@military_cots

# Military EMBEDDED SYSTEMS

MIL-EMBEDDED.COM

October 2015 | Volume 11 | Number 7

## SDR SECURITY AND SHARED SPECTRUM CHALLENGES

P 20

P 16

*An interview with Mike Jones, Vice President and General Manager of Rockwell Collins Communication and Navigation*

## Taking on encryption's usability and key management problems

P 36

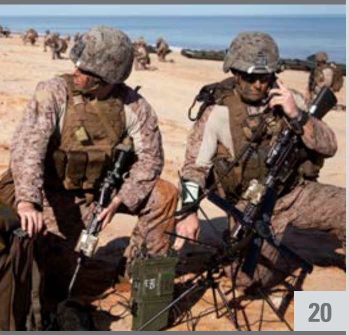
# Military EMBEDDED SYSTEMS

Volume 11
Number 7

October 2015

www.mil-embedded.com

12


20

28

36

## SPECIAL REPORT

## MIL TECH TRENDS

## INDUSTRY SPOTLIGHT

## COLUMNS

## DEPARTMENTS

## EVENT

**DMC (Defense Manufacturing Conference)**
Nov. 30 – Dec. 3, 2015 • Phoenix, AZ
www.dmcmeeting.com

## WEB RESOURCES

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

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

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

@military_cots

Published by:

OpenSystems media™

ISSN: Print 1557-3222

ENVIROINK The inks used to print the body of this publication contain a minimum of 20%, by weight, renewable resources.

**ON THE COVER:**

**Top image:** U.S. Marine Corps 1st Lt. Gary Goodwin, right, talks on a radio with his leadership team as Australian and Japanese soldiers conduct an amphibious assault using combat rubber reconnaissance craft onto Gold Beach during Talisman Sabre 2015 at Fog Bay, Australia. Goodwin is assigned to the Battalion Landing Team, 2nd Battalion, 5th Marine Regiment, 31st Marine Expeditionary Unit. Photo courtesy of Department of Defense.

**Bottom image:** Encryption is not particularly easy to use, but efforts are underway to solve its key management and usability problems to bring it into datacenters and possibly even help it finally go mainstream.

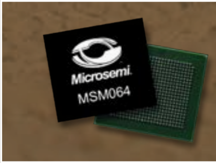
# Information Security and Performance... From the Ground Up

## Microsemi's Military-Grade Solid State Drives (SSD) Provide a Total Defense Solution

- AES-256 XTS Encryption
- Multiple Key Management Modes
- 30ms Key Purge
- Fast Clear (Any Capacity)
- -40°C to +85°C Temperature Range
- Armor™ Processor
- Defense-Grade Ruggedization

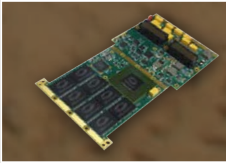
### TRRUST-Stor®

- 64GB to 1TB Storage Density
- 2.5" SSD Case
- 3000 G / 30 Grms Shock/Vibe



### BGA SSD

- 32GB to 64GB Storage Density
- 524 PBGA Module 28 x 32 x 6mm



### XMC

- 256GB to 512GB Storage Density
- XMC Form Factor

### mSATA

- 64GB to 128GB Storage Density
- mSATA Form Factor (50x30mm)

Microsemi
Power Matters.™

For more information, visit www.microsemi.com

Win an iPad mini!

Go to www.microsemi.com/defense

# 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

Sally Cole, Senior Editor
scole@opensystemsmedia.com

Mariana Iriarte, Associate Editor
miriarte@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

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

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

Twyla Sulesky, Strategic Account Manager
tsulesky@opensystemsmedia.com
(408) 779-0005

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

Wyndell Hamilton, Wright's Media
whamilton@wrightsmedia.com, (281) 419-5725

## OpenSystems Media Editorial/Creative Staff

Embedded Computing Design · Military Embedded Systems · Signal Processing Design · Industrial Embedded Systems · PC/104 small form factors · PICMG Systems & Technology · VITA Technologies

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*

Sally Cole, Senior Editor
*Military Embedded Systems*

Mariana Iriarte, Associate Editor
*Military Embedded Systems*
*PC/104 and Small Form Factors*

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

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

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

Joy Gilmore, E-cast Manager
jgilmore@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

Jennifer Hesse, Managing Editor
*VITA Technologies*
jhesse@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, Contributing Designer

Chris Rassiccia, Creative Projects

## 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
rnass@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

## Subscriptions

www.opensystemsmedia.com/subscriptions

subscriptions@opensystemsmedia.com

# Analyzing sale of GE embedded computing to Veritas

*By John McHale, Editorial Director*

Rumors had been floating for about a week, but the official announcement that GE was selling its embedded computing business – which falls under GE Energy Management's Intelligent Platforms subdivision – to venture capital firm Veritas Capital in New York City hit the wires Sept. 22.

The transaction is expected to close later this year. Upon closing, the business – which has about 700 employees worldwide – will be renamed and operate as an independent company at its current headquarters in Huntsville, Alabama. GE officials declined to disclose financial terms of the transaction.

**Market perspective**

It's been while since a big acquisition was made in the military embedded computing space. GE's embedded business – formerly part of GE Fanuc and rebranded in 2007 as GE Intelligent Platforms – was formed through aggressive acquisition, with the company gobbling up VMIC in 2001 and Ramix in 2004. Then in 2006 they swept up Radstone Technology, SBS Technologies, and Condor Engineering. At the time they seemed to be in an acquisition race for military embedded computing firms with Curtiss-Wright and Kontron.

We in the media used to joke that the three companies were using industry trade publications as a shopping list, since they were buying up all our advertisers.

The GE embedded group being snatched up isn't really surprising. There had been scuttlebutt for years that the group never really fit into GE and was going to be grabbed by a defense prime, a competitor like Kontron, or a venture capital (VC) firm, which ended up being the real deal. It would also not be the first military embedded computing company to get swept up by a VC or private equity firm. Emerson sold their Embedded Computing and Power business to Platinum Equity in in 2013, later renaming it Artesyn.

"Veritas is a holding company, which means they typically buy companies, clean them up, then sell them for a profit," says Ray Alderman, Chairman of the Board for the VITA Standards Organization, of which GE Intelligent Platforms is a member. "Therefore they will likely clean up GE, get it more efficient, and then keep it as cash cow or put lipstick on it and sell it. Artesyn operates this way now under their holding company. Pentair does same thing with Schroff. Both have been cleaned up to be cash cows.

"It will take about 18 months for Veritas to figure it out – four months to figure what they bought, six months to clean it up, six months to get it working efficiently, and then six months to sell it if they wish," he adds.

"I compare this GE situation to what happened with the Motorola Computer Group (MCG) years ago," he adds. "Motorola never seemed to see where it fit and shuffled it around to different divisions, finally selling it off. GE is now doing the same thing with their embedded military/aerospace business."Artesyn, when it was Emerson, bought the Motorola Computing Group in 2008.

**What about GE embedded employees and customers?**

Based on chats I've had with others in our industry, many think that losing the cachet of the GE name will hinder the new company's long-term potential, but I disagree. While lost in the global behemoth of GE, the GE embedded operation will no longer be subjected to what seemed like yearly reorganizations or be held back by GE internal processes, allocation costs, and media restraints.

Folks at smaller firms such as Aitech, X-ES, Mercury Systems, etc., often claimed they benefited every time Curtiss-Wright, GE, or Kontron bought one of their competitors. The smaller competitors believed they filled a vacuum by providing more intimate customer service while the large, acquiring companies dealt with growing pains. True or not, it is a perception often shared by the end customer. Now, the new business to be formed under Veritas should regain some of that nimbleness and flexibility they had in years past as Radstone or VMIC.

GE corporate could be a drag on GE embedded when they competed against faster, smaller companies, Alderman says. "It is not the way our marketplace works. I think it will be good for the mil/aero market that they will now be out from under the GE restrictions."

I expect the change will also be positive for most GE embedded employees. Many former Radstone or SBS employees told me they found GE to be a bit stiff and formal and that they missed the personality and flair their previous companies had before they were acquired.

Alderman agrees with me. "There are two ways to do things – the wrong way and the GE way" and that was not a fit for everyone who got acquired over the years, he says.

The trick for the GE embedded folks will be nailing their branding down once they rename and restructure and ensuring their military end customer that there will be no blips in service or quality. Be assured their competitors will be right there to step in if they don't, and Veritas might do as Alderman says and resell them in two years or less. For now, it is good news for GE embedded's employees and hopefully for the market as well.

# Cool power sensation

By Charlotte Adams

A GE Intelligent Platforms perspective on embedded military electronics trends

*Sensor platforms are proliferating around the edges of the network in both the civilian and the military spheres. For examples, think of the remote devices on buses, trucks, and oil rigs that are monitored via the Internet of Things or the unmanned surveillance nodes in the network-centered warfare infrastructure. To be effective, these "edge" devices need to be as self-sufficient as possible, not just in processing capability but also in energy use.*

Size, weight, and power (SWaP) has long been the mantra for embedded electronics. Every military platform, from the humblest handheld device or miniature unmanned vehicle to the largest weapon system must face these constraints at some level. For battery-dependent devices, energy efficiency is a more urgent concern. The smaller the platform, the bigger the bite from power-hungry computers.

Although it's sometimes overlooked, a key driver behind SWaP and system power concerns is chip-level performance per watt. Today's advanced semiconductors, sporting billions of transistors, can burn a lot of power and dissipate a lot of heat. A major challenge for overall power budgets is constraining chip requirements within the tightest possible limits.

In the sensor-processing realm, much has been done with field-programmable gate arrays (FPGAs), chips that can be optimized not only for speed but also for power management. These devices' one-of-a-kind firmware is expensive to create, however, and can be equally costly to upgrade. Therefore, military customers often express a preference for general programmable processors that can use open source software like Linux. Conventional CPUs, which fill the "general" bill, just can't compete in performance with FPGAs, though.

This dilemma has created an opening for general-purpose graphics processing units (GPGPUs). Originally developed for the gaming market, these hybrid chips are designed for efficiency and have improved in power performance. They feature hundreds of parallelizable processing units, or cores, as well as multiple CPUs. Fortunately, GPGPUs have proved to be adaptable to the military market. These software-programmable chips are able to process oceans of image data in a timely fashion, compress it, and transmit it to decision-makers within tactical deadlines.

> *"Today's advanced semiconductors, sporting billions of transistors, can burn a lot of power and dissipate a lot of heat."*

The latest GPGPU in NVIDIA's low-power Tegra system-on-chip (SoC) product line, the Tegra X1, provides a teraflop of compute performance (1 trillion floating-point operations per second) at a power cost of only 10-12 watts.

That's almost three times the raw performance of the company's predecessor chip, the Tegra K1, which delivers 326 gigaflops at a fractionally higher power output, or about twice the performance per watt of the predecessor chip's GPU function. That's in spite of the fact that the X1 has 256 GPU CUDA cores and eight CPU cores compared with the K1's 192 CUDA GPU cores and four CPU cores. (CUDA, which stands for Compute Unified Device Architecture, is NVIDIA's GPU programming model.)

Some of the reasons for this performance-per-watt improvement are the X1's smaller process size (20 nm vs. 28 nm), more efficient memory technology, and enhanced power management features compared with the K1.

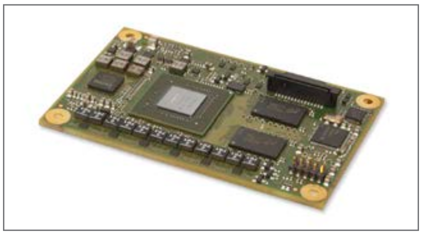


**Figure 1** | GE's mCOM10K1 Type 10 Mini COM Express Module gives designers 326 GFLOPS of performance while consuming minimal power.

The X1 is likely to be attractive to military users, since it can be plugged into existing K1 boards as a more or less seamless upgrade to run K1 applications, only faster.

An example of a minimal-footprint GPGPU product is the GE Intelligent Platforms mCOM10-K1, a ruggedized, extended-temperature, credit card-sized K1 module that is upgradeable to an X1 configuration.

The benefits from improved performance per watt will be significant, especially as the new technology is backwards-compatible. For one thing, it will be possible to fuse higher-resolution sensor data, using more input devices simultaneously. Additionally, new applications such as neural net-based automatic target recognition and autonomous navigation and mapping will become more plausible. The excess compute capacity in these new chip sets might even be sufficient to meet all the processing needs of small robotic vehicles.

**www.gedefense.com**

# Trusted boot in COTS computing

*By Michael Slonosky*
*An industry perspective from Curtiss-Wright Defense Solutions*

Military and aerospace system architects and integrators are faced with new challenges as customers implement increasing requirements for safety- and security-critical applications. Military and aerospace embedded computing applications now need to provide both high-assurance computing focused on ensuring overall mission safety along with high availability to safeguard the integrity, confidentiality, and security of the data within and between systems. Moreover, with increased interest in foreign military sales, it is becoming more important to protect critical IP from compromise or alteration.

Another factor driving the need for security assurance is the growth of embedded network-centric computing and the use of open source software in these interconnected systems. Open source software is increasingly treated like a module that can simply be downloaded and plugged into an OEM's own software. The downside of this approach is that the use of open source code of unknown origin can pose security risks, especially if it has not been analyzed for "back doors."

One approach to mitigating these risks is to implement secure booting so that the system will boot and execute only authentic code. Secure booting prevents the CPU from running untrusted code instead of authentic, OEM-signed code. To achieve this goal, secure booting detects and rejects modified security configuration values and device secrets.

Some examples of high-performance processors that provide secure boot capabilities for military-focused commercial off-the-shelf (COTS) embedded systems include Freescale's QorIQ processors, including the P3041, P4080, P5020, T2080, and T4xxx. Freescale has had years of experience supporting the commercial and automotive computing markets; now the company has integrated trust architecture features into its QorIQ processors. For applications that do not require secure boot, the processors come with secure boot and other trust architecture features disabled by default. When secure boot is enabled, instructions are executed from the internal boot ROM to enable the processor to determine if the image to be loaded into ROM is safe to execute. In the secure state, the image cannot be changed maliciously and the processor can be placed into a state where unauthorized debug or JTAG access is prevented to block snooping or changes to the image to be loaded. Secure boot also prevents the extraction of sensitive values from the CPU by any means short of deprocessing. Once the CPU is in the secure state, a device-specific, one-time-programmable master key (OTPMK) can be used to encrypt and decrypt data.

> *"Secure booting prevents the CPU from running untrusted code instead of authentic, OEM-signed code."*

The starting point for a trusted or secure boot is the creation (by the developer) of a bug-free and malware-free code base. Once the developer "trusts" the code, the developer digitally signs the code so that accidental or deliberate modifications to the code base will be detected during the secure boot cycle. To place a digital signature, an OEM first generates an RSA public and private key pair. It is the responsibility of the OEM to tightly control access to the RSA private signature key. If this key is ever exposed, attackers will be able to generate alternate images that will pass the secure-boot process. If this key is ever lost, the OEM will be unable to update the image.

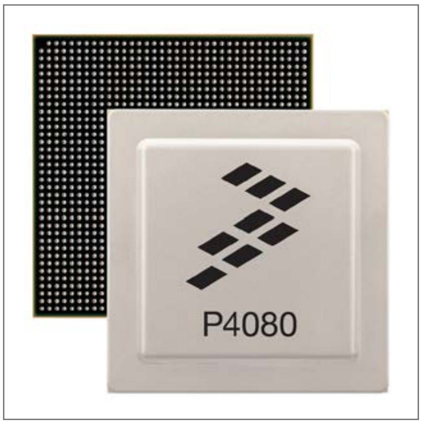


**Figure 1** | The dual-node VPX6-195 OpenVPX board leverages Freescale's Trusted Boot capabilities.

The application is signed using an RSA private signature key. The digital signature and a hash of the public key is appended to the image and written to flash (or other system nonvolatile memory). When the processor boots, the signature is checked using the RSA public key; the CPU uses the hashed RSA public key to check the signed image and compares the signatures. If the values match, the image is considered authentic and is allowed to boot. QorIQ processors also enable portions of the image to be encrypted to prevent attackers from stealing the image from flash memory.

An example of a COTS single-board computer that supports secure boot is Curtiss-Wright's dual-node VPX6-195 6U OpenVPX board. This single-board computer (SBC) provides antitamper and information security levels by leveraging Freescale's "Trusted Boot" technologies and capabilities. The board features two fully independent processor nodes, each of which has a Freescale quad-core T2080 processor that is provided with its own power, I/O, FPGA, and XMC expansion site.

**Michael Slonosky**
**Product Marketing Manager for Power Architecture Single Board Computers, C4 Solutions Group**
**Curtiss-Wright Defense Solutions**
**www.cwcdefense.com**

# DEFENSE TECH WIRE

NEWS | TRENDS | DOD SPENDS | CONTRACTS | TECHNOLOGY UPDATES

By Mariana Iriarte, Associate Editor

NEWS

## USSOCOM orders MRZR tactical vehicles

Polaris Defense began deliveries of the MRZR off-road vehicle platform to the United States Special Operations Command (USSOCOM) in early September. The contract's estimated value is $83 million.

Under the five-year, indefinite delivery, indefinite quantity (IDIQ) contract, Polaris will continue with delivery options on the MRZR 2 and the MRZR 4 vehicles including contractor logistics support (CLS) for spares, training, and support as part of the light tactical all-terrain vehicle (LTATV) program.

The MRZR vehicle platform can be configured a number of ways and includes electronic power steering, fold-down rollover protective structures, and infrared light capability. Polaris Defense has been delivering MRZR vehicles to USSOCOM for the past three years against a GSA contract under a blanket purchase agreement.

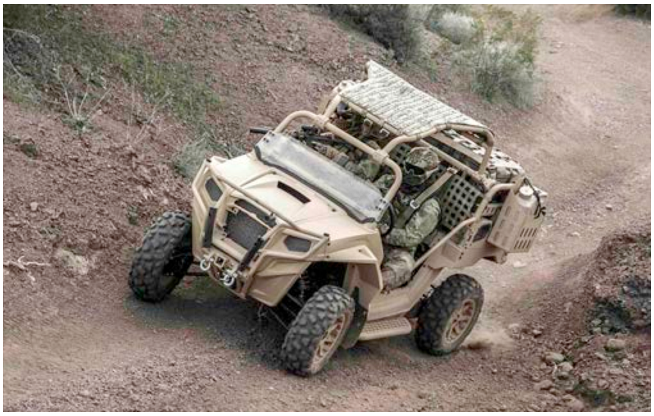


**Figure 1** | MRZRs are in service in more than 20 countries. Photo courtesy of Polaris Defense.

## Raytheon expands its operations in Colorado Springs following NORAD contract

Raytheon officials have announced that they are speeding up the expansion of the company's Colorado Springs presence following a $700 million NORAD multiyear contract for supporting operations at NORAD's Cheyenne Mountain Complex.

Under the NORAD Integrated Space Support Contract (NISSC), Raytheon engineers will enable 24/7 support to warning and attack-assessment systems for air, missile, and space threats. The company plans to hire as many as 700 employees in Colorado Springs by the end of next year.

This contract was initially awarded to Raytheon in April this year; however, protest activity by another company delayed the execution of it. The Government Accountability Office denied the most recent protest on August 25 and authorized Raytheon going forward.

## Hub-drive design and development contract will improve mobility and survivability

The U.S. Defense Advanced Research Projects Agency (DARPA) has selected QinetiQ to develop an electric hub-drive to improve survivability and mobility of military ground vehicles. The contract is initially estimated at $1.5 million, but if all options are exercised, the total could be as much as $2.7 million.

It will fall under DARPA'S Ground X-Vehicle Technology (GXV-T) program. QinetiQ engineers hope that the hub-drive design will improve mobility through enhanced power, torque, integral braking, and high efficiency – all contained within a 20-inch wheel rim unit. The shafts and gearboxes will be removed to increase survivability during an incident.

The hub-drive "also introduces a far greater degree of architectural flexibility, enabling vehicles to be configured in ways which offer greater protection to their occupants," says Dr. David Moore, Director of Research Services at QinetiQ.

## U.S. Air Force radar-support services contract extends another year

BAE Systems has received a contract modification to continue providing the U.S. Air Force with operation and maintenance support services for the Solid State Phased Radar System (SSPARS). The original award began in 2006; with the modification, the contract is now extended another year, thereby bringing the estimated value of the contract up to $550 million.

Under the contract, BAE Systems will continue to support through 2018 the U.S. Air Force's 21st Space Wing – the unit responsible for providing missile warning and space surveillance awareness. SSPARS is comprised of five radar sites in the Northern Hemisphere: Beale Air Force Base, California; Cape Cod Air Force Station, Massachusetts; Clear Air Force Station, Alaska; Royal Air Force Fylingdales, North Yorkshire, England; and Thule Air Base, Greenland.

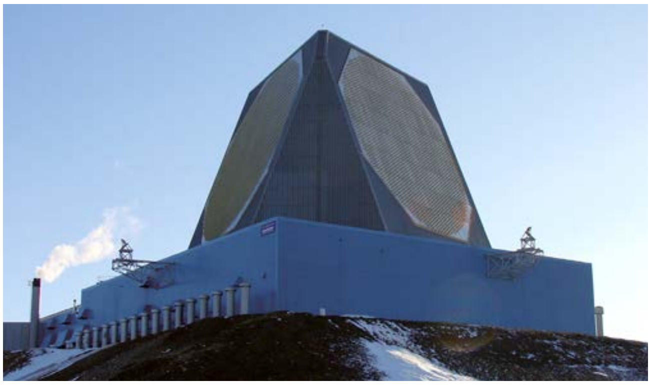


**Figure 2** | Operation and maintenance support for the SSPARS will conducted at five locations in the Northern Hemisphere. Photo courtesy of BAE Systems.

## Marines test augmented-reality system during live-fire training exercises

Engineers at the Office of Naval Research (ONR) and Marines taking the Infantry Officer Course teamed up recently to test ONR's Augmented Immersive Team Trainer (AITT) system during a live-fire training exercise at the Marine Corps Base Quantico in Virginia.

The AITT program is part of the ONR Capable Manpower Future Naval Capability, which is set to wrap up its final year with a large-scale demonstration at Quantico. Pending the results of a Marine Corps assessment in October, the program will transition to the Marine Corps Program Manager for Training Systems for further testing and development.

The AITT system is comprised of a laptop, software, battery pack, and helmet-mounted display. The technology supports live and virtual training scenarios by superimposing virtual objects onto the real environment. It bypasses challenges such as the wait time for a test range and can use virtual ground vehicles, aircraft, and munitions.

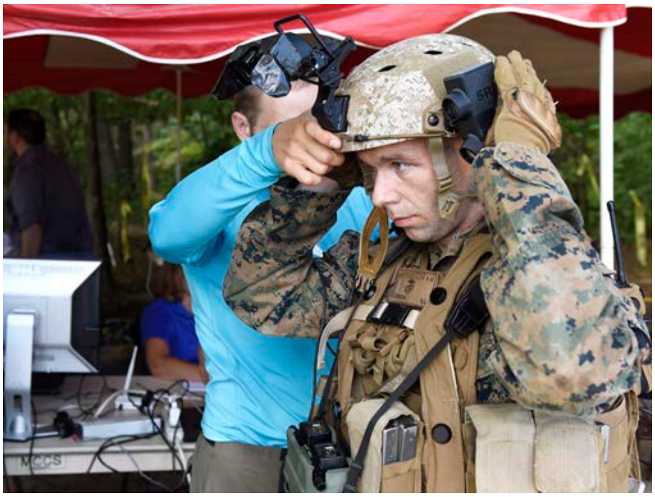


**Figure 3** | Soldier putting on the helmet-mounted AITT display. The system can eliminate maintenance issues or weather-related restrictions. Photo courtesy of ONR.

## Flexible Hybrid Electronics Manufacturing Innovation institute in Silicon Valley receives funding from DoD

Funding for the Manufacturing Innovation Institute for Flexible Hybrid Electronics has been allotted to a consortium – led by FlexTech Alliance – of 162 companies, universities, and nonprofits to advance U.S. leadership in manufacturing flexible hybrid electronics.

The announcement comes after a nationwide bid process for the seventh of nine manufacturing institutes launched by the administration, and the fifth of six manufacturing institutes led by the Department of Defense (DoD).

The U.S. Air Force Research laboratory (AFRL) will manage the cooperative agreement and will receive DoD funding estimated at $75 million over five years, matched with an approximate $90 million from industry, academia, and local governments. The institute is set to receive a total of $171 million to invest in U.S. manufacturing.

## Worldwide UAV market to triple over next decade

Global spending on unmanned aerial vehicle (UAV) programs is expected to triple over the next decade in military, commercial, and consumer markets, according to a recent market analysis from the Teal Group. The analysts estimate that UAV production will rise from the current $4 billion annually to about $14 billion, totaling $93 billion over the next ten years. In addition, military UAV research spending would add another $30 billion.

UAV payloads, such as electro-optic/infrared sensors (EO/IR), synthetic aperture radar (SAR), SIGINT and electronic warfare systems, and C4I (command, control, communications, computers, and intelligence) systems are forecast to double in value from $3.1 billion in fiscal year 2015 to $6.4 billion in fiscal year 2024, Teal analysts say.

Civil UAV growth is also continuing to grow. "Our 2015 UAV study calculates the UAV market at 72 percent military, 23 percent consumer, 5 percent civil cumulative for the decade," says Philip Finnegan, Teal Group's director of corporate analysis and coauthor of the study. The United States accounts for 64 percent of the Research, Development, Test, & Evaluation UAV total worldwide, says Steve Zaloga, the coauthor of the study.

## U.S. Navy teams up for centralized aviation-training hub

The Naval Aviation Training Systems Program Office (PMA-205) and Naval Air Warfare Center Training Systems Division teamed up to design and demonstrate the Navy Aviation Distributed Training Center (NADTC) prototype, a central hub for distributed aviation training where the goal is to provide daily training opportunities for naval aviation. The NADTC is part of the Naval Aviation Vision for 2025.

The demonstration, planned and executed by the two offices, showed the Navy's capability to connect multiple aviation training devices to a central station for dedicated Fleet Synthetic Training – Air (FST-A). During one event, engineers connected a P-3C Orion training device from Naval Air Station (NAS) Jacksonville to H-60R Seahawk at both NAS Jacksonville and NAS North Island via the Navy Continuous Training Environment (NCTE). During a second event, an E-2D Hawkeye training device connected from NAS Norfolk to an F-18C Hornet from NAS Oceana and NAS Lemoore.

The center will also provide a centralized location for technical support, mission planning, opposing-force management, and briefing/debriefing capabilities of training events.

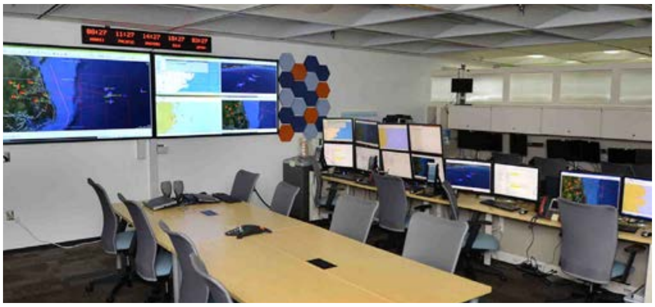


**Figure 4** | NADTC officials hope to have the training center complete in 2017. Photo courtesy of U.S. Navy.

# SWaP: The RF solution that can mean the difference between flying high and being grounded

By Jarrett Liner

Defense airborne platforms – particularly mission-critical applications including electronic warfare, radar, and fire control – must maximize size, weight, and power (SWaP). An E-2C Hawkeye assigned to the Screwtops of Early Warning Squadron (VAW) 123 launches from the flight deck of the aircraft carrier USS Dwight D. Eisenhower (CVN 69) during flight deck certifications. (U.S. Navy photo by Mass Communication Specialist 3rd Class Jameson E. Lynch/Released)

*Defense and commercial airborne platforms differ in many ways: Defense platforms focus on multifunction systems and power management for mission-critical functions such as electronic warfare, fire control, radar, etc., while commercial aircraft place high emphasis on safety and system redundancy. One area of common concern for both is maximizing payload efficiency. Every ounce of weight, cubic centimeter of space, and milliwatt hour of power is carefully planned, as both focus on balancing size, weight and power (SWaP). Advances in RF technology can provide a leapfrog advantage for manned and unmanned aircraft in both markets.*

SWaP refers to arguably the most important specification in new product, project, or platform definition from electronic warfare to avionics. Nearly all new developments – whether shipboard, airborne, terrestrial, man-carried, or carried in hand – share a common requirement: Make it smaller, make it use fewer resources, and make it contribute more to the overall system functionality. A lean system is more desirable in the current social, economic, political, and global environments. Lately, SWaP increasingly seems to be the key driving factor, providing difficult tradeoffs over system performance enhancements and multifunction architectures.

## Culprit identification

Let us take a look at a few of the miscreants, scandalous offenders, and substantially burdensome characters.

Copper is the conductor of choice for electrical power transmission. A thousand feet of AWG 5 gauge copper wire without insulation weighs nearly 100 pounds (50 kg). To add insult to injury, the inherent resistance of wire causes electrical current to be wasted in the form of dissipated heat. The next perpetrator in the lineup is legacy component size. Consider the case of the shipboard radar local oscillator (LO); the LO feeds both the transmitter and receiver. The LO must produce a stable frequency with low harmonics, while the highest-stability requirements must account for temperature, voltage, and mechanical drift. The oscillator must produce enough output power to effectively drive subsequent stages of circuitry, such as mixers or frequency multipliers. It must have low phase noise where the timing of the signal is critical. Historically, the LO was generated and distributed by separate and specially designed subsystems. The same or similar was true for airborne systems: Large size, power-hungry, and heavy due to the solid-state component content.

The legacy component that has provided high-power radio frequency (RF) to a system is the traveling wave tube (TWT), which is a specialized vacuum tube that is used in electronics to amplify RF signals in the microwave range range (Figure 1). The bandwidth of a broadband TWT can be as high as one octave, although tuned (narrowband) versions are more common; operating frequencies range from 300 MHz to 50 GHz. These TWT systems are somewhat efficient, but they are a single point of failure; reliability is a significant concern with TWTs. Microwave tube reliability is strongly dependent on three factors. First, defects introduced during the manufacturing process adversely affect reliability, with concerns about production problems, poor workmanship, and lack of process control. Secondly, tube reliability is heavily dependent upon operating procedures and handling. Finally, adequate design margin must exist between the operating point and the ultimate design capability of the tube in order to have reliable operation. These are just three examples of the many enemies of SWaP.

### The superheroes of SWaP

Advances in semiconductor technology and component integration have played a significant role in reducing SWaP. Solid-state power amplifiers (SSPAs) are not a new technology. GaAs (gallium arsenide) and LDMOS (laterally diffused metal oxide semiconductors) have been used for high power amplifiers for many years. In fact, silicon-based LDMOS FETs are widely used in RF power amplifiers for base stations, as the requirement is for high output power with a corresponding drain to source breakdown voltage is usually above 60 V. Compared to other devices such as GaAs FETs, they show a lower maximum power gain frequency. A gallium arsenide field-effect transistor (GaAsFET) is a specialized type of FET that is used in solid-state amplifier circuits at microwave radio frequencies. This spans the spectrum from approximately 30 MHz up to the millimeter wave band (Figure 2).

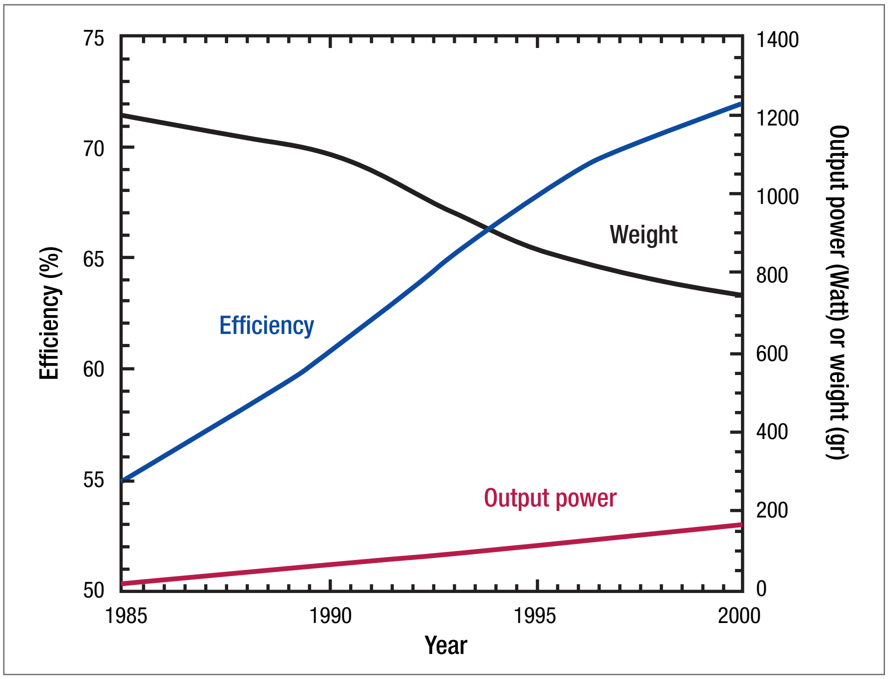


**Figure 1** | Illustration of TWT improvements in efficiency, output power, and weight against time.

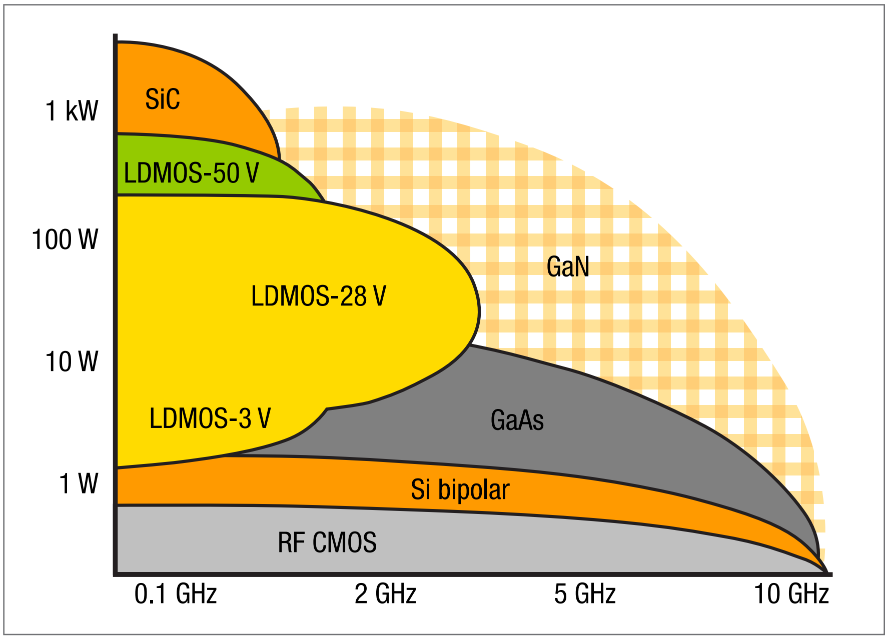


**Figure 2** | Power level per process.

The GaAsFET is known for its sensitivity and also for the fact that it generates very little internal noise. The power density is limited by the breakdown voltage; you can get 20 V breakdown on a good day with a GaAs MESFET.

Let's review: TWTs have high frequency and high power available, but the reliability, weight, and required supporting subsystems make them undesirable. LDMOS allows for high power, but operates below 5 GHz. GaAs MESFETs operate at very high frequencies, yet the low breakdown voltage limits them to the 10 W power range.

Is there an SSPA leapfrog technology available to save the day? SWaP loves gallium nitride on silicon carbide (GaN on SiC). Both GaN and SiC are wide-bandgap material, which means the combined breakdown voltages are as high as 150 V. This enables higher power density along with a lower load line for easier impedance matching. GaN on SiC allows power gain at frequencies in the millimeter bands (Ft~=90 GHz, Fmax~200 GHz).

The market acceptance of GaN on SiC LEDs has helped fill the wafer fabs and drive wafer costs down. The device structure of the RF transistors is such that power densities of five W/mm can be achieved. The MSL levels for GaN on SiC are near or arrived at industry acceptable ratings. GaN on SiC is widely agreed upon to be interruptive technology and the defence and commercial markets are demanding more of it. The performance of GaN on SiC is limited most by thermal transfer; getting the heat away from the device is the last issue to unravel. Some success has been found with GaN on silicon, but the reduced thermal conductivity limit the output power to near 10 W. The best performance comes from GaN on diamond, with some calculations pointing to power densities at up 10 times higher than GaN.

Although the direct growth of GaN on single crystal diamond has been demonstrated, the single crystal diamond substrates currently available have a maximum size that today limits the adoption of the technology. The government and defense contractors are the only early adopters of the GaN on Diamond alliance. Similar to GaAs in the 1980s, GaN on Diamond will be vetted through these government agencies and the commercial market will follow as the reliability increases and the associated cost decreases.

The TWT has an integrated SSPA replacement. ADI offers up to 8 KW High Power Amplifier (HPA) that combines many GaN on SiC SSPA's into a single unit. The KHPA-0811 uses a small, dodecahedron package to pack a considerable amount of power in a small footprint plus cover a wide bandwidth.

**Integration sinks the boat anchor**

A bit of background: In the U.S. Navy, when large electronic (or other) equipment became obsolete and a burden on the system resources, it was referred to as a "boat anchor." An airborne platform, whether manned or autonomous, will have many forms of communications on board. These comms links vary, with voice, navigation, data link, onboard sensor links, radar, munition tracking and on and on as the skies get more crowded and the warfare theatre becomes more complex. In the past, any one of these systems required significant real estate, power resources, and supporting subsystems. The fact that the airborne platforms were actually airborne is amazing. Every ounce was accounted for, every milliwatt was calculated, and the physical system design was considerable to fit into the allotted space. There had to be a better way. Integrated circuit (IC) design advancements, along with system-in-package (SiP) and system-on-chip (SoC) advancements, have made boat anchors of those bloated systems of yesterday.

**Cut the copper umbilical cord**

Defense and commercial aircraft, manned and unmanned, have hundreds, if not thousands, of sensors from

electronic warfare to radar to temperature ones; many have redundancy and backup support systems. These sensors include those to control flap and aileron position, navigation and positioning, engine vibration, brake temperature, and so many more. Each of these sensors – along with their associated redundancies – are connected to a central processor via heavy cables comprised of copper wiring and stainless or aluminum connectors. Significant platform resources are consumed to support these cables and interconnects. RF technological advancements will once again save SWaP by reducing the dependency on these cables. Many major airframe manufactures are working together to qualify commercial off-the-shelf (COTS) technology for a low-cost, reliable replacement for copper interconnectivity.

One example: An inertial measurement unit (IMU) sensor with output data bandwidth requirements of less than tens of KHz, combined with a precision analog microcontroller ARM Cortex M3 with RF transceiver, like the Analog Devices ADuCRF101, a fully integrated data-acquisition solution that is designed for low-power wireless applications. While right now this marriage is purely hypothetical, it would be one example of avionics sensor technology pairing with COTS RF components. Stand by for this type of RF implementation to save SWaP in the very near future.

**What's promising**

The current social, political, and economic environment requires airborne-platform designers to put increased focus on saving size, weight, and power. The reduced load on the system resources allows for longer flight times, reduced fuel requirements, and more efficient payload allowances. The most significant and most interesting advancements to save SWaP come directly from the technological advancements made in the RF community. The most promising revolves around size reduction from TWTs to SSPAs, component integration, and reduced dependency on copper cable interconnects. The solution that provides reduced SWaP is spelled "RF." **MES**

*Jarrett Liner is an RF Systems Application Engineer with Analog Devices in the Aerospace and Defense group, Greensboro, North Carolina. He has significant experience in the area of RF system and component design. Formerly, Jarrett was an applications engineer for GaN on SiC amplifiers for the military and aerospace sector. His prior experience also includes design and test of RF IC WLAN power amplifier and front-end modules for 13 years. He served six years in the United States Navy as an Electronics Technician. Jarrett received his BSEE from North Carolina Agricultural and Technical State University. He can be reached at Jarrett.Liner@Analog.com.*

Analog Devices
www.analog.com

# Software-defined radio (SDR) tech drives military communications today

By John McHale, Group Editorial Director

INTERVIEW

*In this Q&A with Mike Jones, Vice President and General Manager of the Rockwell Collins Communication and Navigation business in Cedar Rapids, Iowa, he discusses how software-defined radio (SDR) technology has changed military communications over the last 25 years, how it is being integrated today, and future communications innovations such as cognitive radio. Edited excerpts follow.*

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

**JONES:** I am Vice President and General Manager of the Rockwell Collins Communication and Navigation business, which reports in through Rockwell Collins Government Systems. My business focuses on the military market where we provide communication products serving air, ground, and naval domains domestically and around the globe. My business also provides navigation products and is involved with the development of global positioning system (GPS) and global navigation satellite system (GNSS) equipment and technology.

**MIL-EMBEDDED: *Can you please give a history of SDR technology, including how it was a key component of the now defunct Joint Tactical Radio System (JTRS) program, which Rockwell Collins was a part of?***

**JONES**: SDR communication systems meet a need for enhanced mission effectiveness through shared situational awareness and improved information sharing and collaboration, as well as synchronizing ground and airborne radios into robust networks. This need – articulated by the Department of Defense (DoD) and ministries of defense around the world since the mid-1990s – was the driving force behind the DoD's JTRS program. While the large JTRS program is now defunct, a number of variants survived and are moving into full-rate production and competition today, such as the HMS Manpack and the Rifleman Radio. On the datalink side the MIDS J still exists, as it enabled Link 16 capability for collaboration between air and ground forces.

The Software Communications Architecture (SCA) standard was what made these variants work by enabling the creation of many types of waveforms such as the Wideband Network Waveform (WNW) and the Soldier Radio Waveform (SRW). More waveforms have since been added and are available in a software repository and are all compliant with the SCA standard. The success of JTRS was in the waveforms and the SCA.

The original program struggled with the hardware side of the equation, which substantiated the need for greater processing power. But now processing technology has caught up and what has developed today is the availability of system-on-chip (SoC) hardware. This SoC capability is being brought to market in the HMS Manpack, Rifleman Radio, and MIDS J family of programs.

**MIL-EMBEDDED: *Many say SDR is now "a solved problem," and that today it is all about how to integrate the technology. Do you agree with that statement and how do you see SDR technology being used today in defense programs?***

**JONES**: When I look at the big picture regarding SDR, I think the industry must deliver technology that meets the concept of operations goals and objectives.

SDR enables the ability to pick a waveform and a set of functions to create an ability to switch around multiple channels, thus bringing situational awareness and enabling voice and data to move across an ad hoc network. The real challenge is to bring simplicity to SDRs in order to make them easier to operate.

The challenge will be around continued improvement in size, weight, and power (SWaP), range, and cost. So while it's fair to say SDR is mature, the technology is being pushed into smaller form factors and there is still a lot of engineering to be done year after year to keep up with that trend.

**MIL-EMBEDDED: *Many say that SDRs will evolve to enable smartphone-like multifunctionality in the near future. What are some new functionalities and capabilities that we may see in future programs?***

**JONES**: There is a current waveform that does much of this and it is called the Mobile User Objective System (MUOS). The MUOS program – for which Lockheed Martin is the prime contractor – brings cellphone-like capability to a tactical radio. The MUOS waveform is Internet Protocol (IP)-based and enables users to run apps over a satellite communications

(SATCOM) network. The Rockwell Collins ARC-210, which currently has Demand Assigned Multiple Access (DAMA) and Integrated Waveform (IW) satellite communications capabilities, will add the MUOS waveform.

Will there someday be additional cellphone-to-cellphone networks? That could happen but there are security challenges that need to be overcome first.

The key capability, in my opinion, is SDR's ability to host modern waveforms over the network. It all starts with fielded and soon-to-be-fielded software-defined tactical radios that can form ad hoc networks, with commanders choosing what to put out over the network, such as video intelligence and surveillance. This type of radio is being deployed and fielded more and more with combat brigades and should continue to be deployed over the next three to five years.

**MIL-EMBEDDED:** ***How are reduced SWaP requirements affecting SDR designs? What are the tradeoffs with smaller tech?***

**JONES**: Regarding SWaP, the first part that needs to be dealt with every time is power management. Savings in weight and heat comes from power management. The first step in designing any SDR is power management, which can be accomplished via waveform optimization, sleep modes, and other methods.

Once you get power management figured out, then you can look at reducing size; modern signal-processing technology has greatly enabled such reductions. Faster processors in smaller chip sizes have created order-of-magnitude performance increases in the same or smaller footprints. As embedded processing continues to enable this capability, it will allow SDR designers to keep up with SWaP requirements.

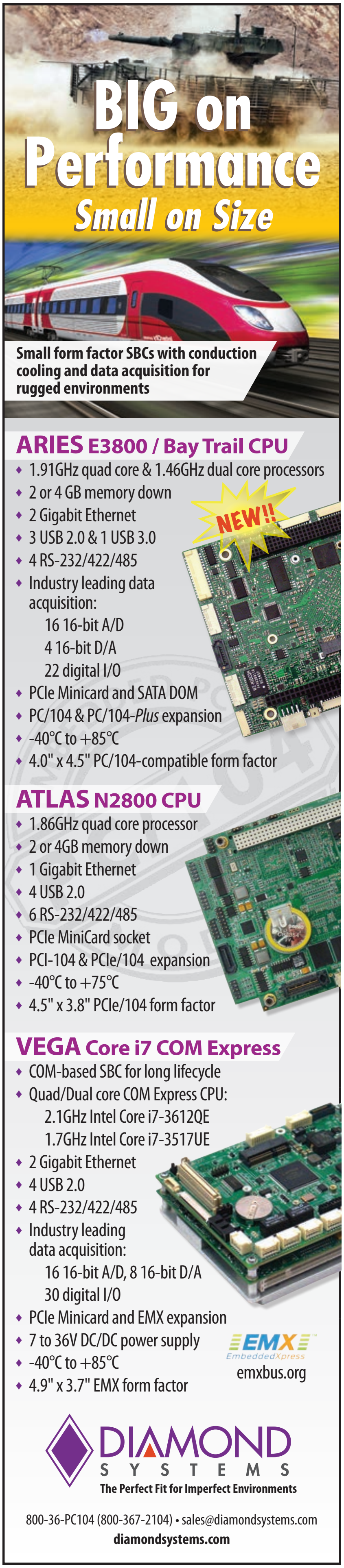
**MIL-EMBEDDED:** ***The DoD's FY 2016 budget request, released earlier this year, had an increase in overall funding, almost a reverse trend from the last few years. How do you see the funding outlook for SDR in DoD programs?***

**JONES**: There are large programs of record entering into competition now and over the next 18 months some will start full-rate production. However, I can't be more specific at this time.

Budgets are trending in the right direction, but the big concern right now is uncertainty. Sequestration has made it difficult to forecast and to find programs of record with steady purchasing power and the continuing appropriation resolutions prohibit new starts. It is difficult to plan and close a business case when you are uncertain of funding priorities and the timing of new starts. If you could move the sequester and continuing resolutions out of the viewfinder, then the base demand for SDR technology is there and will increase, as the network benefit it brings the military cannot be ignored.

Which brings me to the trend toward commonality and how that coincides with the benefits of SDR technology. As SDR has matured – with advanced waveforms facilitating air-ground connectivity and vice versa as well as connectivity amongst the troops – it has been supported by common technology and common waveforms. This is why Rockwell Collins developed our TrueNet family of SDRs, specifically achieving air-to-ground connectivity by leveraging common waveforms and software and hardware standards so the radios can be used in multiple applications. All the technical parts of the TruNet network run the exact same waveforms and capabilities and have the potential to support Joint Services and Coalition forces, enabling them to plug and play and work seamlessly together.

**MIL-EMBEDDED:** ***Many say the next radio tech evolution after SDR will be cognitive radio. What are the benefits of cognitive radio and what are the challenges that still remain in enabling the technology?***



**JONES**: The next layer is cognitive radio: Once you have a SDR with an RF front end and an embedded system that is programmable, the next step is to add sensing. The sensing will enable the radio to change programming by enabling ad hoc networks providing information when it is being jammed or has frequency interference. A cognitive radio will make these changes real-time to deal with multiple spectrum environments. We are about five to seven years from seeing a true cognitive radio fielded.

**MIL-EMBEDDED:** ***Outside of defense, what areas has SDR technology affected?***

**JONES**: SDR technology brings the same benefit to law enforcement and paramilitary that it brings to military applications by enabling multiple waveforms in one device through software and embedded-processing technology. The transition has been mostly determining which waveforms you port to the nonmilitary devices, such as the APCO 25 waveform used by public-safety operators.

**MIL-EMBEDDED:** ***Looking forward, what disruptive technology/innovation will be a game changer in the SDR world? Predict the future.***

**JONES**: I will answer that by saying there are three key problems to solve in the near future – the next five to 10 years. The first is network simplicity and the second is spectrum management; solving spectrum management will require some element of network simplicity.

The third is the ability to operate in an anti-access/area denial (A2/AD) environment. There clearly is a link between spectrum management and A2/AD environment and it will bring additional complexity as well as additional capability. The key to solving this complexity will be through intensive signal processing and spectrum sensing, with software to tie them together to make a whole system. **MES**

***Mike Jones*** *is Vice President and General Manager of Communication & Navigation Products for Rockwell Collins Government Systems. In this role, Jones is responsible for the company's military communications business, including software-defined radios, data link solutions, and satellite communications. Jones, who joined the company in 1998, most recently held the position of Senior Director, Rotary Wing Solutions for Rockwell Collins Government Systems. During his tenure at Rockwell Collins he provided a leadership role in capturing and launching the KC-46, KC-390, KC-10, KC-135 Block 45, and EC-130 programs. Jones has a Bachelor of Science degree in Physics from Washburn University, a Master of Science degree in Optical Engineering from the University of Rochester, and a Master of Business Administration from the University of Iowa.*

**Rockwell Collins**
**www.rockwellcollins.com**

Do more
Spend less
Reduce SWaP
Deploy faster

# SDR security and shared spectrum challenges

By Mariana Iriarte, Associate Editor

*At a time when the commercial market is clamoring to infringe on the allocated military spectrum, the military faces challenges to provide secure communications for its missions – creating a new challenge for designers of software-defined radio (SDR) technology.*

U.S. Marine Corps 1st Lt. Gary Goodwin, right, talks on a radio with his leadership team as Australian and Japanese soldiers conduct an amphibious assault using combat rubber reconnaissance craft onto Gold Beach during Talisman Sabre 2015 at Fog Bay, Australia. Goodwin is assigned to the Battalion Landing Team, 2nd Battalion, 5th Marine Regiment, 31st Marine Expeditionary Unit. Photo courtesy of Department of Defense.

SDR– a solved problem in many ways – has evolved into a standard methodology that enables communication across multiple platforms. The technology, which was nurtured under the auspices of the Joint Tactical Radio System (JTRS program) nearly two decades ago now has become a methodology that enables flexible communications for airborne, ground, and shipboard applications all while meeting stringent size, weight, and power (SWaP) requirements.

"Without the JTRS program to lead the way, who knows what the state of SDR would be today. It invested a lot of money to make SDR technology viable for military purposes and that technology was fed to the commercial markets," says Manuel Uhm, director of marketing at Ettus Research in Santa Clara, California, and chair of the board of The Wireless Innovation Forum.

"SDR is not one product you make and then it's done – it's a methodology of applying digital signal processing technology to implement radios, radars, and communications systems," says Rodger Hosking, vice president and cofounder of Pentek in Upper Saddle River, New Jersey. "And it's a constantly evolving process as the technology becomes more powerful and customers demand more performance. Increasingly challenging mission needs for better systems are driving software-defined radios to do more and more. SDR is an essential and integral part of virtually all warfighting electronics."

The next step in the technology's evolution for SDR designers will be to enhance security for SDRs, especially as military radio users become required to share spectrum use with commercial communication networks.

## Security and bandwidth

"One essential challenge in the military market is to provide reliable, secure information with a lot of information content – that means wider bandwidths, higher signal frequencies, more complex waveforms, and extra encryption and coding for security," Hosking says. "As these signals become more challenging, we need increasingly powerful SDR hardware in the radio to handle the signal processing requirements and complexity of these wideband signals.

One constant in life is that policymaking will never win a race with technology development, as the latter always outpaces the former. This mantra has never been truer than when it comes to developments regarding spectrum management – development comes first, sharing the spectrum and policy matters come second.

Earlier this year, the Federal Communications Commission (FCC) released a regulations update for the Innovative Spectrum Sharing in 3.5 GHz band, in which it states who and when is authorized to use that specific band.

“AS THESE SIGNALS BECOME MORE CHALLENGING, WE NEED INCREASINGLY POWERFUL SDR HARDWARE IN THE RADIO TO HANDLE THE SIGNAL PROCESSING REQUIREMENTS AND COMPLEXITY OF THESE WIDEBAND SIGNALS.”

According to the FCC, Aeronautical Radionavigation Service (ARNS) and the Radiolocation Service (RLS) have incumbent access for federal use of the 3550-3650 MHz band. The Department of Defense (DoD) radar systems fall under this spectrum as well. For security purposes, no one else is allowed to use this band while in use by the federal government. However, because the wireless band network has grown so much over the years, the commercial market has asked for use on this spectrum.

Consequently, spectrum-sharing opens up the possibility of security issues in communications, Uhm says. “Security is important to the military and always has been important. So a potentially bigger issue for them is the actual spectrum availability to use the spectrum when they need it and ensure they are protected from interference from any other radios.”

Therefore, the FCC has put in place a three-tier access model, where the primary user, in this case the federal government, has privileged access to the spectrum and receives protection under these rules and regulations.

“Now you have cognitive radios that could possibly cause spectral interference in multiple bands, which is a major issue because spectrum is such a valuable asset,” Uhm continues. “Part of the issue is that the military has been allocated exclusive use frequencies that commercial industries could use, spectrum that the military may not be using effectively. Now they get into the question of how this spectrum can be better utilized. The FCC is moving to a spectrum-sharing policy of tiered access in the CBRS (Citizen’s Broadband Radio Service) band, which was formerly exclusively used for maritime radar.

“This means that the military no longer has exclusive use to that spectrum, but as the incumbent, they are given priority access and protected from interference from other radios using that spectrum,” Uhm explains. “So they are the top tier. Then there is a second tier: Priority Access License, which those licensees have paid for a higher quality of service in that band, so they are protected from unlicensed users. The last tier, General Authorized Access (GAA), is like Wi-Fi, which means anyone can use it on an unlicensed basis. However, they have no interference protection and they have to make sure that they can’t interfere with tier one and tier two.”

Being able to communicate fast, reliably, and with the promise that no one else is listening is the ultimate goal. However, the military is finding that it is sharing a spectrum with the commercial world.

“CBRS is the first band where spectrum-sharing will be implemented; however, it’s going to happen more and more in the future since everyone wants more data,” Uhm says. “In the case of radar, it becomes an interference issue where one is no longer getting good data from the radar sensor due to other radios in the same spectrum.

“Military tactical radios still have exclusive-use spectrum, so no one is allowed to use their spectrum,” he adds. “But if there were malicious folks out there, the technology is available where people could interfere or possibly intercept communications, which would pose a security issue.”

How secure can warfighter communications be if they share bandwidth with civilian networks? The answer will be part of an ongoing back-and-forth between the military and the commercial world. While both have influenced each other, the commercial world is what really drives technology development today, especially with open standards.

**Open standards and SDR**

The DoD and system integrators increasingly continue to embrace open standards in military electronics applications such as tactical radios and SDR, not only as a way to combat obsolescence but also to make modernization efforts more efficient and enable more security across multiple domains.

“The promise of SDR is a universal platform that can be reconfigured to implement and handle any kind of radio or radar,” Pentek’s Hosking says. “While the philosophy is valid, the cost and complexity of such a universal system is impractical for deployed, targeted solutions that only need a subset of the hardware, software, and specialized interfaces. However, the need for efficient platforms that can be adapted for new SDR applications is still extremely valid. There are a lot of different types of radios and radars operating in a wide range of deployed environments. By using open standards like VPX, we are delivering modular products for platforms that can be reused, reconfigured, and retooled for new requirements without throwing away hardware and without starting over again.”

## SDR technology enables many other markets

While the Joint Tactical Radio System is now long gone, budget funding still exists for SDR technology, but it is spread throughout multiple programs – be they shipboard, unmanned systems, or electronic warfare as all take advantage in some way of communication waveforms defined in software.

“The JTRS budget was a driving factor for the development and commercialization of SDR technology,” says Manuel Uhm, director of marketing for Ettus Research in Santa Clara and chair of the board of The Wireless Innovation Forum. “JTRS has now evolved into programs of record that only fund deployment, not development. However, there are still companies that are developing smaller, faster, cheaper versions of military radios based on the latest available technology.

“Another consideration is that electronic warfare is an area where there is still budget funding for development,” he continues. “Due to the changing nature of asymmetric warfare, electronic warfare is keeping SDR technology development going with funding, which is driving research. It’s a slightly different application but nevertheless it’s funding that is advancing the overall state of technology.

“SDR is a technology that enables many markets, including satellite communications, military radios, and signals intelligence. Electronic warfare systems are also using this technology,” he continues. “It’s already integrated into these systems. Now it’s trying to evolve into ever-smaller, ever-cheaper hardware, so it’s evolutionary, not revolutionary, from a hardware perspective.”

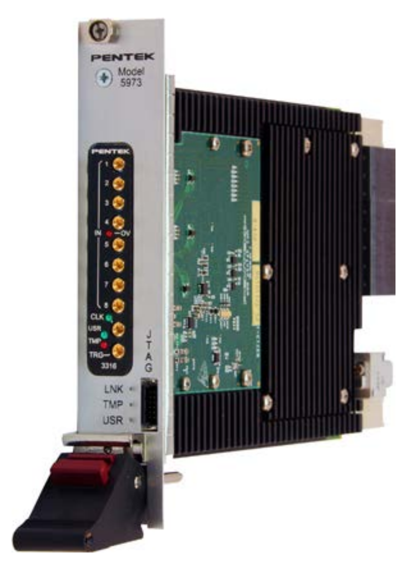


**Figure 1** | The 5973 3U OpenVPX FMC Carrier board from Pentek enables a high-bandwidth connection between boards mounted in the same chassis or separated over extended distances by leveraging a serial protocol in the FPGA.

FPGAs are key to this modularity as they enable SDR designers who need flexibility to take an integrated circuit and program or reprogram it to fit the needs of an end application.

“Each new generation of FPGAs from Xilinx and Altera delivers more resources, more gates, more logic cells, more DSP slices, more memory, and faster interfaces,” Hosking says. “This allows us to develop open-architecture, configurable board-level FPGA products that can be easily integrated into new and current systems,” he adds. (Figure 1.)

“FPGAs excel in implementing the needed functions in hardware to create massively parallel signal processing units,” Hosking continues. “For example, an FPGA can now contain as many as 10,000 DSP engines, all working in parallel. This is quite different from a CPU sequentially executing instructions and sequentially processing data. FPGAs have the ability to perform compute-intensive algorithms in parallel, and it’s the only way you’re going to tackle the toughest real-time tasks. Because it’s configurable, you can arrange FPGA hardware for optimum performance in a specific application, and then reconfigure the same device to do something completely different. FPGAs are configurable hardware, engineers will continue to face escalating development costs in their software designs."

"SDRs and cognitive radios typically have a heterogenous mix of processors, such as an FPGA, DSP, GPP, and/or GPU, and there is no single unified tool or development environment to develop and debug across all those devices," Uhm says. "As a result, the development cost is huge in the software, test, and verification areas. I believe revolutionary steps on the evolution of SDR are going to be on the software side, not hardware side. There is a significant need for a system-level tool that can encompass all the processors in the system."

Uhm's company offers an RF Network on Chip (RFNoC) to enable development and debug of FPGAs and processors for SDR system applications. (Figure 2.)

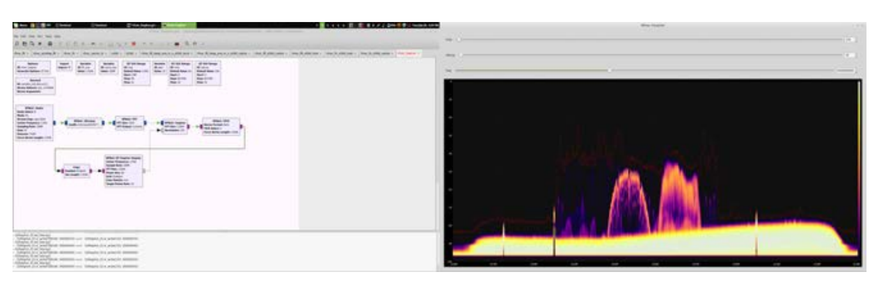


**Figure 2** | The RF Network on Chip from Ettus Research is an open-source tool for development and debug.

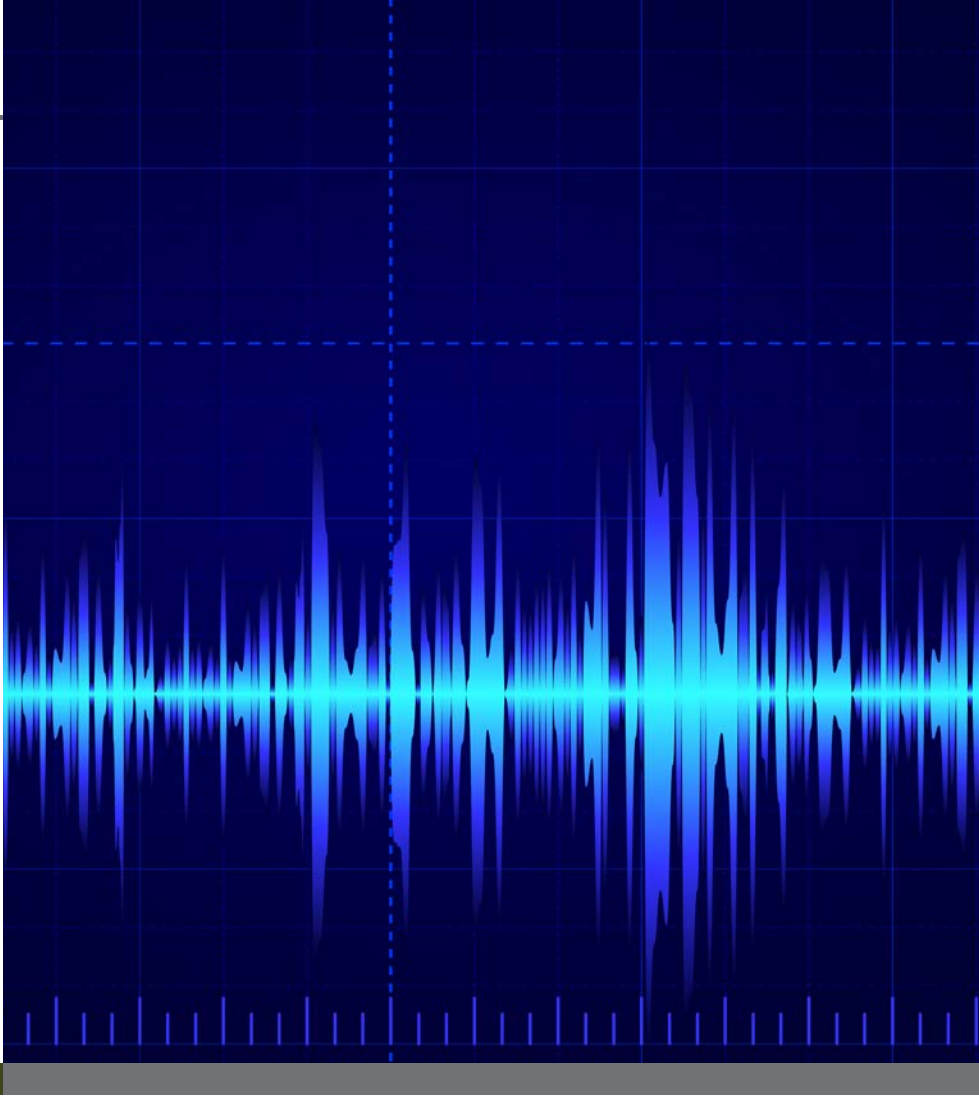
## Maintaining radios through standards

A standard that is helping with radio maintainability is the ANSI/VITA 48, VPX Ruggedized Enhanced Design Implementation (REDI), which defines the approach to module packaging and provides for two-level maintenance.

"One of the open standards our products conform to is VPX, which has numerous extensions to support evolving technology and military customer needs. One of these is VITA 48 or REDI, a ruggedized extension for VPX that provides two-level maintenance, which means a troop in the field can replace a module without having to send that module back to a repair facility," Hosking says. "That makes a lot of difference to our warfighters." **MES**

# SCA-based software-defined radios: Vision, reality, and current status

By Lee Pucker



*The SCA 2.2.2 architecture has achieved significant success in the military-communications market. Hundreds of thousands of SCA-enabled software-defined radios (SDRs) have been deployed to date; worldwide, dozens of programs are working to field more of these types of radios. The success of SDR lies in the benefits brought through adoption of the SCA specification: proven cost and delivery-time advantages, enhanced intercomponent interoperability, simplified insertion of new communications capabilities in deployed radios, and reduced development risk. Additional countries and new organizations have begun to explore the use of the SCA, which is driving a second generation of SDR market adoption.*

Recent market studies have shown that SDR technology has become ubiquitous in modern tactical communications systems, with the total market for SDR-based tactical radio production estimated at $5 billion in 2015. The reasons stated for the extensive use of SDR in the tactical radio market are twofold. First, the defense market generally does not command sufficient volume to justify the fabrication of ASIC-based radio technologies prevalent in the commercial wireless sector. As such, the use of off-the-shelf programmable processing technologies inherent in SDR is the norm, making the deployment of software-defined radios widespread. Second, equipment manufacturers and their customers gain significant advantages by utilizing SDR technology in an environment where migration to a new communication standard is challenging.

A key technology in the deployment of many defense-related SDRs is the Software Communications Architecture (SCA). The SCA is an implementation-independent architectural framework that specifies a standardized infrastructure for a software-defined radio. Initially developed and published by the U.S. Department of Defense (DoD), the SCA is maintained by the Joint Tactical Networking Center (JTNC) in collaboration with various industry partners and organizations, including the Wireless Innovation Forum. The specification has significantly influenced the evolution of the SDR domain and its concepts have been used within multiple industries, products, and countries worldwide.

## SCA: Key technology for SDR

Advances in digital processor technology, increases in analog-to-digital sampling rates, and other technological developments have enabled the continuing growth of complex signal processing in the digital domain. This increase in digital processing has appreciably altered the architecture and design of radio systems. Recent generations of SDRs evolved to become highly software-intensive, complex systems facilitating further advancement of communications capabilities. SDRs have enabled more cost-effective radio platform life cycles by providing for the update and addition of system functions and features without requiring hardware modifications.

Prior to the establishment of the SCA as an open standard, these SDRs were developed using proprietary software architectures that tightly coupled hardware platforms and waveform applications in a manner that was unique to each manufacturer. The SCA has built upon the capabilities of these preceding generations of SDRs, moving today's radios significantly forward by leveraging large-scale commercial software industry investments in technology and by promoting open standardization. The SCA specification and associated technologies facilitate broad software reuse and application portability across SDR platforms while enabling achievement of the key industrywide objectives:

- Enhanced interoperability between SDRs and across entire communications systems, which is especially critical for mission-essential communications.
- Reduction of the time and cost required to develop and deploy SDRs and associated systems, including the incremental rollout of new SDR and communication system features and functions.

The SCA provides a set of rules and constraints, which define the interactions between software applications (i.e., waveforms) and radio hardware platforms, leveraging an Object Oriented (OO) software paradigm and employing Component Based Development (CBD) technologies. CBD technologies are sometimes referred to the "industrial revolution" of software, fostering the advent of interchangeable software parts, built to predefined specifications. With CBD technologies, software components can be thought of as software integrated circuits with a set of defined functionality, performance, and input/output. Components can be assembled together to create entire applications, such as waveform applications for an SDR.

> "A KEY TECHNOLOGY IN THE DEPLOYMENT OF MANY DEFENSE-RELATED SDRS IS THE SOFTWARE COMMUNICATIONS ARCHITECTURE (SCA). THE SCA IS AN IMPLEMENTATION-INDEPENDENT ARCHITECTURAL FRAMEWORK THAT SPECIFIES A STANDARDIZED INFRASTRUCTURE FOR A SOFTWARE-DEFINED RADIO."

The SCA specification also defines a core set of open-system interfaces and profiles that provide for the configuration, assembly, deployment, and management of components, which ultimately comprise the software applications (e.g., waveform). The components of these software applications can be distributed across various SDR hardware processing elements in a manner determined by the platform developers that support the overall SDR requirements, hardware platform capabilities, and design, in conjunction with the SDR software design and configuration.

### Evolving beyond SCA 2.2.2

As with any technology, use in real-world environments highlighted improvements in the SCA specification that were necessary to enable further market penetration. Chief among these suggestions was improving the ability of the architecture to scale to address the size, weight, power, and cost (SWaP-C) requirements of certain radios, thereby enabling faster boot times, and improving support for the digital signal processors (DSPs) and FPGAs that are used in most radio architectures. At the same time, these improvements enhanced 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 to define its own SCA-based SDR software architectures.

To support these capabilities, a new evolution of the baseline specification was needed, so in 2009, the Joint Program Executive Office for the Joint Tactical Radio System (JPEO JTRS) initiated the SCA Next project. 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. The result of these and other efforts was SCA 4.0, which provided improved scalability and better support lightweight and ultra-lightweight environments for development on resource-constrained processors such as DSPs and FPGAs.

In 2012, management of the SCA for the U.S. DoD was transferred to the Joint Tactical Networking Center (JTNC). The evolution of the SCA continued in November 2013, with 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. 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

Successful deployment of SCA 2.2.2-based SDRs has identified improvements to be made to advance the technology even further. The Wireless Innovation Forum has worked in collaboration with the JTNC to evolve the SCA. The resulting SCA 4.1 specification represents the future of defense SDR technology. More than 2,000 hours were volunteered by member representatives of the Wireless Innovation Forum to develop these solutions. Their efforts resulted in five recommendations that have been incorporated into the SCA 4.1 Draft Specification:

- **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.
- **Naming conventions:** This recommendation proposes changes to the SCA 4.0.1 specification to use a naming convention for the interfaces and components, with the goal of improving the readability 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 enabling 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 (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 enable 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.

### Additional standards in 4.1 draft spec

The volunteer efforts also produced two new Wireless Innovation Forum SDR Standards that have been incorporated into the SCA 4.1 Draft Specification:

- **WInnF Lw & ULw application environment profiles (AEPs).** This SDR standard defines POSIX AEPs for interaction between SDR applications and the operating environment (OE) in resource-constrained architectures (Figure 2). Two base AEPs functions groups, the Lightweight (Lw) and the Ultra-Lightweight (ULw), are defined. The documents contains normative content for base AEPs functions groups plus support sections giving SCA-like contents-overview tables and detailed rationale for the design choices. It also provides two function groups that can extend the base AEPs function as required by the porting assumptions. This SDR standard harmonizes and improves prior work from JTNC and ESSOR into a single converged solution.
- **WInnF PIM IDL profiles.** This SDR standard defines Platform Independent Model (PIM) IDL profiles for the definition of application specific interfaces among SDR components. 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 which explains the design choices. This SDR standard also harmonizes and improves prior work from JTNC and ESSOR into a single converged solution.

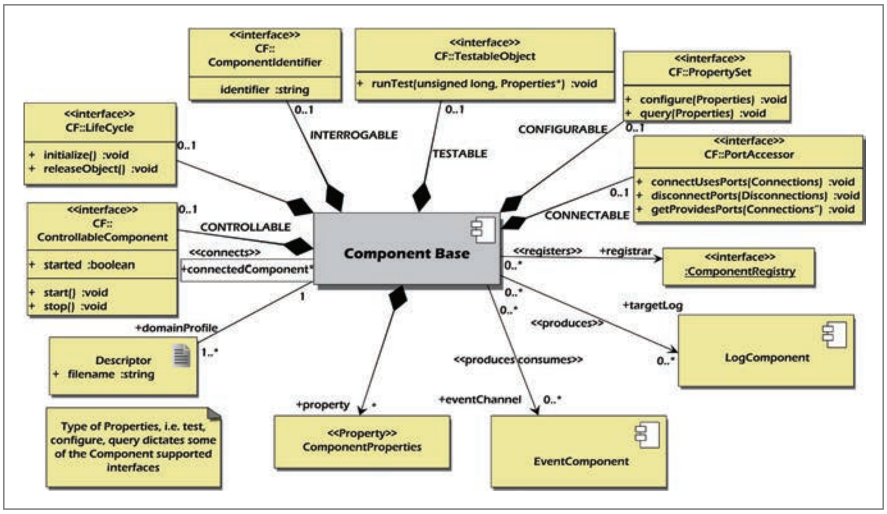


**Figure 1** | Proposed component base UML model.

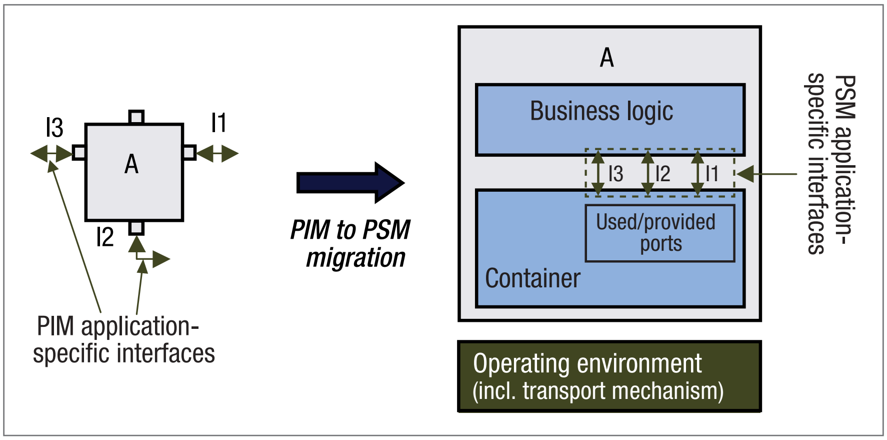

I3
A
I1
I2
PIM application-specific interfaces
PIM to PSM migration
A
Business logic
I3
I2
I1
Used/provided ports
Container
PSM application-specific interfaces
Operating environment
(incl. transport mechanism)

**Figure 2** | Positioning the PIM IDL profile usage.

### SCA 4.1 finalization and perspectives

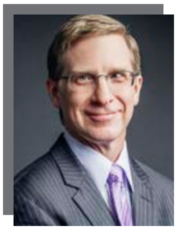
At the time of this writing, the SCA 4.1 Draft has been released by the JTNC, the comment period has closed, and the issues are being adjudicated by the Wireless Innovation Forum to include adding better support for multicore devices and other relevant technologies. The final specification is anticipated to be released by the end of this year. Early implementation results show that the proposed changes have been positive, with early adoption being considered in multiple products and programs. SCA 2.2.2 was in use for almost 10 years; it is anticipated that once released, SCA 4.1 will remain a stable, core reference specification for some time. Near-term enhancements to the SCA-based set of standards will likely lie, therefore, in the development and harmonization of application programming interfaces (APIs) completing the core specification. APIs in development or under consideration include:

- Dynamic spectrum access
- International security services
- Transceiver (WINNF Transceiver Next project)
- Enhanced timing
- Power management

A number of artifacts have also been discussed supporting the migration to this new specification, including an SCA 4.1 users guide, a SCA 2.2.2 to SCA 4.1 porting guide, and definition of industry-agreed metrics for measuring waveform portability.

### Future of radio in defense

SDR is a dominant technology in defense communications, bringing multiple benefits to radio manufacturers and their customers worldwide. The SCA is a proven framework supporting these SDRs, with more than 400,000 SCA-enabled radios currently in deployment. With its component-based design approach, the SCA has changed the way radios are developed, enabling a higher degree of deployment flexibility and leading to cost reduction when supporting multiple missions. From an original DoD vision of a standard military radio development architecture, the SCA – with version 4.1 – has moved forward as an international specification, with government and industry collaborating to leverage the technologies the SCA combines to advance radio communications as a defense capability. **MES**



*Lee Pucker is the CEO of The Wireless Innovation Forum, a nonprofit "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**
**www.wirelessinnovation.org**

NEXSYS
ARINC 429 TO DISCRETE SIGNAL CONVERTER
PART NO.: SR429-353-NPXAA
ARINC LABEL: 353
UNIT SPEED: 100 KBPS
PARITY: ON
OUTPUT: ACTIVE LOW
SDI BITS: ON, BIT 9=0, BIT 10=1

# Military software-defined radio benefits from commercial and consumer trends

By Darren McCarthy

*The pace of technology innovation, together with improvements in component technologies and amplifier design techniques used in the commercial wireless industry, have strong leverage into the requirements for military software-defined radio (SDR).*

U.S. Army Spc. Eligah Jackson communicates over the radio at the end of an observation post operation during a live-fire exercise on Grafenwoehr Training Area, Germany. Jackson is a forward observer assigned to the 2nd Cavalry Regiment field artillery squadron. Photo courtesy U.S. Department of Defense.

With commercial cellular technology accounting for more than two billion cellphones a year and millions of high-power infrastructure-access points (base stations, repeaters, microcells, picocells), the cellphone industry not only addresses our personal connectivity needs, but also connects our homes, automobiles, and devices. Three major trends in the cellular industry are directly applicable to the SDR needs of defense electronics: the increase in the spectrum used by the device, the increase in the waveform bandwidth, and (in consideration of these first two innovations) the ever-increasing need to improve radio-frequency (RF) power efficiency.

**Spectrum range increasing**

The commercial wireless technology follows reports and specifications created by the telecommunications organizational partnership known as the 3rd Generation Partnership Project (3GPP). The 3GPP standards called Long-Term Evolution (LTE) and LTE-Advanced have become the most rapidly deployed and adopted commercial wireless technologies in history. The 3GPP group plans advancements of the LTE technology and reports guidelines for the use of spectrum bands through staged releases on a near-annual basis. Looking at the progress, 3GPP Release 12 demonstrates an increase from 11 operating bands (3GPP Release 8) to 44 bands in the last four years. These spectrum bands are coordinated between national spectrum authorities, international guidelines, and wireless service providers to meet the growing demand of the commercial industry. Some fielded designs of popular smartphones address more than 24 bands. LTE technology is used between 450 MHz to 3.8 GHz today, and with the study of LTE-U (Unlicensed) technology, we could see the implementation of LTE technology reaching 6 GHz in the near future.

The impact of the wide spectrum range within the small form factor of a cell phone or a smartphone is that the RF front-end electronics need to become scalable and function over a much wider bandwidth. Designs from five years ago on a six band phone may have included separate RF paths for transmit and receive bands that contained RF filters and amplifier combinations. These separate RF paths were relatively narrow bands, which use a relatively small fractional bandwidth. For example, a frequency duplex band of 60 MHz at 2 GHz covers requires an RF design to cover only 3 percent of the fractional bandwidth of operation. At the component level, narrowband filters and amplifiers could be designed for optimum performance within these very specific bands.

With smartphone designs now operating across dozens of frequency bands, the scalability of narrow band RF designs is no longer practical. Consider an extreme design example, one that could operate across all 44 frequency bands of the Release 12 spectrum range. This would require the RF design to cover over 88 percent of the fractional bandwidth of operation versus the 3 percent fractional bandwidth of the banded method. While digital tunable filter technology has yet to meet the mainstream price and performance requirements to match this trend in commercial designs, the RF amplifier technologies have already adapted to the wide fractional bandwidth of use for many commercial designs. Filter technologies like Surface Acoustic Wave (SAW) and Bulk Acoustic Wave (BAW) have had tremendous technical advances in size and price to remain cost effective for relatively narrow fractional bandwidth and low power filter requirements.

The cellular infrastructure technology has undergone a similar challenge. To keep pace with a multiband cell phone the design drivers for cellular base stations are creating innovations in higher power technologies. For the higher power infrastructure applications covering broad frequency ranges, the advancements of gallium nitride (GaN) have now lead to commercial power transistors that have been designed for wideband performance with high power density.

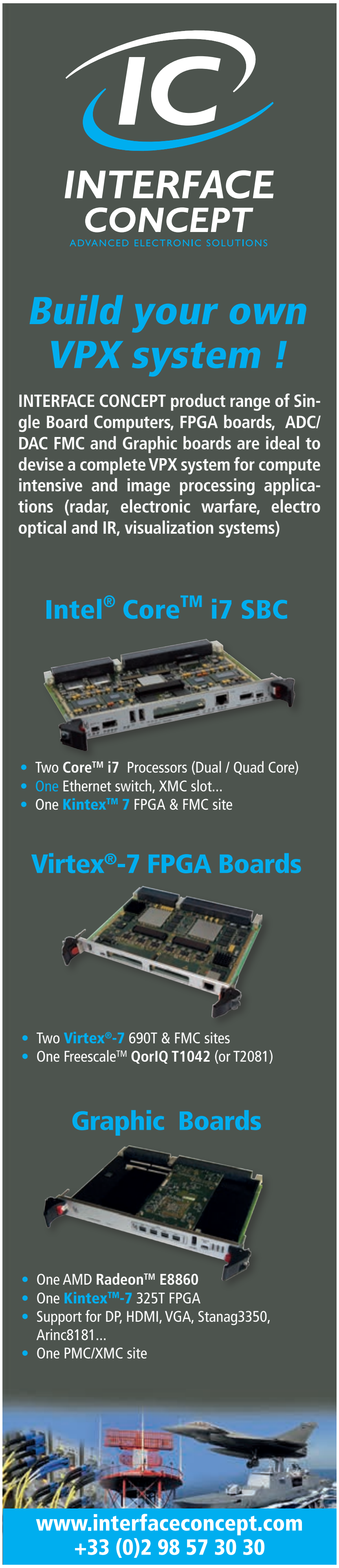
Related to the defense electronics industry, producing a cost effective RF front end for tactical radios has always been a challenge. While no longer a program, the traditional design goal of the Joint Tactical Radio System (JTRS) was to focus on the radio waveforms in the frequency spectrum between 2 MHz and 2 GHz. The operating frequency spectrum, power, and performance requirements of the different JTRS radio waveforms were a major technical barrier to the program. Newer radio programs are looking for more modest integration requirements.

Consider a current tactical multiband radio that currently operates between 30 MHz and 400 MHz. Support for tactical VHF would use the 30 MHz to 88 MHz spectrum, Air Traffic Control VHF between 118 MHz to 137 MHz, maritime VHF between 156 MHz to 174 MHz, and military UHF aeronautical radio and between 225 MHz to 400 MHz. A new requirement might take this existing tactical radio and add an integration requirement for the civil First Responder Network Authority (FirstNet) Band 14 in the upper 700 MHz band. Since the 10 Watt output power requirement of the Band 14 radio is similar to the power of some of the other VHF and UHF band radios, an integrated design might consider an architecture similar to one widely used in the commercial cellular infrastructure industry based on GaN with a shared RF amplifier component design to reduce size and weight of the radio.

In the GaN industry, there are fielded components from major suppliers that now support greater than 10 watts of power between 30 MHz and 2.5 GHz for tactical radio applications. This is over a 98 percent fractional bandwidth from a single RF amplifier device.

### Wideband waveforms

While LTE technology has a maximum signal bandwidth of 20 MHz, the LTE-Advanced technology from 3GPP Release 10 saw the introduction of carrier aggregation and carrier aggregation in noncontiguous spectrum increase the data rates delivered through the network. While the individual channel carrier still is limited to 20 MHz,



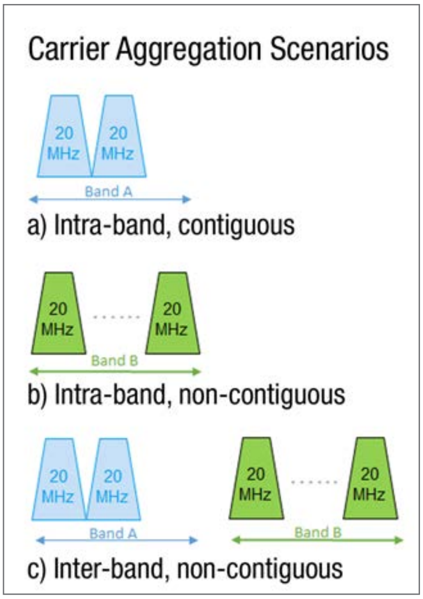

Carrier Aggregation Scenarios
20 MHz
20 MHz
Band A
a) Intra-band, contiguous
20 MHz
20 MHz
Band B
b) Intra-band, non-contiguous
20 MHz
20 MHz
Band A
20 MHz
20 MHz
Band B
c) Inter-band, non-contiguous

**Figure 1** | Carrier Aggregation Scenarios for increased data rates: a) intraband, contiguous; b) intraband, noncontiguous; and c) interband, noncontiguous.

if you consider the carrier aggregation scenarios shown in Figure 1, the bandwidth of the RF signal increases dramatically. A two-carrier contiguous intraband scenario shown in Figure 1a might have as much as 40 MHz output, while an intraband noncontiguous configuration in Figure 1b might have a signal bandwidth of an entire spectrum band (up to 75 MHz). Further, the interband configuration seen in Figure 1c between two separate bands could have several hundred MHz or even over 1 GHz of band separation.

The interband, noncontiguous scenario leads to the requirement for both the low-power cellphone and higher-power base station, creating essentially a single multi-signal waveform across the entire operation bandwidth. The filtering and power amplifier requirements to create this signal continue to be the major drivers of improvements to the component technology and amplifier design.

In the tactical radio environment, wideband waveforms are commonplace and have been used in the field for many years. Take, for example, the Link-16 radio that operates across the Aeronautical Radio Navigation Services (ARNS) band from 960 MHz to 1215 MHz: This radio covers 255 MHz of spectrum using frequency hopping and covers over 20 percent of the fractional band of operation.

### Improving RF efficiency

As cellphone technology improves in functionality, boosts data rates, increases RF bandwidth, and improves the size and quality of the graphical displays, one of the major drivers in the cellular industry is the continued focus on improving the RF efficiency of the devices. In the cellphone, the improved efficiency enables advanced functionality and longer battery life, but in the cellular infrastructure industry, the improved efficiency impacts the bottom line for a wireless service provider by reducing the operating expense of the network. In both cases, the cellular industry has driven improvements in the efficiency of RF devices.

When you consider the efficiency of the RF power within the context of increasing fractional operating bandwidth and signal bandwidth, mentioned previously, both the designs of the cellphone and the cellular infrastructure have driven toward using envelope tracking (ET) bias-modulated designs. (Figure 2.)

In an ET design, the envelope of the modulated signal is matched to the RF through the power amplifier by using an envelope detector and DC bias modulator controlling the supply voltage. With precise timing and matching of the amplifier nonlinear performance, the power amplifier can approach optimum efficiency when operated near the saturation points of the devices themselves.

Operating a component near saturation requires an analysis of the nonlinear device behavior that can vary due to the RF waveform and power level. Digital predistortion is typically used to compensate for the nonlinear effects and improve the spectral purity.

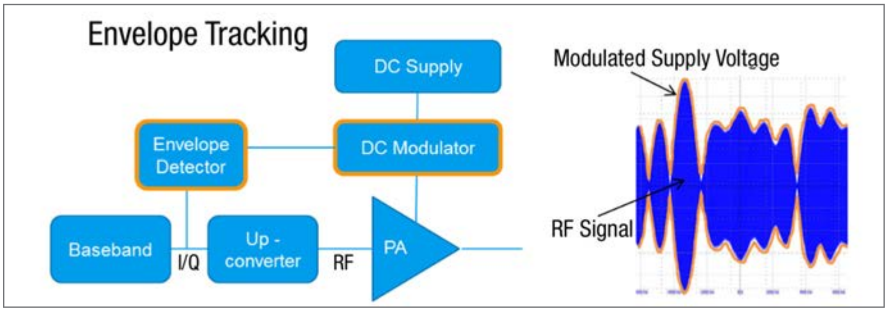
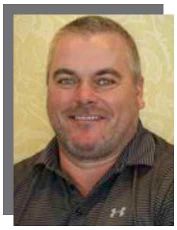


**Figure 2** | Envelope tracking block diagram and waveform.

**Figure 3** | The R&S FSW Signal and Spectrum Analyzer and the R&S SMW Signal Generator performs receiver testing, transmitter testing, and envelope tracking designs for designers of software-defined radios.

As the power amplifier might be used over a very large fractional bandwidth, the power device industry has improved the ability of amplifier components to operate over these larger bandwidths. As the signal of interest uses more bandwidth from the amplifier, whether a frequency hopping signal or multiband signal, it is important to choose the envelope detector and DC modulator that has enough bandwidth to match the wideband signal. The timing and shaping of the bias modulation needs to be carefully characterized. Envelope tracking designs are common now in the cellular industry and some amplifier designs have over 50 percent efficiency.

The Rohde & Schwarz FSW Signal and Spectrum Analyzer and SMW Signal Generator (Figure 3) is aimed at designers and developers of newer envelope-tracking designs directly applicable to use in SDR. **MES**



***Darren McCarthy*** *is the Aerospace and Defense Technical Marketing Manager for Rohde & Schwarz America. He has worked extensively in various test and measurement positions for more than 25 years. He has also represented the U.S. as a Technical Advisor and Working Group Member for eight years on several IEC Technical Committees and Working Groups for international EMC standards. R&S in several industry associations. Darren holds a BSEE from Northwestern University in Evanston, Illinois. Readers may reach him at Darren.McCarthy@rsa.rohde-schwarz.com.*

**Rohde-Schwarz**
**www.rohde-schwarz.com**

# Software-defined radio is key to seamless and effective military communication

By Stephanie Chiao

*To be ready for modern warfare, military communication on the battlefield needs to be interoperable, adaptable, and fast. Software-defined radio (SDR) is the solution that makes seamless communication on the battlefield possible.*

Software-defined radio provides the warfighter with not only standard two-way communication but also secure wireless nodes, multiple users, and low-latency point-to-point wireless links.

Military radio needs have evolved past basic voice and data communication; the warfighter now requires communication that uses several different frequencies and implements several different protocols. SDR has evolved significantly over the years and is able to cater to these specific needs.

Further, SDRs can be utilized for not only standard two-way communication but can also act as communication repeaters (allowing for different wireless devices to communicate with one another), offer secure wireless nodes, engage with a number of different devices concurrently, and provide very low latency point-to-point wireless links.

**What is software-defined radio?**

SDR can be defined as a wireless communication device where the receiver and transmitter functionality is changed or modified by software without making any physical changes to the hardware. It was essentially developed with the idea of software replacing radio tuners and filters. This structure in turn eliminates the need for using resistors and capacitors, as software-based filtering algorithms can be used to select specific frequencies. Such a setup still requires a flexible enough hardware platform; today's designs are ensuring that devices all incorporate this feature.

Although there are different architectures implemented for different SDRs, one high-performance design separates signals from high band and low bands (baseband). Figure 1 outlines the architecture and the steps through the receive chain. The signal is first sampled from the antenna; the analog signal is fed through an RF switch based on the frequency of the signal being sampled. High band is reserved for signals greater than a certain threshold, while the low band is reserved for signals lower than the threshold. Within the respective RF chains (high and low) the analog signal is filtered and divided into "I" and "Q" channels for advanced signal processing on a FPGA or other processor. The high band offers low-noise amplifier (LNA) for weaker signals plus a frequency mixer for desired intermediate frequencies prior to signal processing. The low band offers a varactor circuit to fine-tune the delay between the "I" and "Q" channel. An analog-to-digital (ADC) driver is common between both bands (high and low) prior to the ADC. The ADC will send the data across to the DSP chain within the FPGA using a serial interface.

On the software side, the algorithms are both downloadable and adaptable over the life span of the radio hardware. This capability makes SDR flexible and ideal for military and defense applications. Today's SDR is capable of more than data and voice transmission and its popularity is driven by the ability to implement new functionality on the device through software. Before SDR entered the marketplace, functions like encoding/decoding and modulation/demodulation were all hard-wired. That situation has since changed, however, and tasks such as migration, changes in frequencies, and modulation schemes can be performed simply modifying the software.

### SDR in military communication

In times of conflict, military communications significantly depends on adaptability, clarity, interoperability, precision, and speed. Deficiencies in any aspect of military communication can have dire consequences. As a result, SDRs have grown to have a significant influence on defense mechanisms as the device provides for not only standard two-way communication, but also offers secure wireless nodes, engages with a number of different devices concurrently, and provides very low latency point-to-point wireless links. Further, SDR can also act as a communication repeater.

The defense industry today is currently engaging in monitoring and communications activities on several different frequencies (HF, UHF, and VHF). They also operate using several different protocols (Bluetooth, CDMA, GSM, LTE, and WiFi). Traditional equipment offers military personnel the ability to tune into only one of the preferred frequencies and support only one protocol. With SDR, however, those on the battlefield are able to monitor and communicate over a large portion of the spectrum while supporting multiple protocols.

Not all SDRs are the same, so it is important to highlight some of the important features of SDRs that enable the most applications. The key features, brief description, and how it relates to end applications are highlighted in Table 1 (on following page).

### SDRs are highly portable

The weight carried by soldiers has always been an issue, as it can affect how quickly military personnel can move on the ground. As a result, the military has always searched for ways to make equipment lighter and more portable. In the past, soldiers would have had to carry multiple radios on the front lines, which could essentially hinder their movements and capabilities. SDR has been able to reduce size, weight, and power (SwaP) for

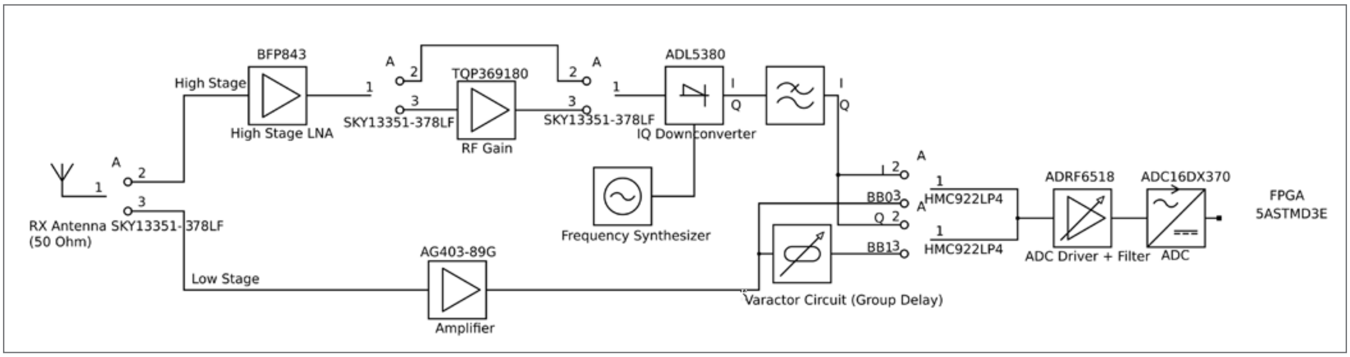


**Figure 1** | Receive architecture separating high band and low band.

those in battle, as it is one device replacing multiple radios. This portability is one of the reasons why the defense-industrial complex has increased its spending to obtain new radios developed for the military that are based on SDR.

### The future of military SDR

SDR has come a long way since the early days when process technology limited the amount of processing, and therefore the capabilities of SDR. At the present time, SDRs are network-control devices and communication repeaters, but in the future, experts predict SDRs to also act as:

- Biological-weapons detector
- Chemical detector
- Nuclear detector
- Area mapper
- Tool for situational awareness
- Tool to offer data on the availability of support
- Tool with the ability to call in an airstrike quickly

With the introduction of SDR, the need for a new military-communications standard was clear. Communication devices on the field needed to be adaptable, clear, interoperable, fast, portable, and light to ensure seamless and effective communication. In the future, SDR is expected to be augmented into cognitive radios that can survey the area, choose the best frequencies, determine and engage in electronic warfare, and set up an ad hoc network on the fly for clear communication.

| Specification | Description related to application |
|---|---|
| Operating frequency | The tunable frequency range that the equipment can operate in (e.g., DC – 6 GHz). This will directly impact the ability to monitor and communicate in specific bands. |
| Number of radio chains | Number of receive and/or transmit chains which are used to tune to the area of interest. For example, if you have two chains, you would be able to tune in to 850 MHz and 1900 MHz concurrently. |
| RF bandwidth | The amount of spectrum that can be captured/visualized at any given time. For example, if you have 50 MHz of bandwidth and tune to a center frequency of 860 MHz, you would be able to capture all data from 835 MHz to 885 MHz. |
| Data transfer link | The method of transferring data from the SDR to a host computer or storage device which is directly related to amount of data transfer and transfer speeds. |

**Table 1** | Key specifications of software-defined radios and related applications

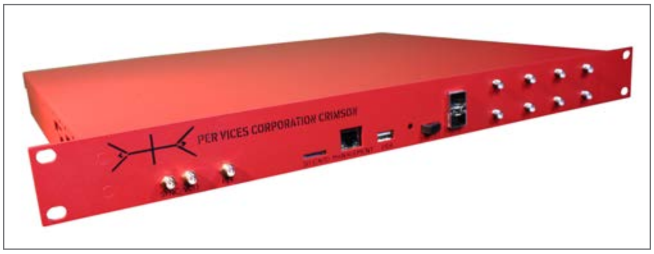


**Figure 2** | The Crimson SDR has four independent receive and four independent transmit chains, each able to carry 322 MHz of RF bandwidth up to 6 GHz.

One platform for SDR technology is the Per Vices Crimson SDR (Figure 2). It operates from DC to 6 GHz with over 1 GHz of RF bandwidth spread across four independent chains (each chain offers 322 MHz of bandwidth). Crimson supports the most common communication frequency ranges: 700 MHz to 950 MHz and 1.7 GHz to 2.6 GHz, while providing the architecture to cleanly sample a signal and/or provide a low-latency link. **MES**

***Stephanie Chiao*** *is the Product Marketing Manager at Per Vices Corporation, where she is responsible for marketing strategy, technical promotion, and media relations. She brings over eight years of consumer and enterprise marketing experience and has worked with brands including Microsoft, Rogers Wireless, and Torstar Corporation. She holds an Honours Bachelor of Business Administration degree from the Schulich School of Business in Toronto. She may be reached at stephanie.c@pervices.com.*

**Per Vices Corporation**
**www.pervices.com**

protomold
PM-F0
PM-F1
PM-T1
PM-T2
SPI-B1
SPI-A2
SPI-C1
<-Knit lines
straight pull

# Refuse to Let Design Fall Flat

Proto Labs is the world's fastest manufacturer of prototypes and low-volume parts. To help illustrate the design challenges encountered with injection molding, we created the Design Cube. See thin and thick sections, good and bad bosses, knit lines, sink and other elements that impact the moldability of parts.

Get a FREE thermoplastic Design Cube at
**go.protolabs.com/MY5CA**

ISO 9001:2008 Certified | ITAR Registered
Major Credit Cards Accepted | © 2015 Proto Labs, Inc.

ADDITIVE MANUFACTURING
CNC MACHINING
INJECTION MOLDING

proto labs®
Real Parts. Really Fast.™

# Taking on encryption's usability and key management problems

By Sally Cole, Senior Editor

*Encryption is not particularly easy to use, but efforts are underway to solve its key management and usability problems to bring it into datacenters and possibly even help it finally go mainstream.*

Encryption is an elaborate mathematical tool primarily used for cloaking data and communications to ensure that they aren't accessed or tampered with by unauthorized parties. An overly simplified explanation is that to encrypt and decrypt data you need keys to "lock" and "unlock" the data. When attackers attempt to steal this data in encrypted form, without the right key, it's unreadable and useless to them.

Unfortunately, encryption isn't as easy to use as it sounds and its widespread use has been held back by basic usability and key management problems.

If you've ever heard the term "military encryption" and wondered how it differs from "normal encryption," you're not alone. They rely on identical mathematics and approaches to protect information.

The subtle difference lies in "the manner in which the cryptographic capability is implemented," says John Droge, director of secure information services for Raytheon's Space and Airborne Systems business in Waltham, Massachusetts (www.raytheon.com). "Military-grade cryptography takes added precautions to ensure the key material is safe at all times."

One way to ensure safety is by designing a system with a separate processor that performs all cryptographic operations. "All key material is delivered to and stored on the system in an encrypted format," Droge elaborates. "When a cryptographic operation is scheduled, the key material is loaded, decrypted, used as intended, and finally destroyed – all in the dedicated processors. This protects the key from being exposed in an unencrypted form. So if at some time the system is infected by an advanced persistent threat (APT), at best the attackers will only gain access to an encrypted version of the key, which is unusable."

It's important to point out that both software and hardware approaches can be vulnerable. Those serious about encryption on end points tend to use hardware security modules (HSMs) to do the key management aspect of encryption in a separate "trust" domain within hardware.

Pushing encryption into the hypervisor via a software-defined networking (SDN) approach is another way to move key management into a separate trust domain that would need to be compromised. An APT on the end host won't have access to the hypervisor memory, and hypervisors are compromised much less often than end points.

Yet another way to go about it is to opt for a secure operating system.

**Encryption's usability and key management problems**

With all of the huge data breaches occurring, it raises the question: Why isn't encryption used to protect data everywhere?

Encryption is "extremely difficult to implement correctly and very easy to get wrong," explains Lillian Ablon, an information systems analyst for Rand Corp. in Santa Monica,

California (www.rand.org). "Even when implemented correctly, there can be hurdles with key management or setting up the infrastructure to handle the key management. But if you collect data, you need to protect it – whether it's intellectual property or access to a database or, for example in the military's case, something like mission-critical air tasking orders. Any pains involved in setting up encryption and the key management infrastructure are well worth the security it provides."

Key management is "typically the main reason cited for not implementing encryption. No question about it – key management is the most difficult discipline within cryptography and requires extreme attention to detail by every vendor and user/operator in the information ecosystem and at every point in the data's life cycle to achieve a secure cryptographic system," says Raytheon's Droge.

Essentially, although encryption has existed for quite some time, no one has ever found a way to make it practical or easy to use.

**Bringing encryption to the datacenter**

One place you're not likely to find encryption is within datacenters. It's not commonly used because encryption is considered too complex to handle the keys for all of the end points involved, and no technology is currently available to help handle this.

Virtualization software giant VMware in Palo Alto, California (www.vmware.com) is working to change that by adding "distributed network encryption" to their software-defined networking (SDN) platform, NSX, with availability at some point in the near future. This platform has the potential to radically change network security, particularly for those already using virtualization.

> HOW CAN SOMETHING LIKE DISTRIBUTED NETWORK ENCRYPTION HELP THE MILITARY? "ONE OF THE BIGGEST PROBLEMS THE MILITARY FACES WITH ENCRYPTION IS THAT THEY'VE GOT MANY PEOPLE WHO NEED TO COMMUNICATE IN MANY DIFFERENT WAYS … IT'S A MASSIVE KEY MANAGEMENT NIGHTMARE," SAYS MARTIN CASADO.

VMware's goal is to enable deploying encryption as an application with NSX – complete with microsegmentation, different trust levels for workloads, and the ability to encrypt, authenticate, and verify all communications. Not up to speed with SDN? NSX is one of the very first examples of SDN, which relies on a set of primitives that can be controlled by software, independent of the physical devices – including white boxes – beneath.

Many people who are unfamiliar with SDN express security concerns about these new types of architectures, but SDN was created with security as its foundation and, in fact, received its initial backing from the intelligence agencies.

NSX embraces a "zero trust" model and taps the hypervisor for the isolation it provides for security. "Pushing encryption into the hypervisor pushes it into a separate trust domain that would also have to be compromised," explains Martin Casado, one of the visionaries behind SDN and NSX, as well as senior vice president and general manager, Networking & Security Business Unit for VMware.

Another frequent misconception surrounding SDN is "white boxes." As Casado notes, however: "SDN is orthogonal to white boxes. You can use white boxes if you want, but across our 700-plus customers and now well over 100 production deployments, I don't know of a single one using white box."

Then, of course there's the "controller," which people tend to assume would be easy to attack, when in fact NSX runs it on a remote compute node so it's not even addressable.

So how is encryption being rolled in? NSX "allows you to think of an application as having encryption as an attribute," Casado says. "To deploy encryption as an application, you'd basically click a button and all communications within that application would be encrypted with a secret only known to that application."

If an attacker ever gains access to the datacenter or compromises a physical machine, all the information they'd see will be completely encrypted. "And you'll be able to choose on a per-application basis whether you want to encrypt or not," adds Casado. "This helps solve the broader problem of making it practical to use encryption and handle key management in a very controlled, fine-grained way."

How can something like distributed network encryption help the military? "One of the biggest problems the military faces with encryption is that they've got many people who need to communicate in many different ways … it's a massive key management nightmare," Casado says.

Say, for example, you're in a datacenter while a mission is happening and you want to spin up a bunch of workloads. "For every one of these missions that you spin up, you can encrypt it, and then if there's a compromise within the datacenter or someone manages to gain access to the traffic from a separate mission … they won't be able to see anything because it's all encrypted," he adds. "Today, it's too difficult to manage keys at the edge of the datacenter, so we use VPN [virtual private networks], which allows people to do encryption to a gateway at the edge, but the problem with that is that within it everything is moving in plain text."

Approaches such as "the one VMware is pursuing with network distributed encryption, along with others who are working on regenerative computing – something those in cloud services are exploring to 'regenerate instances' on a faster time frame – are really interesting if they can make attackers' job more difficult. It's not possible to be 100 percent secure, so the goal of information security instead should be to make it as difficult as possible for attackers in terms of time, money, resources, people, and technical capabilities," says Rand's Ablon.

Startup Keybase (www.keybase.io) is another effort Casado is affiliated with to make encryption more user-friendly via using Twitter handles and email addresses as your public key "so you won't have to remember some goofy stream you can't verify," he says. "It's a practical approach toward solving the outstanding problem in encryption – making it usable."

### R00t of insecurity

With each new data breach – including the recent Office of Personnel Management (OPM) breaches that involved the theft of records of at least 21.5 million individuals, including highly personal security-clearance information and even fingerprints – it becomes more obvious that encryption or other forms of security are necessary to protect sensitive data.

"OPM could have benefited from very standard use of authentication management, two-factor authentication or better access control, updating patches, rethinking their architecture, and by using encryption," Ablon notes. A new security mantra is: 'Don't collect it if you can't protect it.'"

So what's the root of "insecurity"? Two key elements are humans and software vulnerabilities.

### The human element

"Here's the root of insecurity: Humans are interacting with technology, so even with the most secure systems in the world, the odds that human weaknesses will be taken advantage of are quite high. A phishing email with a malicious attachment can easily thwart security," Ablon says.

Phishing emails, a type of social-engineering attack designed to target

you specifically, can be devastating. “A few years ago I received a sweet birthday email from ‘my sister,’ complete with photos of us when we were kids and more recent ones, along with a link to go view a greeting for the card,” Casado recalls, providing a real-life scenario. “My first thought was how nice, but my sister doesn’t usually remember my birthday. After closer inspection of the email header … it was from Russia.”

At the time, Casado was VPN’d [virtual private networked] into the back end of the datacenter at work. If he had clicked the link, the attackers could have downloaded malware onto his laptop and had access to the entire datacenter – all of the information moving in plain text.

Although the attackers would have gained a foothold into the datacenter – and this is likely to happen at some point – with an approach like distributed network encryption, any traffic they’d see would be encrypted and useless to them.

“We definitely advocate pushing encryption into the datacenter,” Casado says. “Both distributed firewalling and distributed network encryption can really help to evolve a security posture within datacenters.”

### Software vulns

One other factor behind network and system insecurity is software vulnerabilities, which exist because it’s difficult to locate all of the bugs within code.

“After a thorough review of several code bases, we found that there typically exists one bug per 2,000 lines of code,” Ablon points out. “Not all bugs are vulnerabilities that can be taken advantage of, but a smaller subset are and will be. That said, common operating systems use roughly 40 million lines of code. Aircraft and vehicles use 20 to 30 million lines of code, so plenty of potentially exploitable vulnerabilities exist.”

When developers are creating code, “there tends to be a ‘get it done and make it functional’ mindset, so a shift toward a mindset of including secure coding in curriculums either before or at the university level would be helpful,” she adds. “It’s extremely rare to find people with computer science degrees who were taught secure coding … especially the next generation who will be creating code and setting up systems and networks, as well as creating the web pages or devices we’ll be using.”

### Quantum future

While many are exploring ways to make encryption easier to use, the National Security Agency (NSA) is focused on an entirely different aspect: quantum computers that could potentially break encryption as we know it today.

Techniques for encryption are continuously evolving, and the NSA is currently preparing for a shift to algorithms considered to be resistant in a future with quantum computers by “working with partners across the U.S. government, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next suite of cryptographic algorithms.” For more about NSA’s encryption plans, visit www.nsa.gov/ia/programs/suiteb_cryptography/. **MES**

# Encrypting storage in small form factors

By Carey Johnson

Small-form-factor encrypted storage is key to satisfying military data-security requirements regarding "data at rest." U.S. Army paratroopers conduct a radio check with a portable radio after calling for close air support during a training exercise at Pocek Range in Postonja, Slovenia, May 11, 2015. Photo courtesy U.S. Department of Defense.

*Self-encrypting storage devices are becoming increasingly popular in embedded systems. Whether employed in the commercial space to prevent end users from modifying manufacturer-installed software and policy (e.g., mobile-phone "rooting") or used in government systems to secure sensitive data against sophisticated adversaries, the threats and general threat-mitigation mechanisms remain the same.*

The primary use for encrypted storage – whether implemented in software, firmware, or hardware – is to satisfy security requirements concerning "data at rest"; that is, requirements for protecting data while it resides in nonvolatile storage. While it may seem obvious that encrypting data while it is at rest will satisfy the letter of the requirement, caution is nonetheless warranted regarding the handling of cryptographic keys.

## Why small form factor?

Increasingly, computation in military systems is moving to mobile devices. If such mobile devices are tied to data sources via cabling or wireless networking, then their flexibility and/or battery life suffers. As a result, mobile devices commonly store (or cache) any data necessary for their operation locally.

A second common motivation for small-form-factor storage relates to system sanitization: To more easily sanitize sensitive data from complex systems, it is frequently helpful to isolate the storage and usage of such data in a removable module. Since such a module is often carried away with the operator as part of standard operating procedure, a pocket-sized form factor is a convenient choice. (Figure 1.) Note that these motivations in favor of small-form-factor storage directly imply a heightened risk of loss, and therefore motivate enhanced security for their data while at rest.

## What is encryption, really?

At its most abstract level, encryption is an invertible means to replace a meaningful message with one that is meaningless. There are two general ways this is accomplished: Symmetric ciphers define a bijection (one-to-one mapping) between the space of meaningful messages (plaintexts) and the space of meaningless ones (ciphertexts). In contrast, asymmetric ciphers compute a mathematical identity in two or more distinct steps, such that "encryption" moves to an intermediate result (ciphertext), and "decryption" completes the identity, returning to the original value (plaintext).

If the underlying mathematical primitive (i.e., bijection or identity-in-use) is well-known or predictable, then anyone can recover the plaintext for a given ciphertext. This is where the keys enter: Successful cryptosystems select the mathematical primitive to be used – from a very large pool of possible

primitives – using the key. AES-256 is a shorthand way to represent $2^{256}$ different block-sized lookup tables, where the key selects which one to use. Without the key, a malicious user cannot practically determine the underlying mathematical primitive.

The critical observation is that encryption alleviates concerns about revealing the plaintext. It does, however, generate a new concern: protecting the key against exposure. Attempting to protect the key via encryption would yield an infinite recursion. Therefore, encryption offers a transformation of the data-confidentiality problem, not a solution. The task of protecting arbitrary data is transformed into the task of protecting a key with a fixed form.

### Securely leveraging small-form-factor encrypted storage

Self-encrypting storage devices must secure cryptographic keys without the aid of cryptography. The need to manage the cryptographic keys is the fundamental engineering challenge in producing secure systems that leverage self-encrypting storage. Listed below are some common security scenarios for military systems and several strategies by which small self-encrypting devices can be leveraged to help provide solutions.

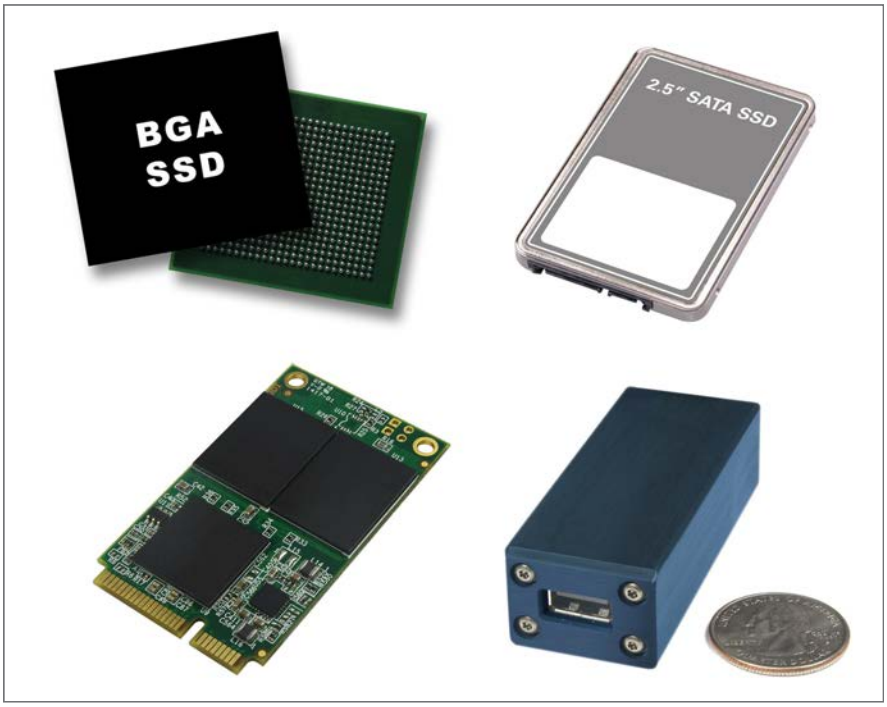


**Figure 1** | Small-form-factor storage enables portable devices. Shown are 2.5-inch SSD drive, mSATA, BGA, and custom module (memory module).

### Purgeable persistent random keying

The inherent risk of military operations sometimes leads to equipment loss, such as the 1999 downing of the F-117A Nighthawk over Serbia, or the modified Blackhawk reportedly lost during the 2011 raid on Osama bin Laden's compound in Pakistan. In cases where weapons systems gain their tactical advantages though advanced software or specialized data, it is imperative that these critical technology elements be rendered permanently inoperable before abandoning the equipment.

This status can be achieved by a self-encrypting storage device that supports persistent static keying if the device is initialized with a high-quality random key. During an abandonment event (e.g., pilot ejection), the random key is immediately cleared. Presuming no record of the key persists, the hosted software and data is rendered immediately unrecoverable while subsequent sanitization procedures execute. As military systems continue to miniaturize and adopt mobile paradigms, small-form-factor self-encrypting storage solutions will play this role with increasing frequency.

### Purgeable persistent user-specified keying

Other systems benefit from having data rendered temporarily unrecoverable. Consider the protection of data recorded during mission execution; such data can reveal tactics or even overarching strategic objectives under intelligence analysis. However, this data is also valuable for enhancing and optimizing tactics for future operations. In cases where recorded data is carried away from a weapons system on mobile media, there is a heightened likelihood of physical loss. Ideally, such physical media should be rendered inoperable during the transit between the weapons system and its secure destination.

This objective can be supported by a self-encrypting storage device that is initialized with a user-specified key before accepting data, and then purging the key for transport. Upon reaching the secured destination, the device can be rekeyed with the same key to re-enable access to the data.

### Volatile keys

In contrast to the preceding scenarios, which respond to an explicit purge command or signal, many systems desire to satisfy their data-at-rest needs by automatically rendering data unrecoverable when power is removed. This strategy is frequently used to reduce protection requirements in designs for systems that must use algorithms and data that are considered "critical technology," but which can offload storage-at-rest of these items to another system. In this usage, the self-encrypting storage acts as a secure volatile cache.

To support this scenario, a self-encrypting storage device simply needs to guarantee that it will hold no remnant of the filled key once power is removed. This may require use of remanence-resistant memories or other technologies to ensure key clearage.[1] Applications arise where a smaller slave system assists a more secure system; for example, an XMC form factor single-board computer attached to a larger system.

### Authenticated key derivation

Many systems do not require autonomous unmanned power-up. When an operator is available, one has the option to protect persistent cryptographic keys by storing them as a split between a persistently stored value and a value derived from an operator password. Any mobile device with a user interface – such as radio, GPS units, and pilot kneeboards – can require the operator to participate in securing cryptographic keys.

A strong password in conjunction with a cryptographically sound password-based key-derivation function can produce a significant barrier to key recovery, even for an adversary with physical access and destructive reverse-engineering capability.

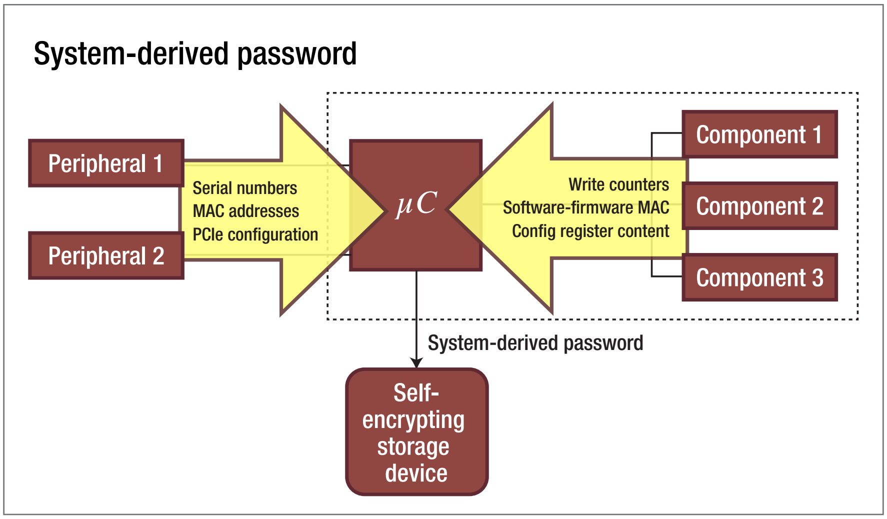


**Figure 2** | Data sources for system-derived password.

**Figure 3** | TRRUST-Stor solid-state devices, engineered specifically for defense applications, can be used in data recorders, ruggedized mobile systems, mobile man-packs, and ground vehicle applications.

To support such an authenticated key-derivation scheme, a self-encrypting storage device must implement little more than a hybrid of the persistent-keying and volatile-keying models described above. If one populates the volatile key by combining the persistent key with the outcome of a password-based key-derivation function, then one has the desired behavior.

Since strong passwords can be difficult for users to remember, considerations must be given to the human-factors side of the design. A password consisting of eight alphanumeric characters represents a space of only $36^8 \approx 2^{41}$ possible passwords. To mitigate the feasibility of a brute-force exhaustion of the password space, significant delays should be introduced after a few incorrect authentication attempts. Higher-security scenarios may also desire permanent disablement (purging of the persistent split of the key or erasure of the drive) upon continued authentication failure.

Additionally, consideration must be given to the eventual need to change passwords, either through security policy or personnel loss. An ideal solution should not require the storage device to be repopulated from scratch when updating the password.

### System-derived password

An enhancement to the authenticated key-derivation approach can be made by removing the human factor from consideration. For example, consider a system that desires to bind the operation of a self-encrypting storage device to a host environment into which it is embedded. Rather than an operator-supplied password, the password can be derived from data strings present in the system (Figure 2).

Applications for this technique arise where common portable devices are used to provision data for specific systems in a secure environment, but which then move into a hostile environment.

Consider, for example, that a pilot provisions his mission-specific data onto the flight computer of his aircraft using common hardware. For safety reasons, it is desirable to retain the mission-specific data in case it must be re-provisioned to the aircraft; however for security during deployment, it is desirable that the mission data be rendered to a form such that it can only be read by the specific aircraft. This can be achieved by re-encrypting the mission-specific data on the portable hardware using a system-derived password – effectively a "password change" in the context of authenticated key derivation.

### Continuing interest

Given the emerging role of small-scale self-encrypting devices in modern military embedded systems – particularly identifying key management and data confidentiality for such systems as the primary security concern – designers should also consider the topics of side-channel analysis, device sanitization, selection of appropriate cipher modes, and the potential for surreptitious interposition of malicious hardware between a self-encrypting storage device and its host system as a means to acquire encrypted data.

To assist designers, Microsemi has designed a family of self-encryption storage drives called TRRUST-Stor that fit into small-form-factor applications. These solutions focus on protecting data at rest in a threat environment using similar keying techniques. (Figure 3.) **MES**

### Reference

1 J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. "Lest we remember: cold-boot attacks on encryption keys," *Communications of the ACM* 52, 5 (May 2009), 91-98. DOI=10.1145/1506409.1506429 http://doi.acm.org/10.1145/1506409.1506429

***Carey Johnson** is the SSD Application Engineer at Microsemi, where he supports the company's SSD business. He has worked in the microelectronic industry for more than 20 years in applications, product, and tactical marketing roles for leading global semiconductor companies. Carey holds Bachelor of Science degrees in electrical and mechanical engineering from North Dakota State University. He can be contacted at cjohnson@microsemi-phx.com.*
*(Scott Miller, Principal Scientist, Microsemi, also contributed to the article.)*

**Microsemi • www.microsemi.com**

# Nanoscale "memristive" RF switches enable on-the-fly IC reconfiguration

*By Sally Cole, Senior Editor*

Superfast nanoscale radio frequency (RF) switches crafted by a team of University of Massachusetts, Amherst researchers are boasting reprogrammable features akin to those involved in interneuron communication.

Reconfigurable RF systems in use by the military today depend upon the availability of tiny switches that can be integrated into chips and easily reprogrammed to serve different RF functions. So far, though, the use of reconfigurable RF switches has been severely limited by performance drawbacks such as added noise, size, power consumption, functional instability, and a lack of durability.

Now, new nanoscale RF switches based on memristor technology can overcome these challenges, thanks to a collaboration that combined the expertise of two assistant professors within UMass Amherst's Electrical and Computer Engineering department, Joseph Bardin and Qiangfei Xia.

Professor Bardin's main area of expertise is RF devices, circuits, and systems, while Professor Xia is an expert in nanoscale memristive devices.

Both Bardin and Xia received the U.S. Defense Advanced Research Projects Agency (DARPA) Young Faculty Award (YFA). "Our collaboration was encouraged by DARPA's Microsystems Technology Office Director Bill Chappell, who served as our mentor within the YFA program," Bardin says.

So, what exactly is a memristor and its role in the "nanoscale memristive RF switches" invented by the duo? "It's essentially a nonvolatile device whose resistance depends on the history of the current/voltage applied to the device," Bardin explains. "By using appropriate programming protocols, the DC resistance of these devices can be switched over ten orders of magnitude. There are many flavors of memristors, but the device that we demonstrated is specifically tailored for RF applications by minimizing OFF-state capacitance and ON-state resistance."

Reconfigurable RF systems are desirable for reducing the parts count in communications and radar systems. "A typical cellphone has several front-end chips, for example, each of which serves to receive a specific communications band," Bardin says. "Emerging reconfigurable RF technologies promise to enable the development of single-chip solutions where the front end can be reconfigured on the fly for the desired functionality."

What's in Xia and Bardin's switches? Just two conductive elements – a pair of gold and silver electrodes – separated by an air gap of 35 nanometers. Specific changes in voltages or currents within these switches trigger the formation of disintegration of conductive silver filaments between the elements, resembling a neuron firing, in which tiny gaps are briefly and reversibly bridged by chemical neurotransmitters to allow electrochemical signals to move from one neuron to the next.

The key significance of this work is that "compared to other RF switches, our memristive RF switch is orders of magnitude smaller in device size, but nonetheless achieves quite promising performance, even outperforming some of the metrics of other state-of-the-art technologies," Bardin notes.

The biggest tech surprise along the way for Bardin and Xia? Simply that the switches worked as well as they did.

They expect the key application of their work to be "the integration of large numbers of switches directly into an IC to enable highly reconfigurable architectures that aren't feasible today because of the large physical dimensions of today's state-of-the-art RF switches," Bardin explains.

The switches' ability to enable on-the-fly IC reconfiguration, could allow the military "to reconfigure a device to act as either a satellite receiver or a radar," he points out. This means users can make the device behave like a cellphone signal emitter, for example, then quickly reprogram it to serve as a collision-avoidance radar component or local radio jammer.

"The nanoscale dimensions of these switches, their performance, and the relative simplicity with which they can be integrated into existing chip technology bodes well for their inclusion within a new generation of reconfigurable RF chips," says DARPA's Chappell. "These switches can change from one type of radio to a completely different type, all without a hardware change. We can even use one chip set to switch from a communications system to a radar, which are traditionally very different designs."

The timeline for this technology? Still at least several years out. "There are open issues that we need to resolve," Bardin says. "We plan to work on improving the endurance – number of times the device can be reconfigured – and RF power-handling capabilities."

DARPA's YFA program (www.darpa.mil/work-with-us/for-universities/young-faculty-award) identifies and engages rising research stars in junior-faculty positions at U.S. academic institutions and introduces them to Department of Defense (DoD) needs and DARPA's program-development process. YFA awardees receive a $500,000 grant for a two-year period, with an opportunity to be considered for another $500,000 under the DARPA Director's Award.

# Great things do come in small packages.

## Acromag ARCX
### Small Form Factor Embedded Computer

The ARCX rugged mission computer offers great flexibility to meet ever-changing requirements with unique expansion features.

PMC/XMC/Mini PCIe/mSATA slots for specialized I/O, memory, and FPGA modules.

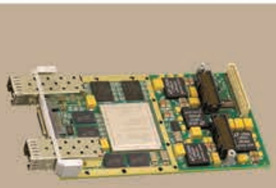
MIL-DTL-38999 connector front panel has options for a custom I/O power filter.

The front panel can be also be modified for customer-specified secondary connectors.

Optional removable solid state drives allows for a variety of configurations including quick security access.

- 4th Gen Intel® Core™ CPU
- Shock and vibration-tested (MIL-STD-810G)
- MIL-STD-38999 high-density connectors
- IP67 sealed against dirt and water
- Customized expansion options
- SWaP-optimized
- Advanced thermal management

## Embedded Computing & I/O Solutions



FPGAs for
PMC & XMC
acromag.com/fpgas

Industry Pack &
PMC Mezzanine I/O
acromag.com/embeddedio

VME & VPX SBC
acromag.com/boards

COM Express
Type 6 System
acromag.com/comexpress

MADE IN USA ISO9001 AS9100

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

Acromag®
THE LEADER IN INDUSTRIAL I/O

ADVERTISER INFORMATION

| Page | Advertiser/Ad Title |
|---|---|
| 45 | **Acromag** – Small things come in small packages |
| 3 | **Annapolis Micro Systems, Inc.** – WildStar OpenVPX Ecosystem |
| 27 | **Applied Avionics, Inc.** – Universal ARINC 429 to discrete signal converter including ADS-B out applications |
| 38 | **Astronics/Ballard Technology** – The industry's most trusted and widely used USB interfaces |
| 6 | **Behlman Electronics** – Improved VME and VPX power performance |
| 31 | **Creative Electronic Systems** – COTS and safety certifiable |
| 39 | **Data Device Corporation** – Your solution provider for connectivity, power, control |
| 17 | **Diamond Systems Corporation** – Big on performance, small on size |
| 18 | **Elma Electronics** – Reduce, save, improve. Elma's rugged platforms do all that – and more |
| 43 | **Evans Capacitor Company** – Power in the air, power in the sea, power in hand |
| 2 | **Extreme Engineering Solutions (X-ES)** – Unparalleled processing power |
| 47 | **GE Intelligent Platforms, Inc.** – Rugged capability without compromise |
| 29 | **Interface Concept** – Build your own VPX system! |
| 15 | **Kimdu Corporation** – Advanced technology ... personal touch |
| 5 | **Microsemi** – Information security and performance ... from the ground up |
| 19 | **North Atlantic Industries** – Rugged SBCs from NAI |
| 6 | **Orbit Power Group and Orbit Electronics Group** – 135+ VME and VPX solutions |
| 48 | **Pentek, Inc.** – Critical recording in any arena |
| 34 | **Phoenix International** – Airborne, shipboard, ground mobile data recording, and data storage |
| 35 | **Proto Labs** – Refuse to let design fall flat |
| 14 | **Sealevel Systems, Inc.** – High-speed tactical communications |
| 23 | **TE Connectivity** – Lightweights that pack a punch |

# CONNECTING WITH MIL EMBEDDED

*By Mil-Embedded.com Editorial Staff*

CHARITY

## AMVETS National Service Foundation

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. To back that up, our parent company – OpenSystems Media – will make a donation to every charity we showcase on this page.

This month we're featuring the AMVETS National Service Foundation, which has been assisting returning veterans since 1948 with the goal of aiding in their readjustment back into civilian life. AMVETS fields a group of National Service Officers whose job it is to aid a veteran or a veteran's dependent in the process of obtaining compensation and benefits from the Veterans' Administration. This service is free to veterans and their dependents.

The organization has assigned a full-time Guard Liaison Officer to the Family Support Staff at the National Guard Bureau and Walter Reed Army Medical Center to assist in the physical evaluation boards and Department of Veterans Affairs claims processing. These additional commitments have strengthened government efforts to assist returning veterans at the time of separation, retirement, or release from active federal service through the Transition Assistance Program.

The Veterans' Affairs Voluntary Service is a structured program of volunteers who regularly aid veterans obtaining care in VA medical centers across the United States.

The organization also offers educational scholarships to eligible veterans and dependents, fields a program with the AMVETS Ladies Auxiliary for schoolchildren, and has established a program of installing memorial carillon bells in a number of national and state veterans' cemeteries in the U.S. and overseas. Another of the organization's programs is called "Task Force DVD," which collects and sends safe entertainment for U.S. troops stationed overseas.

For more information, visit www.amvetsnsf.org.

WHITE PAPER

## Software-Defined Radio Handbook *(11th Edition)*

*By Rodger Hosking, Pentek*

Software-defined radio (SDR) has revolutionized electronic systems for a variety of applications, including communications, data acquisition, and signal processing. In SDR, components that have been typically implemented in hardware (for example, mixers, filters, amplifiers, modulators/demodulators, and detectors) are instead implemented by means of software on an embedded system.

This white paper compares conventional analog receiver and transmitter systems to their digital counterparts, highlighting similarities and differences. It also explores the inner workings of the SDR, with an in-depth description of the internal structure and the devices used. Some board- and system-level implementations and available off-the-shelf SDR products and applications based on such products are presented.

Read the white paper:
http://embedded-computing.com/white-papers/white-handbook-11th-edition/

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