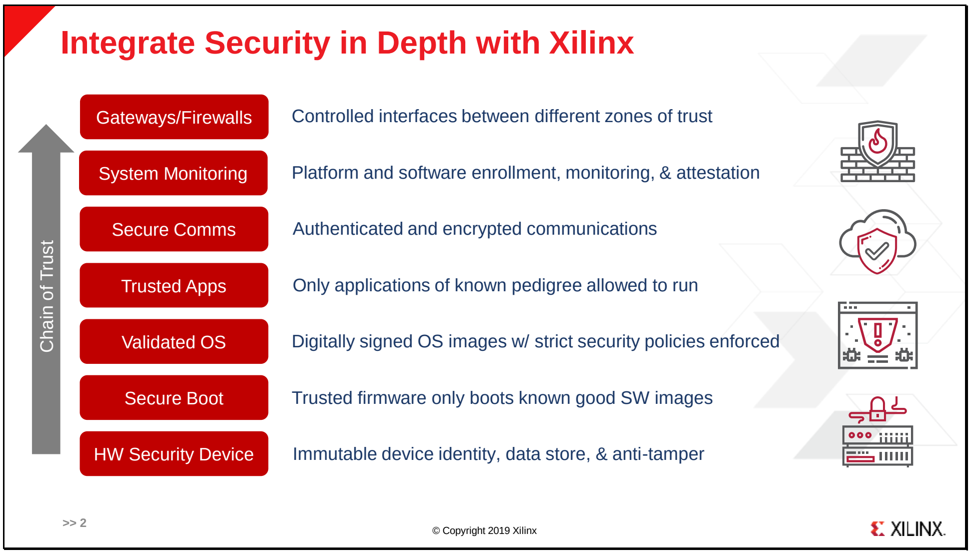
Slide 1

Xilinx Cybersecurity offering in Industrial Internet of Things (IIoT)

Slide 2



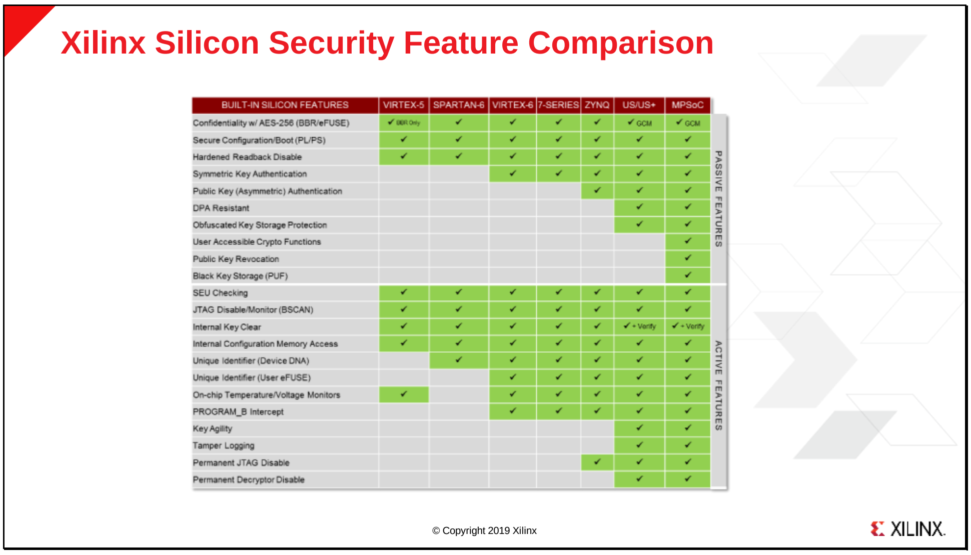
Integrate Security in Depth with Xilinx

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.

Slide 3



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)	✓	✓	✓	✓	✓	✓	✓	
Hardened Readback Disable	✓	✓	✓	✓	✓	✓	✓	
Symmetric Key Authentication			✓	✓	✓	✓	✓	
Public Key (Asymmetric) Authentication					✓	✓	✓	
DPA Resistant						✓	✓	
Obfuscated Key Storage Protection						✓	✓	
User Accessible Crypto Functions							✓	
Public Key Revocation							✓	
Black Key Storage (PUF)							✓	
SEU Checking	✓	✓	✓	✓	✓	✓	✓	ACTIVE FEATURES
JTAG Disable/Monitor (BSCAN)	✓	✓	✓	✓	✓	✓	✓	
Internal Key Clear	✓	✓	✓	✓	✓	✓ + Verify	✓ + Verify	
Internal Configuration Memory Access	✓	✓	✓	✓	✓	✓	✓	
Unique Identifier (Device DNA)		✓	✓	✓	✓	✓	✓	
Unique Identifier (User eFUSE)			✓	✓	✓	✓	✓	
On-chip Temperature/Voltage Monitors	✓		✓	✓	✓	✓	✓	
PROGRAM_B Intercept			✓	✓	✓	✓	✓	
Key Agility						✓	✓	
Tamper Logging						✓	✓	
Permanent JTAG Disable					✓	✓	✓	
Permanent Decryptor Disable						✓	✓	

XILINX.

Link/Overview:
-> https://www.xilinx.com/products/technology/design-security.html#overview

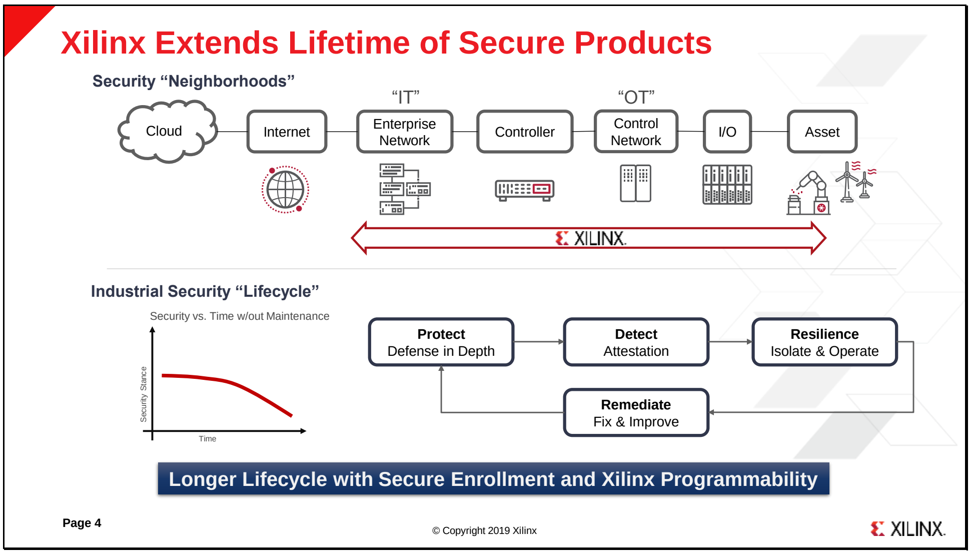
Anti Tamper Details:
-> https://www.xilinx.com/support/documentation/application_notes/xapp1084_tamp_resist_dsgns.pdf (6series & 7series)
-> https://www.xilinx.com/support/documentation/application_notes/xapp1323-zynq-usp-tamper-resistant-designs.pdf (US & US+)

Explanation for built-in silicon features:
Confidentially w/ AES-256 (BBR/eFUSE) … Storing an encrypted bitstream in external flash (or other means) and then decrypting it dynamically during FPGA configuration (inside the FPGA’s decryption engine) provides for a high level of confidentiality.
Secure Configuration/Boot (PL/PS) … Because of the value of intellectual property (IP), and because the incremental effort and cost to boot securely is small, secure boot should be used to boot Zynq devices. Secure boot of Zynq devices uses public and private cryptographic algorithms.
Hardened Readback Disabling Circuitry … Whenever an encrypted bitstream is loaded into the FPGA, readback of the internal configuration memory cannot be performed by any of the external interfaces (including JTAG). All external readback is automatically blocked (disabled) by hardened triple-redundant logic.
Symmetric Key Authentification … <u>Definition</u>: *Same key* used for both encryption and decryption

Public Key (Asymmetric) Authentification … Definition: Private (secret) key used for decryption and/or signature creation at a secure facility / Public key used for encryption and/or signature verification in a fielded device
DPA Resistant … Xilinx provides DPA resistance by limiting the amount of side-channel data that an adversary can collect on any one key. This protocol-based data limiting technique is used on Zynq UltraScale+ devices to mitigate against DPA attacks of the on-chip bitstream decryptor.
Obfuscated Key Loading and Storage … Optionally, key data written and stored into a UltraScale+ device eFUSE array can be obfuscated. The key data is encrypted using a fixed family key that is identical for all Zynq UltraScale+ devices, and is known only to Xilinx. (The Zynq UltraScale+ device family key is different from the UltraScale+ FPGA family key).
User accessible crypto blocks … Access and use the AES-GCM, RSA and/or SHA hardened crypto accelerators post secure boot. / Develop PS code or PL logic to interface with the desired crypto accelerator for use by the application.
Public key revocation … Revoke the primary public key (PPK) or secondary public key (SPK) in response to a key management event which could be due to a breach in security or a normal crypto period key update. / Develop PS code to invalidate an expired PPK or SPKs.
PUF-enabled Black Key Storage … In Zynq UltraScale+ devices there is a hardened physical (sometimes also called physically) unclonable function (PUF) which is a function that produces a unique signature or fingerprint for a device. The PUF output is different from device to device, even those devices from the same silicon wafer. In some PUF implementations, as is the case in Zynq UltraScale+ devices, the output (or response) is only known to the device itself and no one else (including the manufacturer). A PUF leverages minute CMOS manufacturing process variations that produce uniqueness between devices, such as threshold voltage, oxide thickness, metal shape, resistances, and capacitances. Xilinx devices are designed to operate within these normal process variations without affecting functionality. For a PUF to be useful and effective it must be able to reliably recreate this unique signature or fingerprint without being impacted by environmental conditions or aging effects.
SEU Checking … Corruption of any of the PL internal configuration memory cells (that are configured by the decrypted bitstream) could cause the Xilinx FPGA/SoC device to operate in an unknown or undesired manner. The corruption could occur by an intentional post-configuration tamper attack or by an unintentional event such as a single-event upset (SEU). By using the SEM IP core, continuous readback of configuration data in the background of a design is performed to detect any bit flips. The SEM IP core can also perform SEU corrections.
JTAG Port Temporary Disable / Monitor … JTAG port temporary disable (Prevent an unauthorized JTAG access. Boot device securely (JTAG is disabled by default).) / JTAG port monitor (Detect unauthorized JTAG access. Enable the JTAG toggle detect in the corresponding csu_tamper register.)
Internal Key Clear … BBRAM key zeroize (erase + verify) / Zeroize the battery-backed key in response to a tamper event. / Develop PS code to determine the proper conditions for clearing the AES key through the aes_key_clear register and for reading the verification bit in the aes_status register.

Internal Configuration Memory Clearing … Erase the configuration memory in response to a tamper event. / Instantiate ICAP primitive and develop FPGA logic to determine the proper conditions for sending an IPROG command.
Unique Identifiers (Device DNA and User eFUSE) … Prevent the design from operating (or operate in a limited manner) if unique identifier is not recognized. / Develop FPGA logic to be able to read/process the unique identifier(s) and determine if they are valid. / Device DNA consists of a xx-bit device-specific serial number and is set by Xilinx in one-time programmable (OTP) fuses on the FPGA during the manufacturing flow (FPGA logic read access to the value is via the DNA_PORT primitive, or it can be read externally via JTAG). User eFUSE provides xx-bits of user read/write OTP area and is set by the user via JTAG (FPGA logic read access to the value is via the EFUSE_USR primitive). Both of these UIs can be used separately or in conjunction for security purposes.
On-Chip Temperature and Voltage Monitors/Alarms (Detection/Response) … Ensure device is operating within normal environmental limits. / Instantiate the PS and PL system monitor (SYSMON) primitives and develop PS code and PL logic to check and respond to environment status.
PROG Intercept (Prevention and Detection) … Not all memory elements in the FPGA are cleared upon configuration. For example, there might be microprocessor caches or gigabit speed serial I/Os (GTX and GTH transceivers) with FIFOs in use that retain state even after the external PROGRAM_B pin is asserted (assertion of PROGRAM_B causes the FPGA to reset and become reconfigured via the bitstream). An attacker could potentially assert the PROGRAM_B pin and replace the user bitstream with their own bitstream (one that is designed to dump out the contents of the uncleared memory elements after the FPGA is configured). By using the PROG intercept feature (there is a PROG request/acknowledge pair on the STARTUP block PREQ/PACK), the user can indefinitely delay the reconfiguration of the FPGA so that these memory elements can first be cleared by the user design (or any other housekeeping tasks that might need to be performed before allowing a PROGRAM_B to happen).
Key agility (BBRAM only) … Update the BBRAM key securely in the field without having to return the board or module to a secure facility. / Develop PS code or PL logic that can perform a secure key exchange in logic in response to a key management event and load the new BBRAM key through the PS.
Non-volatile (eFUSE) tamper event logging … Securely log a tamper event in non-volatile memory (eFUSE) for later forensic analysis. / Develop PS code for logging tamper events in the USER_0 through USER_7 eFUSE registers.
Permanent JTAG Port Disable … JTAG port permanent disable (eFUSE) (Permanently prevent unauthorized JTAG access in response to a tamper event. Dynamically program the jtag_dis eFUSE bit in the sec_ctrl eFUSE register.)
Permanent Decryptor Disable … Cryptography extensions can be permanently disabled through eFUSEs.

Slide 4



Xilinx Extends Lifetime of Secure Products

Security “Neighborhoods”

“IT”

“OT”

Cloud

Internet

Enterprise Network

Controller

Control Network

I/O

Asset

Industrial Security “Lifecycle”

Security vs. Time w/out Maintenance

Protect
Defense in Depth

Detect
Attestation

Resilience
Isolate & Operate

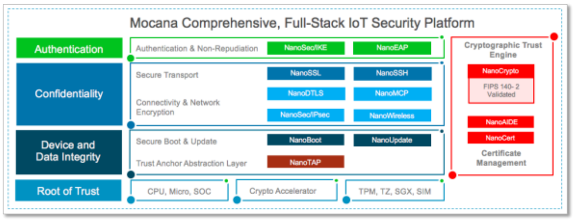
Remediate
Fix & Improve

Longer Lifecycle with Secure Enrollment and Xilinx Programmability

Slide 5

Measured Boot and Secure SW Enrollment

MOCANA



- > **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

XILINX.

Link: https://www.infineon.com/cms/en/partner-network/Security-Network/Preferred-Security-Partners/mocana/

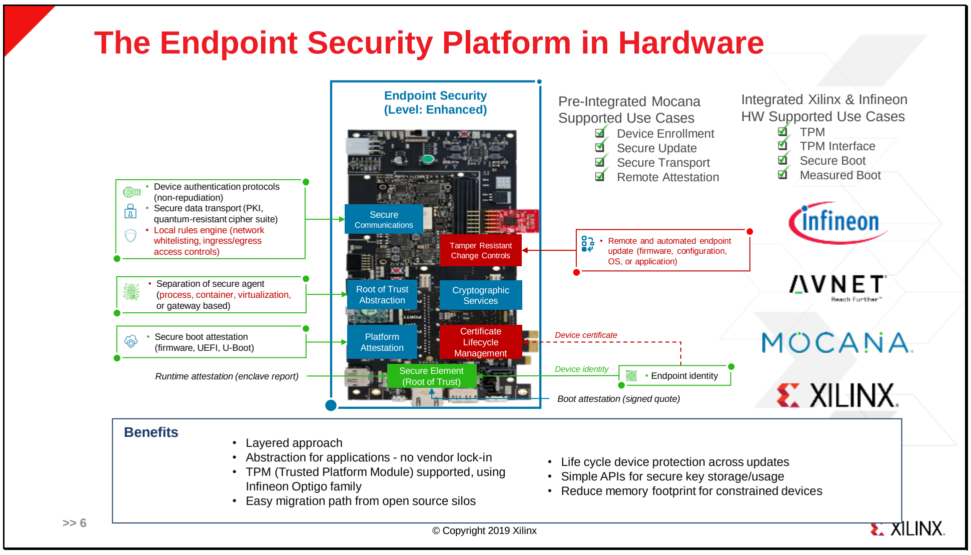
«**Mocana's contribution to the Infineon Security Partner Network**
Mocana works with Infineon on their OPTIGA^{TM} TPM 1.2 and 2.0 chips to tie root of trust down to the hardware level. Mocana's TPM support provides the tools to increase security surrounding sensitive information on devices containing a TPM. Our software licensing is subscription based, and can be implemented to interface with the TPM chip to generate hardware or software keys that can only be decrypted by the TPM. Mocana's security solutions are generally used by large industrial firms, automakers and device manufactures. Especially when it comes to Industrial Control Systems (ICS), it is hard to manage the Operation Technologies (OT) security systems that are in place. Mocana software was developed and tested to give companies architectural and safety benefits, having unified API- and General Public License (GPL)-free code.» Source: https://www.infineon.com/cms/en/partner-network/Security-Network/Preferred-Security-Partners/mocana/

«Infineon OPTIGA™ TPMs have been certified to Common Criteria Evaluation Assurance Level (CC EAL) 4+. They include 6 KB of user-accessible non-volatile memory, as well as Elliptic Curve Cryptography (ECC-256) and RSA2K encryption, with the private key stored in secured hardware. As shown in Figure 1, Infineon also offers OPTIGA™ products with other security feature sets (Trust B, E, X and P) that can be used to address a variety of system trust requirements.» Source: https://www.infineon.com/dgdl/Infineon-Secured+Network+Equipment+Whitepaper-Whitepaper-v01_00-EN.pdf?fileId=5546d46269e1c019016ab5c00a3d542d

https://www.mocana.com/trustpoint

https://www.mocana.com/technology

Slide 6



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)

Secure Communications

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

Root of Trust Abstraction

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

Platform Attestation

Runtime attestation (enclave report)

Secure Element (Root of Trust)

Tamper Resistant Change Controls

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

Cryptographic Services

Certificate Lifecycle Management

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

infineon

AVNET Reach Further™

MOCANA

XILINX

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

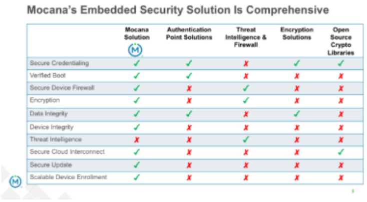
- Life cycle device protection across updates
- Simple APIs for secure key storage/usage
- Reduce memory footprint for constrained devices

XILINX.

Slide 7

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	✓	✗	✗	✗	✗

Slide 8

Adaptable.
Intelligent.

XILINX.