JANUARY 2021

Military & Aerospace Electronics®

RELEVANT. TRUSTED. ENABLING TECHNOLOGIES.

Anti-ship missile guidance

BAE Systems to provide sensor fusion missile seekers for LRASM anti-ship missile. PAGE 4

Latest trends in rugged computing

Connected systems has been enabled by military embrace of commercial off-the-shelf (COTS). PAGE 20

militaryaerospace.com

TOP TECHNOLOGIES FOR THE WARFIGHTER

Defense technologies for the 2020s chart a path to high-priority military programs. PAGE 12

ENDEAVOR BUSINESS MEDIA

GENERAL MICRO SYSTEMS, INC.

ADVANCED SERVERS

ONE COMPANY FOR ALL YOUR SERVER NEEDS

RUGGED SERVERS

INDUSTRIAL SERVERS

COMMERCIAL SERVERS

MADE IN U.S.A.

GMS

GENERAL MICRO SYSTEMS, INC.

TRUSTED AND DEPLOYED SINCE 1979

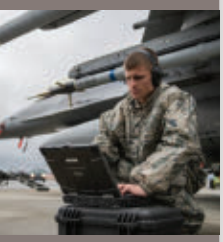
(800) 307-4863 / GMS4SBC.COM

All General Micro Systems, Inc. products are proudly designed and manufactured in the U.S.A.

JANUARY 2021
VOL. 32, NO. 1

Military & Aerospace Electronics

COVER STORY



FOLLOW US

FACEBOOK.com /MilitaryAerospaceElectronics
TWITTER @MilAero
LINKEDIN.com /showcase/military-&-aerospace-electronics

Military & Aerospace Electronics® (ISSN 1046-9079, print; 2688-366X, digital / USPS 005-901) is published 12 times a year by Endeavor Business Media, LLC, 1233 Janesville Avenue, Fort Atkinson WI 53538. Periodicals postage paid at Fort Atkinson, WI 53538 and at additional mailing offices. SUBSCRIPTION PRICES: USA $185 1yr., $327 2 yr., $466 3 yr.; Canada $280 1 yr., $479 2 yr., $618 3 yr.; International $335 1 yr., $638 2 yr., $834 3 yr. POSTMASTER: Send address corrections to Military & Aerospace Electronics, P.O. Box 3257, Northbrook, IL 60065-3257. Military & Aerospace Electronics is a registered trademark. Printed in the USA. GST No. 126813153. Publications Mail Agreement no. 875376.

BY **JOHN KELLER**, EDITOR IN CHIEF

Longtime *Military & Aerospace Electronics* correspondent J.R. Wilson has died

Longtime Military & Aerospace Electronics correspondent J.R. Wilson, 75, died Saturday 19 Dec. 2020 in a Las Vegas hospital. He had freelancing for the magazine as western bureau chief since 1992. As a technology journalist he had focused primarily on aerospace, defense, and high technology.

He had been a full-time freelance writer since 1992, when he finished a four-year assignment as North American Group Editor for the United Kingdom-based Jane's Information Group. In addition to Military & Aerospace Electronics and Jane's Information Group, J.R. Wilson's byline has appeared in Faircount Media Group in St. Petersburg, Fla.; Aerospace Asia/Pacific; Aerospace America; Air Transport World; Armed Forces Journal; C4ISR Journal; Destination Las Vegas; Military Technology; Military Medical Technology; Parlay; PM Network; Sea Power; Signal magazine; Training & Simulation Journal; Unmanned Vehicles; World Dredging; MySAP, WiredLounge.com; and the Las Vegas Chamber of Commerce.

He was a 1971 graduate of the University of Missouri School of Journalism in Columbia, Mo., and also attended the California State University-Long Beach College of Business from 1980 to 1983.

J.R. Wilson worked for United Press International (UPI) from 1972 to 1979 in Atlanta, and Tulsa, Okla., where he gained extensive experience reporting on politics, retail and corporate business, crime, natural disasters, civil and criminal trials, entertainment, riots, and energy. He also covered college and professional sports, including NASCAR, NHRA, LPGA, football, hockey, baseball, tennis and even international parachute-jumping. His reporting involved print and radio, as well as some still photography and cable TV news.

After UPI, J.R. Wilson worked for McDonnell Douglas Astronautics Co. in St. Louis from 1979 to 1983 as head of public relations for the space sector. From 1983 to 1986 he held a similar post with defense simulation contractor Cubic Corp. in San Diego. Later he was president and CEO of a small manufacturing firm in San Diego.

For 25 years he wrote a bi-weekly computer magazine column, was creative director and editor-in-chief of Today's Officer magazine, and created three of the first professional, for-profit magazines exclusive to the Internet: AeroWeb, CompuWeb, and DefenseWeb.

During his life he traveled the world for research and interviews on more than 2,000 articles that have appeared in dozens of international magazines and websites. He authored or co-authored more than 150 books. He covered international air shows in Singapore, Chile, England, and Canada, and reported on airports, airlines, space launch operations, and defense issues in South Korea, Germany, Mexico, French Guiana, and Switzerland.

In addition to aerospace and defense, J.R. Wilson covered medicine; computers; Las Vegas shows, restaurants, hotels and casinos; homeland security; and personal finance. In 1994 J.R. Wilson launched Pollux Communications.

He had been a member of Toastmasters International since 2013, where he was named Distinguished Toastmaster in August 2016. He also was a member of American Mensa Ltd., Sigma Pi fraternity, Sigma Delta Chi Society of Professional Journalists, J-School Dean Search Committee (1970), Journalism Students Association (1969-71), Miss Mizzou production team (1969), Mizzou chapter representative to 1970 SDX National Convention, and was Editor of J-School student newspaper (1970-71).

J.R. Wilson was born on 5 Oct. 1945 in Ozark, Mo. Survivors include cousins Randy Burnett and Cheri Russell of Ozark, Mo. He also leaves behind many friends and colleagues who will remember him fondly. Funeral arrangements are pending.

A PROCESSOR FIRST, BUT WITH THE PROGRAMMABILITY OF AN FPGA.

- Industry-first multiprocessor system-on-chip (MPSoC)
- Impressive power management
- Soft and hard engines for real-time control
- 32-bit to 64-bit processor scalability

XPedite2600

X-ES

Extreme Engineering Solutions
608.833.1155 www.xes-inc.com

MADE IN THE USA

Designed, manufactured, and supported in the USA

BAE Systems to provide sensor fusion missile seekers for anti-ship missile

BY **John Keller**

NASHUA, N.H. — Munitions guidance experts at the BAE Systems Electronic Systems segment in Nashua, N.H., will provide additional advanced missile seekers for the Long Range Anti-Ship Missile (LRASM) under terms of a $60 million contract from Lockheed Martin Corp.

The seeker comprises long-range sensors and targeting technology that help the stealthy missile find and engage protected enemy ships amid attempts to jam or spoof the missile.

LRASM is for use against high-priority enemy targets like aircraft carriers, troop transport ships, and guided-missile cruisers. BAE Systems has delivered more than 50 LRASM seekers to date that have demonstrated technical performance over several tests.

The BAE Systems LRASM seeker uses sensor fusion to blend information from the missile's on-board radar, semi-autonomous guidance, Global Positioning System (GPS) satellite navigation, high-speed secure tactical networking links, and nearby sensors to strike high-value targets from long range while avoiding shipboard missile counter-fire.

The missile guidance sensor uses semi-autonomous guidance and target cueing data to locate and attack targets precisely and reduce reliance on airborne intelligence, surveillance, and reconnaissance (ISR) aircraft, networking links, and GPS navigation.

BAE Systems designers also are working to make the seeker system smaller, more capable, and more efficient to produce. Building LRASM is the Lockheed Martin Missiles and Fire Control segment in Orlando, Fla. Lockheed Martin is in charge of LRASM overall development, and the BAE Systems is developing the LRASM onboard sensor systems.

Photo (above): The U.S. Navy F/A-18E/F jet fighter bomber, shown above, will carry the LRASM anti-ship missile with sensor fusion-based guidance systems.

LRASM is a joint project of the U.S. Defense Advanced Projects Agency (DARPA) in Arlington, Va., the Navy, and the Air Force to design an advanced anti-ship missile that can launch from the Navy F/A-18E/F Super Hornet jet fighter bomber, as well as from the Air Force B-1B Lancer long-range strategic bomber.

In the future LRASM also will launch from the F-35 Lighting II joint

Largest Selection of
High Power Amplifiers

Class AB High Power Amplifiers with Available Heatsinks

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

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

In-Stock and Shipped Same Day

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

PASTERNACK®
an INFINITE brand

strike fighter, as well as from the Navy Mark 41 shipboard Vertical Launch System. The missile travels at high subsonic speeds, and likely will give way in the future to expected new generations of hypersonic missiles. Submarine-launched versions are under consideration.

LRASM is designed to detect and destroy high-priority targets within groups of ships from extended ranges in electronic warfare jamming environments. It is a precision-guided, anti-ship standoff missile based on the Lockheed Martin Joint Air-to-Surface Standoff Missile-Extended Range (JASSM-ER).

Lockheed Martin has been designing LRASM for the last 11 years, primarily under DARPA supervision. The advanced anti-ship missile is intended to replace the ageing Harpoon anti-ship missile. It has a multimode radio frequency sensor, a new weapon data-link and altimeter, and an uprated power system.

The LRASM can be guided toward enemy ships from as far away as 200 nautical miles by its launch aircraft, can receive updates via its datalink, or can use onboard sensors to find its target. LRASM will fly towards its target at medium altitude then drop to low altitude for a sea skimming approach to counter shipboard anti-missile defenses.

The LRASM uses on-board targeting systems to acquire the target independently without the presence of intelligence or supporting services like Global Positioning System (GPS) satellite navigation and data links. Lockheed Martin is designing he missile with advanced counter-countermeasures to evade hostile active defense systems.

The Lockheed Martin LRASM has a 1,000-pound penetrator and blast-fragmentation warhead, multi-mode sensor, weapon data link, and enhanced digital anti-jam global positioning system to detect and destroy selected surface targets within groups of ships.

LRASM development is in response to a gap in Navy anti-ship missile technology identified in 2008. The standard Navy anti-ship missile is the subsonic Harpoon, which has been in the inventory since 1977.

Since LRASM started development more than a decade ago, however, hypersonic cruise missiles able to fly faster than five times the speed of sound have become one of the Pentagon's top priorities. This has the potential to limit overall LRASM production numbers.

On this contract BAE Systems will do the work in Wayne, N.J.; Greenlawn, N.Y.; and Nashua, N.H. For more information contact BAE Systems online at www.baesystems.com, or Lockheed Martin Missiles and Fire Control at www.lockheedmartin.com.

IARPA eyes revolutionary new computers for data analytics in intelligence applications

BY **John Keller**

WASHINGTON — U.S. intelligence researchers are kicking off a project to develop revolutionary computer architectures and integrated circuits for a new class of high-performance computers for large-scale data analytics.

Officials of the U.S. Intelligence Advanced Research Project Activity (IARPA) in Washington briefed industry last month on the Advanced Graphic Intelligence Logical Computing Environment (AGILE) program (IARPA-PRS-21-01).

Explosive data growth far outpaces the ability of today's computers to extract meaningful insights quickly because today's computers were designed to address yesterday's compute-intensive problems rather than today's data-intensive problems.

Transforming massive, random, heterogeneous data streams into actionable knowledge with trusted-computing requires a rethinking of computers to one that places primary focus on data movement, storage, and access.

Data of interest to intelligence analysts is sparse, random, heterogeneous, and is distributed across the computer. Moreover, several applications might try to access the same data at the same time.

The AGILE program seeks to develop computers that not only can process large-scale data-analytic intelligence applications, but also that can address other classes of large problems.

The focus is on new system-level intelligent ways to move, access, and store large, random, time-varying data streams that enable scalable and efficient execution of dynamic graph analytics work flows. Proposed designs must emphasize an integrated system, not individual functionalities like memory or computation.

Achieving AGILE's goals will likely require new memory and interconnection architectures to address data structures for large, irregular, dynamic data sets, which will require massive data throughput and rapidly accessible high-density storage. Designs must demonstrate a fundamental re-thinking of the system architecture and its microelectronics components.

Designs should be efficient and scalable when executing large-scale data analytics; energy efficient; cost effective; realizable in silicon prior to 2030; open sourced or licensable.

The AGILE program will provide performers with the source code for work flows, plus work flow-based kernels and links to industry-standard benchmark codes or benchmark descriptions to be used in the co-design development process and to evaluate the performance of AGILE designs. The program is broken into two 18-month phases: architectural design, and detailed design.

Proposed computers will have four fundamental functions: communications, memory, computation, and runtime. Key challenges involve efficient processing elements; fine-grained irregular data movement; parallelism at all levels; new memory and storage architectures; I/O subsystem that can ingest high-velocity data streams; and system security and trusted computing.

More information is online at https://beta.sam.gov/opp/dcfe7fadab1c-4334859d1e79269ddd19/view.

The DARPA AGILE program seeks to develop computer architectures and integrated circuits for a new class of high-performance computers for large-scale data analytics.

Mercury to boost expertise in avionics with acquisition of Physical Optics

ANDOVER, Mass. — Executives of Mercury Systems Inc. in Andover, Mass., are boosting their company's expertise in avionics, electronic warfare (EW) and trusted computing with their acquisition of Physical Optics Corp. in Torrance, Calif.

Mercury officials have signed a definitive agreement to acquire Physical Optics, a designer of advanced technologies primarily focused on avionics and mission subsystems for defense applications.

Mercury Systems will acquire Physical Optics for an all-cash purchase price of $310 million. Physical Optics is expected to generate revenue of over $120 million for its fiscal year ending 31 Dec. 2020.

Founded in 1985, Physical Optics employs about 350 people, including more than 160 engineers, and holds more than 160 patents worldwide, covering 60 technologies. The acquisition is expected to close by the end of January.

"The acquisition of Physical Optics adds important capabilities on new and existing airborne programs in the platform and mission management market," says Mark Aslett, Mercury's president and CEO. "The combination of Mercury's safety-certifiable and secure avionics processing solutions with Physical Optics's deep portfolio of data storage, transfer, and encryption technologies will enable us to deliver more complete, pre-integrated avionics subsystems to our customers."

Photo (above): Mercury will enhance its expertise in avionics, EW, and trusted computing by acquiring Physical Optics Corp.

Physical Optics supports mission-critical programs with common-use products spanning data transfer systems, flight data recorders, mission computers, high-definition data and video recorders, and advanced encryption devices.

For more information contact Physical Optics online at www.poc.com, or Mercury Systems at www.mrcy.com.

Raytheon to design open-systems avionics for Special-Ops AC-130J aircraft

BY **John Keller**

MacDILL AIR FORCE BASE, Fla. — U.S. Special Operations Command (SOCOM) aviation experts needed open-systems aircraft mission processor avionics to replace outdated equipment aboard Special Operations AC- and MC-130J aircraft. They found their solution from Raytheon Technologies Corp.

SOCOM officials announced a $99 million contract last month to the Raytheon Intelligence & Space segment in McKinney, Texas, to provide Next-Generation Special Mission Processors (NextGen SMP) that enable technicians to install unique Special Forces equipment aboard the aircraft.

The NextGen SMP enables Special Forces tactical mission systems to integrate with AC- and MC-130J aircraft controls and provides future software capabilities.

The AC-130J Ghostrider is a modified C-130J aircraft with advanced two-pilot flight station, digital avionics, dual inertial navigation systems, color weather radar, and Global Positioning System (GPS) for extremely accurate navigation. The aircraft is for close air support, air interdiction, and armed reconnaissance.

The MC-130J Commando II aircraft has avionics similar to the AC-130J, and has a combat systems operator and auxiliary flight deck stations; 13 color multifunctional liquid crystal displays; head-up displays; integrated navigation systems; improved fuel, environmental, and ice-protection systems; enhanced cargo-handling system; infrared sensors; satellite communications for voice and data; increased DC electrical output; and provisions

Raytheon will build new open-systems aircraft mission processor avionics for the Special Operations AC-130J Ghostrider and Commando II versions of the C-130J aircraft.

for the Large Aircraft Infrared Counter-Measure system (LAIRCM).

These new mission processor avionics systems provide capability improvements, and potentially will replace the AC- and MC-130J's current SMPs. This contract has the potential to replace the current two-each SMPs on as many as 94 AC- and MC-130J aircraft, plus spare parts.

SOCOM officials have compiled a long list of capabilities they want for the NextGen SMP. First, it must be a modular open systems architecture that complies with the Open Mission Systems standard.

The new systems will be based also on the VITA Open VPX standard, as well as align to the future Sensor Open Systems Architecture (SOSA) standard. It also must conform as much as possible to the legacy SMP size, weight, and power specifications, wiring, and connectors.

The NextGen SMP also must support safety-critical information in a segregated real-time operating system; provide an any-video-anywhere capability across at least 16 independent displays; and use commercial-off-the-shelf (COTS) processors as much as possible.

The devices also will have modular external data storage for at least one terabyte of data; red/black separation; and cyber security, anti-tamper, and system declassification backup information.

Raytheon should be finished with the contract by December 2027. For more information contact Raytheon Intelligence & Space online at www.rtx.com, or U.S. Special Operations Command at www.socom.mil.

U.S. military eyes open-systems software standards to ensure interoperability

Open-systems software architectures for all new military programs are to be a requirement for component interoperability. Open-systems software will be the new requirement from the U.S. military Joint Requirements Oversight Council (JROC) as it lays the foundation for Joint All-Domain Command and Control (JADC2) for the U.S. military. The military oversight council will not instruct the services simply to employ non-proprietary software; its members also will provide standards to ensure cross-service and cross-domain compatibility, says Maj. Gen. Dawn Dunlop, Air Force director of operational capabilities. The idea is to ensure interoperability for new subsystems like radar or fuzes for warheads so they all can be linked through common software interfaces as they come on line.

Military seeks information security to protect databuses on combat vehicles

What if an armored combat vehicle was rapidly moving to enemy contact through rigorous terrain while facing enemy fire, when its navigational and targeting systems were subject to cyber attacks that suddenly gave false, wrong or misleading information — thus derailing the mission? What if its on-board data flow was instantly jammed, denied or disabled? Such a scenario, which would immediately compromise or even destroy an otherwise successful attack mission, could happen if a vehicle's on-board serial databus were hacked by enemy cyber intruders. This possibility of an information security breach is increasingly realistic given the alarming pace at which enemy cyber attackers are leveraging new technologies to innovate previously unknown or impossible methods of intrusion. There is a critical need to enhance trusted computing of a vehicle or aircraft's databuses, which allows for the transmission of mission critical information within platforms.

Israel ramps-up quantum computing research for ASW and stealth tracking

It may have started slowly, but Israel is barreling ahead to confront the challenges and opportunities of the quantum computing age which is just over the horizon. Tal David, head of quantum research in the Israeli Defense Ministry says the Israeli government approved $387.5 million this summer and that a huge volume of quantum technology projects are moving forward. This is a huge jump from the $31 million announced in December 2018. Quantum computers are built differently, using different materials, operate differently, and once at full speed, will achieve results that put today's computers to shame. A major area that will be transformed is the military, for cracking enemy communications and protecting internal communications, to tracking stealth aircraft and anti-submarine warfare (ASW).

Researchers seek to enable warfighters to communicate silently with brain waves

A breakthrough in decoding brain signals could be the first step toward a future where soldiers silently communicate using brain waves during operations. Research funded by the U.S. Army Research Office in Adelphi, Md., seeks to enable a brain-decoding machine to provide feedback to soldiers so they can take corrective action to protect their health. The brain puts out stress and fatigue signals before someone actually realizes he is stressed or tired, thus letting troops know when they should take a break. Another potential future use is silent communications. Researchers could build on the research to enable the brain and computers to communicate so soldiers can talk silently in the field via a computer.

BAE Systems to build 36 more ACV amphibious armored combat vehicles and vetronics

U.S. Marine Corps amphibious warfare experts are ordering 36 Amphibious Combat Vehicles and accompanying vetronics to replace the Corps's ageing fleet of amphibious assault vehicles (AAVs). Officials of the Marine Corps Systems Command at Quantico Marine Base, Va., announced A $184.4 million order in December to the BAE Systems Platforms & Services segment in Sterling Heights, Mich., for 36 more ACV armored combat vehicles. In 2018 the Marine Corps chose BAE Systems as the ACV prime contractor over competitor Science Applications International Corporation (SAIC) in Reston, Va. The ACV is a wheeled armored combat vehicle able to move Marine infantry warfighters from ships offshore to fight their way onto invasion beaches. For more information contact BAE Systems Platforms & Services online at www.baesystems.com, or Marine Corps Systems Command at www.marcorsyscom.marines.mil.

Raytheon to build missile defense radar systems for Burke-class destroyers

Shipboard radar experts at Raytheon Technologies Corp. will build and integrate the new AN/SPY-6(V) Air and Missile Defense Radar (AMDR) into late-model Arleigh Burke-class (DDG 51) Aegis destroyers under terms of a $82.7 million U.S. Navy order. Officials of the Naval Sea Systems Command in Washington are asking the Raytheon Intelligence & Space segment in Marlborough, Mass., for AN/SPY-6(V) integration and production support. The Raytheon AN/SPY-6(V) AMDR will improve the Burke-class destroyer's ability to detect hostile aircraft, surface ships, and ballistic missiles, Raytheon officials say.

A U.S. Air Force chief master sergeant uses a virtual reality headset, which can provide training on how to maintain aircraft, fly remotely piloted aircraft, or perform other technical tasks in a safe environment.

Top technology challenges this decade for the warfighter

Top aerospace and defense applications and enabling technologies for the 2020s chart a path to the highest-priority military programs and technology research projects.

BY **John Keller**

Providing machines with human-like intelligence — only faster; cruise missiles that streak through the air at one mile per second; unmanned vehicles that require no human supervision; networked computers that are impervious to hackers; weapons that use laser light instead of bullets ... these are only a portion of the military applications and enabling technologies that could make their mark the 2020s.

Here are some more: secure wireless communications able to control unmanned vehicles, military resupply, and battle management; rehearsing critical missions through virtual reality; a new generation of open-systems embedded computing; affordable satellites able to blanket the earth with communications and sensors; and the ability to navigate anywhere in the world without GPS signals.

These capabilities represent the top military applications and enabling technologies that will dominate the third decade of this century. Our list: artificial intelligence (AI) and quantum computing; hypersonic munitions; autonomous unmanned vehicles; cyber security and cyber warfare; directed-energy and laser weapons; 5G wireless communications; virtual and augmented reality

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

Available for Same-Day Shipping!

OPERATING IN A HARSH ENVIRONMENT?

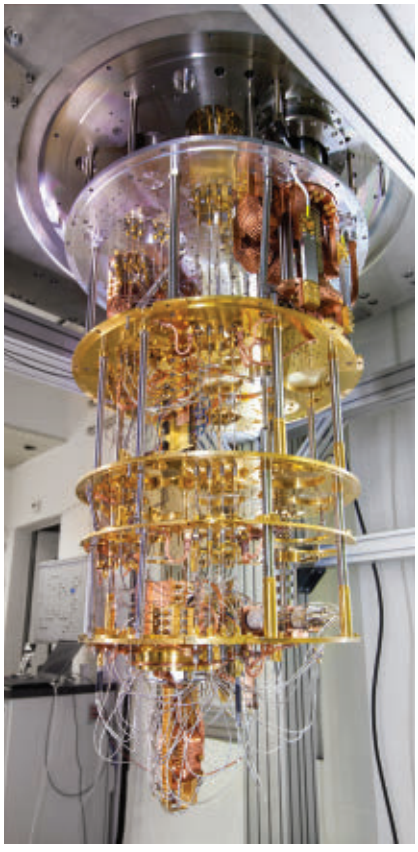
Are you operating in a harsh environment where cabling and interconnectivity components must withstand temperature extremes, moisture, corrosive materials, shock and vibration? To address these challenges L-com delivers connectivity solutions to keep your networks operating – ***anytime…anywhere.***

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

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

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

L-com™
an INFINITE brand



This quantum computer based on superconducting qubits is inserted into a dilution refrigerator and cooled to a temperature less than 1 Kelvin. It was built at IBM Research in Zurich.

in simulation, training, and mission rehearsal; SOSA and open-systems standards; New Space; and alternatives to GPS navigation.

AI and quantum computing

Artificial intelligence seeks to develop new kinds of computer hardware architectures, software operating systems, programming languages, and software programs for applications like machine autonomy, aids for human decision making, military maintenance, logistics and resupply, fast sensor and intelligence data processing, unmanned vehicles command and control, realistic simulation and training, and military planning and battle management.

Although computer researchers have made great strides in AI over the last 30-plus years, this technology still is in its infancy. Systems designers today are nowhere near the armies of intelligent robots of science fiction. Today's AI relies on innovative computer programming, parallel-processing capabilities of advanced general-purpose graphics processing units (GPGPUs), high-performance embedded computing (HPEC), and similar enabling technologies to create what passes for machine intelligence.

Artificial intelligence can be a tough term to pin down. Is it real intelligence? Probably not. Essentially it describes a computer's ability to learn from its experience — particularly from its mistakes, like a human does. The aim is to pull relevant data out of experience and then do what a computer does best, which is to process that data very quickly.

That processing speed is key for today's AI technology. In specific tasks like enabling manned and unmanned aircraft to navigate to and from their mission areas, and making sure the right equipment is on the battlefield to supply the troops, AI can make decisions more quickly than humans can. Results of AI computing also are likely to be more consistent than human decisions, because computers don't get tired, distracted, or have bad days at the office.

To give an idea of the importance of AI to the warfighter, the U.S. military plans to spend $800 million for AI research in 2021. Among the Pentagon's leaders in AI research is the Defense Advanced Research Projects Agency (DARPA) in Arlington, Va. DARPA researchers are working on enabling an unmanned jet fighter to dogfight successfully with manned fighters in the AlphaDogfight trials.

DARPA also is pursuing the Ditto: Intelligent Auto-Generation and Composition of Surrogate Models project to develop a new class of computer-generated design models with embedded machine-learning algorithms to help engineers develop and train artificial intelligence (AI) systems more quickly and accurately than they can today. Another recent DARPA AI project is Fast Event-based Neuromorphic Camera and Electronics (FENCE) to enable intelligent electro-optical sensors for tactical military applications.

Not to be outdone, the U.S. Air Force Research Laboratory at Wright-Patterson Air Force Base, Ohio, launched the Soaring Otter program last November to develop fast and efficient ways to move enabling technologies for machine autonomy from the laboratory to flight testing. This project focuses on AI, machine learning, neural networks, neuromorphic computing, and data exploitation.

Quantum computing, meanwhile, is even younger than AI, and seeks to work with quantum bits which can be in many different states at the same time, unlike conventional computing that uses on binary on or off states. Researchers say quantum computers will be able to solve complex problems quickly that no classical computer could solve in any feasible amount of time.

Hypersonic munitions

Think of a cruise missile that can travel at five times the speed of sound, which is faster than 3,600 miles per hour. That's about one mile per second, and is what military leaders mean when they describe hypersonic

munitions. This is a disruptive technology that in a short time has forced top military leaders to reshuffle their research spending plans. Hypersonics represents one of the Pentagon's highest priorities — so much so that the military plans to spend $3.2 billion for hypersonics research this year.

Why is hypersonic technology so important? Think of a surface warship under threat of hypersonic anti-ship missiles. An opposing ship or aircraft that attacks with hypersonic missiles from 100 miles away will have less than two minutes to react. That means just 100 seconds to detect the incoming threat, classify it, decide on the most effective course of action, and deploy countermeasures. That's not much time, and it's a good bet that hypersonic missiles can overwhelm air-defense sensors and countermeasures.

The problem gets a lot worse when and if hypersonic missiles can be developed that are substantially faster than Mach 5. Double that speed, and it cuts detection, reaction, and defense time in half. Now ask a warship commander if he relishes the notion of less than a minute of warning time of hypersonic missile attack. These are the reasons that U.S. military leaders are considering developing hypersonic munitions and defenses against these weapons as equally important.

Such battlefield conditions will require vast advances in computational capabilities, and likely will involve the latest generations of artificial intelligence and quantum computing. Not only that, but hypersonic munitions will require big leaps in rugged electronics for guidance, propulsion systems, sensors, and tactical datalinks. A hypersonic missile must withstand extreme operation conditions akin to a spacecraft re-entering Earth's atmosphere. Crucial electronic components must be able to operate through heat, shock, and vibration like no weapon's system ever has.

The nose cones of such missiles will be reinforced against the extreme temperatures of hypersonic flight through the atmosphere, would be immune to direct-energy weapons like high-energy lasers. Counter-hypersonic weapons, instead, must concentrate on the missile's less-protected body as it passes over defense systems. That would create its own set of challenges. The need to target a hypersonic missile's vulnerable mid-body would require tracking and targeting at speeds beyond human capability — another application of AI.

On the front lines of hypersonics technology development are The contractors are the Boeing Co. Phantom Works in Washington; the Lockheed Martin Corp. Skunk Works segment in Palmdale, Calif.; and the Raytheon Technologies Corp. Missiles & Defense segment in Tucson, Ariz.

Autonomous unmanned vehicles

Unmanned vehicles operating on land, in the air, and at sea have been around for quite some time. The difference between today's unmanned vehicles and those of the future, however, is full autonomy. Today's unmanned vehicles, for the most part, do not operate and make decisions on their own. Instead, most of them are remotely operated, with a human in the loop, and are likely to remain so for the foreseeable future.

What will separate today's unmanned vehicles and those of the future will be the ability to make independent decisions with little or no human intervention. This will mean

Special Operations cyber warfighters upload coordinates during an exercise showcasing the capabilities of the Advanced Battle Management System. Cyber security is crucial for sensitive battle-management systems.

planning routes, selecting weapons, compensating for unforeseen circumstances during missions, interacting with other unmanned vehicles, and even for unmanned systems to work closely together in swarms.

There is an understandable reluctance to unleash fully autonomous unmanned vehicles on the battlefield because of the potential for conflict among unmanned vehicles and human commanders, accountability for decisions on deploying weapons, and the potential for humans to lose strategic control over unmanned forces.

Nevertheless, enabling technologies like artificial intelligence, quantum computing, and high-performance embedded computing are likely to make autonomous unmanned vehicles too difficult to resist — especially for mundane or dangerous tasks like battlefield resupply, explosives detection and disposal, ocean reconnaissance, and persistent surveillance.

Uncoupling unmanned vehicles from human operators and giving the unmanned systems full autonomy also will be necessary to enable drones to work together on their own as teams or in swarming behavior. Enabling technologies for full machine autonomy in the near term will include fast heterogeneous embedded computing, GPGPUs that offer parallel processing, networked sensors, and advanced computer algorithms. In the far term quantum computing most likely will be applied.

Cyber security and cyber warfare

The ability to keep computers and digital networking free from the prying eyes of hackers, and from all forms of computer malware, is more important today than it ever has been — and the imperative to implement trusted computing measures grows more important with each passing year.

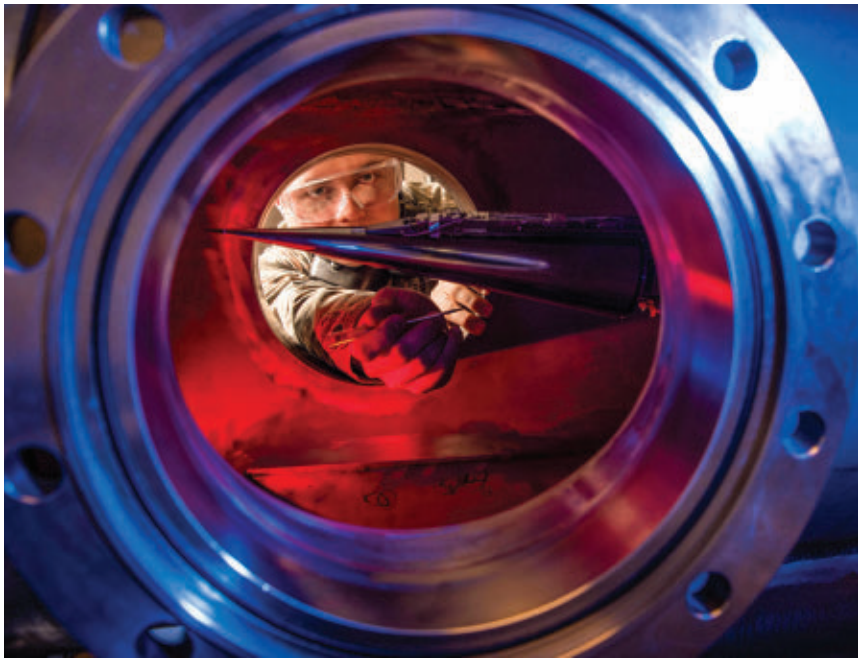
U.S. military organizations are requiring encryption and similar cyber security for most acquisition programs, and defense contractors who handle secret or sensitive digital information must have approved measures in place to monitor suspicious network traffic and block any unauthorized attempts to log on to their networks.

Power grids, water treatment and distribution facilities, hospitals, traffic control, aviation, railroads, sea transport, space-based communications, position, time and navigation - all are part of the cyber domain. That domain also encompasses home appliances, office equipment, children's toys, medical devices, TV sets, unmanned vehicles, baby monitors, and espionage.

One indicator of the importance of trusted computing and cyber security is the amount that Pentagon officials plan to spend this year: $9.8 billion, which up 81 percent from $5.4 billion requested for 2020.

One year ago U.S. Department of Defense (DOD) leaders were to release new cyber security standards that represented the new cost of doing business in attempts to require universal auditing of contractors' cyber safeguards. The military's vast commercial supply chain, especially smaller vendors, has emerged as a critical national security weakness. About 300,000 contractors are to be subject to these standards, which DOD has dubbed the Cybersecurity Maturity Model Certification, or CMMC.

More recently DOD was set to adopt an initial zero-trust architecture by the end of 2020, in an effort to switch from a network-centric to a data-centric modern information security model. Zero trust means an organization does not inherently trust any user. Trust must be continually



An Air Force Cadet uses a Ludwieg tube, a type of wind tunnel, to measure the pressures, temperatures, and flow fields of basic geometric and hypersonic research vehicles.

assessed and granted in a granular fashion. This allows defense agencies to create policies that provide secure access for users connecting from any device, in any location.

Last summer the U.S. Air Force Research Laboratory Information Directorate in Rome, N.Y., launched a potential $950 million Agile Cyber Technology 3 (ACT 3) to develop enabling technologies for the U.S. military to achieve cyber superiority.

The ACT 3 program will emphasize enabling technologies for user requirements; prototype technologies for evaluation in an operational environment; and ways for the Air Force to buy limited product quantities necessary for operational introduction. Technical requirements will encompass rapid development, design, prototyping, demonstration, scenario development, experimentation and evaluation, integration, testing, technical installation, initial operations and cyber technologies.

Directed-energy weapons and high-energy lasers

Reliable laser weapons are among today's most sought-after military capabilities. These weapons operate at the speed of light, and may represent one of the few ways possible for surface warships, military bases, and logistics centers to defend themselves from advanced enemy hypersonic weapons. Supplies of ammunition also is a big advantage; laser weapons never run out of bullets — providing they have an adequate supply of electrical power.

One of the biggest technological challenges to widespread deployment of laser weapons, however, is size, weight, and power consumption (SWaP). These systems tend to be large, heavy, and power-hungry, which prevents them — at least in the near term — from being deployed on tactical jet fighter aircraft, and other relatively small and SWaP-constrained military platforms. Another challenge is scaling-up the output power of laser weapons sufficiently to destroy or disable enemy systems like jet fighters and armored combat vehicles.

This is the reason that today's most promising laser weapons platforms are Navy surface warships where prototypes already are being deployed to defend these vessels from cruise missiles, manned and unmanned aircraft, swarming fast maneuverable missile boats, and even from modern-day pirates.

As early as 2014 the Navy deployed the AN/SEQ-3 Laser Weapon System (LaWS) from Kratos Defense & Security Solutions in San Diego aboard the amphibious transport dock USS Ponce while the ship operated in and around the Persian Gulf. Most recently the Navy has deployed a counter drone dazzler laser weapon called the Optical Dazzling Interdictor (ODIN) aboard the guided missile destroyer USS Dewey. ODIN is configured to track and disable enemy unmanned aerial vehicles (UAVs) by throwing them off course and jamming their sensors.

Laser weapons are not confined only to large platforms like surface warships, however. The U.S. Marine Corps has tested a portable ground-based laser weapon called the Compact Laser Weapons System (CLaWS) for shooting down enemy UAVs on small combat vehicles like the Humvee or Joint Light Tactical Vehicles (JLTV).

5G wireless communications

Emerging fifth-generation wireless communications — better-known as 5G — for the military holds the promise of ubiquitous high-speed data

A specially modified NC-130H aircraft equipped with the Advanced Tactical Laser weapon system fired its laser while flying over White Sands Missile Range, N.M., successfully hitting a target board located on the ground.

A U.S. Air Force F-22 Raptor and F-35A Lightning II manned combat aircraft fly in formation with the XQ-58A Valkyrie low-cost unmanned aerial vehicle over the U.S. Army Yuma Proving Ground testing range, Ariz.

connectivity: vastly improved intelligence, surveillance, and reconnaissance (ISR); fast and secure command and control; more efficient logistics; swarming unmanned vehicles; and wide use of virtual reality and augmented reality for simulation, training, and mission rehearsal.

The promise of 5G is for instant situational awareness anywhere on Earth, smart hypersonic weapons with re-targeting on-the-fly, rich access to mission-critical data on the leading edge of the battlefield, and unmanned aircraft that can fly safely alongside passenger aircraft in commercial airspace.

5G, however, will not come easily, quickly, or inexpensively. When compared to the overall 5G vision for the military, commercial interests, and for the consumer, the technology today only is in its infancy — despite the advertising we see on TV from cell phone providers. Bringing the 5G future to fruition will require time, much testing, experimentation, investment — and a whole lot more cell towers than we have today.

5G is to increase the speed, reduce the latency, and improve reliability of data transfer compared to existing 4G technologies, and support interconnected or autonomous devices like smart homes, self-driving vehicles, precision agriculture and industrial machinery, and advanced robotics, according to the U.S. Congressional Research Service in Washington, in an October report titled National Security Implications of Fifth Generation (5G) Mobile Technologies.

For the military, 5G could improve ISR systems and signal processing, enable new command-and-control applications, and streamline logistics. 5G also could give the military broad access to augmented and virtual reality, 5G smart warehousing, distributed command and control, and dynamic spectrum use. Military leaders plan to spend $1.5 billion for military microelectronics and 5G networking this year.

The U.S. Department of Defense (DOD) 5G Strategy report, published last May, says 5G has the potential to transform military capabilities. "Ubiquitous high-speed connectivity will also transform the way militaries operate," according to the report. "Tomorrow's warfighters will use local and expeditionary 5G networks to move massive amounts of data to connect distant sensors and weapons into a dense, resilient battlefield network.

"This data-rich environment will fuel powerful algorithms that will allow commanders to better understand, shape, and adapt to complex and contested physical and information environments," the report continues. "Low-latency communications will enable new generations of unmanned and autonomous weapons systems across all domains. The warfighter will be empowered with far richer access to data at the tactical edge, so that even small units can achieve strategic effects."

Virtual reality in simulation and training

Military forces do their best to ensure their training is as realistic as possible, and travel to far-flung places like the jungles of Central America, snowy mountains in Alaska, and to deserts of the Southwest to ensure they train in the same conditions in which they are expected to fight.

Now consider: what if warfighters could train in realistic conditions without ever leaving their home bases — sometimes without ever leaving their buildings?

Virtual- and augmented-reality training and mission rehearsal have the potential to save perhaps millions of dollars from the Pentagon's operations and maintenance budget by

enabling warfighters to practice their missions on computer-generated ranges, rather than on distant training centers. Plus, warfighters could train individually or in networked groups virtually any time, without having to wait in line for precious range time.

Virtual reality creates an entire scene, and those using it typically use special headsets on which they view and interact with these simulated environments. Augmented reality, conversely, generates only part of the scene when viewed through battlefield goggles or night-vision devices. It's a computer-assisted heads-up display for infantry warfighters.

Among the enabling technologies of virtual- and augmented reality are general-purpose graphics processing units (GPGPUs), electro-optical headsets, wearable electronics, smart phones and tablet computers, and sometimes devices like treadmills that enable users to run, jump, and roll to enhance realism.

Open systems and SOSA

Open-systems standards for embedded computing and other kind of military electronics are being devised for rapid technology insertion, rapid technology development, and to promote industry competition by enabling many third-party component suppliers to participate in large military projects. If they can build to an open standard, chances are good they can provide embedded computing technology without running afoul of proprietary systems.

One of the highest-profile open-systems standards taking shape today is the Sensor Open Systems Architecture (SOSA), which seeks to drive down the cost and complexity of aerospace and defense electronics components and systems by adopting and then enforcing the use of widely accepted open-systems standards to promote component interoperability; rapid technology insertion and upgrades; reuse; and critical mass in the supplier market.

SOSA is going through its last pre-releases called snapshots, and then SOSA 1.0 should roll out early this year. SOSA has support from the U.S. Army, Navy, and Air Force, as well as from a broad range of embedded computing suppliers in industry.

SOSA seeks to take the best of several influential industry standards, such as OpenVPX; the Tri-Service Memo mentions the Future Airborne Capability Environment (FACE); Hardware Open Systems Technologies (HOST); Vehicular Integration for C4ISR/EW Interoperability (VICTORY); Open Mission Systems/Universal Command and Control Interface (OMS/UCI); Command, Control, Communications, Computers, Intelligence, surveillance and Reconnaissance (C4ISR) / Electronic Warfare (EW) Modular Open Suite of Standards (CMOSS); and Modular Open RF Architecture (MORA).

The idea is to form industry consensus on standards that already have momentum in the embedded systems market, as well as to adopt the core of other standards into SOSA. That way it's not a far leap for systems designers that meet the guidelines of FACE, VICTORY, OMS/UCI, CMOSS, or MORA to conform to SOSA.

Moreover, SOSA seeks to narrow down OpenVPX standards to a manageable level that is appealing to the Pentagon. For example, SOSA reduces OpenVPX slot profiles from 37 to three; 3U switch profiles from 24 to three; and 6U slot profiles from 19 to three, Littlefield points out.

SOSA also seeks to settle on 12-volt power to make it less likely that systems designers will need custom-designed power conditioning and control, as well as offer certified solutions for software packages such as security and system management.

AT&T technicians and civilian contractors assemble a "Cell on Wings" drone to provide 5G connectivity for the Advanced Battle Management Systems Onramp 2 at White Sands Missile Range, N.M.

The latest trends in rugged computing

The proliferation of connected systems has been enabled by the U.S. military embrace of the commercial off-the-shelf (COTS) revolution.

BY **Jamie Whitney**

How do you make things smarter? That's the question industry experts expect to answer as they develop small rugged mobile computers and network equipment for military vehicles and command posts.

Precision-guided munitions — or smart bombs — deployed during Operation Desert Storm 30 years ago made headlines, so-called intelligent munitions have roots even farther back, during the Vietnam War in 1967.

Today the U.S. armed forces only have increased the use of smart devices. The proliferation of connected systems has been enabled by the U.S. military embrace of the commercial off-the-shelf (COTS) revolution.

By using consumer-grade hardware in hardened enclosures, warfighters can repair, upgrade, and replace components at forward operating bases instead of relying on experts with a deep understanding of proprietary and secret technologies.

In addition to COTS, the embedded computing industry has used technology to pump even more power into systems by focusing on the size, weight, and power (SWaP) requirements of the components used. Now, warfighters have more power at their fingertips than ever before, and that trend is continuing.

That power is enabled by using the Internet of Things (IOT), machine learning, and artificial intelligence (AI).

The PacStar Secure Wireless Command Post has demonstrated transformation for military requirements because it marries a modular communications package of hardware and software that reduces the management burden for tactical high-security communications.

Smarten up

David Jedynak, chief technology officer at the Curtiss-Wright Corp. Defense Solutions Division in Ashburn, Va., says industry is getting more "smarts" into more devices than ever before.

"How do you make things smarter? How do you take everything that you possibly have and suddenly make it the smart version?" Jedynak asks. "We're talking about man-machine teaming and artificial intelligence and technology."

The Curtiss-Wright CTO says industry aims to bring small-form-factor computing to the edge by packing more power into ever-shrinking rugged enclosures and by bringing smarts to things like mortar shells.

"You're not putting in the greatest computer ever, but you're putting something that's just good enough," Jedynak says. "You've got cost pressures, you have environmental pressures, and you have all these different sorts of pressures."

Open standards

When it comes to aerospace and defense embedded computing sys-

Largest RF Selection

Available for Same-Day Shipping

The Engineer's Immediate RF Source

Pasternack meets the immediate needs of engineers who are building the future of RF communications.

- Over 40,000 RF, microwave, and mmWave components in 100+ categories of interconnect, passives, actives, and antennas
- 99.4% in-stock availability
- Shipped same day
- No minimum order required

In-Stock and Shipped Same Day

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

PASTERNACK®
an INFINITE brand

A U.S. Marine inputs data into a computer during a flight simulation at Cherry Point Marine Corps Air Station, N.C.

tems, open standards continue to hold a firm place in development and deployment. These include Sensor Open Systems Architecture (SOSA), VITA, Hardware Open Systems Technologies (HOST), and Modular Open Systems Approach (MOSA).

Justin Moll, vice president for marketing and sales at Pixus Technologies in Waterloo, Ontario, says there is a trend for small air transport racks (ATRs) to accommodate two to four OpenVPX slots in the 3U size. In addition, there often will be a single-board computer, a general-purpose graphics processing unit (GPGPU), or a digitizer.

"Increasingly, there will be VITA 67 or VITA 66 RF/Optical interfaces included," Moll says. "There is also a lot of interest in user-programmable SDRs (software-defined radios) where any RF or radio system has the physical layer function performed in software rather than in fixed-function hardware. Engineers have been testing with products like NI's X-series or N-series SDRs in the lab but are seeking field-testable and deployable versions in a rugged form factor."

Moll continues, "The SOSA requirements are pushing higher speeds and higher-Wattage boards. Particularly with 3U OpenVPX backplanes, the cutouts for the VITA 66 and 67 interfaces can take away critical routing space. With Pixus's expertise in high-performance OpenVPX backplane design, even in speeds beyond the capability of the 25G RT-3 connector, we've been able to solve many of the most complex high-speed routing challenges in the industry. Our experience allows us to suggest minor alterations to mitigate issues before the design even starts."

The Pixus 10U x 84HP integrated subrack that accepts as many as 14 6U, 64 or 32-bit CompactPCI boards and as many as two double-wide 6U-power supplies.

Keeping cool

Putting more and more computing power into smaller, ruggedized enclosures means industry needs to find a way to keep everything adequately cooled. Pixus's Moll says that he is seeing more 3U and 6U OpenVPX systems coming in at 2,000 to 2,500 Watts of power, with many boards coming in at the 175-to-225-Watt range.

"Fortunately, in semi-rugged or data center type of defense applications our standard enclosures can meet these challenges with dual 191 CFM hot swappable fans," says Moll. "For MIL rugged, there are designs for Air-Flow-Through and Air-Flow-By solutions where the air is going directly over the fins of the boards' heat sinks. This will help make airflow cooling more effective. Pixus and its partner is also developing a liquid cooled solution

The PacStar 453 NVIDIA GPGPU enhanced server module is suitable for tactical vehicle-mounted and forward operating base virtualization and hosting needs.

for 3U OpenVPX where the liquid flows through the enclosure sidewalls for enhanced cooling in the ATR enclosure format."

Mike Southworth, senior product manager for Curtiss Wright, says embedded computing experts are integrating GPUs to accelerate computing at the edge.

So traditional graphics, engine and GPGPU being repurposed for artificial intelligence and machine learning is a significant trend within the system integrator community that serving the military today. Southworth says that the efficiency of the latest generation of processors and GPUs.

"So, it's not uncommon now to have a hybrid type of architecture where a traditional general-purpose GPGPU is paired with a graphics processing engine to accelerate the computing capabilities of that system," Southworth says. "And that may be done in a very small form factor way as a stand-alone system. That's a shoebox-sized computer or smaller, or it could be something that is in a blade form factor that has many different compute engines on a backplane within an architecture."

Late last year, Curtiss-Wright acquired Pacific Star Communications Inc. (PacStar) in Portland, Ore., PacStar's Chief Technology Officer Charlie Kawasaki says he agrees with his colleague Mike Southworth on processor efficiency driving development of vehicle- or key fob-based computers and servers.

"Improved efficiency that allows us to employ more technology at the edge of the network helps offset the military concern of a contested spectrum," Kawasaki says. "Our deployed organizations don't necessarily have to rely on the compute resources at large facilities or in the cloud, but have the resources available to them out in the field.

"So even if their connectivity is disconnected, they still can do communications," Kawasaki con-

The Pixus Technologies RX310 is a ruggedized version of National Instruments X310 software-defined radio.

tinues. "They can still take advantage of these new machine-learning technologies that can help do things like improve decision-making or reduce the number of people that need to be in harm's way. What are the side effects of this improved efficiency is that we can shrink the size, weight and power required to support these kinds of compute workloads? And one of the things that military organizations are looking at now is to dispense with what used to be a large tent-based command post kind of cities and enable mobility."

Adapting traditional data-center technology for the battlefield plays a factor, Kawasaki says. "So take what used to be sort of data-center-style equipment and get it mounted on communications vehicles and command post vehicles that can now drive around and offer commanders with options for mobility and that improve survivability ... of the way that we conduct warfighting. And so, one of the things we're doing with this shrinking compute resource is you're making that possible."

The Curtiss-Wright Parvus DuraCOR AGX Xavier is suitable for applications in-vehicle and airborne rugged mission computing and sensor integration, as well as for SWaP-sensitive C4ISR autonomous vehicles, electronic warfare, and targeting.

In the field

Last month officials of Systel Inc., a rugged computer designer in Sugar Land, Texas, announced the Kite-Strike rugged supercomputer line, which integrates the NVIDIA AGX Xavier system-on-module. Kite-Strike is built for deployment in harsh environments to enable real-time AI and deep learning capabilities, and provide centralized sensor ingest and data fusion support.

"Kite-Strike represents a massive leap forward in edge computing, providing data center performance in an ultra-compact, fully rugged computer," says Aneesh Kothari, vice president of marketing for Systel. "It combines minimal SWaP with maximum processing density, and is fully configurable and modular, allowing us to deliver reliable systems quickly. Kite-Strike is the next-generation of computing technology demanded by emerging mission demands, specifically next-gen requirements for AI and autonomy."

Kite-Strike features dense I/O capability and supports several configurations including video capture and encode and high-bandwidth networking. Kite-Strike is engineered to environmental specifications including the ability to operating in temperatures from -40 to 70 degrees Celsius, as well to MIL-STD-810H, 1275E, 704F, 461E, and DO-160G.

Curtiss-Wright also announced a Jetson AGX Xavier system-on-module rugged super computer with its Parvus DuraCOR AGX-Xavier SWaP-optimized and small form factor system.

Featuring military-grade ruggedization in a fanless IP67 aluminum enclosure with military-grade circular connectors and a power supply that meets military specifications.

the DuraCOR AGX-Xavier enables system integrators to harness the supercomputer-class capabilities of the AGX Xavier module and deploy in SWaP-constrained extended temperature, high shock, vibration, humidity, altitude, and noisy EMI environments. System I/O expandability supports high-speed NVMe Flash data storage, 10 Gigabit network interfaces, and integration of avionics/vetronics and other cards for various sensor payloads.

Curtiss-Wright officials say the Parvus-DuraCOR AGX-Xavier is suitable for military vehicles, avionics mission computing, sensor integration, unmanned vehicles, electronic warfare (EW) and military targeting.

The DuraCOR AGX-Xavier supports high-speed network connectivity with 10-Gigabit Ethernet optical interfaces, high-speed I/O connectivity with USB 3.1 interfaces, and high-resolution video outputs with HDMI 2.0 and DisplayPort interfaces.

Air Force Senior Airman Ryan Albert installs computer systems at the 497th Intelligence, Surveillance and Reconnaissance Group building on Langley Air Force Base, Va.

In addition to its base system I/O, the system can be modified with mini-PCI Express and PCI Express104 expansion card options. The unit features native eMMC Flash memory and supports high-speed NVMe-based M.2 solid-state drives and removable U.2 NVMe Flash SSD storage.

Star bright

PacStar's 453 NVIDIA GPGPU enhanced server module is suitable for tactical vehicle-mounted and forward-operating-base virtualization and hosting.

The PacStar 453 is based on the PacStar 451 platform that features Intel Xeon D processing, with 128 gigabytes of RAM, 16 terabytes of data storage, and 10 Gigabit Ethernet SFP+ ports, combining high-power, general-purpose computing with a PCI Express connected NVIDIA GPGPU with 896 CUDA cores.

The PacStar 400-series includes routing, switching, and advanced network services with built-in configuration and power options for austere environments. These solutions are driven by PacStar IQ-Core Software to simplify setup and operation.

PacStar also offers its scalable Secure Wireless Command Post (SWCP) to provide, as the name suggests, secure access to Wi-Fi forward bases. The SWCP was recognized by Military & Aerospace Electronics as the recipient of Platinum-level recognition in 2020.

The PacStar SWCP battlefield networking system is a small, modular communications package that enables warfighters to transmit classified and unclassified information securely in tactical settings while using their Wi-Fi and LTE-enabled commercial smartphones and tablet computers.

U.S. Air Force Staff Sgt. Zackery Coder checks computer data during Red Flag-Alaska 14-2, June 19, 2014, on Eielson Air Force Base, Alaska.

PacStar SWCP has proven transformation for military requirements because it marries a modular communications package of hardware and software that reduces the management burden for tactical high-security communications.

At the same time, PacStar shrunk the software and hardware package down to where it could be deployed practically in tactical environments.

The SWCP can help deployed warfighters transmit classified and unclassified information securely in tactical settings while using their Wi-Fi and LTE-enabled commercial smart phones and tablet computers.

Secure wireless tactical eliminates the need for miles of cabling and air-conditioned tents. Instead, warfighters can mount the units on tactical vehicles and pick-up and quickly move as the mission requires.

WHO'S WHO IN RUGGED EMBEDDED COMPUTING

Abaco Systems
Huntsville, Ala.
www.abaco.com

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

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

Combat Proven Technologies (CP Tech)
https://cp-techusa.com
San Diego, Calif.

Core Systems
https://core-systems.com
Poway, Calif.

Crystal Group Inc.
www.crystalrugged.com
Hiawatha, Iowa

Elma Electronic
Fremont, Calif.
https://www.elma.com

Extreme Engineering Solutions (X-ES)
Verona, Wis.
www.xes-inc.com

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

Panasonic Corporation of North America
Newark N.J.
https://na.panasonic.com/us

Pixus Technologies Inc.
Waterloo, Ontario
www.pixustechnologies.com

Systel Inc.
Sugar Land, Texas
www.systelusa.com

Photo (above): Hawklink digital datalinks will help Navy helicopters share information from radar, video, network, and acoustic data with nearby ships and aircraft.

L3Harris for kits to install digital datalinks for allied helicopters

BY **John Keller**

PATUXENT RIVER NAS, Md. — Airborne communications experts at L3Harris Technologies will provide kits to enable six digital datalinks to enable the MH-60R multimission helicopter to share its sensor information in real time with surface warships under terms of a $10.4 million order.

Officials of the Naval Air Systems Command at Patuxent River Naval Air Station, Md., are asking L-3Harris Communication Systems-West in Salt Lake City to build six common datalink Hawklink AN/SRQ-4 kits and components for MH-60R helicopter operated by U.S. military allies.

The L3Harris rugged AN/SRQ-4 Hawklink shipboard terminal is aboard Navy Arleigh Burke-class destroyers and Ticonderoga-class cruisers, and provides command and control, sensor data transfer, datalink operation, and built-in test, L3Harris officials say.

It enables surface ships and MH-60R helicopters to share information from radar, video, network, and acoustic data interfaces, and enables naval personnel to exploit aircraft sensor data in real time to extend situational awareness over the horizon. It has a range of about 100 nautical miles.

The Ku-band communications system runs on an open-systems architecture with touch-screen interfaces. Its 43-inch directional antenna offers auto-switching between open-loop pointing and closed-loop tracking, depending on the range between the helicopter and the ship.

The terminal is interoperable with the AN/SQQ-89 warship undersea warfare combat system and shipboard navigation sensors. It is software-configurable with Common Data Link (CDL) waveforms, and is compatible with SAU7000 digital messaging interfaces.

In addition to the MH-60R helicopter, the system also can work with the Fire Scout unmanned aerial vehicle (UAV), the P-8 Poseidon reconnaissance aircraft, and the P-3 Orion.

On this order L3Harris will do the work in Salt Lake City, and should be finished by December 2022. For more information contact L3Harris Communications-West online at www.l3harris.com/capabilities/defense, or Naval Air Systems Command at www.navair.navy.mil.

Marine Corps installs 5G to help with transportation, energy distribution

Miramar Marine Corps Air Station near San Diego already is partially solar powered, yet the Marines are after an even newer technology; the station has contracted Verizon to build a private 5G cellular network. The fifth-generation standard for cellular communications, 5G has generated buzz since it was codified in 2017. In addition to the existing channels, 5G will employ higher frequencies previously used only for short-range devices such as cordless phones. 5G wireless communications could enable sensors on an energy grid to relay data to a control system almost instantaneously, eliminating the need for costly underground fiber optics. However, the 5G signal won't travel very far, and pretty much everything blocks it. At Miramar Marine Corps Air Station, the future of transportation also will be explored with the same 5G network that will enable control over the flow of solar energy.

U.S. Navy future fast attack submarines to have long-range sonar, networking, and fly-by-wire control

The U.S. Navy's future fast attack submarines will be bigger, faster, more autonomous, networked, and stealthier than the existing Virginia-class attack boats because greater size will allow for more advanced quieting technologies. Set to emerge in the 2030s, a SSN(X) class of attack submarines may be closer in size to the Navy's much larger future Columbia-class ballistic missile submarines. Yet another area of innovation likely to figure prominently in the development of a new generation of attack submarines is fly-by-wire navigational controls such as those built into the Virginia class Block III boats; instead of using mechanically operated hydraulic controls, the Fly-by-Wire system uses a joystick, digital moving maps and various adaptations of computer automation to navigate the boat. This means that computer systems can control the depth and speed of the submarine, while a human remains in a command and control role.

Army tests how soldiers perform under pressure using wearable sensors to measure warfighter stress

Some 530 soldiers from the 10th Mountain Division are taking part in a yearlong human performance study in which they wear special watches and rings that track not just their physical exertion, but also how their heart rate responds under stress. Infantrymen were issued the wearable computing devices to collect physical performance and physiological data, such as resting heart rate, changes in body temperature, respiratory rate, sleep cycles, and activity levels. It's part of the Measuring and Advancing Soldier Tactical Readiness and Effectiveness (MASTR-E) program. Soldiers are encouraged to wear the sensors all the time — even when off duty — to see how different behaviors can affect their performance.

Tethered unmanned aircraft can provide round-the-clock surveillance capability

DARDILLY, France — Elistair in Dardilly, France, is introducing the Orion 2 tethered unmanned aerial vehicle (UAV) for military, government, and industry surveillance and communications applications.

The Orion 2 hexacopter delivers round-the-clock surveillance for as long as 24 hours at a time, making it a persistent surveillance platform.

A lightweight and durable unmanned hexacopter, the Orion 2 is designed as a quick-deploy system with automated push-button takeoff and landing.

"We made it IP54; we optimized the lifespan of the components, including the motors; and we added a safety battery that could recharge in the air," says Pierre-Moana Levesque, director of research and development at Elistair.

With its 330-foot micro-tether, the Orion 2 can carry sensor and communications payloads as heavy as 4.5 pounds, which enables it to serve as an intelligence, surveillance, reconnaissance, and telecommunications platform.

The Orion 2 also can stream geo-referenced imagery from visible-light and infrared sensors at the same time, and can deploy 4G and 5G wireless communications nodes with a fiber-optic cable option.

Photo (above): The Elistair Orion 2 tethered unmanned aircraft, shown above, is a persistent-surveillance system that can deliver communications and reconnaissance data 24 hours a day.

For more information contact Elistair online at https://elistair.com.

Mercury to boost expertise in avionics with acquisition of Physical Optics

ANDOVER, Mass. — Executives of Mercury Systems Inc. in Andover, Mass., are boosting their company's expertise in avionics, electronic warfare (EW) and trusted computing with their acquisition of Physical Optics Corp. in Torrance, Calif.

Mercury officials have signed a definitive agreement to acquire Physical Optics, a designer of advanced technologies primarily focused on avionics and mission subsystems for defense applications.

Mercury Systems will acquire POC for an all-cash purchase price of $310 million. Physical Optics is expected to generate revenue of over $120 million for its fiscal year ending 31 Dec. 2020.

Founded in 1985, Physical Optics employs about 350 people, including more than 160 engineers, and holds more than 160 patents worldwide, covering 60 technologies. The acquisition is expected to close by the end of January.

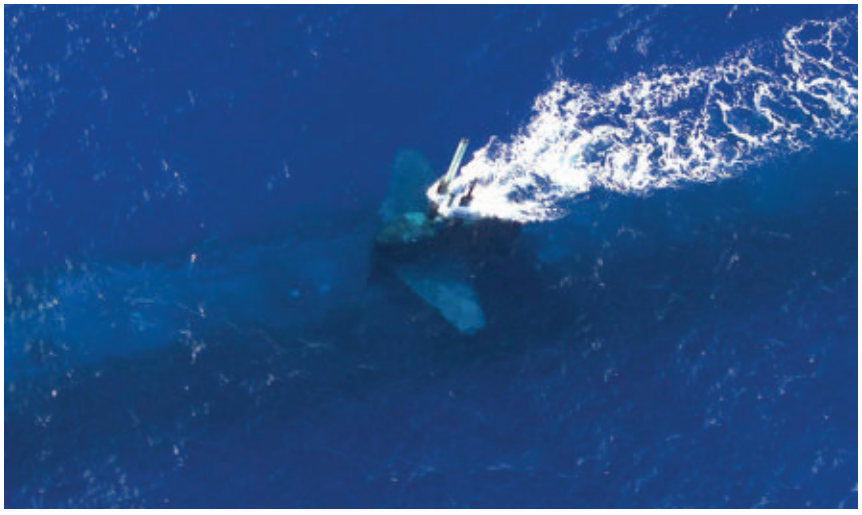
"The acquisition of Physical Optics adds important capabilities on new and existing airborne programs in the platform and mission management market," says Mark Aslett, Mercury's president and CEO. "The combination of Mercury's safety-certifiable and secure avionics processing solutions with Physical Optics's deep portfolio of data storage, transfer, and encryption technologies will enable us to deliver more complete, pre-integrated avionics subsystems to our customers."

Photo (above): Mercury Systems will gain access to electro-optical avionics technologies with its acquisition of Physical Optics Corp.

Physical Optics supports mission-critical programs with common-use products spanning data transfer systems, flight data recorders, mission computers, high-definition data and video recorders, and advanced encryption devices. ←

For more information contact Physical Optics online at www.poc.com, or Mercury Systems at www.mrcy.com.

PRODUCT applications



ANTENNAS

Raytheon to provide SATCOM submarine antennas for communications at periscope depth

Satellite communications (SATCOM) experts at Raytheon Technologies Corp. will provide the U.S., United Kingdom, and Australian navies with high-speed SATCOM antennas for submarines under terms of a $90.3 million contract.

Officials of the Naval Information Warfare Systems Command (NAVWAR) in San Diego are asking the Raytheon Intelligence & Space segment in Marlborough, Mass., to provide 23 Submarine High Data Rate (Sub HDR) antenna systems.

The Sub HDR antennas provide submarines with high-capacity communications in the extremely high frequency (EHF) and super high frequency (SHF) SATCOM bands and enable reception of Global Broadcast Service messages.

The Sub HDR connects submariners to the above-sea world by giving them high-rate data multi-band SATCOM capability. Submariners deploy Sub HDR by raising a mast-mounted antenna above the ocean's surface, while the submarine remains submerged at periscope depth where the boat is difficult to detect.

The system can send and receive mission-critical information such as secure wideband multi-media, voice and data traffic, imagery, and video teleconferencing. Sub HDR enables underwater forces to participate in coordinated fleet battle group operations.

On this contract Raytheon will do the work in Largo, Fla.; Marlborough, South Deerfield, and Stow, Mass.; Fairfield, N.J.; Portsmouth, N.H.; Woodland Hills and Torrance, Calif., and should be finished by January 2024.

For more information contact Raytheon Intelligence & Space online at www.rtx.com, or NAVWAR at www.public.navy.mil/navwar/Pages/default.aspx.

IMAGING SYSTEMS

Customs and Border Protection picks Smart Imaging Systems for explosives-scanning for cars and trucks

The U.S. Customs and Border Protection service in Washington needed compact portable X-ray technology to scan for contraband and explosives in cars and trucks. They found their solution from Smart Imaging Systems Inc. in Beltsville, Md.

The Customs and Border Protection service, the largest law-enforcement group in the U.S. Department of Homeland Security, has issued a $3.5 million purchase order for the company's CXR explosives- and contraband-detection X-ray system for cars and trucks.

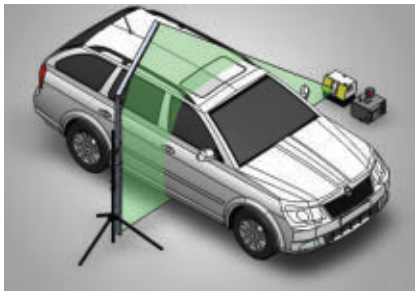
Designed for the MARS Rover, the CXR fits in a car trunk, and Customers and Border Protection personnel can deploy it in minutes at border crossings, government checkpoints, building garages, large event parking facilities, and high security events.

The CXR explosives-scanning sensors system uses safe levels of X-rays to detect drugs, weapons, and improvised explosive devices (IEDs). The system typically scans a car in as little time as five to ten seconds from above or from the sides of vehicles. It can be concealed behind overhead signs or roadside planters. It requires two 12-volt motorcycle batteries to operate.

Land border crossings enable enforcement of immigration and customs laws, and are targets for transnational criminal organizations. These portable car scanners will enable authorities to conduct pulse and surge operations at the nations land and sea ports of entry.

The undisclosed number of units will be delivered and deployed beginning in 2021.

For more information contact Smart Imaging Systems online at www.smartimagingsystems.com, or U.S. Customs and Border Security at www.cbp.gov.



EMBEDDED COMPUTING

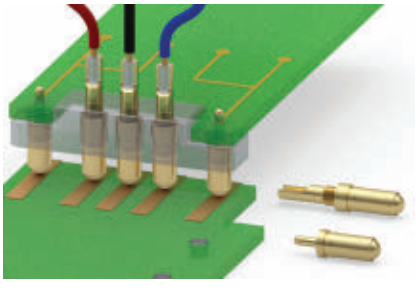
SOSA-aligned board for EW and SIGINT introduced by Aitech

Aitech Systems in Chatsworth, Calif., is introducing the U-C8770 single board computer that couples to the MOSA open-systems standard for I/O-intensive military data processing in radar, signals intelligence (SIGINT), electronic warfare (EW), and sensor signal processing applications. The board offers hardware-based cyber security features, and is aligned with The Open Group Sensor Open Systems Architecture (SOSA) technical standard. The board is an adaptation of Aitech's C877 computer board, and retains the same technical features. It supports PCI Express 4x and 40-Gigabit Ethernet data plane options for fast transport of large amounts of uncompressed video and sensor data. The U-C8770 embedded computing board also features AiSecure, Aitech's innovative and proprietary cybersecurity framework that increases survivability and level of confidence by detecting and preventing unexpected attacks. The inherent security features enable both firmware and data protection, as well as prevention of reverse engineering and tampering with system integrity, while allowing secure transmission and storage of sensitive data. The innovative Trusted Platform solution incorporates a sophisticated, distributed Boot Guard mechanism, based on a combination of trusted hardware and firmware that utilizes TPM 2.0, Intel TXT, enhanced Secure Boot and FPGA-based firmware protection and integrity checks. The onboard SSD supports write protection, secure and quick erase in addition to disk data encryption using AES 256. A battery-backed tamper detection signal ensures system level protection. For more information please call 888-Aitech-8 (888-248-3248), visit http://bit.ly/SOSA-U-C8770 or e-mail info@aitechsystems.com.

CONNECTORS

Spring-loaded contacts for printed circuit boards introduced by Mill-Max

Mill-Max Manufacturing Corp. in Oyster Bay, N.Y., is introducing two Omniball spring-loaded contacts with solder-tail and solder-cup versions for printed circuit boards of various thicknesses. The new contacts come in through-hole mount and solder-cup termination styles, with options for different termination requirements. Omniball contacts are spring-loaded pins in which a gold plated, brass ball replaces the traditional plunger to simplify and improve connections between components in a sliding or rotational motion rather than in an axial or vertical orientation. The Omniball spring-loaded contact features a rolling ball interface, enabling mating components to engage in lateral, rotational and angular alignments while providing optimal electrical, mechanical, and structural reliability. The 7945-1-15-20-09-14-11-0 has a tail length of 2 millimeters, while the 7945-2-15-20-09-14-11-0 has a 3-millimeter tail, and has two press-fit features — a barb, and a knurl — that enables designers to press the pin in from either direction. For more information contact Mill-Max online at www.mill-max.com.



DATA CONVERSION

Rugged digital converter for EW, SIGINT, and radar introduced by Pentek

Pentek Inc. in Upper Saddle River, N.J., is introducing the model 6350 eight-channel A/D and D/A converter system for signals intelligence (SIGINT), communications intelligence (COMINT), military communications, electronic warfare (EW) countermeasures, radar transceivers, test and measurement, satellite communications (SATCOM), LiDAR, 5G, and LTE wireless applications. An addition to the Quartz RFSoC Architecture family, the model 6350 comes in a rugged small-form-factor enclosure, and is based on the Xilinx Zynq UltraScale+ RFSoC FPGA. Optimized for low size, weight and power consumption (SWaP), the model 6350 measures 3.53 by 5.65 by 9.57 inches, and weighs slightly less than eight pounds. Intended for use in rugged environments, the model 6350 is designed to the IP67 specification (Ingress Protection Code, IEC standard 60529) for dust and water immersion. The internal 'I-beam' construction creates a chas-

sis that is rugged and efficient for moving heat out of the box. It also be used with an optional fan plate for desktop development. The model 6350 is pre-loaded with a suite of Pentek IP modules to provide data capture, timing, interface, and processing solutions for many common applications. Modules include DMA engines, DDR4 memory controllers, test signal and metadata generators, data packing and flow control. For more information contact Pentek online at www.pentek.com.

RF AND MICROWAVE

Bi-phase modulators for communications, radio, and radar introduced by Fairview

Fairview Microwave Inc. in Lewisville, Texas, is introducing a line of bi-phase modulators for

military and commercial communications systems, microwave radio, radar, high-data-rate test and measurement, serial data transmission, and wireless base station infrastructure. These bi-phase modulators cover octave frequency bands from 0.5 to 40 GHz, and use TTL logic to phase modulate data onto an RF carrier signal using two-phase shift keying (2PSK). Fairview Microwave's series of 0-to-180-degree bi-phase modulators consists of nine RF and microwave models with performance that includes low insertion loss of 2.5 dB typical, fast switching speed of 40 nanoseconds typical, low voltage standing wave ratio (VSWR) of 1.8:1 typical, and maximum peak RF input power of 0.5 Watts. All designs require dual-bias voltages, and input and output RF ports are bi-directional. These compact and rugged packages use solder pins for TTL control, DC bias and ground, and field replaceable SMA or 2.92-millimeter female connectors. These bi-phase modulators operate in temperatures from -40 to 85 degrees Celsius. All models are reliable, and meet MIL-STD-202 environmental test conditions for humidity, shock, vibration, altitude, and temperature cycle. For more information contact Fairview Microwave online at www.fairviewmicrowave.com.

PRODUCT & LITERATURE SHOWCASE

ADVERTISERS INDEX

Military & Aerospace Electronics

SUBSCRIPTION INQUIRIES
Phone: 1-877-382-9187 / International Callers: +1-847-559-7598
E-mail: MAEM@omeda.com
Web: www.mae-subscribe.com

The Next Big Thing in RFSoC is Here.

(And it's only 2.5 inches wide!)

Now Available with Gen 3 RFSoC!

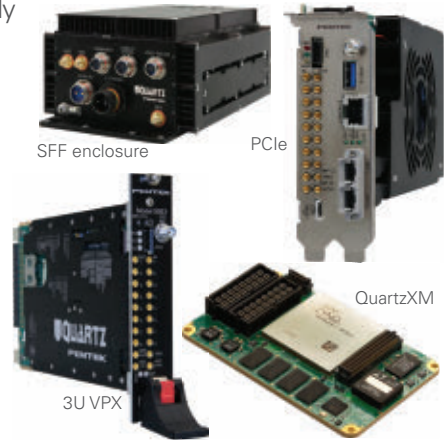
Small | Powerful | Deployable

Pentek's Model 6001 Gen 1 and 6003 Gen 3 RFSoC QuartzXM® modules let you quickly develop and deploy RFSoC technology, while optimizing your system for SWaP.

Mounted on your custom carrier or Pentek's proven 3U VPX, SOSA Aligned 3U VPX, PCIe and SFF platforms, both QuartzXM modules come pre-loaded with a full suite of IP modules, robust software, and fully integrated hardware — all geared to shorten time to market and reduce design risk.

And at only 4"x2.5", it can be deployed in extremely compact environments, including aircraft pods, unmanned vehicles, mast-mounted radars and more.

- **QuartzXM eXpress Module** speeds migration to custom form factors
- **Powerful Zynq® Ultrascale+™ RFSoC** with built-in wideband A/Ds, D/As and ARM processors
- **Dual 100 GigE** interfaces for extreme system connectivity
- **Robust Factory-Installed IP** for synchronous real-time data acquisition, waveform generation and more
- **Board Resources** include PCIe Gen.3 x8 and 16 GB DDR4 SDRAM
- **Navigator® Design Suite** BSP and FPGA design kit for seamless integration with Xilinx Vivado®



RFSoC Gen 3 Product Family

QUARTZ NAVIGATOR Design Suite

All this plus FREE lifetime applications support!

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

SOSA Sensor Open Systems Architecture

30 YEARS

PENTEK
Setting the Standard for Digital Signal Processing

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