Industrial IoT

Amyas Phillips
amyas.phillips@arm.com

ARM spans sensors to servers

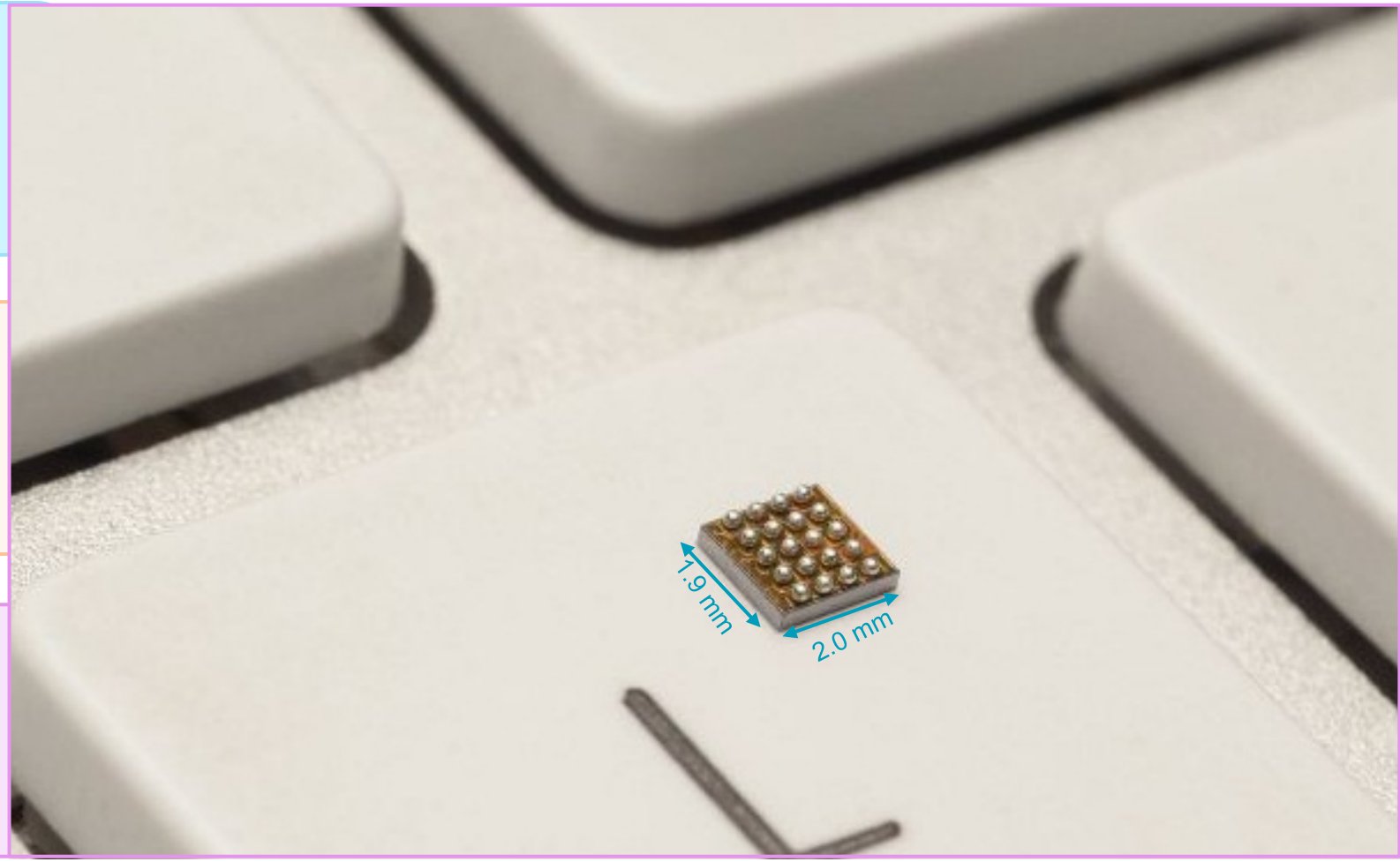
Infrastructure
Servers, network infrastructure

ARM Cortex-A processors

Mobile computing and Gateways
Cellular modems, SBCs
ARM Cortex-R & Cortex-A

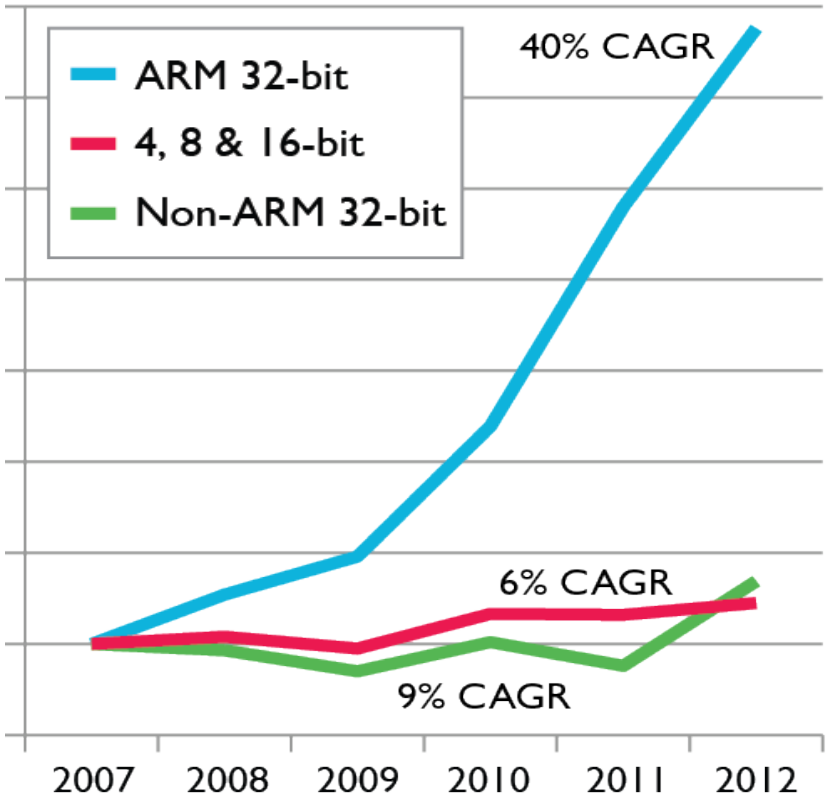
Sensor nodes
MCUs, sensors, low power wireless

ARM Cortex-M



ARM

ARM in embedded



ANALOG DEVICES · Atmel · CYPRESS · ENERGY micro · freescale semiconductor · Infineon · Texas Instruments · NXP · NORDIC SEMICONDUCTOR · nuvoTon · ST

8.7 billion

ARM cores shipped in 2012

2.2 billion

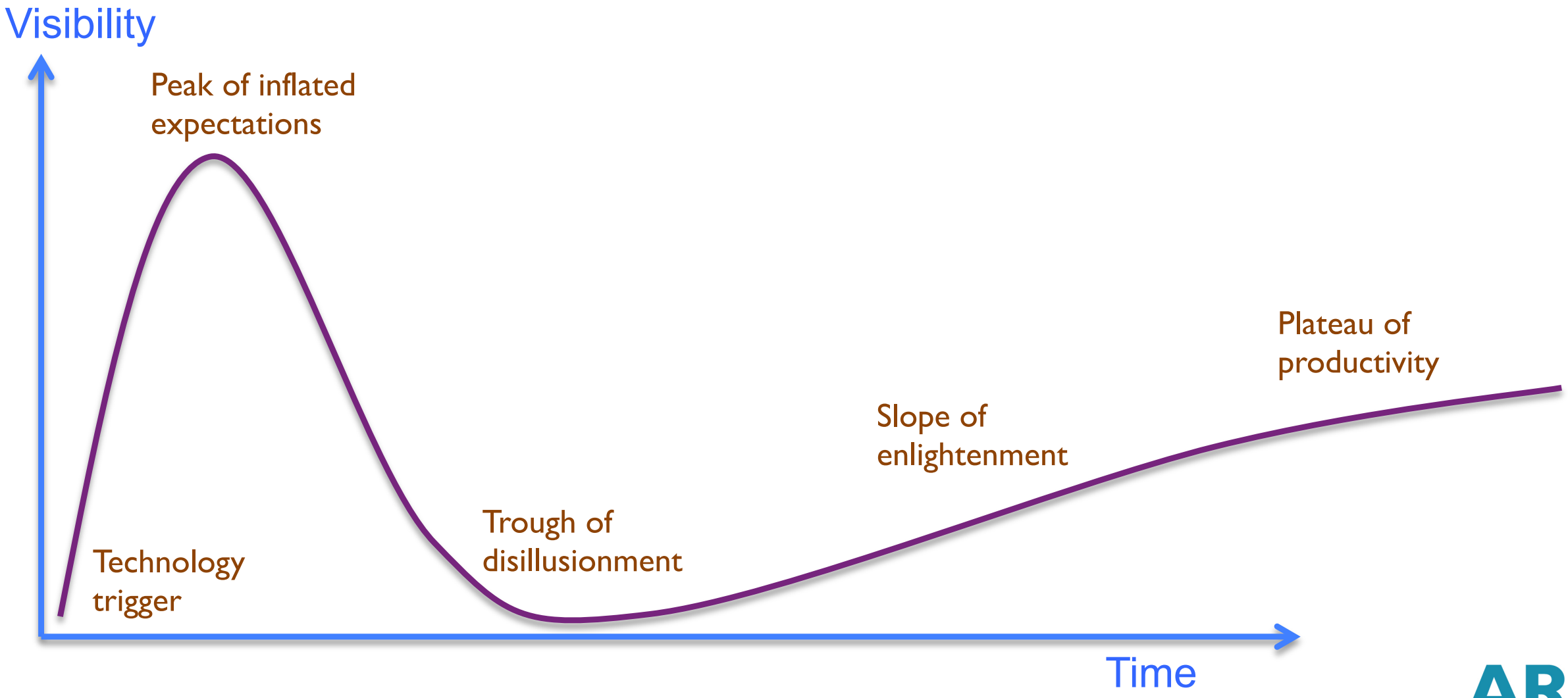
ARM Cortex-M devices shipped in 2012
by leading semiconductor companies

MCUs · radios · sensors

32-bit intelligence starting at $0.50

ARM

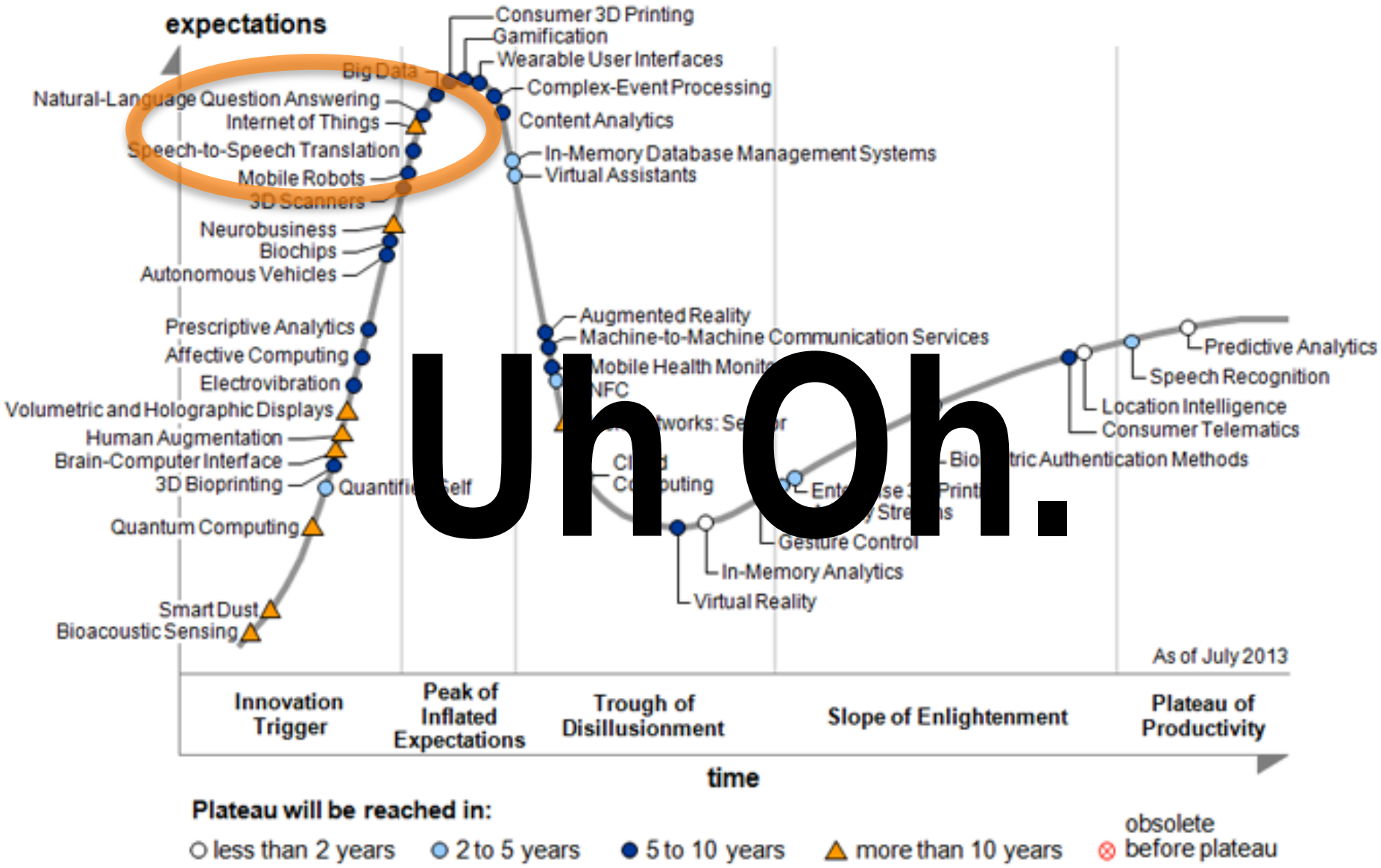
Gartner's hype cycle



ARM

ARM share price

Emerging technologies hype cycle

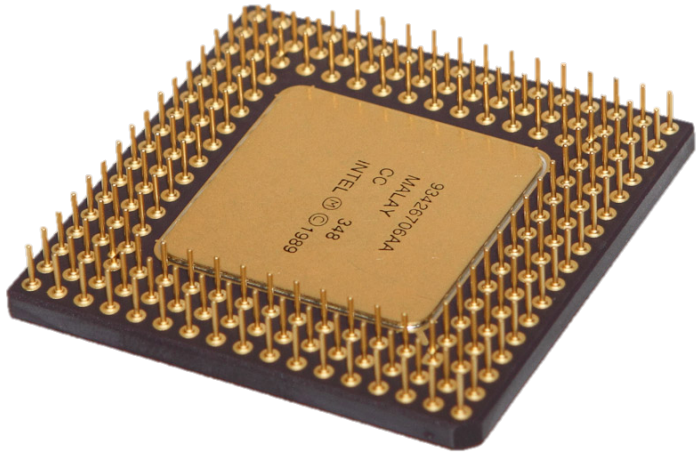


Uh Oh.

Source: Gartner August 2013

ARM

What IoT means



ARM

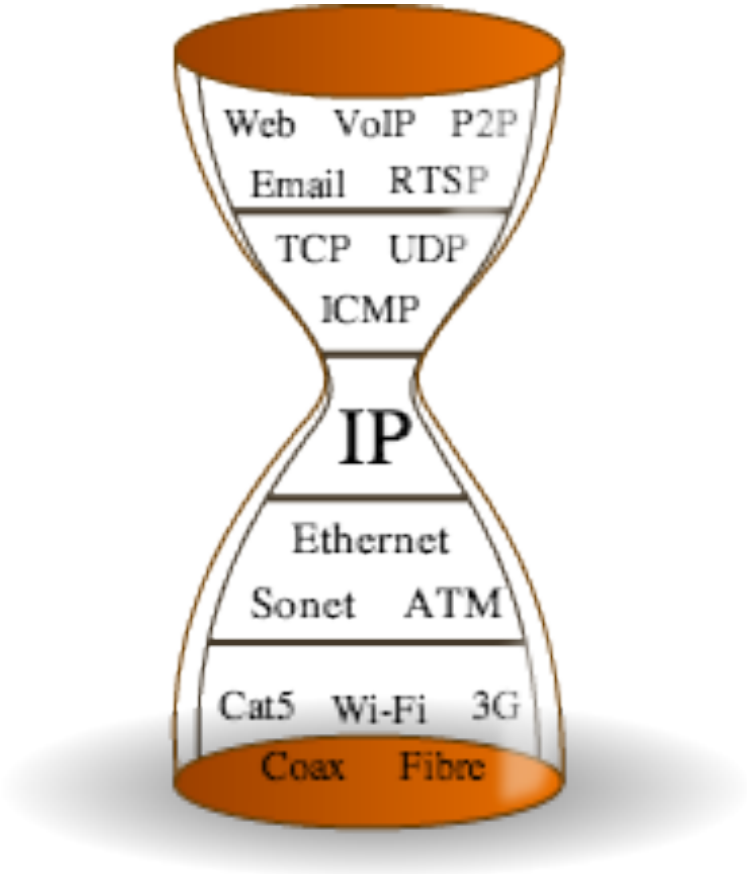
- Industry has used distributed sensing and control for decades

- What's new? Lower cost, increased scale, better utilisation

Not just a network connection

Why is the internet the most successful network?

- IP's "narrow waist"
  - Address system enables packet forwarding
  - Hides physical interfaces from applications
  - Application developers and networking engineers can innovate independently
  - Unifies many small island networks
  - Eliminates protocol gateways
- Permissonless innovation
  - Protocols can change without affecting the network
  - Base for further innovation

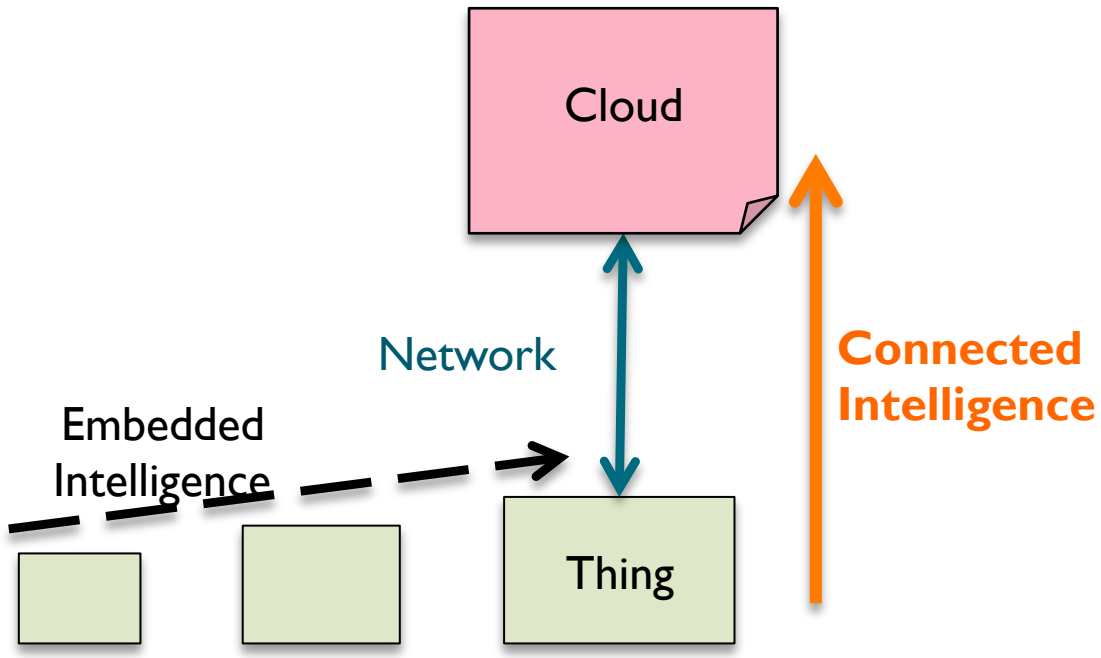


ARM

This time it's different

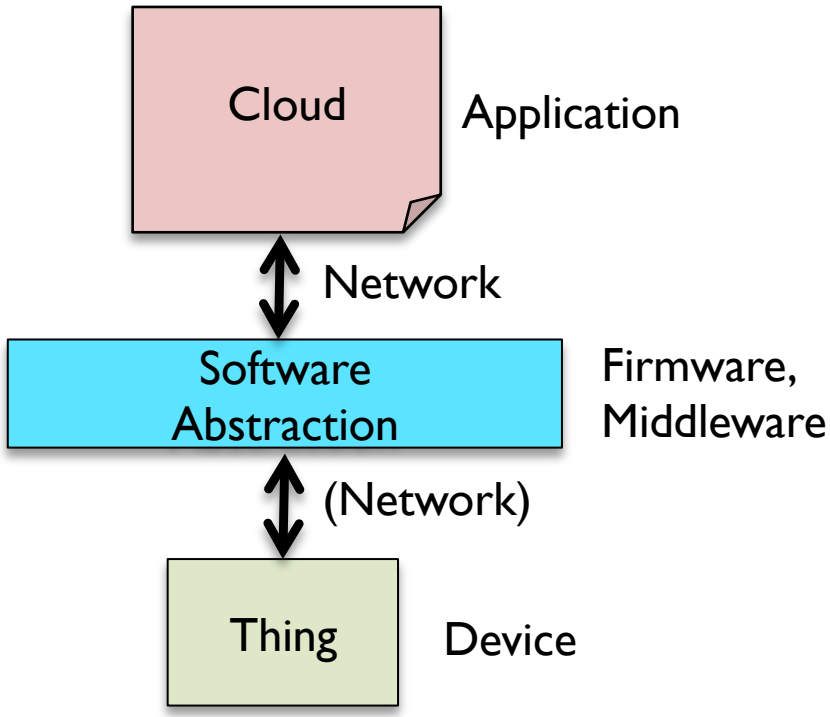
- Ubiquitous connectivity
  - Wireless – anything you want to connect, you can connect
  - Even edge nodes can be internet peers
- Cloud services
  - Co-ordinate processes
  - Deliver anything as a service
- Big data
  - Aggregate the little data
  - Turn data into insight
- Standards
  - We know now what to standardise

Embedded Intelligence vs. Connected Intelligence



ARM

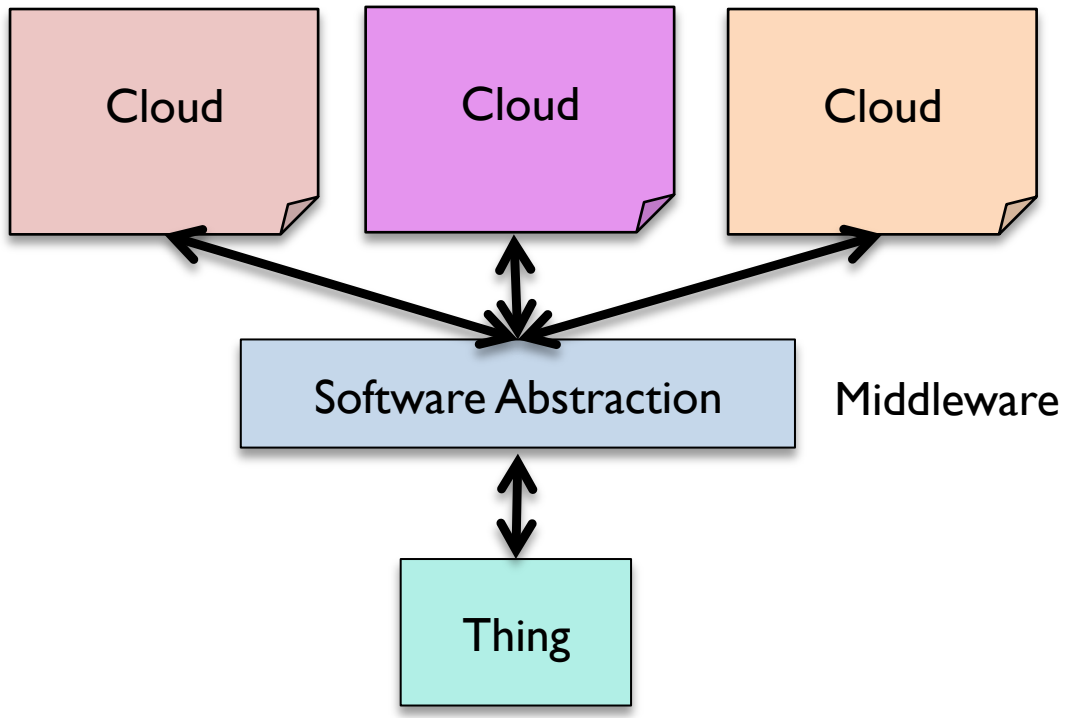
Virtualization of Things



- Web applications interact with virtualized objects through APIs
- Often through a layer of resource caching and indirection, e.g. service platform or gateway

ARM

Virtualization Enables Diverse Software Applications



- Documented interfaces and access control mechanisms enable interoperability
- Common patterns and standards for interfaces can drive compatibility and interoperability
- Discovery interfaces are as important as application interfaces

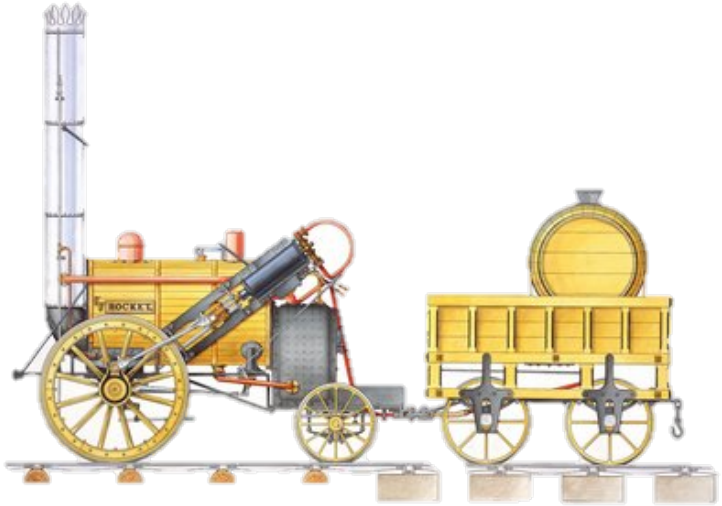
HYPER/CAT

ARM


6:59

- Industrial applications are leaders in IoT

What Industrial IoT means



Innovation

ARM

Drivers of producer surplus

- Situational awareness increases operational efficiency
  - Asset tracking
  - Predictive maintenance
  - Dashboards, analytics, co-ordination

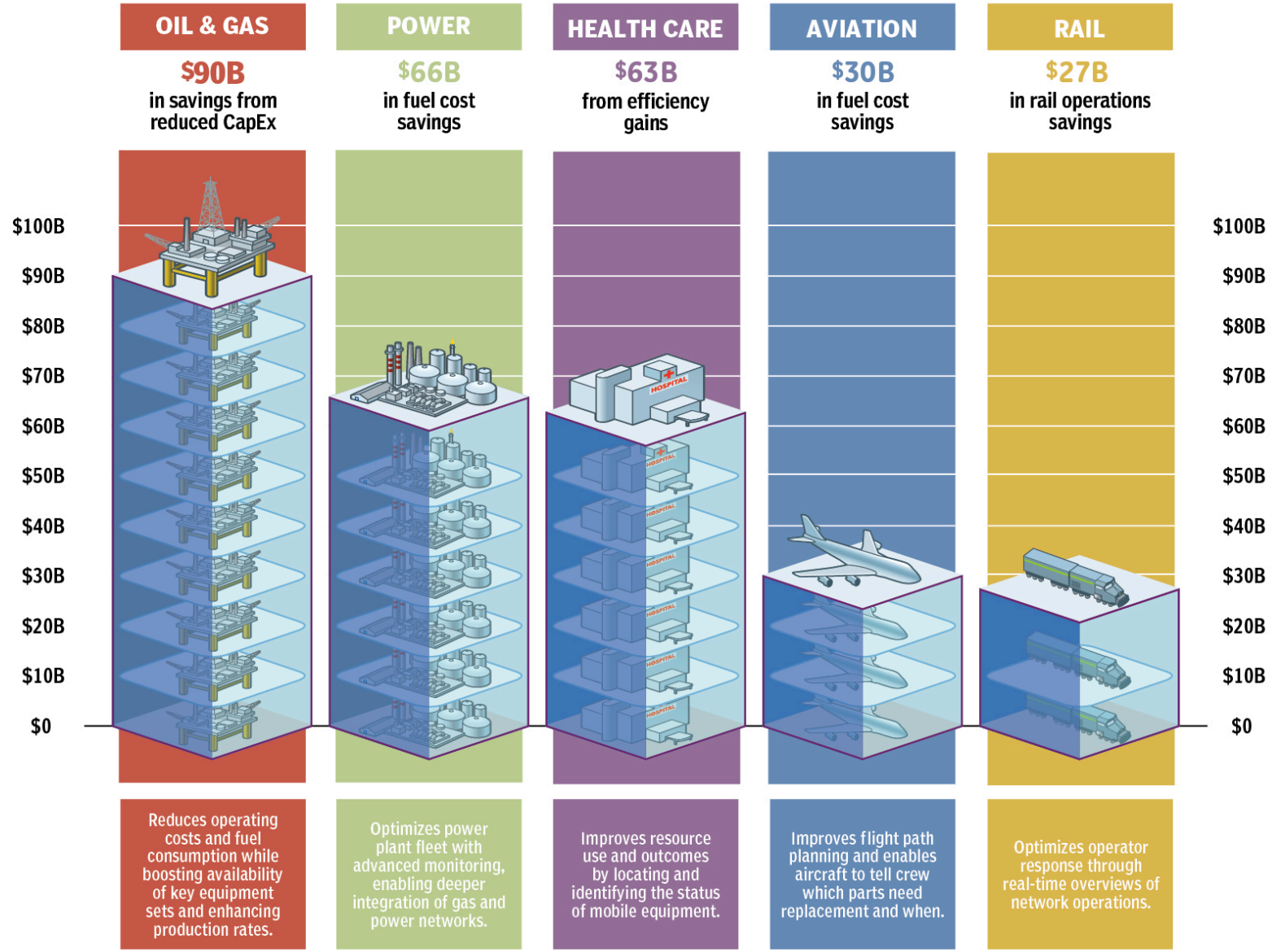
- Apps become become part of the physical environment
  - Convenience, personalisation and user-centricity
  - Service AR, SSO for plant, tracking

- Further shift from capital to operational cost
  - Plant is not just equipment, its a relationship
  - Trains, planes and cars

The Power of 1%

Small savings at industrial scale over 15 years (GE)

- Better information enables better process management
- Small savings at industrial scale easily provide necessary ROI



INDUSTRIAL INTERNET BENEFITS

SOURCE: GE ESTIMATES / POSTMEDIA

Role of Security

- Insights come from big data
- Big data needs little data to be shared
- Sharing needs trust
  - "Whether a transaction would be organized within a firm or whether it would be carried out on the market depended on a comparison of the costs of organizing such a transaction within the firm with the costs of a market transaction that would accomplish the same result. All this is very simple and obvious. But it took me a year to realize it – and many economists seem unaware of it (or its significance) to this day…" – Ronald Coase, 1994 Nobel Lecture
- Trust needs security …
- … and transparency, in consumer applications
- **Security is just a means to an end**

Role of security II

Cyberwar, safety, extortion, reputation..

- Connected devices are more vulnerable
- In industrial applications even a single breach might have serious consequences
- They need to be defended
- Proportionate measures always depend on the specific situation
  - assets, applications, deployments
- Manageable with existing techniques
  - All of IT's armoury available
  - Firewalls, logs, per-device keys
  - Applied to a simpler domain

Gateways

- Non-IP "island" networks need protocol translation to talk to one another
- Adds engineering cost
- Inserts single point of failure
  - Unless only acting as observer
- Computer networks did this in the 1980s before moving to all-IP
- Necessary as a legacy integration solution
  - e.g. SCADA
  - SCADA is not designed to be on the internet
  - http://www.cpni.gov.uk/advice/cyber/scada/

Designing for long deployment lifetimes

20+ year deployments

- Must support in-field, remote firmware updates
  - Even constrained devices need bandwidth, energy and memory to accept ~10kB firmware patches, ~annually
- Ideally AES in HW,
- Ideally very good entropy source (RNG)
- See NIST/BSI key length guidance for cryptography
  - http://www.keylength.com/
  - >>2030 AES: 192b ECC: 384b RSA: 384b/7680b
- Must be an owned asset
  - Or have defined transfer-of-ownership
  - Ownership meaning possession of the keys

Build or buy?

- Lots of people want to sell you a "you do the application" solution
- Lots of people would like to be "the IoT platform"
- Mostly there is still much clearer ROI in verticals

IoT design patterns

Edge device

LWM2M, HTTP, TCP, IP

Cloud application

Embedded Devices

Backend – Private or Public Cloud

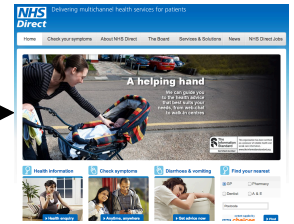
ARM

IoT design patterns

Edge device

LWM2M, HTTP, TCP, IP

Cloud application



Your IT / Ops department

Embedded Devices

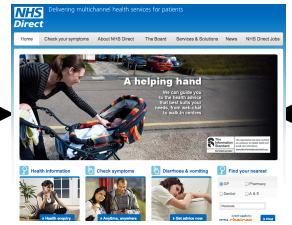
Backend – Private or Public Cloud

ARM

IoT design patterns

Embedded linux edge device

LWM2M, HTTP, TCP, IP



Your IT / Ops department

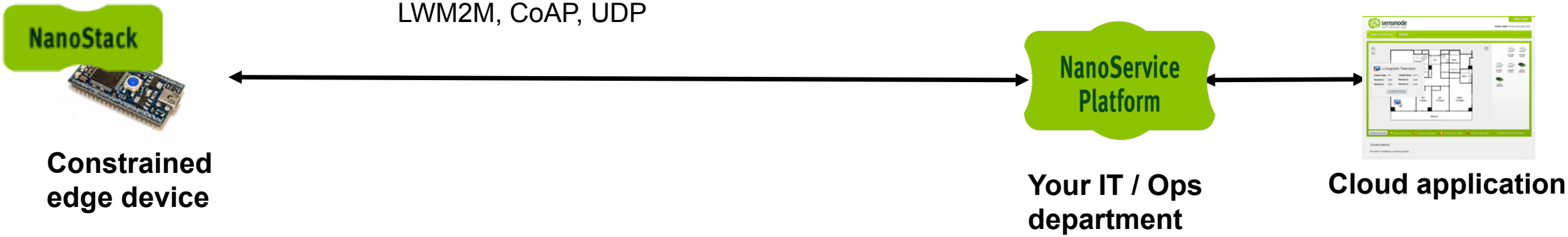
Cloud application

Embedded Devices

Backend – Private or Public Cloud

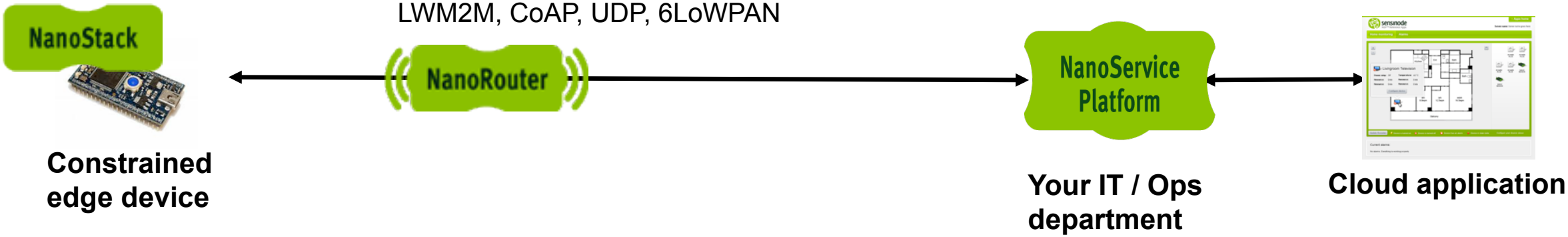
ARM

IoT design patterns

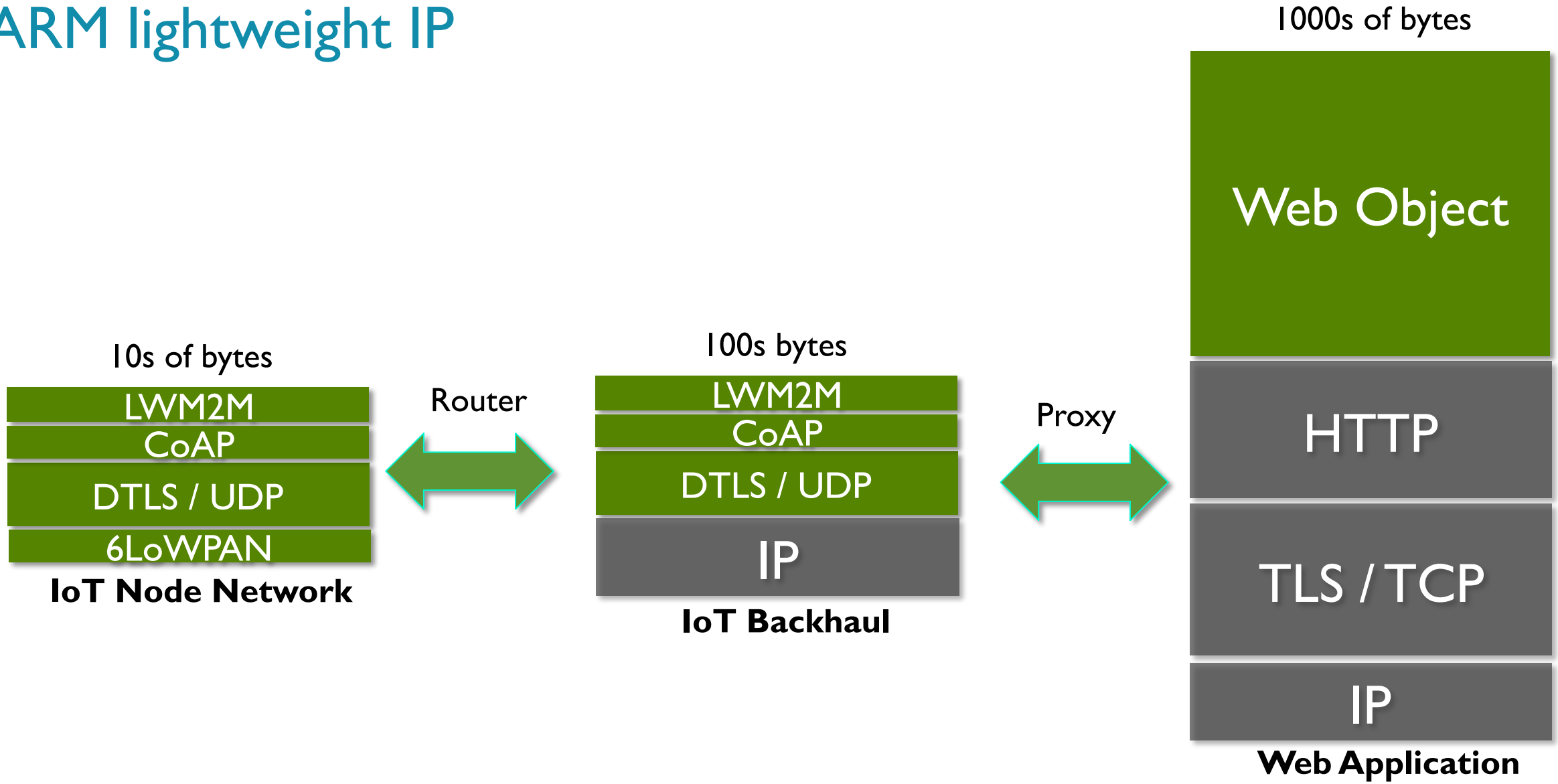


ARM

IoT design patterns

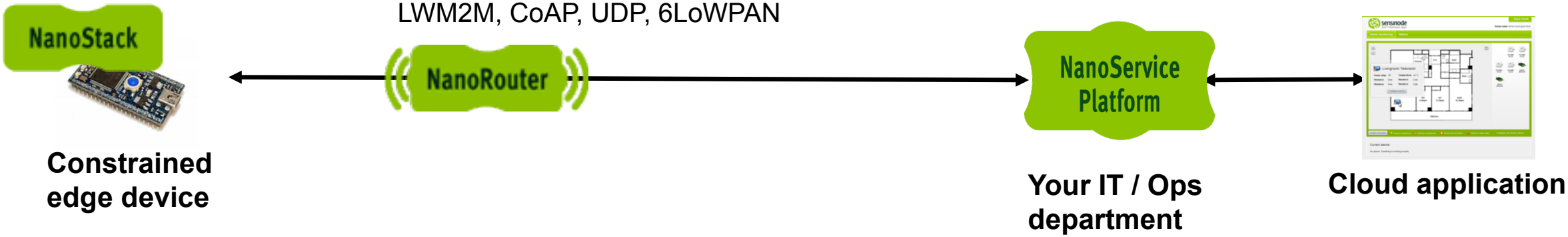


ARM lightweight IP



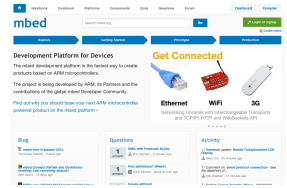
ARM

IoT design patterns



IoT design patterns

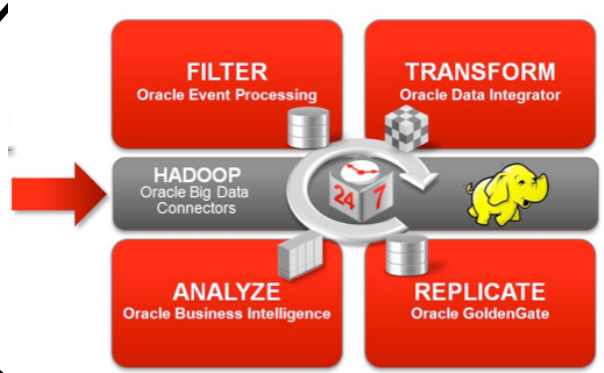
Multiple cloud applications



LWM2M, CoAP, UDP, 6LoWPAN

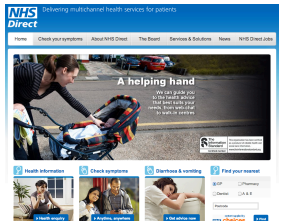
NanoRouter

NanoService Platform



Constrained edge device

Your IT / Ops department



Embedded Devices

Backend – Private or Public Cloud

ARM

IoT design patterns

Legacy edge device

SCADA / LON / CAN

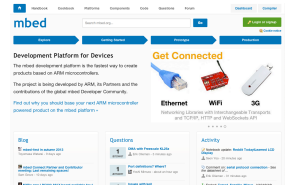
Gateway device

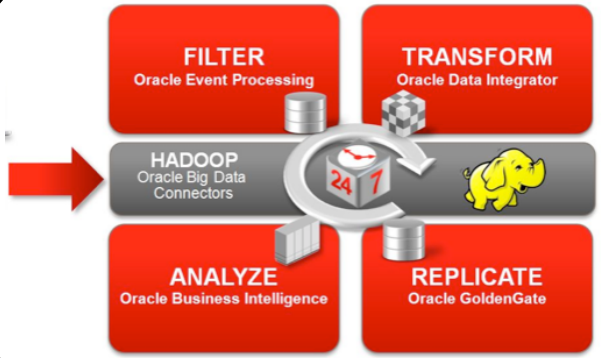
LWM2M, HTTP, TCP, IP

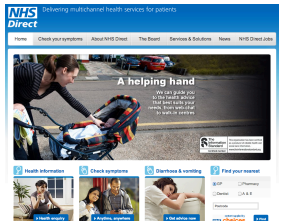
NanoService Platform

Your IT / Ops department

Multiple cloud applications







Embedded Devices

Gateway

Backend – Private or Public Cloud

ARM

Takeaways

- IoT is
  - applications that span physical and cloud environments
  - IP to the edge
  - devices as web services
  - standards based
  - led by industrial applications
- IoT enables
  - greater visibility on assets
  - increased analytic capability
  - better coordination of processes
- To take advantage you need to
  - Feel free to experiment with hosted services to understand potential gains
  - Prepare your IT and ops departments to take control of connected assets
  - Assess and defend new threats

ARM

Amyas Phillips
amyas.phillips @arm.com

Background

ARM

Key length guidance

NIST recommendations compiled by keylength.com

Date	Minimum of Strength	Symmetric Algorithms	Asymmetric	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
2010 (Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1** SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
2011 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
> 2030	128	AES-128	3072	256	3072	256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
>> 2030	192	AES-192	7680	384	7680	384	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
>>> 2030	256	AES-256	15360	512	15360	512	SHA-512	SHA-256 SHA-384 SHA-512

ARM

Design patterns

- IP to the edge
- Devices are web services too
- Design for intermittent offsite connectivity
  - Tight control loops over public internet are not advisable
  - In fact any tight control loop ought to be local and have dedicated connections on site
- Every device has its own public-private key pair
  - Prevent class breaks
  - Greater provisioning flexibility
- Connected devices' connectivity managed by IT departments
  - "Device networks" managed as infrastructure, similarly to corporate WiFi
  - Also hold the security keys and documentation of web APIs
  - Control access by internal and external services
  - What devices *do* is managed by ops teams

Is interoperability inevitable?

- Remains to be seen which industry verticals have an interest in standard models
- Needs interoperability to be in everyone's interests
- Standards solve common problems
- Likely to solve a problem you have, even if you don't need interoperability

Why now?

- 1990s: Why would we want to connect edge devices to the internet?
  - Facilitate integration
  - Eliminate costly protocol gateways
  - Use cheap off-the-shelf parts and well-tested protocols
- 2000s: Is it feasible to connect edge devices to the Internet?
  - Lightweight IP stacks run on kBs RAM and ROM
  - 6LoWPAN / CoAP standards cut overheads
  - Low cost embedded linux devices, wifi and cellular became widespread
- 2010s: What can we do with internet-connected edge devices?
  - Capabilities beyond local control

i vs. l

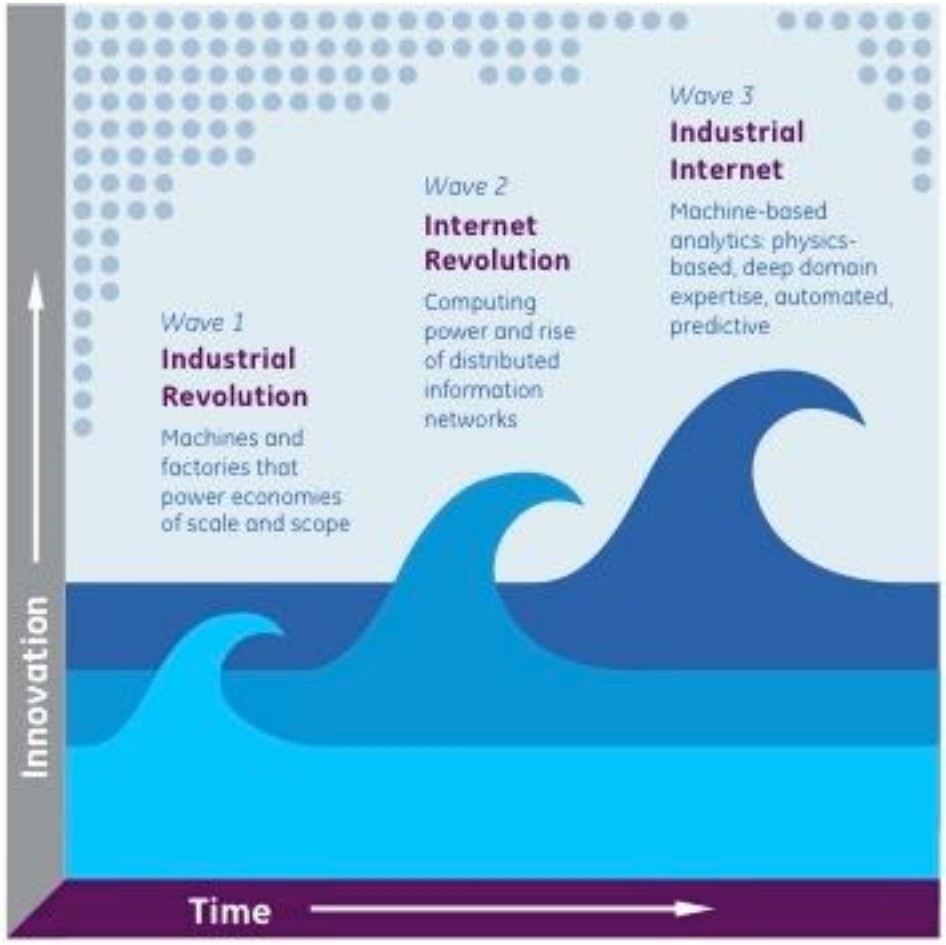
- Edge devices may be constrained by
  - energy
  - bandwidth
  - compute (RAM, Flash, MHz)
- Constraints propagate to protocol choices
  - Can cut IP stacks right down to 10kB Flash, 2kB RAM
  - Painful to program, sacrifice some of the benefits of IP
- Sensible minimum internet peers
  - 512k Flash, 128k RAM (for networking, security, application, scratch space for updates)
  - Bandwidth to accept ~10kB firmware patches, energy budget to accept them ~annually
  - Ideally AES in HW, very good entropy source (RNG)

INTERNET OF THINGS LANDSCAPE

© Matt Turck (@mattturck), Sutian Dong (@sutiandong) & FirstMark Capital (@firstmarkcap)

ARM

The third industrial revolution?



ARM