Military EMBEDDED SYSTEMS

@military_cots

MIL-EMBEDDED.COM

June 2016 | Volume 12 | Number 4

COTS IN SPACE PRESENTS RELIABILITY CHALLENGES

P 26

P 34

Radiation-tolerance screening for missions of all sizes
By Victor Brisan, VPT Rad

Enabling secure satellite communications

P 22

Acromag
THE LEADER IN INDUSTRIAL I/O

PCIe-Based Next Generation AcroPack™ I/O Modules

For the next 25 years

Acromag.com/AcroPacks

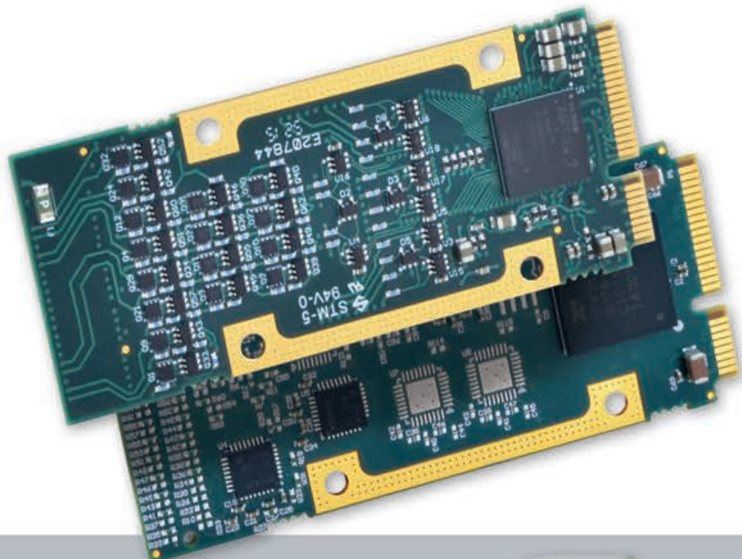
AcroPack™ I/O mezzanine modules and carriers provide a cost-effective, modular approach to system assembly and application specific customization.

These new innovative PCIe-based I/O modules are an extended version of the mPCIe specification and feature a 100-pin connector to handle the I/O.

The modules plug into connectors on AcroPack™ carriers to add analog or digital input and output or communication in any combination for applications running on Linux®, Windows®, or VxWorks® operating systems. Acromag's AcroPack™ PCIe carrier holds up to two mini-PCIe or AcroPack™ mezzanine modules.

AcroPack™ I/O cards are excellent for applications in scientific development labs, the defense industry, military and aerospace applications, and automation applications.

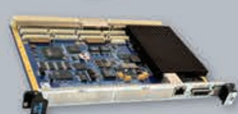
- PCI Express generation 1 interface
- Multi-purpose I/O modules
- Same functionality and memory map of the existing IP modules
- RoHs compliant
- Mix-and-match flexibility and high channel density to save valuable card slots
- Extended temperature range from -40°C to 80°C



Embedded I/O Solutions

FPGA Modules
Acromag.com/FPGAs

I/O Modules
Acromag.com/EmbeddedIO



VME SBCs
Acromag.com/Boards

SFF Embedded Computers
Acromag.com/ARCX

www.acromag.com | solutions@acromag.com | 877-295-7088

MADE IN USA
ISO9001
AS9100

June 2016

Military EMBEDDED SYSTEMS

Volume 12
Number 4

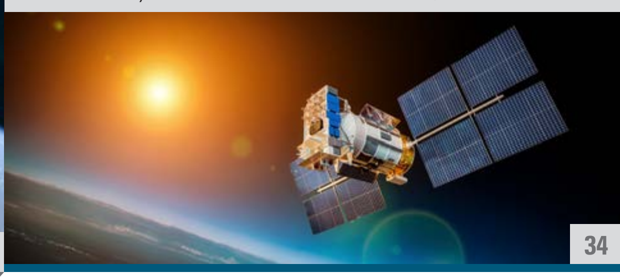
www.mil-embedded.com


10


22


26


38


34

EVENT
IEEE Nuclear Space Radiation Effects Conference (NSREC)
July 11-15, 2016
Portland, OR
www.nsrec.com

WEB RESOURCES
Subscribe to the magazine or E-letter
Live industry news | Submit new products
http://submit.opensystemsmedia.com

White papers:
Read: http://whitepapers.opensystemsmedia.com
Submit: http://submit.opensystemsmedia.com

www.linkedin.com/groups/Military-Embedded-Systems-1864255

@military_cots

Published by:

OpenSystems media

ISSN: Print 1557-3222

ON THE COVER:

Top image:
The use of COTS parts in satellites and other space applications may depend on length of mission, space constraints, and cost concerns.

Bottom image:
Pictured is an artist rendering of ViaSat 1 in space. Image courtesy of ViaSat.

PROVEN POWER SOLUTIONS FOR SPACE PROGRAMS

MIL-PRF-38534 Class H and Class K DC-DC converters and EMI filters from VPT are mission-proven, released on DLA SMDs and ready for the rigors of your LEO, MEO, GEO and deep space missions.

Features:

- Compliant to MIL-HDBK-1547/Aerospace TOR Component Level Screening
- -55°C to +125°C Continuous Operation
- Hermetic Hybrid Technology
- MIL-PRF-38534 Class H & Class K Certified Manufacturing Facility
- Extreme Reliability, High Efficiency

Radiation Hardened – SVR Series – Isolated and Non-Isolated

Input DC Voltage (V)	Total Dose w/ ELDRS	Single Event Effects (SEE)
18 to 37.5 Vin plus 50 V transient	100 krad(Si)	85 MeV-cm2/mg

Available to Aerospace TOR component level element evaluation

Radiation Tolerant – SV Series – Isolated and Non-Isolated

Input DC Voltage (V)	Total Dose w/ ELDRS	Single Event Effects (SEE)
15 to 50 Vin plus 80 V transient	30 krad(Si)	44 MeV-cm2/mg

VPT®
Power Your Critical Mission Today

www.vptpower.com

EFFICIENT & RELIABLE | DECADES OF PROVEN HERITAGE | CERTIFIED QUALITY | SHIPS FROM STOCK

ADVERTISER INFORMATION

E-CASTS

http://ecast.opensystemsmedia.com

Cut DO-178C Avionics Software Costs with Adaptable Data Distribution
Presented by DDC-I
http://ecast.opensystemsmedia.com/601

How to Develop Mission-Critical Avionics and Defense Systems with Ada and DDS
Presented by RTI
http://ecast.opensystemsmedia.com/603

Military EMBEDDED SYSTEMS

GROUP EDITORIAL DIRECTOR John McHale jmchale@opensystemsmedia.com
ASSISTANT MANAGING EDITOR Lisa Daigle ldaigle@opensystemsmedia.com
SENIOR EDITOR Sally Cole scole@opensystemsmedia.com
ASSOCIATE EDITOR Mariana Iriarte miriarte@opensystemsmedia.com
DIRECTOR OF E-CAST LEAD GENERATION AND AUDIENCE ENGAGEMENT Joy Gilmore jgilmore@opensystemsmedia.com
CREATIVE DIRECTOR Steph Sweet ssweet@opensystemsmedia.com
SENIOR WEB DEVELOPER Konrad Witte kwitte@opensystemsmedia.com
WEB DEVELOPER Paul Nelson pnelson@opensystemsmedia.com
DIGITAL MEDIA MANAGER Rachel Wallace rwallace@opensystemsmedia.com
CONTRIBUTING DESIGNER Joann Toth jtoth@opensystemsmedia.com

VITA EDITORIAL DIRECTOR Jerry Gipper jgipper@opensystemsmedia.com
PICMG EDITORIAL DIRECTOR Joe Pavlat jpavlat@opensystemsmedia.com
MANAGING EDITOR Jennifer Hesse jhesse@opensystemsmedia.com

SALES

SALES MANAGER Tom Varcie tvarcie@opensystemsmedia.com (586) 415-6500
STRATEGIC ACCOUNT MANAGER Rebecca Barker rbarker@opensystemsmedia.com (281) 724-8021
STRATEGIC ACCOUNT MANAGER Bill Barron bbarron@opensystemsmedia.com (516) 376-9838
STRATEGIC ACCOUNT MANAGER Eric Henry ehenry@opensystemsmedia.com (541) 760-5361
STRATEGIC ACCOUNT MANAGER Kathleen Wackowski kwackowski@opensystemsmedia.com (978) 888-7367
SOUTHERN CALIFORNIA REGIONAL SALES MANAGER Len Pettek lpettek@opensystemsmedia.com (805) 231-9582
SOUTHWEST REGIONAL SALES MANAGER Barbara Quinlan bquinlan@opensystemsmedia.com (480) 236-8818
NORTHERN CALIFORNIA REGIONAL SALES MANAGER Twyla Sulesky tsulesky@opensystemsmedia.com (408) 779-0005
ASIA-PACIFIC SALES ACCOUNT MANAGER Elvi Lee elvi@aceforum.com.tw
EUROPE SALES ACCOUNT MANAGER James Rhoades-Brown james.rhoadesbrown@husonmedia.com

OpenSystems media®
WWW.OPENSYSTEMSMEDIA.COM

PUBLISHER Patrick Hopper phopper@opensystemsmedia.com
PRESIDENT Rosemary Kristoff rkristoff@opensystemsmedia.com
EXECUTIVE VICE PRESIDENT John McHale jmchale@opensystemsmedia.com
EXECUTIVE VICE PRESIDENT Rich Nass rnass@opensystemsmedia.com
CHIEF TECHNICAL OFFICER Wayne Kristoff
EMBEDDED COMPUTING BRAND DIRECTOR Rich Nass rnass@opensystemsmedia.com
EMBEDDED COMPUTING EDITORIAL DIRECTOR Curt Schwaderer cschwaderer@opensystemsmedia.com
TECHNOLOGY EDITOR Brandon Lewis blewis@opensystemsmedia.com
TECHNICAL CONTRIBUTOR Rory Dear rdear@opensystemsmedia.com
CREATIVE PROJECTS Chris Rassiccia crassiccia@opensystemsmedia.com
FINANCIAL ASSISTANT Emily Verhoeks everhoeks@opensystemsmedia.com
SUBSCRIPTION MANAGER subscriptions@opensystemsmedia.com

CORPORATE OFFICE
16626 E. Avenue of the Fountains, Ste. 201 • Fountain Hills, AZ 85268 • Tel: (480) 967-5581

SALES AND MARKETING OFFICE
30233 Jefferson • St. Clair Shores, MI 48082

REPRINTS

WRIGHT'S MEDIA REPRINT COORDINATOR Wyndell Hamilton whamilton@wrightsmedia.com (281) 419-5725

COTS, GaN, cybersecurity flavor spring trade shows

By John McHale, Editorial Director

Attendees and exhibitors at trade shows I attended this spring – regardless of the show's subject matter or location – wanted fewer product pitches and more technology demonstrations, education on new technology, and more commercial off-the-shelf (COTS) solutions and open standards. The three shows – Aviation Electronic Europe in Munich, International Microwave Symposium (IMS) in San Francisco, and Xponential in New Orleans – reflected these trends.

While none were pure military trade shows, they all covered technology essential to military systems such as avionics, radar, and unmanned systems, with the exhibitors at each event demonstrating their technology for these applications. No one just pitches a board or a chip anymore; to make a sale, they have to demonstrate it running an avionics display, operating a power-distribution system, or analyzing radar signals.

In Munich, many booths touted their product in a graphical avionics demo that leveraged CoreAVI OpenGL SC 2.0 graphics drivers, which help enable safety certification of programmable graphics. IMS exhibitors ran radar and telecommunications demos to show off their RF and microwave components. At Xponential, formerly the AUVSI Unmanned Systems show, demos focused on not only military applications but also unmanned platforms for agriculture, law enforcement, oil and gas, and transportation.

Military industry folks attending these shows reiterated these common trends and, of course, COTS. Let's take a quick look at each show. We'll go alphabetically.

Aviation Electronics Europe

COTS and the safety certification of COTS hardware and software is always of primary interest to the design engineers attending this event.

"There seemed to be more interest in COTS support of certification than previously; people were looking for products supporting both hardware and software certification," said Matt Jackson, technical project manager, Embedded Graphics, at Presagis in Swindon, U.K. "It seems that the drive for more features and systems on aircraft is stretching development times while resources are becoming tighter. Where previously bespoke solutions were developed, people were looking for COTS to fill the gap."

[Editor's note: OpenSystems Media and Aerospace & Security Media, the owner of this event, co-produce the Avionics Design newsletter.]

Most of the conference content covered the modernization of Europe's air-traffic-management (ATM) system, known as Single European Sky ATM Research (SESAR), but the most popular session was a panel on cybersecurity and avionics.

During that session, Ravi Nori, Aircraft Systems Security SME at Teledyne Controls, said that more participation is needed in aviation cybersecurity working groups and that the bodies need to approach security the way they approach safety certification.

Cyberattacks can hit anywhere: from the cockpit to the engine room, anything connected is vulnerable. "Increased connectivity [also] means increased vulnerability to cyberattacks," said Matt Shreeve, principal consultant at Helios, during his presentation. "Aviation will always be a cyberattack target, as it is symbolic."

IMS

Same as last year, the hot topic at IMS was GaN, GaN, and more GaN, whether the device is COTS or custom-designed. RF components based on GaN, or gallium nitride, are showing performance advantages; moreover, their growing popularity in commercial markets has lowered the cost, making GaN more attractive for military system designers, especially in radar and electronic-warfare (EW) applications.

Also trending is greater levels of integration in RF designs, enabling multifunctionality in new phased-array-radar systems and EW platforms, said Bryan Goldstein, general manager for the Analog Devices Aerospace and Defense Group. In addition, the ability to put the functionality of 20 chips into the footprint of one enables designers to reduce size, weight, and power (SWaP).

Xponential

The folks at AUVSI changed the name of their unmanned system event to Xponential to reflect the potentially huge markets for autonomous systems beyond military applications … and while driverless cars, hobbyists, small drones for retail delivery, and the like were more evident at this event than in past years, military users remain the main operator of unmanned platforms.

Among military system designers at the event, interoperability was the key trend, from the signal-processing systems to the payloads themselves.

"The future will be about plug-and-play payloads so multiple missions can be performed with one airplane configuration by swapping out the payloads in a way that takes no longer than a few minutes," said Peter Klein, director, UAS Programs, Airborne Business Unit, Elbit Systems of America. "End users are [also] definitely looking more at COTS as an option, especially with the push toward more interoperability in payloads."

Despite the push toward commercial applications, I still see this event as important for military embedded designers, especially if they want to get a jump on commercial market opportunities.

Graphics processing – having it both ways

By Charlotte Adams
An Abaco Systems perspective on embedded military electronics trends

Military systems are noted for their high processing demands, a situation that is particularly true for graphics processing. Like their commercial counterparts, military displays are becoming faster, higher-resolution, and more complex. Both defense surveillance and commercial video-game applications, for example, share a need for the maximum possible raw graphics computational horsepower.

Driven by the consumer market, chip companies upgrade their products every year or two, sometimes delivering two times the performance per watt in successive generations. Board designers, in turn, use these chips to provide significant increases in performance per slot at their level in the food chain. We can be very thankful that the consumer-electronics industry yields to contractors the building blocks for national defense. Just think what it would cost otherwise.

Embedded graphics-processing units (GPUs) can perform both general-purpose computing and video and graphics generation, making them suitable for applications such as persistent wide-area surveillance; intelligence, surveillance, and reconnaissance (ISR); and radar or sonar processing. Even ground vehicles need specialized graphics processing in order to piece together a picture of the situation around them.

Designers of next-generation ISR systems, like designers of immersive video games, want the fastest, most massively parallel GPUs that the industry can provide. High-performance GPUs give defense system developers the throughput required to accomplish tasks such as sensor fusion, where data from different sensors is integrated into a whole that is greater than its individual parts; and video stitching, in which elements of a picture are sewn together to form a larger view.

Mil applications have unique needs

While they share with gamers a need for some of the same basic components, military applications also have a host of dissimilar requirements. For military users, backward compatibility is not just a "nice-to-have," but an essential: New stuff still must talk to old stuff and built-in obsolescence is a fault, not a virtue. Perhaps more important, for military applications SWaP – size, weight, and power – is king. Thermal management, life cycle cost, and long-term support are also far more important in the military realm than in the commercial sphere.

So, while designers of ISR systems want the latest GPUs with hundreds of parallelizable processing units or cores – including single- and double-precision floating-point units – that's just the start. Equally important is the accommodation of new as well as legacy video standards; form, fit, and function compatibility at the board, box, system, and platform levels; long-term logistics support; ease of upgradability; affordability and life cycle cost; and performance per watt. These factors carry different weights depending on the age of the platform, but none can be discounted. Flexibility is key.

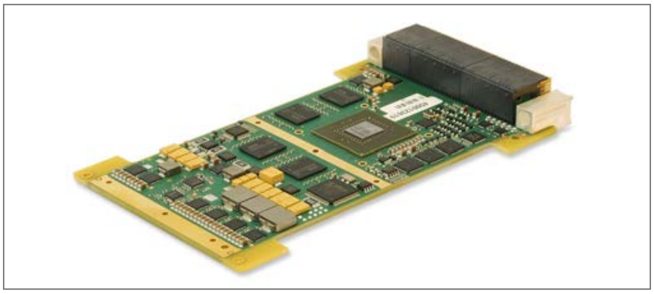


Figure 1 | The Abaco Systems GRA113 3U VPX rugged high-performance graphics board features a 640-core GPU from NVIDIA.

A high-end GPU application might involve an airborne ISR system with multiple operators, where the chip simultaneously drives multiple displays, using multiple video standards. Or take a ground vehicle, where multiple sensors feed multiple displays, all with varying resolutions and formats, and with an even greater emphasis on SWaP and thermal management.

The same would be true of a sonar display on a submarine or a fire-control radar on a fighter aircraft, both of which need to minimize SWaP. The best graphics solution for these must provide not only optimal SWaP trades but also the most flexible processing and video-output technology.

All of these applications need to process a lot of sensor data quickly and efficiently. High-performance GPUs provide the throughput required to accomplish sensor fusion and video stitching. Moreover, graphics chips that include double-precision floating-point hardware minimize the impact of artifacts introduced by single-precision processing.

An example of such a backward-compatible graphics processing board is Abaco Systems' rugged GRA113 3U VPX product with NVIDIA's 640-core GPU, which features configurable video outputs to accommodate multiple resolutions, aspect ratios, and legacy displays. (See Figure 1.)

The performance curve of the semiconductor industry – propelled by the demands of the consumer electronics market – is a gift that keeps on giving. Continuous upgrades and performance increases make it possible for board designers to do more with less – exploiting greater throughput in the same volume, while potentially lowering life cycle costs.

www.abaco.com

10 Gigabit backplane Ethernet for embedded supercomputers

By Andrew McCoubrey

An industry perspective from Curtiss-Wright Defense Solutions

Designers of next-generation high-performance embedded computing (HPEC) solutions for demanding intelligence, surveillance, and reconnaissance (ISR) systems applications got a boost from the introduction of Intel's multicore Xeon D system-on-chip (SoC) processor earlier in 2016. This device provides as many as 16 cores in the same power footprint as earlier four-core devices and features the rugged ball-grid-array (BGA) packages and extended temperature range needed for deployed applications.

Since this processor family and Ethernet serve as the workhorse of the HPC clusters that drive large-scale commercial data centers, development tools for building highly scalable embedded supercomputers can be leveraged to help build HPEC systems. Xeon D enables a level of compute performance that previously was only available on 6U VPX processing boards to migrate to size, weight, and power (SWaP)-optimized 3U cards. This higher performance means that a wide variety of high-end ISR applications such as radar, sensor, and image processing can now be deployed on smaller space- and weight-constrained platforms.

An essential element of HPEC systems is support for high-speed 10 and 40 Gigabit Ethernet (GbE) networks. More good news for the HPEC system designer is the fact that the Xeon D features two ports of built-in 10GBASE-KR "backplane" Ethernet. This capability is important because ISR applications are increasingly turning to large-scale SWaP-optimized 3U VPX architectures, with ten or more boards per box; KR Ethernet hits the sweet spot by supporting 10GbE on a single serializer/deserializer (SerDes) lane. The upshot: 3U cards, with many fewer available backplane pins than 6U VPX, can now support 10 GbE with only four pins on the backplane, compared to the eight or 16 pins it takes to support other styles of Ethernet.

For HPEC system designers, the benefit is clear: KR Ethernet can deliver four times as many 10 GbE ports as previously. With 10GBASE-KX4 or XAUI technology, 3U VPX Ethernet switch cards were effectively limited to eight ports. Since 10GBASE-KR uses far fewer pins, a 3U switch card can now support 32 ports of 10 GbE, enabling system designers to build much larger 3U-based HPEC systems. While it was possible in the past to add KR Ethernet to a 3U board before the advent of the Xeon D, doing so required a separate Ethernet controller – consuming valuable board real estate and power. With the Xeon D, HPEC designers get true supercomputer multicore performance with KR Ethernet provided natively on-chip.

Because many systems will require a mix of boards and a range of Ethernet types, it's important to be able to support 1 GbE, 10 GbE, and 40 GbE network speeds. Since the IEEE standards for backplane Ethernet are closely related, the SerDes interfaces on newer switch chips can be configured to support all three speeds. 3U switches based on backplane Ethernet can potentially support 32 x 1 GbE, 32 x 10 GbE, 8 x 40 GbE, or a mix of all three. Those numbers mean that today's newest 10 GbE processors can coexist with older cards that only support 1 GigE in the same system. For future-proofing, when 40 GbE boards become widely available, the same switch card could be able to support them as well.

An example of a next-generation 3U VPX Ethernet switch card that supports KR Ethernet is Curtiss-Wright's VPX3-687 (Figure 1). The open-architecture card uses standard-industry connectors to provide 320 Gbps of line-rate switching, with support for 1000BASE-KX, 10GBASE-KR, and 40GBASE-KR4. In addition to supporting backplane Ethernet interconnects, this switch also offers media access control/physical layer (MAC-PHY) links such as XFI and SFI for connection to optical transceivers for outside-of-the-box networking.

Figure 1 | The Curtiss-Wright VPX3-687 3U VPX Ethernet switch can offer 320 Gbps of line-rate switching plus links for connection to optical transceivers.

Providing the right mix of optics on a switch has been a challenge in the past – there are many different standards using different wavelengths, types of fiber/connector, and varying power levels for short or long reach. Designing a switch that can connect to off-the-shelf optical transceivers enables the system designer to address the project's unique optical data requirements.

As the 3U form factor becomes increasingly popular for building scalable HPEC systems, the ability of the network switch card to support the higher speed processing made possible by the Xeon D processor becomes critical. To fulfill the promise of HPC supercomputing-class computing in the harsh environments of deployed defense applications requires flexible network switching that talks today's 10 GbE language while supporting older 1 GbE cards and is poised to support the next generation of 40 GbE cards over the horizon.

Andrew McCoubrey,
product marketing manager for switching and routing products,
C4 Solutions Group
Curtiss-Wright
www.cwcdefense.com

EXECUTIVE INTERVIEW

Military rad-hard designs and big data in space systems

By John McHale, Editorial Director

Ricardo Gonzalez

The BAE Systems Semiconductor Technology Center in Manassas, Virginia, designs, fabricates, packages, and tests radiation-hardened space products.

In this Q&A with Ricardo Gonzalez – product line director, Space Products and Processing at BAE Systems in Manassas, Virginia – he discusses the effect that Department of Defense (DoD) budget cuts have had on the military space market, growth in demand for radiation-hardened (rad-hard) components, and how BAE Systems handles big data and reduced size, weight, and power (SWaP) requirements in its space products. Edited excerpts follow.

MIL-EMBEDDED: *Please provide a brief description of your responsibility within BAE Systems and your group's role within the company.*

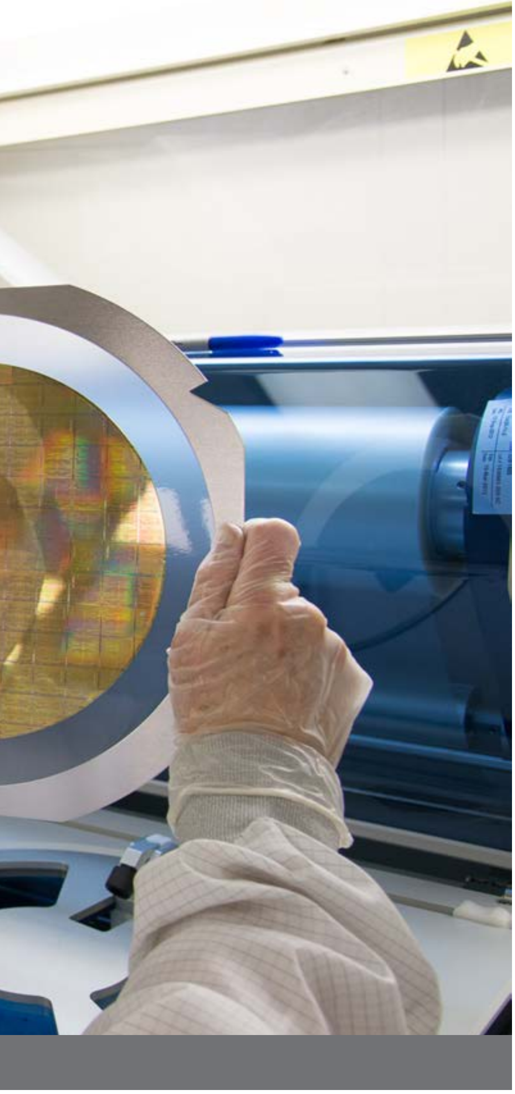
GONZALEZ: I am the product line director for Space Products and Processing (SP&P) at BAE Systems. SP&P is part of our Intelligence, Surveillance & Reconnaissance Solutions (ISRS) business area. It is the focal point for all space-related products, and we're responsible for developing and manufacturing a wide array of space subsystems and components that leverage world-class digital, infrared (IR), and radio-frequency (RF) technologies. The organization supports a variety of customers and our products are used in applications for DoD, civil, commercial, and national-security space missions.

MIL-EMBEDDED: *Please provide an example or two of current military and/or NASA platforms that use your BAE Systems radiation-hardened component technology?*

GONZALEZ: Our single-board computer (SBC) products, based on our RAD750 and RAD6000 microprocessors, are flying on more than 250 different spacecraft, including three generations of Mars rovers and Advanced Extremely High Frequency (AEHF) communication satellites. We also have memory products and application-specific integrated circuits (ASICs) on these platforms and on many others. Our RAD750 [SBCs] have truly become the trusted workhorse of the satellite computer market.

MIL-EMBEDDED: *The DoD released its FY 2017 budget request last month with a slight increase in overall funding. How do you view the DoD funding outlook for programs that make use of radiation-hardened components?*

GONZALEZ: For the market segments that we serve, the demand for radiation-hardened components is rather stable with less volatility than the overall DoD budget. We also see pockets of strong growth in the area of rad-hard components that enable higher levels of onboard processing capability. Highly integrated processors and reconfigurable computing components



are essential building blocks that are required for current and future demands of the evolving space market.

MIL-EMBEDDED: ***In many terrestrial platforms, innovation is happening at the intelligence, surveillance, and reconnaissance (ISR) payload level. How are satellite payloads evolving in terms of capability and the progress in electronics that enables new capabilities?***

GONZALEZ: Similar to the terrestrial platforms, satellite payloads are evolving by leveraging the increased onboard processing performance that we're able to deliver with advanced capabilities like BAE Systems' RH45 technology offering. For a myriad of reasons, the space community will likely always follow in the footsteps of terrestrial and airborne advances. Recently, however, we've seen a greater emphasis on closing the time gap between fielding a technology on the ground and flying the technology in space.

MIL-EMBEDDED: ***Reduced SWaP requirements are hitting all applications in defense electronics. How are they impacting your space system designs? What are the tradeoffs with smaller tech?***

GONZALEZ: SWaP has always been a major driver for satellite systems, and we see that continuing into the foreseeable future. We like to look at optimizing the performance of a solution within the power envelope for the electronics on a specific platform. Smaller technologies certainly help in providing more performance for the same SWaP constraints, but there are reliability, radiation, and thermal-density concerns that need to be considered in the trade. Care must be taken to balance all of these constraints in order to develop and manufacture optimal solutions.

MIL-EMBEDDED: ***How is big data being addressed in your rad-hard systems?***

GONZALEZ: Historically, the space community has been somewhat constrained by technology and a bit reluctant to equip satellites with the onboard electronics necessary to process and act on big data. In our view, evolving requirements and newer enabling technologies will drive more of this capability into the satellite. By providing autonomous onboard processing, we'll see the benefit of reducing the volume of data – which will therefore reduce the bandwidth required to transmit it for post-processing. But the biggest benefit will be a significant reduction in the time it currently takes to generate actionable information.

MIL-EMBEDDED: ***Is there more demand today for customized, rad-hard components such as microchips?***

GONZALEZ: In today's marketplace, there is more demand for system integration, and that drives the need for more advanced technologies. At the same time, many customers are also looking for standardization, so they don't own all of the risk and cost that are associated with custom microchips. Future systems – especially in the small-satellite segment – will likely have lower part counts. Many individual components will then need to be more capable.

MIL-EMBEDDED: ***Regarding the radiation-hardening process, what method is most preferred today?***

GONZALEZ: Radiation-hardened by design (RHBD) techniques leverage commercial wafer-fabrication processes, and that has become the preferred method for hardening microchips. At BAE Systems, we perform RHBD techniques at the custom circuit, in logic design, and at several steps in the physical-design process. This shift to RHBD occurred for multiple reasons. First, advanced technologies are more robust in response to certain radiation phenomena, while the remaining phenomena can be effectively mitigated or managed through design practices. Moreover, it's much more difficult to make invasive process modifications at the more advanced technology nodes. There will always be a few missions that will benefit from radiation-hardening by process, but that number is shrinking.

MIL-EMBEDDED: ***Budget- constrained environments for DoD programs often make it difficult to balance reliability with cost-effectiveness. How does BAE Systems handle reduced cost requirements from the DoD? Do you leverage commercial manufacturing processes, as some companies have done?***

THE RISKS AND COSTS OF UPSCREENING LOWER-QUALITY PARTS, FLYING AND MANAGING MORE REDUNDANCY, OR SPENDING MORE DOLLARS ON SOFTWARE TO MITIGATE AN ARRAY OF FAILURE MODES QUICKLY DWARFS THE SAVINGS THAT RESULT FROM STARTING WITH A LOWER-RELIABILITY BILL OF MATERIAL.

GONZALEZ: In response to budgetary constraints, BAE Systems closed its internal fabrication foundry, and now we operate as a fabless rad-hard electronics provider. We leverage commercial manufacturing processes to the greatest extent possible, while at the same time providing QMLV-qualified, high-reliability, rad-hard components. Where it's possible, we're able to provide lower levels of screening to meet mission requirements while reducing cost. But the cost of components is often a small percentage of the value for the overall mission. The risks and costs of upscreening lower-quality parts, flying and managing more redundancy, or spending more dollars on software to mitigate an array of failure modes quickly dwarfs the savings that result from starting with a lower-reliability bill of material. One way to look at the situation would be to total up the cost of all of the parts in a system and then compare it to the overall cost of the mission. In many cases, the right answer is to continue to fly higher-reliability components.

MIL-EMBEDDED: ***Looking forward, what disruptive technology/innovation will be a game changer for space electronics? Predict the future.***

GONZALEZ: At some point, we will have to break away from traditional transistor-based designs. But it does seem that every time we think we're reaching the limits of transistors, creative folks find a way to extend the useful life. The latest of these is the three-dimensional FINFET technology, which is enabling sub-10-nanometer transistors and three-dimensional packaging that further reduce parasitic loads. If not in the electrical realm, the game-changing technology of the future may be based on light or even biology. More than likely, we'll see a hybrid solution as a new technology takes shape. We've spent the better part of 50 years learning how to design with transistors, and it will take a while to learn a new way to solve problems. Once a few brilliant innovators show the way, the shift will likely happen faster than we could imagine. **MES**

__Ricardo Gonzalez__ is the director of space products and processing (SP&P) at BAE Systems in Manassas, Virginia. He oversees the team responsible for developing and manufacturing a wide array of space subsystems and components leveraging digital, IR, and RF technologies. He has been with BAE since 1997; he previously held the role of engineering director for SP&P and has taken a wide variety of leadership roles in engineering, program management, and new-business captures.

By Mariana Iriarte, Associate Editor

Navy destroyer detects/tracks medium-range ballistic missile

The U.S. Navy completed the Flight Test Other – 21 (FTX-21), demonstrating the Aegis Baseline 9.C1 capability to detect and track a medium-range ballistic missile (MRBM) target.

During the exercise, the target was launched from the Pacific Missile Range facility (Barking Sands, directly off the coast of Kauai, Hawaii) with the USS John Paul Jones (DDG 53) positioned west of Hawaii. Sailors were able to detect and track the target with the AN/SPY-1 radar using the Aegis Baseline 9.C1 weapon system.

The test was conducted with the support of the Missile Defense Agency, U.S. Pacific Command, Lockheed Martin, and Navy sailors aboard USS John Paul Jones. It marks the first demonstration of the Aegis system's ability to conduct a tracking exercise against an MRBM during the terminal phase of flight, Lockheed Martin officials say.

Figure 1 | USS John Paul Jones conducted the FTX-21 test, detecting and tracking a medium-range ballistic missile. Photo courtesy U.S. Navy.

Intel selects Mercury Systems to join FPGA tech-based network

Intel has selected Mercury Systems to join the company's field-programmable gate array (FPGA) technology-based Design Solutions Network (DSN) as a platinum-tier provider.

Mercury officials say that the DSN program brings together the former Altera Design Services Network, AMPP, and board/commercial off-the-shelf (COTS) members into a single program with common membership criteria and benefits. At the end of 2015, Intel acquired Altera, which is now the Intel Programmable Solutions Group (PSG).

DSN enables customers to find and utilize members to help accelerate time to market and lower product-development risk. At the same time, the members benefit by accelerating new Altera customer projects or board/IP development.

MicroGram GPS receivers ordered for Navy's ordnance-disposal robotics program

Neya Systems and Northrop Grumman officials contracted to deliver as many as 2,000 of the company's MicroGRAM global positioning satellite (GPS) receivers. MicroGRAM global positioning satellite (GPS) receivers. Engineers will integrate the receivers into Neya's Autonomous Behavior Capability Module, in support of Increment 1 of the Naval Surface Warfare Center's Advanced Explosive Ordnance Disposal Robotic System (AEODRS). MicroGRAM is a selective availability antispoofing module (SAASM)-based GPS receiver employed by military micro-users, who require secure position, navigation, and timing (PNT) to comply with Department of Defense (DoD) policy that all combat-support systems use SAASM-based GPS devices.

The Navy is leading the AEODRS program, which aims to develop a family of explosive-ordnance disposal (EOD) robotics. Officials say that Increment 1 will be the first of three that will be fielded.

U.S. Navy certifies Aegis Ashore site in Europe

U.S. Navy officials have certified the first Aegis Ashore site at Deveslu Air Force Base in Romania for operational use. The base is now monitoring southern Europe for ballistic-missile threats.

The activation of the system fulfills phase II of the European Phased Adaptive Approach, a plan begun in 2011 to protect deployed U.S. forces and European allies from ballistic-missile threats from the Middle East. Lockheed Martin is currently in the production process for certain elements of a second Aegis Ashore site, including SPY radar arrays in Europe that are set to be located in Poland.

Lockheed Martin officials say that testing and installation contracts have not been awarded yet for the second site, but U.S. Missile Defense Agency officials are expected to award contracts during spring/summer of 2016.

Figure 2 | A second European Aegis Ashore site is planned for Poland. Photo courtesy of Missile Defense Agency.

USS Zumwalt joins the fleet; homeport to be San Diego

U.S. Navy officials have accepted the delivery of the first Zumwalt (DDG-1000)-class ship, named appropriately enough, the USS Zumwalt. The ship will be commissioned in Baltimore following delivery and crew certification at General Dynamics-Bath Iron Works on October 15, Navy officials say. Mission System Activation will continue in conjunction with Post Delivery Availability in San Diego, the ship's homeport.

The ship underwent tests, trials, and demonstrations before Navy officials accepted the delivery. Testing included the ship's mechanical assemblies, electrical systems, and boat handling, while personnel performed drill demonstrations of damage-control, navigation, and communications systems. USS Zumwalt is scheduled to arrive in San Diego later this year.

The ship uses both active and passive sensors together with a multifunction radar (MFR). The arrangement of the ship's antennas reduces radar cross-section, thereby giving the ship a stealth capability. Its integrated power system (IPS) distributes 1,000 volts of direct current throughout the ship; the operator can allocate all 78 megawatts of power to propulsion, ship's service, and combat system loads.

Figure 3 | The USS Zumwalt is the first of three ships planned in this class to enter the fleet. Photo courtesy of the U.S. Navy.

MQ-8 Fire Scout deploys with upgraded mission-control system

The U.S. Navy's Naval Air Systems Command MQ-8 Fire Scout unmanned aerial vehicle (UAV) has deployed onboard the Littoral Combat Ship (LCS) USS Coronado, carrying Raytheon's upgraded mission-control system.

The Fire Scout UAV is designed to add situational awareness to the LCS. Raytheon officials say the Navy's hardware and Raytheon's software were combined to maximize Fire Scout missions from ships in littoral waters. The hardware and software are built with an open architecture in an effort to maximize flexibility and add new technology as needed.

Fire Scout now provides the potential for multiple platforms to be controlled from a single mission control aboard the ship, says Captain Jeff Dodge, the U.S. Navy Fire Scout program manager. USS Coronado is the first LCS to use this upgraded Fire Scout mission control operationally.

Railgun system demonstrated at Army Maneuver and Fires Integration Experiment

General Atomics Electromagnetic Systems (GA-EMS) officials demonstrated its Blitzer electromagnetic railgun system at the U.S. Army's Fires Center of Excellence annual Maneuver and Fires Integration Experiment (MFIX), held in April at Fort Sill in Lawton, Oklahoma.

The company performed 11 firings of the Blitzer railgun during the MFIX event, all at a target with a range that was greater than previous Blitzer firings. At the end of MFIX, the GA-EMS Blitzer railgun system was transported back to Dugway Proving Ground in Utah for more testing later this year.

The GA-EMS Acoustic Detection System, an unattended ground sensor system for multitarget simultaneous detection and tracking, was also showcased at the MFIX event. This system is designed to monitor multiple sensors simultaneously and enable visual detection and tracking of acoustic and seismic sources. MFIX is an annual exercise held to communicate requirements, validate and refine concepts, address capability gaps, and assess solutions for incorporation into the future Army Warfighting Assessments. The exercise brings together military and industry partners to view and conduct demonstrations of key technologies.

Air Force ARTS program contract won by Textron Systems

Textron Systems Electronic Systems has won an $11 million order from the U.S. Air Force for 12 Advanced Radar/Electronic Warfare Test Station (ARTS) Automatic Test Equipment (ATE) systems to support the B-1B Lancer strategic bomber fleet.

ARTS will replace the older ATE systems with a single integrated unit with an advanced COTS test system that meets the testing requirements of the ALQ-161 Defensive Avionics Systems. ARTS is an advanced radio frequency (RF) test station used by Air Force personnel for complex avionics systems.

"The ARTS system's initial platform is the venerable B-1; however, this advanced test station architecture could support many future Air Force requirements," says Steve T. Mensh, Textron Systems Electronic Systems' senior vice president and general manager.

Figure 4 | A B-1B Lancer takes off from Nellis Air Force Base. Photo courtesy of U.S. Air Force/Airman 1st Class Keven Tanenbaum.

ITAR COMPLIANCE TRENDS

Cybersecurity and export controls? Not for now in the U.S.!

By Kay Georgi

Designers of weapons systems, infrared technology, high-end radar, and intelligence, surveillance, and reconnaissance (ISR) systems all know that they need to ensure they've thoroughly checked every box regarding export compliance. But what about cybertechnology? How does the U.S. government manage and enforce export compliance for this area?

The regulations surrounding cybertechnology are complicated and new rule changes have been proposed that some in the tech industry find objectionable.

In spring of 2015, the Bureau of Industry and Security (BIS) within the Department of Commerce (DoC) published a proposed rule that will affect exports of products dubbed "cybersecurity items." These items include intrusion software and network communications surveillance systems, along with related systems, equipment, software, components, and technology.

Although some of these "cybersecurity items" are currently controlled for their "information security" functionality, the proposed rules:

- Substantially increase the items controlled;
- Require a license for the export, re-export, or transfer (in-country) of these items to all destinations except Canada;
- Increase the information that must be supplied to support a license application;
- Impose relatively stringent licensing policy on license applications; and
- Substantially narrow the license exceptions available.

The purpose of these proposed rules is to implement the Wassenaar Arrangement (WA) 2013 Plenary Agreements, which require so-called Participating States such as the United States to control for all items on the WA control lists.

In response to the BIS request for public comments to be submitted by July 20 2015, software and technology companies have uniformly objected to this regulation. For example, Google posted an article on its public policy blog stating that "these proposed rules, as currently written, would have a significant negative impact on the open security research community. They would also hamper our ability to defend ourselves, our users, and make the web safer. It would be a disastrous outcome if an export regulation intended to make people more secure resulted in billions of users across the globe becoming persistently less secure." Industry groups and nonprofits, such as the Electronic Frontier Foundation (EFF) and the Internet Association (whose members include major industry players), have submitted similar comments.

In response to the comments, BIS has backed off and is not implementing the Wassenaar changes for now. BIS officials have publicly stated that the U.S. government has taken the proposed cybersecurity controls back to Wassenaar in Austria to see whether they can be adjusted to make them more acceptable to industry. This delay means that the other countries, such as the European Union (EU) member states, now control items that are not subject to export controls in the United States. This situation could well lead unsuspecting U.S. exporters to forget that their products are in fact export-controlled in the EU.

Although the proposed rule will not go forward as written, it is useful to see what it would have covered had it been implemented. Specifically, the BIS proposed rule would have included changes related to intrusion software and network communication surveillance systems:

- Creating a new definition of "intrusion software":
  1. "Software" specially designed or modified to avoid detection by "monitoring tools," or to defeat "protective counter-measures," of a computer or network-capable device, and performing any of the following:
     - a: The extraction of data or information, from a computer or network-capable device, or the modification of system or user data;
     - b: The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions;
  2. "Monitoring tools" are software and hardware devices that monitor system behaviors, such as antivirus products, endpoint security products, personal security products (PSP), intrusion detection products (IDS), intrusion prevention systems (IPS), or firewalls. Thus, any software that is specially designed or modified to avoid detection by antivirus products or firewalls would be captured, provided it also performed either the extraction of data/information or modification of program requirements;
  3. Protective countermeasures" are defined as techniques to ensure the safe execution of code, such as data execution prevention (DEP), address space layout randomization (ASLR), or sandboxing;
  4. However, "intrusion software" does not include:
     - a: Hypervisors, debuggers, or software reverse engineering (SRE) tools;
     - b: Digital Rights Management software;
     - c: Software designed to be installed by manufacturers, administrators, or users for the purposes of asset tracking and recovery;
  5. "Network-capable devices" would include mobile devices and smart meters;

- Adding two new export control classification numbers (ECCNs) for software (ECCN 4D004) and related systems, equipment, software, and components (ECCN 4A005) related to "intrusion software" to the Commerce Control List (CCL). Because these new ECCNs would be controlled for national security (NS), regional stability (RS), and anti-terrorism (AT), an export license would be required for all destinations, except Canada. There are no license exceptions available for these items, except for certain portions of License Exception GOV [e.g., exports to or on behalf of the United States government pursuant to § 740.11(b) of the Export Administration Regulations (EAR)];
  1. ECCN 4A005 covers "systems," "equipment," or "components" for intrusion software, "specially designed" for the generation, operation or delivery of, or communication with, "intrusion software";
  2. ECCN 4D004 covers "software" "specially designed" for the generation, operation or delivery of, or communication with, "intrusion software."

  It is noteworthy that ECCNs 4A005 and 4D004 are both far broader than the intrusion software itself but encompass systems, equipment, components, *and software specially designed for the "generation, operation or delivery of, or communication with, 'intrusion software.'"*

- Amending two existing ECCNs affected by "intrusion software." No license exceptions are available for these items, including Strategic Trade Authorization (STA) or Technology and Software Under Restriction (TSR):
  1. 4D001 would additionally control "software" "specially designed" or modified for the "development" or "production" of equipment controlled by new ECCN 4A005;
  2. 4E001 would additionally control "technology" "required" for the "development" of intrusion software;
- Amending ECCN 4E001 so that it covers technology for the newly added 4A005 and 4D004, as well as technology "required" for the development of "intrusion software";
- Adding 5A001.j to control IP network communications surveillance systems, equipment, and components that meet all of a number of criteria.

Exports of these newly cybersecurity-controlled items would require a license to all countries except Canada, and be subject to a relatively strict licensing policy with a favorable policy of review only for:

- Exports to subsidiaries of U.S. companies, but not those located in D:1 or E:1 countries such as China, Russia, or Ukraine;
- Exports to "foreign commercial partners" in A:5 – that is, foreign-based nongovernmental end users that have a business need to share the proprietary information of a U.S. company and are contractually bound to the U.S. company;
- Exports to government end users in Australia, Canada, New Zealand, and the United Kingdom.

All other license applications will receive a case-by-case review to determine if the transaction is contrary to the national security or foreign policy interests of the United States, including promoting the observance of human rights around the world.

Cybersecurity items that have encryption functionality are controlled under the new cybersecurity ECCNs but still have to undergo all the encryption review requirements. **MES**

Cuba removed from E:1 country list; massive additional regulatory changes creating new license/exception opportunities

While Cuba opening up to U.S. imports may not be a boon to military-specific suppliers per se, it will create opportunities for U.S. tech suppliers and of course is a historic step towards normalizing relations. Cuba's removal from the E:1 list of terror-sponsoring nations last summer by the Bureau of Industry and Security (BIS) – along with the series of regulatory changes implemented by the BIS and Office of Foreign Assets Control – do not reflect a true open door for U.S. exports, but rather a small opening. While the comprehensive U.S. embargo of Cuba remains in effect, the new rules issue a series of general licenses/license exceptions and authorizations that simplify the process for those traveling to Cuba and expand the number of permitted activities.

Both 2015 and 2016 have been busy years for Cuba export controls and sanctions laws:

- On January 15, 2015, Departments of the Treasury and Commerce revised the Cuban Assets Control Regulations (CACR) and the Export Administration Regulations (EAR);
- On May 29, 2015, the Secretary of State rescinded the designation of Cuba as a State Sponsor of Terrorism;
- On July 20, 2015, the U.S. and Cuban embassies reopened as embassies in Havana and Washington, respectively;
- On July 22, 2015, the BIS amended its Export Administration Regulations to remove Cuba from some of the controls applicable to State Sponsors of Terrorism; they did, however, ensure that the embargo remained in force;
- On September 21, 2015, January 15, 2016, and March 16, 2016, BIS and The Office of Foreign Assets Control (OFAC) published additional amendments to the CACRs and EARs to provide additional limited relief.

The regulations provide a complicated web of small economic opportunities that must be matched by Cuban market access to be valuable to the U.S. exporter.

For example, BIS established License Exception: Support for the Cuban People (SCP), which authorizes the export of EAR99/AT-only items commercially sold or donated to private-sector entrepreneurs as end users, for use in private agricultural activity, and building materials and equipment for private-sector use. Moreover, for first time in 60 years, U.S. companies can establish a limited physical presence in Cuba. However, even companies that have products in the range of allowed goods for sale into Cuba have to find a Cuban private-sector end use to sell those goods to. This Cuban private sector is hard to find, making the license exception less useful than it otherwise may seem.

Exports to Cuba of items for telecommunications, including access to the Internet, use of Internet services, infrastructure creation, and upgrades are also eligible for export under License Exception SCP; there is no private-sector end-use requirement, although there are some limitations. Another license exception, CCD, authorizes the export of certain EAR99- and AT-controlled computer hardware and software for use in cloud services to Cuba.

If a product cannot fit under a license exception, BIS will consider favorably applications for licenses to export items to meet the needs of the Cuban people, including to state-owned enterprises and agencies of the government in Cuba that provide goods and services to the Cuban people. It will also consider exports and re-exports that would enable or facilitate exports of items produced by the private sector in Cuba. However, to be considered, such exports cannot primarily generate revenue for the Cuban state.

The removal of Cuba from the list of State Sponsors of Terrorism and the BIS regulation from July 2015 implementing this change primarily impacts the de minimis rule applicable to foreign-origin items destined for Cuba that incorporate U.S.-origin content and certain license exception restrictions, such as aircraft, vessels, and spacecraft (AVS) and replacement of parts and equipment (RPL).

Cuba and the de minimis rule

Foreign-produced products are subject to export and re-export controls under the EAR if they contain more than a certain percentage (by value) of U.S.-origin controlled content or are the "direct product" of certain U.S. technology. Under the de minimis rules, U.S.-origin content is considered controlled when it requires a license to the intended ultimate country of destination for the foreign-made item, which for Cuba includes all items subject to the EAR, including EAR99 items not on the Commerce Control List. This rule primarily impacts non-U.S. manufacturers who incorporate U.S.-origin materials, parts, or components in their non-U.S. products, U.S.-origin software in their non-U.S. software, or U.S.-origin technology in their non-U.S. technology.

Previously, an item produced outside the United States for export to Cuba was subject to the EAR if it contained more than 10 percent U.S.-origin content. For most other destinations, EAR re-export jurisdiction is triggered under the de minimis rules only when an item contains more than 25 percent U.S.-origin content.

By removing Cuba from Country Group E:1, Cuba is now eligible for the general 25 percent de minimis level. In other words, a foreign-origin item from a non-U.S.-owned or controlled foreign firm that contains less than 25 percent U.S.-origin parts and components destined for Cuba will no longer be subject to the EAR, no longer require a BIS license, and no longer be subject to a general presumption of denial. Foreign-made items destined for Cuba that incorporate U.S.-origin 9x515 or ''600 series'' content (including items identified in the ".y" paragraph of the "600 series" ECCN) and certain encryption and other special items, however, continue to be subject to the EAR regardless of the level of U.S.-origin content. That is, there is no de minimis for these items when destined for Cuba.

Overall, this change will assist non-U.S. companies, provided they are not owned or controlled by U.S. persons. It will have little impact on U.S. companies or their U.S.-owned or U.S.-controlled foreign subsidiaries. Under OFAC regulations, U.S.-owned or controlled foreign firms must first get a specific license from OFAC to re-export any foreign-made item to Cuba even if no U.S.-origin parts and components are included therein. In addition, all companies exporting non-U.S. items to Cuba will need to continue to confirm that they are not the direct product of certain U.S. technology that is controlled for national security reasons. Such items will continue to require a license under the foreign direct product rule, which has been amended to include E:2 countries – currently Cuba remains on this list.

The new Cuba regulations are complex. BIS has published helpful FAQs explaining its regulations, including which regulations were changed and when, at: https://www.bis.doc.gov/index.php/policy-guidance/faqs. OFAC has also published helpful FAQs at https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cuba_faqs_new.pdf. However, any U.S. exporter wishing to dip its toes in the Cuban waters would be well advised to consult qualified counsel or experts in the area.

Export compliance in 15 steps

Kay Georgi, an export compliance attorney and partner at Arent Fox LLP in Washington, D.C., outlines 15 key steps to International Traffic in Arms Regulations (ITAR) compliance – updated for 2016:

1. Get management buy-in for your compliance program. If management does not support the program, it likely will not work;
2. Identify two persons in your organization who will be your export compliance personnel – one is not enough. If you do not have good candidates, you might have to recruit from outside your organization;
3. Make sure your export-compliance personnel have thorough export-control training. For most companies except the very largest, this usually means outside training;
4. Classify all the products, services, software, and technology that your company exports. This might mean classifying all items, even if you do not export them in the traditional sense, if you employ foreign nationals or procure offshore. Put in your new product development a gate for classification, and put in your new contract review system a gate for classification. MAKE SURE YOU HAVE RECLASSIFIED ANY OF YOUR PRODUCTS, SOFTWARE, OR TECHNOLOGY THAT JUST WENT THROUGH (OR IS ABOUT TO GO THROUGH) EXPORT-CONTROL REFORM. YOUR PRE-2013 ITAR CLASSIFATION MAY NO LONGER BE WORTH THE PAPER IT IS PRINTED ON: YOUR PRODUCT MAY NOW FALL UNDER THE 600 SERIES ON THE COMMERCE CONTROL LIST, OR EVEN BE DECONTROLLED ALTOGETHER;
5. Make sure any controlled products are identified in your ERP system or in another fashion so that your personnel will know that those products are controlled. If you procure controlled products, be sure your vendor understands and agrees to implement export compliance procedures (and is ITAR registered as applicable). If you procure overseas, make sure you obtain any necessary license or other authorization to do so;
6. Put in place automatic and other gates in your enterprise resource planning (ERP) system and in your sales/customer service departments to make sure that any controlled products are not exported, re-exported, imported (for items on the U.S. Munitions List and U.S. Munitions Import List), or transferred without any required license;
7. Put in place a gate in your returns and repairs department, to make sure that all returns of defense articles to the U.S. are properly authorized (exemption claimed) and returned pursuant to license or exemption. Also, make sure the department recognizes if the item has ended up in the hands of an unlicensed end user;
8. Create a technology-control plan to cover controlled technology. Be sure to include IT, human resources, and procurement/purchasing (for offshore procurement) departments in your plan. In particular, with the assistance of IT, HR, and procurement departments:
   - Put in place standard operating procedures (SOPs) to identify, correctly label, and protect controlled technology;
   - Put in place SOPs to identify and to obtain DSP-5 or Bureau of Industry and Security (BIS) licenses for foreign persons hired both permanently and temporarily (for example, through temp agencies);
   - Analyze the risks associated with your IT system and use encryption, secure FTP sites for communications with customers, user-access controls, software that can identify access, and the location of servers to reduce risk of inadvertent export/access issues. Put in place SOPs for the above. MAKE SURE YOUR IT SYSTEM IS TAKING ADVANTAGE OF THE NEW BIS RULE, EFFECTIVE SEPTEMBER 1, 2016, THAT SAYS EAR-CONTROLLED TECHNOLOGY THAT IS (1) UNCLASSIFIED, (2) ENCRYPTED USING END-TO-END-ENCRYPTION, (3) SECURED USING FIPS 140-2 OR EQUIVALENT ENCRYPTION, AND (4) NOT STORED IN ARMS EMBARGOED COUNTRIES OR RUSSIA, IS NOT "EXPORTED, REEXPORTED OR TRANSFERRED". But watch out, the new rule does not apply to ITAR-controlled technical data, yet, although a companion rule is expected to be issued by the State Department;
   - Create and put in place a laptop, USB, and Blackberry/smartphone SOP;
   - Create and put in place SOPs for international travel;
   - Create and put in place SOPs for visits.
9. Create a license/agreements/exemptions/exceptions management system, including the export process and filing of Automated Export Records, to ensure compliance with all licenses, license exceptions (EAR), or license exemptions (ITAR). Be sure you are taking advantage of license exception Strategic Trade Authorization (STA) and have a procedure and recordkeeping to ensure compliance. Make sure your foreign licensees understand and agree to all license conditions and provide the STA consignee letter;
10. Be sure to screen all customers and suppliers against the restricted party lists, both at the initial input stage and on a regular (or evergreen) basis; also record and preserve screens;
11. Train personnel for red flags of prohibited end use and diversion and create a process for resolution of red-flag screening;
12. Create a problem-management SOP to deal with issues as they arise, as well as for government inquiries and visits and voluntary disclosures;
13. Put all of the aforementioned procedures into a compliance manual and SOP document;
14. Train and test all personnel, or at least most personnel, on the compliance manual and SOPs on a regular basis;
15. Audit regularly, alternating responsible internal auditors (if you have them) with experienced outside auditors. Follow up on audit results. File voluntary disclosures where warranted.

__Kay Georgi__ is an export compliance attorney and partner at Arent Fox LLP in Washington, D.C. She is the co-editor with Paul M. Lalonde of the new "Handbook of Export Controls & Economic Sanctions," published by the American Bar Association's (ABA's) Export Controls and Sanctions Committee. The book also is expected to be available in e-format for downloading on the ABA web store shortly after the release of the printed book. For more information, visit http://bit.ly/10FDGtN. Kay and Paul are currently working on the second edition.

Compliance pitfalls

Export compliance, while not rocket science, does require vigilance and a rigorous attention to detail if companies and individuals want to avoid big fines and in some cases criminal charges. Errors are bound to happen, but Kay Georgi, an export compliance attorney and partner at Arent Fox LLP in Washington, D.C., says there are three points that defense suppliers need to focus on in today's environment. "The first one is to make sure to disclose any unlicensed export or transfer of ITAR items immediately," she says. "Do not pass go, do not collect a hundred dollars. State Department agents might have a problem later, especially if the items went to China or other arms-embargoed countries. The State Department is very clear that they want to know now.

"The second one is not new, but still important," Georgi continues. "You must make sure you have your facts correct in any disclosure – the first time it happens. Minor voluntary disclosures are not what I'm referring to, but if it involves security or any intentional misdoing you really need to go on the deep dive and get outside legal counsel. This is not the case to skimp on but potentially abet the company case. Make sure you get your facts right because your company and your company's employees are both potentially at risk for criminal violations.

"The third one is to make sure you don't skimp on compliance after you get your license," she warns. "State Department licenses such as Manufacturing License Agreements (MLAs) and Technical Assistance Agreements (TAAs) can last as long as 10 years. That is a long time and creates a huge potential for you and your company to make mistakes. Suppliers must be vigilant and do periodic checks on their compliance practices such as making sure no foreign nationals have been hired [who are] now working on ITAR technology. In that way, it is like raising children. Many first-time parents think it's all about the pregnancy, but that's nothing compared with raising the child. Once State approves the export license, the job isn't over – it's just beginning."

Smart in your world®

Arent Fox

Shown here is an artist rendering of a U.S. Air Force Advanced Extremely High Frequency (AEHF) satellite in space. Photo courtesy of Lockheed Martin.

Military secure satellite communications capacity is evolving rapidly

By Sally Cole, Senior Editor

The capacity and capabilities of military satellite communications systems are evolving, but so are the multifaceted security challenges they now face.

The secure satellite communications (SATCOM) equipment used by the U.S. military is currently undergoing impressive capacity and performance advances; at the same time, it faces increasing security threats on several fronts.

In 2014, researchers at security firm IOActive in Seattle, Washington, identified serious design flaws and vulnerabilities within the firmware of popular SATCOM devices that could allow remote attackers to intercept, manipulate, block, and even take full control of critical communications systems on terminals used on the ground, in the air (except in space), and at sea. [The products involved in IOActive's study were manufactured or marketed by Harris, Hughes Network Systems, Cobham, Thuraya Telecommunications, Japan Radio Company, and Iridium Communications.]

"Fortunately, some of the SATCOM devices and related infrastructures are now more secure than two years ago," says Ruben Santamarta, principal security consultant for IOActive. "There's been a significant push from companies to introduce security into the common life cycles of products. We recommend taking security seriously – by deploying a security development life cycle from the very beginning."

How are SATCOM terminals being attacked? "They can be compromised in different ways, closely related to the threat scenario," Santamarta says. "Physical attacks, which involve taking the terminal apart and installing a new hardware module or a malicious firmware, are the most difficult to prevent. This type of attack, however, also requires significant resources and even human intelligence. Remote attacks are feasible, but should always be analyzed on a case-by-case basis. And some systems end up exposed to the Internet due to improper configurations. The problem is that a single compromised device may serve as the entry point for a wider attack that affects other assets."

One of the biggest problems is that "encryption use isn't as common as it should be," according to Santamarta. "SATCOM services are expensive and data charges are a major drawback when introducing secure communications."

Broadband services and technology company ViaSat in Carlsbad, California, confirms that hacking attempts are indeed a significant concern. "Encryption is necessary, but even that isn't sufficient to defend against the denial-of-service (DoS) threats we're seeing," says Jerry Goodwin, chief operating officer of ViaSat Inc.'s Government Systems Division. "Most networks are being attacked at the system level – hackers are finding weaknesses within systems that allow them to maneuver around encryption. Traditional IT approaches don't address the real-time nature of these attacks."

The biggest threat ViaSat is experiencing comes in the form of DoS attacks. "In terms of the layers of security involved, users usually encrypt their data end-to-end … and they decide how to do it. Governments, for example, have their own encryption solutions," Goodwin explains. "And we provide security in the transmission system and have protection in place to deal with DoS attacks in our infrastructure."

BROADBAND SERVICES AND TECHNOLOGY COMPANY VIASAT IN CARLSBAD, CALIFORNIA, CONFIRMS THAT HACKING ATTEMPTS [ON SATELLITES] ARE INDEED A SIGNIFICANT CONCERN.

ViaSat's security approach involves traditional best IT practices, firewalls, intrusion-detection systems, and analytics – known as "defense in depth," with layered security. "But we're trying to figure out a more real-time and comprehensive solution," Goodwin says.

This situation is particularly difficult when facing down a multifaceted challenge. "If someone is trying to steal your data it's encryption's job to protect it," Goodwin points out. "When someone's trying to prevent you from transmitting, it might be because they're trying impact your ability to serve your customers by jamming the satellite. Part of our response is designing satellite networks to be resistant to jamming and to respond automatically to threats."

On the ViaSat-1 satellite, significant effort went into developing an automated DoS threat response. "Every day, our service networks see bot-based DoS attacks. These attacks are constantly directed toward the infrastructure, which we can visualize on our threat-mitigation screens," Goodwin says. "You can actually see the traffic rising up and attacking one of the nodes."

To counter this type of attack, ViaSat designed a system on the edges of the network to look at the threat, recognize it, and start dumping those bits into what it calls a "bitbucket" so the network doesn't try to deliver them. "We have arrangements with our ground infrastructure partners to do some of this automatically. That's an example of what we're trying to do, not just with that type of threat, but all threats. It's a whole-network systems approach," Goodwin notes.

ViaSat's next-gen satellite's security infrastructure will feature "distributed cyber-sensors, visualization techniques, and greater automation of attack response," Goodwin says. "Many things are occurring at machine time, and people can't respond quickly enough to the threats. So there's a lot of research going on to figure out better ways to handle it."

As IOActive's Santamarta sums it up: "In terms of military strategy, you always need to take into account capabilities, not intentions, because these can change overnight. So it seems reasonable to assume critical military communications, including SATCOM, are now and will continue to be a valuable target in the future."

AEHF designed for resiliency

Potential security threats are among the reasons that the engineers working on Lockheed Martin's Advanced Extremely High-Frequency (AEHF) satellite communications designed it to be one of the world's most resilient satellite communications systems. AEHF serves not only the U.S., but also partner nations Canada, the Netherlands, and the United Kingdom.

"AEHF provides a necessary assured-communications link for national leaders and military commanders transmitting sensitive information in contested areas," says Iris Bombelyn, vice president of Lockheed Martin's Protected Communications mission area in Bethesda, Maryland. (Figure 1.)

Figure 1 | Lockheed Martin engineers inspect the U.S. Air Force's second Advanced Extremely High Frequency (AEHF) satellite before it is shipped from Sunnyvale California to Cape Canaveral Air Force Station in Florida for launch.

What makes AEHF so resilient? It's made up of nuclear-hardened communications satellites designed to stave off high-tech jammers, eavesdropping, and cyberattacks. "Onboard signal processing and satellite-to-satellite crosslinks insulate communications from vulnerability by eliminating the need for ground-relay stations," Bombelyn explains. "We also use an extremely wide bandwidth to transmit the signal and antennas that can pinpoint and eliminate jammers. All of these features and capabilities combine to protect against, deflect, and overpower threats."

While there are many secure satellite communications systems serving both the civil and military sectors, AEHF "is the only current system protected against the full spectrum of threats," she points out.

Figure 2 | Pictured is ViaSat 1 launching into space. Photo courtesy of ViaSat.

As the worldwide need for data increases, communications satellites must be capable of providing the requested bandwidth when and where needed. With this in mind, "AEHF was designed to significantly increase capacity for the U.S. government," Bombelyn notes. "Compared to its predecessor Milstar, a single AEHF satellite has a greater total capacity than the entire Milstar constellation."

AEHF satellites provide expansive global coverage to enable data-transfer capabilities that promote increased flexibility during worldwide military operations. "AEHF offers faster connections up to 8.2 Mbps, as much as five times faster than the legacy constellation," she adds.

With these speeds, AEHF "rapidly transmits tactical military communications, such as real-time video, battlefield maps, and targeting data," Bombelyn says. "Lockheed Martin is also exploring capabilities that will be required for the satellites of tomorrow, and has developed concepts that provide users with even more bandwidth and flexibility to support their missions."

Capacity advances on the way

Lockheed Martin isn't alone in making capacity advances: Also increasing capacity significantly is ViaSat.

"For decades, the industry has focused on how to eke the last bit of efficiency out of the modem side of the link. The problem is that modems are operating at near-theoretical performance, and it isn't going to get much better," ViaSat's Goodwin says.

ViaSat contends that the problem is in space, not on the ground. "It's how the satellite is organized and designed," Goodwin continues. "Today, we can put more than 700,000 customers on a single satellite. And with ViaSat-2, which will launch in 2017, we'll double the capacity from ViaSat-1. When the ViaSat-3 constellation launches in 2019, it'll offer 1 Tbps per satellite and will deliver 100 Mbps to each user." (Figure 2.)

Can ViaSat make the data go faster? "Yes – we could make it 200 Mbps, but 100 Mbps seems like the right rate for that time frame. A conventional satellite does 2 Gbps per satellite, so ViaSat-3 will be 500 times that amount and will give us more flexibility in the service plans we offer," Goodwin says.

Costs, as always, a factor

Satellite communications traditionally have been dominated by the cost of the capacity, even more than the cost of equipment on the ground. "In a commercial market, the cost of capacity is directly related to how much it took to put that capacity into space, as well as supply and demand," Goodwin says. "Capacity costs completely dominate over equipment costs for the life span of the equipment."

To this end, ViaSat is changing the space side of the equation because "it provides more benefit to customers," he adds. "We're building satellites focused on capacity for communicating large amounts of data. We're also breaking with tradition by designing satellites to support two-way communication."

On Lockheed Martin's end of things, although the U.S. government is currently studying military communication architectures beyond the planned AEHF 5 and 6, it is "already working to develop low-cost, follow-on options that leverage economies of scale by using standardized components from commercial satellite contracts," Bombelyn notes.

Use of commercial off-the-shelf (COTS) products in AEHF must first be evaluated to determine whether they're robust enough for the environments Lockheed Martin intends to use them in, according to Bombelyn. "Our mission requires that we are the communications channel that stands when all others fail," she points out.

Quantum future?

Another challenge looming on the horizon comes in the form of quantum computing, which may arrive years earlier than expected and head directly to space.

China has announced its intention to launch a quantum space satellite (known as QUESS) in July 2016. The satellite will be operated by China's Academy of Sciences, which claims QUESS "may provide the path to an uncrackable communications system by turning messages quantum and taking them into space."

Does the U.S. have its own quantum goals for securing its military satellite communications? If so, they're keeping it a secret.

"Although I can't specifically discuss quantum communications, safeguarding and preserving our satellites and their missions is of the utmost importance, and continued advancement in protective technologies by the entire industry must remain a top priority," says Lockheed Martin's Bombelyn.

The biggest challenge Bombelyn sees ahead for military communications is providing systems that are capable of handling a variety of threats from adversaries at an affordable price point. "Solving this problem will require combining design solutions from our commercial satellite systems, common satellite components, and new technologies," she says. "Space has typically been a cooperative environment, with spacefaring entities working together for the greater good. With new entrants to this arena, the future is unclear." **MES**

TRENDS IN RADIATION-HARDENED ELECTRONICS

COTS in space? Not so fast, say some rad-hard designers

By Mariana Iriarte, Associate Editor

The role of commercial off-the-shelf (COTS) parts fielded in satellites and other space applications remains a hot topic as the demand for low-cost nanosatellites grows. COTS signal-processing designs are also attractive to military space system designers, but they fear the reliability of such components in long space missions.

Smaller satellites about the size of these CubeSats deployed from the International Space Station (ISS) will likely change the way COTS technology is used in space applications. Photo by astronaut Tim Peake onboard the ISS on May 16, 2016. The bottom-most CubeSat is the NASA-funded MinXSS CubeSat, which observes soft X-rays from the sun; such X-rays can disturb the ionosphere and thereby hamper radio and GPS signals. Photo courtesy of NASA.

Budget constraints, demand for inexpensive small satellites, and other issues are forcing space-platform designers to consider using COTS components for space, but COTS parts may not be appropriate or desirable for all space missions.

Space 2.0

The market is open to the idea of using COTS in space. “This whole concept of building large constellations with COTS components, we refer to it as ‘new space.’ I’ve also heard it referred to as Space 2.0,” says Ken O’Neill, director of marketing, space, and aviation for Microsemi’s SoC Products Group in San Jose, California. “We are in dialogue with many companies who are proposing to create systems along the lines of using commercial parts and we are doing what we can to support it. We also have to acknowledge the reliability of such systems is going to be the proof of the pudding. Everyone is waiting to see if they can create a constellation with cheap commercial products.”

Budget constraints may be the driving factor for designers of space applications to find new ways of addressing the challenged posed by COTS components. The reality: Military officials want COTS components in applications where cost needs to be reduced. However, using COTS components where radiation-hardened components are required becomes more of a challenge to implement, versus spending the money in order to have a high-reliability system.

“COTS components put a burden on the design team in order to do mitigation on the part,” O’Neill says. “There are mitigation techniques that are in the open domain – redundancy and using spares – those are the two things that you do to mitigate.”

However, even using mitigation techniques, “You have to put more parts into the system than you would have otherwise,” he continues. “If you were using a COTS part, you would need to put triple-redundancy parts into this. That presents some challenges from the perspective of board space and power consumption. Now you have to supply power to three parts instead of one.

Using COTS components in space translates to more work: “Even worse,” O’Neill continues, “you also have to put some kind of voting and control mechanism, a system that monitors activity and makes a decision that one of the parts has an upset or is transient and that renders it inoperable, which needs to be reset. Something has to be a watchdog on there. That’s an extra component that needs to be powered and consumes board space.”

Extra processing steps would have to be taken to make COTS components meet rad-hard requirements. Therefore, “most of the customers we are talking to today

are leaning towards traditional, high-reliability hermetic ceramic packaged products to use in space," says Larry Longden, vice president and general manager at Data Device Corp. (DDC) in San Diego, California.

There are still pros to using COTS components. "COTS to me has always had the ability to have a product on the shelf versus having to build to order," says Chuck Tabbert, vice president of sales and marketing at Ultra Communications in Vista, California. "The advent of the Qualified Manufacturing Line (QML) system has made it possible to have companies build products to forecast and qualify the fabrication line versus building to the next order that comes in the door and running a lot-specific qualification."

Space applications need to last for a few years in orbit. "With small satellite constellations, they're mostly in low-Earth-orbit (LEO) applications, chasing the 'Internet in the sky' mobile communications and Earth observation markets," he continues. "The mission profile will probably not be that of the geosynchronous constellations and therefore the radiation requirements for these LEO applications will be less severe."

Mission-specific small satellites

COTS components might be the answer for small satellites that are mission-specific only. "In recent years the U.S. military has had their own initiative on smaller satellites, with the intent to reduce launch costs and the time taken between making a decision to create a satellite to fulfill a mission and "getting that satellite in orbit," O'Neill says. "The military runs the program called Operational Responsive Space (ORS), which is managed by the Air Force Research Laboratory (AFRL). There have been a number of ORS satellites already built and launched. Other, experimental, satellites have already been developed and launched, some of which have intended to see what can be done with small form factors."

Tabbert asserts that in order to make COTS components successful in space, rad-hard semiconductor folks [must be able] to anticipate what products will be selling in the small satellite market, keep the line qualified, and have products on the shelf in-house or at distributors, as well as keep the unit price competitive.

The good news about the military is that "they will use whatever they can to get the job done – be it small satellite constellations, to hosted payload applications, to standard GEO and MEO constellations," he continues. "With rumors of nation-states developing anti-satellite capabilities, it just makes sense to diversify one's assets on numerous platforms so no one strike can take down a capability. Small sat constellations have their place for certain missions."

The lure of high-end signal processing

COTS components are attractive because they offer so much in terms of bandwidth and performance. "The design community in radiation-hardened electronics is really working on solving the big signal-processing challenge," O'Neill says. "The issue is that satellite operators are looking for an increased amount of information to come from their space assets, whether it's remote sensing satellites, imaging, radar, or spectrometry."

High bandwidth demands in satellite applications dictate the path designers take with rad-hard electronics. "The industry is leaning towards higher density memory products and higher speed A/D or D/A converters, along with more high-speed interface options," Longden says.

Also commanding attention is the need for speed. "Intra-satellite data-transfer bandwidth requirements are exploding. Point-to-point solutions between sensors and instruments to flight computer to mass-memory storage requirements are requiring 40 [Gigabits per second] Gbps transfer rates, which will increase to 100 Gbps in the next three to five years," Tabbert says.

Because of the high demand, "hardened- [field-programmable gate array] FPGA manufacturers are struggling to keep up. The need for 10 Gbps to 25 Gbps per channel connectivity is coming quickly," he adds.

The ultimate goal of these parts is "to be able to store and process all the data that [operators] are connecting on satellites. It's a tremendous amount of data, and they need faster and bigger memory to do that," Longden says. "As well, they need faster and more accurate conversion products to be able to read that data from different analog systems."

One such memory product is DDC Microelectronics' NAND-Flash memory, aimed at reaching those high-density, high-speed memory requirements for space. (See Figure 1).

Another example of a product intended to meet the high-density, high-bandwidth data demands of space is Microsemi's RTG4 board (see Figure 2). "It is intended to satisfy that demand for onboard signal processing. It has more logic resources and it's got more multiply-accumulate blocks," O'Neill says.

Embracing standards

Taking advantage of signal processing innovation today also means leveraging standards. "We are seeing a lot of industry involvement in standards such as SpaceVPX," says O'Neill. "It's a standard that has a lot of industry alignment behind it," he says.

The standard "provides form factor and interconnect standards for board-to-board communications. In space systems, designers are using serial interconnects – 2.5 Gbps, even some as high as 3 1/8 Gbps, per lane – and of course those lanes can be ganged together," O'Neill adds.

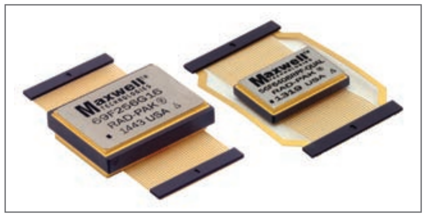


Figure 1 | NAND and NOR with RadPak technology. Photo courtesy of DDC.

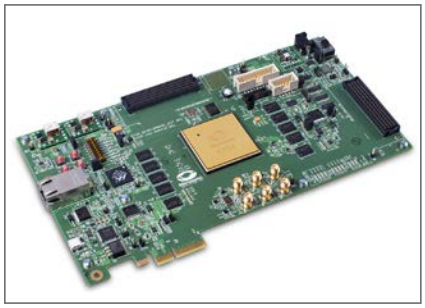


Figure 2 | RTG4 development board with FPGA. Photo courtesy of Microsemi.

Figure 3 | The UT64CAN333x series is packaged in an 8-lead ceramic flatpack. Photo courtesy of Cobham.

Standardization evens the playing field. Moreover, says Michelle Mundie, business area director, standard products, at Cobham Semiconductor Solutions in Colorado Springs, Colorado, "Leveraging open standards will enable more capabilities for the sensor payload. The SpaceVPX architecture of interconnects drives the standards for performance. New products can interconnect with one another to achieve performance. Standardizing the platforms will reduce design complexity and cost."

Cobham Semiconductor Solutions' UT64CAN333x series of Controller Area Network (CAN) transceivers are designed to manage rates ranging from 10 kbps to 8 Mbps; all are designed in accordance with the ISO 11898-2/-5 standard (see Figure 3). "Cobham is focusing on rad-hard by design and rad-hard at process techniques while also addressing size, weight, and power (SWaP) requirements," Mundie says. "This angle allows the company to look at different technology notes and interconnect architectures in satellites." **MES**

Space-satellite funding continues to be slow

While the military space market has never been known as an explosive one in terms of investment due to its long design cycles and low volumes, industry players say that orders are picking up.

"Funding for military space programs have been slightly increasing," says Ken O'Neill, director of marketing, space, and aviation for Microsemi's SoC Products Group in San Jose, California. "[However,] the last two or three years have been quite difficult from the point of view of suppliers working with the U.S. defense community, as funding has been slow to release. We feel like we are being drip-fed a little bit."

Funding for satellites is being released at a rate of one satellite at a time, whereas five to ten years ago, those programs would have released funding for two, three, or four satellites at a time," he notes. "It gives us less visibility from a forecasting point of view and makes things a little more difficult."

Those programs that are funded in manageable chunks only see "some pockets for procurements in the military side, but they are primarily related to satellites that have been on hold since sequestration began," says Larry Longden, vice president and general manager at Data Device Corp. (DDC) in San Diego, California. "The market is not increasing. An example is that this year they began procurement again on Joint Polar Satellite System (JPSS) satellites, which had been on hold for a while."

To make the situation even more backlogged, already tested platforms are getting first dibs on funding, which puts the brakes on innovation. "I see procurements occurring for already designed satellites, ones that are ready, but I don't see new budgets being created in the marketplace," Longden continues. "The government has eliminated most of the budget for development in the space arena."

That's not always the case, though, says Chuck Tabbert, vice president of sales and marketing at Ultra Communications in Vista, California. "For high data rate transfer applications, the market is booming. Most worldwide prime contractors are through the experimental evaluation and system design phase and many are moving into qualification and production in fiscal years 2016 through 2020."

Rad-hard for the long haul

By Doug Patterson

Managing the long-term effects of radiation in space environments is essential for designers of components headed for space. Mission length, more than any other factor, contributes most heavily to the sustainability of electronic components in radiation-laden applications.

Shorter, nanosat missions may leverage COTS in space effectively, but anything longer or military-based requires greater rad-tolerance than traditional COTS components provide. Image courtesy of NASA.

Next in line is how critical the mission is – is it a question of loss of life in the event of a failure, a catastrophic communication breakdown, or merely a blip in the timetable update of a local bus or railway network?

Different levels of Earth's orbits contribute separately to radiation exposure as well. High geostationary (GEO) orbits, for example, have harmful galactic cosmic rays and solar flares (protons and electrons) at much higher levels than lower orbits like medium Earth orbit (MEO) and low Earth orbit (LEO), because of the lack of the inherent shielding effects of the Earth's magnetic shield. However, what is not to be ignored in LEO and MEO is the higher concentrations of trapped particles localized within the Van Allen belts.

There are also anomalies in the Earth's magnetic field – most notably the South Atlantic Anomaly (SAA) – where those trapped particles wreak havoc with unshielded or non-radiation-tolerant commercial off-the-shelf (COTS) electronics (Figure 1). Orbiting the Earth 16 times in a 24-hour period, the International Space Station and Hubble Telescope both often pass through and must therefore deal with the SAA's effects by either shutting down sensitive electronics or suspending imaging tasks during the transition.

Component reliability in space applications comes down to endurance in the face of radiation exposure, both from accumulated levels and the myriad of radiation types that can affect total dose, single-event effects, and other deleterious effects that can include gate burnout, substrate latchup, heavy ion bombardment, neutron and heavy ion-induced lattice atoms displacement (i.e., destruction of the base silicon or sapphire crystal structures at the atomic level), or thermal cycling.

The question of qualification

Mission length and mission criticality, such as manned versus unmanned, will dictate whether or not to use the tried-and-true NASA EEE-INST-002 (Electronic, Electrical, Electro-mechanical) components guidelines to guarantee maximum reliability or think about using different component selection criteria. A major consideration is to either select components not yet flight-proven, but that can be qual-tested and are therefore characterized for space flight, or to select strictly industrial or extended-temperature COTS components.

COTS components without any space heritage or characterization can have one-tenth to one one-thousandth the reliability and longevity of the NASA EEE parts in certain radiation types and exposure times. (Table 1.) Although the COTS parts may cost less, they can fail catastrophically in hours or days versus years – depending on their suborbital and/or orbital application – and the price of failure can be immeasurable.

The EEE to COTS component cost differences between these varied approaches can be several orders of magnitude, but because reliability and mission lengths can be drastically reduced due to unreliable components, component choice needs to be careful and wise.

The long view approach to in-orbit systems

All the supposed advantages regarding size, weight, power, and cost (SWaP-C) and other issues that pertain to a terrestrial military and aerospace program are invalid when it comes to manned or unmanned spacecraft and radiation-induced failures. For university experiments with shoestring budgets, standard COTS components will work, but not for long. Radiation total ionizing dose (TID) will wipe out a command and data handling system, perhaps in only a couple months. Particles and heavy ions can and do accumulate in the component substrates and cause latent damage, powered or not.

Orbital launch platforms are not cheap and launch options are still limited, so it still costs thousands of dollars per pound, per unit mass, whether launch is of one large telecommunications or military-communications satellite or a group of "shoestring" Nanosats built from Arduino processor boards bought one Sunday from the local electronics hobby shop.

Mission length is something that cannot be ignored, and for good reason: In only a few days in orbit, COTS components can fail the mission-success-criticality factors, making the premise of using those "cheaper" COTS components a misnomer.

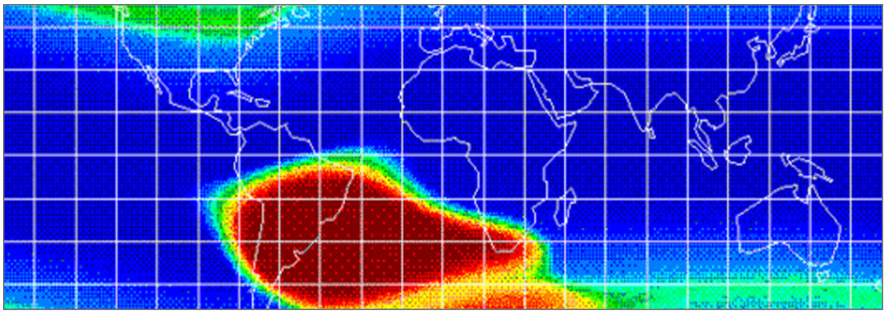


Figure 1 | South Atlantic Anomaly (SAA): Depiction of radiation density of the Van Allen belt over the SAA, with the areas in red being the most intense. Image courtesy of NASA/Goddard Space Flight Center.

Radiation Source	Particle Type	Primary Effects in Devices
Trapped Radiation Belts	Electrons	Ionization damage
	Protons	Ionization damage; Single event effects in sensitive devices
Galactic Cosmic Rays	High energy charged particles	Single event effects
Solar Flares	Electrons	Ionization damage
	Protons	Ionization damage; Single event effects in sensitive devices
	Lower energy heavy charged particles	Single event effects

Table 1 | High-level summary of space radiation environments and their effects on LSI/MSI devices.

Properly employing COTS in space

Radiation-tolerant electronics are typically characterized in the range of 15 to 50 krad (Si), with rad-hard over 100 krad (Si). Most standard COTS components rarely make it past 1k, which can be easily hit within the first month in flight, depending on the orbital altitude and angle of inclination. Testing at heavy ion cyclotrons have shown that most of today's COTS complementary metal-oxide semiconductor (CMOS)-based processors suffer from miserable TID stats: Most, if not all, are well under 300-400 rad (Si) TID, which is accumulated in less than two or three weeks in a typical LEO.

Device physics cannot be ignored – as the number of processor cores increases and the line geometries decrease in the chip, the worse it gets.

For reference, the average launch cost for a Space-X Falcon 9 to LEO is around $5,000 per pound ($2,300 per kg); an Atlas 5 is about $13,000 per kilogram. Moreover, finding an open launch platform can literally take from two to more than five years to secure a slot on a booster, even a Russian one.

Recently, 11 SmallSats were launched, designed to last in orbit between two and three years: How does one measure success and ROI if all of them – based on COTS components – died off in the first couple of months?

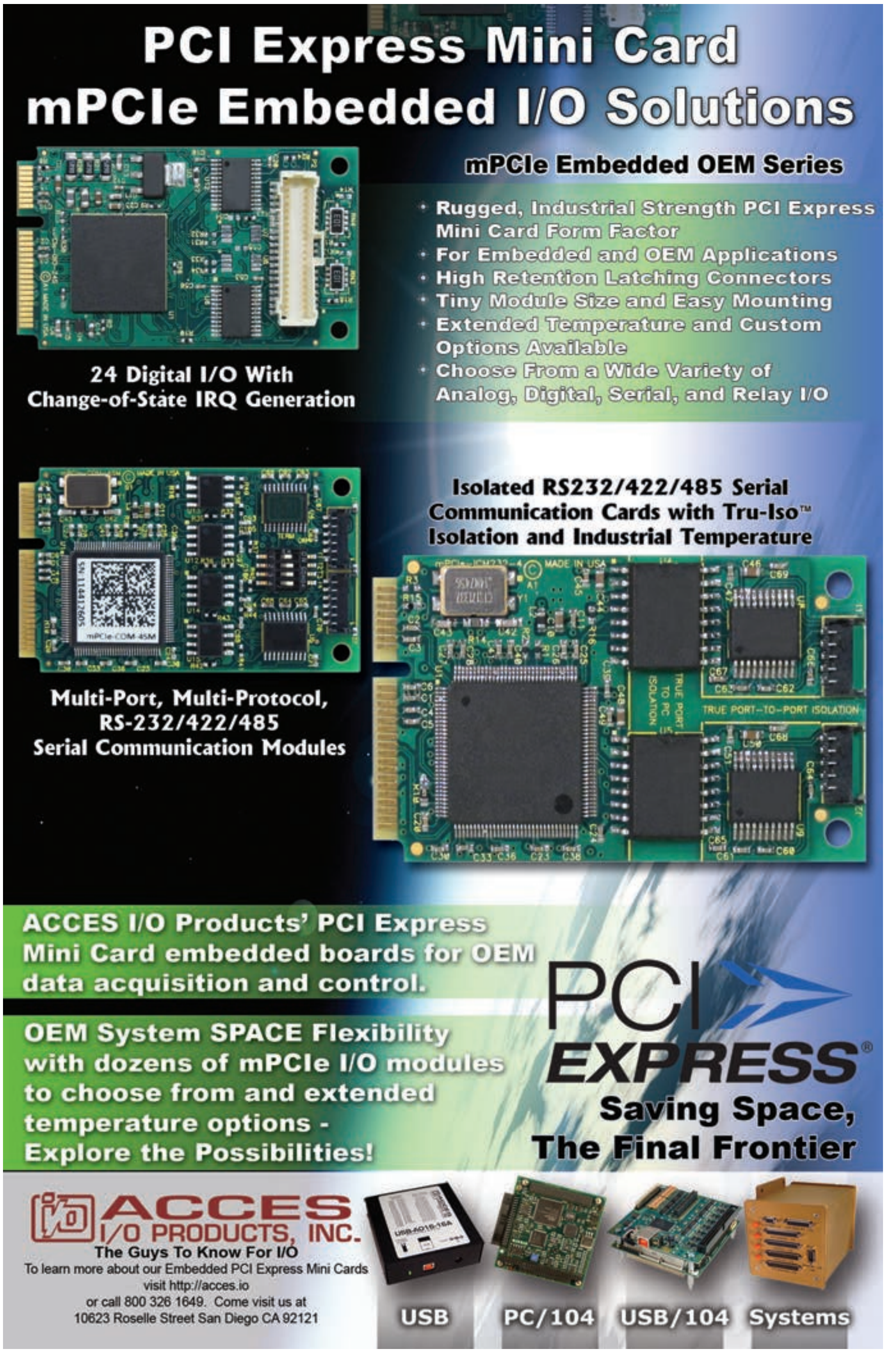
If a program truly has a limited mission length of only one or two months of failure-free operation, then the cheaper approach using COTS components may suffice. The designer can take that chance, as long as failure is an option. In manned spacecraft, such as the International Space Station in LEO, or in lunar and interplanetary (Mars) missions, which are measured in years, not months, early failure due to component fatigue is never an option.

Evaluating and selecting radiation-hardened components

Due to a rapid decline in the availability of MIL-STD-883B Class S – or for that matter, 883B Rev. C components – the appropriate parts selection and accurate qualification needed to accommodate the demanding physics encountered in space applications is more critical than ever. Their qualification for space usage now falls on the systems integrators.

For example, the potential for outgassing in a high vacuum can significantly impact system performance. Components selected must minimize outgassing that can create a corrosive or a deleterious atmosphere in a confined capsule wherever possible, regardless of whether it is a manned or unmanned environment. Specifying conformal coatings that will minimize the potential for outgassing problems caused by the high vacuum levels in space (>10-4 Torr) can also help mitigate these effects.

With regard to screened components, insisting on 100 percent environmental and radiation testing – with manufacturer lot and date-code traceability of all components – is mandatory to ensure the radiation hardness and long-term reliability of component performance in the space environment. Neither the probability batch testing of single devices, nor the characterization testing of just one board, is a satisfactory process for certifying space-qualified designs.



Characterizing components

Every batch of semiconductors exhibits some level of process variation. Such variations can encompass overall transistor gains, etch boundaries, transistor-well depths, and even package epoxies which, in turn, affect speed, performance, radiation tolerance, and outgassing properties.

For these reasons, each component used in each design should be individually radiation tested, certified, and tracked against component lot and date codes, with complete and full documentation and traceability. (Figure 2.) Just because a semiconductor design passed testing in an earlier application does not mean that a subsequent production run of the identical design will yield the same results, especially since these components can come from physically different fabs.

By definition, components to be characterized must be from the exact same lot and date code. If they do not, that completely nullifies the testing.

The importance of safety margins and the extreme consequences of potential component failures far outweigh the expenditures associated with proper testing. Performance and certification of appropriately conducted tests and characterizations can increase radiation tolerance levels to nearly five times that of unscreened devices.

Considerations for any space mission

While the need to accommodate the degrees of radiation may vary based on mission longevity and the specific Earth orbit, the effect of radiation on system components in space need to be evaluated. Rad-tolerance in space components defines the success of a mission, so accounting for the proper levels before launch is critical.

There may be less expensive, less qualified alternatives, but the cost of a failure in system operation while in flight needs to be assessed as well. For a small satellite cluster designed to last only a few years, it may not be as important for all satellites to remain operational across the entire mission. In contrast, for a system exploring the deeper regions of space or destined to stay in orbit for several years, reliability far outweighs saving a few dollars in the development phase.

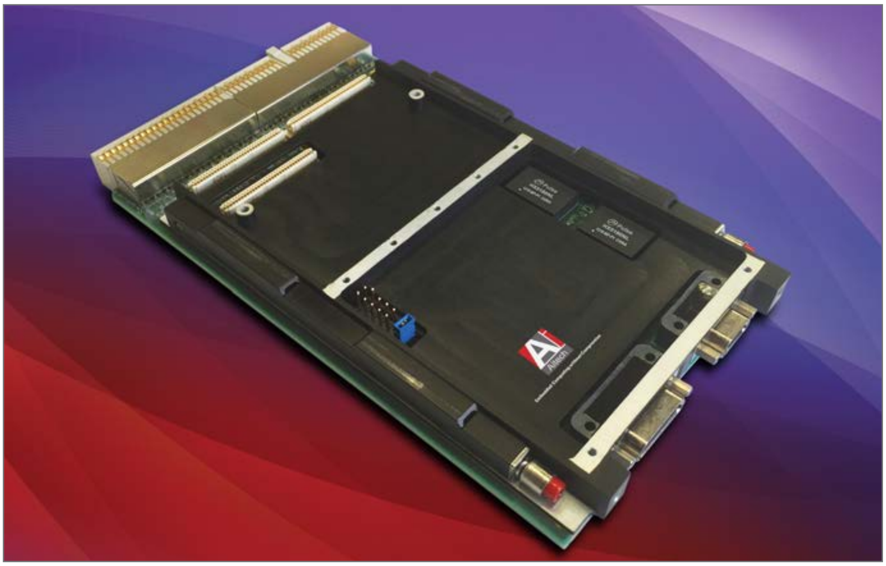
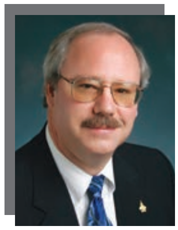


Figure 2 | Boards qualified for space applications should include individually-characterized components.

The bottom line? Designers must make sure to account for all design aspects that will affect the success – or failure – of the mission. **MES**



Doug Patterson *is vice president of the military and aerospace business sector for Aitech Defense Systems, Inc. He has more than 25 years of experience in marketing and business development as well as product management in telecommunications and harsh environment electronics. He served on VITA's board of directors and holds three patents in advanced metered mailing systems and nonvolatile memory redundancy mapping. Doug holds a BSEE from BEI/Sacred Heart University. He can be contacted at doug.patterson@rugged.com.*

Aitech • www.rugged.com

Targeted testing of commercial off-the-shelf (COTS) parts can assure designers of satellites that the parts they seek are radiation-tolerant and conform to federal regulations.

Radiation-tolerance screening for missions of all sizes

By Victor Brisan

Decreasing costs for satellite launches have created new opportunities for nontraditional small satellites in alternative orbits. The application of expensive radiation-hardened (rad-hard) certified components is often not warranted for these applications. Rather, radiation-tolerant technology can provide these smaller projects with both substantial savings and an enhanced safety margin. Reliable methods to determine if commercial off-the-shelf (COTS) components are radiation tolerant can allow designers to screen components for the target radiation criteria that meet the mission requirements.

The global aerospace and defense industry is estimated to grow by three percent in 2016, according to Deloitte's 2016 global aerospace and defense sector outlook. Innovations in component miniaturization and ever-decreasing satellite launch costs represent much of this revenue growth. These factors, in turn, have led to the dramatic increase in the number of small-satellite constellations. Companies such as Planet Labs launch and operate constellations, which are groups of many small satellites; the company's FLOCK 1 solution, to take one example, consists of 28 small Low Earth Orbit (LEO) satellites working together for earth-mapping applications. For communications applications, constellations can be made up of hundreds of small satellites working collectively in order to remain in constant contact with ground stations. Several companies are working to launch even larger constellations in the coming years and are considering how to reduce the affiliated volume costs.

Selecting components certified as rad-hard under the adopted Radiation Hardness Assurance (RHA) procedures of MIL-HDBK-814, MIL-HDBK-816, and MIL-HDBK-817 is the way to go for designers. The rigorous RHA standards certify entire production lines of parts to various specified standards for total ionizing dose (TID), neutron displacement damage, and single-event effects (SEE). While this guaranteed quality affords designers great peace of mind, the added expense of rad-hard components can give designers and financial managers pause. Costs of single dies of certain semiconductors or integrated circuits can easily run into hundreds of dollars. With these high individual component costs, the bill of materials (BOM) cost of even simple subsystems can balloon into the tens of thousands of dollars.

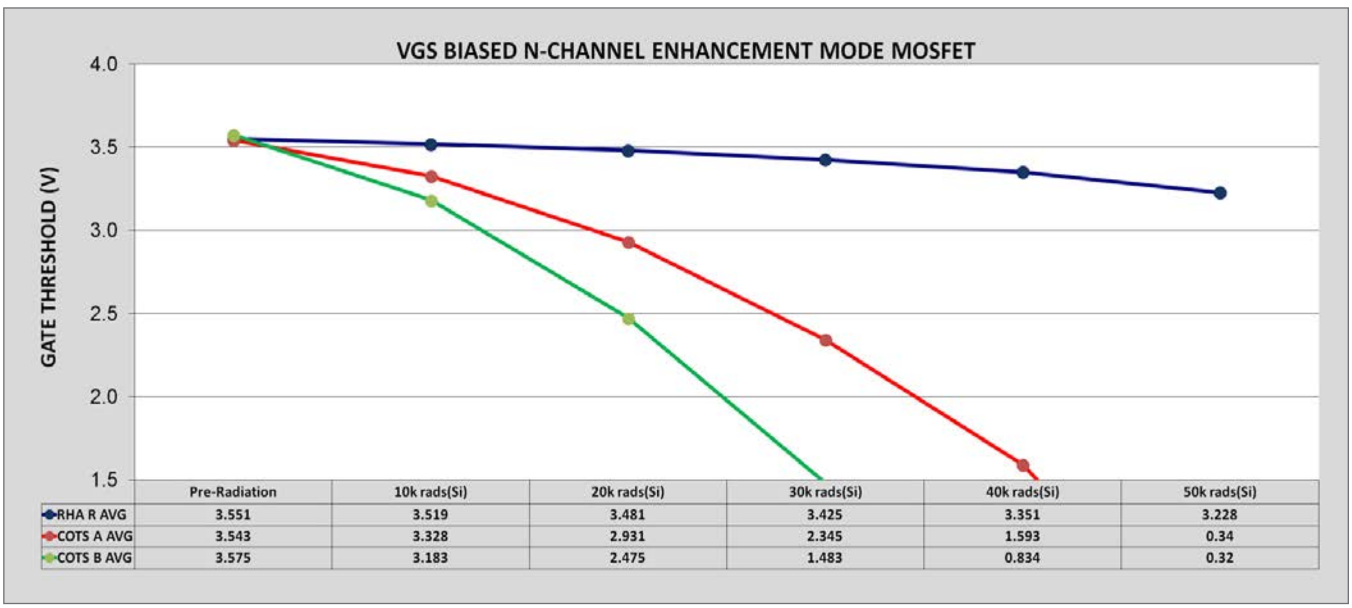
The most inexpensive alternative to using rad-hard parts is simply to use COTS products. With no guarantee of radiation tolerance, however, the potential for unforeseen and critical failures often outweighs the savings.

The compromise between using rad-hard parts and using completely untested COTS parts is to use parts from selectively screened COTS lots. With this approach, specific lots of components are screened for RHA tolerance. Selective screening of lots of readily available and lower-cost COTS components is much easier than certifying entire production lines. Furthermore, screening can have other advantages, such as uncovering tolerances to mission-specific levels while testing to the same rigorous standards set forth in MIL-STD-750 and MIL-STD-883.

Rad-hard overkill

In order for manufacturers to brand their semiconductor or hybrid products with JAN (Joint Army and Navy)- or RHA (radiation-hardness assured)-level designators from MIL-PRF-38534, MIL-PRF-38535, or MIL-PRF-19500 specifications, a strict, time-consuming, and costly certification process must be followed, which naturally leads to a price tag premium for these rad-hard parts. Military handbooks typically recommend parts designated to at least RHA level R [1.0E05 rad(Si)] as preferred for any space application; this "R" level is fairly high on the designator totem pole, further driving up the price.

The good news for smaller projects, such as those requiring launches of low-weight LEO satellites, is that these high standards are unnecessary. While LEO satellites experience substantially more aerodynamic drag than those in high orbit, they also see less radiation. As an example, with a typical LEO radiation dose rates of 1.0E-04 rad(Si) per second, a 10-year-lifespan satellite would only accumulate 3.0E04 rad(Si), substantially less than the 1.0E05 rad(Si) level required of RHA level R. Figure 1



	Pre-Radiation	10k rads(Si)	20k rads(Si)	30k rads(Si)	40k rads(Si)	50k rads(Si)
RHA R AVG	3.551	3.519	3.481	3.425	3.351	3.228
COTS A AVG	3.543	3.328	2.931	2.345	1.593	0.34
COTS B AVG	3.575	3.183	2.475	1.483	0.834	0.32

Figure 1 | MOSFET threshold vs. TID.

depicts the gate threshold of two wafers of COTS and one wafer of RHA MOSFETs reacting to TID. Commercial devices will almost always have a more significant reaction in such tests, but it is still possible to find devices that pass parametric limits at mission-specific doses of radiation.

Although these LEO-accumulated radiation levels are usually substantially lower than those used in rad-hard certifications, using unscreened parts can be quite risky. Untested components can exhibit unknown behavior after accumulating TID or being exposed to displacement damage or SEE. The failure of a key COTS part can easily lead to overall system failure. Without characterizing how these parts respond to radiation exposure, it is not possible to predict when failure or behavioral changes will occur.

The lower the project budget, the more it makes sense to rely on readily available products, due to both cost efficiency and ease of replacement. Modern COTS components, especially from manufacturers counting on business from the aerospace and defense industry, continue to push the boundaries of both quality and performance; these products are often manufactured alongside their RHA equivalents with very similar processes. Except for their unproven reliability against RHA effects, COTS parts have little reason to be viewed as inferior, as long as their guaranteed specifications are kept in mind.

MODERN COTS COMPONENTS, ESPECIALLY FROM MANUFACTURERS COUNTING ON BUSINESS FROM THE AEROSPACE AND DEFENSE INDUSTRY, CONTINUE TO PUSH THE BOUNDARIES OF BOTH QUALITY AND PERFORMANCE; THESE PRODUCTS ARE OFTEN MANUFACTURED ALONGSIDE THEIR RHA EQUIVALENTS WITH VERY SIMILAR PROCESSES.

Screening COTS

Lots or wafers of COTS semiconductors or hybrids can be screened for radiation tolerance to the same strict standards of quality and reliability as those demanded of RHA-certified parts. In fact, Defense Logistics Agency (DLA)-approved radiation-testing facilities conform to all relevant regulations applicable to the devices being tested, commonly using standards MIL-STD-750 or MIL-STD-883.

The higher the confidence of the designers in the required response of the parts to TID, displacement damage, or SEE, the better the chance of finding COTS wafers suitable for use in their projects. Out of the large number of mass-produced devices in a product line, there are always various wafers that happen to respond well to one or more of the types of radiation, even if they shift out of their original specifications. A COTS equivalent to a JAN high-reliability bipolar junction transistor (BJT) would likely fail one or more parameters in a post-radiation MIL-PRF-19500 Group D inspection, but it could still be entirely suitable for use in a project if the parametric shift is predictable, and therefore accounted for in the overall design.

Figure 2 | Low-dose-rate radiation testing of components enables designers to screen parts for suitability for use in space. Photo courtesy of VPT Rad.

The ultimate goal of a COTS radiation-tolerance-screening program is to make a project more cost-effective by avoiding RHA premiums wherever possible. However, this approach does come with some pitfalls that would defeat this purpose. Since finding wafers of devices that have favorable characteristics is random, deciding how many wafers of each device to screen is a significant challenge. If too many are screened, the associated cost no longer seems favorable, but testing only a single wafer pits the significant cost of radiation screening against the odds of the wafer responding in acceptable fashion. Selecting at least a few different wafers should improve the odds while still maintaining cost-effectiveness.

An additional strategy to assuring cost-effectiveness is to set up the tests that best characterize the conditions the device will experience in the final product. (See Figure 2.) This approach includes test points at well-spaced exposure levels that establish exactly when negative effects can endanger intended use, and – if relevant – considering annealing tests to determine if the part can shift back towards normal specifications. **MES**

Victor Brisan *is senior test engineer for VPT Rad in Chelmsford, Massachusetts. He holds a Bachelor of Science degree in Electrical and Computer Engineering from the Worcester Polytechnic Institute. Readers may reach Victor at vbrisan@vptrad.com.*

VPT Rad • www.vptrad.com

TRENDS IN RADIATION-HARDENED ELECTRONICS

Readying radiation-hardened ICs for space flight

By Josh Broline and Nick van Vonno

The radiation environment of space presents several challenges for satellites and deep-space flight systems. Acceptance testing of integrated circuits (ICs) ensures predictable performance and prevents system failure while in flight through the various radiation environments encountered in nearly all mission profiles.

The Orion Crew Module EFT-1 test vehicle stack contains the crew module, the service module, a partial launch-abort system containing only the jettison motor, and the Orion-to-stage adapter. (Photo credit: NASA.)

Understanding space radiation

To understand the effects of radiation on electronic systems and integrated circuits, one must first understand the source of radiation. Radiation in space consists almost entirely of particles, including electrons, protons, and energetic heavy ions. Most of these particles originate from the solar wind or solar flares. Superimposed on this particle flux are very high-energy protons and heavy ions, which are isotropic. The moderate energy particles – such as electrons and protons – are trapped by the Earth's magnetic field in the Van Allen belts; depending on a satellite's orbit, the belts may cause most of the ionizing radiation damage. High-energy protons and heavy ions also are affected by the magnetosphere but are much more difficult to trap.

All of these particles interact with the materials used in electronic devices. This interaction occurs because solar electrons and protons are abundant and cause ionization in materials. In a simplified model, low- and moderate-energy charged particles generate hole-electron pairs in the thermal oxides used in integrated circuits. The electron mobility in these oxides is very high and any applied electric field sweeps the electrons out of the oxide in picoseconds. The hole mobility is much lower, so a much greater proportion of holes get trapped. The result of these asymmetrical trapping dynamics is the positive volume charging of dielectric layers and degradation of both bipolar and metal-oxide semiconductor (MOS) circuit devices.

Figure 1 shows that when the particle energy is increased, the particle abundance decreases, with the abundance-versus-energy curve spanning 25 orders of magnitude and culminating in very low fluxes of relativistic TeV (teraelectronvolt) heavy ions. The effects of the abundant lower-energy particles are uniform through the volume of the IC, but high-energy heavy ions cause single-event effects, defined as the interaction of a single energetic ion with a silicon device. Energy is lost by these high-energy particles as they pass through the semiconductor lattice, generating a track of hole-electron pairs. The resulting charge is collected and can change the voltage on sensitive nodes, which can affect circuit operation.

Single-event effects can be divided into destructive and nondestructive phenomena. Nondestructive effects include bit flips, functional interrupts in digital applications, and transients on the outputs of analog functions. Destructive effects include latchup, burnout, and MOS gate oxide rupture, which can lead to permanent damage. The most commonly used unit in single-event-effects work is the linear energy transfer (LET) of the incoming ion, which equates to the energy loss (dE/dx) per unit track length for a given material density; this unit is expressed in MeV.cm^2/mg. The key takeaway: Shielding is ineffective as it only filters out the low-energy end of the spectrum. The high-energy ion flux

is unaffected, and mitigation must be performed at the IC and system levels.

Impact of commercial space

Since the end of the space shuttle program, the U.S. has seen a definite trend towards increased commercial participation in launches and missions. Today's launch-vehicle market has changed from government-run programs carried out by private contractors to programs run by private industry. Also seen has been the growth of space tourism and commercial spaceports. These trends, in addition to cost-reduction pressures in government-funded programs, have resulted in increased market penetration by low-cost alternatives to high-reliability ICs. Some of the alternatives include military-grade Class Q parts, straight commercial off-the-shelf (COTS) parts, and even automotive parts. The leading edge of this trend is in commercial launch vehicles, which did not use high-grade ICs to begin with, due to short mission time and emphasis on cost control.

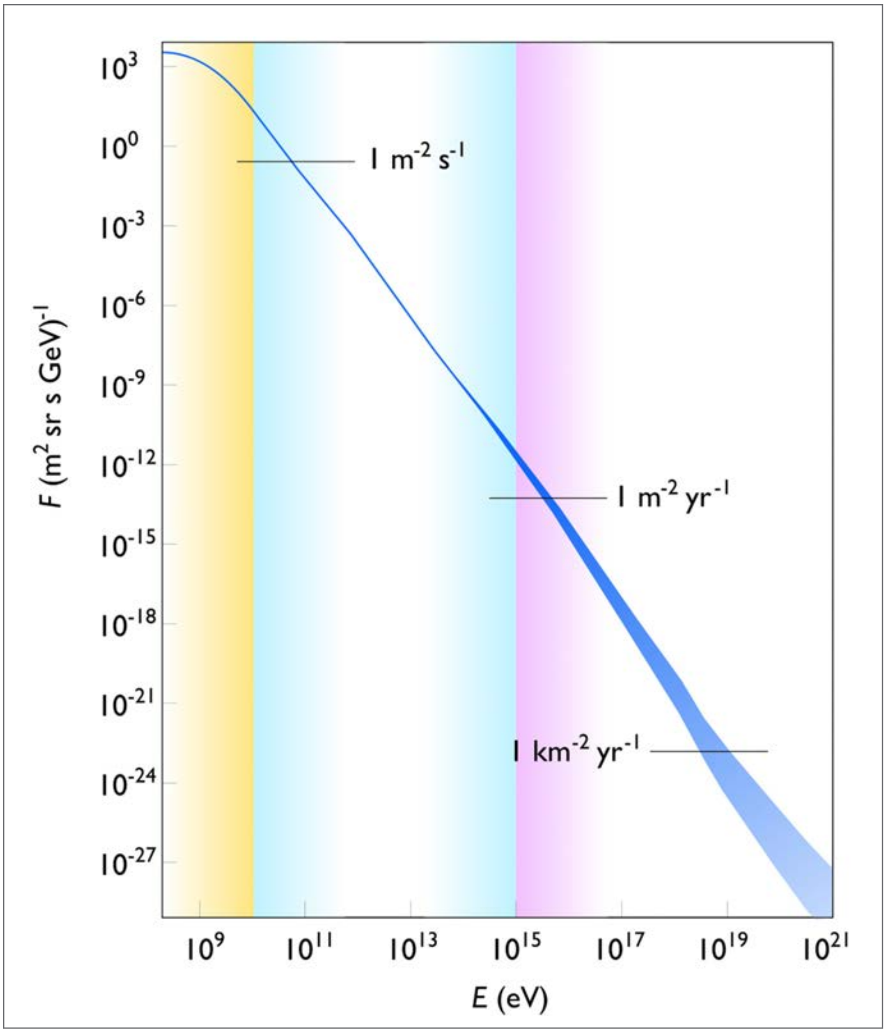


Figure 1 | Galactic cosmic-ray energy spectrum – particle flux plotted as a function of particle energy.

The objectives of private industry are to reduce the cost and increase the reliability of access to space – and to make a profit. This model demands simplicity, reliability, and sharply reduced cost throughout the entire launch vehicle, payload, and launch infrastructure system. Commercial space products are designed for compatibility with multiple and limited capability infrastructure facilities used for production, launch, and mission support.

NASA's focus

NASA's key initiative in this space is the Orion program, which is developing a manned spacecraft to be used as an exploration vehicle for a range of missions including a manned mission to Mars. Orion provides launch, launch abort, transit to the specific objective, and reentry upon its return to Earth. The Orion EFT-1 flight launched from Cape Canaveral on December 5, 2014, for a two-orbit, four-hour demonstration mission. Orion EFT-1 evaluated launch and re-entry systems such as avionics, attitude control, parachutes, and the heat shield required for high-speed re-entry. Orion is a steppingstone to later manned exploration of Mars. Until now, Mars has been explored through an intensive program of rovers, orbiters, and imagers, supplemented by extensive research into the human and health aspects of a long-duration mission in a difficult radiation environment.

NASA has historically categorized parts for space applications by reliability assurance levels. In this system, a Grade-1 part is considered the most reliable and is suitable for mission-critical and manned flight applications. Grade-2 parts are intended for general-purpose applications, while Grade-3 parts are suitable for non-mission, higher-risk applications. These grades correlate with MIL-PRF-38535 QML-V or QML-S compliance, Class B, Q, or H compliance, and MIL-STD-883 compliance, respectively, and the part-procurement cost follows this sequence. The main differences in grades are the types and extent of screening and the product assurance procedures used in production.

Commercial parts are routinely "up-screened" through implementation of some or all of the screens for a given grade, but the resulting costs are typically equal to or even greater than parts screened by the manufacturer. Radiation hardness is a key issue here – one that COTS may have problems with – including radiation effects that range from total dose degradation of performance parameters, which can cause system degradation; to destructive single-event effects, which can be mission-ending.

COTS systems are predominantly one-off systems, typically built with stringent cost limitations and a mixture of COTS and high-reliability (hi-rel) parts: The hi-rel parts go into mission-critical sockets, while the COTS parts are used in the rest of the system.

In this model, COTS parts are procured on the commercial market, usually with several known date codes or other traceability indicator and in quantities sufficient for the entire mission requirements. The parts are then qualified on a sampling basis, with some lots passing and the failing lots discarded. Overall, this may be a cost-effective method, but its risk and unpredictability are not consistent with high-stakes missions such as communications satellites and national-security payloads. Commercial communications missions have stringent time-to-market and insurance constraints and so have historically used the highest-quality parts available. They are expected to continue doing so, as are national-security assets.

Low-dose-rate testing and qualification

The effects of space radiation are caused by particles interacting with the materials used in electronic devices, so truly rigorous radiation tests would replicate these particle environments. Electron and proton testing is inconvenient and expensive, though, so the space community has historically used gamma rays for ground testing. While it is in fact a simulation, behind it is 50 years of correlation and high confidence using high-energy photons to predict part response to charged particles.

PART HARDNESS AT THE LOW DOSE RATES FOUND IN SPACE HAS TURNED INTO AN IMPORTANT HARDNESS-ASSURANCE ISSUE, WITH MANY USERS INSISTING ON LOW-DOSE-RATE TESTING ON A CHARACTERIZATION OR ACCEPTANCE BASIS AND DEEMPHASIZING HIGH-DOSE-RATE TESTING ALTOGETHER.

One inexpensive gamma-ray source – ^{60}Co – is a synthetic isotope of cobalt that has two photon energies at 1.17 million electron volts (MeV) and 1.33 MeV. It is widely used for "total dose" testing of electronic components, in which the actual dose rate during irradiation was found to play a major role. Note that the unit for total ionizing dose is the radiation-absorbed dose (rad), which is equivalent to 100 ergs per gram. The energy absorption is specific to the material being irradiated, so the common unit in silicon technology becomes the rad(Si).

Total dose testing was originally performed at high dose rates in the 50 to 300 rad(Si)/s range, which is a convenient approach as the test takes a few minutes for a 100 krad(Si) exposure. Research performed in 1992 showed enhanced vulnerability of bipolar analog parts at dose rates of as low as 0.01 rad(Si)/s. However, the problem is that the dose rate in space is even lower than that. High-dose-rate testing is now recognized as an excessively accelerated test in many technologies. The downside is that a low-dose-rate test to 50 krad(Si) at the 0.01 rad(Si)/s dose rate required by MIL-STD-883 Test Method 1019 takes 10 weeks, which increases the cost of acceptance testing. Part hardness at the low dose rates found in space has turned into an important hardness-assurance issue, with many users insisting on low-dose-rate testing on a characterization or acceptance basis and deemphasizing high-dose-rate testing altogether.

In response to customer demand, Intersil Corporation in 2012 introduced an industry-leading low-dose-rate hardness-assurance program, which performs wafer-by-wafer acceptance testing at both low and high dose rate using on-site production irradiators. The distinct part number suffix (EH) defines a part type as having been acceptance tested at both dose rates; most Intersil radiation-hardened ICs are now available with this option.

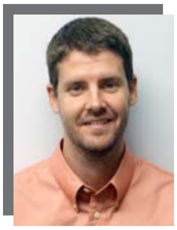
In the development stages of the low-dose-rate acceptance-testing program, Intersil considered using accelerated low-dose-rate testing, in which irradiations are carried out at elevated temperature or in a modified, hydrogen-rich package atmosphere. While these methods produced encouraging results in a research and development environment, they were inconsistent with the limited production of QML-V-compliant parts. A detailed correlation study would be required for each part number, with periodic verification of correlation accuracy, and it was found that simply performing the tests was the most cost-effective approach.

The Intersil EH parts (see Figure 2) are low-dose-rate tested (biased and unbiased) to 50 krad(Si), with a parallel high-dose-rate test (biased only) to the applicable data sheet level. At 0.01 rad(Si)/s, the 50 krad(Si) irradiation test takes 10 weeks to perform.

Future missions

While commercial space will continue using a mix of COTS and high-reliability parts, high-stakes mission profiles will continue to rely on low-dose-rate testing to meet the mission-assurance needs of military and communications satellites as well as manned spacecraft for deep-space exploration. Successful spaceflight system performance requires radiation hardening at the part level as well as thorough characterization and acceptance testing. **MES**

Figure 2 | The ISL71840SEH 16-channel multiplexer is a drop-in replacement for Intersil's HS9-1840ARH, which has been aboard nearly every satellite and space exploration mission, including NASA's Orion spacecraft flight test.



Josh Broline *is a product marketing manager for Intersil's mil/aero products group. He is responsible for developing and driving strategic plans and product roadmaps for radiation-hardened products used in spaceflight applications. Josh holds a BSEE from the University of Central Florida and an MBA from Florida Institute of Technology. Readers may reach him at jbroline@intersil.com.*

Nick van Vonno *is a principal engineer in Intersil's mil/aero products group. He has 42 years of service with Intersil and its predecessors in a number of technical and management posts. He is currently responsible for radiation-effects research, customer support, and product technology development. Nick holds a BSEE from the University of Florida; he is also a senior member of IEEE and won the 2009 IEEE Radiation Effects Award. His email address is nvanvonn@intersil.com.*

Intersil • www.intersil.com

Solid-state drive carries encryption certification

Soligen Corp.'s Crypto Secure 2.5 SATA encrypted solid-state drive (SSD) offers secure data storage for a range of applications that aim to prevent data from getting into the wrong hands. Crypto Secure, which carries the federal information processing standard FIPS 140-2 encryption certification, is available with as much as 512 GB density. The integrated memory processor supports different operating system requirements. The SSD includes self-monitoring, analysis, and reporting technologies together with built-in-test capability. The device was designed and built in the U.S.

The self-encrypting Crypto Secure SSD also includes key management, 256-bit pass phrase protection, and authentication. The SSD supports a dual host interface, either SATA 1.5 Gb/s or 3 Gb/s. It also has SMART command attributes, and supports legacy and native command queuing. The system has SLC/MLC NAND-type flash, intelligent "recycling" for advanced free-space management, whole-drive dynamic wear leveling, and data integrity while under power cycling. The flash interface and memory also supports an external bus switch to reduce bus loading. In the event of failure, the SSD can perform a full-drive erase in less than 10 seconds.

Soligen | www.soligencorp.net | www.mil-embedded.com/p373500

VPX power supplies employs series of control features

SynQor's VPX power supplies are compliant with VITA 62, MIL-STD-704, and MIL-STD-461 for 28 V-in systems. The VPX-3U-DC28P-002 power supply has a maximum total output power of 500 W. It has overcurrent, overvoltage, and overtemperature protection. The system – which employs current sharing on VS1, VS2, and VS3 – is VITA 47 and MIL-STD-810G compliant. The power supplies also carry electrostatic discharge protection and are designed to resist shock, vibration, rapid decompression, corrosion, and fungus. Additional features include -40° C to +85° C extended operating temperature, no electrolytic capacitors, and remote-sensing capability.

A control feature on the power supply includes ENABLE, which is used to turn off all of the output voltages when it is high, including +3.3 V_AUX. When it is pulled low to SIGNAL_RETURN, +3.3 V_AUX, power will be turned on and the status of the other outputs will be dependent on the state of INHIBIT. The INHIBIT control feature is used to turn off all the output voltages except +3.3 V_AUX. The FAIL control feature signal is used to indicate a failure has occurred. The SYSRESET signal is an output generated from the module and is used to indicate that startup has completed.

Synqor | www.synqor.com | www.mil-embedded.com/p373438

Test and simulation for single- and dual-stream data buses

An Ethernet-based MIL-STD-1553 test and simulation product from AIM, the ANET1553-x, can be controlled over an Ethernet LAN for analyzing, simulating, monitoring, and protocol testing of single- or dual-stream MIL-STD-1553 A/B data buses. The onboard application support processor (ASP) is based on a system-on-chip (SoC) hardware solution running under an embedded Linux OS. The ANET1553-x uses the ASP to execute the AIM Network Server for all customer applications and interfaces with the standard application programming interface (API) common to MIL-STD-1553 interfaces. During the initialization, the API needs to be given the IP address for the ANET15530x simply as an additional parameter.

Software support is included with the ANET1553-x modules, as are board-software packages for Windows and Linux operating systems. The ANET1553-x can act as bus controller, multiple remote terminals (31), and chronological/mailbox bus monitor. All modules have the built-in capability to handle eight general-purpose discrete I/O signals and also offer trigger-I/O and synchronization to external IRIG-B via an APU1443-x pin-compatible D-sub connector. A full range of MIL-STD-1553 protocol errors can be injected and detected; in addition, the modules can also electrically reconstruct and replay previously recorded MIL-STD-1553A/B record files physically to the MIL-STD-1553A/B bus with accurate timing.

AIM-USA | www.aim-online.com | www.mil-embedded.com/p373501

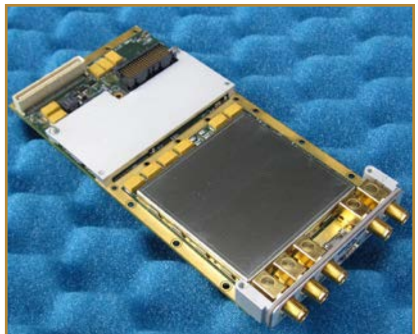
Rugged computer customizable to extreme requirements

A waterproof rugged computer with military-grade connectors, the Germane XtremeBox GSC-1100D has a sealed aluminum housing with MIL-38999 connectors, all of which are designed to operate submerged in one meter of water. Engineers designed the GSC-1100D without a fan so that the box is solid and resistant to sand and dust. It uses a custom cold-plate design that lets the unit operate under full CPU load from -40° C to +75° C. In addition, the chassis is designed to continue running even when subjected to repeated vibration and shock in excess of 30 G.

The system comes with a 2.5 GHz dual-core Intel i7 processor, dual solid-state hard drives, four 1 Gigabit Ethernet ports, integrated PCI/104, and two PCIe Mini card slots to facilitate user flexibility. Additional features include 4 GB ECC SDRAM memory (soldered), single 8 GB DDR3 SODIMM (204 pin), two SSD or HDD SATA 3.0, four 1 G Ethernet ports, MIL-38999 connectors, IP67 rating, four USB 3.0 ports, and one PCI/104 port.

Germane | www.germane.com | www.mil-embedded.com/p373502

Signal acquisition for various applications



The Red Rapids Model 277 signal converter can supply either raw analog/digital converter (ADC) samples or complex samples produced by the embedded digital down converter, which features a tuning resolution of Fs/223 and 10 selectable octave sub-bands in addition to the full-output bandwidth of the ADC. The Model 277, designed around the Texas Instruments ADS42LB69 16-bit ADC, allows either the onboard frequency synthesizer or an external source to supply the 250 MHz sample clock. Typical applications include multichannel signal acquisition, high-speed instrumentation, signal intelligence (SIGINT) collection, software-defined radio, and signal recorder.

The Model 277 is available as a PCI Express mezzanine card (XMC), conduction-cooled mezzanine card (CCXMC), or half-length PCI Express (PCIe) adapter card. The CCXMC can be mounted to any VITA 20-2001-compliant host without modification. All form factors offer four-lane (x4) or eight-lane (x8) bus operation at Gen 2 performance. Software command, software trigger, external hardware trigger, or preset time of day can start signal acquisition, with these same options used to stop collection. The Model 277 monitors both power consumption and temperature during normal operation, with current measurements available on all of the primary voltage supplies. Temperature sensors monitor the DSP die temperature, ADC die temperature, and four additional locations on the card.

Red Rapids | www.redrapids.com | www.mil-embedded.com/p373503

Software-defined radio kit integrates with module SDR-PM 402

SDR-KIT 980B is designed to integrate 9.8 GHz X-band software-defined radio (SDR) transmitter-receiver systems with the processor module SDR-PM 402 for various applications. Ancortek's SDR processor module SDR-PM 402 is compatible with this SDR-RF 980B module. The graphic user interface software SDR-GUI is able to activate this radio frequency (RF) module, select operation parameters, and collect data; the SDR-GUI controls the configuration of the SDR Evaluation Kit via a USB 2.0 cable. Digital samples of control voltage are generated by the field-programmable gate array (FPGA) firmware and are then converted to analog control voltage that directly feeds the voltage-controlled oscillator (VCO). The output of the mixer in the receive chain is digitized and streamed to host computer for real-time processing.

The SDR evaluation kit includes one SDR-RF 980B module, one SDR-PM 402 processor module, one copy of the SDR-GUI graphical user interface software, one AC/DC power adapter (5 V, 3.0 A), one mini USB retractable cable, one pair of RF cables, and one pair of the transmitting and receiving antennas. Additionally featured are FMCW/FSK/CW waveforms, wide bandwidth up to 400 MHz (9.6GHz-10.0GHz), output power >17 dBm, low power consumption, suppression of cooling-fan interference, and onboard automatic correction of voltage-controlled oscillator nonlinearity.

Ancortek | www.ancortek.com | www.mil-embedded.com/p373504

Paving the way for fast, secure quantum communications

By Sally Cole, Senior Editor

Quantum key distribution (QKD) will play a central role in the next generation of secure communications, and new software from university researchers helps quickly evaluate security protocols for QKD.

In a major breakthrough for secure quantum communications, researchers at the University of Waterloo's Institute for Quantum Computing (IQC) in Canada recently discovered an efficient numerical approach for evaluating the performance of QKD protocols. They also developed the first available software to quickly evaluate the security of any protocol for QKD.

"Secrecy is becoming increasingly important in light of the hacking efforts around the world. But it's even more important than often appreciated, due to the fact that quantum computers may be coming online in the near future," says Patrick Coles, an IQC postdoctoral fellow and one of the researchers behind the discovery and software. "Quantum computers could break many aspects of our current Internet security, which is based on the computational difficulty of certain problems. This would be catastrophic … so it's imperative to explore new methods of encryption."

The secrecy in QKD centers on the foundations of quantum physics, particularly Heisenberg's uncertainly principle. It allows two parties, referred to as Alice and Bob, to establish a shared key to exchange photons. Since photons behave according to the laws of quantum mechanics, you can't measure a quantum object without disturbing it. So if an eavesdropper, called Eve, intercepts and measures the photons, it causes a disturbance that Alice and Bob can detect. No disturbance means Alice and Bob can guarantee the security of their shared key.

Loss and noise create some disturbances, but a small disturbance implies that a small amount of information about the key is available to Eve. Characterizing this amount of information allows Alice and Bob to remove it from Eve at the cost of the length of the resulting final key. The main theoretical problem in QKD is how to calculate the allowed length of this final secret key for any given protocol and the experimentally observed distance.

"I thought it was incredible that quantum physicists could play a central role in revolutionizing the way we do secret communication and wanted to contribute," Coles says. "Our approach has three main advantages: it's robust, user-friendly, and relatively fast."

By "robust" he means that it can handle any protocol, which is impressive because previous analytical methods were limited to idealized protocols without experimental imperfections. "Our approach enables exploring new protocol ideas and, in particular, protocols that are practical to implement with existing optical hardware," Coles says. "Also, any imperfections in your devices can be explicitly accounted for in our software. The robustness is crucial for the analysis of real, practical systems."

Until now, only a handful of skilled experts in the world were capable of analyzing the security of QKD protocols. "Our software has the potential to bring QKD analysis to a much wider audience," he notes. "You simply enter a description of a protocol of interest and the computer does the calculation."

Then there's speed: "Calculating the secret key output of a QKD protocol is essentially an optimization problem," Coles says. "The main reason we can make our software is because we proved a mathematical theorem that reformulated the problem into an efficiently computable form. It typically takes a few seconds to run our software and get the answer to your problem."

And, as you can imagine, QKD technology has military applications. "The U.S. Office of Naval Research is interested in QKD for secure communications between naval vessels," Coles points out. But adversaries may also exploit QKD, so it begs the question of whether there is a potential for eavesdropping.

With quantum computing coming online, quantum-safe cryptography will become necessary. "This refers to encryption methods that cannot be efficiently attacked by quantum computers," Coles explains. "But another method is to find mathematical problems that even a quantum computer can't efficiently solve."

QKD isn't vulnerable to retroactive attacks, whereas methods based on computational difficulty are. "A retroactive attack is one in which the eavesdropper records the ciphertext and public key, and then waits years for computational power to improve," Coles says. "Once computers become fast enough, the eavesdropper obtains the private key and plaintext."

So the future of quantum-safe crypto may well "end up being some combination of keys generated by QKD and keys generated via computationally difficult tasks," Coles notes.

Future advances in QKD will include "global networks, either on the ground or via satellite," he says. "We'll need to choose the best protocols for these networks, and our software should be a useful tool to help guide that choice."

CONNECTING WITH MIL EMBEDDED

By Mil-Embedded.com Editorial Staff

CHARITY

Veteran Tickets Foundation

Each issue in this section, the editorial staff of *Military Embedded Systems* will highlight a different charity that benefits military veterans and their families. We are honored to cover the technology that protects those who protect us every day. To back that up, our parent company – OpenSystems Media – will make a donation to every charity we showcase on this page.

This issue we are featuring Veteran Tickets Foundation (known as Vet Tix), a national nonprofit organization that provides free tickets – to sporting events, concerts, arts performances, and family activities – to active military troops, veterans, and family members of troops lost in service.

According to the foundation, attendance at such entertainment events can encourage service members to stay engaged with their communities; tickets to cheer for local teams, to enjoy a night at the symphony, or to see their favorite band can enhance their lives by getting them out into their neighborhoods, increasing family bonds through shared interests, and reducing stress through entertainment. Many veterans state that they feel most comfortable around other service members; Vet Tix events often have groups of veterans attending, allowing Vet Tixers to feel comfortable attending an event. Strong family bonds and community reintegration opportunities are essential tools for veterans, says the foundation, during active-duty, post-deployment, and post-service years.

The foundation announced in May 2016 that since its inception in 2008, it has delivered more than two million tickets to service members and families in all 50 U.S. states and Washington, D.C.

Mike Focareto, a U.S. Navy veteran and the founder and CEO of Vet Tix, says that he founded the organization in 2008 after attending a football game during which he noticed many empty seats. "I began thinking of how many veterans were missing out on this type of 'all-American' experience for which they sacrificed so much and would have been thrilled to be sitting in one of those seats."

For more information, visit www.vettix.org.

E-CAST

FACE Aligned Reference Platform: Built on COTS and DO-178C-certifiable components

Sponsored by RTI

The primary objective of the Future Airborne Capability Environment (FACE) Technical Standard is to define a reference software architecture. This webinar examines a case study of such a reference implementation in order to demonstrate capabilities that can be integrated using FACE-aligned components.

These components include an Operating System Segment (FACE Safety Base Profile-aligned) utilizing both C and C++ runtimes, a Transport Services Segment (TSS) utilizing DDS and ARINC port services, a Platform Specific Services Segment (PSSS) including graphic services, a Portable Components Segment (PCS) implemented within a partition providing the primary flight display, and an IO Services Segment (IOS).

View archived e-cast: ecast.opensystemsmedia.com/631

View upcoming e-casts:
http://opensystemsmedia.com/events/e-cast/schedule

WHITE PAPER

Prototyping for defense tech via additive manufacturing reduces time costs

By Stratasys

Development of any sort of defense application, whether unmanned aircraft or shipboard weapon, depends on speed and efficiency. The components and systems involved must not fail; otherwise, human lives could be lost. It can be expensive, however, to build prototypes, because they are often built of the same materials as the deployed parts.

Thanks to the advent of additive manufacturing, however, this situation is no longer necessarily true. Defense and aerospace engineers can now produce parts through 3-D printing, which can significantly reduce the time and cost of prototyping for defense technologies. Ideal for small volumes, customized production, and protoyping, 3-D printing makes lighter weight, fully assembled components at a fraction of the cost and time compared to just a few years ago.

Read the white paper: http://mil-embedded.com/white-papers/white-reduces-time-costs/

Read more white papers:
http://whitepapers.opensystemsmedia.com

Got Tough Software Radio Design Challenges?

Unleash The New Virtex-7 Onyx Boards!

Pentek's Onyx® Virtex-7 FPGA boards deliver unprecedented levels of performance in wideband communications, SIGINT, radar and beamforming. These high-speed, multichannel modules include:

- A/D sampling rates from 10 MHz to 3.6 GHz
- D/A sampling rates up to 1.25 GHz
- Multi-bandwidth DUCs & DDCs
- Gen3 PCIe with peak speeds to 8 GB/sec
- 4 GB SDRAM for capture & delay
- Intelligent chaining DMA engines
- Multichannel, multiboard synchronization
- ReadyFlow® Board Support Libraries
- GateFlow® FPGA Design Kit & Installed IP
- GateXpress® FPGA - PCIe configuration manager
- OpenVPX, AMC, XMC, PCIe, cPCI, rugged, conduction cooled
- Pre-configured development system for PCIe
- Complete documentation & lifetime support

With more than twice the resources of previous Virtex generations plus advanced power reduction techniques, the Virtex-7 family delivers the industry's most advanced FPGA technology.

Call 201-818-5900 or go to www.pentek.com/go/vitaonyx for your FREE online *Putting FPGAs to Work in Software Radio Handbook* and Onyx product catalog.

NOW AVAILABLE! RF Slot Downconverters

Onyx

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 • e-mail:info@pentek.com • www.pentek.com