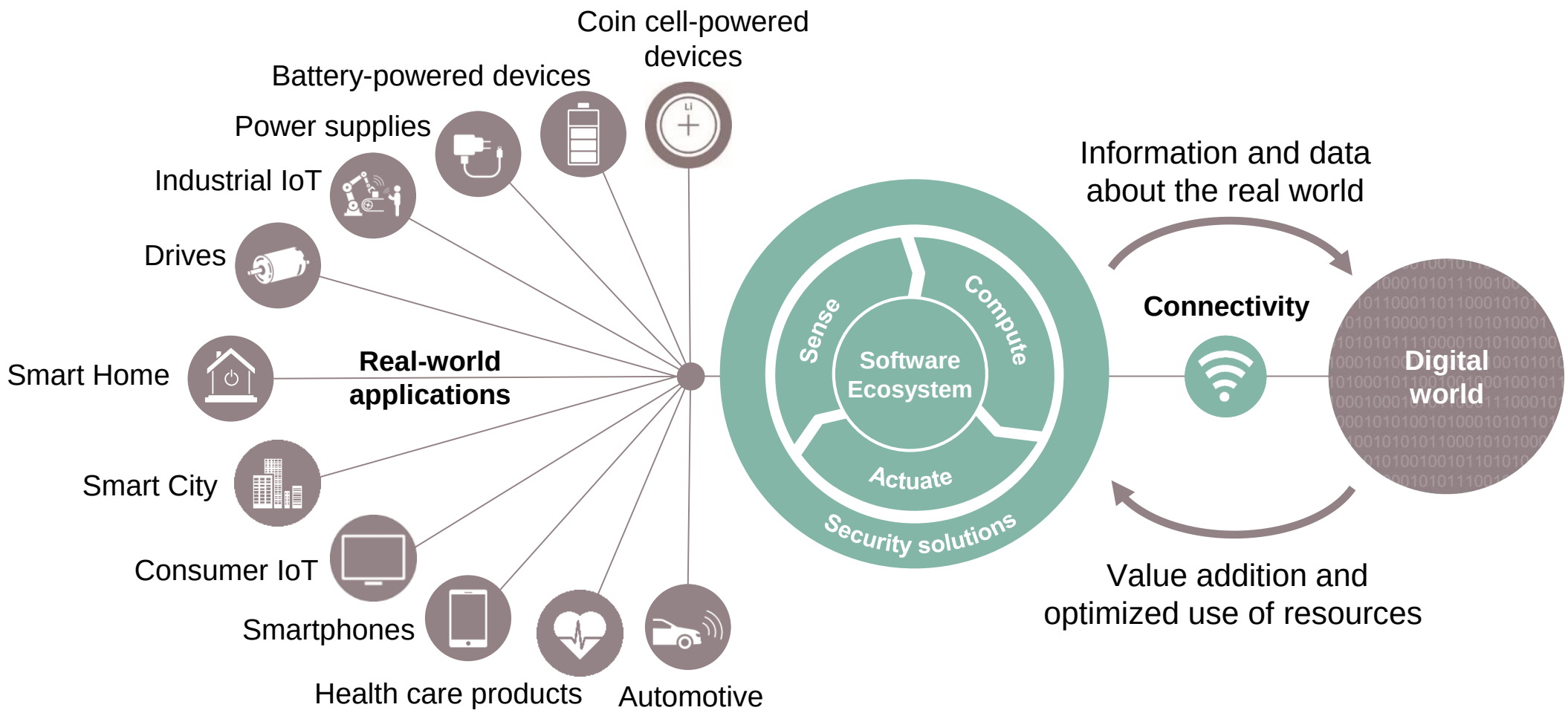
Update on Infineon’s IoT Solutions with focus on embedded security

March 2022

Agenda

Agenda

Infineon offers a unique portfolio that links the real and the digital world



Sense: sensors Compute: microcontrollers, memories Actuate: power semiconductors Connectivity: Wi-Fi, Bluetooth, USB

CSS IoT Systems – Our Core Capabilities mapped to products

COMPUTE

- Arm® Cortex® Processors
- Mixed Signal MCU Architectures
- Application Co-processors

PSoC®4
PSoC®6
XMC™1000
XMC™4000

SECURE

- Device authentication
- embedded SIM
- Hardware security controllers

OPTIGA™
- Trust, TPM
- Connect
- Authenticate

ENHANCE

- Graphics
- Machine Learning
- NFC

PSoC®6
Next gen MCU
My-d™ NFC (SCS)

CONNECT

- Wi-Fi / BT Combo
- BT / BLE

AIROC™
- CYW43/55xxx
- CYW20xxx, PSoC®4/6-BLE

CONTROL

- Capacitive / Inductive Sense
- Wireless Charging
- Motor Control
- Power Conversion

PSoC®4
PSoC®6

XMC™1000 (Spark)

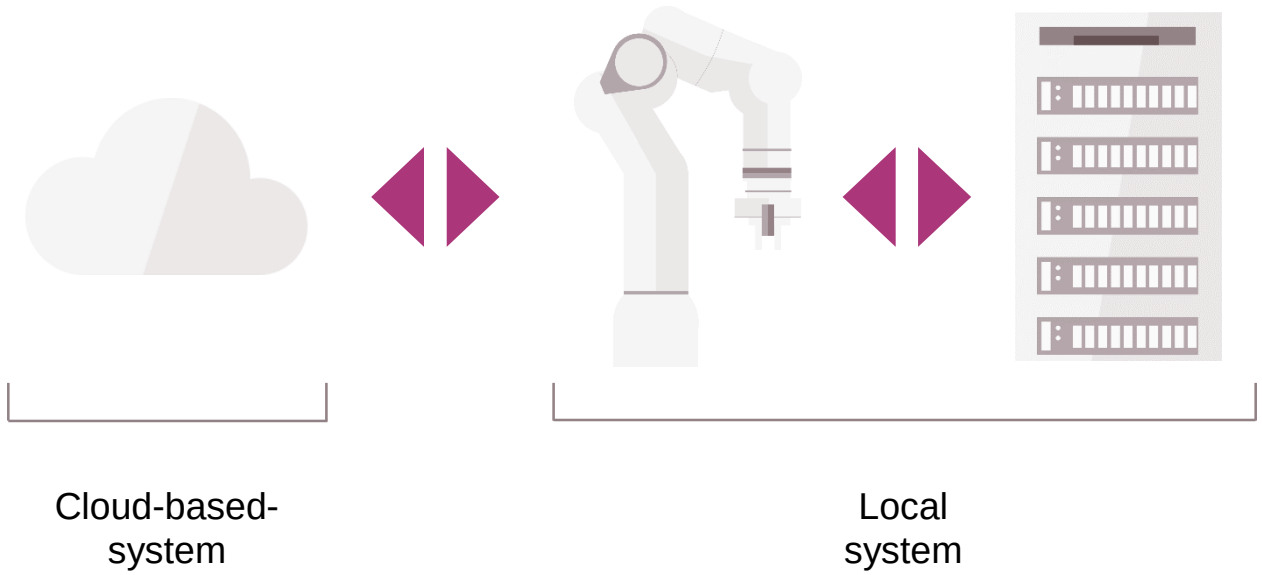
XMC™1000
XMC™4000

Agenda

Find suitable security

Connecting local systems to the cloud enables new technical possibilities and business models, but it also makes devices more prone to attacks

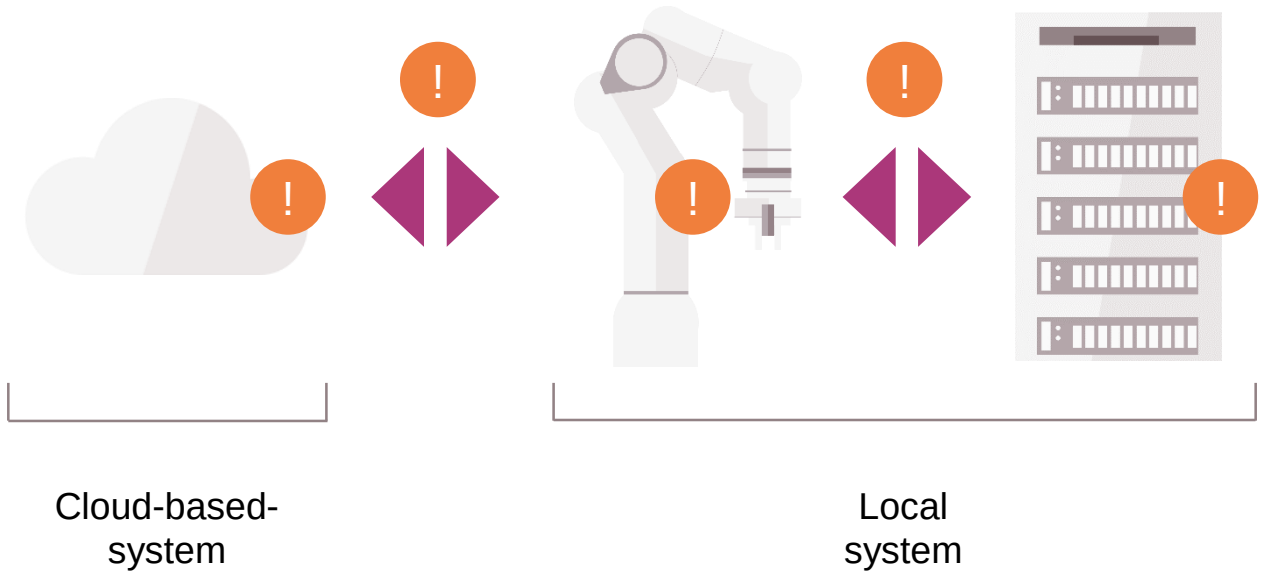
Industry



- Data analytics
- Predictive maintenance
- Remote access

Connecting local systems to the cloud enables new technical possibilities and business models, but it also makes devices more prone to attacks

Industry



Logical attacks

Typically, can be performed remotely with low-cost equipment

Access by attackers:
Normal interfaces used to communicate in an unexpected way to the device

Methods of attackers:
Confusing the communication protocol, sending too many data to overflow the communication buffers and others

Goal of attackers:
To inject wrong information (compromise the integrity) or to get secrets out (break confidentiality)

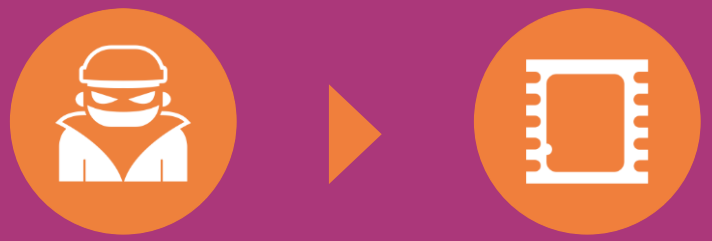
Physical attacks

Typically, physical access to the device is needed

Observative attacks:
Monitoring the behavior of the device, such as its power consumption, to break confidentiality and get secrets out

Semi-Invasive attacks:
Introducing faults in the device to change data or program flow and thereby compromise the integrity such as stored information

Manipulative attacks:
Modification of the silicon of the device to inject wrong information (compromise the integrity) or to get secrets out (break confidentiality)



Countermeasures for reaching high security

Logical attacks

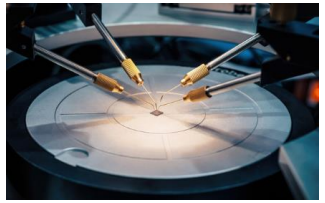
Physical attacks

Logical attacks
e.g. protocol fuzzing, jamming, replay, …

Observative attacks
e.g. side-channel attacks, SPA, DPA, Spectre, Meltdown

Semi-invasive attacks
e.g. spiking, radiation, light attacks, clock manipulation, DFA

Manipulative attacks
e.g. FIB manipulation, micro-probing, …



Countermeasures

PKI, digital signatures, buffer overflow protection, software isolation, time-stamps, encryption, CMAC, blockchain, MISRA C-CERT coding, …

Runtime-invariant operation, randomization, bus and memory encryption, hardened coprocessors, dynamic encryption in computation, …

Error detection codes, redundancy, code-fetching, sensors, semaphore usage, mathematical cross-checks, double computation, …

Synthesized design, passive covering, secured wiring, active shielding, front- and backside sensors, full data path encryption and error detection, …

Countermeasures in Software

Countermeasures in Hardware

The challenge

Every device needs a

MCU*

?

…but when do I need a dedicated

HW-security-anchor?

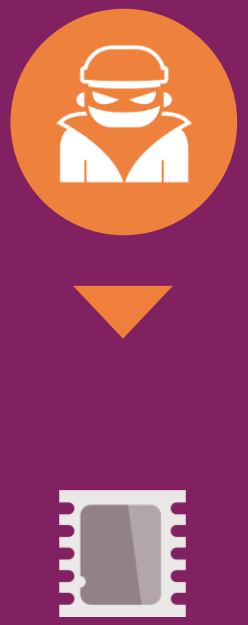
*or Linux based MPU

The concept of scalable security

Summary of truth table and main positioning messages

	Basic Security	Enhanced Security		Highly secured
	Logical/Application level protection. **Security implemented by customers**	RoT, logical protection with off-the-shelf security FW	Strong physical protection with turnkey security use cases	Physical and logical protection against all known attacks based on off-the-shelf security use cases
	PSoC™ 61/62/63	**PSoC™ 64**	**PSoC™ 61/62/63 plus OPTIGA™ Trust M**	**PSoC™ 64 plus OPTIGA™ Trust M**
Customer security expertise	Customer with high security expertise	Customer **Off-the-shelf solution**	Customer **Own logical security FW**	Customer **Off-the-shelf solution**
Security requirements		Need for **logical security:** “logically secure” boot, FW updates & processing isolation using preconfigured security FW	Need for **physical security:** “physically secure” small data assets & security services	Need for **logical security & physical security**
Certification	**No need** to be compliant with security certifications	Requirements to comply with **certifications** (**PSA** – minimum security stamp of approval)	Requirements to comply with **security certifications** (CC) or **regulations** (IEC62443) over time	Requirements to comply with **high security certifications** (PSA, CC) or **regulations** (IEC62443) over time
Personalization (unique ID)	Own provisioning of security relevant assets (no secured supply chain)	Secured provisioning of security relevant assets on backend level	Secured & certified provisioning of security relevant assets on wafer level	Secured & certified provisioning of security relevant assets on wafer level

If at least one of those statements is true for your device, then you need hardware security



Attackers are able to **physically access** your device

Device needs to **protect its secrets** even against the user

No device **individual secrets**

Different segments show different needs for security – it's all about the right level of security

	Basic security	Enhanced security	Highly secured
Consumer electronics	Rice cooker	Door locks	Home gateways
Industry	Sensor modules	Programmable logic controllers (PLC)	Energy meters
Commercial	Displays	Thermostat	Building automation control

Agenda

Microcontroller Product Portfolio

Note: Automotive, AURIX™ for Industrial, iMOTION™ covered separately

8-Bit	32-Bit Arm® Cortex®-M0/M0+	32-Bit Arm Cortex-M3	32-Bit Arm Cortex-M4 / Arm Cortex-M0+	32-bit Arm Cortex-Mx (next generation)

IoT / Consumer

PSoC 6 MCUs for the broad-base of IoT and Consumer applications, bringing best in class low power, connectivity, and security
PSoC 4 delivers unique software-defined peripherals and industry leading capacitive sensing designs

PSoC 3
8051 CPU
67 MHz, 64KB Flash
Up to 19 PAB, 30 PDB, 72 I/Os

PSoC 1
M8C CPU
24 MHz, 32KB Flash
16 PAB, 16 PDB, 64 I/Os

8FX
8-bit RISC MCU
16 MHz, 32–50KB Flash

PSoC 4
Cortex-M0/M0+
48 MHz, 384KB Flash
Up to 13 PAB, 20 PDB, 98 I/Os

FM0+ MCUs
Cortex®-M0+
40 MHz, 512KB Flash, 102 I/Os

XMC1000 MCUs
Cortex®-M0
32-48 MHz, 200KB Flash, 55 I/Os

PSoC 5LP
Cortex-M3
80 MHz, 256KB Flash
20 PAB, 30 PDB, 72 I/Os

FM3 MCUs
Cortex-M3
144 MHz, 1.5MB Flash, 154 I/Os

PSoC 6
150 MHz Cortex-M4/100 MHz M0+
2MB Flash
7 PAB, 56 PDB, 104 I/Os

FM4 MCUs
Cortex-M4
200 MHz, 2MB Flash, 190 I/Os

XMC4000 MCUs
Cortex®-M4
80-144 MHz, 2MB Flash, 119 I/Os
Industrial Comms, Ta 125C

Industrial

XMC™ is a family of high-performance Arm Cortex-M-based
MCUs for industrial applications, with industrial control peripherals and extended temp range
FM is a portfolio of high-performance Arm Cortex-M-based MCUs for industrial and consumer applications

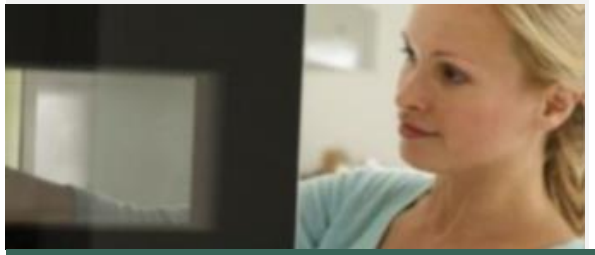
Next Gen IoT MCU
Multi-core Cortex-Mx
ML-Ready, HMI Rich

Industrial Evolution
Multi-core Cortex-Mx
Industrial Quality, ECC Memories

Other

Specialized and Legacy

Industrial Focus: Application and Portfolio Mapping

Home Appliances	Power Conversion and Lighting	Transportation	Factory and Building Automation
			
Applications			
			
Requirements			
› Form factor, size and weight › Family concept › Copy protection › Fast ramp-up	› Energy efficiency › Ease of use › Remote monitoring › Form factors	› Robustness › Functional safety › Reliability & quality › Lifetime	› Connectivity (EtherCAT) › Reliability & quality › Lifetime › Functional safety
PSoC & XMC/iMotion	XMC	XMC	XMC/FM/Aurix

All HMI, IoT, wired/wireless communications subsystems: PSoC4/PSOC6

Consumer/IoT Focus: Application and Portfolio Mapping

Home Automation	Human Machine Interface	Wearables	Battery-Powered Applications	Portable Medical
				
Applications				
				
Requirements				
› HMI: Touch/ Proximity Sensing › Analog/Digital Sensor Interfaces › Connectivity	› CapSense › MagSense › Gestures › Wake-word and Voice commands	› Ultra-Low-Power › High-performance and small form factor › Connectivity	› Ultra-Low-Power › High-performance and small form factor › Connectivity	› Ultra-Low-Power › Connectivity › Customizable Analog Front End › Reliability

PSoC

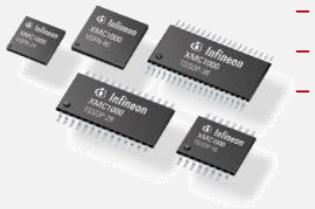
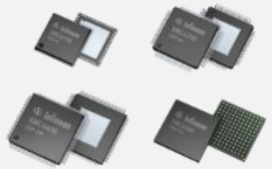
What is XMC™

XMC™ - Microcontroller

are characterized by….

- **Industry Standard Core** - ARM® Cortex® M
- **Application specific peripherals** for Lighting, Motor Control, Power Conversion, Industrial Communication (EtherCAT)
- **Performance & real-time** with hardware acceleration
- **Quality and robustness**: Long-term availability (through 2031 or longer), up to T_A 125°C (XMC4000)

- **XMC™ comprises of 2 major families**

XMC1000	XMC4000
	

– Cortex® M0 based
– Up to 200kB Flash
– Applications:
  – Low cost motor control
  – Lighting
  – Power conversion
	– Cortex® M4 based
	– Up to 2MB Flash
	– Applications:
	  – Automation (Industrial Drives, PLC, I/O)
	  – Power conversion

XMC™ Application View
What makes XMC™ the perfect fit…

	XMC™ Entry	LED Lighting	Digital Power	Motor Control	Ind. Automation
XMC4000 ARM® Cortex®-M4F up to 144MHz core 64KB - 2MB Flash up to 125°C T_{amb}	**XMC4100** Basic control & Connectivity VQFN-48 LQFP-64		**XMC4200** Server power 150ps HRPWM LQFP-64/100	**XMC4700** Industrial Drives, Hall & Encoder I/F, ΔΣ Demodulator LQFP-100/144, LFBGA-196 **XMC4100/4400** Industrial Drives, Hall & Encoder I/F ΔΣ Demodulator LQFP-64/100/144 LFBGA-144	**XMC4800/4300** EtherCAT,+Drives MultiCAN - 6 nodes, LQFP-100/144, LFBGA-196 **XMC4500** MultiCAN - 3 nodes Ethernet, +Drives ext.Memory,SD/MMC LQFP-100/144, LFBGA-144
XMC1000 ARM® Cortex®-M0 up to 48MHz core/ 96MHz peripheral 8 - 200KB Flash up to 105°C T_{amb} 1.8V-5.5V	**XMC1100** Basic control & Connectivity TSSOP-16/38 VQFN-24/40	**XMC1400** Flicker-free, 4-Ch LED, DALI SMPS VQFN-40/64 LQFP-64 **XMC1200/1300** Flicker-free, 3-Ch LED, SMPS, Connectivity TSSOP-16/28/38 VQFN-24/40	**XMC1300/1400** SMPS control Connectivity TSSOP-16/38 VQFN-24/40/64 LQFP-64 **XMC-SC** Wireless Charging, incl. SW from Spark Connected Support for Qi, AirFuel VQFN-24/40	**XMC1400** Hall & Encoder I/F, MATH,CAN VQFN-40/64 LQFP-64 **XMC1300** Hall & Encoder I/F MATH Co-processor TSSOP-16/38 VQFN-24/40	**XMC1400** MultiCAN - 2 nodes VQFN-48/64 LQFP-64

Infineon MCUs: Enabling more developers to get products to market

Integrated software for lower total cost of ownership in development and ongoing maintenance

Unique capabilities for differentiated products

High-reliability, low-power networking for higher-quality, differentiated products

Integrated compute and connectivity for faster time-to-market

Tools and documentation for simplifying new product development, certification

PSoC™ 6: Purpose-built for the IoT

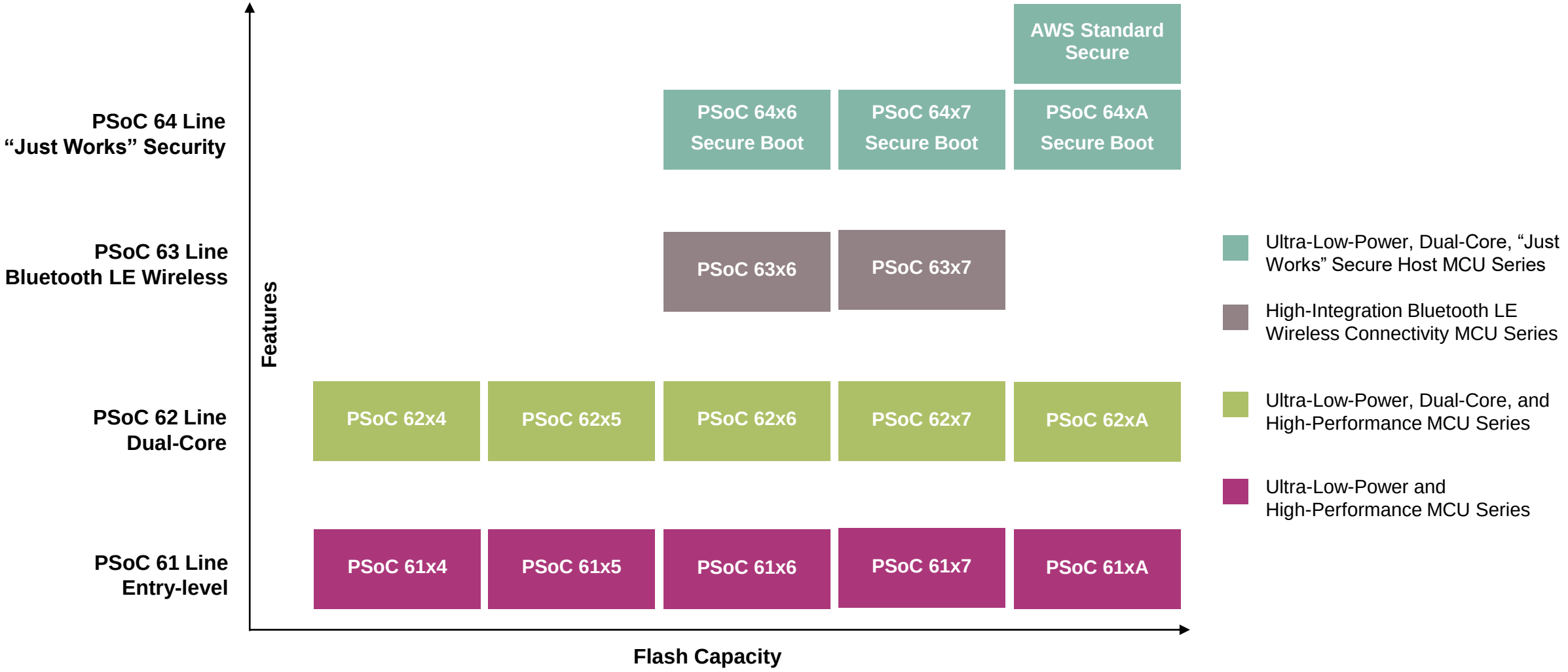
Emerging IoT devices require connectivity with increased processing and security without a power or cost penalty

Application Processors
Expensive, High-Power Consumption

Microcontrollers
Limited Processing Capacity

- The PSoC 6 portfolio bridges the gap between application processors and standard microcontrollers
  - High performance 150-MHz and 100-MHz dual-core Arm® Cortex®-M4 and Arm Cortex-M0+ architecture
  - Ultra-low-power 40-nm technology and design that consumes as little as 22-µA/MHz in active power mode
  - Best-in-class Wi-Fi connectivity options enabled with ModusToolbox and cloud services support like Amazon Web Services
  - Integrated, hardware-based Secure Execution Environment with secure data storage

PSoC™ 6 portfolio



PSoC™ 6

Ultra-Low-Power | Flexibility | Hardware-Based Security and Root of Trust

Performance and Integration

PSoC 61 Line
Ultra-Low-Power and High-Performance MCU Series

CY8C61xA
Arm Cortex-M4
2MB/1MB
DAC, QSPI, FS-USB, SDHC, DC-DC

CY8C61x8
Arm Cortex-M4
1MB/512KB
DAC, QSPI, FS-USB, SDHC, DC-DC

CY8C61x7
Arm Cortex-M4
1MB/288KB
DAC, QSPI, UDB[6], FS-USB,DC-DC

CY8C61x6
Arm Cortex-M4
512KB/128KB
DAC, QSPI, UDB, FS-USB,DC-DC

CY8C61x5
Arm Cortex-M4
512KB/256KB
QSPI, UDB, FS-USB,CAN FD[7], SDHC

CY8C61x4
Arm Cortex-M4
256KB/128KB
QSPI, FS-USB,CAN FD, 2x ADC

PSoC 62 Line
Ultra-Low-Power, Dual-Core, and High-Performance MCU Series

CY8C62xA
Arm Cortex-M4 & Arm Cortex-M0+
2MB/1MB
DAC, QSPI, FS-USB, SDHC, DC-DC

CY8C62x8
Arm Cortex-M4 & Arm Cortex-M0+
1MB/512KB
DAC, QSPI, FS-USB, SDHC, DC-DC

CY8C62x7
Arm Cortex-M4 & Arm Cortex-M0+
1MB/288KB
DAC, QSPI, UDB, FS-USB, DC-DC

CY8C62x6
Arm Cortex-M4 & Arm Cortex-M0+
512KB/128KB
DAC, QSPI, UDB, FS-USB, DC-DC

CY8C62x5
Arm Cortex-M4 & Arm Cortex-M0+
512KB/256KB
QSPI, FS-USB, CAN FD, DC-DC, SDHC

CY8C62x4
Arm Cortex-M4 & Arm Cortex-M0+
256KB/128KB
QSPI, FS-USB,CAN FD, 2x ADC

PSoC 63 Line
High-Integration Wired/Wireless Connectivity MCU Series

CY8C63x7
Arm Cortex-M4 & Arm Cortex-M0+
1MB/288KB
DAC, QSPI, UDB, Bluetooth LE, DC-DC

CY8C63x6
Arm Cortex-M4 & Arm Cortex-M0+
512KB/128KB, 1.71–3.6V
DAC, QSPI, UDB, Bluetooth LE, DC-DC

PSoC 64 Line
Ultra-Low-Power, Dual-Core, "Just Works" Secure Host MCU Series

CYB064xA
Arm Cortex-M4 & Arm Cortex-M0+
2MB/1MB
Secure-Boot MCU
Secure Flashboot, CY Secure Bootloader,

CYB06447BZI-D54
Arm Cortex-M4 & Arm Cortex-M0+
1MB/288KB
Secure Flashboot, CY Secure Bootloader
MbedOS, AFR, fRTOS Support

CYB06447BZI-BLD53
Arm Cortex-M4 & Arm Cortex-M0+
1MB/288KB, Bluetooht LE
Secure Flashboot, CY Secure Bootloader
MbedOS, AFR, fRTOS Support

CY8B064x5
Arm Cortex-M4 & Arm Cortex-M0+
512KB/256KB
Secure Flashboot, CY Secure Bootloader
MbedOS, AFR, fRTOS Support

CYS0C64xA
Arm Cortex-M4 & Arm Cortex-M0+
2MB/1MB
AWS Standard Secure MCU
ARM_v7-M TF-M w/ PSA API
TF-M Integrated with AFR

Status: Concept | Development | Sampling | Production

XMC™ MCU Product Portfolio

ARM® Cortex®-M4 (with FPU)

- CPU Frequency up to 144MHz
- **High Performance Flash technology**
- Timers CCU4, CCU8, POSIF
- USB / Up to 3x CAN / Up to 6x Serial Channels
- Up to 4x 12Bit ADC / 2x DAC

XMC4100/4200
Up to 256kB Flash / 40kB RAM
48-64pins

XMC4400
Up to 512kB Flash / 80kB RAM
64-100pins

- 120MHz Core
- Ethernet
- ΔΣ Demodulator

XMC4500
Up to 1MB Flash / 160kB RAM
100 – 144pins

- EBU
- SD Card

XMC4700
Up to 2MB Flash / 352kB RAM
100 – 196pins

- 144MHz Core
- 6ch CAN

XMC4800
Up to 2MB Flash / 352kB RAM
100 – 196pins

- EtherCAT

XMC4300
256kB Flash / 352kB RAM
100 pin

ARM® Cortex®-M0

- Core up to 48MHz / Peripherals up to 96MHz
- Capture Compare Units (CCU4)
- 2x Serial Channels
- 12Bit ADC
- **1.8V-5.5V**
- TA = -40C to 105C

XMC1100
up to 64kB Flash
16 – 40 pins

- 9ch LED Control (BCCU)
- 3x Analog Comparators

XMC1200
up to 200kB Flash
16 – 40 pins

- Math Co-Processor
- CCU8 PWM Timer
- Hall & Encoder I/F

XMC1300
up to 200kB Flash
16 – 40 pins

- 48MHz/96MHz clock
- 2x CAN
- 2x CCU8
- 4x Analog Comparators

>70% performance increase

XMC1400
up to 200kB Flash
40 – 64 pins

XMC – SC

Wireless Charging Series

- Support for different standards and topologies
  - Qi
  - Proprietary Inductive
  - Proprietary Resonant
  - AirFuel
- Turnkey system solutions for wireless charging based on Infineon components:
  - MOSFETs – OptiMOS™ and StrongIRFET™
  - Gate driver ICs
  - Wireless power controller (including software IP) – XMC™-SC
  - PWM/flyback controllers and integrated power stage ICs – CoolSET™
  - Gallium nitride (GaN) – CoolGaN™ e-mode HEMTs
  - Voltage and buck regulators
  - Authentication – OPTIGA™ Trust
  - ...

Agenda

Our Core Capabilities mapped to products

COMPUTE

- Arm® Cortex® Processors
- Mixed Signal MCU Architectures
- Application Co-processors

PSoC®4
PSoC®6
XMC™1000
XMC™4000

SECURE

- Device authentication
- embedded SIM
- Hardware security controllers

OPTIGA™
- Trust, TPM
- Connect
- Authenticate

ENHANCE

- Graphics
- Machine Learning
- NFC

PSoC®6
Next gen MCU
My-d™ NFC (SCS)

CONNECT

- Wi-Fi / BT Combo
- BT / BLE

AIROC™
- CYW43/55xxx
- CYW20xxx, PSoC®4/6-BLE

CONTROL

- Capacitive / Inductive Sense
- Wireless Charging
- Motor Control
- Power Conversion

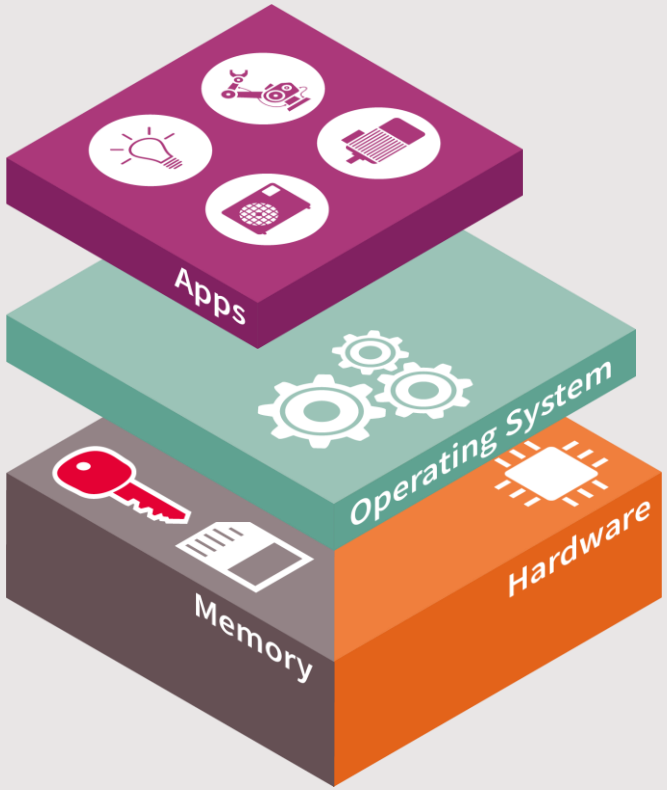
PSoC®4
PSoC®6

XMC™1000 (Spark)

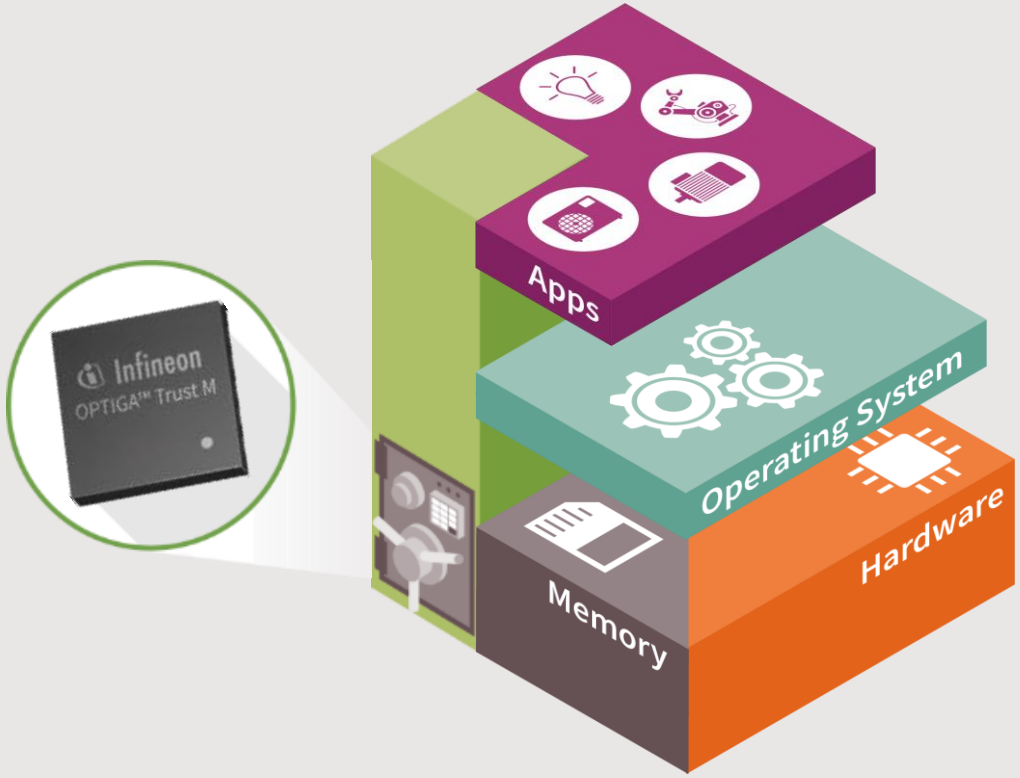
XMC™1000
XMC™4000

Hardware Security makes the difference – chose the right level of security for the threats at hand

Logical security

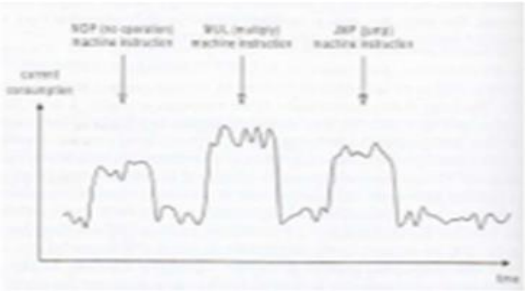


Logical and physical security

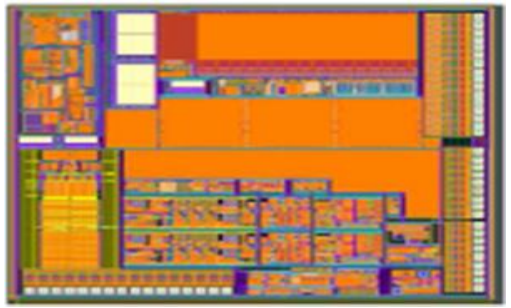


Hardware Security makes the difference – chose the right level of security for the threats at hand

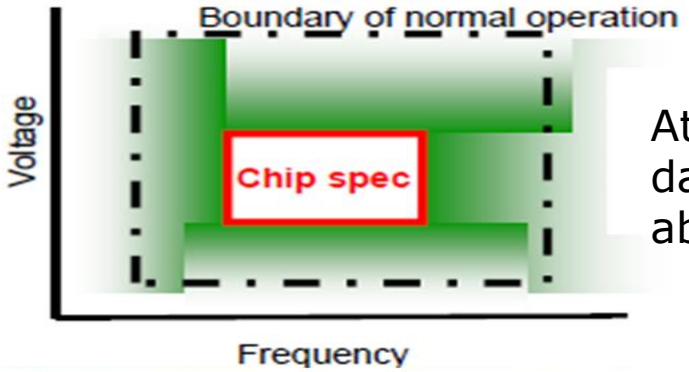
Standard Micro



Attacker can read data by **monitoring** current consumption

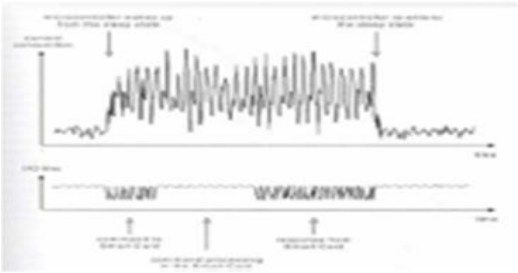


Attacker can capture data by **probing** metal patterns

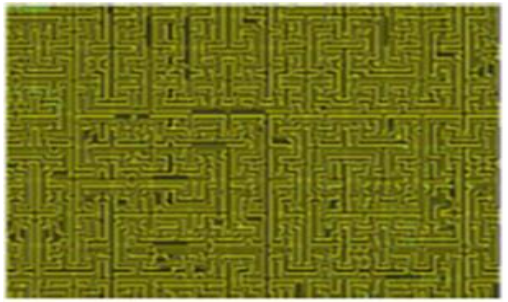


Attacker can read data by **triggering** abnormal conditions

OPTIGA™

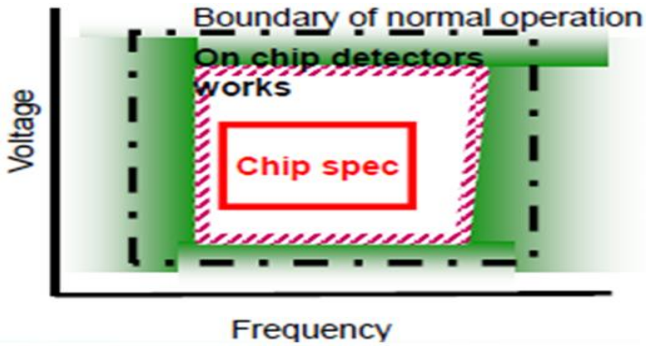


Current consumption is scrambled by **dynamically generated noise** so that Data cannot be extracted by current monitoring.



Chip is protected with:

- **"Active" metal shield** to prevent data capture
- **Randomized layout**



On-chip sensors force to stop operation under abnormal conditions

50+ active sensors protection the device, not just detection

Embedded Security – OPTIGA™ Family Overview

OPTIGA™ - Embedded Security Solutions

OPTIGA™ Authenticate

- OPTIGA™ Authenticate S
- OPTIGA™ Trust Charge
- Legacy Solutions
  - OPTIGA™ Trust B
  - OPTIGA™ Trust E

Device Authentication

OPTIGA™ Connect
(embedded SIM solutions)

- OPTIGA™ Connect Consumer
- OPTIGA™ Connect IoT

OPTIGA™ TPM
(standardized by TCG)

- OPTIGA™ TPM SLB
- OPTIGA™ TPM SLI - automotive
- OPTIGA™ TPM SLM - industrial

OPTIGA™ Trust
(security for IoT nodes)

- OPTIGA™ Trust M
- Legacy Solutions
  - OPTIGA™ Trust X
  - OPTIGA™ Trust P

IoT Security

Feature product: OPTIGA™ Trust M

Why is a Hardware-based “Root of Trust” important?
Internal countermeasures for highest security

Logical attacks	Side channel attacks	Fault injection	Invasive attacks
e.g. protocol fuzzing, Jamming, replay,…	e.g. SPA, DPA, Spectre, Meltdown	e.g. Spiking, radiation, light attacks, clock manipulation, DFA	e.g. FIB manipulation, micro-probing,…

Countermeasures

PKI, digital signatures, encryption, CMAC, blockchain, MISRA C-CERT coding guidelines…	Runtime invariant SW implementation, randomized processing in HW and SW, dual-rail HW implementation, encrypted computation…	Double computation, all safety HW measures…	Tamper protection, implanted ROM, full-custom design

Software

Hardware

OPTIGA™ Trust M
High-end security solution for your IoT devices

Main Features

- Based on CC EAL 6+ certified HW
- Secured IoT device identity (x.509 cert) injected in CC certified facility
- Flexible customization (e.g. PKI)
- State-of-the-art cryptography

Typical Use Cases

- Secured cloud authentication
- Secured cloud communication
- Secured Software Updates
- IP Protection
- … and more!

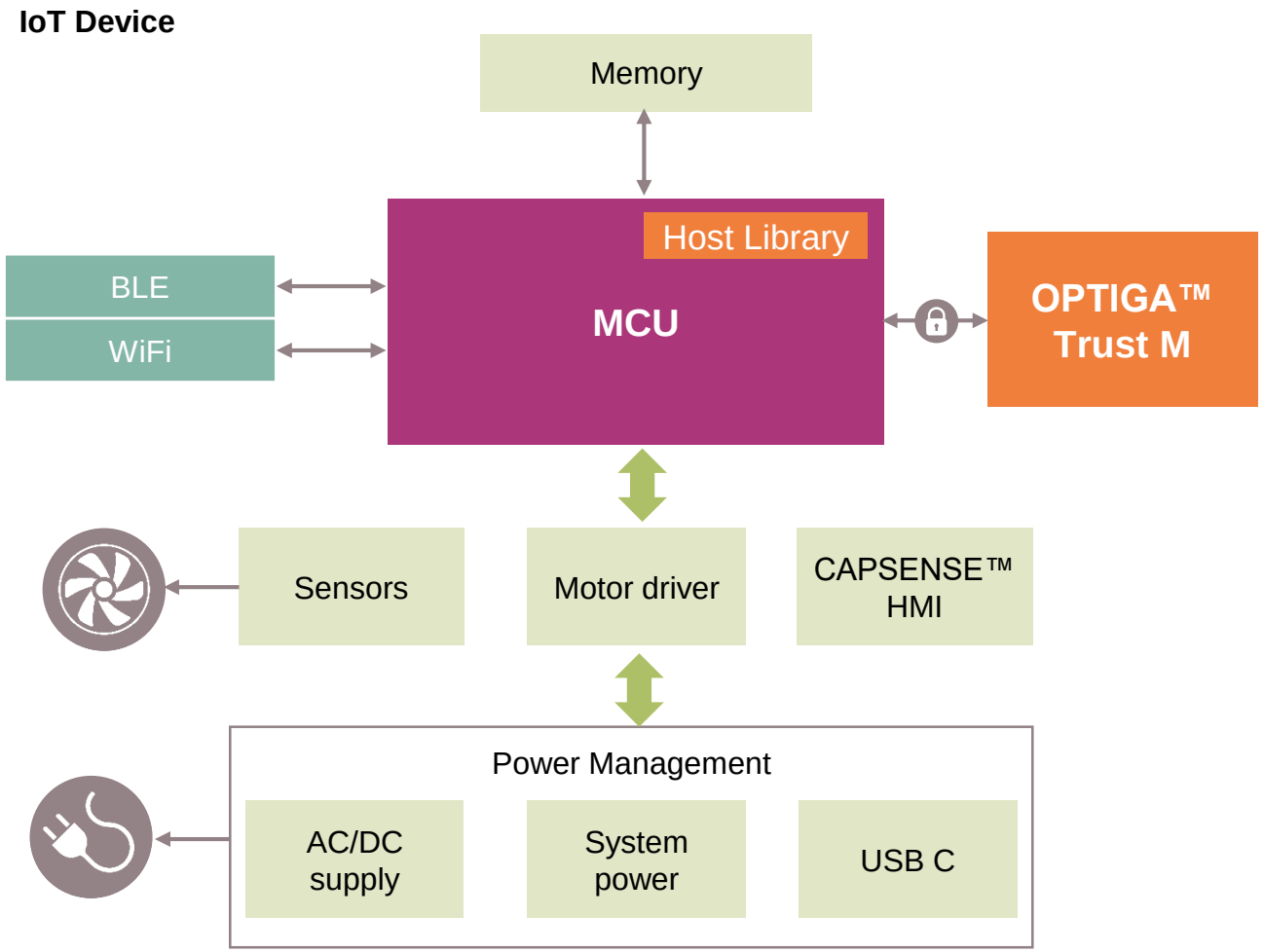
Host compatibility

- Cortex M4: XMC4xxx, PSoC6x
- Cortex M0: XMC1xxx family
- SoC: NRF5x; ESP32
- OS: Linux, Zephyr OS, FreeRTOS

Tools and support

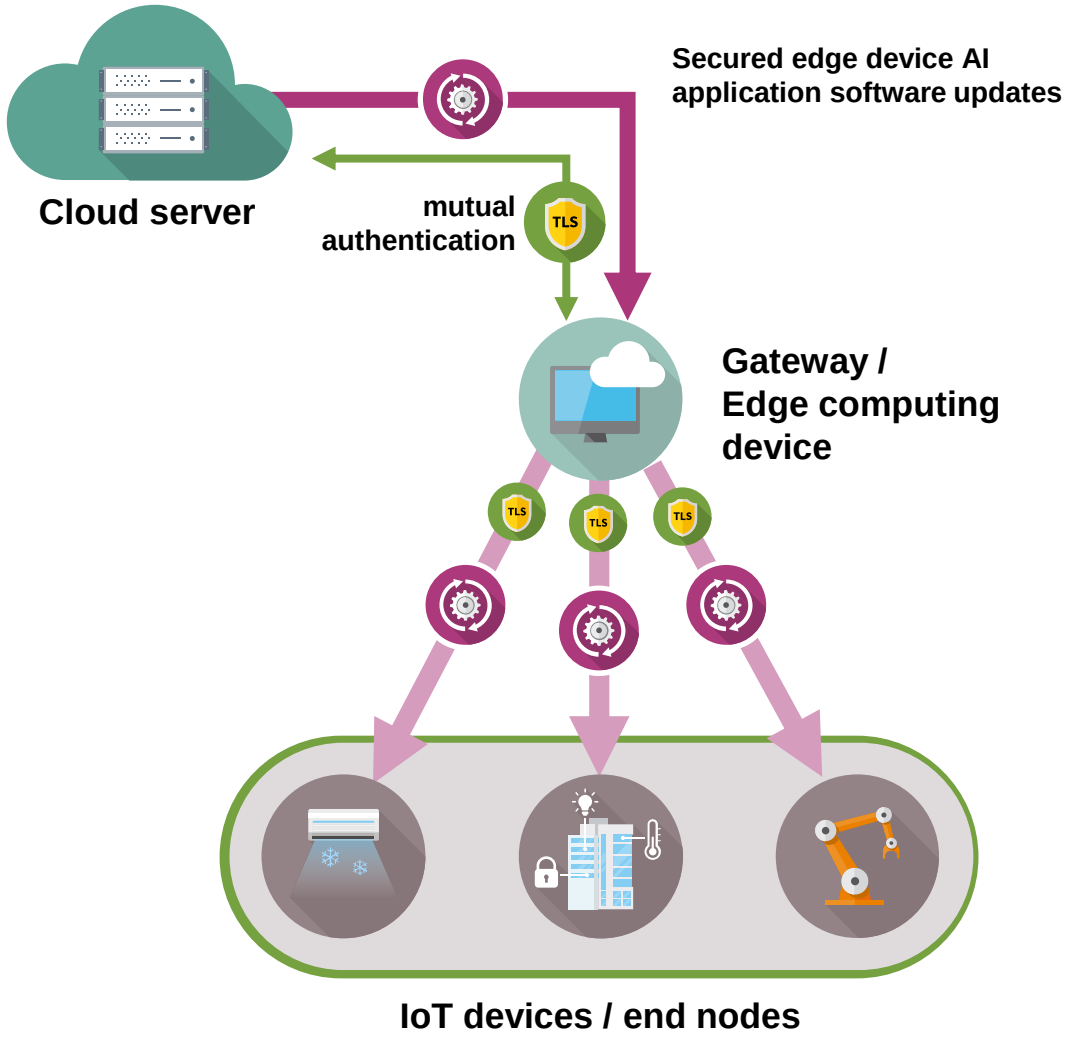
- Open Source framework (MIT)
- NDA-free application notes and code examples
- Modus Toolbox™ support
- Development kits

OPTIGA™ Trust M
Typical system diagram and focus applications



Typical Applications		
Smart Home	Enterprise / Smart Building	Industrial Automation
Smart speaker	Smart door lock	PLC
Residential HVAC	Commercial HVAC	Drives
Ceiling fan	Surveillance camera	Service robots
Refrigerator Washing machines	Street lighting	
Other home appliances		

OPTIGA™ Trust M
Protecting the IoT from cloud to end nodes

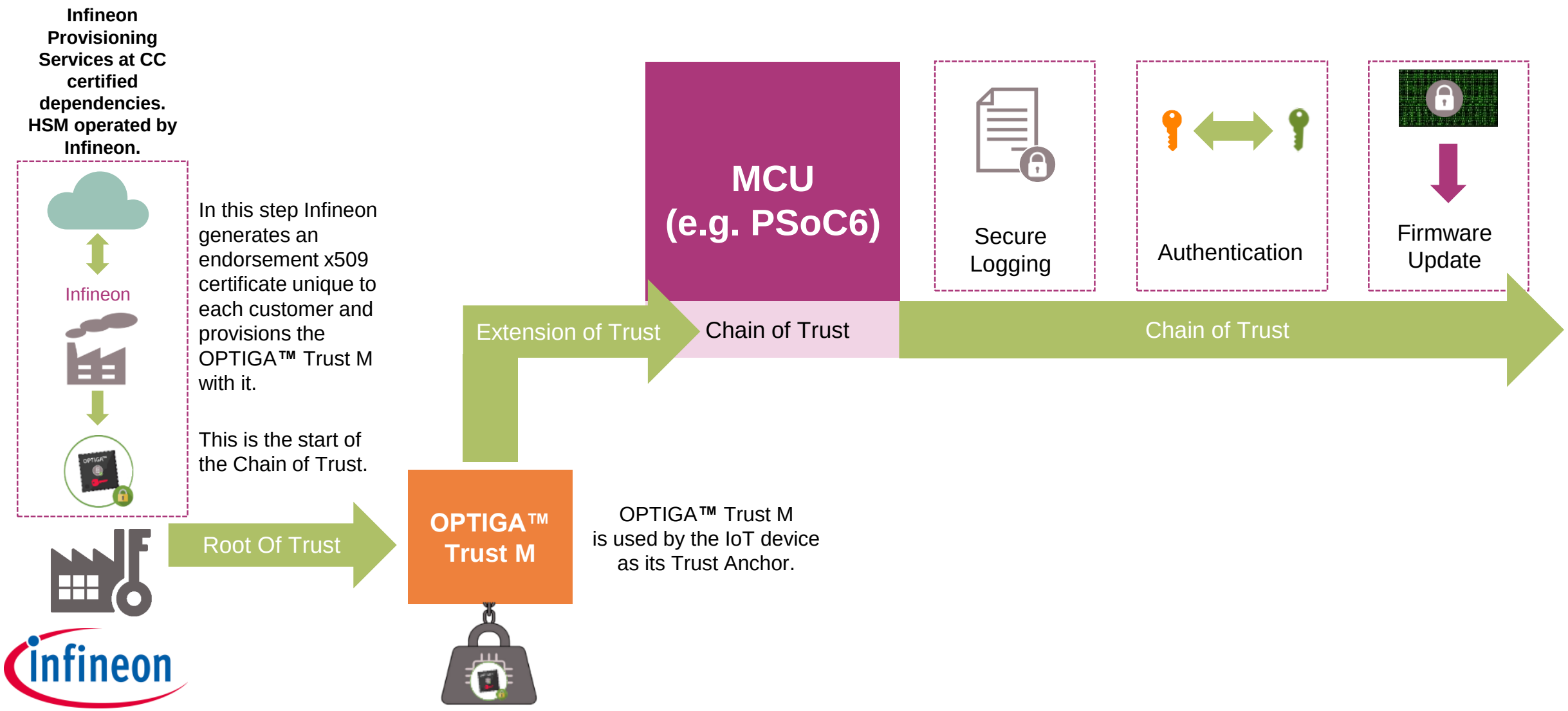


Secured connectivity

Secured cloud authentication

Secured software update over-the-air

OPTIGA™ Trust M
Secure provisioning as the foundation for a secured chain of trust



OPTIGA Trust M – provisioning solutions

OPTIGA™ Trust M
Simplifying the customer journey with improved provisioning services

OPTIGA™ Trust M Express	OPTIGA™ Trust M Fit	OPTIGA™ Trust M Pro
OPTIGA™ Trust M version pre-configured with unique device certificates and is ready to be used by customers for easy and fast integration into an IoT device. It includes Cloud ID support to simplify device-to-cloud authentication. Target customer: customers with short T2M, limited security know-how and resources. These customers are looking for a secure element that “just works”.	Highly customized OPTIGA™ Trust M version that fits specific customer needs (e.g. integration into customer’s own PKI). Infineon produces a dedicated SKU per customer configuration. Target customer: high security know-how and complex customization requirements typically derived from an existing PKI infrastructure.	Highly flexible service to enable customers to customize the OPTIGA™ Trust M by themselves and load their configurations “over-the-air” without involvement from Infineon. Target customer: looking for flexibility and independence in their design and manufacturing process. These customers are looking for a secure element that can “flexibly integrated into their supply chain.

OPTIGA™ Trust M
Open Source Framework

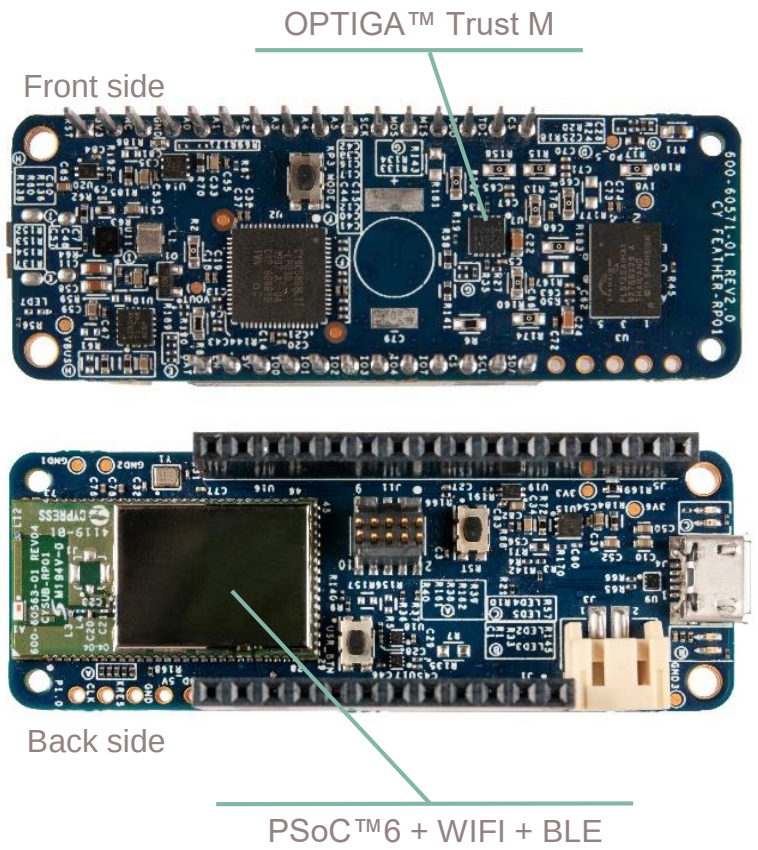
The OPTIGA™ Trust M host software is Open Source, and available without NDA on GitHub together with the product documentation

https://github.com/Infineon/optiga-trust-m

Agenda

Evaluation Kit

New IoT Security Development Kit featuring streamlined design and Infineon's MCU, WIFI and BLE modules



Key facts

- IoT Security Development Kit featuring Adafruit Feather compatibility, OPTIGA™ Trust M, PSoC™ 62 MCU and AIROC™ Wi-Fi + Bluetooth® combo
- The kit comes pre-configured with a specific security use case:
  - AnyCloud MQTT connectivity to AWS
- OPTIGA™ Trust M Host Library available on ModusToolbox™ to enable further use cases
- Available for online ordering

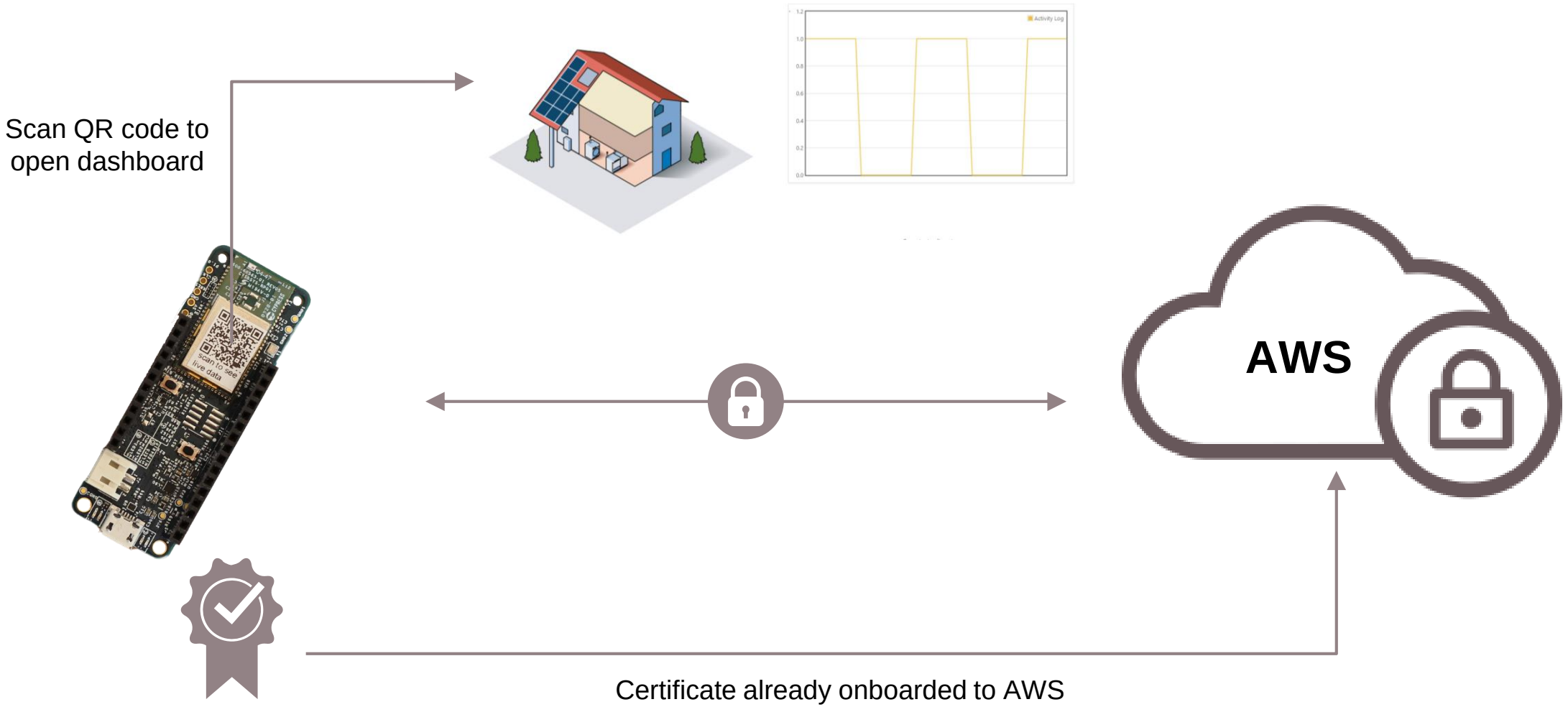
What's in the box?

Instructions sheet

Board

Micro USB cable

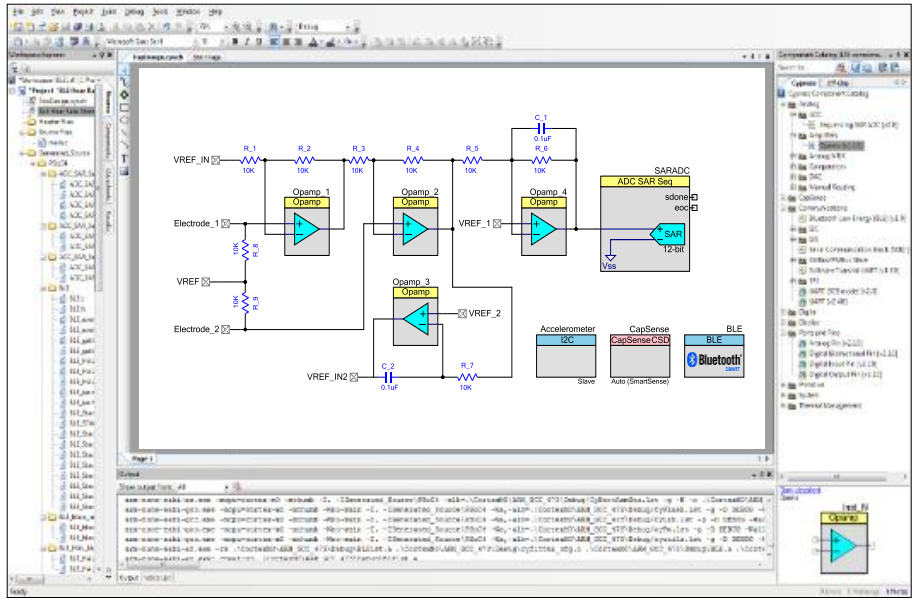
Use case 1
Secured AnyCloud MQTT connectivity to AWS



Agenda

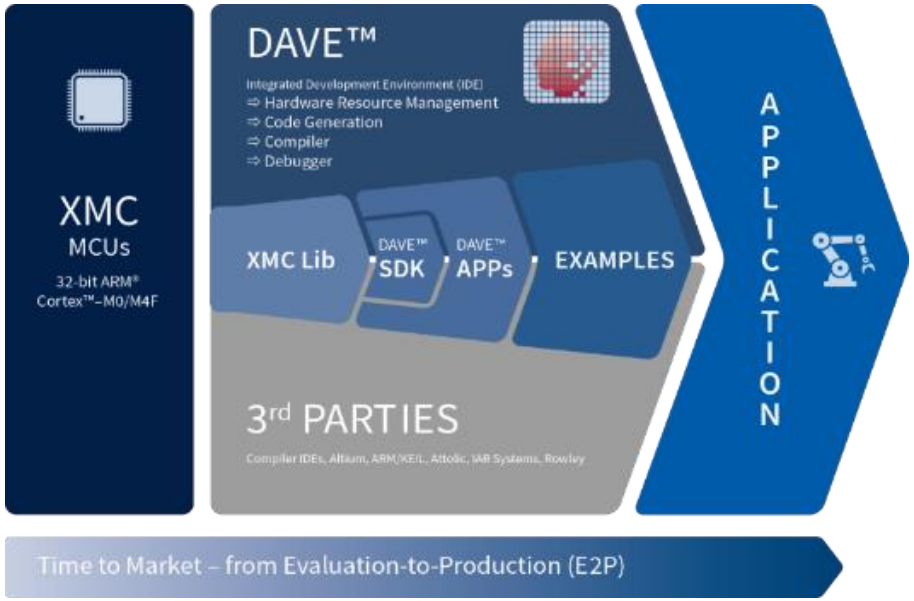
Legacy Software: PSoC Creator and Dave

PSoC Creator



- Software IDE for PSoC 3, PSoC 4, PSoC 5
- Schematic-based capture tool enables custom analog front end and programmable digital development
- Component-based design with graphical configuration tools

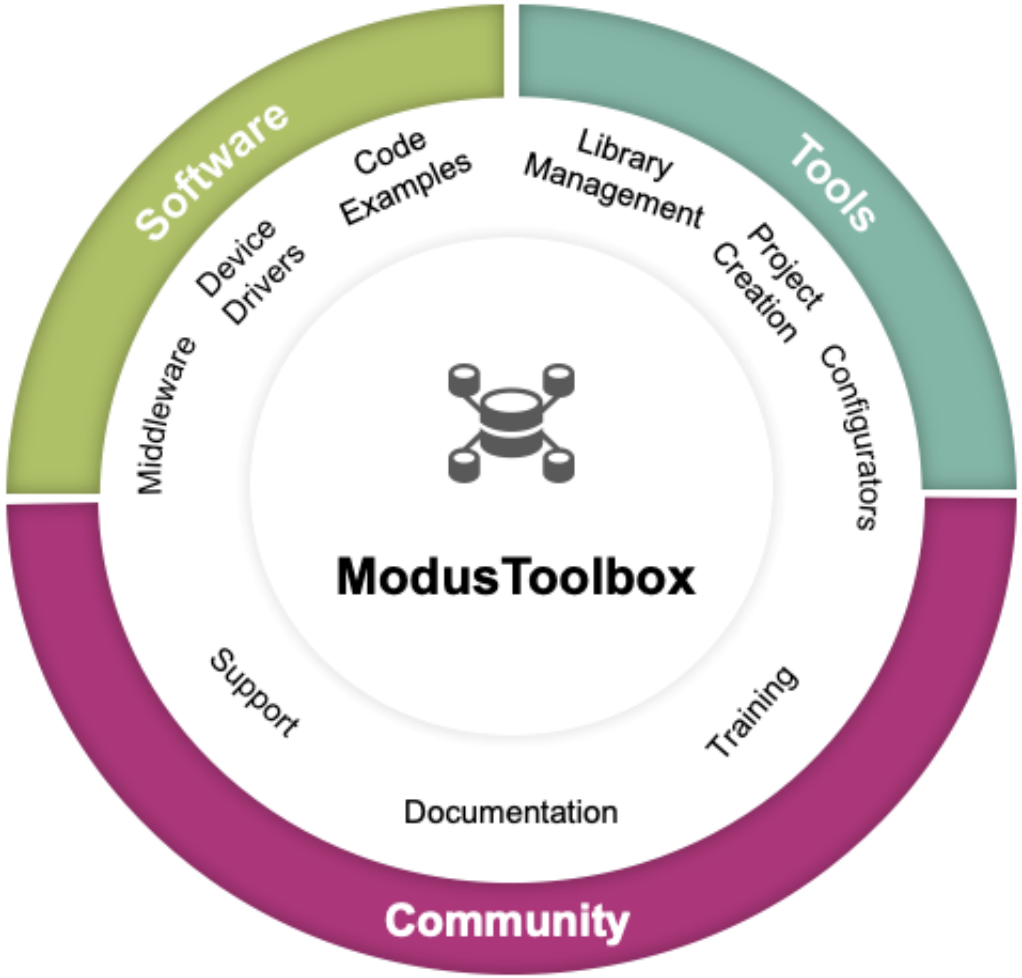
DAVE



- Free Eclipse-based code development platform/IDE offering code repository, graphical system design methods, and automatic code generator
- Guides XMC™ microcontroller user along the entire process – from evaluation to production (E2P).
- XMC™ Lib and DAVE™ generated code is tested and released for use with 3rd party tool.

ModusToolbox™

ModusToolbox™ Software – Created for Developers



- Multi-platform development tools
  - Create projects for any hardware
  - Add libraries and update versions
  - Set up peripherals graphically
  - Build with the best optimizations (GCC, IAR, ARMCC)
  - Edit and Debug in your favorite tools (Eclipse, IAR Workbench, Arm uVision)
- Complete set of Libraries covering Device Drivers, Board Support Packages (BSPs), RTOS, Connectivity stacks, Graphics, Security
- Hundreds of well documented and tested Code Examples to get started.
- Get support and brainstorm ideas as part of a vibrant developer community

Summary

- The need for Security is increasing – the challenge is to find the right level of security
- Infineon offers a complete portfolio of secure microcontrollers and secure elements to best address your requirements to security
- With certified dependencies, front-end provisioning and billions of shipped secure microcontrollers Infineon wants to be your partner to facilitate the integration of security into your industrial IOT devices

Thank you
and stay secure!

Part of your life. Part of tomorrow.

Appendix

PSoC™ 6 MCU package portfolio

	PSoC 61 Line Ultra-Low-Power and High-Performance MCU Series	PSoC 62 Line Ultra-Low-Power, Dual-Core and High-Performance MCU Series	PSoC 63 Line High-Integration Wired/Wireless Connectivity MCU Series	PSoC 64 Line Ultra-Low-Power, High-Performance, and Secure MCU Series
TQFP	64-TQFP[1] 10 x 10-mm² 80-TQFP[1] 12 x 12-mm² 100-TQFP 14 x 14-mm² 128-TQFP 14 x 20-mm²	80-TQFP[1] 12 x 12-mm² 100-TQFP 14 x 14-mm² 128-TQFP 14 x 20-mm²		
BGA	124-BGA 9 x 9-mm²	124-BGA 9 x 9-mm²	116-BGA 5.2 x 6.4-mm² 124-BGA 9 x 9-mm²	116-BGA 5.2 x 6.4-mm² 124-BGA 9 x 9-mm²
QFN	68-QFN 8 x 8-mm²	68-QFN 8 x 8-mm²	68-QFN 8 x 8-mm²	68-QFN 8 x 8-mm²
CSP	49-WLCSP 3.0 x 3.0-mm² 80-WLCSP 3.7 x 3.2-mm² 100-WLCSP 3.9 x 4.1-mm²	49-WLCSP 3.0 x 3.0-mm² 80-WLCSP 3.7 x 3.2-mm² 100-WLCSP 3.9 x 4.1-mm²	104-M-CSP 5.2 x 6.4-mm²	

PSoC™ 6 MPN decoder

CY XX 6 A B C DD E - FF G H I JJ K L

Field	Description	Values	Meaning
CY	Cypress	CY	Cypress
XX	Firmware	8C	Standard
		B0	Secure Boot v1
		S0	Std. Secure - AWS
		S1	Std. Secure - Pelion
		S2	Std. Secure - Alibaba
		S3	Std. Secure - Google
6	Architecture	6	PSoC 6
A	Line	0	Value
		1	Programmable
		2	Performance
		3	Connectivity
		4	Security
B	Speed	2	100 MHz
		3	150 MHz
		4	150/50 MHz

Field	Description	Values	Meaning
C	Memory size (Flash/SRAM)	0-3	RFU
		4	256K/128K
		5	512K/256K
		6	512K/128K
		7	1024K/288K
		8	1024K/512K
		9	RFU
		A	2048K/1024K
DD	Package	AZ, AX	TQFP
		LQ	QFN
		BZ	BGA
		FM	M-CSP
		FN,FD,FT	WLCSP
E	Temperature range	C	Consumer
		I	Industrial
		Q	Extended Industrial
FF	Feature code		Standard MCU
		S2-S6	Standard MCU
		BL	Integrated Bluetooth LE

Field	Description	Values	Meaning
G	CPU core	F	Single core
		D	Dual core
H	Attribute code	0-9	Feature set
I	GPIO count	1	31-50
		2	51-70
		3	71-90
		4	91-110
JJ	Engineering sample (optional)	ES	Engineering samples or not
K	Die revision (optional)		Base
		A1-A9	Die revision
L	Tape/Reel shipment (optional)	T	Tape and Reel shipment

E.g.

CY8C6247BZI-D54

CYB06447BZI-D44

CY8C6247BZI-D54ES3T