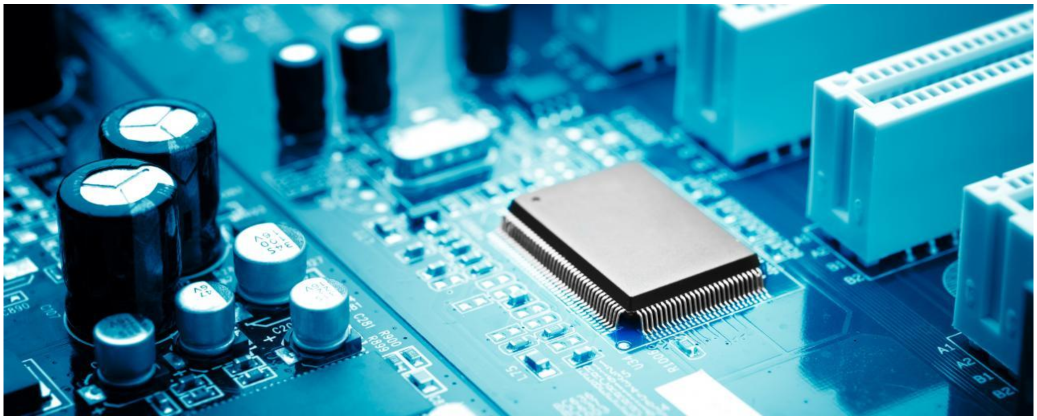
ECN

April 1, 2019

Rugged Embedded Technology

by John W. Koon, contributing writer



Rugged embedded systems designed for sectors such as defense, aerospace, and industrial (oil and gas, utility, and mining), need to perform reliably in harsh conditions with extreme temperatures, high radiation levels (for space applications), and high moisture or pressure. In addition, they must deal with power and security constraints. The rugged embedded market has been growing to meet such demands. The following three emerging trends will impact future technology deployments in the rugged embedded sectors.

1. Development and Deployments of the Open VITA and Related Standards

During the last few decades, the flattening military and aerospace budget has been leaving less room for high development costs or new R&D projects. The emerging civilian aerospace sector is also mindful of the high cost of development from the ground up. In the place of customized devices, users have increasingly turned to commercial off-the-shelf (COTS) products or components, which reduce the cost of device development, maintenance and training, shorten time to market, and offer the latest technologies. However, COTS components must meet users' expectations for high interoperability, thus facilitating integration into new or larger systems and technology partnerships.

Since the 1980s, the nonprofit VMEbus International Trade Association (VITA) organization has been advocating the standardization of modular embedded computing systems and the establishment of guidelines on relevant materials, devices, and practices. Cooperating with VITA, The SOSA Consortium created a **Sensor Open Systems Architecture (SOSA)**, which provides a reconfigurable and upgradable infrastructure to support an open systems architecture such as OpenVPX. The civilian—not just the military—aerospace sector is emerging as an important user of VITA standards.

Since the VPX standard is not specific to space flight requirements, SpaceVPX was launched to augment OpenVPX and focus on redundancy, single-point failure tolerance, spare module support, status reporting, and diagnostic support for space applications (Figure 1). "Open standards are key to the success of today's complex computing platforms. The cost and complexity make it very difficult to develop any platform that cannot leverage the work of others, thus driving the need for standards. Add to that the modular nature of many platforms that drives the need for standards at all levels to reasonably ensure interoperability between platforms and key components. Our work in the realm of standards is just beginning." Jerry Gipper, VITA Executive Director says.

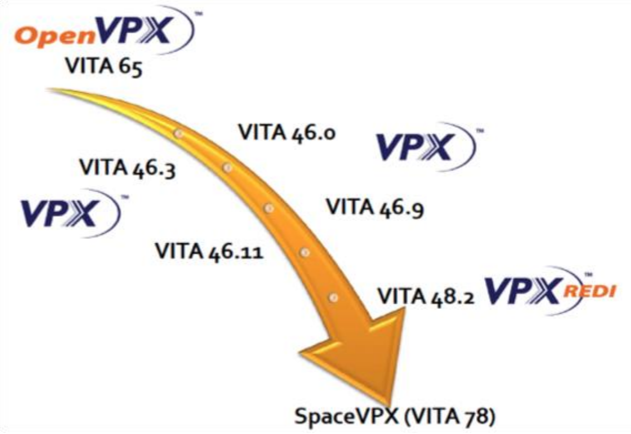


Figure: 1: SpaceVPX is the byproduct product of VPX and OpenVPX. Rugged and ready for space exploration by focusing on redundancy, single-point failure tolerance, spare module support, status reporting, and diagnostic support. (Image Source: Rapidio.org)

2. AI for Mil-Aero Applications

Military and aerospace operations often occur in remote areas with scarce resources, support, or maintenance; therefore, using artificial intelligence (AI) to make the machines "smarter" will greatly increase the chance of operational success. While AI has gained traction in many spaces, enhancing security, for example, or making manufacturing lines more efficient, it faces challenges integrating into rugged systems. Not only does AI require intensive, high-performance computing, but the use of AI technology may not easily dovetail with traditional decades-long equipment life cycles. And any device targeting rugged environments must also face size and weight constraints, exposure to heavy battering during warfare, and stringent safety requirements.

A rugged system incorporating AI can use computer vision to differentiate between legitimate risks—a rifle-carrying person, for instance—and a similar but benign person, such as someone carrying a hoe over his shoulder. AI can also relieve humans from such monotonous tasks as watching the same location for hours. AI is still in its infancy and is expected to grow rapidly. However, its deployment and adaptation may require intense computing power existing processors cannot provide. The good news is that with VPX or XMC (part of VITA specification), the processor boards can be upgraded with faster processors from Intel or FPGA from Xilinx without changing the whole system. An example is Pentek's Jade architecture XMC module, which is plug-compatible with and can replace outdated XMC modules (Figure 2).

Figure: 2: Based on Xilinx Kintex UltraScale FPGA, Pentek Model 71810, with fully customizable I/O signal status and control interface supports up to 8X gigabit links. (Image Source: Pentek, Inc.),

3. Seeking More Robust Safety and Cybersecurity

In a hostile world full of conflicts, safety and cybersecurity are more critical than ever before. The two major areas that must be addressed to increase product safety and security are:

- Securing the supply chain
- Increasing cybersecurity and anti-tampering efforts

<u>Securing the Supply Chain</u>

Any manufacturer of rugged embedded hardware systems, whether the system is VPX-based or not, needs security not only within the manufacturer's own factories, but extended to the full supply chain. Otherwise the final products produced used in military, space, nuclear plants, and other critical areas will be unreliable and unsafe. Some considerations include maintaining the integrity of the manufacturing process, ensuring the absence of counterfeit parts, and verifying that supply sources can be clearly identified and tracked at all times. In addition, the subcontractors working with authorized suppliers must also be scrutinized. Finally, protecting proprietary information (intellectual property) is of the utmost importance. Product design information and document control have to be managed so no unauthorized third parties can have access.

<u>Increasing Cybersecurity and Anti-Tampering Efforts</u>

Some of the best practices to increase cybersecurity and anti-tampering, as offered by Curtiss-Wright include having a process already in place to deal with problems and upgrading old technology in order to strengthen security. When a security software bug is discovered, it's important to have a process already in place to deal with the problem efficiently.

That's in contrast to certain companies, as reported in the media, which discovered software security vulnerabilities in their systems but did not take action for many months, resulting in critical data being stolen by hackers. In an age in which open software is commonly used, it is important to discriminate between software to use and not to use. It's possible to bolster cybersecurity with practices such as using cryptography as an integral tool and using secure boot and system partitioning, so that if one section is attacked, the malware does not spread to the entire system. Its strengths in fighting tampering and hackers mean that the battle for cybersecurity will be one in which AI is more involved.

Conclusion

The benefits of having standards such as OpenVPX, SOSA, and SpaceVPX include efficient deployment and upgrades of technologies, cost savings, and interoperability among suppliers. The users will not be limited to a single source. Standard-based technologies will continue to grow for defense and space applications in rugged and demanding environments. The application of AI promises to be another growth area. Finally, the surge of cyberattacks has prompted the use of cybersecurity hardware and software technologies, and the application of reliable processes to ensure product safety and cybersecurity. The rugged embedded market has multiple reasons to anticipate a future that brings greater use of standards-based technology, AI, and security-related deployments.

https://www.ecnmag.com/article/2019/04/challenges-facing-rugged-embedded-technology