Windows 10

# Windows IoT

Thomas Pfenning
8/1/2017

# IoT Market: Three Classes of Devices

| | **PC-Like Embedded Devices**<br>~100 million units<br>*ATM, Retail Point of Service* | **Smart Things**<br>~800 million units<br>*PLC, Edge Gateway, Thermostat* | **Things**<br>~9 billion units<br>*Temp Sensor, Lightbulb* |
|---|---|---|---|
| Typical Silicon BOM | Intel Core<br>$100+ | ARM Cortex-A7, Intel Atom<br>$5-50 | MCU<br>$0.50-5 |
| Typical OS | Windows Embedded, Linux | QNX, Wind River, Android Things | FreeRTOS |
| Typical Runtime | Win32 | Node.js, Python, C APIs | C APIs |
| MSFT Offering Cost | Windows IoT Enterprise<br>$30-120 + Services | Windows IoT Core<br>$0 + Services | |

**Smart Things Trends**

1. Fragmented silicon market in Smart Things, fuzzy line between Smart Things and PC-Like Embedded
2. Partners are still specialists per sub-vertical, but are selling more end-to-end solutions including services
3. OS volume shifted from pay RTOS to Linux and Android
4. Data processing moving to edge: compute power, lower bandwidth and latency

# Windows 10 IoT Editions

## Windows 10 IoT Enterprise

2GB RAM, 16 GB Storage | X86/X64

## Windows 10 IoT Mobile

1 GB RAM, 4 GB Storage | ARM

## Windows 10 IoT Core

256MB RAM, 2GB Storage | X86/X64 or ARM

## Secure and Manageable Platform

**Powerful Industry Devices**

Rich user experience

Lockdown and multi user support

Windows 32 and UWP apps

**Ruggedized Handheld Devices**

Modern Shell and UWP apps

Lockdown and role support

ARM support

**Small and low-cost Smart Things**

Single purpose device experience

UWP apps

Low-cost silicon

# GETTING THE BEST OF BOTH WORLDS

Secure systems
and peace of mind

Benefits of cloud
connected solutions

# IoT End-to-End Security Offering & Investment Opportunity

## Protect

### Core HW & Platform

Malware resistance w/ **SecureBoot***

Securing keys in the **TPM***

Information protection for data at rest with **BitLocker***

Execution control via **DeviceGuard***

Security **updates** via WU*

Malware protection with **Windows Defender AV**

### Trusted Execution Control

**Secure point-to-point communication from cloud to IO pin**

**Securing IO** operations through policy-based execution on cyber physical systems (CPS)

**Non-repudiated auditing** for tamperproof logging

### Health Attestation

Security related data points validated by **Remote Health Attestation Service**

**Measured boot data**, protected by the TPM, sent to service for verification

**Conditional Access** to sensitive assets based on a health assessment of the device

## Detect

### Windows Defender ATP

**Advanced Threat Protection** with cloud-powered, behavioral-based, post-breach detection

**Anomaly detection**, combined with Microsoft threat intelligence knowledge base

**Forensic investigation and mitigation** capabilities

## Remediate

### Portals and DM

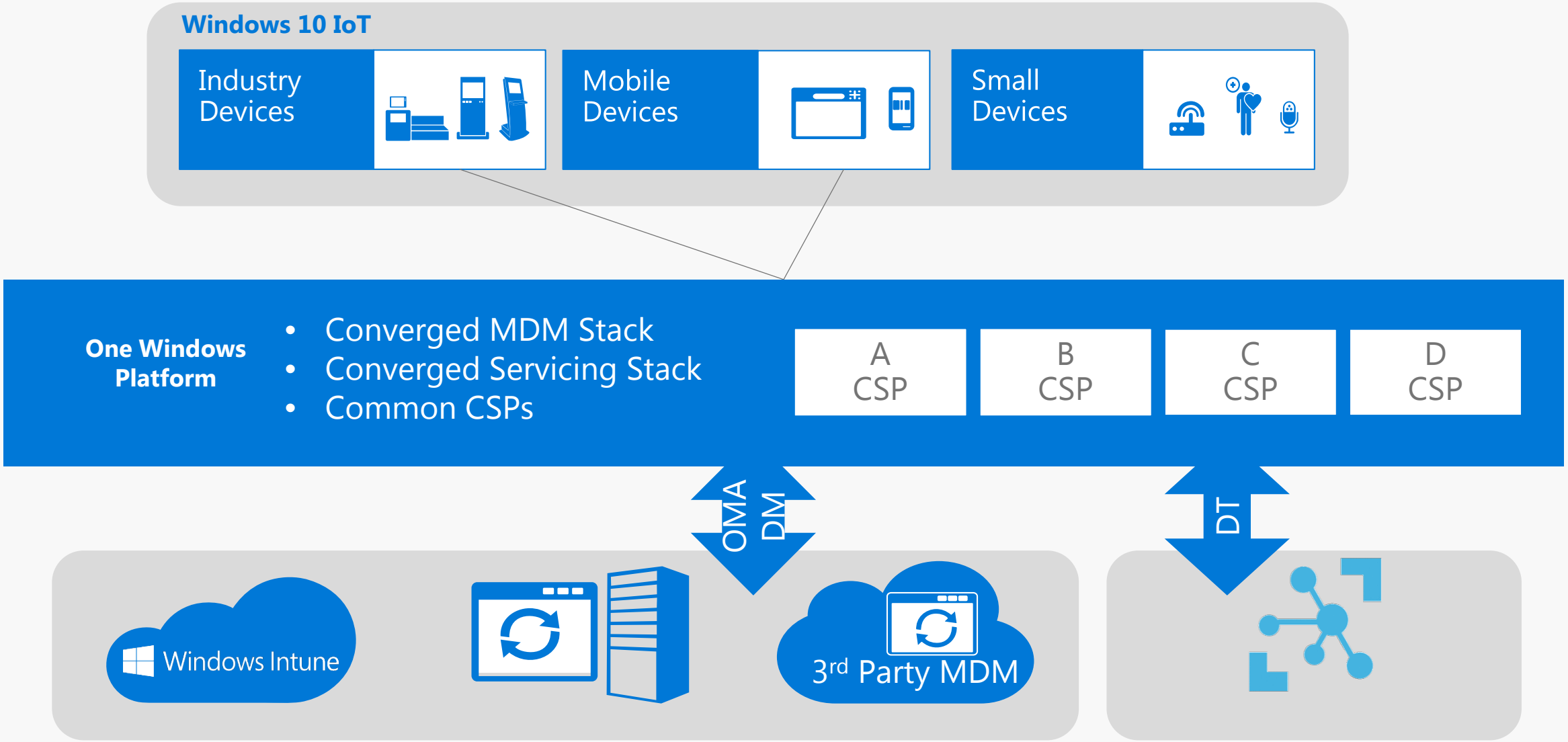
Portal with a view to threats identified within the network, including deep analytics, historical data points and the ability to **respond** to threats

**Remediate** the affected device **via DM** (e.g. flash the device)

* Feature currently supported on IoT Core RS2

# Consistent Device Management Capabilities

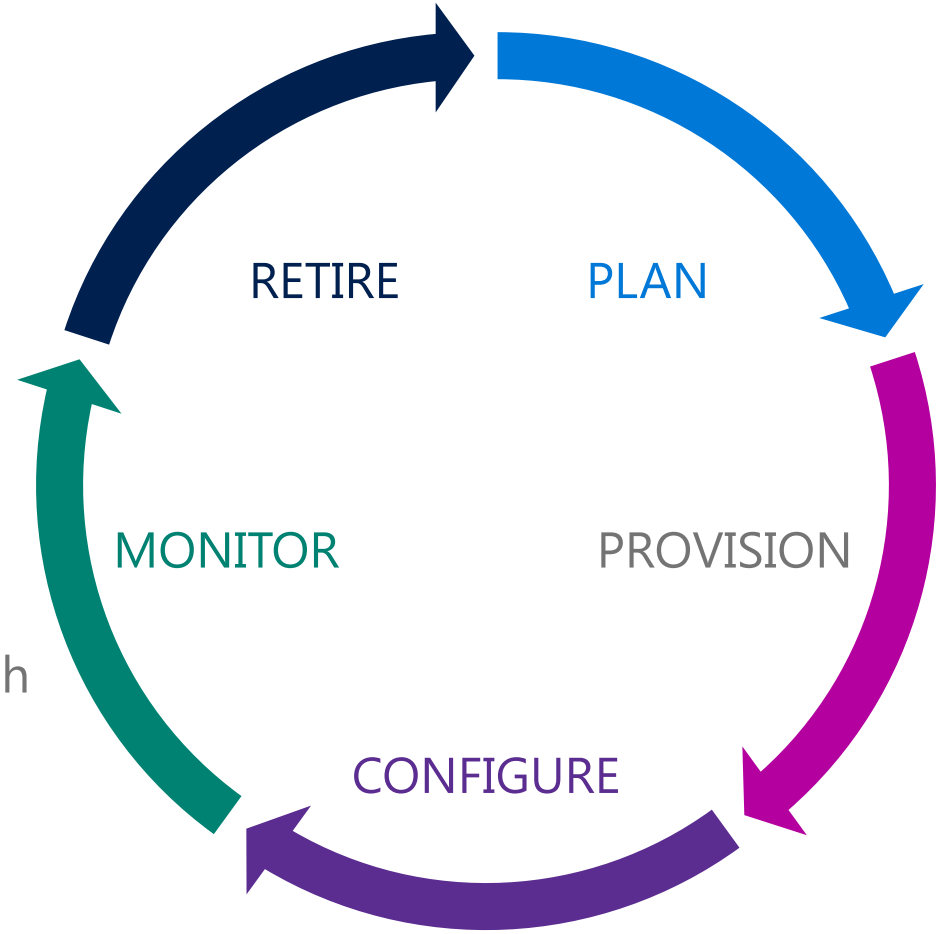
for all Windows 10 IoT devices



# Easier to manage devices at scale

Replace or decommission devices after failure, upgrade cycle or service lifetime

Group devices and control access according to your organization's needs

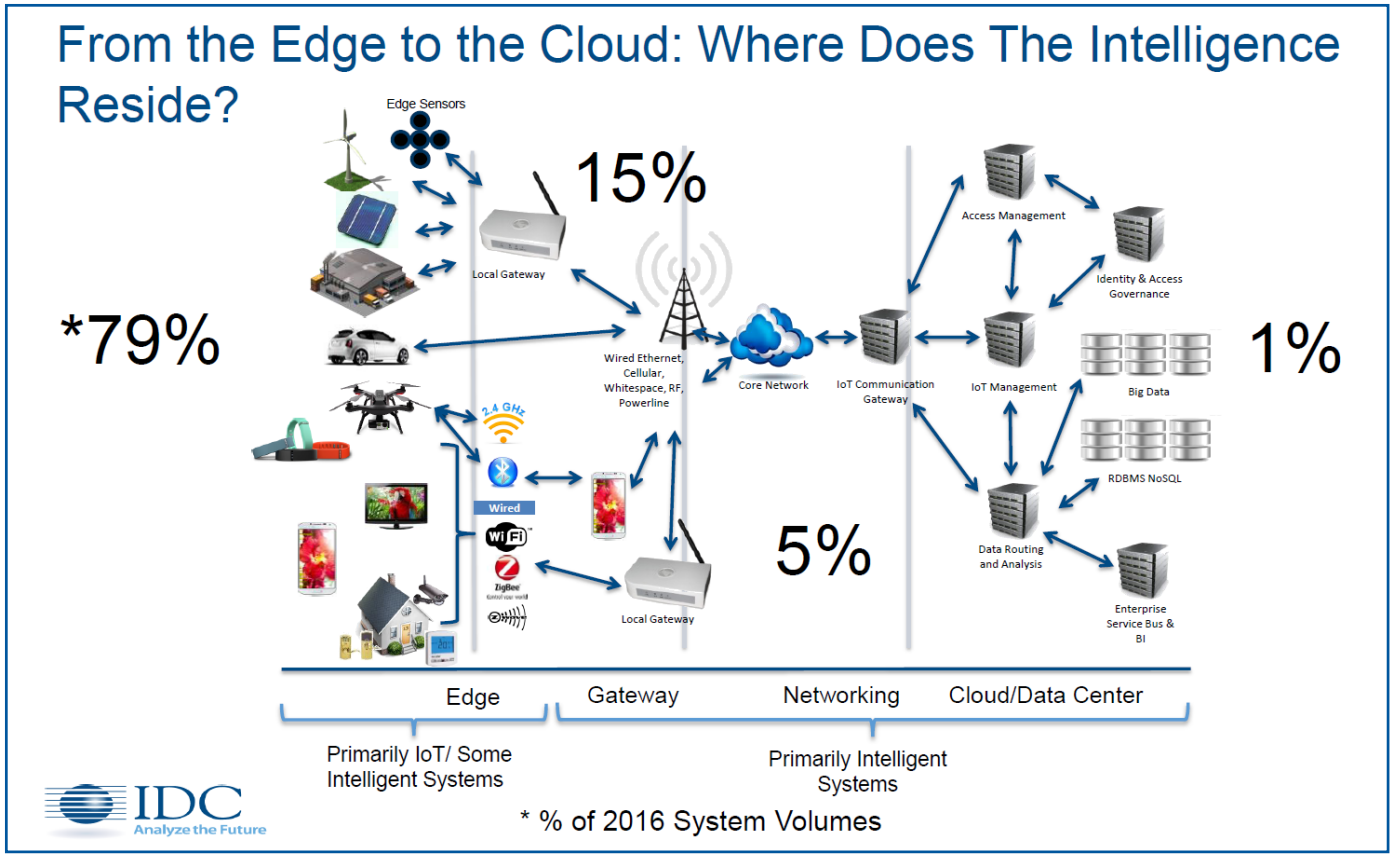



Monitor device inventory, health & security while providing proactive remediation of issues

Securely authenticate devices, on-board for management and provision for service

Provide updates, configuration & applications to assign the purpose of each device

# Intelligence at the Edge




- Led by Automotive, there is a growing push to improve semiconductors for advanced analytics at the edge and the cloud
- Smart gateways can act as a hub to ensure that data is analyzed in the optimal location, whether that is the cloud or the edge
- Efficient coprocessors allow for the processing acceleration needed to create edge and gateway devices that understand and learn from their environment

- IDC estimates that 1% of devices sit in the “cloud” while the remainder sit at “edge” or “fog”
- Demand for edge analytics driven by security, reliability, and efficiency

# Significant Silicon Investment at the Edge

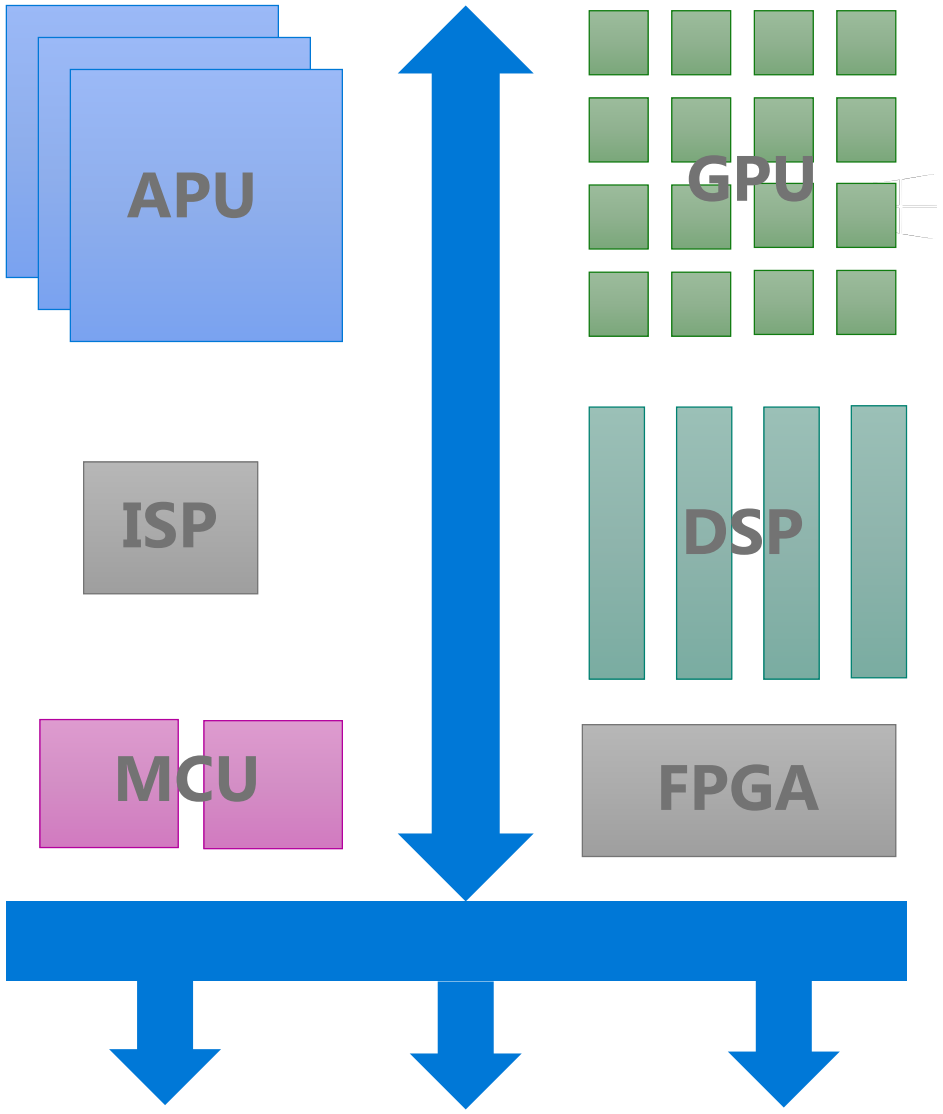
SoC dynamics have resulted in complex clusters of large and small APUs, accelerators, dedicated function cores

Constant flow of additional silicon to handle market demand for machine vision, AI, AR/VR, software defined radio, spatial audio, …

Qualcomm – CPU, GPU, DSP, ISP, Neural Processor

Intel – CPU, GPU, Sensor Hub, Pattern Matcher, Vision Processor (Movidius), FPGA (Altera)

Other ARM SVs – RT (MCU) cores, GPU, DSP, …

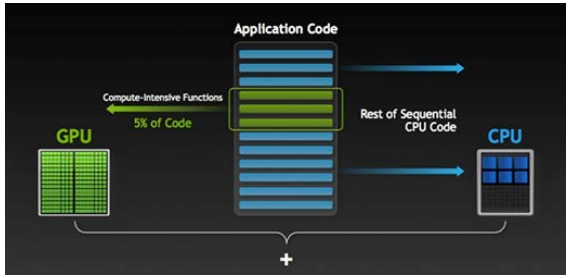


# Innovation Spotlight Topic:

## Semiconductor Innovations Enabling Analytics at the Edge through coprocessors

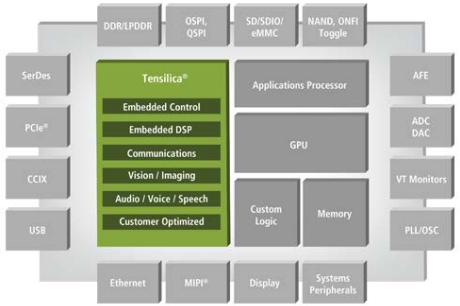
Nvidia Jetson SoC for embedded AI

GPU handles compute intensive deep learning algorithms



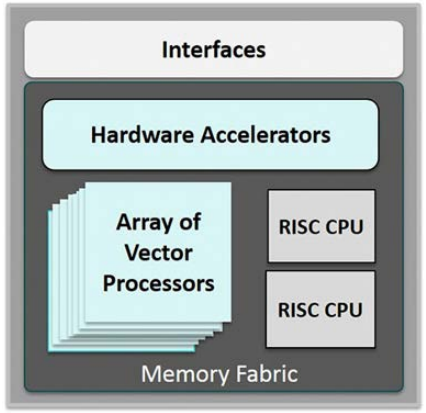

ARM based CPU handles majority of code

Tensilica Customizable Processor IP




IP designed for easy customization to specific workloads

Movidius Myriad 2 VPU




Myriad 2 Vision Processor Unit (VPU)

- Processor designed specifically for vision processing
- Framework to transfer deep learning trained on servers to edge devices

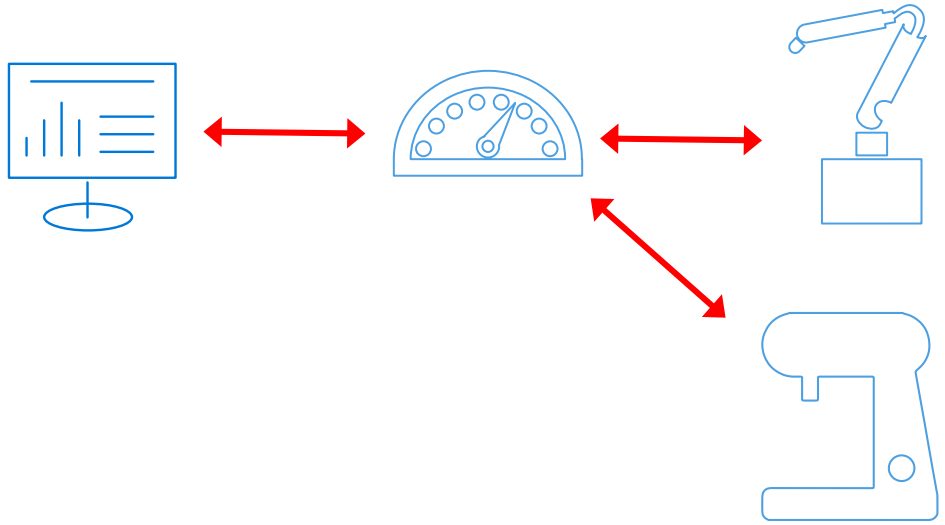
Lattice ICE40 FPGA


reprogrammable for specific algorithms

# Factory Device interoperability

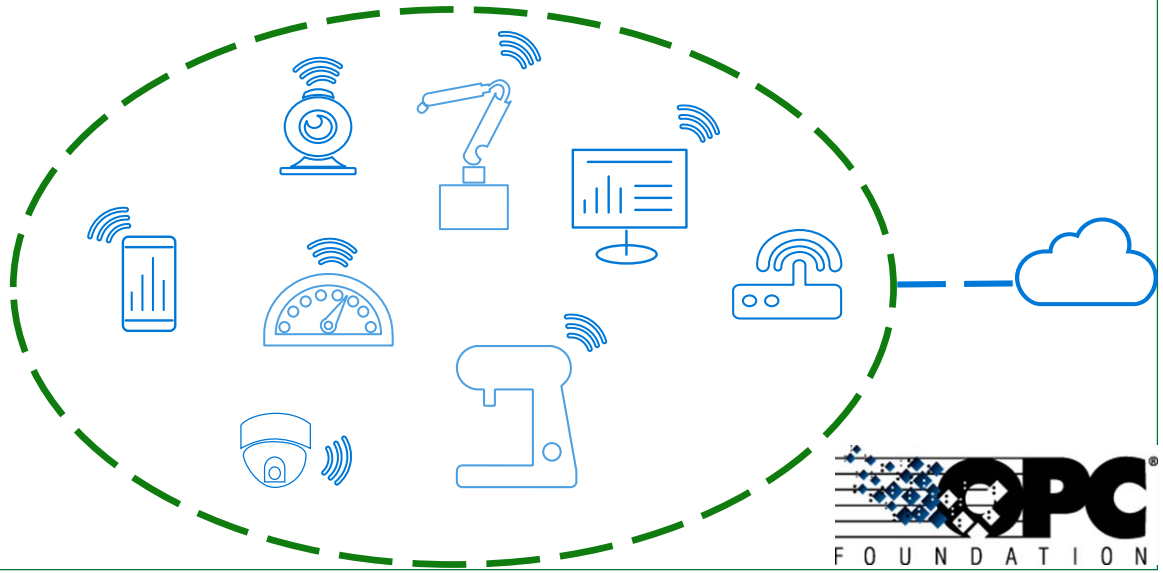
Traditional factories

Traditional factories have been constrained by **siloed legacy platforms** and a lack of interoperability. As **smart connected devices** enter the factory setting, the need for a **unified**, **scalable** industrial communications standard for **reliability** and **manageability** has grown stronger.



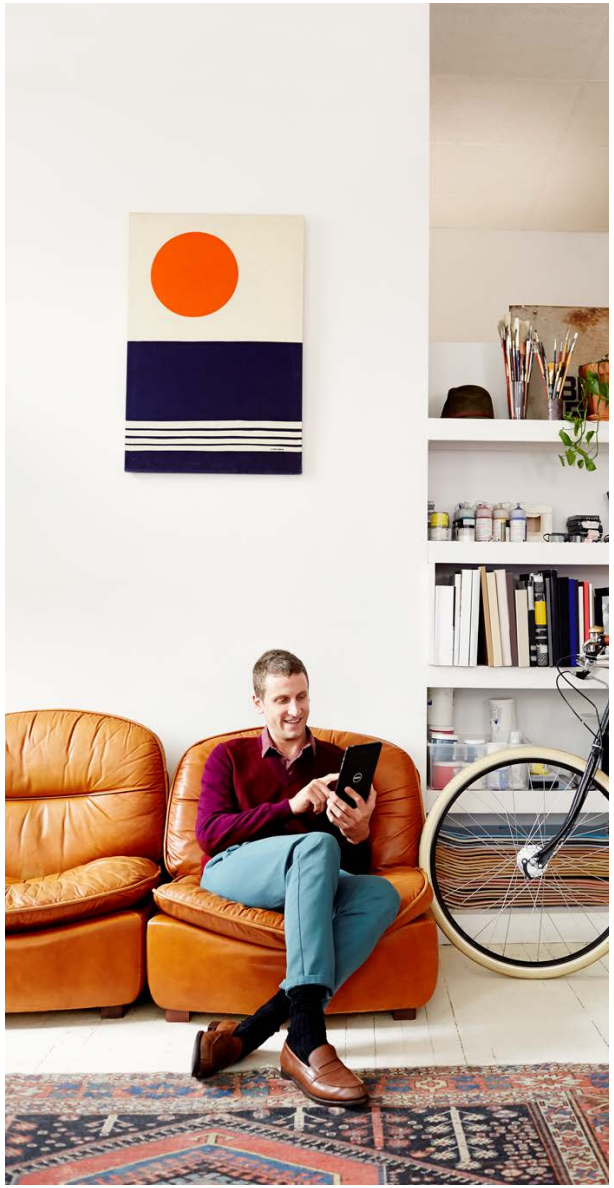
Smart factories

**OPC-UA** is the unified communications standard designed specifically for connecting industrial IoT devices – from basic "things" like attenuators and sensors to smart devices like industrial PCs, industrial IoT gateways, robotic arms, and Programmable Logic Controllers (PLCs) to servers and mainframes.



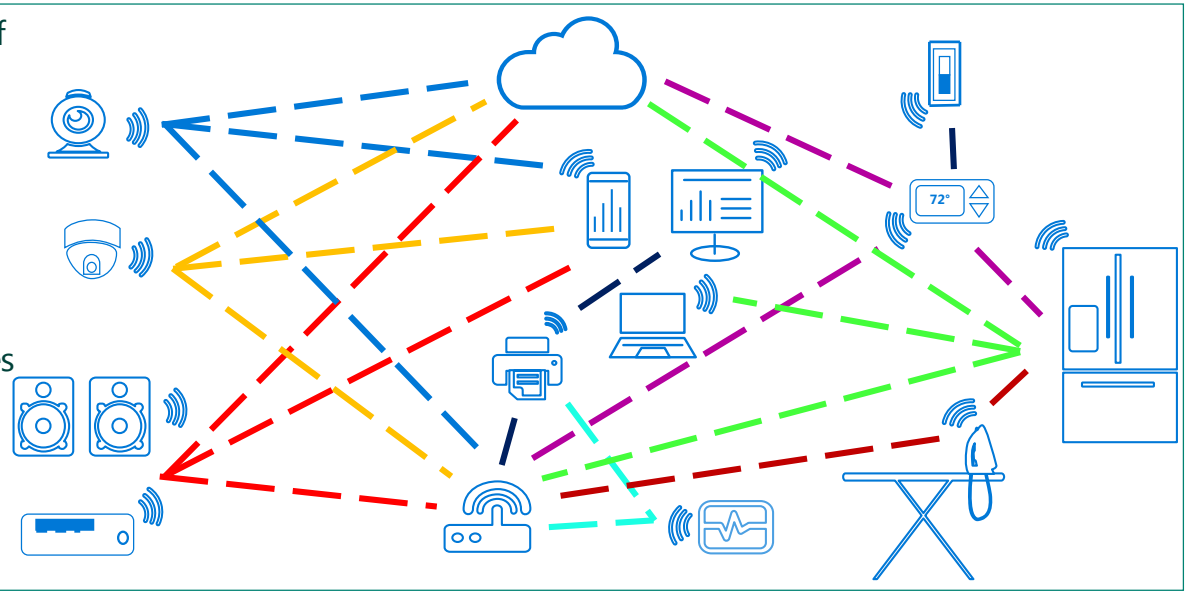
OPC FOUNDATION

# Consumer IoT interoperability



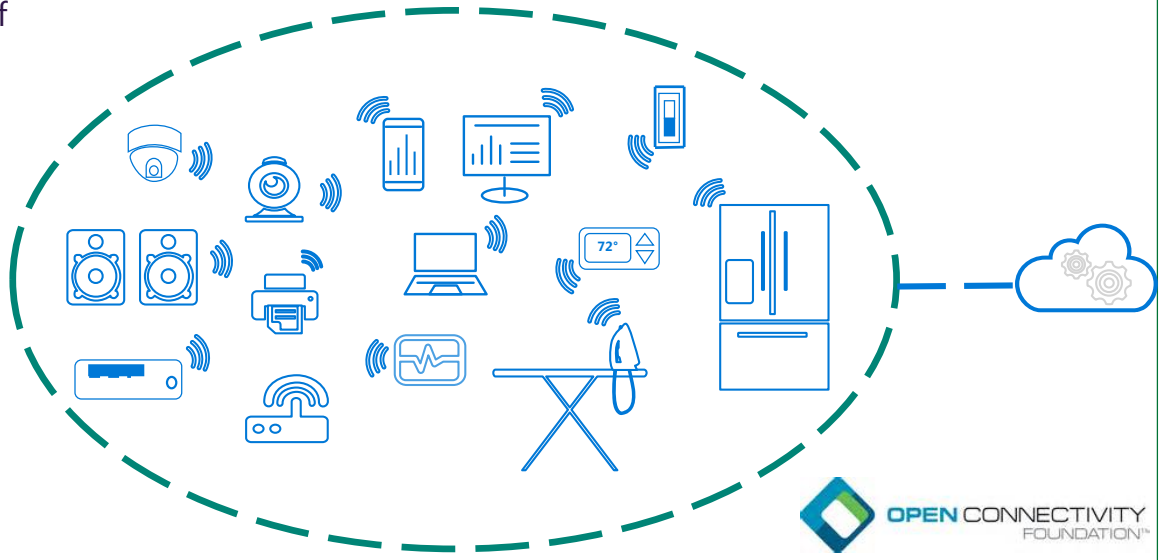
Traditional consumer IoT

The rapid proliferation of IoT devices has resulted in many **different communications standards** and a fragmented IoT device landscape with limited interoperability. Connecting these devices to one another securely becomes more important every day.




Smart consumer IoT

**OCF** solves the problem of interoperability in consumer IoT devices by providing a common communications framework, allowing a broad range of devices to communicate and interoperate **securely**.



Microsoft