Embedded Intelligence:
A Path to Unlocking the value of IoT

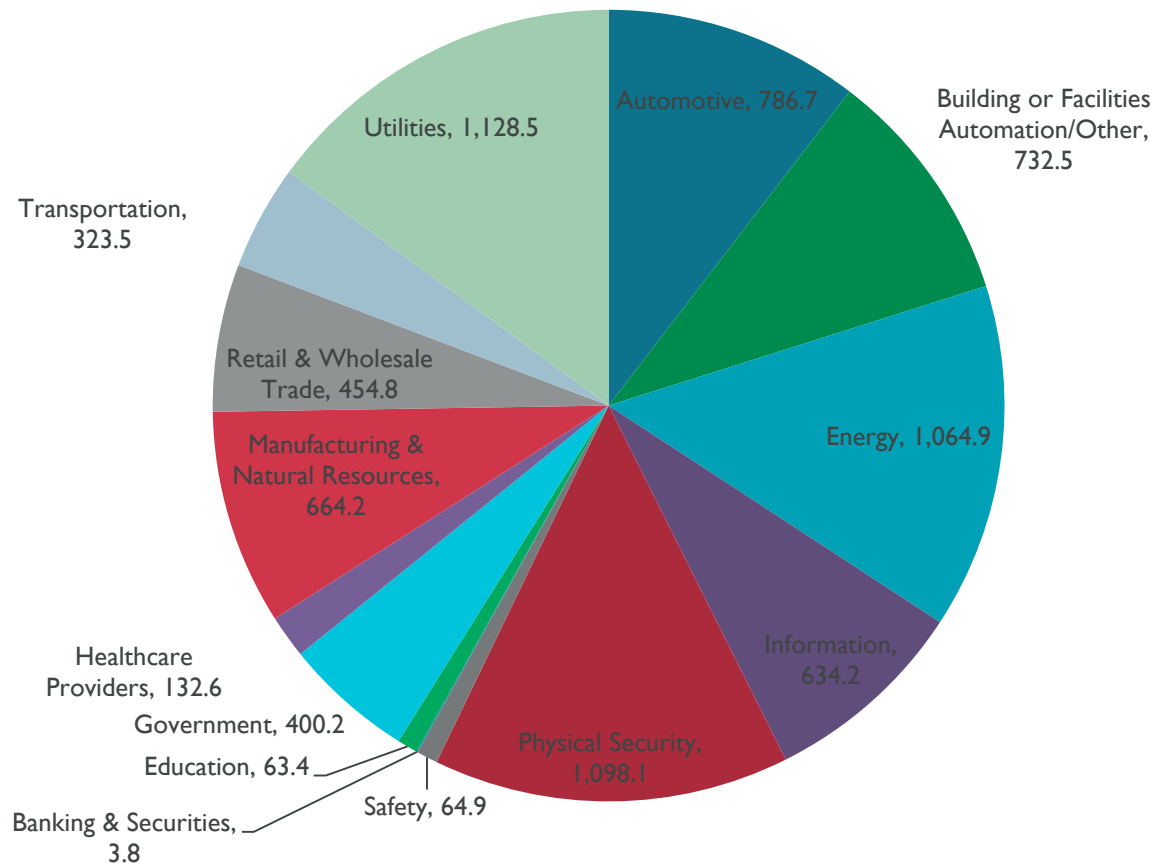**ARM**

Lifeng Geng

IoT Segment Senior Manager

ARM Embedded IoT Seminar
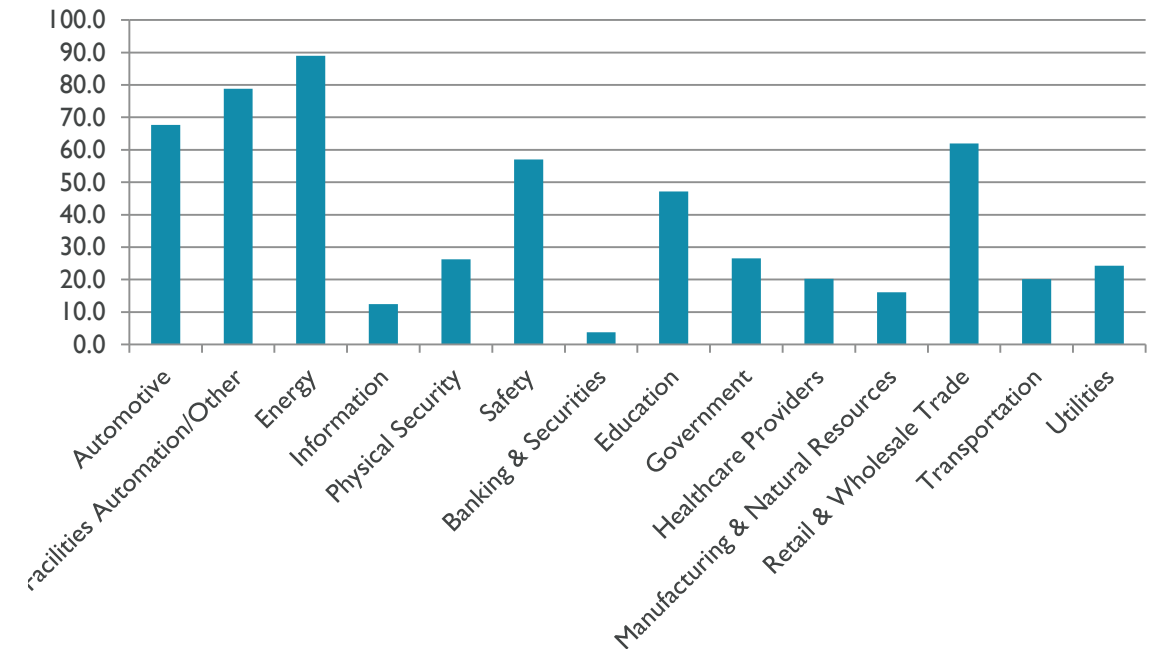July, 2017

Gartner: IoT End Nodes by sectors

2020 Installed Base (Units in MU)

Pie chart sectors:
- Automotive, 786.7
- Building or Facilities Automation/Other, 732.5
- Energy, 1,064.9
- Information, 634.2
- Physical Security, 1,098.1
- Safety, 64.9
- Banking & Securities, 3.8
- Education, 63.4
- Government, 400.2
- Healthcare Providers, 132.6
- Manufacturing & Natural Resources, 664.2
- Retail & Wholesale Trade, 454.8
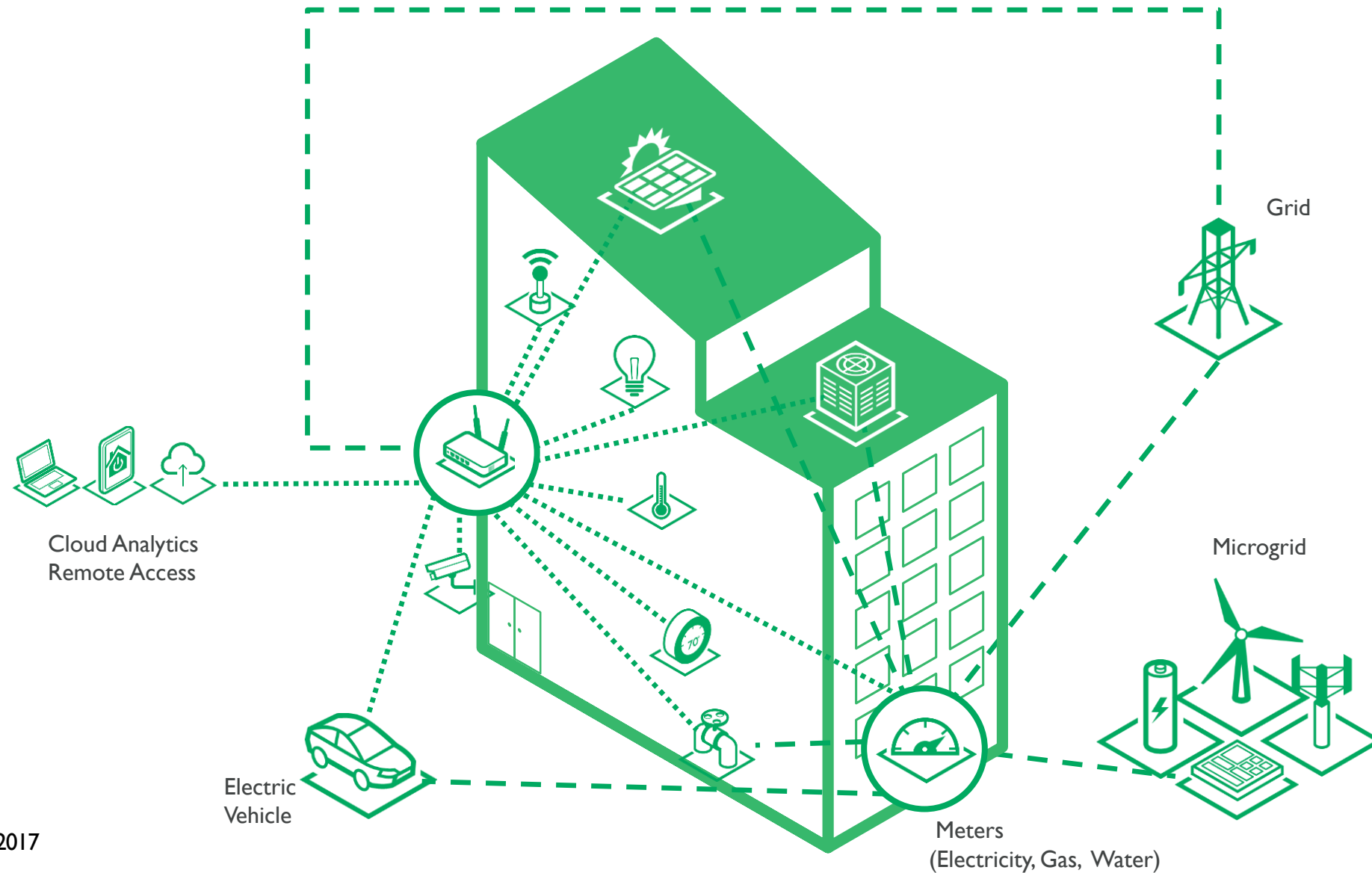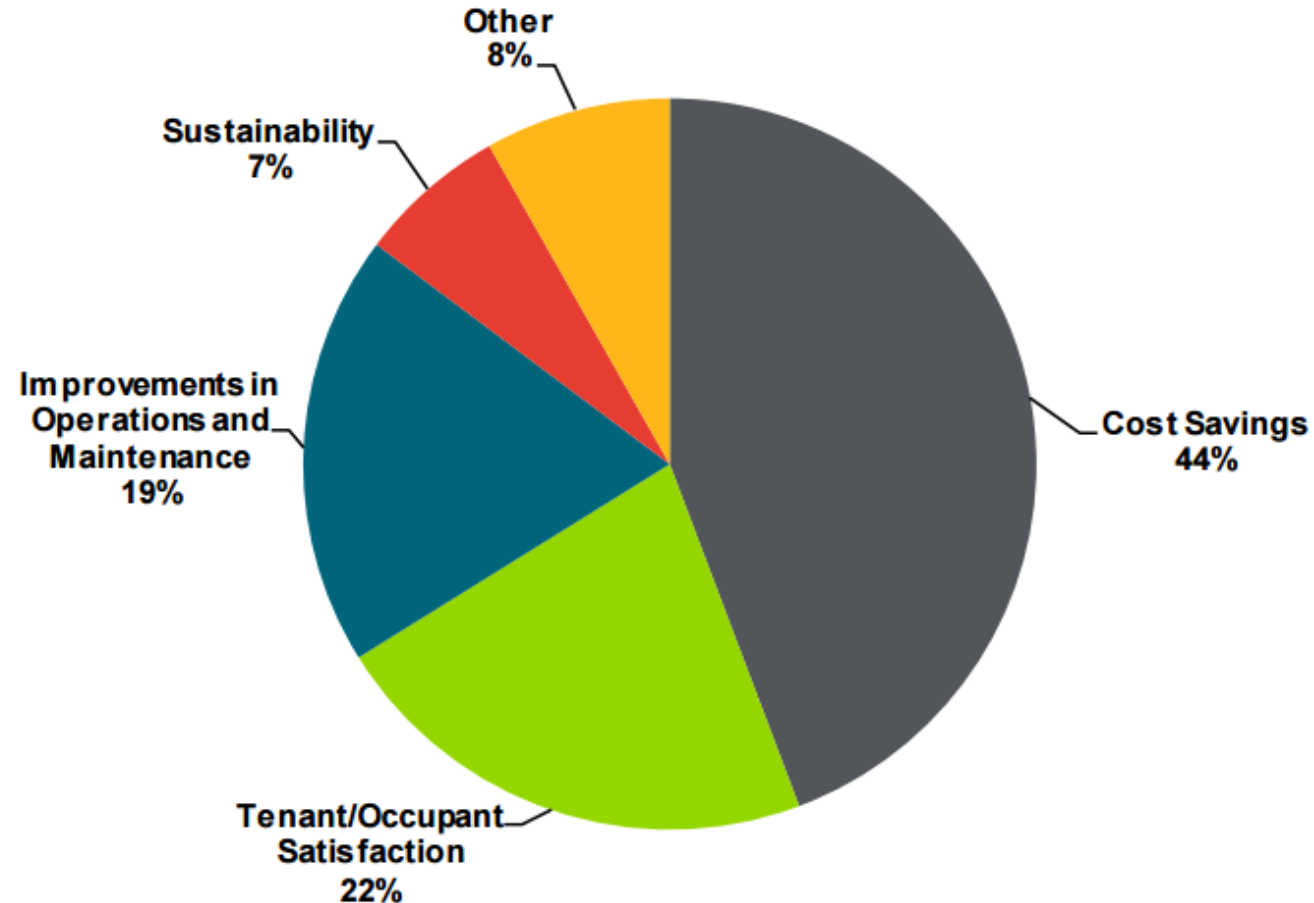- Transportation, 323.5
- Utilities, 1,128.5

2015-2020 CAGR

- Government includes LED street lamps, asset tracking, parking meters
- Utilities include smart meters

ARM

Smart Building / Smart Energy

Grid

Cloud Analytics
Remote Access

Microgrid

Electric
Vehicle

Meters
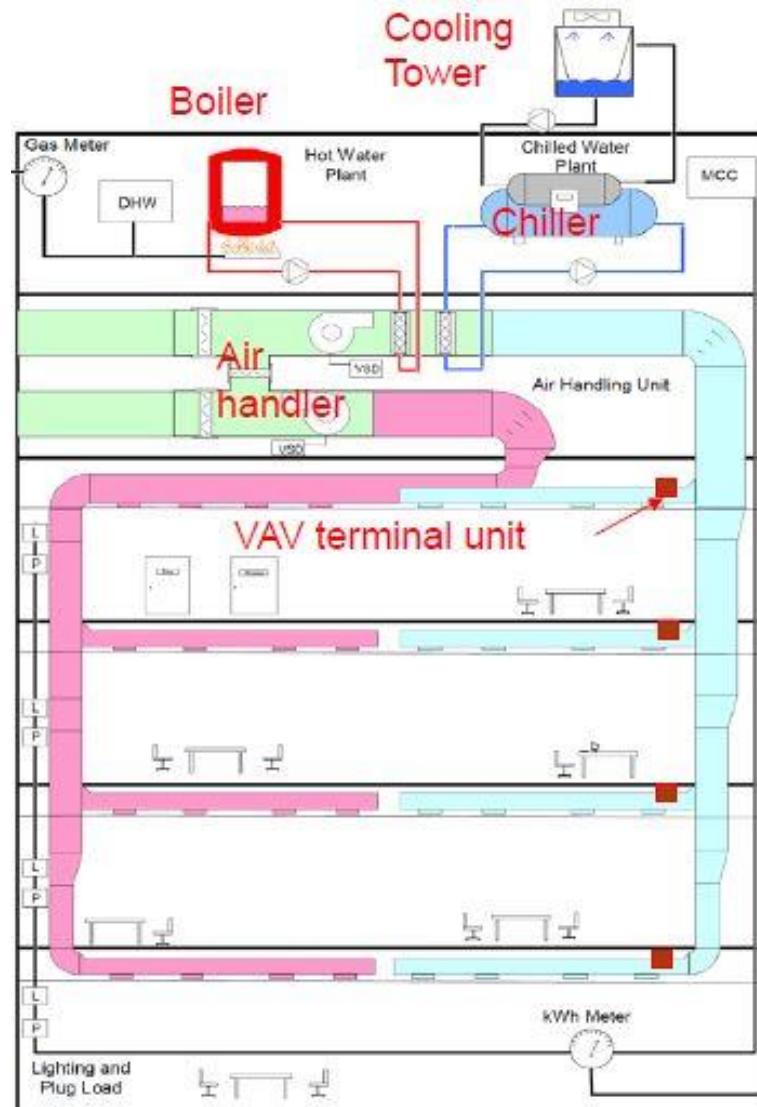(Electricity, Gas, Water)

ARM

Most Influential Drivers in Smart Building

Chart 1   **Most Influential Driver for Investment in Energy Efficiency & Intelligent Building Technologies**
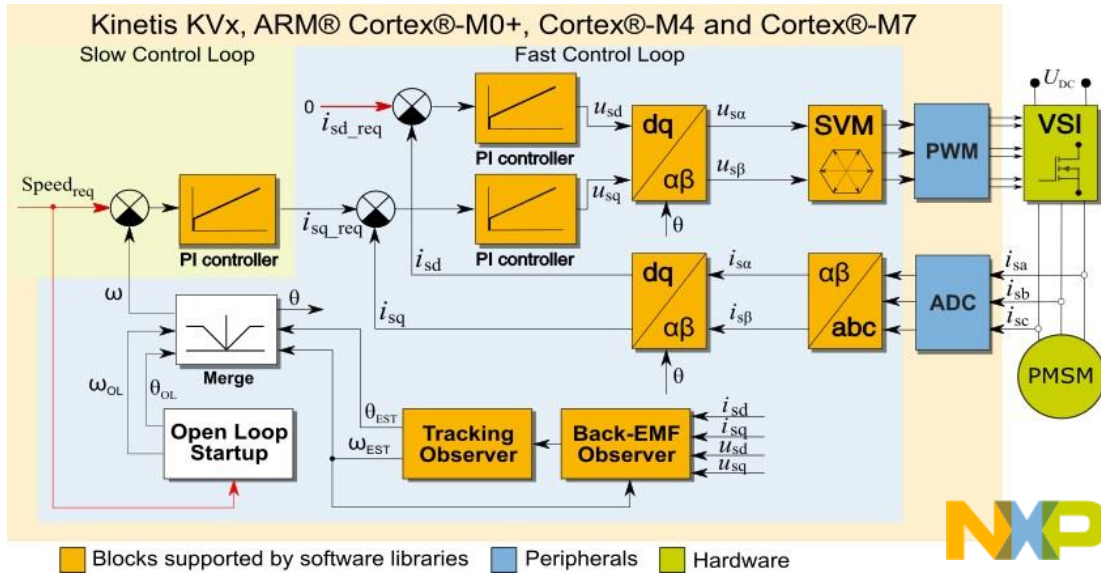
Other
8%

Sustainability
7%

Improvements in
Operations and
Maintenance
19%

Cost Savings
44%

Tenant/Occupant
Satisfaction
22%

(Source: Navigant Research)

ARM

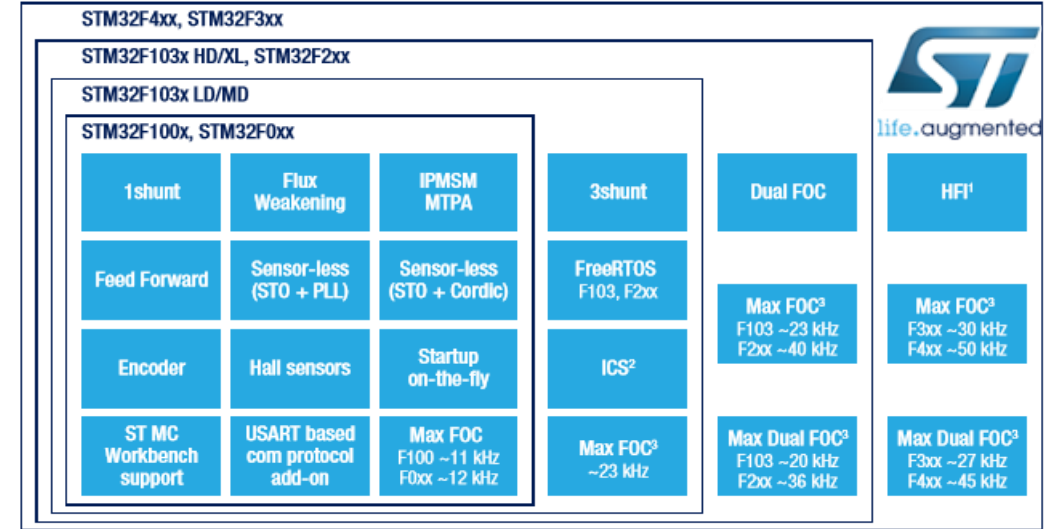# A typical commercial building HVAC system

- **Central Plant:**
  - Boiler
  - Chiller
  - Cooling Tower

- **Distribution System:**
  - Pumps
  - Pipes
  - Control Valves

- **Secondary System:**
  - Air handler unit (AHU)
  - VAV terminal units (VAV)
  - VRV (Variable Refrigerant Volume)
  - Sensors
  - Thermostat

ARM

ARM Partners for Motor Control

Kinetis KVx, ARM® Cortex®-M0+, Cortex®-M4 and Cortex®-M7

Blocks supported by software libraries | Peripherals | Hardware

MOTOR CONTROL FIRMWARE FEATURES

Note: 1. High Frequency Injection
2. STM32F103, F2, F4
3. Max FOC estimated in sensorless mode

SOLUTIONS   PRODUCTS   DESIGN SUPPORT   BUY & SAMPLE   ABOUT CYPRESS

Home › Products › Microcontroller (MCU) and Programmable System-on-Chip (PSoC®) Families › 32-bit ARM® Cortex® Microcontroller (MCU) Families

32-bit ARM® Cortex® Microcontroller (MCU) Families

INTRODUCING THE FM4 PORTFOLIO
Best-in-class ARM® – Cortex® M4
Performance for Safety-critical,
Real-time Industry System

Overview | Products | Design Support

Cypress's Flexible Microcontroller (FM) portfolio, which is based on the ARM® Cortex®-M4, Cortex®-M3, Cortex®-M0+ CPUs is a scalable platform for industrial and consumer applications. Cypress's FM Portfolio delivers high-performance capabilities such as dedicated motor control peripherals, zero-wait high-speed flash accelerators, graphics coprocessors, high-speed CAN-FD interfaces and other peripherals integrated with ARM's latest,
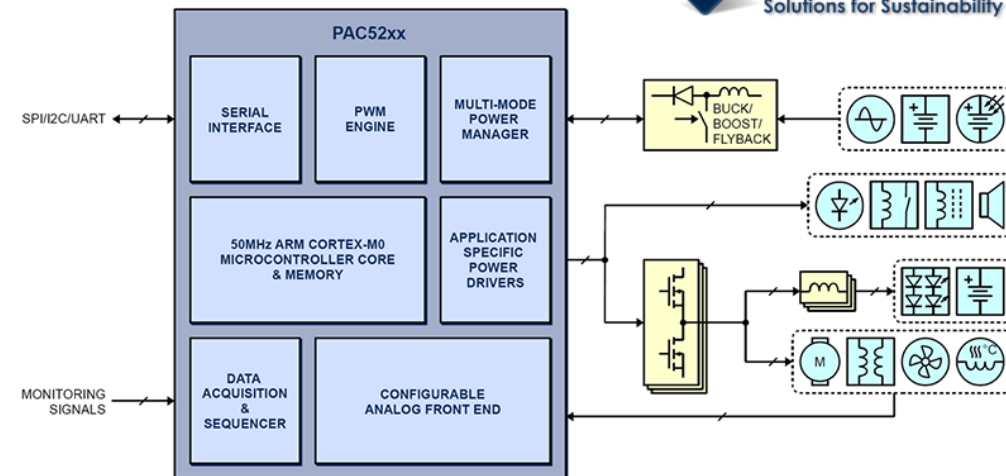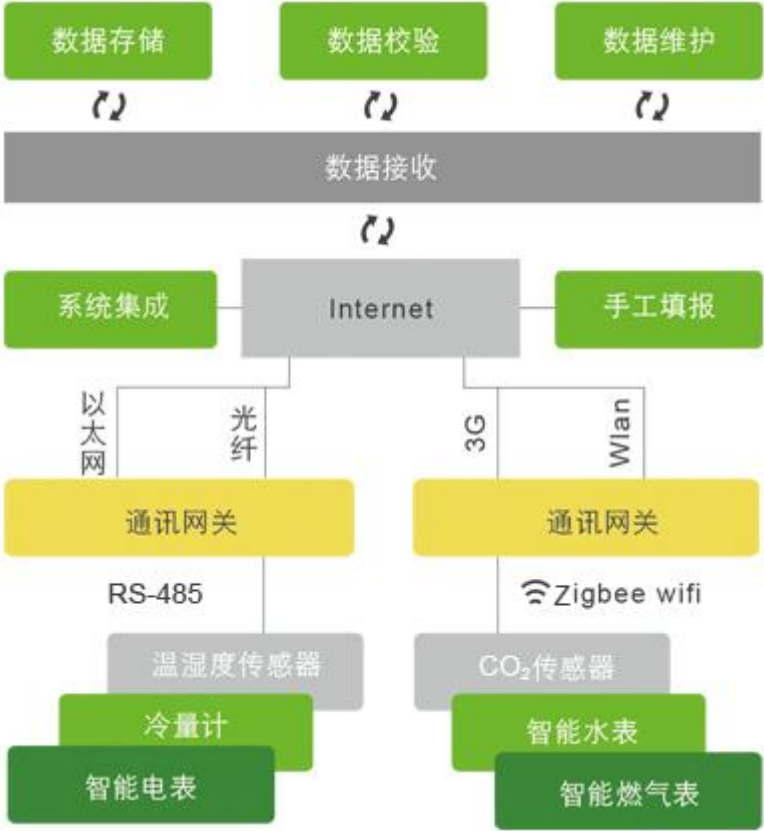
Building Energy Management System

©ARM 2017

TI Cortex-A8

ARM

Smart Parking

- Smart Parking System is an integrated system to organize cars in public parks (Buildings or Cities), to balance parking supply and demand, help drivers for better user experience.

ARM

Embedded System: 智能快递柜

智能快递终端是一种联网的储物柜，快递员将快件送达指定地点后，只需将其存入柜中，系统便自动向收件人手机发送一条短信，包括取件地址和密码，收件人在方便时，到柜前输入密码即可取出快件。邮宝智能快递终端能为用户提供自由的取件时间和地点，同时降低快递企业的成本。

快递员存件
① 刷卡
② 扫描条形码
③ 选箱投递
④ 系统发送验证码给用户

用户取件
① 输入验证码
② 刷卡
③ 开箱取件

系统操作流程

三泰控股 SANTAI HOLDING.

日日顺

丰巢 HIVE BOX

ADVANTECH Enabling an Intelligent Planet

华北工控 NORCO

NXP

TEXAS INSTRUMENTS

©ARM 2017   i.MX6, Cortex-A9   ARM

"Buy vs. Make" Embedded Boards

Customer Challenges	Full Custom (Make)	Standard Board (Buy)
Time-to-Market	• Longer time required to do hardware development	• Shorter period as hardware and BSP is ready immediately allowing faster reaction to market needs.
BOM Costs	• Lowest	• Potentially lower as R&D cost can be amortized over a larger customer base per board
Lowering development costs as system complexity increases	• Dedicated resources need to keep up with each technologies in the system translates into more costs for human capital	• Complex boards designed by module vendors reduces risky, complexity and costly for OEM
Increase value through internal IP development	• Some IP may not be differentiating or valued by the customer	• Limits the OEM investments and allows critical resources to be applied to IP that creates value.
Long product life cycles	• OEM takes responsibility for all elements of design	• OEM off loads some of the responsibility to system board maker

ARM

ARM for Single Board Computers:

- **Energy Efficiency**
  - Performance per watt; Small form factor
  - Simpler power electronics to reduce BOM and weight
  - Save cost for heat sink, transport and installation
  - Broader application space such as battery powered

- **Increased Customer Choice**
  - Embedded computing spans diverse applications
    - Peripherals to meet application needs
    - Competition and constant innovation

- **Partnering and Ecosystem**
  - Increasing Software Complexity (Linux, Android, Microsoft)
  - Trend to lower cost faster development cycles

ARM
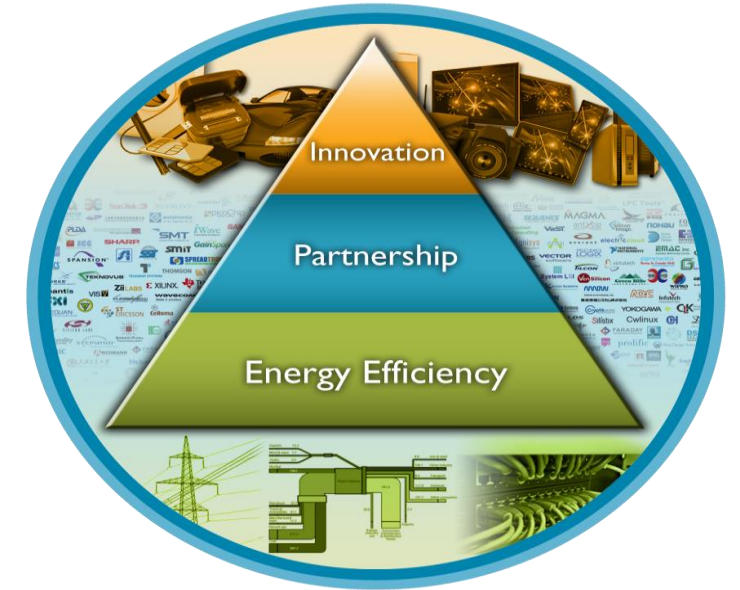
Architecting the IoT opportunity
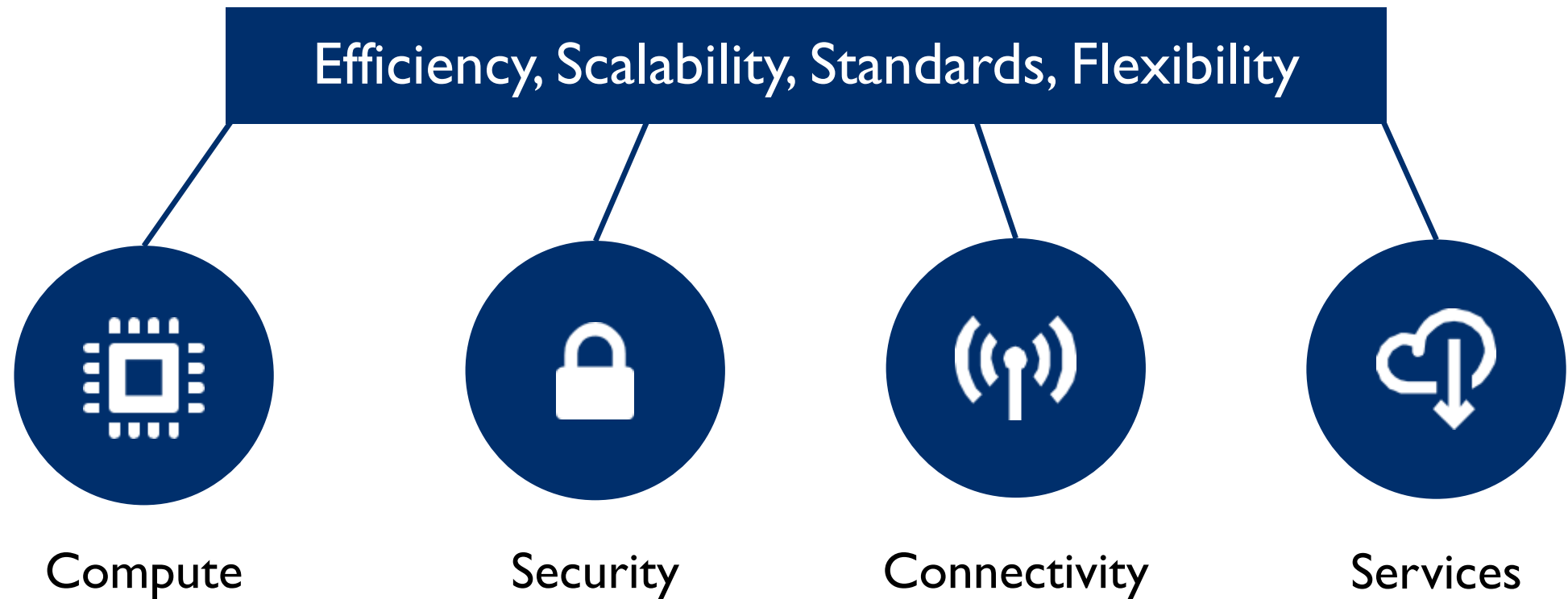
Efficiency, Scalability, Standards, Flexibility

Compute

Security

Connectivity

Services

ARM

Cortex-M7 Processor

Highest Performance Cortex-M Processor

- **High performance core with DSP capabilities**
  - Six-stage dual-issue pipeline with branch prediction
  - Powerful DSP instructions and SP/FP Floating Point Unit

- **Flexible memory system**
  - Tightly-coupled memories for real-time determinism
  - 64-bit AXI AMBA4 memory interface with I-cache and D-cache for efficient access to external resources

- **ARMv7E-M architecture**
  - 100% binary forwards compatibility from Cortex-M4
  - Key Cortex-M processor family characteristics: ease of use, excellent interrupt latency

- **Safety features**
  - Memory ECC (SEC-DED), MPU, on-line MBIST, lock-step operation, full instruction and data trace
  - Up to ASIL D, SIL3 systematic capability

ARM
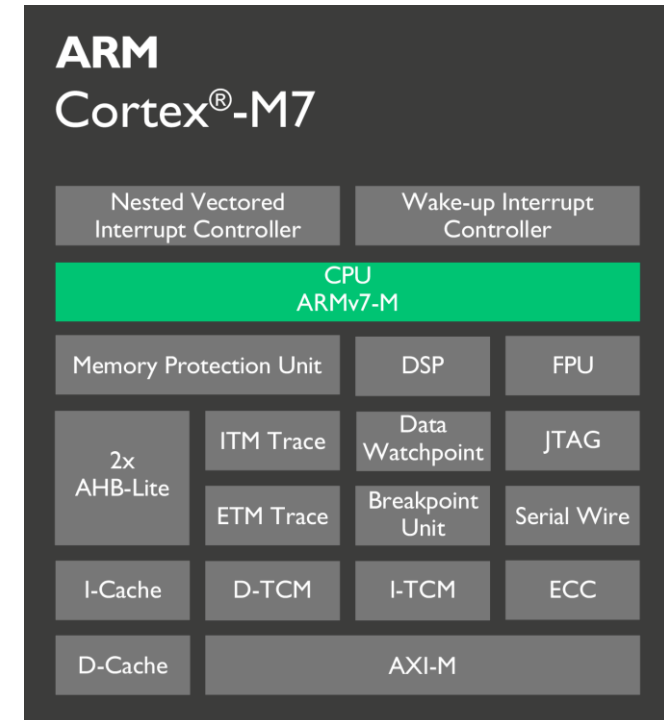
Cortex-M7: Harnessing the Cortex-M Ecosystem

> " With support for the new Cortex-M7 processor, we are further strengthening our leading market position by delivering development tools for ARM with an outstanding benchmark score of 5.04 CoreMark/MHz "
>
> - Stefan Skarin, IAR Systems

> "Our robust embedded software components are designed to be used in high performance applications targeted by Cortex-M7, including industrial control, safety and IoT "
>
> - Jean Labrosse, Micrium

> " ARM Cortex-M7 will bring substantially more computing power to embedded applications, and SEGGER will continue to innovate new products and features for each new generation of ARM processors "
>
> - Rolf Segger, SEGGER

©ARM 2017

DesignStart: The fastest route to silicon

Fast, simple and no-risk access	Design with confidence	The most accelerated route to success

Start designing today!

World's most proven processors

Most comprehensive services, tools, and software

$0 license fee

Cortex-M0 & Cortex-M3

Design assistance

Success-based royalty model

Comprehensive subsystems

Largest technology ecosystem

Cortex-M0, Cortex-M3 and subsystems available at designstart.arm.com

ARM

Cordio: Complete and qualified wireless solutions

Easiest path to leading ultra-low-power
wireless connectivity

**Complete solution
from RF to software**
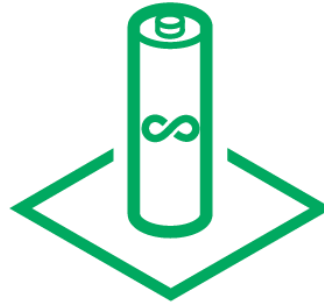
**Energy efficient
Sub one volt radio**

**Flexible and configurable
RF, standards, software stacks**

ARM

Cordio: Design flexibility is yours

Bluetooth 5 and/or 802.15.4
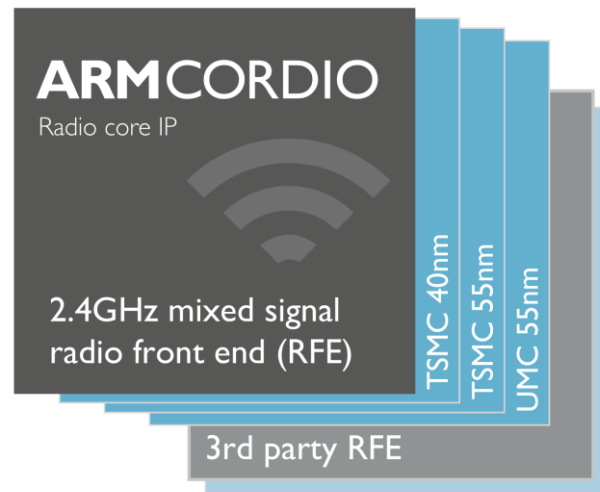
Select your fab   Select your features/standards   Match your stack(s)

©ARM 2017   ARM
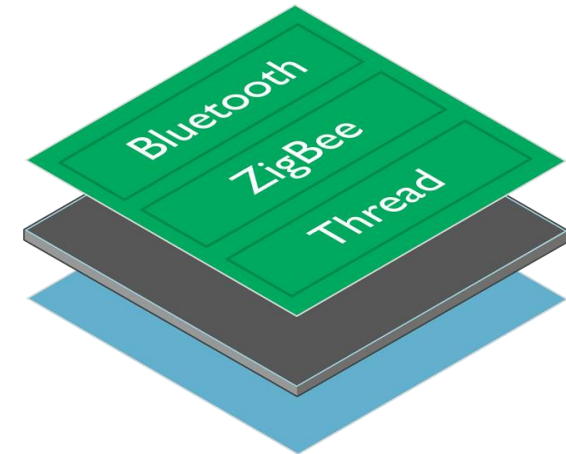
Growing Cordio ecosystem

RF Front End

CATENA

Aura Semiconductor

Stacks

ubisys

DSR
Skilled, Trusted Software Development

Foundries

tsmc

55nm, 40nm

UMC

55nm

Alliances

Bluetooth
SPECIAL INTEREST GROUP

THREAD GROUP

ZigBee Alliance

ARM
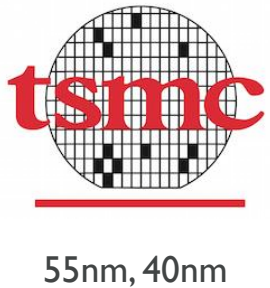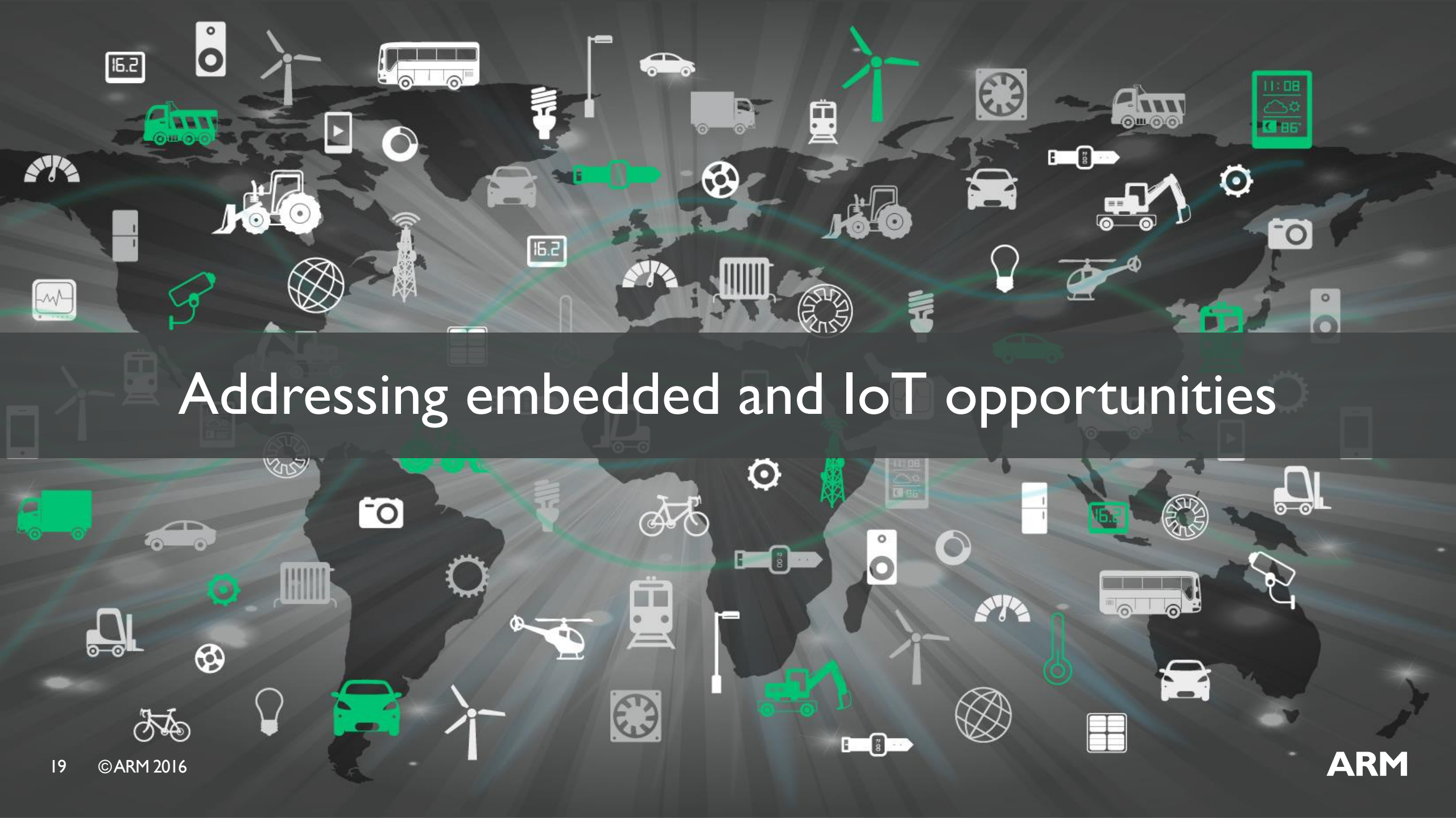
Addressing embedded and IoT opportunities

ARM

Security for all embedded applications

- Root of trust applications - IoT

Trusted software			
Trusted hardware			
Crypto	Secure system	Secure storage	TRNG*

- IP Protection

Valuable firmware
Trusted drivers
Trusted hardware

untrusted	trusted 🔒

- Sandboxing

Certified OS / functionality
Trusted drivers
Trusted hardware

*True random number generator

ARM
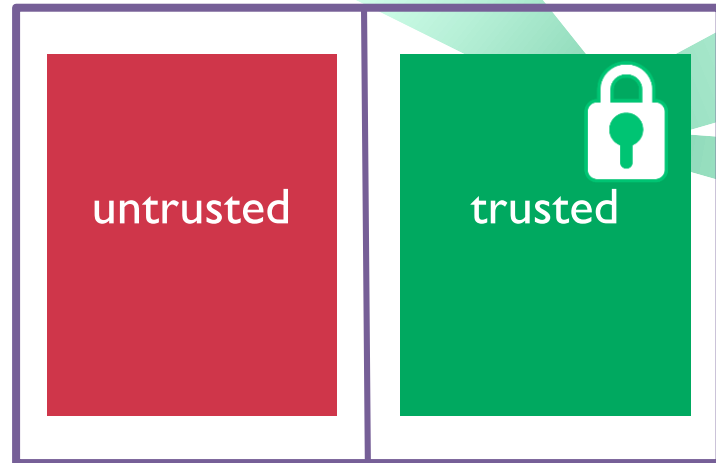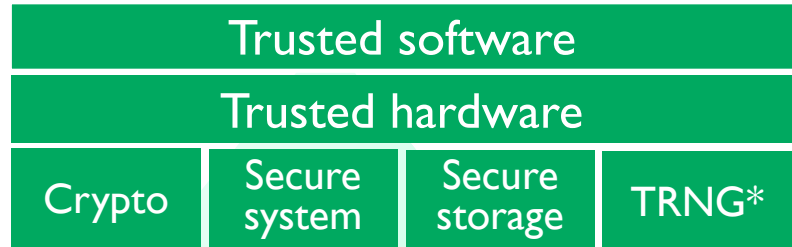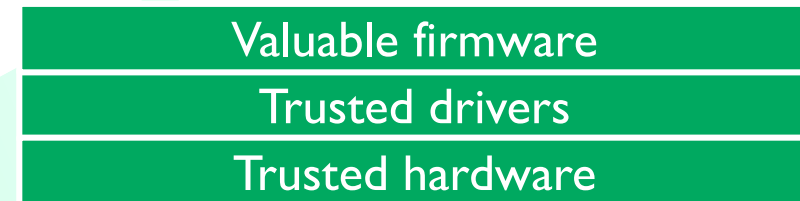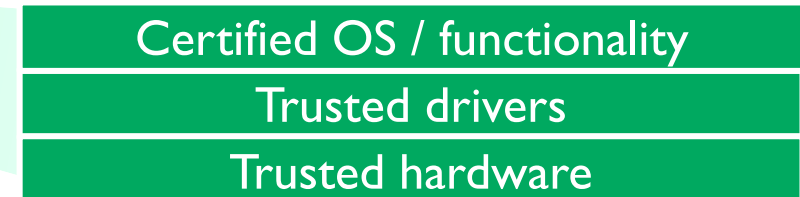
What sort of security?

Standard, affordable

Developer friendly

Ecosystem friendly

ARM

TrustZone for ARMv8-M

Separation and access control (containers)

- Isolate trusted software and resources
- Reduce attack surface of key components

Trusted software

- Provision of security services
- Small, well-reviewed code

Trusted hardware

- Hardware assist for cryptography
- Secure-access validation built into SoC

ARM TRUSTZONE
System security

untrusted	trusted

Software			
Hardware			
Crypto	Secure system	Secure storage	TRNG

©ARM 2017

ARM
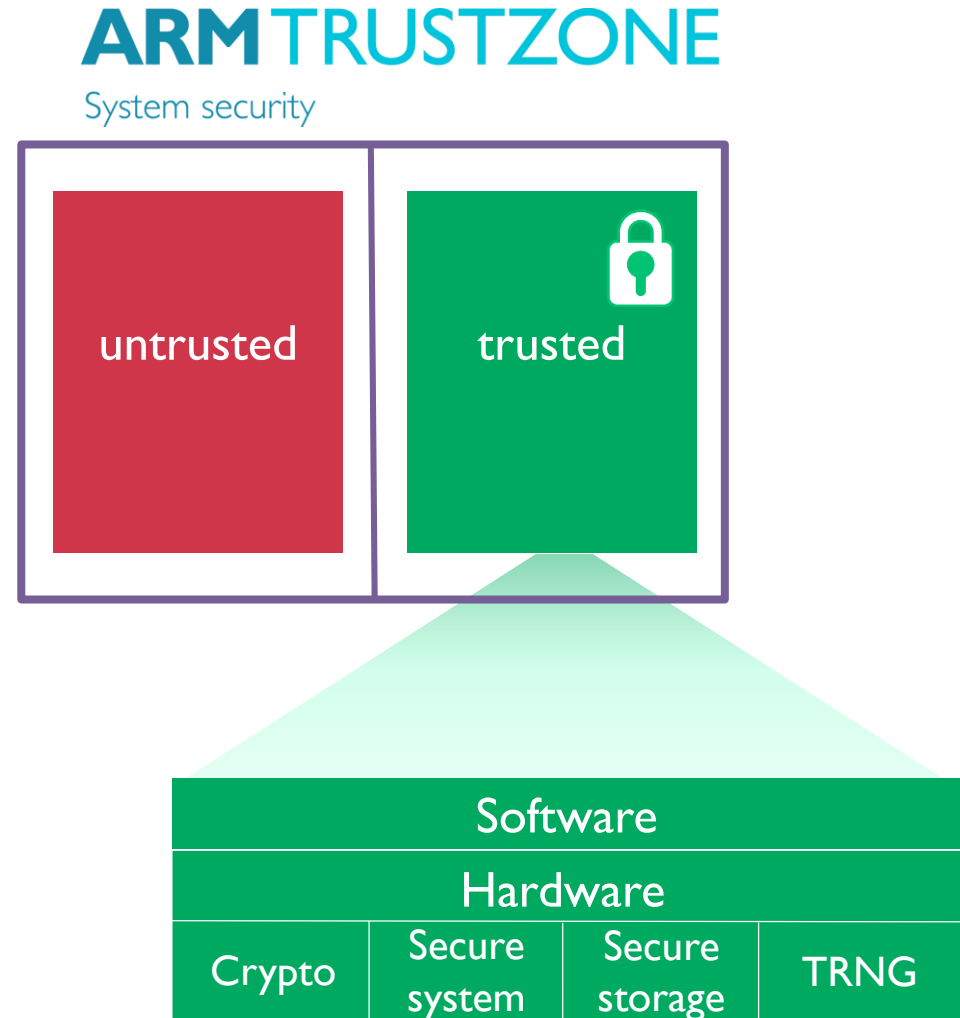
Retain the familiar programmers' model

Classic embedded design
ARMv7-M

Secure embedded design
with TrustZone for ARMv8-M

Untrusted   Trusted

Unprivileged

Firmware

Privileged

RTOS

Unprivileged

Firmware

Trusted libraries

Privileged

RTOS

Trusted resource manager and libs

ARM
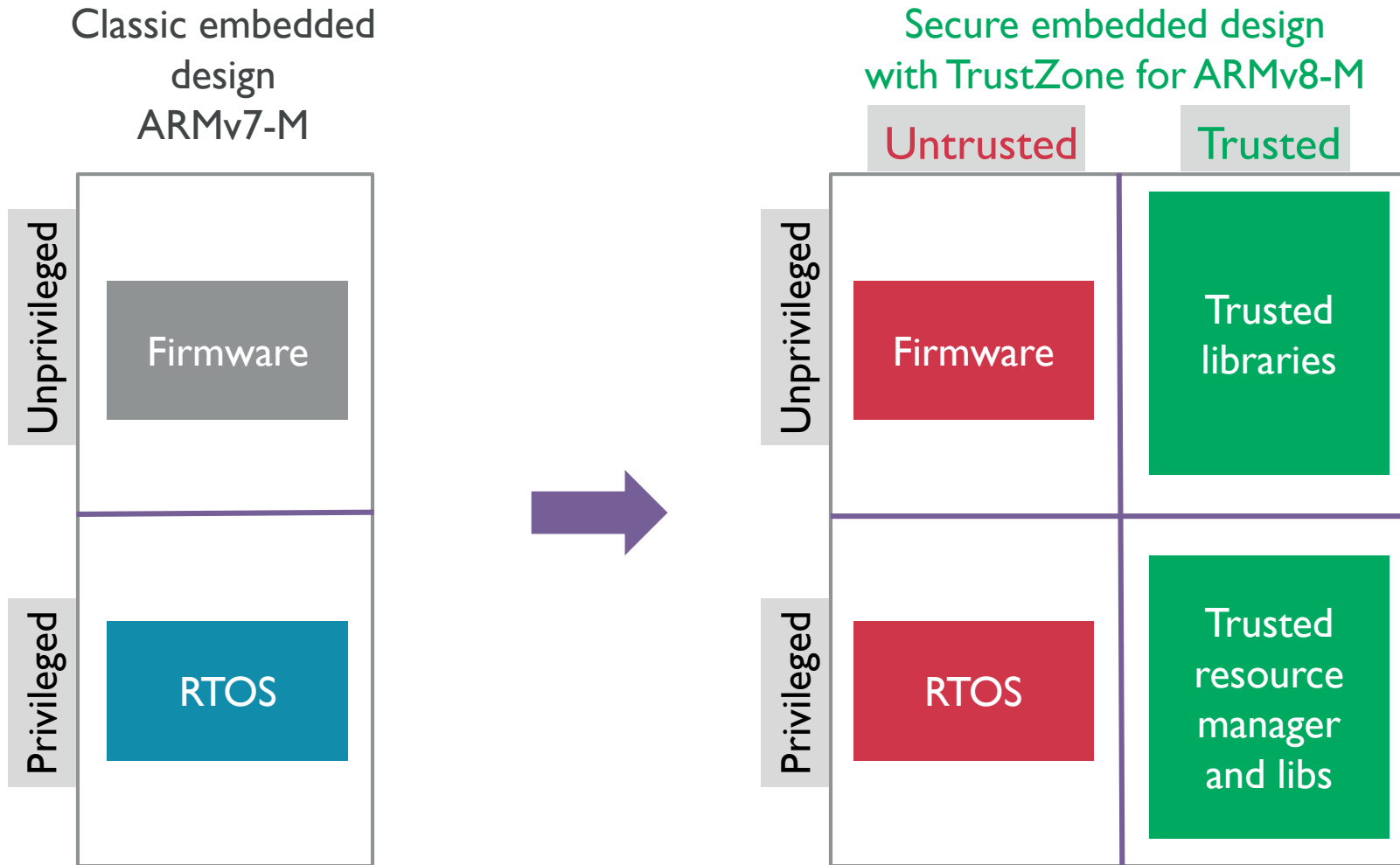
Bringing TrustZone protection to the system

- **Secure the system, secure the processor**
  - Hardware separation and isolation
  - Protect memories, peripherals, legacy IP

- **AMBA AHB5 bus protocol**
  - Signals security through the interconnect
  - Complementary to ARMv8-M

- **Optimized for embedded systems**
  - Fewer wires saves area and power
  - Hardware protection simplifies software

CPU

Non-trusted DMA

AMBA AHB5 compliant interconnect

Flash

SRAM

Trusted peripheral A

Non-trusted peripheral B

Trusted region   Non-trusted region

ARM
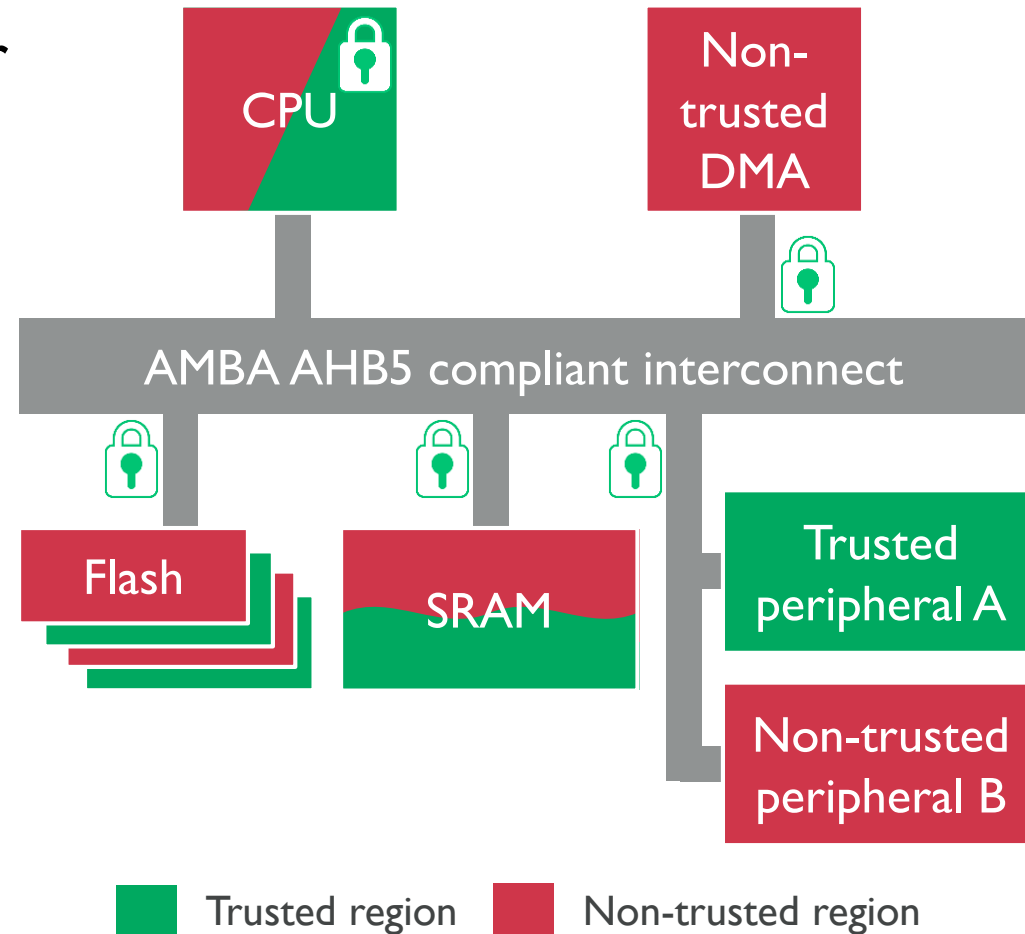
CoreLink SIE-200: System IP for embedded
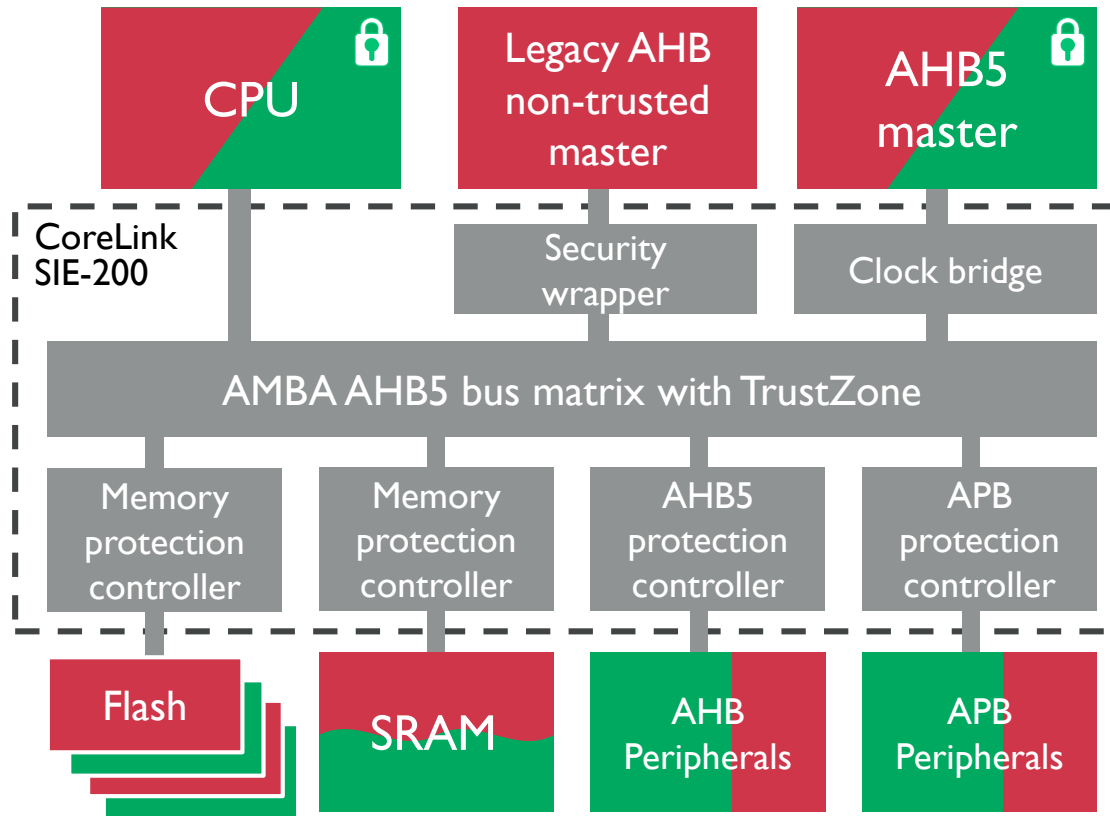
Simplify the design of a secure system
- Designed and verified with latest ARMv8-M CPUs

Reduce design time with IP reuse
- Re-use and secure existing IP in AHB5 systems

Extend security to peripherals
- Integrate legacy peripherals
- Programmable at run-time

Protect code and data
- Programmable regions for multiple applications

ARM

CoreLink SSE-200: Subsystem for embedded

CoreLink SSE-200 Subsystem for embedded

- Secure debug
  - CoreSight SoC
- Cortex-M33
  - Instruction cache
  - TCM
- Always-on domain
- Power control
- Multi-layer AHB5 interconnect
- AHB5 expansion ports
- TrustZone protection
- TrustZone protection
- TrustZone protection
- APB bridge
- TrustZone protection
- SRAM control
- Peripherals
- Flash controller
- Embedded or External Flash
- Artisan SRAM
- Cordio radio
- TrustZone CryptoCell

Options

ARM CoreLink SSE-200 IP

Other ARM IP

- **Hardware IP**
  - Dual core - Cortex-M33
  - Instruction cache and memories
  - Debug and power infrastructure
  - CryptoCell, Cordio radio (options)
  - CoreLink SIE-200 system IP

- **Software IP**
  - mbed OS
  - Integration of secure libraries, drivers and protocol stack
  - Delivered as open source

ARM

Bringing TrustZone to the Cortex-M family

Cortex-M7 — Maximum performance, control and DSP

Cortex-M3 — Performance efficiency

Cortex-M4 — Mainstream control and DSP

ARM TRUSTZONE System security

Cortex-M33 — Flexibility, control and DSP with TrustZone

Cortex-M0 — Lowest cost, low power

Cortex-M0+ — Highest energy efficiency

Cortex-M23 — TrustZone in smallest area, lowest power

High performance

Performance efficiency

Lowest power & area

ARMv7-M

ARMv6-M

ARMv8-M

ARM

Cortex-M23 enhancements over Cortex-M0+

Cortex-M23

Cortex-M23
TrustZone
Stack limit checking
Hardware divide
Exclusive memory accesses
Enhanced debug
ETM
NVIC (max 240 IRQs)
MPU (PMSAv8)
AHB5
WIC
Fast I/O bus
MTB
Serial wire / JTAG
ARMv8-M baseline

Cortex-M0+

Cortex-M0+
NVIC (max 32 IRQs)
MPU (PMSAv6)
AHB Lite
WIC
Fast I/O bus
MTB
Serial wire / JTAG
ARMv6-M

■ New or updated

CoreMark®/MHz: 2.46   2.50

DMIPS/MHz: 0.95   0.98

ARM
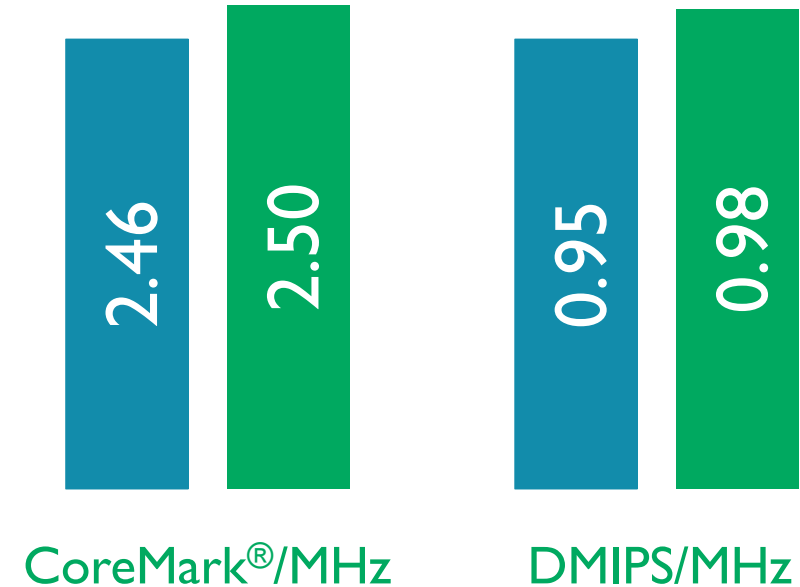
Cortex-M33 enhancements over Cortex-M4

Cortex-M33

TrustZone
Stack limit checking
Co-processor interface
Enhanced debug
MTB
ETM
NVIC (max 480 IRQs)
MPU (PMSAv8)
AHB5
FPU
SIMD/ DSP
WIC
Serial wire / JTAG
ARMv8-M mainline

Cortex-M4

ETM
NVIC (max 240 IRQs)
MPU (PMSAv7)
AHB Lite
FPU
SIMD/ DSP
WIC
Serial wire / JTAG
ARMv7-M

■ New or updated

CoreMark®/MHz +13%
3.40 3.86

DMIPS/MHz +20%
1.25 1.50

ARM
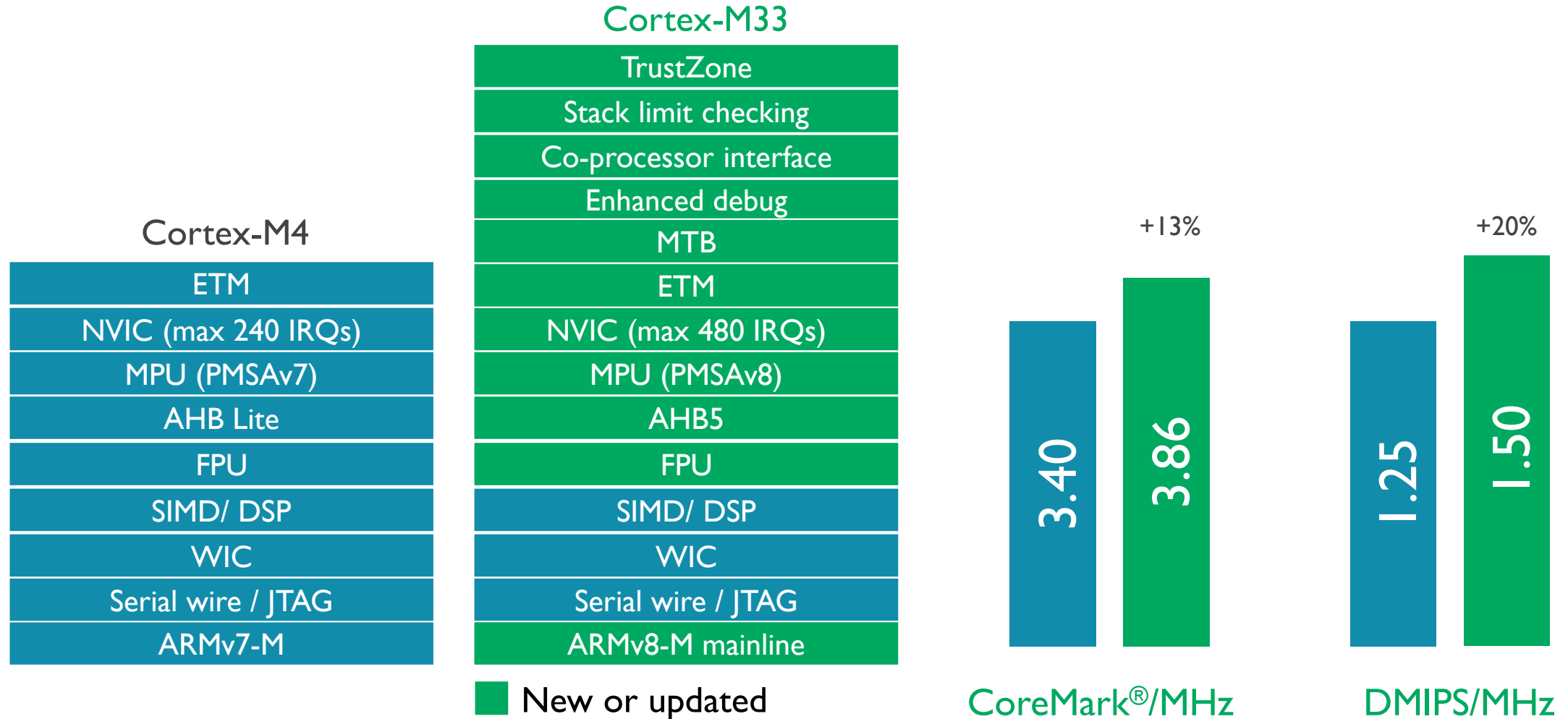
Ever-expanding world's #1 embedded ecosystem

Public silicon lead partners

Public ecosystem lead partners

©ARM 2017

ARM

Economist IoT business index 2017

2013

Surveyed

800+ senior leaders

400+ C-suite respondents

Sectors covered:

Financial services, manufacturing, healthcare, biotechnology, IT and energy, construction and facilities management

©ARM 2017   Read the latest report at: www.arm.com/iot17

ARM

Key findings: What can accelerate IoT?

Challenge

- **IoT infrastructure costs** remain a high barrier to business scale

- Businesses are daunted by **security concerns**

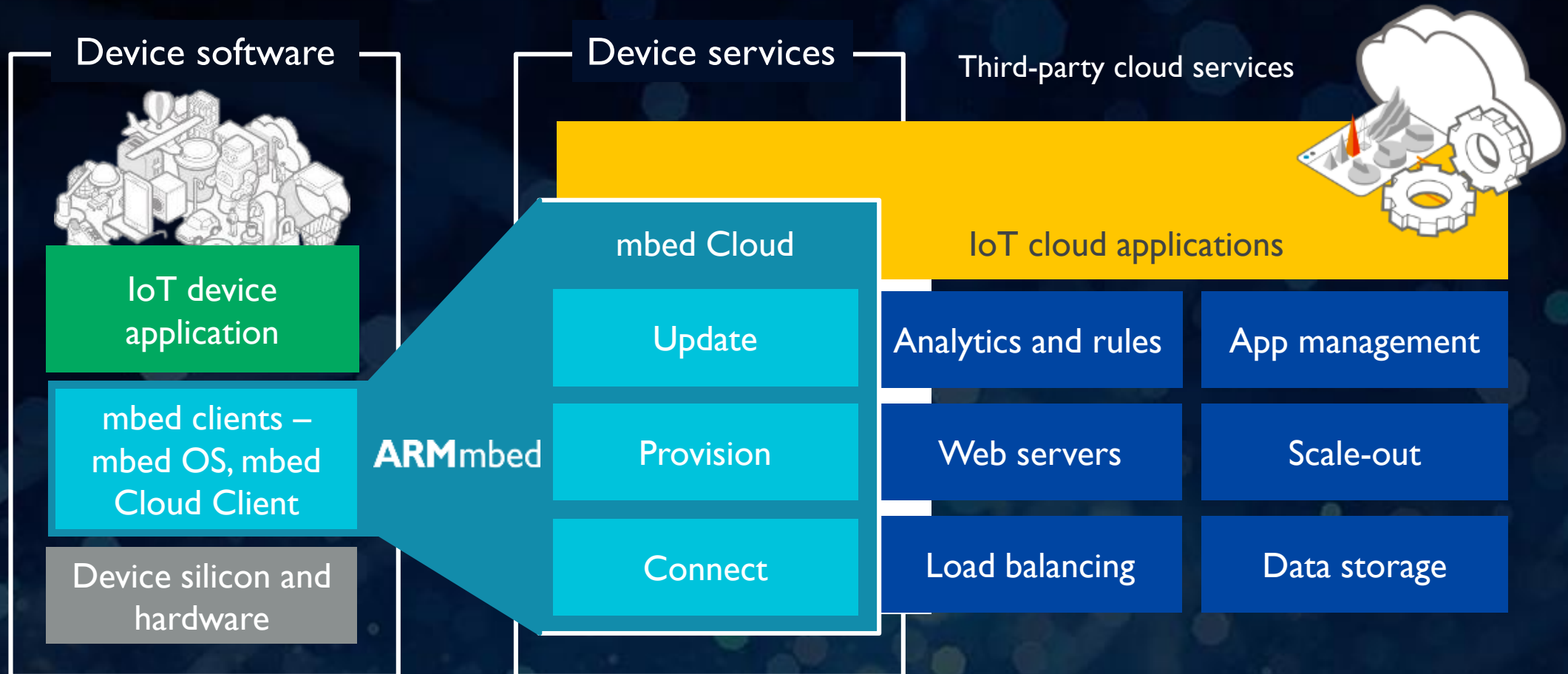- **IoT device development** and connectivity costs are high

Recommendations

Innovative SaaS solutions instead of PaaS and middleware offerings can help reduce these costs

Businesses should look for off-the-shelf chip-to-cloud solutions that allow agile security implementation

Invest in platform OS that accelerates application development on a wide choice of silicon

ARM

Connecting chip to cloud

Device software

Device services

Third-party cloud services

IoT device application

mbed clients – mbed OS, mbed Cloud Client

ARMmbed

Device silicon and hardware

mbed Cloud

Update

Provision

Connect

IoT cloud applications

Analytics and rules

App management

Web servers

Scale-out

Load balancing

Data storage

©ARM 2017

ARM

Today enterprises are under pressure to unlock the value in the Internet of Things. Our mission is to help businesses access how this can be the Internet of Possible by enabling them to create, deploy and manage them securely across their lifetime.

ARM

ARM