FPGA System and Device Level Security Considerations

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

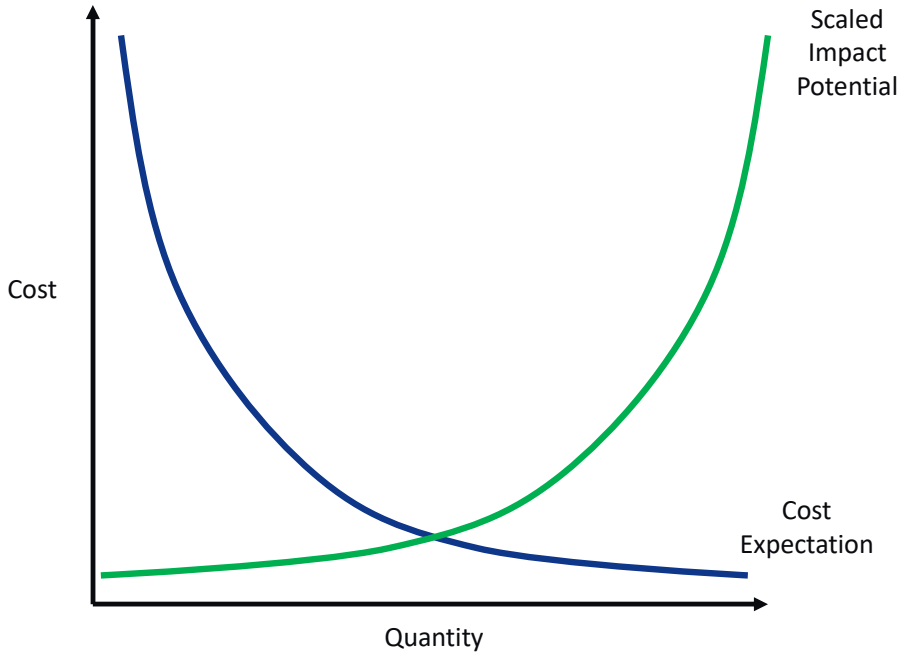
Ian Pearson

FPGA Frontrunners Nov23

Connected Embedded Spans Multiple Sectors

Spot the Difference

- **What is the attack surface and how does an attacker view these use-cases?**
- **What asset am I protecting?**
- **The fiscal value and prize value may be different**
- **The scaled fiscal impact potential may be polar opposite of cost sensitivity**
- **Classic Embedded Architectures may be inadequate due to bolt-on-security –v- secure-by-design**
- **If they are all connected, utilize largely the same devices, same protocols and core (security) software and share the same bugs and attack vectors are they all equally vulnerable to the same threat scenarios?**

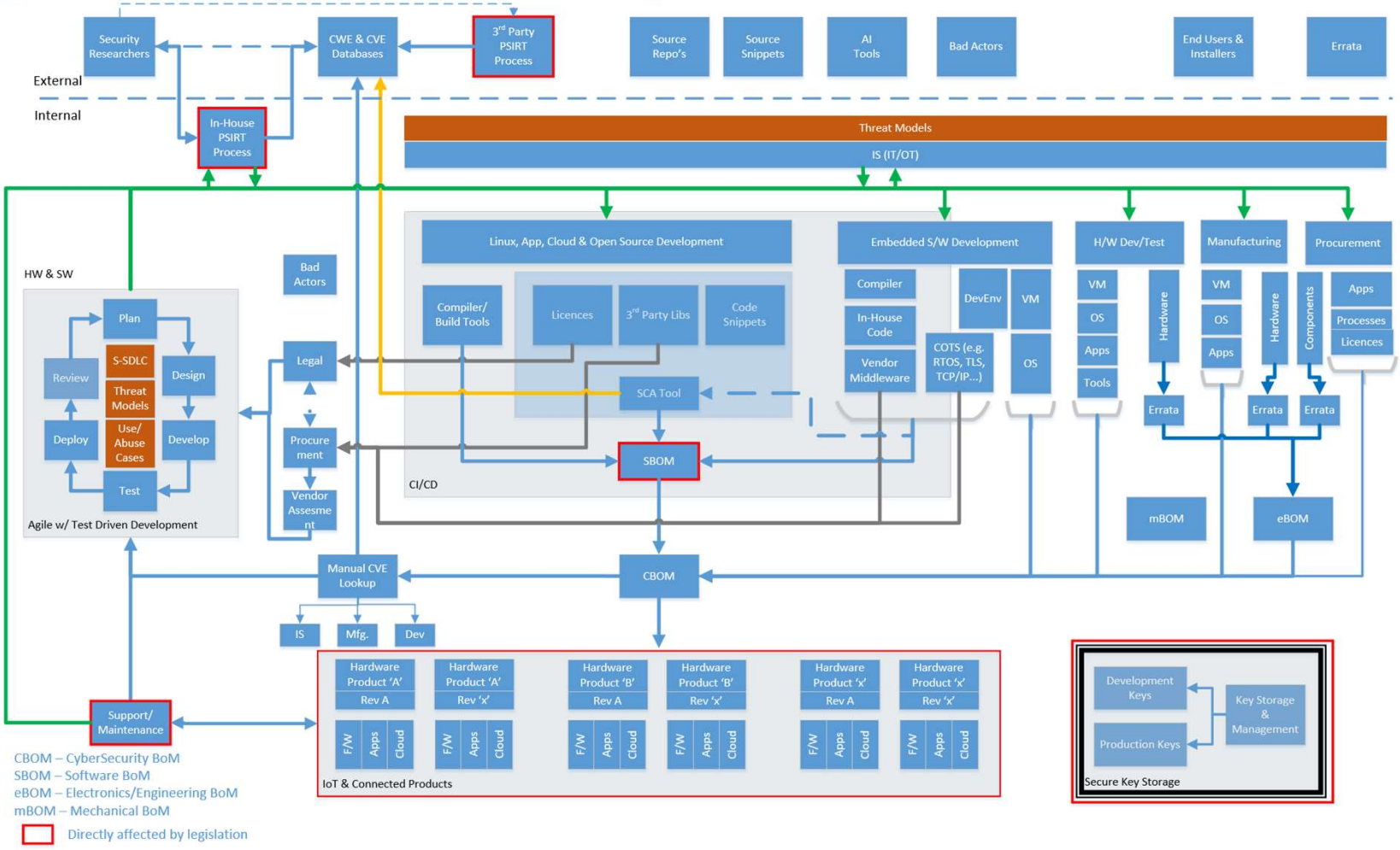


Attack Surface

MICROCHIP

A Whole of Business Approach

Security is a Whole of Business Challenge



Security Landscape

What are we protecting against?

Potential Threats in Your Supply Chain And Equipment

Insiders
Industrial Espionage
Criminal Profiteers
Nation-States

Chip Manufacturer

Gray Market

OEM

System User

- Trojan Horse in Hard IP
- Trojan Horse in IC Design
- Insert Trojan in Mask
- Overbuild & Steal Wafers
- Load Wrong Keys
- Sell Failed Devices

- Re-mark packages
- Refurbish Used Parts
- Steal Finished Goods

- Trojan Horse in Soft IP
- Trojan Horse in FPGA
- Modified EDA Tools
- Load Wrong Keys
- Load Wrong Configuration
- Overbuild Equipment
- Reverse Engineer

- Fielded Systems
- Side Channel Analysis
- 3rd-Party Clones
- Tampering

Secure Hardware and Trust | Design Security & Anti-Tamper | Data Security & Information Assurance

MICROCHIP

Embedded System Attacks Summarized

Secure Boot

- comprising

Memory

- Read (Dump object code)
- Replace
- Re-flash

Bus

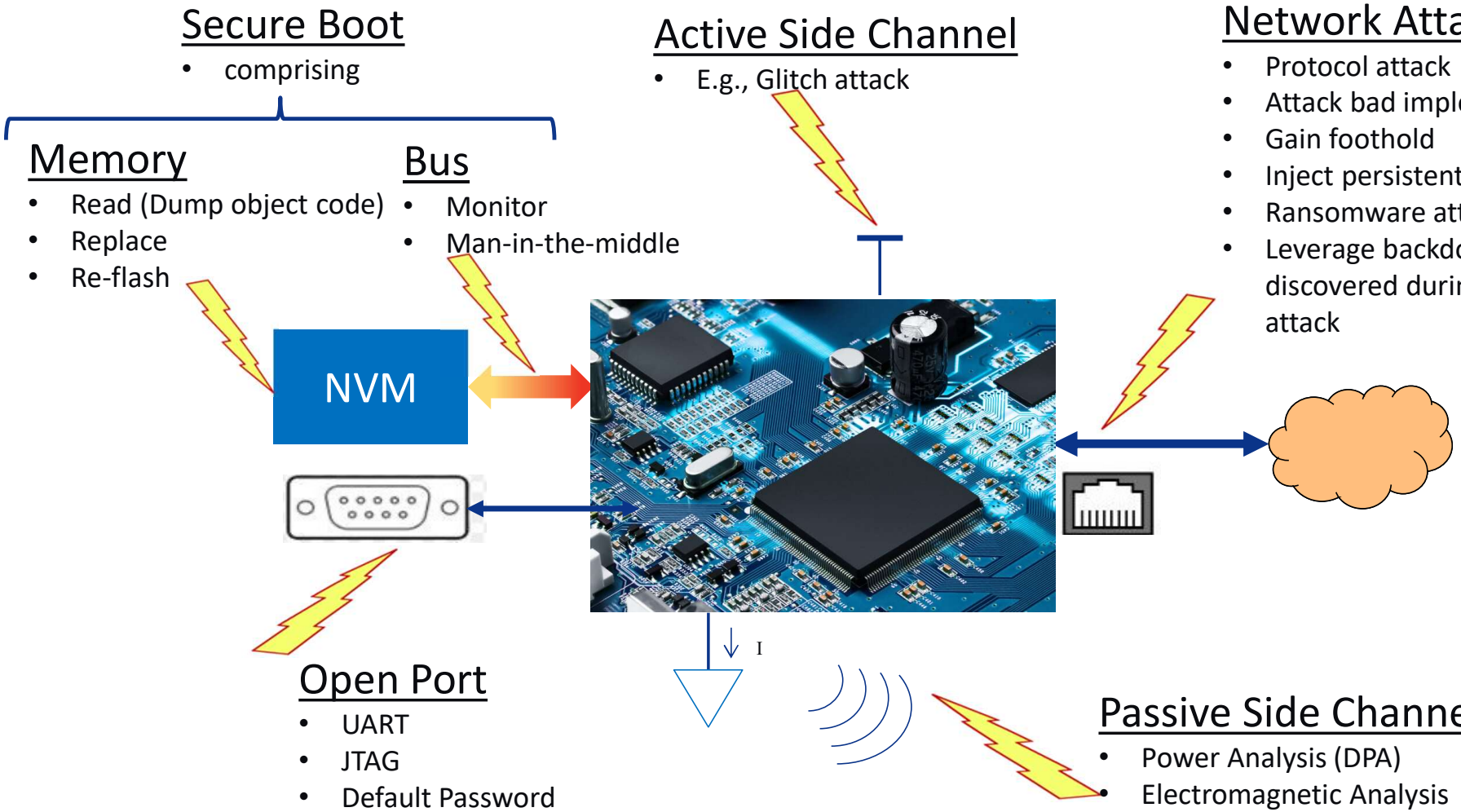
- Monitor
- Man-in-the-middle

Active Side Channel

- E.g., Glitch attack

Network Attack

- Protocol attack
- Attack bad implementation
- Gain foothold
- Inject persistent malware
- Ransomware attack
- Leverage backdoors/faults discovered during physical attack



Open Port

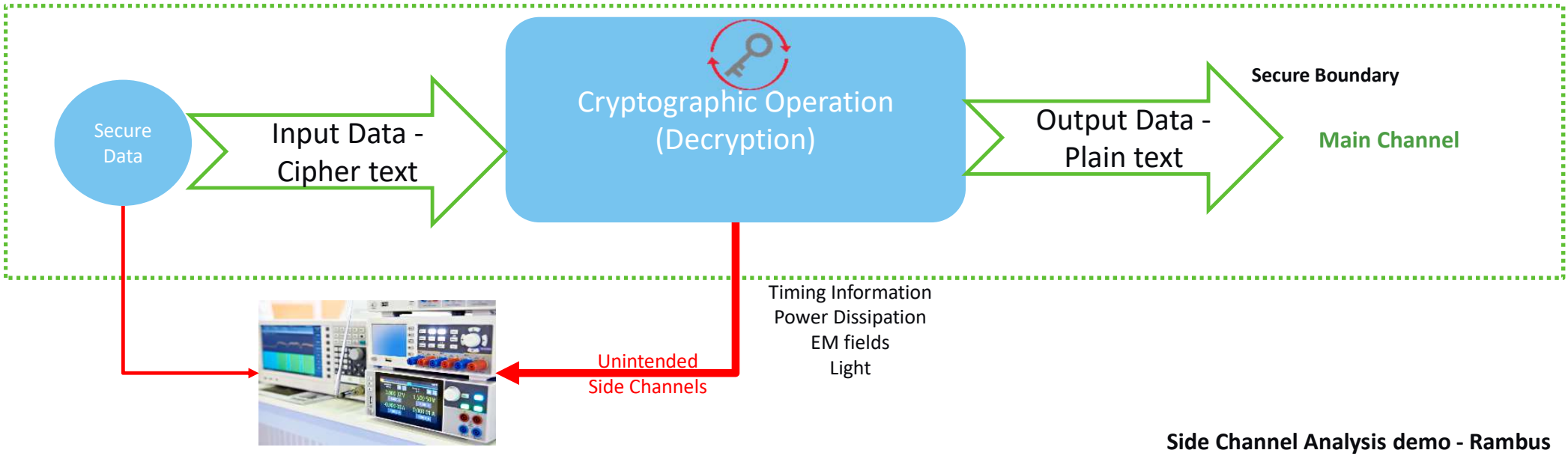
- UART
- JTAG
- Default Password

Passive Side Channel

- Power Analysis (DPA)
- Electromagnetic Analysis

MICROCHIP

Side Channel Analysis

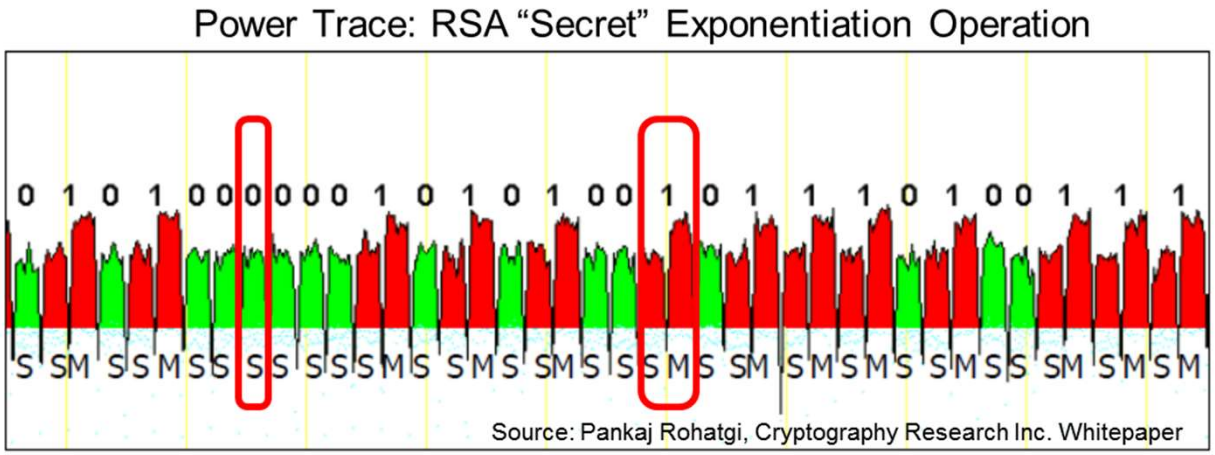


Side Channel Analysis demo - Rambus

Value of secrets such as keys leak out via unintended side-channels:

- SPA – Simple Power Analysis
- DPA – Differential Power Analysis
- DEMA – Differential Electro-magnetic Analysis

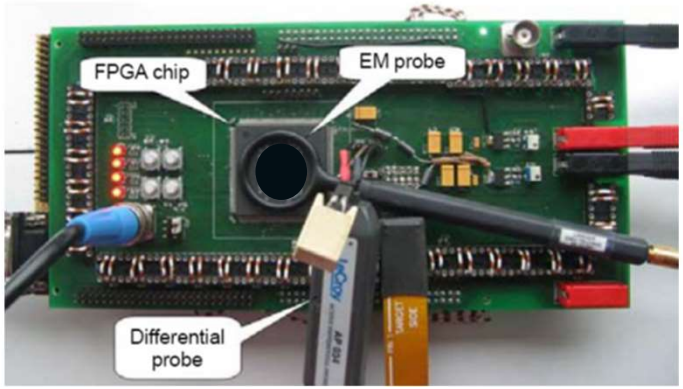
Simple Side Channel Analysis



Secret Exponent
{0 or 1}

S = Square
M = Multiply

If Secret Exponent = 0
Square
Else
Square + Multiply



Side Channel Analysis

A $400 setup can cost you millions

https://www.newae.com/chipwhisperer

MICROCHIP

The Cost of Overbuilding & Cloning

- **The U.S. Chamber of Commerce estimates that intellectual property (IP) threats cost domestic companies more than $250 billion per year in lost revenues. Add to that the loss of approximately 750,000 jobs**

- **The annual revenue loss due to IP theft equates to current annual level of U.S. exports to Asia — more than $300 billion. Over 55 million jobs in the U. S. are supported by IP intensive industries.**

MICROCHIP

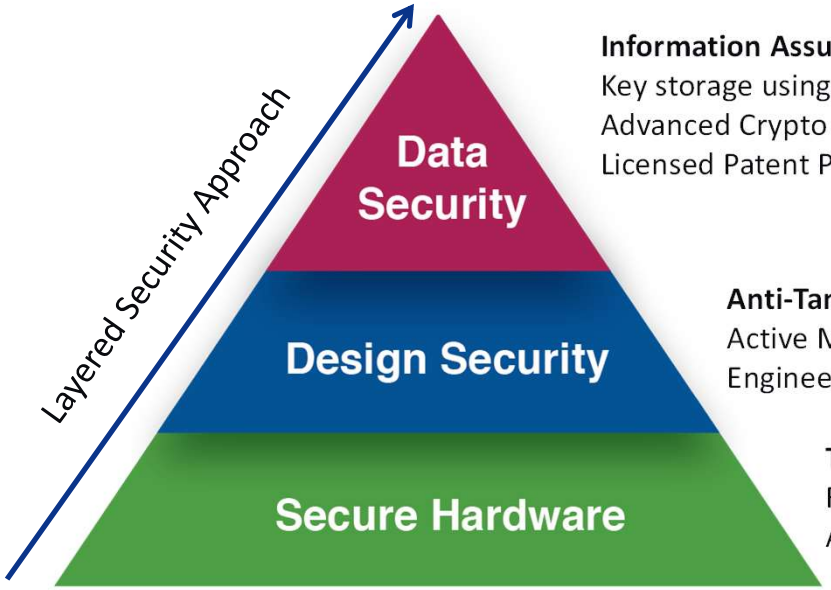
Microchip FPGA Security

What security measures do we have

Microchip FPGA and SoC

Secure Foundations for Comprehensive Security

To protect your information you need
Secure Hardware, Design Security and Data Security



Information Assurance:
Key storage using Physically Unclonable Function (PUF)
Advanced Crypto Accelerators
Licensed Patent Protected DPA Resistance Pass through License

Anti-Tamper: Secure Bitstream, Tamper Detection, Active Mesh, No Copying. Cloning, or Reverse Engineering

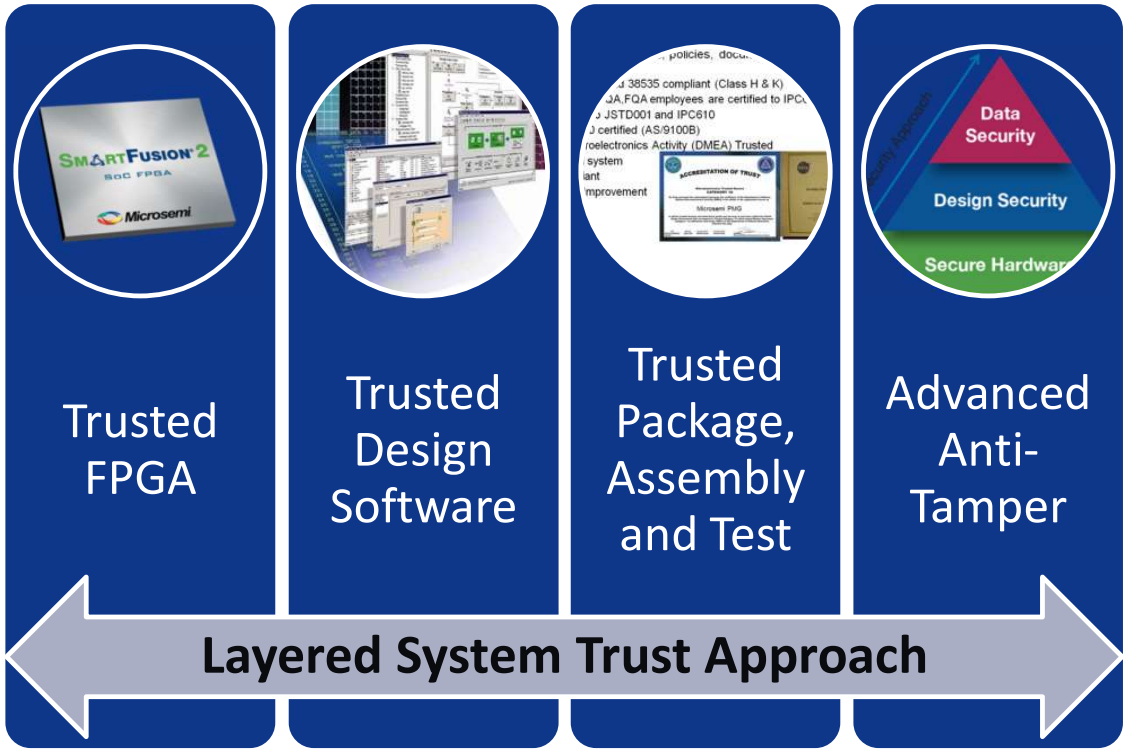
Trust: Licensed Patent Protected DPA Resistance, NIST Certified Crypto Accelerators, Secure Supply Chain

Microchip FPGAs provide
a solid foundation for your security needs

The Licensed DPA Logo and the Security Logo are trademarks or registered trademarks of Cryptography Research, Inc. in the United States and other countries, used under license.
The following SmartFusion®2 and IGLOO®2 FPGA protocols and services were evaluated: BSP, BAS, KVP, PTP, OTP, DCS and PPS, in obtaining the Security Logo certification

Microchip FPGA

Trusted System Supply Chain



LICENSED DPA COUNTERMEASURES™

Microchip has the industry's most secure FPGAs and accredited manufacturing flow

MICROCHIP

PolarFire FPGA

"Successfully Reviewed" by NCSC

Microchip's PolarFire® FPGA's Single-Chip Crypto Design Flow "Successfully Reviewed" By the United Kingdom Government's National Cyber Security Centre

The Review confirms strength of PolarFire FPGA's security solution

CHANDLER, Ariz., August 30, 2023 – Security is now an imperative for all designs in every vertical market. Today, system architects and designers received further evidence of the security of their communications, industrial, aerospace, defense, nuclear and other systems relying on Microchip Technology's **(Nasdaq: MCHP)** PolarFire FPGAs. The United Kingdom Government's National Cyber Security Centre (NCSC) has reviewed the devices when used with the Single-Chip Crypto Design Flow against stringent device-level resiliency requirements.

"The NCSC conducts a very rigorous analysis, and the work done with Microchip on the Design Separation Methodology in the PolarFire FPGA enables the user to take advantage of improved resilience and functional isolation within the device. This reinforces Microchip's commitment to our comprehensive approach to security," said Tim Morin, technical fellow at Microchip's FPGA business unit. "This analysis provides the option for single-chip cryptography in addition to what already exists within the devices for protecting IP, securing data and protection against physical tampering—an often overlooked and very powerful threat to every electronic system, especially those at the intelligent edge."

PolarFire FPGAs implement Microchip's industry-leading security architecture to protect intellectual property, secure data and secure supply chains.

- **PolarFire FPGA IP protection includes:**

MICROCHIP

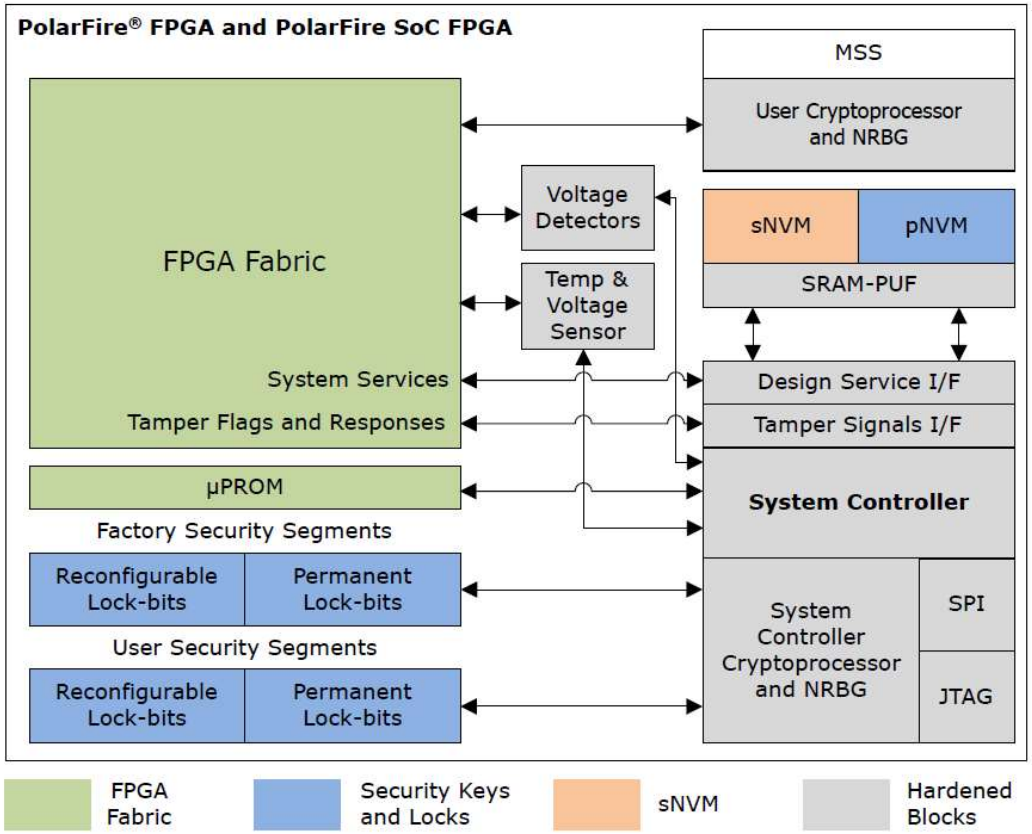
Microchip FPGA Security Evolution

Security Layer	Generation 3	Generation 4	Generation 5
Logic Elements	100 - 30K	5K - 150K	PolarFire : 50K - 480K PolarFire SoC : 25K - 460K
Transceiver rate	--	1-5 Gbps	250 Mbps-12.7 Gbps
Hardware Security		• Anti-counterfeiting and supply chain protection • Secure Production programming solution	• **Spectre and Meltdown immunity [2]** • **Device integrity check** • Anti-counterfeiting and supply chain protection • Secure Production programming solution
Design Security	Optional Encryption	• SRAM PUF[1] • Encrypted keys • Licensed and certified DPA counter measures • Hardware locks	• **Physical memory protection [2]** • **Standard and User Secure boot[2]** • **SRAM PUF enhanced w/buskeepers** • **Enhanced anti-tamper** • **Enhanced crypto services w/TeraFire EXP-F200ASR** • Licensed and certified DPA counter measures • Hardware locks
Data Security	• AES encryption • FlashLock Pass Key protection	• Cryptographic services (AES, SHA, ECC) • True Random Number generator (NRBG) • Pass through DPA countermeasure license	• **Integrated Athena™ TeraFire® EXP-5200B DPA-resistant Crypto Processor** • **Encrypted/authenticated Secure NVM(sNVM)** • True Random Number generator (NRBG) • Pass through DPA countermeasure license

1 - only available in the -060, -090 and -150 devices
2 - PolarFire SoC Feature

Microchip FPGA Security Architecture

PolarFire SoC and PolarFire FPGA



- **System Controller**
  - Powers up the device
  - Security enclave
  - System Services
    - Standard API to the System Controller
  - NVM memory
    - Private NVM (pNVM)
      - Patch code/keys for the controller
    - Secure NVM (sNVM)
      - Init data for user xcvrs config
      - User key store

MICROCHIP

Secure Non-Volatile Memory - sNVM

- **56K Bytes**
- **Three Modes**
- **Pages can be “ROM’d”**

Plaintext Mode

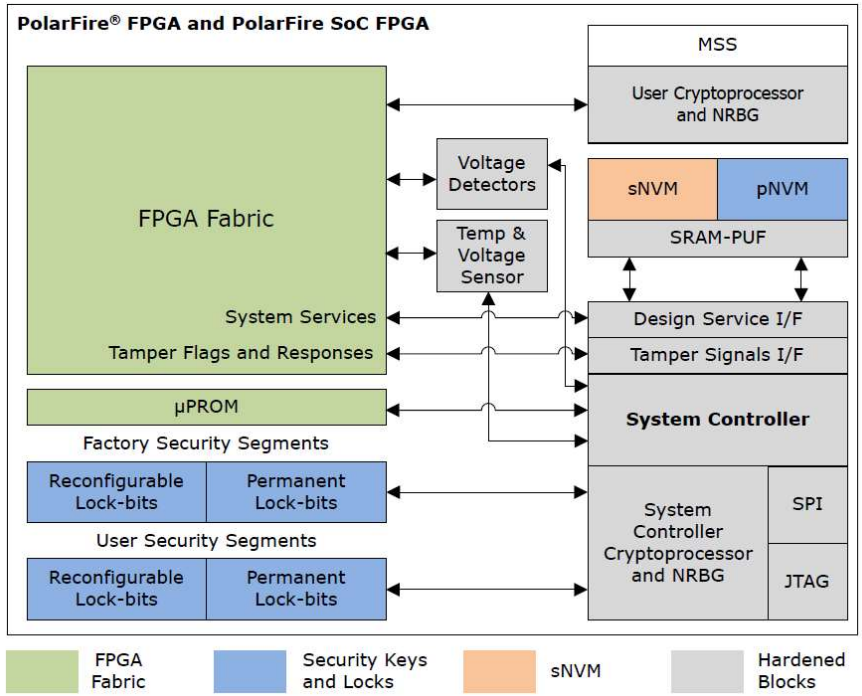
4 bytes (32 bits) — 252 bytes (2016 bits)

Authenticated Plaintext Mode

4 bytes (32 bits) — 16 bytes (128 bits) — 236 bytes (1888 bits)

Authenticated Ciphertext Mode

4 bytes (32 bits) — 16 bytes (128 bits) — 236 bytes (1888 bits)



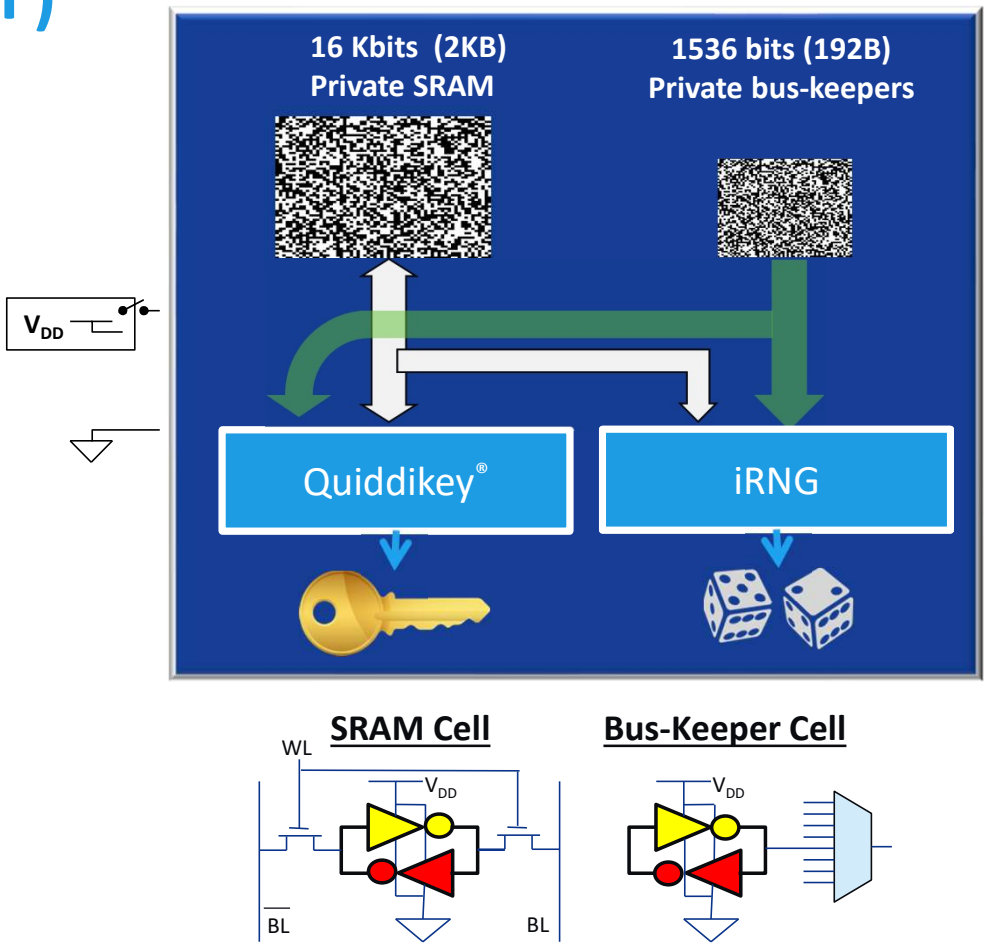
MICROCHIP

Polarfire® FPGA and SoC

Physically Unclonable Function (PUF)

INTRINSIC ID

- **Two PUFs in One:**
  - SRAM-PUF
  - Bus-Keeper PUF
- **Power-gated to**
  - Reduce aging affects
  - Reduce attack surface
- **Used to**
  - Wrap keys



MICROCHIP

Locks

Multiple Layers of Locks and Passcodes

- **Locks**
  - Programming Operations
  - Disable Interfaces
  - User Security
  - Bitstream Loading
  - FPGA and sNVM update
  - Debug
  - Factory Test Mode Access
  - JTAG/SPI Command
- **Permanent Locks**
  - Zeroisation CANNOT RESET them
  - Disable Features
    - Passcodes
    - Debug
    - Test Mode
    - Programming Interfaces
- **Passcodes**
  - Plaintext or One-Time
  - Salted and Hashed at rest
  - Unique per device

MICROCHIP

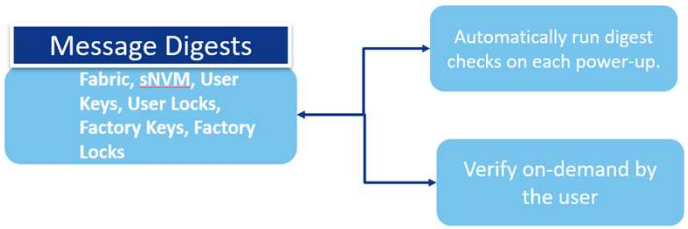
Anti-Tamper

Digital and Analog Anti-Tamper Mechanisms

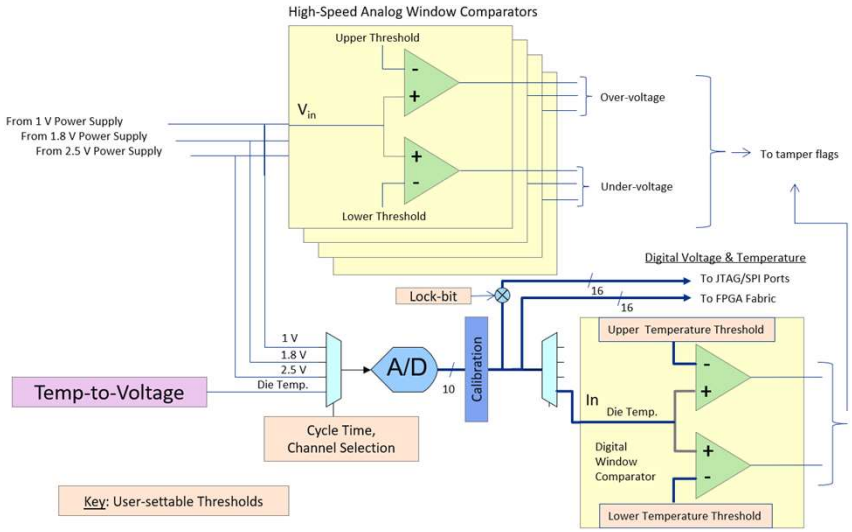
Digital Anti-Tamper Flags

Flag Name	Description
MESH_ERROR	Active Mesh Tamper Flag. This flag is asserted whenever the active security mesh observes a mismatch between the actual metal mesh output and the expected output. This allows protection against invasive attacks, such as cutting and probing of traces using focused ion beam (FIB) technology with an active metal mesh on one of the higher metal layers.
CLOCK_MONITOR_GLITCH	Asserted whenever the clock glitch monitor detects a pulse width violation
CLOCK_MONITOR_FREQUENCY	Asserted whenever the clock frequency monitor observes a frequency mismatch between the 160 MHz and 2 MHz RC oscillators.
SECDED	Asserted when a 2-bit error occurs in the System Controller's internal memory. This is a fatal condition which results in a POR.
SCB_BUS_ERROR	Asserted when an error has been detected on the System Controller bus.
WATCHDOG	Asserted when the System Controller's watchdog reset is about to fire.
LOCK_ERROR	Asserted when a single or double-bit error is detected in the continuously monitored security lock segments.
DIGEST	Asserted when a requested digest check is failed.
INST_BUFFER_ACCESS	The flag is asserted when read/write access is performed to the system controller's shared buffer using JTAG/SPI interface.
INST_DEBUG	Asserted when a debug instruction executed.
INST_CHECK_DIGESTS	Asserted when an external digest check has been requested.
INST_EC_SETUP	Asserted when an elliptic curve slave instructions have been used.
INST_FACTORY_PRIVATE	Asserted when factory JTAG/SPI instruction is executed.
INST_KEY_VALIDATION	Asserted when key validation protocol is requested.
INST_MISC	Asserted when uncategorized SPI slave instruction executed.
INST_PASSCODE_MATCH	Asserted when an attempt has made to match a passcode.
INST_PASSCODE_SETUP	Asserted when the one-time-passcode protocol is initiated.
INST_PROGRAMMING	Asserted when an external programming instruction has been used.
INST_PUBLIC_INFO	Asserted when a request for device public information is issued.
INST_PASSCODE_FAIL	Asserted when the passcode match fails.
INST_KEY_VALIDATION_FAIL	Asserted when the key validation fails.
INST_UNUSED	Asserted when the unused instruction opcode is executed.
BITSTREAM_AUTHENTICATION_FAIL	Asserted when the bitstream authentication fails.
IAP_AUTO_UPDATE	Asserted if an IAP update occurs (either by IAP system service or auto-update at device boot).
IAP_AUTO_RECOVERY	Asserted if the IAP recovery procedure occurs.

Digest Hashing



Temperature and Voltage Sensors



Anti-Tamper

Tamper Responses

Responses your design can perform

Fabric Signal	Action
IO_DISABLE	When asserted will disable selected device IO pins
LOCKDOWN	Forces all locks active and clears all the security unlocks that may have been set
RESET	Forces a DEVRST of the device, Fabric will be power cycled, and the device will restart
ZEROIZE	System Controller Starts the zeroization process

Mode	Zeroization
Like New	Zeroizes the device to “like new”
Unrecoverable	Zeroizes everything, device is unrecoverable

Zeroization triggered by tamper response macro or via JTAG or SPI command
Zeroization Mode is pre-programmed as part of the bitstream

MICROCHIP

Proven Data Security With “S” Devices

- **CRI pass through license – no need to negotiate with CRI**
  - Use your own DPA resistant FPGA IP, CRI license free
  - Licensed DPA-resistant FPGA IP from Microchip partners, CRI license free

PolarFire Enhancements

- **Integrated Athena™ TeraFire® EXP-5200B DPA-resistant Crypto Processor**
  - ASIC implementation: saves power, cost

The Licensed DPA Logo is a trademark of Rambus Cryptography Research, Inc., used under license.

- **How do you order an “S” Device?**
  - MPF100TS-1FCG484 (S device, EAR 5A992.c)
  - MPFS250TS-1FCG1152 (S device, EAR 5A992.c)

MICROCHIP

Data Security - Athena TeraFire EXP-F5200B

User Cryptoprocessor incorporates
NRBG + AES counter mode-based DRBG, compliant with NIST SP800-90A

TeraFire ® EXP-F5200B supported protocols/features
TRNG : SP800-90A CTR_DRBG-256[5]; SP800-90B (draft) NRBG
AES-128[5]/192[5]/256[5] E/D (ECB[5], CBC[5], CTR[5], OFB[5], CFB, GCM[5], KeyWrap)
SHA-1[5]/224[5]/256[5]/384[5]/512[5]
HMAC-SHA-1[5]/224[5]/256[5]/384[5]/512[5]; GMAC-AES[5]; CMAC-AES
SHA-256 Key Tree
ECC: NIST P256[5]/384[5]/521[5] and Brainpool P256/384/512 curves; KeyGen, KAS - ECC CDH, ECDSA SigGen[5] & SigVer[5], PKG[5], PKV[5]
IFC: 1024/1536/2048[5]/3072[5]/4096[6] RSA E/D; SSA_PKCS1_V1_5 SigGen[5] & SigVer[5]; ANSI X9.31 SigGen[5] & SigVer[5]
FFC: 1024/1536/2048[5]/3072[5]/4096[6]; KAS - DH, DSA SigGen[4] & SigVer[5]

[5] TeraFire EXP-F5200B NIST CAVP certifications available:

- AES: 3950, 3951
- DSA: 1077
- RSA: 2018
- ECDSA: 867, 868
- SHS: 3258, 3259
- DRBG: 1153, 1154
- HMAC: 2573

On lines where a second cert is shown, it is for the TeraFire EXP-F200ASR used by the system controller for FPGA design security, which also certified ECC CDH: 790

[6] 4096 bit keys are only supported with DPA countermeasures "off"

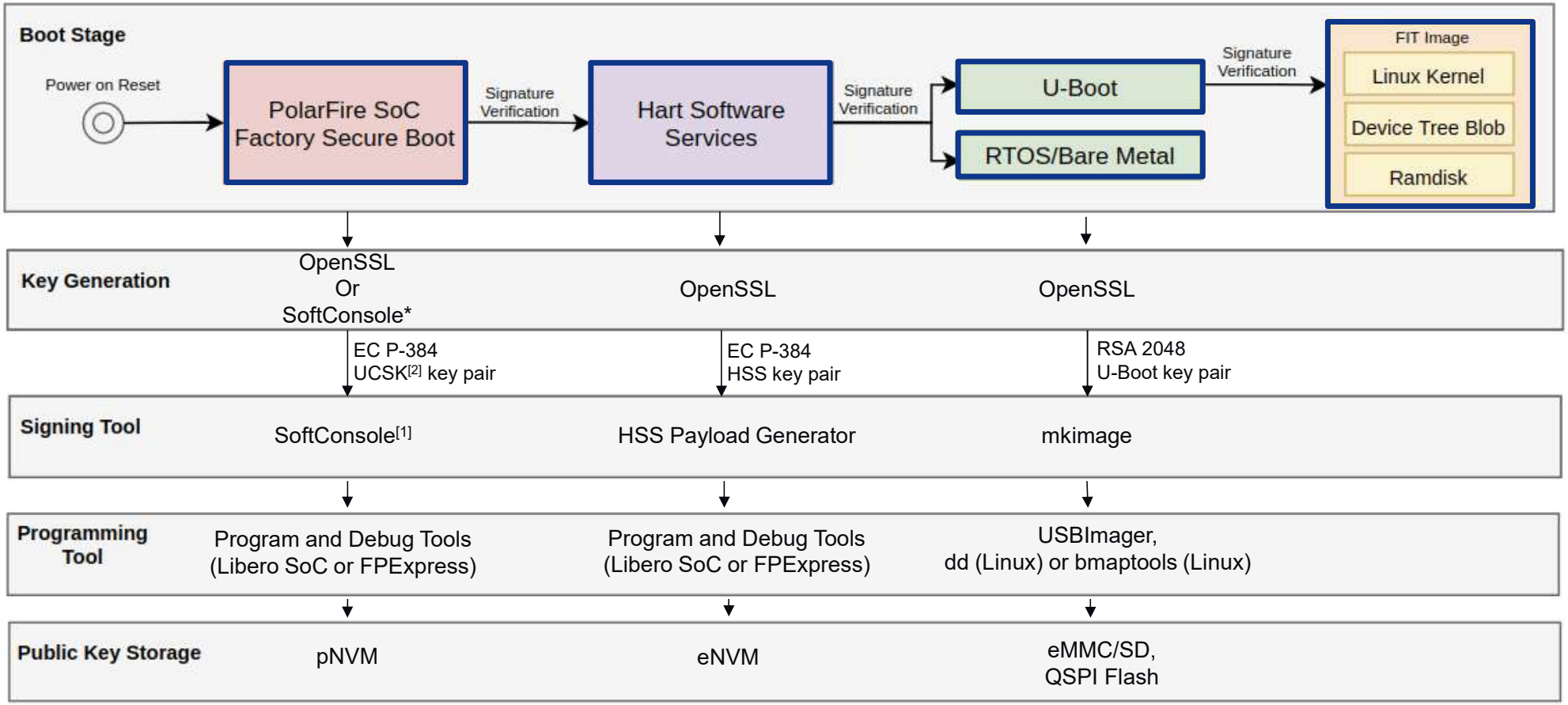
ATHENA
THE ATHENA GROUP

DPA resistant
No FPGA fabric resources
Save Power, Cost

MICROCHIP

A secure boot implementation for PolarFire SoC

PolarFire SoC AMP Chain of Trust Example

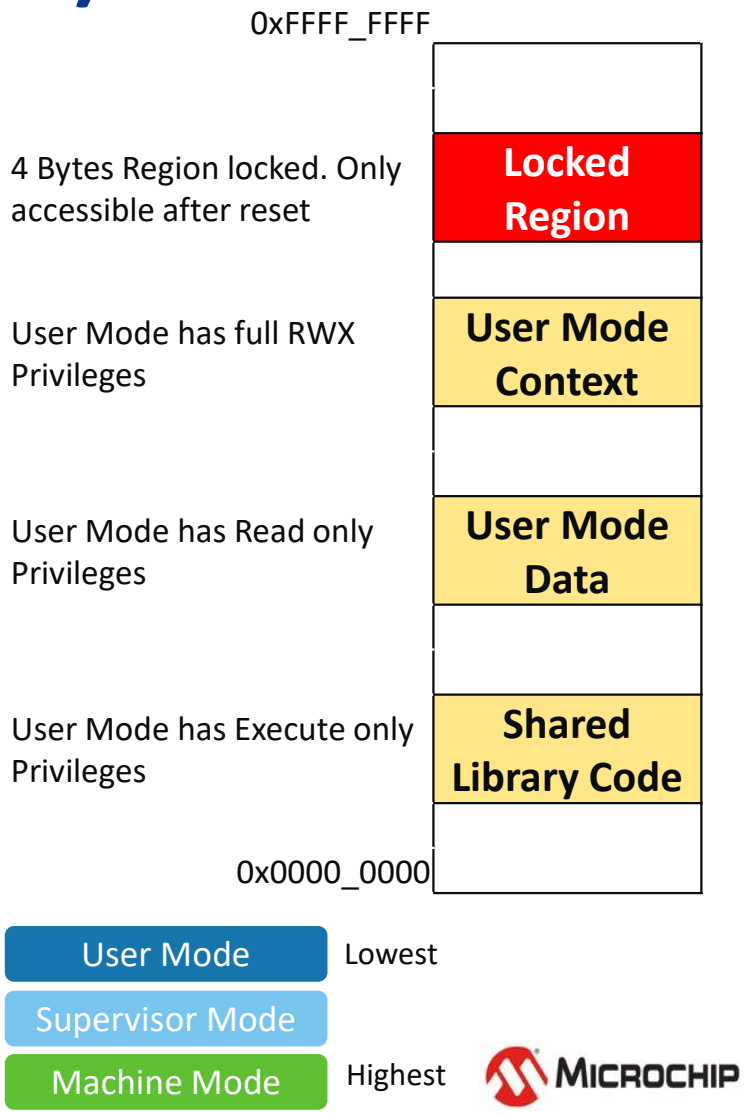


[1] Boot Mode Programmer tool built-in SoftConsole
[2] User Code Signing Key

MICROCHIP

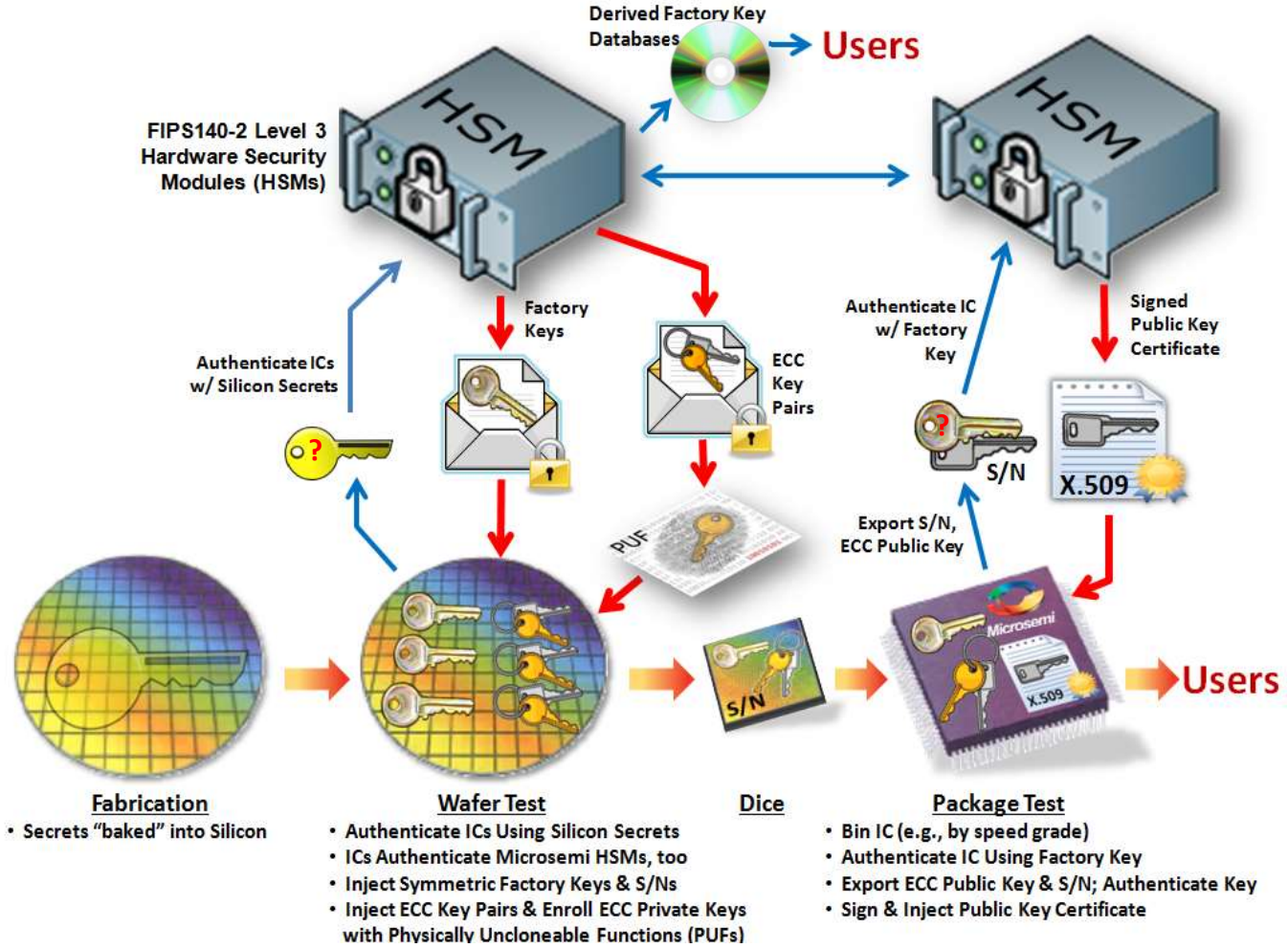
Physical Memory Protection (PMP)

- **Enforce access restrictions on less privileged modes**
  - Prevent User Mode software from accessing restricted memory
- **Lock a region**
  - A locked region enforces permissions on all accesses, including M-Mode
  - Only way to unlock a region is a Reset
- **Up to 16 regions with a minimum region size of 4 bytes – regions can overlap**



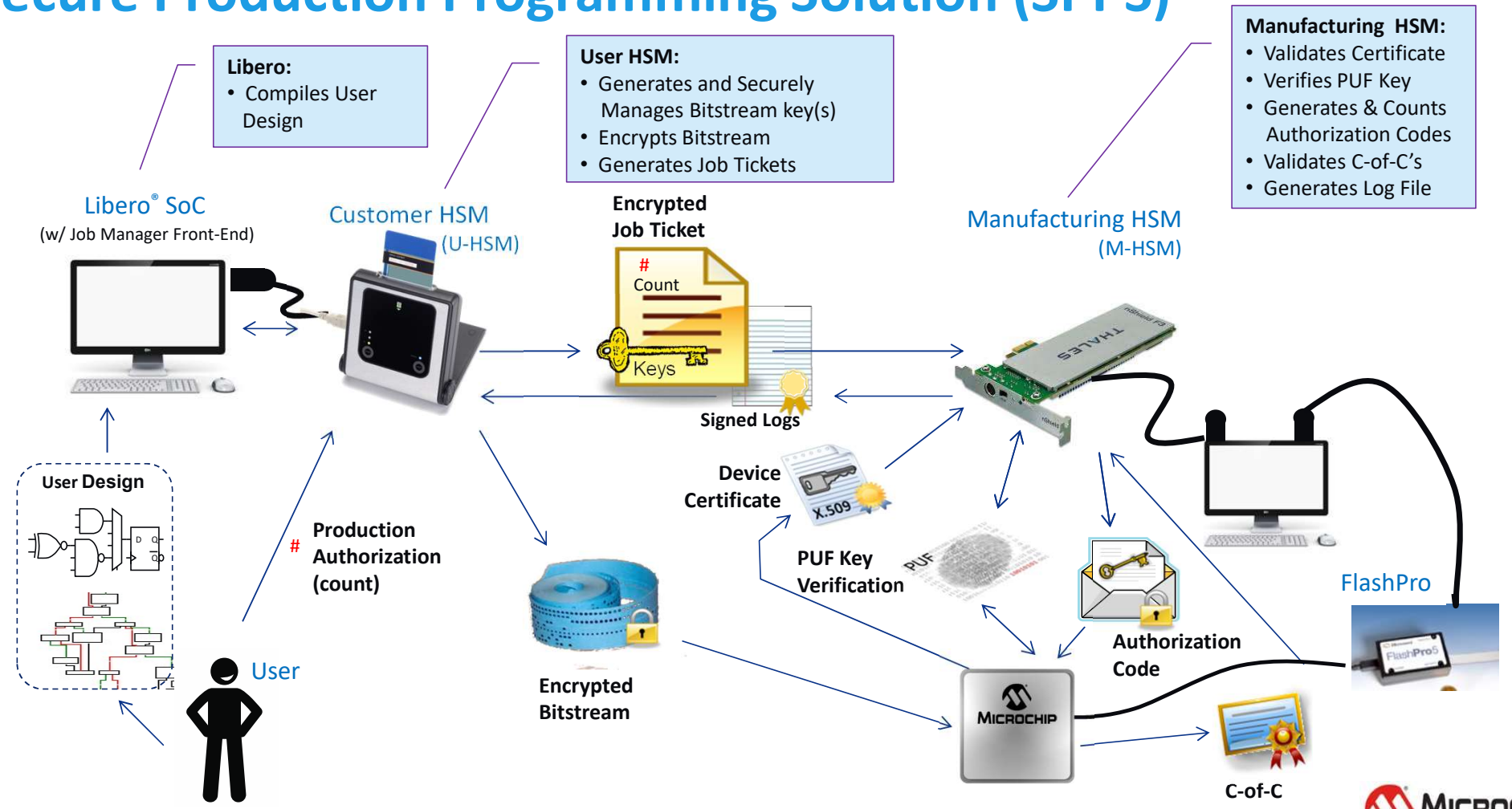
Microchip FPGA

HSM Based Manufacturing Flow



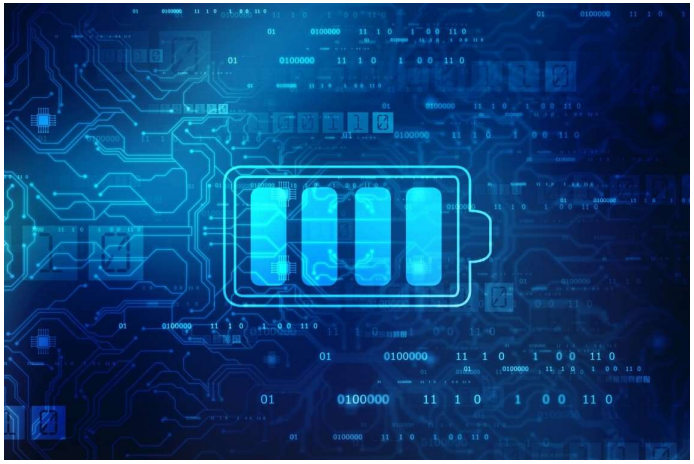
Secure User Device Configuration Data Flow

The Secure Production Programming Solution (SPPS)

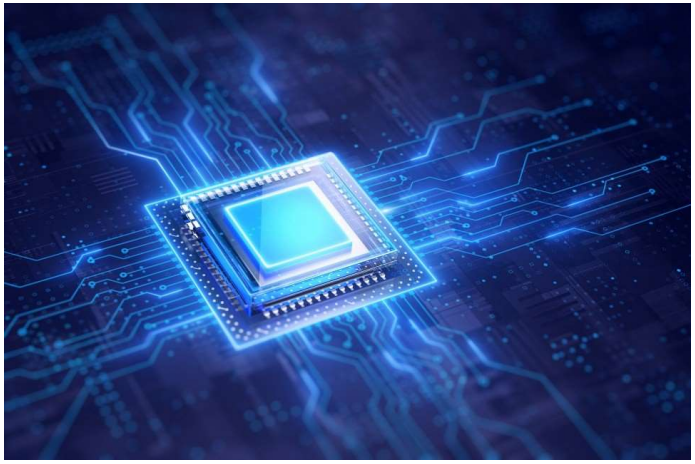


Summary

- **Microchip offers Power-Efficient Mid-Range FPGAs and SoCs With the Highest Reliability and Best-in-Class Security**
- **The PolarFire® family of FPGAs and SoC FPGAs is built upon the three fundamental security principles of confidentiality, integrity and authenticity.**



Most Power-Efficient FPGAs
Two Times More Performance Per Watt



Exceptional Reliability
Zero Configuration Upsets

Military-Grade Security
Best Cyber and Anti-Tamper Security

MICROCHIP

Thank You!
Questions and Answers

Leveraging Hi-Reliability Product Design Flows

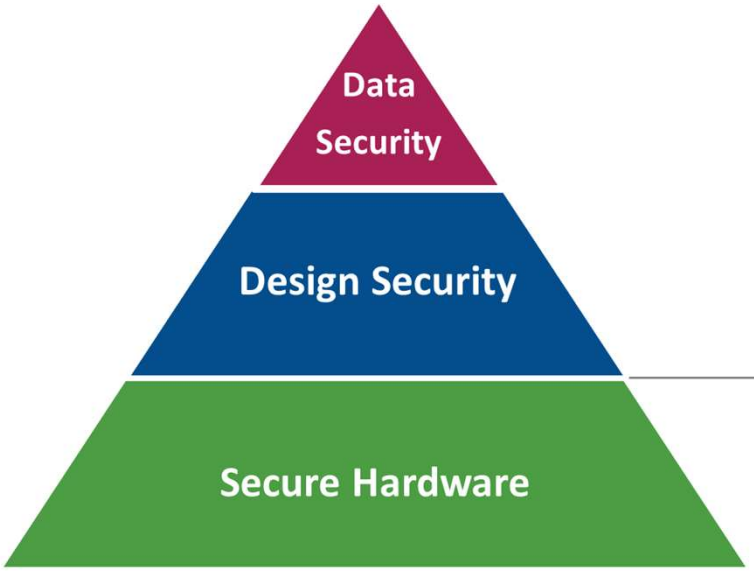
To continue the discussion or find out more please use the resources below:

euro.enquiry@microchip.com

https://page.microchip.com/show.html

MICROCHIP

Appendix



Design Security

Protect your IP

MICROCHIP

Bitstream Security

Bitstream Security

IP Protection

- **Bitstreams can contain any combination of**
  - FPGA, sNVM, eNVM, & Security Segment payloads.
- **Authentication**
  - Licensed protocol from Rambus (CRI) and SHA256 that resists DPA and other side channel attacks
- **Encryption/Decryption**
  - Authentication must pass first before a bitstream segment is decrypted
  - AES-CTR, 256-bit key. Keys are rolled and hashed using a key tree algorithm to provide side channel resistance.
- **Back Level Protection - available**

Bitstream Programing

IP Protection

- **Initial Key Loading on a blank device**
  - A default key can be used (KLK) to load a bitstream
  - SPPS uses an ECDH scheme to generate an initial ephemeral shared key for initial bitstream loading
- **User's keys (UEK1 and UEK2) can be provisioned on the device prior to loading a user encrypted bitstream**
- **Generally, a two-step process when using anything other than KLK**
  - Provision security
  - Program Bitstream

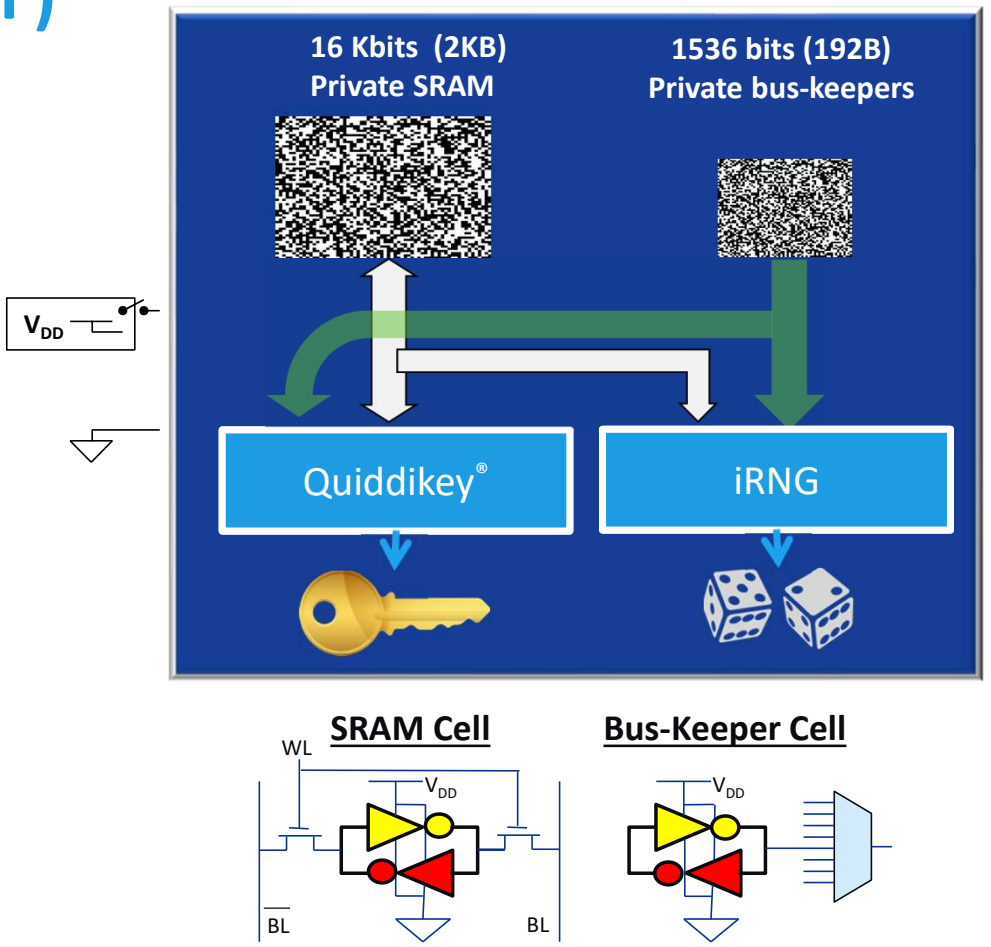
Keys

Polarfire® FPGA and SoC

Physically Unclonable Function (PUF)

INTRINSIC ID

- **Two PUFs in One:**
  - SRAM-PUF
  - Bus-Keeper PUF
- **Power-gated to**
  - Reduce aging affects
  - Reduce attack surface
- **Used to**
  - Wrap keys



MICROCHIP

Keys

- Factory Key (FK) – symmetric factory key
- Factory ECC Key (KFP) – asymmetric factory key
- Factory Pass Code Key (FPK) – pass code to enter test mode, can be disabled
- Microchip Certificate Public Key (MCPK) – validates x.509 before export
- Key Loading Key (KLK) – default if UEK1 or 2 is not used.
- User Encryption Key 1 (UEK1) – user bitstream encryption key
- User Encryption Key 2 (UEK2)
- User Passcode Key 1 (UPK1) – user pass code for all locks
- User Passcode Key 2 (UPK2)
- Debug Pass Key (DPK) – ephemeral debug pass code
- PUF Emulation Key (PEK) – emulate a strong PUF via key tree algorithm
- User ECC Private Key Mode (KUP) - HSM
- User ECC Private Key Ephemeral Mode (KUPE) – HSM
- sNVM Master Key (SMK) - unique per device encryption/authentication key

Secure Non-Volatile Memory - sNVM

- **56K Bytes**
- **Three Modes**

Plaintext Mode

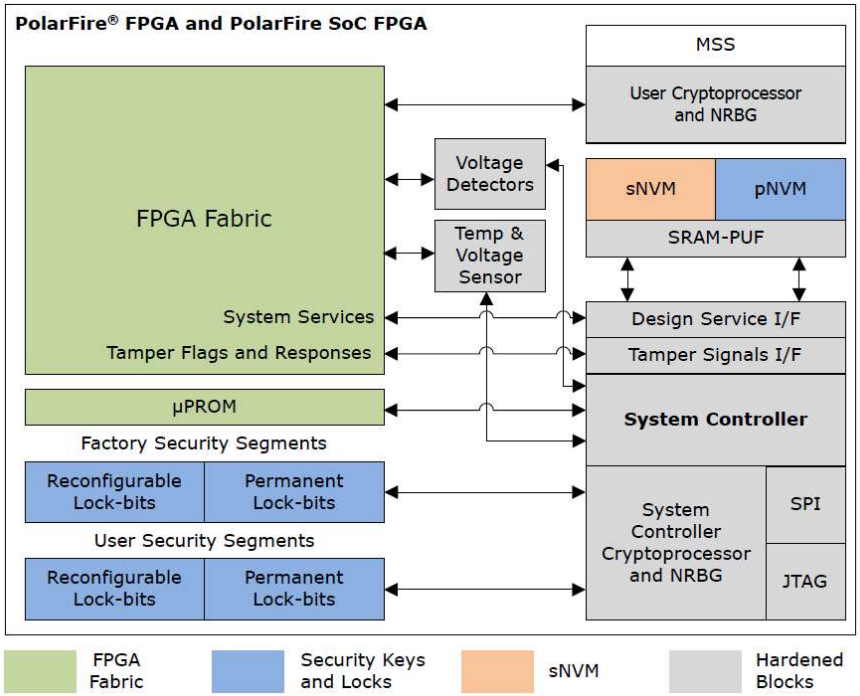
Metadata	Plaintext User Data
4 bytes (32 bits)	252 bytes (2016 bits)

Authenticated Plaintext Mode

Metadata	Tag	Plaintext User Data
4 bytes (32 bits)	16 bytes (128 bits)	236 bytes (1888 bits)

Authenticated Ciphertext Mode

Metadata	Tag/IV	Ciphertext User Data
4 bytes (32 bits)	16 bytes (128 bits)	236 bytes (1888 bits)



Secure Non-Volatile Memory - sNVM

- **sNVM Master Key (SMK)**
  - 512 bit symmetric key for securing sNVM content
    - 256 bits for authentication, 256 for encryption
  - Randomly generated on each device
  - Stored in pNVM (Private NVM), wrapped by the PUF ID.
  - Used to provide unique per device encryption of sNVM content
- **AES cipher mode “tweaks” each page’s encryption/MAC with:**
  - Page address; Page write-counter; 96-bit per-page user key (USK)

- **USK – used to authenticate the page**

Secure Non-Volatile Memory - sNVM

- **Each page can be “ROM’d”**
  - Set the page write protect bit in libero
  - Page payloads will be encapsulated in the bitstream
- **Write Protected pages are included in the respective digest check**
- **Read/Write via standard API**

Offset	Length (bytes)	Parameter	Description
0	1	SNVMADDR	SNVM Starting address
1	3	RESERVED	For alignment
4	236	Payload	Data to write to SNVM
240	12	USK	User Secret Key

Authenticated Plaintext Write System Service

MICROCHIP

Locks

Layers of locks to provide defense in depth

Locks

- **User Security Locks**
  - When UEK1 or UEK2 are used a lock bit is automatically set to prevent erasing and over-writing these keys
  - You can disable UEK1/UEK2 using the User Passcode Key 1 or 2 (UPK1, UPK2)
- **Key bitstream loading mode locks**
  - Key modes associated with keys that are not loaded are automatically locked.
- **FPGA and sNVM update locks**
  - Can be temporarily unlocked using the Users Passcode Key (UPK1, UPK2)

Locks

- **Programming Functions**
  - Disable Auto Programming, In Application Programming
  - Disable JTAG/SPI slave programming.
    - Auto Programming and IAP system services are not affected
  - Disable JTAG/SPI Slave Bitstream Authentication
    - Auto Programming and IAP system services are not affected
  - Disable JTAG/SPI Bitstream standalone Verify
    - Auto Programming and IAP system services are not affected
- **Disable Interfaces**
  - Disable JTAG
    - Breaks the JTAG chain, pins are active, TAP controller doesn’t respond.
  - Disable SPI Slave

Locks

- **Debug Locks**
  - Disable JTAG/SPI access to
    - SmartDebug and SmartDebug Active Probes
    - SmartDebug Live Probes
    - sNVM
    - Temperature and Voltage sensors
  - Disable JTAG 1149.1 boundary scan
    - BYPASS, IDCODE, and USERCODE instructions will remain functional
- **Factory Test Mode Access Lock**
  - Can be enabled for FA, can be permanently disabled (OTP mode)
  - Default is enabled

Locks

- **JTAG/SPI Slave Commands**
  - Disable access to PUF Emulation service
  - Disable Digest requests
  - Disable Zeroization requests

Permanent Locks

- **They are Permanent**
  - Zeroization cannot reset them.
- **Disable:**
  - User Passcode Key 1 and 2
  - SmartDebug and reading of TVS via JTAG/SPI
  - Debug Passcode key
  - Factory Test Mode
  - Auto-programing, JTAG and SPI programming interfaces (OTP)
- **Write Protect the Fabric (OTP)**

Passcodes

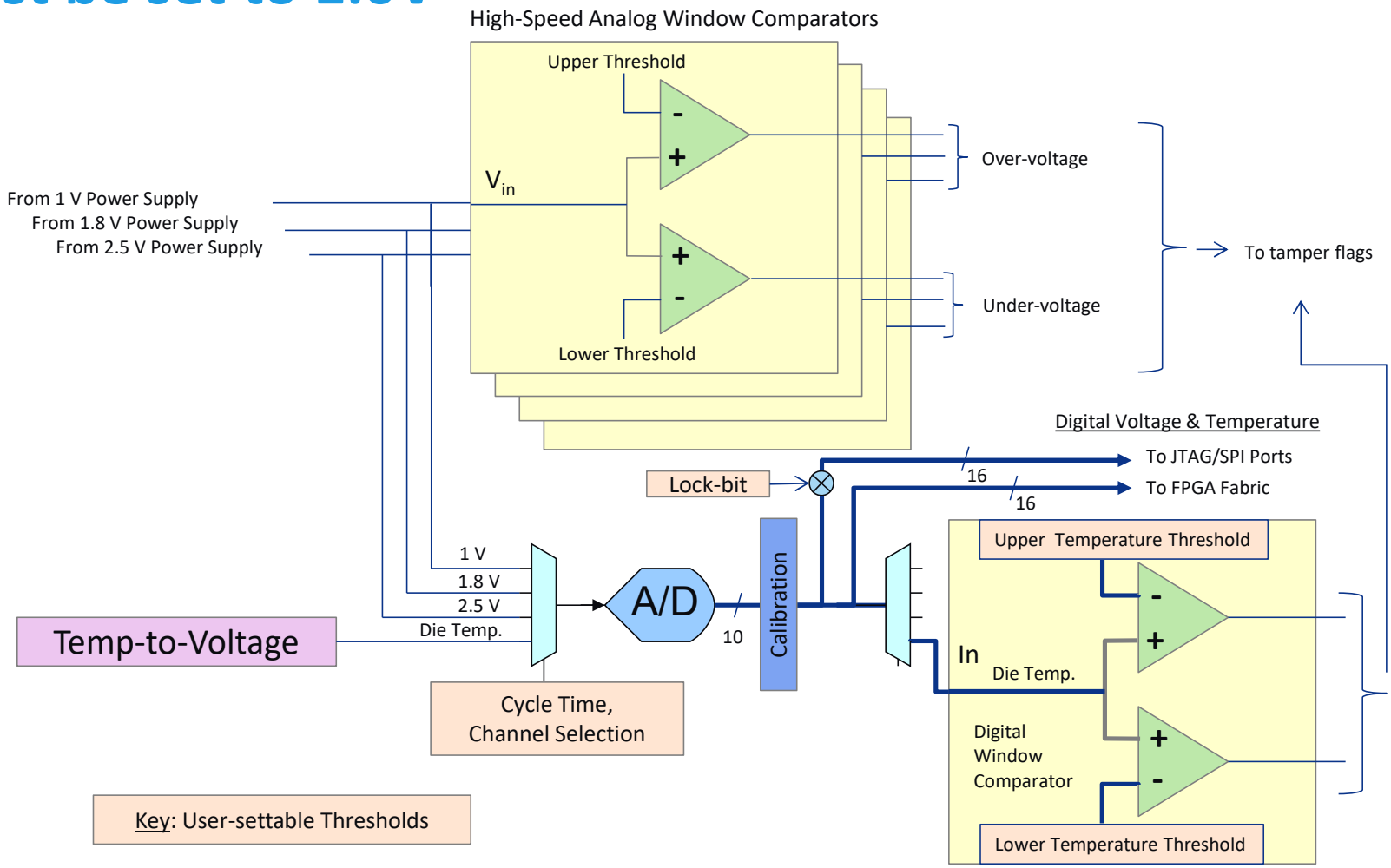
- **Passcodes are 256 bits long, salted and hashed when stored, and are unique per device**
- **Passcodes:**
  - FlashLock™ or User Passcode Key 1 (UPK1)
  - User Passcode Key 2 (UPK2)
  - Factory Passcode Key (FPK)
  - Debug Passcode Key (DPK)
- **Passcodes can be**
  - plaintext
  - One time use passcode protocol (PolarFire, RTPolarFire)
    - Requires an HSM ie SPPS
  - One way passcode protocol (PolarFire SoC) – no HSM required
  - See the PolarFire and PolarFire SoC Security Users Guide for more information

Anti-Tamper

Equipment will be left behind or observed

Temperature and Voltage Sensors

Vdd must be set to 1.0V

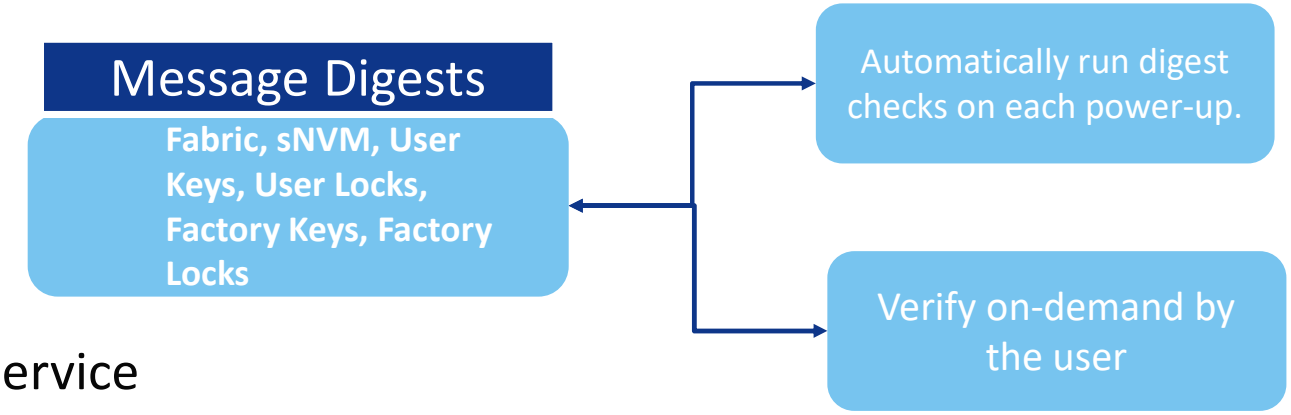


Digital Anti-Tamper Flags

Flag Name	Description
MESH_ERROR	Active Mesh Tamper Flag. This flag is asserted whenever the active security mesh observes a mismatch between the actual metal mesh output and the expected output. This allows protection against invasive attacks, such as cutting and probing of traces using focused ion beam (FIB) technology with an active metal mesh on one of the higher metal layers.
CLOCK_MONITOR_GLITCH	Asserted whenever the clock glitch monitor detects a pulse width violation
CLOCK_MONITOR_FREQUENCY	Asserted whenever the clock frequency monitor observes a frequency mismatch between the 160 MHz and 2 MHz RC oscillators.
SECDED	Asserted when a 2-bit error occurs in the System Controller's internal memory. This is a fatal condition which results in a POR.
SCB_BUS_ERROR	Asserted when an error has been detected on the System Controller bus.
WATCHDOG	Asserted when the System Controller's watchdog reset is about to fire.
LOCK_ERROR	Asserted when a single or double-bit error is detected in the continuously monitored security lock segments.
DIGEST	Asserted when a requested digest check is failed.
INST_BUFFER_ACCESS	The flag is asserted when read/write access is performed to the system controller’s shared buffer using JTAG/SPI interface.
INST_DEBUG	Asserted when a debug instruction executed.
INST_CHECK_DIGESTS	Asserted when an external digest check has been requested.
INST_EC_SETUP	Asserted when an elliptic curve slave instructions have been used.
INST_FACTORY_PRIVATE	Asserted when factory JTAG/SPI instruction is executed.
INST_KEY_VALIDATION	Asserted when key validation protocol is requested.
INST_MISC	Asserted when uncategorized SPI slave instruction executed.
INST_PASSCODE_MATCH	Asserted when an attempt has made to match a passcode.
INST_PASSCODE_SETUP	Asserted when the one-time-passcode protocol is initiated.
INST_PROGRAMMING	Asserted when an external programming instruction has been used.
INST_PUBLIC_INFO	Asserted when a request for device public information is issued.
INST_PASSCODE_FAIL	Asserted when the passcode match fails.
INST_KEY_VALIDATION_FAIL	Asserted when the key validation fails.
INST_UNUSED	Asserted when the unused instruction opcode is executed.
BITSTREAM_AUTHENTICATION_FAIL	Asserted when the bitstream authentication fails.
IAP_AUTO_UPDATE	Asserted if an IAP update occurs (either by IAP system service or auto-update at device boot).
IAP_AUTO_RECOVERY	Asserted if the IAP recovery procedure occurs.

Digests

- **Hash of various Non-Volatile components**
  - FPGA, sNVM, eNVM (SoC), Security Segments, etc.
- **Can be initiated**
  - On every power-up
  - On demand
    - Internally through a system service
    - Externally through JTAG/SPI



Data Integrity

Digest commands and Services

	JTAG/SPI Command	System Service
Bitstream, IAP, and device Init Authentication Services (SPI Flash)		**Yes**
Export C-of-C tags (during bitstream programming)	**Yes**	
Export Digests Stored During Programming (on demand)	**Yes**	**Yes**
Compute/Export Fresh Digests (on demand)	**Yes**	**Yes**
Compute/Report Fresh Status Flags (on-demand)	**Yes**	**Yes**
Compute/Report Fresh Tamper Flag (after Power-on-Reset)		**Yes**
Export Zeroization Proof (after zeroization)	**Yes**	
Device Integrity Flag (for new devices)	**Yes**	
sNVM Authentication (when page is read)		**Yes**

MICROCHIP

Tamper Responses

Only your design can generate a response.

Fabric Signal	Action
IO_DISABLE	When asserted will disable selected device IO pins
LOCKDOWN	Forces all locks active and clears all the security unlocks that may have been set
RESET	Forces a DEVRST of the device, Fabric will be power cycled, and the device will restart
ZEROIZE	System Controller Starts the zeroization process

Mode	Zeroization
Like New	Zeroizes the device to “like new”
Unrecoverable	Zeroizes everything, device is unrecoverable

Zeroization triggered by tamper response macro or via JTAG or SPI command
Zeroization Mode is pre-programmed as part of the bitstream

MICROCHIP

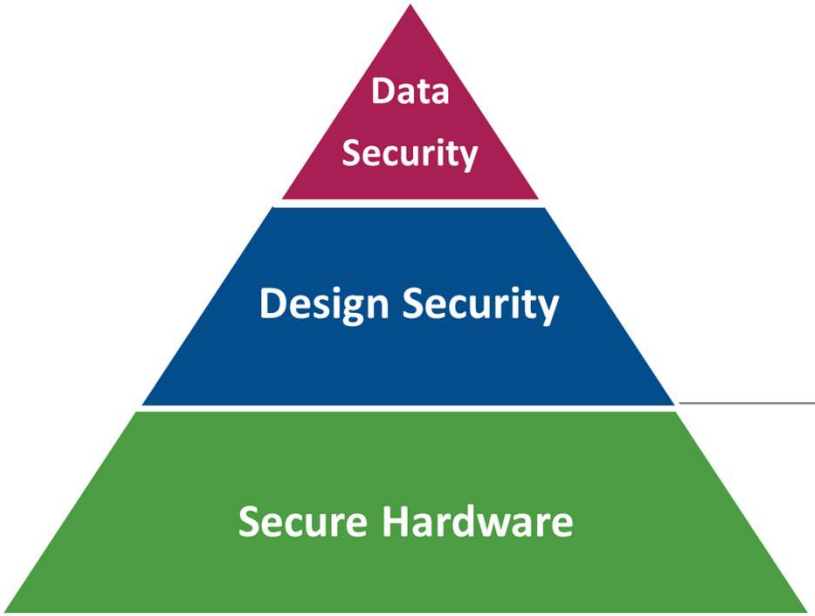
Design Security - Athena TeraFire® F5200ASR

System Controller Cryptoprocessor

	Athena TeraFire® F5200ASR EXP-F200ASR
AES	3951
DSA	-
RSA	-
ECDSA	868
SHS	3259
DRBG	1154
HMAC	-
ECC CDH	790

- **System Controller contains Side channel resistant NIST certified cryptoprocessor**

MICROCHIP



Data Security

Information Assurance

MICROCHIP

Proven Data Security With “S” Devices

- **CRI pass through license – no need to negotiate with CRI**
  - Use your own DPA resistant FPGA IP, CRI license free
  - Licensed DPA-resistant FPGA IP from Microchip partners, CRI license free

PolarFire Enhancements

- **Integrated Athena™ TeraFire® EXP-5200B DPA-resistant Crypto Processor**
  - ASIC implementation: saves power, cost

The Licensed DPA Logo is a trademark of Rambus Cryptography Research, Inc., used under license.

- **How do you order an “S” Device?**
  - MPF100TS-1FCG484 (S device, EAR 5A992.c)
  - MPFS250TS-1FCG1152 (S device, EAR 5A992.c)

MICROCHIP

Data Security - Athena TeraFire EXP-F5200B

User Cryptoprocessor incorporates
NRBG + AES counter mode-based DRBG, compliant with NIST SP800-90A

TeraFire ® EXP-F5200B supported protocols/features
TRNG : SP800-90A CTR_DRBG-256[5]; SP800-90B (draft) NRBG
AES-128[5]/192[5]/256[5] E/D (ECB[5], CBC[5], CTR[5], OFB[5], CFB, GCM[5], KeyWrap)
SHA-1[5]/224[5]/256[5]/384[5]/512[5]
HMAC-SHA-1[5]/224[5]/256[5]/384[5]/512[5]; GMAC-AES[5]; CMAC-AES
SHA-256 Key Tree
ECC: NIST P256[5]/384[5]/521[5] and Brainpool P256/384/512 curves; KeyGen, KAS - ECC CDH, ECDSA SigGen[5] & SigVer[5], PKG[5], PKV[5]
IFC: 1024/1536/2048[5]/3072[5]/4096[6] RSA E/D; SSA_PKCS1_V1_5 SigGen[5] & SigVer[5]; ANSI X9.31 SigGen[5] & SigVer[5]
FFC: 1024/1536/2048[5]/3072[5]/4096[6]; KAS - DH, DSA SigGen[4] & SigVer[5]

[5] TeraFire EXP-F5200B NIST CAVP certifications available:

- AES: 3950, 3951
- DSA: 1077
- RSA: 2018
- ECDSA: 867, 868
- SHS: 3258, 3259
- DRBG: 1153, 1154
- HMAC: 2573

On lines where a second cert is shown, it is for the TeraFire EXP-F200ASR used by the system controller for FPGA design security, which also certified ECC CDH: 790

[6] 4096 bit keys are only supported with DPA countermeasures "off"

ATHENA
THE ATHENA GROUP

DPA resistant
No FPGA fabric resources
Save Power, Cost

MICROCHIP

Crypto-Coprocessor

Throughput

TeraFire ® EXP-F5200B algorithms and expected throughput[1]	
DRBG	37 Mbps[2]
AES-256	180 Mbps[2]
SHA-256	142 Mbps[2]
ECDSA-384	67/34 ms[3,4]
DSA-3072	148/130 ms[3,4]
SSA-3072	400/5 ms[3,4]

[1] With DPA countermeasures “on,” Mi-V RV32IMA running at 95 MHz and TeraFire processor running at 190 MHz using DMA where possible
[2] Average over a long message
[3] Single SigGen / SigVer execution, respectively
[4] All ECDSA P256, DSA 2048 & SSA 2048 operations are all roughly 2.3x faster than shown for P384 & 3072 bit keys

PolarFire SoC FPGA User Cryptoprocessor Modes

- **PolarFire FPGA – Standalone block**
- **PolarFire SoC FPGA – Integrated within the MSS**

Mode	Description
Reset	The Cryptoprocessor is not available to the MSS or Fabric and is held in reset
MSS	The Cryptoprocessor is only available to the MSS
Fabric	The Cryptoprocessor is only available to the Fabric
Shared-MSS	The Cryptoprocessor is initially connected to the MSS, and may be requested by the Fabric
Shared-Fabric	The Cryptoprocessor is initially connected to the Fabric, and may be requested by the MSS

Refer to the PolarFire Datasheet for information on TeraFire ® EXP-F5200B algorithms and expected throughput

MICROCHIP

PolarFire Security Addons

PolarFire SoC Security Addons

Defense Grade Security, Ready for IoT

- **Spectre and Meltdown Immunity**
- **Secure Boot**
  - Options to securely boot application processors
- **Physical Memory Protection (PMP)**

MICROCHIP

PolarFire SoC Secure Boot

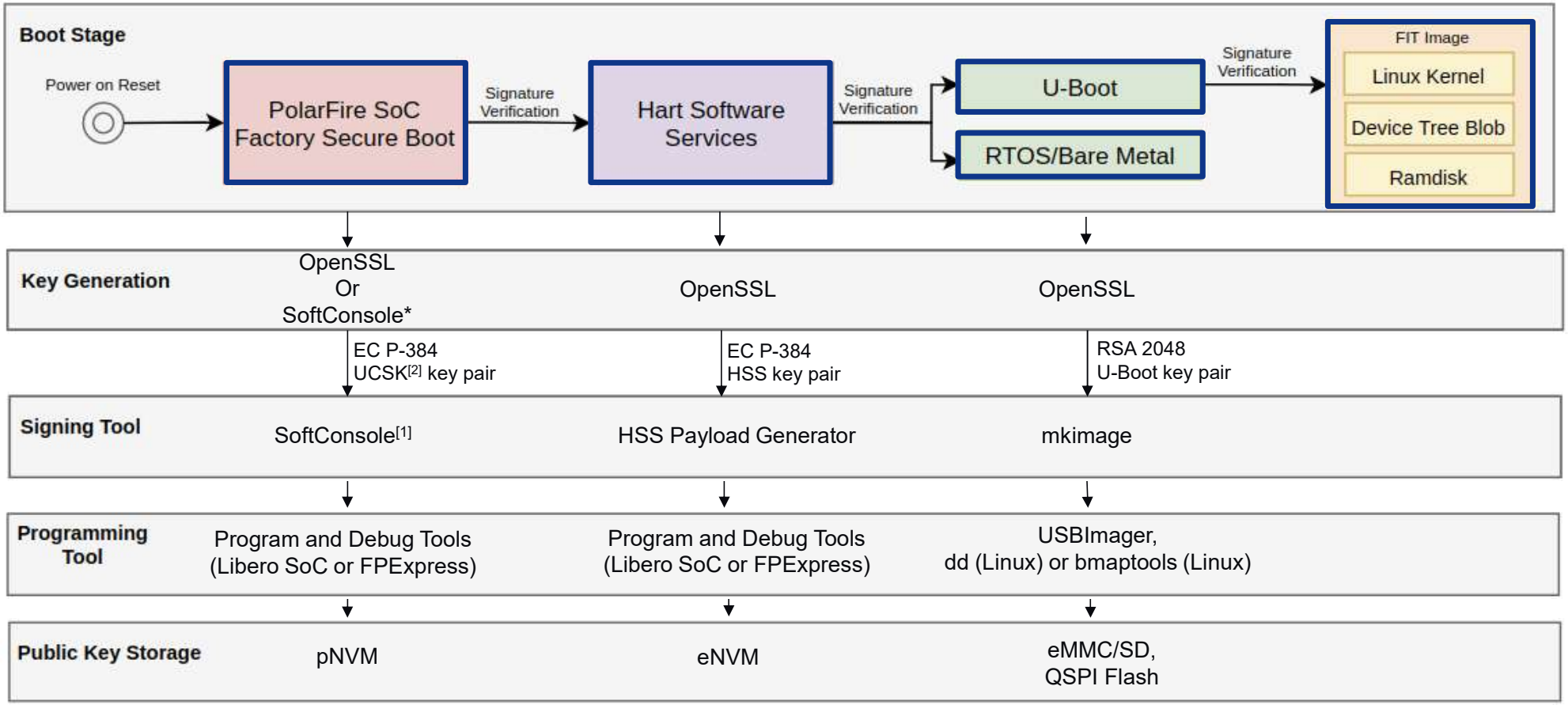
- **MSS boot code may reside in either of two on-chip NVM**
  - eNVM - Programmable via bitstream, and Directly writeable by the MSS using factory-supplied firmware drivers
  - sNVM- Authenticated modes use PUF-protected key generated by device, Managed by System Controller, accessed by bitstream or system service

MSS Boot Mode	Description
MSS Boot Mode 0	**Idle Mode** Default mode for a new device, All 5 cores are in idle state
MSS Boot Mode 1	**Direct boot** All 5 cores execute code from the eNVM without any authentication
MSS Boot Mode 2	**User Secure Boot**
MSS Boot Mode 3	**Factory Secure Boot**

MICROCHIP

A secure boot implementation for PolarFire SoC

PolarFire SoC AMP Chain of Trust Example

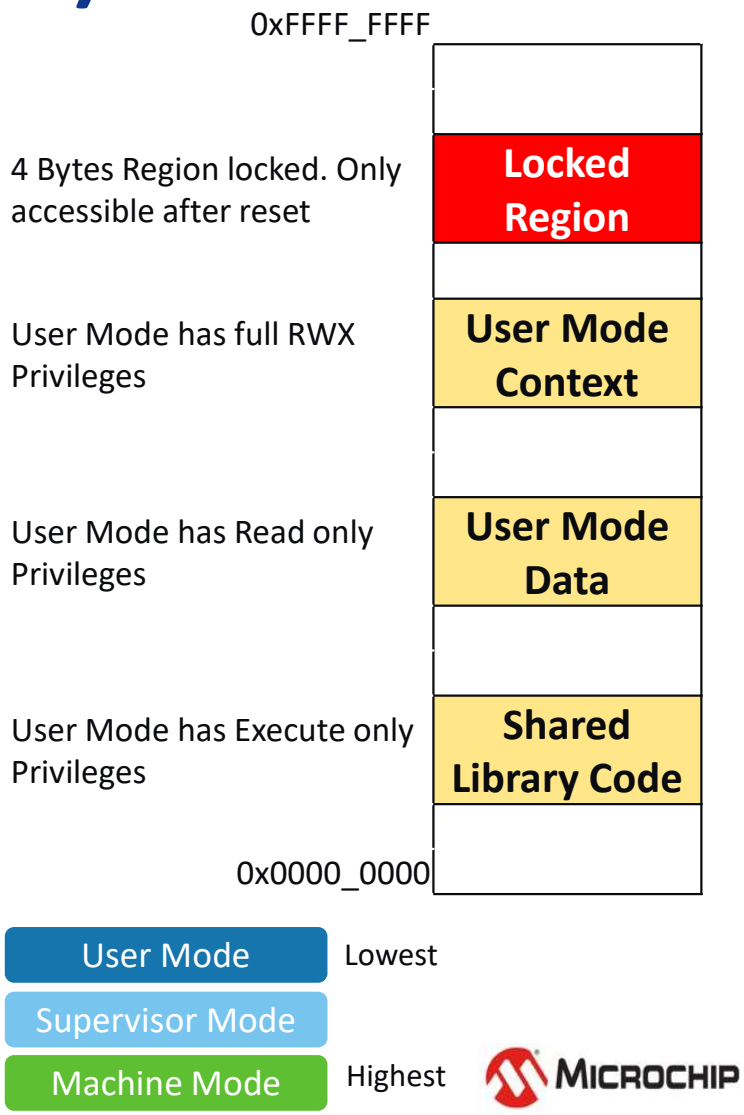


[1] Boot Mode Programmer tool built-in SoftConsole
[2] User Code Signing Key

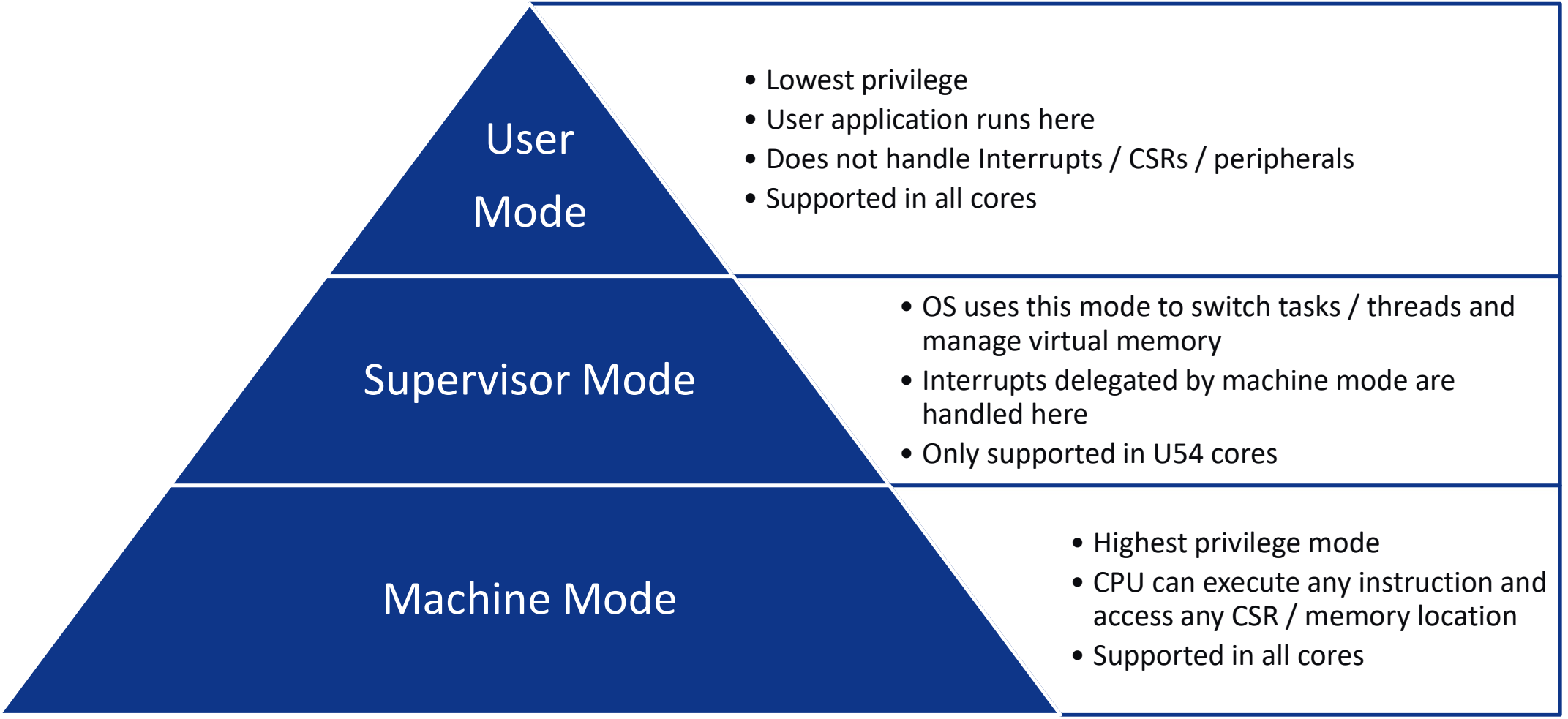
MICROCHIP

Physical Memory Protection (PMP)

- **Enforce access restrictions on less privileged modes**
  - Prevent User Mode software from accessing restricted memory
- **Lock a region**
  - A locked region enforces permissions on all accesses, including M-Mode
  - Only way to unlock a region is a Reset
- **Up to 16 regions with a minimum region size of 4 bytes – regions can overlap**



Privilege Modes



PolarFire Export Control Data

- **Data Security devices are denoted by an “S” in the root part number.**
  - **Ex: MPF300T-FCVG484I contains design security features whereas MPF300TS-FCVG484I contains both design security and data security features.**

Part Number	Classification Number (ECCN)
All extended commercial, industrial and automotive temperature-grade PolarFire FPGA family members	5A992.c
All extended commercial, industrial and automotive temperature-grade PolarFire SoC FPGA family members	5A992.c

Documentation and Resources

FPGA Security Website	Secure FPGAs and SoC FPGAs
PolarFire SoC and PolarFire	
User Guides	PolarFire FPGA and PolarFire SoC FPGA Security User Guide
Application Notes	AC464: PolarFire FPGA: Implementing Data Security using UserCrypto Processor Application Note
Videos and Webinars	PolarFire SoC FPGA Secure Boot Implementing Multizone Security in RISC-V Applications RISC-V Enclaves
SmartFusion2 SoC and IGLOO2	
User Guides	UG0443: SmartFusion2 and IGLOO2 FPGA Security Best Practices User Guide TU0823: Secure Production Programming Solution Using HSM
Application Notes	AC435: Using ECC System Service in SmartFusion2 - Libero SoC v11.7 Application Note AC407: Using NRBG Services in SmartFusion2 and IGLOO2 Devices - Libero SoC v11.8 Application Note AC410: Using AES System Services in SmartFusion2 and IGLOO2 Devices - Libero SoC v11.8 Application Note AC406: Configuring IGLOO2 and SmartFusion2 Devices for Safety-Critical Applications Application Note AC432: Using SHA-256 System Services in SmartFusion2 and IGLOO2 Devices - Libero SoC v11.8 Application Note AC433: Using Zeroization in SmartFusion2 and IGLOO2 Devices - Libero SoC v11.6 Application Note AC436: Using Device Certificate System Service in SmartFusion2 - Libero SoC v11.7 Application Note AC434: Using SRAM PUF System Service in SmartFusion2 - Application Note
Generation3 and Prior	
All Resources	https://www.microsemi.com/product-directory/fpga-soc/1738-security#resources
Secure Production Programming Solution	
All Resources	Secure Production Programming Solution

MICROCHIP