Curtiss-Wright and Wind River: Trusted Foundations for Mission-Critical Applications

CURTISS-WRIGHT

A Complete, Secure Hardware and Software Solution

System security is a top priority for protecting today's warfighters from sophisticated remote and physical threats. But a system's security level is not simply equal to the sum of its parts – its hardware and software components' Trusted Computing capabilities must work with and leverage one another for a cohesive security strategy.

That's why Curtiss-Wright and Wind River have partnered to deliver a secure hardware and software solution for applications where trust is critical. Developed by Wind River's technology protection and cybersecurity group, Star Lab, Titanium Security Suite has been integrated, tested, and validated on Curtiss-Wright hardware to strengthen system security while delivering system engineers several advantages:

+ **Minimize development, deployment, and program risk** with a software suite that's been tested and validated on Curtiss-Wright hardware
+ **Reduce costs and simplify development** with an integrated commercial off-the-shelf (COTS) solution
+ **Fast-track deployment** with shortened development schedules

Curtiss-Wright Processing Modules

The CHAMP-XD1 and CHAMP-XD1S processor cards are two of Curtiss-Wright's high-performance boards that include built-in Intel® Trusted Computing mechanisms and flexible APIs to support secure software solutions. The CHAMP-XD1 has been tested and proven as a trusted hardware foundation for Titanium Security Suite, with testing on the CHAMP-XD1S to follow.

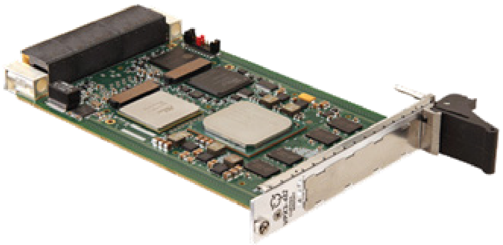
CHAMP-XD1 High-Performance Processor Card

For highly compute-intensive industrial, aerospace, and defense applications, the CHAMP-XD1 processor card provides Trusted Computing features alongside leading-edge processing technology for unmatched performance.

This high-performance module, designed for the rigors of digital signal processing (DSP) and emerging machine learning and artificial intelligence applications, delivers incredible processing capability through its 8 or 12-core Intel Xeon D processor. The board includes a core function FPGA for critical board functions and general purpose I/O, and includes a dedicated Intelligent Platform Management Interface (IPMI) for system monitoring and health.

Security features:

+ Intel Trusted Execution Technology (TXT)
+ Intel Virtualization Technology (VT-x)
+ Trusted Platform Module (TPM) 1.2
+ UEFI Secure Boot
+ Non-Volatile Memory Sanitization
+ TrustedCOTS Trusted Boot Protections



CHAMP-XD1 High-Performance Processor Card
with Intel Xeon® D 8-Core D-1539 or 12-Core D-1559 processor

WNDRVR

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

TRUSTED
PROVEN
LEADER

CHAMP-XD1S High-Performance Processor Card

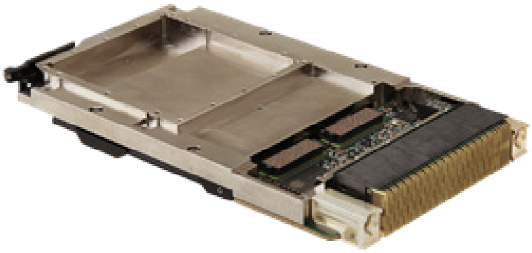
For applications where Trusted Computing is critical, the CHAMP-XD1S builds on the CHAMP-XD1's high-performance design with an even stronger security profile.

The CHAMP-XD1S pairs its 8 or 12-core Intel Xeon D processor with a Xilinx® MPSoC FPGA. Wind River software can leverage this FPGA, enabling even more tightly integrated hardware and software security.

The CHAMP-XD1S is developed in alignment with the SOSA™ technical standard.

Security features:

- Intel Trusted Execution Technology (TXT)
- Intel Virtualization Technology (VT-x)
- Trusted Platform Module (TPM) 2.0
- UEFI Secure Boot
- SSD Encryption
- Non-Volatile Memory Sanitization
- Security FPGA
- TrustedCOTS Enhanced Trusted Boot Protections
- Specialized Security Software
- Customizable FPGA IP



CHAMP-XD1S High-Performance Processor Card
with Intel Xeon D 12-Core D-1559 processor

Wind River Titanium Security Suite

The Titanium Security Suite includes a variety of capabilities to ensure secure, trusted, and controlled execution, as well as protection from cyber attacks, tampering, and reverse engineering.

Titanium Linux (formerly known as Titanium)

Titanium Linux offers the most robust Linux® system hardening and security capabilities available on the market today for operationally-deployed Linux systems. Designed using a threat model that assumes an attacker will gain root (admin) access to your system, Titanium Linux maintains the integrity and confidentiality of critical applications, data, and configurations while assuring operations. Titanium Linux is compatible with Wind River Linux, Red Hat®, CentOS, Ubuntu, RedHawk, and other embedded Linux distributions.

Titanium Secure Hypervisor (formerly known as Crucible)

Titanium Secure Hypervisor lets system engineers leverage virtualization to greatly simplify maintaining and upgrading defense systems that operate in the most hostile computing environments. Secure Hypervisor enables combat systems to survive and operate through cyber attacks using advanced isolation, attack surface minimization, and cyber resiliency capabilities. Curtiss-Wright's CHAMP-XD1 and CHAMP-XD1S modules are equipped with Intel Virtualization Technology (VT-x) to offer the perfect platform for Secure Hypervisor.

Titanium Secure Boot (formerly known as TrueBoot)

Titanium Secure Boot authenticates the boot process and chain on Intel processors from the hardware root of trust. Its hardware-backed key storage extends trust to the operating system (OS) launch and its provisioning tools allow for trusted OS updates without requiring any hardware re-provisioning. Secure Boot is portable across kernels and bootloader types, and leverages the CHAMP-XD1 and CHAMP-XD1S's Trusted Platform Module (TPM), a security chip that can be set up to use cryptographic methods to ensure platform integrity throughout the entire boot process until applications are running.

For more information on Titanium Security Suite and Curtiss-Wright hardware, contact us:

Curtiss-Wright Defense Solutions

333 Palladium Drive, Ottawa, ON K2V 1A6
☎ +1-613-599-9199
curtisswrightds.com
✉ ds@curtisswright.com

Wind River Systems, Inc.

500 Wind River Way, Alameda, CA 94501
☎ +1-800-545-WIND
windriver.com

TRUSTED PROVEN LEADER