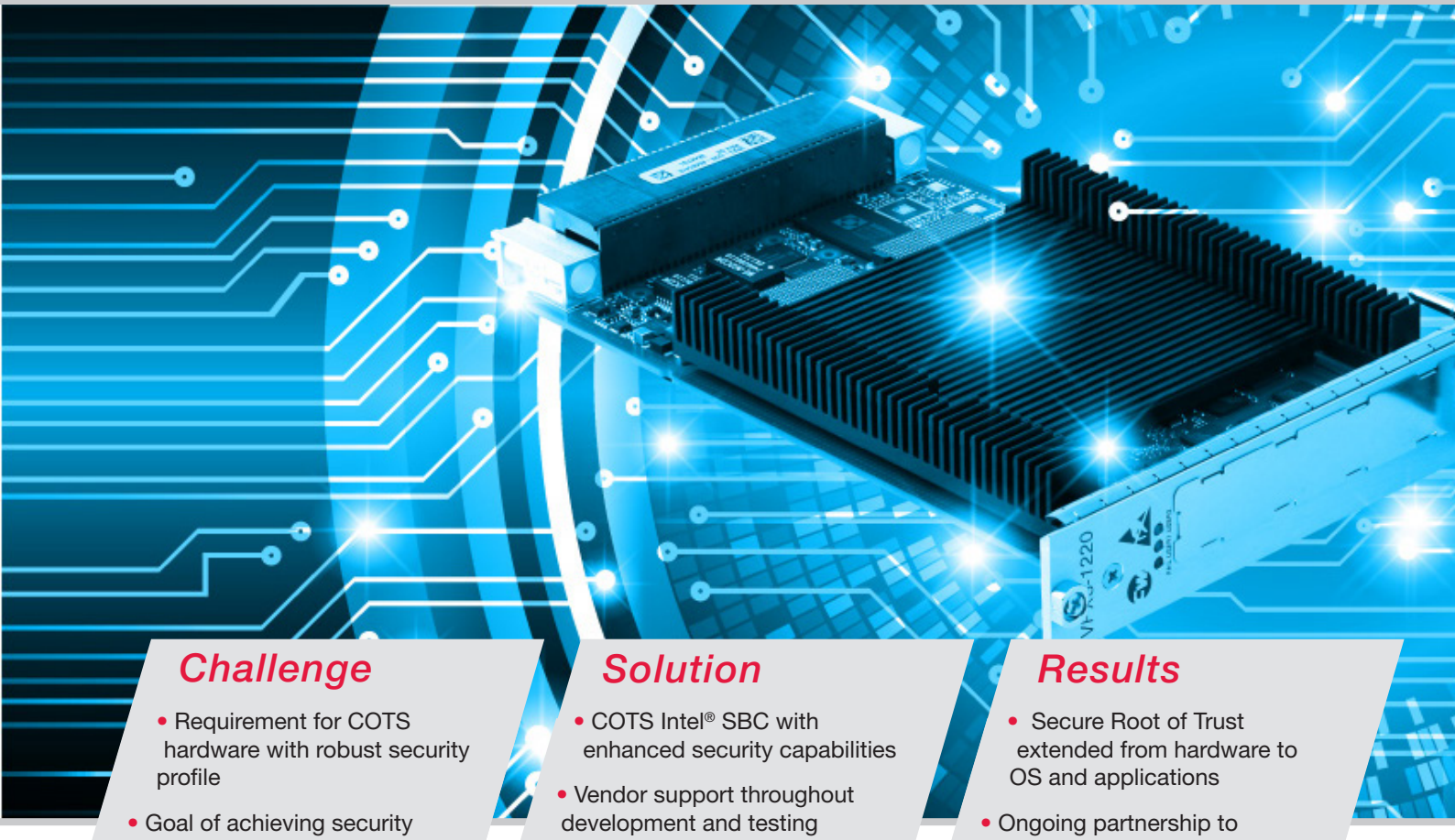
CASE STUDY

# Building a Truly Trusted Computing Solution with COTS Hardware and Intel Security Capabilities

CURTISS-WRIGHT

DEFENSE SOLUTIONS



## Challenge

- Requirement for COTS hardware with robust security profile
- Goal of achieving security certification from a renowned intelligence agency
- Need for investment protection for finished solution

## Solution

- COTS Intel® SBC with enhanced security capabilities
- Vendor support throughout development and testing
- Total LifeCycle Management™ services

## Results

- Secure Root of Trust extended from hardware to OS and applications
- Ongoing partnership to mitigate potential security threats
- Reduced program and financial risk

## Challenge

When a global manufacturer of secure systems in the aerospace and defense industry began developing a new computing solution designed to mitigate modern cybersecurity threats, it was aware of the many challenges it would face while evaluating hardware and software components. The company sought a commercial off-the-shelf (COTS) 3U VPX single board computer (SBC) with a robust and proven security profile upon which to build its Trusted Computing solution, a processor board that would provide a fully protected Root of Trust-based boot process and extend this trust to its hardened Red Hat® Linux® operating system and application software.

Ultimately, this Trusted Computing solution would be developed specifically to meet stringent security requirements and be tested by a prominent intelligence agency in order to receive its prestigious security certification, a recognition that would approve the solution for use in secure environments on a variety of platforms. In order to achieve this highly valuable certification, the company would need to perform rigorous security hardening of the board, followed by security vulnerability analysis and penetration testing on all hardware and software components, knowing the intelligence agency would perform similar testing to an even higher degree of scrutiny before awarding the certification.

VPX3-1220 3U VPX 7th Gen
Intel Xeon® Single Board Computer

In addition to meeting these critical security requirements, suppliers would be evaluated on their ability to demonstrate a truly trusted supply chain with processes in place for manufacturing security, component supply chain integrity and counterfeit parts mitigation, among others. As well, it was important for all technology to make it through the thorough security certification process and still offer a lucrative useful life and period of market availability. For this reason, all hardware components were evaluated on their ability to offer a long and stable lifecycle, as well as their supplier's support to combat obsolescence.

## Solution

With an internal security team dedicated to hardening and testing all hardware and software that would potentially be included its final solution, the firm began evaluating various industry suppliers. While many offered hardware with similar performance and claimed security capabilities, few candidates had actually implemented and tested their solution and could demonstrate true trusted technology.

After careful and thorough consideration, the company chose to partner with Curtiss-Wright, evaluating multiple Trusted Computing solutions before selecting the VPX3-1220. Leveraging a quad-core Intel 7th generation Xeon processor, the VPX3-1220 is a mid-performance, safety-certifiable SBC that offered the ideal balance of power and performance for the firm's Trusted Computing solution. Its high technology readiness level (TRL) was testament to its suitability for the program, and its nearly immediate availability meant testing and implementation could begin quickly, accelerating the development schedule. Further, knowing the VPX3-1220 was manufactured following Curtiss-Wright's stringent trusted supply chain processes added extra assurance and protection against malicious supply chain threats.

The VPX3-1220 includes a Trusted Platform Module (TPM) device, which is used to create a secure computing environment and ensuring only signed and trusted BIOS and software components can execute on the board. Most contemporary Intel processor designs include a TPM device; however, the TPM device provides no security capabilities until it's configured and locked by the supplier. While hardware vendors may include a TPM device in their hardware, they rarely put the time and effort into implementing a fully secure boot mechanism, and instead expect system integrators to understand, design, verify and implement all of these complex tasks. During the development of the VPX3-1220, all TPM boot security features were carefully implemented in order to activate its protection capabilities, allowing this Curtiss-Wright customer to take its secure solution to market faster (read more about why a hardware vendor's boot security implementation is so important).

The VPX3-1220's demonstrated trust architecture met the company's security requirements and, what's more, its proven field history provided confidence that the board would perform reliably through both internal and external testing.

## Results

Through this partnership, the company has developed a solution based on Curtiss-Wright's trusted hardware, with a Root of Trust extended into its operating system and applications to deliver a truly secure Trusted Computing solution. After performing its internal security testing, the company is now working with the intelligence agency to continue testing towards achieving its security certification. Because ongoing, rigorous security testing will inevitably reveal areas to strengthen even the most hardened solutions, support from Curtiss-Wright throughout the development and testing process has been immeasurably important in order to mitigate potential threats and prepare the product for third-party examination.

Once the company's Trusted Computing solution has received its certification, this Curtiss-Wright customer can be confident its investment will pay off well into the future. Because Curtiss-Wright offers extensive lifecycle management services, the VPX3-1220's components are protected beyond their officially supported lifetime. As components near the end of their lifecycle, Total LifeCycle Management customers will have the opportunity to secure parts that enable them to build past the product's official end of life date. This proactive supply management protects the customer's initial investment and helps mitigate risk for the duration of its program.

INFO: CURTISSWRIGHTDS.COM
EMAIL: DS@CURTISSWRIGHT.COM