



The Low Power Programmable Leader

The Challenges of the Cyber Resilience Act and How FPGAs Can Help You

Cresitt Orleans : October 14th, 2025

Security Storm Ahead Demands Cyber Resilience

FINANCIAL TIMES

A hacker's paradise? 5G and cyber security

Internet-connected devices using fifth-generation mobile networks offer prime targets for criminals



Experts say the faster speeds of 5G will enable hackers to target more devices and launch bigger cyber attacks © Alamy

Cyber Resilience Act



Exec Order 14028

5G

Ubiquity of High Speed Cellular

Cyber Resilience Compliance Req'd

NIST Platform
Firmware Resiliency
TRUSTED COMPUTING GROUP
CyRes

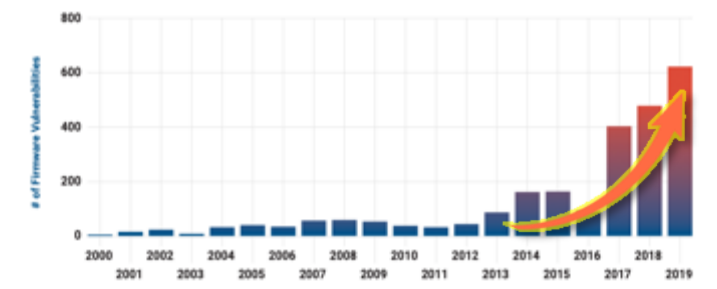


Firmware Attacks Accelerating

Post Quantum Crypto Impacts



Firmware Vulnerabilities By Year



Source: National Vulnerability Database November 13, 2019



Preparing Critical Infrastructure for Post-Quantum Cryptography

Quantum Risk to Digital Communications

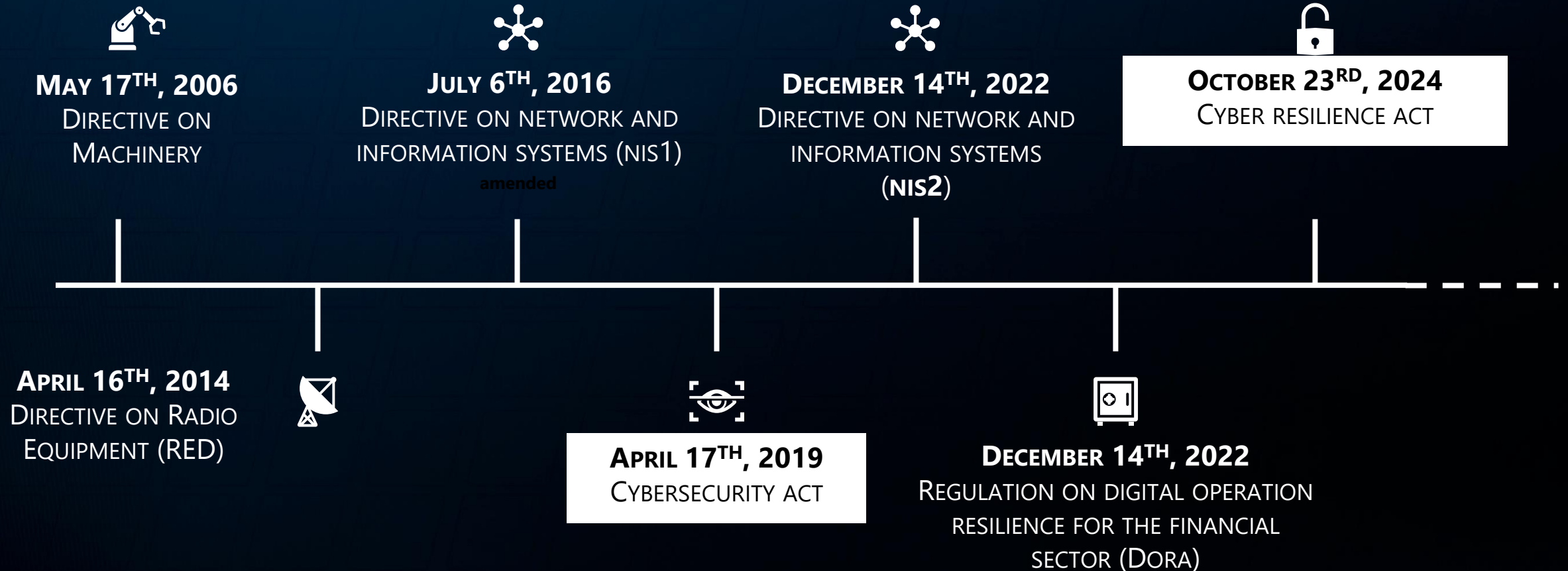
NIST Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

White Paper NIST CSWP 15
Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms

Date Published: April 26, 2023
Author(s): William Barber (Shakti Consulting), W. Paul (NIST), Manojkumar (NIST)

DOCUMENTATION
Publication: 17 White Paper (2023)

An ever-evolving european cybersecurity Regulatory environment leading to CRA...

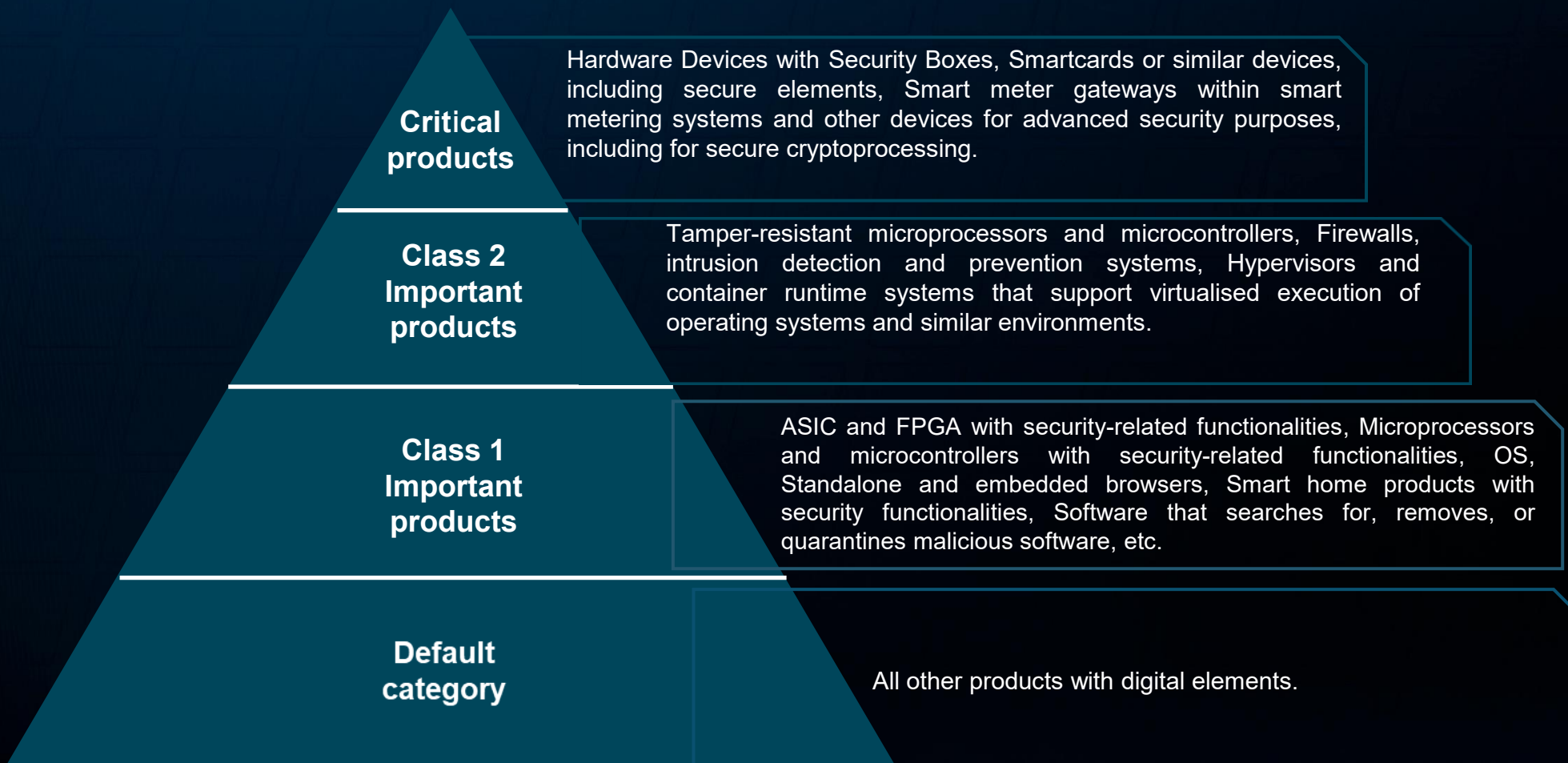


... with a well-defined implementation timeline towards 2027



Four categories of electronic devices are defined as part of CRA...

Scope: All products that are directly or indirectly connected to another device or network



... WITH ASIC AND FPGA being CLASS 1 Important products

Scope: All products that are directly or indirectly connected to another device or network.

OJ L, 20.11.2024

EN

ANNEX III

IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS

15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities

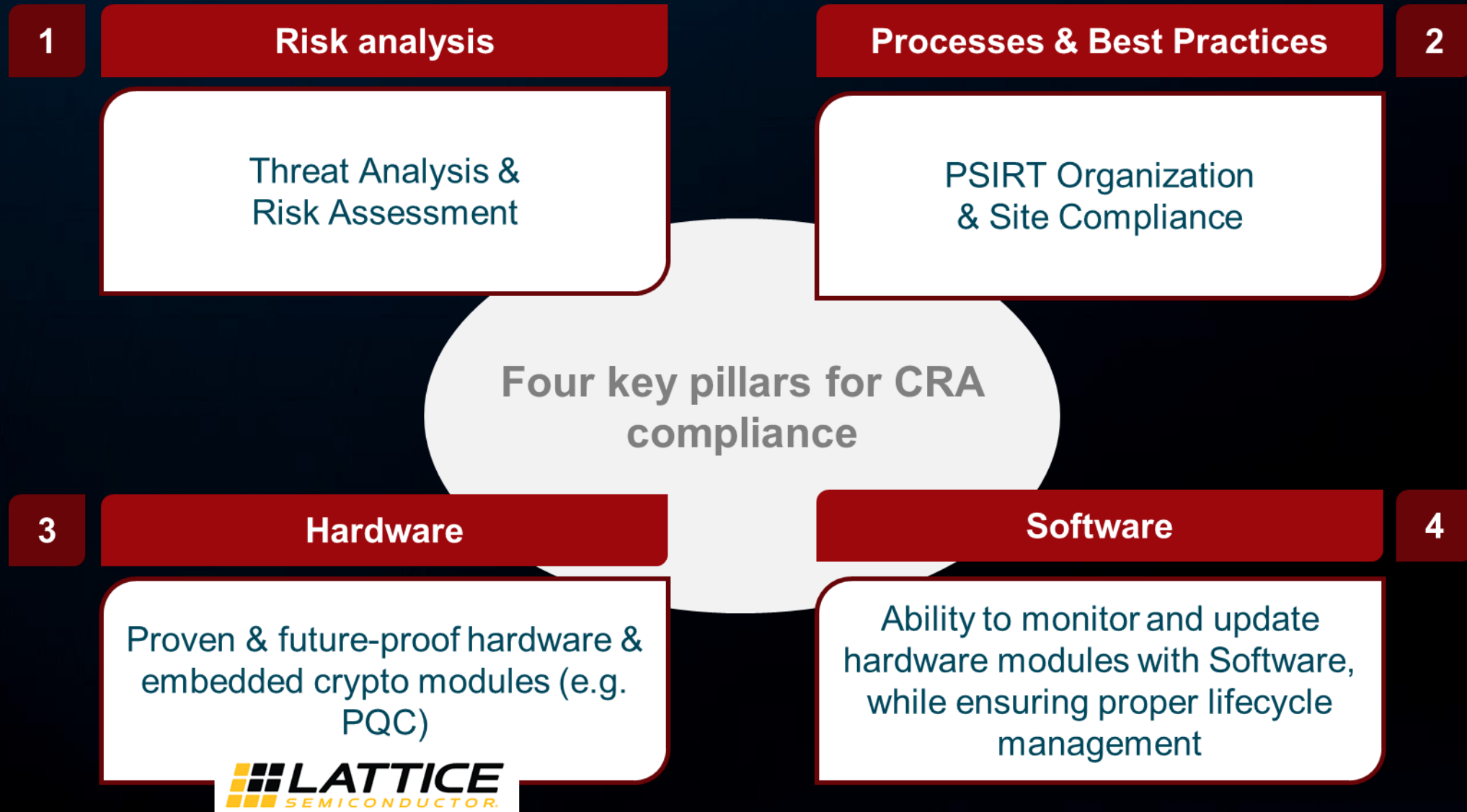
Hypervisors and container runtime systems that support virtualised execution of operating systems and applications in secure environments.

**Class 1
Important
products**

ASIC and FPGA with security-related functionalities, Microprocessors and microcontrollers with security-related functionalities, OS, Standalone and embedded browsers, Smart home products with security functionalities, Software that searches for, removes, or quarantines malicious software, etc.



How to comply with CRA for current and future connected devices





The Low Power Programmable Leader

Security Solutions / CRA

Q4 2025

Lattice FPGA Portfolio

BROAD FAMILY OF LOW POWER FPGAs

Mid-Range



GENERAL PURPOSE

Addresses a broad range of applications across multiple markets

- Lowest power and smallest package with up to 10G SERDES and 500K LUTs
- Industry-leading reliability and efficient processing with class-leading on-chip memory

FPGA FAMILIES TAILORED FOR SPECIFIC NEEDS

VIDEO CONNECTIVITY



Optimized for high-speed video and sensor applications

- First FPGA with hardened MIPI D-PHY
- Highest performance at lowest power

ULTRA LOW POWER



World's lowest power FPGAs; Optimized for small form factor

- Static current as low as 25 uA
- World's most popular ultra-low power FPGA

CONTROL & SECURITY



Optimized for platform management & security applications

- 50% market share
- Highest I/O density

Lattice Security Solutions

FOUNDATIONAL ROOT OF TRUST TECHNOLOGY



Si HARDENED STANDARDS
BASED CRYPTO ENGINES

INTEGRATED DUAL BOOT FLASH w/
ADVANCED LOCKING & PROTECTIONS,
ENABLING PQC TRANSITION

SILICON
FOUNDATION

CYBER RESILIENT PIONEERS



LEADER IN CPU AGNOSTIC
PFR/CYBER RESILIENCE
(NIST 800-193 Compliance)

STRONG ECOSYSTEM PARTNER
NETWORK

SOLUTION
STACK

LEADING SUPPLY CHAIN PROTECTIONS



LOCKED PARTS FROM
LATTICE TO YOUR CM/ODM

SECURE OWNERSHIP TRANSFER
WITHIN PART

SECURE
SERVICE

What is Root-of-Trust ?

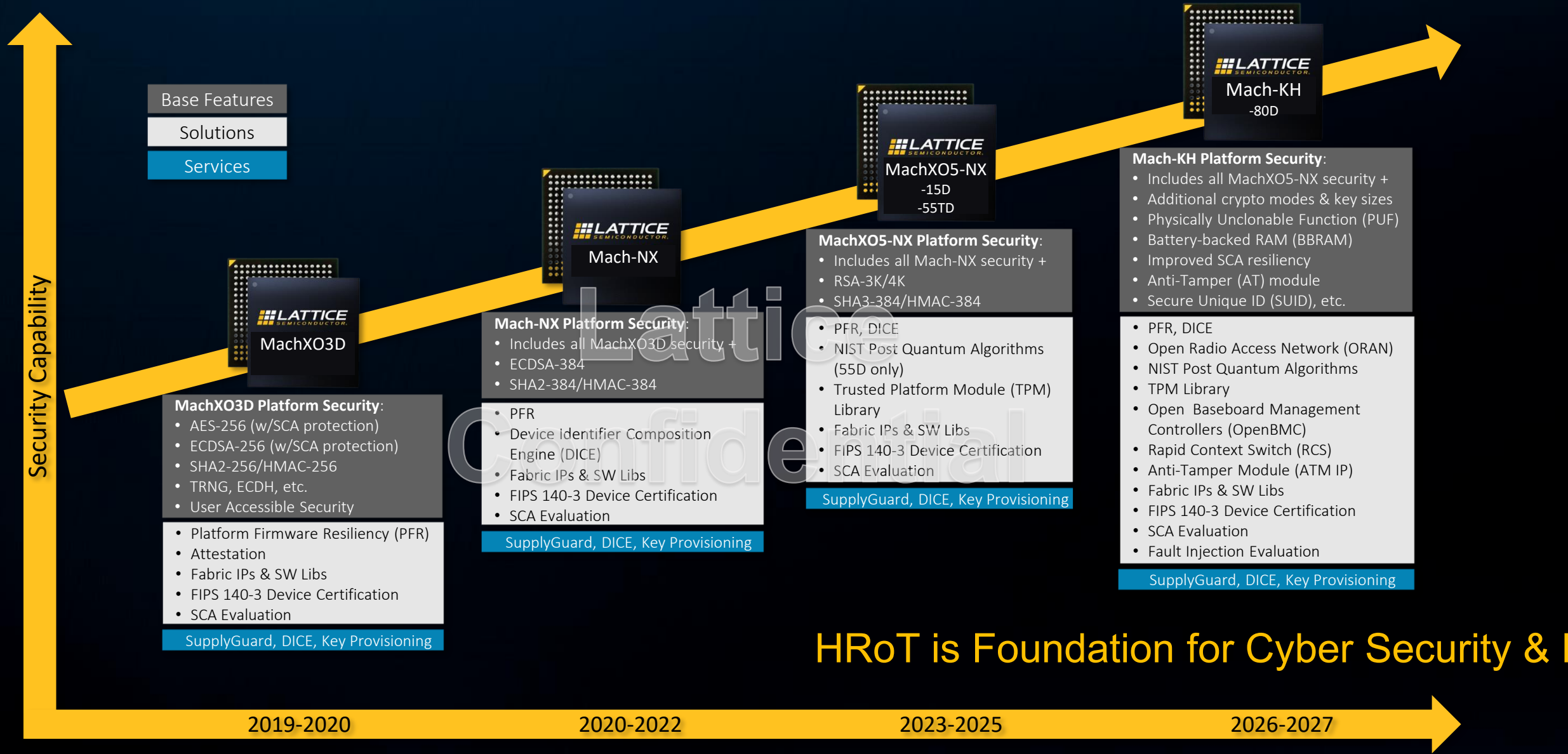
NIST :

Root of trust (RoT) is a foundational component within a system that is inherently trusted. It's the bedrock upon which all other security mechanisms are built. Think of it as the ultimate source of truth and integrity within a system

- Unique silicon level **Identification**, self attest-ability
 - Immutable unique electronic ID tied to each device at silicon level
- Hardened **Cryptographic Services**
 - Standards based
 - Trusted 3rd Party Certified
- Secure Boot (CIA Triad)
 - Authorized, **Authenticated Code**
 - Optional **Code Confidentiality** (i.e. encrypted bitstreams)
 - **Available** when needed (i.e. denial of service resistant (Flash on-board with lock controls))
 - Rollback protection on updates
- Ideally a digital device : **first-on / last-off**
 - Initiates Platform Trust Chain - First link in chain of trust that protects entire systems



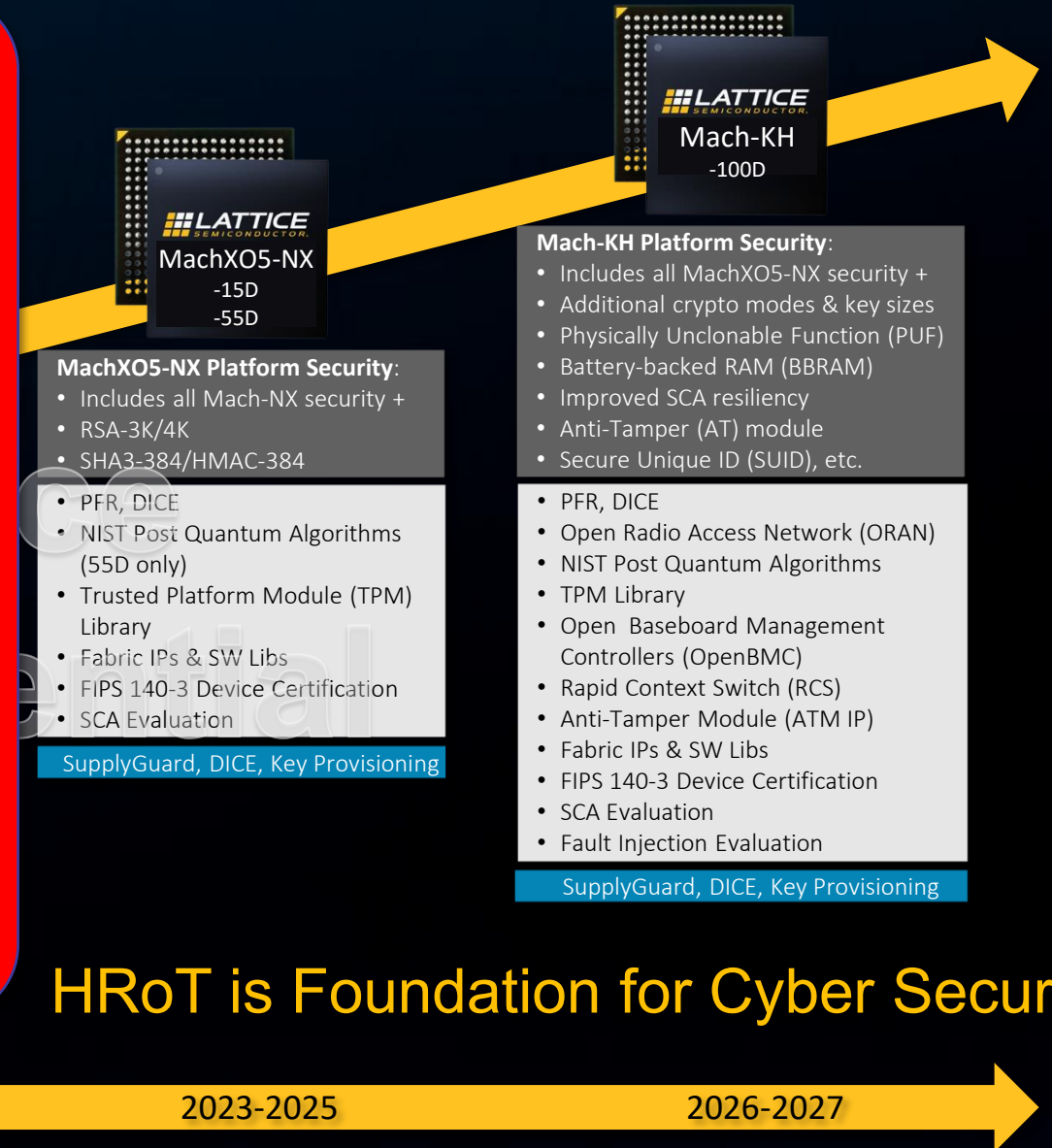
Hardware Root of Trust (HRoT) Evolution & Roadmap



Hardware Root of Trust (HRoT) Evolution & Roadmap

Future Proof Security Roadmap

- FPGAs ideal for evolving Security Compliance Standards
- **Crypto Agility** for enhanced Algorithms & Key lengths (e.g. PQ Crypto)
- **PQC-enabled FPGAs** can directly implement new TPM standards or augment existing TPMs.
- **Unbypassable System Security** when coupled with Power Control & Strong AT



HRoT is Foundation for Cyber Security & P



The Low Power Programmable Leader

Security Solutions / CRA

Q4 2025

Regulations & Standards Driving Adoption of Security Solutions



CISA Mandates & Initiatives

CISA Zero Trust Initiative

Advisory on FW Protection – Mandates HW RoT, Secure Boot, Monitoring



European Union's Cyber Resilience Act

Increasing alarm for protection of critical infrastructure



ORAN Working Group 11

Secure Communication, Zero Trust and Hardware Root of Trust requirements



NSA Commercial National Security Algorithms 2.0 (CNSA 2.0)



Quantum Computing Cybersecurity Preparedness Act

EU Cyber Resilience Act - CRA

- EU Council agreed to move CRA to Legislation on 19th July 2023

Main articles will be mandatory as from Dec 2027

Introduces mandatory cybersecurity requirements for hardware and software products, throughout their whole lifecycle

- Manufacturers of Electronic Devices Must:

- Ensure Cybersecurity is considered through whole product lifecycle:
 - Planning, **Design**, Development, Production, Delivery and **Maintenance**
 - Ensuring a swift and effective response to identified vulnerabilities
- Security updates to be made available for at **least five years**
 - All cybersecurity risks are documented
 - Report actively exploited vulnerabilities and incidents
- Achieve **mandatory certification** for products sold into EU
 - Self-Assessment (mostly consumer) or 3rd Party (Mostly infrastructure)

[The CRA, explained - Cyber Resilience Act](#)

[Cyber Resilience Act - Questions and Answers \(europa.eu\)](#)

European Commission

CYBER RESILIENCE ACT

New EU cybersecurity rules ensure more secure hardware and software products

#DigitalEU #SecurityUnion #Cybersecurity #SOTEU 2022

SEPTEMBER 2022

A first ever EU wide legislation of its kind: the **Cyber Resilience Act** introduces **mandatory cybersecurity requirements for hardware and software products**, throughout their whole lifecycle.

The Act will

- Ensure that **products with digital elements** placed on the EU market have **fewer vulnerabilities** and that manufacturers remain **responsible for cybersecurity** throughout a product's life cycle;
- **Improve transparency** on security of hardware and software products;
- Business users and consumers benefit from **better protection**.

Every 11 seconds there is a **ransomware attack**

Ransomware attacks alone are estimated to have cost the world roughly **€20 billion** in 2021

The **global annual cost** of cybercrime was estimated to be **€5.5 trillion** in 2021

EU Cyber Resilience Act – Categories

- Industrial Electronics mostly into Critical Class I / II

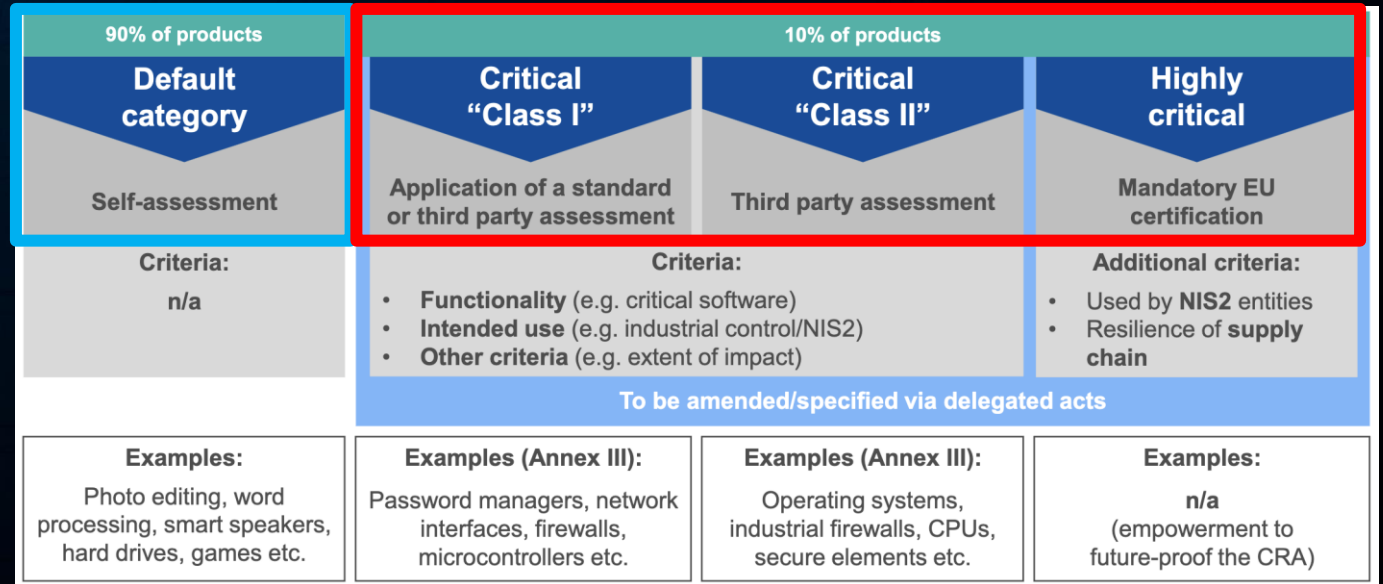
- Products with critical software / control / impact

- Related EU directives & standards:

- NIS2 – Network Infrastructure Security – 2024 - [link](#)
- IEC 62443 – Industrial Control Security - [link](#)
- Automotive SAE 21434 Cyber Security – [link](#)
- DORA – Finance entities – [link](#)
- ISO 14971 – Medical Devices risk assessment - [link](#)
- ISO 27002 - Information security controls - [link](#)
- ...

- Related Cyber Security (US)

- NIST Framework



[IEC 62443 Standard GAP Analysis to the Cyber Resilience Act \(CRA\)](#)

[What is NIS2? An easy-to-understand guide | Advisera](#)

[Guardians of the Digital Realm: Dissecting the NIS2 and NIST Cybersecurity Paradigms | LinkedIn](#)

[Harmonizing Cyber Resilience: How DORA, NIS2, and NIST CSF 2.0 Embrace Continuous Cyber Risk Management | LinkedIn](#)

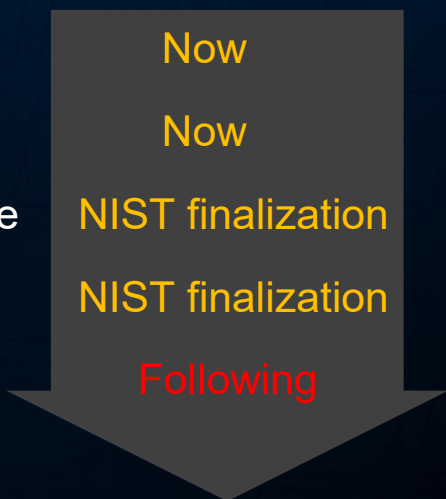
Post Quantum Cryptology - PQC

Future Resilience

- Quantum computing to become a threat around 2030+
- “Steal now – Decrypt later” is a concern **TODAY**

New Crypto Algorithms Adoption

- Wireless Coms
- Data-Center
- Aerospace & Defense
- Automotive
- Industry / IoT



Post-Quantum Encryption Algorithms

ALGORITHM	CNSA 2.0 SUITE ALGORITHM	NIST STANDARD AVAILABLE	TYPE	PURPOSE	REPLACES
LMS	Yes	Yes	Stateful hash-based digital signature scheme	Code and firmware signing	ECDSA, RSA
XMSS	Yes	Yes	Stateful hash-based digital signature scheme	Code and firmware signing	ECDSA, RSA
ML-DSA (Dilithium)	Yes	Yes	Lattice-based	All digital signing use cases	ECDSA, RSA
ML-KEM (Kyber)	Yes	Yes	Lattice-based	Key Exchange	ECDSA, RSA, Diffie-Hellman
ML-SLH (SPHINCS+)	No	Yes	Stateful hash-based	All digital signing use cases	ECDSA, RSA
FALCON	No	No	Lattice-based	All digital signing use cases	ECDSA, RSA



[\[Blog\] Quantum-Proof Your Systems: A Deep Dive into NIST’s PQC Standards](#)

[Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography](#)

Cyber Resilience : Protection & Markets

90% of products	10% of products		
Default category	Critical "Class I"	Critical "Class II"	Highly critical
Self-assessment	Application of a standard or third party assessment	Third party assessment	Mandatory EU certification
Criteria: n/a	Criteria: • Functionality (e.g. critical software) • Intended use (e.g. industrial control/NIS2) • Other criteria (e.g. extent of impact)	Criteria: • Used by NIS2 entities • Resilience of supply chain	Additional criteria: • Used by NIS2 entities • Resilience of supply chain
To be amended/specified via delegated acts			
Examples: Photo editing, word processing, smart speakers, hard drives, games etc.	Examples (Annex III): Password managers, network interfaces, firewalls, microcontrollers etc.	Examples (Annex III): Operating systems, industrial firewalls, CPUs, secure elements etc.	Examples: n/a (empowerment to future-proof the CRA)

CRA – Critical Classes



Industry



Networking



Medical



Defense



Public-Infra



Government

- Industry 2.0 Networking
- Medical Equipment
- Instrumentation
- Public Power infrastructure
- Compute Centers
- Broadcasting
- Government / Defense
- Public Transportation
- Satcom Electronics
- Special Vehicles
- High Value Industries
- Robotics / FuSa
- Wireless Networking



- Root of Trust
- Secure Boot
- Secure Communication
- IP Protection
- Firmware Protection
- Cyber-Attack Detection
- Secure field provisioning

Cyber Resilience Cycle

CyRes Specifies Using a Hardware **Root-of-Trust** Device to **Identify** and perform **Detect, Recover, and Protect** Functions

DETECTION
Cryptographically detect multiple channels of corrupted platform firmware & critical data in real time +
At Power-on
After In-System Updates



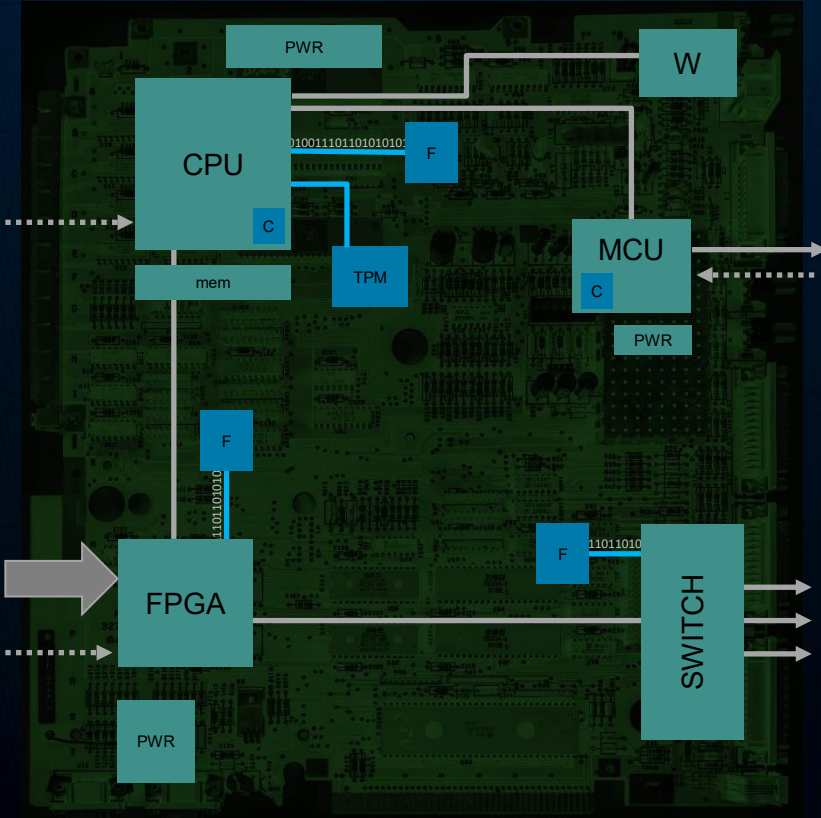
PROTECTION
Protect platform firmware & critical data from corruption
Ensure authenticity & integrity of firmware updates

RECOVERY
Restore corrupted firmware & critical data to its previous value - Initiate a trusted recovery process

Resistance while being attacked

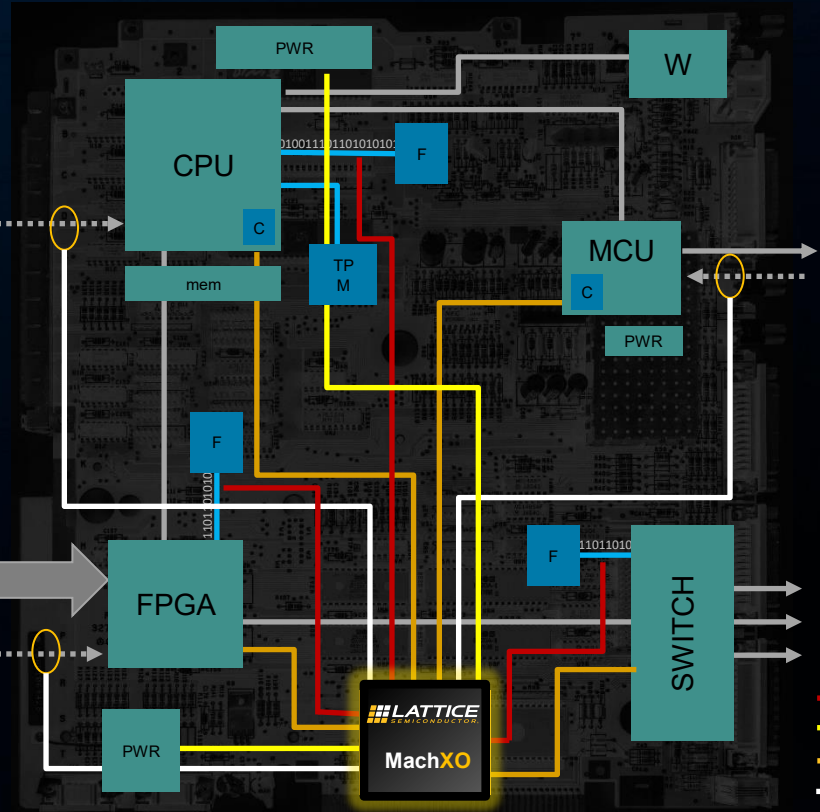
Security – Cyber Resilience by Lattice

Chip-Level Security



✓	Identify	✓
✓	Protect	✓
?	Detect	✓
?	Respond	✓
?	Recover	✓

System-Level Security



Hardware **Root of Trust**
 Platform Firmware Resilience – **PFR**
 Board level **Monitoring**
 System **Recovery**

Cyber Resilient : **Lattice** MachXO-series

Hardware

- Instant-On (first-on, last-off)
- Secure (Dual) Boot Flash
- Crypto Engines (incl PQC)
- TRNG, DICE
- Multi level IO
- Low SEU (FDSOI on XO5)

Software IP

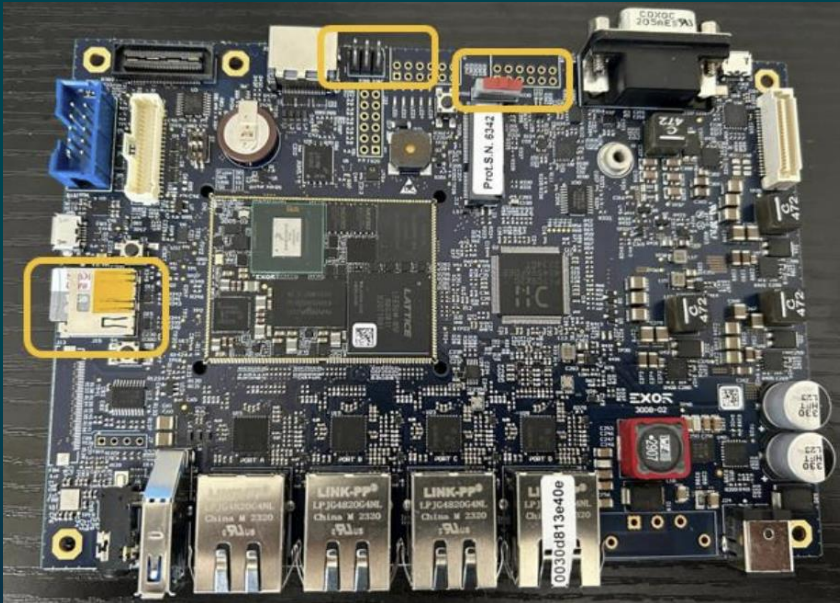
- PFR - Firmware functions
- RoT functions
 - Key store
 - Secure Enclave
- RiscV
- Power Sequence Logic
- CPU-IO management
 - QSPI monitoring / streamer
 - I2C / SMBus Filter + Mailbox
 - I3C controller
 - SGPIO Gateway
 - JTAG locking



Industrial Gateway

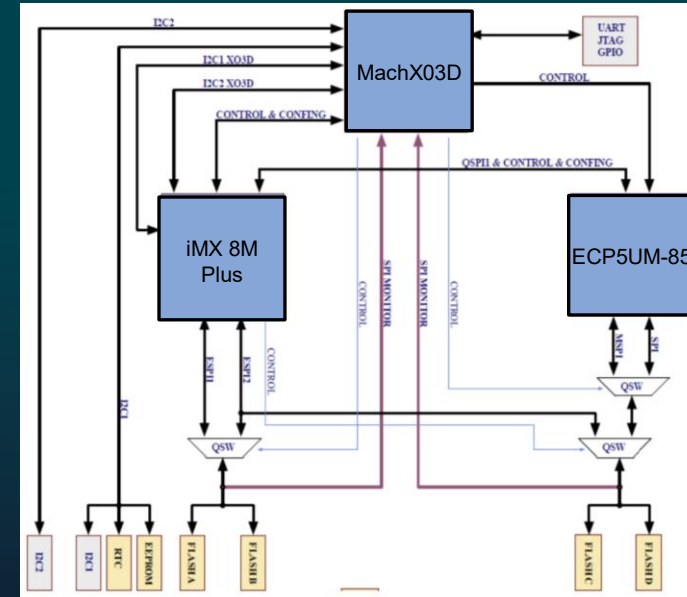
EXOR US 10 kit

Hardware Setup:
EXOR SOM with the US10 Development Kit



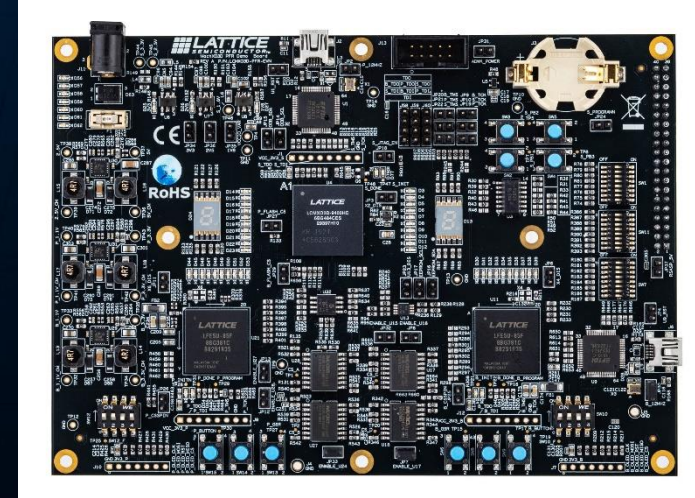
MachXO3D

- Dedicated Hard Security Engine with Secure Unique ID
- Highly configurable user fabric for Security Extensions and Cyber Resilience cycle (PFR stack)
- Secure and Dual boot from onboard Flash
- Onboard user Flash for key storage, manifests and log management
- Interface and asset protection options to Configuration lock and control



How to Evaluate

MachXO3D Sentry Evaluation Board :
[LCMXO3D-PFR-EVN](#)

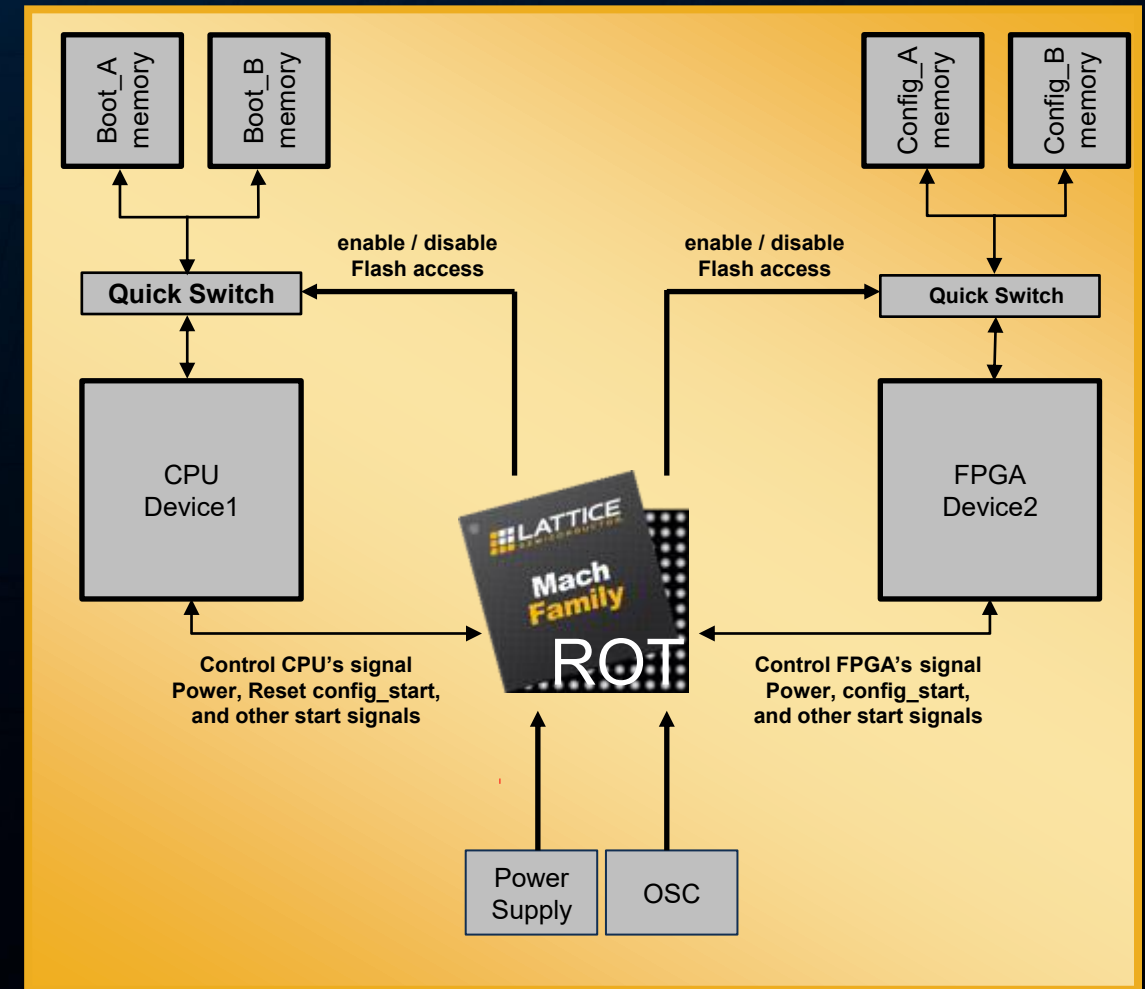


MachXO5D Sentry Evaluation Board :
[LFMXO5D-4P0-SENTRY-EVN](#)



Focus Application for Mach-XO3D

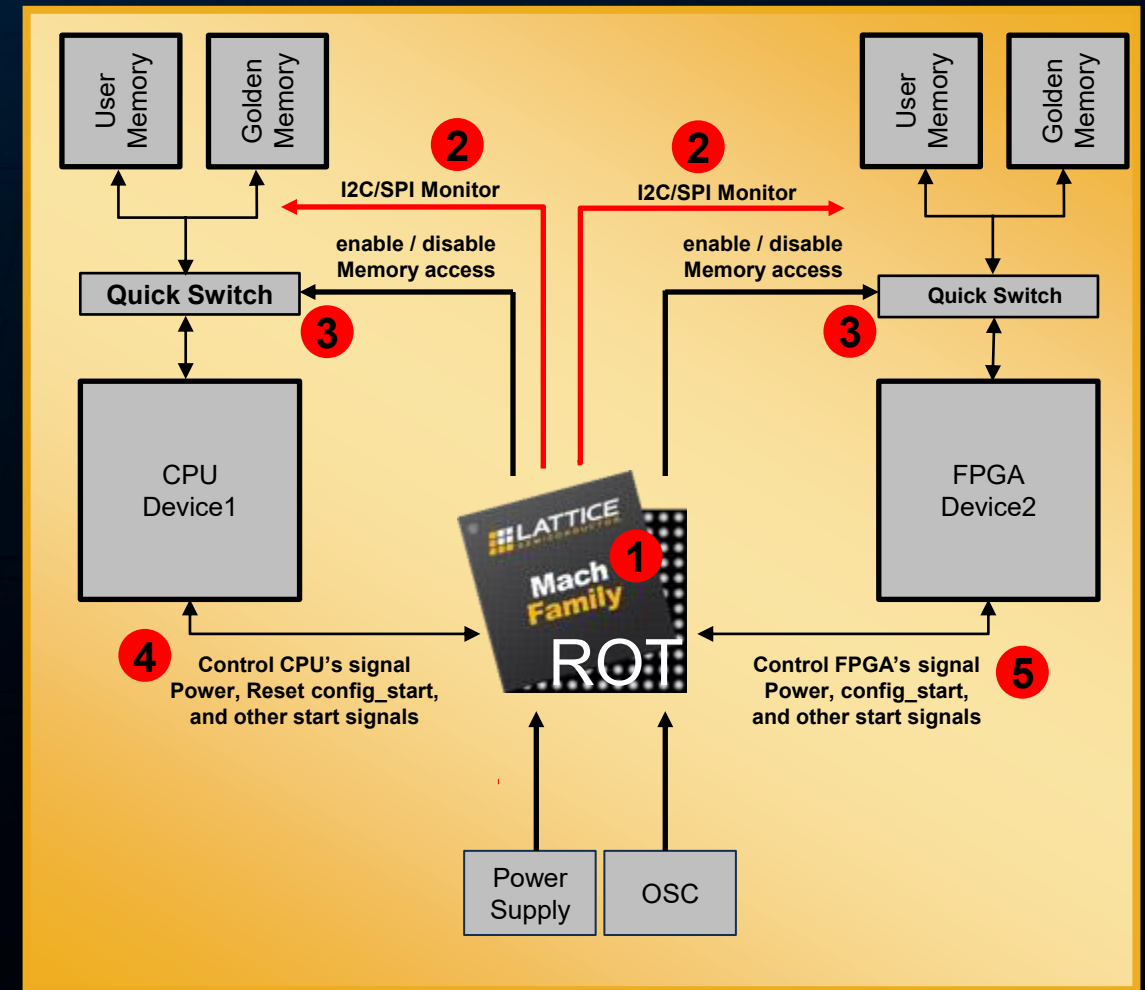
- **Mach-XO3** low-power device for security Root of Trust (ROT), cyber-security & cyber-resilient functionalities and board management functionalities
- **Mach-XO3 Root of Trust (ROT)**
 - Unique silicon level identification, self attest-ability
 - Hardened Cryptographic Services
 - Secure Boot (CIA Triad)
 - Ideally first digital device on
- **Mach-XO3** IEC62443-4-2 certified



PROTECT phase with Mach-XO3D

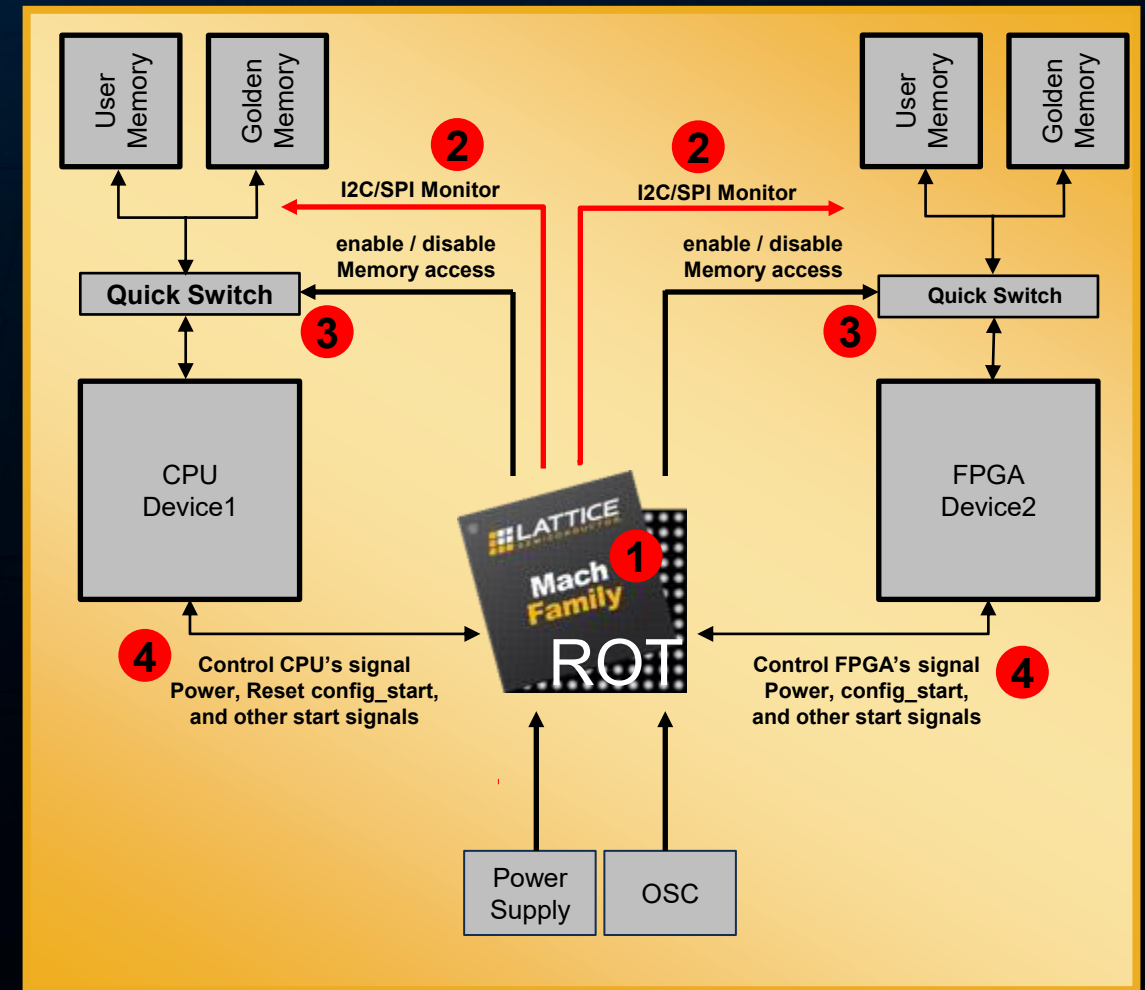
1. Mach-XO3D (ROT) secure boot
 - disable Device1/2 flash access
 - Disable Device1/2 boot
2. Mach-XO3D authenticated all Memory images
 - NOK, corrupted image => **Recovery Phase**
3. Memory Image OK => Enable access
4. Release Device1/2 boot process
5. Move into **Detect Phase**

Option encrypted bitstream or boot images



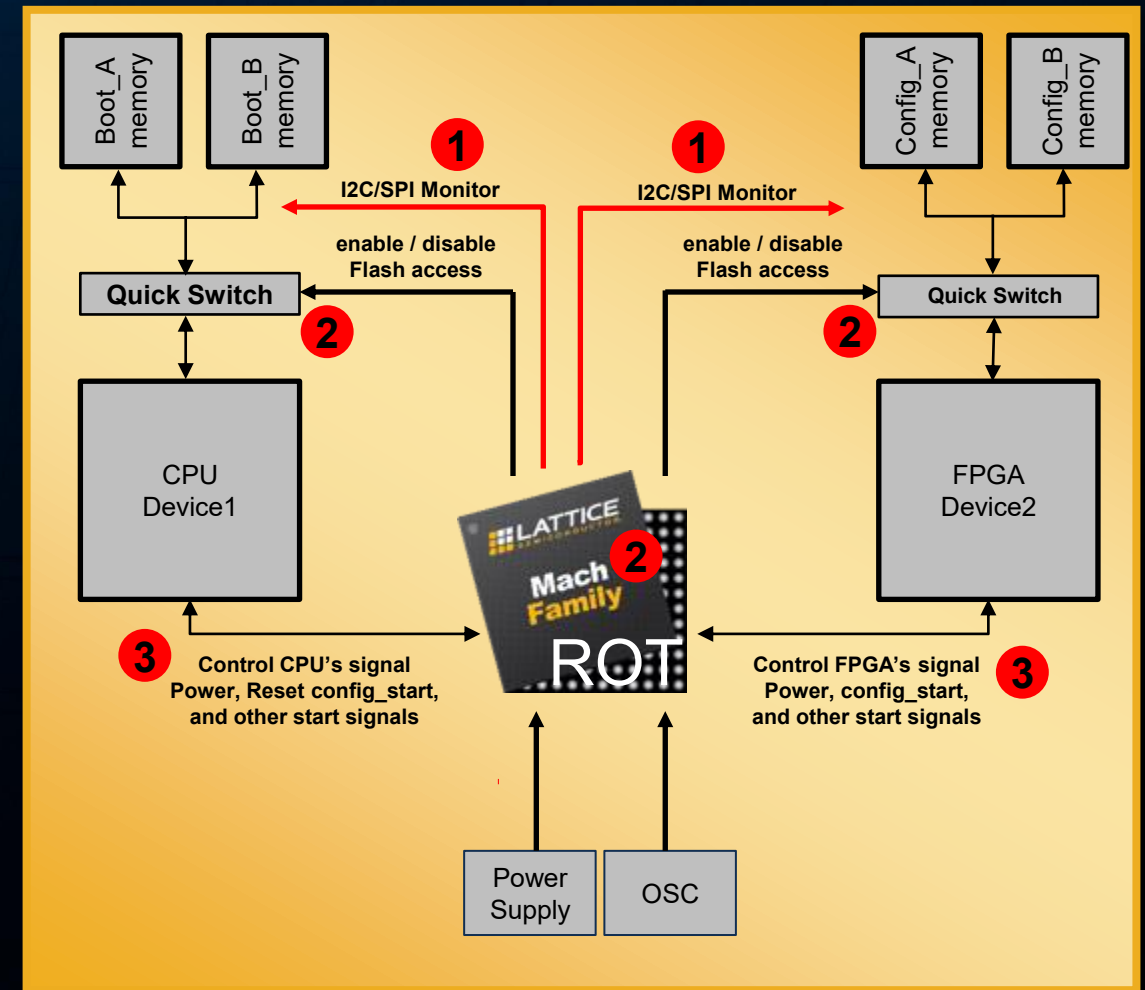
DETECT phase with Mach-XO3D

1. Mach-XO3D self-test
2. Mach-XO3D monitor Memory access
 - authenticated Golden Memory images
3. Risk definition in Filter monitor IP in Mach-XO3D
4. Risks are detected
 - disable Memory access
5. Reset CPU and reconfig FPGA
6. Move into **Recovery Phase**



RECOVERY phase with Mach-XO3D

1. Mach-XO3D authenticated Flash Golden image
 - Code with I2C/SPI Monitor Detect corrupted flash image => recovery Phase
2. Golden is ok => enable CPU/FPGA flash access
3. Memory Image OK => Enable access
4. Release Device1/2 boot process
5. Move into **Detect Phase**

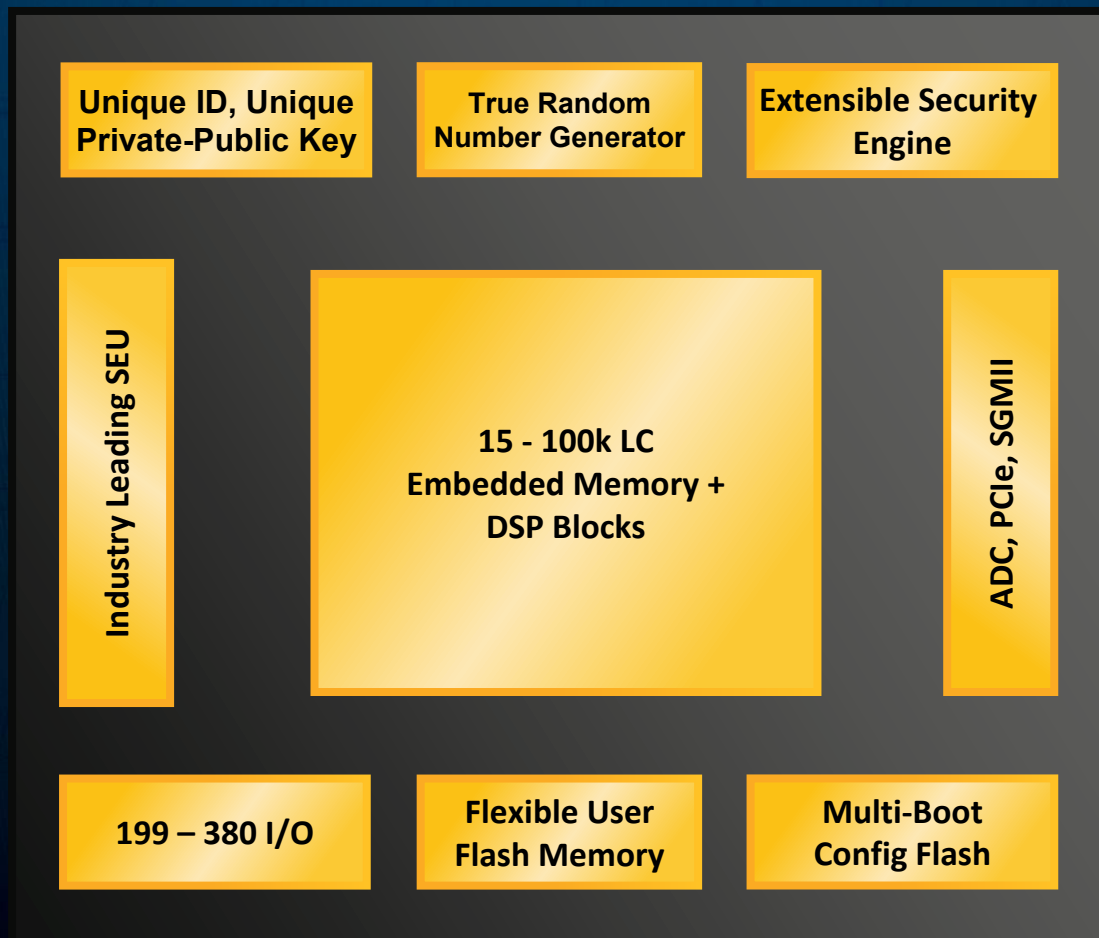


MachXO5-NX

MachXO5-NX

Control Optimized FPGA w/ extensible security

Change graphic to match CNX style



Nexus Programmable Logic Core

- Low power, faster fabric
- LRAM blocks (0.5M) and DSP
- Industry leading SEU performance

Flexible Interfaces

- WR 3.3V I/O and HP 1.8V I/O
- GbE SGMII, ADC
- PCIe Gen 2 (≥ 35 k LC)

Internal Flash Memory


- Multi-boot
- Flexible UFM
- UFM sector protection

Security

- Bitstream encryption/authentication
- User AES256/ECC/SHA256, TRNG, UDS
- Hard and soft port lock
- Extensible engine ECC/HMAC/SHA512
- Secure Root of Trust

MachXO5-NX FPGAs

Product Family		MachXO5-NX (IO Optimized)					MachXO5-NX (Logic Optimized)		
Product Line		LFMXO5-15D	LFMXO5-25	LFMXO5-20TD	LFMXO5-30TD	LFMXO5-65T	LFMXO5-55T	LFMXO5-55TD	LFMXO5-100T
Logic	Logic Cells	14k	27k	20.4k	30k	65k	53k	53k / 38k	96k
Embedded RAM	M18k Blocks / kb	20 / 360	80 / 1440	42 / 756	60 / 1080	130 / 2340	166 / 2988	166 / 2988 (702)	208 / 3744
	M512k Blocks / kb	1 / 512	1 / 512	1 / 512	1 / 512	1 / 512	5 / 2560	5 / 2560	7 / 3584
Distributed RAM	Dist Bits (kb)	95	184	122	190	300	320	320	639
Flash	UFM (kb)	13312	15360	15360	15360	15360	79872	72192	79872
DSP	18x18 Multiplier	16	20	48	72	128	146	93	156
Clocking	Phase Lock Loop	2	2	2	2	2	4	4	4
DDR	DDR Memory	DDR3/DDR3L 1066Mbps x16	DDR3/DDR3L 1066Mbps x16	DDR3/DDR3L 1066Mbps x16	DDR3/DDR3L 1066Mbps x16	DDR3/DDR3L 1066Mbps x16	DDR3/DDR3L, LPDDR4 1066Mbps x16	DDR3/DDR3L, LPDDR4 1066Mbps x16	DDR3/DDR3L, LPDDR4 1066Mbps x16
Serial IO	Hard PCIe	-	-	1xGen2	1xGen2	1xGen2	2 x 1xGen2	2 x 1xGen2	2 x 1xGen2
Security	Dual Boot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	PQC	-	-	-	-	-	-	-	-
	Encrypt/Authenticate	AES-256, ECDSA-384, SHA-384, HMAC-384, TRNG	AES-256, ECDSA-256, SHA-256, HMAC-256, TRNG	AES-256, ECDSA-384, SHA-384, HMAC-384, TRNG	AES-256, ECDSA-384, SHA-384, HMAC-384, TRNG	AES-256, ECDSA-256, SHA-256, HMAC-256, TRNG	AES-256, ECDSA-256, SHA-256, HMAC-256, TRNG	AES-256, ECDSA-521, SHA-512, HMAC-512, TRNG	AES-256, ECDSA-256, SHA-256, HMAC-256, TRNG
Packages									
Ball Pitch	Type (Size)	Total (WRIO,HPIO,ADC)/ (PCIe Gen2)							
0.8 mm	256 BGA (14 x 14 mm)	199 (159,40,6) /(0)	199 (159,40,6) /(0)	181 (145,30,6)(1)	181 (145,30,6)(1)				
	400 BGA (17 x 17 mm)	299 (251,48,6) /(0)	299 (251,48,6) /(0)		336 (282,48,6)/(0)	336 (282,48,6)/(0)	291 (159,132,6) /(1+1)	291 (159,132,6) /(1+1)	291 (159,132,6) /(1+1)
	484 BGA (19 x 19 mm)			378(324,48,6)/(1)	378(324,48,6)/(1)	378(324,48,6)/(1)			


 Pin Migration

 Development

v10252024

MachXO5-NX FPGAs (with PQC) : Lattice Launches Industry-First PQC-Ready FPGA Family: MachXO5-NX TDQ

Product Family		MachXO5-NX (IO Optimized)					MachXO5-NX (Logic Optimized)		
Product Line		LFMXO5-15D	LFMXO5-25	LFMXO5-20TDQ	LFMXO5-30TDQ	LFMXO5-65T	LFMXO5-55T	LFMXO5-55TDQ	LFMXO5-100T
Logic	Logic Cells	14k	27k	20.4k	30k	65k	53k	38k	96k
Embedded RAM	M18k Blocks / kb	20 / 360	80 / 1440	42 / 756	46 / 828	130 / 2340	166 / 2988	39 / 702	208 / 3744
	M512k Blocks / kb	1 / 512	1 / 512	1 / 512	1 / 512	1 / 512	5 / 2560	5 / 2560	7 / 3584
Distributed RAM	Dist Bits (kb)	95	184	122	190	300	320	248	639
Flash	UFM (kb)	13312	15360	15360	15360	15360	79872	72192	79872
DSP	18x18 Multiplier	16	20	48	72	128	146	93	156
Clocking	Phase Lock Loop	2	2	2	2	2	4	4	4
DDR	DDR Memory	DDR3/DDR3L 1066Mbps x16	DDR3/DDR3L 1066Mbps x16	DDR3/DDR3L 1066Mbps x16	DDR3/DDR3L 1066Mbps x16	DDR3/DDR3L 1066Mbps x16	DDR3/DDR3L, LPDDR4 1066Mbps x16	DDR3/DDR3L, LPDDR4 1066Mbps x16	DDR3/DDR3L, LPDDR4 1066Mbps x16
Serial IO	Hard PCIe	-	-	1xGen2	1xGen2	1xGen2	2 x 1xGen2	2 x 1xGen2	2 x 1xGen2
Security	Dual Boot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	PQC	-	-	XMSS/LMS	XMSS/LMS	-	-	XMSS/LMS ML DSA ML KEM	-
	Encrypt/Authenticate	AES-256, ECDSA-384, SHA-384, HMAC-384, TRNG	AES-256, ECDSA-256, SHA-256, HMAC-256, TRNG	AES-256, ECDSA-384, SHA-384, HMAC-384, TRNG	AES-256, ECDSA-384, SHA-384, HMAC-384, TRNG	AES-256, ECDSA-256, SHA-256, HMAC-256, TRNG	AES-256, ECDSA-256, SHA-256, HMAC-256, TRNG	AES-256, ECDSA-521, SHA-512, HMAC-512, TRNG	AES-256, ECDSA-256, SHA-256, HMAC-256, TRNG
Packages									
Ball Pitch	Type (Size)	Total (WRIO,HPIO,ADC)/ (PCIe Gen2)							
0.8 mm	256 BGA (14 x 14 mm)	199 (159,40,6)/(0)	199 (159,40,6)/(0)	181 (145,30,6)(1)	181 (145,30,6)(1)				
	400 BGA (17 x 17 mm)	299 (251,48,6)/(0)	299 (251,48,6)/(0)		336 (282,48,6)/(0)	336 (282,48,6)/(0)	291 (159,132,6)/(1+1)	291 (159,132,6)/(1+1)	291 (159,132,6)/(1+1)
	484 BGA (19 x 19 mm)			378(324,48,6)/(1)	378(324,48,6)/(1)	378(324,48,6)/(1)			

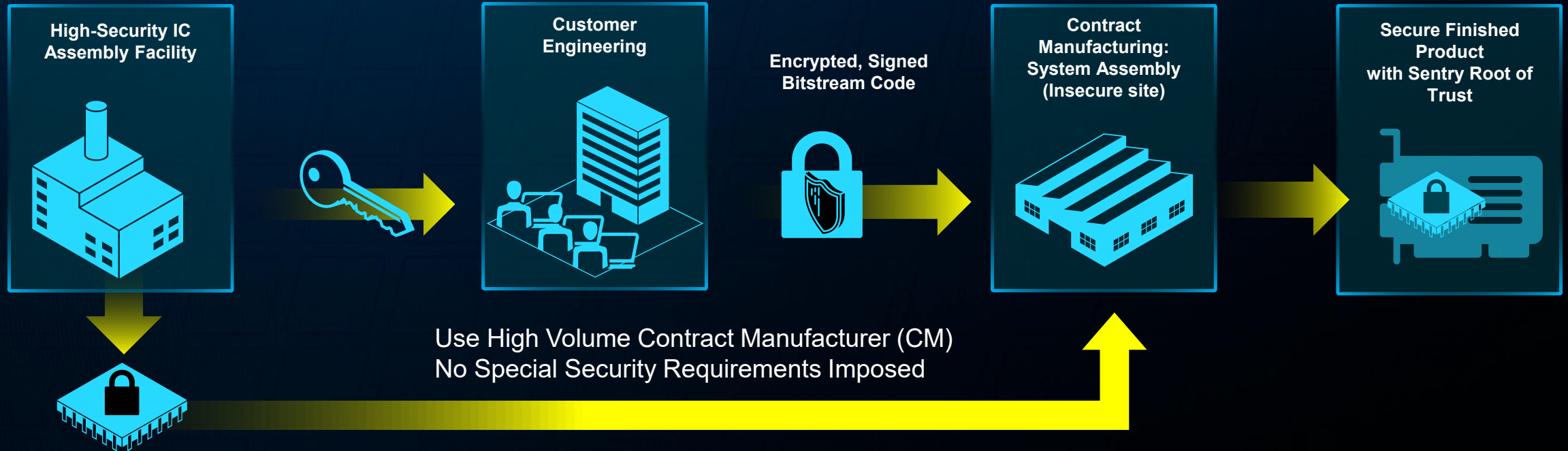
 Pin Migration

 Development

v10252024

SupplyGuard Provisioning

Preserves Trust through today's Dynamic Supply Chain at the Lowest Cost



- Protection against
 - Overbuilding
 - Cloning
 - Counterfeiting
 - Trojan insertion
- Ability to track devices through the supply chain

LATTICE
SupplyGuard

More info

[Time is Ticking to Implement PQC \(latticesemi.com\)](#)

[Quantum-Proof Your Systems: A Deep Dive into NIST's PQC Standards \(latticesemi.com\)](#)

[Addressing Design Complexity in System Control Architecture \(latticesemi.com\)](#)

[Lattice SupplyGuard™ | End-to-End Supply Chain Protection Service \(latticesemi.com\)](#)

[Lattice Sentry™ Solutions Stack | FPGA PFR Root of Trust \(latticesemi.com\)](#)

[Lattice Sentry Root of Trust Demo for MachXO3D | Lattice Demos \(latticesemi.com\)](#)

[Welcome To Trusted Computing Group | Trusted Computing Group](#)

[SP 800-193, Platform Firmware Resiliency Guidelines | CSRC \(nist.gov\)](#)

[Cyber Resilience Act - Questions and Answers \(europa.eu\)](#)

[Time To Act on Cyber Resilience? | Keysight Blogs](#)

[The True Cost of a Security Breach | How Much is a Security Breach \(bitlyft.com\)](#)

[Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024](#)

[Why CEOs can't afford to ignore cybersecurity: The hidden costs of inaction - BFT \(thebftonline.com\)](#)

Solution Brief



SECURING MODERN COMPLEX SYSTEMS WITH LATTICE FPGA-BASED ROOT OF TRUST SOLUTIONS

Achieve Cyber Resilience and Enable Compliance with Key CNSA, NIST and EU Regulations for Enhanced Security and Trust

Overview

Lattice FPGA solutions with advanced security features enable Hardware Root of Trust (HrOT) capabilities. These solutions come in a variety of form factors, supporting a wide range of use cases.

Lattice enables system level security with its hardware-based Root of Trust solutions, providing secure boot and ensuring security of FPGA bitstreams, firmware, software, and device configuration. This solution provides virtually instant detection against multiple types of attacks and compliance with multiple security standards including NIST 800-193 (Platform Firmware Resiliency) and the Trusted Computing Group's Device Identifier Composite Engine (DICE) Specification.

KEY CHALLENGES

- Modern systems cannot be secured with point solutions or by adding a single layer of security.
- Organizations need a holistic approach to protect modern systems against cyber threats.
- Security solutions must be updatable to stay ahead of evolving attacks.
- Strong locking and tamper detection is needed to prevent malicious malware installations or code modifications.

LATTICE SOLUTION

- Secure boot
- Platform Firmware Resiliency (PFR)
- Device Identifier Composition Engine (DICE)
- Secure Enclave
- Cyber Resilience Act (CRA) compliance
- Regulatory compliance
- Identity, encryption, and authentication
- Agile Post Quantum Cryptography
- Denial of Service attack resistance
- CNSA 1.0 and CNSA 2.0 compliance

Lattice Security Capabilities

Cybersecurity for modern devices cannot be achieved with point solutions or by adding a single layer of security. Security must be considered holistically, and Lattice supports a broad range of security features needed to protect devices against the latest cyber threats.

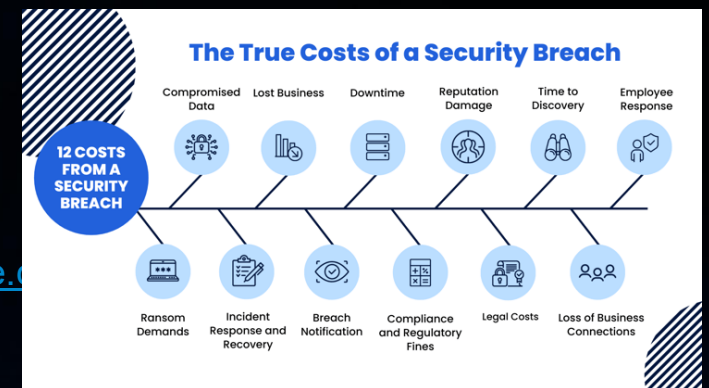
- HrOT, PFR, DICE
- Secure the Wire™: Mutually authenticated ORAN PCIe® & IEEE 1588, Crypto Bridge across protocols (AES-256)
- Hardware enabled security: crypto acceleration, flexible port lock control, secure key storage, PUF
- Anti-tamper capabilities
- Supply chain security
- Key provisioning
- On chip flash enabling recovery to known good image

These security features provide the foundation needed to achieve cyber resilience through an integrated, end-to-end approach to security.

Hardware Root of Trust

Cybersecurity starts at the device level with a Hardware Root of Trust. Lattice FPGAs provide market-leading HrOT capabilities with critical security features including:

- Unique hardware based device identity
- Secure storage of cryptographic keys
- Hardened cryptography
- Support for Post Quantum Crypto (PQC) algorithms
 - XMSS and LMS
 - ML-DSA (Dilithium) and ML-KEM (Kyber)
- Compliant with CNSA 2.0 requirements
- Secure dual boot with lockable onboard Flash
- Secure programming, authentication and encryption
- Anti-tamper protections and side-channel attack resistance (SCA) to protect against physical attacks
- Flexible lock control to ensure tightly controlled access to debug ports and other interfaces





The Low Power Programmable Leader

Smallest
SIZE



Lowest
POWER



Highest
SECURITY



RELIABLE
by Design



EASE
of Use

