



# #GlobalAzure

#CloudGenVerona

@cloudgen\_verona

Thanks to all the sponsors



## PREMIUM SPONSOR

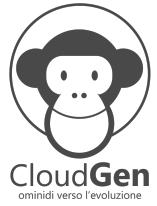


## BASIC SPONSOR



CODICEPLASTICO

**dgroove**  
Tecnologia emozionale.



TOPIC

# Azure Sphere

---

A New Solution for Creating Highly-Secured,  
Connected MCU Device

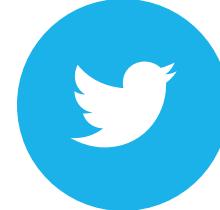
# Who I am



Mirco Vanini



Microsoft® MVP Windows Development  
Open Connectivity Foundation - OCF®  
Ambassador



@MircoVanini



<https://github.com/MircoVanini>



<https://it.linkedin.com/in/proxsoft>



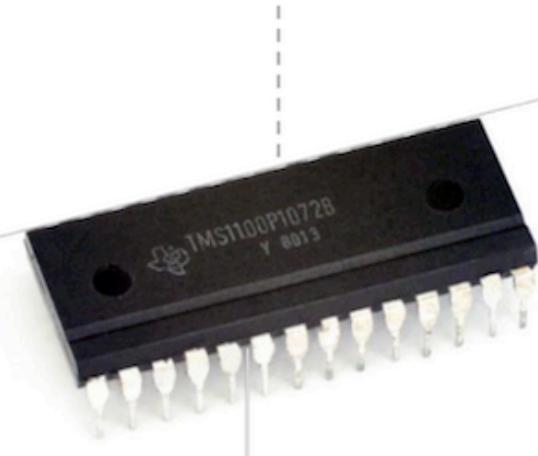
# Agenda



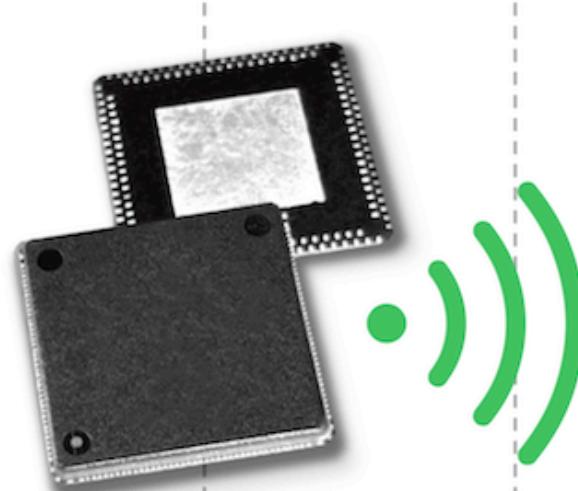
- Digital Transformation
- Opportunity | Risk
- The 7 Properties of HSD
- Azure Sphere
  - MCU
  - OS
  - Cloud
  - DevKit



Prepare for the 2nd wave of Digital Transformation...



Wave 1:  
**The Microcontroller (MCU)**



Wave 2:  
**Internet Connectivity**

1970's

1980's

1990's

2000's

2010's

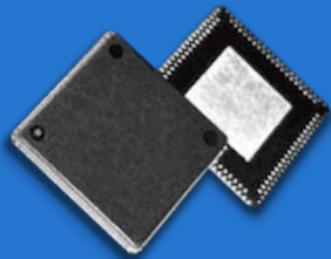
2020's

2030's

# Digital Transformation



The microcontroller (MCU)  
a low-cost, single chip computer



**9 BILLION** new MCU devices  
built and deployed every year

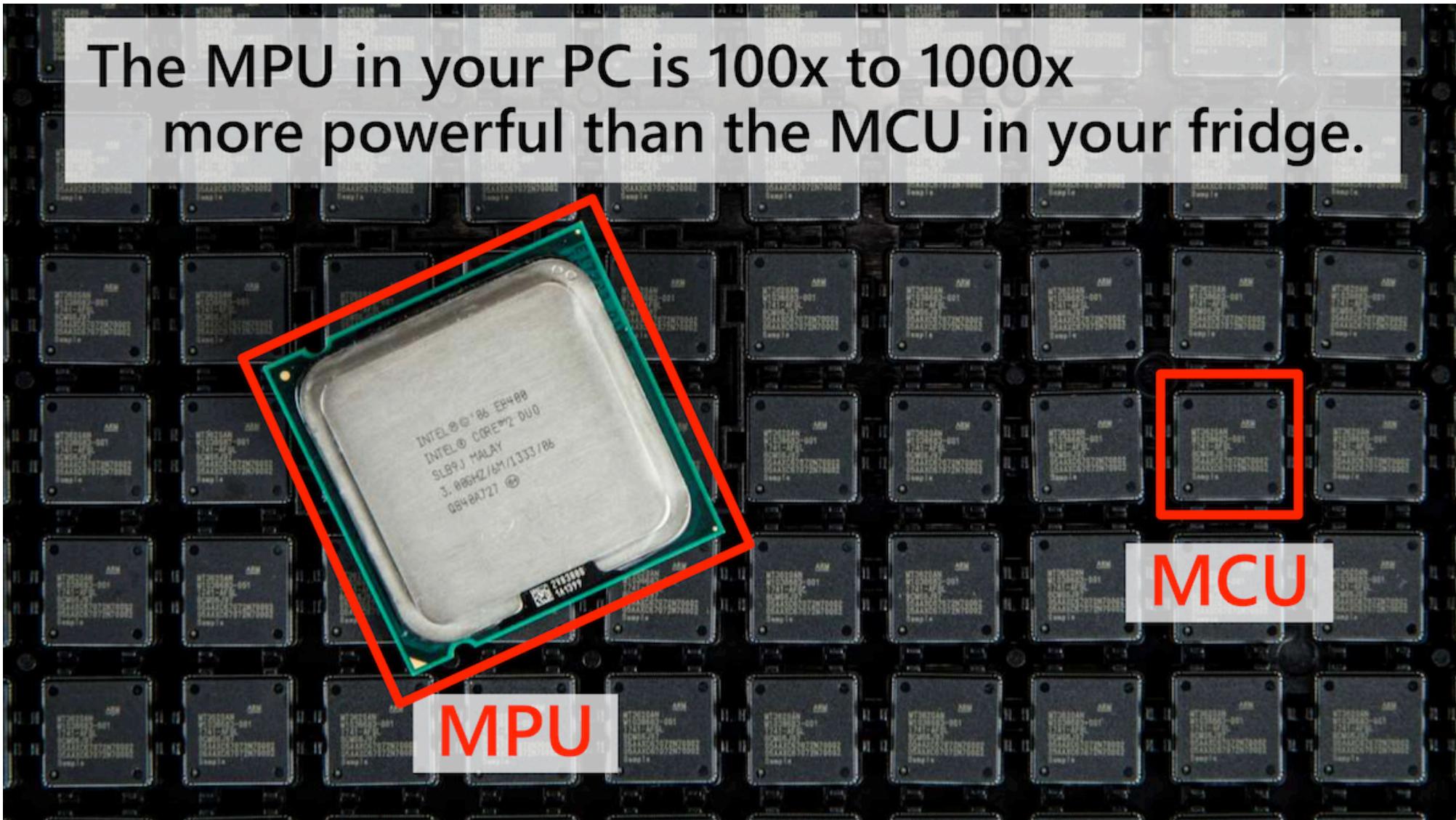




Fewer than 1% of MCU are connected today !



The MPU in your PC is 100x to 1000x more powerful than the MCU in your fridge.



# Opportunity



Manufacturers have a compelling desire to build connected MCU-based devices



**How does** a consumer know the compressor in their fridge needs to be replaced?

**Option 1**

Melted ice cream and spoiled milk

**Option 2**

Message that a technician with replacement compressor will arrive tonight

Connected devices  
create profoundly better  
customer experiences

# Risk



The Mirai Botnet (aka Dyn Attack), Oct 2016: Largest IoT DDoS attack. Large portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit and CNN. Affected devices: Webcams, DVR players, Deutsche Telekom routers (900.000 - TR-069 protocol).



The Jeep Hack, July 2015: A team of researchers was able to take total control of a Jeep SUV by exploiting a firmware update vulnerability.



The Hackable Cardiac Device from St.Jude, Jan. 2017: The vulnerability provided access to drain the battery, change heartbeat pace and to trigger shocks.



The TRENDnet Webcam Hack, Jan. 2012. Access to camera and microphone over TCP/IP.



The Printer Hack to catch fire, Nov. 2011: Made the fuser overheat, causing the paper in the printer to catch fire.

# The internet security battle



Microsoft has been fighting it for decades so they have some experience to share.  
Also on hardware side!

## Example X-BOX

- XBOX: Hacked within weeks  
Standard Intel x86 system
- XBOX 360: Hacked within 3,5 month  
HW hack to compromise the bus
- XBOX One: Not hacked until today  
also thanks to in-chip bus firewalls

# Beginning



**SECURITY IS FOUNDATIONAL**

**It must be built in from the beginning.**



# Highly-secured connected devices require 7 properties



## Hardware Root of Trust

Is your device's identity and software integrity secured by hardware?



## Small Trusted Computing Base

Is your device's TCB protected from bugs in other code?



## Defense in Depth

Does your device remain protected if a security mechanism is defeated?



## Dynamic Compartments

Can your device's security protections improve after deployment?



## Certificate-Based Authentication

Does your device use certificates instead of passwords for authentication?



## Failure Reporting

Does your device report back about failures and anomalies?



## Renewable Security

Does your device's software update automatically?



<http://aka.ms/7properties>



## Azure Sphere empowers manufacturers to create highly-secured, connected MCU devices

### SECURITY

Every device built with Azure Sphere is secured by Microsoft. For its 10 year lifetime.

### PRODUCTIVITY

The Azure Sphere developer experience shortens OEM time to market.

### OPPORTUNITY

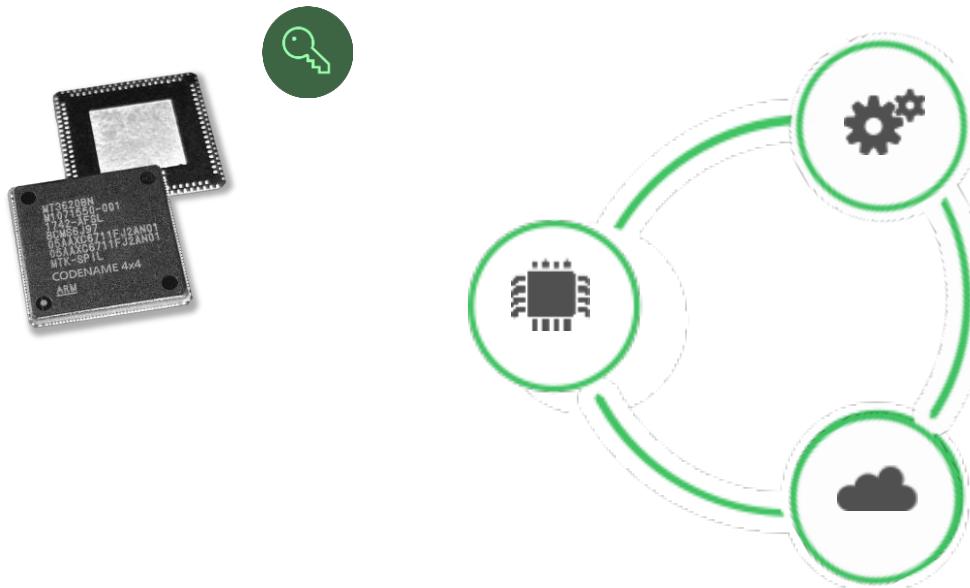
Azure Sphere empowers OEMs to create new customer experiences and business models.

# End-to-end solution for securing MCU powered devices



## Secured MCUs

A new class of crossover **Azure Sphere MCUs**, from our silicon partners, with built-in Microsoft security technology provide connectivity, high performance, and a secured hardware root of trust.



## Secured Operating System

The highly-secured **Azure Sphere IoT OS** combines the best of Microsoft and OSS technologies to create a **trustworthy platform** for new IoT experiences.

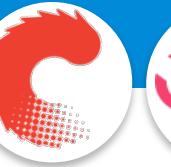


## Secured by our Cloud Service

The **Azure Sphere Security Service** guards every Azure Sphere device; it **protects** your devices and customers, **detects** emerging threats, and proactively **responds**.



# Compare



Today, only Azure Sphere provides all 7 Properties for secured IoT

Chip	OS& Service	Hardware Root of Trust	Defense in Depth	Small TCB	Dynamic Compartments	Certificate-based Auth.	Failure Reporting	Renewable Security
MT3620	Azure Sphere							
Espressif ESP32	RTOS & ?							
Marvell 88MW300/2	RTOS & ?							
Qualcomm QCA4010	RTOS & ?							
Broadcom BCM43907	RTOS & ?							
TI CC3220x	RTOS & ?							

= Full, Partial, or No Silicon support

= Full, Partial, or No OS support

= Full, Partial, or No Cloud Security Service support

# History



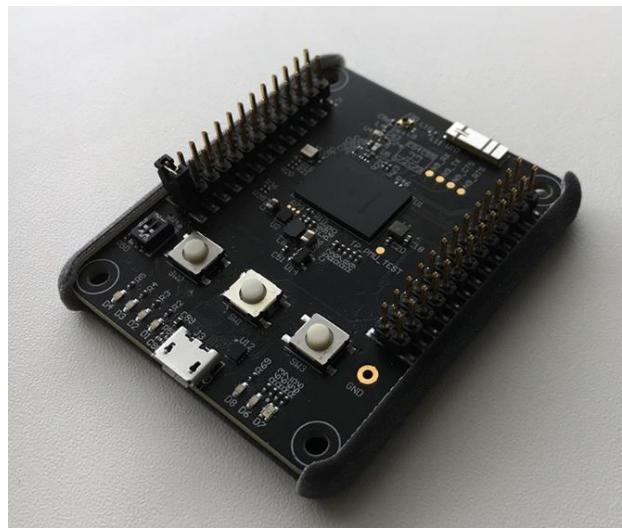
Project started in 2014 in Microsoft Research, now part of AI&R division

Started working on prototype chip and OS in 2015

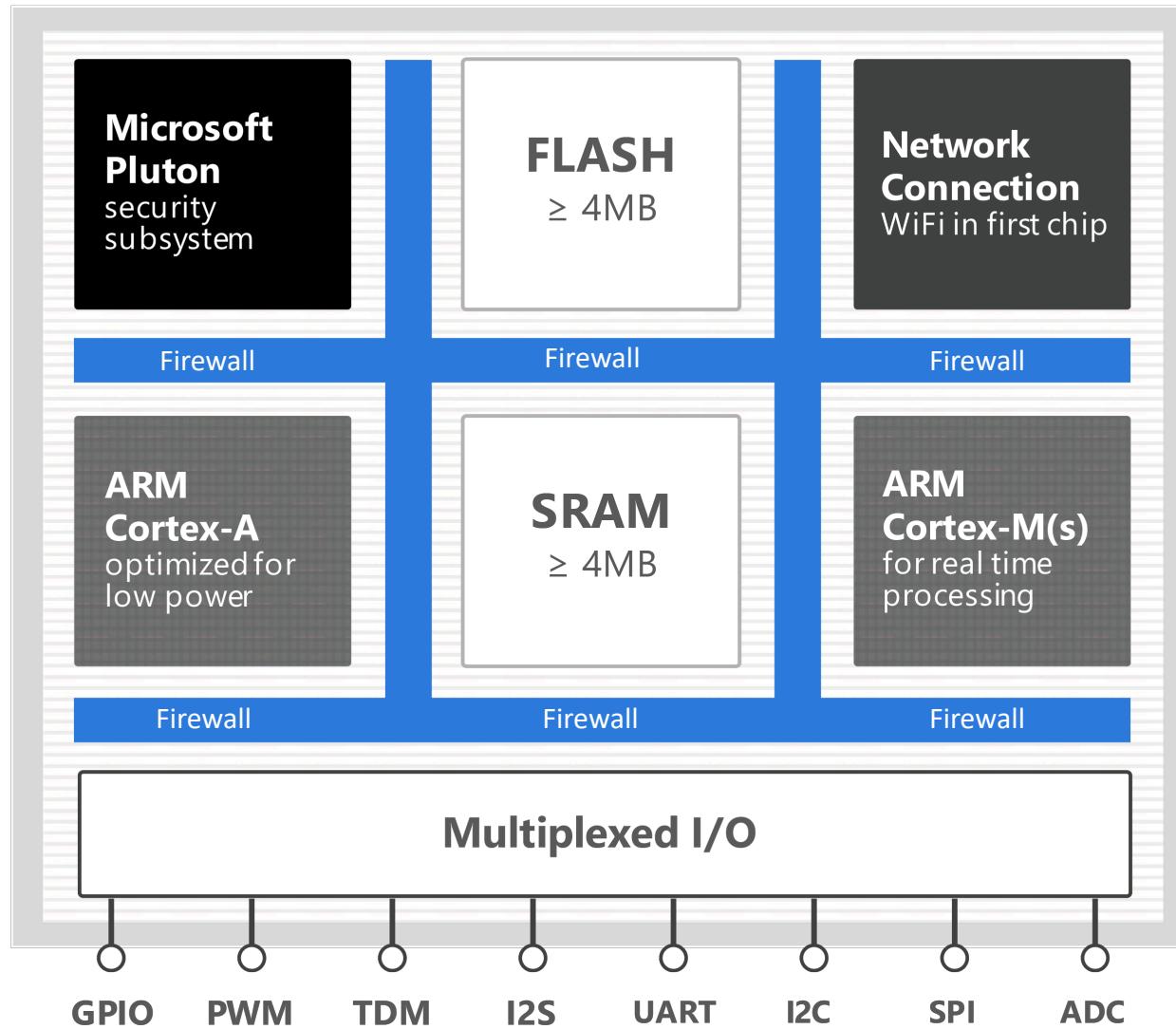
Established “seven properties of highly secured devices”

Ran a “security challenge” based on prototype chip and OS in 2017

Actively working with partners and customers for production in 2018



# Azure Sphere MCU



## Secured

With built-in Microsoft security technology  
i.e. I/O bus firewalls  
including the Pluto Security Subsystem

## Performance

With built-in Cortex-A processors  
Delivers significantly greater performance  
vs. similar traditional MCU

## Connected

With built-in networking

# Azure Sphere Silicon Partners



Microsoft is working with other suppliers to implement the Azure Sphere Pluto Security Core into their HW



ARM



Hilscher



LitePoint



LongSys



MediaTek



Nordic



Nuvoton



NXP



Qualcomm



Seeed Studio



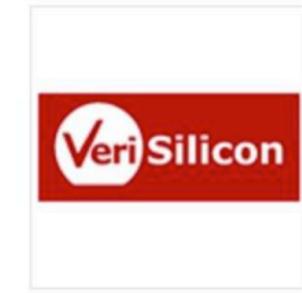
Silicon Labs



STMicroelectronics



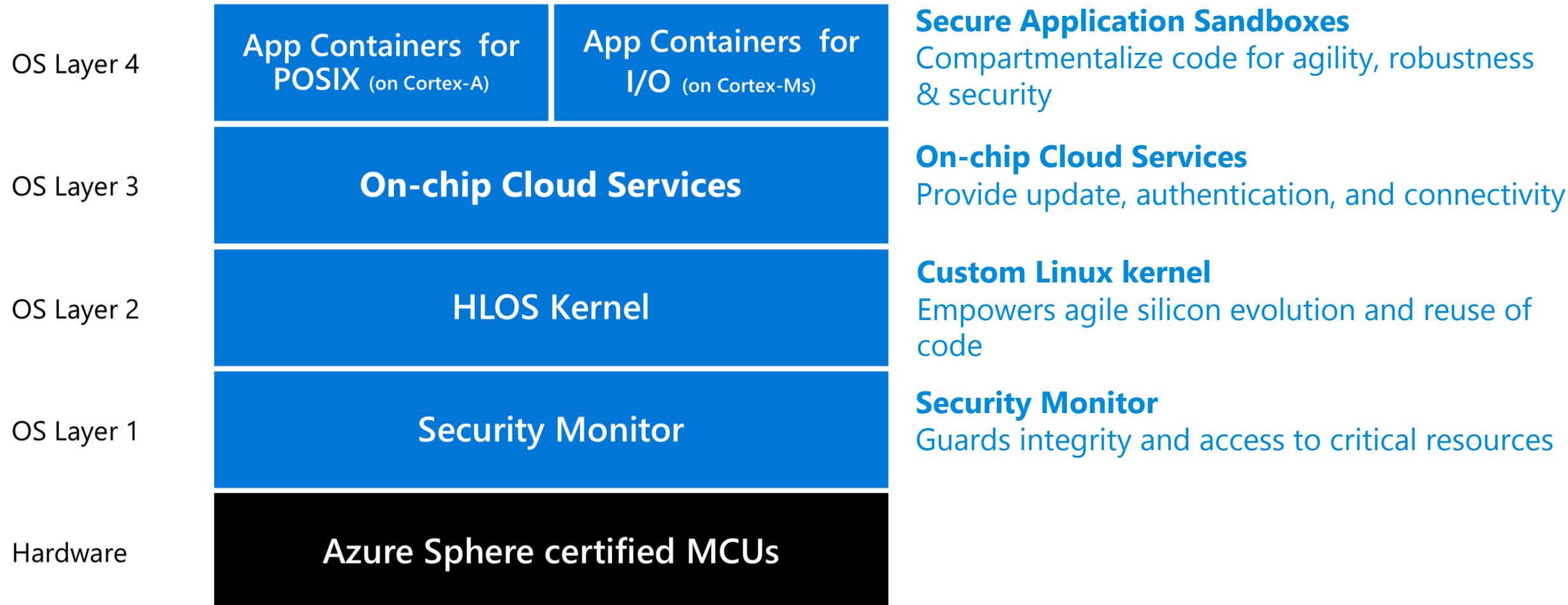
Toshiba



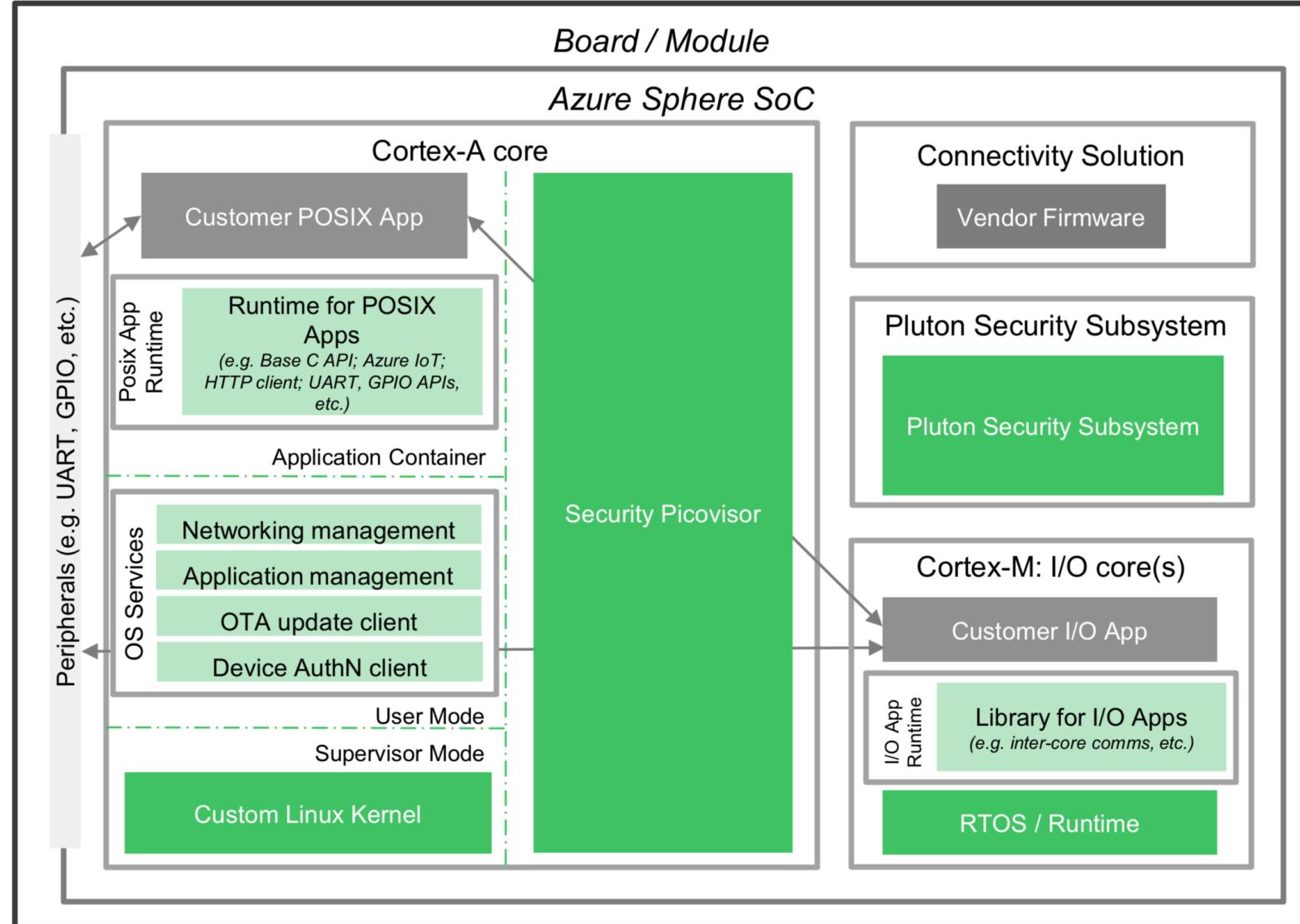
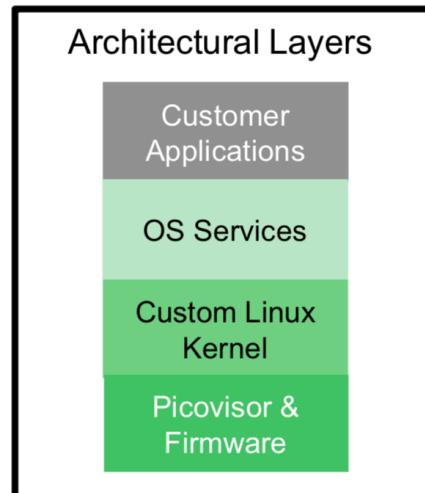
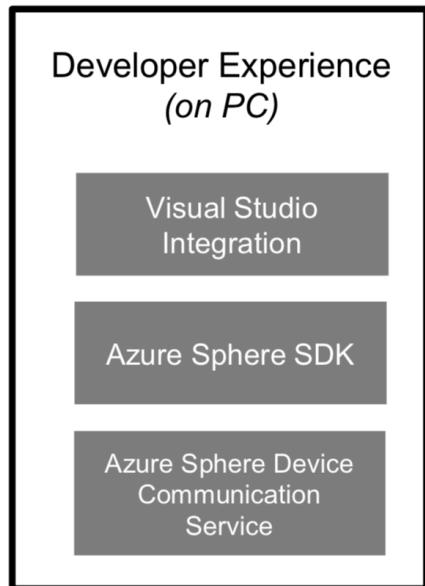
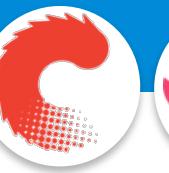
VeriSilicon



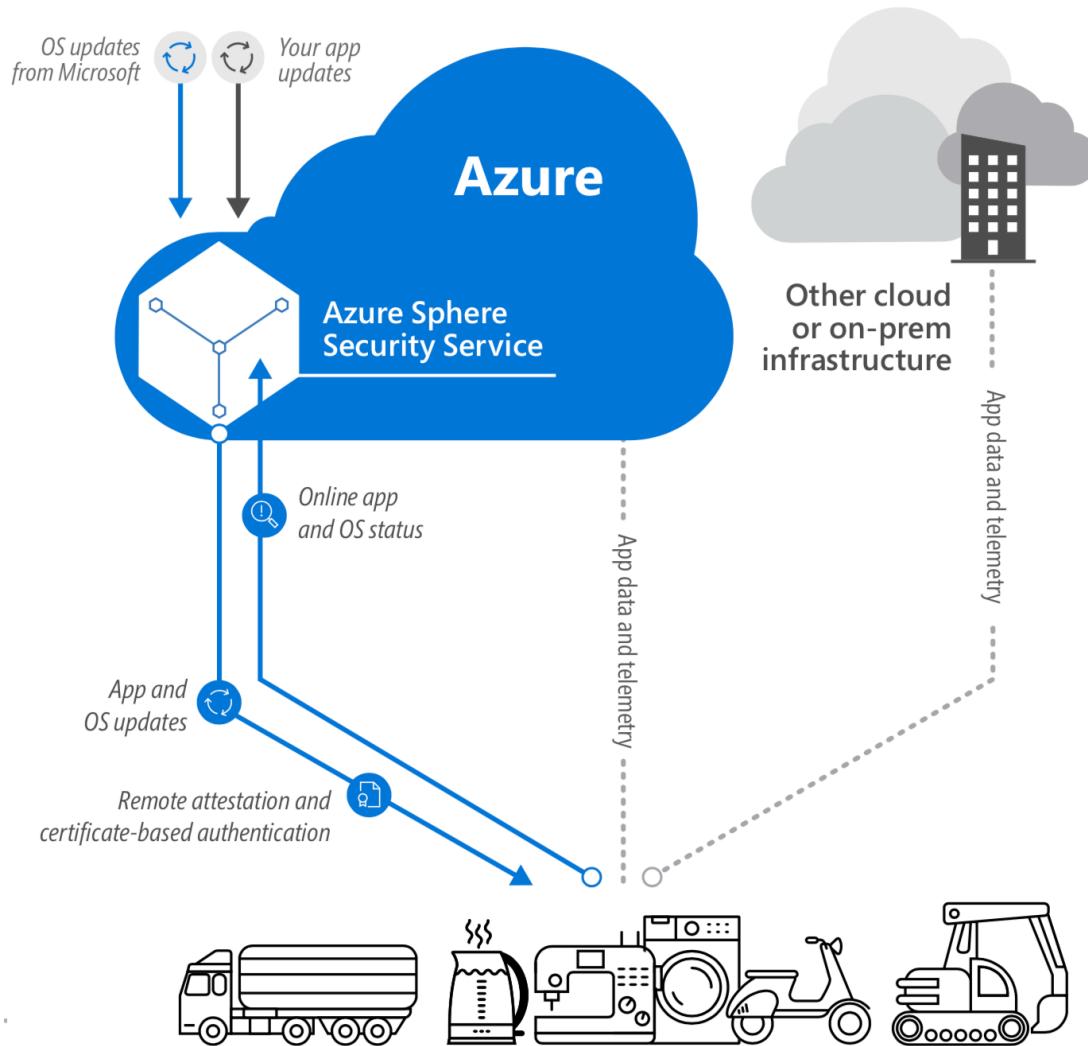
## Azure Sphere OS Architecture



# Azure Sphere OS | Basic Architecture



# Azure Sphere Cloud Security Service



The Azure Sphere Security Service connects and protects every Azure Sphere device

**Protects** your devices and your customers with certificate-based authentication of all communication

**Detects** emerging security threats through automated processing of on-device failures

**Responds** to threats with fully automated on-device updates of OS

**Allows** for easy deployment of software updates to Azure Sphere powered devices

# Azure Sphere and Visual Studio



## Modernize MCU development with Azure Sphere and Visual Studio

### Simplify development

Focus your device development effort on the value you want to create

### Streamline debugging

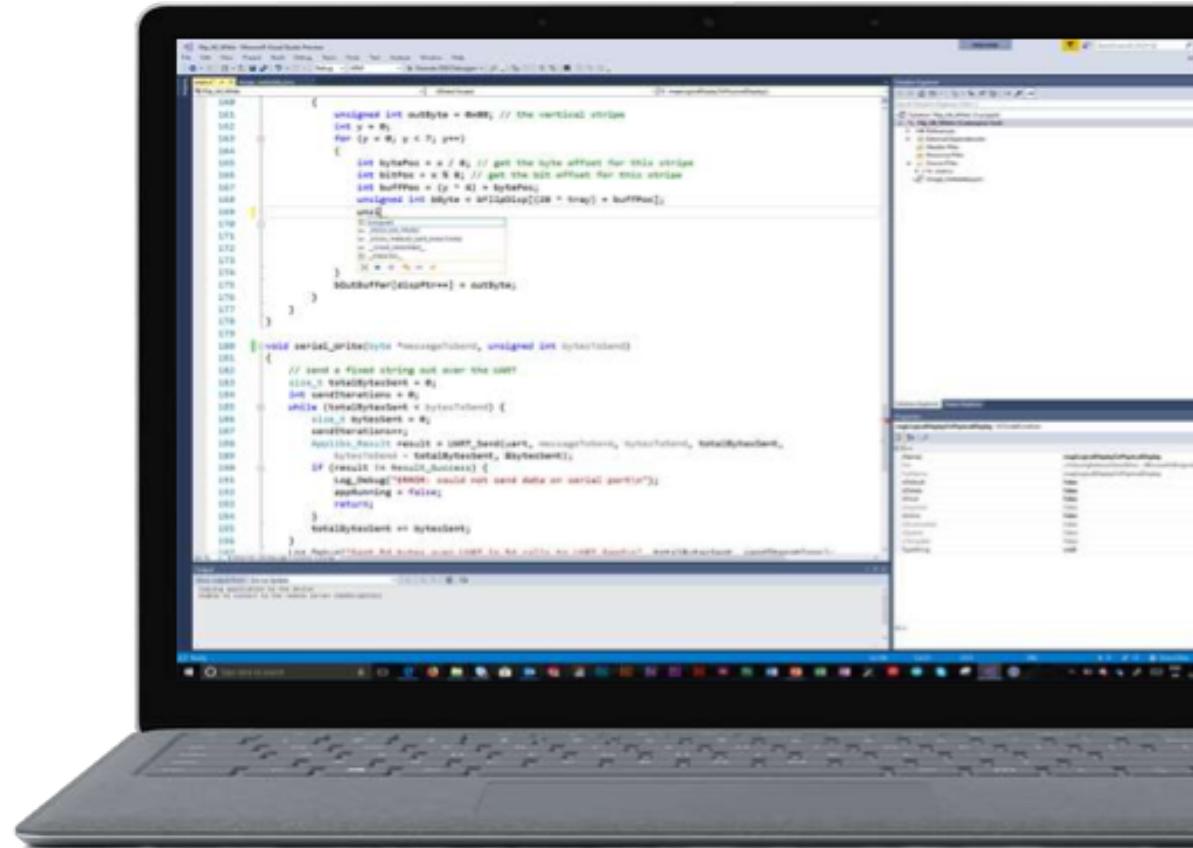
Experience interactive, context-aware debugging across device and cloud

### Collaborate across your team

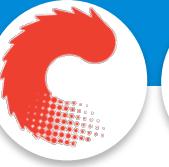
Apply tool-assisted collaboration across your entire development organization

### Simplify Azure connect

Connect your Azure Sphere devices quickly and easily to Azure IoT



# Azure Sphere is open



## **Open to any MCU manufacturer**

We are licensing our Pluto security subsystem royalty free for use in any chip\*

## **Open to any cloud**

Azure Sphere devices are free to connect to Azure or any other cloud, proprietary or public for application data

## **Open to any innovation**

MCU manufacturers are free to innovate with our GPL'd OSS Linux kernel code base

\* Azure Sphere branding requires an Azure Sphere chip with Azure Sphere OS and Azure Sphere Security Service

# Getting started



An [Azure Sphere development kit](#)

A PC running [Windows 10 Anniversary Update](#) or later

Visual Studio 2017/9 Enterprise, Professional, or Community, version 15.7 or later

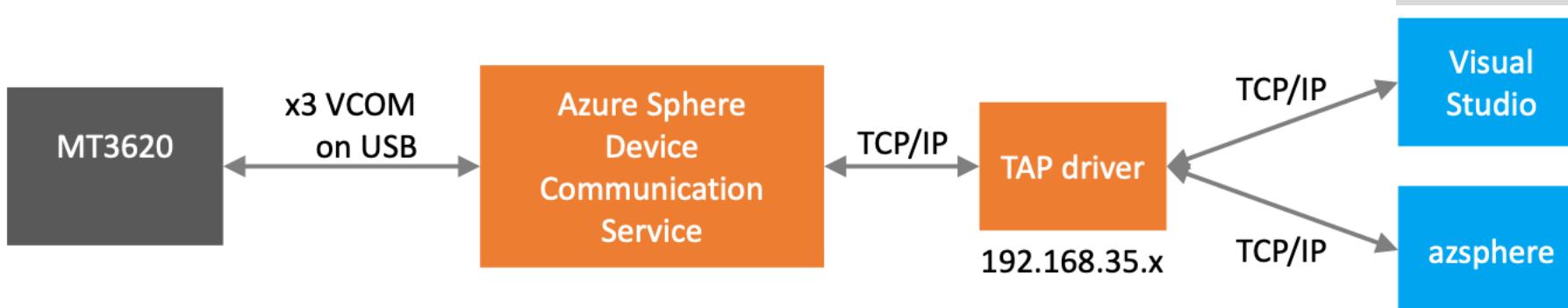
Download the [Azure Sphere SDK for Visual Studio Preview](#).

- Azure Sphere Developer Command Prompt Preview
- Visual Studio Tools Preview for Azure Sphere
- Open VPN TAP driver
- Azure Sphere Device Communication Service

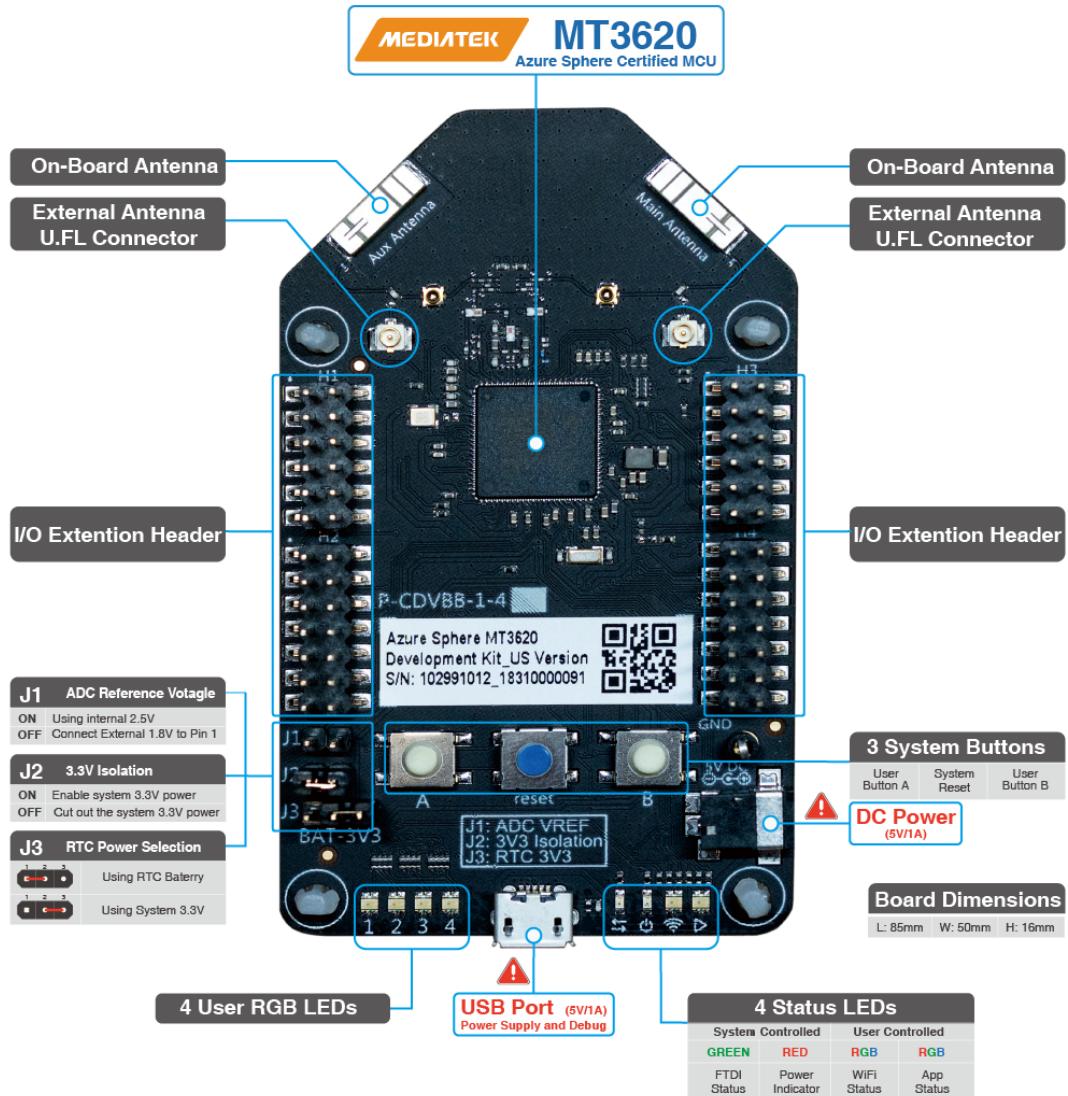
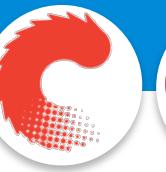
The current SDK does not support all features of the MT3620 hardware. The following are not yet supported:

- 2 x ARM Cortex-MA with FPU
- ADC, I2S, PWM peripheral interfaces

**Microsoft acquires Express Logic, accelerating IoT development for billions of devices at scale - ThreadX RTOS**



# Azure Sphere MT3620 Development Kit



## Hardware

### MCU

#### MT3620

- 1 \* ARM Cortex A7 core @500MHz, 4MB RAM
- 2 \* ARM Cortex M4 core @200MHz, 64KB RAM

### ISU

#### 4 \* "ISU" serial interface which can be configured as:

- I2C runs at up to 1MHz
- SPI runs at up to 40MHz,
- UART runs at up to 3Mbps

### Connectivity

2.4/5GHz dual-band 802.11 b/g/n Wi-Fi

### I2S

1 \* I2S support slave and TDM slave mode

### ADC

4 \* 12-bit ADC input I/O

### RTC

1 \* RTC with CR2032 3V battery holder

### USB

1 \* Micro USB port for power supply and debugging, 5V/1A

### DC Jack

1\* 5V/1A DC power jack

### Operating Temperature

-40~85°C

### Dimensions

L:85mm\*W:50mm\*H:16mm

### Certification

CE / FCC / MIC / RoHS

## Software

### IDE

Visual Studio

### System

Windows 10

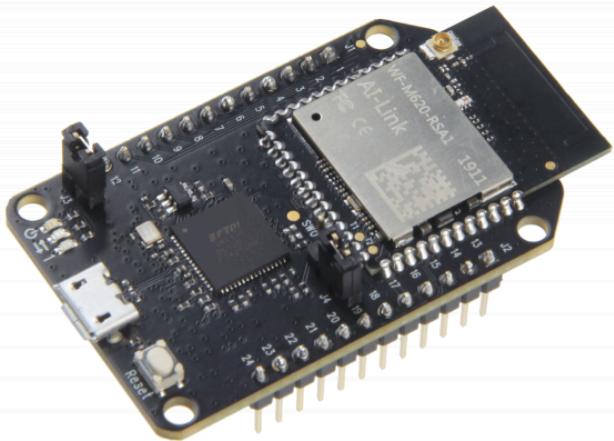
### Language

C

# MT3620 boards



## MT3620 Mini Dev Board



## MT3620 Module



### Specification

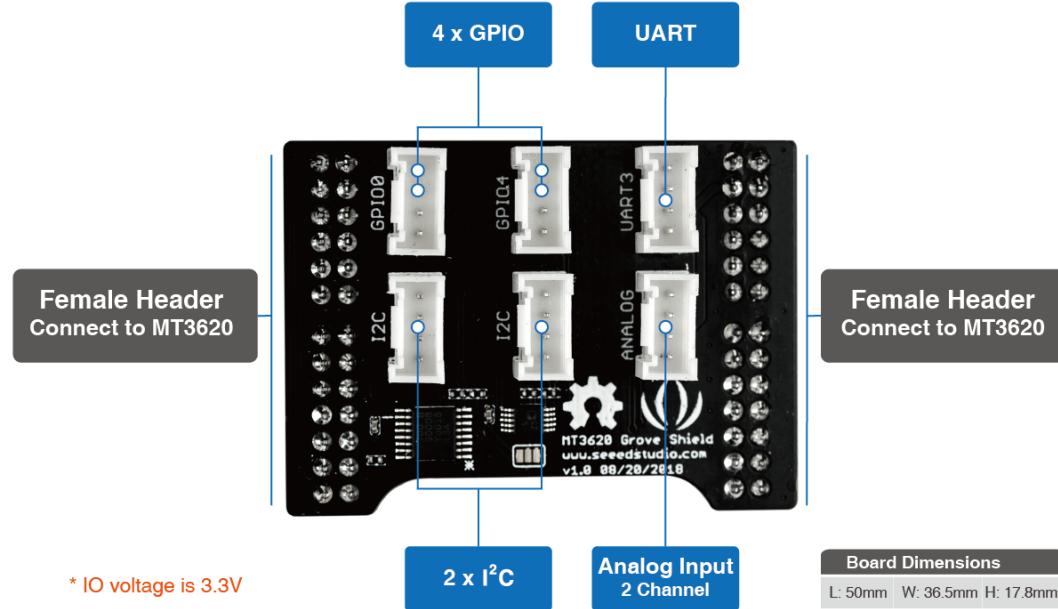
<b>MCU</b>	<b>MT3620</b> <ul style="list-style-type: none"><li>1 * ARM Cortex A7 core @500MHz , 4MB RAM</li><li>2 * ARM Cortex M4 core @200MHz , 64KB RAM</li></ul>
<b>Interface</b>	ISU0(configured as SPI 0 or UART 0) ISU1(configured as SPI 1 or UART 1 or I2C 1) PWMx8: PWM4~PWM11 ADCx4: ADC0~3 GPIO: 14 GPIO pins with multi-functions
<b>Connectivity</b>	802.11 b/g/n Wi-Fi
<b>Antenna Type</b>	Integral PCB Trace Antenna/Option to fit IPEX connector for external antenna
<b>Operating Temperature</b>	-40~85°C
<b>Dimensions</b>	L:30mm*W:22mm*H:2.5mm±0.2mm
<b>Certification</b>	CE / FCC / MIC / RoHS

\*\*\* This Azure Sphere development kit can be only used for prototyping. It cannot be built into a product for commercial distribution. It cannot be re-sold or used as part of a production environment. \*\*\*

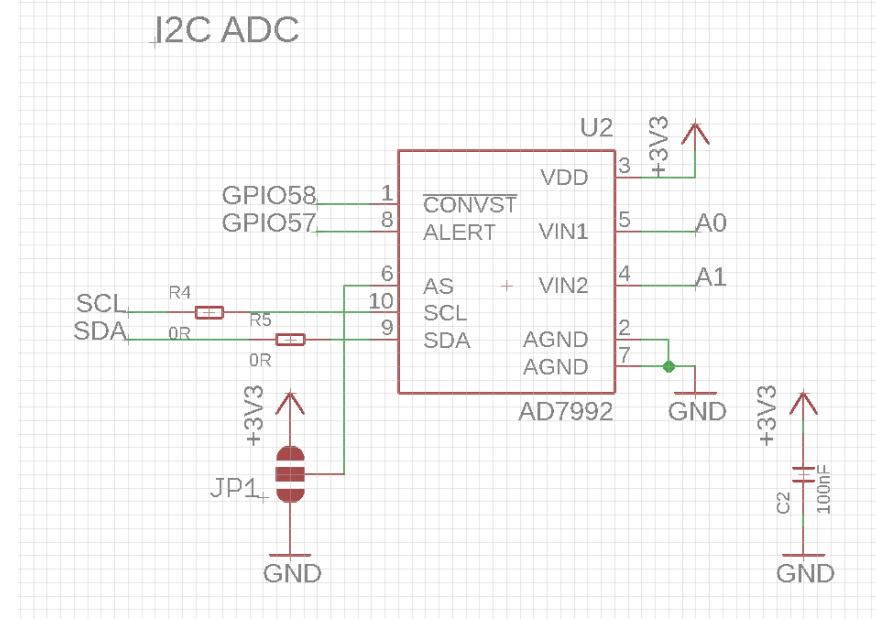
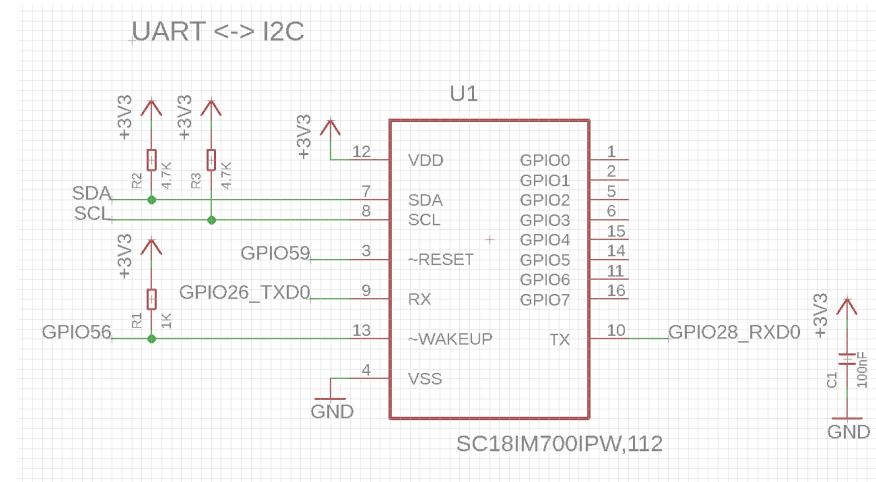
# MT3620 Grove Shield

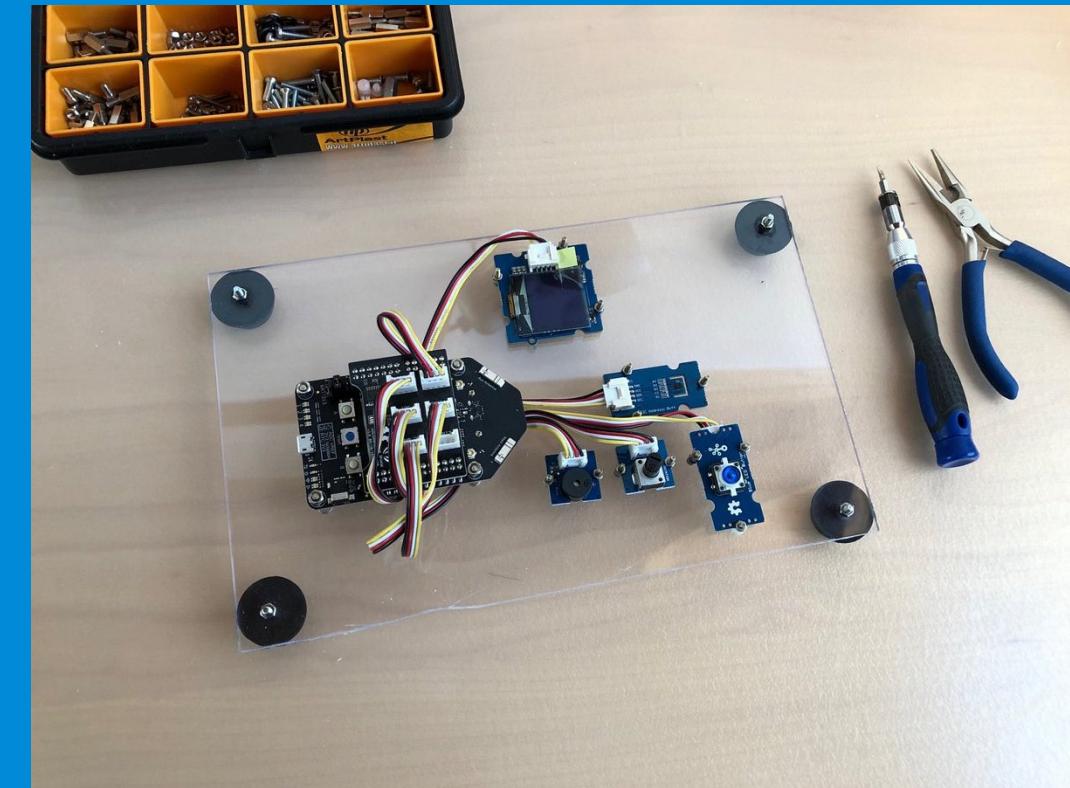


CloudGen  
omindi verso l'evoluzione



<b>UART to I<sup>2</sup>C</b>	NXP SC18IM700IPW,128 • Master I <sup>2</sup> C-bus controller with UART interface
<b>ADC</b>	ADI AD7992BRMZ-1 • 12-Bit ADC with I <sup>2</sup> C-Compatible
<b>IO Voltage</b>	3.3V DC
<b>Operating Temperature</b>	-40~85°C
<b>Dimensions</b>	L:50mm*W:36.5mm*H:17.8mm





Azure Sphere MT3620 Development kit

Rotary Angle Sensor

Buzzer

Blue LED Button

Temp&Humi Sensor (SHT31)

OLED Display 1.12" V2

# Recap



Azure Sphere is not a single chip but a security solution / technology built with a combination of a special microcontroller, a special operating system and the corresponding cloud services.

Azure Sphere is a high-value, cost effective solution, secured by Microsoft.

The solution today contains:

**Azure Sphere Chip MT3620**

**Azure Sphere Security Services** for 10 years

**Azure Sphere IoT OS** with 10 years of on device updates





# Thanks

Questions?



<https://github.com/MircoVanini>



@MircoVanini



<https://it.linkedin.com/in/proxsoft>