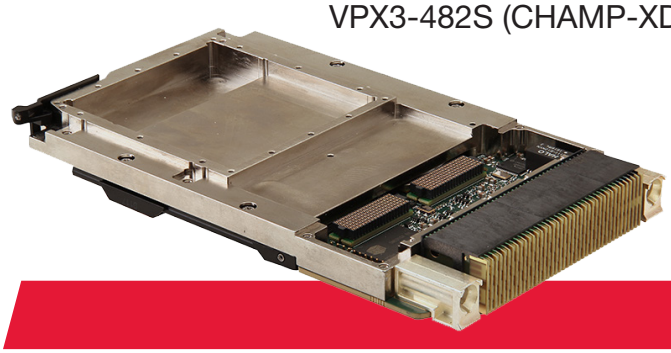
eTCOTS: Security at the Speed of COTS

XMC-528

VPX3-482S (CHAMP-XD1S)



Curtiss-Wright Defense Solutions has partnered with defense industry security leaders Raytheon Technologies, Idaho Scientific, and Wind River to provide defense-grade security functionality on COTS processors through our eTCOTS initiative.

In support of the DoD's Tri-Services Memo directing the use of a Modular Open Systems Approach (MOSA) in DoD systems, Curtiss-Wright's eTCOTS products are designed in alignment with The Open Group Sensor Open Systems Architecture™ (SOSA) Technical Standard. This approach allows users to minimize NRE cost and schedule, as well as meet the DoD's security requirements with a MOSA solution.

VITA
Open Standards, Open Markets

SOSA™
Sensor Open Systems Architecture
MEMBER

Supports Open Systems Architecture

Enhanced TrustedCOTS (eTCOTS)

Security at the Speed of COTS

The threats facing today's defense and aerospace applications are more varied and sophisticated than ever. To defend both mission success and safety from compromise, embedded electronics require enhanced protections from physical and remote attacks, as well as hardware and software failures.

Curtiss-Wright's enhanced TrustedCOTS (eTCOTS) pairs our proven expertise and products with the latest innovations from leading suppliers of defense-grade security to the DoD market. Curtiss-Wright was one of the first companies to provide the Mil-Aero market with commercial off-the-shelf (COTS) processors in response to the Perry Memo in the 1990s calling for a faster and cheaper way to get capability to the warfighter by leveraging the commercial computer industry. Our eTCOTS approach will do the same for providing secure embedded processing faster and cheaper than the traditional custom approach.

Traditionally, defense-grade security solutions required custom hardware somewhere in the system to protect Critical Program Information (CPI). This was an expensive and time-consuming effort, and often would cause significant program schedule delays. Curtiss-Wright's eTCOTS approach provides the necessary infrastructure on select processor modules to allow the hosting of IP from our partners and provide users with the defense-grade security they need – and only what they need.

Curtiss-Wright is dedicated to providing the right security infrastructure on our hardware and working with the right partners with the experience and expertise to provide the necessary IP to protect a program's CPI. We and our partners each focus on our areas of expertise to bring a best-in-class solution to our customers.

Curtiss-Wright has partnered with the following industry leaders to be able to provide our customers with the security they need, when they need it:

- Raytheon Intelligence & Space
- Idaho Scientific
- Star Lab, a Wind River company

Key Features

+ 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 protections your program requires
+ Enables Security IP to be added at any phase of the program to support changes in Security Policy

eTCOTS Hardware

+ VPX3-482S (CHAMP-XD1S) high-performance 3U VPX processor card
+ VPX3-483 (CHAMP-XD3) high-performance 3U VPX processor card (Q1 2022)
+ XMC-528 eTCOTS embedded FPGA card (Q1 2022)

Partners Summary

WNDRVR

Wind River Titanium Security Suite

Titanium Linux

+ Most robust Linux® system-hardening available
+ Simplifies mandatory access control
+ Enables OS hardening and attack surface reduction
+ Remains secure during runtime and rest
+ Provides comprehensive certifications and compliance

Titanium Secure Hypervisor

+ Virtualization, isolation, and cyber resiliency
+ Type-1 hypervisor
+ Direct allocation of resources
+ No oversubscription
+ Multiple levels of separation and isloation
+ Available for Intel® and Arm® (MPSoC) CPUs

Titanium Secure Boot

+ Measured boot
+ Authenticates boot process and chain
+ Hardware-backed key storage
+ Trusted updates without hardware reprovioning

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 encryption and authentication core to protect external memory
+ UNITED Security Reference Design
  - Security reference design for Intel x86 architectures
    - Secure BIOS
    - Side Channel Resistant Crypto Cores
    - Embedded Hardware Security Module
    - Tamper sense, response, logging
  - Desktop tool chain for life cycle management

Raytheon Intelligence & Space

Night Cover Security

+ Extension of Security (EoS) for intermediate COTS solutions reduces GOTS cost and complexity
+ Suite of layered security capabilities that are modular and scalable
+ Reduces cost, schedule, and certification risk
+ Embedded system security
+ Local or remote attestation
+ Strong PUF stable over environmental conditions
+ Device and board sensor(s)
+ Policy and functionality manager for rapid customization

CURTISS-WRIGHT

OMS AT ICD Protocol Gateway

+ Implementation of classified OMS AT ICD
+ Inter & intra-system, consensus-based, secure communications
+ Pre-tested/integrated on CW products for lower cost/schedule risk
+ Can be used to force system level attacks

Secure Guard™ Tamper Sense and Response

+ Customers can create/implement tamper policies per program protection plan
+ Pre-tested to work with Curtiss-Wright IP
+ Create/install new policy as required