Military
EMBEDDED SYSTEMS

February 9, 2017

Low-latency processing, open architectures key for smarter radar/EW systems

MARIANA IRIARTE, ASSOCIATE EDITOR

System-performance requirements and open architectures are driving development of smarter radar and electronic warfare (EW) systems. For EW systems, low-latency processing is a key requirement.

Meeting system performance requirements and delivering radarand EW systems that can face current and emerging threats is an ongoing battle for system designers. What it comes down to for the warfighter, is how "fast [they] can respond to an incoming signal and define what it is," says Lorne Graves, technical director at Mercury Systems in Chelmsford, Massachusetts. Engineers need to take into account the challenges of getting that information and translating it into actionable intelligence. For this arc to happen, Graves says, "Low-latency processing is key. It's similar with radar systems, which are going to be looking for low-latency processing and in some cases you'll see a trend to adaptive or cognitive radars."

With slight differences in radar and EW systems, engineers face challenges when developing these systems, because each has a different goal. In radar and EW systems, "the sensor and the system to defeat a sensor use similar technology – but have fundamentally different objectives. We often see signal processingon a radar system that performs functions such as phase calculations for beamforming or frequency domain Doppler processing; many of these operations are too complex and impose too much latency on the data path in an EW system," says Haydn Nelson, director, marketing and applications engineering, 4DSP Products, at Abaco Systems in Austin, Texas.

Radar/EW differences

The system designer must know the mission goal or application: "The largest difference is that electronic warfare systems often require extremely low latency. An EW system must often respond to a threat in nanoseconds, whereas radar can tolerate latencies in the milliseconds," Nelson explains.

Threats also factor into these systems, particularly if the user is unaware of where the threat is within the EW domain. "The spectrum is very broad, so it has to be very low-latency processing because you have to respond anywhere in that broad radio frequency (RF) spectrum to look for a particular threat," Graves notes.

"In the radar domain, one of the things that you do know is what was transmitted and you understand where that is," Graves continues. With radar systems, "you have some fixed latency and there is a certain amount of time to respond."

To handle the low-latency processing, Nelson says, "radar applications can often tolerate the latency of serial interfaces, allowing the use of higher sampling rates and more channels; as such, they can leverage the benefits of JESD204B interfaces, which typically deliver higher bandwidth and more channels on a single interface."

Where they come together "in some of the multifunction system that we're beginning to see today is where both of these systems are doing some type of cognitive or adaptive algorithms; those typically are done on the same kind of processing machines," Graves says.

To increase system performance, "In terms of I/O implementation, there are two ways to interface: serial and parallel," Nelson notes. "Parallel interfaces are often implemented with buses, whereas serial interfaces often use specialized FPGA [field-programmable gate array] I/O with multigigabit transceivers with a JESD204B protocol on top. The latency of a JESD204B interface is typically higher than 100 ns, which is unacceptable to many EW applications. Thus, parallel LVDS [low-voltage differential signaling] is preferred," notes Nelson.

COTS driving cognitive systems

Commercial off-the-shelf (COTS) solutions help solve the processing issue. "One of the things that COTS signal-processing solutions are doing to enable cognitive EW applications is bringing a server asset,” Graves says. “What we’re doing at Mercury is bringing a server class asset directly behind the very fast, very agile, low-latency processing board for the EW domain.”

The beauty of COTS solutions is that “If the DoD needs to deploy a certain application within four months and has defined that application and need now, COTS solutions are programmable and configurable and can address that new mission and threat,” says Rodger Hosking, vice president and cofounder of Pentek in Upper Saddle River, New Jersey. Ideally, when the human is taken out of the picture, Nelson says, “A cognitive EW system would need a processor architecture that can dynamically adapt using machine learning algorithms. The execution of a machine-learning algorithm isn’t addressed by an FPGA-only architecture. Typically, GPPs [general-purpose processors], and sometimes GPUs [graphics processing units], handle these types of problems better, with their ability to execute modern languages like C/C++. Traditional processor architectures handle branching and complex decision trees much more efficiently than an FPGA device. Today’s GPUs are better at branching than their predecessors, but it is still not a strength for them. GPPs continue to handle this better.

“The ‘cognitive’ aspect of cognitive EW is such that the system would have the intelligence to dynamically adapt, based on the effectiveness of a specific technique, and learn in real time,” he continues. “This type of machine-learning approach to EW is considerably more advanced and requires a different computational architecture.”

What it comes down to is using the right tool for the job: “The same high-channel-count I/O and FPGA system is still needed, but the added signal intelligence and cognitive aspect of the system requires a parallel module based on a leading edge commercial GPP or GPU technology," Nelson says. The Abaco Systems GRA113 graphics module is an example of such a module," says Nelson. (See Figure 1.)

Figure 1: The GRA113 leverages commercial NVIDIA technology on a form factor aimed at use in rugged radar and electronic warfare applications. Photo courtesy of Abaco Systems.

The open systems architecture agenda

A COTS discussion also necessitates the use of open architectures to enable faster, cost-effective technology refreshes.

"The desire to maintain technologically advanced radar and EW systems has driven many programs to adopt open standard architectures to have better control of technology refreshes," Nelson explains. "The adoption of open architectures has benefits in terms of technology, mitigation of program risk, and reduction of cost, which accounts for the significant adoption of the 3U VPXplatform in the past few years."

The benefits expand throughout the life cycle of the system: "COTS solutions have a shorter development time," Hosking says. "Because of open standards, engineers can repurpose the system for other solutions, depending on the demand or new mission requirements. COTS technology is really great for putting together a system that is low cost and has a shorter development cycle."

Products like Pentek's Model 5973 (Figure 2) is an FMC carrier board that has an optical backplane interface and is compliant with several VITA standards including VITA-46, VITA-48, VITA-66.4, and VITA-65 (OpenVPXTM System Specification). The idea behind these systems is to remain configurable and modular, even down the road.

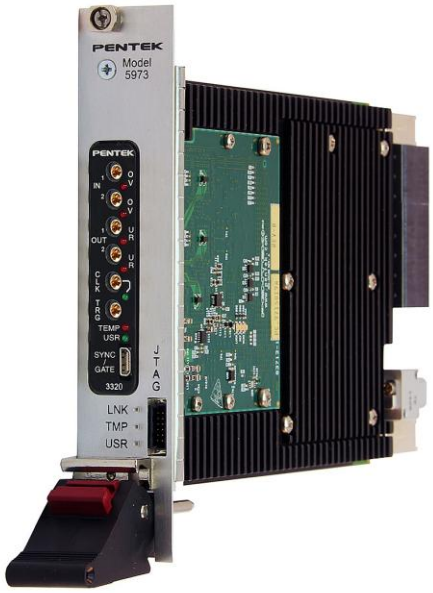


Figure 2: Pentek's Model 5973 has a user-configurable gigabit serial interface. Photo courtesy of Pentek.

The main impetus for the shift toward open standards is to "move towards open architectures for signal processing in these areas; [because they] have the ability to adapt quickly to newer threats that evolve and they are evolving at a very rapid pace due to commercial technology that is now available to our adversaries that used to always be locked away in the United States DoD," says Mercury's Graves. "Those areas are no longer available just to us; they are now available through commercial products to our adversaries."

The industry is finding that open architecture is "becoming a bigger and bigger deal across different domains within the DoD. This is particularly true with radar systems, when they look at what is best of breed in terms of different modes, the different capabilities, and what all the providers are delivering," says Shaun McQuaid, director of product management for Mercury Systems' Embedded Products Group in Chelmsford, Massachusetts.

DoD program officials are pushing the industry to support open architectures and the standards that underpin them. "Examples include FACE [Future Airborne Capability Environment, an open avionics environment for military airborne platforms], SOSA [Sensor Open Systems Architecture for interfacing sensor suites], OMS [Open Mission Systems standards for integrating subsystems and services into airborne platforms], etc.," Nelson says. "Beyond the technology, risk, and cost benefits of open architectures, they also allow the government to have more control over system designs and technology refreshes."

Smarter radar/EW systems

Open architectures and COTS processing solutions have combined to evolve radar and EW systems toward the cognitive side, creating smarter systems for the warfighter.

"Radar/EW signals have become exponentially more sophisticated over the years and customers are looking to exploit new technology to deal with them. Radars must glean more detailed information from targets to gain actionable intelligence, while countermeasures must struggle to defeat detection from the first moment of each threat," Hosking says.

The desire to handle the sophisticated technology and have the upper hand in system performance for radar and EW has pushed engineers to increase synchronized channels enabled by wider bandwidth receivers and transmitters, Nelson says: "The inclusion of more channels has several applications. The most obvious is beamforming systems for radar and being able to create more advanced EW techniques like simulating the polarization of a rotating aircraft turbine in a spoofed radar return. The combination of wideband and multichannel systems has a direct consequence on the analog I/O and FPGA signal processing.

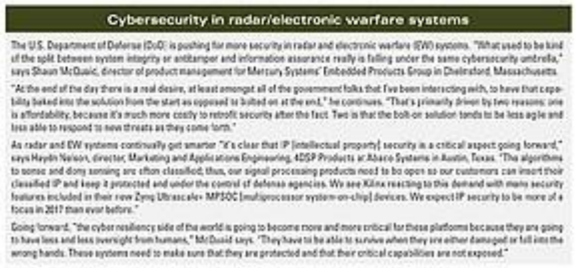
"An increase in bandwidth means that data is coming faster and often requires more FPGA resources to handle this volume of data," he continues. "The result is that designers often require larger FPGA devices like the Xilinx Ultrascale class of products. Further increasing the requirement for FPGA resources: this 'faster data' is coming on multiple channels."

Since there is an increase in channels, the data coming in requires a significant amount of bandwidth, "which ends up looking like a big-data problem," McQuaid says. "On the other side of that is a processing solution that can handle that and you know that is analogous to commercial big-data solutions."

Engineers are then accommodating the needs of the users with "multiple Ultrascale FPGAs and FMC+ interfaces to accommodate both wideband digital receivers and transmitters and the accompanying increase in signal processing load," Nelson says.

Driven by the additional complexity of new FPGA devices, "there's a push to abstract low level resources to boost design productivity," Hosking says. "That means software, hardware, and FPGA designers are working at a higher level of design entry. They can now choose from libraries of high-level functional blocks, create their own custom blocks, and interconnect them all using graphical tools. The tools take care of most of the lower details of this process, saving significant time for engineers."

These advances in technology and "the new techniques we have made are what people are looking for," Hosking continues. "It's the ability to do a better job of developing advanced signal-processing technology – for both incoming and outgoing signals – to improve detection and threat-avoidance capabilities. Users are looking for smarter, faster, and more capable systems."



Cybersecurity in radar/electronic warfare systems

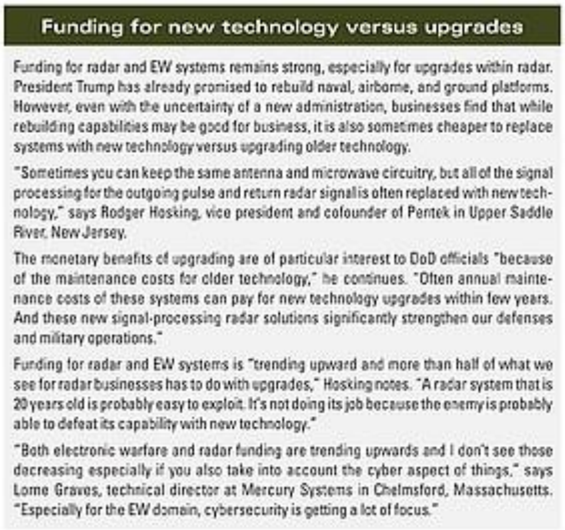
The U.S. Department of Defense (DoD) is pushing for more security in radar and electronic warfare (EW) systems. "What used to be kind of the split between system integrity or antitamper and information assurance really is falling under the same cybersecurity umbrella," says Shaun McQuaid, director of product management for Mercury Systems' Embedded Products Group in Chelmsford, Massachusetts.

"At the end of the day there is a real desire, at least amongst all of the government folks that I've been interacting with, to have that capability baked into the solution from the start as opposed to bolted on at the end," he continues. "That's primarily driven by two reasons: one is affordability, because it's much more costly to retrofit security after the fact. Two is that the bolt-on solution tends to be less agile and less able to respond to new threats as they come forth."

As radar and EW systems continually get smarter "it's clear that IP [intellectual property] security is a critical aspect going forward," says Haydn Nelson, director, Marketing and Applications Engineering, 4DSP Products at Abaco Systems in Austin, Texas. "The algorithms to sense and deny sensing are often classified; thus, our signal processing products need to be open so our customers can insert their classified IP and keep it protected and under the control of defense agencies. We see Xilinx reacting to this demand with more security features included in their new Zynq Ultrascale+ MPSOC [multiprocessor system-on-chip] devices. We expect IP security to be more of a focus in 2017 than ever before."

Going forward, "the cyber resiliency side of the world is going to become more and more critical for these platforms because they are going to have less and less oversight from humans," McQuaid says. "They have to be able to survive when they are either damaged or fall into the wrong hands. These systems need to make sure that they are protected and that their critical capabilities are not exposed."

Sidebar 1



Funding for new technology versus upgrades

Funding for radar and EW systems remains strong, especially for upgrades within radar. President Trump has already promised to rebuild naval, airborne, and ground platforms. However, even with the uncertainty of a new administration, businesses find that while rebuilding capabilities may be good for business, it is also sometimes cheaper to replace systems with new technology versus upgrading older technology.

"Sometimes you can keep the same antenna and microwave circuitry, but all of the signal processing for the outgoing pulse and return radar signal is often replaced with new technology," says Rodger Hosking, vice president and cofounder of Pentek in Upper Saddle River, New Jersey.

The monetary benefits of upgrading are of particular interest to DoD officials "because of the maintenance costs for older technology," he continues. "Often annual maintenance costs of these systems can pay for new technology upgrades within few years. And these new signal-processing radar solutions significantly strengthen our defenses and military operations."

Funding for radar and EW systems is "trending upward and more than half of what we see for radar businesses has to do with upgrades," Hosking notes. "A radar system that is 20 years old is probably easy to exploit. It's not doing its job because the enemy is probably able to defeat its capability with new technology."

"Both electronic warfare and radar funding are trending upwards and I don't see those decreasing especially if you also take into account the cyber aspect of things," says Lorne Graves, technical director at Mercury Systems in Chelmsford, Massachusetts. "Especially for the EW domain, cybersecurity is getting a lot of focus."

Sidebar 2

http://mil-embedded.com/articles/low-latency-key-smarter-radarew-systems/