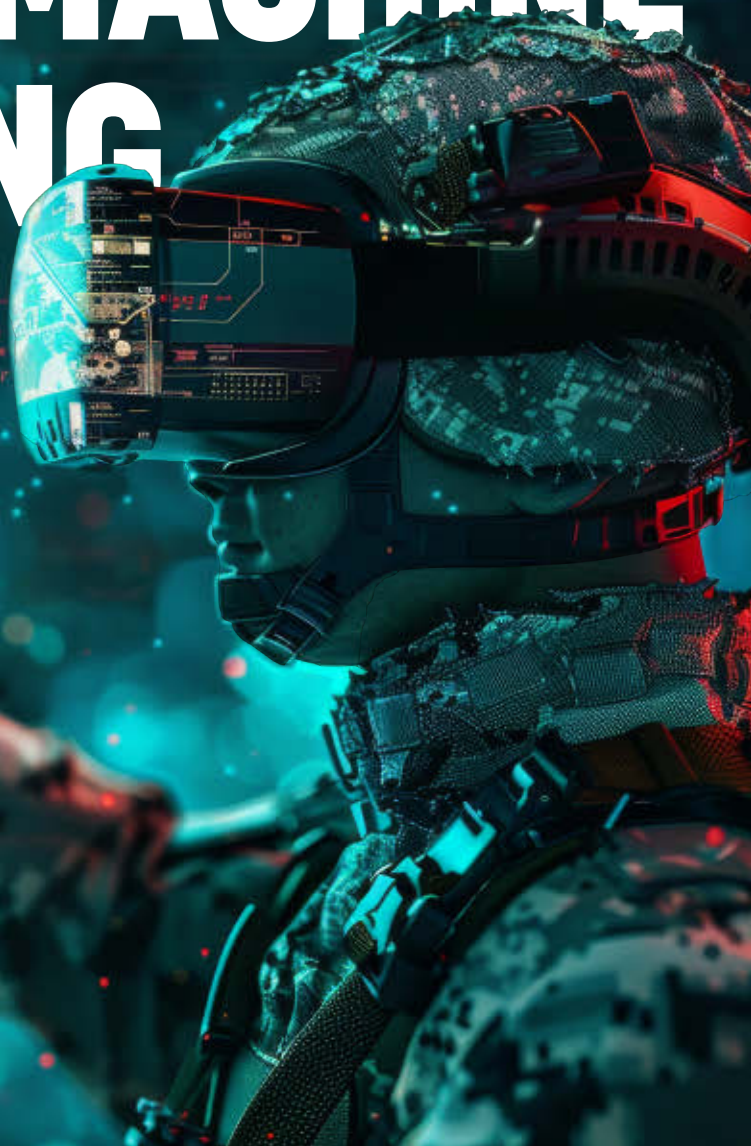


JULY/AUGUST 2024

Military+Aerospace Electronics®

AI AND MACHINE LEARNING

Artificial Intelligence can speed military command and control, target detection, and help analysts sift through sensor data. PG. 14





WHEN IT HAS TO WORK, THINK AXIOM ELECTRONICS



Military, avionics and aerospace hardware must function flawlessly in challenging environments. Robustness of the manufacturing process is a critical step in achieving that goal. Axiom Electronics assembles and tests complex circuit boards and complete systems for mission critical products, supporting our customers' needs for prototype, pilot run and production builds. Our supply chain management and engineering teams work together to identify availability or obsolescence issues during project transition. We can work from your designs using mature or newly-introduced technologies, building to virtually any standards and specifications you choose. From Earth to Mars, our manufacturing expertise is helping our customers deploy mission critical products.

Our registrations include ITAR, ISO 9001:2015 and AS 9100D.

If you are looking for a contract manufacturer expert in supporting the rigorous requirements inherent in military and aerospace hardware, give us a call at **503-643-6600** or visit our website at **www.axiomelectronics.com**.

To learn more about our manufacturing processes download our latest whitepaper, "*Critical Factors in Ensuring Solder Joint Integrity*" at **www.axiomelectronics.com/mae**.





Features

14 SPECIAL REPORT

Artificial intelligence and machine learning

AI can speed military command and control, target detection, electronic warfare (EW) and communications, and help analysts sift through mountains of sensor data.

26 TECHNOLOGY FOCUS

Trusted computing shields military computers from cyber thieves

Cyber security advances to safeguard military computers and networking from determined enemy hackers seeking to disrupt operations.

D1 DIGITAL EXCLUSIVE

Commercial Aerospace

www.militaryaerospace.com/subscribe

Columns

2 TRENDS

37 UNMANNED VEHICLES

4 NEWS

40 ELECTRO-OPTICS WATCH

6 IN BRIEF

43 PRODUCT APPLICATIONS

34 RF & MICROWAVE

46 NEW PRODUCTS

FOLLOW US



FACEBOOK.com
[/MilitaryAerospaceElectronics](https://www.facebook.com/MilitaryAerospaceElectronics)



X
[@MilAero](https://twitter.com/MilAero)



LINKEDIN.com
[/showcase/military-aerospace-electronics](https://www.linkedin.com/showcase/military-aerospace-electronics)

Cover Photo: 314995420 © Chartchai Suwanachun | Dreamstime.com

Military+Aerospace Electronics® USPS Permit 5901, ISSN 1046-9079 print, ISSN 2688-366X online, is published 6 times a year in January/February, March/April, May/June, July/August, September/October, November/December by Endeavor Business Media, LLC, 201 N Main St 5th Floor, Fort Atkinson, WI 53538. Periodicals postage paid at Fort Atkinson, WI, and additional mailing offices. POSTMASTER: Send address changes to Military+Aerospace Electronics, PO Box 3257, Northbrook, IL 60065-3257. SUBSCRIPTIONS: Publisher reserves the right to reject non-qualified subscriptions. SUBSCRIPTION PRICES: U.S. \$171 per year; Canada \$198 per year; All other countries \$224 per year. All subscriptions payable in U.S. funds.

Printed in the USA. Copyright 2024 Endeavor Business Media, LLC. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopies, recordings, or any information storage or retrieval system without permission from the publisher. Endeavor Business Media, LLC does not assume and hereby disclaims any liability to any person or company for any loss or damage caused by errors or omissions in the material herein, regardless of whether such errors result from negligence, accident, or any other cause whatsoever. The views and opinions in the articles herein are not to be taken as official expressions of the publishers, unless so stated. The publishers do not warrant either expressly or by implication, the factual accuracy of the articles herein, nor do they so warrant any views or opinions by the authors of said articles.

WWW.MILITARYAEROSPACE.COM

Mission impossible



VPX AND SOSA ALIGNED SOLUTIONS FOR ANY MISSION

LCR products enable realization of the best aspects of VPX and SOSA aligned system architectures. Integrated systems, chassis, backplanes and development platforms that help streamline the journey from early development to deployment.

Look to LCR to realize what's possible in demanding environments across a wide range of defense applications.



Find out how we can help you
achieve mission success.

SERVING CRITICAL DEFENSE
PROGRAMS FOR OVER 35 YEARS



LCR

 EMBEDDED
SYSTEMS

lcrembeddedsystems.com
(800) 747-5972

Army moves out on cannon that fires hypersonic projectiles for battlefield air defense



BY **John Keller**
EDITOR IN CHIEF

U.S. Army aerial defense experts are working with industry to develop a hypervelocity gun system able to destroy or disable high-priority targets like incoming missiles or mobile weapons launchers.

The future Hypervelocity Gun Weapon System (HGWS) will have three primary parts — a special 155-millimeter cannon able to withstand the pressures of launching munitions at hypersonic speeds; a hypersonic artillery shell with precision guidance; and a radar system able not only to detect incoming threats, but also to communicate with the hypersonic artillery shell to guide it to its targets.

Army experts got the project started in early July by issuing requests for information for the Hypervelocity Projectile (HVP); the Multi-Domain Artillery Cannon (MDAC); and the Multi-Function Precision Radar (MFPR). Industry was asked to respond to these initial requests for information by 24 July 2024.

The HGWS is to be a small, flexible hypervelocity projectile able to shoot from an Army M144 155-millimeter howitzer, as well as and Navy 5-inch deck guns on destroyers. The project is run out of the Army Rapid Capabilities and Critical Technologies Office (RCCTO) at Fort Belvoir, Va.

The Multi-Domain Artillery Cannon (MDAC) will be designed to shoot down enemy manned and unmanned aircraft, missiles, and artillery shells with hypervelocity projectiles. The MDAC air defense prototype will be a wheeled self-propelled 155-millimeter artillery system able to shoot the Hypervelocity Projectile (HVP). The HVP and its sister subsystem, the Multi-Function Precision Radar (MFPR), are being developed under separate projects as part of the future Hypervelocity Gun Weapon System (HGWS) program.

The MDAC will interface with an external Army-furnished Command and Control

Battle Manager (C2BM) and the Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS). The Army wants a company to build and deliver MDAC prototypes using existing fielded and mature technologies. MDAC will be air-, rail-, and sea-transportable per MIL-STD-1366; will be able to move rapidly for survivability; have automated high rates of fire with HVP; and have emote weapon firing; have deep magazine capacity, rapid ammunition resupply, and high operational availability. Companies interested also will demonstrate supportability, safety, and cyber security. The MDAC project also calls for a new propelling charge that makes the most of muzzle velocity performance.

The Multi-Function Precision Radar (MFPR) should perform not only search, detection, and precision tracking of incoming threats, but also provide Army hypervelocity projectiles with the ability via datalink to navigate, fuze accurately, and possibly even provide battle damage assessment.

The multi-function radar would provide accurate and low-latency detection of hostile threats and help guide future Multi-Domain Artillery Cannon System (MDACS) projectiles at long ranges and in bad weather conditions.

The MFPR must be accurate enough to help the hypervelocity projectile intercept incoming threats. What's significant is the hypervelocity projectile does not have an onboard seeker. Hypervelocity projectiles fly through the air at speeds of 8 or 9 times the speed of sound. Hypersonic munitions and aircraft travel at least five times the speed of sound.

Developing this kind of multi-function precision radar technology has the potential to help drive down the costs of air- and missile-defense munitions by enabling these weapons to operate without expensive onboard seekers and guidance systems. ◀

In-Stock & Shipped Same-Day



NEW Waveguide Standard Gain Horn Antennas

We offer a broad portfolio of in-stock, standard gain horn (SGH) waveguide antennas with either waveguide or coax connectivity that offer increased precision in wireless test and measurement.



SAME-DAY SHIPPING



CUSTOM CABLES



LIVE TECH SUPPORT

fairviewmicrowave.com
+1 (800) 715-4396

 **Fairview Microwave®**
an INFINIT® brand



Air Force asks industry for artificial intelligence (AI) high-performance computing for target tracking

BY John Keller

ROME, N.Y. — U.S. Air Force researchers are asking industry to use artificial intelligence (AI), machine learning, and machine inferencing in developing a high-performance computing (HPC) system for next-generation target tracking that uses a plethora of data sources.

Officials of the Air Force Research Laboratory Information Directorate in Rome, N.Y., have issued a presolicitation (FA875024S7004) for the Advanced Tracking Architecture Using AI (ATA-AI) project.

From industry, the ATA-AI project seeks algorithms and applications for 3D pixel, vector, and point cloud processing and accelerations on high-performance computing systems; and ways to use AI and machine learning for identification, classification, and pattern learning from signals and image intelligence.

The project also asks industry to develop ways to synthesize signals from satellite and inertial navigation, RF identification trackers, or telematic-based data into traffic tracks that can measure how an adversary uses lines of communication.

In addition, the ATA-AI target tracking project asks industry to develop ways of processing cell phone, satellite and inertial navigation, RF identification trackers, accelerometers, altimeters, and personal fit devices into graphic data that first responders

▲ The ATA-AI project seeks ways to synthesize signals from satellite and inertial navigation, RF identification trackers, or telematic-based data into traffic tracks that can measure how an adversary uses lines of communication.

can use to locate people in disaster areas based on last known location from their personal devices.

For now, Air Force researchers are asking industry to submit white papers. Those submitting promising white papers will be invited to submit formal proposals. Several awards are expected for this program that will be worth about \$99 million over the next four years.

Companies interested should email white papers to the Air Force's Carolyn Sheaff at AFRL.RIEDBAA.2024@us.af.mil and Peter Rocci at AFRL.RIEDBAA.2024@us.af.mil no later than 30 Nov. 2028.

Email technical questions or concerns to Carolyn Sheaff at AFRL.RIEDBAA.2024@us.af.mil and Peter Rocci at AFRL.RIEDBAA.2024@us.af.mil. Email business questions to Amber Buckley at Amber.Buckley@us.af.mil. More information is online at <https://sam.gov/opp/6c4457cee0ca48f-09c0331e635711c53/view>. ←



PICO

ELECTRONICS

DC-DC CONVERTERS

Your Path to Optimized Designs

Outputs to 10,000 VDC - Optimize Your Designs, Custom Units Available

- Outputs to 10,000 VDC, 1-300 Watt Wide Input Voltages Available
- Programmable Regulated Proportional Isolated
- Over 2,500 Standard Modules including Surface Mount
- Ruggedized Encapsulated for Harsh Environments

Optional Military Upgrades Available:

Expanded Operating Temperature
Selected MIL-STD Screening Options

PICO
ELECTRONICS

Engineering Assistance:
info@picoelectronics.com

800-431-1064

www.picoelectronics.com


TÜVRheinland
Precisely Right.

Certified to
AS9100D
ISO 9001:2015


ANAB
ACCREDITED
ISO/IEC 17021
MANAGEMENT SYSTEMS
CERTIFICATION BODY



Air Force asks BAE Systems to help safeguard military avionics from cyber attack

BY John Keller

WRIGHT-PATTERSON AFB, Ohio – U.S. Air Force researchers needed new ways to identify and mitigate vulnerabilities to military avionics from cyber attack. They found a solution from the BAE Systems Space & Mission Systems segment in Boulder, Colo.

Officials of the Sensors Directorate of the Air Force Research Laboratory at Wright-Patterson Air Force Base, Ohio, have announced a \$30 million contract to BAE Systems for the Radio Frequency (RF) Electronic Warfare (EW) Focused Laboratory Evaluations of Critical Technologies (REFLECT) program.

BAE Systems Space & Mission Systems (formerly Ball Aerospace) joins SRC Inc. in North Syracuse, N.Y., which won a \$60 million REFLECT contract in April.

This trusted computing contract provides for exploring new and emerging concepts related to development, integration,

► **BAE Systems and SRC Inc. are exploring new and emerging technologies in cyber security, open system architecture, novel avionics, sensor technologies, and electronic warfare (EW) for avionics.**

assessment, evaluation, and demonstration of cyber security, open system architecture, novel avionics, sensor technologies, and multi-domain technologies focusing on the electric warfare piece of the avionics, Air Force officials say.

REFLECT also seeks to develop simulation capabilities necessary to develop advanced sensors and avionics technologies, develop agile electronics architecture, and expand emerging open-systems standards for military weapons. The goal is to explore new and emerging technologies related to fending-off cyber-attacks, cyber security, open system architectures, avionics, and sensors.

Lockheed Martin moves forward on hypersonic missiles for submarines and surface warships

The U.S. Navy is moving forward with developing hypersonic cruise missiles for deployment aboard surface warships and submarines to attack enemy valuable mobile targets. Officials of the Navy Strategic Systems Programs office in Washington announced a \$534 million order to the Lockheed Martin Space segment in Littleton, Colo., for systems engineering and testing for Conventional Prompt Strike (CPS) hypersonic missiles. CPS is a conventional boost-glide hypersonic missile with a two stage solid rocket motor, a hypersonic glide body, and kinetic-energy warhead. A hypersonic projectile travels at speeds of at least five times the speed of sound, or about 3,800 miles per hour. The Lockheed Martin Space is the CPS prime systems integrator. A hypersonic missile traveling at Mach 5 or faster doesn't need an explosive warhead; its kinetic energy alone is sufficient to destroy or disable nearly any target it hits. Military leaders say they plan to launch CPS from Zumwalt-class destroyers and

Virginia-class attack submarines to strike valuable mobile targets. First deployment of the CPS is scheduled for as early as 2028 aboard Virginia-class attack submarines.

NASA selects RTX's Blue Canyon Technologies to provide CubeSat buses for PolSIR mission

The U.S. National Aeronautics and Space Administration (NASA) has selected RTX's small satellite manufacturer and mission services provider Blue Canyon Technologies in Lafayette, Colo., to build two 12U CubeSat buses for NASA's PolSIR mission. The PolSIR mission will study ice clouds that form at high altitudes throughout tropical and sub-tropical regions. In addition to designing and manufacturing the bus platforms, Blue Canyon will also provide mission operations services. The PolSIR instrument – Polarized Submillimeter Ice-cloud Radiometer – will observe the full diurnal cycle of high-altitude ice clouds to improve climate forecasts and provide climate models with important insights into how Earth's atmosphere will change in *Continued on page 9*



REFLECT avionics involve manned, unmanned, autonomous, and remotely piloted vehicles; on-board intelligence, surveillance, and reconnaissance (ISR) systems; EW systems, and munitions.

The specific focus is on advanced RF and digital EW simulations, threat models, sensor evaluations, and cutting-edge technology development in the RF domain.

The contract requires BAE Systems and SRC to have Top Secret or Sensitive Compartmented Information (SCI) clearances, and deep knowledge of the information related to International Traffic in Arms Regulation (ITAR) export control regulations.

For more information contact BAE Systems Space & Mission Systems online at www.baesystems.com/en-us/capability/space-systems, or SRC at www.srcinc.com, or the Air Force Research Laboratory at www.afrl.af.mil. ←



Hermetic Microelectronic Packaging

Fully Automate Processing | Hi-Rel Automation



MicroCircuit Laboratories provides superior design, development, tooling, prototyping, testing and 24/7 on-demand technical support on the entire hermetic encapsulation process.



Learn more | 610.228.0161 | microcircuitlabs.com



Air Force asks industry for cyber security in electronic warfare (EW) and SIGINT

BY John Keller

ROME, N.Y. – U.S. Air Force cyber security experts are asking industry to develop next-generation cyber security prototypes for existing military aircraft and spacecraft; intelligence and reconnaissance; global strike; and command and control systems.

Officials of the Air Force Research Laboratory Information Directorate in Rome, N.Y., have issued an advanced research announcement for the Advanced Cyber Operations Prototypes (A-COP) project.

A-COP seeks to develop enabling technologies for an assured and trusted cyber infrastructure; for continually accessing command and control; for providing continuous situational awareness; for delivering effects-based defenses; for offering situational understanding; and for enhancing

▲ A-COP seeks to develop enabling technologies for an assured and trusted cyber infrastructure; for continually accessing command and control; and for providing continuous situational awareness.

signals intelligence (SIGINT), electronic warfare (EW), and cyber operations.

Assured and trusted cyber infrastructure begins with

proven-correct designs that are technologically immune to threats and have an autonomous ability to modify the cyber domain to avoid unforeseen attacks and emerging threats.

Continually access and exercise command and control applies to cyber assets supporting on-demand missions. Continuous situational awareness seeks to avoid most threats and attacks. Effects-based defenses means using the assured and trusted infrastructure to compute, provision, and deliver effects-based defenses automatically.

Situational understanding seeks to establish a dependency map of mission functions and threads to infrastructure.

SIGINT, EW, and cyber operations technologies include involves operational and contingency planning.

A-COP areas of interest include cloud architectures; code analysis and evaluation; cyber modeling and simulation; decision support for cyber missions; design frameworks; evaluation and measurement techniques; mobile and embedded device security; non-traditional cyber security in untrusted environments; protocol development and analysis; cyber situational awareness and risk estimation; secure development tools and techniques; standards for information exchange; trusted hardware and software; virtualization; and zero-trust computing.

Military systems of interest to the Air Force include embedded devices and firmware; mobile and bring-your-own devices; automation systems; tactical systems; and wired and wireless networks at the enterprise and tactical levels.

Air Force experts say they expect to spend nearly half a billion dollars on the A-COP project through 2028, and involve several different contractors. Deadlines for A-COP submissions are 1 Oct. 2024; 1 Oct. 2025; 1 Oct. 2026; and 1 Oct. 2027. This solicitation is open until 30 Dec. 2028.

Companies interested should email white papers to the Air Force's Thomas Parisi at afri.riga.firestarter@us.af.mil. Companies submitting promising white papers will be invited to submit full proposals.

Email business and contracting questions to Amber Buckley at Amber.Buckley@us.af.mil. More information is online at <https://sam.gov/opp/a33858f292154a5094b4f25012f4cdcf/view>. ←

Continued from page 6

the future. Each spacecraft will be equipped with radiometers that will observe the clouds' daily cycle of ice content through two separate wavelengths in two spectral bands and will fly in orbits separated by three to nine hours. Over time, these two instruments will observe the clouds' daily cycle of ice content.

Army wants to develop hypervelocity artillery shells for air defense against manned and unmanned aircraft

U.S. Army air-defense experts are asking industry to develop prototypes of hypervelocity artillery shells to defend against enemy aircraft, missiles, artillery projectiles, and unmanned aerial vehicles (UAVs). Officials of the Army Rapid Capabilities and Critical Technologies Office (RCCTO) at Fort Belvoir, Va., have issued a request for information for the Hypervelocity Projectile (HVP) project. Army officials want a company able to deliver HVP prototypes no later than fall 2027 for operational demonstrations in 2028, and later for possible deployment. Hypervelocity projectiles fly through the air at speeds of 8 or 9 times the speed of sound. The HVP for air defense applications seeks to reduce munition costs and enhance the value of wheeled 155-millimeter artillery systems firing HVPs. The HVP prototypes will communicate with off-board sensors that track the HVP and the threat to be intercepted. BAE Systems has developed a hypervelocity projectile for potential naval use. The HVP prototypes *Continued on page 13*

64 GS/s Direct RF Is at Hand!

FEATURING:

- Altera Agilex™ 9
- Jarret Electra-MA™
- Analog Devices Apollo MxFE™

3U & 6U VPX & Small Form Factors

Reduce SWaP-C & Latency!

Annapolis Micro Systems

SOSA

Tel: 410-841-2514 • www.AnnapMicro.com

NOAA taps BAE to build ocean color instrument for GeoXO constellation

BY Jamie Whitney

BROOMFIELD, Colo. – BAE Systems in Broomfield, Colo., will build the Ocean Color Instrument (OCX) for the National Oceanic and Atmospheric Administration (NOAA) Geostationary Extended Observations (GeoXO) satellite constellation.

BAE Systems will build all three hyperspectral instruments for the mission, including OCX, the GeoXO Sounder (GXS), and the Atmospheric Composition Instrument (ACX).

GeoXO aims to enhance observations made by NOAA's current Geostationary Operational Environmental Satellites-R series (GOES-R) of weather satellites. The constellation is scheduled for launch in the early 2030s and will operate through 2055.

The OCX instrument, developed by BAE Systems, is a hyperspectral imager that will provide high-spatial resolution observations of the Great Lakes and the U.S. Exclusive Economic Zone (EEZ). It will capture data across a spectrum from ultraviolet to near-infrared light, offering insights into water quality, ocean biology, chemistry, and ecosystem changes. OCX will also deliver more frequent observations, completing surveys every two hours to enhance monitoring of rapidly changing conditions.

"OCX offers exciting new capabilities that will provide NOAA and other end users with novel insights into the dynamics of our aquatic ecosystems, allowing us to better monitor endangered species, track oil spills and harmful algal

blooms, and protect key economic drivers like reef systems and fisheries," said Dr. Alberto Conti, vice president and general manager of Civil Space for BAE Systems Space & Mission Systems. "This selection reinforces our commitment to advancing scientific endeavors that directly contribute to safeguarding public health and promoting environmental sustainability."

In addition to OCX, BAE Systems is developing the GXS and ACX instruments. GXS will supply real-time data on the vertical distribution of atmospheric moisture, winds, and temperature to improve weather prediction models and short-term severe weather forecasting. ACX will conduct hourly, daytime air quality measurements to enhance air quality forecasts and track emissions such as aerosol particles, nitrogen dioxide, formaldehyde, glyoxal, sulfur dioxide, and ozone. ←

◀ **BAE Systems will build three hyperspectral instruments for the mission, including OCX, the GeoXO Sounder (GXS), and the Atmospheric Composition Instrument (ACX).**



Attracting Tomorrow



GENESYS™

Advanced Programmable DC Power

- Outputs from 10V to 1500V (1kW to 22.5kW)
- High Power Density 1kW/1.5kW in 1U Half-Rack Profile
- Worldwide AC Inputs (1 Φ /3 Φ) with Active PFC
- CV/CC/CP Limit Operation with Auto-Crossover
- Advanced Features Built-In (Waveform Generator with Auto-Trigger, Slew-Rate Control (V/I), Internal Resistance Programming, Pre-Load Control, Watchdog Timer)
- Bench-Top, Rack-Mount, Chassis-Mount w/ Zero-Stack
- Parallel Systems (up to 60kW) / Series Operation
- Built-In: LAN, USB, RS-232/RS-485 and Isolated 5V/10V Interfaces
- Optional: IEEE (488.2), EtherCAT, Modbus-TCP, Isolated 4-20mA
- Blank Front Panel Option
- Air Filter / Parallel Connection Accessory Kits
- Safety Agency Approvals/CE-UKCA Marks/5Yr Warranty

TDK-Lambda

www.us.lambda.tdk.com
www.us.lambda.tdk.com/products/programmable-power

1-800-526-2324

Army eyes radar to detect threats and guide hypervelocity munitions accurately to their targets

BY John Keller

FORT BELVOIR, Va. – U.S. Army sensors experts are reaching out to industry to find companies able to prototype a multi-function precision radar (MFPR) able not only to track enemy airborne threats, but also to guide Army hypervelocity weapons to their targets.

Officials of the Army Rapid Capabilities and Critical Technologies Office (RCCTO) at Fort Belvoir, Va., have issued a request for information for the Multi-Function Precision Radar (MFPR) project.

Army officials want a company able to deliver at least two multi-function precision radar prototypes no later than fall 2027 for operational demonstrations in 2028, and later for possible deployment.

Multi-function precision radars should perform not only search, detection, and precision tracking of incoming threats, but also provide Army hypervelocity projectiles with the ability via datalink to navigate, fuze accurately, and possibly even provide battle damage assessment.

The multi-function radar would provide accurate and low-latency detection of hostile threats and help guide future Multi-Domain Artillery Cannon System (MDACS) projectiles at long ranges and in bad weather conditions like heavy rain, snow, wind, and dust. MDACS is to be new development program next year for air and missile defense against cruise missiles and unmanned aircraft.

The MFPR is to track the cannon-fired Hypervelocity Projectile, as well as incoming threats, and help guide the munition to incoming threats using external government-furnished Command and Control Battle Manager (C2BM) and the Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS).

The MFPR must be accurate enough to help the hypervelocity projectile intercept incoming threats. What's significant is the hypervelocity projectile does not have an onboard seeker. Hypervelocity projectiles fly through the air at speeds of 8 or 9 times the speed of sound.



▲ **The Multi-Function Precision Radar will track incoming threats, and communicate with Army hypervelocity projectiles via datalink to navigate, fuze accurately, and possibly even provide battle damage assessment.**

Developing this kind of multi-function precision radar technology has the potential to help drive down the costs of air- and missile-defense munitions by enabling these weapons to operate without expensive onboard seekers and guidance systems.

The MFPR Prototypes should perform in an operational band that is available or could be available for military use worldwide; provide precision radar track data to support projectiles in flight via a communications link; provide long-range high-precision angular coverage for search detection; be able to detect threats and friendly projectiles; operable in high-clutter environments; interface with government-furnished command and control; and demonstrate supportability, safety, and cyber security.

Companies interested were asked to email unclassified white papers by 24 July 2024 to the Army's Joshua Flinn at joshua.e.flinn.civ@army.mil and Sydney Horn at sydney.m.horn.civ@army.mil. ◀

Continued from page 11

should fire from rifled and smooth-bore 155-millimeter cannons; interface with Army-provided off-board sensors to intercept the incoming threat. Companies interested were asked to email unclassified capability statements by 24 July 2024 to the Army's Joshua Flinn at joshua.e.flinn.civ@army.mil and Sydney Horn at sydney.m.horn.civ@army.mil. More information about the Hypervelocity Projectile (HVP) request for information is online at <https://sam.gov/opp/8e1e28029c9f4e5ba5fa56d52af0cba6/view>.

Honeywell acquires CAES for radiation-hardened microelectronics, military technologies

Honeywell Inc. in Charlotte, N.C., will acquire CAES Systems Holdings LLC in Arlington, Va., to boost Honeywell's electromagnetic military technologies for RF signals management under terms of a \$1.9 billion cash deal. This acquisition will enhance Honeywell's defense technologies in critical military systems like the F-35 and EA-18G military aircraft, the AMRAAM and GMLRS military weapons, radar, and uncrewed systems. Combining the two companies also can boost capabilities in radiation-hardened integrated circuits for applications ranging from military nuclear forces to so-called rad-tolerant electronic components for commercial new space uses. The Honeywell Aerospace centers in Clearwater, Fla., and Plymouth, Minn., are some of the nation's most important activities for strategic rad-hard electronics parts. CAES has a microelectronics center in Colorado Springs, Colo., with a long history in radiation-hardened microelectronics. CAES (formerly Cobham Advanced Electronic

Solutions) has 13 facilities in North America, including automated manufacturing facilities with automated test and tuning processes. For more information contact Honeywell Aerospace online at <https://aerospace.honeywell.com>, or CAES at <https://caes.com>.

Northrop Grumman moves forward with designing ballistic missile tracking satellites with infrared sensors

U.S. Space Force experts are taking another step toward deploying four new satellites to keep watch over Earth's northern polar region to provide early warning of ballistic missile launches toward the United States. Officials of the Space Systems Command at Los Angeles Air Force Base, Calif., announced a \$93.8 million order to the Northrop Grumman Corp. Space Systems segment in Redondo Beach, Calif., for Next Generation Overhead Persistent Infrared Polar (NGP) space vehicles 1 and 2. The satellites will use advanced infrared sensors to detect and track ballistic missile launches. NGP is to augment and then replace the current Space-Based Infrared System (SBIRS) missile warning constellation. The six SBIRS satellites have been operating in geosynchronous orbit since last March. These satellites are scheduled for first launch as early as 2028. Northrop Grumman and Ball Aerospace will design and develop the sensor payloads for the two NGP ballistic missile tracking satellites at Northrop Grumman's site in Azusa, Calif. The two satellites, operating in highly elliptical orbits, will use infrared sensors for missile tracking. ←

AirBorn
a i r b o r n . c o m

Introducing

Power Blade® 2300W+ VPX Power Module

AirBorn's new VPX Power Supply is a VITA 62, Open VPX compliant, 6U system with models for a 270 VDC input IAW MIL-STD-704. Power Blade is a SOSA aligned, conduction cooled, switch mode unit built for high-end defense applications.



Artificial intelligence and machine learning aim to boost tempo of military operations

AI can speed military command and control, target detection and attack, electronic warfare (EW) and communications, and help relieve human analysts of sifting through mountains of sensor data.



314995420 © Chertchai Suwanachun | Dreamstime.com
405736099 © Vladislav | stock.adobe.com

BY John Keller

Technology development in artificial intelligence (AI) and machine learning are among the highest research and development priorities for the U.S. Department of Defense (DOD) to provide enabling technologies for applications like, command, control, and situational awareness; machine autonomy and robotics; munitions guidance and targeting; image recognition; electronic warfare (EW) and communications; human and machine teaming; technology assessment, and even weather forecasting and space observation.

The past year has seen many AI and machine learning technology initiatives and development contracts to build on progress in AI made over the past several decades. While these technology still fall far short of duplicating human intelligence, they are making great strides in processing vast amounts of data quickly and efficiently; enabling unmanned vehicles to operate autonomously on the ground in the ocean, and in the air; making sense of sensor data from many different sources and synthesizing this data into actionable intelligence;

quickly recognizing targets in intelligence imagery; automating spectrum warfare tasks; and helping humans and computers work together.

Among the enabling technologies that are crucial to making the AI and machine learning vision a reality are advances in artificial neural networks; powerful general-purpose graphics processing units (GPUs); field-programmable gate arrays (FPGAs), advanced software-engineering tools; and intelligent networking of disparate sensors, data processors, and communications nodes.

AI in command and control

U.S. Air Force researchers kicked-off the Artificial Intelligence and Next Generation Distributed Command and Control project last March to apply artificial intelligence (AI) to distributed command and control in contested environments.

This project's eight technical areas are: command and control of AI to achieve mission-tailored AI; federated, composable autonomy and AI toolbox; advanced war gaming agents;

interactive learning for C4I; command and control complexity dominance generative AI C4I; software defined distributed command and control; and tactical AI.

Air Force researchers are trying to apply AI to command and control, and to consider enemy AI use in mission planning by pursuing a switch from monolithic command and control node to distributed command and control. The project focuses on adapting AI models to specific problems quickly, and to define the roles, responsibilities, and supporting infrastructure. It also seeks to develop battle management tools that bring together a distributed team of specialists to train and deploy mission-tailored AI.

The Artificial Intelligence and Next Generation Distributed Command and Control project should spend about \$99 million over the next four years, and several contract awards are expected. The project is accepting white papers until March 2027.

▼ **A U.S. Marine Corps technician uses artificial intelligence to fly an unmanned aircraft system during a squad attack range as a part of an exercise in Australia earlier this year.** Marine Corps photo


Companies interested should email white papers to each technical area's technical contact, and to the Air Force's Gennady Staskevich at gennady.staskevich@us.af.mil. Those submitting promising white papers may be asked to submit full proposals. Email technical questions to Gennady Staskevich at gennady.staskevich@us.af.mil, and business questions to Amber Buckley at Amber.Buckley@us.af.mil. More information is online at <https://sam.gov/opp/d8eb1d7f980d4c02b080d87747297ee6/view>.

Last September the Air Force kicked-off the Geospatial Intelligence Processing and Exploitation (GeoPEX) project, which proposes spending nearly \$100 million over the next two years to apply artificial intelligence and machine learning to geospatial intelligence (GEOINT) from imagery, imagery intelligence, or geospatial data and information.

GeoPEX seeks to develop enabling technologies for providing GEOINT from imagery, imagery intelligence, or geospatial data and information for military mission planning and decision-making. The project encompasses aspects of imagery and includes data ranging from the ultraviolet through the microwave portions of the electromagnetic spectrum, as



NEW Low PIM In-Building DAS Antennas



Low PIM In-Building DAS Antennas to meet the most demanding low-PIM requirements for 5G and LTE/4G bands. These low PIM in-building antennas cover 600-5800 for LTE and 5G throughout the globe.

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

In-Stock & Shipped Same-Day

pasternack.com
+1 (800) 715-4396



PE PASTERNAK
an INFINIT® brand



▲ **Unmanned aerial vehicles equipped with specialized software, artificial intelligence at an experiment last winter that showcased systems designed to enhance amphibious operations.** Navy photo

well as information derived from imagery; geospatial data; georeferenced social media; and spectral, spatial, temporal, radiometric, phase history, polarimetric data.

The project also seeks to develop analytic techniques for advanced geospatial sensor data. The goal is to take advantage of all available geospatial data from traditional and non-traditional sources to create cost-efficient actionable intelligence.

Data may come from GEOINT data from several different sources, and correlated to provide actionable intelligence for mission decisions. Sources and technologies may include knowledge-based processing; panchromatic imagery; synthetic aperture radar; bistatic radar processing; long-wave infrared sensors; multi and hyper-spectral; video; overhead persistent infrared; 3D point clouds; artificial intelligence (AI); and machine learning.

Technologies of interest include AI; machine learning; cloud-based high performance computing; artificial intelligence acceleration technologies; 3D point cloud generation; modeling and visualization; and photogrammetry technologies. Cyber security should be part of all proposals. This solicitation will be open until September 2026, and now is soliciting white papers. Companies interested should email white papers no later than 30 Sept. 2025 to the Air Force's Bernard J. Clarke at Bernard.Clarke@us.af.mil. Email questions or concerns to the Air Force's Amber Buckley at Amber.Buckley@us.af.mil. More information is online at <http://www.fbodaily.com/archive/2023/09-September/16-Sep-2023/FBO-06831325.htm>.

Buckley@us.af.mil. More information is online at <http://www.fbodaily.com/archive/2023/09-September/16-Sep-2023/FBO-06831325.htm>.

Machine autonomy and robotics

Artificial intelligence and machine learning play central roles in the latest technology developments in machine autonomy and robotics. Peraton Labs Inc. in Basking Ridge N.J., won a U.S. Defense Advanced Research Projects Agency (DARPA) contract last fall for the Learning Introspective Control (LINC) project. LINC seeks to enable AI systems to respond well to conditions and events that these systems have never seen before.

LINC aims to develop AI- and machine learning-based technologies that enable computers to examine their own decision-making processes in enabling military systems like manned and unmanned ground vehicles, ships, drone swarms, and robots to respond to events not predicted at the time these systems were designed. LINC technologies will update control laws in real time while providing guidance and situational awareness to the operator, whether that operator is human or an autonomous controller.

Today's control systems seek to model operating environments expected at design time. Yet these systems can fail when they encounter unexpected conditions and events. Instead, LINC will develop machine learning and introspection technologies that can characterize unforeseen circumstances like a damaged or modified military platform from its behavior, and then update the control law to maintain stability and control.

A LINC-equipped platform will compare the behavior of the platform, as measured by on-board sensors, continually with a learned model of the system, determine how the



▶ The U.S. Air Force experimental X-62 VISTA aircraft incorporates machine learning and specialized software to test autonomous aerial combat flying. Air Force photo

system's behavior could cause danger or instability, and implement an updated control law when required. This could be an improvement of today's approaches to handling platform damage, which places the burden of recovery and control on

the operator, whether that operator is human or an autonomous controller.

LINC will help operators maintain control of military platforms that suffer damage in battle or have been modified in

The **HIGHS** & **LOWS** of thermal management

One Part Epoxy Features Very Low Thermal Resistance
Supreme 18TC

LOW

Thermal resistance, 75°F
 $5-7 \times 10^{-6} \text{ K} \cdot \text{m}^2/\text{W}$

HIGH

Thermal conductivity, 75°F
 $3.17-3.61 \text{ W}/(\text{m} \cdot \text{K})$

THIN

Forms bond lines
as thin as 10-15 microns



MASTERBOND®
ADHESIVES | SEALANTS | COATINGS

Hackensack, NJ 07601 USA • +1.201.343.8983 • main@masterbond.com

www.masterbond.com

READY FOR SPACE BUILT FOR THE EDGE

Introducing the

VA7230

Arm® Cortex®-A72
SpaceGrade Edge Computing MPU



VORAGO
TECHNOLOGIES

voragotech.com



▲ **An Air Force technician observes Atom the artificially intelligent robotic dog as teammates operate it via remote control training at Barksdale Air Force Base, La., last fall.**

Air Force photo

the field in response to new requirements. LINC-enabled control systems will build models of their platforms by observing behavior, learning behavioral changes, and modifying how the system should respond to maintain uninterrupted operation.

LINC focuses on two technical areas: learning control by using onboard sensors and actuators; and communicating situational awareness and guidance to the operator. Learning control by using onboard sensors and actuators will perform cross-sensor data inference to characterize changes in system operation, rapidly prune possible solutions to reconstitute control under changed dynamics, and identify an area of nondestructive controllability by continually recalculating operating limits. Communicating situational awareness and guidance to the operator involves informing the operator of changes in system behavior in a concise, usable form by developing technologies to provide guidance and operating cues that convey details about the new control environment and its safety limitations. LINC is a four-year, three-phase program. Initial work involves an iRobot PackBot and a remote 24-core processor.

The remote processor has an Nvidia Jetson TX2 general-purpose graphics processing unit (GPGPU), dual-core

NVIDIA Denver central processor, Quad-Core ARM Cortex-A57 MPCore processor; 256 CUDA software cores, eight gigabytes of 128-bit LPDDR4 memory, and 32 gigabytes of eMMC 5.1 data storage. A key goal of the program is to establish an open-standards-based, multi-source, plug-and-play architecture that allows for interoperability and integration — including the ability to easily add, remove, substitute, and modify software and hardware components quickly.

Ethics in AI

The entire topic of robotics and machine automation can become controversial when people worry that these technologies might evolve to become better than human intelligence. Some people believe that AI eventually may pit humans and machines against each other in a battle of survival.

U.S. military researchers are sensitive to this issue. DARPA began the Autonomy Standards and Ideals with Military Operational Values (ASIMOV) project last February to explore the ethics and technical challenges of using artificial intelligence (AI) and machine autonomy in future military operations. ASIMOV aims to develop benchmarks to measure the ethical use of future military machine autonomy, and the readiness of autonomous systems to perform in military operations.

The rapid development of machine autonomy and artificial intelligence (AI) technologies needs ways to measure and evaluate the technical and ethical performance of autonomous systems. ASIMOV will develop and demonstrate autonomy

benchmarks, and is not developing autonomous systems or algorithms for autonomous systems. The ASIMOV program intends to create the ethical autonomy language to enable the test community to evaluate the ethical difficulty of specific military scenarios and the ability of autonomous systems to perform ethically within those scenarios.

ASIMOV will autonomy benchmarks — not autonomous systems or algorithms for autonomous systems — will include an ethical, legal, and societal implications group to advise the performers and provide guidance throughout the program. ASIMOV will use the Responsible AI (RAI) Strategy and Implementation (S&I) Pathway published in June 2022 as a guideline for developing benchmarks for responsible military AI technology. This document lays out the five U.S. military responsible AI ethical principles: responsible, equitable, traceable, reliable, and governable. Email questions or concerns about the ASIMOV project to DARPA at HR001124S0011@darpa.mil. More information is online at <https://sam.gov/opp/bebfb61ed56e4d78bdefde9575b2d256/view>.

Trust in AI

AI also can be a touchy subject when it comes to creating teams of humans and AI computers. The core issue: can humans

really trust machine intelligence, and how can humans be sure that AI is making the best decisions?

DARPA launched the Exploratory Models of Human-AI Teams (EMHAT) project last January to help answer some of these questions. This project seeks to develop modeling and simulation of teaming humans with AI to evaluate understand capabilities and limitations of such teams. EMHAT seeks to create a human-AI modeling and simulation framework that provides data that helps evaluate human-machine teams in realistic settings. The project will use expert feedback, AI-assembled knowledge bases, and generative AI to represent a diverse set of human teammate simulacra, analogous to digital twins.

Teams are critical to accomplishing tasks that are beyond the ability of any one individual, researchers explain. Insights in human teaming have come from observing team dynamics to identify processes and behaviors that result in success or failure. Comparatively little progress has been made, however,

▼ **U.S. Navy sailors recover an artificial intelligence-equipped MK 18 Mod 2 unmanned underwater vehicle following a mine hunting training exercise in Apra Harbor, Guam.** Navy photo



in applying human team analysis or in developing new ways of evaluating human-machine teams; machines traditionally have not been considered as equal members.

EMHAT researchers will capitalize on digital twins to model human interaction with AI systems in human-machine task completion; and adapting AI to simulated human behavior. While the U.S. Department of Defense (DoD) has forecast the importance of human-machine teaming, significant gaps remain in understanding and evaluating the expected behaviors of human-AI teams. The project seeks to define when, where, why, and how humans and machines can function together productively as teammates. Email questions or concerns to William Corvey, the EMHAT program manager, at EMHAT@darpa.mil.

Just last June DARPA began the Artificial Intelligence Quantified (AIQ) project to find ways to guarantee the

performance and accuracy of artificial intelligence (AI) in future aerospace and defense applications, and stop relying on what amounts to be ad-hoc guesswork.

AIQ seeks to find ways of assessing and understanding the capabilities of AI to enable mathematical guarantees on performance. Successful use of military AI requires ensuring safe and responsible operation of autonomous and semi-autonomous technologies. Still, methods for guaranteeing the capabilities and limitations of AI do not exist today. That's where the AIQ program comes in. AIQ will develop technology to assess and understand the capabilities of AI to enable guaranteed performance and accuracy, which up to now has not been possible.

The program will test the hypothesis that mathematical methods, combined with advances in measurement and modeling will enable guaranteed quantification of AI capabilities. The program will address three interrelated capability levels: specific problem level; classes of problem level; and natural class level. The state-of-the-art methods for assessment are ad hoc, deal with the simplest of capabilities, and are not properly grounded in a rigorous theory.

▼ **An Army intern tries on a virtual reality headset simulating an M2 .50-caliber Browning machine gun on an M1A2 Abrams tank at the Pentagon last summer.** Army photo





▲ **A Seagull unmanned surface vessel operates in the Persian Gulf at an unmanned and artificial intelligence integration event in 2022.** Army photo

AIQ brings together two technical areas: providing rigorous foundations for understanding and guaranteeing capabilities; and finding ways to evaluate AI models. This program to guarantee the performance of AI has two 18-month phases — one that focuses on specific problems; and the other that focuses on compositions of classes and architectures. Email questions or concerns to DARPA at AIQ@darpa.mil. More information is online at <https://sam.gov/opp/78b028e5fc8b4953acb74fabf712652d/view>.

Munitions control, guidance, and targeting

Among the chief goals of military AI and machine learning are to enable smart munitions to navigate, maneuver, detect targets, and carry out attacks with little or no human intervention. The U.S. Air Force Research Laboratory has reached out to industry for enabling technologies that would do just this.

The 2024 Air Dominance Broad Agency Announcement program, launched in January, seeks to develop modeling and simulation; aircraft integration; target tracking; missile guidance and control; and artificial intelligence (AI) for swarming unmanned aircraft. This project seeks to uncover the state of the art in 13 air munitions-research areas: modeling, simulation, and analysis; aircraft integration technologies; find fix target track and datalink technologies; engagement management system technologies; high velocity fuzing; missile electronics; missile guidance

and control technologies; advanced warhead technologies; advanced missile propulsion technologies; control actuation systems; missile carriage and release technologies; missile test and evaluation technologies; and artificial intelligence and machine autonomy.

The technical contact for each topic is Terrance Dubreus, whose email address is terrance.dubreus@us.af.mil. The technical contact is Sheli Plenge, whose email is sheli.plenge@us.af.mil. Companies interested were asked to email white papers describing their capabilities and expertise, relevant past experience no later than 2 Feb. 2024 to the Air Force's Misti DeShields at misti.deshields.1@us.af.mil. Email questions or concerns to Misti DeShields at misti.deshields.1@us.af.mil. More information is online at <https://sam.gov/opp/f7fac729dbf543ee8d31256c5c71bba5/view>.

The U.S. Army also is interested in AI-aided target recognition and detection. The Army Tank-Automotive & Armaments Command (TACOM) in Warren, Mich., sent out a request for information last December for the Aided Target Detection and Recognition (AiTDR) project, which seeks to develop machine-learning algorithms to reduce the time it takes to detect, recognize, and attack enemy targets. AiTDR seeks to shorten sensor-to-shooter engagement



▲ **An Army technician assigned to the Army Futures Command's Artificial Intelligence Integration Center, conducts field testing with the Inspired Flight 3 drone at Fort Irwin, Calif. in October 2022, to demonstrate autonomy, augmented reality, tactical communications, advanced manufacturing, unmanned aerial systems, and long-range fires.** Army photo

time with machine learning algorithms. The RFI seeks to understand the state of aided target recognition technology to detect trained and untrained new targets.

Traditional machine learning techniques focus on aided target recognition, Army researchers say. This requires a large training image database of target images captured under conditions such as background terrain, target pose, lighting, and partial occlusion. This limits the ability to detect new targets or trained targets under untrained new conditions. The emphasis of the AiTDR project is on detecting generic classes of targets, rather than on identifying specific targets with the risk of missing a target because of insufficiently trained algorithms. Achieving this will help accelerate engagement times and optimize crew performance by developing reliable, intuitive, and adaptive automated target detection for crewed vehicles by no later than 2026.

Companies interested were asked to respond by last January to the Army's Ashraf Samuel at ashraf.i.samuel.ctr@army.mil and Edlira Willer at edlira.willer.civ@army.mil. More information is online at <https://sam.gov/opp/d3ddaa9d736a4fcab76a0ae5cdf5a6cd/view>.

AI in communications and electronic warfare

Electronic warfare (EW) and communications present important opportunities for AI and machine learning. To the point, AI offers the potential to speed-up EW and communications, and enable U.S. and allied forces to carry out operations much more quickly than the enemy.

Last fall SRI International in Menlo Park, Calif., and the University of Southern California (USC) in Los Angeles won DARPA contracts for the Processor Reconfiguration for Wideband Sensor Systems (PROWESS) project to develop high-throughput streaming-data processors that reconfigure themselves within 50 nanoseconds for advanced RF applications in radar, communications, and EW.

SRI International and USC researchers are developing reconfigurable processors that provide autonomous RF and microwave systems with situational awareness about complex and uncertain electromagnetic environments. PROWESS aims at RF autonomy, where radios use AI to sense the

spectrum and adapt to the environment. RF autonomy can help resist the effects of radio interference and improve the capacity of the spectrum to accommodate an increasing number of transceivers.

Although the preferred processors for today's autonomous radios are field programmable gate arrays (FPGAs), signal environments can change in nanoseconds, which is far faster than FPGAs can reprogram. What are necessary are new classes of receiver processors. PROWESS aims to develop high-throughput, streaming-data processors that reconfigure in real time to detect and characterize RF signals. Through processors that self-reconfigure within 50 nanoseconds, PROWESS will enable real-time synthesis of processing pipelines in uncertain environments. PROWESS will help enable future radio receivers to optimize performance to measured spectrum conditions and the needs of cognitive RF decision logic.

High-throughput streaming-data processors can enable just-in-time synthesis of receiver processing pipelines in uncertain environments where pre-programmed solutions are likely to fail, DARPA researchers say. PROWESS is expected to combine emerging high-density reconfigurable processing arrays with embedded real-time schedulers to expose new architectural tradeoffs that deliver fast program switching and high-compute density.

The PROWESS project seeks create reconfigurable processors to improve RF autonomy by enhancing spectrum sensing, which enables RF systems to optimize to actual spectrum conditions and react to interference in real time, DARPA researchers say. These kinds of computer architectures potentially offer significant benefits for spectrum sensing and related applications, particularly when systems must operate in dynamic and sometimes-confusing environments. PROWESS expects to focus on the development of runtime reconfigurable processing hardware and support software.

Just last June Geon Technologies LLC in Columbia, Md., won a \$9.9 million order from the U.S. Air Force Research Laboratory to develop small and lightweight real-time 5G communications signal processing for command and control. Geon experts will develop real-time signal processing for command and control, and size-, weight-, and power-constrained systems to capitalize on next-generation 5G communications waveforms and technologies.

Geon will focus on developing a 5G scanner to map out the 5G radio frequency environment and develop cyber security technologies for 5G communications. Geon specializes in RF communications for military and intelligence applications. The company's expertise revolves around software-defined



MACHINE-AUTOMATION

For more information on AI and machine learning search for "machine automation" at www.militaryaerospace.com

radio applications; field-programmable gate array (FPGA) and digital signal processing (DSP) chips; signal processing, and geolocation techniques.

Last fall Vadum Inc. in Raleigh, N.C., won a contract from the U.S. Naval Surface Warfare Center Crane Division in Crane, Ind., for the Reactive Electronic Attack Measures (REAM) project to develop detection and classification techniques that identify new or waveform-agile radar threats using AI and machine learning to respond automatically with an EW attack.

Waveform-agile radar is able to change the time, frequency, space, polarization, and modulation of its signal from pulse to pulse to enhance its sensitivity, or to confuse potential adversaries about its design and use. The company is looking into software algorithms that provide EW protection against new and unknown threats, as well as the capability to characterize unknown radar threats, and scalable and modular capability to support additional platforms.

Today's airborne EW systems are proficient at identifying analog radar systems that operate on fixed frequencies. Once they identify a hostile radar system, EW aircraft can apply a preprogrammed countermeasure technique. Yet the job of identifying modern digitally programmable radar variants using agile waveforms is becoming more difficult. Modern enemy radar systems are becoming digitally programmable with unknown behaviors and agile waveforms, so identifying and jamming them is becoming increasingly difficult.

New approaches like REAM seek to enable systems to generate effective countermeasures automatically against new, unknown, or ambiguous radar signals in near real-time. They are trying to develop new processing techniques and algorithms that characterize enemy radar systems, jam them electronically, and assess the effectiveness of the applied countermeasures.

The Northrop Grumman Mission Systems segment in Bethpage, N.Y., won a \$7.3 million contract in 2018 to develop machine-learning algorithms for the REAM program. The company is moving machine-learning algorithms to the EA-18G carrier-based electronic warfare jet to counter agile, adaptive, and unknown hostile radars or radar modes. REAM technology is expected to join active Navy fleet squadrons around 2025. ◀



Trusted computing shields military computers from cyber thieves

► While “zero trust” security is often associated with enterprise systems, it also is applicable to embedded systems in the field. Dreamstime.com photo

316999522 | Center © Andrei Dzemizdenka | Dreamstime.com

Trusted computing technology advances to safeguard military computers and networking from determined enemy hackers seeking to disrupt operations.

BY Jamie Whitney

In an era where cyber threats pose significant risks to national security, the military embraces trusted computing to safeguard its technology systems. This approach involves rigorous security to ensure the integrity, confidentiality, and reliability of computing environments used in the military.

With trusted computing, U.S. military leaders aim to protect sensitive information and maintain operational security against increasingly sophisticated cyber attacks.

Hardware-based security

Trusted computing in military technology systems begins with hardware-based security. This involves the use of secure hardware components, such as Trusted Platform Modules (TPMs), which provide a root of trust. These components are capable of securely storing cryptographic keys, passwords, and other critical data, and form the foundation of a secure computing environment.

Richard Jaenicke, director of marketing at Green Hills Software in Santa Barbara, Calif., explains that the U.S. Department of Defense (DOD) is driving the development of a unified alignment between government and industry stakeholders on “zero trust.”

The concept of zero trust fundamentally changes the approach to network security. Unlike traditional models that assume everything inside the network is trustworthy, zero trust operates on the principle that no entity — whether inside or outside the network — should be trusted automatically.

“In November 2022, the Zero Trust Portfolio Management Office (ZT PfMO) within the DOD chief information office (CIO) released the DOD Zero Trust Strategy and Roadmap,” Jaenicke points out. “That roadmap includes the intent to implement almost a hundred different zero trust capabilities and activities by 2027. However, the director of the ZT PfMO, Randy Resnick, has said his office received pushback



▲ An Oklahoma Army National Guardsman from the 205th Network Signal Company, 45th Field Artillery Brigade, wins the annual “NetWars” games during the Cyber Shield training event earlier this year. North Carolina National Guard photo

a need to codify its role in the government-wide race toward network security. To that end, he said we should expect a ‘directive type’ memo that will give his office more authority to put pressure on the Defense Department to meet cybersecurity deadlines.”

Although zero trust mostly is associated with enterprise systems, Jaenicke says, it also is applicable to embedded computing systems in the field. “Most deployed embedded systems implement perimeter-based security, often as simple as a user ID/password combination granting broad admin-level privileges to change the configuration and security posture of the system, Jaenicke says. “Implementing zero trust starts with assuming that those perimeter defenses can be breached and not implicitly trusting any application already inside the perime

A firm base

This zero-trust approach has changed the thinking on what vulnerabilities are front-of-mind for the DOD, says Massimiliano De Otto, senior field application engineer at

Wind River Systems in Alameda, Calif.

“In the military sector, major threats come from DoS [denial of service] attacks and the compromising of a system by injecting malware. There has been a change in perspective over time,” Wind River’s De Otto says. “For example, in the past, people working on these systems were often considered trusted. This is not the typical scenario any longer. The introduction of zero-trust architecture in the infrastructure, more stringent secure coding standards, and continuous monitoring of deployed devices in the field are common practices. While this may be challenging in some specific areas, it has often become necessary to prevent or mitigate bigger problems.”

Another key aspect is secure boot, a process that ensures the system only boots using software that is trusted and verified. This mechanism prevents malicious software from being loaded during the startup process, thereby maintaining the integrity of the system from the outset.

“The most secure embedded systems use a hardened separation kernel to isolate applications, providing a base for zero trust,” says Green Hills’s Jaenicke. “Each application is isolated in a partition such that any breach or malware in one partition is guaranteed not to migrate or affect an application in any other partition. A separation kernel limits access to the least privilege necessary to get the job done. It also follows a policy of ‘deny by default,’ allowing

only pre-approved information flow between partitions as defined in a static configuration file. Separation kernels have a very small attack surface and can be small enough to enable security evaluation of each line of code.”

Jaenicke says that Green Hills’s INTEGRITY-178 separation kernel has a formal proof of correctness. “The INTEGRITY-178 tuMP secure RTOS runs on a variety of ARM cores, including the Cortex-A53 found in many FPGAs, and has available security life-cycle evidence to support system certification. INTEGRITY-178 tuMP is designed to Common Criteria EAL 6+ and NSA defined “high robustness” for resiliency against threats from well-funded and determined actors such as hostile nation-states.”

Airborne approach

De Otto from Wind River notes a convergence between traditional trusted computing and conventional computing.

“In other words, there is more awareness that cyber threats can happen everywhere and that the impact caused by them can be catastrophic. As a result, almost any new design in the military sector must consider security aspects,” De Otto



▲ Rich Jaenicke from Green Hills Software says that the approach avionics suppliers took in avoiding unproven hardware mechanisms that are in complex CPUs when achieving high design assurance levels (DALs) are now being embraced in designing systems with high security outside of the airborne realm. 304786414 © andrbk | Dreamstime.com



ARINC 818

Avionics & Mission System Building Blocks

ARINC 818 Provides High-Speed, Low-Latency, Uncompressed Digital Video Used in Sensors, Processors, & Displays.

Integrate legacy equipment using HDMI, SDI, and RS-170 interfaces with EO/IR sensors, processors, and displays that use ARINC 818-3.

Multi-Channel Video Converter Module



Customizable for protocol conversion, switching, splitting, concentration, & resizing

Embedded Converters



Embed directly into displays, processors, or sensors with customizable form factors



says. “This can be disruptive in specific areas, such as avionics since it is mandatory to adopt security strategies following the ED-20x/DO-3xx set of documents issued by [civil regulators] EuroCAE and FAA. New processes must be put in place, and different skills and mindsets need to cooperate.”

While avionics designers are avoiding unproven hardware in complex CPUs in high design assurance levels (DALs), Jaenicke says, this approach is being embraced for high security computing outside of airborne electronics.

“The reason for avoiding such so-called ‘novel’ hardware is the difficulty in proving the assurance level and integrity of those mechanisms, Jaenicke explains. “An example of a well-understood and proven CPU mechanism is the memory management unit (MMU), which is a cornerstone of safety and security that partitions memory address space. On the other hand, an example of a novel hardware mechanism is single root I/O virtualization (SR-IOV). SR-IOV

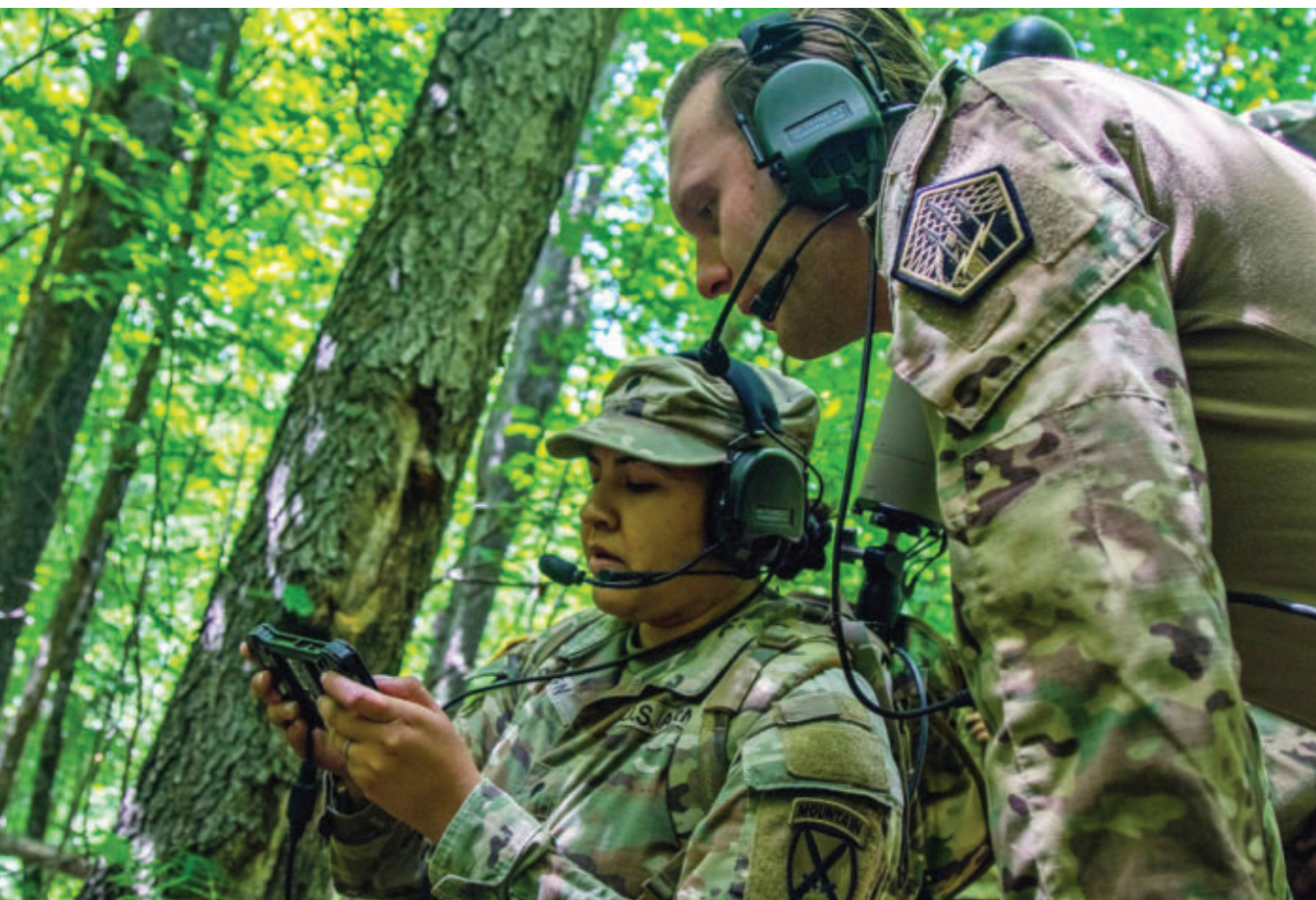
is a hardware-based virtualization solution that allows one physical PCI Express device to be used by multiple virtual machines simultaneously without the mediation from the hypervisor, thus significantly decreasing the overhead of I/O virtualization.

Jaenicke continues, “However, the safety and security of SR-IOV hardware have not been shown. To the contrary, several Critical Vulnerabilities and Exposures (CVEs) have been filed related to SR-IOV, and the NSA has banned SR-IOV from use in cross domain systems (CDS), which protect National Security Systems (NSS). Some hypervisors require SR-IOV to operate, so software developers should be careful to choose a virtualization solution that does not. For example, the virtual machine monitor (VMM) for the INTEGRITY-178 tuMP RTOS does not use SR-IOV.”

Looking back

With zero trust joining most modern technology, there still are concerns with safety and security in legacy military systems, in which security problems remain difficult to spot because of the proprietary software employed, De Otto says. Because of

▼ **A U.S. Army electromagnetic warfare (EW) specialist helps a colleague with the 10th Mountain Division Artillery Brigade calibrate EW equipment at Fort Drum, N.Y.** Army photo





▲ A U.S. military network cryptologic technician helps a high school student complete cyber security challenges.

the proprietary nature of some legacy systems, issues may not be listed on standard knowledge repositories like the National Vulnerability Database.

“However, in general, it is still possible to use the practices adopted for current developments: using vulnerability scanners and performing static analysis of all the code or

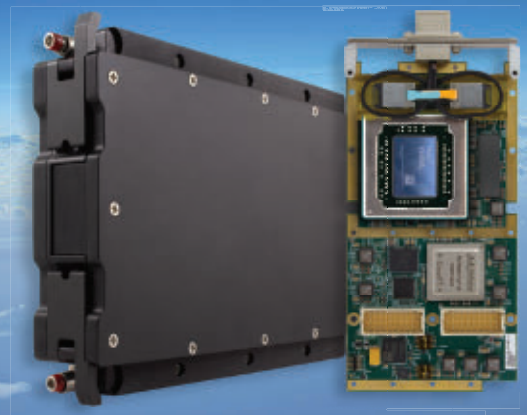
NWD New Wave Design

Tel: +1.952.224.9201

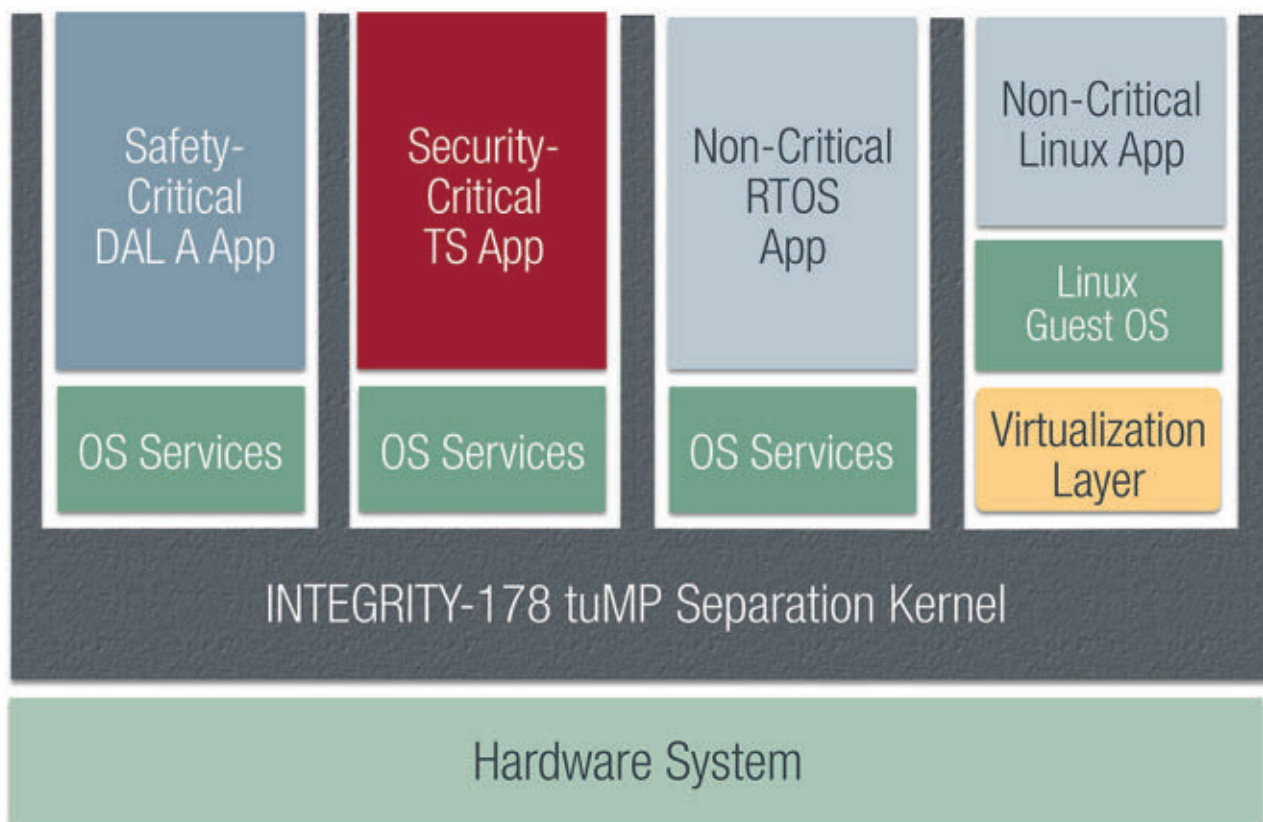
info@newwavedv.com

www.newwavedv.com

Delivering Intelligent Computing Solutions at the Edge



3U VPX & XMC Experts



▲ **The Green Hills Software INTEGRITY-178 tuMP is designed to Common Criteria EAL 6+ and NSA defined high robustness for resiliency against threats from well-funded and determined adversaries.** Green Hills photo

adopting threat analysis methods - such as MITRE,” De Otto says. “Difficulties arise when legacy code is written in languages that are different than C, C++ or Ada, such as FORTRAN. Manual analysis is required in that case and that might be impractical, time-consuming, or too expensive. Mitigation can be also challenging, since mechanisms to allow on-line updates, or updates in general, might not be available. A general strategy for a legacy system is difficult. They typically must be addressed on a case-by-case basis.”

Eyes on AI

As industry looks for ways to harness the potential of machine learning (ML) and artificial intelligence (AI), secure systems used by commercial aviation and military branches will be later to adopting both until their relative safety can be assured.

“The trend of AI is growing, and it is already being used in software development, as in the case of security scanners adopt AI to analyze and identify potentially misbehaving code,” says De Otto at Wind River. “However, AI is currently

scarce in deployed systems, because there are many concerns about the security of AI itself, and there are challenges in terms of protecting AI itself from external attacks. This is a work in progress and as AI’s role continues to grow, it will be important to use it within the context of proper regulations.”

Jaenicke at Green Hills says that ML “excels at pattern matching and can improve the efficiency and effectiveness of intrusion detection and response based on predictive variations of known attacks. Generative Artificial Intelligence (GenAI) can be used to speed decision-making when intrusions are detected.

“A big challenge with intrusion detection is keeping up with the data flow for 100 Gigabit Ethernet. FPGAs are ideal for this type of high-performance, real-time computation, which involves identifying multiple patterns in each of tens of thousands of intrusion signatures. The security of the intrusion detection system itself also is a key consideration. Luckily, modern FPGAs are the most secure type of programmable hardware, often being used to enhance secure boot capability for CPU systems. Having a secure operating system running on the FPGA’s processor cores adds another layer of security assurance.”

Green Hills’ Jaenicke says that while GenAI still is in its early developmental stages, it shows potential for offering

insights to security analysts regarding the type and extent of detected threats and recommended responses. Although the large models supporting GenAI are trained on GPUs, high-performance CPUs can be a more cost-efficient option for running the inference engine, especially for specialized models. Securing these inference engines is challenging due to the large attack surface of both the hardware and software involved.

At the edge

Edge computing is a distributed computing concept that moves computation and data storage closer to the data source, such as sensors, mobile devices, or local servers. This approach improves response times and saves bandwidth by processing data at the edge of the network instead of relying solely on centralized data centers.

Despite its advantages, edge computing introduces unique security challenges. Unlike centralized systems, edge computing involves multiple distributed devices and nodes, each requiring security measures. This decentralized architecture increases the attack surface, making it more difficult to protect the entire system.

Data processed at the edge can be sensitive, necessitating robust encryption both at rest and in transit to ensure data integrity and confidentiality, preventing unauthorized access and data breaches. Edge devices, such as IoT sensors and mobile devices, are often less secure than traditional data center equipment. Therefore, these devices need strong security measures, including secure boot, firmware updates, and physical security, to prevent tampering.

De Otto from Wind River says that his company's edge products like VxWorks, Wind River Linux, and the Helix Virtualization Platform "provide all the most recent security technologies that customers can implement in their applications, as well as compliance to established methodologies such as NIST SP800-53, DO-3xx and more."

He continues, "Wind River puts a strong focus on security in all phases of the Software Development Life Cycle. For example, Wind River has established alignment with [the] NIST SP 800-218 publication 'Secure Software Development Framework (SSDF)' across our products. Our secure development life cycle (SDL) is aligned with NIST 800-218 principles: prepare the organization, protect the software, produce well-secured software, and respond to vulnerabilities."

Continuous monitoring and auditing are essential for detecting and responding to potential security incidents.



CYBER SECURITY

For more information on trusted computing, search for "cyber security" at www.militaryaerospace.com

By maintaining logs and monitoring systems for suspicious activity, the military can swiftly address any threats that arise, thus enhancing overall security.

Compliance with established security standards and protocols, such as those set by the National Institute of Standards and Technology (NIST) and the DOD ensures a baseline level of security. Adhering to these standards helps maintain consistency and reliability across all military technology systems.

Through comprehensive measures, trusted computing aims to fortify military technology systems against a wide range of threats, ensuring the reliability and security of critical operations and information. ←

AS 9100D / ISO 9001:2015 CERTIFIED

**PHALANX II:
THE ULTIMATE NAS**

Supports AES-256 and FIPS140-2 encryption

Utilizing two removable SSDs, the Phalanx II is a rugged Small Form Factor (SFF) Network Attached Storage (NAS) file server designed for manned and unmanned airborne, undersea and ground mobile applications.

www.phenixint.com





Boeing, BAE Systems to help F-15 operate against modern electronic warfare (EW) threats

BY John Keller

WRIGHT-PATTERSON AFB, Ohio – U.S. Air Force airborne electronic warfare (EW) experts are the Boeing Co. and BAE Systems to provide EW systems for the U.S. F-15E jet fighter-bomber under terms of a \$21.3 million 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 St. Louis to install the F-15 Eagle Passive/Active Warning and Survivability System (EPAWSS) on F-15E aircraft.

The BAE Systems Electronic Systems segment in Nashua, N.H., is the primary designer and manufacturer of the F-15 EPAWSS airborne EW avionics.

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

The updated EW avionics improves pilot situational awareness with the capability to autonomously detect, identify,

▲ **EPAWSS enhances situational awareness about when the aircraft is targeted, using advanced techniques to counter modern integrated air defense systems.**

and locate threat systems, and then deny, degrade, and disrupt those threats.

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

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. This order brings the total value of this EPAWSS contract to Boeing and BAE Systems to \$805.5 million.

On this order Boeing and BAE Systems will do the work in Nashua, N.H., and should be finished by November 2025. For more information contact BAE Systems Electronic Systems online at www.baesystems.com/en-us/product/eagle-passive-active-warning-survivability-system-epawss, Boeing Defense, Space & Security at www.boeing.com/company/about-bds, or the Air Force Life Cycle Management Center www.afllcmc.af.mil. ◀

Researchers ask industry for low-SWaP-C antennas to help detect and track elusive targets

BY John Keller

ARLINGTON, Va. – U.S. military researchers are asking industry for ideas in next-generation antennas to find difficult and elusive targets of interest.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., has issued a solicitation for the Bringing Classified Innovation to Defense and Government Systems (BRIDGES) Topic Area Addendum 1 – Next Generation Antennas project.

Finding, tracking, and engaging targets requires the ability to detect, track, and maintain that track across different sensors for air, land, and space applications, researchers say.

Today's sensors have shortcomings that limit their capabilities in high-quality persistent sensing at low-cost and low-power. Instead, DARPA is seeking new antenna design, materials, manufacturing, or processing with significantly increased performance and substantial reduction in size, weight, power, and cost (SWaP-C) for air and space applications.

Companies interested should email proposals no later than 12 July 2024 to NexGenAntennas_BRIDGES@DARPA.mil. Email questions or concerns to BRIDGES@darpa.mil. More information is online at <https://sam.gov/opp/f8e712ad896e424e8a4ce5747921fb82/view>. ←



▲ **DARPA wants the ability to detect, track, and maintain that track across different sensors for air, land, and space applications.**

Airport security experts ask industry for open-architecture threat detection

U.S. airport security experts are reaching out to industry to find companies able to provide open-architecture enabling technologies in a future connected transportation security system of systems. Officials of the Transportation Security Administration (TSA) of the U.S. Department of Homeland Security in Springfield, Va., have issued a request for information (TSA25-04-03789) for the agency's Open Architecture Initiatives program. TSA's primary technology interests are digital imaging and communications in security image data; detection algorithms; common workstations; and threat image projection. Detection

algorithms seek to enable rapid deployment and evaluation of enhanced and new anomaly and threat detection algorithms. TSA's open-architecture approach seeks to use standardized interfaces, data formats, communication protocols, and related solutions, and to establish infrastructure to make security screening data accessible, interoperable, and reusable. Agency leaders seek to use commercial-off-the-shelf (COTS) products as much as possible. Companies interested were asked to email responses by June to the TSA's siobhan.mullen at siobhan.mullen@tsa.dhs.gov, and to Siobhan Lawson at siobhan.lawson@tsa.dhs.gov. More information is online at <https://sam.gov/opp/fbe7075cb182462eb-3c0c66d827a2b7d/view>. ←



Wanted: airborne EW situational awareness software that runs on SOSA-aligned computers

BY John Keller

WRIGHT-PATTERSON AFB, Ohio – U.S. Air Force electronic warfare (EW) experts are reaching out to industry for software to help aircraft pilots understand and manage electromagnetic situational awareness for airborne EW.

Officials of the Air Force Research Laboratory at Wright-Patterson Air Force Base, Ohio, have issued a solicitation (FA2385-24-S-9760) for the Ephemeral Paragon (E-Gon) program.

E-Gon seeks an advanced software suite of tactical single-ship EW capabilities to provide an enhanced understanding of the electromagnetic operating environment with a focus on algorithm adaptation, EW system management, and data management of the electromagnetic operating environment.


Researchers are asking for industry to develop E-Gon computer hardware for the E-Gon program that complies with the Sensor Open Systems Architecture (SOSA), Open Mission systems (OMS), and Big Iron open-systems standards.

▲ **Enabling technologies for the E-Gon program may go into military systems like the future Compass Call electronic-attack aircraft, shown above.**

The E-Gon's five technical areas and details are in a controlled unclassified document available to companies with the proper clearances. Email a request for the program's statement of objectives to the Air Force's Paul Repasky at paul.repasky@us.af.mil.

The Air Force will award one contract for each of the five technical areas. Each technical area will mature existing government-owned algorithms until technologies are mature enough for prototype demonstration in a real-world environment. Ultimately, the project seeks to mature E-Gon software sufficiently to enable one systems integrator to build the software into a tactical platform.

Companies interested were asked to email five-page white papers by 7 June 2024 to the Air Force's Paul Repasky at paul.repasky@us.af.mil. Email technical questions or concerns to Paul Repasky at paul.repasky@us.af.mil, and contracting questions to the Air Force's Colleen McDonald at colleen.mcdonald@us.af.mil. More information is online at <https://sam.gov/opp/defecd8bbf814f258913b6735789cedd/view>. ◀



► Avionics upgrades are expected to enable the Navy E-2D carrier-based surveillance aircraft to team closely with unmanned aircraft.

Navy asks Northrop Grumman for avionics upgrades to team E-2D with unmanned aircraft

BY John Keller

PATUXENT RIVER NAS, Md. — U.S. Navy aviation experts needed avionics computer and display upgrades to enable the E-2D surveillance aircraft to team with unmanned aerial vehicles (UAVs) during aircraft carrier operations. They found their solution from Northrop Grumman Corp.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., announced plans Friday to contract with Northrop Grumman Corp. Aeronautics Systems segment in Melbourne, Fla., provide software and hardware upgrades to E-2D mission computers and displays to demonstrate manned and unmanned teaming (MUM-T) capability. The value of the contract has yet to be negotiated.

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

The 18-month sole-source contract also will include technical support to update the E-2D mission computers and displays to process and display additional Joint Range Extension Applications Protocol (JREAP) messages.

MUM-T involves a standardized systems architecture and communications protocol that enables the sharing of live and still images gathered from UAV sensor payloads. MUM-T enables manned aircraft to connect with UAVs to enhance decision-making and mission effectiveness, and offer new levels of interoperability among ground forces, manned aircraft, and UAVs.

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

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

Northrop Grumman officials call the E-2D reconnaissance aircraft a “digital quarterback” to sweep ahead of Navy

aircraft carrier strike groups, manage missions, and keep U.S. network-centric carrier battle groups out of harm's way. The aircraft provides battle management, theater air and missile defense, and multi-sensor fusion capabilities.

Compared with its E-2C predecessor, the E-2D has a new radar with mechanical and electronic scanning capabilities; glass cockpit; advanced identification friend or foe (IFF) system; new mission computer and tactical workstations; electronic support measures enhancements; and modernized communications and data link suite, Northrop Grumman officials say.

The plane is nearly 58 feet long, has an 80-foot wingspan, can fly faster than 300 knots, and can fly to altitudes as high

as 37,000 feet. It carries a crew of five: two pilots and three mission systems operators. The co-pilot also can act as a fourth mission systems operator.

The E-2D first flew in 2007, and Navy officials say they hope to procure 73 of these aircraft by 2022. These plans started going to the fleet in 2015. Northrop Grumman is the sole designer of the E-2D, and is the only source with the knowledge, experience, and technical expertise to do this project, Navy officials say.

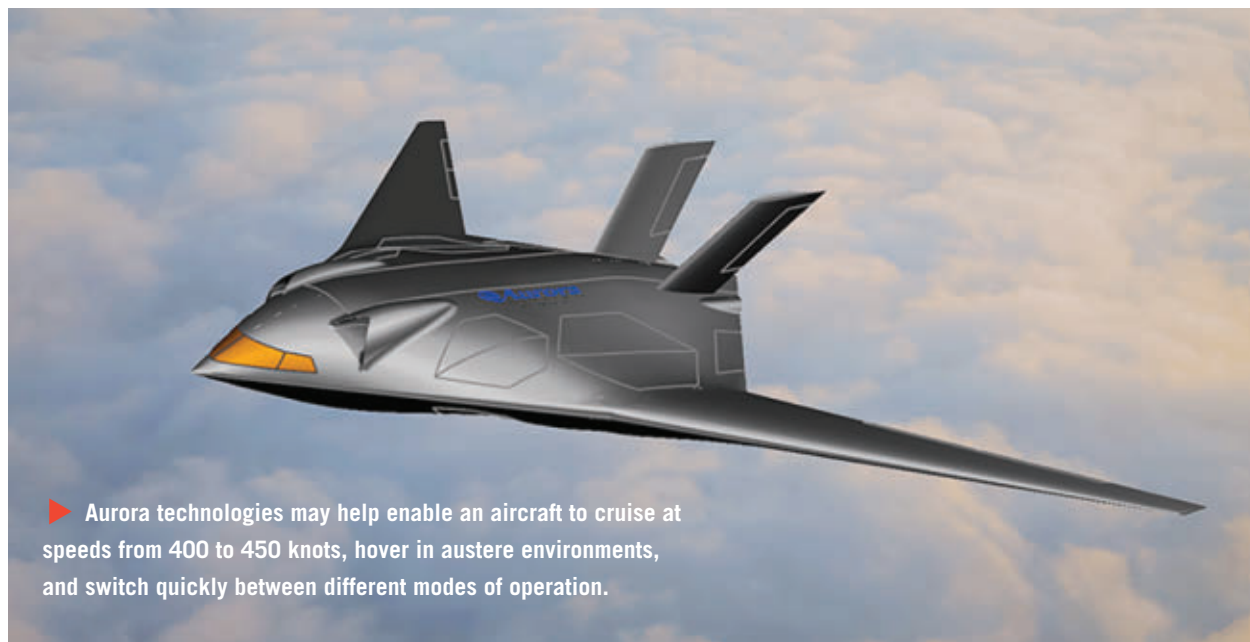
For more information contact Northrop Grumman Aeronautics Systems online at www.northropgrumman.com/who-we-are/business-sectors/aeronautics-systems, or Naval Air Systems Command at www.navair.navy.mil. ←

Navy picks General Dynamics to upgrade Black Pearl unmanned underwater vehicles with new payloads

U.S. Navy researchers needed a company to replace, upgrade, and modify their fleet of Black Pearl-class unmanned underwater vehicles (UUVs) to accommodate a variety of new sensor and signal-processing payloads. They found their solution from the General Dynamics Corp. Mission Systems segment in Quincy, Mass. General Dynamics — the original designer of the Black Pearl UUV — will design and modify NRL's existing Black Pearl-class UUVs to accommodate newly developed NRL payloads. The company also will build five uniquely modified Black Pearl-class UUVs to accommodate payloads developed and provided by NRL, and provide UUV maintenance, at-sea operations support, and engineering of the specialized modified vehicles during research missions. The Black Pearl is based on the Bluefin 21 design from Bluefin Robotics, which General Dynamics acquired in 2016. The Bluefin 21 design is 16.2 feet long, 21 inches in diameter, and weighs 1,650 pounds. It can dive to nearly 15,000 feet, can operate for 25 hours on one battery charge, and moves at speeds to 4.5 knots while using a total of 13.5 kilowatts of electricity. General Dynamics will develop a new tail cone; fabricate modified Black Pearl systems; build and test five Black Pearl UUVs; build a battery section, empty payload receiver, and nose section for each of the Black Pearl UUVs; and provide topside support. For more information contact General Dynamics Mission Systems online at <https://gdmission-systems.com/about-us/major-locations/quincy>, or the Naval Research Laboratory Acoustics Division at www.nrl.navy.mil/Our-Work/Areas-of-Research/Acoustics.

AeroVironment to build Switchblade unmanned smart mortar with video feeds

U.S. Army fire support experts needed manpackable armed unmanned aircraft that have become notable for their use in Ukraine against invading Russian military forces. They found their solution from AeroVironment Inc. in Simi Valley, Calif. Officials of the U.S. Army Contracting Command at Redstone Arsenal, Ala., announced a \$32.1 million order to AeroVironment to build the Switchblade armed loitering unmanned aerial vehicle (UAV) that launches from a small tube that can be carried in a warfighter's backpack. The Switchblade attack drone, which essentially functions as a smart mortar round, transmits live color and infrared video wirelessly after launch for display on a small ground-control unit. The operator confirms the target using the live video feed, commands the air vehicle to arm its payload and lock its trajectory onto the target. The Switchblade anti-personnel UAV weapon reportedly has been successful in Ukraine against Russian light combat vehicles and other valuable targets of opportunity. Ukraine officially uses the Switchblade 300 attack drone. Controllers can manipulate the Switchblade loitering munition from as far away as 6.2 miles, and the missile can operate for as long as 10 minutes. It can engage long-range targets and help to relieve warfighters who are pinned down by enemy fire. The Switchblade warhead has an explosive charge equivalent to a 40-millimeter grenade that is able to destroy light armored vehicles, enemy infantry, and supplies. For more information contact AeroVironment online at www.avinc.com/lms, or the Army Contracting Command at www.army.mil/acc. ←



▶ Aurora technologies may help enable an aircraft to cruise at speeds from 400 to 450 knots, hover in austere environments, and switch quickly between different modes of operation.

Aurora Flight Sciences eyes X-plane to demonstrate unmanned enabling technologies

BY John Keller

ARLINGTON, Va. – Unmanned aerial vehicle (UAV) experts at Aurora Flight Sciences Corp. are moving forward with developing an X-plane to demonstrate enabling technologies in speed and runway independence for future crewed and unmanned aircraft.

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va. announced a \$25 million order to Aurora Flight Sciences on Tuesday for phase 1B of the SPeed and Runway INdependent Technologies (SPRINT) program.

Aurora engineers will design, build, certify, and fly an X-plane to demonstrate enabling technologies for a combination of aircraft speed and runway independence for the next generation of crewed and unmanned aircraft.

Aurora won a \$2.9 million DARPA SPRINT phase-one contract last November. Other companies taking part in the DARPA SPRINT program's first phase are Bell Textron Inc. in Fort Worth, Texas; Northrop Grumman Aeronautic Systems in Falls Church, Va.; and Piasecki Aircraft Corp. in Essington, Pa.

Aurora will describe a scaled experimental X-plane demonstrator to validate the enabling technologies at a relevant size, and

reach first flight of the demonstrator by April 2027. Aurora engineers first focused on conceptual design, and now will work on selected X-plane designs, and finally on limited detailed design.

Enabling technologies that Aurora will develop may help enable an aircraft to cruise at speeds from 400 to 450 knots, hover in austere environments, and switch quickly between these modes of operation.

The SPRINT X-plane is not to be a pre-production aircraft, but instead will be a proof-of-concept technology demonstrator to validate technologies that can scale to different-size military aircraft.

The runway-independent SPRINT X-plane should have useable flight hours left after the DARPA flight demonstration, and likely will be turned over to U.S. Special Operations Command for further evaluation.

On this contract Aurora will do the work in Manassas, Va., and St. Louis, and should be finished by June 2025. For more information contact Aurora Flight Sciences online at www.aurora.aero/2023/11/15/aurora-flight-sciences-to-design-high-speed-vertical-lift-x-plane, or DARPA at www.darpa.mil/program/speed-and-runway-independent-technologies. ◀

Navy orders Honeywell ring laser gyros for navigation systems on ships and submarines

BY John Keller

MECHANICSBURG, Pa. — U.S. Navy shipboard navigation and guidance specialists needed inertial navigation and gyro ring laser units for the AN/WSN-7 ring laser gyro navigation system for Navy surface vessels and submarines. They found their solution from Honeywell Aerospace in Minneapolis.

Officials of the Naval Supply Systems Command Weapon Systems Support activity in Mechanicsburg, Pa., is asking Honeywell for inertial navigation and ring laser gyros for the AN/WSN-7 performance-based logistics combat system, Cruiser/Destroyer Integrated Weapon Support Team, under terms of an \$11.3 million order.

The AN/WSN-7 is a self-contained ring laser gyro inertial navigation system that senses ship motions, computes the ship's precise position, velocity, attitude, heading, and rates in digital and analog formats, and forwards the data to other vital ship systems.

The WSN-7 has been in service with the Navy for decades, and was designed as a replacement for spinning-mass gyro navigation equipment aboard Navy warships. The system is as a more reliable ring laser gyro-based replacement for the old WSN-2 navigation system.

The Northrop Grumman Corp. operating unit in Charlottesville, Va., is the prime systems integrator for the AN/WSN-7 ship inertial navigation system.

Navy officials are extending the life of the WSN-7 shipboard electronics as long as possible as they develop a WSN-7 replacement

— the new AN/WSN-12 inertial sensor module (ISM), a next-generation sensor that improves maritime navigation in GPS-denied environments for surface ships and submarines.

The AN/WSN-7 uses 25-year-old technology based on the NATO MK49 inertial navigation system deployed in the late 1980s. The INS-R will provide improved real-time navigation for Navy surface warships, and enable future technology growth.

The standard WSN-7 shipboard configuration consists of two independent cabinets for redundancy and survivability. It is not be susceptible to jamming or detection by enemy forces.

The ring laser gyro uses two counter-propagating laser beams operating on different frequencies with the differ-

ence dependent on rotation rate. Measurement of this difference provides the rotation angle or rotation rate about the device's sensitive axis.

Compared with older spinning-mass gyro navigation systems, ring laser gyros are much smaller, do not resist changes in direction, are frictionless, have low power consumption, and feature almost no moving parts to enhance reliability while still providing adequate accuracy.

The Navy awarded Northrop Grumman a production contract in June 2022 for the AN/WSN-12, which provides maritime positioning data with or without GPS, and is a key component of the U.S. Navy's AN/



▲ The AN/WSN-7 self-contained ring laser gyro senses ship motions, computes the ship's position, velocity, attitude, and heading, and forwards that data to other ship systems.

WSN-12 Inertial Navigator System (INS), upgrading the Northrop Grumman built AN/WSN-7 INS.

Surface ships and submarines rely heavily on the positioning data provided by GPS for navigation, for safety at sea, and to fire weapons. The AN/WSN-12 ISM helps establish assured position, navigation, and timing (A-PNT) maritime solutions in the absence of satellite navigation technology.

The first ISM was to be fielded in 2023, Northrop Grumman officials say. Northrop Grumman reported completion of the ISM's preliminary design review in May 2016, and critical design review in June 2018.

The AN/WSN-12 will help will provide mission critical ship positioning, velocity, and altitude data to

shipboard sensors, combat systems, guns, and missile systems. It will use an open-systems architecture using a modular design, standards-based interfaces, and widely supported consensus-based standards.

On this order for inertial navigation and ring laser gyros for the AN/WSN-7, Honeywell will do the work in Minneapolis. Delivery should begin next September and be finished by October 2025.

For more information contact Honeywell Aerospace online at <https://aerospace.honeywell.com>, or the Naval Supply Systems Command Weapon Systems Support activity at www.navsup.navy.mil/NAVSUP-Enterprise/NAVSUP-Weapon-Systems-Support. ←

Motorized pan-tilt stages for optics, laser scanning, and positioning introduced by OIS

Optimal Engineering Systems Inc. (OES) in Van Nuys, Calif., is introducing the PT60 series of motorized dual-axis pan-tilt stages to meet the precision and speed of travel requirements of different motion-control applications. The dual-axis pan-tilt stages are for optics, laser scanning, reverse engineering, inspection, tracking, positioning, assembly, camera mounts, and measurements. These four compact high-precision pan-tilt stages integrate two 60-millimeter-diameter rotary stages capable of 360 degrees of continuous rotation set at 90 degrees to each other. The PT60-01 features a resolution of 0.001 degrees (3.6 arcsec) with a 10 microsteps-per-step micro stepping driver and has a knob on the motor for manual adjustments. The motor option -02 is driven by three phase brushless servo motors with quadrature optical encoders. The option -03 uses DC brushed servo motors with quadrature optical encoders, and the -04 option is stepper motor driven with quadrature optical encoders for position verification. The servo motor options -02 and -03 offer the greatest resolution, repeatability, positional accuracy, and speed of travel in closed-loop operation. For more information contact OES online at www.oesincorp.com.

Rugged LCD monitor for naval, ground, and airborne applications introduced by EIZO

EIZO Rugged Solutions Inc. in Orlando, Fla., is introducing the Talon RGD2443W 24-inch 4K rugged liquid crystal display (LCD) monitor for high-detail rugged naval display, ground control, and airborne applications. The

Talon RGD2443W display is designed to meet demanding size, weight, power consumption, and cost (SWaP-C) requirements, measures 599 by 369 by 70 millimeters, and weighs less than pounds. The Talon RGD2443W monitor displays at 3840-by-2160-pixel resolution, and offers a high-resolution display in a minimal physical footprint. LCD flicker can cause user eye fatigue. EIZO has developed a flicker-compensation algorithm called E-LFC to ensure that sonar images are clear and details are discernible to the operator, while also addressing eye fatigue. For more information contact EIZO Rugged Solutions online at www.eizorugged.com.

Raytheon to build and upgrade FIM-92 infrared-guided Stinger missiles

U.S. Army air-defense experts are asking Raytheon Technologies Corp. (RTX) to build and upgrade FIM-92 Stinger shoulder-fired anti-aircraft missiles under terms of a \$418.3 million order. Officials of the Army Contracting Command at Redstone Arsenal, Ala., are asking the RTX Raytheon segment in Tucson, Ariz., for Stinger missile upgrades and replacement. 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. These missiles *Continued on page 42*

Army picks infrared illuminators from L3Harris for battlefield night vision

BY John Keller

WARREN, Mich. — U.S. Army armored combat vehicles experts needed infrared illuminators for a variety of battlefield applications. They found their solution from the L3Harris Technologies Integrated Vision Solutions segment in Londonderry, N.H.

Officials of the Army Contracting Command-Detroit Arsenal in Warren, Mich., announced a \$34.9 million five-year contract to L3Harris for infrared illuminators.



▲ An infrared illuminator emits infrared light that is invisible to the human eye, but that acts like a flashlight for night-vision goggles and weapons sights.

An infrared illuminator emits light in the infrared spectrum that is invisible to the human eye, but that acts like a flashlight for infrared devices like night-vision goggles and weapons sights.

In total darkness, even the most advanced night-vision devices require IR illuminators to function. Infrared illuminators can be integrated into night-vision devices, or can be attachable or handheld. Infrared illuminators are common in infrared monoculars and goggles designed for walking and traveling at night.

Handheld infrared illuminators, for example, basically are night-vision flashlights that the unaided human eye cannot detect. Some illuminators come with infrared laser systems that the naked eye also cannot see.

Although infrared illuminators are invisible to the human eye, those with infrared-detection devices can see them, which can reveal the positions of forces to the enemy. Infrared light is invisible to the human eye, but using an infrared illuminator does make the user visible to others with night vision capability.

Infrared illuminators are not preferred for covert or military operations, though may be necessary for navigating and sighting targets in extreme darkness. The advantage of is that infrared illuminators can help enable military night vision with no visible light on the scene.

On this contract L3Harris will do the work at locations to be determined with each order, and should be finished by February 2029. For more information contact L3Harris Technologies online at www.l3harris.com. ←

Continued from page 41

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 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. 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. On this order Raytheon will do the work in Tucson, Ariz., and should be finished by March 2028. For more information contact RTX Raytheon online at www.rtx.com/raytheon, or the Army Contracting Command-Redstone at <https://acc.army.mil/contracting-centers/acc-rsa/>. ←



POWER GENERATION

▲ Cummins to build mil-spec mobile power generators in near-half-billion-dollar contract

U.S. Army battlefield power experts needed mil-spec advanced medium mobile power sources generators. They found their solution from Cummins Power Generation Inc. in Minneapolis. Officials of the Army Contracting Command at Aberdeen Proving Ground, Md., announced a \$495 million contract to Cummins for advanced medium mobile power sources generators.

Cummins makes the Rugged Mobile Power (RMP) generators, which are versions of the company's original Advanced Medium Mobile Power Sources (AMMPS) generator for military use in tactical environments.

The Rugged Mobile Power Unit (RMP) AMMPS technology, and offers military benefits such as reduced logistics demands, improved mobility and transportability, and operating and maintenance cost savings. The RMP generators offer power output from 5 to 60 kilowatts.

The Cummins AMMPS generator is 21 percent more fuel efficient, 35 percent quieter, and 40 percent more reliable than previous fleet of Tactical Quiet Generators (TQGs), company officials say.

The RMP generators are designed to MIL DTL 32496; use JP-8, JP-4, DF-1, DF-2, and DF-A fuels; operate in temperatures of -45 to 57 degrees Celsius; offer battlefield mobility; have 24 volts starting with NATO slave connection; can survive the effects of nuclear,

biological and chemical contamination; have low infrared and noise signatures; can withstand the effects of high-altitude electromagnetic pulse (EMP); offer electromagnetic compatibility per U.S. MIL-STD 461F; have built-in diagnostics and prognostics; offer networking and automatic start/stop capability; can run for eight hours between refuelings; and are low velocity air drop (LVAD) capable.

On this contract, Cummins will do the work at locations to be determined with each order, and should be finished by February 2033. For more information contact Cummins online at www.cummins.com/generators/military-ammgs.

NETWORKING RADIOS

▼ Air Force picks mobile ad-hoc networking (MANET) radios from Persistent Systems

U.S. Air Force communications experts needed mobile ad-hoc networking (MANET) radios for overseas military communications applications. They found their solution from Persistent Systems LLC in New York.

Persistent won a \$5.1 million contract from Air Force Air Mobility Command at Scott Air Force Base, Ill., with more than 280 MPU5 handheld MANET radios and 10 integrated sector antennas.

MANET technology will enable the Air Force 621st and 821st Contingency Response Groups to react quickly to international situations that require the Air Force to set up overseas airstrips, amass fuel and other resources, and coordinate aircraft landings with host countries.

"Our MPU5s deliver robust, secure, broadband, line-of-sight and beyond-line-sight communications," says Adrien Robenhymer, Persistent's vice president of business development for Air Force and intelligence community programs. "They do so without Air Force personnel having to rely on third-party infrastructure, which is key in a contested environment."

The Air Mobility Command personnel today employ traditional land-mobile radios that cannot share video,



still imagery, or use geospatial awareness programs like Android Team Awareness Kit (ATAK).

These limitations mean that first-in contingency response groups operate in a relatively slow fashion when setting up runways. Likewise, relying only on audio can lead to planning errors, experts say.

The MPU5 radio runs the Persistent Systems self-forming, self-healing Wave Relay MANET. With this adaptable, high-throughput network, users with MPU5s can share voice, video, text, GPS, and sensor data in a peer-to-peer fashion. The radio also has a Cloud Relay capability, which connects the line-of-sight MANET to beyond-line-of-sight LTE and satellite communications (SATCOM).

Working with the MPU5s, the Integrated Sector Antennas extend the Wave Relay MANET over a massive geographic area. Persistent Systems plans to deliver a full complement of MPU5 MANET radios and Integrated Sector Antennas to the Air Force.

For more information contact Persistent Systems online at www.persistentsystems.com, or Air Mobility Command at www.amc.af.mil.



FIRE-DETECTION SENSORS

▲ **Army chooses Logos for fire-detection and persistent surveillance airborne sensors**

U.S. Army surveillance and reconnaissance experts needed hostile fire detection systems to pinpoint enemy hostile fire over broad areas. They found their solution from Logos Technologies LLC in Fairfax, Va.

Officials of the Army Contracting Command at

Aberdeen Proving Ground, Md., announced a \$19.4 million contract to Logos for the company's Serenity persistent surveillance systems to detect enemy fire and unmanned aerial vehicles (UAVs) from aerostats, manned and unmanned air platforms, static ground positions, and moving vehicles.

The Serenity system weighs 50 to 75 pounds, depending on the configuration, and can mount on towers, aerostats, and some aircraft. On an aerostat, Serenity can work with wide-area motion imagery (WAMI) systems to provide operators with additional near real-time and archived imagery.

This contract asks Logos to supply, maintain, and operate deployed Serenity hostile fire detection systems, which employ dual-sensor systems to safeguard U.S. expeditionary forces against potential terrorists.

The system combines electro-optical and acoustic sensors to pinpoint the origin of heavy weapons fire and explosions from distances as far away as 6.2 miles away in any direction, with fewer false alarms than single-sensor systems.

The U.S. Army Research Laboratory is trying to reduce the size and weight of Serenity and install it on a gyrocopter as a surrogate for a UAV.

On this contract Logos will do the work in Fairfax, Va., and should be finished by February 2029. For more information contact Logos Technologies online at www.logostech.net, or the Army Contracting Command at Aberdeen Proving Ground at <https://acc.army.mil/contractingcenters/acc-apg/>.

PERIMETER SECURITY

► **Army taps Leidos for interoperable military installation access control technology**

U.S. Army base security experts needed upgraded access control technologies for as many as 92 new government installations worldwide. They found their solution from Leidos Inc. in Reston, Va.

Officials of the U.S. Army Contracting Command at Aberdeen Proving Ground, Md., announced a \$249 million contract to Leidos for the Automated Installation Entry (AIE) Next system.

AIE Next is the Army's enterprise military installation electronic physical access control system (ePACS) for authenticating personnel against several different authoritative state and federal databases.

The system is an interoperable and integrated solution that helps automate and standardize installation access control for enhanced efficiency across the Army security enterprise.

AIE Next is an unclassified information system that optimizes guard force use, increases pedestrian and vehicle throughput with enhanced security, and adapts to increased authentication requirements at high threat levels.

The AIE Next contract will procure, field, and sustain AIE systems at about 92 potential new U.S. government installations and facilities inside and outside of the continental U.S. For the AIE-Next contract Leidos will handle sustainment and technology refresh for AIE-3 systems previously deployed to 98 Army U.S. Installations.

AIE-Next will insert required emerging commercial off-the-shelf (COTS) hardware and software capabilities while maintaining existing external interfaces. The system will be interoperable with other U.S. military-approved physical security access control systems and authoritative databases.



Leidos prevailed in the AIE-Next competition over two other bidders. The company will do the work at locations to be determined with each order, and should be finished by February 2030. For more information contact Leidos online at www.leidos.com, or the Army Contracting Command-Aberdeen Proving Ground at <https://acc.army.mil/contractingcenters/acc-apg/>. ←



WOLF
ADVANCED TECHNOLOGY

North Atlantic Industries
www.naii.com

NAI for Immediate Impact

North Atlantic Industries, Inc. introduces EagleAI, the latest generation of SOTA™-aligned Intel® Quad Core™ i7, Intel® Octal Core Xeon® and NVIDIA RTX™ GPU for Artificial Intelligence (AI) and High Performance Embedded Compute (HPEC) processing for autonomous control in air, land and sea systems. EagleAI is ideally suited to support uncrewed systems for dangerous and tiresome tasks, enhancing situational awareness and logistical capabilities while reducing risks to human personnel. FIPS-140-2 Level 3 Cybersecurity support increases mission success by preventing unauthorized access and safeguarding critical information.

Ideal System Solution for EagleAI are:

- Flight Control Computers
- Vehicle Management Computer
- Actuator Interface Units
- Mission Computers
- Adjunct Processor
- HPEC





POWER ELECTRONICS

▲ Rugged hermetically sealed SiC power for space and avionics introduced by Solitron

Solitron Devices Inc. in West Palm Beach, Fla., is introducing the SD11487 hermetically sealed silicon carbide (SiC) power module for high-reliability applications in avionics, space, and down-hole exploration. The 51-by-30-by-8-millimeter outline is a small hermetically sealed high reliability, high voltage, half-bridge that makes the most of power density while minimizing loop inductance. 60-mil pins for the power output stage are isolated on one side of the package for simple power busing while 30-mil pins on the opposite side control signals. The SD11487 is a half bridge configuration with two 1200-volt SiC metal-oxide-semiconductor field-effect transistors (MOSFETs). Also included in the module are two freewheeling 1200-volt SiC Schottky diodes in parallel with the MOSFETs. With operating temperatures of -55 to 175 degrees Celsius, the SD11487 comes in a hermetically sealed copper package combined with the alumina nitride direct bond copper substrate that provide thermal conductivity as well as case isolation. Integrated temperature sensing enables high-temperature protection. Silicon Carbide provides better switching performance than silicon MOSFETs and insulated-gate bipolar transistors (IGBTs) with minimal variation versus temperature, Solitron officials say. For more information contact Solitron Devices online at <https://solitrondevices.com>.

EMBEDDED COMPUTING

► SOSA-aligned development chassis for EW, C4ISR, and sensor payloads introduced by Elma

Elma Electronic Inc. in Fremont, Calif., is introducing the CompacFrame family of embedded computing development chassis and enclosures that accommodates a

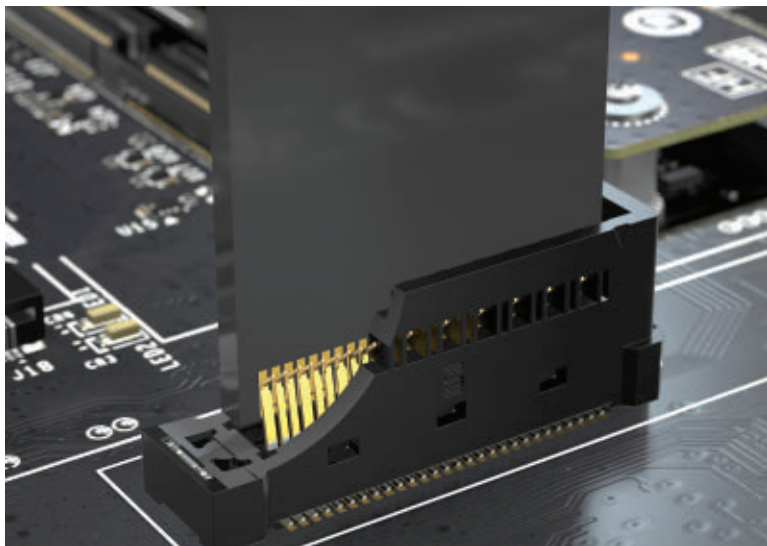
5-slot VITA 48.8 air flow-through (AFT) backplane for designing rugged aerospace and defense applications. The CompacFrame development platforms assist in testing and application development, and facilitates air flow-through thermal management and electronics cooking for sensor payloads, electronic warfare (EW), target tracking and display, navigation systems, and threat detection. The Type 39A unit is aligned to the Sensor Open Systems Architecture (SOSA) open-systems industry standard and accommodates 3U plug-in cards housed in 1.5-inch wide modules, according to VITA 48.8. In place of the 5-slot AFT backplane at a 1.5-inch pitch, the CompacFrame can accept 1-slot VPX power and ground backplanes in a 1-, 1.2-, or 1.5-inch pitch. The development chassis includes a VITA 46.11 chassis manager with Ethernet and serial ports accessible at the rear as well as voltage monitoring LEDs, test points, zeroize, NVMMRO, reset, and power switches on the front panel. The card cage of the VITA 48.8 AFT cooling platform provides a five-degree upward tilt for access to the 3U cards. A 1400-Watt ATX power supply comes standard and a convenient carrying handle provides for easy transport. For more information contact Elma online at www.elma.com.



CONNECTORS

► PCI Express-6.0 card connector for artificial intelligence (AI) introduced by Samtec

Samtec USA in New Albany, Ind., is introducing the HSEC6-DV micro edge card connector for signal integrity performance and high cycle life for artificial intelligence (AI) embedded computing hardware designs. The HSEC6-DV micro edge card connector supports 64-gigabit-per-second PAM4 (32-gigabit-per-second NRZ) applications and are PCI Express 6.0 capable. It serves as the interconnect between the motherboard and add-in cards. HSEC6-DV complies with SFF-TA-1002 x4 (1C), x8 (2C), x16 (4C and 4C+). The edge card socket strip is available with 28, 42, 70, and 84 positions per row, and mates with 1.6-millimeter-thick cards. Optional weld tabs provide extra mechanical strength of the connector to the circuit card. The HSEC6-DV micro edge card connector is RoHS compliant, lead-free solderable, is rated at 240 volts AC, and the current rating is 1.92 amps with 2 pins energized. Mating cable assemblies also are PCI Express 6.0 compatible, supporting 64-gigabit-per-second PAM4 applications. The cable is 34 AWG Samtec Eye Speed ultra-low skew twinax. GC6 cable assemblies are available in 28, 42, and 70 positions, and are standard with 100-Ohm differential pair signal routing. For more information contact Samtec online at www.samtec.com.



NETWORKING

► Gigabit Ethernet switch for networking in harsh environments introduced by Kontron

Kontron Modular Computers S.A.S. in Toulon, France, is introducing the VX3908 managed 3U VPX Layer2/3 Gigabit Ethernet switch for networking applications in harsh environments in transportation, military, and aerospace applications. Based on the VX3940 with lower power consumption, the VX3908 features 1/10/40/50 Gigabit Ethernet bandwidth, and supports as many as 12x 10GBASE-KR ports on the VPX backplane with a standard configuration of 6x 10GBASE-KR and 1x 1000BASE-T ports. The Ethernet networking switch offers remote monitoring and configuration through SNMP and a command line interface to manage via serial or network interfaces. Supporting IPv4/IPv6 forwarding,

time synchronization per IEEE802.1AS and IEEE1588 standards, and Time Sensitive Networking (TSN) readiness, the VX3908 ensures low latency, low delay variation, and extremely low data loss for time and/or mission critical traffic. The VX3908 guarantees communication safety with features such as VLANs, Quality of Service, and extensive Ethernet bridging and routing protocols. The networking switch for harsh environments egress ACLs, intelligent health management via IPMC, and a powerful QorIQ LayerScape family processor ensure security and also scalability and responsiveness for management systems. The VX3908 includes a front QSFP28 cage supporting as many as four 25 Gigabit Ethernet or two 50 Gigabit Ethernet links, and is free from International Traffic in Arms Regulations (ITAR) restrictions. For more information contact Kontron online at www.kontron.com.



DATA STORAGE

► **Small-form-factor data storage AI applications introduced by General Micro**

General Micro Systems Inc. in Rancho Cucamonga, Calif., is introducing the X9 Spider data storage system for sensor data recording, artificial intelligence (AI), and network-attached storage applications. The rugged military-focused X9 Spider storage system includes a 4- or 8-drive removable cartridge supporting secure industry-standard 2.5-inch or M.2 solid state storage. The small-form-factor system offers 128 terabytes of removable data storage, CSfC or FIPS-140-2 secure encrypted solid-state drives, and as fast as 80 gigabytes per second of data I/O streaming. The X9 Spider storage uses high-cycle high-reliability connectors for the canister and a miniature small-form-factor system size to move data between locations. The X9 Spider storage offers high-performance rugged storage; measures 6 by 4.75 by 2 inches; weighs 2 pounds; provides as much as 100 Watts of downstream power; high reliability removable canister cartridge with 5K mating cycles; support for quad NVMe (x4 PCIe) or SATA drives; dual Thunderbolt 4 In/Out ports; sealed, rugged storage canister and locking lever with tamper proof security; and QuadroLock active wedge lock technology. For more information contact General Micro Systems online at www.gms4sbc.com.



375/420 volts DC. All of the modules meet the stringent requirements of DO-160, ABD-100, and MIL-STD-704 specifications. The AC/DC front-end modules have a soft-start, active current limitation, short-circuit protection, and inhibit function. The soft-start/active current limitation prevents inrush current during startup. The short-circuit protection safeguards the module from short circuits by shutting down and restoring to normal when the overload is removed. Front end series under 50 Watts offer two isolated low voltage outputs. Series above 150 Watts provide non-isolated high voltage output. For more information contact Gaïa Converter online at www.gaia-converter.com.

POWER CONDITIONING

► **MIL-STD-704-compliant AC/DC converter introduced by Gaïa Converter**

Gaïa Converter in Le Haillan, France, is introducing four AC/DC converter front-end power electronics modules for use in centralized power architectures with point-of-load converters or isolated DC modules. The AC/DC power-factor-corrected front-end modules are compatible with common airborne AC input bus voltages and variable frequencies for aircraft and avionics applications. Each device has a power input of 115 volts at 400 Hz. The HGMM-35 AC/DC converter has maximum power of 35 Watts, is isolated, and has two 17-volt DC output voltages. The HGMM-50 has maximum power of 50 Watts, is isolated, and has two 17-volt DC output voltages. The HGMM-150 has maximum power of 150 Watts, is not isolated, has an output of 375 volts DC. The HGMM-350 has maximum power of 350 Watts, is not isolated, and has an output of



POWER CONVERSION

► **High-rel DC-DC converters for aerospace applications introduced by Crane**

Crane Aerospace & Electronics in Lynnwood, Wash., is introducing the Interpoint xMOR 120-Watt power converters for military, aviation, and space applications. The Interpoint xMOR features four DC-DC converters with a shared core



architecture, and includes its cMOR (Hi-Rel COTS), hMOR (Class H high-reliability), sMOR (Class K deep space) and rMOR (space) power converters. The cMOR is a high-reliability commercial off-the-shelf (COTS) power electronics offering for aerospace and defense, while the hMOR converter is for mission-critical defense applications. The hMOR is Class H-certified and features high efficiency. The sMOR supports deep-space applications, is Class K-certified, and features high performance and has a 19-to-50-volt input range. The rMOR is for New Space applications, and features 92 percent efficiency in a radiation-tolerant design tested to 30-kilorad and 43MeV. For more information contact Crane Aerospace online at www.craneae.com/xmor-product-family. ◀

ADVERTISERS INDEX

ADVERTISER	PAGE
Airborn Inc.	13
Annapolis Micro Systems Inc.	9
Axiom Electronics	C2
Fairview Microwave	3
General Micro Systems Inc.	C4
Great River Technology	29
LCR Embedded Systems Inc.	1
Master Bond Inc.	19
MicroCircuit Laboratories LLC	7
New Wave Design and Verification	31
North Atlantic Industries	45
Pasternack	17
Phoenix International	33
Pico Electronics Inc.	5
TDK-Lambda	11
Vorago Technologies	19

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

ASSOCIATE GROUP PUBLISHER **Peter Fretty**
435-233-7716 / pfretty@laserfocusworld.com

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

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

CHIEF CONTRIBUTOR **Jim Romeo**

ART DIRECTOR **Tracy Arendt**

PRODUCTION MANAGER **Sheila Ward**

AD SERVICES MANAGER **Shirley Gamboa**

AUDIENCE DEVELOPMENT MANAGER **Debbie Bouley**
603 891-9372 / dbouley@endeavorb2b.com

ENDEAVOR
BUSINESS MEDIA.
www.endeavorbusinessmedia.com

EDITORIAL OFFICES

Endeavor Business Media, LLC
Military & Aerospace Electronics
61 Spit Brook Road, Suite 401, Nashua, NH 03060
603 891-0123 / www.milaero.com

SALES OFFICES

EASTERN US & EASTERN CANADA & UK
Michael Burke, Sales Executive
5248 Neil Dr St Petersburg, FL 33714
918-409-4517
mburke@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 OPERATING OFFICER **Patrick Rains**

CHIEF REVENUE OFFICER **Paul Andrews**

CHIEF DIGITAL OFFICER **Jacquie Niemiec**

CHIEF ADMINISTRATIVE AND LEGAL OFFICER **Tracy Kane**

EVP, TECHNOLOGY GROUP **Tracy Smith**



X9 SPIDER

BY GENERAL MICRO SYSTEMS

COMMUNICATION
SYSTEMS

NUIS/VIDEO
PROCESSING

BLUE FORCE
TRACKING

SMART SENSOR
PROCESSING

FITS IN
BACKPACK

HEALTH
MONITORING

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

LESS THAN 3 POUNDS!

X9 MANPACK

- Intel® Xeon® W (8 cores at 2.6GHz w/ 4.7GHz Turbo)
- Up to 128GB of DDR4 RAM with ECC
- NVIDIA® RTX-A4500 GPU (5888 CUDA® and 384 Tensor cores, 16GB GDDR6 x256-bit RAM, Up to 17.66TFLOPS FP-32 performance)
- Up to 16TB of native high-performance SSD
- 4x Thunderbolt™ 4 ports each with 100W power delivery
- 4x 100GigE fiber ports (RMC-50)
- 3x M.2 I/O expansion sites for Wi-Fi®/Bluetooth®/Cell/GPS
- System I/O port with USB/COM/GPIO/SAM™ I/O
- 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



FAA seeks industry insight on air traffic cyber security

BY Jamie Whitney

WASHINGTON – The Federal Aviation Administration (FAA) announced that the agency is conducting a market survey to ensure the cyber security of the nation's air traffic and airspace.

The FAA's National Airspace System (NAS) Security and Enterprise Operations (NASEO) are tasked with minimizing the impact of - and recovery from - cyber security programs for Air Traffic Organization (ATO).

The FAA runs a multi-faceted cyber security program to protect the NAS per Federal Information Security Management Act (FISMA). The ATO Cybersecurity Group (ACG), a line of business under NAS NASEO within the ATO, is the lead organization for governing, implementing, and managing cyber security controls for NAS.

The ATO Cybersecurity Strategic Plan has been developed to ensure that critical infrastructure remains secure and resilient. This plan aims to maintain the functionality of essential services under various cyber conditions, adapt NAS

▲ **The FAA is surveying industry for enabling technologies on the cyber security of the nation's air traffic and airspace.**

311109637 © Garpinina I Dreamstime.com

cybersecurity capabilities to evolving threats, and enable rapid recovery from disruptions.

The increasing sophistication of cyber adversaries requires deep institutional knowledge of critical infrastructure to ensure the mission space's resiliency. The ATO Cyber security Group (ACG) manages ATO cyber security, integrating functions into NAS and ATO operations. ACG's responsibilities include providing an enterprise-wide view of cyber security risk, securing NAS and ATO-operated systems through authorization, continuous monitoring, and ensuring compliance. The foundation of ATO cyber security is understanding and managing risk to protect and enable operational missions.

The FAA anticipates that the requirements will encompass several areas. Program Control and Governance will cover program management, cyber security policy management, privacy, data calls, audits, and authorization management, including System Security Officers (SSOs), Cyber Security Assessment and Management (CSAM), and related memos.

Enterprise Architecture, Design, and Solutions will include enterprise and system architecture, cyber supply chain risk management, cyber security strategic planning and analysis, future technology and capability insertion, and operating environment definitions.

Cyber security Engineering will focus on cyber engineering requirements development, system domain subject matter experts, the Risk Management Framework, software development, and enterprise solutions development.

Integration, Outreach, and Planning will involve training, workforce development, cyber security outreach and communication, cybersecurity tabletops, and operation risk management.

Industry was asked to respond in July to Elizabeth H. Williams, who can be emailed at elizabeth.h.williams@faa.gov. More information is online at <https://sam.gov/opp/79ef1ef95e-214063b30059a363a4f860/view>. ◀

Study of commercial aircraft running on 100% SAF show significant emissions reduction

Participants in the first-ever in-flight study of the impact of using 100% sustainable aviation fuel (SAF) on both engines of a commercial aircraft announced results show a reduction in soot particles and formation of contrail ice crystals compared to using conventional Jet A-1 fuel. The ECLIF3 study, in which Airbus in Toulouse, France, Rolls-Royce in London, the German Aerospace Center (DLR) in Cologne, and SAF producer Neste in Espoo, Finland, collaborated, measured emissions from both engines of an Airbus A350 powered by Rolls-Royce Trent XWB engines and followed by a DLR chase plane. Compared to a reference jet A-1 fuel, the number of contrail ice crystals per mass of unblended SAF consumed was reduced by 56%, which could reduce the climate-warming effect of contrails. Global climate model simulations conducted by DLR were used to estimate the change in the energy balance in Earth's atmosphere – also known as radiative forcing – by contrails. The impact of contrails was estimated to be reduced by at least 26 percent with 100% SAF use compared to contrails resulting from the Jet A-1 reference fuel used in ECLIF3. These results show that using SAF in flight could reduce the climate impact of aviation in the short term by reducing non-CO₂ effects such as contrails, in addition to reducing CO₂ emissions over the life cycle of SAF. The full report is available to read here: <https://acp.copernicus.org/articles/24/3813/2024/>.

Joby announces successful hydrogen-electric air taxi flight
Joby Aviation, an advanced air mobility company in Santa Cruz, Calif., announced that the company accomplished a first-of-its-kind hydrogen-electric air taxi demonstrator flight of 523 miles. The aircraft, which takes off and lands vertically, builds on Joby's successful battery-electric air taxi

development program. The flight test, which Joby believes to be the first forward flight of a vertical take-off and landing (VTOL) aircraft powered by liquid hydrogen, was completed last month using a converted pre-production prototype battery-electric aircraft fitted with a liquid hydrogen fuel tank and fuel cell system. It landed with 10% of its hydrogen fuel load remaining. Using the same airframe and overall architecture as Joby's core, battery-electric aircraft, this demonstrator features a liquid hydrogen fuel tank, designed and built by Joby, which stores up to 40 kilograms of liquid hydrogen, alongside a reduced mass of batteries. Hydrogen is fed into a fuel cell system, designed and built by H2FLY, to produce electricity, water, and heat. The electricity produced by the hydrogen fuel cell powers the six electric motors on the Joby aircraft, with the batteries providing additional power primarily during take-off and landing.

Dovetail Electric Aviation selects Siemens software to develop its sustainable aircraft

Dovetail Electric Aviation in Docklands, Australia, needed software to aid the development of battery and hydrogen-electric propulsion systems for commercial aircraft. They found their Siemens Digital Industries Software in Plano, Texas. The propulsion systems, designed with Siemens' Xcelerator software, will be retrofitted into existing airplanes used by regional airlines and leisure and cargo flights. Dovetail is converting Cessna 208s into zero-emission battery-electric aircraft and developing a hydrogen-electric retrofit for the Beechcraft King Air. Dovetail recently signed Scandinavian Seaplanes as a customer and has financial backing from Regional Express, the Victorian Government, Air Nostrum, and Volotea. The NX X software for cloud-enabled computer-aided design (CAD) will *Continued on D4*



NASA seeks industry support for Geostationary Littoral Imaging and Monitoring Radiometer (GLIMR)

BY Jamie Whitney

WASHINGTON – The National Aeronautics and Space Administration (NASA) has announced that the agency is seeking assistance from industry as it begins a study into its Geostationary Littoral Imaging and Monitoring Radiometer (GLIMR) Access to Space (ATS) approach.

The GLIMR mission aims to provide transformative rapid observations of dynamic coastal zone ecosystems throughout the Gulf of Mexico (GoM) and coastal continental U.S. (CONUS). Its goal is to observe and monitor ocean biology, chemistry, and ecology to help protect ecosystem sustainability, improve resource management, and enhance economic activity. This includes identifying and tracking harmful algal blooms and oil spills, while also observing, quantifying, and understanding processes associated with rapid changes in phytoplankton growth.

The GLIMR ATS scope is expected to include several key components and activities: the spacecraft itself, the launch

The GLIMR mission aims to provide transformative rapid observations of dynamic coastal zone ecosystems throughout the Gulf of Mexico (GoM) and coastal continental U.S. (CONUS). 149421955 © Antartis | Dreamstime.com.

vehicle, the integration and testing of the GLIMR payload with the spacecraft, and the integration of the spacecraft with the launch vehicle and subsequent launch. It will also cover the command uplink from the industry-provided Mission Operations Center (MOC), the downlink of GLIMR engineering and science telemetry to industry-allocated ground stations, and the delivery of error-checked GLIMR data to various mission partners. Additionally, it encompasses all related tasks and support required during the planned GLIMR Mission, such as pre-launch planning, launch support, in-orbit check-out, and operations.

The environmental considerations depend on whether the approach includes a launch vehicle in a total Contractor-provided solution or utilizes a government-provided launch vehicle. If the study recommends a government-provided launch vehicle, specific environmental requirements will be provided during the study to encompass all available launch vehicles.

Deployments for the initial payload configuration are acceptable and should be noted by the contractor. This might include protective aperture covers or release mechanisms for systems locked during launch. The spacecraft must retain any deployed hardware, and no hardware should be released into orbit under normal operations.

First, conduct a concept study exploring various methods to achieve the defined pointing and on-orbit disturbance requirements. This includes evaluating pointing accuracy, knowledge, stability, and jitter. Constraints such as the relative placement of inertial measurement sensors necessary to meet these requirements must be defined. Additionally, the study should outline calibration methods, their feasibility, and any required spacecraft functionality. On-orbit jitter analyses should be performed to demonstrate spacecraft disturbances at the sensor assembly interface plane during nominal science collection operations and the worst-case spacecraft operation modes, such as orbit raising or reaction wheel dumping.

Next, conduct a concept study considering different methods to achieve the defined launch environment requirements. This involves performing spacecraft-to-payload integrated launch environment structural and dynamic analyses at all proposed spacecraft-to-payload interfaces to ensure positive margins against the structural launch environment requirements. The

launch vehicle environment interface specifications can either be supplied by the contractor as part of a full ATS approach or by the government if the government is providing the launch vehicle. Constraints needed to meet launch environment requirements and maintain positive structural margins, such as soft ride systems, component isolators, and additional support structures, should be defined. The study should also outline the proposed methods for verifying the launch environment requirements, whether through analysis or testing.

Finally, develop ATS approaches to demonstrate that the proposed approach balances technical risk and cost while meeting the design requirements. This should include details on stowed and deployed configurations (where applicable), mass properties, power, thermal, and data rate. Key and driving requirements should be identified, along with their impact on design, performance, cost, schedule, and risks. The study should include analyses showing where performance and accommodation requirements can or cannot be met and propose different methods to achieve spectrum licensing and orbital slot authorization. Constraints such as the launch vehicle, required deployments, and any changes to requirements should be defined. Cost factors, such as a rough order of magnitude for the ATS approach(es), should be included, along with development plans and timelines, considering unique supply chain and long-lead procurement considerations.

Companies interested were asked to respond by July. NASA's primary contact for this project is Kacey Hickman, who can be emailed at kacey.l.hickman@nasa.gov. More information, including technical documentation, is available at <https://sam.gov/opp/cfa8245f39fc4d4480462d99b8182428/view>. ◀

Continued from D2 assist Dovetail in developing propulsion systems and engines, enabling collaboration between teams in Spain and Australia. This technology allows Dovetail to turn digital twin design concepts into prototypes more quickly, saving time in design and rework. Dovetail is also developing a hydrogen-electric version, including a fuel cell and hydrogen storage system. NXX will allow Dovetail to edit and view complex design models, speed up product development, and manage the design process through a digital thread.

Airbus announces partnership with European rotorcraft operator Avincis on AAM development

Airbus in Toulouse, France, and Avincis, a Stockholm-based European helicopter operator, have signed a memorandum of understanding (MoU) to partner on the development of

advanced air mobility (AAM). The companies will collaborate to explore opportunities for operating electric vertical take-off and landing (eVTOL) aircraft throughout Europe. Through the agreement, Airbus and Avincis will focus on defining the concept of operations for eVTOLs in Europe and beyond. Both parties will jointly work to define mission profiles for eVTOL operations in Europe and other target regions. This agreement is another step towards the creation of an AAM ecosystem and is an expansion of Airbus' long-standing relationship with Avincis. The Avincis global fleet currently includes around 60 Airbus aircraft operating from its bases across Europe, Africa, and South America. Avincis and Airbus have enjoyed longstanding and successful cooperation, developing a solid and trusting relationship that will form the foundation of this new eVTOL collaboration ◀

Technology is helping reduce baggage mishandling rates says SITA

BY Jamie Whitney

GENEVA—The air transport industry's rate of mishandled baggage is improving, according to experts at the SITA aviation communications group in Geneva.

The SITA Baggage IT Insights 2024 reports the number of bags mishandled by the industry has fallen from 7.6 to 6.9 per 1,000 passengers in 2023 — despite passenger numbers rising above 2019 levels for the first time in five years.

The long-term trend underlines the positive impact of technology investments. A steep 63% drop in the mishandling rate from 2007 to 2023 happened as passenger traffic rose by 111%. But the industry still faces challenges, particularly managing surges in baggage volumes. Pushing ahead with the industry's digital agenda is vital, argues the survey, focusing on AI for data analysis and computer vision tech in automated baggage handling.

SITA research highlights increasing passenger anxiety about delays and cancellations, with 32% expressing concerns in 2023. Two-thirds of airlines now provide unassisted bag drop services, and 85% of airports offer self-service bag drop. This trend indicates a growing demand for self-service technology to improve passenger flow. Additionally, 32% of passengers use mobile phones for bag collection information, showing a need for better communication and visibility in the baggage process.

Collaboration between airlines and airports is essential, though there is room for improvement in data sharing. Currently, 58% of airlines share baggage collection data, while 66% of airports share baggage delivery data with airlines. SITA's Baggage IT Insights survey references IATA's Resolution 753, advocating for full baggage tracking and real-time status data. The Airports Council International also calls for enhanced self-service, communication, and visibility to reduce passenger stress.

In North America, the report notes a decrease in the baggage mishandling rate from 7.1 per 1,000 passengers in 2007 to 5.8 in 2023. U.S. airlines reduced mishandled baggage by 9% in 2023, aided by additional frontline workers and investments in baggage technology.

In Europe, the mishandling rate dropped from 16.6 per 1,000 passengers in 2007 to 10.6 in 2023, the largest long-term decline globally.

In the Asia-Pacific region, the mishandling rate remained steady, with 3.1 per 1,000 passengers in 2007 and 3.0 in 2023. Despite recovery challenges, this region maintains the lowest mishandling rate globally, attributed to successful investments in digitizing baggage handling processes.

David Lavorel, SITA CEO, said: "The improved mishandled baggage rate in 2023 is great news for passengers and for aviation. It's especially impressive as global passenger traffic grew strongly in 2023 and is set to double by 2040. We clearly see from the SITA Baggage IT Insights results that baggage automation is the way forward, with more collaboration, more communication with passengers, and investments in new technologies such as AI and computer vision to make the journey smoother. From my own travel experiences, I can say this will be really welcome. Technologies like these are essential because they help us gather, integrate, and share data effectively. This means we can uncover important insights that make decision-making easier and more automated."

SITA's baggage-handling report is online at <https://www.sita.aero/resources/surveys-reports/sita-baggage-it-insights-2024/>. ←



▶ Data sharing is helping reduce the rate of mishandled airline passenger baggage worldwide.

33570705 © Flynt | Dreamstime.com