Military
EMBEDDED SYSTEMS

October 12, 2015

SDR Security and Shared Spectrum Challenges


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.

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. 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.

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.”

Sidebar 1

(Click graphic to zoom)

“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.”

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.)

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.

(Click graphic to zoom)

“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.)

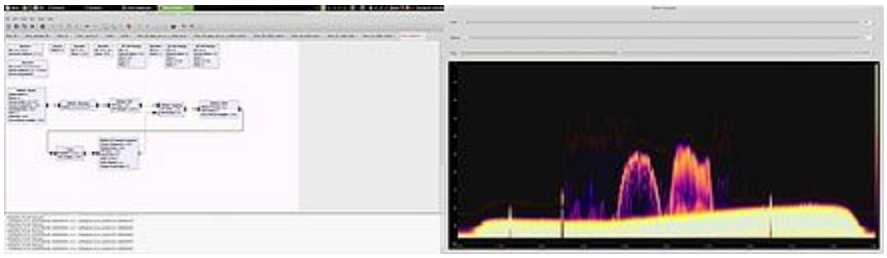

Figure 2: The RF Network on Chip from Ettus Research is an open-source tool for development and debug.

(Click graphic to zoom by 1.9x)

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."

http://mil-embedded.com/articles/sdr-security-shared-spectrum-challenges/