Defense Grade Security Solutions for Industrial Systems

Industrial Market Challenge

Unlike a general purpose computing platform such as a PC, laptop or tablet, embedded systems in Industrial markets are typically built for a single purpose. In the past, embedded systems have been stand-alone, walled off from inter-device communication and never connected to the Internet. Over the years, these embedded systems have increased in sophistication, are being deployed worldwide, and built-in Internet connections have become more prevalent. Unfortunately while the connectedness, distribution, and sophistication of these systems are increasing, the security of these systems is not.

The reliability, safety, performance, cost, power, longevity, and security concerns of Industrial platforms require mature, proven, solutions. Microsemi® can leverage numerous technologies such as field programmable gate array (FPGAs), power modules, timing and synchronization, sensors, memory, and storage for robust Industrial solutions. Critically, Microsemi provides the industry's best products and services for securing communications, protecting hardware designs, and hardening software IP.

Industrial Security Products

Hardware security, software IP hardening, and cryptography products ensure to reduce the Industrial system susceptibility to IP theft, counterfeiting, or reverse engineering.

The Need for Security

Chinese Corporate Espionage of AMSC Wind Turbine

Unfortunately while the connectedness, distribution, and sophistication of Industrial systems is increasing, security is not.

Industrial Security Products

Microsemi's security products are proven effective for the most stringent security needs such as hardening embedded industrial systems' software, securing communications, and protecting designs from reverse engineering and tampering.

Hardware Design Security	EnforcIT® is a set of VHDL IP cores for Microsemi System-on-Chip (SoC) FGPAs, Xilinx, and Altera. Each IP core is a standalone security mechanism protecting against one or more reverse engineering, counterfeiting, or tampering attacks.
Software IP Hardening	CodeSEAL™ hardens IP on desktop and embedded systems in software against reverse engineering and tampering. Layers of active software security forces attackers to attack a complex network of countermeasures.
Cryptography	Microsemi's WhiteboxCRYPTO™ product combines mathematical algorithms, data, and code obfuscation techniques to transform the key and related crypto operations in complex ways requiring deep knowledge in multiple disciplines to attack. Importantly, the key is never present in static or runtime memory. Rather, the key becomes an inert collection of data that is useless without the uniquely generated white box algorithm. Support is provided for AES, RSA, ECC, and many other public and custom ciphers. The EnforcIT product includes Suite B, FIPS 140-2 certified cryptography cores.

	The Microsemi Advantage
Integrated Professional Services	Microsemi offers a full staff of experienced security professionals to perform risk assessments, design and implement protections, and to integrate security into Industrial systems.
Targeted Security Products	Hardware security, software IP hardening, and cryptography products ensure to reduce the Industrial system susceptibility to IP theft, counterfeiting, or reverse engineering.

Defense Grade Security Solutions for Industrial Systems

Professional Services

Microsemi was founded over 50 years ago and has highly skilled, dedicated services professionals with more than a decade of experience in IP protection, design security, and cryptography. Microsemi provides end-to-end solutions: creation of protection plans, development and implementation of secure designs, and red-teaming of protected systems to ensure IP is properly protected. We work with development teams to design protections that best leverage characteristics of the underlying platform and to build a robust protection network with no single point of failure.

Risk Management Services identify, scope, and integrate security requirements with project capabilities. A risk assessment supplies information helpful in analyzing costs/benefits, as well as in making critical security decisions to mitigate threats with minimal impact to project cost or schedule. A risk assessment reviews your system in detail to discover vulnerabilities, enumerate threats, and outline the likelihood and consequence of system compromise. These services, performed by engineers experienced in attack tree modeling, reverse engineering, and exploitation tools and techniques, provide the basis for protection planning and security engineering services.

Secure Design Services help design a robust, secure architecture for your embedded system that will remain resistant against reverse engineering, IP theft, counterfeiting, and data loss throughout your systems life. Using a risk assessment and other compiled data, you will receive documentation including a protection design and an implementation approach. The documentation describes how to mitigate identified system vulnerabilities and ensure system threats are addressed and security requirements satisfied.

Protection Evaluation Services review the security of your protection design to document vulnerabilities in the exposed system. **Red Teaming Services** start with a black-box approach, pitting experienced reverse engineers with state-of-the-art attack tools against your system in a deployed setting. **Blue Teaming Services** use the same experienced engineers, but provide them with full access to documentation, architecture diagrams, and other engineering expertise. A Blue Teaming approach typically reveals flaws in the secure design or protection implementation. While similar to a Red Teaming exercise, Blue Teams can produce results in a shorter time frame.

Security Engineering Services assists customers by providing an engineering team experienced with the tools, processes, and methods required to analyze, design, implement, and test security features for existing systems to satisfy ever changing protection requirements. Our engineers can develop custom security solutions and novel protection mechanisms that are unique to your application.

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at www.microsemi.com.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com