Industrial IoT Security Attacks & Countermeasures

Chris Shire – Infineon Technologies

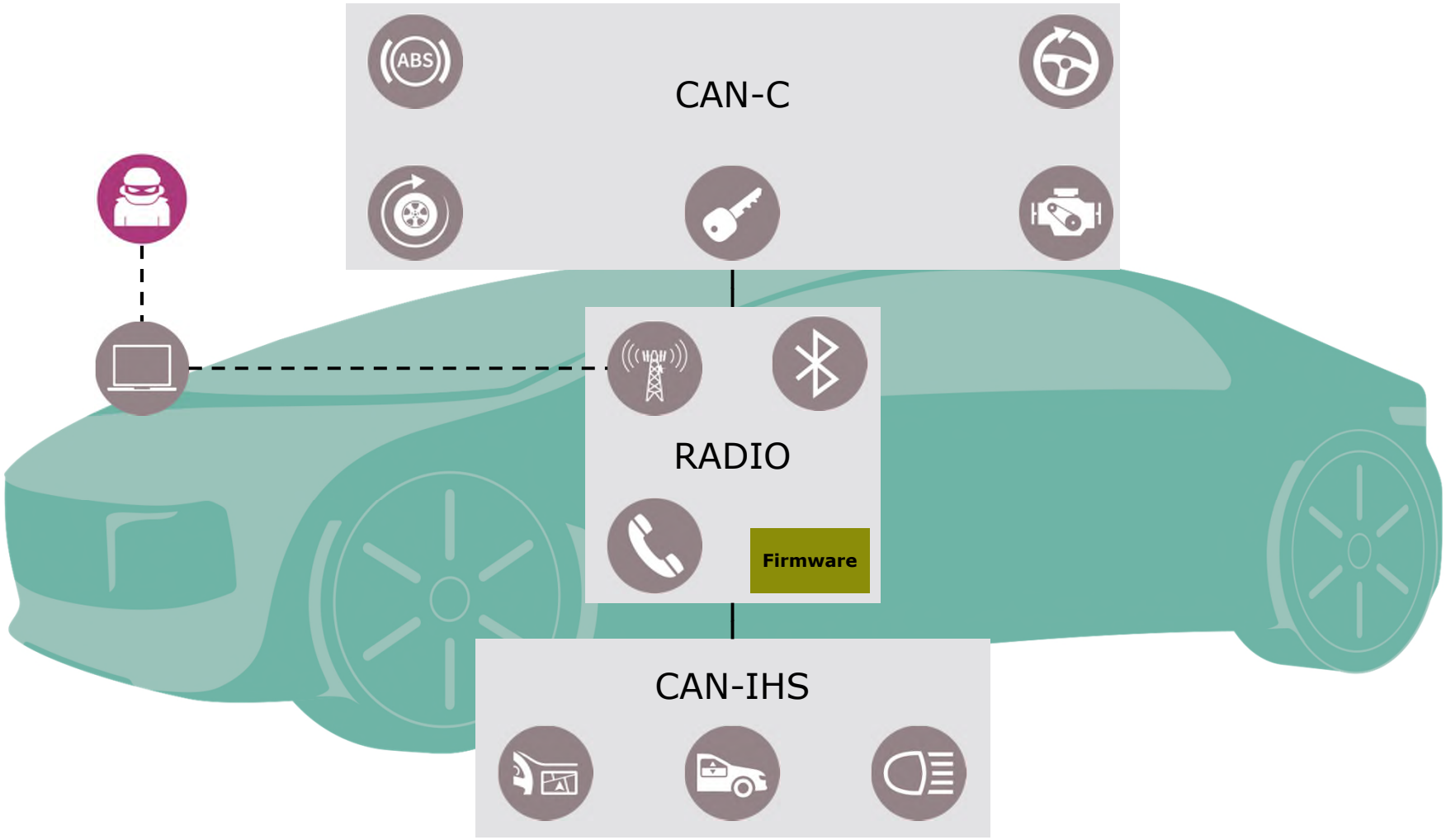
06.12.16

Conference 2016

Agenda

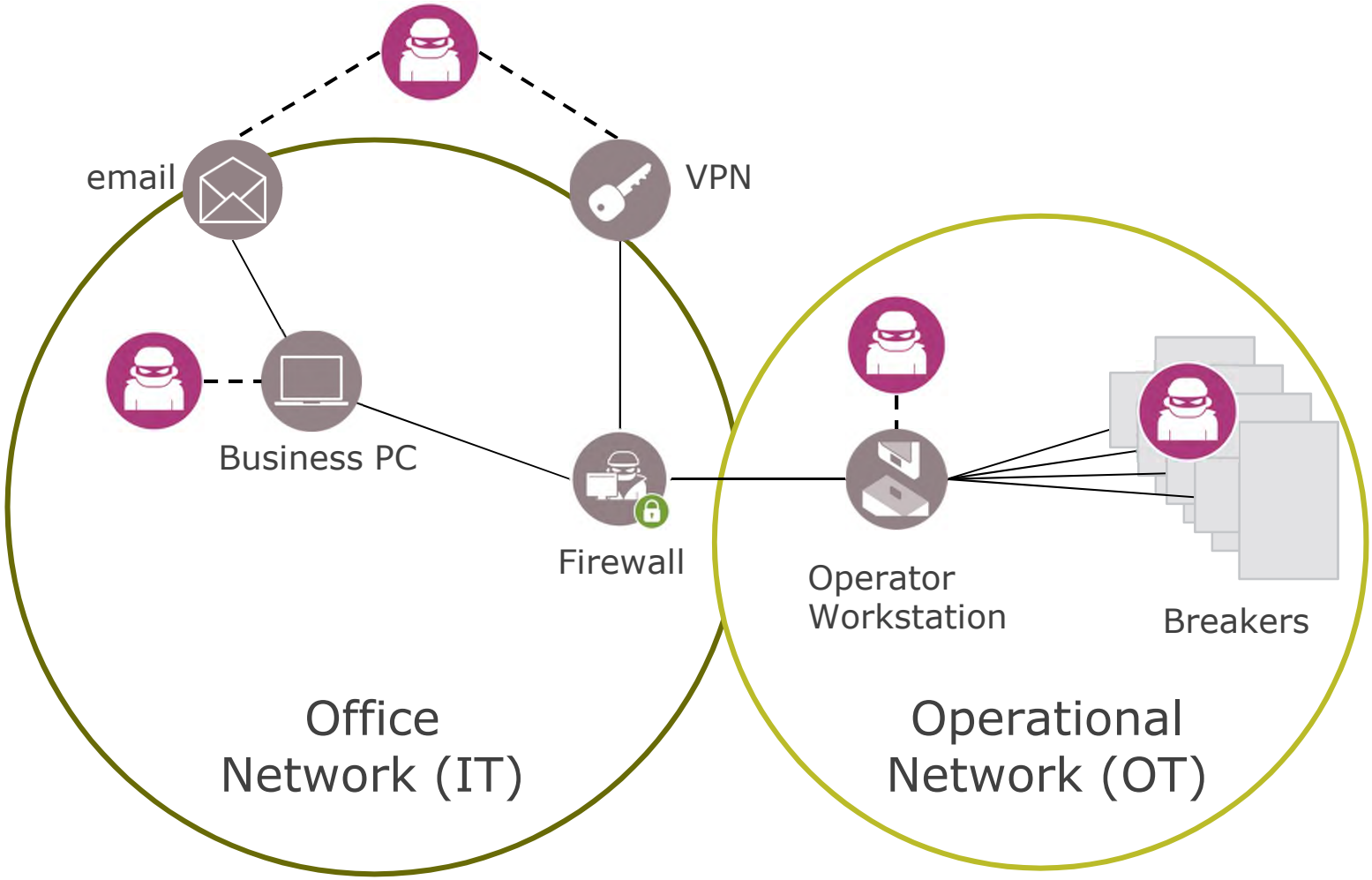
1. Firmware Attacks
2. Countermeasures
3. Reference Designs

Jeep Cherokee



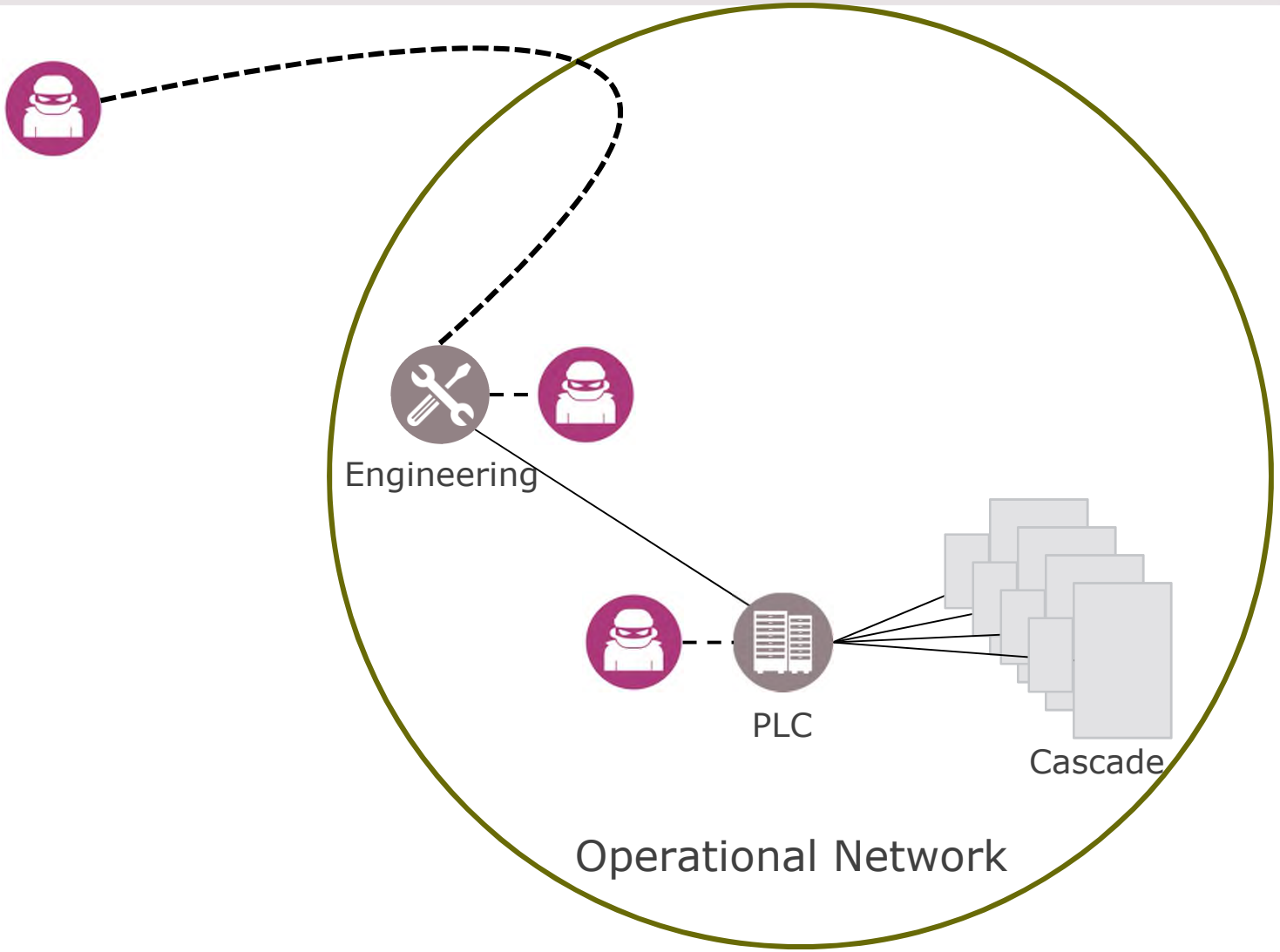
Source: Remote Exploitation of an Unaltered Passenger Vehicle, Miller & Valasek, 2015. http://illmatics.com/Remote%20Car%20Hacking.pdf

Ukrainian Power Grid



Source: Analysis of the Cyber Attack on the Ukrainian Power Grid, SANS & E-ISAC, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.p

Stuxnet



Source: To Kill a Centrifuge, Langner, 2013. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

Recent U.S. Government communications

- Congressional Testimony of James Clapper, Dir Nat Intel, 2015-09-10
  - "Unknown Russian actors successfully compromised the product supply chains of at least three Indl Control System vendors so that customers downloaded malicious software ("malware") designed to facilitate exploitation directly from the vendors' websites along with legitimate software updates, according to private sector cyber security experts."

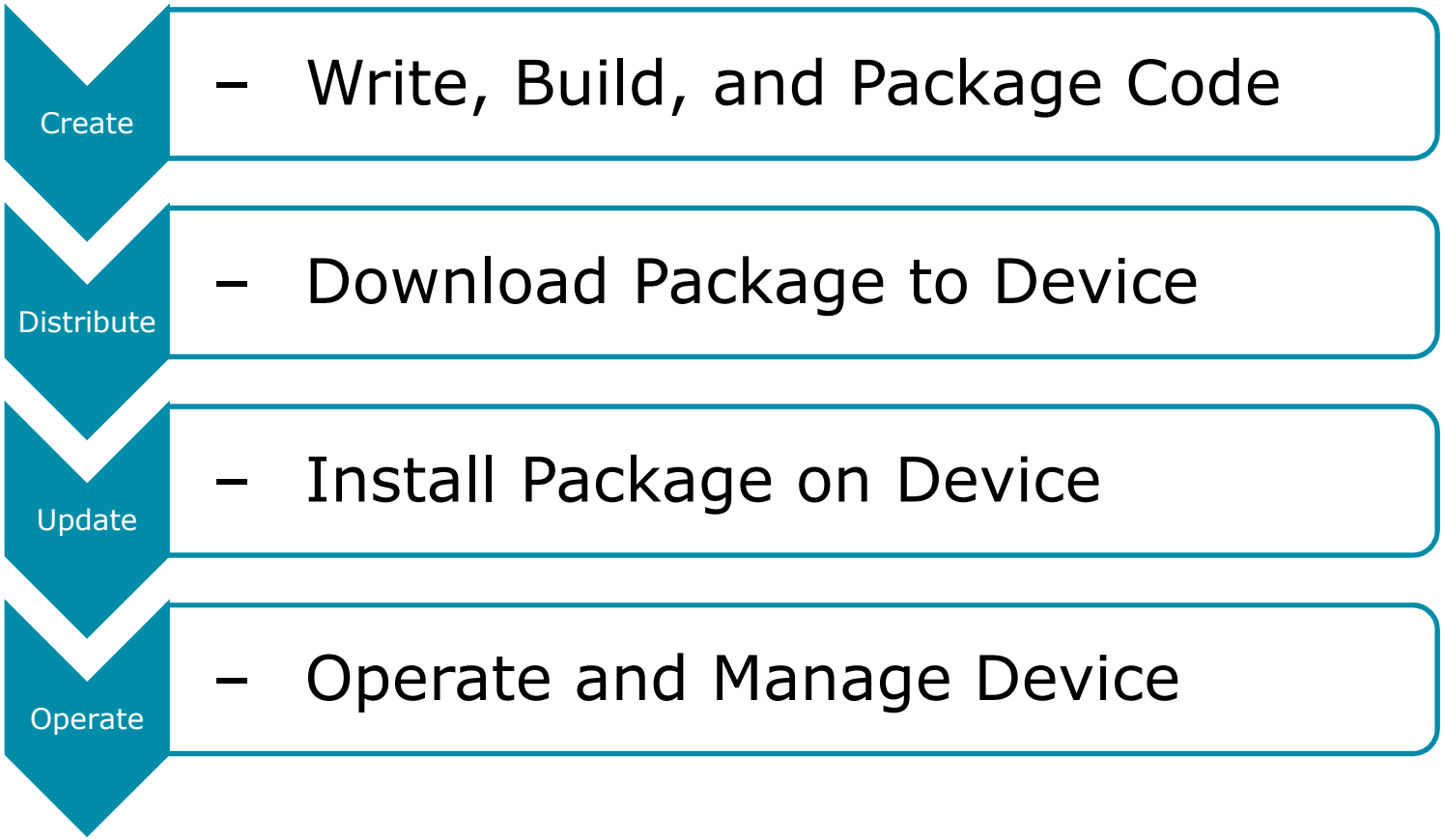
- Federal Energy Regulatory Commission : Final Rule 829
  - NERC must develop a Reliability Standard that addresses Software Integrity and Authentication

- National Telecommunications and Information Administration
  - NTIA convening multi-stakeholder process on Internet of Things Security Upgradability and Patching

Agenda

1. Firmware Attacks
2. Countermeasures
3. Reference Designs

Firmware Upgrade Process



Types of Firmware Attacks

- Attacks on Create Step
  - Steal code signing key
  - Get access to code signing process, sign bad firmware
  - Introduce vulnerabilities or malware into firmware before signing
- Attacks on Distribute Step
  - Substitute bad or old firmware during distribution
  - Block distribution of updates
- Attacks on Update Step
  - Exploit vulnerability in firmware update process
- Attacks on Operate Step
  - Find vulnerability and develop exploit
  - Escalate privilege, rewrite firmware

Attacks and Countermeasures

- **Attacks on Create Step**
  - Steal code signing key
  - Get access to code signing process, sign bad firmware
  - Introduce vulnerabilities or malware into firmware before signing

Secure Creation

- **Attacks on Distribute Step**
  - Substitute bad or old firmware during distribution
  - Block distribution of updates

Secure Distribution

- **Attacks on Update Step**
  - Exploit vulnerability in firmware update process

Secure Update

- **Attacks on Operate Step**
  - Find vulnerability and develop exploit
  - Escalate privilege, rewrite firmware
  - Inject malicious firmware via tampering

Secure Operations

Our Focus

Agenda

1. Firmware Attacks
2. Countermeasures
3. Reference Designs

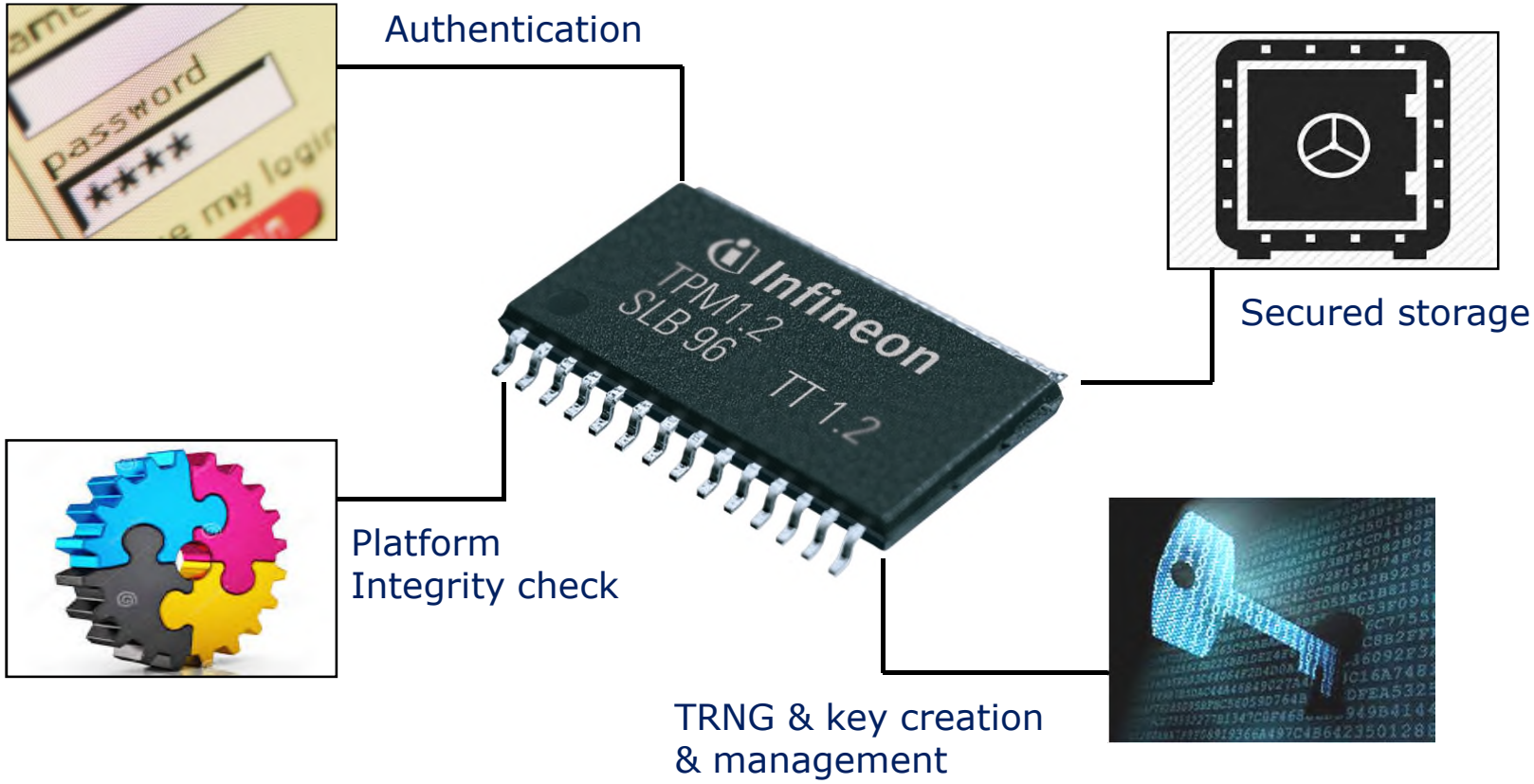
Countermeasures for Operate Step attacks

- **Find vulnerability and develop exploit**
  - Employ secure development process to reduce vulnerabilities
  - Restrict access to firmware source and object code to prevent finding vulnerabilities
  - Use **measured boot** to detect firmware with known vulnerabilities & trigger update
- **Escalate privilege, rewrite firmware**
  - Restrict upgrades to RTU (Root of Trust for Upgrade)
  - Use **secure boot** to prevent execution of unauthorized firmware
- **Inject malicious or obsolete firmware via tampering**
  - Use **secure boot** to prevent execution of unauthorized firmware
  - Use **measured boot** to detect obsolete firmware & trigger update

Trusted Platform Module (TPM)

- The **Trusted Platform Module (TPM):**
  - is a secure microprocessor that is designed to **add hardware security** to any system
  - is based on a standard written by the **Trusted Computing Group (TCG)**, an international industry standardization group
  - is currently available based on two different standardized specifications – **TPM 1.2** and **TPM 2.0** (the most recent one)
  - Specified pin outs with **I²C, LPC or SPI** interfaces
    - available in **VQFN-32 or TSSOP-28** package and **Ext Temp** Ranges

How can TPM protect your computer?



Making computers so secure even your BIGGEST SECRETS are SAFE

Infineon OPTIGA™ TPM SLB 96xx
TPM v1.2 and 2.0 Certified Platform Protection

Trusted Platform Module: Secure your Software and Data

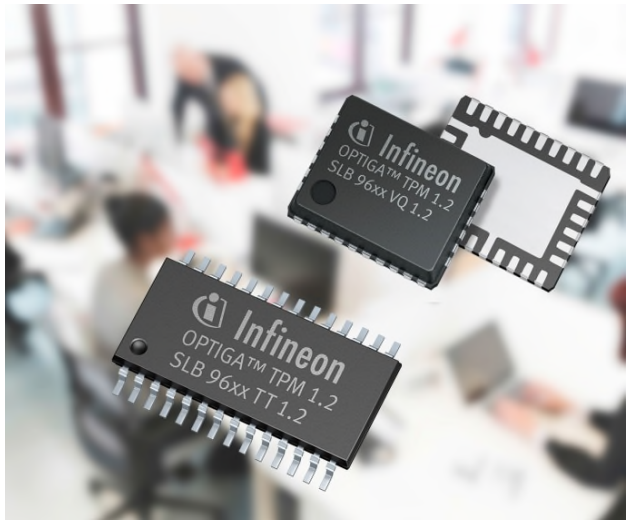
- Strong Authentication of Platform and Users
  - **Unique embedded Endorsement Certificate**
- Secure Storage and Management of Keys and Data
- Platform protection for embedded systems
  - **Measured/Trusted Boot**
  - TRNG, Tick-Counter, Dictionary Attack Lock-out
- Built-in algorithms including RSA, ECC, SHA-256
- Industrial Temp range working

Certified & Standardized Security

- Official TPM product listed at Trusted Computing Group (TCG)
- Security evaluated and certified to Common Criteria EAL4+

Infineon OPTIGA™ TPM products

Product	TPM	Domain
SLB9645	TPM 1.2	I2C: ARM/non-x86 architectures
SLB9670	TPM 1.2 / TPM2.0	SPI: Intel/ARM architectures
SLB9660	TPM 1.2	LPC: Intel/x86 architectures
SLB9665	TPM 2.0	



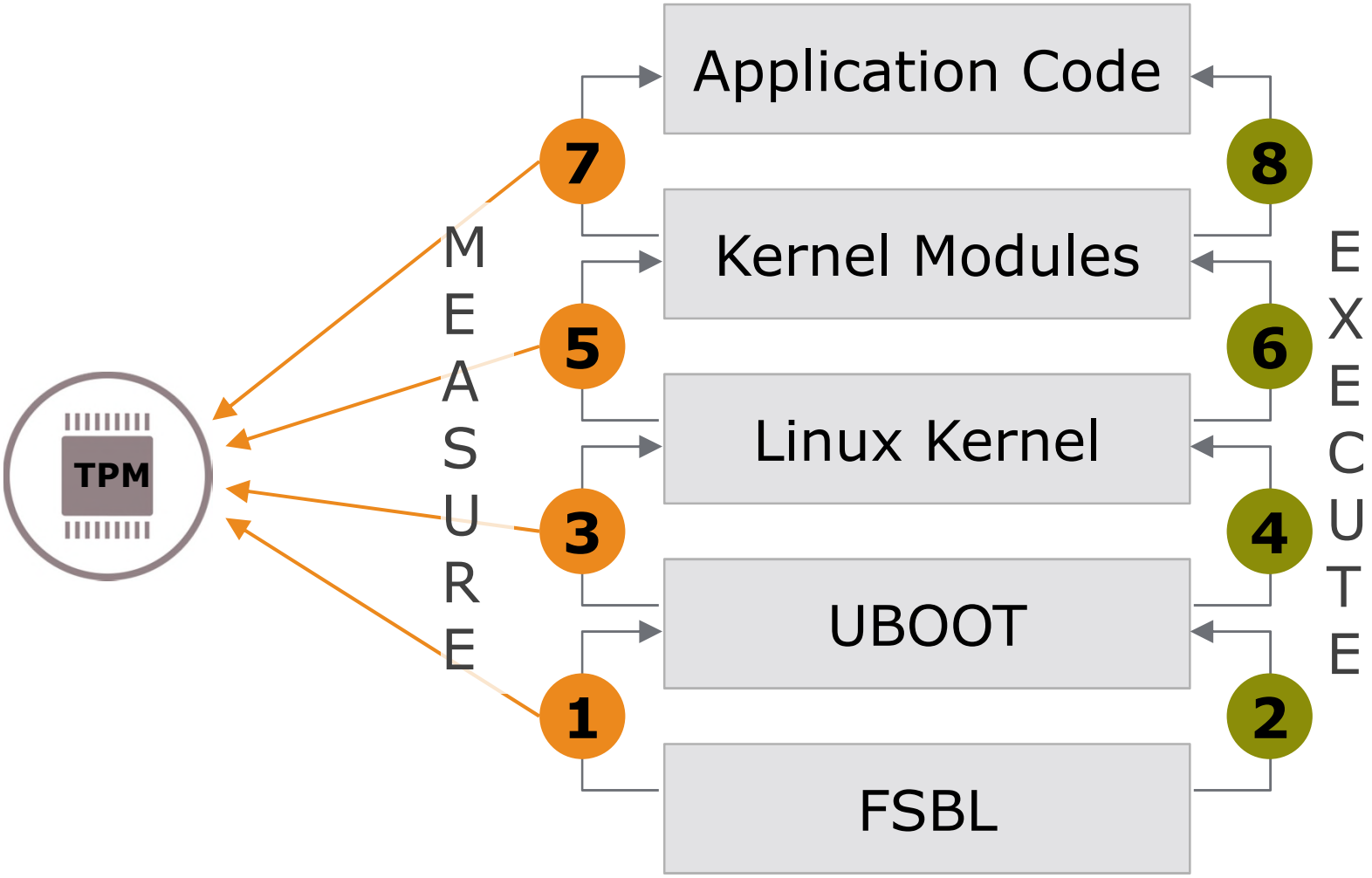
Applications:

- Embedded Devices
  - Industrial, Medical, Networking, Transport, Gaming etc.
- PC and Mobile Computing
- Intel x86, ARM platforms and others

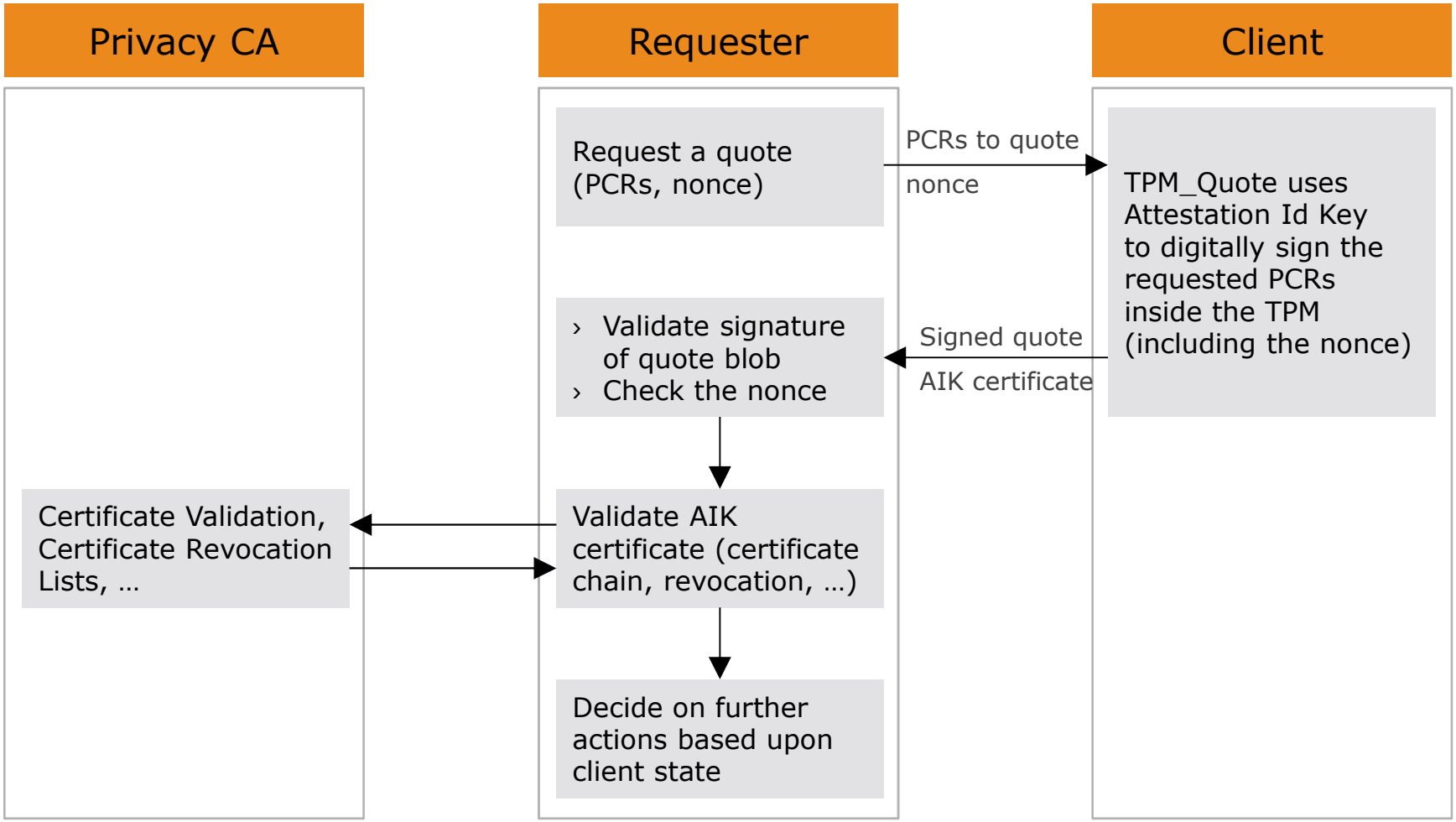
More Info:

www.infineon.com/tpm
www.trustedcomputinggroup.org

Measured Boot



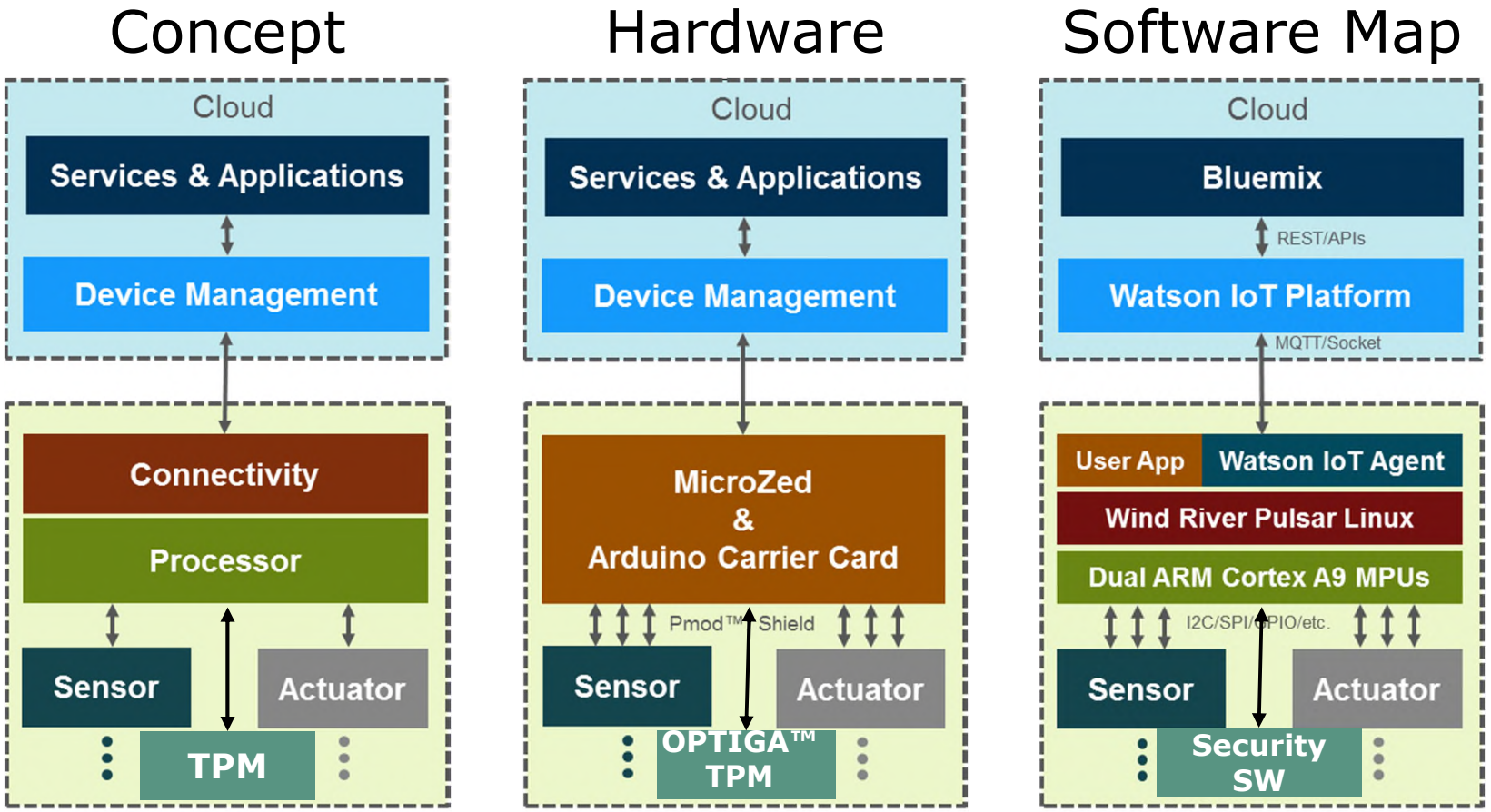
Remote Attestation



Agenda

1. Firmware Attacks
2. Countermeasures
3. Reference Designs

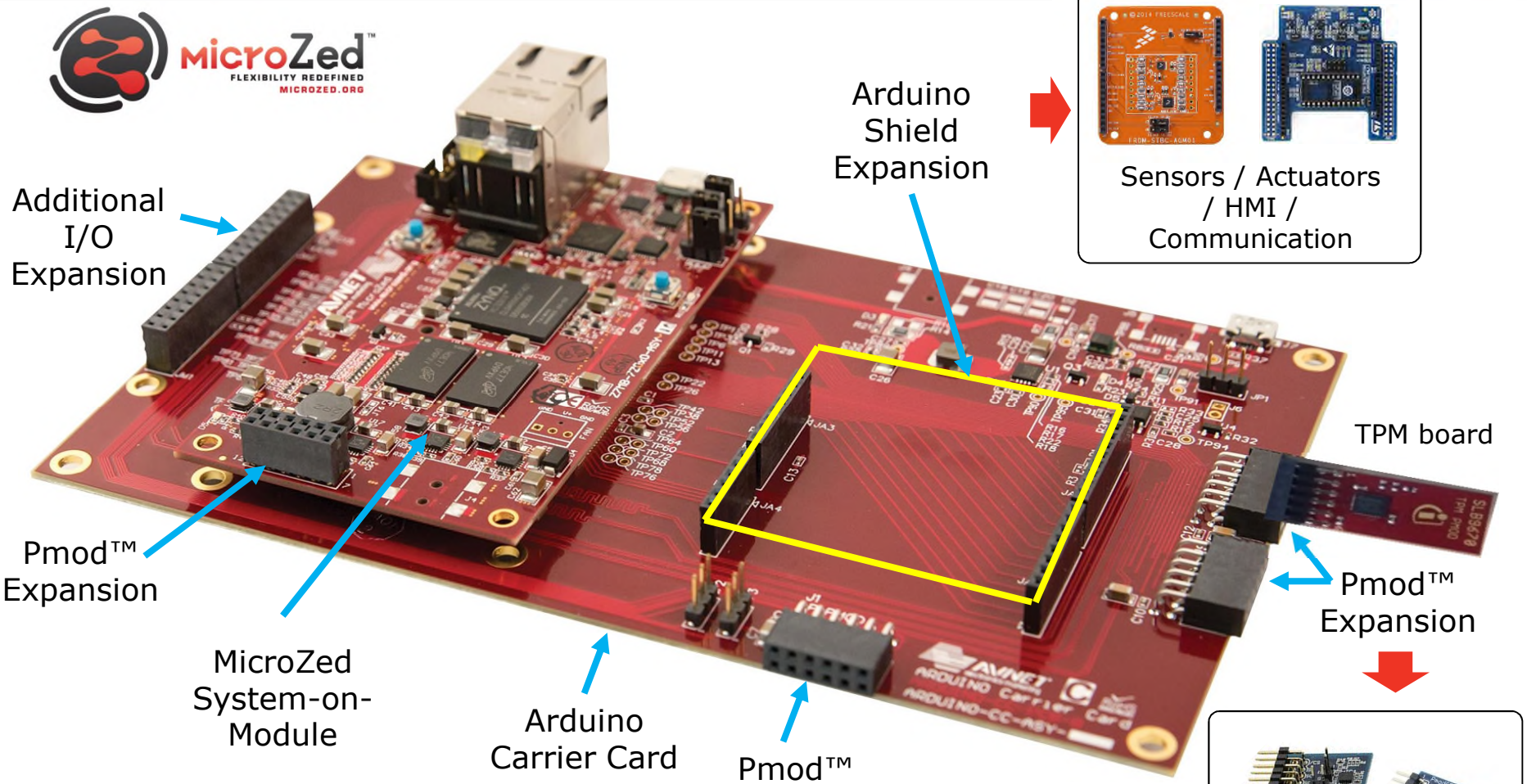
Anatomy of an Industrial IoT Platform



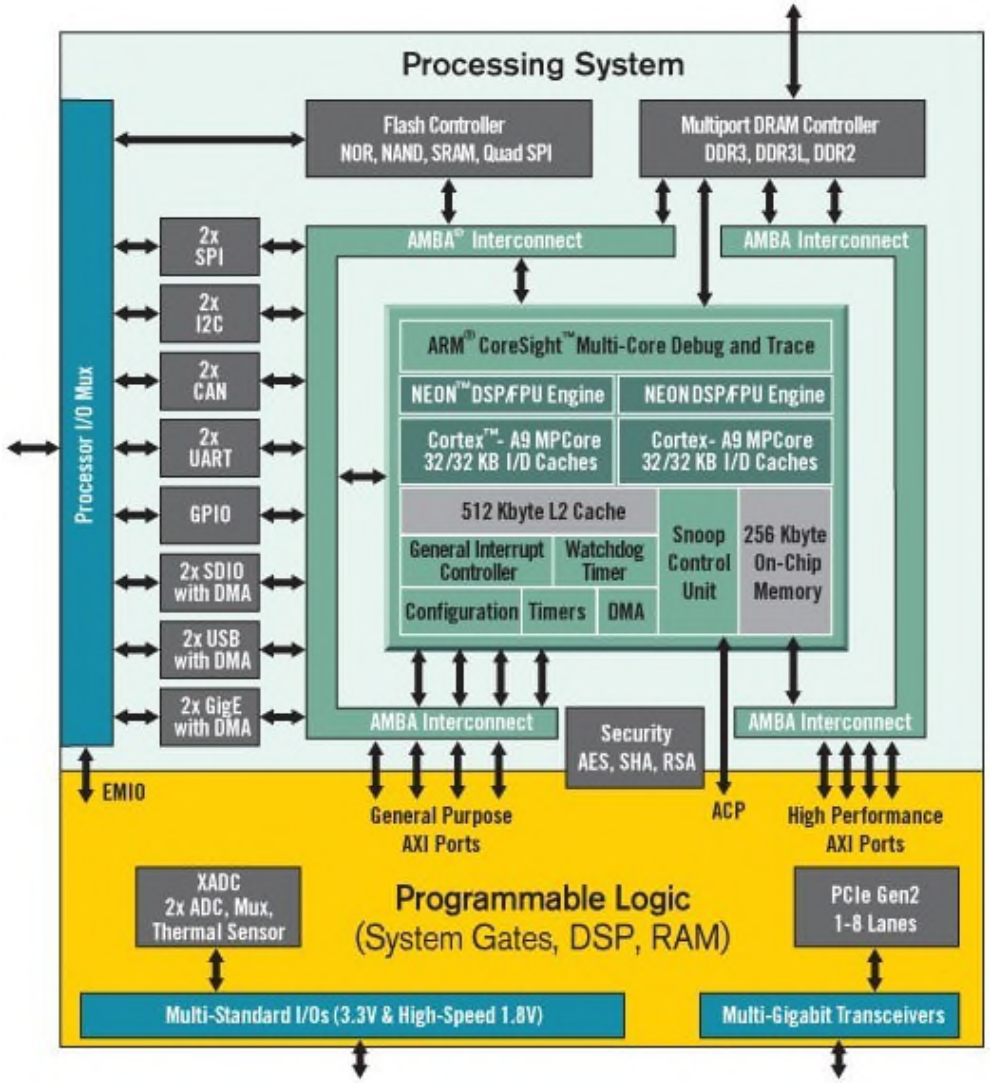
Security Software Stack

StrongSWAN Client
TrouSerS
Wind River Linux Kernel with TPM Driver
UBOOT
FSBL
BootROM

Avnet's Industrial IoT Starter Platform



Why Zynq?



Xilinx's Zynq-7000 SoC offers an industrial IoT platform

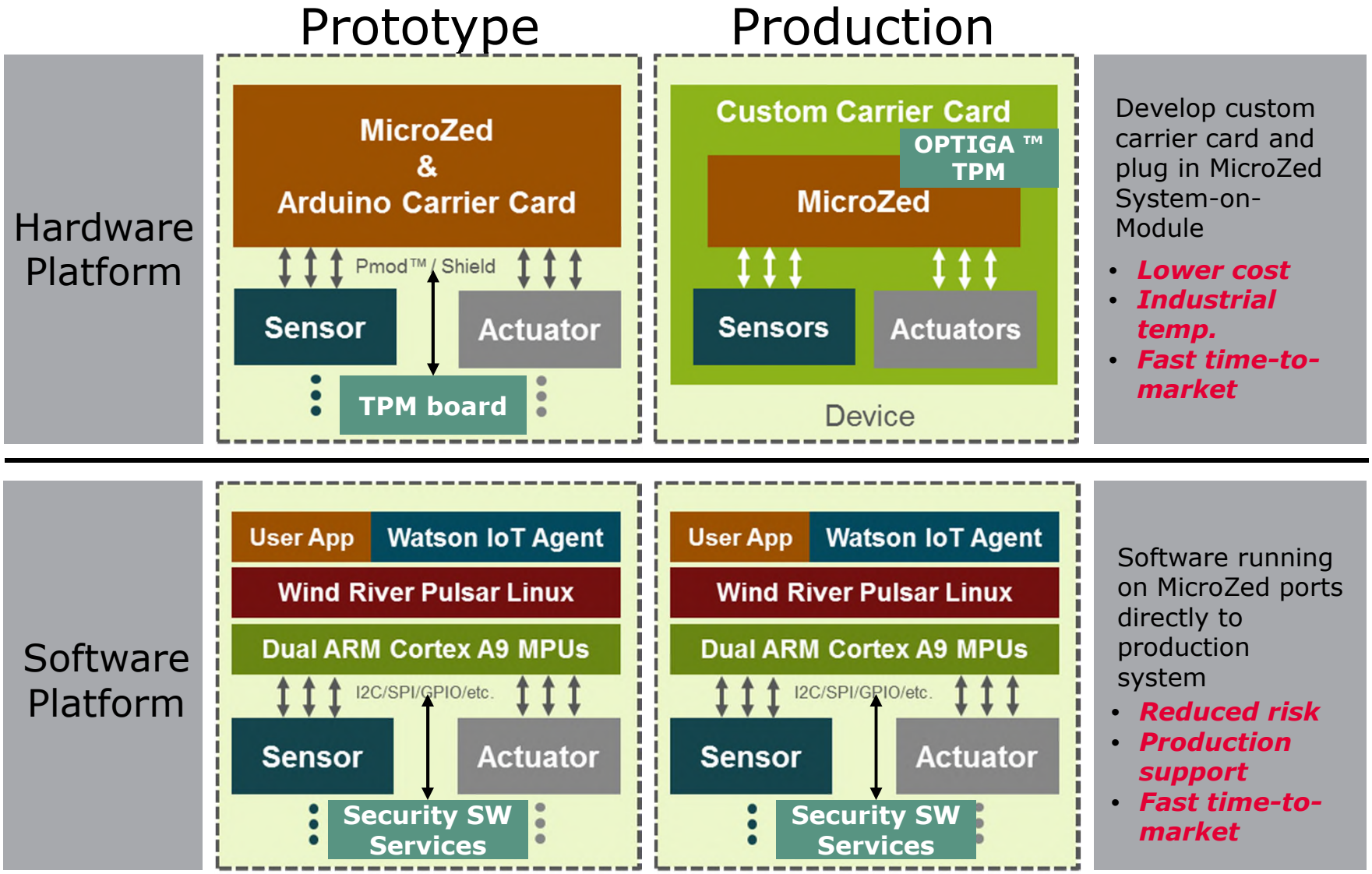
Processing System

High-performance ARM MPU architecture
Standard peripherals
Gigabit Ethernet
I2C, SPI, USB, CAN, UART, SDIO
Security
RSA, AES, and SHA,
ARM® TrustZone®

Programmable Logic

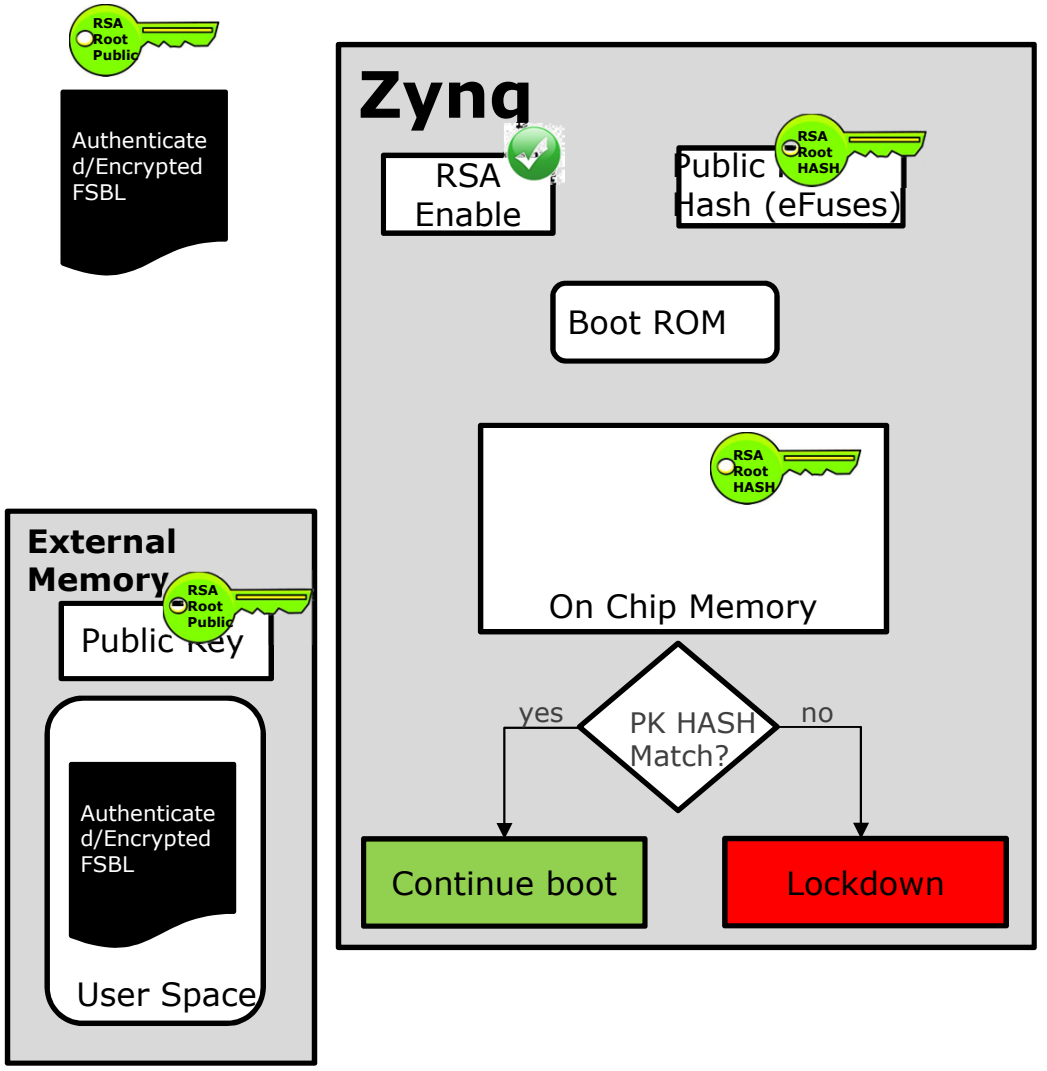
Flexible custom sensor interfaces
High-performance custom accelerators
Scalable logic density

Easy Transition from Prototype to Production



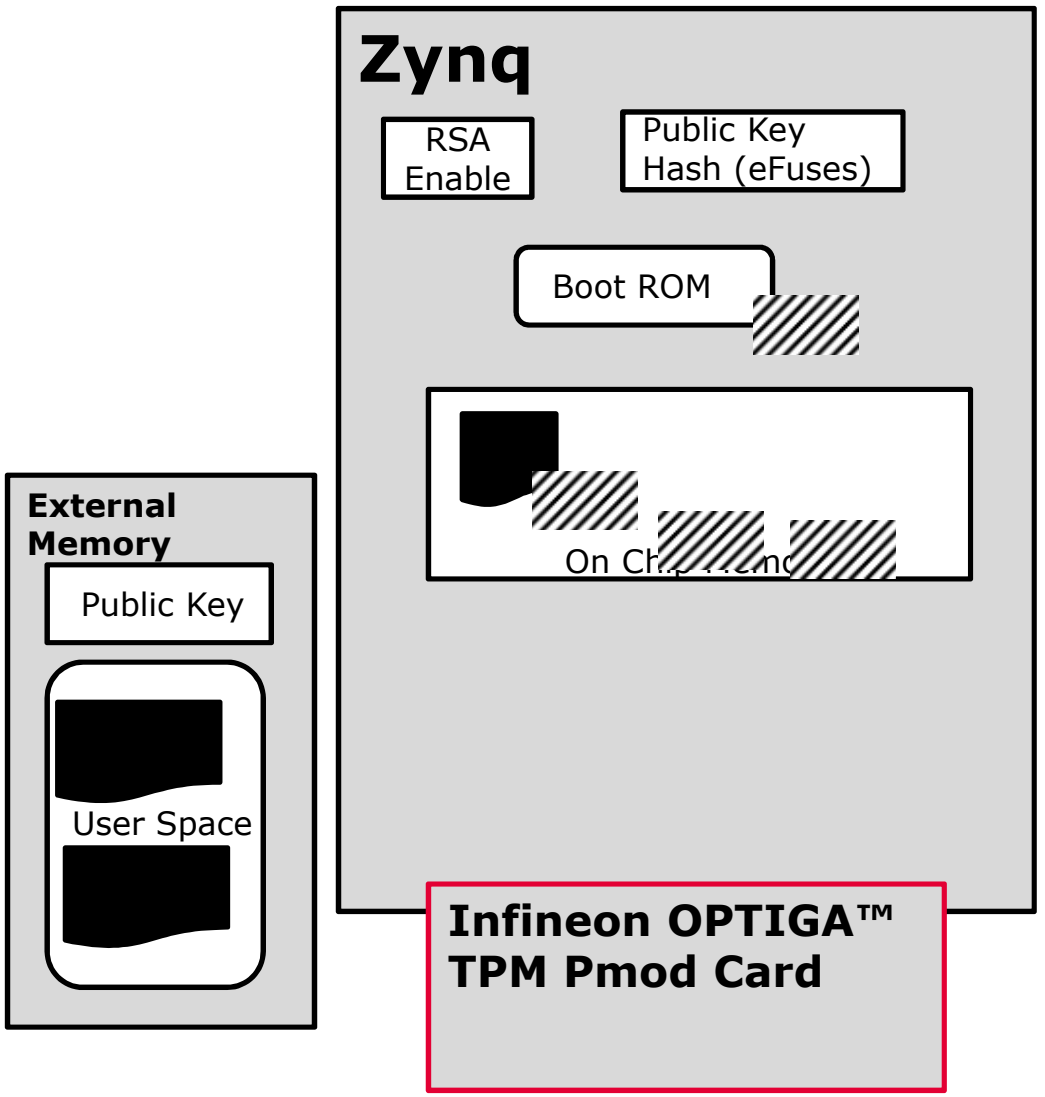
Existing Zynq-7000 SoC HW Root of Trust Boot

- Step 1: Provision Device Before
  - Load your RSA-2048 public key HASH into device
  - Load your public key into Flash
  - Load your signed FSBL into Flash
  - Turn On Root of Trust Boot
- Step 2: Field System
- Step 3: Apply Power, ROM Boots
  - Device loads public key from Flash into OCM
  - Device calculates HASH of public key
  - Device compares calculated HASH vs stored HASH
    - If Successful – load, authenticate/decrypt and execute FSBL
    - If failure – go into Secure Lockdown and notify system

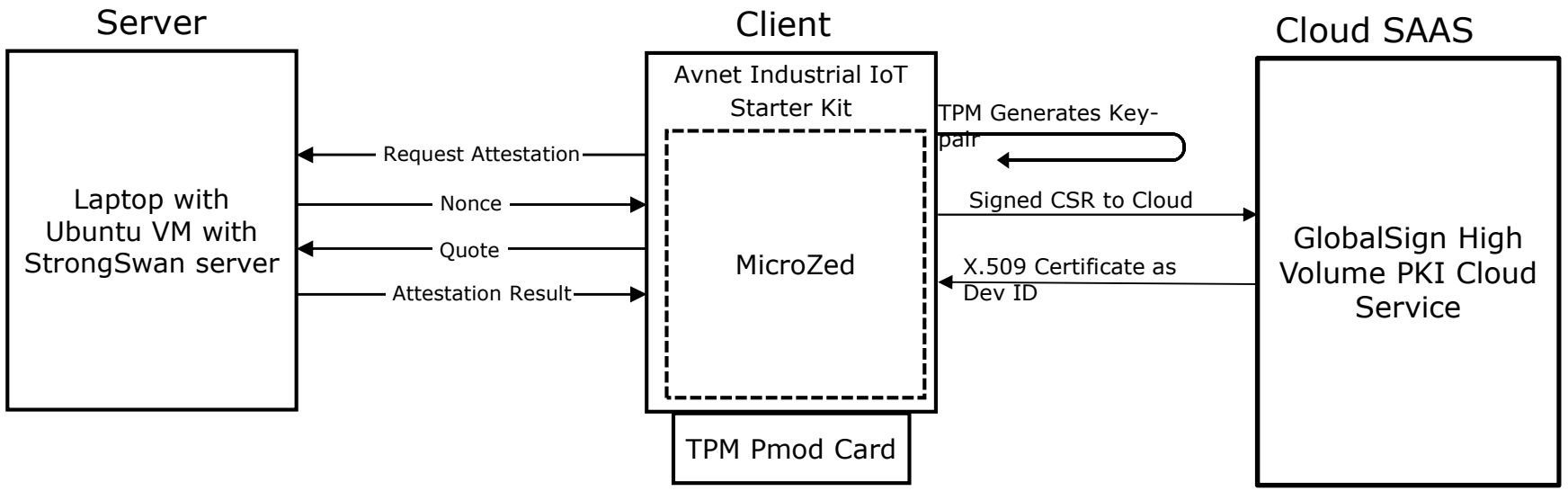


New Measured Boot Capability with TPM

- Step 4: First Stage Boot Loader Measures and Extends Boot ROM and FSBL
  - Hash code
  - Send hash to TPM with Extend command
- Step 5: FSBL Hashes, Extends, and Runs Universal BOOT loader
  - Hash code
  - Send hash to TPM with Extend command
  - Run code
  - Decryption and authentication is optional here – up to the customer
- Step 6: Boot Sequence Continues
  - Each Stage Hashes, Extends, and Runs the Next
  - Decryption and authentication is optional here – up to the customer



Adding Remote Identity Provisioning



Agenda

1. Firmware Attacks
2. Countermeasures
3. Reference Designs - 2

Enhancing Smart Building Security

- Industrial buildings rely on networks for control and physical security
- Attackers may attempt to attach fake subsystems e.g. cameras to facilitate theft.
- Networks need to ensure node integrity.

Enhanced secure building security

Raspberry Pi based Camera

Cisco Router CGR 1120

Demo built by Cisco, Infineon and Intel,

With the Assistance of HSR University of Applied Sciences, Rapperswil

Cisco UCS 240 Server

Authentication Flow Between Camera & Router

Raspberry Pi Camera

Cisco CGR 1120

1. Start Session?

2. Who are you? Can I trust you?

3. Here is my identity and TPM-signed integrity information

4. Verify identity and integrity (done locally)

5. Session authorized

6. Open SSL session to Server through CGR

Authentication of Server & Router

Cisco CGR 1120

Cisco UCS 240 Server

1. Start Session?

2. Who are you? Can I trust you? Here are my credentials

3. Verify identity and integrity (done locally)

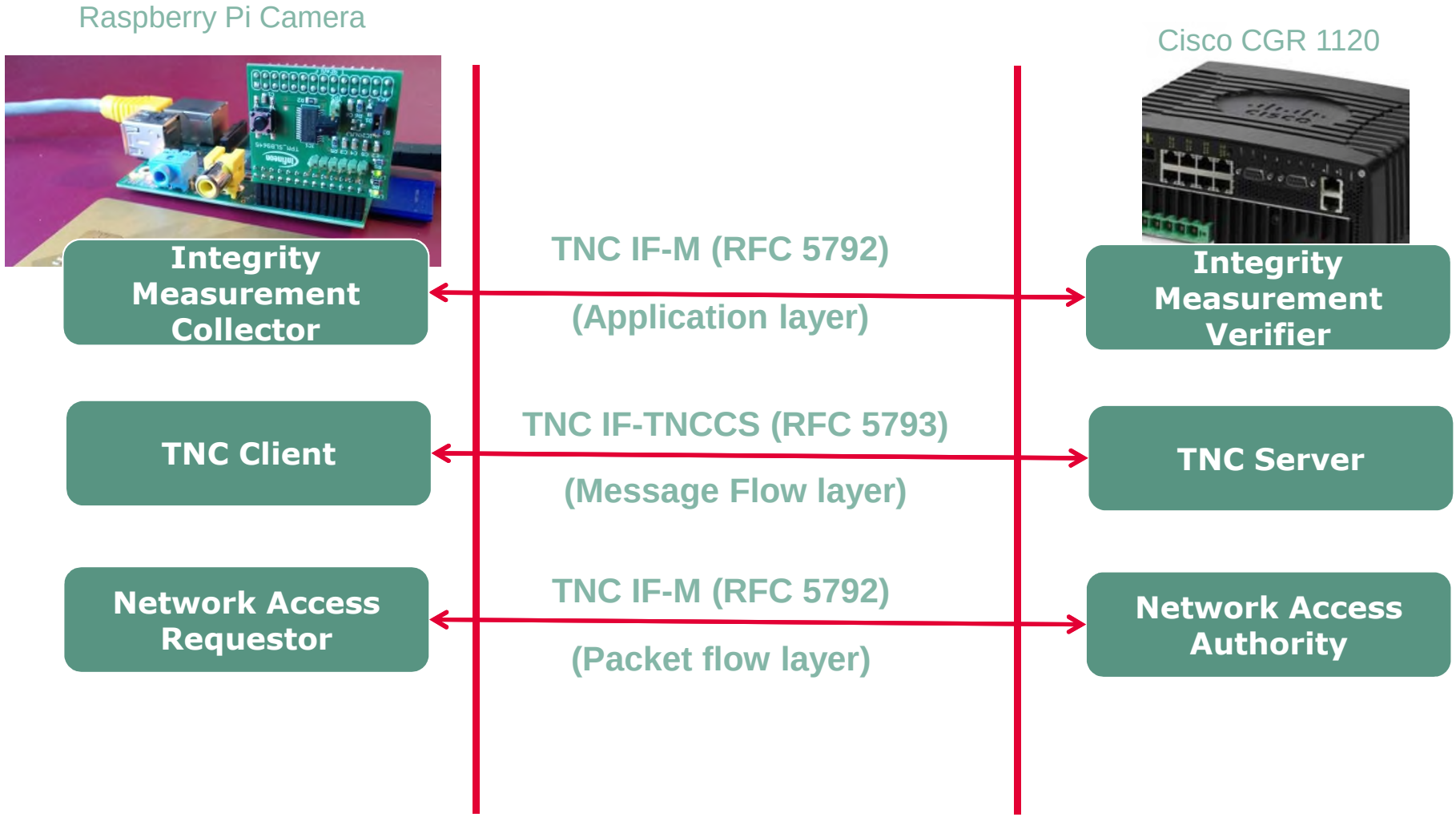
3. Verify identity and integrity (done locally)

4. Session authorized

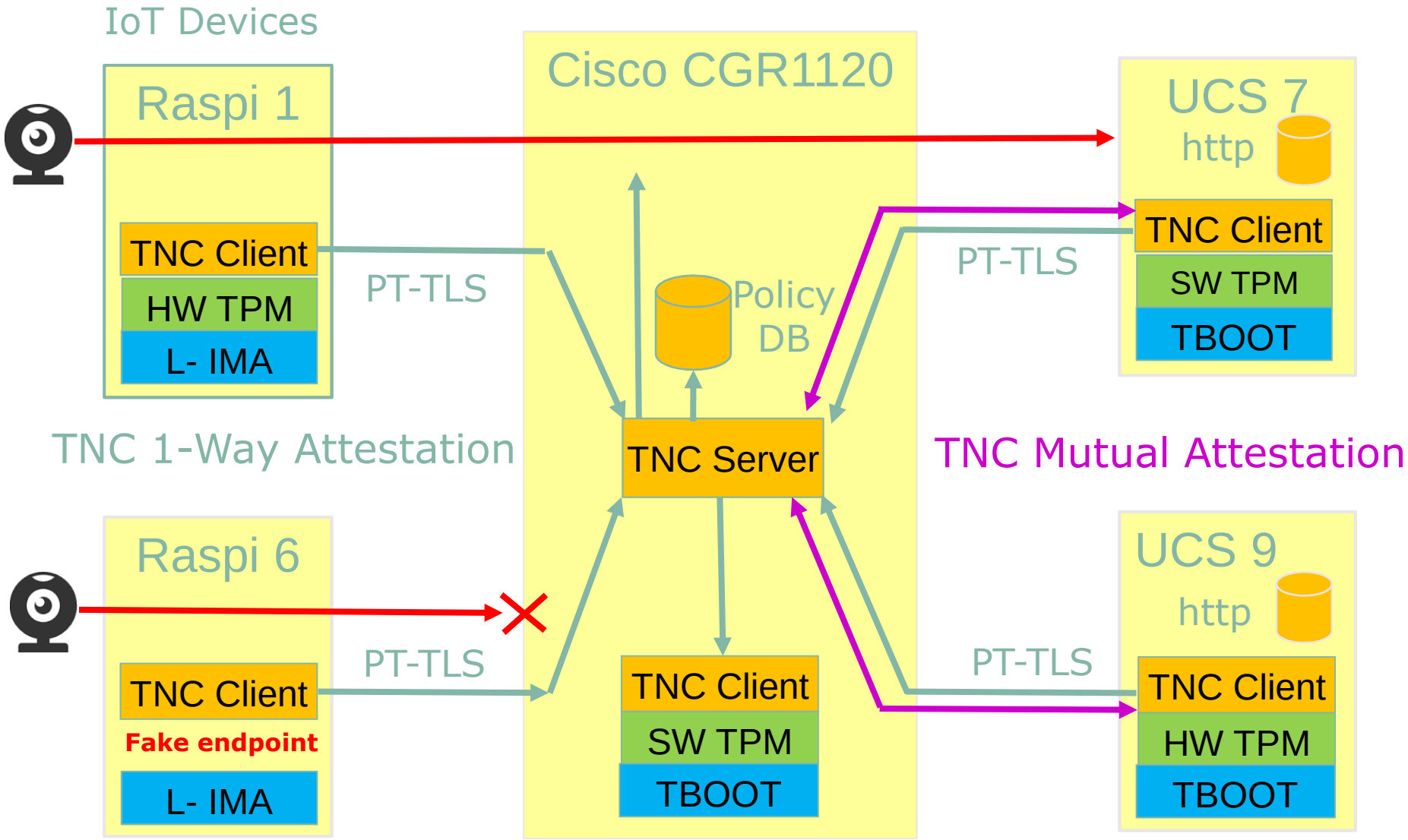
4. Session authorized

5. Open SSL session to rPi through CGR

Authentication Architecture for Trusted Network Connect



Secure Network Topology



Protecting Your Industrial IOT Systems

- Add a TPM to your design
  - Measured Boot
  - Remote Attestation
  - Strong Authentication
  - True RNG
  - Sealing
  - Tamper Resistance
- Use Measured Boot and Remote Attestation to manage firmware versions
  - See NIST SP 800-155 for details
- For more information visit www.infineon.com/tpm

Our IoT Security Portfolio
The Right Security for your IoT design

Embedded security	Secured connectivity	User identification
› OPTIGA™ product family - **security** products for **Embedded Systems** › **Tailored, scalable**, and **easy to implement** security for IoT, ranging from basic authentication products to advanced implementations	› Security controllers with increased **lifetime**, mechanical **robustness** and **extended temperature** range › Ideal for embedded SIM cards in **industrial M2M** and **Automotive** applications	› Enabling User-friendly two-factor authentication according to **new FIDO 1.0** specifications › **Boosted NFC SE** secured NFC experience for SIM, MicroSD™ or wearables
› OPTIGA™ TPM › OPTIGA™ Trust Family › For Programmable & Turnkey designs	› M2M Industrial: SLM 76 and SLM 97 SOLID FLASH™ Families › M2M Automotive: SLI 76 and SLI 97 SOLID FLASH™ Families	› Embedded Secure Element › Boosted NFC › FIDO › USB Tokens
		

www.infineon.com/iot-security

Part of your life. Part of tomorrow.

infineon