Security Solutions

Securing the World's Embedded Systems

Secured Ethernet Connectivity

IEEE 1588

FPGA and SoC Solutions

Data Center Security Solutions

Secure Packet Optical Transport Solutions

Synchronous Time Generation Solutions

Industrial Security

Microsemi

Power Matters.™

Microsemi Security Solutions

Hardware, Firmware, and Software Protection for Data-in-Motion, Data-in-Use, and Data-at-Rest

In today's hyperconnected world, cyber threats and security are top concerns of practically every organization. Embedded technology and system solutions are ingrained within our technology infrastructure, especially as they interconnect with communications networks, data centers, automated platforms, and emerging Internet of Things (IoT) devices. While this connectivity allows an unprecedented level of efficiency and transparency in many aspects of our lives, having systems subject to increasing digital control also makes them increasingly vulnerable to attack.

Cyber threats can emanate from virtually anywhere and can include:

- IP theft or reverse engineering
- Trojan horses, viruses, and worms
- Memory attacks
- Board level attacks (probing, memory tampering)
- Fault analysis
- Network attacks
- Side-channel analysis
- Supply chain attacks
- Signal jamming, spoofing, and denial-of-service

Consequently, the need to safeguard critical network infrastructure and information systems has never been greater. And it is not enough to simply harden the edge of our networks. A layered security approach—encompassing a hardware root-of-trust, security for data-in-motion, data-in-use, and data-at-rest, as well as cryptography and software protection—is critical. Microsemi's security solutions portfolio is specifically aligned to enable this layered approach and weave together the requisite elements to address multiple threat vectors. Our security solutions are broadly used by U.S. federal organizations and commercial entities in applications requiring robust protections such as financial, automotive, medical, digital rights management, gaming, and industrial automation.

Flexible Ethernet Solutions

Secured Ethernet Connectivity

Our increasingly connected lives now rely on Ethernet throughout most of the world's wide-area network (WAN) infrastructure to deliver voice, video, and data traffic. Standardizing on Ethernet for network communications opens up new options for data-in-motion security, because Ethernet networks work at Layer 2 (L2) and have their own encryption protocol defined in the IEEE 802.1AE MACsec standard. MACsec secures communication for authorized endpoints on the network to prevent data from being monitored or altered on the wire. Microsemi's secured Ethernet connectivity solutions include Gigabit Ethernet (GE) PHYs and 10GE PHYs.

Microsemi's secured Ethernet connectivity portfolio features Intellisec™ IEEE 802.1AE MACsec security, the industry's first technology to enable flow-based IEEE 802.1AE MACsec security encryption end-to-end over any network, including multi-operator and cloud-based networks, independent of the network's awareness of security protocols.

Microsemi's GE and 10G physical layer devices with Intellisec IEEE 802.1AE MACsec security are the world's only PHYs with 128-/256-bit AES encryption technology to have passed FIPS 197 256-bit AES encryption certification. FIPS 197 is a de facto benchmark encryption standard issued by the National Institute of Standards and Technology (NIST) that specifies the approved cryptographic algorithm to protect electronic data. 256-bit AES offers exponentially better data protection with ~10^{38} more key possibilities than 128-bit encryption.

Making Secure IEEE 1588 a Reality: Timing over MACsec

Highly accurate coordination of time is an essential part of operating many distributed systems including power grids, water and gas distribution systems, mobile communications networks, and industrial automation. The precision time protocol (PTP) as defined in the IEEE 1588 standard is used in all of these applications for time distribution.

As today's connected world is greatly dependent on reliable access to services—such as electricity and water, Internet and mobile services, and efficient manufacturing of goods—virtually any sector is vulnerable to cyber threats, making the security of operations vital. The good news is that MACsec can be used to eliminate threats on vulnerable Ethernet links and even connections over third-party Ethernet service providers. The need for a combined solution is clear: MACsec must secure the PTP distribution tree.

For tight network synchronization, PTP requires accurate time stamping of the packet. However, MACsec requires insertion and removal of the 24-byte to 32-byte MACsec header on all or some of the frames on the link, causing large delay variations between the egress time stamping point and the link connector (and similarly on the ingress). The PTP protocol assumes that the delay on a link is constant. However, with MACsec, this is not the case.

Encryption and timing accuracy have historically been incompatible. Microsemi has solved this challenge with our Intellisec PHYs, which fully preserve time stamping accuracy on a MACsec- enabled link. Secure 1588 is a reality.

FPGA and SoC FPGA Solutions

FPGAs and SoCs

Establishing a system root-of-trust is fundamental for any security scheme to protect critical data from attacks. Microsemi offers the industry's most secure FPGAs with licensed, patented, and certified Differential Power Analysis (DPA) protection to protect your design IP from copying and reverse engineering, built-in certified security functions, as well as supply chain assurance to ensure that the FPGA is authentic. Protecting your data-at-rest or data-in-motion is impossible without secure hardware and design security.

Our secure FPGA and SoC solutions include:

- PolarFire™ FPGAs
- SmartFusion®2 SoC FPGAs
- IGLOO®2 FPGAs

Microsemi is the only FPGA supplier offering a Secure Production Programming Solution (SPPS). Using the built-in device certificate, unique factory keys in each device, and Hardware Security Modules (HSMs), customers can program devices and inject key material in untrusted locations around the world. Using this technique provides the best assurance available that the device being programmed is free from supply chain counterfeiting issues such as upgrading of components, reclaiming and reselling used components as new devices, and overbuilding by foundry or test suppliers or rogue insiders. Microsemi's complete PolarFire FPGA, IGLOO2 FPGA, and SmartFusion2 SoC FPGA anti-counterfeit solutions enable true supply chain assurance and system authentication, providing the functions and production controls you need for a complete secure supply chain, from design and fabrication, to user programming and deployment, to field operation.

PolarFire Cost-optimized FPGAs Deliver the Lowest Power at Mid-range Densities

Microsemi extends its non-volatile FPGA leadership with the PolarFire family of cost-optimized FPGAs. PolarFire FPGAs deliver up to 50% lower power than equivalent SRAM FPGAs. The devices are ideal for a wide range of applications within wireline access networks and cellular infrastructure, defense and commercial aviation markets, as well as industrial automation and IoT markets.

As a true broad-range FPGA supplier, Microsemi offers FPGA product families spanning 1K to 500K logic elements (LEs).

Wireline access and cellular infrastructure markets can leverage Microsemi's expertise in delivering mission-critical security and high-reliability designs to defense and industrial markets when designing with PolarFire FPGAs. The devices offer unprecedented capabilities while maintaining all the advantages traditionally associated with non-volatile FPGAs such as the lowest static power, security, and single event upset (SEU) immunity. The PolarFire FPGA family delivers up to 50% lower power in a cost optimized architecture for mid-range densities.

With the introduction of PolarFire, the market now has a cost-optimized mid-range FPGA solution that not only delivers outstanding power efficiency, but significantly higher security and reliability than alternative solutions.

Cost-optimized Architecture

- Transceiver performance optimized for 12.7 Gbps, which yields smaller size
- Architecture and process optimizations for specific bandwidths (10 Gbps–40 Gbps) at specific densities
- 1.6 Gbps I/Os—best-in-class hardened I/O gearing logic with CDR (supports SGMII/GbE links on these GPIOs)
- High-performance, best-in-class hardened security IP in mid-range devices

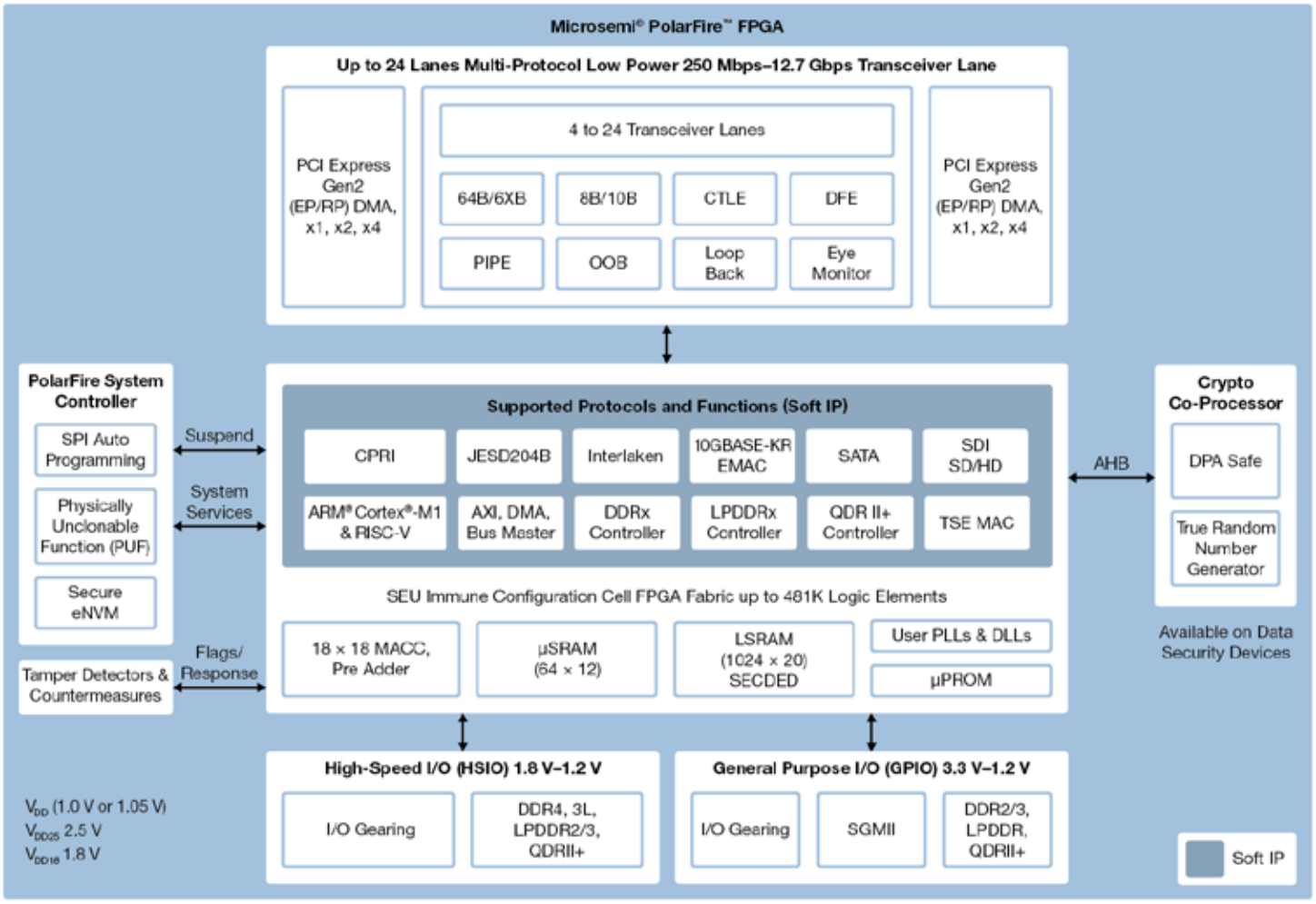
Power Optimization

- The lowest static power—28nm non-volatile process yields very low static power
- Optimized for 12.7 Gbps, which yields the lowest power
- Low power modes—Flash*Freeze yields best-in-class standby power
- Integrated hard IP—DDR PHY, PCIe endpoint/root port, crypto processor
- Total power (static and dynamic)—up to 50% lower power

PolarFire FPGA Architecture

PolarFire FPGAs Deliver Up to 500K Logic Elements, 12.7G Transceivers at 50% Lower Power

- High-speed serial connectivity with built-in multi-gigabit/multi-protocol transceivers from 250 Mbps to 12.7 Gbps
- Up to 481K logic elements consisting of a 4-input look-up table (LUT) with a fractureable D-type flip-flop
- Up to 33 Mbits of RAM
- Up to 1480 18x18 multiply accumulate blocks with hardened pre-adders
- Integrated dual PCIe for up to x4 Gen 2 endpoint (EP) and root port (RP) designs
- High-speed I/O (HSIO) supporting up to 1600 Mbps DDR4, 1333 Mbps DDR3L, and 1333 Mbps LPDDR3/DDR3 memories with integrated I/O gearing
- General purpose I/O (GPIO) supporting 3.3 V built-in CDR to support SGMII for serial gigabit Ethernet, 1067 Mbps DDR3, and 1600 Mbps LVDS I/O speed with integrated I/O gearing logic



Reliability Features

- SEU immune FPGA configuration cells
- Built-in SECDED and memory interleaving on LSRAMs
- System controller suspend mode for safety-critical designs

Security Features

- Cryptography Research Incorporated (CRI)-patented differential power analysis (DPA) bitstream protection
- Integrated physically unclonable function (PUF)
- 56 Kbytes of secure eNVM (sNVM)
- Built-in tamper detectors and countermeasures
- Integrated Athena TeraFire EXP5200B Crypto Co-processor, Suite B-capable
- Digest integrity check for FPGA, µPROM, and sNVM
- True random number generator
- CRI DPA countermeasure pass through license

FPGA Security

Cyber Security is the #1 Concern for Connected Devices on the Network Edge

It is not enough for today's demanding applications to meet the functional requirements of their design—they must do so in a secured way. Security starts during silicon manufacturing and continues through system deployment and operations. Microsemi's PolarFire FPGAs represent the industry's most advanced secure programmable FPGAs.

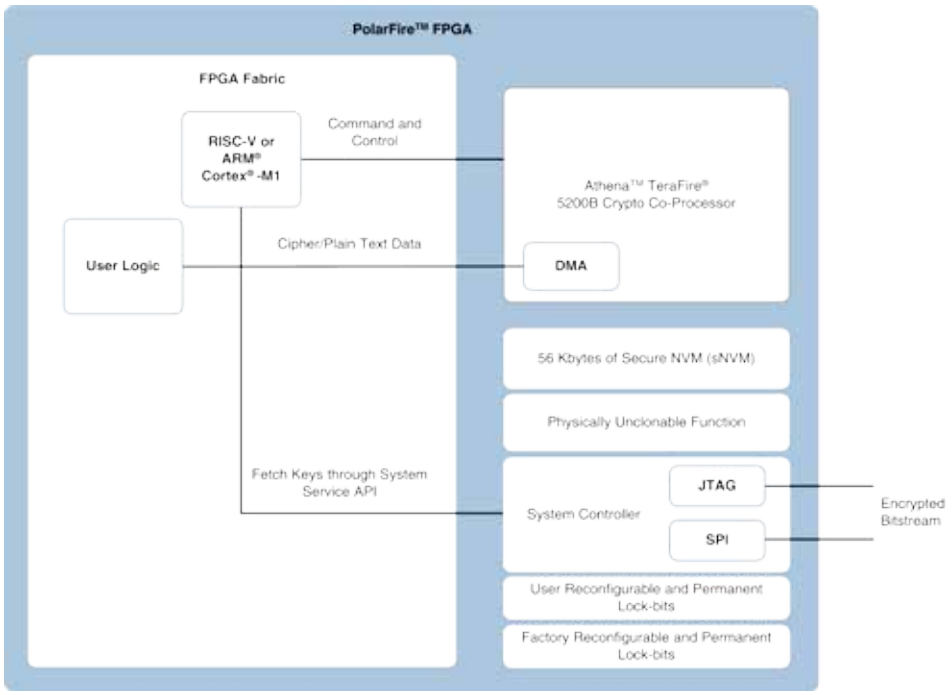
Microsemi Security Leadership

Security Advantage	Low Density		Mid-Range	
	Microsemi	Competition	Microsemi	Competition
Prevent overbuilding and cloning	Best Low-density Security	N/A	Best Security in the Industry	N/A
Full design IP protection		N/A		Weak
Root of trust		N/A		N/A
Secure data communications		N/A		Weak
Anti-tamper		N/A		N/A

Athena TeraFire® Cryptographic Processor

Select Microsemi PolarFire FPGAs build on the design security capabilities in all PolarFire FPGAs by enabling high-speed DPA resistant cryptographic protocols at wireline speeds. PolarFire data security FPGAs include the following additional features.

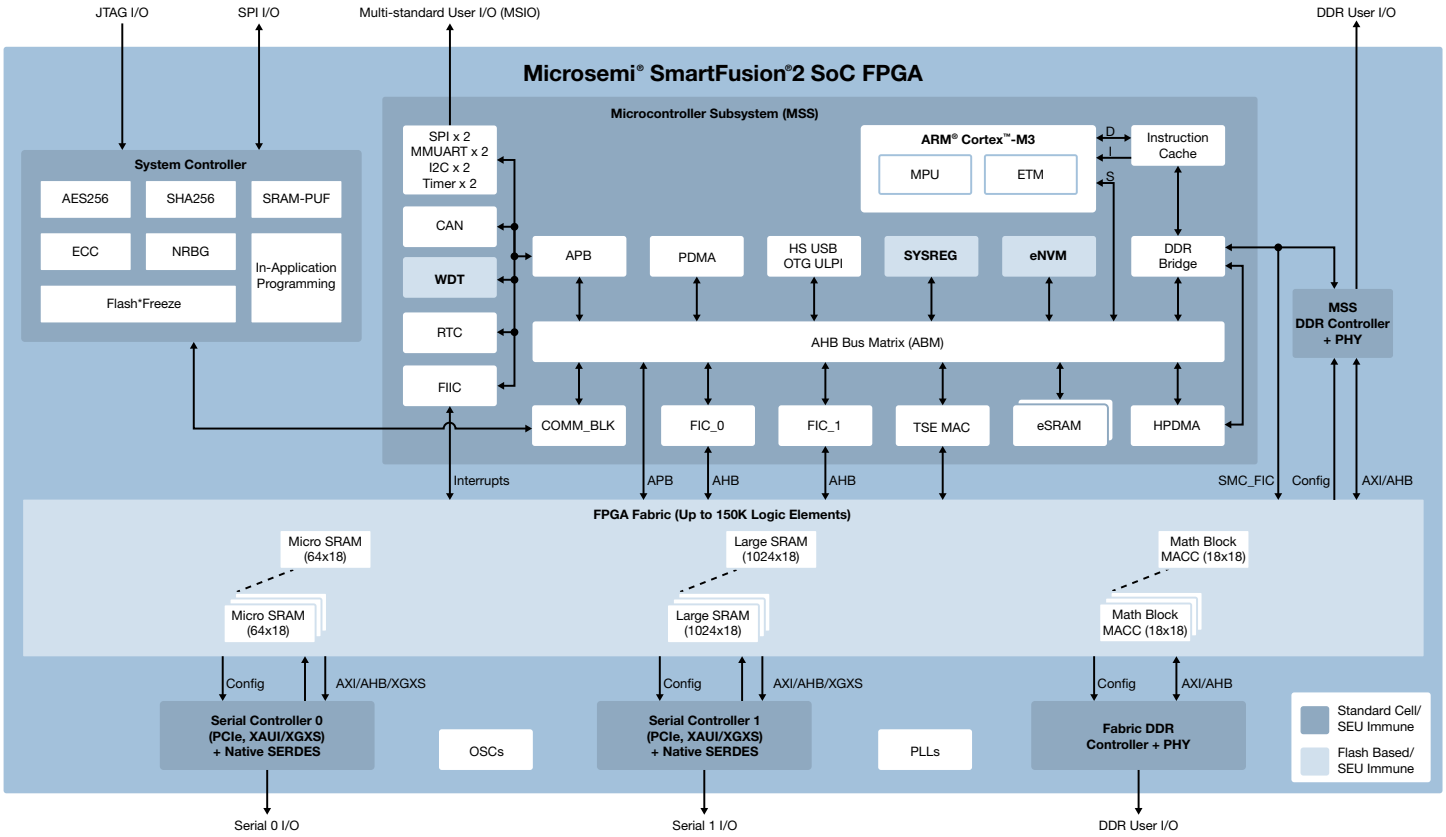
- Integrated true random number generator for enabling modern cryptographic protocols capable of generating random numbers at greater than 100 Mbps
- ~200 MHz Athena TeraFire F5200B DPA resistant cryptographic processor capable of implementing all Suite-B+ algorithms, and more.
- Rambus/CRI DPA pass-through licensing enabling DPA resistant high-speed cryptographic designs in the FPGA fabric. A CRI license is included in the purchase price of the TS devices. There is no need to negotiate a separate license.
- NIST-certified algorithms



More Resources in Low-Density Devices with ARM® Cortex®-M3 Processor

SmartFusion2 SoC FPGAs deliver more resources in low-density devices with the lowest power, proven security, and exceptional reliability. These devices are ideal for general purpose functions such as Gigabit Ethernet or dual-PCI Express control planes, bridging functions, input/output (I/O) expansion and conversion, video/image processing, system management, and secure connectivity. Microsemi SoC FPGAs are used by customers in communications, industrial, medical, defense, and aviation markets.

- Embedded ARM Cortex-M3 microcontroller subsystem (MSS)
- PCIe Gen2 endpoints starting at 10K logic elements
- Embedded DDR3 memory controllers
- Small packages
- 1 mW in Flash*Freeze mode
- Instant-on
- Zero FIT FPGA configuration cells
- SECDED memory protection
- NRBG, AES-256, SHA-256, ECC cryptographic engine
- User physically unclonable function (PUF)
- CRI DPA pass-through license



Secure Boot

We hear of security breaches in the news every day. This is primarily because most electronic systems are not secure and robust security protocols are not diligently observed by human beings. Processors are used extensively throughout these systems, and as most do not boot securely, they represent vulnerabilities to applications, systems, infrastructure, and personal data.

Microsemi's SmartFusion2 SoC FPGAs and IGLOO2 FPGAs are unique in that they have built-in security capabilities that can be used to provide a root of trust to an external processor.

SmartFusion2 SoC FPGAs and IGLOO2 FPGAs can uniquely solve this problem due to three simple facts:

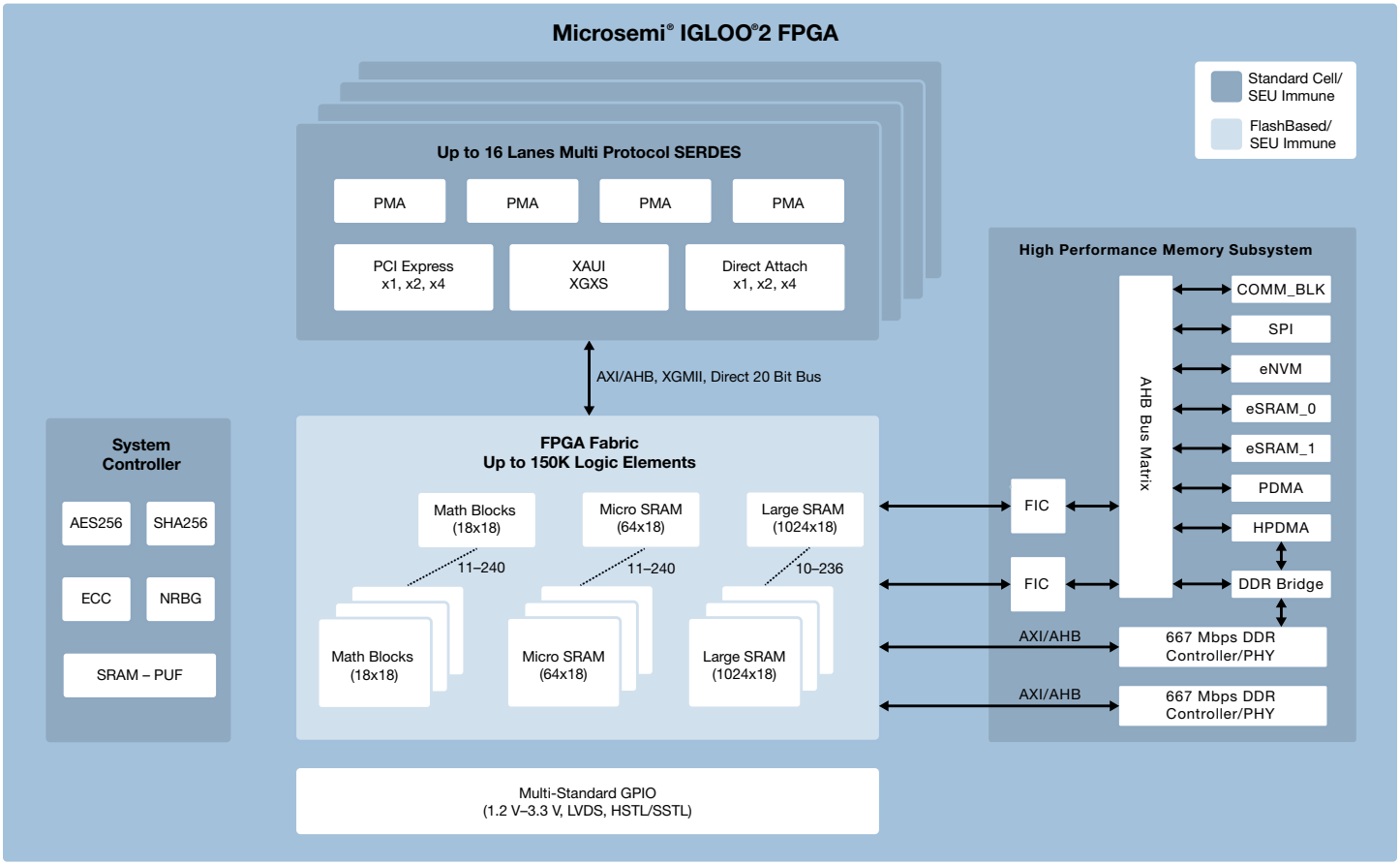
- They are the most secure FPGA's available that can establish a root of trust
- They embed internal secure eNVM for storing Phase 0 boot code
- They have fast IO's and fast programmable logic that can emulate any memory interface that a processor needs at speed

Microsemi makes it very easy to add security to your existing processor. Microsemi has created a reference design that uses a SmartFusion2 SoC FPGA as a root of trust to securely boot a processor.

More Resources in Low-Density Devices with High-Performance Memory Subsystem

IGLOO2 FPGAs deliver more resources in low-density devices with the lowest power, proven security, and exceptional reliability. These devices are ideal for general purpose functions such as Gigabit Ethernet or dual-PCI Express control planes, bridging functions, input/output (I/O) expansion and conversion, video/image processing, system management, and secure connectivity. Microsemi FPGAs are used by customers in communications, industrial, medical, defense, and aviation markets.

- High-performance memory subsystem
- PCIe Gen2 endpoints starting at 10K logic elements
- Embedded DDR3 memory controllers
- SECDED memory protection
- 1 mW in Flash*Freeze mode
- Instant-on
- Zero FIT FPGA configuration cells
- CRI DPA pass-through license
- Small packages
- NRBG, AES-256, SHA-256, ECC cryptographic engine
- User physically unclonable function (PUF)



Secure Production Programming and Secure Boot

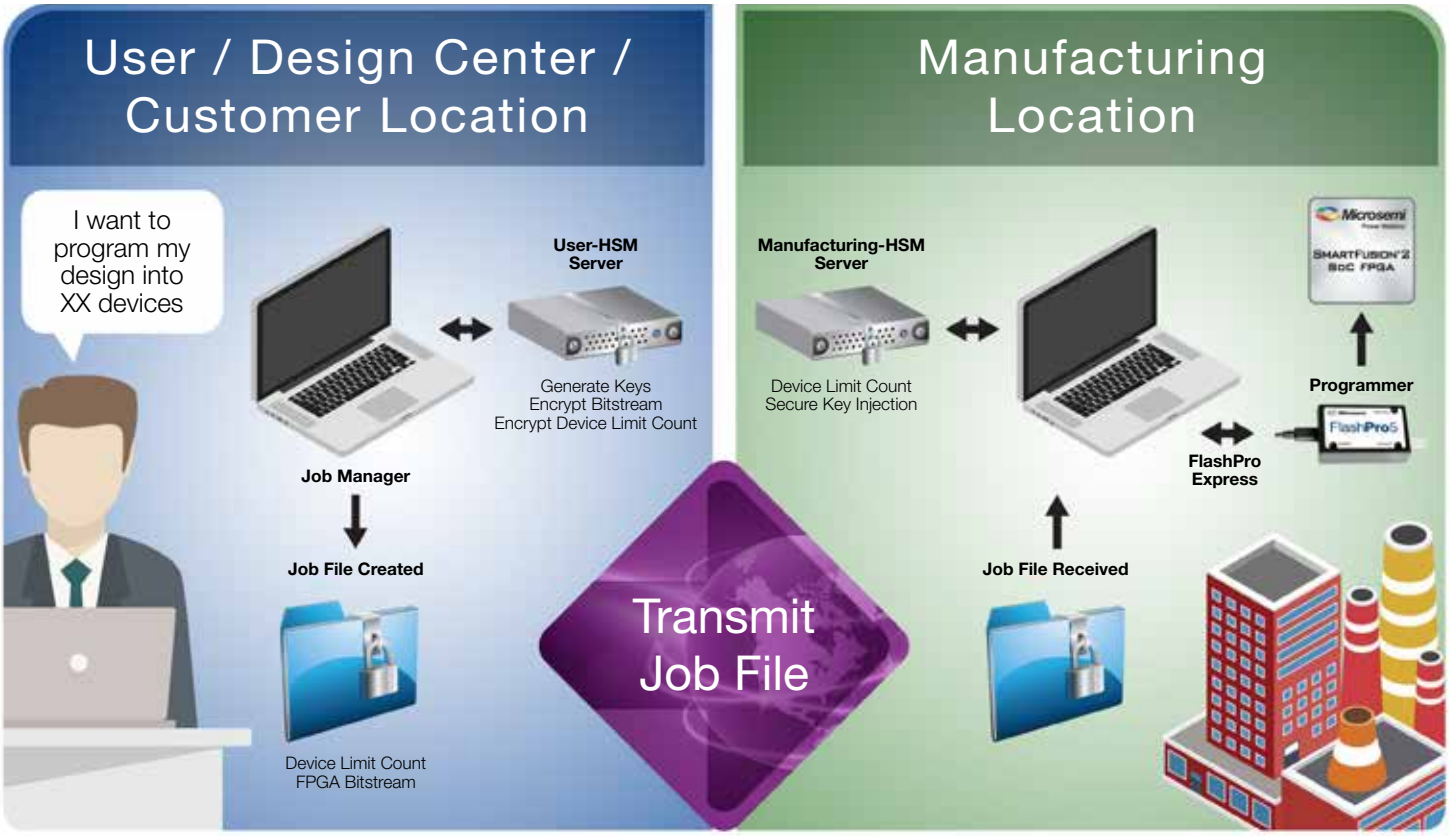
How to Prevent Overbuilding and Cloning

Overbuilding of electronic systems is the fastest way for OEMs to go out of business. When a contract manufacturer has the bill of materials (BOM), programming files, and test programs, they have everything they need to build more than they are authorized to build. Overbuilding can result in a significant loss of revenue, and additional support costs for systems that generated zero revenue for you.

Microsemi's Secure Production Programming Solution (SPPS)

Using Thales e-Security FIPS140-2 level 3-certified hardware security modules (HSMs), custom firmware, and the state-of-the-art security protocols built into every Microsemi PolarFire, SmartFusion2, and IGLOO2 FPGA, customers can automatically prevent overbuilding of their systems in any manufacturing facility anywhere in the world, saving millions of dollars in lost revenue.

How Does Secure Production Programming Work?



- The customer can control exactly how many devices are to be programmed
- The customer can specify who will be programming the devices
- The contract manufacturer can only program the exact number of devices specified
- Only validated Microsemi original devices can be programmed

No one else can access the programming information, and the system will not allow additional units to be programmed. No more overbuilding!

Data Center Security Solutions

Security. Performance. Scalability.

Safeguarding network infrastructure and storage systems is critical, now more than ever. Microsemi's IO and RAID solutions featuring controller-based data encryption (CBE) and secure boot FPGAs provide data center architects with the most secure and reliable server and storage infrastructure available.

Microsemi offers an industry-leading portfolio including solutions for system trust with our secure boot FGPA solutions, and robust data protection and security solutions for data-in-motion, data-in-use, and data-at-rest in data center environments. Our portfolio of technologies simplify time- and path-to-market with solutions tailored to an organization's unique security, platform, performance, and business requirements.

SAS/SATA Controller-Based Data Encryption

Alternative security solutions to protect data in transit to and from hard drives are power-hungry and expensive to deploy. Controller-based encryption offers several advantages over drive-based encryption including:

- Architectural—Supports all SAS or SATA disk media (HDD, SSD), including legacy devices. Microsemi's CBE technology enables hundreds of unique keys per drive (thousands of key per server) which enables more flexible use-cases such as instant user delete in multi-tenancy applications. Microsemi's CBE solution also addresses security holes by ensuring that 100% of the data on the drive can be encrypted as well as all data between the drive and controller as well as the data in the RAID controller cache.
- Performance—using a controller-based approach for data encryption delivers the utmost in scalable enterprise solutions. The ability to run at line rate protects your data center performance. Local or remote key management ensures your data-at-rest security with 256-bit XTS-AES encryption and FIPS 140-2 compliance.
- Operational—Controller-based data encryption does not require a special drive SKU to be managed, qualified and supported. All the standard management tools operate across our controller based encryption solutions.

Smart Stack: A Secure Solution for Storage

Microsemi's SmartRAID and SmartHBA solutions deliver a winning formula for managing and securing storage in data centers. Our converged architecture for hardware and software enables advanced performance and manageability in a unified portfolio that enables seamless integration for our OEMs, hyperscale data centers, and channel customers.

Data Center Secure Boot Solutions

While robust security measures to protect data-in-motion, data-in-use, and data-at-rest are fundamental to embedded systems security, establishing a hardware root of trust is equally essential. In the data center, adding a secure boot FPGA to the control CPU provides a means to ensure the authenticity of the underlying platform, manage keys securely, and provide strong anti-tamper countermeasures to protect against unauthorized physical access and reverse engineering.

Microsemi is a leader in embedded systems security and smart storage solutions, with a history of market leadership in controller-based data encryption and a complete portfolio based on a unified stack.

Proven Technology Solutions

Data Protection and Security Solutions for the Data Center

Building on our track record of technology leadership, Microsemi's innovative semiconductor and software solutions for data center infrastructure increase performance and enable next-generation services transforming networks that connect, store, and move big data.

Microsemi's high-density, high-performance, and low-power SAS/SATA and NVMe media controllers enable differentiating volume or velocity storage solutions for the data center.

Microsemi Flashtec® NVRAM Drive family is a PCI-Express® NVRAM solution based on the most advanced NVMe controller on the market. This family provides a new level of performance to the memory/storage hierarchy, ushering storage system OEMs, cloud applications, and service providers to the era of storage-class memory.

Microsemi's SAS, PCIe, and Ethernet fabrics enable extreme storage system scalability. Our fabrics are found within leading rack scale architectures where disaggregation of media and CPU resources create highly-optimized designs.

Microsemi Adaptec® host bus adapters are an ideal solution for server-based storage systems that require maximum bandwidth and I/O connectivity, low power, and high reliability. Our SAS/SATA RAID adapters meet the storage needs from entry-level to the most performance-hungry transactional database applications, and our SAS expander cards offer a scalable connectivity/fan-out option for additional drives when used in conjunction with a SAS RAID adapter or SAS HBA.

Microsemi's SAS/SATA Storage and PCIe (NVMe) Flash Controllers have XTS-AES encryption engines and key management assist functions (AES Key Unwrap, TRNG), enabling controller-based encryption (CBE) or self-encrypting drive (SED) solutions for data-at-rest encryption. Our secure boot FGPAs ensure a secure boot loader for bare metal or virtualized environments. MACsec PHYs are used for end-to-end network encryption.

Our proven technology solutions support software-defined storage (SDS), synchronous replication, time stamping, or network analytics (microburst detection).

Secured Optical Transport Solutions

Securing the Optical Layer with OTN Encryption

Due to the mass migration of data, services, and workloads to the cloud, 'in-flight' data security in the optical transport network (OTN) is a top priority issue and a key component in any holistic end-to-end security strategy for cloud and communications service providers today. However, data encryption in these networks cannot come at the expense of compromising service quality. Encrypting the optical layer end-to-end using OTN is a compelling option that addresses this need, offering a low latency, service agnostic solution that makes efficient use of expensive network resources.

OTN is the de-facto transport protocol for next-generation 100G+ metro and core optical transport networks worldwide. OTN, defined by the ITU G.709 standard, is a multi-service, multi-rate convergence layer that is capable of supporting multiplexing, transport, and switching of virtually all client types and protocols, from Ethernet and SONET/SDH, to datacenter-focused Constant Bit Rate (CBR) clients such as Fiber-Channel, spanning 1 Gbps to 100 Gbps data rates.

OTN encryption delivers the following benefits to network operators.

- Service agnostic end-to-end optical encryption—OTN encryption secures all client types and protocols end-to-end in optical transport networks, from 1G to 100G data rates
- Low latency
- No impact to network efficiency—OTN encryption does not require 'padding' to encrypt traffic
- Flexible deployment—encrypted traffic can traverse switched or point-to-point optical networks without the need for intermediate nodes to add encryption/decryption capabilities
- Strong encryption and authentication—AES-based block ciphers with support for GCM and CTR authentication modes

Microsemi OTN Processing Encryption Solutions

Microsemi's innovations in OTN processing silicon, represented by the DIGI-G4 400G OTN processor, address the needs of cloud and communication service providers for secure, flexible, scalable, SDN-ready, optical transport infrastructure.

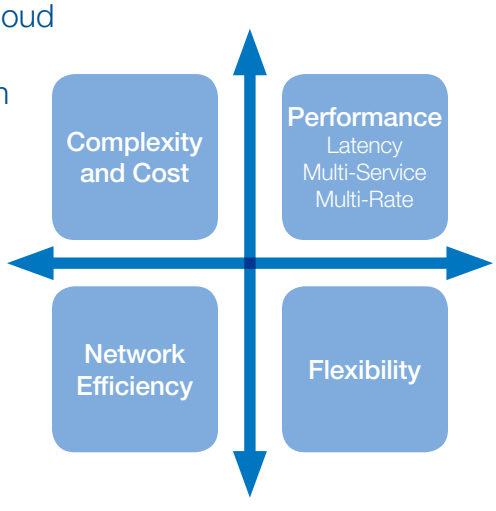
Microsemi's DIGI-G4 family of devices integrate rate-agile, protocol-agnostic, standards-certified (FIPS 197) AES-256 OTN encryption functionality, delivering sub-180 ns encryption latency performance, which allows secure transport of mission-critical data without trading off network performance and efficiency.

Microsemi's DIGI-G4 supports flexible encrypted service delivery and network deployment models, allowing service providers to deploy encryption-enabled transport platforms with confidence end-to-end in the transport network. The DIGI-G4 uniquely delivers the industry's first sub-wavelength Layer 1 encryption solution, enabling for the first time end-to-end encrypted transport services that are compatible with the OTN switched networks that are fast becoming the backbone of optical networks worldwide. End-to-end encrypted links can be offered at 'service-layer' granularity and can be switched efficiently through 100G metro OTN switched networks, without requiring disaggregation of 'bulk' encrypted links at every node in the network.

Key differentiating features of Microsemi's DIGI-G4's OTN encryption solution include:

- Ultra-low latency (sub-180 ns)
- Scalable, multi-service, wire-speed and rate-agnostic encryption from 1 Gbps up to 100 Gbps

Securing the Cloud with Microsemi OTN Encryption



Synchronous Time Generation Solutions

Mitigating GPS Vulnerabilities with Leading-Edge Network Timing Solutions

Positioning, navigation, and timing (PNT) systems are heavily reliant on GPS. A fundamental challenge that touches many industry sectors is that GPS is often treated as a trusted source of PNT. However, few systems have the mechanisms to ensure the integrity of the GPS information that they receive. In many cases, there are deliberate attempts to disrupt the GPS signal to take control of critical assets or to bring down certain systems. GPS attacks are categorized according to the failure mode they induce.

- GPS Jamming—this type of attack causes partial or complete loss of the GPS signal. It is commonly the result of unintentional interference from nearby RF sources. More complex jamming attacks can be orchestrated by adversaries to make it more difficult to detect the source of the jamming, but the result is the same. In such cases, the GPS receiver fails to receive the GPS signal.
- GPS Spoofing—this type of attack is the result of reception of illegitimate GPS signals. The GPS receiver is tricked into tracking GPS-like signals and it continues to operate, but the solution for position and time given by the receiver will be wrong. These types of attacks are almost always intentional attacks and can be difficult to detect.

The most common type of GPS signal outages today continue to be caused by extreme weather conditions including high winds, lightning strikes, large hailstones, and heavy snow/ice accumulation, all of which can damage or adversely affect the performance of an outdoor GPS antenna. Back-up systems are needed to assure timing and synchronization for critical infrastructure applications such as electrical power transmission, telecommunications, transportation, and financial/banking services, among others.

Microsemi provides a complete solution set to protect network disruption for the 24/7, 365 world we live in.

Network Infrastructure Protection

Timing and synchronization are indispensable in our increasingly digital, networked world. Precise time enables virtually all infrastructures such as data centers, wired and wireless communications, financial exchanges, industrial networks, smart power grid, and other secure communications. Securing synchronous time is vital to protecting critical communications infrastructure, particularly when organizations rely on publicly available time servers acting as sources of coordinated universal time (UTC).

Microsemi is the world leader in network synchronization and precise time solutions, delivering robust network solutions for a comprehensive and secure timing infrastructure. Our end-to-end timing solutions generate, distribute, and apply precise time. Microsemi's portfolio includes:

- Timing and synchronization systems supporting today's precise timing standards: GPS-based timing, IEEE 1588 (PTP), Network Time Protocol (NTP), synchronous Ethernet, and DOCSIS timing.
- Clock and frequency references including hydrogen, cesium, and rubidium standards, and quartz oscillators to ensure continuity and integrity of synchronization through GPS outages.
- Timing and synchronization ICs for clock management (clock synthesis, rate conversion, jitter attenuation, and fan-out buffer timing), OTN and packet timing.

Secured Industrial Infrastructure

Industrial Grade Technology: Power-Optimized, Flexible, and Reliable

A migration to Industry 4.0 architectures and smart connectivity are fundamentally changing business operations. Improving operational efficiencies with data-driven decision-making translates to increased networking of industrial automation and control with business systems. Expanded machine to machine (M2M) communications proliferates the use of fielded sensors and nodes. The growing rise of cloud services for aggregating raw sensor data and handling the big data requirements of the Industrial Internet of Things (IIoT) requires decentralized, secure computing. Coupled with the pervasive imperatives for portability, cyber security mitigation, and functional safety in the industry settings, businesses must be able to securely manage this evolution.

More than ever, industrial platforms need integration of additional communications protocols into existing form factors, greater processing power throughout the network and in portable equipment, as well as data security to ensure system integrity.

Microsemi provides a complete hardware and software solutions portfolio for reliable, safe, secure, lower-power, and cost-optimized designs for industrial infrastructure. Our solutions include non-volatile/SEU-immune, secure, and low-power low density FPGAs, and silicon carbide (SiC) diodes/MOSFETS/module solutions to power your designs. Microsemi's networking portfolio offers Ethernet switches, Ethernet PHYs, and full Industrial Ethernet software stacks, signal integrity ICs, cost-optimized, low-power, mid-range density FPGAs, and Power over Ethernet (PoE) midspans and injectors (including industrial grade PoE) to bridge and power your communication networks. Microsemi also provides timing solutions to synchronize your networks, and security layers protecting hardware/software, manufacturing, and data integrity.

Microsemi is the only IC, systems, and software provider with power-optimized, flexible, and reliable industrial networking solutions offering Ethernet and fieldbus protocol support. Whether designing for programmable logic control, human machine interface (HMI), or smart grid infrastructure, Microsemi solutions readily address the needs of both business IT and operational technology, enabling flexible and adaptable support of evolving business needs in industrial settings.

Join us at an upcoming Microsemi Security Forum

Hosted annually in the United States and Europe, the Microsemi Security Forum is a specifically designed, one-day conference for system-level architects, research and development engineers, design and component engineers, and other industry professionals seeking the latest innovations in the unique, evolving security market. The Microsemi Security Forum is an invitation-only event for our customers and partners, as well as industry architects and engineers interested in the latest security solutions. Check our website or contact our sales team to learn more.

www.microsemi.com/events

Microsemi is continually adding new products to its industry-leading portfolio.

For the most recent updates to our product line and for detailed information and specifications, please call, email, or visit our website:

Toll-free: 800-713-4113

sales.support@microsemi.com

www.microsemi.com

Microsemi
Power Matters.™

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

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center 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; enterprise storage and communication solutions, 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, California and has approximately 4,800 employees globally. Learn more at www.microsemi.com.

SEC-03-17