Military EMBEDDED SYSTEMS

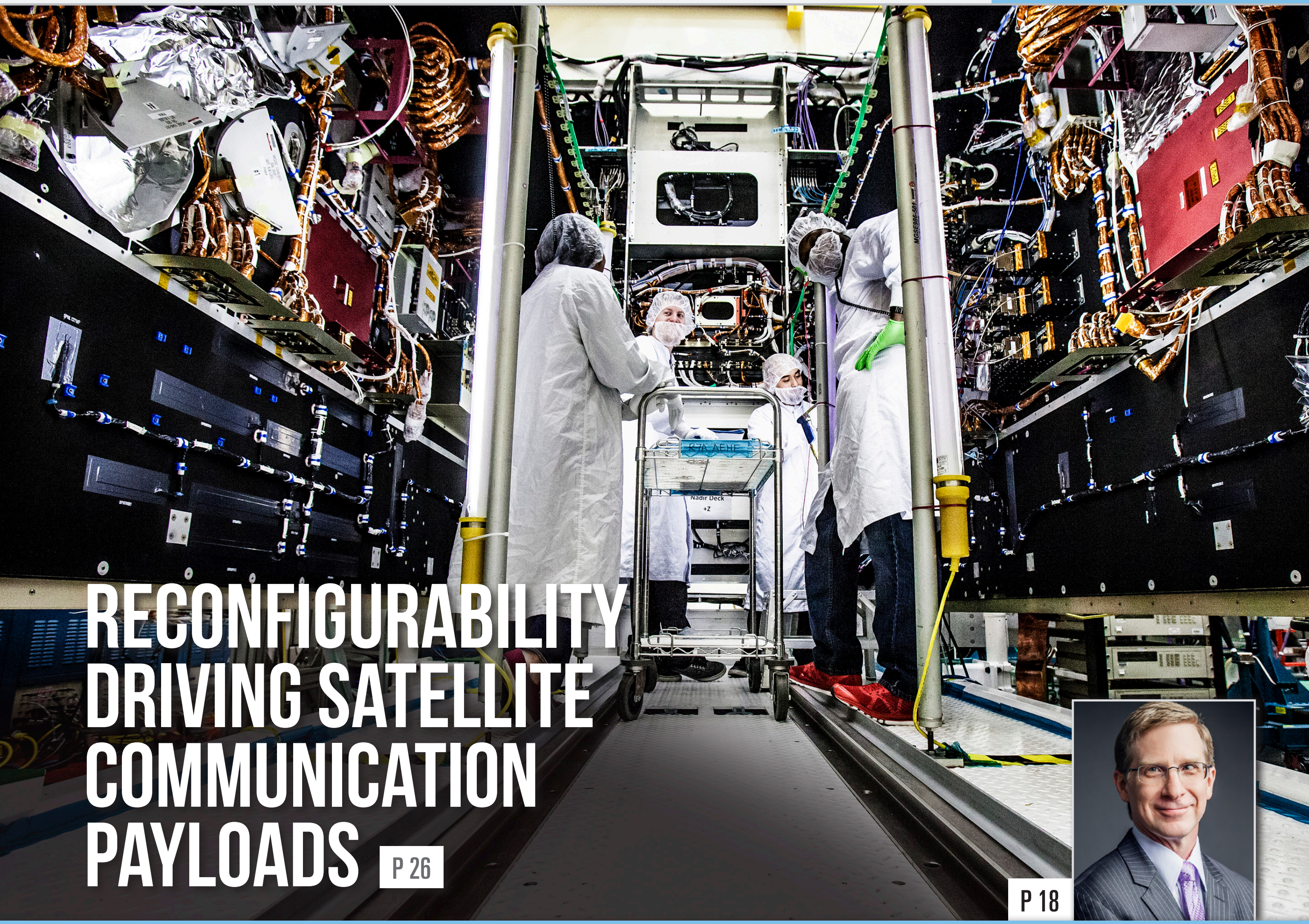
October 2014
Volume 10 | Number 7
MIL-EMBEDDED.COM

John McHale 8
F-35 helmet fittings

Special Report 14
Cognitive radio

Industry Spotlight 44
Mitigating counterfeit part threat

Mil Tech Trends 30
Voltage references for signal integrity



RECONFIGURABILITY DRIVING SATELLITE COMMUNICATION PAYLOADS

P 26

P 18

Wireless Innovation Forum contributions to SCA 4.1
By Lee Pucker, Wireless Innovation Forum

P 22

Solving multiband challenges through software defined radio

Military EMBEDDED SYSTEMS

www.mil-embedded.com

ON THE COVER:

Top photo: Pictured is the integration of the payload module for the fourth Advanced Extremely High Frequency (AEHF) protected communication satellite at Northrop Grumman's facilities in Redondo Beach, Calif., prior to its recent shipment. Northrop Grumman photo by Alex Evers.

Bottom photo: Marines radio a mass casualty report during Exercise Koolendong on Bradshaw Field Training Area in Australia. U.S. Marine Corps photo by Cpl. Scott Reel.

October 2014 | Volume 10 | Number 7

COLUMNS

Editor's Perspective

8 Getting fit for your jet fighter helmet
By John McHale

Field Intelligence

10 SWaP sweeps and edge processors adapt
By Charlotte Adams

Mil Tech Insider

11 VICTORY prevails
By Aaron Frank

DEPARTMENTS

12 **Defense Tech Wire**
By Amanda Harvey

50 **Connecting with Mil Embedded**
By Mil-Embedded.com Editorial Staff

EVENTS

Aerocon
November 19-20
Montreal, Quebec
www.canontradeshows.com/expo/aerocon_all

DMSMS
December 1-4
San Antonio, Texas
www.dmsmsmeeting.com

WEB RESOURCES

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

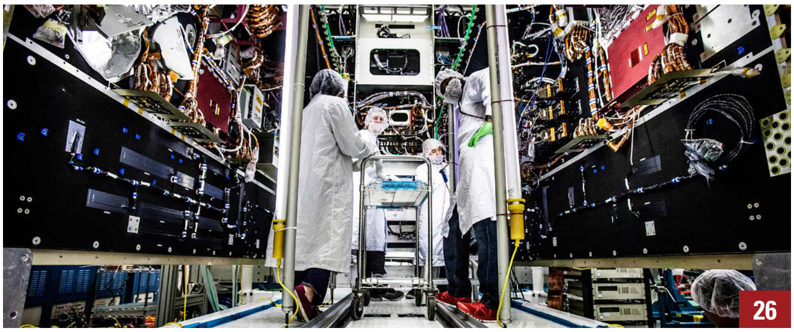
White papers:
Read: http://whitepapers.opensystemsmedia.com
Submit: http://submit.opensystemsmedia.com

SPECIAL REPORT | Military radio design trends

14 Cognitive radio's fate 'uncertain' as the spectrum battle plays out
By Sally Cole, Senior Editor

18 Wireless Innovation Forum contributions to SCA 4.1
By Lee Pucker, Wireless Innovation Forum

22 Multiband military communications challenges overcome by software-defined radio
By Duncan Bosworth, Analog Devices



MIL TECH TRENDS | Satellite communications

26 Reconfigurability and extended data rates drive satellite communication payloads
By John McHale, Editorial Director

30 Shutting out the noise: Voltage references for precision analog signal paths in space applications
By Dan Goodhew, Intersil Corp

INDUSTRY SPOTLIGHT | Managing the supply chain: Obsolescence and counterfeits

36 Designing for forward and backward compatibility is key to managing obsolescence
By Michael Carter, IXI (formerly Sabtech)

40 A volatile supply chain: What is in your future?
By Kaye Porter, GDCA

44 Counterfeit threat taking malicious turn?
By Don Sawyer, Avnet

Published by: OpenSystems media

ISSN: Print 1557-3222

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

ADVERTISER INFORMATION

Page	Advertiser/Ad Title
15	**Acromag** – The complete package
47	**Aeroflex** – Problem: Embedded computing. Solution: Aeroflex
3	**Annapolis Micro Systems, Inc.** – WILDSTAR OpenVPX ecosystem
42	**Aries Electronics** – The end of your military IC obsolescence problems!
9	**Astronics Test Systems** – Freedom 2 choose
34	**Astronics Test Systems** – ATS3000 Series electronic communications test solutions
37	**Avionics Interface Technologies** – Test instrumentation
7	**Ballard Technology** – Portable avionics databus interfaces
48	**beneq** – Mission critical displays – how to keep them running
31	**Creative Electronic Systems** – Flexibility and ruggedness from CES
38	**Elma Electronic** – Integrated rack level server systems
17	**Excalibur Systems, Inc.** – Dragon – it's not a myth
51	**GE Intelligent Platforms, Inc.** – We earn your trust, one platform at a time
43	**Interface Concept** – Intel Core i7, VPX FPGA boards
34	**Kimdu Corporation** – Protocol converters
34	**MPL AG** – Swiss-made firewall and VPN router
34	**North Atlantic Industries** – Configurable communications systems
20	**Omnetics Connector Corp.** – High density connectors
29	**Orbit Power Group and Orbit Electronics Group** – Building the world's most powerful VME-VPX resource
21	**Parvus Corporation** – Qualified to perform
52	**Pentek, Inc.** – Critical recording in any arena – when you can't afford to miss a beat!
42	**Phoenix International** – Rugged deployable RAID data storage
25	**Proto Labs** – Some say they're FAST ... but do they have the SCALE to deliver?
39	**Sealevel Systems, Inc.** – Smart IP cores for MIL-STD-1553
49	**SynQor** – VPX military DC-DC power supplies
32	**VadaTech Inc.** – "The Game-Changer"
35	***Wind River Aerospace & Defense Division*** – Secure smartphones enable warfighters to operate more safely
5	**WinSystems, Inc.** – Freedom from support delays and long lead-times
2	**X-ES** – Module and system-level solutions from X-ES

Military EMBEDDED SYSTEMS

OpenSystems media

MES Editorial/Production Staff

John McHale, Group Editorial Director
jmchale@opensystemsmedia.com

Lisa Daigle, Assistant Managing Editor
ldaigle@opensystemsmedia.com

Amanda Harvey, Assistant Editor
aharvey@opensystemsmedia.com

Sally Cole, Senior Editor
scole@opensystemsmedia.com

Steph Sweet, Creative Director
ssweet@opensystemsmedia.com

Konrad Witte, Senior Web Developer
kwitte@opensystemsmedia.com

Sales Group

Tom Varcie, Sales Manager
tvarcie@opensystemsmedia.com, (586) 415-6500

Shannon E. Alo-Mendosa
Strategic Account Manager
shannona@opensystemsmedia.com, (978) 501-9116

Rebecca Barker, Strategic Account Manager
rbarker@opensystemsmedia.com, (281) 724-8021

Eric Henry, Strategic Account Manager
ehenry@opensystemsmedia.com, (541) 760-5361

Kathleen Wackowski
Strategic Account Manager
kwackowski@opensystemsmedia.com
(978) 888-7367

Asia-Pacific Sales
Elvi Lee, Account Manager
elvi@aceforum.com.tw

Regional Sales Managers
Barbara Quinlan, Southwest
bquinlan@opensystemsmedia.com
(480) 236-8818

Denis Seger, Southern California
dseger@opensystemsmedia.com
(760) 518-5222

Sydele Starr, Northern California
sstarr@opensystemsmedia.com
(775) 299-4148

Europe Sales
James Rhoades-Brown
james.rhoadesbrown@husonmedia.com

Reprints and PDFs

republish@opensystemsmedia.com

OpenSystems Media Editorial/Creative Staff

John McHale, Group Editorial Director
Military Embedded Systems
PC/104 and Small Form Factors
PICMG Systems & Technology
VITA Technologies

Lisa Daigle, Assistant Managing Editor
Military Embedded Systems
PC/104 and Small Form Factors

Amanda Harvey, Assistant Editor
Military Embedded Systems
VITA Technologies

Sally Cole, Senior Editor
Military Embedded Systems

Jerry Gipper, Editorial Director
VITA Technologies
jgipper@opensystemsmedia.com

Curt Schwaderer, Editorial Director
Embedded Computing Design
cschwaderer@opensystemsmedia.com

Christine Long, DIY Brand Manager
clong@opensystemsmedia.com

Joy Gilmore, Assistant Webcast Manager
jgilmore@opensystemsmedia.com

Joe Pavlat, Editorial Director
PICMG Systems & Technology
jpavlat@opensystemsmedia.com

Rich Nass, Embedded Computing Brand Director
Embedded Computing Design
rnass@opensystemsmedia.com

Monique DeVoe, Managing Editor
Embedded Computing Design, DSP-FPGA.com
mdevoe@opensystemsmedia.com

Brandon Lewis, Assistant Managing Editor
PICMG Systems & Technology
Embedded Computing Design
Industrial Embedded Systems
blewis@opensystemsmedia.com

Rory Dear, Technical Contributor
Embedded Computing Design
rdear@opensystemsmedia.com

Konrad Witte, Senior Web Developer

Steph Sweet, Creative Director

David Diomede, Creative Services Director

Joann Toth, Senior Designer

Jake Rojas, Graphic Designer

Corporate

www.opensystemsmedia.com

Patrick Hopper, Publisher
phopper@opensystemsmedia.com

Rosemary Kristoff, President
rkristoff@opensystemsmedia.com

John McHale, Executive Vice President
jmchale@opensystemsmedia.com

Rich Nass, Executive Vice President
jmchale@opensystemsmedia.com

Christine Long, Vice President Online Business
clong@opensystemsmedia.com

Wayne Kristoff, CTO

Emily Verhoeks, Financial Assistant

Headquarters – ARIZONA:
16626 E. Avenue of the Fountains, Ste. 201
Fountain Hills, AZ 85268
Tel: (480) 967-5581

MICHIGAN:
30233 Jefferson
St. Clair Shores, MI 48082
Tel: (586) 415-6500

Subscriptions

www.opensystemsmedia.com/subscriptions

subscriptions@opensystemsmedia.com

Getting fit for your jet fighter helmet

By John McHale, Editorial Director

"You're gonna like the way you look, I guarantee it," was what the guy in the old Men's Wearhouse commercials promised customers who got fit for a suit in his stores. Anyone who has been fitted for a suit, a tux, or even a set of golf clubs knows the difference the fitting can make. It's no different for warfighters. As technology gets more sophisticated it's essential that pilots, Marines, soldiers, and sailors be properly fitted for their gear.

This summer I was fitted for a new set of golf clubs and was fascinated by the fitting technology that analyzed swing speed, side spin, ball speed, you name it, but the process pales in comparison to how F-35 fighter pilots are fitted for their Helmet-Mounted Display System (HMDS). A F-35 helmet fitting is so granular it measures the distance between your eyes and how your pupils react to light. Makes figuring out the lie angle on a 9-iron seem quite mundane.

I was given a tutorial on the process during the Air Force Association (AFA) event last month in Washington from Martin Gunther, product marketing manager for Airborne Marketing at Rockwell Collins. Gunther, a former Navy fighter pilot, has been designing fighter helmets more than 30 years.

The HMDS, designed and developed by Rockwell Collins ESA Vision Systems, places a virtual Head Up Display (HUD) and other critical flight data directly onto the helmet's visor, he says. It has a bi-ocular, 40 by 30 field of view, and a high-resolution, high-brightness display, with integrated digital night vision. It is also integrated with multiple sensors on the aircraft such as the Distributed Aperture System (DAS), designed by Northrop Grumman, that enables pilots to essentially see through the structure of the aircraft for a 360-degree view and see a direct picture of the ground beneath them, Gunther notes.

The only people authorized to assemble and custom-fit a helmet to an F-35 pilot are Rockwell Collins employees (pictured) – Dan Kalsow, a senior systems engineer, and Rodney Breuer, a senior customer support manager – according to Rob McKillip, senior director of F-35 programs for Rockwell Collins. They have fitted more than 120 pilots from the U.S. Air Force and Navy, as well as three foreign national pilots from the Netherlands since 2011. To fit F-35 pilots for the helmet, [Kalsow and Breuer] start by laser scanning the pilot's head so the helmet's optics package on the display visor is within two millimeters of exact center of each of the pupils, Gunther says.

This part of the process takes about four hours per helmet and involves spending two days with each pilot, he continues. On the first day, measurements are taken of the pilot's head, including a 3D head scan and the use of a pupilometer to measure the distance between the pupils, Gunther adds.

Rockwell Collins employees Dan Kalsow (back) and Rodney Breuer (front) test to ensure a pilot's pupils are within two millimeters of exact center to be properly aligned with the optics package on the F-35 HMDS. (Photo courtesy of Rockwell Collins.)

Once the measurements are made they begin assembling the helmet. This process includes custom-milling each helmet liner so the helmet sits comfortably on the pilot's head while maintaining stability under high gravity (G) maneuvers so the optics continue to match up to the individual's field of view, explains McKillip. "They custom fit the pads in the helmet based on head size," Gunther says.

Once the helmet is assembled, the pilot comes in for a final fitting on the second day. During this time the optics are aligned to the pilot's pupils and the display visor is custom contoured – a process that must be done precisely so the pilot has a single focused image at infinity, says McKillip. Many would assume that people's eyes are aligned, but that is not the case, Gunther says.

Rockwell Collins engineers have developed the third generation of the HMDS (Gen III), which is scheduled for flight-testing at Edwards Air Force Base in California this fall, Gunther says. For the Gen III version the team made improvements to night vision acuity, the latency of the DAS imagery displayed on the visor, and solved a jitter challenge. The jitter – a symptom of the aircraft shake generated during a high G turn – has been totally eliminated in Gen III, Gunther says. "The big difference between the Gen II and the Gen III helmets is the improved optical design performance across the exit pupil," Gunther notes. "Gen III also has blacker blacks and no green glow that was associated with previous models."

Gunther says if he had this type of helmet back in the 1970s it would have made landing on aircraft carriers at night a lot less complicated.

It would have also made the fitting process more fun for the pilots. Whether you fly jets, need a new suit, or want to lower your handicap with new irons, don't buy off the rack. Get fitted.

SWaP sweeps and edge processors adapt

By Charlotte Adams

A GE Intelligent Platforms perspective on embedded military electronics trends

Size, weight, and power (SWaP) considerations have always been important for embedded electronics, but as platforms shrink, SWaP constraints are becoming ever more critical. Larger platforms will, of course, continue to use "big" processors that are optimized for performance. However, the proliferation of intelligence at the tactical edge is driving military demand for rugged off-the-shelf chips, modules, and boards that provide just enough performance for their applications. These parts must burn minimal power and produce minimum heat but at the same time offer maximum design flexibility, upgradability, and support.

Autonomous air, ground, and sea platforms are being miniaturized to previously unheard-of levels. Moreover, the expanding, TCP/IP-powered, connected battlefield – analogous to the Industrial Internet in civilian life – means that more and more small machines at the edge are getting smart. The number of intelligent sensors, handheld devices, and wearable technologies, for example, will gradually increase, as they prove themselves force multipliers. As these machines run on batteries, they are extremely power-constrained. The higher the power consumption, the shorter the mission life.

These developments are increasing the demand for processing adaptations. Instead of aiming for the very highest data throughput, regardless of power and thermal costs, designers of these smaller systems are willing to trade MIPs (millions of instructions per second) for watts – in other words, pure performance for power efficiency. Power requirements, heat dissipation, and size will trump sheer speed in these applications. Performance per watt will mean more than MIPS per dollar.

Follow the phones

System and subsystem designers at this leading edge of the military's evolution now are treading paths already blazed by cellphones and tablets. Today's Apple and Android offerings combine voice, data, and video communications, games, calendar, alarm clock, and a myriad of other functions, yet require minimal silicon and dissipate negligible heat.

How do they pull this off? Like cellphone designers, military system developers are adopting low-power, low-heat architectures such as ARM. Not to be outdone, traditional chip developers also are adding functionally integrated, lower-power system-on-chip (SoC) architectures to their product lines.

This shift means moving from traditional central processing units (CPUs) to ultra-low-power chips. Low-power SoCs consolidate as many functions as possible into a single, highly integrated chipset, lowering the system's overall size and thermal penalty. Their host platforms simply lack the space, size, and power budgets to dedicate a whole die to the CPU and so distribute memory controller, graphics processor, and other support to ancillary silicon.

This well-understood approach enables a high degree of flexibility and customization, as multiple manufacturers create implementations of standard architectures, using off-the-shelf chipset components. Due to commoditization at the subchip level, each processor can be tailored to the particular power and performance demands of the application.[1]

XMC

Military designers also are using XMC, an evolution of the PCI Express-based PMC (PCI mezzanine card) module, which provides a high degree of flexibility in a small form factor. Used with a low-power chip architecture and a minimum of other onboard resources, an XMC module can burn less than 10 W. These modules are themselves pluggable, allowing a range of CPU core and memory options to suit the customer's roadmap.

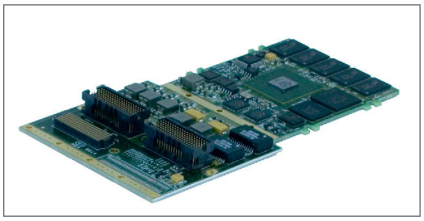


Figure 1 | The GE rugged XMCM01 XMC features a Marvell ARMADA XP processor with up to four ARMv7-compliant 1.6 GHz CPU cores for SWaP-constrained applications such as small form factor C4I (Command, Control, Communications, Computers and Intelligence).

An example of these new low-power modules is the GE Intelligent Platforms rugged XMCM01 XMC module, featuring the ARM-based ARMADA XP processor (see Figure 1).

Ironically, military imperatives, which initially drove the invention of transistors and integrated circuits, have circled around, in part, to enable processing that better suits the tradeoffs at the edge of the battlefield.

Similar developments in the commercial world have driven even more explosive growth of processing power at the edges of the Internet. Pundits predict that this burgeoning of intelligence at the peripheries will localize much processing, as bandwidth to the "cloud" of powerful servers at the center comes under pressure. How this movement will work itself out in the military and civil spheres remains to be seen, but the trend presents the command structure, at a minimum, with opportunities to speed some critical battlefield transactions by increasing processing efficiencies.

References:

1 Robert Swope Fleming in "The End of the Intel Age," his 2011 master's thesis at MIT, p.11, explains this dynamic and the evolution of processing architectures.

defense.ge-ip.com

VICTORY prevails

By Aaron Frank
An industry perspective from Curtiss-Wright Defense Solutions

The U.S. Army's VICTORY initiative has come into its own. Today's combat vehicles are typically deployed with multiple independent systems that have limited ability to share their functionalities or data. To address and mitigate this problem, the VICTORY (Vehicular Integration for C4ISR/EW Interoperability) initiative was kicked off in 2010 to encourage the use of size, weight, power, and cost (SWaP-C)-optimized commercial off-the-shelf (COTS) open-architecture subsystems and Ethernet-based in-vehicle data-sharing services. The promise of VICTORY is that its wide adoption will help to increase interoperability, enable the elimination of redundant functionality and hardware, and ultimately reduce vehicle acquisition and upgrade costs. From our perspective, the VICTORY standard has passed the "tipping point," and has now become a de facto requirement, becoming a common line item in many requests for proposal issued today by the Department of Defense (DoD) and system integrators. Government Program Executive Offices (PEOs) are now commonly stipulating VICTORY as a requirement for upgrades.

From Curtiss-Wright's perspective, VICTORY is prevailing as the DoD's mandated approach for eliminating "stovepiped" system functionality and increasing interoperability. Today, work on the standard continues apace, and VICTORY 1.6.1, the latest version of the specification, was recently released. The standard has undergone a number of iterations and seen numerous implementations since it was first announced. VICTORY has also undergone significant maturation and seen numerous implementations since the first deployable version of the specification (1.0) was released in July 2011. As a result, the market is now seeing VICTORY-compliant equipment at work. To further the standard's acceptance and to verify interoperability, several VICTORY System-Integration Labs (SILs) have been established across the U.S. and are currently testing VICTORY components to analyze how well they work together.

From the COTS vendor side, suppliers are now better able to respond to the growing requirements for VICTORY with compliant products. Helping to speed the development of compliant COTS solutions is the recent "fine-tuning" of the required minimum function set that defines a workable VICTORY architecture. The initial version of the specification defined 54 VICTORY component types that provide a variety of functional elements, such as direction of travel, time services, and shared storage. By increasing its focus on core in-vehicle networking requirements, the government was able to identify a subset of 17 core components needed to implement a useful VICTORY architecture. This decision has enabled COTS vendors to focus on these essential required services. Additional component sets beyond the core 17 can be added based on the usage profile of a particular vehicle.

In today's budget climate, with fewer new platform designs getting started, these VICTORY solutions are well-positioned for use in enhancement upgrade packages to help reduce the number of boxes that are needed to add capabilities into a particular ground vehicle. VICTORY also helps combat obsolescence, since its core architecture fosters interoperability and provides an upgrade path that speeds and eases the addition of new capabilities to vehicles in the future.

In September 2012, Curtiss-Wright introduced the Digital Beachhead 16-port Gigabit Ethernet (GbE) Network Switch combined with a tightly integrated Vehicle Management Computer (see Figure 1). This product is a low-cost rugged ground vehicle "appliance" for modernizing ground vehicles to comply with the VICTORY standard. Since its debut it has generated significant interest in the ground vehicle community, multiple U.S. Army SILs, and other government contractors for evaluation. Recognizing the rapidly proliferating demand for certified VICTORY-compliant solutions in program requirements, the company has expanded VICTORY validation testing for select existing and new products across its family of rugged line-replaceable modules (LRMs) and line-replaceable units (LRUs), including network switches and routers, and computing resources. Curtiss-Wright has also developed a range of derivative products in different form factors, including VICTORY-compliant 3U OpenVPX-based Ethernet switch module and other compact, low-weight rugged LRU-based network switches.

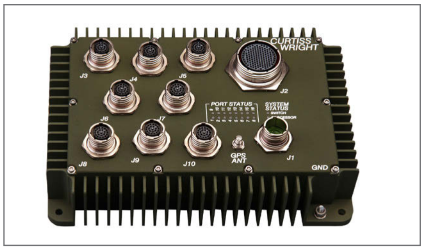


Figure 1 | The Digital Beachhead from Curtiss-Wright combines an Ethernet switch with a vehicle-management computer to provide VICTORY network services in ground vehicles.

The news is that VICTORY is now at hand. Its ascendance enables government program managers and system integrators to better achieve their goals of cost-effectiveness, especially in this time of sequestration and cost-cutting. Instead of viewing each separate vehicle LRU as a discrete function, VICTORY encourages designers to look at the overarching system architecture. That's when the benefits of VICTORY become readily apparent – it enables LRU consolidation and information sharing like never before.

Aaron Frank
Product Marketing Manager,
COTS Switching/Routing, Intel SBC
Curtiss-Wright Defense Solutions
www.cwcdefense.com

DEFENSE TECH WIRE

NEWS | TRENDS | DOD SPENDS | CONTRACTS | TECHNOLOGY UPDATES

By Amanda Harvey, Assistant Editor

NEWS

Air Force Talon HATE program design review completed by Boeing

Boeing engineers completed the final design review for the Air Force's Talon HATE program, which is aimed at improving communication and information sharing among various platforms. The system combines data from fighter networks, national sources, and joint command and control assets. Transmitting over data links, the information may then be used by joint aircraft, ships, and ground stations, to enhance communication and information sharing across the battlespace. Boeing personnel worked with defense industry suppliers to quickly prototype the Talon HATE system for the U.S. Air Force Tactical Exploitation of National Capabilities office within Air Combat Command. The Talon HATE system is designed to be carried in a pod attached to the F-15C fighter aircraft. Boeing is scheduled to deliver multiple Talon HATE systems to operational squadrons in 2015.

Figure 1 | The Talon HATE system is designed to be carried in a pod attached to Boeing's F-15C fighter aircraft, as shown in this artist concept. Photo courtesy of Boeing.

Modernized ARC-210 Gen5 radio delivered to Navy Air Combat Electronics program

Rockwell Collins delivered their first Modernized Type I Cryptographic Airborne radio to the U.S. Navy. The AN/ARC-210, certified by the National Security Agency with Tactical Secure Voice (TSV) 2, replaces existing ARC-210 radios. The ARC-210 Gen5 radio has a software-defined Multi-Waveform Architecture, which is an optimized Software Communications Architecture that has embedded programmable next-generation crypto and extended frequencies to 941 MHz. The modernized radio also provides Joint Precision Approach and Landing System (JPALS) UHF data link, SATCOM Integrated Waveform (IW), and Combat Net Radio capabilities.

High-voltage HEMP filters from API protects sensitive electronic equipment

API Technologies Corp. is now offering high-voltage High-Altitude Electromagnetic Pulse (HEMP) filters that are designed to protect sensitive electronic equipment for military and telecommunications applications. The HEMP filters and surge suppressors ensure the continued performance of critical communication, defense systems, and infrastructure from potentially destructive energy transients such as electronic pulses, electrostatic discharge, nuclear electromagnetic pulse, lightning strikes, and line surges. The HEMP filters exhibit a high off-state impedance, so it appears transparent to the circuits it protects. If a voltage exceeding the switching voltage is applied, the HEMP filter/suppressor circuit switches to very low impedance, shunting the potential damaging energy to ground. It then remains in a state of low impedance until the current flow is either interrupted or the transient voltage drops to a safe level. Once this happens, the filter resets, returning back to a high off-state impedance.

New safety certifiable COTS module solutions released by Curtiss-Wright

Curtiss-Wright Defense Solutions has introduced a new rugged commercial off-the-shelf (COTS) graphics display and video capture engine, the VPX3-718. Designed for use in civil and military aviation applications, the VPX3-718 supports DO-254 DAL C and DO-178C DAL C safety certifiability. The VPX3-718 graphics display and the VPX3-150 single board computer (SBC) are the first members of Curtiss-Wright's new family of safety certifiable COTS module solutions.

The VPX3-718 is powered by an AMD Radeon E4690 GPU and is the first Curtiss-Wright graphics module to support full stream video capture and 1.485 Gbps HD-SDI output to support the transfer of uncompressed HD video. The VPX3-718 eases the integration of dual independent channels of 2D/3D graphics display into deployed airborne systems that require optimal performance in harsh environments.

Figure 2 | The VPX3-718 is a rugged commercial off-the-shelf (COTS) graphics display and video capture engine. Photo courtesy of Curtiss-Wright.

Northrop Grumman, U.S. Navy develop aerial refueling system for E-2D Advanced Hawkeye

Northrop Grumman and the U.S. Navy have been working on developing an aerial refueling system for E-2D Advanced Hawkeyes, and have successfully conducted the preliminary design review. In 2013, Northrop Grumman was awarded a $226.7 million engineering, manufacturing, and development contract to design system upgrades for the E-2D to accommodate an aerial refueling capability. Included are formation lights for enhanced visualization and air space orientation; new seats to reduce crew fatigue and provide pilots an enhanced field-of-view; and upgraded software in the aircraft's flight control system to assist pilots with aircraft handling qualities while refueling. Plans are to install the system on new E-2Ds as well as retrofitting it onto E-2Ds that are currently operating in the U.S. Navy fleet. The extended range of the E-2D Advanced Hawkeye provided by aerial refueling will provide further maritime security as the U.S. continues its shift of focus to the Asia-Pacific region.

Figure 3 | The E-2D Advanced Hawkeye provides 360-degree surveillance to the warfighter. Photo courtesy of Northrop Grumman.

Rugged chassis from GMS replaces multiple workstations via virtual machine technology

General Micro Systems, Inc. (GMS) engineers have developed a rugged, conduction-cooled, secure virtual machine (SVM) server that has six hardware independent I/O modules. The Tarantula, developed to replace multiple workstations with one box via the use of virtual machine technology, leverages an enterprise-level Layer 2 or Layer 3 intelligent switch for high-speed connectivity. The solution consists of a host CPU module and 18-port intelligent Gigabit Ethernet switch module – each housed in one low-profile, lightweight package that is smaller than a shoe box. Tarantula is targeted at applications that require ultra-efficient information sharing between several computers serving varied purposes. It features the Intel Ivy-Bridge-EP Xeon processor as the host CPU driver and has 10 physical cores each operating as fast as 2.4 GHz, with the ability to TurboBoost to 3.0 GHz.

FAA grants Logos Technologies authorization to flight test UAS in New York

The Federal Aviation Administration (FAA) has authorized Logos Technologies to begin flight-testing the Tactically Expandable Maritime Platform (TEMP) unmanned aerial system (UAS). The testing will be conducted in Rome, N.Y., at the Northeast UAS Airspace Integration Research Alliance (NUAIR) FAA UAS test site at the Oneida County Griffiss International Airport. The TEMP UAS is a lightweight autonomous- and powered-flight-capable parafoil aircraft. Developed in partnership with Atair Aerospace, it is designed for a variety of missions, such as precision cargo delivery to inaccessible and remote areas to assist with emergency response situations.

The FAA certificate of authorization (COA) is the first step for TEMP to become the first UAS to be tested out of Griffiss International Airport (formerly Griffiss Air Force Base), with oversight provided by NUAIR. Testing is scheduled to begin in October 2014.

General Dynamics UK to provide 589 SCOUT SV platforms to the UK army

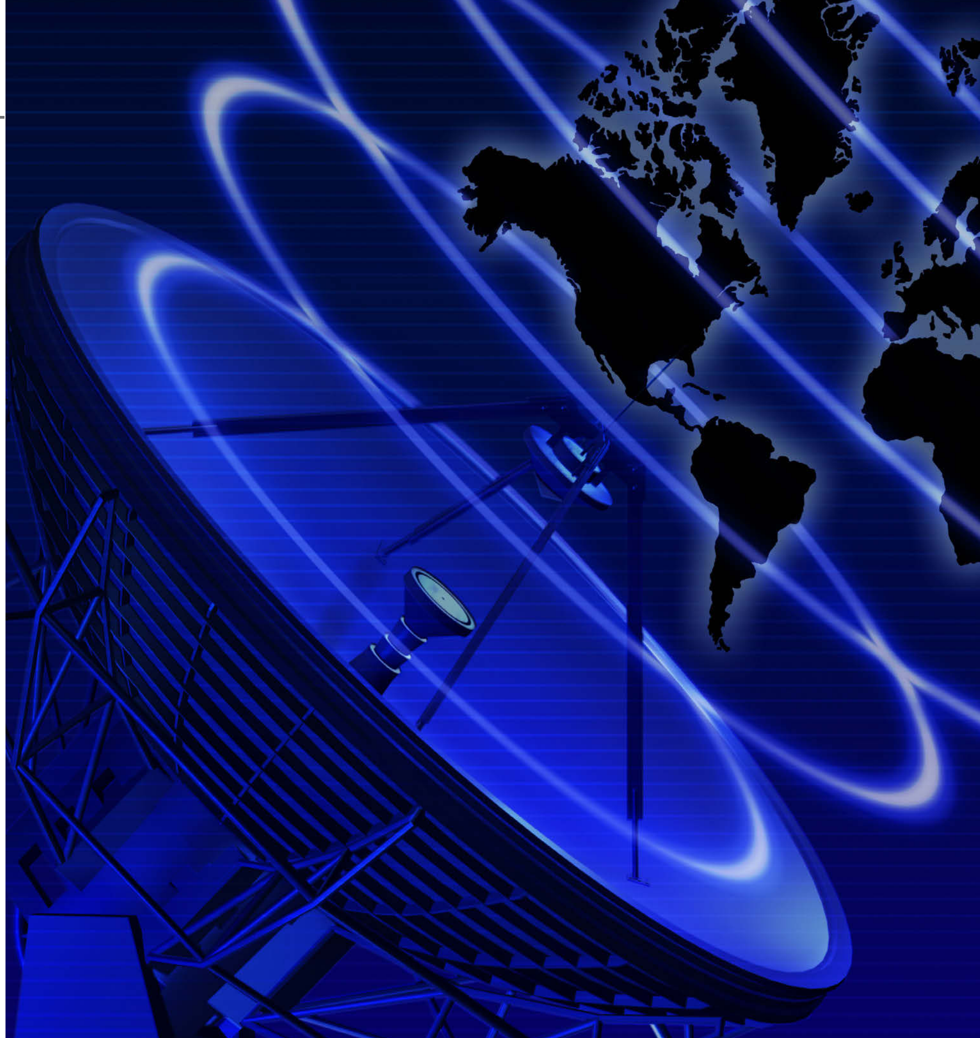
General Dynamics UK won a contract worth about $5.76 billion from the UK Ministry of Defence (MoD) to provide 589 SCOUT Specialist Vehicle (SV) platforms to the British army to add capability to the Armored Cavalry within Army 2020. The platforms, which consist of six variants, will be deployed to the British army between 2017 and 2024, alongside the provision of initial in-service support and training. SCOUT SV provides protection and survivability, reliability, and mobility and all-weather intelligence, surveillance, target acquisition, and recognition (ISTAR) capabilities.

Figure 4 | Shown in this image is the PMRS variant of the Scout Specialist Vehicle (SV) demonstrating its mobility during roll-out in Seville, Spain in June 2014. Photo courtesy of General Dynamics UK.

Cognitive radio's fate 'uncertain' as the spectrum battle plays out

By Sally Cole, Senior Editor

The U.S. Federal Communications Commission (FCC) is attempting to find a regulatory fix – striking a balance between national defense and economics – to eliminate electromagnetic spectrum inefficiencies. For now, this is making the exact role cognitive radio technology will play in the U.S. military's future unclear.



During the past few years, there's been a lot of talk about an impending "electromagnetic spectrum scarcity" within the U.S. But what's actually happening is that mobile operators aren't able to keep up with the demand generated by the rapid proliferation of smartphones, tablets, laptops, and other wireless gadgets – so these devices are hitting wireless traffic jams that could be avoided in the future by tapping cognitive radio technology to exploit the unused or underused parts of the electromagnetic spectrum.

In the U.S., the vast majority of spectrum designated to specific users is either used lightly, around 10 percent, or not at all – a gigantic utilization problem. Federal agencies have exclusive use of 18.1 percent (629 MHz) of the "beachfront" frequencies between 225 MHz and 3700 MHz, according to the FCC's Office of Spectrum Management, while non-federal users have exclusive licenses to 30.4 percent (1058 MHz). The remaining 51.5 percent is shared, with federal use primary and private sector use secondary.

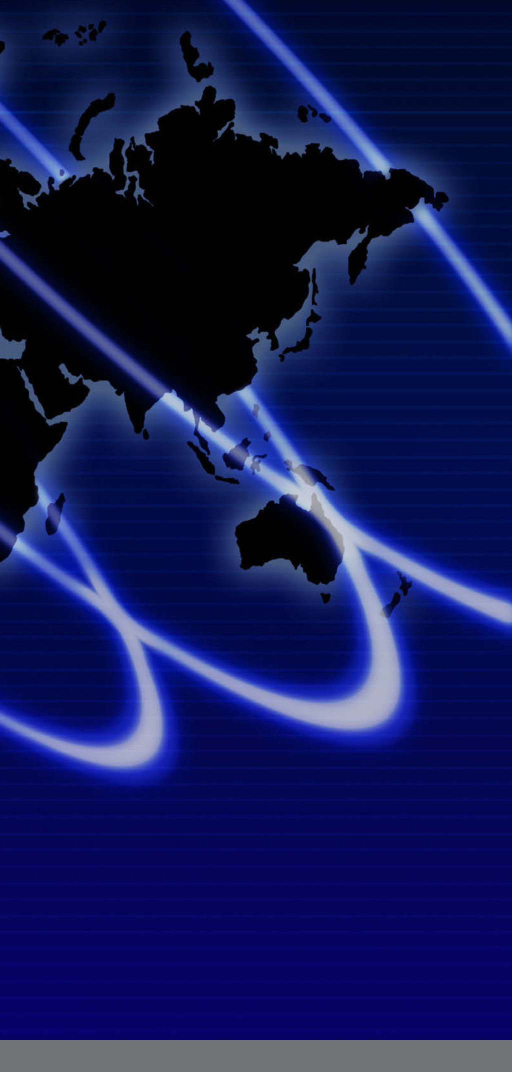
With the transition from analog to digital television, white space "channel guards" within the UHF spectrum (~500 to 700 MHz) are no longer needed to prevent interference between channels. Unlike analog signals, digital signals can be cut off or filtered precisely, so the FCC is proposing to "repack" or essentially eliminate the white spaces between the channels, freeing up and consolidating all the available white space into a single, highly desirable block of spectrum to be auctioned off.

This is all playing out as a cognitive radio battlefield, but this war is political and regulatory in nature. It is a big deal for the U.S. military, because its different forces all make use of different parts of the spectrum, not only for radio but also radar. But the military's spectrum needs aren't the only ones at stake. Other government agencies, mobile operators – such as AT&T and Verizon – and all of the various television broadcasters also want more spectrum, so there are many big stakeholders involved, billions of dollars at stake, and everyone is vying for the same spectrum.

"It's a fascinating battle – essentially a spectrum war," says Manuel Uhm, vice president of marketing for Coherent Logix (Austin, Texas; www.coherentlogix.com), as well as a board member of the Wireless Innovation Forum (Reston, VA; www.wirelessinnovation.org), a nonprofit international industry association dedicated to driving the future of radio communications and systems worldwide. "How this all plays out will ultimately determine how fast and effective cognitive radio technology will roll out," he continues.

Cognitive radio

Cognitive radio technology was developed many years ago, with an initial goal of providing flexible channels that could ensure high bandwidth, inference-free communications – mainly for military radio applications – over software-defined radio platforms.



The U.S. Department of Defense's (DoD) military forces maneuver within the electromagnetic spectrum to gain tactical, operational, and strategic advantages, and their stated vision is to have spectrum access "when and where needed to achieve mission success. To support this goal, DoD has stated that its future systems must become "more spectrally efficient, flexible, and adaptable." In short: cognitive radios.

So, what exactly are cognitive or "smart" radios? "Intelligent wireless devices that can dynamically access radio spectrum, rather than waiting for statistically assigned frequencies, cognitive radios can detect locally unused spectrum ranges and intelligently share them with nearby peers based on their instantaneous demands," explains Heather Zheng, a wireless networking and cognitive radio expert, as well as computer science professor at the University of California, Santa Barbara.

One of the key benefits cognitive radio provides the military is "the ability to access spectrum in a versatile manner, especially within hostile environments," Zheng says. "Usable spectrum within these environments are unpredictable and can change dynamically on-the-fly. Cognitive radios are capable of adapting spectrum usage on-the-fly to maintain reliable communication despite such dynamics."

There are still challenges ahead for the technology, and a big one is how to "realize cognitive radios that are both affordable and energy efficient so that they can be mobile portable devices," she adds.

That's not to say primitive forms of cognitive radio aren't already in use; they are. "An example is the automated cellular offload to WiFi," says Lee Pucker, chief executive officer of the Wireless Innovation Forum.

While cognitive radio and dynamic spectrum access define an entire set of technologies, the application of these technologies tends to be band specific. "Leaders of providing database/spectrum access system services, for example, include Federated

Wireless, Google, Spectrum Bridge, and KeyBridge Global," Pucker says.

Beyond government-funded R&D programs such as DARPA's xG and WNaN, and NSF's EARS, Pucker is seeing "limited investment in dynamic spectrum sharing technologies in advance of FCC regulation. Regulatory uncertainty in already-existing spectrum sharing bands is also inhibiting growth."

Spectrum management

More efficient management of the spectrum will help enable cognitive radio. Government agencies, the military, research communities, and companies interested in the technology are all exploring methods to efficiently monitor and enforce spectrum usage.

"An increasingly difficult challenge in spectrum management is how to perform real-time spectrum monitoring with strong coverage of deployed regions," points out Zheng. Today's spectrum measurements are basically "carried out by government employees driving around with specialized hardware that's bulky and expensive – making the task of gathering real-time, large-scale, spectrum-monitoring data extremely difficult and cost prohibitive," she explains.

One solution to the spectrum-monitoring problem, proposed by Zheng and colleagues, is to leverage the power of the masses – in the form of millions of wireless users – using low-cost, commoditized spectrum-monitoring hardware. "We envision an ecosystem in which crowd-sourced smartphone users perform automated and continuous spectrum measurements using their mobile devices to report the results to a monitoring agency in real-time," she says.

Spectrum monitoring and enforcement are critical problems frequently cited as being the main obstacles facing widespread deployment of dynamic spectrum systems, according to Zheng. "Without monitoring and enforcement, cognitive radio users could potentially 'misuse' spectrum without authorization, and such transmissions could disrupt legacy users and break the safety guarantees necessary for deploying dynamic spectrum access," she adds.

Emerging spectrum sharing trends

"The biggest spectrum sharing trend to emerge so far is the FCC's 3550 Citizen's Band Radio Service Proceeding, which proposes a three-tier model with federal users at the top tier as the protected incumbent, followed by a priority access tier, and a general authorized access tier," Pucker says.

This supports the model proposed by the President's Council of Advisors on Science and Technology in a spectrum sharing report, which states that the relocation/reallocation of federal users' spectrum for use by the commercial sector isn't a sustainable model. Instead, they propose spectrum sharing between federal and commercial users as the way forward in many bands.

"At the same time, new regulations for dynamic spectrum sharing can't be made unless there's a clear understanding that incumbents – commercial, civil, or defense – can be protected by the spectrum-sharing technology used and there's a valid business model under which investment can occur," Pucker says. "New business model development

Global redefining of airwaves

Each country around the globe is free to choose how to set up their own airwaves, so there is a spectrum battle playing out now, not just in the U.S., but in every country.

"One of the reasons spectrum is so critical in the U.S. is because the military has more access to spectrum than many other military services do within their respective countries, and some spectrum potentially up for grabs is currently allocated solely for radar," explains Manuel Uhm, vice president of marketing for Coherent Logix, as well as a board member of the Wireless Innovation Forum. "The U.S. military uses the low end of the spectrum for satellite communications and long-range radar, for example, and the high end for high-bandwidth communications and air defense."

The FCC has requested on more than one occasion to reduce the military's amount of spectrum so it can be auctioned off and made available for commercial purposes, but of course they would rather not give it up.

"Some military spectrum will almost certainly never be given up, because it's necessary for battle or military communications," Uhm says. "But there is some spectrum, which the military has ownership of that it isn't using or is underutilized."

In the United Kingdom, they've opted to let some spectrum exist unlicensed or as shared spectrum so that anyone can potentially access it – a perfect use case for cognitive radio, according to Uhm. "If interference is detected, the radio jumps to another band or available channel. It also means they can aggregate free spectrum to get more bandwidth by combining more of these channels," he adds.

In the U.S., at the moment, it is unclear how the spectrum battle will play out. "The FCC is hoping the broadcasters will auction off some of their licensed spectrum so they can repack it at one end and possibly sell off the remaining contiguous spectrum at the other end," Uhm says. "If that happens, there will be no whitespace market in the U.S. Quite frankly, this has negatively affected innovation around cognitive radio in the U.S. because if there isn't going to be a market, why invest in it? It's uncertain right now whether there will or won't be a market in the future."

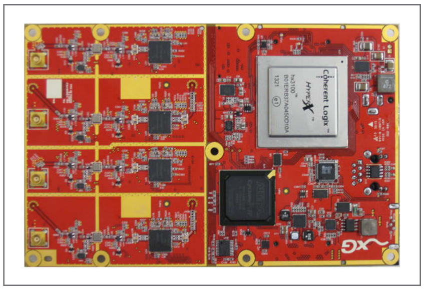


Figure 1 | The HyperX CRDP from Coherent Logix C programmable via the HyperX hx3100 100-core DSP and enables designers to quickly create a cognitive radio system.

is driven by an understanding of the technology's potential and limitations, as well as the regulatory environment under which they'll operate."

The industry is "incrementally winding its way around the technology, regulatory, and business circle – aided by government-funded R&D programs – and this evolution will continue," Pucker says.

Timeline for cognitive radio

The POTUS Wireless Broadband Initiative to free up 500 MHz of spectrum, initiated back in 2010, is driving some activity in cognitive radio, with a 2020 deadline.

Cognitive radio is expected to happen for the military in one form or another. The U.S. military is at the leading edge with cognitive radio and continues to make substantial investments in the technology. For example, earlier this year, University at Buffalo engineers received a $2.7 million grant from the Air Force to further develop cognitive radio, with a goal of making wireless 10 times faster.

"While regulatory uncertainty is one of the biggest concerns right now, another factor to consider is the possibility of needing to replace all of the associated radio-based equipment being used within a particular band today if it has to move to another band, which could happen if the FCC opts not to take a sharing approach and licenses all of the spectrum," Uhm says. "And, of course, no incumbent wants to take on that cost or effort." (See Figure 1.)

If spectrum "continues to be viewed as an asset to be allocated and not shared, then we will run out. But if, instead, it's viewed as an asset to be shared, everyone will need to learn to play nicely with others," he adds. Using inexpensive receivers that don't stay within band is a classic example of not playing well with others. This occurred with LightSquared and GPS receivers in the U.S.

For this reason, the Wireless Innovation Forum is advocating receiver specifications, not just transmitter specifications. Today, all the specs are on the transmit side in terms of how much power can be radiated. This is one more change that will need to happen before cognitive radio can truly take off.

Ultimately, cognitive radio's real beauty is that it "enables all of these new and efficient ways of using the spectrum, but at a level of flexibility that can also be viewed as a drawback if it makes it too difficult to map out a course forward or reach an agreement between users," Uhm says. "A spectrum-sharing friendly regulatory environment can help to ensure the creation of successful business models that will enable cognitive radio technology to transform how we use spectrum." MES

Wireless Innovation Forum contributions to SCA 4.1

By Lee Pucker

Successful deployment of Software Communications Architecture version 2.2.2 (SCA 2.2.2)-based software defined radios has identified improvements to be made to advance the technology further. The Wireless Innovation Forum is working in collaboration with the U.S. Department of Defense Joint Tactical Networking Center (JTNC) to evolve the SCA with the production of eight document packages providing six technical recommendations and two specifications for the next version of the SCA.

Global SCA standards for defense communications.

The need to evolve beyond SCA 2.2.2
"The SCA Specifications are an important cornerstone to SDR Standardization, and…a prerequisite to enable timely and cost efficient porting and integration of waveforms, especially multinational and secure waveforms for combined operations," said Dr. Ruediger Leschhorn, Head of Studies in the Radio Communications Division of Rohde & Schwarz, Germany.

The SCA 2.2.2 architecture has achieved significant success in the military communications market[1]. Hundreds of thousands of SCA-enabled software-defined radios (SDRs) have been deployed to date, and dozens of programs are currently working to field more of these types of radios moving forward (see lead image). The reasons for this success lie in the benefits brought through adoption of the SCA: proven cost and delivery-time advantages, enhanced intercomponent interoperability, simplified insertion of new communications capabilities in deployed radios, and reduced development risk and time to market.

The success of the SCA to date has led new countries and new organizations to begin exploring its use, driving a second generation of SDR market adoption[2].

As with any technology, actual use in real-world environments highlighted the improvements in the SCA specification that were necessary to allow further market penetration. Chief among these were improving the ability of the architecture to scale to address the size, weight, power, and cost requirements of certain radios; finding modifications in the architecture that could enable radios to boot faster; improving support for devices such as digital signal processors (DSPs) and field-programmable gate arrays (FPGAs) that are used in most radio architectures; and enhancing the ability to migrate legacy waveforms to an SCA model. The need for these improvements led programs such as the European Secure Software Defined Radio (ESSOR) program in Europe to define their own SCA-based SDR architectures[3].

New specification needed
In 2009, the Joint Program Executive Office for the Joint Tactical Radio System (JPEO JTRS) initiated the SCA Next project to provide these improvements. The Wireless Innovation Forum brought the voice of the international community to the collaboration process, providing contributions from member organizations worldwide and from programs such as ESSOR[4,5,6,7]. The result of these and other efforts was SCA 4.0, which provided improved scalability and better support for lightweight applications by removing the requirement for Common Object Request Broker Architecture (CORBA) middleware and defining lightweight and ultra-lightweight environments for development on resource-constrained processors[8].

In November 2013 the evolution of the SCA continued through a workshop hosted by the Wireless Innovation Forum's Coordinating Committee on International SCA Standards (CCSCA) and with participation from the JTNC to

further improve the SCA specification[9]. Key areas for additional improvement defined at this workshop included better backwards compatibility with SCA 2.2.2 and additional updates to the Application Environment Profiles (AEPs) and Interface Definition Language (IDL) profiles. A work plan was established, with the Wireless Innovation Forum taking the lead in developing technical solutions in multiple areas.

Technical contributions to SCA 4.1

Well over 1,000 hours were volunteered by the Forum's member representatives in developing these solutions. Their efforts resulted in six recommendations[10]:

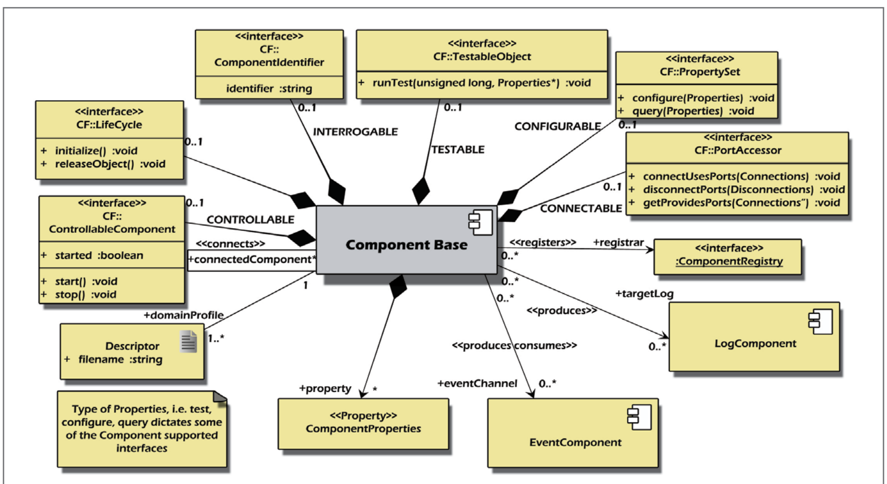


Figure 1 | Proposed Component Base UML model.

- **Application-Backwards Compatibility.** This recommendation provides comments on the modifications to SCA 4.0 necessary to support application-backwards compatibility with SCA 2.2.2.
- **Application Mixture.** This recommendation proposes changes to the next SCA specification, which will allow an application to be comprised of both SCA 2.2.2 and SCA 4.1 components. This change will allow developers to perform a more incremental transition from SCA 2.2.2 to SCA 4.
- **Naming Conventions.** This recommendation proposes changes to the SCA 4.0.1 specification to use a naming convention for the names of the interfaces and components. The goal is to improve readability of the next release of the specification.
- **Push Registration Allocation Properties.** This recommendation proposes changes to the SCA 4.0.1 specification to support late device registration with the domain manager. This change will allow the core framework to better accommodate device components with multiple implementations and to manage plug and play devices.
- **Scalable Components.** This recommendation proposes changes to the SCA 4.0.1 specification to improve component scalability by allowing component developers to choose whether or not to implement some of the standard subcomponent interfaces. The scalability will also be used to support the different profiles of the specification (see Figure 1).
- **Scalable Manager Components.** This recommendation proposes changes to the SCA 4.0.1 specification to add support for scalability of the manager components. This will allow developers to choose whether or not to implement all of the manager interfaces. The manager scalability will also be used to support the different profiles of the specification.

The volunteer efforts also produced two specifications[11]. The first is WInnF Lw & ULw AEPs. This specification defines POSIX AEPs for interaction between SDR applications and the operating environment (OE) in resource-constrained architectures. Two Base AEPs functions groups, the Lightweight (Lw) and the Ultra-Lightweight (ULw), are defined. The documents contain normative content for Base AEP functions groups plus support sections giving SCA-like contents-overview tables and detailed rationale for the design choices. The specification also provides two function groups that can extend the Base AEPs function groups if required for porting, with negligible impact on portability. The specification harmonizes and improves prior work from JTNC and ESSOR into a single converged solution (see Figure 2).

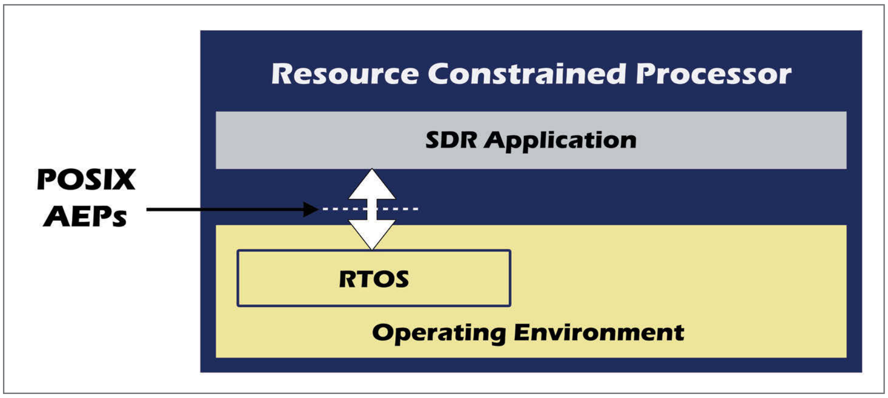
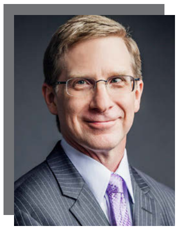


Figure 2 | Positioning the AEP specification.

The second spec is the WInnF PIM IDL Profiles. This specification defines platform-independent model (PIM) IDL profiles that may be used to define platform-independent SDR component APIs. Two PIM IDL profiles are defined: the "Full" and the "Ultra-Lightweight" profiles. The document contains normative content for the defined profiles, a support section with content-overview tables and extension perspectives, and a rationale section to explain the design choices. This specification also harmonizes and improves prior work from JTNC and ESSOR into a single converged solution.

Where to next?

The document packages above have been submitted to the JTNC for consideration to be included in the SCA 4.1 specification. At the time of this writing, a release date for this new specification has not yet been defined, but it is anticipated that a draft will be available late in 2014 or early 2015. In the interim, a preview event has been scheduled for October to present the proposed changes and to explore requirements for future SCA updates[12]. **MES**



Lee Pucker *is the CEO of The Wireless Innovation Forum, a non-profit "mutual benefit corporation" dedicated to advocating for the innovative use of spectrum, and advancing radio technologies that support essential or critical communications worldwide. Lee is a certified association executive (CAE), a project management professional (PMP), and holds a BSc degree from the University of Illinois and an MSc degree from The Johns Hopkins University. Readers may reach him at lee.pucker@wirelessinnovation.org.*

Wireless Innovation Forum
604-828-9846
www.wirelessinnovation.org

References

1 http://groups.winnforum.org/d/do/6610
2 http://groups.winnforum.org/d/do/6527
3 http://www.occar.int/296
4 http://jtnc.mil/sca/Documents/JPEO-NR-2010-004.pdf
5 http://groups.winnforum.org/d/do/4983
6 http://groups.winnforum.org/d/do/4984
7 http://groups.winnforum.org/d/do/4985
8 http://jtnc.mil/sca/Pages/default.aspx
9 http://groups.winnforum.org/p/cm/ld/fid=403
10 http://groups.winnforum.org/Recommendations
11 http://groups.winnforum.org/Specifications
12 http://www.wirelessinnovation.org/sca-4-1-standard-preview-event

Multiband military communications challenges overcome by software-defined radio

By Duncan Bosworth

Marines radio a mass casualty report during Exercise Koolendong on Bradshaw Field Training Area in Australia. U.S. Marine Corps photo by Cpl. Scott Reel.

The ability to access accurate, real-time information across secure data links is a cornerstone of any successful military campaign. This ability is especially needed today given the requirement of the command-and-control center to communicate directly and instantly with soldiers in the field via both voice and data. What should be a strategic and tactical advantage, however, is only as good as the ability of advanced wireless technology to navigate a web of complex radio frequency (RF) and signal-processing technologies and to render a seamless, reliable, and secure communications network that delivers the right information at the right time in an ever-more-challenged RF spectrum.

Historically, the military has relied on a profusion of different, incompatible radios and waveforms serving needs as varied as tactical soldier radios, airborne links, satellite communications, base-relay stations, and emergency transmitters, as well as emerging application-specific functions such as unmanned aerial vehicle (UAV) operation needing both control and in some instances, relaying of video surveillance images. Each of these radios establishes a vital communications link, and leaving one out of the mix would place the operational team at a disadvantage. Yet each radio carries a cost in size, weight, and – in the case of soldier systems – spare battery needs. The problem is further complicated and becomes unmanageable as new requirements and waveforms are added to the list.

To compound matters further, future operational requirements are demanding that systems be multifunctional. In addition to the need for radios to support multiple voice and data waveforms across wider RF frequencies, future soldier systems are also looking to incorporate features such as electronic surveillance and warfare functionality, thereby further increasing the system design challenges.

The solution to all of these challenges is a universal full-duplex radio module that can be used across all platforms and can be dynamically real-time reconfigured in the field to provide flexibility, versatility, efficiency, and longer operating life from a single set of batteries, all while providing significant size, weight, and power (SWaP) advantages.

Making the "universal" radio concept into a reality has proven harder than envisioned: Providing the suitable analog front end (AFE) has been particularly difficult. To complicate matters further, a next-generation "universal" radio would have to combat the challenges posed by increased spectral congestion, driven by the explosion of commercial radio and cellular systems. This not only leads to increased out-of-band signal filtering or

dynamic range needs to manage the potential signals of interference, but it also requires the system to provision for operation in other frequency bands where congestion may be less of an issue.

Until recently, an AFE for this type of versatile radio potentially required an array of overlapping parallel channels, each designed to cover a particular segment of the RF spectrum, with bandwidth matched to the intended signal format and potentially with specific filtering to meet the out-of-band signal-rejection requirements. At best, this approach is costly in terms of final printed-circuit-board footprint, weight, and power; in the worst case, it requires multiple complete radios to be developed.

Adopting a software-defined approach

A software-defined radio (SDR) is the ultimate solution to this problem. By increasing the emphasis from analog to digital and software-based signal processing, it can accommodate various physical-layer formats and protocols, encrypt data, and convert analog-to-digital signals with software running on a processor or FPGA, which makes it perfect for military requirements. Users can dynamically control the frequency, modulation, bandwidth, encryption functions, and waveform requirements.

SDR also has the flexibility to incorporate new waveforms and functionality into the system, without having to upgrade or replace hardware components. These SDRs would be used not only by the soldier for data access and communicating back to the command center but also to create wide-area sensor/mesh networks for position/detection and communication among combat soldiers.

The most important component in SDR is the transceiver. To enable all of the flexibility and versatility outlined, the transceiver needs to have an exceptionally wide RF range and be capable of rapidly tuning and configuring the channel bandwidth via software; it must support both frequency-division multiplexing (FDM) and time-division multiplexing (TDM). For advanced waveform support, it must also have high performance in terms of dynamic range and reliability, even under noisy conditions and in environments with intentional and unintentional interference. At the same time, it should operate under reduced power to minimize drain on the soldier's battery pack.

A highly integrated, mixed-signal RF integrated circuit (RFIC) makes broadband SDR designs smaller, lighter, and less power-hungry. The real challenge comes in the extremely broadband nature of the AFE in the SDR, which in a classical design would need many spectrum- and possibly waveform-specific front ends, each of which is a challenge to design and evaluate, with the final product likely to fall short in the SWaP ranking.

Component requirements

A new generation of wideband, programmable front-end transceivers that support dual independent transceiver channels has the potential to meet these SDR challenges. The system processor can dynamically reconfigure key parameters (such as bandwidth and RF frequency) to match the application needs and deliver optimum results and also has the potential to serve the fast-growing multiple-input, multiple-output (MIMO) segment as well as non-MIMO needs.

The new generation of wideband integrated RF transceivers are the ideal solution for many of the next generation of military communication and electronic surveillance systems. As they support wide channel bandwidths, the devices match many of the new data-centric waveforms being deployed in next-generation systems. This high level of configurability enables cognitive radio systems and the use of adaptive waveforms. With the ability to rapidly tune across a wide RF bandwidth, the devices can be a solution for electronic surveillance, particularly in platforms where power may be limited.

One such transceiver is the Analog Devices AD9361 RF Agile Transceiver (see Figure 1), a 10 mm x 10 mm chip-scale device with a user-tunable bandwidth from 200 kHz to 56 MHz; it also includes other features and performance attributes needed to build a signal chain spanning 70 MHz to 6 GHz. This 2 x 2 direct-conversion component reduces the entire AFE into a single, relatively simple circuit and interfaces with the host processor via an LVDS or CMOS port. Within the IC are 12-bit A/D and D/A converters, fractional-N synthesizers, digital and analog filters, automatic gain control, transmit power monitoring, quadrature correction, and other critical functions.

The receiver noise figure is also less than 2.5 dB, while transmitter error vector magnitude (EVM) is better than -40 dB and transmitter noise floor is below -157 dBm/Hz. For both transmit and receive paths, the local oscillator step size is just 2.5 Hz for precise tuning. Despite the many functions within the IC, power consumption is still low, generally around 1 W.

Integrated system design

A flexible, wideband SDR platform involves a major circuitry-design effort, algorithm development, and consideration of tradeoffs. Although at first glance this may seem a daunting development, a new generation of transceivers must include an available reference design to simplify the system development. In addition to being fully customizable in software without any hardware changes, the reference platform must be optimized for use with FPGAs and provide a guide for both power supply and board layout to ensure optimum performance. Furthermore, to support the increasing prevalence of MIMO configurations, supporting options for beamforming and beamsteering reference designs should illustrate multi-device synchronization (see Figure 2).

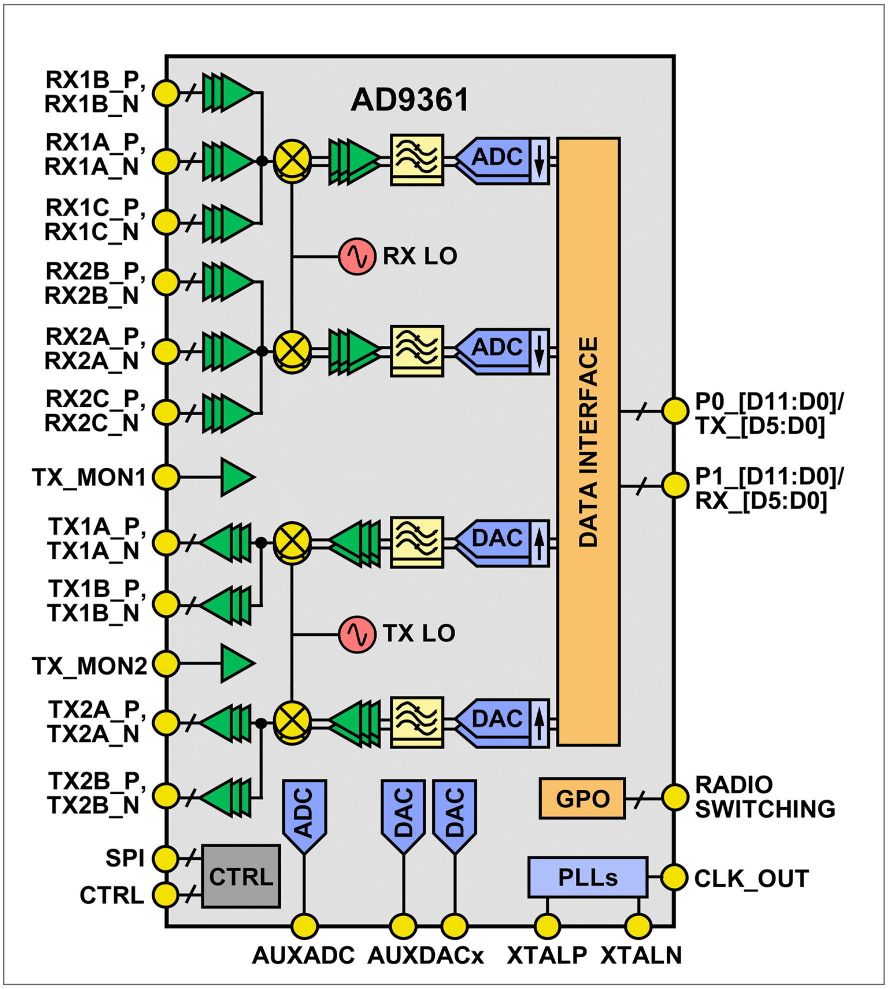


Figure 1 | AD9361 2 x 2 RF transceiver architecture.

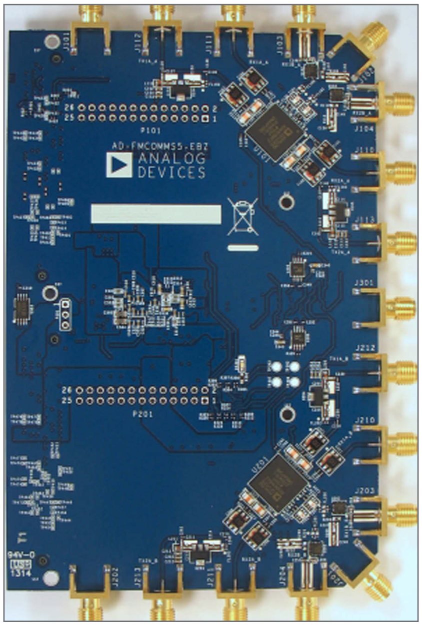
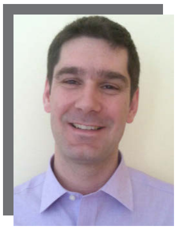


Figure 2 | The AD-FMCOMMS5-EBZ MIMO FMC platform for evaluation and prototyping.

By adhering to the design guidelines outlined in the reference designs, engineers can quickly move from evaluation to prototyping through to successfully implementing a full-duplex, lightweight, long-lasting platform that can be dynamically reconfigured in the field and finally bring the "universal" radio from drawing-board concept to real-world applications. **MES**



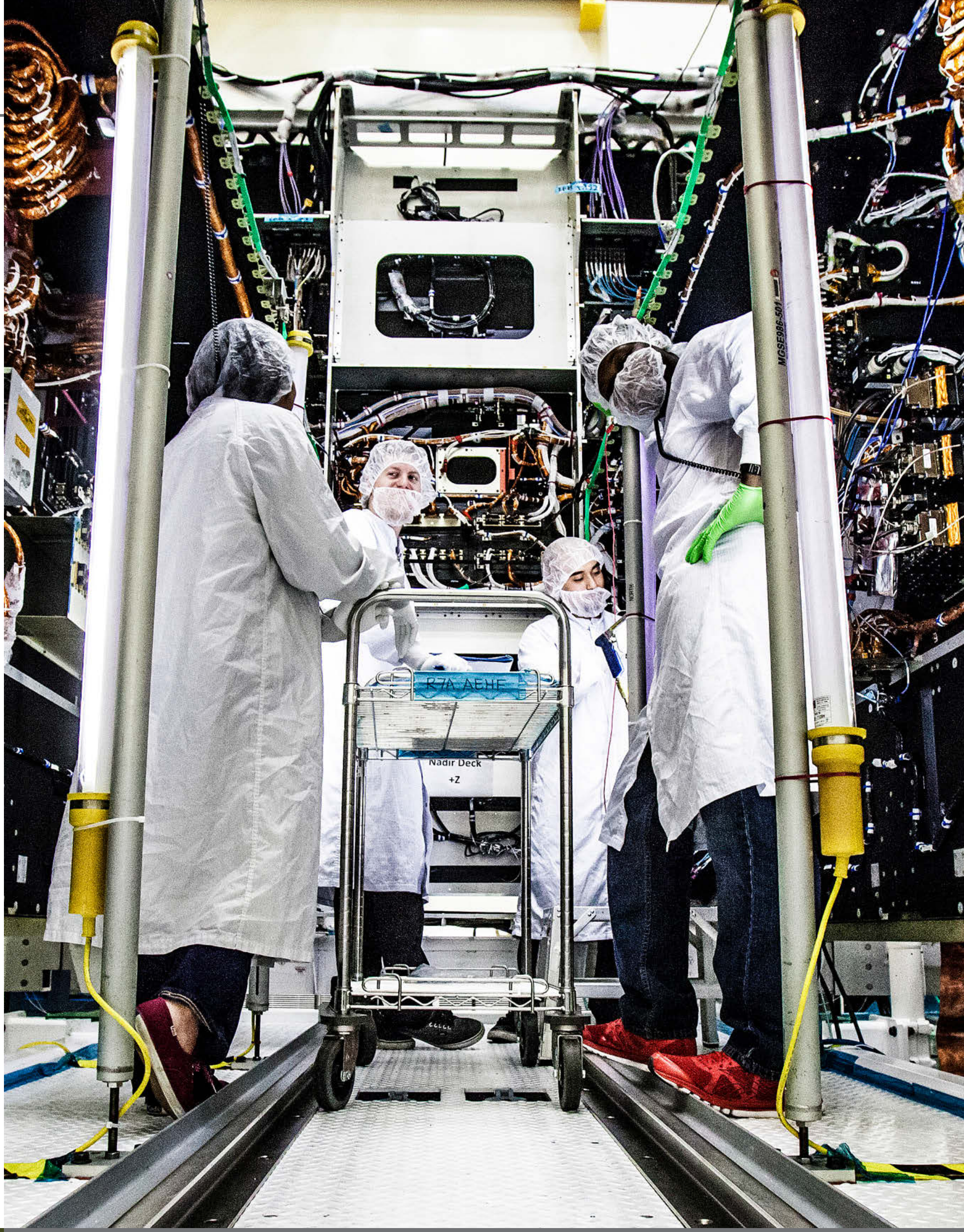
***Duncan Bosworth** is a Marketing Engineer with Analog Devices in the Industrial and Instrumentation Segment focusing on aerospace and defense. Prior to his role at Analog Devices, Duncan held senior defense-focused engineering roles for over 17 years. Duncan received his MEng from University of York, U.K. in 2001 and is a U.K. Chartered Engineer. Readers may reach him at duncan.bosworth@analog.com.*

Analog Devices • 781-329-4700 • www.analog.com

Reconfigurability and extended data rates drive satellite communication payload designs

By John McHale, Editorial Director

Military satellite program managers are demanding greater on-orbit flexibility to reconfigure payloads based on evolving battlefield requirements. They also want to move more and more data, extending the rates of current payloads. Both of these needs require innovation at the electronic component level.



Pictured is the integration of the payload module for the fourth Advanced Extremely High Frequency (AEHF) protected communication satellite at Northrop Grumman's facilities in Redondo Beach, Calif., prior to its recent shipment. (Northrop Grumman photo by Alex Evers.)

Space platforms are not often associated with flexibility. Once launched and in orbit, satellites do not see many payload repairmen flying up from Earth. Therefore, systems onboard must work for 15 years or more. Designers build in redundant components and systems in case the electronics are damaged by cosmic rays or other threats. Now thanks to advanced software architectures, extended bandwidths, and high-performance FPGAs, military SATCOM payload designers are getting that flexibility.

"Reprogrammable technology allows operators more flexibility in a satellite's mission," says Jill Krugman, a spokeswoman for Lockheed Martin. "With a 15+ year lifespan, needs change throughout the course of a satellite's life and the ability to dynamically modify a mission assures that our satellites deliver value as long as they are in orbit."

An example of this is "the reprogrammable processor designed by Lockheed Martin," she continues. "It is the only technology of its kind being offered on the commercial market today. It is used on the A2100 satellite, which has served both commercial and military customers. The A2100 is the common framework behind the Advanced Extremely High Frequency, Mobile User Objective System, Geostationary Operational Environmental Satellite Series-R, and GPS III satellites," she says.

The fully reprogrammable mission processor enables users to modify payload configurations and performance in-orbit, suppress interference, and adjust satellite-to-ground communication, Krugman says. Today, satellites typically amplify incoming signals and route them back to Earth, but reprogrammable technology will enable signals to be processed and routed to multiple users and locations. For example, if a thousand mobile calls came into a single satellite, the onboard processor can switch all those calls to discrete users and locations, she adds

"Military satellite users are looking for flexibility through reconfigurability," says Peter Cash, director of the Space, Defense, and Avionics Frequency and Time Division

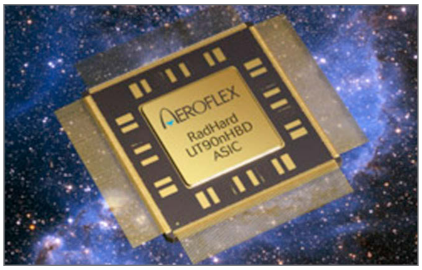


Figure 1 | The radiation-hardened UT90nHBD ASIC from Aeroflex provides logic and memory bit advantages for satellite communication payloads.

at Microsemi in Aliso Viejo, Calif. "They want to be able to quickly reconfigure payloads in orbit. Right now the methods for reconfigurability are pretty limited particularly in severe radiation environments."

Engineers at Northrop Grumman in Redondo Beach, Calif., leveraged reconfigurability in the protected communications payload for the U.S. Air Force's third Advanced Extremely High Frequency (AEHF) satellite.

"The payload's software-based communication network architecture allows us the unprecedented ability to reconfigure assets as needed for an evolving battlefield," says Stuart Linsky, vice president of communication programs, Northrop Grumman Aerospace Systems. "This software-based architecture has enabled Northrop Grumman to deliver new capabilities our leaders and warfighters requested through the Milstar constellation for all 20 years since the launch of the first Milstar in February 1994."

FPGA or ASIC

Much of the reconfigurability in satellite payloads is enabled by radiation-hardened FPGAs such as those from Xilinx and Microsemi.

"To enable reconfigurability, designers are using multiple transceivers and in parallel with multiple FPGAs," says Chuck Tabbert, vice president of sales and marketing at Ultra Communications in Vista, Calif. "For example, they may use a Xilinx space-qualified FPGA with 16 lanes at 2.5 gigabits per second [Gbps] and multiplex those channels into one transceiver, enabling a 40 Gbps electrical-to-optical conversion for point-to-point solutions."

Figure 2 | One Advanced Extremely High Frequency (AEHF) satellite will provide greater total capacity than the entire Milstar constellation currently on orbit. Photo courtesy of Northrop Grumman.

"For the implementation of digital logic, two fabrics solutions dominate the landscape: ASICs or FPGAs," says Tony Jordan, vice president of Product Marketing and Applications Engineering at Aeroflex Microelectronics Solutions in Colorado Springs, Colo. "System designer trade-off power, operational frequency, size, schedule, design risk, flexibility (i.e.: ability to reprogram on orbit), and cost when selecting a digital fabric. Mission and budget requirements will ultimately dictate the selection of the digital technology. Perceived ease of on-orbit reconfiguration, flexibility, and limited or one-time use payloads drive system implementers to FPGAs. ASICSs have a decided advantage in power, performance, and recurring cost," he continues.

"Satellite communication payloads opportunities remain a focus market segment for Aeroflex," Jordan says. "We are developing standard products to meet with future requirements and on the ASIC side our 90-nanometer capability offers very attractive logic and memory bit densities, as well as gigabit-per-second serial communication solutions. We look forward to new architectures that will take advantage of these capabilities." (See Figure 1.)

Extending data rates

One thing satellite designers want even more than reconfigurability is more bandwidth. The demand for more and more information over existing frequencies is forcing satellite designers to extend the bandwidth of new commercial and military payloads.

"Data rate demands really depend on the mission platform," Tabbert says. "If you are talking about sensing applications in low Earth orbit for the intelligence community then there will be requirements for more bandwidth between sensors and computers. However, interesting things are happening with communication payloads when it comes to bandwidth. Communication payloads are demanding greater and greater throughput due to mobile communication devices."

Northrop Grumman engineers used crosslinks to enable extended data rates (XDR) on their AEHF communication payloads on both sides of an AEHF satellite. This was not possible with only two AEHF satellites on orbit, says a Northrop Grumman spokeswoman. Testing involved establishing communications networks between combinations of AEHF terminals on the ground that use Milstar's medium data rates and other terminals equipped to handle the wideband AEHF XDR. They exercised and further proved payload software that configures worldwide networks (see Figure 2).

"One AEHF satellite will provide greater total capacity than the entire Milstar constellation currently on orbit," the spokeswoman says. "Individual user data rates will be five times improved. The higher data rates will permit two-way, jam-resistant transmission of tactical military communication such as real-time video, battlefield maps, and targeting data."

"Military satellite payload integrators are challenged trying to send more information bits in a given frequency spectrum; enhanced digital electronics is key to meeting this challenge," Jordan says. "Enabling digital technologies optimize logic and memory per unit area, and afford the system designer with gigabit-per-second serial communication capabilities ['fat pipes']. Satellite payload programs require small footprint [pin count] fat pipes to reduce payload size and mass. For example, advanced architectures will interface giga-sample per second ADCs and fast DACs to digital processing elements using these small footprint fat pipes. Four pin, single-lane, gigabit-per-second CML SerDes are now replacing eight pin LVDS-based solutions while providing upwards of 2x the performance," he continues.

"The increased data rate demands bode well for suppliers of fiber optic components," Tabbert says. "Fiber optic interconnected networks are winning when data rates per channel are 2.5 Gbps and above from a size, weight, and power [SWaP] perspective. That said, just as you should never bet against silicon in the semiconductor world, you should never bet against copper solutions in the interconnect world.

"The military satellite market is constant and bandwidth requirements are always increasing," Tabbert continues. "The commercial fiber optic community is fielding 100 Gbps solutions right now and I expect the satellite and avionics markets to follow close behind. Ultra Communications' standard X80 platform, which is a 40-gigabit fiber optical transceiver, is used across all market configurations – for space avionics, missiles, and ships. 40 gigabit box-to-box connectivity is hard over copper interconnects and fiber wins the SWaP trade-offs."

Leveraging commercial manufacturing processes

With the demand for more data and enhanced flexibility comes the never-ending demand for reduced costs. Nothing is ever inexpensive when it comes to space, but system integrators are leveraging commercial manufacturing techniques to improve time to market and reduce development costs where possible.

Commercial practices have long benefitted the military satellite market, Krugman says. As mentioned previously, the A2100 serves as the framework for multiple government satellites. "To that end, we will continue to derive military applications from the A2100 as we modernized the system for the commercial world including advances in digital design, manufacturing, and 3D printing."

Stable atomic clocks

"Military satellite designers want greater stability from atomic clock solutions to maintain the stability of the frequency as it is sent to the ground," says Peter Cash, director of the Space, Defense, and Avionics Frequency and Time Division at Microsemi in Aliso Viejo, Calif. "To do this they need to get more efficient timing capability into orbit with the satellite."

"There is not a whole lot up there right now that can provide compact timing in a master oscillator," he continues. "The key is to tie it into one FPGA, which will not only enable reconfigurability but also reduce footprints, which helps create more redundancy onboard the satellite. Reduction of size, weight, and power (SWaP) is an important characteristic of FPGAs."

For these applications Microsemi offers the 9500B oven-controlled quartz crystal oscillator that produces a highly stable, low noise reference frequency output, Cash says. It can be used as the onboard frequency reference for a satellite or its ground station. The solution has a third overtone SC-cut quartz resonator which, along with its sustaining electronics, is completely enclosed in an insulating dewar and then kept at a precisely controlled temperature. The result is excellent short-term stability, phase noise, and aging characteristics (see Sidebar Figure 1).

Precise timing for ground stations

"Precise, low-noise timing instrumentation technology is needed to manage the satellite ground station infrastructure, which is very critical to manage the onboard clocks in the satellite constellation," says Ramki Ramakrishnan, director of Product Line Management & Business Development for the Clocks Business Unit/Frequency and Time Division at Microsemi. "Latest generation timing systems reduce the power consumption and the footprint at the ground station level and enable network connectivity. The heart of a good ground station lies in its precise, accurate, and stable clocks."

Solutions with smaller footprints also help drive costs down while meeting the SWaP objectives, he adds. For SWaP-constrained applications in space, Microsemi offers the 9600 oscillator, which uses hybrid circuitry to enable the size reduction.

Sidebar Figure 1 | The 9500B oven-controlled quartz crystal oscillator from Microsemi produces a highly stable, low noise reference frequency output.

High-power GaN amplifiers for Ka-band satellite communication terminals released by Northrop Grumman

Engineers at Northrop Grumman Corp. in Redondo Beach, Calif., introduced two new high-power gallium nitride (GaN) monolithic microwave integrated circuit (MMIC) power amplifiers for Ka-band satellite communication terminals and point-to-point digital communication links.

The APN228 and APN229 power amplifiers were developed leveraging the company's GaN high-electron mobility transistor (HEMT) power process and enable saturated output power of 13 and 8 watts, respectively. The broadband, two-stage amplifiers operate from 27 to 31 GHz, and, when designed into high efficiency solid-state power amplifiers (SSPAs), enable higher data rate in communication systems.

"GaN-based SSPAs are a far more desirable solution to costly traveling-wave tubes which require more complex, higher voltage power supplies and a lengthier production time," says Frank Kropschot, general manager, Microelectronics Products and Services, Northrop Grumman Aerospace Systems. These products will enable users to cut down on the cost and complexity of power-combining, he adds.

The APN228 is a 16.0 mm2 GaN HEMT power amplifier that operates between 27 and 31 GHz. This MMIC PA has 19.5 dB of linear gain, 41.2 dBm (13 W) of saturated output power, and a Power Added Efficiency (PAE) of more than 27 percent. It is targeted at next-generation, high-power, and efficiency SSPAs for commercial and military satellite applications.

The APN229 is a 7.41 mm2 GaN HEMT power amplifier that operates between 27 and 31 GHz, provides 20 dB of linear gain, 39 dBm (8 W) of saturated output power, and a PAE greater than 30 percent. It is also a complimentary driver amplifier to the APN228.

Northrop Grumman leveraged commercial practices during the manufacture of specialty compound semiconductors for the AEHF fifth and sixth satellites at its advanced microelectronics wafer fabrication facility in Manhattan Beach, Calif. The more than 36,000 integrated circuits produced at the facility enable production to ramp up on a broad scale for both payloads, says a company spokeswoman.

"By implementing commercial best practices in making military integrated circuits, we're able to generate further cost savings for the Air Force," Linsky says. Each payload contains some 18,000 high-frequency monolithic microwave integrated circuits (MMICs) for frequency conversion, amplification, and switching, he says. They are integrated throughout the payload's major subsystems that enable real-time mobile, global access such as anti-jam uplinks and downlinks, secure crosslinks, and super high gain Earth coverage antennas. **MES**

Shutting out the noise: Voltage references for precision analog signal paths in space applications

By Dan Goodhew

Class V/Q radiation-hardened ICs deliver high reliability for orbital space flight. (Photo courtesy of Intersil Corp.)

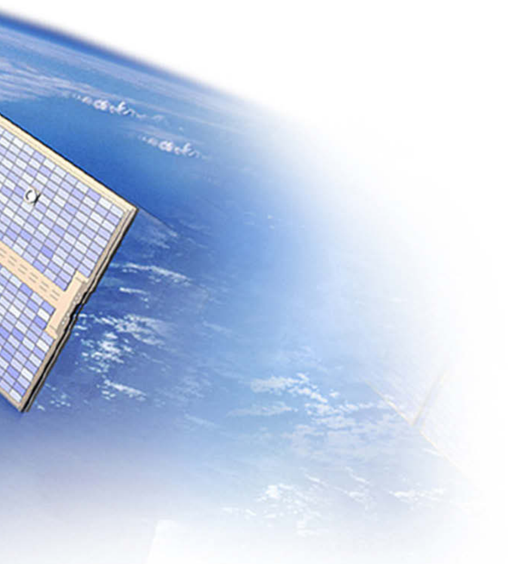
When designers are trying to select a component in the signal path of a satellite system, it is often difficult to find a device with both the radiation tolerance and accuracy required. Signal integrity is, after all, the key specification when designing an analog signal chain. The main causes of error to the integrity of the signal chain can be divided into two categories: inaccuracies due to noise and inaccuracies due to shifts in voltage. While it is important to consider all components in the signal path, one component is the most critical in achieving precision performance: the voltage reference.

Reducing noise

Noise in a system can be reduced with the correct use of filters and the averaging of measurements when converting a signal from the analog domain to the digital domain. However, large or complex filters require board space and increased component count, not to mention added weight, which results in higher costs. Large filters also increase the settling time for transient response. Averaging saves on extra component cost but comes at the expense of sample frequency. The A/D converter requires a voltage reference with lower noise than the signal being measured to take advantage of averaging. For example, a 20-bit system requires the voltage reference to have a noise of less than 1 part per million (ppm). If the system requires higher precision than a voltage reference can deliver, averaging can still be used but will be extremely costly, as multiple analog-to-digital converters are needed. Each converter has its own voltage reference and the measurement from each is then averaged.

In the last five years, several manufacturers have offered references with noise in the single-ppm peak-to-peak levels. For traditional bandgap references, about 600 mV of Proportional To Absolute Temperature (PTAT) voltage is generated and added to a single-transistor base-to-emitter voltage (Vbe) to produce the basic bandgap voltage of ~1.22 V. An output amplifier (which may be part of the bandgap itself) gains and buffers the internal bandgap voltage up to a standard output. The 600 mV of PTAT has been created from a single delta-Vbe (ΔVbe) structure made from two transistors running at different current densities generating a voltage ΔVbe=(KT/q)*ln(R) where K is Boltzmann's constant, T is absolute temperature, q is the electric charge, and R is the current density ratio between the two transistors. A common design has R=8 and ΔVbe=54 mV. To bring this up to 600 mV will require a gain of about 11. That gain of 11 will amplify device noises and instabilities directly.

One solution to reduce the noise in a bandgap reference is to employ cascaded ΔVbe rather than an amplified ΔVbe. That is to say, the design effectively adds 11 of those R=8 units in sequence to generate the 600 mV. This has profound effects on the noise. If one adds the noise of 11 identical units, the result is only √11 noise amplification or a 3.3-fold improvement. It is better than that, though, because the mechanisms that give the gain of 11 in a standard



bandgap more than double the ΔVbe noise. Figure 1 shows the peak-to-peak noise of a bandgap reference with the cascaded ΔVbe topology.

When a voltage reference is exposed to radiation, the noise increases. Although the increase in noise is not large, the above solution keeps the increase even lower. Also, popcorn noise sources would only exist sparsely with perhaps one site on a die, and

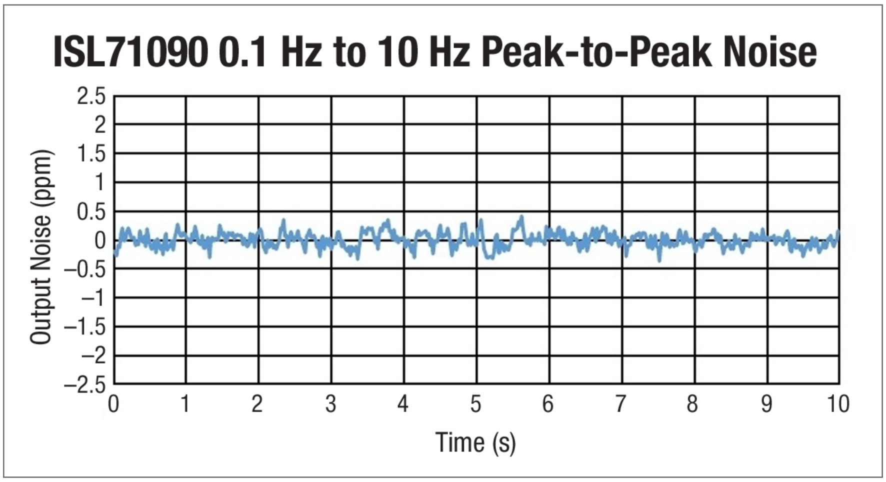


Figure 1 | ISL71090 voltage reference peak-to-peak noise plot.

they would not receive the gain of 11. If popcorn noise is in fact found, it will be an order of magnitude smaller than in a traditional bandgap reference.

Lowering voltage shifts

Voltage shifts in a system may be reduced with fairly simple additional circuitry, although making adjustments across a full temperature range presents added difficulty. The cost of the additional circuitry is also high. Furthermore, offset voltages can only be corrected if they are actually detected, meaning there must be a fixed voltage accurate enough to use as a base for the rest of the system. Once again, the critical component of the system is the voltage reference, which sets the common mode for amplifiers, can be used to trigger comparators, and may be used to provide a stable supply to sensitive sensors. Most importantly, it sets the accuracy for the A/D and D/A converters.

THE MAIN CAUSES OF ERROR TO THE INTEGRITY OF THE SIGNAL CHAIN CAN BE DIVIDED INTO TWO CATEGORIES: INACCURACIES DUE TO NOISE AND INACCURACIES DUE TO SHIFTS IN VOLTAGE.

Key aspects to consider on a voltage reference include initial accuracy, drift over temperature, drift over time, and shift over radiation. Many voltage references provide trim options to adjust initial accuracy; however, the process requires external circuitry and may adversely affect the other specifications. A much simpler approach is to calibrate out the error on the digital side. Note that digital calibration reduces the total input signal voltage range by the amount of the error. Bandgap references can be found with an initial accuracy within hundredths of a percent before radiation.

Drift over temperature in precision voltage references is caused by imperfections in the elements making up the device and is not linear. The uncompensated curve of a bandgap reference is about 20 ppm. One solution to improve the temperature coefficient of the device is to use translinear circuitry to compensate for the curve by adding an exponential term to the current summation. With curve compensation, a designer is able to achieve a temperature coefficient lower than 3 ppm.

Drift over time is independent of other shifts and occurs predominantly toward the beginning of the life of the reference. Thus, initial calibration does not help correct for this drift. Calibration after an initial burn-in period is an option, albeit at the expense of the burn-in time. Moreover, the cascade design for creating a bandgap reference does not only

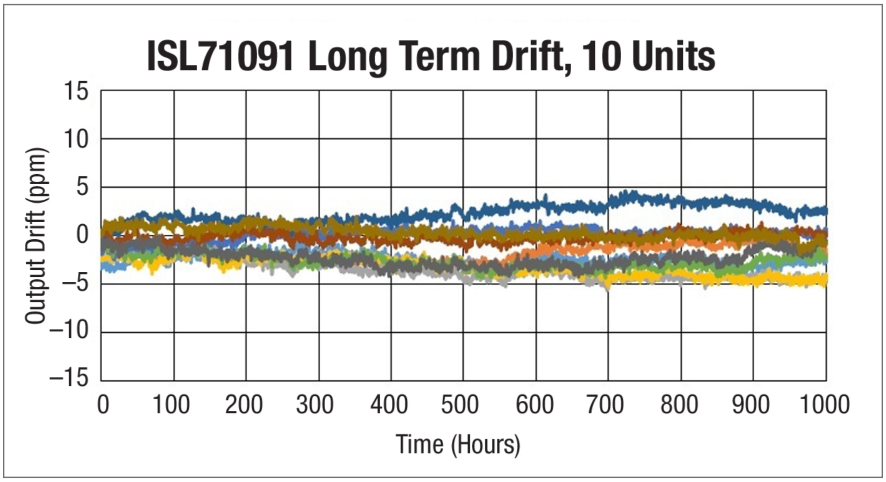


Figure 2 | ISL71091 voltage reference long-term drift.

help reduce noise, but it also has been found to reduce the long-term drift as well. The improved drift performance is seen in Figure 2.

Shifts due to radiation are critical in space applications. Many voltage references provide excellent accuracy in industrial environments but have large shifts when exposed to radiation. Research has shown that low-dose-rate radiation best mimics the actual conditions in space. Low dose rate used in testing is typically 10 mrad(Si)/s. While this is a higher rate compared to the naturally occurring radiation in space, it is a compromise between the time needed to complete the radiation testing and the dose rate chosen. Testing at high dose rates (50-300 rad(Si)/s) can produce secondary effects due to the accelerated nature of the dose rate. It is highly recommended to select devices that have undergone both low-dose and high-dose-rate radiation testing on a wafer-by-wafer basis. Radiation hardening is achieved both through design and also through the process used in creating the device. A good solution for a radiation-tolerant process is to have the transistors oxide-isolated and diffused neither too shallow so as to be sensitive to radiation-damaged oxides, nor diffused so deeply as to increase layout size and lower frequency responses. Table 1 shows a comparison of key specifications over radiation of three of the top competing voltage references.

Voltage references directly affect signal integrity because they are used as the standard that the signal is compared to when it is converted from the analog domain to the digital domain. Calibration and compensation methods exist, but are often expensive and may consume significant board space. New designs, testing, and wafer process techniques, like those used in Intersil's ISL71090 and ISL71091 voltage references (shown in Figure 3), are improving specifications and minimizing or even eliminating the need for calibration. **MES**

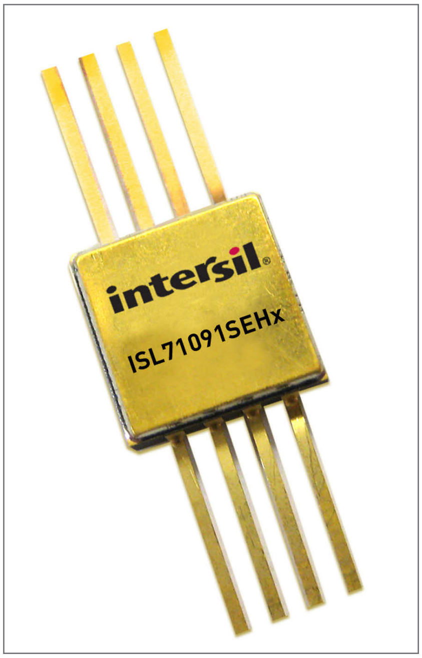
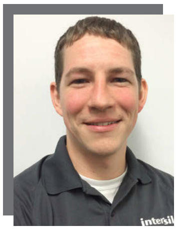


Figure 3 | ISL71091SEH voltage references ensure signal-processing integrity and improve voltage accuracy in satellite applications. (Photo courtesy of Intersil Corp.)



Dan Goodhew *is an Applications Engineer for Precision Products at Intersil Corp. He specializes in precision op amps and voltage references, both commercial and radiation-hardened, along with digitally controlled potentiometers and their application in data-acquisition systems. He holds a BSEE from the University of Central Florida. Readers may reach him at dgoodhew@intersil.com.*

Intersil Corp
408-432-8888
www.intersil.com

Device	ISL71090SEH	ISL71091SEH	Competitor A	Competitor B
Radiation Testing	Low dose and high dose rate tested on each wafer	Low dose and high dose rate tested on each wafer	High dose rate tested	Low dose and high dose rate tested
0.1 Hz to 10 Hz Peak-to-Peak Noise	0.8 ppm typical	1.6 ppm typical	1.6 ppm typical	Not specified
Initial Accuracy	±0.175% Max (2.5V option)	±0.25% Max	±0.2% Max	±0.2% Max
Temperature Coefficient	10 ppm/°C Max	6 ppm/°C Max	15 ppm/°C Max	33 ppm/°C Max
Long-Term Drift	15 ppm/kHr typical	20 ppm/kHr typical	Not specified	20 ppm/kHr typical

Table 1 | Comparison of top voltage references for space applications.

Military Communications Product Spotlights

Swiss Made Firewall and VPN Router

- Wide input 8-36VDC
- 3x Gigabit Ethernet
- Ext. temp. -40°C to +85°C
- Customizable alum housing (175x182x60mm)
- mini PCI slot for WLAN, GPRS, ... expansion
- Open WRT pre-installed, configurable

MPL High-Tech • Made in Switzerland

MPL AG Switzerland
+41 56 483 34 34
info@mpl.ch
www.mpl.ch

Protocol Converters

- Already Qualified! (MIL-STD-461, MIL-STD-704, MIL-STD-810, MIL-E-5400T)
- ARINC 429, MIL-STD-1553, RS-232/422, SYNCHRO, CSDB
- Multi-Protocol
- Firmware allows the unit to operate completely transparent – acting as bridge between systems
- Operates from 28vDC
- Custom designs with little or no NRE with minimum quantity order

KIMDU CORPORATION

Kimdu Corporation
1-800-677-6174
www.kimducorp.com
sales@kimducorp.com

ATS3000 Series Electronic Communications Test Solutions

- Field-Portable or Bench-Top Solutions
- Synthetic Instrumentation
- Net-Centric Capability
- Front-Line Diagnostic or Depot Test
- Standalone or Automated System
- Supports Radio, Avionics, Navigation, and Electronic Warfare Systems

ASTRONICS TEST SYSTEMS

www.AstronicsTestSystems.com

Configurable Communications Systems

- Remote Interface Unit
- Intel, PowerPC and ARM options
- 10/100/1000Base-T
- High density configurable data & I/O interfaces
  - MIL-STD-1553
  - RS-232, 422/485, 423
  - MIL-STD-188C
  - ARINC 429/575, CANBus
- Rugged, conduction cooled
  - MIL-STD-461
  - MIL-STD-810
- 28VDC & AC input options

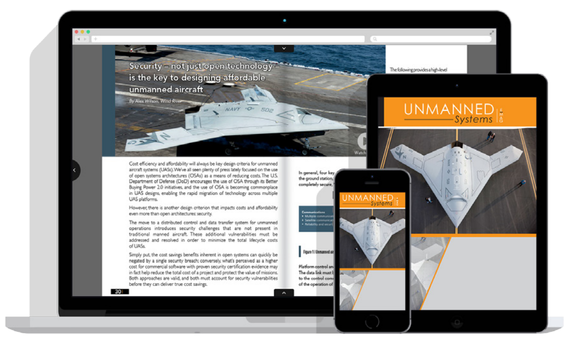
North Atlantic Industries
Accelerate Your Time-to-Mission

North Atlantic Industries, Inc.
www.naii.com

UNMANNED Systems E-MAG

OpenSystems media™

The Unmanned Systems E-mag brought to you by Military Embedded Systems targets trends and technology in autonomous vehicles, from SWaP-constrained UAS payloads and software certification to the disruptive regulatory and market impact of unmanned systems outside the defense sector.



Read it now!
http://opsy.st/Unmanned2014

Secure smartphones enable warfighters to operate more safely

Q&A with Chip Downing, Wind River

MIL EMBEDDED: ***Military leaders want to bring commercial smartphone technology to the warfighter. How can virtualization solve the security challenges inherent in these devices to make that possible?***

DOWNING: Enabling today's warfighter with advanced communications and situational awareness is the foundation of a successful mission. There is a long history of radios in the field using highly optimized, specialized equipment. However, due to rapid advancement of commercial mobile communications along with budget constraints, next generation military communication systems will be composed from commercial-off-the-shelf (COTS) hardware (handsets and tablets) and software components designed to leverage the latest advances in network communications.

Communications on the battlefield have always carried high risk and today's smartphones have exacerbated this risk. Although there are many technologies that will enable smartphones on the battlefield, the critical technologies that overshadow all others in utility are those that secure the device for the intended user(s) and its end-to-end communications to geographically dispersed C3I systems. No singular technology or architecture can adequately protect the warfighter and the critical information on the device – a multi-layered approach to security is required starting when power is applied that maintains a foundation of trust throughout the lifecycle of the device while in mission mode.

Single level security (SLS) radio devices are prevalent today, but next generation mobile communications devices will need to support a wide range of communications channels from multiple services, agencies and sensors, and be able to rapidly include communications with trusted coalition partners. In the past, multiple channels meant multiple hardware platforms. However in the future, mixed communications environments must be supported by a single hardware platform that can securely separate and control the flow of information through the device.

This security is neither simple nor free. For example, these are just a few technologies that are needed to ensure security of the device:

1. Virtualization technologies and separation kernels with secure partitioning and clear domain indicators
2. Support for multiple user personalities with independent security policies
3. Hardware and/or software root-of-trust
4. Secure boot loader
5. Role-based access control
6. Data flow protection / enablement
7. Device / machine / user authentication
8. Software updates and patches
9. Independent data-at-rest (DAR) and data-in-transit (DIT) modules
10. Hardware Integrity Verification, memory sanitization

Here is a look at a few of these capabilities in more detail:

- **Virtualization technologies and separation kernels (SKs):** These are paramount to the security of battlefield-ready smartphones. Virtualization technologies partition the device into virtual compute environments providing full management authority and access to hardware resources. This increases security by preventing operating systems and applications from directly accessing the physical hardware. Separation kernels harden the security of data and networks by locking down security domains into highly controlled virtual address spaces, and then strictly controlling the flow of information between the virtual environments.
- **Secure boot loader:** When power is first introduced to the device, the authenticity and integrity of the software on the device is verified using cryptographically generated digital signatures. This digital signature is then attached to the software image and verified by the device to ensure that only the software that has been authorized runs on that device.
- **Role-based access control:** Mandatory role-based access controls built into the operating system limit the privileges of device components/capabilities and applications so that access to these resources is only granted when required to perform their function, enforcing the principle of least privilege.
- **Device / machine authentication:** A secure smartphone may have many personalities, some of which may not be connected to human input. These autonomous processes need to authenticate, using role-based access control, with the smartphone prior to receiving or transmitting data in support of a human warfighter.
- **Software updates and patches:** Once a mobile device is in operation, it will need to receive hot patches and software updates. Military systems operators need to roll out patches, and devices need to authenticate them, in a way that does not consume bandwidth or impair the functional security of the device, or compromise the warfighter in any way.

Security cannot be thought of as an add-on to a smartphone – it is integral to the device's reliable function. Security must be addressed throughout the device lifecycle, from the initial design to the end of its operational environment. Next generation smartphones built with a wide array of protection mechanisms will enable warfighters to operate more safely in more challenging missions by having better situational awareness and communications to a wide range of manned and autonomous support resources.

***Chip Downing** is the Senior Director for Aerospace and Defense at Wind River. He can be contacted at chip.downing@windriver.com.*

Designing for forward and backward compatibility is key to managing obsolescence

By Michael Carter

Managing obsolete electronics is a challenge faced by every defense platform from Navy destroyers to Army tanks to Air Force combat aircraft. Pictured is the guided-missile destroyer USS Stockdale (DDG 106) steaming through the Pacific Ocean. DoD photo by U.S. Navy.

The military and defense community struggles with the issue of obsolescence as it works to accept new designs for COTS products. This environment requires suppliers, especially smaller ones, to innovate or die. But the outlook is not bleak for companies that are able to produce products with high value to the defense market. In an era of declining budgets, service-life extension of systems is critical to maintaining the operational availability of every ship and aircraft.

When a component or technology is forecast to go out of manufacture, technology suppliers typically provide ample notice to users relative to the date the item will no longer be available. Company management must be made aware of these situations and develop a plan to mitigate such an event. Product plans and development schedules must take into account the design-cycle time and the date that the item will no longer be available.

If there are no direct replacements for a particular item, the solution is to design out the obsolete item. In this case, users must be notified of the situation and given the opportunity to purchase the old design prior to the product's end of life (EOL). Users need a specific date past which the old design will no longer be available along with a schedule for when redesigned prototypes will be available for testing and general production release. Every user will require a different solution; few will simply accept a redesign with open arms.

Such is the nature of commercial off-the-shelf (COTS) technology. To mitigate user problems, the goal of a supplier should include designing a new product that is forward- and backward-compatible in performance, has the same physical size as the previous iteration, and contains the same connector interfaces as the design that is becoming obsolete. However, not all, if any, of these design goals may be achievable when addressing obsolescence.

To replace the notion of "obsolescence," a set of systematic evaluation, design, and review processes must be generated and implemented. Design standards and practices should be continuously evolving, with the goal of meeting performance requirements, providing a long product life cycle, reducing design-cycle time, and improving manufacturability and testability.

Stringent design and development procedures

The use of robust design processes is well-suited to meet these objectives. Product design and development procedures and processes are complex and must establish design requirements for, or to meet, the following:

- Market requirements
- Performance specifications
- Design-process documentation and control
- Regulatory requirements

- Thermal performance
- Environmental performance and qualification
- Hardware and software qualification
- Design reviews
- Material and manufacturing cost
- Mechanical design, including geometric dimensioning and tolerances
- Tooling
- Design for mechanical assembly
- Printed circuit board design and review criteria
- Component selection and analysis
- Component footprints, orientation, and placement
- Printed circuit board assembly manufacturability
- Printed circuit board assembly design for test
- Systems test
- Packaging

Company management has responsibility to manage the cost, schedule, and performance requirements of all design efforts. The development and management of budgets, activity schedules, and design verification is mandatory for successful design processes. Design-cycle time can be reduced and on time release can be improved by implementing "Figure of Merit" and "Dynamic Cycle Time" reduction techniques during the engineering phase.

Although not an approach to be taken without adequate customer notification, one way COTS suppliers can manage obsolescence is by forcing new technology adoption. Even with advance notice and information, many users do not plan for the loss of supply of products affected by obsolescence.

Examples of users' responses who are unhappy about potential or upcoming loss of product supply can include:

"No, we won't allow it." "Buy all the items going end of life and stock them at your expense for us." Sometimes it's "Buy all the items going end of life, build completed boards and systems, and stock them for us at your expense." Or perhaps "Buy the quantity of items going end of life we need for our program and stock them at your expense for us." Some have heard "Buy the quantity of items going end of life we need for our program, build boards and systems and stock them at your expense for us," Or the ever-popular "Why can't you control the supplier?"

Obviously, these responses are from users who have not planned for the loss of supply. COTS product and system suppliers are faced with the obsolescence dilemma every day. Beyond advance notice and specific dates of availability, methods used to mitigate negative impacts include the purchase of the technology going EOL based on historical usage, forecast demand, and customer input.

Unfortunately, real-world experience shows that many users are unable or unwilling to provide a forecast for future demand. In addition, few are willing to buy components and associated products that have items going EOL.

Nonetheless, suppliers who make new design prototypes available for test and evaluation by users at specified dates will give the users the opportunity to integrate the new design into their products and systems. The time required to evaluate the new design is dependent on the magnitude of design and configuration changes.

Those who work with suppliers on obsolescence issues will be ahead of the curve, while those who do not will see a negative impact. Ultimately, when supply is gone, it is gone for good and users will be forced to adopt the new technology.

New designs cost money. Who pays for the new design? The COTS supplier does in most cases. The decision to start a new design to replace obsolete

	Sales	Cost of Goods	Profit	Cumulative Profit	ROI
Year 1	$2,000,000	$1,600,000	$400,000	$400,000	20%
Year 2	$3,000,000	$2,400,000	$600,000	$1,000,000	50%
Year 3	$4,000,000	$3,200,000	$800,000	$1,800,000	90%
Year 4	$4,000,000	$3,200,000	$800,000	$2,600,000	130%
NRE Cost:	$2,000,000				

Table 1 | Example ROI of an aging FPGA.

technology is one of economics. If development costs are not supported by an adequate return on investment (ROI) a supplier may decide to discontinue the product or system entirely.

Consider the following example: A major FPGA supplier announces the EOL of an aging FPGA that is used by a COTS supplier. The COTS supplier's engineering department develops a plan, including cost, schedule, and performance elements to replace the FPGA. The cost of the design is determined to be $2 million.

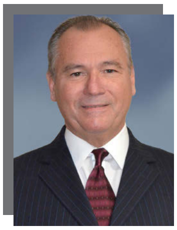
The COTS supplier's sales and marketing departments determine the total demand for the product to be $2 million the first year after the new product is released, $3 million in the second year, and $4 million in year three. Sales in year four are forecast to be $3 million, with sales in decline in the years thereafter.

The operations department of the COTS supplier determines the total cost of goods sold of the product to be 80 percent of the sales price (see Table 1). In this example, the ROI is over three years. Because of the unacceptable ROI, executive management should not approve the design.

Development costs must be supported by an appropriate ROI and are amortized as part of cost of goods sold. If the ROI of a part development is two years or less, designing out obsolescence has a chance.

COTS obsolescence is increasingly migrating to the adoption of platform architecture but not necessarily in legacy configurations. As older systems are not supported, or even available, military program executive officers and contracting officers are looking to COTS technology for systems emulation through hardware and software. Recently, legacy-system emulation and data translation is being driven to be a complete software simulation running on new generation servers.

Obsolescence in COTS technology is not slowing down; it is speeding up. COTS suppliers in the mainstream can be proactive in addressing its impact while supporting both users and the military and defense industry. **MES**



***Michael Carter** is the CEO of IXI (formerly Sabtech). He is an industry veteran with more than 30 years of technology and product-development experience. He has developed systems and technology employed in early warning, fire control, navigation, embedded computing, servers, data I/O, communications, and power control. Readers may reach him at michaelcarter@ixitech.com.*

IXI (formerly Sabtech) • 714-692-3800 • www.sabtech.com

A volatile supply chain: What is in your future?

By Kaye Porter

More than ever, programs require ongoing collaboration between industry and government teams. As a result, the Department of Defense finds itself dealing with international supply chains two and three tiers deep. The F-35 Joint Strike Fighter partners with thousands of suppliers and nine partner countries. (Photo by Rennett Stowe, licensed under Creative Commons.)

Defense programs are growing in complexity. Not only are programs becoming more complicated, but the supply chain has become volatile and difficult to navigate. The F-35 Joint Strike Fighter aircraft alone partners with more than 1,200 domestic suppliers and nine "partner countries" to produce "thousands of components from highly sophisticated radar sensors to the aircraft's mid fuselage."[1] In 2010, the United States stopped being the world's leading high-technology exporter, and as a result more manufacturing now occurs overseas. This shift puts the supply chain for both defense and commercial technology at risk from threats that designers have limited control over, such as natural disasters, obsolescence, and counterfeit electronics.

In 2011, several natural disasters hit Asia. Suppliers and subcontractors found themselves needing to manage a decreased supply of memory, capacitors, and hard disks and the consequential project delays and increased costs. In fact, one study stated that a full 85 percent of companies reported at least one supply-chain disruption in 2011, with about 50 percent dealing with more than one disruption. In cases where warfighter readiness is critical, this puts depots and primes in a high-risk situation where product availability is decreased and they are forced to compete with commercial demand. This dilemma creates a prime environment for budget disruption and increased counterfeit risk, even on active (non-legacy) electronics.

Even the U.S. domestic supply chain is vulnerable. While the Department of Defense (DoD) encourages large primes to partner with smaller companies whose expertise can bring a competitive advantage to the warfighter, small businesses struggle with often intricate requirements, long contract approval cycles, and heavy investments into meeting the needed government standards. Today, few small businesses can afford to rely on government contracts alone, and must also compete with commercial manufacturing overseas. These smaller businesses may be forced to reevaluate whether they are able to remain active in the defense supply chain.

If a company can no longer thrive in the current environment, the DoD risks losing access to critical technology necessary to a program. Similar to losing designs due to obsolescence, the loss of small, innovative companies forces program managers to evaluate alternative sources and determine whether an overseas supplier can be trusted. With the supply chain becoming increasingly

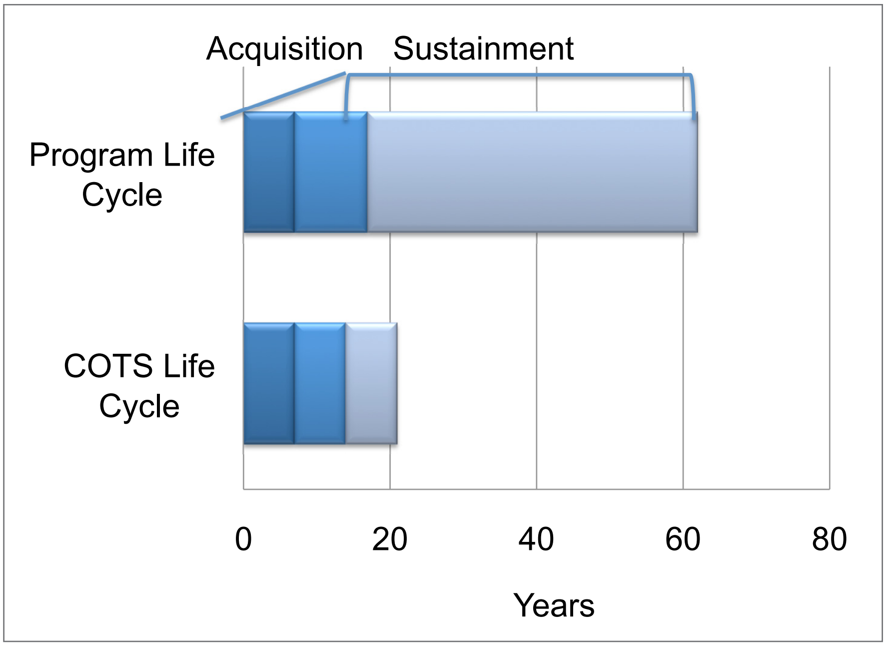


Figure 1 | A program taking 10-15 years before reaching production can see as many as three generations becoming obsolete. End-of-life of microelectronics rolls up into boards, creating the "waterfall effect," thereby creating a gap between new technology and ongoing product demand.

fragile and the growing threat of cyber-terrorism, the need to aggressively protect programs becomes more and more challenging.

A comprehensive sector-by-sector, tier-by-tier study, dubbed the "S2T2" has revealed a rapidly weakening manufacturing industrial base. Supporting these revelations, the 2012 Annual Industrial Capabilities Report to Congress demonstrates that systems across the DoD are being negatively affected by the loss of medium and small domestic manufacturers who, due to the current acquisition and financial environment, have stopped doing business with the government altogether.

Counterfeit: The supply chain's response to ongoing demand

Both acquisition and sustainment teams have been tasked with providing the best technology to the warfighter, while maintaining predictable affordability. However, defense programs have notoriously longer life cycles than commercial products[2]. Started in 2007, the Joint Air-to-Ground Missile (JAGM) program is still in development and as a result is vulnerable to demand-related obsolescence. The average commercial off-the-shelf (COTS) life cycle is five to seven years, leaving programs vulnerable to obsolescence risks while still in development. This constitutes a real problem as reported by the 2012 Annual Industrial Capabilities Report, which states that "most of the R&D funding in the munitions and missile sector is associated with legacy program upgrades or modifications that limit competitive opportunities…the Department remains concerned that the industrial design engineering capabilities needed for these systems may not be readily available should the sector atrophy in the absence of demand."

Engineering capability and component availability are not the only problems plaguing these programs, however; counterfeits have emerged as the supply chain's answer to ongoing demand. In 2012, the National Defense Authorization Act, Sec. 818, outlined the growing threat of counterfeit electronics in the supply chain. In 2014, the Defense Federal Acquisition Regulation Supplement (DFARS) released additional guidance specifically outlining and addressing obsolescence as a risk to the defense supply chain with the following definition of what an obsolete part is:

"'An electronic part that is no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the design activity or original manufacturer.' Obsolescence control is a fundamental aspect of counterfeit prevention and should be addressed by the contractor in its counterfeit detection and avoidance system."[3]

Supply-chain management: From acquisition to phase-out

A program that takes 10-15 years before reaching production can see as many as three generations becoming obsolete. End-of-life (EOL) of microelectronics rolls up into the board sector, in the "waterfall effect" – creating a gap between new technology and ongoing product demand (see Figure 1).

Today's sustainment teams are being tasked with ensuring readiness while balancing affordability and modernization. Although requirements outlining obsolescence risk management must be written to take into account a program's life cycle, solutions are often underfunded and brought in too late to manage the realities of the current supply chain. To stay competitive in a highly demanding market, component manufacturers EOL their products, which forces computing suppliers to EOL their respective products, which then forces equipment suppliers and engineers to scramble for long-term support solutions to avoid ongoing counterfeit and obsolescence risks.

> THE AVERAGE COMMERCIAL OFF-THE-SHELF (COTS) LIFE CYCLE IS FIVE TO SEVEN YEARS, LEAVING PROGRAMS VULNERABLE TO OBSOLESCENCE RISKS WHILE STILL IN DEVELOPMENT.

Managing acquisition of a new program often involves aligning requirements, budget, and processes, all of which can have different timelines. In order to effectively manage the supply chain throughout each phase, it is critical to understand the inherent risk and have solutions developed in parallel as new technology is developed.

Risk: How much is too much?

No system, application, or program is immune to obsolescence issues. Although sustainment teams are pressed to be proactive, program managers, engineers, and life cycle logisticians (including supply-chain managers and inventory managers) typically manage the problem only after an EOL event has already occurred. As a result, few teams have the opportunity to effectively head off obsolescence risk and EOL problems, as they are often engaged too late in the process to be proactive.

Obsolescence is both a symptom and a driver of a fragile supply chain. As a result, it is critical for a team to understand the nature of the risks it faces, and also to be aware of which program pieces are likely most vulnerable. Without understanding the risks, teams find themselves in the reactive position of having to address each issue as it comes up. Having an understanding of how risk-tolerant the system components are can help teams outline a comprehensive plan that takes both readiness and affordability into account. Teams can collaborate with legacy partners to ensure that programs have an internal, organic capability to resolve

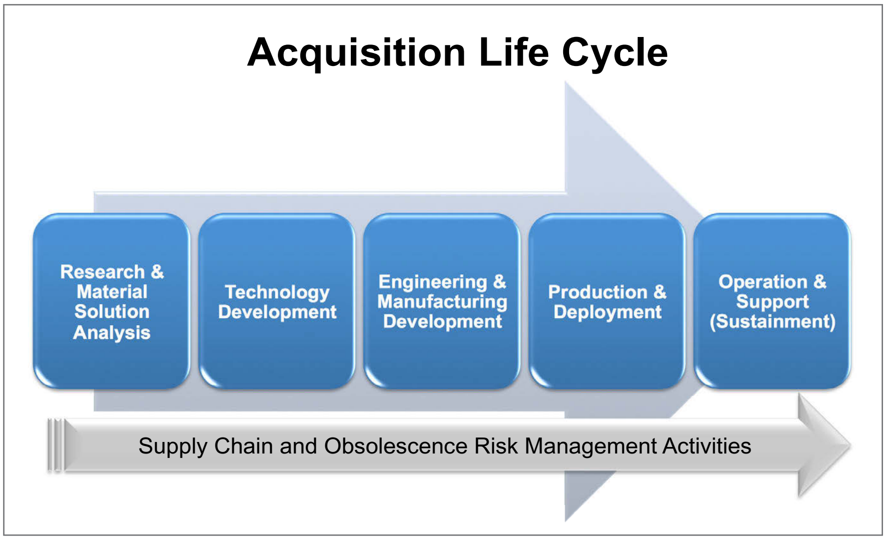
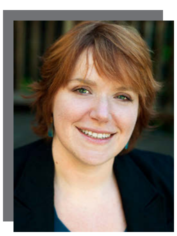


Figure 2 | In order to manage the volatile nature of the supply chain, sustainment activities cannot wait until after full operations capability is established, but instead need to be integrated early in the acquisition life cycle. Once run in conjunction with research and development teams, supply-chain and obsolescence risk-management solutions can be developed and deployed proactively.

these issues. Money can be set aside to redesign areas that are most vulnerable, while low-risk areas can take advantage of substitutions, emulation, and possibly refurbished parts.

In order to manage the volatile nature of the supply chain, sustainment activities cannot wait until after full operational capability is established, but instead need to be integrated early in the acquisition life cycle (see Figure 2). Once they are run in conjunction with research and development teams, supply-chain and obsolescence risk-management solutions can be developed and deployed proactively.

In the face of a volatile supply chain, sustainment activities need to be planned before parts run out and the warfighter faces the risk of equipment no longer available due to supply disruption. While obsolescence management traditionally starts after products are EOL, having a plan to address risks from the perspective of total life cycle management must begin in the design and development phase. Having an ongoing legacy-sustainment plan in place during the acquisition phase to address the issues of obsolescence will give sustainment teams a step up on managing the sometimes-fragile nature of the DoD supply chain. **MES**



***Kaye Porter** is Director of Marketing at GDCA. Her current focus is bringing awareness to the embedded industry on the critical issues of obsolescence, legacy, and the realities of long-term product support. She can be reached at kporter@gdca.com.*

GDCA • 925-456-9900 • www.gdca.com

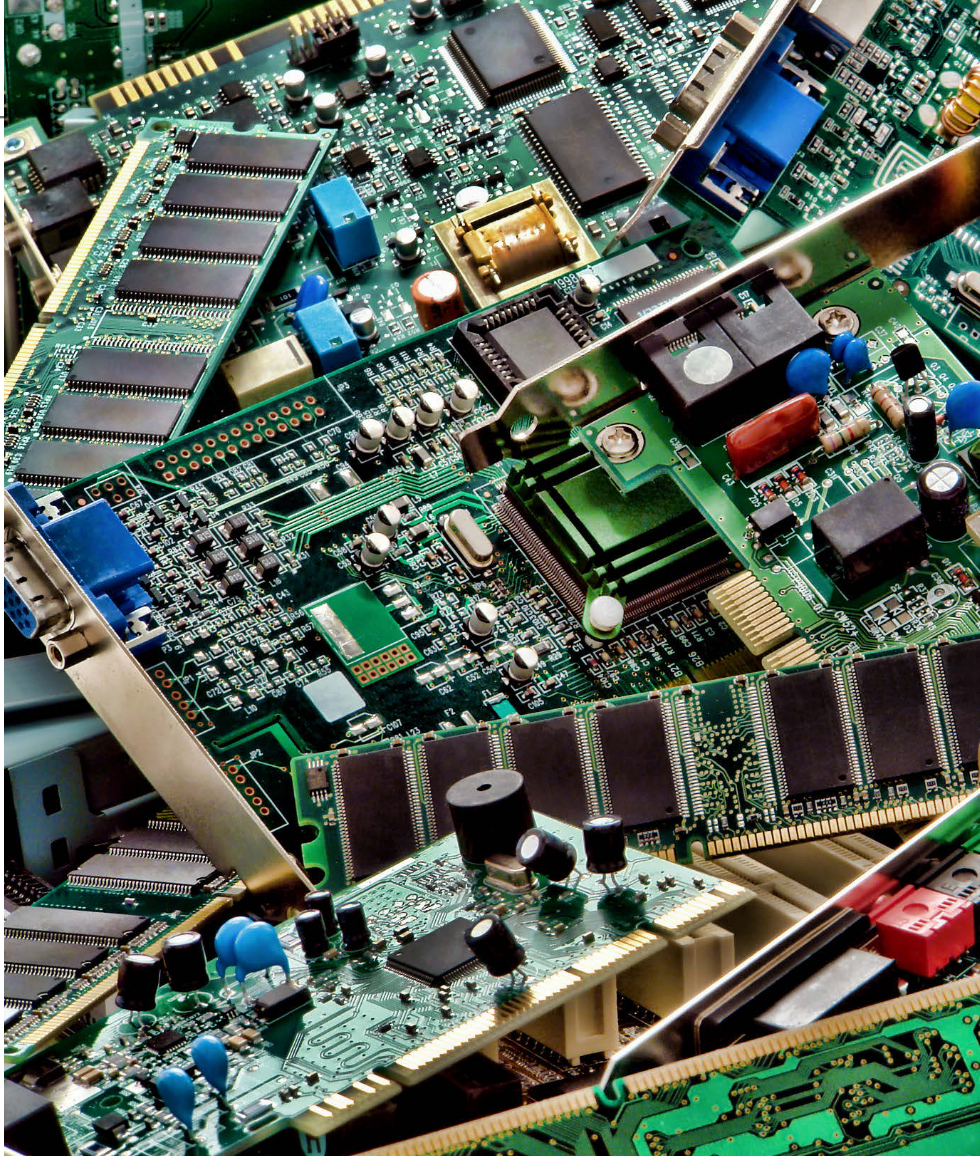
References:

1 Lockheed Martin, F-35 Lightning, "Powering Job Creation for America and its Allies" (https://www.f35.com/about/economic-impact)

2 Annual Industrial Capabilities Report to Congress, August 2012 (Some products and services sold by companies in the defense industrial base are unique to defense applications, while most have substantial levels of non-defense demand or are sold exclusively on commercial terms such that the supplier may not even know that the product is used in military systems. Likewise, the military may not know it depends upon a primarily commercial component.)

3 DFARS 246.870-2(b)(12) and paragraph (c)(12) of the clause at DFARS 252.246-7007.

MANAGING THE SUPPLY CHAIN: OBSOLESCENCE AND COUNTERFEITS



Counterfeit threat taking malicious turn?

By Don Sawyer

In June 2014, an American contractor from Massachusetts admitted to conspiring to traffic counterfeit military goods for his role in shipping counterfeit semiconductors from Hong Kong to a U.S. Navy submarine base in Connecticut. The chips – sold as new – were actually refurbished and remarked. Had this criminal scheme not been thwarted, the parts would have been installed in nuclear submarines. The catastrophic potential cannot be overstated.

One could say we all got lucky in this instance, but luck had nothing to do with it. Coordinated actions within and between federal and state lawmakers and law enforcement, as well as various electronics industry organizations and representatives, have put a spotlight on the once-veiled counterfeit component issue. With the National Defense Authorization Act (NDAA) rule on the Detection and Avoidance of Counterfeit Electronic Parts finally in effect, the mil/aero sector is now better equipped than ever before to stem the flow of fraudulent chips into the supply chain.

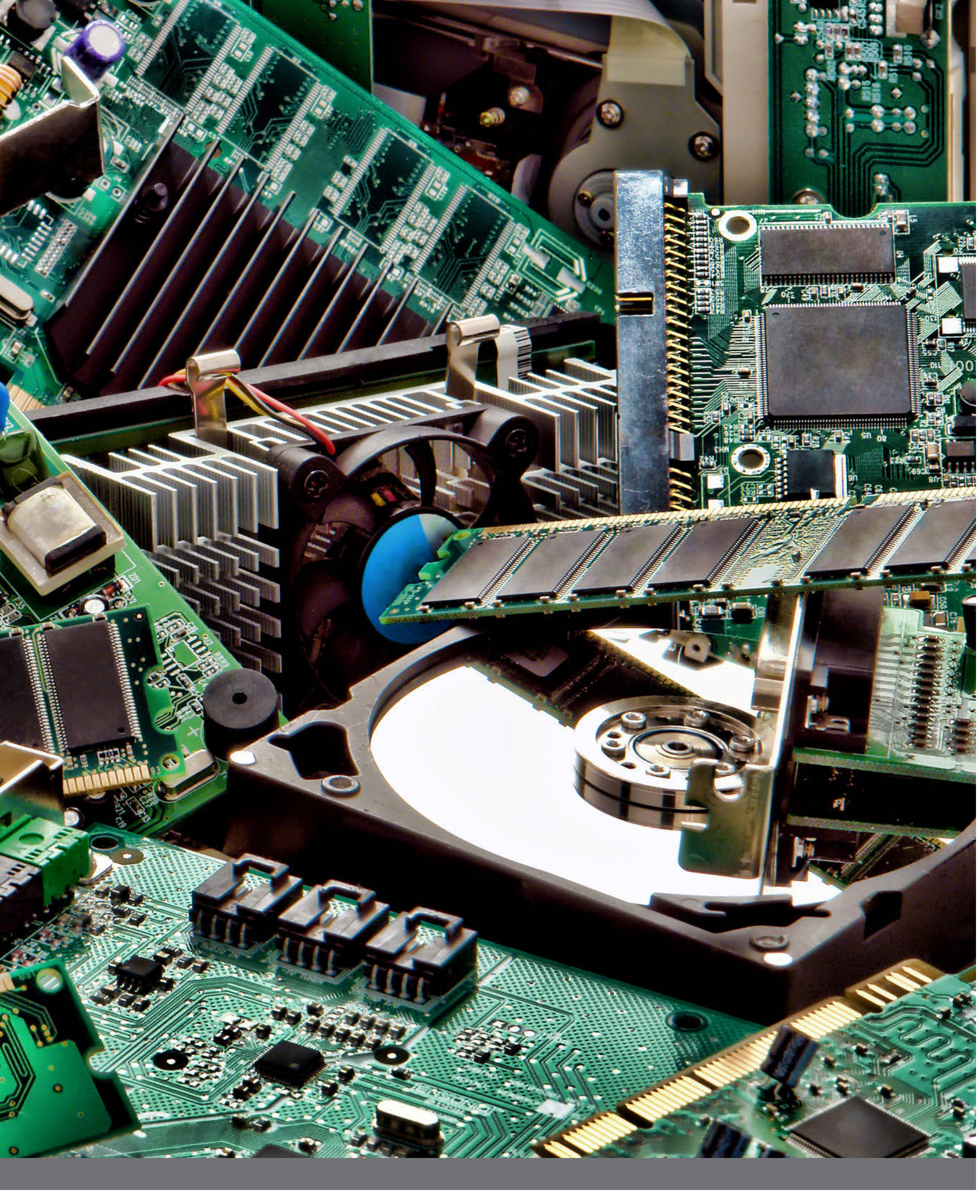
Cyber setback

That's the good news. The bad news is that as the threat landscape evolves, current anti-counterfeit defenses may prove inadequate. Today, the vast majority of the safeguards within the supply chain are predicated on the assumption that profit is the primary motive of these perpetrators; therefore, detection strategies focus on the identification of parts that have been reclaimed, remarked, re-engineered, or otherwise fraudulently represented. A lesser-known, but significantly more ominous threat, is the potential for malicious counterfeits.

In a case like this, chips are intentionally altered during the IC design process to insert malignant functionality into the code before it is manufactured. The tainted code remains dormant in the device until it is triggered to launch a cyberattack that may intercept classified intelligence or compromise critical infrastructure capabilities. Because it does not initially impede the normal functioning of the chip, this kind of tampering is unlikely to be detected via standard inspection and testing protocols.

Malicious counterfeiting is not a new threat, and most discourse about it is largely theoretical, but the increasing globalization and complexity of the semiconductor supply chain leaves the U.S military "uncomfortably dependent on foreign sources for the critical components that underpin our war-fighting capability," according to Sonny Maynard, program manager of the Department of Defense (DoD) Trusted Foundry initiative.

Programs like Trusted Foundry have helped insulate the DoD from this exposure, but the mil/aero sector's reliance on commercial off-the-shelf (COTS) components limits the benefit. Securing the commercial semiconductor supply chain is significantly more challenging due to the offshore outsourcing of IC design and fabrication. As a result, chip design represents "a gaping and exploitable hole" in the current approach to supply chain security, according to a paper by John Villasenor, senior fellow in



Governance Studies and the Center for Technology Innovation at the Brookings Institute. Figure 1 shows the goals, attack method, and attacker location of possible breaches of cybersecurity.

Statement of work

At this point, it may sound like there is a whole lot more bad news than good news. Let's look at it this way: There are many promising solutions on the horizon that could dramatically mitigate the threat of both fraudulent and malicious electronic components in the future. In addition, members of the supply chain can take action now to better protect our economic interests and national security.

The first step is acknowledging that the counterfeit threat is bigger – and more malevolent – than most members of the commercial supply chain have previously realized. The threat exists both upstream and downstream; therefore, a comprehensive anti-counterfeit strategy must include buy-in from all members of the supply chain. Such a strategy must also confront exposures throughout the entire life cycle – from cradle (secure IC design) to grave (ethical e-waste disposal) and everything in between, including Trusted Foundry, proactive technology management, responsible sourcing, and secure logistics.

Without the benefit of a resource like the Trusted Foundry program, members of the IC supply chain must be particularly vigilant in their efforts to defend against chip tampering at the design level. Greater awareness of the risk should prompt more stringent vetting of offshore suppliers and their subcontractors, together with improvements in testing and verification methods.

Secure by design

The Semiconductor Research Corporation, a leading university-research consortium, is working with the National Science Foundation on a $9 million joint research effort called Secure, Trustworthy, Assured, and Resilient Semiconductors and Systems (STARSS). The stated goal of this group is to develop new strategies for IC architecture, specification, and verification that will provide "assurance and confidence

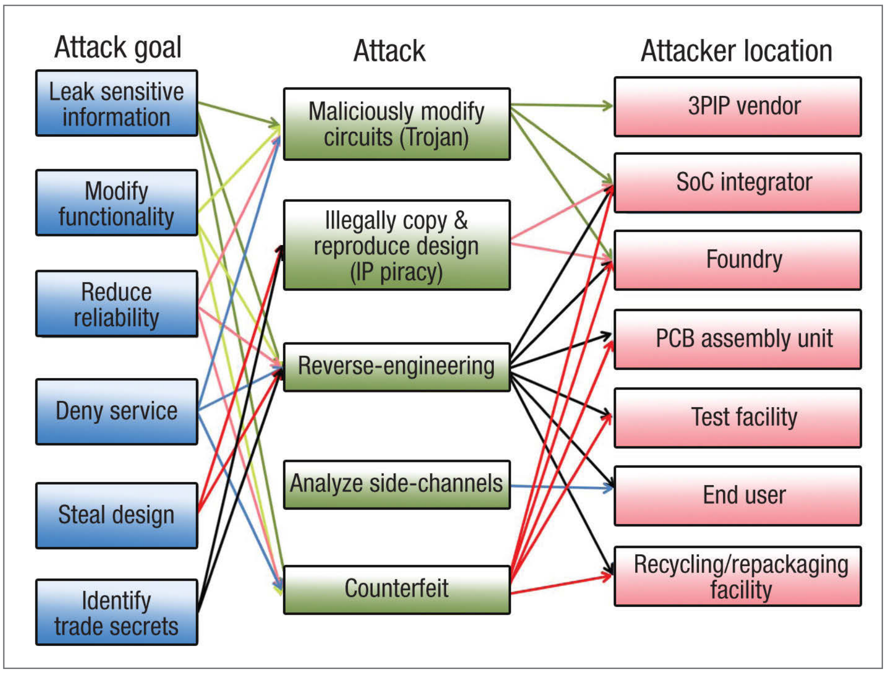


Figure 1 | The left column shows the goals of the attack, while the right column shows the location of the attacker. (Source: Rostami et al., A primer on Hardware Security: Models, Methods, and Metrics, Vol. 102, No. 8, August 2014, Proceedings of the IEEE 1285.)

in the trustworthiness, reliability, and security of electronic systems, strategies, and techniques that incorporate security in all stages of design and manufacture."

Adaptations to the chip-fabrication process could also enable the U.S. to leverage global semiconductor manufacturing capacity while still protecting design integrity. The Intelligence Advanced Research Projects Activity (IARPA) government research agency – part of the Office of the Director of National Intelligence – is said to be investigating the feasibility of an advanced chipmaking technology under its Trusted Integrated Chips program that entails what it calls the "split-manufacturing" process. This method would divide chip fabrication into Front-End-of-Line (FEOL) manufacturing, consisting of transistor layers to be fabricated by offshore foundries, and Back-End-of-Line (BEOL) development, with pieces that would be fabricated by trusted U.S. facilities.

Breaking the cycle

As initiatives to more firmly secure IC-level hardware progress, it is incumbent upon the rest of the supply chain to continue to actively support the anti-counterfeit movement within our respective domains.

It has been well documented that counterfeit components are most often introduced into the supply chain through non-authorized, gray market sources. A 2012 report from the DoD stated that the "overwhelming majority" of the more than one million counterfeit parts identified in an investigation of the DoD's supply chain were sourced from independent electronic parts distributors.

Since part obsolescence is a known trigger for the less-than-vigilant sourcing practices that drive buyers to the gray market, it stands to reason that avoiding obsolescence will go a long way toward mitigating the counterfeit risk.

Defense systems engineers can help minimize these part crises through more proactive technology planning and management. Using resources like the Government-Industry Data Exchange Program (GIDEP), designers can assure that they are specifying products offering the greatest life cycle support. Designers can also avert obsolescence by designing with open architecture, which allows for easier part replacement; by proactively planning new technology insertion through the production and support life of the program; and by sourcing "COTS+" parts with enhanced performance and extended product life cycle support.

Still, there will be occasions when the authorized channel cannot fulfill customer demand for legacy parts. This is typically where panic begins and procurement discipline ends. Rather than taking that dive into the murky waters of the Internet broker market, those looking for product can talk to companies like Rochester Electronics, e2v, and Micross Components, who develop authorizations to manufacture pedigreed and traceable products using original die, IP, test fixtures, and some of the identical packaging subcontractors used by the original component manufacturers (OCMs) themselves. Although this option has traditionally been considered too costly, advancements in both technology and cooperation between OCMs, distributors, and aftermarket suppliers are now making this a much more cost-effective alternative.

Support the troops

As a franchised distributor, Avnet is confident in the pedigree of its product while recognizing that every time a part changes hands – whether through the returns process, testing in an outside lab, warranty/repair work or other physical value add – it is vulnerable to tampering. Avnet's policy, therefore, is trust, but verify. The company maintains a materials-control process that includes traceability mechanisms such as barcodes and date coding, which provides assurance that the chain of custody remains secure. The company also audits the materials-handling and return policies of its supplier partners.

To assure that designers can satisfy their bill-of-materials requirements without risking the integrity of their supply chain, Avnet offers inventory and product-lifecycle-management support, executes end-of-life bridge buys to assure ongoing supply, and works with suppliers to develop product continuity programs, assuring longer-term manufacture and supply of components.

Going all in

The supply chain's approach to the counterfeit issue can almost be regarded as a dam with a number of individuals working feverishly to plug a few gaping holes, while countless smaller leaks go largely unnoticed. To win the battle against counterfeits, the industry has to be more vigilant in identifying weak points throughout the supply chain and use its collective strength to secure these breaches before it's too late. What appears to be an insignificant trickle today could become a life-threatening flood tomorrow. **MES**

***Don Sawyer** is a supply chain and quality systems expert with more than 25 years of experience in the electronics industry including time spent in the automotive, microelectronics, military, aerospace, industrial, and contract manufacturing sectors. Don joined Avnet in 2012 as director of quality for the defense/aerospace group with responsibility for ensuring incoming and outgoing quality of electronic components within Avnet's supply chain. Prior to Avnet, Don worked for companies such as STMicroelectronics and Ford Motor Company. He holds a BS degree in Electronic Engineering from Colorado Technical University. Readers may reach him at Don.Sawyer@avnet.com.*

Avnet
1-800-409-1483 • www.avnet.com

Mission critical displays – how to keep them running

LUMINEQ® POWERED BY Beneq

MIL EMBEDDED: ***What can Lumineq Displays offer for the harsh requirements of military applications?***

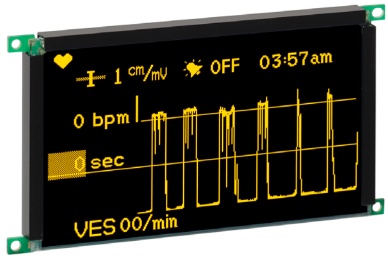
Designed to deliver

While looking at the specifications of our displays, it quickly becomes apparent why very demanding applications are our core business. We deliver to projects where demands exceed the capabilities of most commercial displays available today. We take pride in delivering rugged tools for crystal clear visual communication, regardless of the conditions. For example, our displays exhibit instant-ON down to -60 °C, with no motion blur. Other extremes we tackle include humidity, vibration and pressure fluctuations.

We have been serving military display projects for the past 20 years. Since being introduced to the stringent requirements of military applications, TFEL displays have been used on land, at sea and in the air. Our plant has delivered more than 3 million displays during the past 30 years.

Broad product range

The TFEL portfolio of displays consists of several product lines. Sizes range from 3.1" (diagonal) to 10.4". Display resolutions start at 160 × 80 (columns × rows) and reach VGA 640 × 480. In addition, customers can chose from many options in order to tune their display. These include conformal coating, locking connectors, extended temperature range, dimming, anti-glare film, wide input voltage and different mounting options.



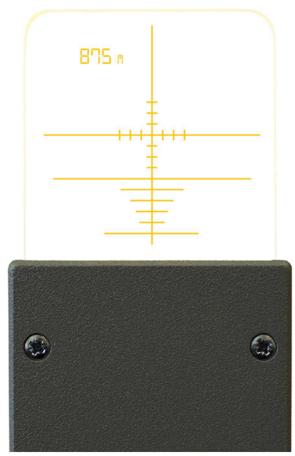
*The **EL240.128.45** houses a built-in LCD controller for easy interfacing with embedded systems.*
Mean time between failure (MTBF): 100,000 h

*The **EL320.240-FA3** is a multi-color display with AMLCD-type interface, 3 and 5 V logic compatible.*
Operating temperature range: -50 to +85 °C

*The **EL640.480-AM8** is designed for heavy industrial use in extreme low operating temperatures, down to -60 °C.*

Transparent displays you can really see through

Lumineq Displays has launched a line of transparent displays based on TFEL technology. These TASEL displays offer unbeaten see-through capabilities (transparency >80%) for optical peripherals, such as scopes and range finders. The complete self-emitting display structure is only 1.5 µm thick (excluding glass). On the right a TASEL example.



***Ari Tervonen** is Product Manager, Lumineq Displays, Beneq Products Oy. Contact him at ari.tervonen@beneq.com*

Lumineq Displays
+358 9 7599 530 • www.lumineq.com


SynQor
SynQor
SynQor

CHARITY

Veterans Workshop

Each month 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 and to back that up, our parent company – OpenSystems Media – will make a donation to each charity we showcase on this page.

This month we're featuring the Veterans Workshop, which is a veteran-operated organization that assists disabled veterans with technology-related job training and mainly work-from-home positions. Veterans Workshop is a 501(c)(3) charity organization that aims to improve the lives of injured or disabled veterans as they assimilate back into civilian life after duty. They mainly focus on providing workshops to blind, deaf, paralyzed, and unemployed veterans.

There are four teaching programs veterans can apply for on the website. These workshops include teaching blind veterans how to make phone calls for deaf veterans using Adobe connect virtual classroom technology; teaching deaf veterans to convert websites to be 508-compliant (equally accessible to people with disabilities); teaching paralyzed veterans how to communicate with technology; and teaching unemployed veterans a new skill that will benefit them in the workplace. According to the website, www.vetsworkshop.org, most of the training will allow vets to get a job within three months or less, with the benefit of most of the positions being in the IT sector, where vets can work from the comfort of their own homes.

Some of the jobs available to vets who complete the training include: Blind Relay Operator; Certified Salesforce Administrator; Technical Support; Video and Image Interpretation; ADA 508 Compliance Validator; Eye Tracking Communication Specialist; Social Media Analyst; and more.

All of these programs are free to qualified veterans and are available due to donations. These not only include monetary donations, but other forms such as donating your car, boat, truck, or RV via Kars4Vets; volunteering with a project or providing programming knowledge; and donating computer equipment for the vets to use when they secure a work-from-home position.

For more information on how you can donate to this cause, visit www.vetsworkshop.org/how-you-can-help.

E-CAST

Managing SWaP in ISR systems

Presented by Advanced Cooling Technologies, Curtiss-Wright, GE Intelligent Platforms, and TE Connectivity

Even in today's budget-constrained environment the Department of Defense (DoD) is still funding Intelligence, Surveillance, and Reconnaissance (ISR) missions from payloads in unmanned aerial vehicles (UAVs) to radar and maritime surveillance. All of these applications are driven by requirements for more and more signal processing performance and reduced size, weight, and power (SWaP). Innovation in these systems is happening at the embedded electronics level where designers are overcoming thermal and power dissipation challenges in small system footprints through unique solutions and open architectures. This e-cast of industry experts will discuss the reduced SWaP challenges in ISR systems and more.

Register for the e-cast:
http://ecast.opensystemsmedia.com/482

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

WHITE PAPER

The benefits of integrated video management

By Curtiss-Wright Defense Solutions

Today's advanced video management systems (VMS) solutions are built from a wide mix of video switches, displays, mission computers, and recorder offerings. When these components are sourced from a mix of heterogeneous vendors, the VMS integration process can quickly become complex. A better approach, one that maximizes operator usability and system flexibility while ensuring optimal interoperability, is provided by a fully integrated VMS. Even better, an integrated VMS offers the headroom for expansion needed to support future technology upgrades without locking you into a one-off solution.

Read the white paper: http://mil-embedded.com/white-papers/white-paper-benefits-integrated-video-management/

More white papers:
http://whitepapers.opensystemsmedia.com/

GE
Intelligent Platforms

We earn your trust, one platform at a time

Discover why GE is one of the most trusted suppliers of military and aerospace COTS solutions

Program managers around the world consistently put their trust in GE for COTS computing and communications products for ground-up developments as well as technology insertions into existing platforms. For a hundred years, GE has been supplying the defense industry with innovative products. GE carries forward that legacy with embedded computers that reduce costs, leverage the latest commercial technologies, slash time-to-market, and reduce engineering risk.

Numerous high-visibility programs for manned and unmanned ground, air, and sea platforms have incorporated GE products to achieve targeted hardware and software benchmarks with a minimum of program risk. Let us help you achieve that same level of success with your next program.

For white papers and application details, visit:
defense.ge-ip.com

imagination at work

Critical Recording in Any Arena

When You Can't Afford to Miss a Beat!

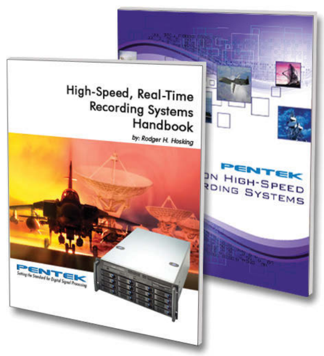
Introducing Pentek's expanded line of Talon® COTS, rugged, portable and lab-based recorders. Built to capture wideband SIGINT, radar and communication signals right out-of-the-box:

- Analog RF/IF, 10 GbE, LVDS, sFPDP solutions
- Real-time sustained recording to 4 GB/sec
- Recording and playback operation
- Analog signal bandwidths to 1.6 GHz
- Shock and vibration resistant Solid State Drives
- GPS time and position stamping
- Hot-swappable storage to Windows® NTFS RAIDs
- Remote operation & multi-system synchronization
- SystemFlow® API & GUI with Signal Analyzer
- Complete documentation & lifetime support

Pentek's rugged turn-key recorders are built and tested for fast, reliable and secure operation in your environment.

Call 201-818-5900 or go to www.pentek.com/go/mestalon for your FREE *High-Speed Recording Systems Handbook* and *Talon Recording Systems Catalog*.

TALON



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