TECHNOLOGY WHITE PAPER

Beyond Trusted Computing

Extending Protection Capabilities to Deliver TrustedCOTS™ Solutions

CURTISS-WRIGHT

DEFENSE SOLUTIONS

Read About

Technology, data and parts protection

Secure boot, key management and cybersecurity

Curtiss-Wright TrustedCOTS capabilities

A Holistic View of Protection Is Essential

Many vendors of embedded computing solutions for the defense and aerospace industries say their solutions provide Trusted Computing. Solutions that offer Trusted Computing are based on technologies and techniques that provide protection from physical and remote attacks and from hardware and software failures. Although this level of protection is adequate for some applications, the many attack vectors that can compromise commercial off-the-shelf (COTS) solutions for defense and aerospace applications require a higher level of protection.

In addition to the protection provided by standard Trusted Computing best practices, mission success depends on every module, subsystem, and system on every platform performing exactly as expected under the harshest conditions. This single, overriding consideration becomes increasingly important as defense organizations worldwide leverage new technologies to give warfighters indisputable advantages on the battlefield.

The development and integration strategies used to deploy these new technologies are key to creating a higher degree of dependability in every solution and system. This can only be achieved by going beyond standard approaches to Trusted Computing and applying rigorous protection standards at every stage of the development process.

Curtiss-Wright takes a holistic view of Trusted Computing, going above and beyond the efforts of other vendors to apply the advanced protection capabilities needed to develop truly secure COTS solutions. And it is one of the main reasons the company has been a trusted, proven leader in the global defense and aerospace industries for decades.

Figure 1: There are many aspects to consider in compiling and delivering a complete TrustedCOTS solution.

Info

curtisswrightds.com

Email

ds@curtisswright.com

Depth and Breadth Make the Difference

Curtiss-Wright TrustedCOTS solutions extend Trusted Computing best practices to every part of the development process — from design and testing to supply chain and manufacturing. The highest possible levels of protection are built into every aspect of solution development to increase the overall value that COTS solutions can provide in a secure system.

This process includes careful analysis of the relationships, intersections, and dependencies among all of the various protection domains, and investigation into potential faults and failures at the lowest levels to identify the associated security vulnerabilities.

Not All Solutions Are Created Equal

When defense organizations, aerospace companies, and system integrators are evaluating embedded computing solutions, it is extremely important to understand exactly what vendors mean when they say their solutions provide Trusted Computing. It is even more important to understand the difference between solutions that provide Trusted Computing and those that offer a TrustedCOTS level of protection.

The Road From Trusted Computing to TrustedCOTS

Integrity Verifies Data Has Not Been Altered

There are three main aspects to building protection into the Curtiss-Wright TrustedCOTS solutions:

- **Technology protection** safeguards how computing tasks are executed. It combines the hardware capabilities, software algorithms, and operations needed to protect functionality, such as how the algorithm in a radar application works.
- **Data protection** safeguards software algorithms, data-at-rest, and data-in-motion. It ensures that, for example, when data is sent from one system to another, it is not compromised.
- **Parts protection** safeguards the supply chain and manufacturing processes. It ensures there are no compromises made in terms of the components themselves or how they are handled.

To develop TrustedCOTS solutions that encompass all of these aspects, Trusted Computing techniques and technologies must be built into every layer of each solution that comprises a system.

The importance of the layered approach to Trusted Computing should not be underestimated. No single layer of security is impenetrable. With a layered approach, one broken or compromised layer does not compromise the entire solution. The other layers continue providing protection.

To design an effective mesh of protection layers, critical capabilities from each Trusted Computing protection domain must be combined into a seamless, cohesive whole. Figure 2 illustrates the Trusted Computing protection domains that must be addressed and the intersections among them that should be considered to deliver TrustedCOTS solutions.

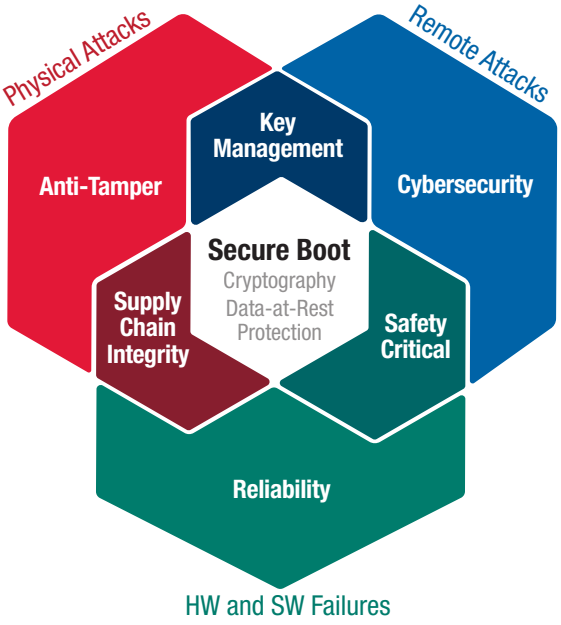

Figure 2: The Trusted Computing Protection Domains in TrustedCOTS Solutions

Secure Boot: The Foundation for All Protection Measures

Secure boot capabilities protect equipment from being reverse-engineered or controlled by adversaries in the field. Boot security starts with a hardware-based Root of Trust, a unique element in the hardware that cannot be replicated or duplicated. The Root of Trust is used to establish a secure chain of trust that extends all the way to the operating system so that it loads only when authenticated.

Implementing robust boot security measures is time-consuming and difficult. When system integrators take on the task, it adds significant time and risk to programs. However, when advanced boot security capabilities are built into solutions from the ground

up and offered as turnkey starting blocks, system integrators have new opportunities to jump-start development efforts, accelerate time to market, and reduce risks.

The Trusted Platform Module (TPM) on modules with Intel® processors is a good example. The TPM is a security chip that uses cryptographic methods to ensure platform integrity throughout the entire boot process until applications are running. It is often used as the basis for a hardware Root of Trust. But, it provides no security capabilities until it is instrumented (configured) and enabled by the original equipment manufacturer (OEM).

While many hardware solutions include a TPM device, it is typically not instrumented. In an implemented TrustedCOTS solution, the time, money, and resources needed to create a hardware Root of Trust and an instrumented TPM as part of a layered approach to boot security have already been applied. This extra initiative helps system integrators significantly reduce program time, effort, and budget requirements.

Key Management: A Complete Life Cycle for Cryptographic Keys

Cryptographic keys are closely tied to secure boot mechanisms. For example, a private cryptographic key or Physically Unclonable Function (PUF) that is unique to a single instance of a board may be used to create the hardware Root of Trust.

TrustedCOTS solutions employ an end-to-end key management strategy that considers the complete life cycle of cryptographic keys within the system, from key generation and storage through use, retirement, and destruction.

Cybersecurity: Applying the Techniques Needed for the Application

Cybersecurity generally refers to the software, or data, side of security. However, to ensure robust protection, many cybersecurity protection techniques incorporate features at the hardware level and at the software level. In many cases, hardware-based techniques are more difficult to duplicate or crack and can react much faster than software-based techniques. For example, cryptography is often implemented at the hardware level because speed is crucial.

The key here is to implement the optimal combination of cybersecurity measures for the expected threats and application requirements. TrustedCOTS solutions go beyond generic approaches to cybersecurity to incorporate the right balance of cybersecurity measures. If too many measures are implemented, the solution becomes inflexible and difficult to use. If too few measures are implemented, vulnerabilities may not be mitigated.

Cybersecurity techniques include:

- **Confidentiality** techniques that keep information private so only authorized users can see it. Confidential information is typically encrypted using complex cryptography algorithms, so even if it is exposed or intercepted, it cannot be understood.
- **Data integrity** techniques that check whether data has been changed since it was last known to be valid. These checks are key to determining, for example, whether malware has been inserted into an operating system or application.
- **Authentication** techniques that grant the right data access levels to the right people and systems based on logins, passwords, and other credentials. Authentication must occur before access to confidential information is granted.
- **Availability** techniques that ensure each system has the data needed to function. These techniques increase the resiliency of systems to protect against attacks, such as jamming, so the correct data continues to flow despite malicious efforts to stop it.
- **Non-repudiation** techniques that ensure the systems on both sides of data exchanges consider the transaction to be valid. This helps to protect against spoofing attacks that send invalid information back to a system.

Anti-Tamper: Protecting Against Physical Attacks

To protect systems in situations where adversaries gain physical access to equipment, TrustedCOTS solutions include anti-tamper mechanisms that provide protection before, during, and after attacks:

- **Protection** mechanisms may include ways to enclose technology in secure packaging to prevent physical access to it.
- **Detection** mechanisms provide notifications if there is an attempt to physically access protected technologies.
- **Response** mechanisms prevent access to technology even if physical access is detected. These mechanisms often involve automatically destroying the hardware or erasing data.

Our previous white paper, The Many Faces of Trusted Computing, explores cybersecurity and anti-tamper techniques in greater detail.

Supply Chain and Manufacturing Integrity: Quality Parts, Stringent Processes

TrustedCOTS solutions include numerous mechanisms to protect supply chain and manufacturing integrity. Here are four of the most important initiatives.

- **Demanding Supplier Selection Criteria.** Component suppliers must be selected with the utmost care. Each supplier must comply with detailed terms, conditions, and specifications. And it is crucial that solution providers work only with component suppliers through authorized franchise distribution channels that control and track the physical movement of parts. To ensure peace of mind, every customer should have the opportunity to approve authentication reports for non-franchise materials.
- **Counterfeit Parts Avoidance.** TrustedCOTS solutions are manufactured following a number of best practices to minimize the risk that counterfeit parts enter the supply chain. Key standards include:
  - AS5553, the SAE International aerospace standard for avoidance, detection, mitigation, and disposition of counterfeit electronic parts.
  - ARP6328, the SAE International guidelines for implementing an AS5553-compliant counterfeit mitigation program.
  - AS9100D, the SAE International standard for quality management system requirements in aviation, space, and defense organizations.
  - Defense Federal Acquisition Regulation Supplement (DFARS), the Department of Defense (DoD) procurement process for goods and services.

  Companies that play an active role on the SAE International G-19CI Continuous Improvement Committee have the deepest understanding of the AS5553 standard and ARP6328 guidelines.
- **Supplier Quality Assurance.** All suppliers must be closely monitored for quality, compliance, and on-time delivery. But, it is not enough to monitor only direct suppliers. The suppliers' suppliers must also be closely monitored, and on down the line to the original manufacturer of each component and part that is used. This is the only way to safeguard the entire supply chain.

  In addition, innovations and best practices for improving quality must be shared with supply chain and manufacturing partners to increase the quality and consistency of every part supplied.
- **Smart and Secure Factory Operations.** Equally strict standards must be applied in manufacturing facilities. It is imperative that COTS suppliers provide robust mechanisms to protect their own manufacturing facilities and mitigate insider threats. Employees working on the manufacturing floor must be subject to background checks and other security requirements, such as International Traffic in Arms Regulations (ITAR) clearance, before they are allowed to work on the manufacturing line. In addition, all employees must receive comprehensive training to ensure their competency.

  Facilities that operate using lean methodologies and smart factory technologies are in the best position to continuously improve operations and increase quality. Factory operations should be fully digital so every component is electronically tracked and its exact location and stage in the process is known at all times. And all metrics and continuous improvement activities should be monitored and actioned to enable real-time adjustments to processes, as needed.

  In addition, all of the operational data collected must be analyzed so performance can be measured against key performance indicators (KPIs). To ensure optimal manufacturing performance at all times, quality metrics should be used to determine when equipment needs updating or replacing.

Safety-Critical Solutions: Combining Safety and Security

There is an increasing need to deliver safety-certifiable solutions that also meet security requirements.

TrustedCOTS solutions are designed to meet these intersecting requirements. They are based on deep analysis of exactly where and how safety and security domains overlap and complement one another, and where they require different approaches. For example, safety and security mandates overlap during secure boot procedures, but typically diverge in cases of an attack on the system.

Secure, safety-certifiable, TrustedCOTS solutions are developed following a number of industry standards, including:

- RTCA DO-326 Airworthiness Security Process Specification
- DO-254 Design Assurance Level (DAL) for hardware
- DO-178C DAL level for software

Long-Term Reliability: The Ultimate Goal

To provide long-term reliability, TrustedCOTS solutions must dependably perform under the harshest conditions in the field for many years. Providing this level of reliability means going beyond standard processes in a number of key areas. Here are just a few examples of Curtiss-Wright's efforts to increase long-term reliability in TrustedCOTS solutions:

- **VPX testing.** Curtiss-Wright led the original VPX (VITA 46.0) connector testing effort back in 2005, which proved much of the connector's capabilities, but also identified weaknesses to be resolved. This testing approach is now considered the benchmark for any new VITA connector testing, and has been repeated several times on different VPX connectors, including optical interconnects, as the most comprehensive evaluation of connector reliability.
- **Thermal cycling tests.** We perform thermal cycling testing on a periodic basis to determine the risks involved with new and challenging electronic packaging, such as fine pitch BGAs, leadless packages (e.g. QFNs), stacked microvias, and lead-free. Mitigations are tested at the same time. At the product level, we test to the VITA 47 ECC4 level as part of our standard product evaluation and continuous improvement processes. A key value of all this testing is to analyze the results to better understand the reliability physics, especially when failures occur. This understanding has contributed to innovations in such areas as lead-free solder and microvia techniques and technologies that increase long-term reliability in the field.
- **Lead-free solder.** Curtiss-Wright is a pioneer in the use of lead-free in harsh defense and aerospace applications. Our involvement in industry consortia such as AREA and PERM, in combination with IRAD projects and testing for over a decade, have built one of the most advanced capabilities for lead-free implementation in the industry. This capability is critical for the long-term reliability requirements of our industry, especially with the trends in RoHS and REACH legislation towards more and more restrictions on the use of lead.
- **PWB interconnects.** We have been performing reliability evaluations and tests on our PWB technologies and designs for close to two decades, and this has become a critical capability with the ever-increasing interconnect density found on today's designs that lead to early failure if not designed properly. Presently, there is a high degree of concern related to the use of microvias in high reliability applications, like defense & aerospace. Curtiss-Wright has a long history of successful microvia use in our PWBs, including stacked microvias, which are particularly difficult.

The Journey Never Ends

While long-term reliability is the ultimate goal for every TrustedCOTS solution, the journey to get there never ends. There are always new tests to run, new results to analyze, new opportunities to innovate, and new ways to improve performance in every area of TrustedCOTS solution development.

Curtiss-Wright is fully committed to continuing this journey and to strengthening our role as a trusted, proven partner to defense organizations and aerospace companies around the world. We are dedicated to:

- Investing in best-in-class technologies so we can further every one of the initiatives described in this paper
- Partnering closely with our suppliers and customers to build Trusted Computing measures into every solution from the ground up
- Increasing our understanding of the relationships and interactions among all of the elements that comprise Trusted Computing to deliver TrustedCOTS solutions with the highest possible levels of trusted operation
- Helping our customers continue to reduce risk, increase control, and optimize program costs after solution delivery through a comprehensive Total Life Cycle Management Program

All of the initiatives described in this paper apply to air, ground, and sea platforms. Together, they put Curtiss-Wright in a better position than any other solution vendor to provide TrustedCOTS solutions with the rugged performance, reliability, improved safety, and data security needed for any mission, anywhere, at any time.

As the most-experienced single source of comprehensive, rugged, and secure solutions for defense and commercial aerospace applications, Curtiss-Wright has the expertise, experience, and dedication needed to reduce risk and accelerate time to market for even the most challenging programs.

Author

Steve Edwards,

Director, Secure Embedded Solutions & Technical Fellow,

Curtiss-Wright Defense Solutions

David Sheets,

Security Architect,

Curtiss-Wright Defense Solutions

Aaron Frank, BaSC,

Senior Product Manager,

Curtiss-Wright Defense Solutions

Learn more

Technologies: Curtiss-Wright TrustedCOTS

White Paper: Introduction to COTS-based Trusted Computing

White Paper: The Many Faces of Trusted Computing

White Paper: Trusted Boot

White Paper: Getting Secure, Intel-Based Solutions to Market Faster - Why the Hardware Vendor's Boot Security Implementation Is So Important

White Paper: Hardware Features for Maintaining Security During Operation

White paper: Considering the Role of Hardware in Securing OS and Hypervisor Operation