TrustedCOTS™: Leading the Way to Secure Systems

Read About

Anti-Tamper

CyberSecurity

NSA type 1

FIPS 140-2

Commercial Solutions for Classified (CSfC)

Trusted Execution Technology (TXT)

Secure Guard Extensions (SGX)

AS5553

Info

curtisswrightds.com

Email

ds@curtisswright.com

Executive Summary

Curtiss-Wright has a long history of developing state of the art solutions for a wide variety of defense applications, from high-performance radar and electronic warfare applications to mission computing, fire-control, sensor management and real-time data recording and storage. Curtiss-Wright is a leader in designing and manufacturing rugged, deployable COTS hardware solutions to meet the demanding needs of the warfighter.

Curtiss-Wright COTS modules and subsystems host application software and firmware developed by our customers. These applications may contain Critical Program Information (CPI) which if compromised can lead to a loss of competitive advantage to the U.S. Military and put the warfighter in danger.

To protect this CPI, Curtiss-Wright has developed, and continues to develop, capability built into the hardware from the beginning, to protect the CPI that our customers create. We work closely with our customers to understand their requirements and ensure that our solutions can meet those requirements. We do this all on products that meet all the requirements for openness being demanded by the Department of Defense. We use open architecture hardware and software components, with non-proprietary libraries and interfaces.

This white paper highlights the capabilities that Curtiss-Wright has established to protect the leading-edge deployed systems developed by our customers.

Lockheed F-117A Nighthawk, shot down over Yugoslavia in March 1999

Curtiss-Wright TCOTS for Hardware and Software Security

Curtiss-Wright Defense Solutions doesn't just make the aerospace and defense industry's most reliable, highest performance embedded modules and systems. As a leading supplier of open architecture commercial-off-the-shelf (COTS) modules and systems for deployed defense applications we are ever more frequently asked by our customers to help them address their evolving and expanding Anti-Tamper (AT) and Cybersecurity requirements. To meet these requirements we go beyond the hardware itself to offer our customers comprehensive solutions that ensure that their system's critical information stays robust and effectively protected.

Curtiss-Wright understands that effective security must address requirements at many levels. Our TrustedCOTS (TCOTS™) approach includes capabilities built directly into the modules to detect, deter and respond to security threats while they are powered on. But it also goes far beyond, because a successful and effective response to security requirements must do much more. It must also include protecting data-at-rest while the module is turned off. Protecting critical hardware and data must also include the processes used to design and manufacture the modules and to source components, to ensure that integrity is maintained throughout the product's entire lifecycle.

The Defense Solutions division's headquarters, located in Ashburn, Virginia, serves as Curtiss-Wright's TrustedCOTS Center of Excellence (CoE). The TrustedCOTS CoE oversees all Anti-Tamper and Cybersecurity related activities, including the definition of relevant strategies and policies, manages related third-party vendor relationships and supervises all manufacturing of TCOTS products. It provides Curtiss-Wright customers with a single point of contact to ensure the highest level of support and responsiveness needed to implement effective TCOTS capabilities.

TCOTS for Hardware and Software Security

In response to the critical nature of data security requirements, Curtiss-Wright has developed and implemented industry-leading TCOTS technologies and techniques that enable our customers to protect their software application and critical data from being improperly accessed or maliciously exploited. While these security techniques cannot be described in detail, this white paper provides a high-level overview of some of the AT and Cybersecurity techniques at our disposal. These techniques and other security capabilities have been implemented on a select range of our rugged electronic module products, including single board computers (SBC), digital signal processors (DSP), Network Switches and FPGA-based processing boards and as well as on our family of data recorder products.

Security Implemented on Standard COTS Modules

Curtiss-Wright TCOTS hardware and software solutions are based on our standard COTS products. They include security features that have been designed-in to enable customers to quickly and economically implement their own protection plans for critical technology and data. These products enable customers to rapidly begin their system development on standard COTS hardware and software. When they are ready to implement their program protection requirements, we enable our customers to move to a TCOTS-Ready variant of their product, one that is 100% software and performance compatible.

Defense in Depth: Protection for the Device, Module, and Volume

Curtiss-Wright pursues a "Defense in Depth" strategy for implementing its TCOTS technologies. The Defense in Depth approach implements multiple layers of security for system hardware, including the device, module and volume level, to provide the strongest possible defense against unauthorized intrusion. This strategy provides a set of capabilities and solutions that enable our customers to optimally fit the protection strategies implemented to the unique requirements of the program.

Today, there are a variety of available options for protecting hardware at the device and module level. Vendors of microprocessors, FPGAs, and other semiconductor components are increasingly adding tamper resistance to their devices. Many of these security features are driven primarily by requirements outside the defense industry. These capabilities, such as Intel's Trusted Execution Technology (TXT) and Secure Guard Extensions (SGX), provide protection to the BIOS and application code running on Intel processors. Another example is NXP's

Freescale QorIQ architecture, which includes a security engine that protects the boot and application code. The latest generation of FPGAs provides differential power analysis (DPA) resistant devices that protect the encrypted data bitstream and provides security IP that monitors for attacks and can zeroize the device if needed.

Malicious encroachments into system hardware can result in anomalous conditions that can be identified in real-time. Capabilities are built into the module hardware to establish trust in the module, monitor for malicious activity and, when necessary, take immediate action.

The simple fact is that adversaries never rest. For that reason, the protection of critical hardware and data is a constantly evolving endeavor. In response, Curtiss-Wright is actively developing next-generation TCOTS technologies and strategies to add to our extensive roster of security options.

Working with Partners to Develop Next-Generation Security

To speed the implementation and verification of advanced AT and Cybersecurity technologies, Curtiss-Wright works closely with select best-in-class partners. In order to facilitate the development of secure systems we work with our partners to integrate their IP to one of our protected modules, enabling our customers to rapidly demonstrate their proprietary AT/Cybersecurity technology on Curtiss-Wright hardware.

For unique requirements that cannot be effectively addressed with our standard COTS solutions, we offer customization or Modified COTS (MCOTS) capabilities that leverage our extensive data security IP as well as select data security solutions from leading third-party vendors in order to provide the most complete solution that meets the customer's security requirements.

TCOTS and Data Protection

At Curtiss-Wright we understand that it is not sufficient to have a security strategy that only addresses data protection when a system is powered up. It is equally vital to provide unassailable security for critical Data-at-Rest while the system is powered down. In today's world it is becoming increasingly important to protect classified Data-at-Rest with encryption for critical data, such as that collected and stored during airborne ISR missions. To that end, we build sophisticated protection capabilities into our standard COTS products at the very beginning of the design process. Our data storage products provide secure storage that is certified to either FIPS 140-2 or NSA Type I requirements.

Lowering the Cost of Data-at-Rest Protection with Two-Layer Encryption

The highest level of data protection is National Security Agency (NSA)-approved Type 1 encryption. Type 1 encryption can be costly and time consuming - typically several millions of dollars for a new development, and multiple years to reach full certification. For those programs that have limited budgets and schedules, Type 1 encryption may prove infeasible. The cost and schedule required to deliver Type 1 encrypted hardware has limited industry's ability to quickly provide robust and cost-effective solutions. The good news is that, in response to the growing need to protect more and more data, the NSA has recently initiated an alternative approach. The NSA now provides an approved route for the use of commercially sourced encryption technologies in applications that don't require the highest levels of protection, such as Top Secret/Unattended. To help facilitate and expand the protection for these less demanding applications, the NSA/Central Security Service's (NSA/CSS) Information Assurance Directorate (IAD) launched the Commercial Solutions for Classified Program (CSfC).

In response to the CSfC's support for cost-effective, faster to field data encryption solutions, Curtiss-Wright developed the industry's first COTS rugged Network Attached Storage (NAS) product designed to support the NSA-defined Two-Layer encryption scenario. This data storage system is a proven, 4th generation rugged Network Attached Storage (NAS) file server that provides high-capacity secure storage. It implements Two-Layer encryption by combining an ASIC and Linux O/S hardware + software encryption methodology in a single device. This small form factor, single-slot NAS data transport system provides 2 TB of storage. It also helps to reduce size, weight and power (SWaP) by eliminating the need for local storage in a platform's computer, display or management devices. The DTS1 also enables any network client to securely store and retrieve critical data.

For aerospace and defense COTS customers, the advantages and benefits of the CSfC-defined Two-Layer encryption approach are clear. Once a product is listed on the NSA's Component List, the cost of data protection should essentially disappear, dropping from several million dollars to zero, since the COTS vendor has absorbed all the costs of the approval process. Once the system integrator gets the NSA's "go-ahead" to use an approved Component List product in their program, the customer can simply purchase the desired product without seeking additional NSA certification. This breakthrough approach, using commercial encryption technologies, promises to speed the protection of vast amounts of critical data using COTS hardware.

For data-in-motion applications, Curtiss-Wright offers embedded Cisco networking technology on some of our Gigabit Ethernet switches and routers. This technology supports requisite cryptography policies needed for CSfC compliance.

Security by Design

Security starts with design. Curtiss-Wright has the processes and personnel in place to ensure that security is built into our hardware and software from day one. This includes making sure that only authorized personnel have access to the product design and manufacturing information, and then only for their part of the process. Secure design goes beyond hardware and software. It also includes ensuring that we have the right processes in place during design and manufacture to ensure that our products have security built in from the beginning. All Curtiss-Wright manufacturing employees, as well as its independent contractors, must pass a rigorous background screening process prior to having access to TCOTS products. These personnel are continually rescreened on a periodic basis. In addition, personnel must have a provable need to access the TCOTS products.

Counterfeit Mitigation at Curtiss-Wright

Curtiss-Wright routinely engages with our customers and suppliers in the development and maintenance of internal processes regarding counterfeit mitigation policies. In addition to structured methods, systems, trending, monitoring processes we also actively participate in industry consortia committees. Curtiss-Wright has held a seat on the SAE G19 AS5553 committee for several years. We are also members of several industry and non- governmental agencies that report on and track sources counterfeit materials and issue updates on trends for their detection. Our counterfeit mitigation teams conduct daily Government-Industry Data Exchange Program (GIDEP) monitoring and specify IDEA standard deployment and testing at approved test labs.

Curtiss-Wright's interdisciplinary approach to materials management includes a close partnership between the Counterfeit Mitigation teams and Component and Mechanical Engineering, Procurement, and Life Cycle Services Team. The Life Cycle services team minimizes the risk of obsolescence by executing last time buys (LTB) to extend product life and avoid the need to procure obsolete parts from component brokers post-LTB.

Designing Security into Your System

Curtiss-Wright is leading the industry by bringing together the most comprehensive set of advanced data and hardware security technologies and processes. Knowing that adversaries never rest, our commitment to developing new capabilities and expanding our range of effective and cost-effective COTS-based intrusion mitigating techniques and strategies also never ceases. Our powerful and innovative TCOTS approach to Cybersecurity and Anti-Tamper system design provides our customers with the tools and options that enable them to address their application's unique data security requirements. Because data security is an evolving field, and each program and system design brings with it a unique set of challenges, the best starting point is a dialogue between the customer and Curtiss-Wright's TCOTS team as early as possible in the design cycle. We can help you protect your system's critical data.

Authors

Steve Edwards, B.S.E.E.
Director Secure Embedded Solutions
Curtiss-Wright Defense Solutions

Learn More

White Paper: Continuum Lifecycle PLUS Services - Extended Counterfeit Electronic Parts Protection

Technology:

- TrustedCOTS: Secured Embedded Solutions
- Commercial Solutions for Classified Program (CSfC)