Bringing security to legacy systems for modern missions

By Steve Edwards
An industry perspective from Curtiss-Wright Defense Solutions

Many defense and aerospace processing systems are upgraded or refreshed rather than replaced for cost efficiency and to reduce out-of-service time. Particularly in the defense domain, upgraded systems require security to be built-in to protect sensitive mission information and maintain warfighter technology advantage. What's more, system protection is mandated by U.S. government policy for new research, development, and acquisition programs. While adding new capabilities, an opportunity is created to add security to legacy systems originally designed with minimal or no protection capabilities. The system integrator's challenge becomes how to protect these systems while minimizing the impact on the overall design.

Until now, embedding security IP into fielded systems required extensive customization of the target system hardware. System integrators were forced to upgrade all the hardware (system replace), a complicated process that consumes considerable time and materials and usually requires system-level recertification after completion. Alternatively, integrators were forced to add a new dedicated security card to the target system, which requires a slot to be available and usually calls for extensive software reconfiguration.

A better, third approach is to use a plug-in mezzanine module to address system security and provide additional system processing capability. This method enables system designers to add security to any module supporting an XMC (VITA 42/61) site, including OpenVPX or VME modules, as well as modules designed to align with SOSA Technical Standard 1.0 and the U.S. Army's C5ISR/EW Modular Open Suite of Standards (CMOSS) technical standards. Additionally, high-performance rackmount servers can be supported using an appropriate PCIe/XMC carrier, which enables embedding security to fielded systems without a complete system redesign. This approach is especially well-suited for addressing three types of security solution use cases:

- Trusted boot
- Secure enclaves for mission-critical applications
- Extension of security

Trusted boot

An XMC security card can provide the system with secure boot capabilities if it hosts a contemporary FPGA [field-programmable gate array] device, such as a Xilinx Ultrascale+ MPSoC. The security card can use the built-in security features of the FPGA, such as authentication and encryption, to provide confidentiality, integrity, and authentication (CIA) of the boot code and user application – both software and FPGA bitstream. Additional security features, such as a 256-bit physically unclonable function (PUF), are options on many leading-edge FPGAs.

Secure enclaves for mission-critical applications

To provide secure enclaves using a security XMC module, the application is separated into nonsecure components and secure components requiring protection. The secure components are hosted on one or more of the FPGA's processing cores, while the remainder of the application continues to run on the root of performance (e.g., an Intel processor). The secure application is encrypted at rest and either stored in the XMC card's flash memory or remotely loaded over PCIe/Ethernet after the card has booted. Additional security components can be loaded during the secure boot process.

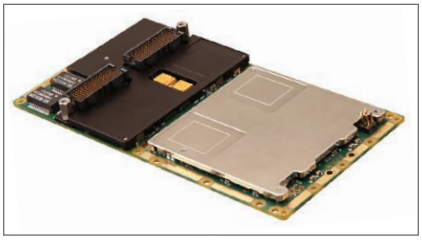

Figure 1 | The XMC-528 XMC module can add security IP to COTS modular open systems.

Extension of security

Extension of security (EoS) from a trusted module to additional commercial off-the-shelf (COTS) components within a system can be realized through the integration of advanced security IP. EoS ensures that standard COTS modules can be interrogated to verify unique identities and security states prior to use within a system; EoS can also free system developers and architects from using outdated custom solutions. This approach enables system security architectures to remain in sync with the latest advancements in high-performance COTS offerings from commercial vendors.

An example of an XMC module for enabling the security of critical data and technology on deployed systems is Curtiss-Wright's XMC-528 Xilinx Ultrascale+ MPSoC XMC mezzanine card (Figure 1). It can ease the integration of advanced security IP, such as Idaho Scientific's Immunity cryptographic products, into OpenVPX and legacy VMEbus system solutions to lower overall life cycle costs by capitalizing on the economies of scale that COTS devices provide. If preferred, the same security IP suite provided by the XMC mezzanine module can also be integrated directly into the onboard security FPGA resident on security-ready OpenVPX digital signal processor card and next-generation processor modules.

Steve Edwards *is Director of Secure Embedded Solutions for Curtiss-Wright.*

Curtiss-Wright Defense Solutions
https://www.curtisswrightds.com/