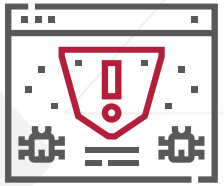
Xilinx Cybersecurity offering in Industrial Internet of Things (IIoT)

XILINX

Integrate Security in Depth with Xilinx

Chain of Trust

Gateways/Firewalls	Controlled interfaces between different zones of trust
System Monitoring	Platform and software enrollment, monitoring, & attestation
Secure Comms	Authenticated and encrypted communications
Trusted Apps	Only applications of known pedigree allowed to run
Validated OS	Digitally signed OS images w/ strict security policies enforced
Secure Boot	Trusted firmware only boots known good SW images
HW Security Device	Immutable device identity, data store, & anti-tamper



XILINX

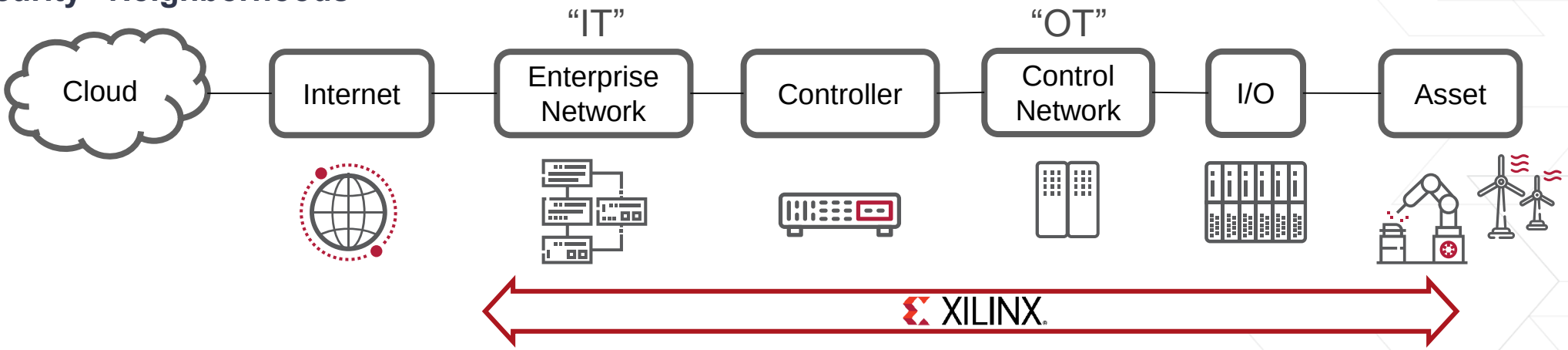
Xilinx Silicon Security Feature Comparison

BUILT-IN SILICON FEATURES	VIRTEX-5	SPARTAN-6	VIRTEX-6	7-SERIES	ZYNQ	US/US+	MPSoC	
Confidentiality w/ AES-256 (BBR/eFUSE)	✓ BBR Only	✓	✓	✓	✓	✓ GCM	✓ GCM	PASSIVE FEATURES
Secure Configuration/Boot (PL/PS)	✓	✓	✓	✓	✓	✓	✓	PASSIVE FEATURES
Hardened Readback Disable	✓	✓	✓	✓	✓	✓	✓	PASSIVE FEATURES
Symmetric Key Authentication			✓	✓	✓	✓	✓	PASSIVE FEATURES
Public Key (Asymmetric) Authentication					✓	✓	✓	PASSIVE FEATURES
DPA Resistant						✓	✓	PASSIVE FEATURES
Obfuscated Key Storage Protection						✓	✓	PASSIVE FEATURES
User Accessible Crypto Functions							✓	PASSIVE FEATURES
Public Key Revocation							✓	PASSIVE FEATURES
Black Key Storage (PUF)							✓	PASSIVE FEATURES
SEU Checking	✓	✓	✓	✓	✓	✓	✓	ACTIVE FEATURES
JTAG Disable/Monitor (BSCAN)	✓	✓	✓	✓	✓	✓	✓	ACTIVE FEATURES
Internal Key Clear	✓	✓	✓	✓	✓	✓ + Verify	✓ + Verify	ACTIVE FEATURES
Internal Configuration Memory Access	✓	✓	✓	✓	✓	✓	✓	ACTIVE FEATURES
Unique Identifier (Device DNA)		✓	✓	✓	✓	✓	✓	ACTIVE FEATURES
Unique Identifier (User eFUSE)			✓	✓	✓	✓	✓	ACTIVE FEATURES
On-chip Temperature/Voltage Monitors	✓		✓	✓	✓	✓	✓	ACTIVE FEATURES
PROGRAM_B Intercept			✓	✓	✓	✓	✓	ACTIVE FEATURES
Key Agility						✓	✓	ACTIVE FEATURES
Tamper Logging						✓	✓	ACTIVE FEATURES
Permanent JTAG Disable					✓	✓	✓	ACTIVE FEATURES
Permanent Decryptor Disable						✓	✓	ACTIVE FEATURES

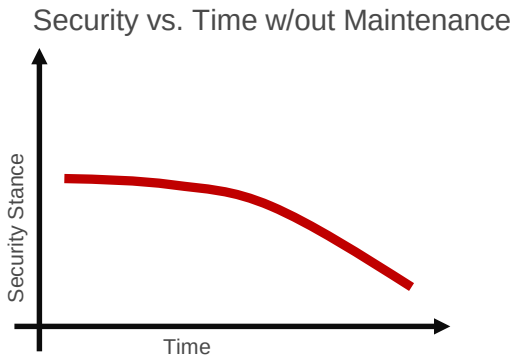
XILINX

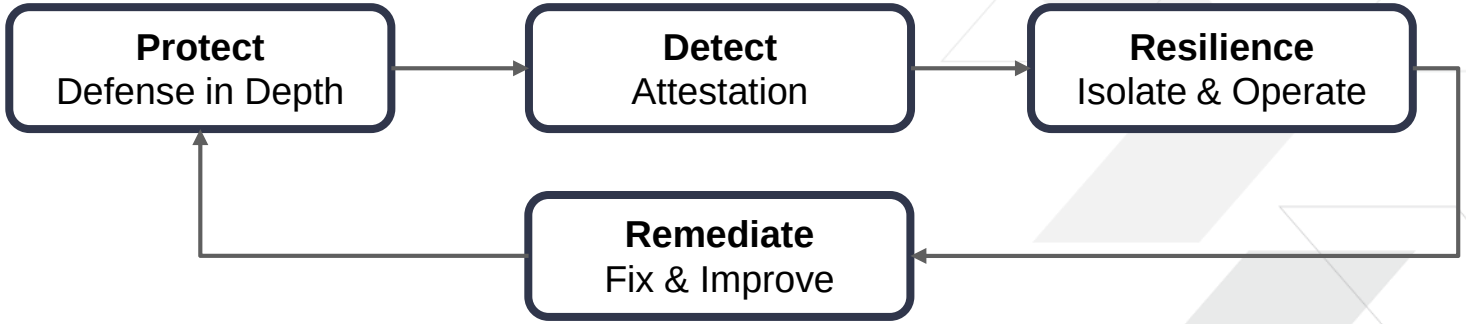
Xilinx Extends Lifetime of Secure Products

Security "Neighborhoods"



Industrial Security "Lifecycle"

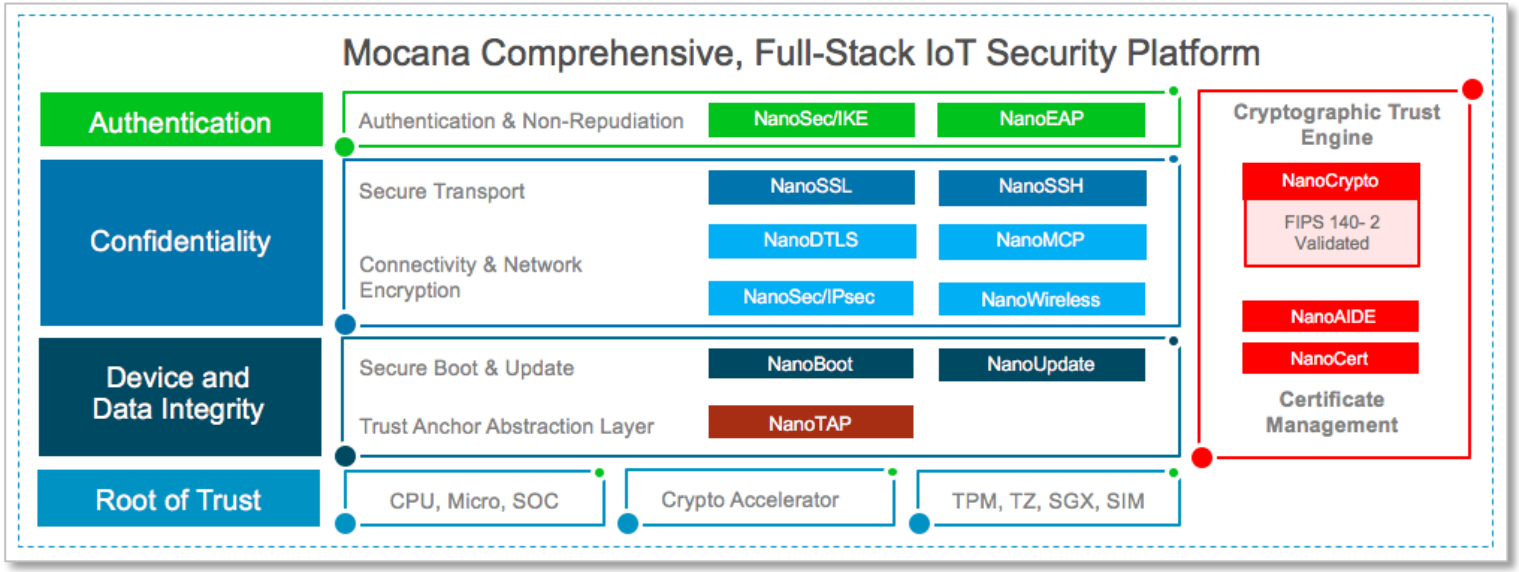




Longer Lifecycle with Secure Enrollment and Xilinx Programmability

XILINX

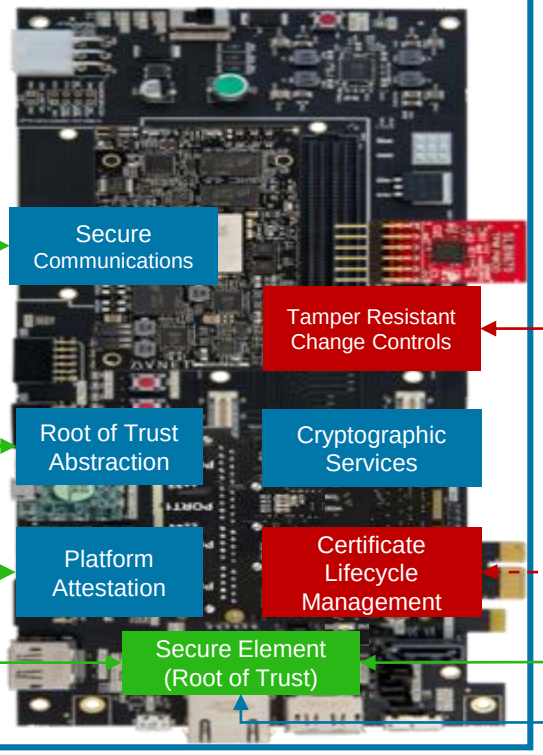
Measured Boot and Secure SW Enrollment



- **Cybersecurity is key challenge for PLC and IPC**
- **Primary solution: Mocana's IoT Security Platform on Xilinx SoC**
  - Fully assembled and validated
  - Builds on HW Root of Trust
  - IEC 62443-2-4 and 62443 3-3, level 4 compliant
  - Endpoint Security IIC Industrial Internet Security Framework compliant
  - Trusted Computing Group for IIoT Security compliant

The Endpoint Security Platform in Hardware

Endpoint Security (Level: Enhanced)



- Device authentication protocols (non-repudiation)
- Secure data transport (PKI, quantum-resistant cipher suite)
- Local rules engine (network whitelisting, ingress/egress access controls)

- Separation of secure agent (process, container, virtualization, or gateway based)

- Secure boot attestation (firmware, UEFI, U-Boot)

Runtime attestation (enclave report)

- Remote and automated endpoint update (firmware, configuration, OS, or application)

Device certificate

Device identity

- Endpoint identity

Boot attestation (signed quote)

Pre-Integrated Mocana Supported Use Cases

- ☑ Device Enrollment
- ☑ Secure Update
- ☑ Secure Transport
- ☑ Remote Attestation

Integrated Xilinx & Infineon HW Supported Use Cases

- ☑ TPM
- ☑ TPM Interface
- ☑ Secure Boot
- ☑ Measured Boot

Benefits

- Layered approach
- Abstraction for applications - no vendor lock-in
- TPM (Trusted Platform Module) supported, using Infineon Optigo family
- Easy migration path from open source silos
- Life cycle device protection across updates
- Simple APIs for secure key storage/usage
- Reduce memory footprint for constrained devices

Mocana on Xilinx ZU+: Competitive Differentiation

- Only fully assembled and validated **solution** on market built on HW Root of Trust spanning from Edge to Cloud
  - IEC62443 Level 4 compliant
  - Endpoint Security IIC Industrial Internet Security Framework compliant
  - Trusted Computing Group for IIoT Security compliant

- Mocana offers significantly more than a Crypto library for TTM
  - Curated and Updated
  - Certified to FIPS140-2, IEC 62443-3-3, NERC CIP 003-3
  - Contains no open source
  - Already widely adopted → we can plug into their user base

Mocana's Embedded Security Solution Is Comprehensive

	Mocana Solution	Authentication Point Solutions	Threat Intelligence & Firewall	Encryption Solutions	Open Source Crypto Libraries
Secure Credentialing	✓	✓	✗	✓	✓
Verified Boot	✓	✓	✗	✗	✗
Secure Device Firewall	✓	✗	✓	✗	✗
Encryption	✓	✗	✓	✗	✗
Data Integrity	✓	✓	✗	✓	✗
Device Integrity	✓	✗	✗	✗	✗
Threat Intelligence	✗	✗	✓	✗	✗
Secure Cloud Interconnect	✓	✗	✗	✗	✓
Secure Update	✓	✗	✗	✗	✗
Scalable Device Enrollment	✓	✗	✗	✗	✗

9

XILINX

Adaptable.
Intelligent.

XILINX