKE will prototype components that enable red teams to plan, build, and deploy cyber infrastructure that is informed by machine-readable signatures of sophisticated cyber threats.

To ensure realism, DARPA experts will evaluate SMOKE components on real-world networks controlled by SMOKE performers and government partners — first on emulated environments, and perhaps later on live networks.

The SMOKE program seeks breakthrough approaches in abstracting away complexities of diverse network environments; operating in partially denied environments, reasoning under uncertainty, and reacting to unforeseen detection and/or attribution events; measuring tradeoffs among efficiency and effectiveness of plans in terms of speed and evasion; overcoming state space explosion of typical models for cyber infrastructure planning; developing mechanisms to acquire, manage, and maintain infrastructure elements that conform to signature management policies; executing infrastructure changes in accordance with real-time attribution assessments and plan contingencies; discovering latent associations between infrastructure artifacts; automating expert judgments used to build and traverse infrastructure associations; and expanding knowledge of adversary infrastructure.

SMOKE is a four-year effort divided into two: developing, demonstrating, and evaluating individual components; and comparative evaluations formed by integrating program components. The contract includes one option that could increase its value to \$24.7 million.

SMOKE has two technical areas: automated planning and execution of attribution-aware cyber infrastructure; and generating infrastructure signatures. ➡

On this contract BlackHorse Solutions will do the work in Herndon, Va.; Cincinnati; Herriman, Utah; Sykesville, Md.; and Denver, and should be finished by September 2025. Georgia Tech, meanwhile will do its work in Atlanta and Athens, Ga., and should be finished by October 2026. For more information contact BlackHorse Solutions online at www.parsons.com, or Georgia Tech Research at <https://gtcr.gatech.edu>.

Red team exercises are designed to exceed simple penetration testing, and emulate cyber attacker behaviors as realistically as possible, to form a picture of network defense readiness. Towards the aim of realism, red teams use tactics that mimic advanced cyber threats to evade network defenders and assess how critical networks fare against a determined cyber attack.

A core aspect of red team security assessments are procedures to build domain names, IP addresses, virtual servers, and other components to control red team tools. This infrastructure must exist openly on the public Internet and emits signals that, if detected too easily, can end the assessment quickly without much gain, but at considerable expense.

Signatures are patterns of the way an organization performs cyber operations. Attribution is the ability to link a cyber attack to a likely hacker. Red team members don't want the blue team to attribute attacks to likely perpetrators too quickly, which can weaken a cyber security assessment.



NASA seeks commercial partners to collaborate on low-Earth orbit space technology

BY Jamie Whitney

HOUSTON - U.S. National Aeronautics and Space Administration (NASA) officials are offering contracting opportunities for the space industry to work with the agency through the Collaborations for Commercial Space Capabilities (CCSC-2) initiative.

NASA officials have announced continuation of the Commercial Low-Earth Orbit Development Program (CLDP) and Commercial Crew Program to foster space industry development and growth.

This CCSC-2 initiative pursues goals set in the U.S. National Space Policy and NASA's strategic plan that will benefit human spaceflight and the U.S. commercial low-Earth orbit economy by meeting future business and government needs through unfunded Space Act Agreements (SAA).

These unfunded SAAs are to advance commercial space efforts through NASA contributions of technical expertise, assessments, lessons learned, technologies, and data.

▲ **NASA is forming partnerships with industry to advance commercial space efforts through contributions of technical expertise, assessments, lessons learned, technologies, and data.**

Structured sharing of NASA expertise demands minimal government resources but fosters development of technologies crucial to development of a safe, robust low-Earth orbit ecosystem. The due date for proposal submission was 9 December 2022 at 3 p.m. eastern time. NASA hosted a pre-proposal conference to answer industry questions related to this solicitation last month. ◀

Submit any questions regarding this Announcement for Proposals in an email with the subject line "Q&A CCSC2" to jsc-ccsc2-competition@mail.nasa.gov. Kelly L. Rubio is the point of contact at NASA for this endeavor. They can be reached by email at kelly.l.rubio@nasa.gov, or by phone at 281-244-7890.

Collins Aerospace receives STC to modernize Hawker 800 cockpit communications

Collins Aerospace, a Raytheon Technologies company in Cedar Rapids, Iowa, has received a supplemental type certificate (STC) for the installation of its CMU-4000 on the Hawker 750/800/850/900 series of aircraft. This communications management unit (CMU), according to Collins Aerospace, enables Hawker operators to fly in preferred oceanic and international airspace, create flight efficiencies ranging from more direct routing, quicker departure and landing clearances, reduced fuel consumption and fewer CO2 emissions to meet evolving airspace requirements. The CMU-4000 supports the controller-pilot data link communications

(CPDLC) portion of the Future Air Navigation Standard (FANS 1/A) by enabling the replacement of operational radio communications with text messaging, helping decongest radio frequencies, ease pilot workloads and reduce potential human error in the form of voice misreads. While alternative solutions utilize only one or two radio frequencies (RF) to transmit communications, CMU-4000 uses all three RF sub-networks available (VHF, HF and SATCOM, including Iridium and Inmarsat). This tiered coverage approach provides quality communications regardless of flight condition – including within congested airspace, at higher elevations or in wide-open areas – while also helping eliminate drops in coverage and communication interference. ◀



VIEW EXCLUSIVE CONTENT

Update your subscription to include our Digital Edition and gain access to exclusive articles, promotions, updates, videos and more... You will receive an email each month when the Digital Issue is released.

DON'T MISS THE NEXT ISSUE!

UPDATE YOUR SUBSCRIPTION

militaryaerospace.com/subscribe



Trusted computing for national defense

Cyber security enters the realm of zero trust, as military forces seek to safeguard sensitive military technologies from enemy cyber hackers and spoofers.

BY Jamie Whitney

Founding father, inventor, author, and statesman Benjamin Franklin introduced several lasting thoughts and inventions in his storied lifetime. In his adopted home of Philadelphia, Franklin told fellow residents they would be wise to support his volunteer fire company — the first in what would become the United States — in 1736. Franklin sold his idea with a pithy saying: “An ounce of prevention is worth a pound of cure.”

Perhaps nowhere is this saying more apropos than in keeping vital equipment, systems, and secrets secured. After all, robust cyber security can keep nefarious actors at bay, but so long as

systems remain connected to one another, corporate and state-sponsored spies will attempt to learn their secrets, vulnerabilities, and ways to destroy or takeover components, networks, and even entire weapons systems.

In October, President Joseph Biden Jr. released his administration’s 48-page National Security Strategy (NSS), in which the president lays out a multi-point plan to keep the United States ahead of rival and semi-adversarial nations like Russia and the People’s Republic of China (PRC) while ensuring the nation can keep itself rolling technologically if those rivals — China in particular — become adversarial.



▲ Army cyber security experts check the status of an Army network. Army photo



Naval Information Warfare Center Pacific's warehouse manager Paul Cox and lead logistician Sara Singer-Seviern inventory outbound information systems equipment. Navy photo

Security priorities

The NSS document notes that “Our starting premise is that a powerful U.S. military helps advance and safeguard vital U.S. national interests by backstopping diplomacy, confronting aggression, deterring conflict, projecting strength, and protecting the American people and their economic interests. Amid intensifying competition, the military’s role is to maintain and gain warfighting advantages while limiting those of our competitors. The military will act urgently to sustain and strengthen deterrence, with the PRC as its pacing challenge. We will make disciplined choices regarding our national defense and focus our attention on the military’s primary responsibilities: to defend the homeland, and deter attacks and aggression against the United States, our allies and partners, while being prepared to fight and win the Nation’s wars should diplomacy and deterrence fail.”

The PRC looms large in President Biden’s NSS, as the document says that China is the “only competitor” in the world with both the intent and power to reshape the international order.

“Beijing has ambitions to create an enhanced sphere of influence in the Indo-Pacific and to become the world’s leading power,” the NSS says. “[China] is using its technological capacity and increasing influence over international institutions to create more permissive conditions for its own authoritarian model, and to mold global technology use and norms to privilege its interests and values. Beijing frequently uses its economic power to coerce countries. It benefits from the openness of the international economy while limiting access to its domestic market, and it seeks to make the world more dependent on the PRC while reducing its own dependence on the world.”

Pillars of security

The 2018 U.S. Department of Defense (DOD) cyber strategy embraced Benjamin Franklin’s “ounce of prevention” as the military intended to help all networks, including those outside the branch, when malicious attacks happened; update critical infrastructure networks; and streamline public-private information sharing.

“We can’t do this mission alone,” wrote the DOD. “So, the DOD must expand its cyber-cooperation by:

- building dependable partnerships with private-sector entities who are vital to helping support military operations;
- sharing information with other federal agencies, our own agencies, and foreign partners and allies who have advanced cyber capabilities. This will increase effectiveness;
- looking for crowdsourcing opportunities such as hack-a-thons and bug bounties to identify and fix our own vulnerabilities; and
- upholding cyberspace behavioral norms during peacetime.

“I think we’ve thwarted a good number of attacks by our intelligence sharing and your sharing of information about things going on in your network,” David McKeown, DOD’s chief information security officer and deputy chief information officer for cyber security told their industrial/commercial partners at a March 2022 town hall.

Trust issues

One way industry and the DOD are keeping defense and industrial secrets under wraps is to embrace a “zero trust” environment with networked systems. In August, DOD acting deputy chief information officer Lily Zeleske spoke at an industry event



RF Connectors Ready to Ship!

Your One Source for RF Connectors

Pasternack RF connectors are built in male, female, plug, jack, receptacle or sexless gender, in 50 Ohm or 75 Ohm Impedance and in standard polarity, reverse polarity or reverse thread designs. Our radio frequency connectors are available in quick disconnect (QD), push-on or standard interfaces, as well as straight, radius right angle or right angle versions. We offer RF connectors with standard and precision performance levels constructed with brass or stainless steel bodies. Other RF connector options include hermetic, bulkhead, 2 hole panel or 4 hole panel configurations.

Place your order by 6 PM CT, and have your connectors or any other components shipped today.



hosted by Worldwide Technology and Intel, where she noted an enterprise modernization approach is a priority.

“Our ability to deliver information at resilience and speed, as well as [delivering] secure information to our people, is paramount to staying ahead of adversaries,” Zeleske said, and noted that funding the technologies within budget constraints achieves a balance between cost and mission effectiveness. “We’re working for the public and for the country. I emphasize that resources and costs are critical, but the mission is just as critical, so it is a balance between cost effectiveness and mission effectiveness for us.”

One way to make commercial IT components and systems secure from state actors who can buy them off the shelf and probe for vulnerabilities is to embrace a “zero trust” strategy. Zero trust architecture (ZTA) removes the implicit trust that a user should get access to the system solely because they, for example, know the correct passcode. The DOD has set a target of 2027 to implement ZTA across itself and its services, according to Richard Jaenicke, who is the marketing manager of Green Hills Software (GHS) in Santa Barbara, Calif.

“Zero trust assumes your perimeter and networks have been breached and implements a high-level policy to ‘never trust, always verify,’” Jaenicke says. “In an enterprise setting, that includes continuous validation of users and devices. In embedded systems, zero trust includes not implicitly trusting each application but limiting access and communication to the least privilege necessary to get the job done.

He continues, “A proven security solution that provides the foundation for a ZTA in an embedded system is a separation kernel, where applications run in partitions isolated by the separation kernel. A separation kernel is very small in size because it implements only the four fundamental security policies required to support higher security functionality running in user mode. Those four security policies are data isolation, control of information flow, resource sanitization, and fault isolation. A separation kernel uses a static configuration file to define permitted applications and communications patterns



Naval Information Warfare Systems Center engineers check a fleet-bound OE570D UHF antenna onboard Naval Information Warfare Systems Command's Old Town San Diego campus. Navy photo



The Air Force IT and Cyberpower Education and Training event took place in Montgomery, Ala. in August. Military and industry collaboration is instrumental in achieving cyber security goals, industry experts say. Air Force photo

using the principle of least privilege. Because the separation kernel is the only software running in kernel mode, it cannot be bypassed or tampered with. The small size enables it to be scrutinized and evaluated to the highest security levels.”

Jaenicke explains that to achieve zero trust, the separation kernel needs to load properly. “That requires establishing a chain of trust back to a hardware root of trust, where each link in the chain authenticates the next piece of software before loading it.”

The NSA-defined Separation Kernel Protection Profile (SKPP) provides the security assurance and security functional requirements for a separation kernel to meet their definition of high robustness. That protection profile is based on a mix of Common Criteria objectives from Evaluation Assurance Levels (EAL) 6 and 7, with EAL 7 being the highest level.

At the system level, Raise the Bar (RTB) is a set of cyber security standards published by the National Cross Domain Strategy and Management Office (NCDSMO) in the NSA. First published in 2018, the RTB standards are a set of security guidelines and requirements for cross domain solutions (CDS) deployed by the U.S. government to protect National Security Systems (NSS). The RTB standards go well beyond the Risk Management Framework (RMF) controls that many government agencies implement. RTB standards ensure systems are at low risk of failing, even under persistent attack.”

Scott Miller, a scientist with Mercury Systems in Andover, Mass., explains that by seeking out potential vulnerabilities, it is possible to not only eliminate them, but utilize them to send enemies on something of a digital snipe hunt.

“The increase in connected technologies definitely presents new cyber security challenges, but there are ways to identify the exploitable vulnerabilities,” Mercury’s Miller says. “Although not encouraged as a primary strategy, ‘security through obscurity’

can mitigate risk as a secondary one, if it is thought that code may bear vulnerabilities. This strategy requires a careful balance, though, as broad exposure is often the most effective path to discovery and remediation of vulnerabilities.

Miller continues, “The controversial strategy of employing disinformation, where software systems intentionally misreport their configuration, can be effective in confounding adversaries who are selecting attacks know to be effective against particular software versions or configurations. But it can also confound patching and maintenance efforts to make the right decisions contrary to what the software self-reports.”

Limitations in trust

While the “zero trust” movement gains traction in the DOD and its industry partners. Dominic Perez, the chief technology officer (CTO) for Curtiss-Wright Defense Solutions in Ashburn, Va., explains that the concept is less a panacea for cyber security — it’s more an architecture.

On top of that, Perez says that even the name is somewhat of a misnomer, as “the first thing you’re doing is establishing trust, and what you’re doing is reestablishing trust whenever certain

attributes of the communication session or the user change or appear to have changed. And I think most people have encountered something like this; you get a new phone and you log on to your bank’s website and it asks you those security questions that it probably hasn’t asked you for many months because it has noticed something different about this session.

“I think people should just caution that zero trust is going to solve all of their security problems,” he continues. “It is a powerful tool and a powerful concept, and we have lots of partners that enable various pieces of the zero-trust ecosystem like Cisco and Aruba and Palo Alto, but it’s not going to by itself solve all of your security issues.”

On the move

Like the commercial off-the-shelf (COTS) revolution that has fueled field-replicable and upgradable hardware components, the National Security Agency (NSA) looked to commercial solutions for cyber security. The NSA’s Commercial Solutions for Classified (CSfC) program allows agencies and military services to communicate securely using a diverse set of commercial products.

NSA experts say the CSfC program provides NSA designed and approved solutions, leveraging a cadre of vetted, trusted

Functionally Sized and I/O Optimized

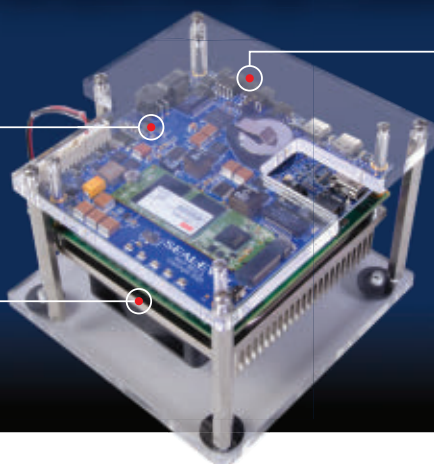
12009 COM Express Compact Type 6 Evaluation Board

ROBUST PROCESSING

- Designed for the congatec® conga-TC370 COM Express Family
- Support for 8th generation Intel® Core™ Processors

SMALLEST-IN-INDUSTRY COMPACT TYPE 6 FOOTPRINT

- 95mm x 95mm
- Identical in size to a Compact Type 6 COM Express Module



DIVERSE I/O MIX

- Gigabit Ethernet, USB 2.0/3.0
- Mini DisplayPort
- M.2 SATA SSD
- RS-232, UART, GPIO



Sealevel Systems, Inc. is the leader in COTS, full custom, and OEM hardware and software for critical communications. Wide-ranging industries and every major military contractor recognize Sealevel for our unmatched engineering expertise, world-class manufacturing, and customer satisfaction commitment.

Whether you want to leverage existing technology or create something entirely new—we’d love to set new standards. Together.

SEALEVEL
sealevel.com

Reliability, Availability, and Support Beyond the Life of Your Mission



A Marine Corps anti-tank missileman aims a Javelin shoulder-fired anti-tank missile aboard the Wasp-class amphibious assault ship USS Kearsarge (LHD 3). Navy photo

system integrators; NIAP-validated components; and collaborative protection profile requirements, validated against the international Common Criteria; enables clients to keep pace with technological progress; and employs the latest capabilities

The CSfC program also helps reduce the time it takes to build, evaluate, and deploy solutions by using mature technologies already available to the commercial sector. Potential cost savings may be realized through marketplace competition and rapidly deployable, scalable commercial products.

Other CSfC benefits include open, non-proprietary interoperability and security standards; situational awareness about components use and location, as well as documented incident handling procedures; and technical expertise NSA's team of system engineers, threat analysts, and cyber experts.

With the NSA's CSfC, Curtiss-Wright Defense Solutions' Perez says that warfighters — including those at the front lines — can use wireless technologies that civilians have taken for granted for decades now.

Cyber security was the impetus to keep DOD systems off the airwaves and keeping systems tethered together with Ethernet cables to allow information sharing between computers.

"From the advent of Wi-Fi at the tail end of the '90s until just a few years ago, no one in the military would be allowed to use WiFi," Perez points out. "But with the NSA CSfC program, we are able to deploy WiFi and other wireless commercial technologies like 4G LTE, and even 5G now in a secure manner. What that really does is it dramatically speeds-up the deployment of a secure network.

"In [Curtiss-Wright's] PacStar group, we are focused on enabling these forward operators — either in the tents that they're setting up or the vehicles that they're deploying with — to set up networks quickly," Perez continues. "Quickly' used to be measured in days then, now is in hours or less. They need to be able to set up a network when they come to a stop. And our secure wireless command post lets them do that. In less than a half an hour, they can have 100 users online, and they'd barely be getting open the boxes of Ethernet cabling if they were using a traditional cabling solution."

In addition to rapid deployment, Curtiss-Wright's Perez says that going wireless affords the DOD with significant cost savings as many of the miles of

Ethernet cable used in the field, which was rarely if ever reused, can be eliminated.

Reliability in redundancy

With Wi-Fi making use of radio frequency (RF) technology, all sorts of sensitive and classified information is flying through the air. How do the DOD and their industry partners keep it out of the hands of bad actors who wish to obtain it? In short, trustworthy hardware and redundancy in encryption.

Curtiss-Wright's Perez explains that redundancy is achieved by using multiple equipment manufacturers with different ways of encryption.

"So, let's just say one layer is a VPN developed by Cisco and another layer is a VPN developed by Aruba," Perez says. "By running the traffic between the first tunnel and then taking the tunnel traffic and running it through the second tunnel, they have prevented a lot of the vulnerabilities that might be present in just one of those solutions."

Perez's colleague Steve Edwards, who is Curtiss-Wright's director of secure embedded solutions, likened the redundancy to overlapping pieces of Swiss cheese.

"So, each of those solutions on their own have certain vulnerabilities, but because they're independently developed, they're going to have different vulnerabilities from each other," Edwards says. "And so the idea is you layer them on top of one another. It's like putting two pieces of Swiss cheese together. The holes don't line up, so you've actually reduced your vulnerability surface quite a bit by doing [this]."

The CWDS duo notes that in some instances, the NSA will grant certification from the same company so long as the systems were not co-developed the same way.

"There are a significant number of additional requirements in order to become registered with the NSA for one of these encryption solutions," CWDS' Perez explains. "However, the premise is the dual layer of encryption... [Our] persistent storage division has actually gone and gotten a waiver because we were able to show that our two layers are developed independently. So, the NSA says, 'OK, it says Curtiss-Wright on the box for both of them,' but one came from an internal development, and then one is an open source program that we manage and make it meet requirements. So, while the premise is that you need two different vendors, there are just a couple of waivers that the NSA has given out for that. And Curtiss-Wright has one of those."

Eyes on supplies

One way industry and the warfighters that use connected technology can get some peace of mind is by assuring their source for components and software aren't built with back doors built-in by countries and companies who may not be entirely trustworthy.

President Biden has made domestic chip and other technology manufacturing a priority in his first two years in office as a way to reduce dependency on overseas sources in the wake of the COVID-19 pandemic.

"The software cyber security problem is hard enough; but consider if you can't trust the hardware executing the software. This is why DARPA ERA and the CHIPS bill is so important — these seek to preclude the need to consider intentional manipulation of component hardware designs from which modules are composed," says Mecury's Miller. "However, much like social engineering produces an 'accidental insider,' accidental hardware vulnerabilities will remain a concern."

At a groundbreaking at a new Intel manufacturing facility in Ohio in September, President Biden noted that decades ago, the United States produced more than 30 percent of the world's computer chips. With much of its manufacturing needs sent overseas, Biden said that figure dropped to approximately 10 percent. The president also said that the shortage of semiconductors drove approximately one third of inflation.

The president told the Ohio crowd that in addition to Intel, Micron in Boise, Idaho; GlobalFoundries in Santa Clara, and

RUGGED HIGH PERFORMANCE DATA STORAGE*

AS 9100D / ISO 9001:2015 CERTIFIED



RPC16 NAS Magazine Based AFA

- 16 SSDs in 2U of rack height
- 10/40/100 GbE
- MIL-STD-810G and MIL-STD-461E Certified

Open VPX NVMe Data Storage Module

- Capacities to 30TB per module
- Transfer rates to 3.5GB/s read, 3.1GB/s write
- SOSA Aligned

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
- SOSA Aligned
- Vita48 REDI conduction cooled



* AES-256 Encryption and FIPS140-2 Validated



www.phenxint.com 714-283-4800

PHOENIX
INTERNATIONAL

WHO'S WHO IN TRUSTED COMPUTING

Amazon Web Services

Seattle
<https://aws.amazon.com>

CRU Data Security Group

Vancouver, Wash.
<https://cdsg.com>

**Curtiss-Wright Corp.
Defense Solutions**

Ashburn, Va.
<https://www.curtisswright.com/>

Green Hills Software

Santa Barbara, Calif.
<https://ghs.com/>

Intel Corp.

Santa Clara, Calif.
<https://www.intel.com/>

Microsoft Corp.

Redmond, Wash.
<https://www.microsoft.com/en-us/>

Northrop Grumman Corp.

Falls Church, Va.
<https://www.northropgrumman.com>

Shift5

Arlington, Va.
<https://www.shift5.io/>

Rinderer explains that a “Die Hard” scenario is unlikely to play out where a person or country gets control of a vehicle remotely and crash it.

“What I want to do is simply keep your entire fleet on the ground when you need it in the air,” Rinderer says, speaking as a hostile actor. “Or I want to stop an entire brigade of ground vehicles as soon as they roll across the boundary, invisible GPS boundary that represents my border. The way that

I’m going to do that, I’m going to do very

Qualcomm in San Diego, Calif.; and Wolfspeed in Durham, N.C. were investing billions into manufacturing chips at home for consumer goods.

The president also explained to the crowd that earlier in 2022, he had visited the Lockheed-Martin Javelin missile plant in Troy, Ala. Those missiles were among the materiel assistance the U.S. has provided to Ukraine as it battles an invasion by neighboring Russia.

“We need semiconductors not only for those Javelin missiles, but also for the weapons systems of the future that are only going to be more reliant on computer chips,” President Biden said. “This goes well beyond commercial need. Unfortunately, we produce zero — zero — of these advanced chips in America. Zero. And China is trying to move way ahead of us in manufacturing them.”

China has loomed large in the minds of security-minded professionals looking to prevent the Asian power from building exploitable weaknesses into hardware.

Emil Kheyfets, who is the director of mil-aero business development at Aitech in Chatsworth, Calif., explains that “It is a big concern, especially since infiltration can come from external and internal system resources. To highlight the magnitude of it, note that DoD programs prohibit the use of Chinese EEE parts to prevent internal infiltration. Protection of all external interfaces, as found in the [Aitech’s] AiSecure architecture, is crucial to combat infiltration of secure systems.”

Adversarial ambitions

Of course, keeping prying eyes off data is job number one, as Benjamin Franklin notes. But what happens if nations like China and Russia overcome physical security at sensitive sights, bypass physical barriers, or defeat cyber security systems? And if they do, what would an adversary seek to do with access to the sensitive systems that warfighters count on? According to E. Egon Rinderer, the CTO of Shift5 in Arlington, Va., it’s not what Hollywood puts on the screen.

sophisticated attacks that get me persistence on those platforms very quietly. And supply chain is a great way to do that. I can bake something in at a hardware level that’s completely hidden, isn’t doing anything. It’s completely dormant as well and it has some sort of wake-up effect at some point, which you may or may not ever see. But I need to be able to detect if that thing behaves differently than it should.”

Shift5 provides a system-monitoring platform in rail, defense, and aerospace vehicles that logs every “conversation” between components and flags abnormalities it discovers.

For instance, Rinderer provides an example where five vehicles in a fleet of 300 are flagged as having computing processes acting differently than the other 295. By finding commonalities between the “abnormal” vehicles, like they’re the only in the fleet that have had a particular component replaced with something new, it can be effectively audited down to the bus level to see if there’s been a security breach. In addition, Rinderer provides an example of vehicles traveling to a particular area known for attempts to break in to systems.

“Maybe those five vehicles all transit the Strait of Hormuz through a known offensive cyber operations hotspot,” says Shift5’s Rinderer. “And since coming back now they’re exhibiting that behavior they’re affected... We conduct what’s called full take data capture. I want every single frame of data that’s put on that bus by any device. So, we watch things passively at the bus level because it’s, number one, ubiquitous, and number two, it’s unobtrusive. And so, what I can do is I can say, okay, great, we’re watching everything. We detected this anomaly on these five vehicles ever since they transit in this area. Take me to the first occurrence of that anomaly, and then I want to see all the bus messages that led to that.” With an eye on supply chains, manufacturing, deployed systems — and the redundant systems that protect them — today’s cyber security experts are bringing more than an ounce of prevention to today’s technologies. With proactive monitoring, perhaps that “pound of cure” will come in a little lighter, too. ◀

Data storage making the transition to network-based systems

Network-attached secure data storage architectures not only can help warfighters get broad access to mission-critical data, but also help to keep data safe from hackers and other cyber security threats

BY John Keller

Rugged data storage technologies for aerospace and defense applications are making the transition from point-to-point interconnects to fast network-centric architectures that offer quicker data access to warfighters than they have today, and new shared-data applications such as artificial intelligence (AI) in intelligence gathering and retrieval.

Driving this trend to networked data storage are increases in network performance — particularly fast Ethernet — which is growing rapidly from 25 gigabits per second to 100 gigabits per second, and beyond.

“I’m seeing a move away from block-based direct-attached storage for external disk arrays,” says Amos Deacon III, president of data storage specialist Phoenix International Systems in Orange, Calif. “We see a lot of moving to file-level storage in the realm of network-attached storage.”

The switch to networked storage represents a fundamental shift away from industry stalwarts like Serial Attached SCSI (SAS), Serial ATA Attachment (SATA), and Fibre Channel connects to networked approaches that overwhelmingly rely on Ethernet, Deacon says.

“Traditionally we have had SAS and Fibre Channel connections in block based systems, and yet we are moving toward Ethernet for file-level data,” Deacon says. File level data transfer typically is used in Ethernet-based data storage systems that move data as packets. “There typically is a lot of overhead involved,” Deacon says.

This approach, while it has more overhead, is more simple to implement than other data-transfer approaches like Internet

Small Computer Systems Interface (iSCSI), Fibre Channel, or SAS. “It comes down to simplicity and access,” Deacon says. “More people can access it. Block level is a direct connect, and you have to be on that storage network to access it, while file level is a regular Ethernet network.”

The high performance of Ethernet networking also is overcoming traditional network overhead problems. “Historically, block level is a lot lower latency because of the overheads involved, but that is starting to overcome because of the performance on the

network-attached devices. Now we’re talking about 25-, 40-, and 100-Gigabit Ethernet. That’s giving the network attached devices much higher performance,” Deacon says. “A lot of that inherent latency goes away.”

Speed and performance can go a long way in new applications that involve AI. “Typically if you have a

real-time environment you would want that data transfer to happen instantaneously, especially in an AI environment where you need to make decisions based on the data as it comes in. That typically has been a block-based direct-connect environment,” Deacon says.

Is all that speed and performance really necessary in today’s aerospace and defense applications? Perhaps not today, but it will in the future. “The performance that is available now with 100 Gigabit Ethernet is more than what 90 percent of the people out there need,” Deacon points out. “There are specific applications that require super-high-speed capability, but I think it is the actual application that determines where that goes.”



▲ This DIGISTOR FIPS-certified self-encrypting solid-state drive has a tamper-evident coating for additional assurance of data integrity.

Today's high-performance data storage is seeing enhanced performance not only from Ethernet networking, but also because of Non-Volatile Memory Express, better-known as NVMe. "We are now seeing some of that change because of the performance that is now capable with the NVMe storage device," Deacon says. "In block-level storage you go through a host adapter for the CPU to talk to the storage, but with NVMe you don't have that intermediate step because the storage device talks directly to the CPU."

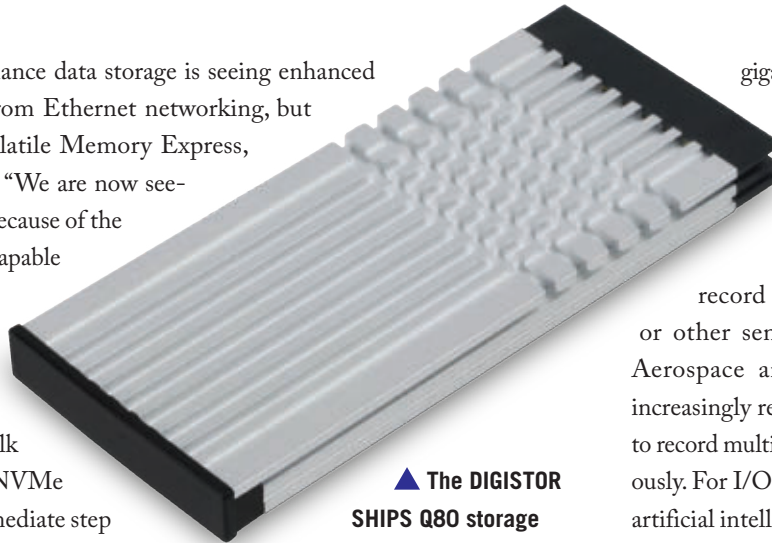
NVMe data storage

Solid-state storage media today overwhelmingly leans toward NVMe, where the biggest advantage is pure speed, which for the vast majority of systems designers outweighs NVMe's drawbacks in power consumption, thermal management, and ruggedization.

NVMe's speed is the biggest reason that it has surpassed in popularity other solid-state storage media such as Serial AT Attachment (SATA) and Serial Attached SCSI (SAS). SATA is a computer bus interface that connects host bus adapters to data storage devices like hard disk drives, optical drives, and solid-state drives.

NVMe typically is six times faster than SATA and SAS. Moreover, the NVMe design approach enables data storage media such as solid-state drives to access processors via the PCI Express databus, rather than through relatively slow specialized data storage interfaces. It also enables host hardware and software to capitalize on levels of parallelism possible in modern solid-state drives. NVMe essentially connects data storage directly to system processors, and avoids throughput bottlenecks of data storage interfaces.

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



▲ The DIGISTOR SHIPS Q80 storage module use NVMe technology to provide rugged removability for use in PCs, laptops, and other devices that need to store encrypted data securely.

gigabytes per second. One principle behind NVMe is switching from serial to parallel data interfaces to increase data throughput.

NVMe technology can record several streams of video or other sensor data simultaneously. Aerospace and defense applications increasingly rely on speed and the ability to record multiple data streams simultaneously. For I/O-intensive applications like artificial intelligence (AI) NVMe devices speed-up workflows.

The PCI Express interface for NVMe is gaining widespread popularity in aerospace and defense applications. NVMe data storage bypasses the SATA interface

and goes directly to PCI Express to boost throughput speeds.

In addition to its big advantages in speed, NVMe also is smaller than SATA and SAS, which lends itself to today's demands for small size and light weight in aerospace and defense systems. NVMe solid-state drives are much smaller than SATA drives and weigh about four times less, which makes them suitable not only for laptop computers, but also for size- and weight-sensitive military applications. In addition, systems designers can attach NVMe memory components directly to motherboards and single-board computers, which also can cut down on size and weight.

NVMe, however, has disadvantages for military and aerospace systems designers. Compared with its predecessors, SATA and SAS, NVMe is more expensive, more difficult to ruggedize, consumes more power, and can be a challenge to keep cool enough for maximum performance.

NVMe memory is not as rugged as SATA and SAS data storage, which can increase the challenge of packaging NVMe for mobile military applications that must operate in extreme temperatures, shock, and vibration.

One of the most serious weaknesses of

NVMe for rugged military applications is its relatively weak ability to operate in cold and hot temperatures. Compounding the picture is the relatively high power consumption of NVMe vs



▲ The DIGISTOR SHIPS QX448 ingestion frame, typically mounted in a PC or custom device, can house as many as four SHIPS modules in a standard 5.25-inch bay.

RF and Microwave Terminations IN-STOCK



Your One Source for RF & Microwave Terminations

RF terminations from Fairview Microwave are available with 1.0/2.3, 2.4mm, 2.92mm, 3.5mm, 7/16 DIN, BMA, BNC, MCX, Mini SMP, MMCX, N, QMA, SMA, SMB, SMC, SMP, SSMA, SSMC, TNC and UHF connectors. Fairview Microwave RF terminations include standard feed-thru load and rf load versions with male, female, jack and plug genders. Our coaxial terminations (also known as RF loads or Dummy loads) have some precision designs as well as models with chain and without chain and frequency range as high as 50 GHz.

Place your order by 6 PM CT, and have your terminations or any other components shipped today.

In Stock & Shipped Same-Day

fairviewmicrowave.com
+1 (800) 715-4396

 **Fairview Microwave®**
an INFINIT® brand

SATA and SAS storage media. More power consumption means generating more waste heat, which forces designers either to design-in cooling, or throttle-down the speed of the data storage to keep within temperature constraints.

Information security

In today's adversarial digital world, it matters less how quickly data can be stored and retrieved than it does how secure the data

can be kept from those who seek to steal it, corrupt it, or destroy it. That's where information security comes in.

Unfortunately some of today's cyber security technologies may not be up to the information security challenge where data storage is concerned.

"The data security model today is quite fractured, if not broken," says Chris Kruell, director of marketing, at the DIGISTOR brand of CRU Data Security Group in Vancouver,



▲ The Phoenix International VP1-250-eSSDC is a FIPS 140-2 validated encryption Open VPX NVM Express (NVMe) solid state disk data storage module that helps designers remove legacy layers of hard drive interfaces such as SATA and SAS.



▲ The Phoenix International Phalanx II is SWaP-optimized and provides high performance, high capacity, and secure data storage for unmanned aerial, underwater and surface vehicles and crewed intelligence and surveillance applications.

WHO'S WHO IN RUGGED DATA STORAGE

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

Annapolis Microsystems
Annapolis, Md.
<https://www.annapmicro.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, DIGISTOR
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.
Parsippany, N.J.
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

Smart Modular Technologies
Newark, Calif.
www.smartm.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>

Wash. “All these technologies are taking on a piece of the data security issue.”

Perhaps the most important aspect of information security for data storage is the so-called “zero-trust” concept, which requires all users — inside or outside the organization’s network — to be authenticated, authorized, and continuously validated before receiving access to applications and data. This approach, in other words, trusts no one, and assumes that cyber attacks could come from anywhere — especially from those inside the organization.

“Insider threats haven’t been a topic of conversation, even five years ago as much as it is today,” Kruell says. “It is basically saying you can’t trust anyone or anything, so you need to focus on locking down your data,” Kruell says. “We are seeing greater and greater adoption of a zero-trust philosophy.”

Although zero-trust may sound new, it’s actually been around for the past 10 or 15 years; it’s just now that it’s becoming widely known and accepted, Kruell says, explaining that it takes time for zero-trust to catch on — especially since this discipline is so demanding.

“It comes down to people and processes,” Kruell says. “Do people have the discipline to follow processes, and do you know that the guy in the cubicle beside you is not a threat? This was accelerated by cyber attacks that come from inside a network or physical perimeter; that attack has a good chance of succeeding. That threat could be anywhere, even next door.”

CRU Data Security specializes in self-encrypting data storage drives, and takes advantage of today’s high-speed data storage networking. “A lot of our devices go into aircraft that capture surveillance data,” Kruell says. “You can never capture or analyze data fast enough, and you always want a cocoon of security.”

To achieve that cocoon of security, CRU Data designs data drives according to 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 the U.S. National Institute of Standards and Technology (NIST) in Gaithersburg, Md.

Company engineers also used layered software to go alongside FIPS-certified drives to enhance security. “Our customers are asking for additional cyber security functions beyond the drive itself,” Kruell says. “In this market, self-encrypting drives are table stakes.”

CRU Data also is pursuing secure data storage that meets guidelines of the National Security Agency (NSA) Common Criteria for Information Technology Security Evaluation, administered by the NSA’s National Information Assurance Partnership (NIAP). Common Criteria certification also is one of the first



▲ The Phoenix International RPC6 rugged network-attached storage server can help the military capitalize on the deluge of data generated by intelligent, connected devices.

steps toward implementing the NSA’s Commercial Solutions for Classified (CSfC) two-layer encryption for protecting classified information in aerospace and defense applications.

CRU Data doesn’t yet offer a security data storage device that meets all the guidelines of CSfC, but Kruell says he wouldn’t be surprised” to see the company offer a full CSfC solution in the near future. ←

6-Channel Discrete-to-Digital Sensor with Galvanic Isolation



Sense Analog Voltages in 5V and 28V Aircraft Systems

- Galvanically isolated GND/Open discrete-to-digital sensor
- Airbus ABD0100H specification compliant
- 400V galvanic isolation between digital and analog interfaces
- Two sensing modes for 5V and 28V systems
- Supports 28V analog supply
- DISCONNECT digital output signal indicates all sense input lines are “Open”

HOLT
INTEGRATED CIRCUITS

For further information on these and other Holt products contact:
(949) 859-8800 • sales@holtic.com • www.holtic.com
AS9100D: 2016 Registered



Air Force installs EPAWSS electronic warfare (EW) aboard F-15E combat aircraft

BY John Keller

SAN ANTONIO – Military avionics experts from the Boeing Co. have begun installing an advanced electronic warfare (EW) system on the U.S. Air Force fleet of F-15E jet fighter-bomber aircraft.

The Air Force supervised the first installations of the F-15 Eagle Passive/Active Warning and Survivability System (EPAWSS) on operational F-15E aircraft in July at the Boeing facility in San Antonio.

Boeing previously installed EPAWSS hardware on eight test F-15 combat aircraft and is installing the system on the new F-15EX aircraft at the Boeing production facility in St. Louis.

F-15 EPAWSS replaces an analog, federated system with a next-generation, digital, integrated EW suite that enables the F-15 to operate in a modern threat environment with dense radio-frequency backgrounds.

The updated EW avionics improves pilot situational awareness with the capability to autonomously detect, identify, and locate threat systems, and then deny, degrade, and disrupt those threats.

▲ **EPAWSS replaces an analog, federated system with a digital EW suite that enables the F-15 to operate amid modern threats with dense radio-frequency backgrounds.**

Boeing manufactures the F-15 and serves as the integrator for the program, and BAE Systems is producing the advanced EW hardware.

In 2021 and 2022, the program team delivered six iterations of mission system software, conducted 12 major ground test events, participated in three open air range events/exercises, and flew 1,521 hours in flight test, all while standing up the modification line in San Antonio and building up sustainment capabilities.

In addition to maturing system performance, over the past 18 months the combined government-industry program team completed final development and qualification of the EW hardware, ensuring the system meets reliability and maintainability metrics, laying the foundation for long-term system sustainment.

EPAWSS increases the aircrew's situational awareness, helps them understand when they are being targeted by radar, and it provides them with advanced techniques to counter modern integrated air defense systems. ◀

Navy looks to next-gen destroyer with electromagnetic weapons and integrated power

BY John Keller

WASHINGTON – U.S. Navy surface warfare experts are taking another step toward building a next-generation guided-missile destroyer eventually to replace the Ticonderoga-class (CG 47) cruisers and early model Arleigh Burke-class (DDG 51) destroyers.

Officials of the Naval Sea Systems Command in Washington have announced contracts of undisclosed value to two U.S. military shipbuilders for preliminary design of the future Guided Missile Destroyer now known as DDG(X).

Contracts went to General Dynamics Bath Iron Works in Bath, Maine, and to Huntington Ingalls Inc. in Pascagoula, Miss., to carry out preliminary design work for the future DDG(X) surface warship. The value of the contracts was not released because it is competition-sensitive.

Navy leaders say they want to procure the first DDG(X) in 2030, and add the new ship to the fleet as early as 2034. Procurement of Burke-class destroyers would end sometime after 2030. The Navy approved the DDG(X) major features in December 2020.

Navy officials envision the DDG(X) as displacing about 12,700 tons, which would make it larger than the 9,700-ton Flight III Burke-class destroyer and 9,600-ton Ticonderoga-class cruiser, yet smaller than the 15,700-ton Zumwalt-class (DDG 1000) land-attack destroyer.



The next-generation Navy destroyer is expected to have electromagnetic weapons, high-energy lasers, and an advanced integrated power system.

The new ship also will have a mid-body hull section called the Destroyer Payload Module to provide additional payload capacity. Future capabilities could include laser and electromagnetic weapons; hypersonic missiles; and advanced sensors.

At roughly 12,700 tons, the DDG(X) would be close to the size of the 1970s-vintage Virginia-class cruiser, or World War II-era Boston-class cruiser. The ship would be about half the size of the massive Russian Kirov-class battle cruiser.

Navy leaders speculate that the DDG(X), compared to late-model Burke-class destroyers, will have more space, weight-carrying capacity, room for growth; higher-power equipment; reduced infrared, acoustic, and underwater electromagnetic signatures; increased range; and increased weapons capacity.

The new ship also will have elements of the Flight III Burke-class destroyer Aegis combat system, enhance electrical power and cooling capacity, and an integrated power system.

The DDG(X) will have 96 standard Vertical Launch System (VLS) cells, with an ability to incorporate 12 large missile-launch cells in place of 32 of the 96 standard VLS cells, and will include two 21-cell Rolling Airframe Missile (RAM) launchers.

Navy leaders have not specified how many DDG(X) surface warships they want to buy, yet by 2031 could buy as many as three additional ships each year. The ship should cost between \$3.5 billion and \$4 billion to build.

On these preliminary studies contracts, Bath Iron Works will do the work in Bath and Brunswick, Maine, and in Washington, D.C. Huntington Ingalls will do the work in Pascagoula, Miss.; Avondale, La.; and Newport News, Va. Both companies should be finished by July 2023. ◀

For more information contact Bath Iron Works online at <https://gdbiw.com>, Huntington Ingalls at <https://huntingtoningalls.com>, or Naval Sea Systems Command at www.navsea.navy.mil.

Wanted: real-time oscilloscope to detect and analyze electromagnetic warfare signals

BY John Keller

WRIGHT-PATTERSON AFB, Ohio – U.S. Air Force electromagnetic warfare experts have reached out to industry to find companies able to provide a real-time oscilloscope to detect and evaluate electromagnetic threats.

Officials of the Air Force Research Laboratory (AFRL) at Wright-Patterson Air Force Base issued a sources-sought notice in late September (SS-AFRL-PZLEQ-2022-0011) for the Real-Time Oscilloscope project.

This test instrument must offer bandwidth of at least 50 GHz; data acquisition rate per channel of at least 256 gigasamples per second; four independent channels; configurable millimeter-wave extension window of less than or equal to 10 GHz; DDC bandwidth of at least 2 GHz; ability to provide vector signal analysis and pulse signal analysis; onboard memory of at least 5 gigapoints per channel; ability to provide de-embedding; and five-year warranty.

The oscilloscope must support software modules and a specialty transit case with pulse signal analysis and vector signal analysis capability.

Electromagnetic warfare uses aimed electrical and magnetic energy to destroy or disable critical enemy electronics for navigation and guidance, computing, communications, displays, timing, sensors, and many other military applications. Typical electromagnetic weapons use high-power microwaves.

Experts have determined they can mitigate many new electromagnetic threats by moving to ultra-short pulse lengths. This presents the need to characterize these ultra-fast pulses with a high degree of sampling fidelity, Air Force experts say.

Data acquisition rate capabilities over the past decade, however, have limited data fidelity. The threshold for measuring these ultra-fast rise time events requires a sampling rate that has become commercially available.

Previous efforts have relied on the perfect reproduction of the threat pulse for several times and then sampling several pulses and interpolating the data to enable Air Force researchers to measure a single pulse directly and not rely on reproducing an ultra-short pulse for 10 times, which is not able to be verified.

This will help researchers measure the threat pulse and resulting performance simultaneously over the oscilloscope's four ports. This would represent a unique cutting-edge capability for the Air Force Research Laboratory, experts say. ◀

Companies were asked to respond by early October. Email questions or concerns to jacob.britt.4@us.af.mil, with "Real-Time Oscilloscope Requirement" in the subject line. More information is online at <https://sam.gov/opp/c59ebe75203e411b8e27807b3113775c/view>.



The Air Force is looking for a real-time oscilloscope to detect and evaluate electromagnetic threats, which must support software modules and a specialty transit case with pulse signal analysis and vector signal analysis capability.

Northrop Grumman to build 13 AN/APG-83 AESA radar systems for F-16 jet fighter

U.S. Air Force aerial radar experts are ordering 13 modern active electronically scanned array (AESA) radar systems for the F-16 jet fighter under terms of a \$25.4 million order. Officials of the Air Force Life Cycle Management Center, Fighter Bomber Directorate, F-16 Division, at Wright Patterson Air Force Base, Ohio, are asking the Northrop Grumman Corp. Mission Systems segment in Linthicum Heights, Md., to build 13 AN/APG-83 AESA radar systems and spare parts for the F-16. The APG-83 AESA fire-control scalable agile-beam radar (SABR) integrates within the F-16's structural, power, and cooling constraints without Group A aircraft modification, Northrop Grumman officials say. The company leverages technology developed for the APG-77 and APG-81 radar systems on the U.S. F-22 and F-35 combat aircraft. In a 2013 competition, Lockheed Martin Corp., the F-16 manufacturer, selected the APG-83 as the AESA radar for the F-16 modernization and update programs of the U.S. and Taiwan air forces. The bandwidth, speed, and agility of AESA radar systems enable legacy fighter aircraft like the F-16 to detect, track, and identify many targets quickly and at long ranges, and to operate in hostile electronic warfare (EW) environments. Northrop Grumman is building APG-83 radar systems for global F-16 upgrades and new aircraft production, as well as for the U.S. Air National Guard. Northrop Grumman also has installed a production APG-83 SABR on a U.S. Marine Corps F/A-18C Hornet jet fighter-bomber, company officials say. On this order Northrop Grumman will do the work in Linthicum Heights, Md., and should be finished by July 2025. For more information contact Northrop Grumman Mission Systems online at www.northropgrumman.com, or the Air Force Life Cycle Management Center at www.afclmc.af.mil.

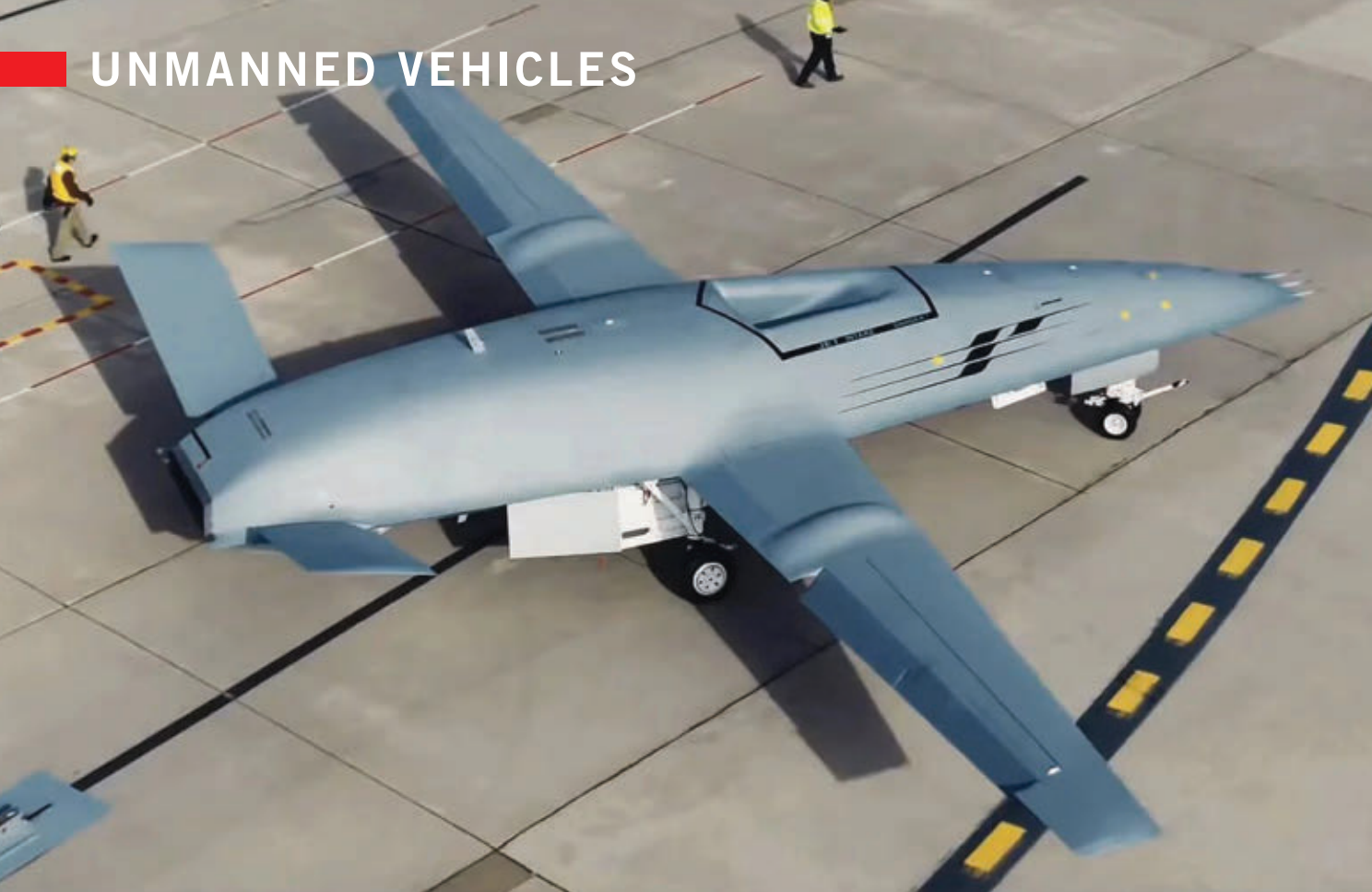
Solid-state power amplifier for X-band radar introduced by Comtech PST

Comtech PST Corp. in Melville, N.Y., is introducing the model BHCDP928978-4000 solid-state power amplifier for ground and surface X-Band radar applications. The AB linear power electronics device operates over a 9.2-to-9.7-GHz frequency range over an instantaneous bandwidth of 500 MHz, and is for a traveling wave tube (TWT) replacement. The amplifier design features self protection for load voltage standing wave ratio (VSWR), duty factor, pulse width, temperature, and graceful degradation in case of a RF power module failure. A mean time between failures (MTBF) increase of 10 times that of a the TWT helps improved reliability and lower maintenance costs. Comtech supports custom configurations for power levels as

high as 16 kilowatts. The radar power amplifier offers output power of 4,000 Watts peak; power gain of 66 decibels nominal; pulse width of 40 microseconds typical; pulse rise and fall time of 20 nanoseconds typical; input VSWR of less than 1.5 to 1; and harmonics of -60 decibels relative to the carrier (dBc). The power electronics device operates in temperatures from 0 to 50 degrees Celsius at the baseplate; works in humidity as high as 95 percent; meets MIL-STD-810F for resistance to the effects of shock and vibration; works at altitudes as high as 10,000 feet; uses RJ-45 Ethernet as its control interface; and uses SMA RF connectors. The unit measures 19 by 17 by 7 inches, and weighs 60 pounds. For more information contact Comtech PST online at <http://comtechpst.com>.

Raytheon to provide F/A-18 combat jets with open-systems AN/APG-79 radar

Radar experts at Raytheon Technologies Corp. will provide the U.S. Navy with six AN/APG-79 active electronically scanned array (AESA) airborne radar weapon repairable assemblies under terms of a \$36.5 million order. Officials of the U.S. Naval Supply Systems Command Weapon Systems Support activity in Philadelphia are asking the Raytheon Intelligence & Space segment in El Segundo, Calif., for AESA radar weapon repairable assemblies (WRAs) in support of the F/A-18 Hornet carrier-based jet fighter-bomber. 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 provides aircrew situational awareness, near-instantaneous track updates, and multi-target tracking capability. 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 airborne radar uses transmit/receive (TR) modules populated with gallium arsenide (GaAs) monolithic microwave integrated circuits (MMICs). The radar's active electronic beam scanning helps steer the radar beam 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. On this order Raytheon will do the work in Forest, Miss., and should be finished by May 2026. For more information contact Raytheon Intelligence & Space online at www.raytheonintelligenceand-space.com, or the Naval Supply Systems Command Weapon Systems Support activity-Philadelphia at www.navsup.navy.mil/NAVSUP-Enterprise/NAVSUP-Weapon-Systems-Support. ◀



Boeing starts producing MQ-25 Stingray unmanned tanker aircraft for carrier operations

BY John Keller

PATUXENT RIVER NAS, Md. — U.S. Navy carrier aviation experts are ordering unmanned aerial tankers from the Boeing Co. in preparation for future larger orders and eventual carrier deployment of these unmanned tanker aircraft.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., announced an \$47.5 million order to the Boeing Co. Defense, Space & Security segment in St. Louis in late September for MQ-25 Stingray low-rate initial production lot 1 for the U.S. Navy.

▲ **The MQ-25 will provide aircraft carrier-based unmanned refueling capability to extend the combat range of combat aircraft deployed at sea.**

The MQ-25 aerial refueling tanker is the U.S. Navy's first operational carrier-based unmanned aircraft and is designed to provide a much-needed refueling capability, Boeing officials say. Navy officials expect to declare MQ-25 initial operational capability by 2024.

The MQ-25 first flew last fall.

The MQ-25 will provide aircraft carrier-based refueling capability to extend the combat range of deployed F/A-18 Super Hornet, EA-18G Growler, and Lockheed Martin F-35C combat aircraft.

Boeing won a \$805 million development contract to build four MQ-25 carrier-based unmanned aerial tankers in 2018, prevailing over competing designs built by General Atomics in San Diego and the Northrop Grumman Corp. Aeronautics Systems segment in Palmdale, Calif.

The Boeing MQ-25 aircraft has an advanced, customized remote I/O interface controller based from Aitech Defense Systems Inc. in Chatsworth, Calif. The system is based on the Aitech Ai-RIO avionics remote interface.

The Ai-RIO is expandable with as many as eight units networked together. Added capabilities include I/O, power switching, and mass/SD FLASH memory. The remote I/O subsystem includes a Gigabit Ethernet port with precision time sync IEEE-1588 support, 10 RS-422 ports, eight LVDS or RS-422/485 UARTS, four SpaceWire ports with LVDS I/O, two CANbus ports, and 16 GPIO in two blocks of eight.

The Ai-RIO is an high density, low power rugged subsystem for vehicle platform flight control, attitude and navigation controls, servo-valve and thrust vector control (TVC), robotic motor control, video and image processing and storage, data telemetry, platform stabilization, communications and telematics, high speed data recorders, booster and launch propulsion and thruster control, remote sensor and effector monitoring.

Boeing can use the Ai-RIO as a stand-alone command and data handling platform or networked remote command/response I/O unit. It a radiation-qualified dual-core PowerPC processor with two rad-tolerant FPGAs. All internal electronics are conduction-cooled and mechanically fixed and housed within a sealed, EMI/EMC Faraday cage for maximum thermal transfer.

In addition to Aitech, other subcontractors to Boeing on the MQ-25 project are; BAE Systems; Collins Aerospace; Cox & Co.; Crane Aerospace & Electronics; Cubic; Curtiss-Wright Defense Solutions; General Electric Corp.; L3Harris Technologies; Héroux-Devtek; Honeywell International; Innovative Power Solutions; Moog Aircraft Group; Parker Hannifin; Raytheon; Rolls-Royce; and Triumph Group.

On this order Boeing will do the work in Torrance, Burbank, and Chatsworth, Calif.; McKinney, Texas; St. Louis; Longueuil, Quebec; Palm Bay, Fla.; Indianapolis; Ajax, Ontario; Wayne, N.J.; and Farmingdale, N.Y., and should be finished by September 2026. ←

For more information contact Boeing Defense, Space & Security online at www.boeing.com/company/about-bds, or Naval Air Systems Command at www.navair.navy.mil.

Rugged midwave infrared imaging camera introduced by Teledyne FLIR

Teledyne FLIR in Goleta, Calif., is introducing the Neutrino LC CZ 15-300 midwave infrared (MWIR) camera modules for airborne, unmanned, counter-unmanned, security, intelligence, reconnaissance, and targeting applications. These midwave infrared cameras have integrated continuous-zoom lenses, and are for integrated solutions that require crisp long-range imaging with benefits in size, weight, power, and cost (SWaP-C). Based on Teledyne FLIR HOT FPA technology, the rugged Neutrino LC CZ 15-300 offers high performance, 640-by-512-pixel HD MWIR imagery and 15-to-300-millimeter continuous-zoom. The long-life FL-100 linear cryocooler drives reliable operation. All Neutrino IS products include a Teledyne FLIR continuous-zoom lens integrated with a Neutrino SWaP series camera module (VGA or SXGA). The camera module and lens are designed for each other. Teledyne FLIR also provides technical services. All Neutrino series are classified under U.S. Department of Commerce jurisdiction as EAR 6A003.b.4. and are not subject to International Traffic in Arms Regulations (ITAR). For more information contact Teledyne FLIR online at www.flir.com.

Electro-optical modules for machine vision in robotics introduced by Teledyne e2v

Teledyne e2v, a Teledyne Technologies company in Grenoble, France, is introducing the 2-Megapixel Optimom MIPI CSI-2 optical modules for embedded systems with machine vision like robotics, logistics, drones, and laboratory equipment. Optimom 2M features a native MIPI CSI-2 protocol and standard FPC connector to link with embedded computing boards. Integration is instant using a dedicated development kit that includes an adapter board for hardware integration and Linux drivers for software integration with NVIDIA Jetson or NXP i.MX processors. These electro-optical modules are built with a compact 25-millimeter square outline in one mechanical design that can fit into constrained mechanical systems. Designers of machine vision systems can tailor Optimom 2M for several scenarios with two color options in monochrome or RGB, and three lens options: a multi-focus lens, a fixed-focus lens, and no lens. All Optimom 2M models are powered by Teledyne e2v's 2-megapixel low-noise global shutter image sensor that provides sharp images of fast-moving objects. The multi-focus version combines a broad working distance and wide aperture in one solution with focus adjustment technology. For more information contact Teledyne e2v online at www.teledyne-e2v.com.

Navy picks Hydronalix for micro unmanned aircraft, boats, and sensors research in explosives detection

BY John Keller

LAKEHURST, N.J. – U.S. Navy unmanned vehicles experts needed a company to integrate micro unmanned vehicles with sensor payloads for surveillance and enemy explosives detection. They found their solution from Hydronalix Inc. in Green Valley, Ariz.

Officials of the Naval Air Warfare Center Aircraft Division in Lakehurst, N.J., announced a \$9.1 million order to Green Valley in September for research into a variety of small unmanned aerial vehicles (UAVs) and unmanned surface vessels (USVs).

Some of this micro unmanned aircraft and boat technologies will be for explosive ordnance neutralization in harbors, rivers, and in shallow coastal waters for the U.S. Marine Corps.

Other potential applications of these micro unmanned vehicles are compact, lightweight autonomous underwater vehicle (AUV) with robust navigation and range for riverine reconnaissance; additive manufacturing for sonobuoy applications; swarming unmanned vehicles for humanitarian assistance and disaster relief; efficient propellers for small unmanned vessels; and expeditionary maritime mine countermeasures.

Hydronalix experts will handle sensors integration, control software, and communications systems for micro-unmanned surface and aerial vessels.

Sponsors of this contract include the U.S. Navy, U.S. Marine Corps, U.S. Defense Advanced Research Projects Agency (DARPA); and the National Oceanic and Atmospheric Administration (NOAA).

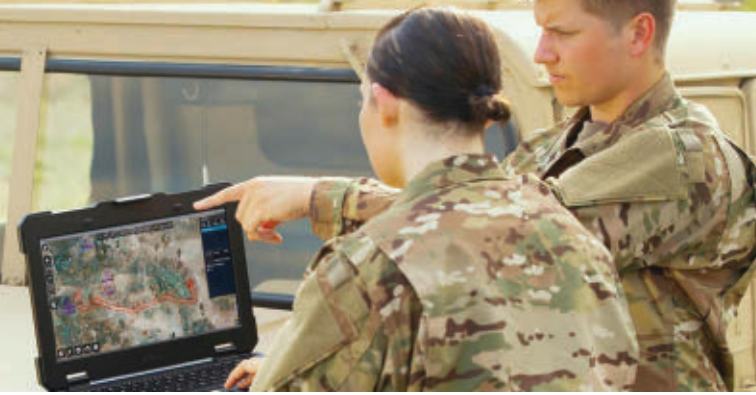
Hydronalix specializes in extreme-performance small unmanned vehicles, for water and air, and offers advanced research and development; design and prototyping; and test and evaluation. Founded in 2009, the company is known for robotic water rescue systems and advanced USVs using composite and ceramic materials.

The company also designs energy-efficient propulsion systems for long-duration missions with high dash speeds. The unmanned systems are man-portable and designed for easy operations, field maintenance, service, and repair. Hydronalix also offers expertise with integrating sensors and communication payloads on UAVs and USVs. ←



Hydronalix Inc. in Green Valley, Ariz., will investigate new generations of micro unmanned marine vehicles and sensor payloads.

On this order Hydronalix will do the work in Green Valley, Ariz., and should be finished by September 2026. For more information contact Hydronalix online at www.hydronalix.com, or the Naval Air Warfare Center Aircraft Division-Lakehurst at www.navair.navy.mil/lakehurst.



Industry briefed on artificial intelligence (AI), sensors, and autonomy program

BY John Keller

ARLINGTON, Va. – U.S. military researchers briefed industry last month on an upcoming project to develop new kinds of artificial intelligence (AI) and machine autonomy for battle management and sensor fusion in the Artificial Intelligence Reinforcements (AIR) project.

The DARPA AIR initiative seeks to fill gaps in research on developing and deploying tactical autonomy capability in real-world military operations.

AIR will focus on previously avoided dimensions to enable tactical autonomy in integrated sensors, scalability to large engagements, adaptability to changing conditions, and the ability to learn predictive models that incorporate uncertain knowledge of adversary and self, as well as deceptive effects.

AIR will pair existing, maturing, and emerging algorithmic approaches with expert human feedback to evolve the cooperative autonomous behaviors rapidly that solve previously avoided challenges.

AIR will address two technical areas: creating fast and accurate models that capture uncertainty and automatically improve with more data; and developing AI-driven algorithmic approaches to real-time distributed autonomous tactical execution within uncertain, dynamic, and complex operational environments. ◀

The AIR program also will develop ways to design, test, and implement future iterations of AIR software. Email questions or concerns to Lt. Col. Ryan Hebron at DARPA-SN-23-06@darpa.mil. More information is online at <https://sam.gov/opp/1b972abff6de4a2fbf7999af316e52c0/view>.

▲ **The DARPA Air program focuses on artificial intelligence and machine autonomy for future autonomous vehicles sensor fusion and battle management.**

'Innervating' smaller, smarter, safer ... and bluer robots and drones

To Innervate means to “put the nerves into” something. In humans, nerves are a key part of the nervous system, which also includes the brain and spinal cord. This system has three overlapping functions: sensory input (receiving information, processing and interpreting it), integration (extracting information and sending it out for an appropriate response), and motor output (initiating a response), writes Col. (Ret.) Retired Air Force Col. Dawn Zoldi writes. “ModalAI’s VOXL 2, when integrated with Doodle Labs’ Smart Radios, provides end-to-end innervation for uncrewed aircraft vehicles (UAVs) or drones, uncrewed ground vehicles (UGVs), autonomous mobile robots (AMRs) and other mobile robotics,” Zoldi writes. “A recent collaboration between these two Defense Innovation Unit (DIU) Blue UAS Framework companies has accelerated the development of smaller, smarter, and safer... and Bluer drones.” Zoldi also notes that “An integrated solution that combines VOXL 2 with the Helix Smart Radio provides the best of all worlds to developers - especially those desiring their platforms to stay NDAA-compliant. This powerful combination of cyber-secure and trusted technology provides developers with the simplification and consolidation they need. Integrating this proven tech into hardware solutions will accelerate development timelines to bring the smallest, smartest, safest and Bluest drones to market sooner.”

Trade show for 3D and airborne technologies set for February in Denver

Geo Week is the event for increased integration between the built environment, advanced airborne/terrestrial technologies, and commercial 3D technologies, bringing together former stand-alone events AEC Next Technology Expo & Conference, International Lidar Mapping Forum, and SPAR 3D Expo & Conference, and powerful partnership events including ASPRS Annual Conference, MAPPS Annual Conference and USIBD Annual Symposium. This year’s Geo Week expo will be Feb. 13 to 15, 2023 at the Colorado Convention Center & Hyatt Regency Denver at 700 14th St. in Denver, Colo. Attendees will get hands-on with technologies that provide data for understanding the world around us, to create more efficient workflows, and aid in decision making based on real-world data. Geo Week exhibitors include leaders in laser scanning, lidar, and reality capture technologies, as well as tools for 3D visualization and analysis, BIM, digital building technologies and more. Registration information is online at <https://xpressreg.net/register/geow0223/landing.php?>, and at <https://www.geo-week.com>. ◀

Industry eyes miniature optical beam steering for laser communications and lidar

BY John Keller

ARLINGTON, Va. – U.S. military researchers have asked industry to develop miniature optical beam steering for applications like free-space laser optical communications and light detection and ranging (lidar).

Officials of the U.S. Defense Advanced Projects Agency (DARPA) in Arlington, Va., issued a microsystems exploration topic last September (DARPA-PA-21-05-01) for the Steerable Optical Aperture Receivers (SOAR) project.

SOAR is to identify promising new approaches to optical beam steering in miniature form factors, and experimentally demonstrate their operation in receive mode with small aperture sizes.

Today, optical beam steering primarily is mechanical, using a gimbal or motor to point optical lenses. The size weight of gimbal-based beam steering systems, however, typically is too big for small and autonomous vehicles that need onboard laser communications and lidar capability.

The rise of integrated photonics, in which microscopic devices on chips replicate the functions of discrete optics. This offers not only dramatic size reduction, but also the potential for new and complex optical system architectures until now have been impractical at the macroscopic scale. The SOAR project seeks to answer key questions about optical receiver performance, scalability, and integration.

SOAR seeks to develop optical interfaces that can receive light from any direction without knowing the incoming angle by

▲ **The DARPA SOAR program is to design optical beam steering in miniature form factors, and demonstrate their operation in receive mode with small aperture sizes.**

steering the angle of acceptance to acquire and couple the input beam into a common output mode, or detect the optical signal within the receiver interface.

The first phase of SOAR will focus on lidar and laser communications receiver design and process development. The second phase will fabricate the receiver, and include a transceiver design study on aperture scalability and system integration.

DARPA researchers want steering components to be significantly smaller than 100 cubic centimeters, and be able to steer light beams at high speed, with pointing time faster than 100 microseconds, and with modest power consumption.

SOAR is technology-agnostic and open to any concept that meets program goals. Researchers would consider, for example, two-dimensional optical parametric amplification (OPA), non-planar integrated photonics, optical metasurfaces, directional optical scattering techniques, and discrete micro-optics. Researchers also are interested in the ability to generate several simultaneous beams. ◀

Companies were asked to respond by October to the DARPA submission website at <https://baa.darpa.mil>. Email questions or concerns to Jonathan Hoffman, the DARPA SOAR program manager, at SOAR@darpa.mil. More information is online at <https://sam.gov/opp/c0bda073553047b1803c11518eae78fc/view>.

Leonardo DRS to provide electro-optical sensors for Australian vetronics

BY John Keller

WARREN, Mich. – U.S. Army combat vehicle experts needed electro-optical systems to enable vehicle crews to see outside while inside and protected from enemy fire. They found their solution from the Leonardo DRS Land Electronics segment in Melbourne, Fla.

Officials of the U.S. Army Contracting Command at Detroit Arsenal in Warren, Mich., have announced a \$9.6 million contract to Leonardo DRS for Integrated Vision Systems vetronics for the government of Australia.

The Integrated Vision Systems enable armored combat vehicle crew members to see outside the vehicle while remaining under protection of the vehicle's armor. It combines uncooled thermal technology in a two-axis stabilized gimbal with the Leonardo DRS Enhanced Situation Awareness camera system.

The Leonardo DRS integrated vision system sensors for armored combat vehicles has a two-axis stabilized gimbal sensor that provides 360-degree vision with image-intensified television, infrared sensor, and laser range finder.

These electro-optical sensors are for Australia's Assault Breacher Vehicle, which is designed to clear pathways for infantry soldiers and military vehicles through dangerous obstacles like mine fields, improvised explosive devices, and other roadside bombs.

The DRS integrated vision system for the Breacher has a two-axis stabilized gimbal sensor that provides 360-degree vision with image-intensified television, infrared sensor, and laser range finder. The Assault Breacher Vehicle is based on the M1A1 main battle tank chassis, weighs 72-tons, is 40 feet long, and has a 1,500 horsepower engine.

The vehicle has a plow that is 15 feet long, supported by metal skis that glide on the dirt. The vehicle carries about 7,000 pounds of explosives, including M58 rockets with C-4 explosives designed to detonate hidden explosives as far ahead of the vehicle as 150 yards to let soldiers troops and vehicles pass by safely.

The Australian military operates several armored combat vehicles, including the Australian Light Armored Vehicle (ASLAV);



Electro-optical sensors from Leonardo DRS will enable armored combat vehicle crews to see outside when their vehicles are buttoned-up for battle.

Bushmaster; G Wagon; M1 Abrams tank; and M113AS4 armored personnel carrier.

The ASLAV is a wheeled, eight-wheel-drive vehicle that has been modified to deal with Australia's harsh conditions. The Bushmaster Protected Mobility Vehicle – Medium (PMV-M) is an Australian-built four-wheel drive armored vehicle. The G-Wagon vehicle and its range of trailers and modules is designed to be used by the Australian army in tactical training, disaster relief, and securing Australia's coastline.

The Abrams main battle tank has the firepower, mobility and survivability to provide the key component in the combined arms team. The M113AS4 armored personnel carrier provides the Australian Defence Force with a protected mobility and armored fighting capability. ←

On this contract Leonardo DRS will do the work in Melbourne, Fla., and should be finished by November 2024. For more information contact Leonardo DRS Land Electronics online at www.leonardodrs.com, or the Army Contracting Command-Detroit Arsenal at <https://home.army.mil/detroit/index.php/units-tenants/acc-dta>.



Army orders Javelin electro-optical imaging infrared anti-tank missiles

BY John Keller

REDSTONE ARSENAL, Ala. — Missiles experts at Lockheed Martin Corp. and Raytheon Technologies Corp. will build additional Javelin anti-tank missiles, which have achieved fame in the Russia-Ukraine war as one of the most lethal weapons used against invading Russian armored combat vehicles.

Officials of the U.S. Army Contracting Command at Redstone Arsenal, Ala., announced a \$311.2 million order last month to the Raytheon/Lockheed Martin Javelin Joint Venture based in Tucson, Ariz., to build Javelin weapon systems. The order is for full-rate production of Javelin missiles.

Javelin, which has electro-optical guidance, is an infantry fire-and-forget anti-armor weapon with lock-on before launch and automatic self-guidance designed to destroy main battle tanks, armored personnel carriers, and other armored combat vehicles. The missile also is effective against buildings and enemy helicopters.

Javelin has an imaging infrared-guided seeker to guide the warhead to its target. The tandem warhead has two shaped

▲ **Javelin, which has electro-optical guidance, has automatic self-guidance and is designed to destroy main battle tanks, armored personnel carriers, and other armored combat vehicles.**

charges: a precursor warhead to detonate any explosive reactive armor, and a primary warhead to penetrate base armor.

Javelin offers lock-on before launch and automatic self-guidance that attacks the vulnerable tops of armored vehicles. A

two-person infantry team typically carries the missile.

Raytheon produces the command launch unit, missile guidance electronic unit, and system software at Raytheon Missile Systems segment in Tucson, Ariz. Lockheed Martin, meanwhile, produces the missile seeker and the electronic safe, arm, and fire electronic module in Ocala, Fla., and performs missile all-up-round assembly in Troy, Ala. ◀

On this order the Raytheon/Lockheed Martin Javelin Joint Venture will do the work in Tucson, Ariz., and should be finished by November 2025. For more information contact Raytheon at www.raytheonmissilesanddefense.com/what-we-do/land-warfare/precision-weapons/javelin-missile, or Lockheed Martin at www.lockheedmartin.com/en-us/products/javelin.html.

6 degrees of freedom motion control system introduced by ALIO Industries

Motion control specialist ALIO Industries in Arvada, Colo., is introducing the Hybrid Hexapod for 6D motion in applications that need flatness and straightness of motion plus stiffness, such as machining and bonding applications. The Hybrid Hexapod technology allows for the provision of documented proof of performance over all 6 degrees of freedom of a body in motion at nanometer-level precision, says Bill Hennessey, president of ALIO Industries. The Hybrid Hexapod is for nanometer applications in the optical, semiconductor, manufacturing, metrology, laser processing, and micro-machining sectors. While all hexapod motion systems operate within 3D space, and have errors in all 6 degrees of freedom, they typically have been characterized only by performance data of a single degree of freedom. This practice leaves error sources unaccounted for in several degrees of freedom, especially in flatness and straightness, which are critical precision needs at the nanometer level. The Hybrid Hexapod is designed to overcome these issues. ALIO Industries designed the Hybrid Hexapod to address the critical weaknesses of conventional legacy hexapod designs and stacked serial stages, and achieve nanometer-level accuracy, repeatability, and high-integrity flatness and straightness during motion. It uses a tripod parallel kinematics structure to deliver Z plane and tip/tilt motion, integrated with a monolithic serial kinematic structure for XY motion. A rotary stage integrated into the top of the tripod provides 360-degree continuous yaw rotation, and customizes individual axes to provide travel ranges from millimeters to more than one meter, while maintaining nanometer-levels of precision. For more information contact ALIO Industries online at <https://alioindustries.com>.

Rugged optical fiber that resists solar radiation introduced by Armadillo SIA

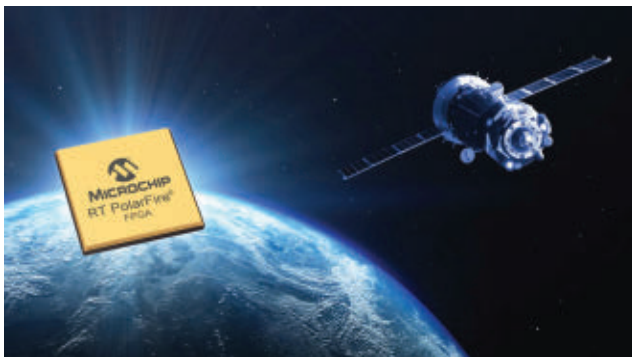
Armadillo SIA in Sunnyvale, Calif., is introducing Opttran UV NSS Fiber to provide deep-ultraviolet solarization resistance in semiconductor technology, laser delivery systems, spectroscopy, and medical technology. The optical fiber features a hermetic carbon layer, low numerical aperture expansion, and superior optical stability while operating in the UVC spectral range from 190 to 1200 nanometers. The high-solarization-resistance fibers resist the effects of ultraviolet radiation are available in any numerical aperture value from 0.12 to 0.30 and can be customized on request. Core diameters are available from 90 to 1000 microns. Composed of biocompatible materials, the operating temperature range of the silica/silica optical fibers is -190 to 150 degrees Celsius. For more information contact Armadillo SIA online at www.armadillosia.com.

Raytheon to build FIM-92 Stinger shoulder-fired anti-aircraft missiles

U.S. Army air-defense experts are asking Raytheon Technologies Corp. to build additional FIM-92 Stinger shoulder-fired anti-aircraft missiles under terms of a \$34.9 million order. Officials of the Army Contracting Command at Redstone Arsenal, Ala., are asking the Raytheon Missiles & Defense segment in Tucson, Ariz., to build Stinger missiles and related equipment. One soldier can operate the FIM-92 Stinger — a portable air-defense system that operates as an infrared homing surface-to-air missile that can be fired from a wide variety of infantry launchers, military ground vehicles, and helicopters. The passive surface-to-air missile can be shoulder-fired by one operator, and can acquire the target when the target approaches the operator, giving much more time to acquire and destroy the target. The FIM-92B missile also can fire from the M1097 Avenger and the M6 Linebacker weapon systems. The missile also can deploy from a Humvee Stinger rack, and can be used by airborne troops. A helicopter launched version exists called Air-to-Air Stinger (ATAS). The shoulder-fired missile is five feet long, 2.8 inches in diameter, and weighs 22 pounds. It has a targeting range of about three miles and can engage low-altitude enemy threats from as far away as 2.3 miles. The missile travels as fast as Mach 2.5. For more information contact Raytheon Missiles & Defense online at www.raytheonmissilesanddefense.com, or the Army Contracting Command-Redstone at <https://acc.army.mil/contractingcenters/acc-rsa/>.

RF-over-fiber systems for satellite communications (SATCOM) introduced by ETL Systems

ETL Systems Ltd. in Madley, England, is introducing the next evolution of StingRay, the company's RF-over-fiber range with additional functionality and flexibility for satellite operations. RF over fiber is a dependable and reliable way of moving satellite communications (SATCOM) signals over long distances than standard coaxial cable. With fiber modules that enable antennas and IRD modems to link from 100 meters to more than 500 kilometers, this is an efficient way to transport IF, L and C-band transmit and receive satellite signals. The RF over fiber products will be incorporated into ETL's next-generation Genus platform that will offer increased modularity and flexibility for ground stations, as well as medium-Earth-orbit and low-Earth-orbit satellites. Within the Genus platform, ETL's StingRay long-range RF over fiber products cover frequency bands including C-Band links operating over 500 MHz to 6,725 MHz. For more information contact ETL Systems online at www.etlsystems.com. ←



SPACE COMPUTING

▲ NASA selects Microchip Technology to develop spaceflight processor

The U.S. National Aeronautics and Space Administration's (NASA) Jet Propulsion Laboratory in La Cañada Flintridge, Calif., has selected Microchip Technology Inc. of Chandler, Ariz., to develop a high-performance spaceflight computing (HPSC) processor. Microchip's HPSC will provide at least 100 times the computational capacity of current spaceflight computers. This capability aims to advance all types of future space missions, including surface missions.

Microchip will architect, design, and deliver the HPSC processor over three years, with the goal of employing the processor on future lunar and planetary exploration missions. Microchip's processor architecture will improve the overall computing efficiency for these missions by enabling computing power to be scalable, based on mission needs. The work will take place under a \$50 million contract, with Microchip contributing significant research and development costs to complete the project.

"We are making a joint investment with NASA on a new trusted and transformative compute platform," says Babak Samimi, corporate vice president for Microchip's Communications business unit. "It will deliver comprehensive Ethernet networking, advanced artificial intelligence/machine learning processing and connectivity support while offering unprecedented performance gain, fault-tolerance, and security architecture at low power consumption."

Current space-qualified computing technology is designed to address the most computationally intensive part of a mission — a practice that leads to overdesigning and inefficient use of computing power. For example, a Mars surface mission demands high-speed data movement and intense calculation during the planetary landing sequence. However, routine mobility and science operations require fewer calculations and tasks per second. Microchip's new

processor architecture offers the flexibility for the processing power to ebb and flow depending on current operational requirements. Certain processing functions can also be turned off when not in use, reducing power consumption. This capability will save a large amount of energy and improve overall computing efficiency for space missions.

"Our current spaceflight computers were developed almost 30 years ago," says Wesley Powell, NASA's principal technologist for advanced avionics. "While they have served past missions well, future NASA missions demand significantly increased onboard computing capabilities and reliability. The new computing processor will provide the advances required in performance, fault tolerance, and flexibility to meet these future mission needs."

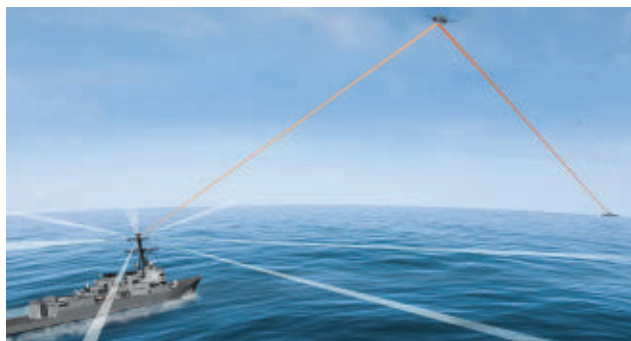
Microchip's HPSC processor may be useful to other government agencies and applicable to other types of future space mission to explore Earth's solar system and beyond, from Earth science operations to Mars exploration and human lunar missions. The processor potentially could be for commercial systems on Earth that require similar mission critical edge computing needs as space missions and are able to continue operations safely if one component of the system fails. These potential applications include industrial automation, edge computing, time-sensitive Ethernet data transmission, artificial intelligence, and even Internet of Things gateways, which bridge various communication technologies.

TACTICAL NETWORKING

▼ L3Harris to provide signal processing for shipboard network

U.S. Navy surface warfare experts needed signal data processors and spare parts for the Cooperative Engagement Capability (CEC) tactical network aboard Navy surface warships. They found their solution from L3Harris Technologies.

Officials of the Naval Sea Systems Command in Washington have announced a \$32 million order to the



L3Harris C5 Integrated Systems segment in Camden, N.J., for CEC spares and signal data processors.

The CEC is a maritime tactical sensor and weapons network for anti-air warfare that combines information from sensors on aircraft and surface vessels that are operating over broadly distributed geographic areas.

CEC combines sensor information into a common tactical picture for battle groups at sea. It improves overall situational awareness, and enables fleet commanders to work closely together to attack enemy forces from long ranges.

The order to L3Harris is a modification to a six-year \$14.9 million contract the company won last July for CEC system production and repair. This contract has options that could increase its value to \$378.9 million.

CEC blends sensors and weapons into an integrated real-time network that expands the battlespace; enhances situational awareness; increases depth of fire; enables long intercept ranges; and improves decision and reaction times.

It extracts and distributes sensor information such that the superset of this data is available to all participating CEC-equipped units by fusing the distributed data from shipboard, airborne, composite tracking network ground-mobile units, Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System (JLENS), and coalition partners into one fire-control-quality air track picture.

The system uses line-of-sight data distribution to share radar-measurement data among sensors and weapons to create one distributed integrated air picture. It combines surveillance and targeting information such that the combined system is greater than the sum of its parts.

The jam-resistant CEC obtains target track information to form one real-time composite track to help coordinate theater air and missile defense to engage incoming cruise missiles.

CEC consists of the Data Distribution System (DDS), the Cooperative Engagement Processor (CEP), and interface with combat systems and sensors.

The DDS encodes and distributes own-ship sensor and engagement data. The CEP processes force levels of data in near real-time, and enables surface warships and other weapons platforms to cue their onboard sensors and weapons to engage targets without actually tracking them.

On this order L3Harris will do the work in Lititz and Lancaster, Pa.; Salt Lake City; and Largo, Fla., and should be finished by April 2023. For more information contact L3Harris C5 Integrated Systems online at www.l3harris.com, or Naval Sea Systems Command at www.navsea.navy.mil.



RADAR

▲ Saab to build two radar systems for shipboard air traffic control

U.S. Navy shipboard surveillance experts needed AN/SPN-50(V) 1 shipboard air traffic control radar systems to replace the Navy's AN/SPN-43C radar aboard aircraft carriers and amphibious assault ships. They found their solution from Saab Inc. in East Syracuse, N.Y.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., has announced a \$31.7 million order to Saab for two AN/SPN-50(V) 1 shipboard air traffic radar systems for aircraft carriers and amphibious assault ships.

The AN/SPN-50(V) 1 radar enables shipboard air traffic controllers to identify, marshal, and direct aircraft within a 50-nautical-mile radius of the ship. The order includes two on-board repair kits, and two depot spares kits.

In recent years, the top 25 percent of the AN/SPN-43C frequency band has been reallocated to the fixed wireless access community prohibiting air traffic control and air search radar operation within 50 nautical miles of the coast, Navy officials say.

The AN/SPN-50(V)1 radar is one of the U.S. versions of Saab's Sea Giraffe agile multi beam radar, functions as the primary air traffic control surveillance radar for manned and unmanned aviation aboard the Navy's nuclear-powered aircraft carriers and large-deck amphibious assault ships.

On this order Saab will do the work in Syracuse, N.Y., and should be finished by September 2024. For more information contact Saab Inc. online at www.saab.com, or Naval Air Systems Command at www.navair.navy.mil.



MISSILE GUIDANCE

▲ Raytheon to build FIM-92 Stinger shoulder-fired anti-aircraft missiles

U.S. Army air-defense experts are asking Raytheon Technologies Corp. to build additional FIM-92 Stinger shoulder-fired anti-aircraft missiles under terms of a \$34.9 million order.

Officials of the Army Contracting Command at Redstone Arsenal, Ala., are asking the Raytheon Missiles & Defense segment in Tucson, Ariz., to build Stinger missiles and related equipment.

One soldier can operate the FIM-92 Stinger — a portable air-defense system that operates as an infrared homing surface-to-air missile that can be fired from a wide variety of infantry launchers, military ground vehicles, and helicopters.

The passive surface-to-air missile can be shoulder-fired by one operator, and can acquire the target when the target approaches the operator, giving much more time to acquire and destroy the target. The FIM-92B missile also can fire from the M1097 Avenger and the M6 Linebacker weapon systems.

The missile also can deploy from a Humvee Stinger rack, and can be used by airborne troops. A helicopter launched version exists called Air-to-Air Stinger (ATAS).

The shoulder-fired missile is five feet long, 2.8 inches in diameter, and weighs 22 pounds. It has a targeting range of about three miles and can engage low-altitude enemy threats from as far away as 2.3 miles. The missile travels as fast as Mach 2.5, and has a 2.25-pound explosive warhead.

It entered service in 1981 and is used by the militaries of the U.S. and 29 other countries. Airbus Defence in

Germany and by ROKETSAN in Turkey also can build the missile under license from Raytheon.

There are three main variants: the Stinger Basic, Stinger-Passive Optical Seeker Technique (POST), and Stinger-Reprogrammable Microprocessor (RMP).

The POST and RMP variants have a dual-detector infrared and ultraviolet seeker that enables the missile to distinguish targets from countermeasures. The Stinger-RMP can load a new set of software via read-only memory.

The weapon has more than 270 fixed-wing aircraft and helicopter

intercepts to its credit. Stinger missiles also can destroy unmanned aircraft with proximity fuzes. For more information contact Raytheon Missiles & Defense online at www.raytheonmissilesanddefense.com, or the Army Contracting Command-Redstone at <https://acc.army.mil/contractingcenters/acc-rsa/>.

SENSORS

▼ Raytheon to build long-range ASARS-2 imaging radar for U-2 reconnaissance jet

U.S. Air Force aerial surveillance experts are asking the Raytheon Co. to build super-high-resolution imaging radar for long-range target detection, radar mapping, and bomb damage assessment.

Officials of the Air Force Life Cycle Management Center at Wright-Patterson Air Force Base, Ohio, announced a \$184 million five-year contract to the Raytheon Intelligence & Space segment in El Segundo, Calif., for the Advanced Synthetic Aperture Radar System-2 — better-known as ASARS-2.



This imaging radar is a multimode real-time, high-resolution reconnaissance system carried on the U-2 Dragon Lady high-altitude reconnaissance jet with all-weather, day-night, long-range mapping capabilities.

ASARS-2 detects and locates stationary and moving ground targets with precise range in search and spotlight imagery modes. It gathers detailed information, formats the data, and transmits it via wideband data link for display of fixed or moving ground objects.

The imaging radar can produce extremely high-resolution images from long stand-off ranges and provides the highest resolution radar ground maps available today, experts say.

ASARS-2 is a descendant of the original ASARS radar used 30 years ago during the Persian Gulf War for battle damage assessment. It has on-board processing, improved image quality, broad area coverage of still and moving targets, and improved target geolocation.

ASARS-2B contains an active electronically scanned array antenna and is designed to double the surveillance range of the U-2 aircraft. ASARS-2B replaces the front end components of the Raytheon ASARS-2A airborne radar, which has become difficult to maintain because of obsolescent components.

ASARS-2B uses liquid electronics cooling and thermal management. It has an open-systems architecture, and the radar's range is nearly double that of the previous ASARS-2A radar, Raytheon officials say.

On this contract Raytheon will do the work in El Segundo, Calif., and should be finished by August 2027. For more information contact Raytheon Intelligence & Space online at www.raytheonintelligenceandspace.com, or the Air Force Life Cycle Management Center at www.aflcmc.af.mil.

ELECTRONIC WARFARE

▲ L3Harris to provide missile-defense electronic warfare (EW) payloads for surface warships

U.S. Navy shipboard electronic warfare (EW) experts are asking L3Harris Technologies Inc. to build special EW payloads to help protect Navy warships from enemy anti-ship cruise missiles.



Officials of the Naval Sea Systems Command in Washington announced a \$31.7 million order for the MK 234 Nulka Advanced Decoy Architecture Program (ADAP)-series payloads.

The ADAP missile-defense payload provides an advanced EW transmitter and increased signal processing capability to target specific threats that the current payload on the shipboard Nulka decoy does not.

ADAP payloads are designed to lure missiles away from their intended targets with advanced electronic techniques. The ADAP payloads are an upgrade to the existing Nulka decoy.

Nulka is a joint program with Australia, and is in service with the Australian, Canadian, and U.S. navies to protect surface warships. Nulka consists of the MK 53 decoy-launching system and MK 234 offboard active decoy to defeat hostile anti-ship missiles.

The MK 53 DLS consists of a decoy launch processor, launching power supplies, and from two to six launchers depending on the ship class. Each launcher can store and launch two Nulka decoys. The MK 53 DLS provides the launch authorization and flight demands to the Nulka decoy when a Nulka engagement is initiated.

The MK 53 DLS has been installed on U.S. Ticonderoga-class cruisers, Arleigh Burke-class destroyers, Nimitz-class aircraft carriers, as well as on Whidbey Island- and Harpers Ferry-class amphibious assault ships.

On this order L3Harris will do the work Clifton, N.J., and should be finished by June 2025. For more information contact L3Harris online at www.l3harris.com, or Naval Sea Systems Command at www.navsea.navy.mil.



AVIONICS

▲ Boeing team to provide 15 KC-46 aerial tanker aircraft, avionics, power, and displays

U.S. Air Force aerial refueling experts are asking the Boeing Co. to build 15 new KC-46 Pegasus military aerial refueling and strategic military transport aircraft under terms of a \$2.2 billion order.

Officials of the Air Force Life Cycle Management Center at Wright-Patterson Air Force Base, Ohio, are asking the Boeing Defense, Space & Security segment in Seattle to build lot 8 of the KC-46 aircraft program. The order includes subscriptions and licenses.

The KC-46 aircraft is based on the Boeing 767-200 wide-body passenger jet. The multirole aerial tanker can refuel all U.S., allied, and coalition military aircraft compatible with international aerial refueling procedures. In addition to refueling other aircraft in midair, the KC-46 also can carry passengers, cargo, and medical patients.

The KC-46 aircraft can detect, avoid, defeat, and survive threats using several layers of electronic protection that enable it to operate safely in medium-threat environments, Boeing officials say.

Honeywell Aerospace, Northrop Grumman Corp., and Raytheon Technologies Corp. are among the companies providing avionics subsystems and components for the KC-46.

Honeywell Aerospace in Coon Rapids, Minn., provides the air data inertial navigation system for the KC-46, while the company's facility in Phoenix provides the auxiliary power unit. The Honeywell Aerospace facility in Tucson, Ariz., provides the KC-46 cabin pressure control system, while the company's facility in Urbana, Ohio, provides the tanker's lighting system.

The Northrop Grumman Electronic Systems segment in Rolling Meadows, Ill., provides the KC-46's Large Aircraft Infrared Countermeasures (LAIRCM), while the Raytheon Intelligence & Space segment in El Segundo, Calif., provides the tanker's digital radar warning receiver and digital anti-jam global positioning system (GPS) receiver.

The Raytheon Collins Aerospace segment in Cedar Rapids, Iowa, provides the KC-46 integrated display system with 15.1-inch diagonal liquid crystal displays, which are based on the avionics suite for the Boeing 787 Dreamliner passenger jet.

Collins Aerospace also provides the

KC-46's tactical situational awareness system, remote vision system 3-D and 2-D technology for the boom operator, the communications, navigation, surveillance (CNI) system, networking, and flight-control systems.

The DRS Technologies Inc. Laurel Technologies Partnership in Johnstown, Pa., provides the KC-46's aerial refueling operator station (AROS). The Eaton Aerospace facility in Grand Rapids, Mich., provides the tanker's electromechanical and cargo door actuation systems.

Woodward Inc. in Skokie, Ill., meanwhile, provides the sensor system, control unit, and telescopic and flight control sticks for the KC-46's aerial refueling boom.

GE Aviation Systems facilities in Grand Rapids, Mich., and Clearwater, Fla., provide the KC-46 mission control system avionics, which provide integrated communications management to support air traffic management data link, and enable the aircraft to perform with navigation precision not currently available to the tanker fleet.

GE Aviation also provides the KC-46 flight management system (FMS), which helps the aircraft fly relatively short flight paths and idle-thrust descents to reduce fuel consumption, while lowering emissions and reducing engine noise.

The KC-46 will replace the Air Force's fleet of KC-135 aerial refueling aircraft, which are based on the 1960s-vintage Boeing 707 four-engine passenger jet. Boeing will build as many as 179 KC-46 aircraft.

On this order Boeing will do the work in Seattle, and should be finished by November 2025. For more information contact Boeing Defense, Space & Security online at www.boeing.com, or the Air Force Life Cycle Management Center at www.afldmc.af.mil.



COMPUTERS

▲ Northrop Grumman to provide battle management computers for sensors and situational awareness

Battle management experts at Northrop Grumman Corp. are preparing to help military authorities quickly deal with uncertain information concerning potential air and missile attacks.

Officials of the U.S. Army Contracting Command at Redstone Arsenal, Ala., announced a \$24.1 million order to the Northrop Grumman Mission Systems segment in Huntsville, Ala., for hardware and software for the Integrated Battle Command System (IBCS).

The IBCS is to be a revolutionary air command-and-control (C2) system to help air and missile defenders make quick decisions and adapt quickly to changing battlefield conditions. Last December Northrop Grumman won a potential \$1.4 billion contract for IBCS low-rate initial production and full-rate production.

The IBCS will help enhance aircraft and missile tracking and situational awareness to enable military commanders and air defenders to make critical decisions within seconds in response to air and missile attacks.

The IBCS represents a modular open-systems architecture to optimize limited resources and facilitate flexible defense designs, company officials say.

The IBCS enables commanders to tailor organizations, sensors, and weapons to meet the demands of diverse missions, environments, and rules of engagement not achievable today, Northrop Grumman officials say. It provides wide-area surveillance and broad protection areas by networking sensors and interceptors.

The system enables affordable integration of current and future sensors, weapons, and modernization efforts, and helps connect systems for joint and cooperative multinational missile defense.

The IBCS is to replace seven legacy command-and-control systems with network-centric battle management to

reduce single points of failure and increase the flexibility for deploying small force packages. The system creates a standard approach across forces to reduce logistics burdens and change training.

On this order Northrop Grumman will do the work in Huntsville, Ala., and should be finished by December 2025. For more information contact Northrop Grumman Mission Systems online at www.northropgrumman.com, or the Army Contracting Command-Redstone at <https://acc.army.mil/contractingcenters/acc-rsa/>.

SENSORS

▼ Lockheed Martin to provide electro-optical sensors for Apache helicopter targeting

U.S. Army aviation experts needed electro-optical assemblies to upgrade the Modernized Target Acquisition Designation Sight/Pilot Night Vision Sensor (M-TADS/PNVS) system, also known as Arrowhead. They found their solution from Lockheed Martin Corp.

Officials of the Army Contracting Command at Redstone Arsenal, Ala., announced a \$121.6 million order to the Lockheed Martin Rotary and Mission Systems segment in Orlando, Fla., for M-TADS/PNVS components and hardware for the AH-64 Apache attack helicopter.

The lower M-TADS turret contains the targeting system, which has day and night electro-optical sensors. The Arrowhead targeting sensor suite has forward looking infrared (FLIR) elements of the TADS and the PNVS to provide modern technological and precision engagement, and ensure the Army's Apache helicopter remains an effective attack helicopter well into the future.

The system's laser rangefinder designator includes an eye-safe rangefinder and day sensor electronics unit, which replace the laser transceiver unit and related electronics in the Apache's legacy day sensor assembly.



The new day sensor structure assembly offers fields of view that match the Arrowhead FLIR fields of view to accommodate image blending. The modernized TV sensor incorporates color and low-light sensitivity. A modern inertial measurement unit replaces three spinning-mass gyros, and the new laser spot tracker uses a four-quadrant detector and improved processing. A laser pointer marker helps enhance coordination with ground and air units.

These targeting components enable Apache flight crews to identify targets at long ranges through an additional field-of-view and extended-range picture-in-picture capability, as well as provide the ability to view high-resolution, near-infrared and color imagery on cockpit displays.

The system provides a new laser pointer marker that improves coordination with ground troops, and an updated multimode laser with eye-safe lasing capability that supports flight in urban environments and home-station training.

M-TADS/PNVS provides Apache helicopter pilots with long-range, precision engagement and pilotage capabilities for mission success and flight safety during day and night and in adverse weather conditions.

On this order Lockheed Martin will do the work at locations to be determined with each order, and should be finished by March 2022. For more information contact Lockheed Martin Rotary and Mission Systems online at www.lockheedmartin.com, or the Army Contracting Command-Redstone at <https://acc.army.mil/contractingcenters/acc-rsa>.

AVIONICS

► **Boeing to procure mission computers for EA-18G aircraft avionics**

Military avionics experts at the Boeing Co. will provide the final 51 Advanced Mission Computer (AMC) retrofit kits for the U.S. Navy EA-18G Growler electronic warfare (EW) aircraft under terms of a \$51.7 million contract.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., are asking the Boeing Defense, Space & Security segment in St. Louis to provide 51 AMC systems, which are designed and manufactured by the General Dynamics Corp. Mission Systems segment in Bloomington, Minn.

The contract calls for Boeing to procure 49 AMC kits for EA-18G aircraft and two kits for software integration labs.

The latest version of the F/A-18 mission computer is the AMC Type 4, which first was flight tested in 2012. Type 4 AMC increases computing power and accelerates image and mission processing functions, Boeing officials say.



Those advances will support new systems and future systems aboard the aircraft, including a distributed targeting system, infrared search and track, and a new high-definition touch-screen display.

The AMC is the nerve center of the Navy Super Hornet. The commercial off-the-shelf (COTS)-based, open-systems architecture product is configurable to many operating environments.

The flight and mission computer is designed to handle mission processing; sensor processing; display processing; stores management; and information management.

The AMC is a rugged avionics embedded computer that performs general-purpose, I/O, video, voice, and graphics processing. Communication is over several buses, including 1553, Fiber Optic Fiber Channel, and Local PCI.

Single-board computers and other modules in the AMC fit in an industry standard 6U VME backplane, and the I/O configuration may be tailored with PCI mezzanine card (PMC) modules. An Ethernet interface supports software development and system maintenance.

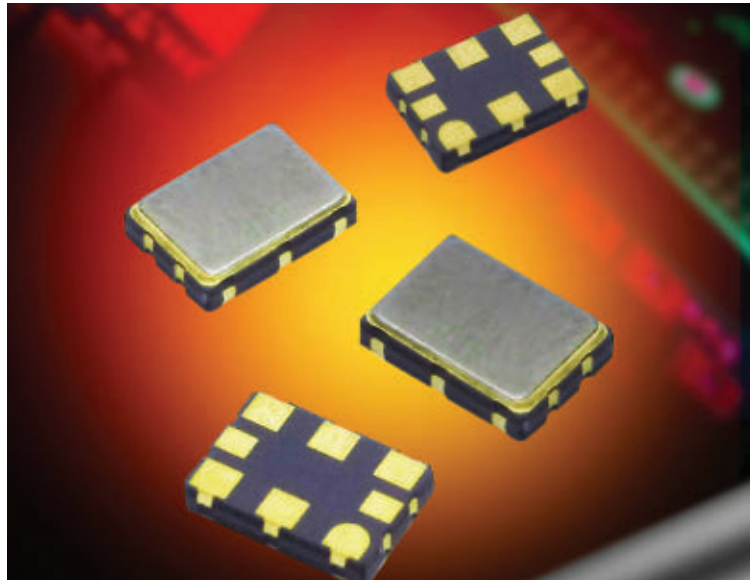
The AMC's core system software (CSS) is a real-time operating system with embedded system software, application program interface, and diagnostic software set for the AMC. The computer's I/O includes MIL-STD-1553 drivers, Fibre Channel drivers, VMEbus drivers, and discrete and serial I/O drivers.

On this contract Boeing and its partners will do the work in Bloomington, Minn.; St. Louis; and Linthicum Heights, Md., should be finished by September 2025. For more information contact Boeing Defense, Space & Security online at www.boeing.com/company/about-bds, General Dynamics Mission Systems at <https://gdmissionsystems.com>, or Naval Air Systems Command at www.navair.navy.mil. ◀

POWER ELECTRONICS

► **Ceramic voltage-controlled crystal oscillators (VCXO) offered by Saelig**

Electronics distributor Saelig Co. Inc. in Fairport, N.Y. is offering the EG-JF series surface-mount voltage-controlled crystal oscillators (VCXO) for applications where ultra-low phase jitter is an essential requirement. The EG-JF series is from frequency control specialist Euroquartz Ltd in Crewkerne, England. The VCXO devices offer high frequency outputs with ultra-low phase jitter performance, and operate at frequencies from 15 to 2100 MHz for CMOS, LVPECL, LVDS, and CML differential outputs and at 15 to 700 MHz for HCSL differential outputs. Typical RMS phase jitter performance ranges from as low as 151 fs at 644.530 MHz to 163 fs at 2000 MHz. The oscillators are housed in a standard format 8-pad 7-by-5-millimeter SMD ceramic package with hermetically sealed metal lid. Power supply voltage options are 1.8 volts plus-or-minus 5 percent (except LVPECL types), 2.5 volts plus-or-minus 10 percent, and 3.5 volts plus-or-minus 10 percent (all types) with current consumption ranging from 70 to 120 milliamps maximum depending on frequency and logic type. Standard temperature stability specification options available are plus-or-minus 25, plus-or-minus 50, and plus-or-minus 100 ppm over commercial temperatures from -10 to 70 degrees Celsius, and industrial temperatures from -40 to 85 C with tighter options available on request. The Euroquartz EG-JF series VCXOs are for applications such as flat panel displays for consumer TVs; video streaming systems via external cables (e.g. LDI); and high-speed serial communications links such as Serial ATA & FireWire, SONET, xDSL, SDH, set-top box, and Ethernet cards. For detailed specifications, free technical assistance, or more information, contact Saelig online at www.saelig.com.



analysis, object detection and recognition capabilities to systems developers. The JetKit-3010 embedded computing kit uses the integrated deep learning capabilities and I/O of the NVIDIA Jetson AGX Xavier general-purpose graphics processing unit (GPGPU) to help designers develop smart and reliable systems for industrial automation, automotive, and agriculture applications. Prior to the open standards-based JetKit-3010, research and development with AI components required extremely powerful and specialized hardware, much of which is purpose-built and expensive. The combination of the NVIDIA GPGPU module in a CompactPCI Serial architecture can help develop applications that require pattern recognition, environment recognition or situation analysis. The JetKit-3010 combines an 8-core ARM processor with 512 NVIDIA CUDA cores and

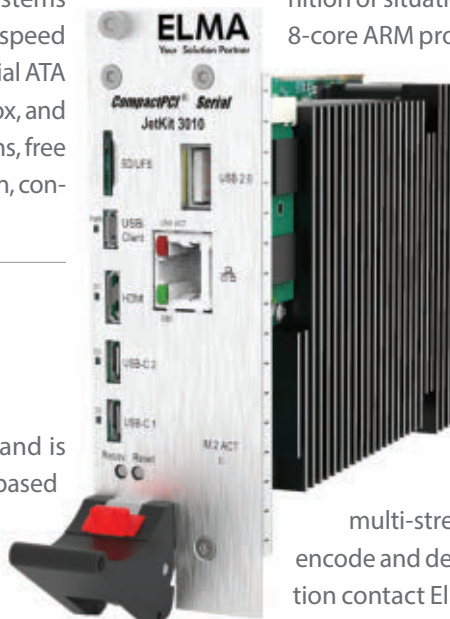
64 Tensor cores to provide compute density, energy efficiency and AI inferencing capabilities. The JetKit-3010 can be packaged as a standalone small-form-factor platform or integrated as a multi-function computer board in an existing CompactPCI system. It provides M.2 NVME, HDMI, 4x USB, 2x Gigabit Ethernet, and x8 PCI Express ports. The display controller supports imaging at 3840-by-2160 resolution at 60 Hz via HDMI, and

multi-stream HD video and JPEG support for most encode and decode video standards. For more information contact Elma Electronic online at www.elma.com.

EMBEDDED COMPUTING

► **NVIDIA Jetson GPGPU-based embedded computing kit introduced by Elma**

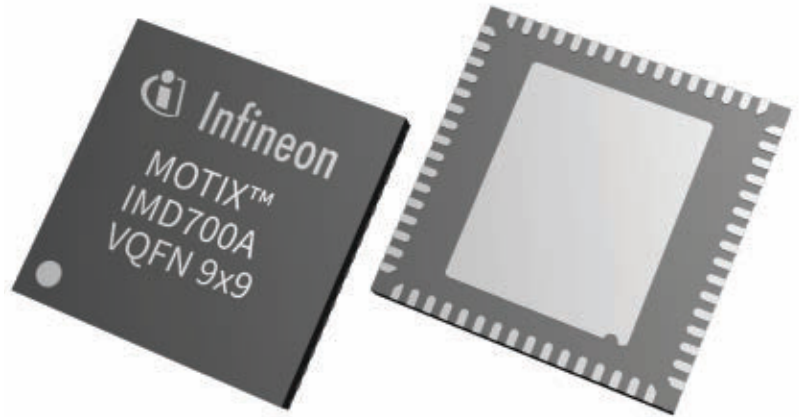
Elma Electronic in Wetzikon, Switzerland is introducing the 3U CompactPCI Serial-based JetKit-3010 single board computing engine that delivers artificial intelligence (AI)-enabled video inspection,



PROCESSORS

► **Microcontroller for SWaP-constrained motor control introduced by Infineon**

Infineon Technologies AG in Neubiberg, Germany, is introducing MOTIX IMD700A and IMD701A programmable motor control devices for unmanned aerial vehicles (UAVs), automated guided vehicles, e-bikes, and cordless power tools. The motor controllers come in 9-by-9-millimeter 4-pin VQFN packaging, and offer the integration and high power density necessary for size-, weight-, and power-consumption (SWaP)-constrained electronics applications. In one package, the MOTIX IMD70xA controllers combine the MOTIX 6EDL7141 3-phase gate driver IC features with an additional XMC1404 microcontroller, whose peripherals and specifications are optimized for motor control and drives. Infineon's XMC1404 microcontroller includes a math coprocessor clocked at 96 MHz to enhance calculations commonly used in sensorless field-oriented control (FOC) algorithms enabling higher system performance. The XMC1404 also inherits most of the high-end peripherals found in the XMC4000 family, including PWM timers, position interface (POSIF), and serial communication modules (including CAN). The motor control IC features controllability of the gate drive slew rate to protect systems from electromagnetic interference (EMI). IMD70xA controllers support adjustable gate drive supply voltage even at low battery voltage levels thanks to built-in high- and low-side charge pumps, as well as many other adjustable gate driver parameters. More information on the Infineon MOTIX IMD700A is online at www.infineon.com/imd700a, and more information on the Infineon MOTIX IMD701A is at www.infineon.com/imd701a.



ranges from -40 to 70 Celsius. Based on 6- or 8-core microprocessors from Intel's 11th Gen Xeon processors with 10-nanometer technology, the Kontron CP6007 blade series is for long-term, general computing and server applications based on PICMG 2.16. This blade also is backwards compatible with previous Kontron blades. Both blades offer performance-per-Watt capability with a scalable power budget allowing users the flexibility to tailor power dissipation. The CP6007-RA embedded computing blade features a 32 gigabytes soldered memory while the CP6007-SA can carry a SODIMM module to provide as much as 64 gigabytes memory with Error Correction Code (ECC) support. The CP6007-RA variant is the successor of the Kontron CP6004-RA blade. Communication and media interfaces are provided, along with hardware and software system security through Trusted Platform Module (TPM 2.0). Extension options like storage, XMC, PMC, and rear-I/O are provided. Included are onboard industrial-grade NVMe and SATA M.2 flash devices, and a 2.5 inch SATA hard disk or solid-state drive to be located on a respective rear-I/O module. XMC compatibility based on XMC.3 is available for supporting x8 PCI Express, or alternatively PMC. For more information contact Kontron online at www.kontron.com.

BOARD PRODUCTS

► **Harsh-environment VITA 47 embedded computing boards introduced by Kontron**

Kontron AG in Ismaning, Germany, is introducing the CP6007 CompactPCI air-cooled blade computer series for use harsh-environment industrial, aerospace, and defense applications. The standard CP6007-SA computer blade and the rugged CP6007-RA blade are for use in harsh environments, and follow the VITA 47 open-systems standard for high shock and vibration demands and temperature



EMBEDDED COMPUTING

► System on module (SOM) for industrial automation introduced by Microchip

Microchip Technology Inc. in Chandler, Ariz., is introducing the SAM9X60D1G-SOM ARM926EJ-S-based embedded computing system on module (SOM) for industrial and automation control, medical equipment, automotive telematics, infotainment, and electric vehicle chargers. The SOM runs as quickly as 600 MHz, and offers software with bare metal or real-time operating system support through MPLAB Harmony3, or Linux mainlined distributions. The SOM for industrial automation, based on the SAM9X60D1G system-in-package (SiP), is a 28-by-28-millimeter hand-solderable module that includes the microcontroller and double-data-rate in one package, along with power supplies, clocks, and memory storage. The SAM9X60D1G-SOM embedded computing device has 4-gigabit SLC NAND Flash, also includes an MCP16501 power management IC (PMIC), and a 10/100 KSZ8081 Ethernet PHY and a 1 Kb Serial EEPROM with pre-programmed MAC address (EUI-48). It has secure boot with on-chip secure key storage (OTP), hardware encryption engine (TDDES, AES, and SHA) and True Random Generator (TRNG). Microchip provides hardware and software development support for the SAM9X60D1G-SOM including the SAM9X60D1G Curiosity Evaluation Kit (CPN: EV40E67A) featuring three Linux distributions: BuildRoot, Yocto and OpenWRT. The bare-metal or RTOS-based systems are supported by MPLAB Harmony 3 embedded software framework, MPLAB X Integrated Development Environment (IDE) and MPLAB XC32 compiler. For more information contact Microchip online at www.microchip.com.



TEST AND MEASUREMENT

► Four-channel touchscreen Shenzhen Micsig oscilloscope offered by Saelig

Electronics distributor Saelig Co. Inc. in Fairport, N.Y., is introducing the Micsig SATO1004 automotive tablet oscilloscope automotive vehicle testing tool from Shenzhen Micsig Technology Co. Ltd. in Shenzhen, China. The

oscilloscope is for evaluating systems such as ABS, accelerator pedal, throttle position, fuel pressure, air flow meter, crankshaft, camshaft, knock, MAP, 12/24-volt charging and start, charging ripple, cranking current sensors, actuators, ignition, and CAN, LIN, Flex ray, and K line networks. The test and measurement device has four channels, a bandwidth of 100 MHz, an easy-use touchscreen operation, and vehicle diagnostics. With its signal sample rate of 1 gigasample

per second, the SATO1004 is designed for portable and benchtop use, and has a built-in 7500mAh Li-ion battery that supports five hours of portable operation. The oscilloscope also can connect to an external 12-volt power adapter for continuous use. The Micsig SATO1004 automotive oscilloscope comes with an automobile diagnostic presets package, signal capture and analysis capabilities, as well as smart bus trigger and decode features that include UART, LIN, SPI, CAN, I2C, 1553B, and 429. It also supports PC and smartphone remote control. This instrument combines a capacitive 8-inch TFT LCD touch screen with traditional button and knob operation. The built-in HDMI output adds educational and demonstration possibilities for large displays or projectors. For more information contact Saelig online at www.saelig.com, or Shenzhen Micsig Technology at www.micsig.com.



BOARD PRODUCTS

► OpenVPX carrier cards for interfacing XMC to VPX introduced by Acromag

Acromag in Wixom, Mich., is introducing the VPX4840 and VPX4850 OpenVPX carrier cards that provide a simple and cost-effective solution for interfacing Switched Mezzanine Card (XMC) modules to a VPX embedded computing system. The VPX4840 and VPX4850 feature two XMC slots with support for front-or rear-panel I/O. They are available with VITA 42, VITA 61, or VITA 88 connectors to route power and interface bus signals to the plug-in mezzanine modules. Both carrier cards support a choice of direct PCI Express connection to the VPX backplane via the data or expansion plane. The XMC sites have a 16-lane PCI Express bus Gen A3 interface enabling rapid data throughput. By inserting XMC mezzanine modules on the carrier, including XMC processor (prXMC) modules, developers can use hundreds of available function



modules. Air-cooled versions of the OpenVPX modules operate in temperatures from 0 to 55 degrees Celsius, and models with extended temperature ranges or conduction cooling are available. For more information contact Acromag online at www.acromag.com.

PRODUCT & LITERATURE SHOWCASE

Zio

Full Motion Video-over-IP Situational Awareness From HQ to Forward Deployments Video Distribution, Recording, and Display



510-814-7000



www.rgb.com/zio



RF AND MICROWAVE

◀ Multiple-bandwidth antennas for wireless telecommunications introduced by KP

KP Performance Inc. in Lewisville, Texas, is introducing a line of eight-port sector antennas featuring dual polarization and multiple bandwidth options for wireless telecommunications applications. The sector antennas feature antenna gain from 14 to 19 dBi and multiple-input and multiple-output (MIMO) capabilities to boost speed and mitigate interference. RF and microwave sensors are engineered for outdoor installation with frequency support from 2.3 GHz to 6.4 GHz, and they also feature a heavy-duty, UV-resistant, plastic radome for all-weather operation. The antennas have powder-coated mounting brackets to allow for easy installation with pipe diameters ranging from 1.25 to 3.5 inches

and various degrees of incline providing alignment. They are built to withstand wind speeds as strong as 100 miles per hour and survive in challenging environments. These RF and microwave sensors and transmitters are designed with single-band and dual-band options. They are available in 2.3 to 2.7 GHz, 3.3 to 4.2 GHz, and 4.9 to 6.4 GHz configurations and support 2x2, 4x4 and 8x8 MIMO. They incorporate advanced low-PIM, dual polarization technology that allows for interoperability with one 8x8, two 4x4 or four 2x2 radios with multiple transmit and receive paths. For more information contact KP Performance Inc., an Infinite brand, online at www.kpperformance.com. ◀

ADVERTISERS INDEX

ADVERTISER	PAGE
Fairview Microwave	3, 23
General Micro Systems	C4
Holt Integrated Circuits.....	25
Mercury Systems	C2
Pasternack Enterprises.....	15
Phoenix International.....	19
RGB Spectrum.....	48
Sealevel Systems.....	17

Military+Aerospace Electronics®

SUBSCRIPTION INQUIRIES

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

E-mail: MAE@omeda.com

Web: militaryaerospace.com/subscribe

VICE PRESIDENT/GROUP PUBLISHER **Steve Beyer**
847-532-4044 / sbeyer@endeavorb2b.com

EDITOR-IN-CHIEF **John Keller**
603 891-9117 / jkeller@endeavorb2b.com

ASSOCIATE EDITOR **Jamie Whitney**
603 891-9135 / jwhitney@endeavorb2b.com

CHIEF CONTRIBUTOR **Megan Crouse**

ART DIRECTOR **Kermit Mulkins**

PRODUCTION MANAGER **Sheila Ward**

AD SERVICES MANAGER **Shirley Gamboa**

AUDIENCE DEVELOPMENT MANAGER **Debbie Bouley**
603 891-9372 / dbouley@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

DIRECTOR LIST RENTAL **Kelli Berry**
918 831-9782 / kberry@endeavorb2b.com

FOR ASSISTANCE WITH MARKETING STRATEGY OR AD CREATION,
PLEASE CONTACT MARKETING SOLUTIONS

SR. DIRECTOR OF PROGRAM MANAGEMENT **Steve Porter**
sporter@endeavorb2b.com

ENDEAVOR BUSINESS MEDIA, LLC

CHIEF EXECUTIVE OFFICER **Chris Ferrell**

PRESIDENT **June Griffin**

CHIEF FINANCIAL OFFICER **Mark Zadell**

CHIEF OPERATING OFFICER **Patrick Rains**

CHIEF ADMINISTRATIVE AND LEGAL OFFICER **Tracy Kane**

EVP, TECHNOLOGY GROUP **Lester Craft**



X9 SPIDER

BY GENERAL MICRO SYSTEMS



COMMUNICATION
SYSTEMS

NVIS/VIDEO
PROCESSING

BLUE FORCE
TRACKING

SMART SENSOR
PROCESSING

FITS IN
BACKPACK

HEALTH
MONITORING

**THE WORLD'S MOST POWERFUL
FULL-FEATURED WEARABLE COMPUTER**



LESS THAN 3 POUNDS!

S1502-MANPACK

- Intel® Xeon® W with 64GB DDR4 ECC DRAM
- 4x Thunderbolt™ 4 with DisplayPort and 100W power
- Thunderbolt™ 4 available as copper or fiber cable with power
- NVIDIA® RTX5000 GPGPU for real-time tip-of-spear image and sensor processing
- Dual 100GigE ports with fiber for at-halt command post connectivity
- Quad M.2 to support Wi-Fi/Bluetooth, MIL-STD 1553, Cellular and GPS
- Dual M.2 high performance SSDs for up to 40TB of data storage
- 3-Axis MEMS accelerometer for Position/Navigation/Timing (PNT)
- Shock, temperature and tamper sensors for safe operations
- Features intelligent CoolTouch™ cooling for optimal comfort and battery life
- Operates via soldier batteries or single +24 VDC



SCAN TO LEARN MORE ABOUT
THE X9 FAMILY OF PRODUCTS

GMS
COMPUTING ENGINES

GMSINC.COM / (800) 307-4863

UAE orders additional systems from Airobotics for autonomous urban drone integration

BY Jamie Whitney

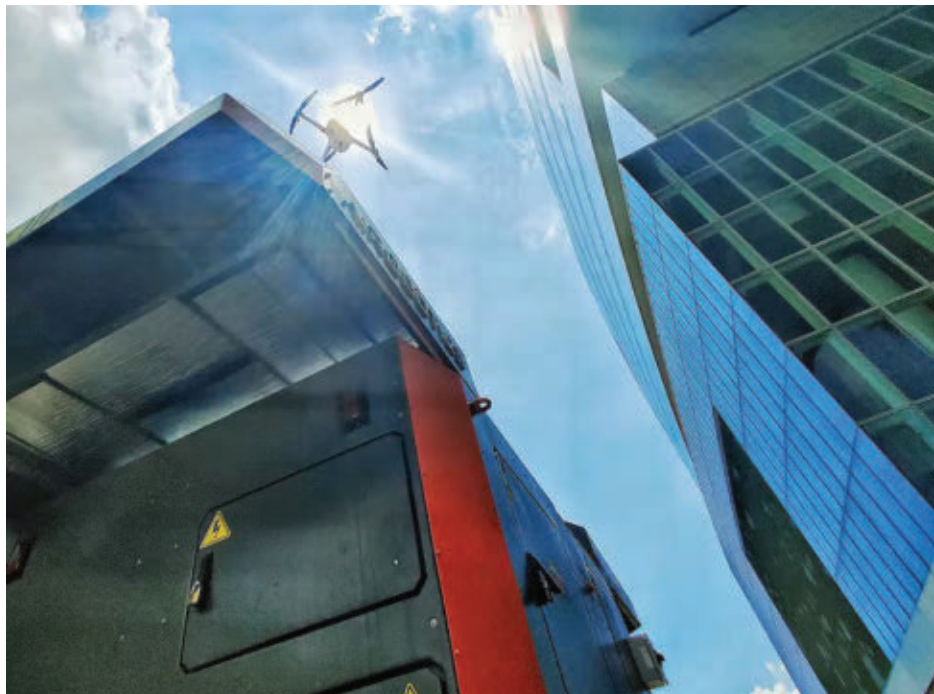
PETAH TIKVAH, Israel - Airobotics Ltd. in Petah Tikvah, Israel announced that the company has been tapped by a government entity in the United Arab Emirates (UAE) to provide additional drone systems and services. Airobotics Optimus urban drone infrastructure collects and analyzes aerial data via its automated drone infrastructure.

The Airobotics system is designed to operate as a network of smart drones linked to an urban control center and will function as a municipal infrastructure providing a variety of automated data solutions.

The primary function of the deployed urban drone infrastructure is to shorten response times of security and rescue forces to emergency situations, supporting law enforcement and homeland security activities. The company is also examining drone parcel delivery and other smart city applications to be provided by the infrastructure.

The order is a follow-on order to initial systems and services that were provided and thoroughly reviewed by the customer during the Dubai Expo. During the event, the Airobotics carried out thousands of operational drone flights without human intervention under challenging environmental conditions and in densely populated areas, to the end user's satisfaction.

Airobotics says it is active in the UAE and additional countries and has plans with other customers to establish permanent infrastructure which rely on fleets of automated drones that do not require on the ground human intervention to operate.



The Airobotics system is designed to operate as a network of smart drones linked to an urban control center.

The drones are able to operate as a taskforce that can simultaneously collect and provide critical information for a variety of customer requirements. The Airobotics drone infrastructure is designed for urban environments and strategic facilities that require immediate security, monitoring and emergency response.

Drone flights can be tasked to carry specific sensors, enabling every drone in the system to execute diverse tasks. The drones can be activated for complex longer-term operations. Flights are overseen by remote operators in a command-and-control center. ◀



Ampaire makes first flight of the company's hybrid regional aircraft

BY Jamie Whitney

CAMARILLO, Calif. - Ampaire in Los Angeles announced that its Eco Caravan, a nine-seat regional aircraft, made its first flight 18 Nov. 2022 on an integrated hybrid-electric propulsion system.

Ampaire officials say they expect the aircraft to be the first electrified regional aircraft to enter commercial service (certification in 2024) and the first in a series of larger Ampaire hybrid-electric aircraft.

The Eco Caravan upgrades the standard Cessna Grand Caravan with Ampaire's integrated propulsion system of a compression ignition engine and an electric engine. A battery pack in a body fairing preserves passenger and cargo capacity for the aircraft.

The Eco Caravan reduces fuel consumption and emissions by as much as 70 percent. Ampaire officials say the cost of operation is reduced by 25 to 40 percent depending on airline route structure, and the cost per available seat mile is near that of driving.

The hybrid-electric aircraft preserves the range/payload capability of the Grand Caravan, and in fact can fly farther than the Grand Caravan with eight passengers.

Maximum range is beyond 1,000 miles. The Eco Caravan's range and load hauling capability is in marked contrast to proposed all-electric, hydrogen-electric and even other hybrid-electric designs.

The Eco Caravan can recharge its batteries in flight or at a charging stations on the ground. Because charging infrastructure will be limited for some years, the ability to operate independent

▲ **The hybrid-electric aircraft preserves the range/payload capability of the Grand Caravan, and in fact can fly farther than the Cessna Grand Caravan while carrying eight passengers.**

of ground charging is critical for preserving the full utility of the Eco Caravan.

The Eco Caravan's propulsion technology is scalable to larger regional aircraft and ultimately to single-aisle airliners. Ampaire plans to rapidly roll out more powerful propulsion systems for larger aircraft, following a building blocks approach that will dramatically improve the sustainability of airline operations.

The first flight was 33 minutes in duration to make initial checks of the propulsion system. With test pilot Elliot Seguin at the controls, the Eco Caravan took off from Camarillo Airport north of Los Angeles at 7:49 a.m. pacific time.

It climbed to 3,500 feet at full power, combining power from the combustion engine and electric engine. Seguin then throttled back to a cruise setting, reducing load on both power sources.

He spent roughly 20 minutes testing various power settings while studying temperatures and other readings before making a descent and final approach to Camarillo at a low power setting.

"The Eco Caravan propulsion system performed just as expected," said Seguin. "It was smooth and quiet. All temperature and power output readings were normal."

Ampaire is already working with the FAA to certify the Eco Caravan in 2024 under a supplemental type certificate (STC). The Ampaire approach differs from others in that it does not require a full aircraft certification program, which can be time consuming and very expensive. The Grand Caravan is already FAA certified. Ampaire will certify it to fly with a new propulsion system. ◀

Venus Aerospace's rotating detonation rocket engine moves toward hypersonic flight

Venus Aerospace in Houston has announced it has achieved the feat of getting room temperature storable liquid fuels to operate in a Rotating Detonation Rocket Engine (RDRE). Detonation engines provide higher performance as compared to a typical rocket engine. The vehicles from Venus, which is developing both hypersonic drones and full scale, hypersonic passenger aircraft, can go faster and further than existing systems with the same amount of fuel, according to the aerospace company. Rotating detonation means the supersonic combustion happens continuously inside the engine, and our video shows the detonation wave moving around the engine at supersonic speeds. Engine testing was completed at Venus Aerospace's headquarters in Houston. The test stand was designed and built over 12 months, and all within 18 months of relocating the company from California to Houston. Proving this technology is a critical step for bringing reusable high speed commercial travel to the general public in a number of years. "Venus Aerospace continues to impress me with both their intentional approach to technology progression and buying down operational risk in years, not decades," says Jim Bridenstine, former NASA administrator, military aviator, and U.S. Congressman. "This important milestone regarding the rotating detonation rocket engine technology represents a key advancement towards real flying systems, both for defense applications and ultimately commercial high-speed travel. And they've done it in the context of building a world-class team and work experience - one that can move quickly but also with an eye towards flight test, certification, safety, and production." When operational, the Venus "Stargazer" will connect distant cities of over 5,000 miles in under an hour. Venus will begin hypersonic RDRE flight testing with a 20-foot drone to support both national security and internal technology development.

IoT SATCOM-based horse tracking collars deployed in Mongolia

Globalstar Europe Satellite Services Ltd., a wholly owned subsidiary of Globalstar, Inc. in Dublin, Ireland, announced that Mongolia-based Spotter has now deployed over 12,000 animal-tracking collars based on SmartOne C and SPOT Trace. These satellite IoT devices are being used in Mongolia, Kazakhstan and Kyrgyzstan to track and safeguard horses, including high-value competitive racehorses. The technology is seeing rapid growth, up from 1,000 Spotter devices deployed in January 2020, now up to 240,000 horses now protected. Horses are part of daily life in Central Asia and horse racing is a major sport in Mongolia. However, with the sparsely populated nation's 4.5

million horses roaming fence-free, keeping tabs on the animals is a major challenge for owners. Spotter's far-reaching technology solutions that can monitor the location of millions of horses. These animals are semi-wild, and free to range across vast expanses to graze. Spotter has developed a new hybrid IoT device that can be connected to SmartOne C. It can be fitted on specific at-risk horses and, as a result, the owner can know if the individual animal has roamed away from the herd. The system can track the breakaway horse up to a 1-kilometer radius, giving the herder the opportunity to locate and retrieve the animal before it has travelled too far. Spotter has deployed 9,000 SmartOne C-fitted collars and 3,000 built on SPOT Trace. Requirements differ among customers. The horses typically roam in herds of around 30, with one lead stallion keeping the animals together and providing protection. As a result, the group can be effectively monitored with just one collar. Spotter has created a new hybrid collar which leverages Globalstar satellite communications along with radio transmissions to create a low-cost solution that makes it possible for owners to track individual horses as well as a herd.

Rolls-Royce and easyJet hail successful hydrogen jet engine test

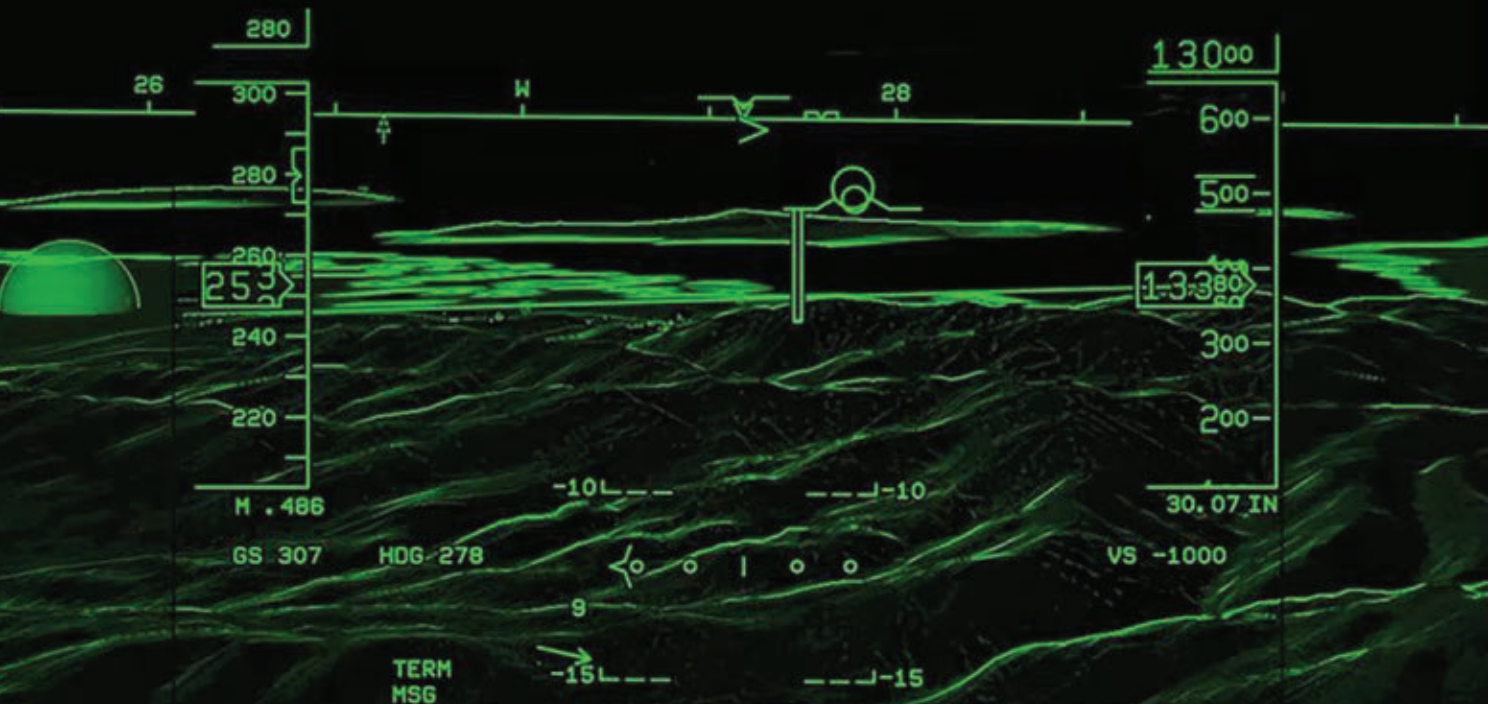
Rolls-Royce and easyJet confirmed in late November that they have set a new aviation milestone with the world's first run of a modern aero engine on hydrogen. The ground test was conducted on an early concept demonstrator using green hydrogen created by wind and tidal power. The companies say it marks a major step towards proving that hydrogen could be a zero carbon aviation fuel of the future and is a key proof point in the decarbonisation strategies of both Rolls-Royce and easyJet.

The test took place at an outdoor test facility at MoD Boscombe Down, UK, using a converted Rolls-Royce AE 2100-A regional aircraft engine. Green hydrogen for the tests was supplied by the European Marine Energy Center generated using renewable energy at their hydrogen production and tidal test facility on Eday in the Orkney Islands, UK.

Following analysis of this early concept ground test, the partnership plans a series of further rig tests leading up to a full-scale ground test of a Rolls-Royce Pearl 15 jet engine.

The partnership is inspired by the global, UN-backed Race to Zero campaign that both companies have signed up to, committing to achieve net zero carbon emissions by 2050.

"The success of this hydrogen test is an exciting milestone. We only announced our partnership with easyJet in July and we are already off to an incredible start with this landmark achievement," Grazia Vittadini, Chief Technology Officer, Rolls-Royce, said. <



Collins Aerospace announces its combined vision system for business jets achieves TSO

BY Jamie Whitney

CEDAR RAPIDS, Iowa - Collins Aerospace, a Raytheon Technologies business in Cedar Rapids, Iowa, has announced that it has achieved a technical standard order (TSO) for its combined vision system (CVS) for business aviation aircraft.

The CVS provides clarity to pilots in all types of weather to confidently and securely navigate aircraft through low visibility situations.

These CVS images are displayed conformably on the HUD and in color on the PFD, providing clarity through low-visibility conditions like smoke, fog and darkness.

Collins, a manufacturer of head-up display (HUD) technology, synthetic vision systems (SVS) and enhanced vision systems (EVS), says its advanced CVS algorithms blend the full EVS image and SVS into a single conformal view, creating the best possible image on the HUD and primary flight display (PFD) that pilots use to safely and efficiently navigate through challenging environments.

"TSO certification is an important step in our journey to provide dynamic CVS technology to our customers who rely on our vision systems to guide them through low visibility situations in

▲ **Collins Aerospace has earned a technical standard order (TSO) for the company's combined vision system (CVS) avionics suite for business jet aircraft.**

every stage of flight," said Craig Brown, general manager of Vision Systems for Collins Aerospace.

"Whether it's poor weather, smoke, dust, demanding terrain or busy airports,

CVS clearly and automatically displays the critical visual information pilots need to safely operate their aircraft," Brown says

The Collins CVS is a single enhanced view, which enables pilot visibility far beyond what the eye can see. This greatly improves situation awareness, reduces workload by eliminating the need for manual switching between vision systems and enables maximum operational credit by allowing aircraft to continue all the way to the runway surface in low visibility scenarios rather than necessitating a go-around. CVS is ready to support these future operations, such as EFVS takeoff and EFVS approaches in lower visibilities.

The Collins Vision Systems solutions are currently installed and flying on commercial and military aircraft, including the military C-130 Hercules utility turboprop and the Boeing 737 family of passenger jetliners, with future certification installments planned for additional military helicopters. ◀