CURTISS-WRIGHT

TrustedCOTS™ and Enhanced TrustedCOTS

For Trusted Computing

Trusted. Proven. Leader.

curtisswrightds.com

Curtiss-Wright's Approach to Program Protection

The threats facing today's defense and aerospace applications are more varied and sophisticated than ever. Embedded electronics require enhanced trusted computing protections to defend mission success from compromise from physical and remote attacks and hardware and software failures.

Curtiss-Wright builds trusted computing technologies and techniques into every aspect of our security solution development, from design and testing to supply chain and manufacturing. This comprehensive, end-to-end approach creates an effective mesh of protection layers that integrate to ensure the reliability of Curtiss-Wright products in the face of attempted compromise.

Our Trusted Commercial-off-the-Shelf (TrustedCOTS™) and Enhanced TrustedCOTS portfolio of embedded security products and capabilities are aligned to give you the flexibility, control, and options you need to build the right assurance level into your program. TrustedCOTS and Enhanced TrustedCOTS leverage the commercial domain's extensive secure state-of-the-art R&D investments, which we integrate into rugged, reliable, and reusable technology blocks. Our modular open system approach (MOSA) to security uses no custom hardware, facilitating rapid and easy integration into host systems. Indeed, this approach is so adaptable it can be retrofitted to existing systems.

TrustedCOTS

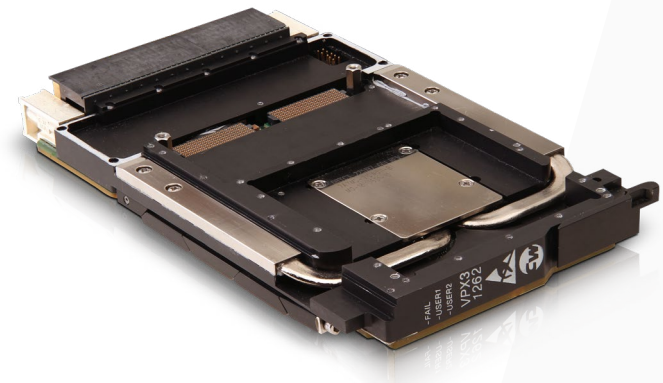
Our approach to embedded security design deploys defense-in-depth and defense-in-breadth strategies to take advantage of the security technologies inherent in commercial components and employ defense-grade security technologies. Our TrustedCOTS framework is a baseline security framework that fully enables the security capabilities of commercial hardware and software technologies to protect your application from compromise. This framework includes protection mechanisms for the boot chain, access control for configuration menus, software authentication mechanisms, encryption, and sanitization routines for onboard memory. Additional software capability can be added for data in transit encryption and firewalls. Designed primarily to assist in meeting risk management framework (RMF), cyber, and secure boot requirements, this level of security applies to systems deployed worldwide.

TrustedCOTS products and capabilities are agnostic and are built to seamlessly complement your in-house capabilities around three major data protection domains:

- Technology protection safeguards how computing tasks are executed. It combines hardware capabilities, software algorithms, and operations to protect system functionality.
- Data protection that safeguards software algorithms, data-at-rest, and data-in-motion from compromise.
- Parts protection safeguards the supply chain and manufacturing processes, ensuring that our components are authentic and approaches meet the strictest quality controls.

Curtiss-Wright TrustedCOTS Solutions

- CHAMP™-XD1 (VPX3-482) 3U VPX Intel® Xeon® D SBC
- VPX3-1262 Intel Core™ i7 13th Gen 14-core SBC
- VPX3-1260 3U VPX Intel 9th Gen Xeon E SBC
- VPX6-1961 6U VPX Intel 11th Gen Xeon W SBC
- VPX3-152 3U VPX NXP® T2080 Power Architecture® SBC
- V3-152 3U VPX NXP T2080 Power Architecture SBC for flight certification
- VPX3-1220 3U VPX Intel 7th Gen Xeon E SBC
- XMC-121 Intel 7th Gen Xeon E SBC Mezzanine cap
- VME-1910 6U VME Intel Xeon E SBC
- VPX3-133 3U VPX NXP T2080 Power Architecture SBC
- VPX6-197 6U VPX NXP T2080 Power Architecture SBC
- VPX3-1703 3U VPX NXP LS1043A Arm® Processor SBC
- VPX3-1708 3U VPX NXP LX2160A Arm Processor SBC
- V3-1708 3U VPX NXP LX2160A Arm Processor SBC for flight certification



VPX3-1262 3U VPX Intel Core i7 14-core hybrid processor

V3-1708 3U VPX NXP LX2160A Arm Processo

TrustedCOTS Security Framework

There's no one-size-fits-all solution when it comes to trusted computing. Our portfolio of TrustedCOTS products is designed to meet many cybersecurity and system integrity requirements to provide protection mechanisms for the boot chain, access control for configuration menus, encryption and sanitization routines for non-volatile memory, a key management infrastructure, and other protections to support cybersecurity requirements.

TrustedCOTS products use hardware and software components, including trusted platform modules (TPM), Intel Boot Guard, NXP Trust Architecture (supported on Power Architecture QorIQ® and Arm Layerscape products), and Arm TrustZone technology. Operating systems rely on boot-chain components such as Intel UEFI or NXP secure boot. Additionally, data-at-rest security may be offered through solid-state drive (SSD) encryption using software-based (LUKS or equivalent) encryption.

TrustedCOTS products can include a Trusted Boot security framework that provides protection mechanisms for the boot chain, access control for configuration menus, encryption, and sanitization routines for non-volatile memory, and other cybersecurity protection mechanisms.

Enhanced TrustedCOTS Framework

The Enhanced TrustedCOTS framework builds upon TrustedCOTS by allowing the use of specialized security capabilities to be added to provide higher levels of protection with a secure state-of-the-art FPGA. Through technology partnerships, Curtiss-Wright can add additional capabilities to meet more demanding security requirements. Using a modular open systems approach to embedded security, industry-leading security IP is easily hosted on our security-enabled hardware to deliver personalized program protection to the customer.

Curtiss-Wright's Enhanced TrustedCOTS provides the necessary agnostic infrastructure on select processor modules to host security IP from our partners and provide programs with the defense-grade security they need.

Enhanced TrustedCOTS:

- Leverages the speed of COTS and the security IP of leading industry partners.
- Allows for customization of security on COTS processors by selecting only the program protections required.
- Enables security IP to be added at any phase of the program to support changes in security policy.

Curtiss-Wright Enhanced TrustedCOTS Solutions

- CHAMP-XD4 (VPX3-485) 6U VPX dual Intel Xeon D-2700 and cognitive DSP SBC
- CHAMP-XD3 (VPX3-484) 3U VPX Intel Xeon D-1700 SBC
- XMC-529 AMD Zynq™ UltraScale+™ MPSoC plug-in security enabled module for new and legacy systems
- XMC-528 AMD Zynq UltraScale+ MPSoC plug-in security enabled module for new and legacy systems
- Industry-leading security IP from our trusted partners:
  - Raytheon Intelligence and Space Night Cover™
  - Idaho Scientific Immunity Cryptographic Suite, inline memory encryption, and Keystone Agent
  - Star Lab Titanium Technology Protection

CHAMP-XD4 6U VPX Dual Intel Xeon D-2700 and Cognitive DSP SBC

Our TrustedCOTS Security Frameworks

			TrustedCOTS							Enhanced TrustedCOTS	
Capabilities	Processor		NXP T2080	NXP LS1043A	NXP LX2160A	Intel Xeon "Kaby Lake"	Intel Xeon "Coffee Lake" "Tiger Lake"	Intel Xeon "Raptor Lake"	Intel Broadwell DE	Intel Ice Lake D + AMD MPSoC	AMD MPSoC
	Product		VPX3-133 VPX3-152 V3-152 VME-196 VPX6-197	VPX3-1703	VPX3-1708 V3-1708	XMC-121 VPX3-1220	VPX3-1260 VME-1910 VPX6-1961	VPX3-1262	CHAMP-XD1 (VPX3-482) CHAMP-XD2 (VPX6-483) CHAMP-XD2M (VPX6-483M)	CHAMP-XD4 (VPX3-485) CHAMP-XD3 (VPX3-484)	XMC-528 XMC-529
	NXP	Trust Architecture	Available	Std	Std						
	Arm	TrustZone		Std	Std					Std	Std
	AMD	Secure Boot								Available	Available
	Intel	Standard Features				SGX VT-x	SGX VT-x	SGX VT-x	VT-x	TME SGX	
		Boot Guard					Available	Available		Available	
		TXT				Contact Factory	Contact Factory	Contact Factory	Contact Factory		
		TME								TME	
		MK-TME						MK-TME			
	Trusted Platform Module					TPM 2.0	TPM 2.0	TPM 2.0	TPM 1.2	TPM 2.0	
	UEFI Secure Boot					Available	Available	Available	Contact Factory	Contact Factory	
	SSD Encryption						Available	Available		Available	
	Security FPGA									XD3: ZU4/5 XD4: ZU15	ZU11

Std: Standard
Available: Available upon request. May incur a separate charge.
TME: Total Memory Encryption
MK-TME: Multi-Key Total Memory Encryption
Contact Factory: Contact Curtiss-Wright for availability and pricing.
All TrustedCOTS products have a built-in capability to sanitize non-volatile memory.

Going Beyond Standard Reliability Processes

To ensure our TrustedCOTS solutions dependably perform under the harshest conditions in the field for many years, Curtiss-Wright goes beyond standard processes in several key areas including:

- Lead-free solder innovations that allow us to continue miniaturizing components and increasing functionality density without negatively affecting reliability.
- Parylene coating of printed circuit boards (PCBs) that effectively double solder joint reliability compared to acrylic and urethane coatings.

Protecting Against Remote Attacks

Cybersecurity mechanisms include hardware and software techniques that protect data from remote attacks. They are built on a solid foundation of secure boot techniques, cryptography, protection for data-at-rest, and key management. Our solutions surpass generic approaches to cybersecurity to incorporate the right balance of confidentiality, data integrity, authentication, availability, and non-repudiation techniques for the expected threats and application requirements.

Customization Capabilities

When a security requirement necessitates modifying our standard products, Curtiss-Wright works with customers to identify, define, and meet these needs. Curtiss-Wright also provides services to customize firmware and/or software to add additional add-in capabilities.

Privacy Considerations

Curtiss-Wright has engineering, manufacturing, and program support capabilities in the U.S., Canada, and multiple locations within Europe. This allows us to meet a variety of regional requirements, including privacy considerations for U.S. secret and sensitive discussions.

Commercial Solutions for Classified (CSfC) – Data-at-Rest

For data-at-rest (DAR), Curtiss-Wright has several storage solutions with various levels and standards of security, including FIPS-140 series, NSA Type 1, and NSA Commercial Solutions for Classified (CSfC), which offers NSA encryption for COTS with two independent layers of encryption. The CSfC program leverages commercial encryption technologies, such as those employed in cars, mobile phones, tablets, and home security systems, to deliver cybersecurity solutions for classified applications quickly.

DTS1+: 1-slot Rugged Network Attached File Server

The Curtiss-Wright DTS1+ is the embedded industry's first COTS DAR network attached storage (NAS) solution that supports two layers of full disk encryption (FDE) in a single device. Having received common criteria (CC) certification, the hardware and software FDE layers used in the DTS1+ are listed on the United States NIAP product compliant list, NSA's CSfC components list, the international common criteria certified products list, and the NATO information assurance product catalog (NIAPC). Selecting an approved device enables system architects to significantly reduce the time, cost, and program risk associated with developing an approved encryption solution.

CSfC – Gateway Services for Classified Networks

For data-in-transit (DAR), Curtiss-Wright has a suite of products utilizing the NSA Commercial Solutions for Classified (CSfC) program. The CSfC program provides a structure for developing, testing, and registering systems for access to and transmittal of classified data utilizing a layered application of commercially available technologies and encryption algorithms such as IPSEC and AES-256. Systems based on CSfC can be deployed more rapidly than legacy Type 1 encryption solutions and enable new architectures, such as secure wireless access and access to classified networks via phones and tablets that would otherwise be impossible.

Curtiss-Wright PacStar® Secure Wireless Command Post and Secure Mesh Command Post products provide turn-key systems based on CSfC for both tactical and enterprise users that require access to classified data. With systems that utilize the Multi-site Capability Package for site-to-site encryption, Campus WLAN Capability Package for securely deploying Wi-Fi (802.11), and Mobile Access Capability Package for providing access to classified networks over any untrusted wired or wireless network, including public or private Wi-Fi and 4G/5G.

Partner and Curtiss-Wright Security IP

Wind River Titanium Technology Protection

Titanium Technology Protection is the most robust system-hardening and security capability available for operationally-deployed systems. Key features include:

Titanium for Linux

- Purpose built for AT use case
- Linux OE hardening eliminates or restricts access to debug and other harmful interfaces
- Effectively deprivileges the root/admin user
- Provides data-at-rest with file encryption and authentication
- Facilitates a simplified Mandatory Accesses Control (MAC) policy to provide runtime protection of application and data files
- Adds IPC restrictions, anti-debug capabilities, address space authentication, etc. to protected applications
- Provides multiple APIs for customizing key storage/release, event reporting/response, etc.

Titanium for Kernel Virtual Machine (KVM)

- The typical KVM host has far more access than is required for special purpose, static configurations, representing a very large attack surface
- Titanium for KVM is well supported and has seen wide adoption
- Titanium for KVM significantly reduces host privileges while also hardening host and hypervisor components to reduce the attack surface
- Significantly reduces the threat of a compromised KVM host, providing the same guarantees for a Titanium VM as are expected on bare metal

Titanium Secure Boot

- Leverages Intel TXT to provide a dynamic root of trust, significantly reducing the impact of vulnerable early boot components
- Post bootloader OE components are encrypted and authenticated to impede instrumentation and targeted exploitation
- Key material is stored in a TPM & sealed/unsealed based on boot environment measurements
- Key material and encrypted OE components are only decrypted if the environment matches the original sealing state
- Simple provisioning process and support for authorized updates ensure ease of adoption

STAR LAB SOFTWARE
A WIND RIVER COMPANY

Idaho Scientific

Side Channel Attack (SCA) Resistant Cores

- Protects key extraction through “side channels” such as power line and radiated emissions
- All Suite B functions
- FIPS 140-2 CAV-P validated

SCA Resistant In-line Memory Encryption

- High-performance, transparent AES-GCM encryption and authentication core to protect external memory

Keystone Security Agent Reference Design

- Security reference design for Intel x86 architectures
- Desktop tool chain for life cycle management

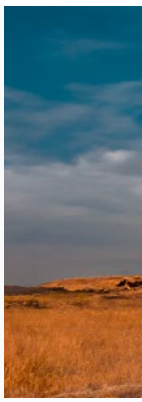
Raytheon Intelligence & Space

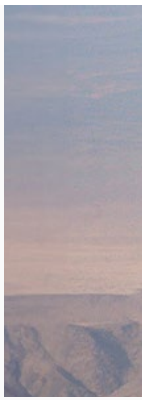
Night Cover

Night Cover is a defense-grade, embedded security product suite that enables a multilayered approach to protect embedded systems. Night Cover’s commercial open standards-based approach to system protection leverages the scale of the broader Defense Department market for system security and augments Curtiss-Wright’s Enhanced TrustedCOTS solutions. Together, they eliminate the need for expensive custom hardware to deliver proven, advanced security capabilities and make it possible to add or upgrade security IP on legacy systems with compatible resident processors.

Key features include:

- Utilizes standard interfaces available in modern COTS modules (e.g., GPIO, PCIe, Ethernet)
- Extension of Security (EoS) for COTS solutions, reduces government-off-the-shelf (GOTS) cost and complexity
- Single root-of-security (RoS) extends trust to other modules in the system
- Suite of layered security capabilities that are modular and scalable
- Reduces cost, schedule, and certification risk
- Embedded system security
- Applicable to new and existing systems





Contact Us

curtisswrightds.com/contact

ds@curtisswright.com

curtisswrightds.com