

Military

EMBEDDED SYSTEMS

October 14, 2020

Managing New Trends for Embedded EW Systems



[RODGER HOSKING](#), PENTEK, INC.



Electronic warfare (EW) not only plays a dominant role in worldwide defense capabilities, but it also must evolve rapidly to counter new threats and take advantage of new technology. Each advance must take into account the ever-changing system design landscape.

Many critical sections of electronic warfare (EW) systems are now combined within single components like the RFSoc [RF system-on-chip], including signal acquisition, processing, and generation functions. Increasing complexity in hardware, firmware, and software adds risk and costs, so effective, high-level development tools are becoming more important than ever before.

At the same time, emerging U.S. Department of Defense (DoD) initiatives like Sensor Open Systems Architecture (SOSA) seek to standardize embedded system architectures for improved interoperability and upgradeability while reducing costs and delivery times.

Scope of electronic warfare

EW has evolved to become a dominant military force, often overshadowing the importance of traditional weapons, manpower, and transport systems. EW encompasses an incredibly diverse range of specific military capabilities, each one focusing on widely different aspects of exploiting the electromagnetic spectrum to gain advantage over the enemy. EW signals extend across nearly a dozen orders of magnitude of both frequency and power levels, using a vast array of different platforms for each application.

Deployed EW systems can be found everywhere, including land, air, sea, underwater, and space. They often use the same increasingly congested slices of the spectrum as nonmilitary radio activities including those used for commercial, entertainment, government, consumer, municipal, emergency, and transportation purposes. Indeed, our electromagnetic spectrum is a finite resource that is carefully controlled, highly congested – and therefore, heavily exploited – by advanced technology to make the most of it.

EW is roughly divided into three major sectors. Electronic attack (EA) includes classic offensive goals to disrupt, deny, degrade, destroy or deceive. Electronic protection (EP) seeks to thwart the effectiveness of EA. Electronic support (ES) harvests the extensive wealth of signal information of all types to improve decision making and strategies.

EW challenges and strategies

Radar represents a major segment of EW, rich with aspects of attack, protection, and support. Under development for nearly a century, radar technology provides critical support for virtually all military platforms. Jamming is one form of electronic attack used to destroy, disable or degrade radar receivers, blinding them to enemy assets. Jamming – originally using brute force, high-power broadband transmitters – has now become extremely sophisticated with highly directed frequency- and pulse-adaptive signals. This structure makes it harder to locate and disable the jamming source.

For electronic protection, clever radar transponders in aircraft can generate artificial reflected signals carefully crafted to simulate multiple targets and can transmit false location, bearing, speed, and target cross-section information. Short reaction times to synthesize these deceptive signals are vital for air-to-air combat, because of close proximities.

After nearly 25 years, network-centric warfare has evolved rapidly to embrace network technology as a fast, reliable mesh of information links among all warfighting elements. By carefully acquiring signals from radar, communication, electro-optical, and other sensors, and feeding those

digitized streams to signal processing elements, algorithms can produce real-time representations of the battlefield for tactical and strategic decisions. Such electronic-support functions are now greatly enhanced with artificial intelligence (AI) and machine learning technologies. Resulting orders containing precise information for the next course of action, carefully tailored for each asset, are distributed quickly across the battlefield network to men and equipment.

These examples illustrate how EW functions for EA, EP, and ES are often highly integrated and interactive within the same platform. All of these operations increasingly rely upon advanced antennas, including phased array designs, and sophisticated signal processing techniques like beamforming, modulation/demodulation, AI, multidimensional algorithms, spread-spectrum techniques, cryptography, adaptive radio, and cognitive radio.

Nevertheless, any single implementation of these strategies will eventually become less effective as new countermeasures are deployed. This self-sustaining cycle is the engine of EW, which virtually guarantees on-going military funding and incentives for new development.

New technologies for EW

To advance EW objectives, several critical technologies are required. Many EW signals now occupy wider bandwidths, not only to simply accommodate higher information rates, but also to support spread-spectrum modulation schemes to improve channel reliability and resiliency against jamming. Another contributor is frequency-hopping, in which RF carrier frequencies are rapidly changed during transmission in a predetermined pseudo-random pattern known only to the receiving device.

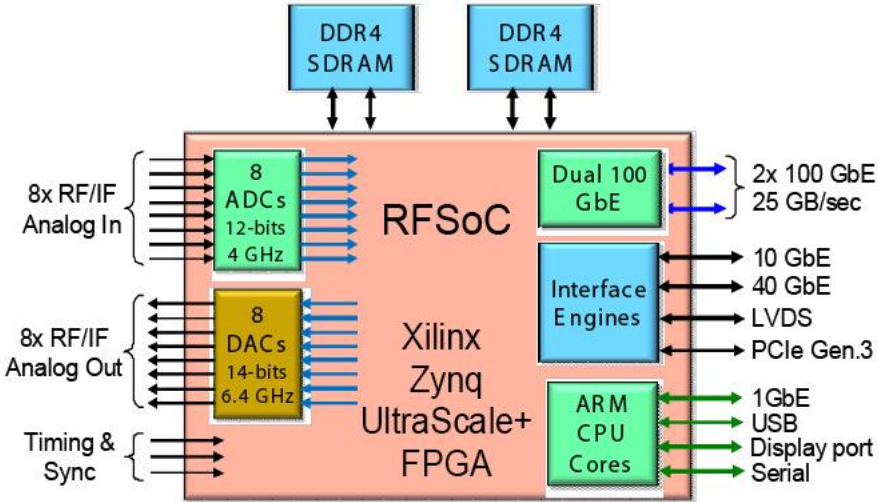
This increase in signal bandwidth means wideband analog front-end RF and intermediate/IF circuits, higher sampling rates for the data converters, and increased data rates for digitized signal interface links. Perhaps the biggest effect is the major impact on the workload for digital signal processing engines, which must now implement AI and other advanced, compute-intensive algorithms.

Phased-array antennas are linear or two-dimensional planar arrays of elements, each one capable of applying independent phase shifts to a common transmit or receive signal. By precisely controlling each phase shift to achieve constructive interference, the antenna can be highly directional, both for receive and transmit. Unlike traditional dish antennas, by applying a new set of phase shifts, phased arrays can be instantly steered to a new direction with no moving parts. Additional signal processing allows simultaneous tracking of multiple targets.

Phased arrays are particularly appropriate for airborne and UAV radars where they can be installed on a hull surface and quickly adapt to threats and targets without the bulky mechanical structures required for a directional dish. But the agility and reliability of phased arrays makes them increasingly popular for ground- and maritime-based radars as well, especially for fire-control systems and countermeasures.

All of these important benefits incur some complexity and cost. Each element of the phased array requires independent phase-shifts (weights). Originally done with analog circuitry, now this is performed on the digitized signals using DSP because of improved precision and speed. Thus, each element in a transceiver array requires its own analog-to-digital converter (ADC) and digital-to-analog converter (DAC), plus its own DSP engine.

To make this more manageable, the RFSoc was introduced by Xilinx in 2018. Based on its UltraScale+ FPGA [field-programmable gate array] Zynq architecture, the RFSoc includes eight ADCs sampling at 4 GS/sec and eight DACs sampling at 6.4 GS/sec. These are connected directly to the Zynq FPGA fabric, eliminating the power, connections, complexity, and latencies of external interfaces to discrete data converters. An onboard, multicore ARM processor acts as a system controller with control/status I/O, and two 100 GbE interfaces connect the RFSoc to external devices supporting 24 GB/sec data transfers in both directions. (Figure 1.)



[Figure 1 | Xilinx’s Zynq UltraScale+ RFSoc device combines all critical components of EW sub-system including eight RF ADCs and DACs, high-speed Ethernet and PCIe, DDR4 SDRAM interfaces, and multi-core ARM processors.

Introduced for commercial 5G wireless markets, the RFSoc nicely integrates the key support functions for eight elements of a phased-array antenna, and is small enough to fit right behind the phased-array panel to reduce cumbersome cabling. By harvesting new technology like RFSoc from commercial markets for military applications, defense vendors are dramatically shrinking size, weight, power, and cost (SWaP-C), especially critical for air vehicles and small EW countermeasure systems.

Because RFSoc offers a complete software radio subsystem on a chip, it opens open a wealth of new military uses previously impractical with earlier technology. These include small standalone monitoring stations, more capable robots, smarter munitions, and portable adaptive radios that can dynamically change operational frequencies to avoid crowded bands or countermeasures.

New development tools for EW

Emerging EW threats and strategies now require answering technologies like exploitation of advanced vector processing, configurable hardware for sensor interfaces, AI, neural networks, machine learning, and scalar processing for analysis and decision-making. Each of these disciplines currently requires specific processing hardware and specialists who are capable of programming them. Even if each section is fully operational, integrating these diverse resources into a tightly coupled, functional system is daunting.

Some new initiatives offer a promising path forward: Xilinx recently announced its Versal ACAP [adaptive compute acceleration platform] family of hardware devices and supporting development tools. Different members of the family provide different blends of three major resources: scalar processors (CPUs), vector processors (GPUs, DSPs) and adaptable logic (FPGAs). One even offers RF ADCs and DACs, similar to the RFSoc and therefore highly appropriate for embedded EW. Onboard, high-bandwidth memory and flexible memory structures eliminates the need for external devices.

To interconnect these resources, ACAP includes an extremely wideband network-on-chip that offers a uniform interface and protocol to simplify system integration.

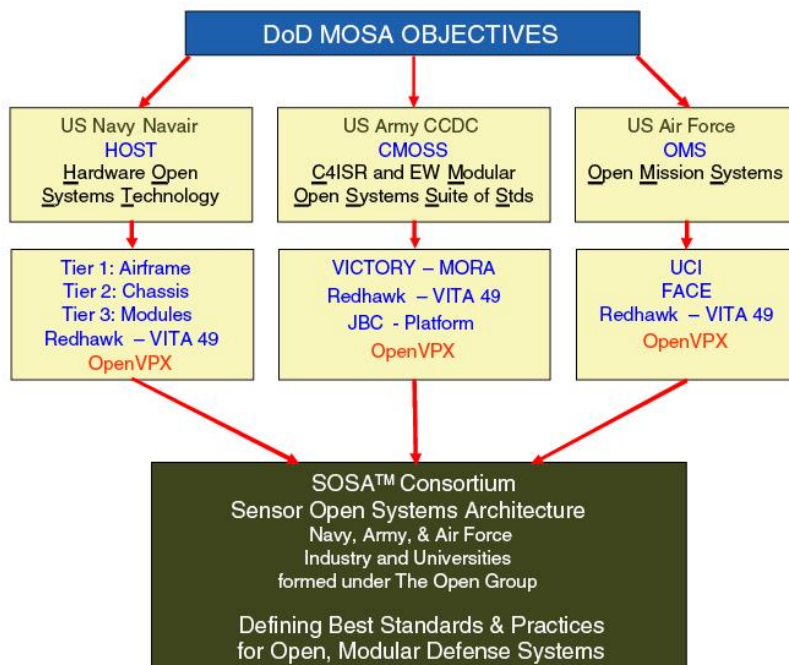
Versal development tools target high-level design entry from frameworks, models, C language, and register-transfer level (RTL) coding. Users can create a custom development environment to suit their project needs and programming preferences.

Other hardware/software platforms will evolve to help speed EW development tasks to help overcome high complexity and extreme performance requirements.

SOSA: A new embedded open standard for EW

In May 2013, the U.S. Department of Defense (DoD) issued a milestone memo mandating that all acquisition activity must incorporate DoD Open Systems Architecture (OSA) principles and practices defined in evolving open standards for well-defined modular hardware and software components. The objectives include multivendor sourcing, reusability for quick-reaction needs, and easier upgrades to new technology, which reduces development risks and ensures significantly longer operational life cycles.

In response, each of the three primary U.S. service branches (Army, Navy, and Air Force), began developing standards that embraced OSA principles to meet future procurement needs of deployed systems for their respective services. Five years later, it was apparent that the three services had many common elements; this realization inspired the formation of the Sensor Open Systems Architecture (SOSA) Consortium to unify these initiatives. (Figure 2.)



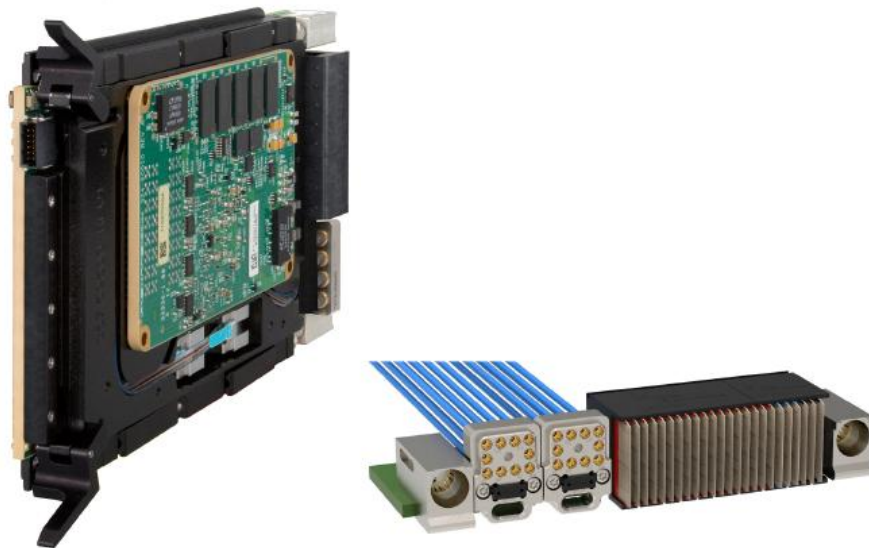
[Figure 2 | Open Systems Architecture initiatives developed independently by the three U.S. DoD services share common elements that are now

consolidated under the Open Group SOSA Initiative for open embedded system acquisition requirements.]

SOSA adopts the most appropriate subsets of existing open standards to form a multipurpose backbone of building blocks for current and future embedded systems for radar, electro-optical/infrared (EO/IR), signals intelligence (SIGINT), EW, and communications. SOSA contributing members are U.S. government organizations including the U.S. DoD, Army, Navy, and Air Force, as well as key representatives from industry and universities.

A major SOSA product is the Technical Standard, which draws primarily from OpenVPX and other related VITA standards, plus emerging extensions for new technologies, topologies, and environmental requirements. Under intensive development for several years, the Technical Standard Snapshot 3 was released in July 2020 for review and amendment prior to the first full release at version 1.0, expected in early 2021.

Dozens of vendors are now offering “SOSA-aligned” products that are well poised to become “SOSA certified” after third-party certification to the final standard once released. (Figure 3.)



[Figure 3 | Pentek Model 5550 SOSA-aligned 3U VPX RFSoc processor card with the QuartzXM module on its conduction-cooled carrier, and dual VITA 67.3 rear-panel connectors for 20 RF coaxial cables and dual 100 GbE optical cables.]

The DoD is now issuing requests for proposals and information clearly favoring respondents that offer OSA-based solutions. A key difference in the SOSA architecture from earlier open standards is the well-defined protection of IP, which encourages innovation and investment. This certainty helps ensure that SOSA is well on its way to revolutionize the future of embedded military EW systems.

Rodger Hosking is vice president and cofounder of Pentek. He has spent more than 30 years in the electronics industry and has authored hundreds of articles about software radio and digital signal processing. He previously served as engineering manager at Wavetek/Rockland; he also holds patents in frequency synthesis and spectrum analysis. He holds a BS degree in physics from Allegheny College in Pennsylvania and BSEE and MSEE degrees from Columbia University in New York.

Pentek www.pentek.com

Featured Companies

PENTEK

[PENTEK](#)

1 Park Way
Upper Saddle River, NJ 07458
<https://www.pentek.com/>

sales@pentek.com

[201-818-5900](tel:201-818-5900)

<https://militaryembedded.com/radar-ew/signal-processing/managing-new-trends-for-embedded-ew-systems>