Edge Computing

1

Develop a passion for learning.

Overview

In many instances, it would be incredibly beneficial to handle data on the device where it's generated. That's where edge computing comes in. Edge computing helps decentralize data processing and lower dependence on a centralized cloud premise.

Overview

Edge computing advantages:

- Increasing data security and privacy
- Better, more responsive and robust application performance
- Reducing operational costs
- Improving business efficiency and reliability
- Unlimited scalability
- Conserving network and computing resources
- Reducing latency

LOGISTICS

Class Hours:

- Start time is 8:30 am PST
- End time is X:XXpm
- Class times may vary slightly for specific classes
- Breaks mid-morning and afternoon (15 minutes)

Lunch:

- Lunch is
- Yes, 1 hour and 15 minutes
- Extra time for email, phone calls, or simply a walk.

Telecommunication:

- Turn off or set electronic devices to vibrate
- Reading or attending to devices can be distracting to other students
- Try to delay until breaks or after class

Miscellaneous

- Courseware
- Bathroom
- Fire drills

DAY 1

Agility

What is Edge Computing?
- Overview
- Architecture
- Platforms
- Use cases
    - Server Parking
    - Driverless cars
    - Edge & IoT

Edge Routing and Networking
- Routing and networking concepts
- TCP/IP network functions at the edge
- Edge-level network security
- Software-defined networking

Edge to Cloud Protocols
- Concepts
- Protocols
    - MQTT
    - MQTT-SN
- Constrained application protocol
- Protocol summary and comparison

Cloud and Fog Topologies
- Overview
- Cloud services model
- Public, private, and hybrid cloud
- Constraints of cloud architectures for Edge & IoT
- Fog computing

DAY 2

Velocity

Edge & IoT Definition and Use Cases
- Internet-of-Things (Edge & IoT) definition
- History of Edge & IoT
- Example use-cases and deployments
- Architecture
  - Sensing and power
  - Data communication
  - Edge computing and Edge & IoT
- Compute, analytics, and machine learning
- Threats
- Security best practices

Sensors, Endpoints, and Power Systems
- Overview
- Sensing devices
- High performance Edge & IoT endpoints
- Functional examples (putting it all together)
- Energy sources and power management

Communications and Information Theory
- Introduction
- Communication theory
- Information theory
- The radio spectrum

Non-IP Based WPAN
- Overview
- 802.15 standards
- Bluetooth
- IEEE 802.15.4
- Zigbee
- Z-Wave

IP-Based WPAN and WLAN
- Concepts
- TCP/IP
- WPAN with IP – 6LoWPAN
- IEEE 802.11 protocols and WLAN
- WPAN with IP - Thread

DAY 3

Observability

Long-Range Communication Systems and Protocols (WAN)
- Overview
- Cellular connectivity
- LoRa and LoRaWAN
- Sigfox

Data Analytics and Machine Learning in the Cloud and Edge
- Introduction
- Basic data analytics in Edge & IoT
- Machine learning in Edge & IoT
- Edge & IoT data analytics and machine learning comparison and assessment

Edge & IoT and Edge Security
- Overview
- Cybersecurity vernacular
- Anatomy of Edge & IoT cyber attacks
- Physical and hardware security
- Shell security
- Cryptography
- Software-Defined Perimeter
- Blockchains and cryptocurrencies in Edge & IoT
- Government regulations and intervention
- Edge & IoT security best practices

Consortiums and Communities
- Concepts
- PAN consortia
- Protocol consortia
- WAN consortia
- Fog and edge computing consortia
- Umbrella organizations
- US government Edge & IoT and security entities
- Industrial and commercial Edge & IoT and Edge Computing organizations

Meet The Instructor

George Niece AKA geo

Digital Transformation, DevSecOps, Edge & IoT Consultant with a Software Engineering, Digital Commerce, and IT operations background. Focused on cloud-native application modernization, datacenter divestiture, and cloud adoption.

Twitter
@georgeniece

LinkedIn
Linkedin.com/in/GeorgeNiece

mail
George.Niece@DigitalTransformationStrategies.net

Expertise
- Cloud-native
- XaaS
- AppDev
- Edge & IoT
- Automation
- CI/CD
- Microservices
- Agile

GTKY

Please let me know your

Name

Where you work from?

Experience with

- Edge Computing
- Internet of Everything
- Content Delivery Network
- Serverless – Functions as a Service

Please rate yourself (1-5) 1 = new joiner, 5 = SME

Lastly, what is your favorite dessert?

Edge Computing

Edge Optimization

- Convergence of business, process, and government standards like Industry 4.0 and Society 5.0

Mass production

↓

Mass customization

Buy

↓

Lease

Pay up front

↓

Pay as you go

Manual

↓

Automatic

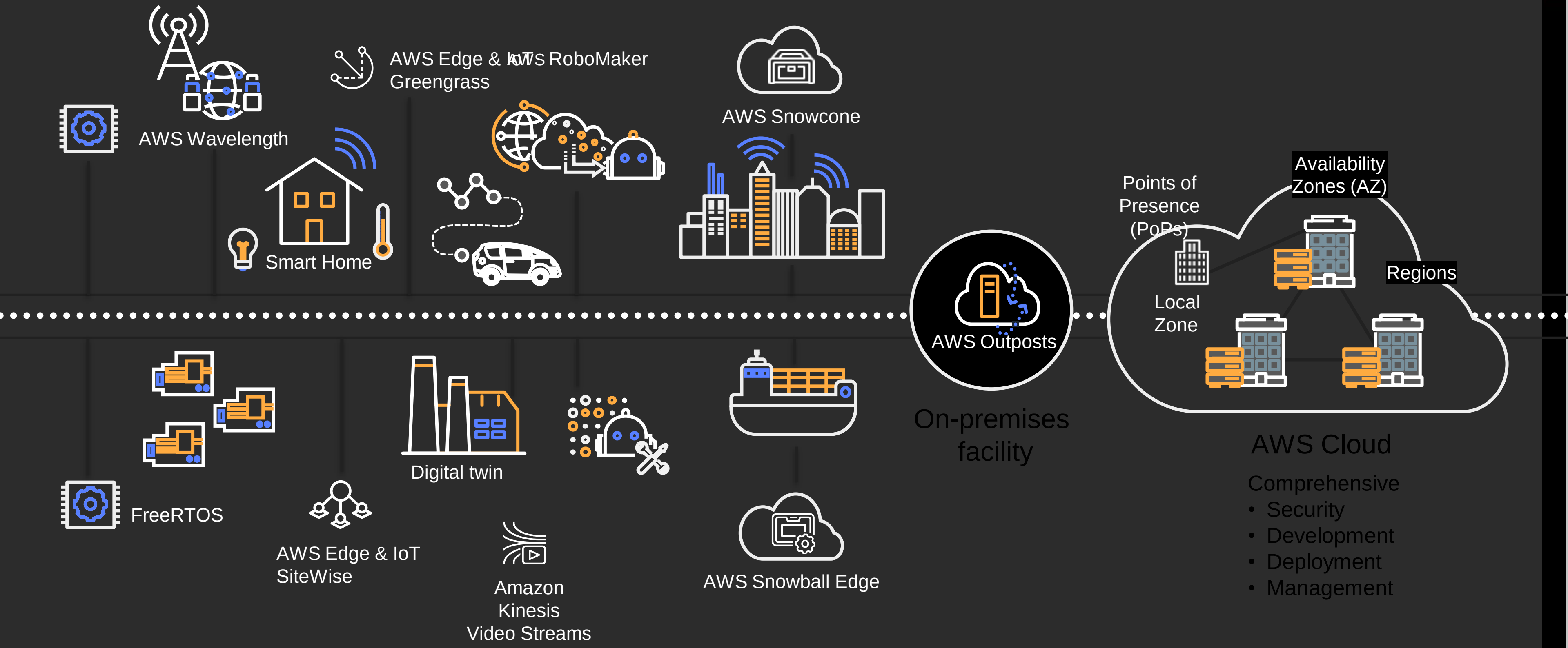
Important industrial application use cases

Predictive maintenance

Predictive quality

Asset condition monitoring

Edge-to-cloud Continuum



Technology problem definition

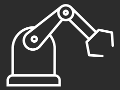
100s OF PRIVATE NETWORKS THAT OPERATE ACROSS EDGE SERVICES AND APPLICATIONS

Requirements in today's world

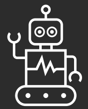
Cell tower
on a robot

Mesh
networks

Leverage 5G Edge Cloud
for low latency



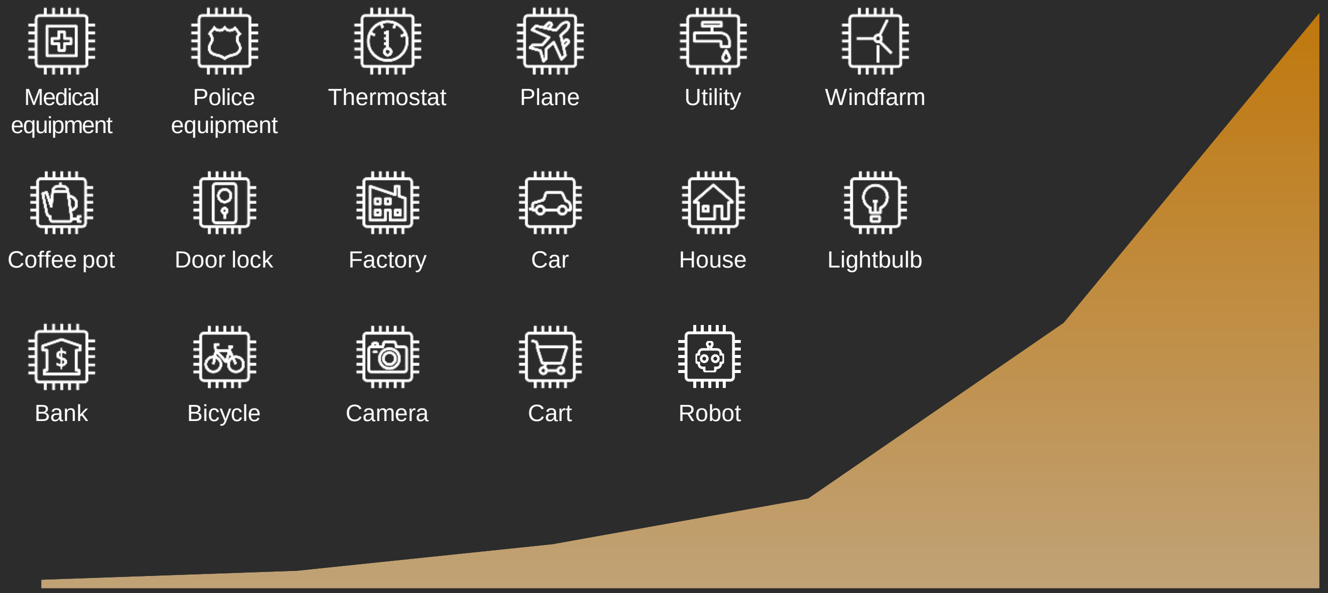
Robot
control



Controller for
robotics

Digital twin

The source of data is increasing—coming from billions of edge devices

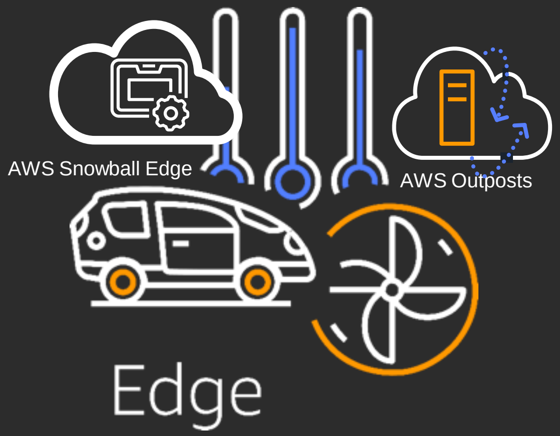


75 billion
connected devices online by:
2025

Sources: McKinsey & Co., Inc., Statista   Source: Statista.com

Source: Statista.com

Working with edge devices is challenging

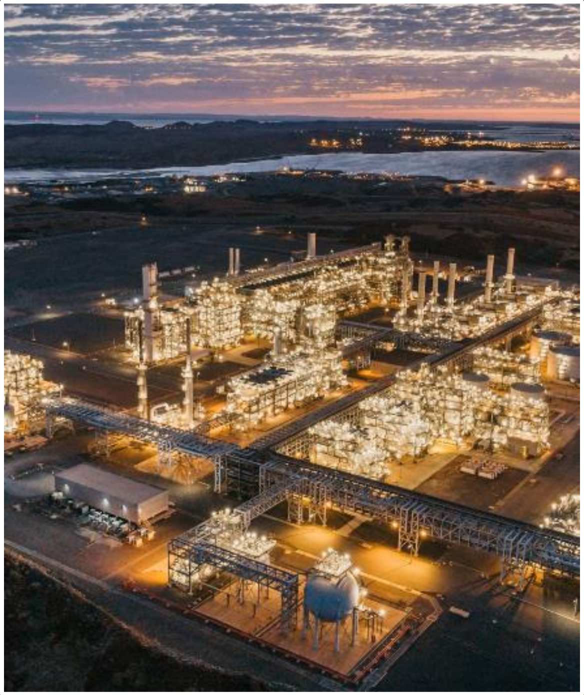


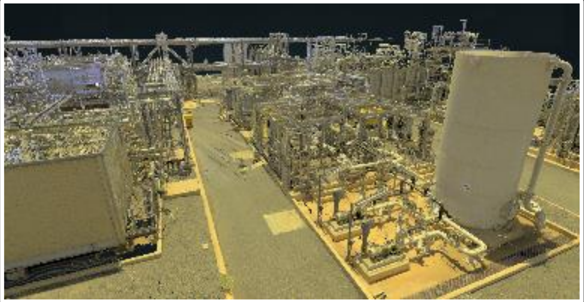
Law of physics

Law of economics

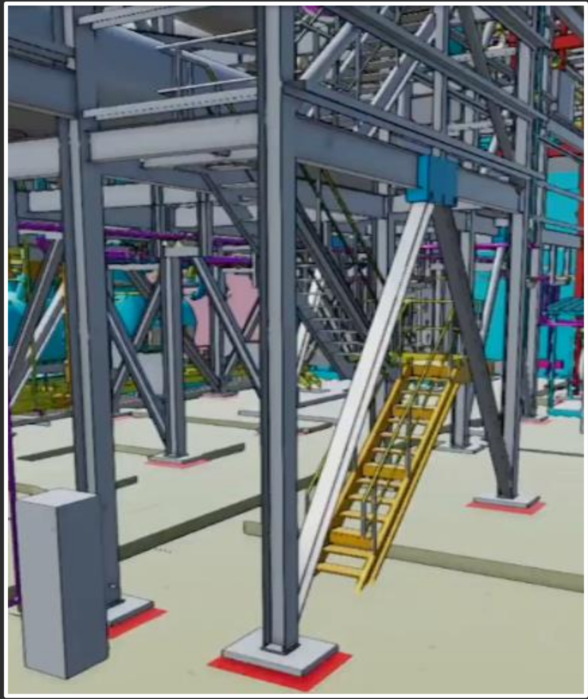
Law of the land

Digital Twin

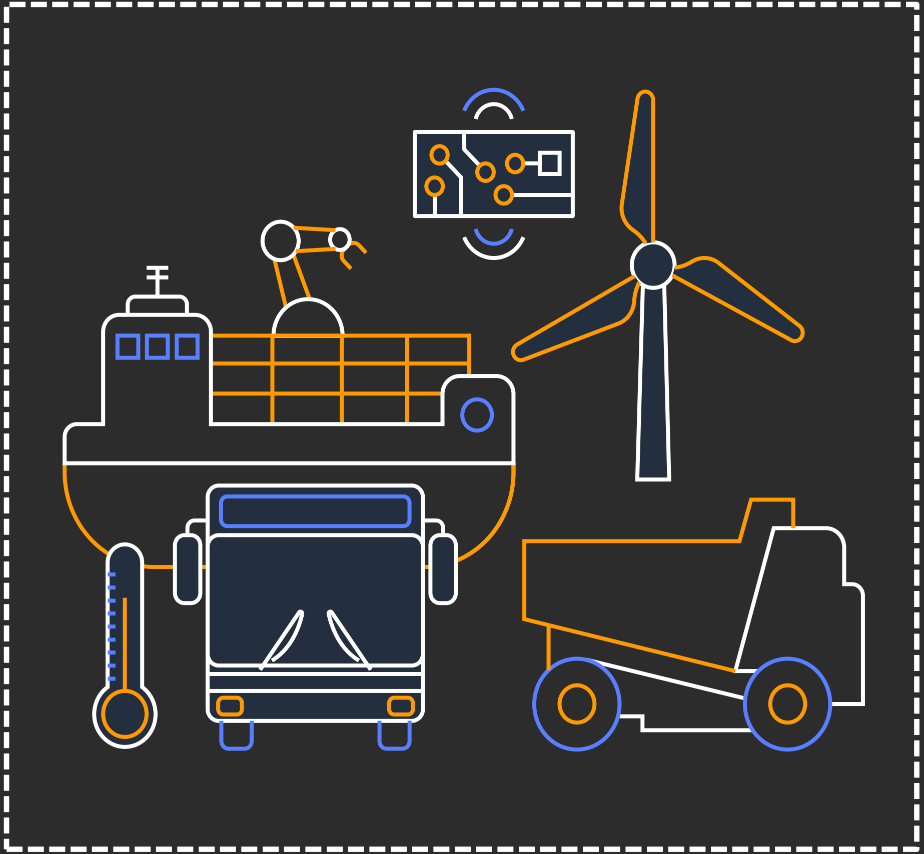




Woodside LNG Plant



Collecting and analyzing data can also be tough



Edge to cloud architecture

Challenges faced at the Edge

Security

Keep devices and data secure

Connectivity

Operate at top performance with local mobility, even in remote locations

Legacy equipment

Onboard greenfield and brownfield devices

Reliable, low-latency, and high-performance services

Industry 4.0 is transforming industrial processes

Edge Computing and Edge & IoT bring sensors, machines, cloud computing, analytics,
and people together to improve productivity and efficiency

Manufacturing

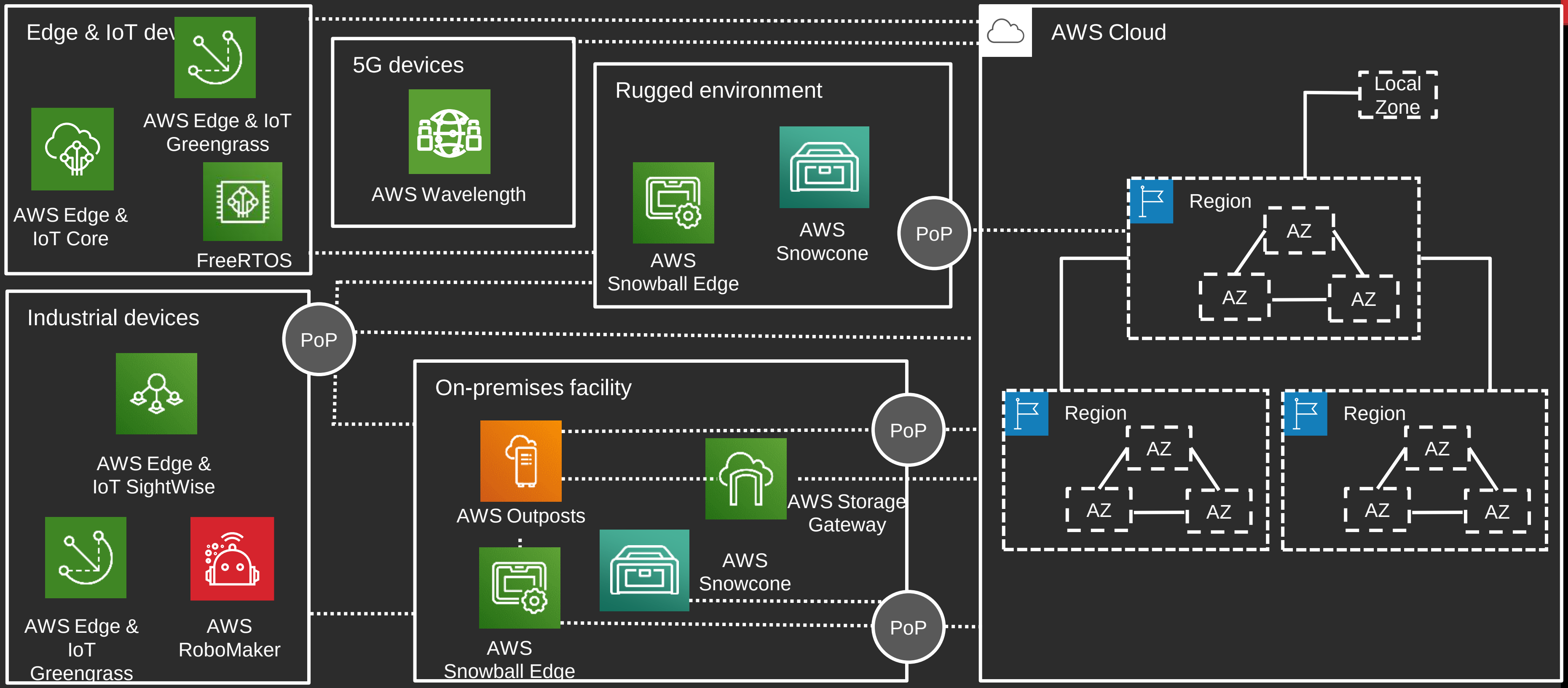
Mining

Oil & Gas

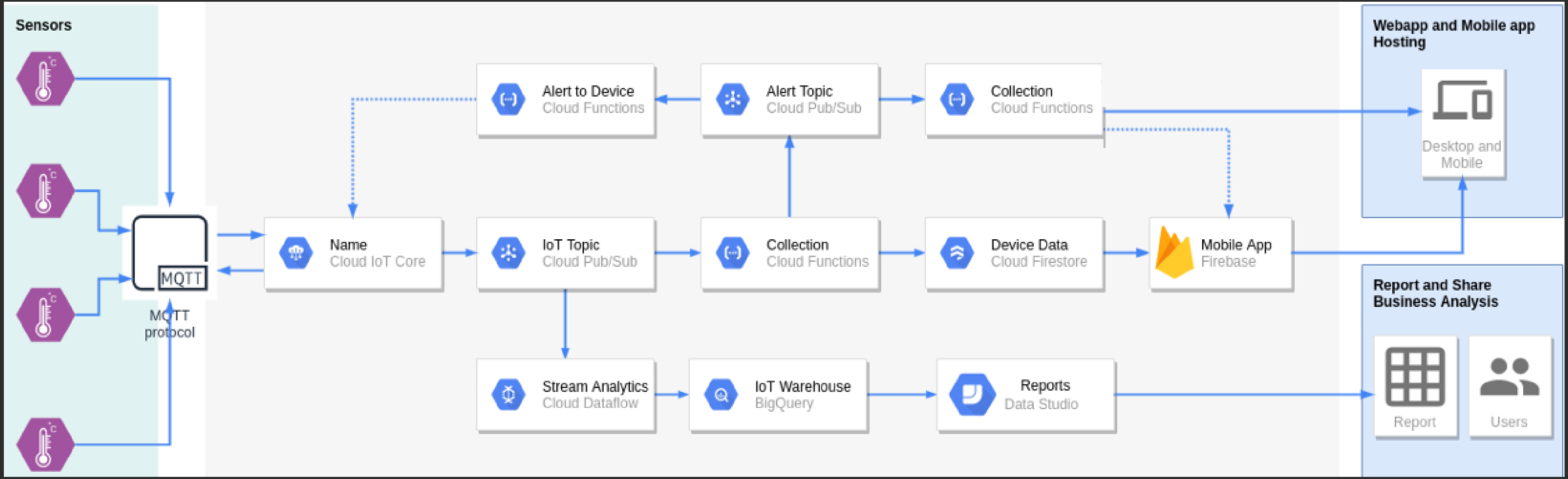
Agriculture

Cloud & Fog Topologies

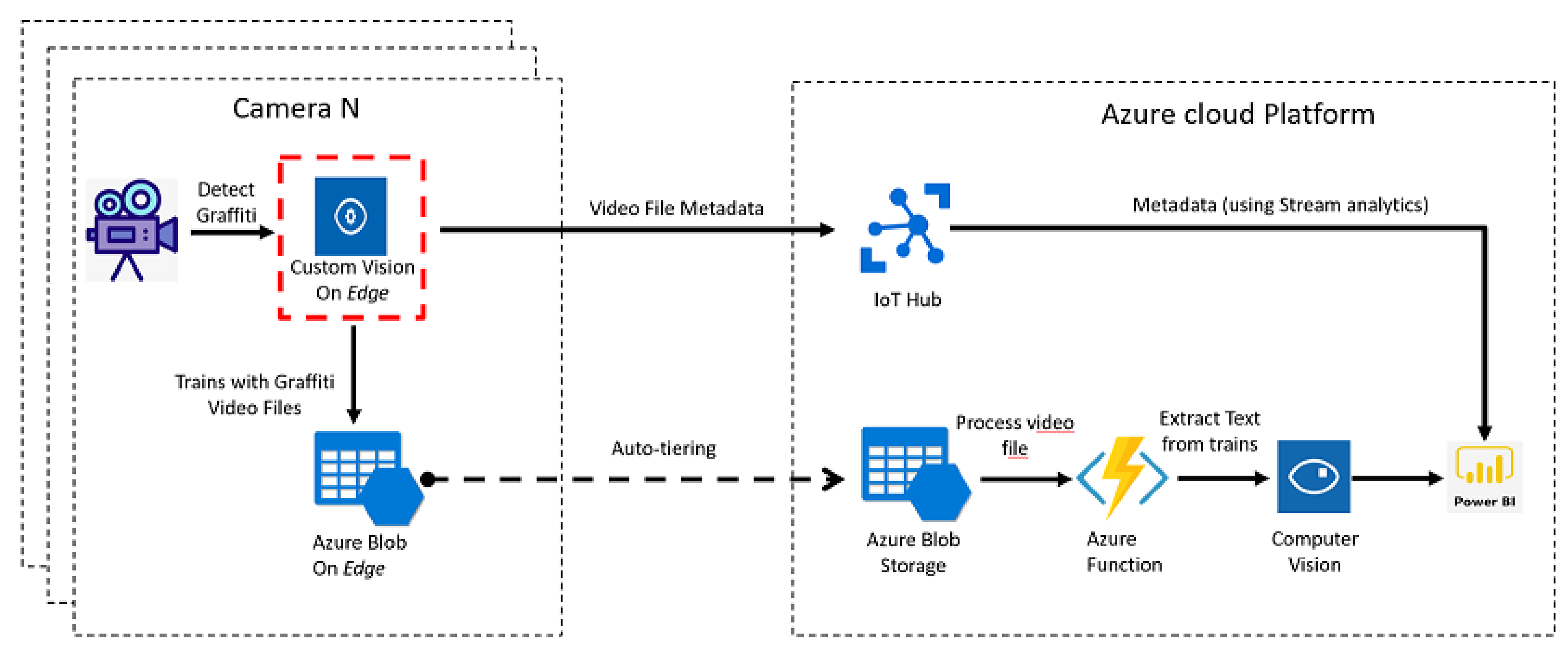
AWS Edge Architecture



Google Edge Architecture



Azure Edge Architecture



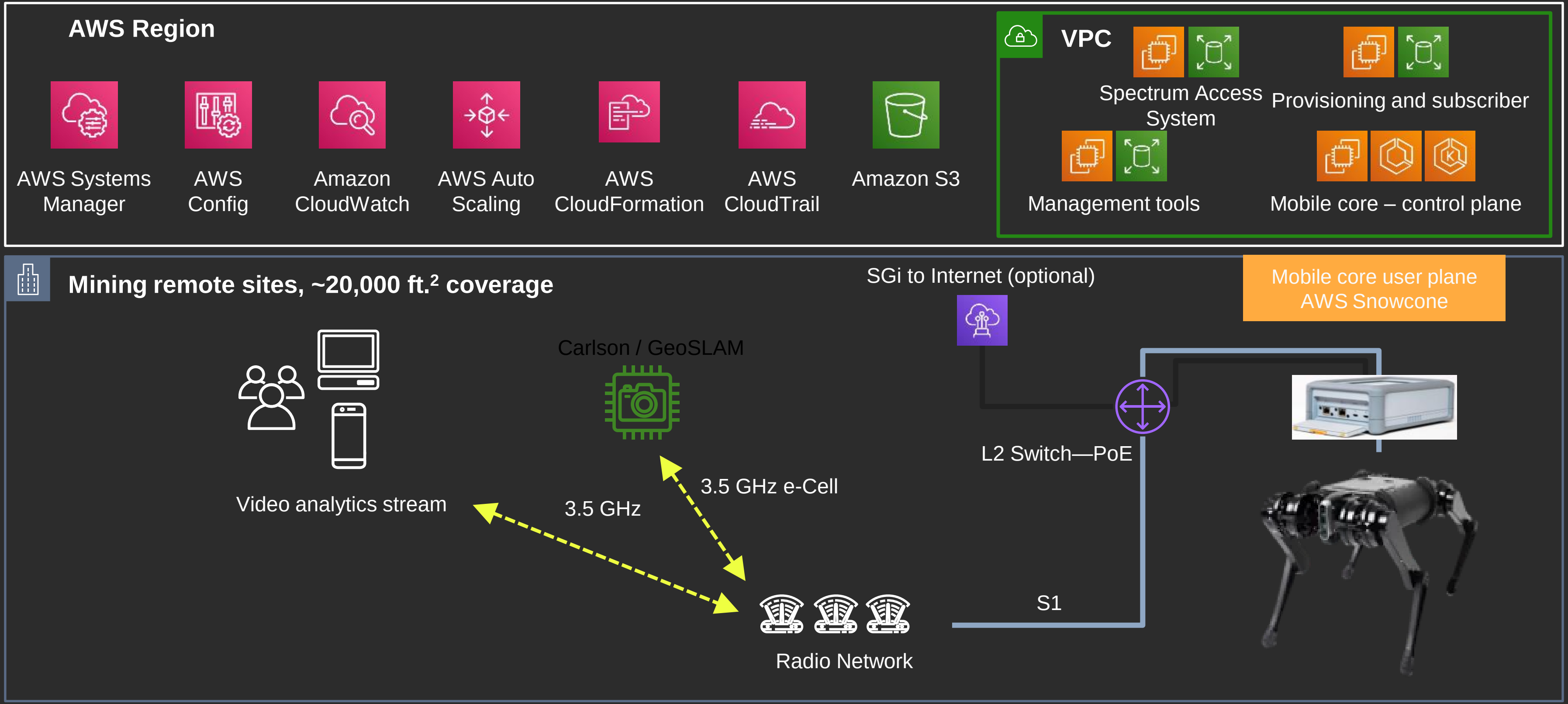
Fog & Edge Computing

Fog & Edge Computing

As the **volume of data created by Edge devices continues to grow**, it has become cumbersome and unrealistic for each thing to send its raw data to a central location for processing. This model of **sending everything to the cloud** has caused **bandwidth challenges, latency issues, and delays in processing**.

In response to these growing challenges, organizations are deploying smaller processing **data centers closer** to where the data is created. This intermediate processing is often referred to as **Fog Computing**.

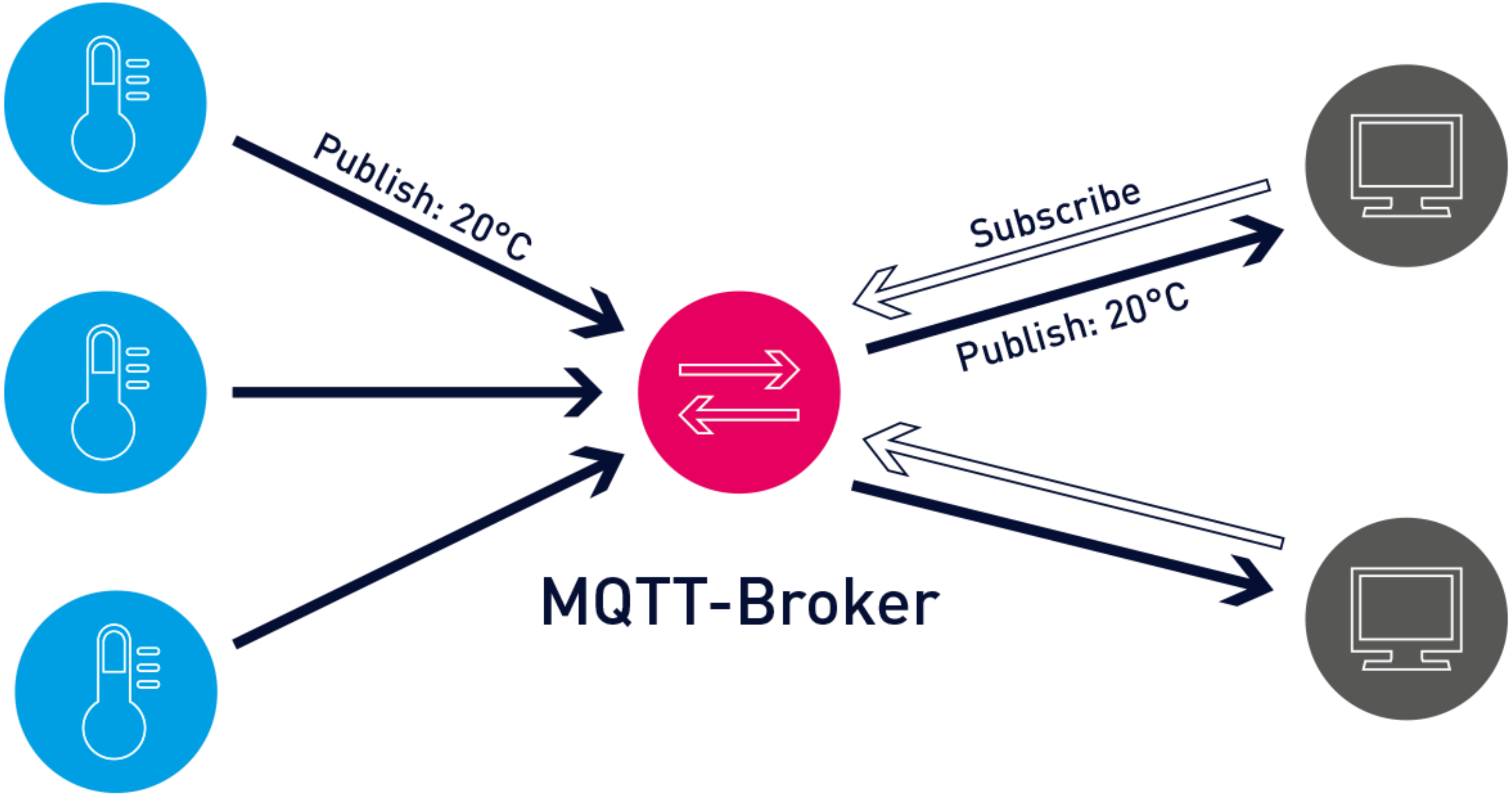
4G / 5G on AWS


AWS Region
AWS Systems Manager
AWS Config
Amazon CloudWatch
AWS Auto Scaling
AWS CloudFormation
AWS CloudTrail
Amazon S3
VPC
Spectrum Access System
Provisioning and subscriber
Management tools
Mobile core – control plane
Mining remote sites, ~20,000 ft.² coverage
SGi to Internet (optional)
Mobile core user plane
AWS Snowcone
Carlson / GeoSLAM
Video analytics stream
3.5 GHz
3.5 GHz e-Cell
L2 Switch—PoE
S1
Radio Network

4G / 5G on Azure

Edge to Cloud Protocols

What is MQTT



What is MQTT

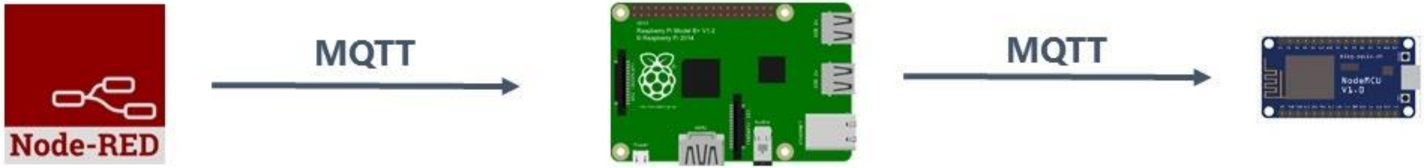
MQTT stands for Message Queuing Telemetry Transport.

It is used in cases where clients need a small code footprint and are connected to unreliable networks or networks with limited bandwidth resources.

It is primarily used for machine-to-machine (M2M) communication, Edge Computing, or Internet of Things types of connections.

MQTT – How It Works

Send a command to **control an output**



Read and **publish** data

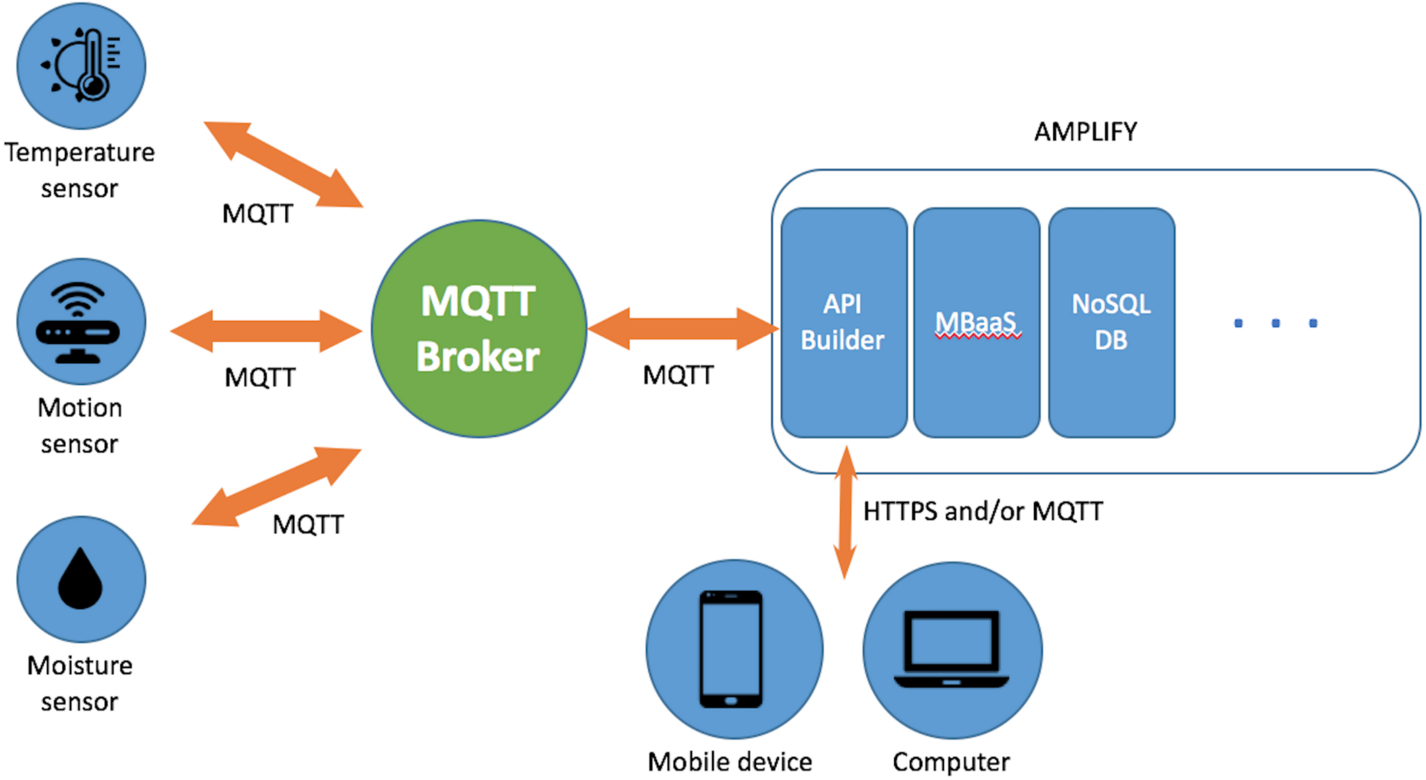
How does MQTT Work?

It is a lightweight publish and subscribe system where you can publish and receive messages as a client.

MQTT is a simple messaging protocol, designed for constrained devices with low-bandwidth. So, it’s the perfect solution for Edge Computing & Internet of Everything (IoE) applications. MQTT allows you to send commands to control outputs, read and publish data from sensor nodes and much more.

Therefore, it makes it really easy to establish a communication between multiple devices.

MQTT in Action

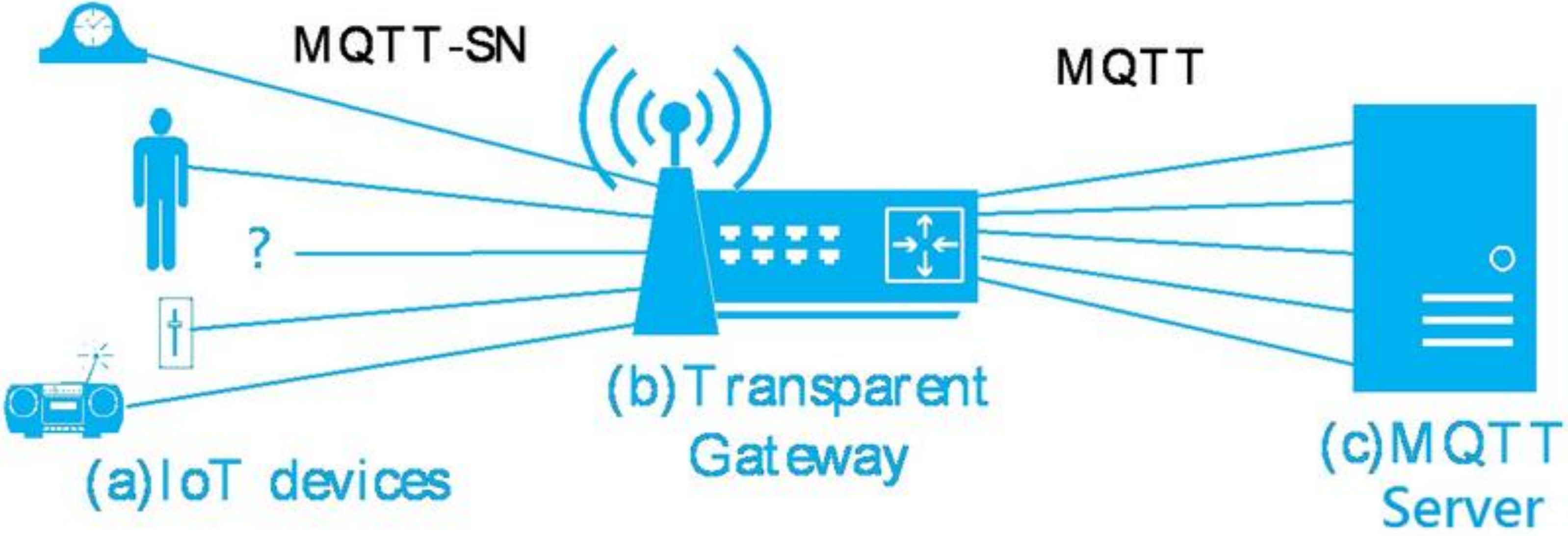


MQTT Vernacular

The important terminologies in MQTT are as follows:

Publisher: Publishes messages to the outer world.
Subscriber: Receives messages that have been published.
Client: A client can be either publisher or subscriber or both. That is a client can publish a message and receive another message at the same time.
Server/Broker: The one receives the messages published by the publisher first, even before the subscriber. Then the server publishes the messages to the subscribers after filtering the messages. Both the names server and broker mean the same entity.
Topic: An UTF-8 string used by the clients and servers to send and receive messages. Eg: sensors/altimeter/1.

MQTT-SN


MQTT-SN
MQTT
?
(b)Transparent
Gateway
(a)IoT devices
(c)MQTT
Server

MQTT-SN vs. MQTT

The main differences involve:

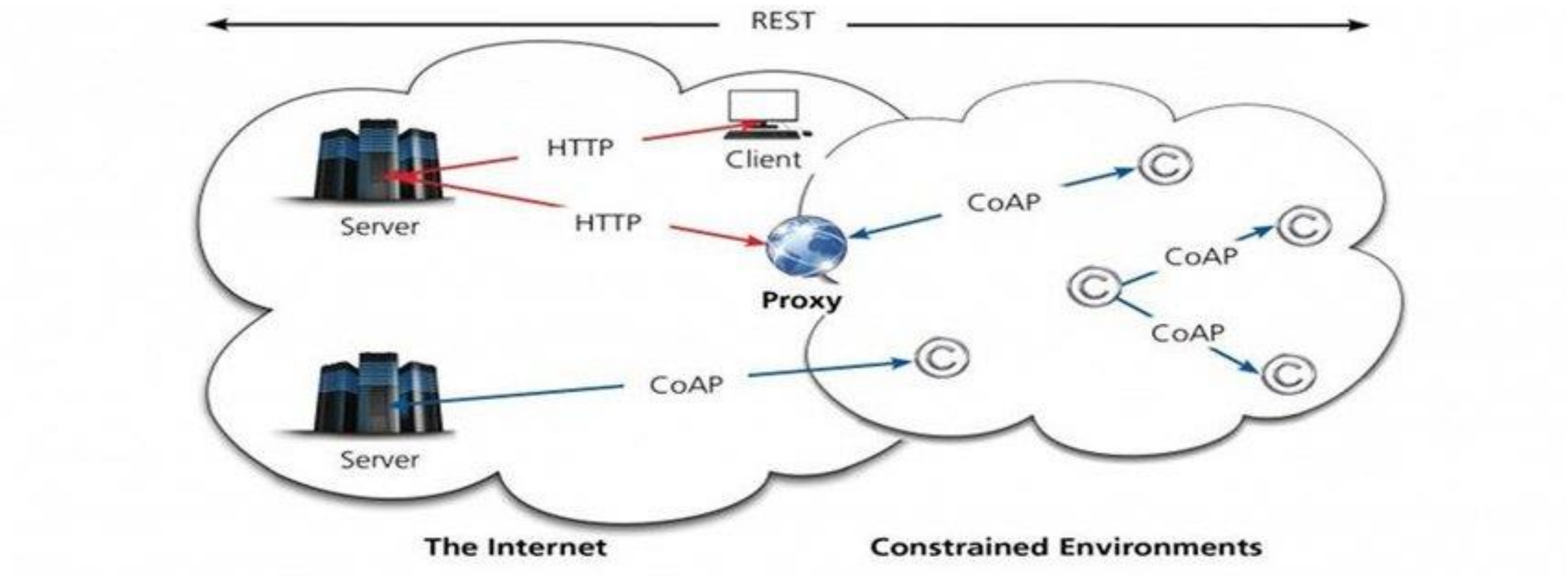
•**Reducing the size** of the message payload
•Removing the need for a permanent connection by using **UDP** as the transport protocol.

MQTT-SN Details

The **MQTT-SN** specification lists these differences.

1. Connect message split into three messages two are optional and are used for the will message
2. Topic id’s used in place of topic names.
3. Short Topic names
4. Pre-defined topics.
5. Discovery process to let clients discover the Gateway
6. Topic and messages can be changed during the session
7. Off-line keep alive procedure for **sleeping clients.**

Constrained Application Protocol



COAP

Constrained Application Protocol (aka CoAP) is a specialized web transfer protocol for use with constrained nodes (low power sensors and actuators) and constrained networks (low power, lossy network). It enables those nodes to be able to talk with other constrained nodes over Internet. The protocol is specifically designed for M2M applications such as smart energy, home automation and many Industrial applications.

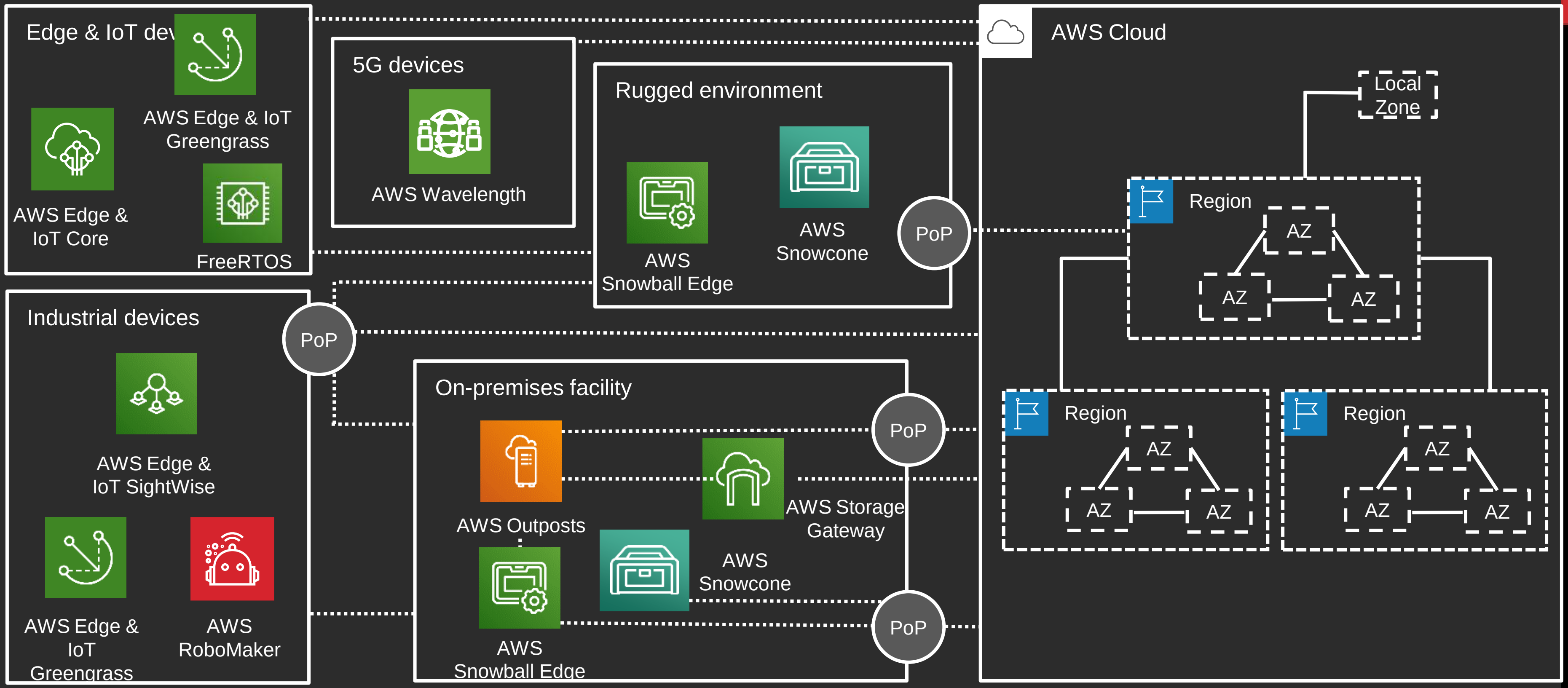
Edge Computing Case Study

Ghost Robotics

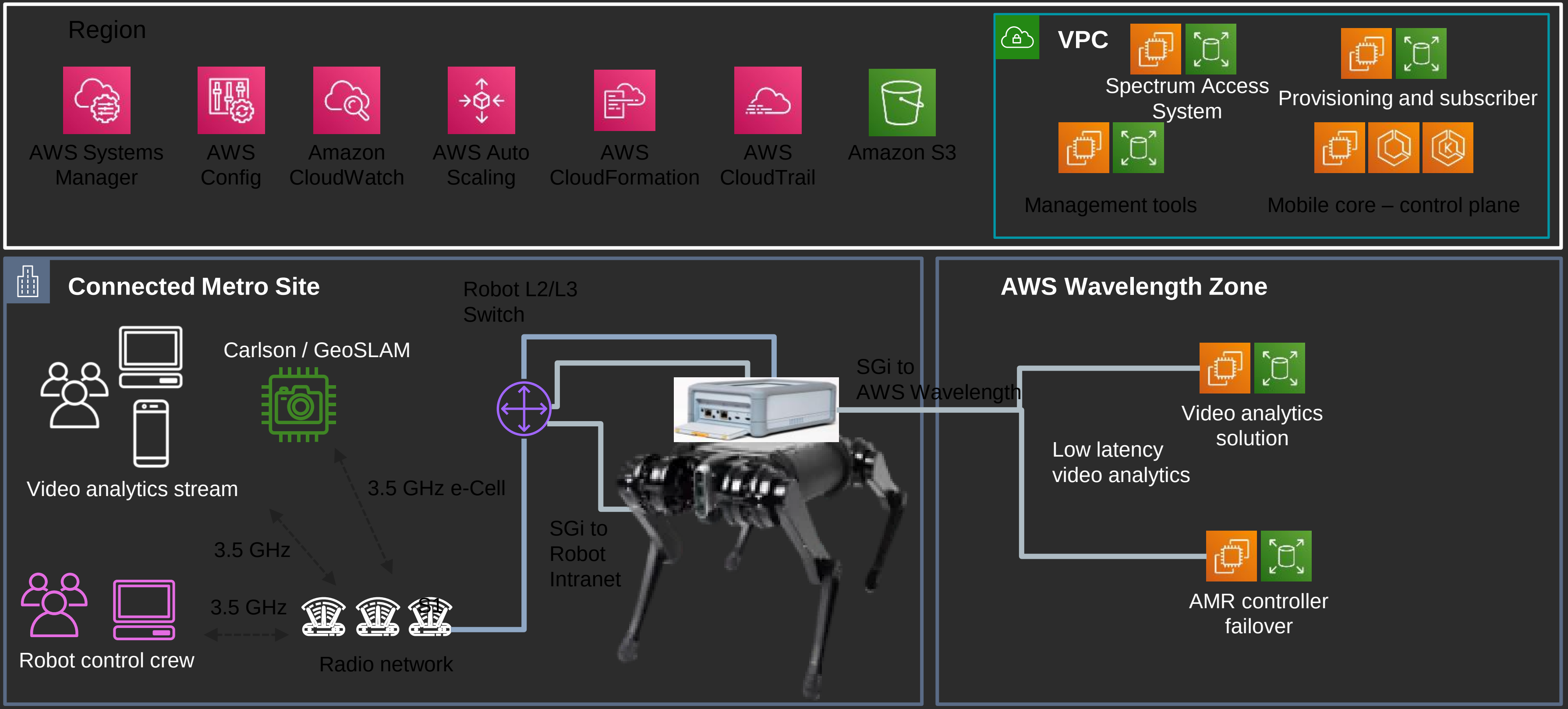
- Company and platform
  - Mobile Edge platform: sensors and comms
  - High-availability, all-terrain, and open architecture
  - Focus: military and homeland, and now enterprise
  - Inspect, manage, and secure
- Challenges and today’s world
  - Continuous coverage in remote / dangerous locations
  - Worker safety
  - Lack of human resources and expertise
  - Data density and persistent comms

GHOSTROBOTICS

Edge services required for GhostRobotics use case

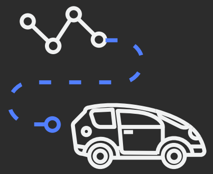


Low Latency Video Analytics on the Edge

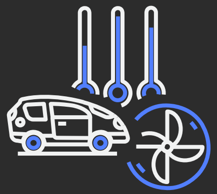


Edge Lessons Learned

Understand the available Edge services and architecture best practices before selecting a solution



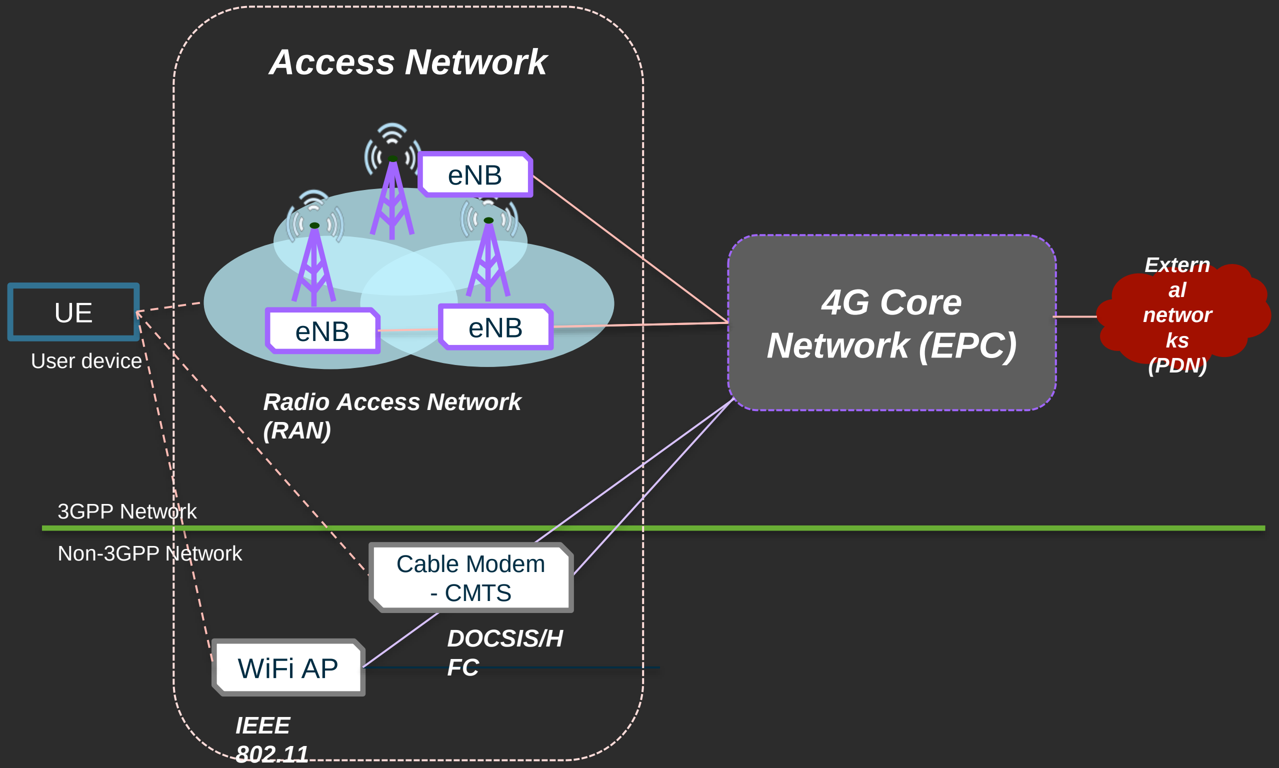
Autonomous mobile robots when integrated effectively with private networks and 5G Edge Cloud can help drive efficiency and improve worker safety



Even industrial customers in AgTech, Mining, Refineries, Construction, and Government need to have a mobility and AMR strategy to realize the vision of I4R

5G Edge

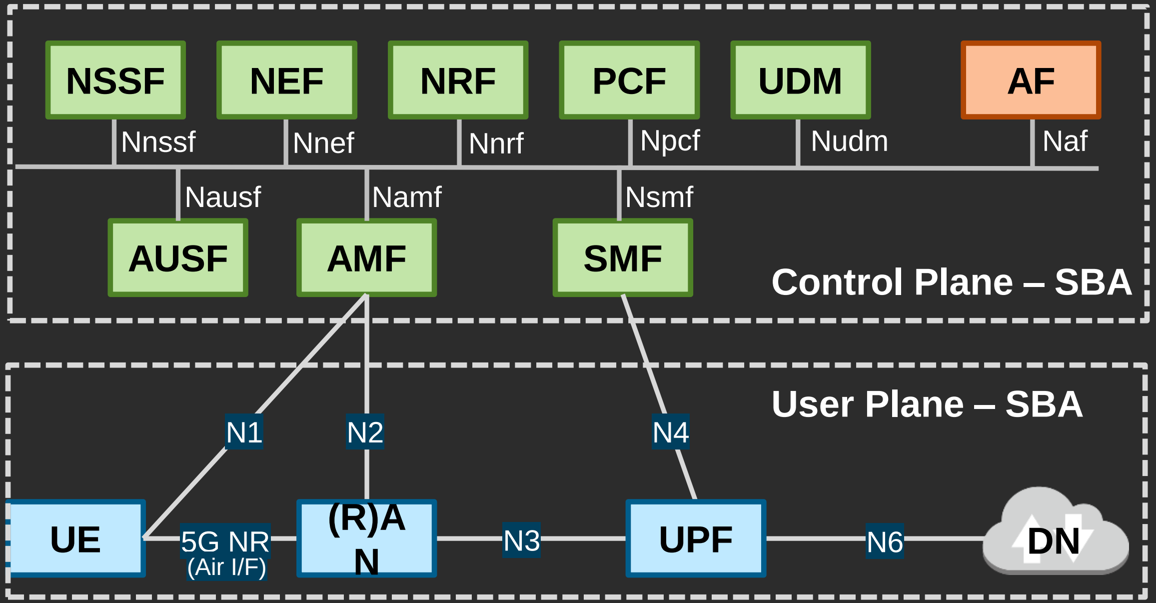
Edge 4G(LTE) architecture



- eNB
  - Evolved NodeB (evolved radio network)
  - Radio resource allocation/scheduling
- 4G Core Network (EPC)
  - Evolved Packet Core
  - Mobility management, user (SIM) authentication
  - Both voice and data service for LTE using IP

Edge 3GPP 5G reference architecture

- **CUPS (Control plane and User plane Separation)**
- **Stateless Architecture**
- **SBA (Service Based Architecture)**
- **Network Slicing**



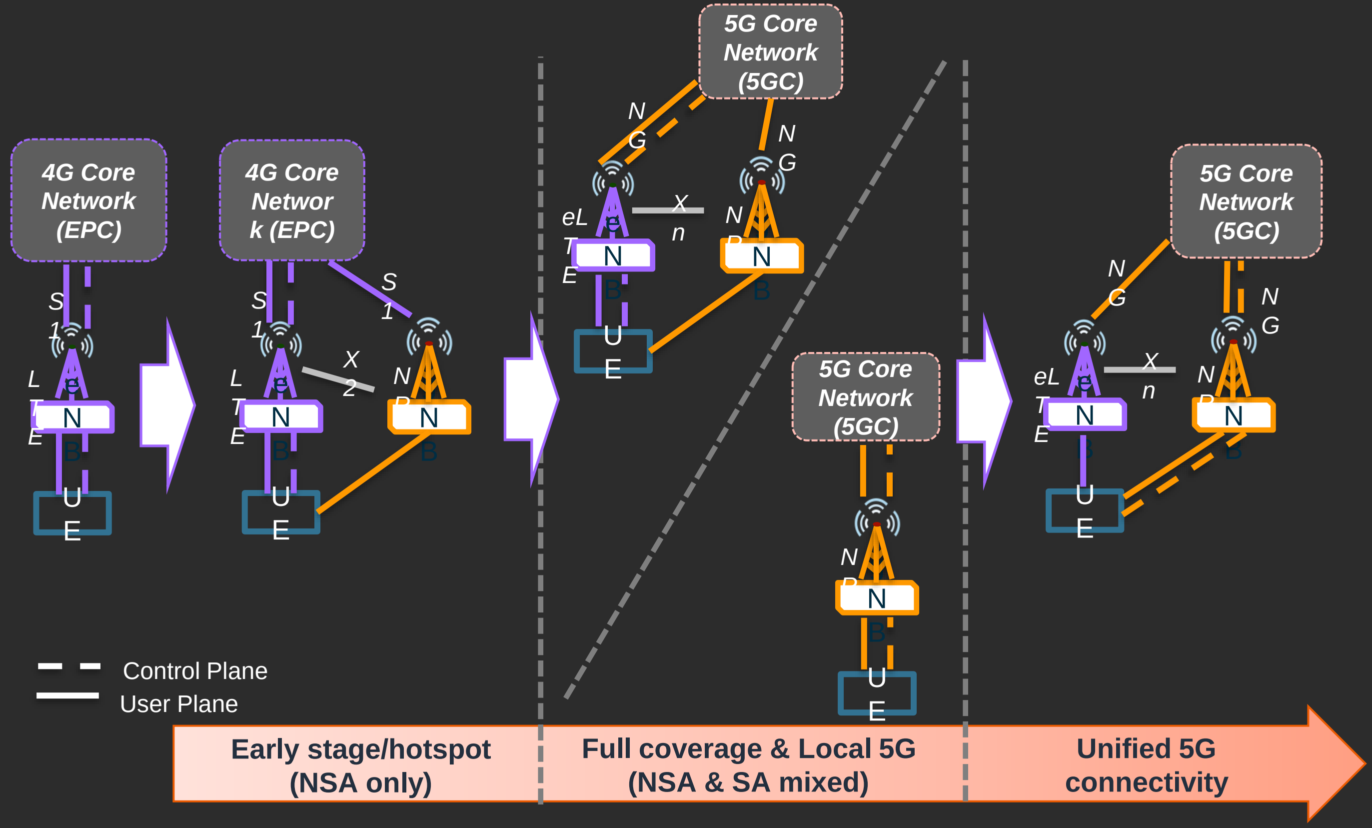
AF: Application Function

AMF: Access & Mobility Management Function
SMF: Session Management Function
AUSF: Authentication Server Function
UDM: Unified Data Management
PCF: Policy Control Function
NRF: Network Repository Function
NEF: Network Exposure Function
NSSF: Network Slice Selection Function

UE: User Equipment
(R)AN: Radio Access Network/5G Access Network
UPF: User Plane Function

DN: Data Network

Edge 4G to 5G migration



- gNB
  - Logical 5G radio node for 5G radio resource allocation/scheduling
  - Consists of Central Unit(CU) and Distributed Unit (DU)
- Non Standalone (NSA)
  - LTE – NR (New Radio) dual connectivity
  - 4G Core Network (EPC) support
- Standalone (SA)
  - NR with 5GC
  - 4G independent

Edge 5G by definition

3GPP Rel-15/Rel-16

- 5G System: 3GPP system consisting of 5G Access Network (AN) and 5G Core network and UE
- 5G Access Network: An access network comprising a NG-RAN and/or non-3GPP AN connecting to a 5G Core Network
- 5G Core Network: The core network specified in the present document. It connects to a 5G Access Network

ITU-R (IMT-2020)

- 5G service enablers:
  - **eMBB** – Enhanced Mobile Broadband
  - **mMTC** – Massive Machine Type Communications
  - **URLLC** – Ultra-Reliable and Low Latency Communications
- The minimum requirements:
  - for peak **data** rate: Downlink: **20 Gbps**, Uplink: 10 Gbps
  - user plane latency (single user, small packets): 4 ms for eMBB, **1 ms for URLLC**
  - **control** plane latency (idle => active): **10-20 ms**

Key of 5G: High bandwidth & low latency = Faster and closer

NR (New Radio)

The abundant spectrum available at mmWave frequency bands above 24 GHz is capable of delivering extreme data speeds and capacity

(from Qualcomm)

New Channel Coding : LDPC

Sub6GHz : Massive MIMO

Edge

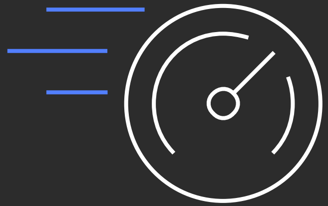
Edge computing as an evolution of cloud computing brings application hosting from centralized data centers down to the network edge, closer to consumers and the data generated by applications. Edge computing is acknowledged as one of the key pillars for meeting the demanding Key Performance Indicators (KPIs) of 5G, especially as far as low latency and bandwidth efficiency are concerned

(from ETSI)

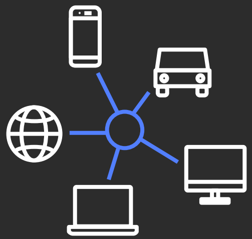
Core Network Evolution

Legacy core network has been rearchitected to have, Service Based Architecture, Stateless Architecture, CUPS (Control and User Plane Separation). This evolution suits well to modern microservice architecture and agile process

5G key challenges for Edge Cloud



Latency



Scalability and flexibility

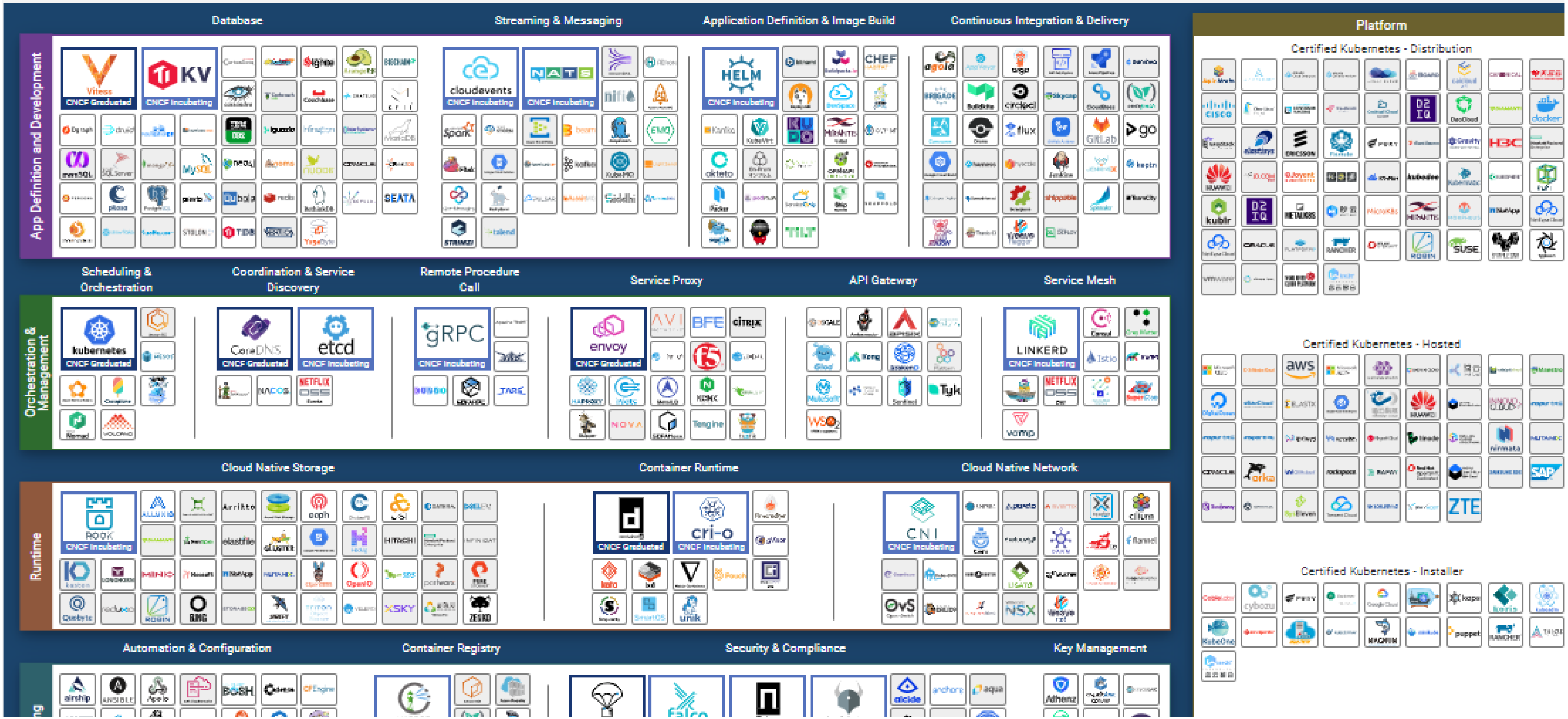
Unified management/ orchestration and automation

Edge Design

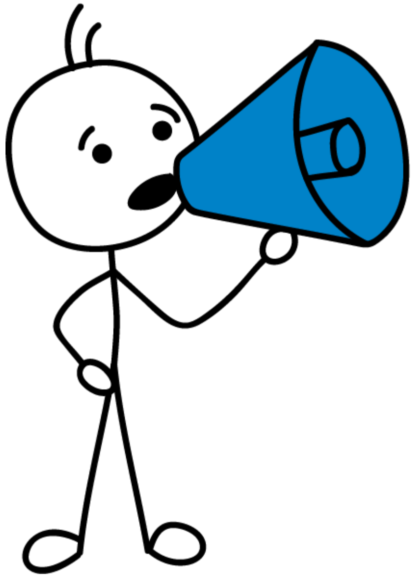
5 Key Architectural Considerations

- What is the semantic definition of the microservice?
- What is the microservice’s SLA?
- How does the microservice expose itself?
- Microservices carry their own data
- Synchronous vs. Asynchronous Interaction

CNCF Landscape



Discussion



- How does CNCF play into Edge?
- What considerations are there for Edge Computing and by extension Edge & IoT?
- Edge interacts with everything else
- On-premise, devices, cloud, and even manual interactions may be part of Edge Computing

Edge & IoT


THINK ACADEMY
Internet of Things
How it Works
0:01 / 3:38

What is the Promise of Edge & IoT?

Realizing new business outcomes by improving the efficiency of workers with process automation, creation and delivery of new digital products through information-fueled insights and actions, and scaling the business by enabling an ecosystem that augments individual capabilities by bringing them together in a unified solution.

Now again without consultant speak

The promise of the Edge Computing & IoT is bringing devices together with people to do things we couldn’t before.

Like …

Snowplows work with traffic lights to allow them to continue without constantly stopping and starting.

Your phone tells you that your child is not home, as expected.

The curling iron texts you to say it's on and you just left the house.

Unlocking Value by Digitizing the Physical World

Defining Edge & IoT

- Edge & IoT describes an eco-system where “things” in the physical world, which have sensors within or attached, are networked to deliver value chains.
- Sensors user local area connections such as RFID, NFC, Zigbee, Wifi, etc.
- Capture of this time series data to derive actionable insight

Edge Computing Definitions

"A new era of ubiquity is coming where humans may become the minority as generators and receivers of traffic and changes brought about by the Internet will be dwarfed by those prompted by the networking of everyday objects"

"From anytime, anyplace connectivity for anyone, we will now have connectivity for anything"

"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts"

Edge & IoT Variations and Word Games

- Most technology and consulting companies have their variation or branding for Edge & IoT platforms
    - Industrial Internet
    - Smarter Planet
    - Machine 2 Machine
    - Cyber-Physical Systems
    - Network of Things
    - System of Things
    - Internet of Everything

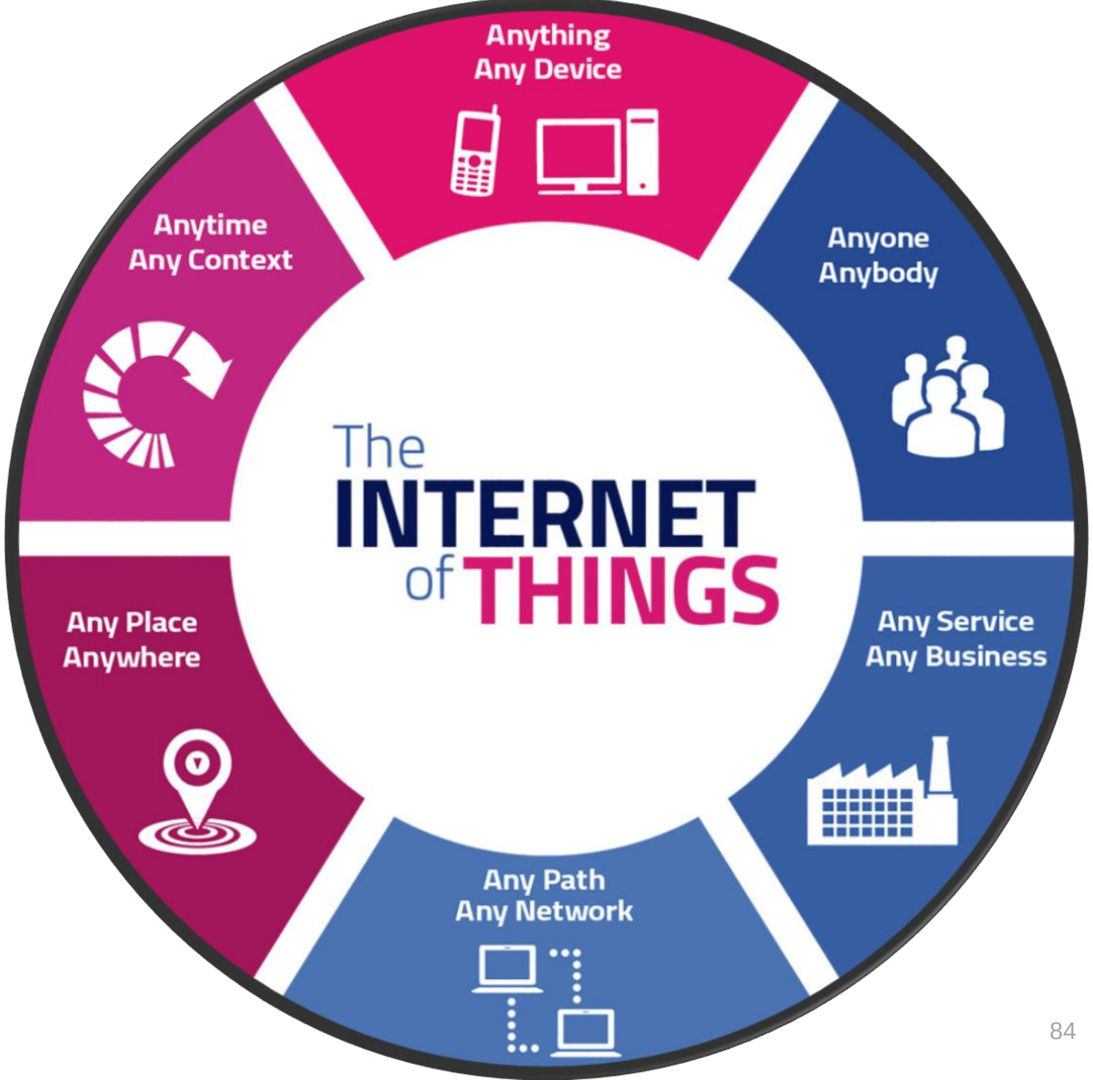
Edge & IoT Interactions

Edge & IoT has a broader scope than other device interactions technologies, like M2M, since it comprises a broader range of interactions:

- Devices or things and other things
- Things and people
- Things with applications
- People with applications

The Edge Computing & IoT also enables the composition of workflows comprising all of the above interactions.

- All Things in the Game



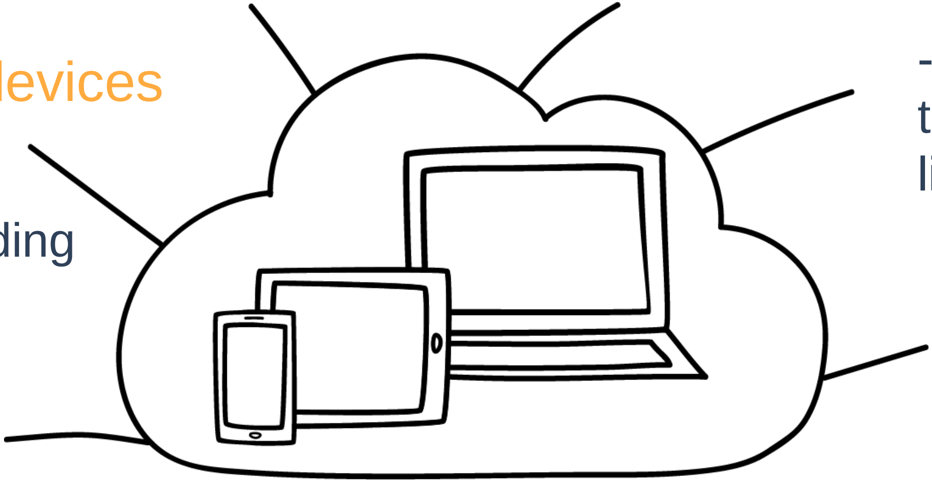
IDC Worldwide Edge & IoT Installed Base by Connectivity Forecast

Edge & IoT devices categories

Smart home devices

M2M devices

- Motion sensors, thermostats, door locks, light switches



-cars, vending machines, aircraft

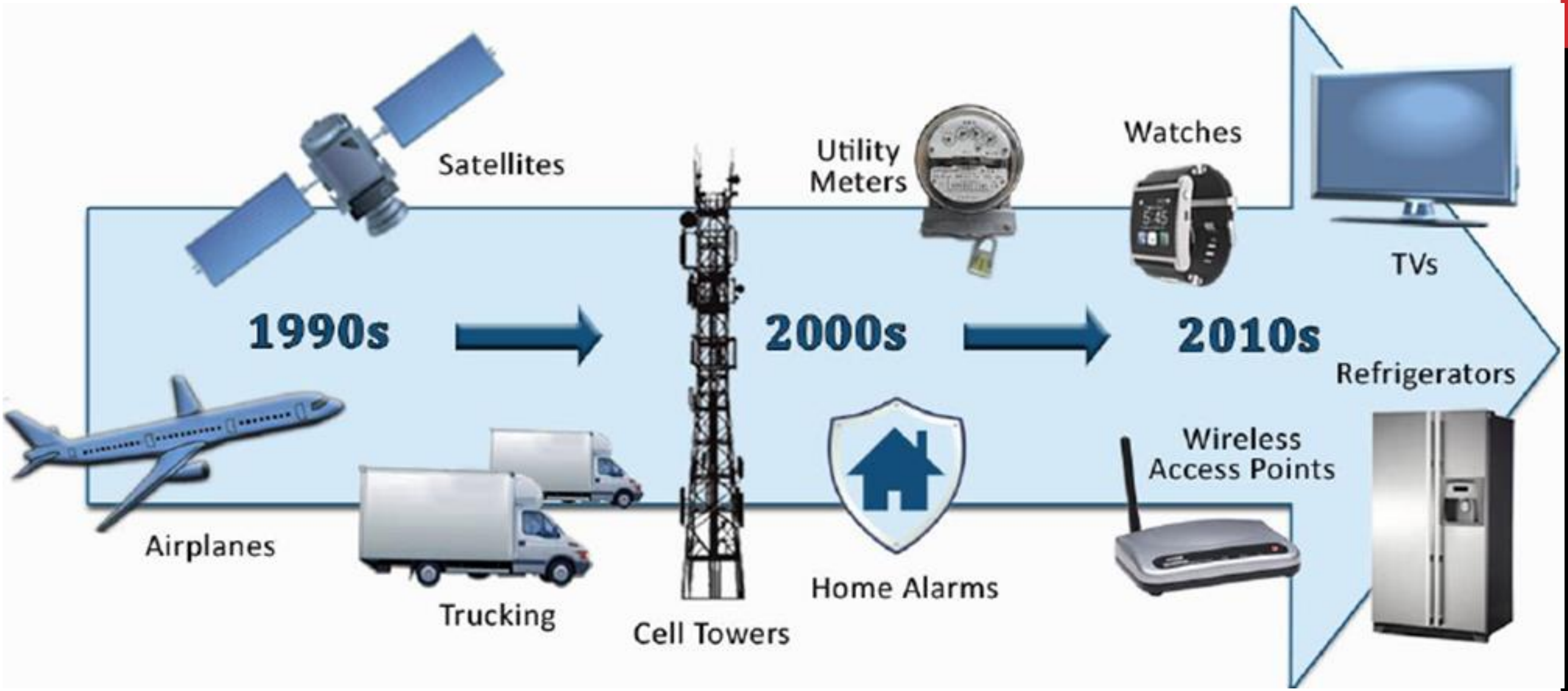
Wearables

-smart watches, fitness bands

Edge & IoT Connection Categories

- Connected Products
- Connected Assets
- Connected Fleets
- Connected Infrastructure
- Connected Markets
- Connected People

Timeline of Edge & IoT



Intergalactic Computer Network

- *A system of computers connected to one another, and a space where all the data is available for everyone from anywhere.*

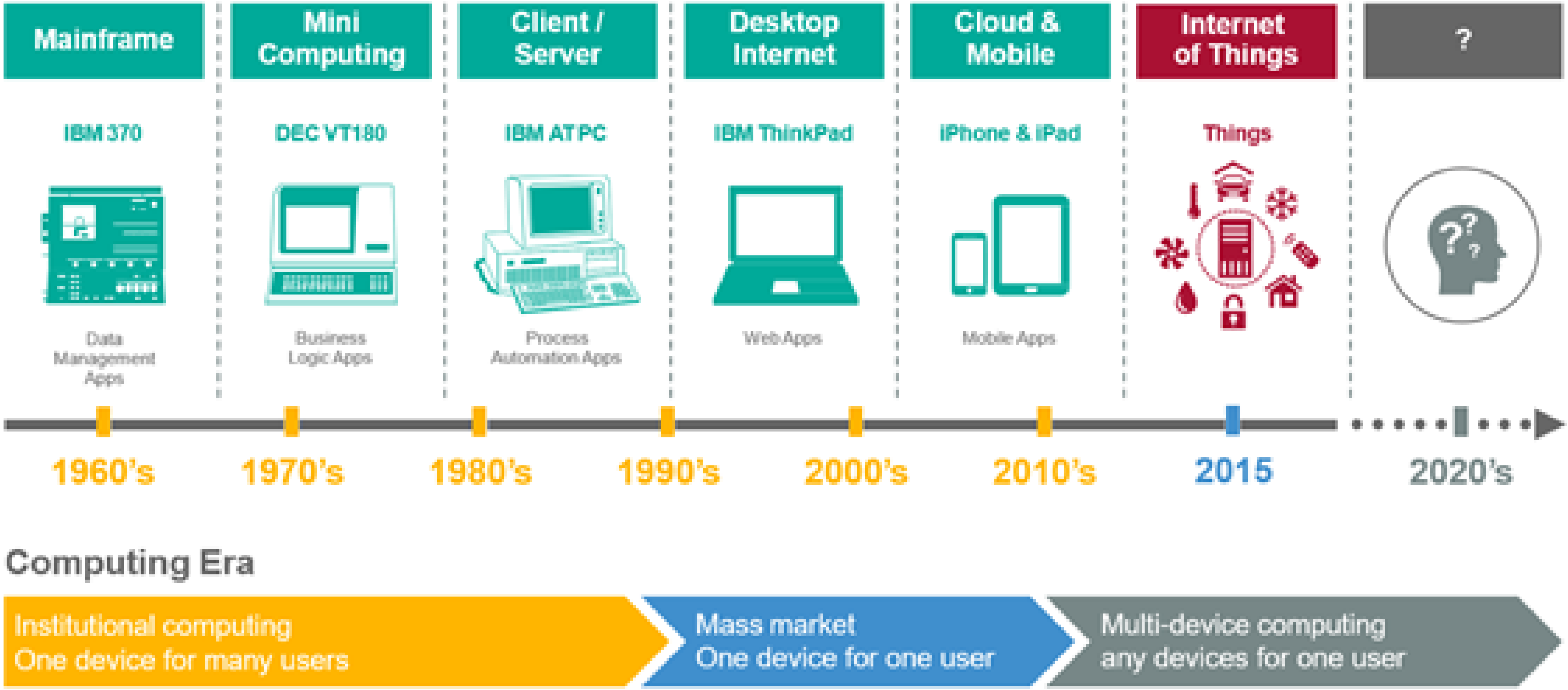
First Wearable Computer

- *American mathematician Edward O. Thorpe, together with mathematician Claude Shannon invented the world's first wearable computer. The cigarette pack-sized device was made to predict the motion of roulette wheels.*

One History of the Edge & IoT

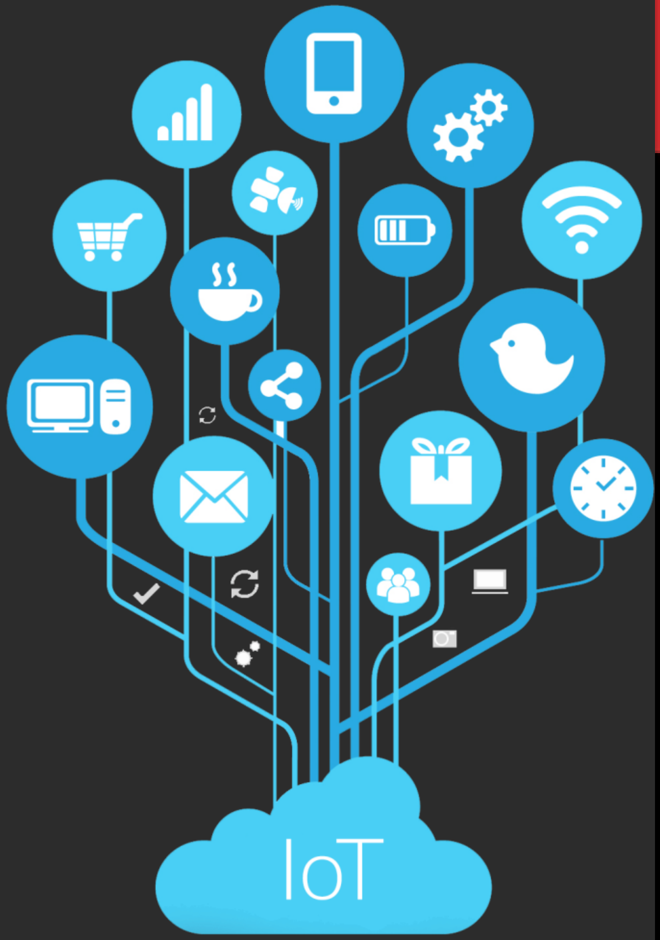
- 1982- The concept of a network of smart edge devices was discussed
- 1997- “Edge Computing & IoT’ is the seventh in the series of ITU Internet Reports originally launched under the title “Challenges to the Network”
- 1999- Auto-ID Center founded at MIT- Keven Ashton
- 2003- EPC Global founded at MIT
- 2005- Four important technologies of Edge & IoT were proposed in WSIS conference
- 2008- First international conference of Edge & IoT held in Zurich
- 2013 – Edge Computing & IoT added to the dictionary

Edge & IoT is the Next Era in Computing

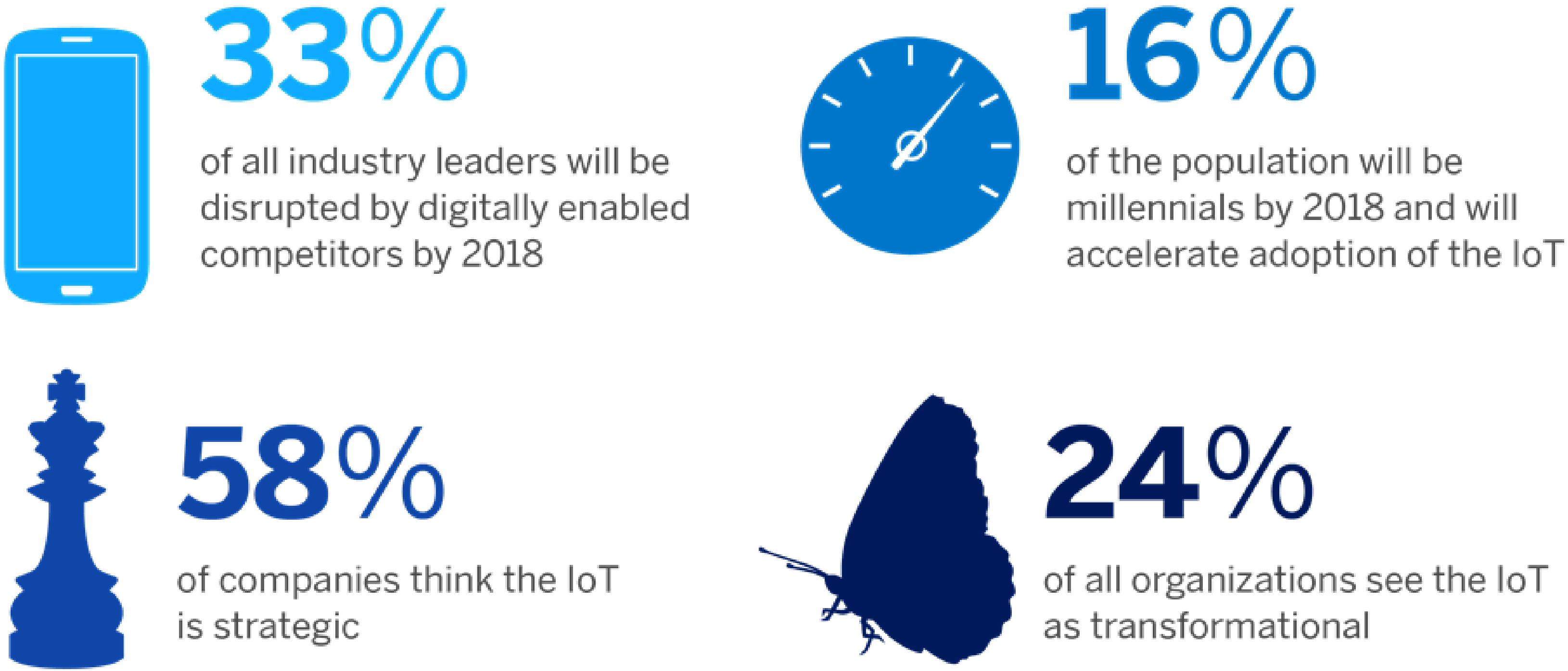


Why implement Edge & IoT?

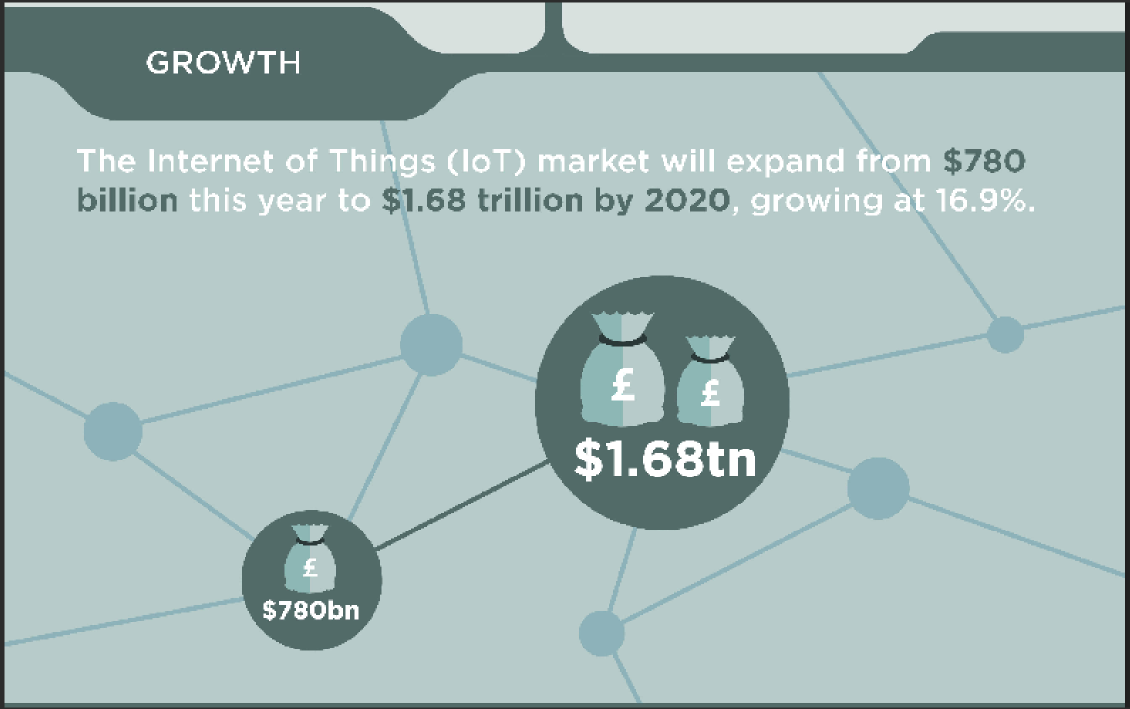
- Edge & IoT is focused on increasing efficiency and creating new profits through connectivity
- With integration of Edge & IoT, there will be economic benefits, efficiency improvements, and less human intervention
- Edge & IoT allows for opportunities and connections that are not even fully understood currently



How important is the Edge & IoT to your company?



Source: IDC 2016



Predicting Growth of the Edge Computing & IoT

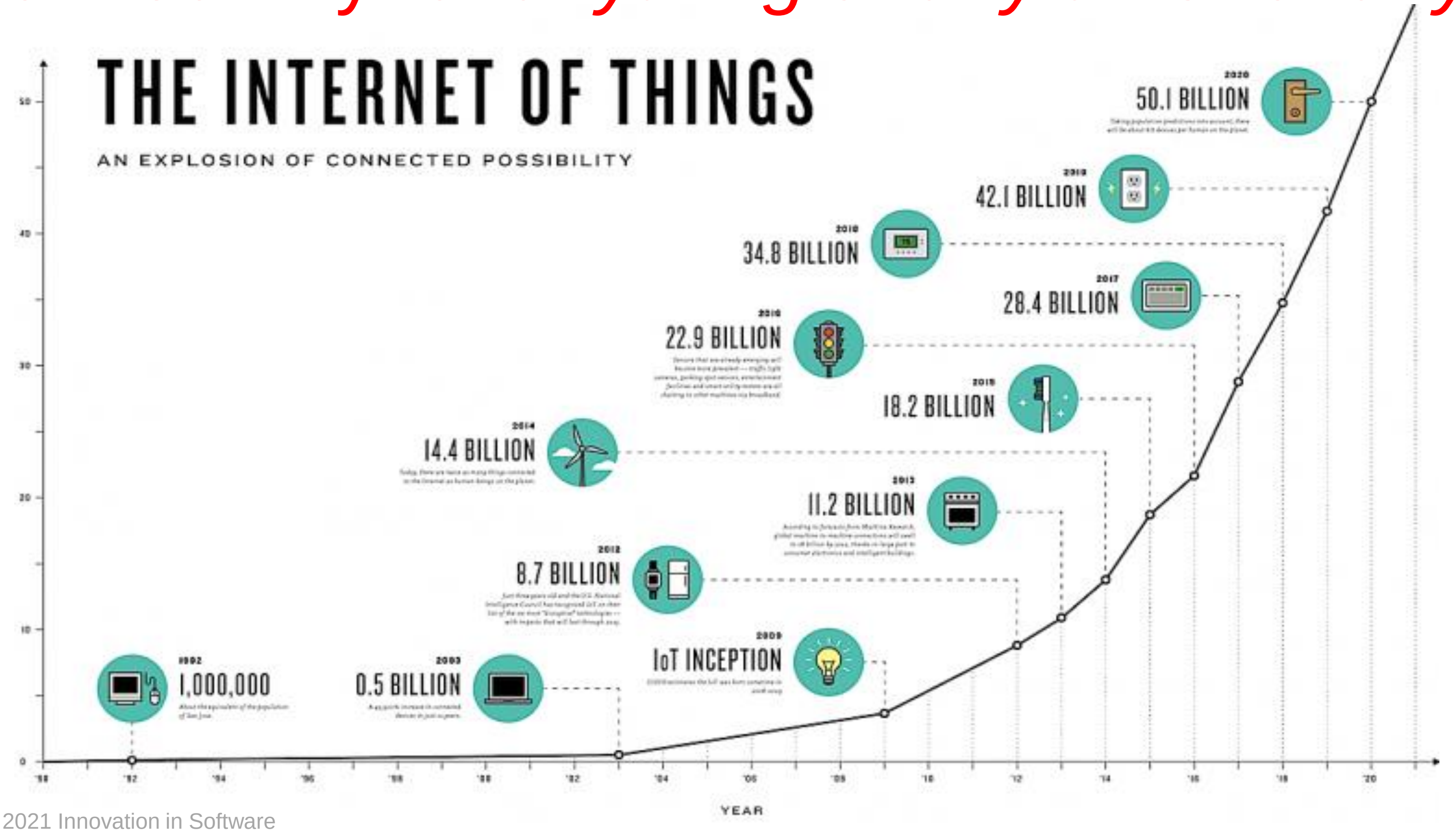
Further importance of Edge & IoT

- “.. the Edge & IoT enables a myriad of applications ranging from the micro to the macro, and from the trivial to the critical.” -Brendan O’Brien

Impact of Edge & IoT:

Complete integration of all sources of information

Connectivity for *anything* at *any time* for *anyone*



Edge & IoT is changing our world

- Edge & IoT is creating a quantifiable and measurable world
- More timely and well-informed decisions can be made due to the wealth of connectedness
- Edge & IoT creates a forever-sensing environment responding to our needs and wants
- Convenience, comfort, health, and safety will all improve

Smart City Evolution


Smart City technology investment
will total $108 billion by 2020.
Pike Research

Smart City Edge & IoT Focus Areas

- Smart Parking
- Structural health
- Noise Urban Maps
- Smartphone Detection
- Electromagnetic Fields
- Traffic Congestion
- Smart Lighting
- Waste Management
- Smart Roads

Edge & IoT Analytics

Volume

Variety

Velocity

Big Data

Edge & IoT will serve as a remedy for any issue by using descriptive, diagnostic, predictive, and prescriptive analytics

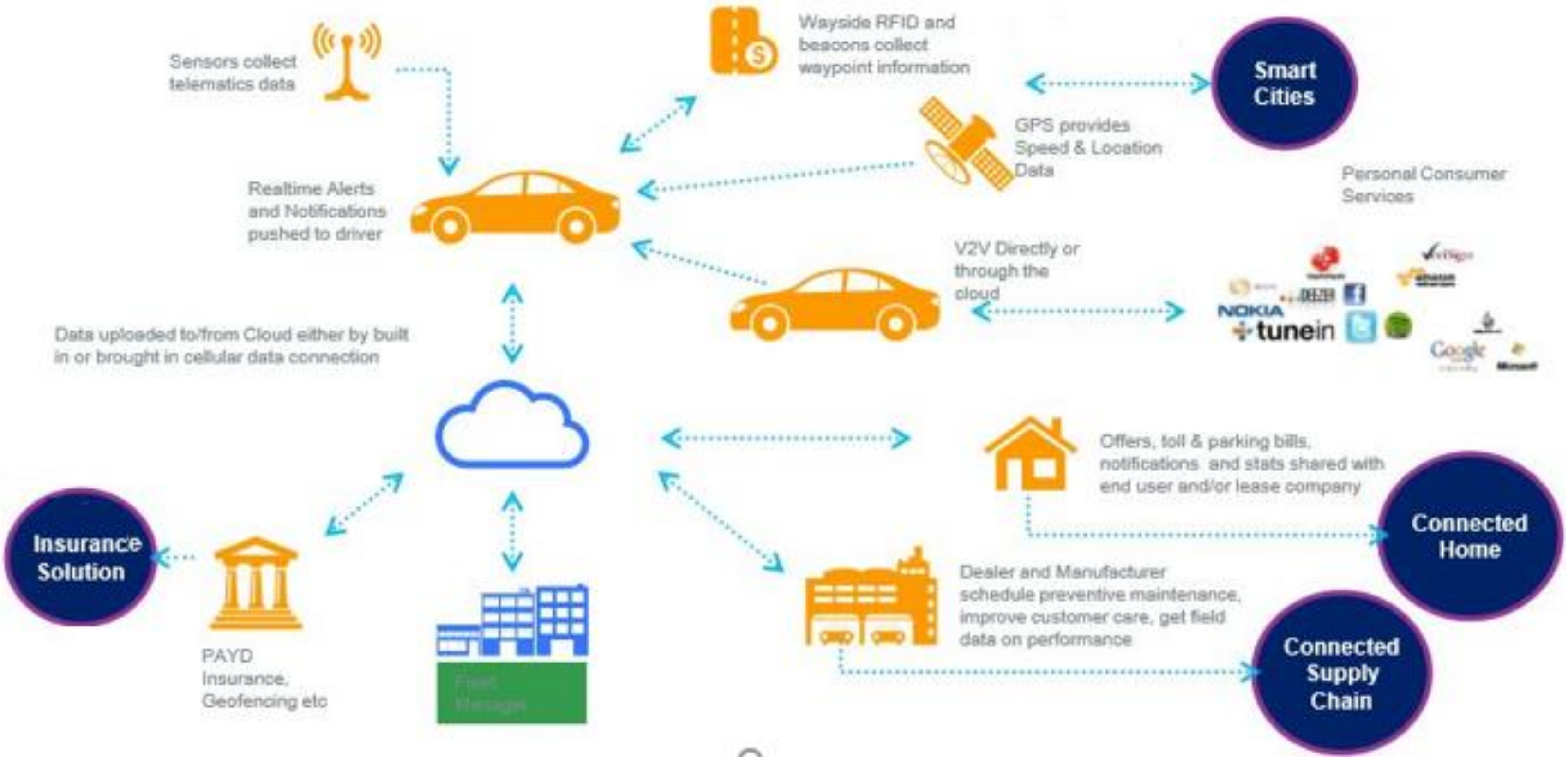
Organizations will organize and collect data from sensors put on equipment for manufacturing, medical supplies, transportation, etc.

Data integration will follow Big Data collection

Enterprise Data and the Digital Data Supply Chain (DDSC)

- Data shared by all users in an organization across departments and regions
- Enterprise data strategy is the comprehensive vision and road map for an organization's potential to harness data-dependent capabilities.
- It includes master data management, business intelligence, big data, etc.
- Focused on the creation of accurate, consistent, and transparent content

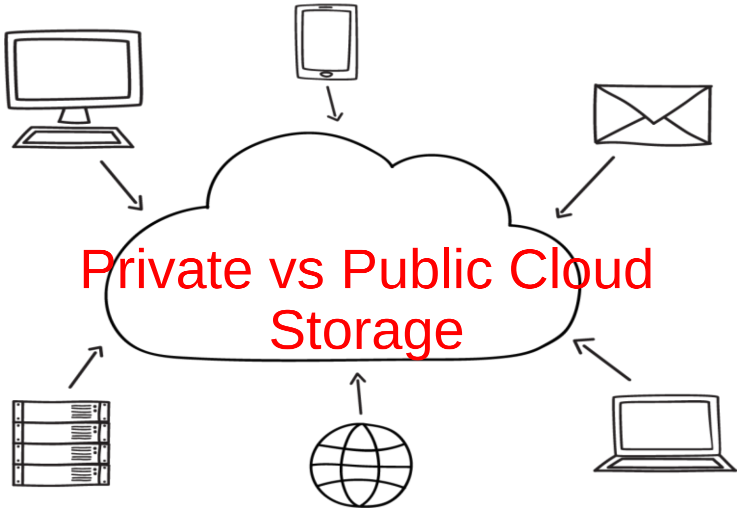
Business Case: Who pays? Who owns the data? Who benefits?



Marketing Automation

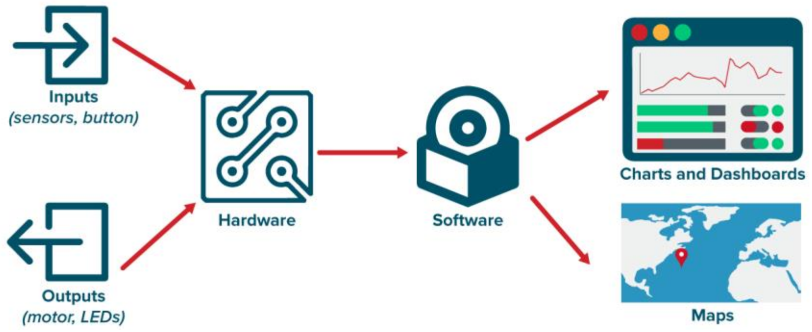
- An in-depth integrated marketing approach looking at benefits, success factors, and evolutions
- 4 components: strategy, practice, evolutions, and vendors
- An increased number of channels and touchpoints are added constantly, which add to connectivity of Edge & IoT
- Link to content management and other platforms

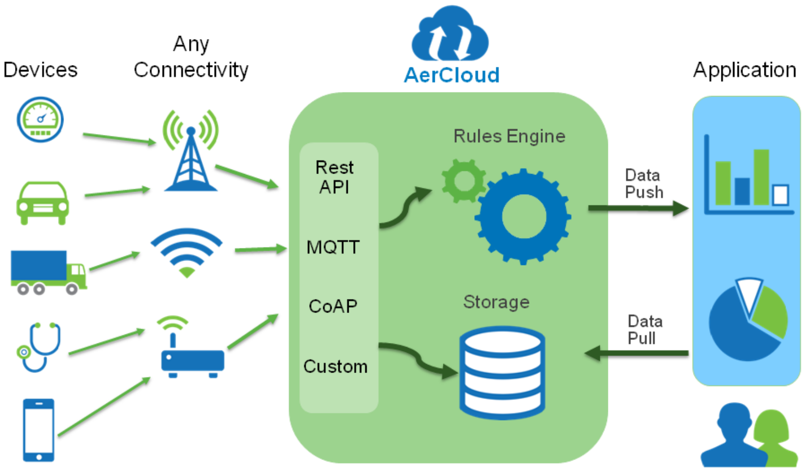
- **Private** cloud storage is a data center for a single business to host and manage data internally
- It is not shared by any other companies and is located on-site
- Preferred option for many big businesses



- **Public** clouds are owned by a cloud service provider (CSP) who is responsible for hosting, managing, and maintaining the network
- They are cost-effective, scalable, and provide access to the newest technologies
- A good choice for small businesses

High rate sensor data

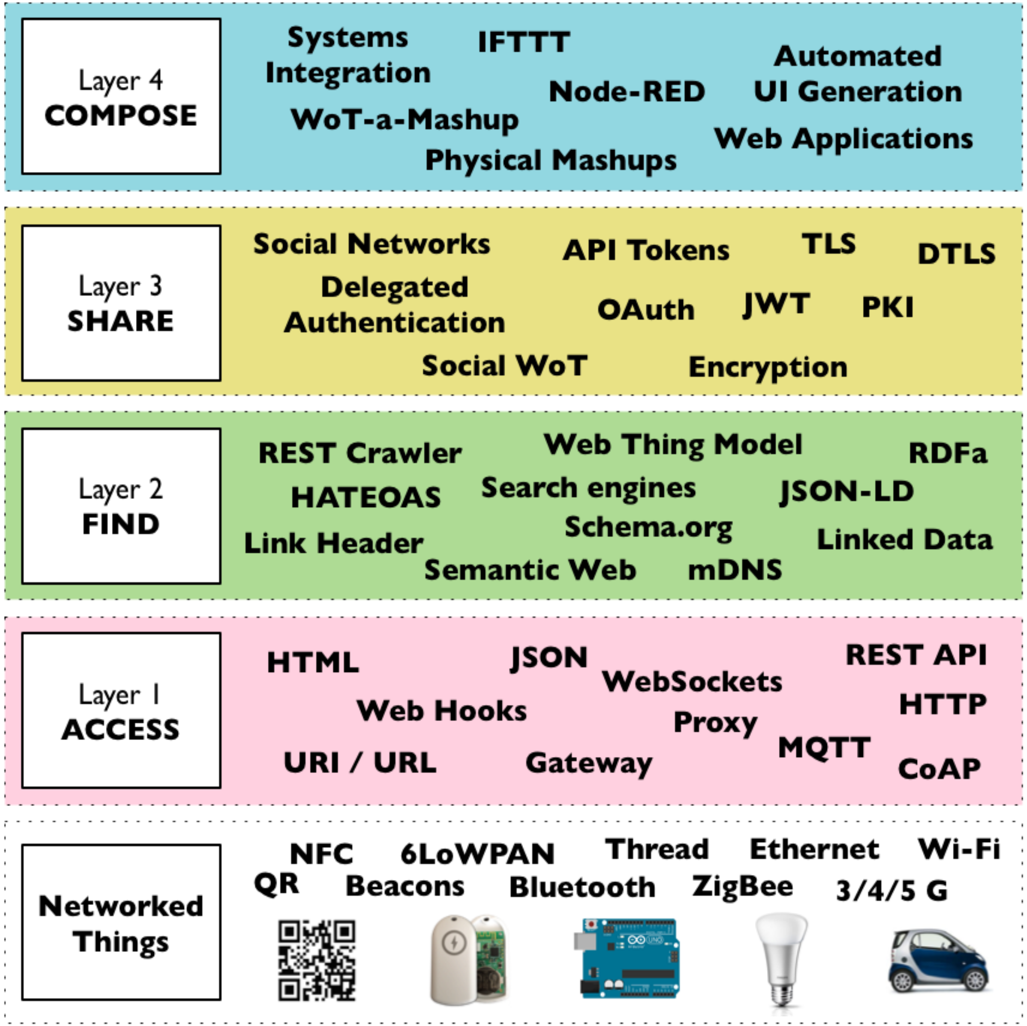




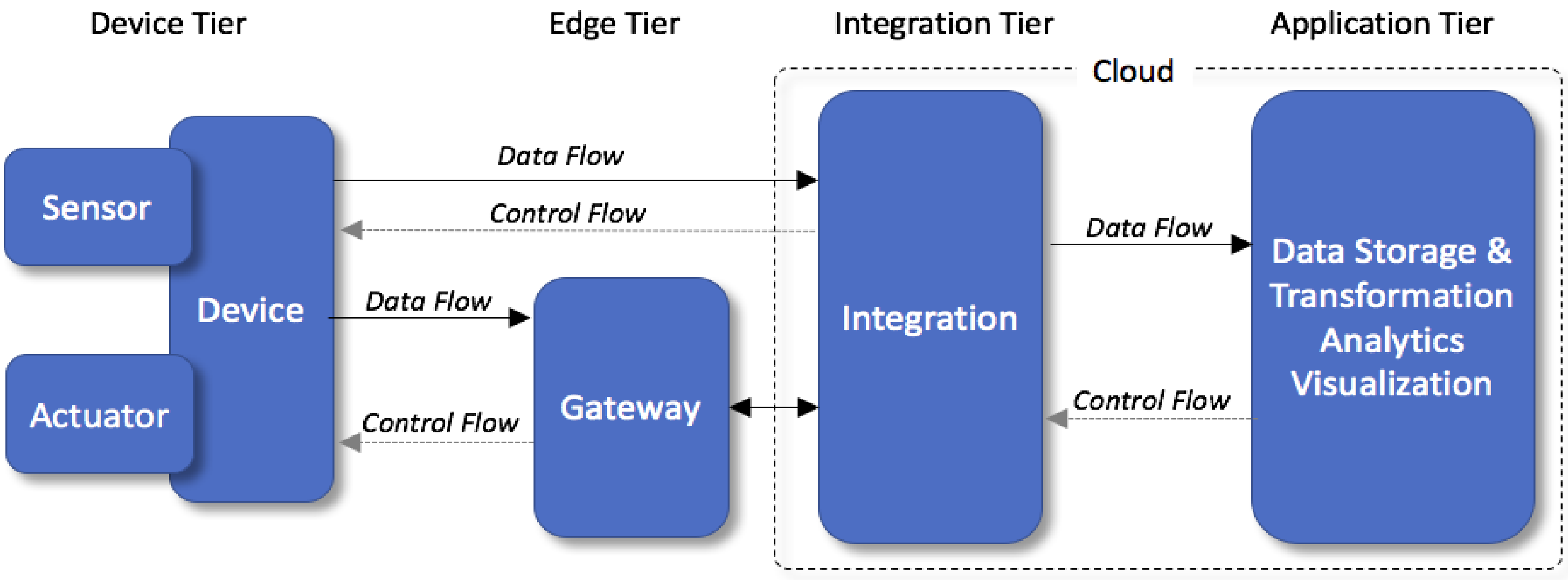
- A sensor network's data streams present, complex issues related to data quality
- Sensor networks generate multidimensional data streams each
- Distributed data storage is a computer network where data is stored on more than one node
- Sensor data is semi-structured and is used as a data exchange format on the web
- Data ingestion is the process of acquiring and importing data into a database
- Data must be processed efficiently through proper planning, expertise, and confidence

Web of Things

- WoT architecture structures the galaxy of Web protocols and tools into a useful framework for connecting any device or object to the Web
- Composed of levels to add extra functionality and integration to each layer

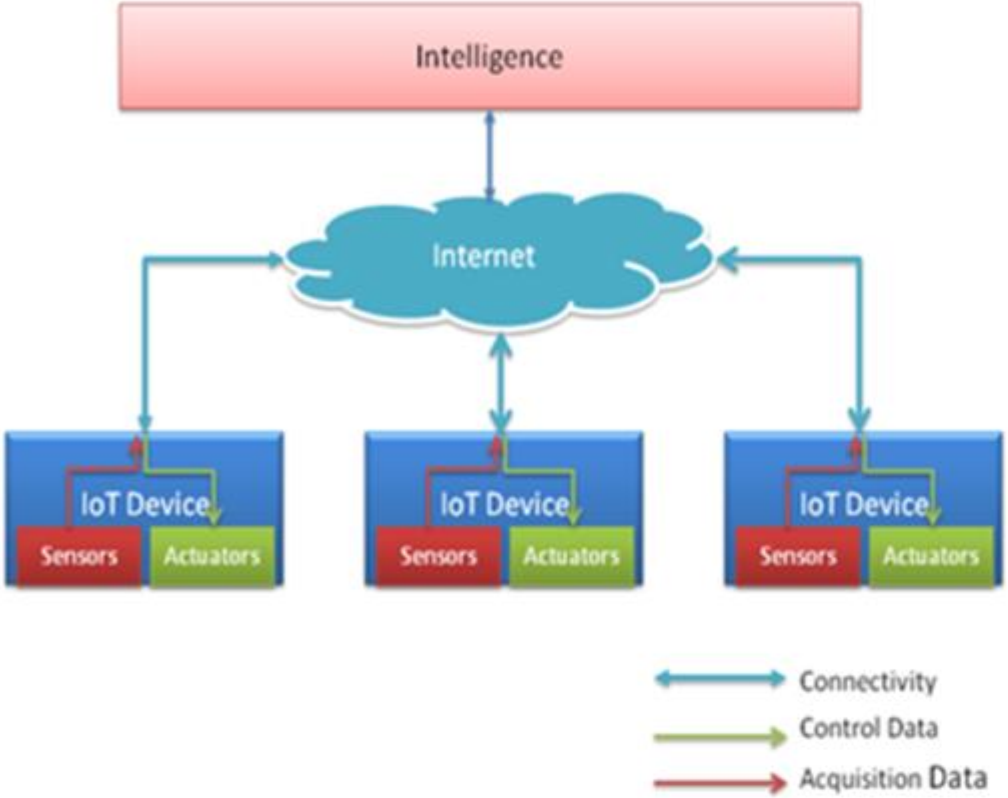


Edge & IoT Architecture



- **Physical devices:** The “things” in the Edge & IoT
- **The gateway:** An edge component to connect resource-constrained devices
- **Integration:** An enterprise service bus and message broker
- **Applications:** Data processing and analytics

Edge & IoT Architecture



Edge & IoT Communication Architectures

- Device-to-device
- 2 or more Edge & IoT devices communicate directly with each other, without an intermediary used in traditional devices.

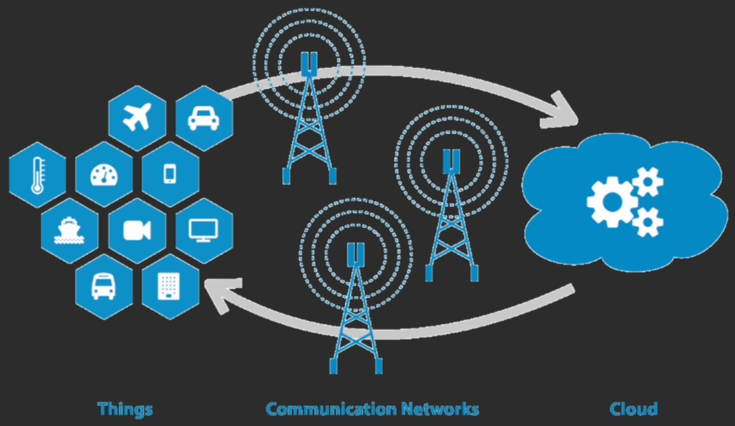
Device-to-cloud

- An Edge & IoT device directly communicates with an application server in the Internet (cloud) and exchanges messages like device status and control commands.

Device-to-gateway

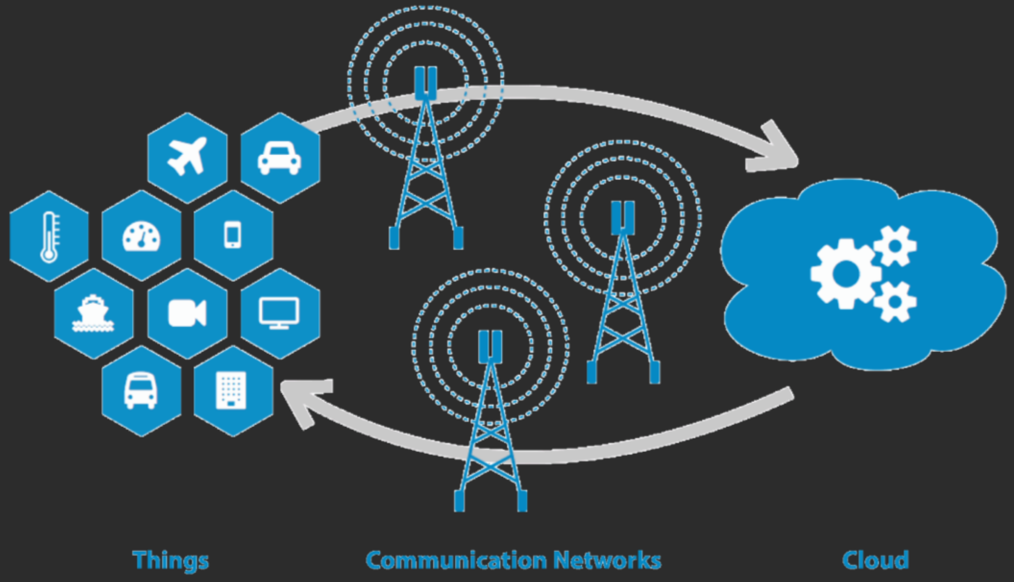
- An application layer gateway (ALG) is used, which is a computer system with 2 or more network interfaces. In this model, Edge & IoT devices are directly connected to an ALG that mediates between the Edge & IoT devices and an application server in the cloud.

Device 2 Device (D2D)



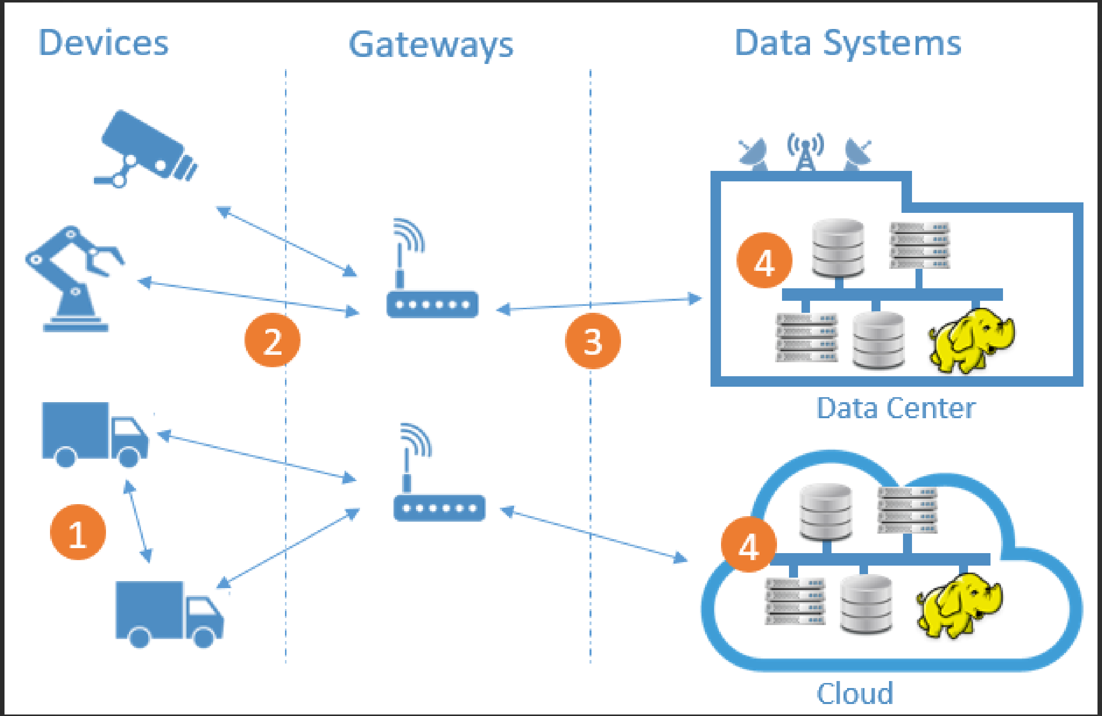
- Devices communicate with each other autonomously without any centralized control and collaborate to gather, share, and forward information.
- Ultimately, the quality of the information gathered depends on how smart the devices are.

Device 2 Cloud



- Direct communication with cloud is the most crucial component
- Edge & IoT cloud platforms are used in application development, device and system management, research, visualization, analysis, monitoring, etc.

Device 2 Gateway (Edge & IoT-GW)



- Direct communication with gateway is the most crucial component
- Edge & IoT gateways are used as waypoints to Public, Private and Hybrid data management, analysis and visualization platforms

Edge Security Risks

Security

Privacy

Authenticity

- With greater connectivity, comes an increase risk of hackers and cyber criminals to sensitive information
- Vulnerability to hacking
- Are devices truly secure?
- Increase of entry points for hackers
- Unwanted public profile leading to employment decisions
- Consumer confidence
- Company confidence and readiness
- Medical privacy concerns

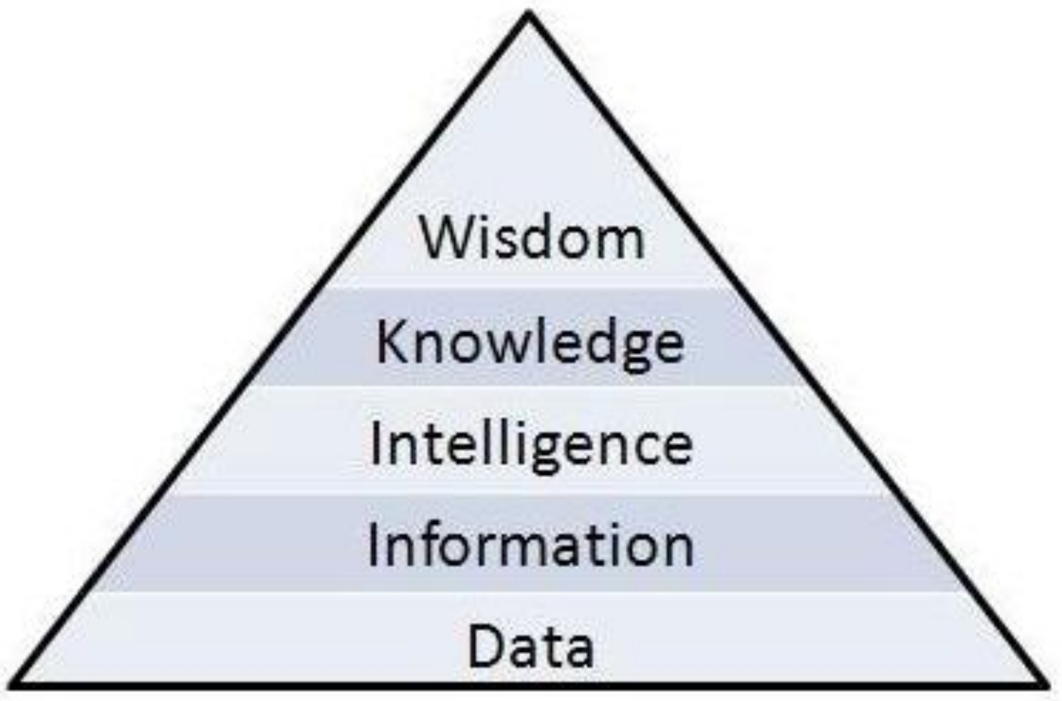
Security Concerns

- Security is the #1 customer concert w.r.t Edge & IoT
- Critical need to secure E2E lifecycle e.g. Data at rest and in motion
- Malware can impact device activity and service levels
- Significant risk to reputation and revenue e.g. Connected Audi A6 being hacked on the M4, Jeep being taken over on US HWY, Edge & IoT camera hacks, Ukraine power grid takeover
- Perception problem developing, especially in Consumer Edge & IoT, with highly vulnerable Smart Cars and Smart Homes

Opportunities for Edge & IoT

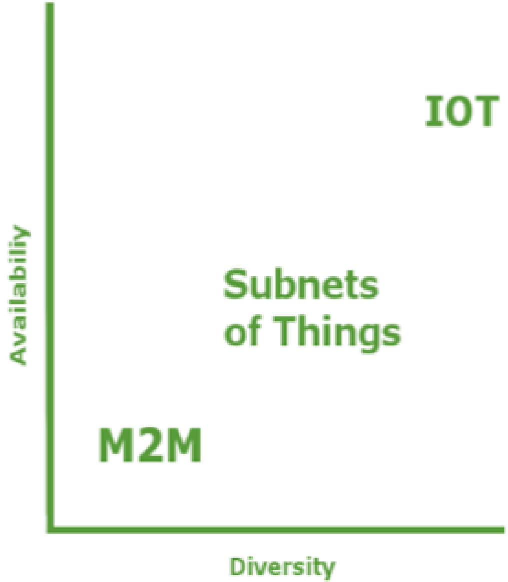
- User visualization
- Combining data streams to create new insights
- Predicting what events will change
- Reduced cost of data collection and storage
- Ease of use
- Finding patterns to turn information into intelligence, wisdom, & insight
- Machine learning and AI can be applied to help extract predictive and prescriptive information

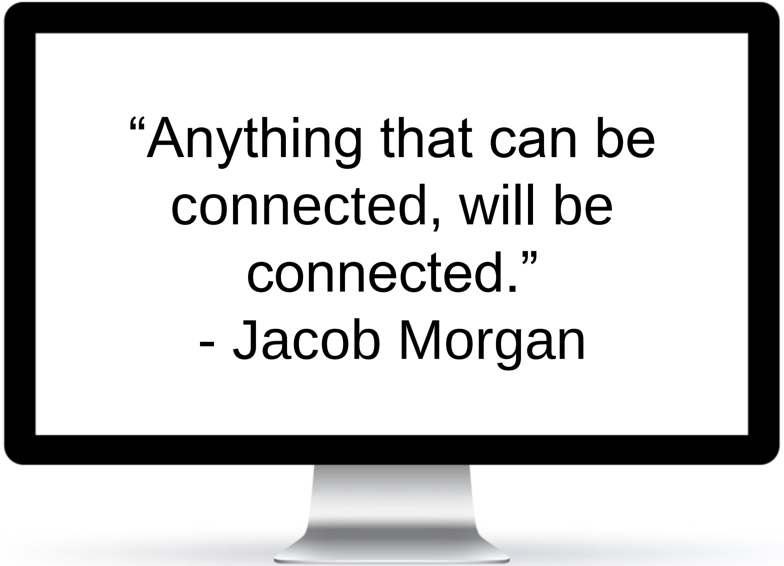
Hierarchy of Edge & IoT Value Stream



Managing Data and the Environment

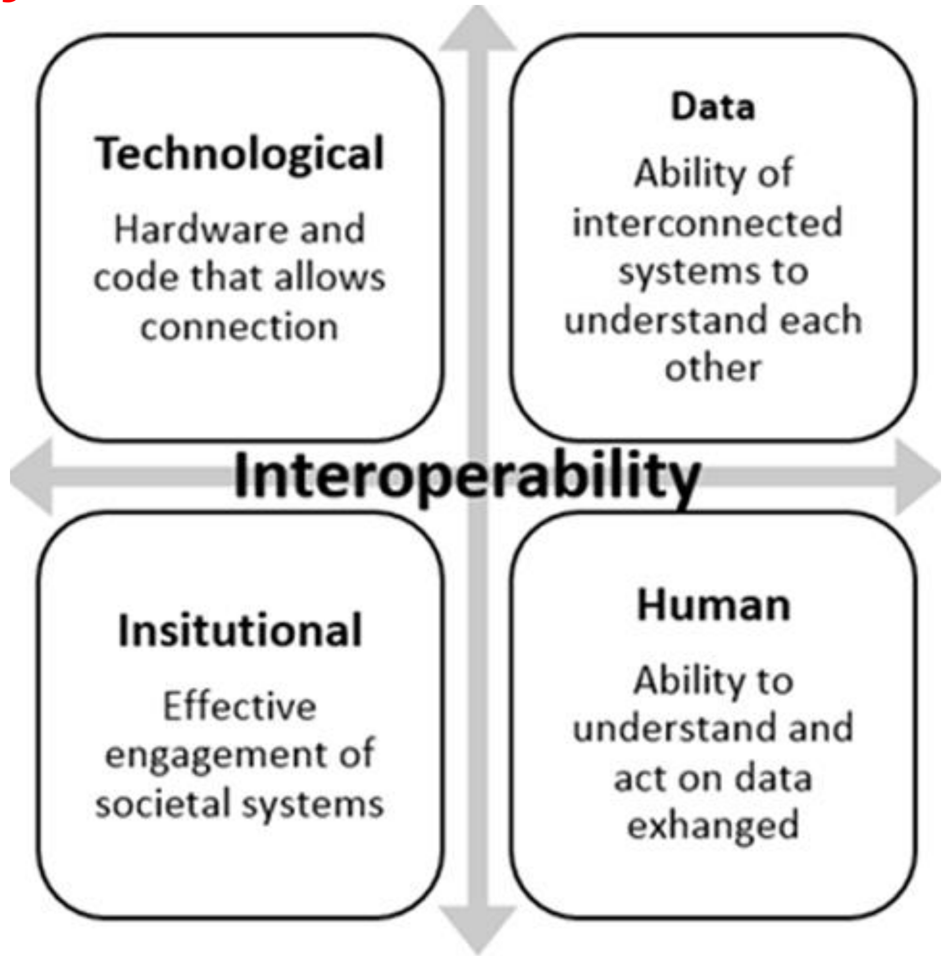
- Machine 2 Machine with built-in sensors
- SoT is a network of devices that converge around one or more central computing units





Edge & IoT is a larger scale than SoT and has higher level of diversity and availability

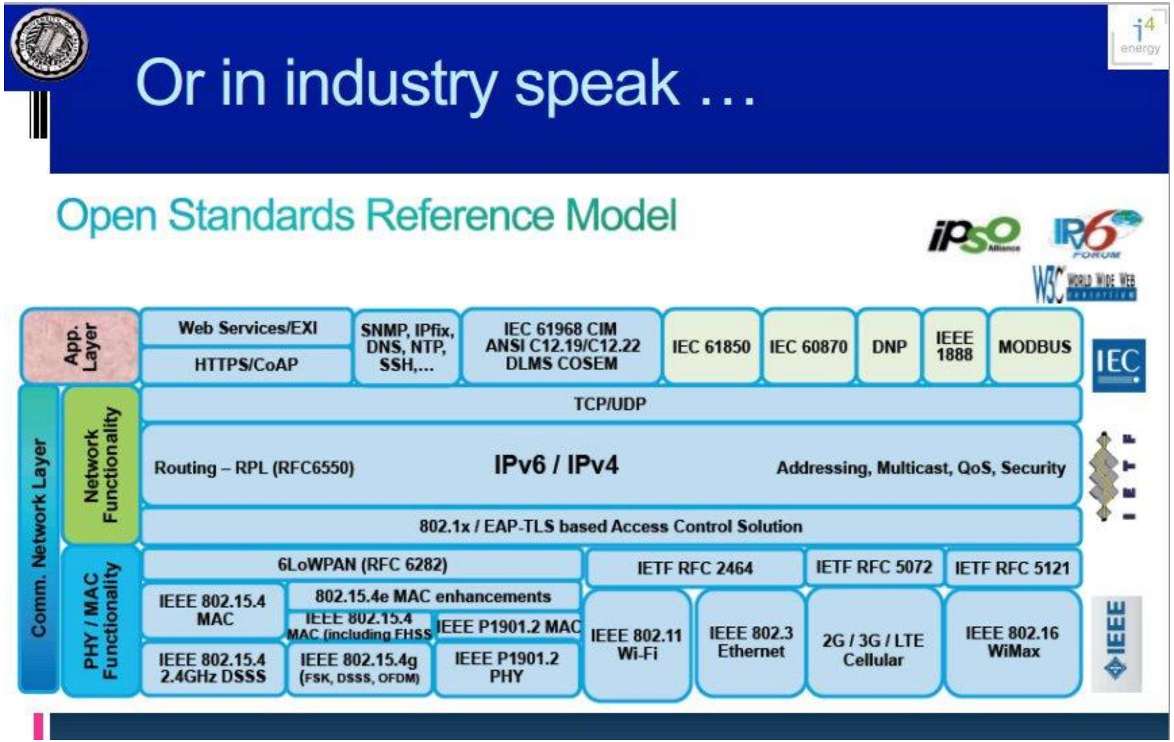
Interoperability



Interoperability

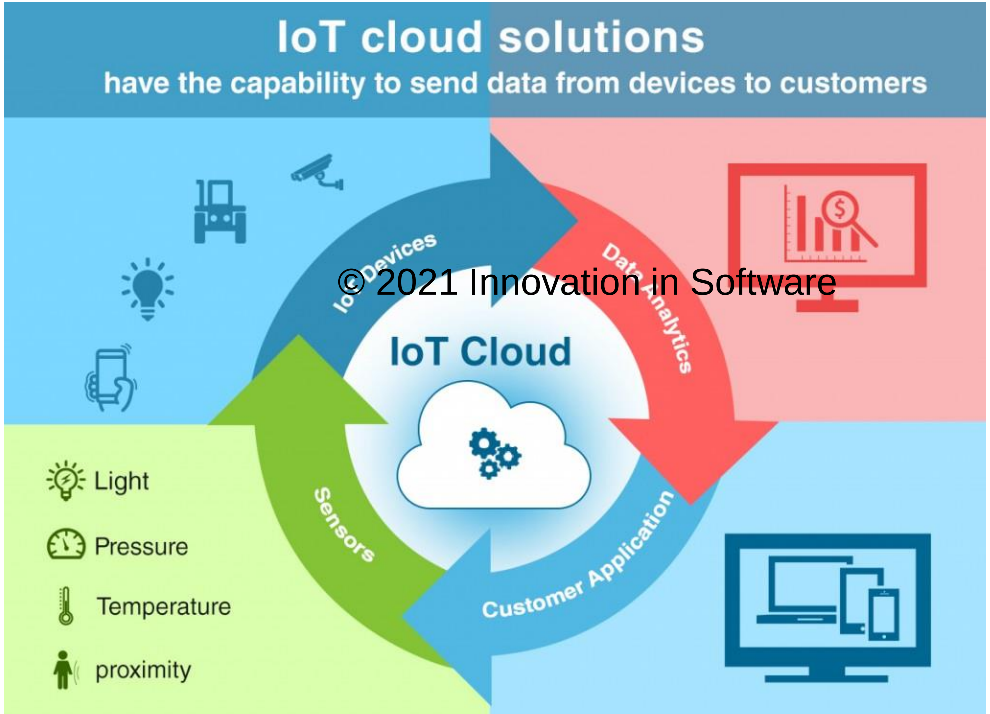
- The extent to which systems and devices can exchange data and interpret shared data
- Interoperability between Edge & IoT systems is critical
- There is high potential for economic value with developing the right systems that optimize and predict anomalies

Industry Standards



- The Open Systems Interconnection (OSI) model
- Ongoing innovation has allowed dropping costs for bandwidth
- New standards have been marked to deliver “high business benefit.”
- Data protocols and device management

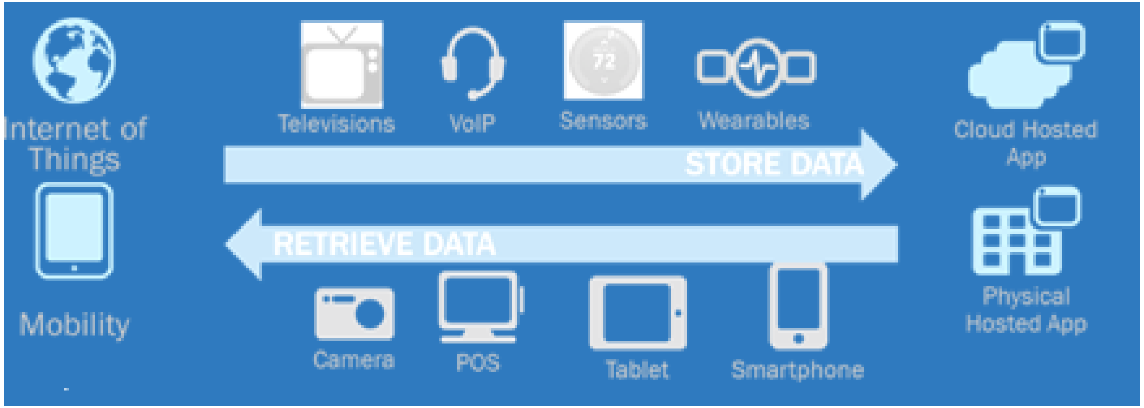
Capabilities



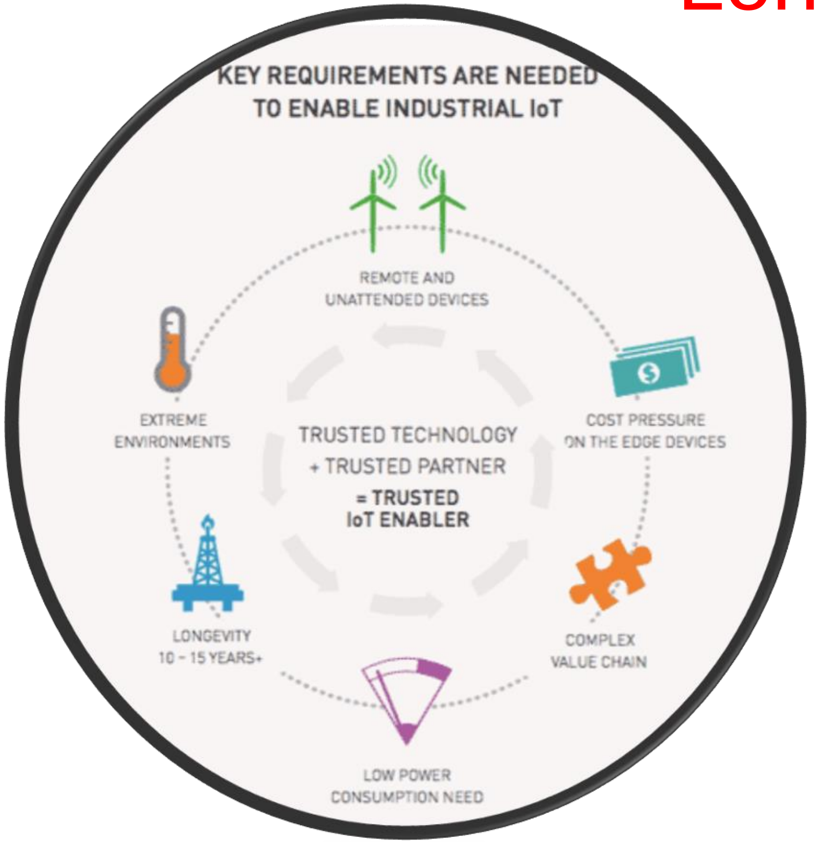
- Solution design
- Analytics
- Security
- Customer service
- Integration

Mobility

- Mobile engagement through mobile messaging, open market sponsored data, mobile loyalty,, and data gifting for a complete mobile experience
- Mobile devices will be seen in a cloud computing environment
- Machine learning applications with support of mobility patterns
- Wearable devices for portability

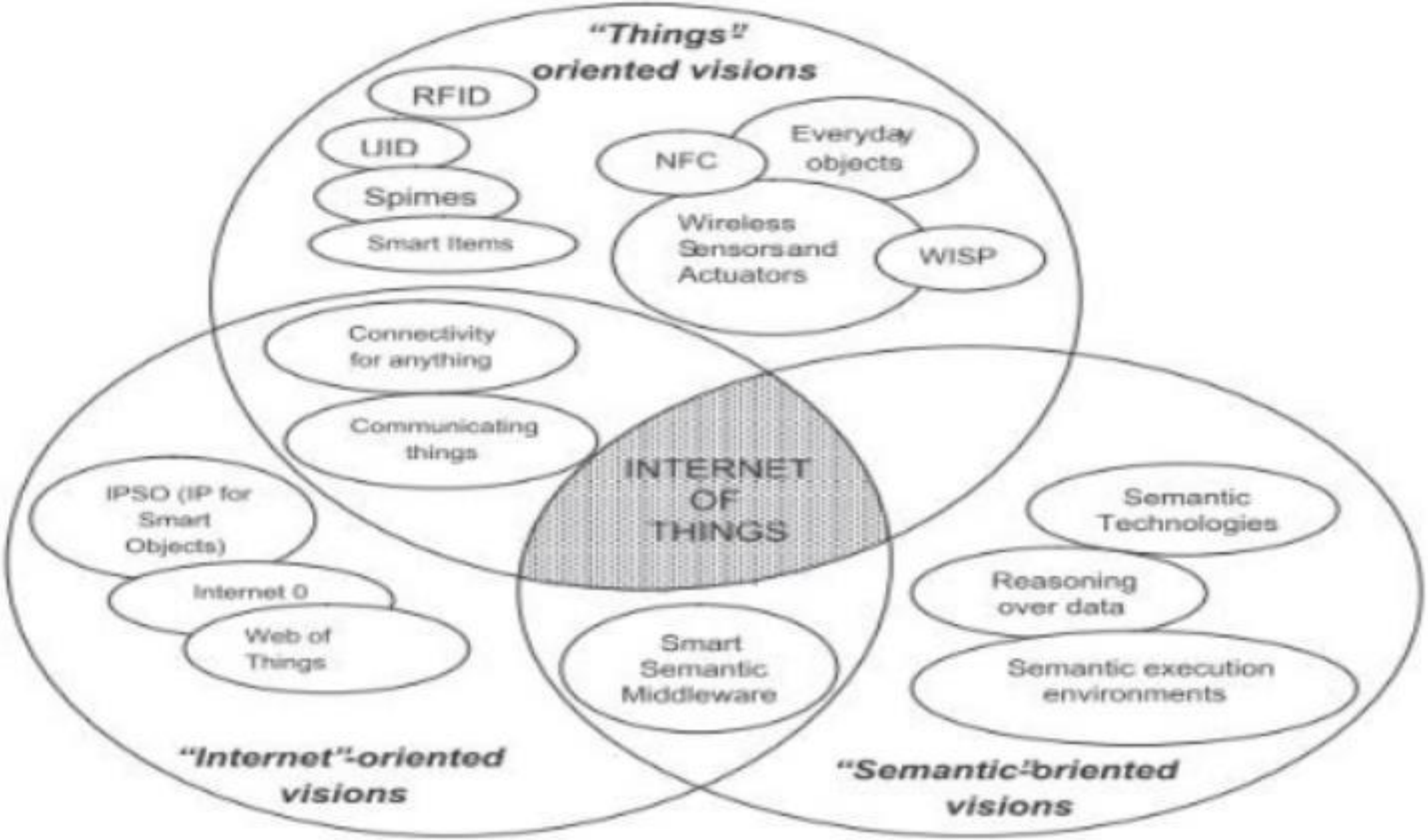


Longevity

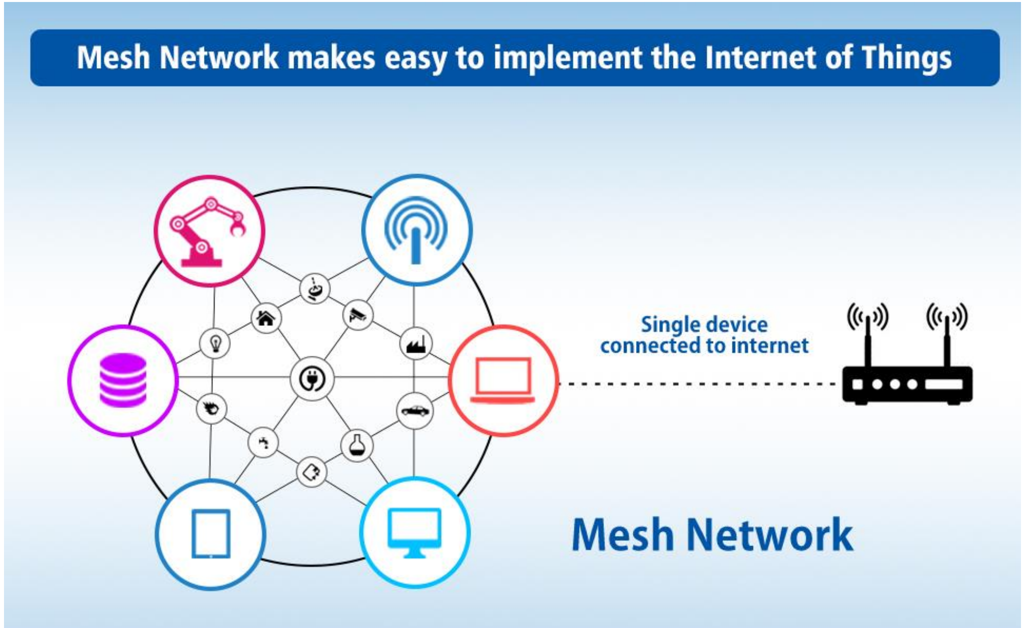


- Longevity is defined as life expectancy, or in terms of technology: a long device life cycle
- For most Edge & IoT applications, the device life cycle is 10-15 years or more
- Once placed, devices supporting infrastructure and enterprise assets need to be left alone to gain the cost efficiencies they offer (example: a windmill)

Edge & IoT Perspective & Visions



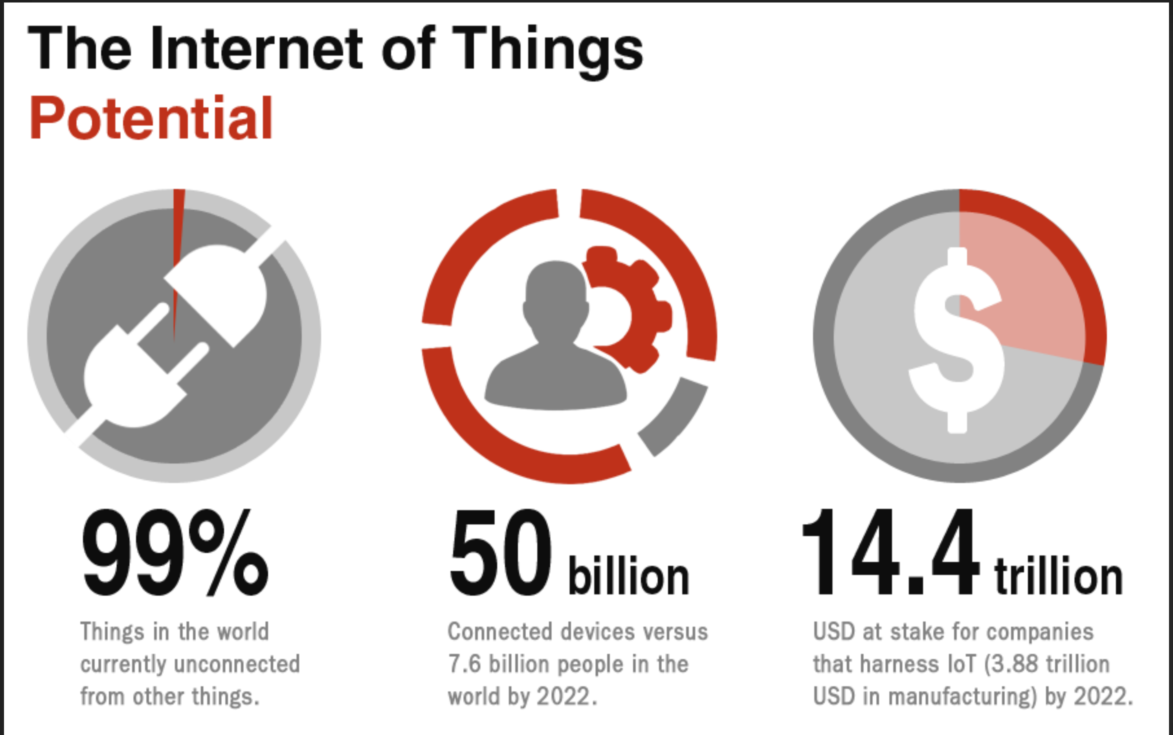
Network of Things (NoT)



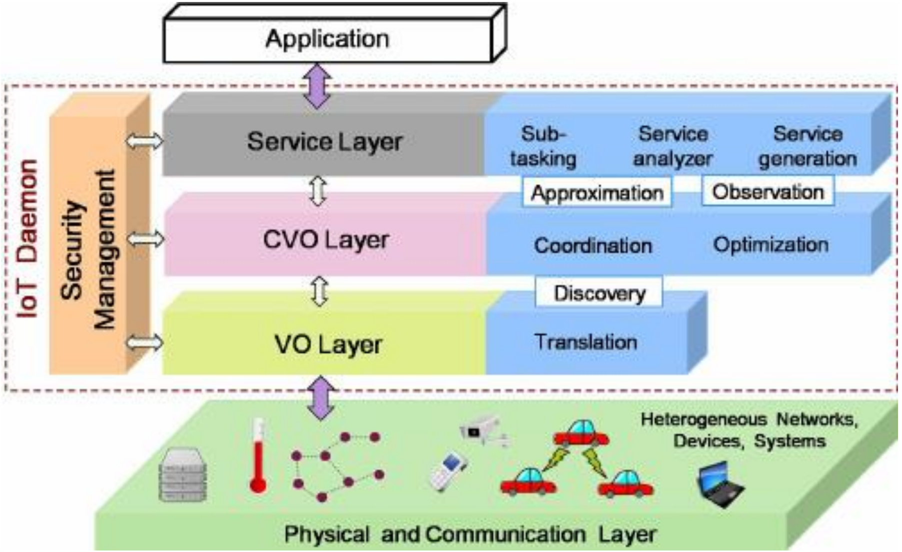
- Networking technologies enable Edge & IoT devices to communicate with other devices and applications
- Transforming an environment into a Network of Things offers operating gains of connectivity
- NoT has many variations

Future of Things

- Smart fitness (fit bits, monitors) and health care
- Programmable homes
- Higher quality data-capture and display capabilities
- Geolocation services and autonomous vehicles
- Inventory management, personalized shopping experiences, self-diagnosing maintenance



System of Things Architecture



Information processing is distributed over computer-based systems rather than one machine

Distributed systems run on an integrated group of cooperating processors linked by a network

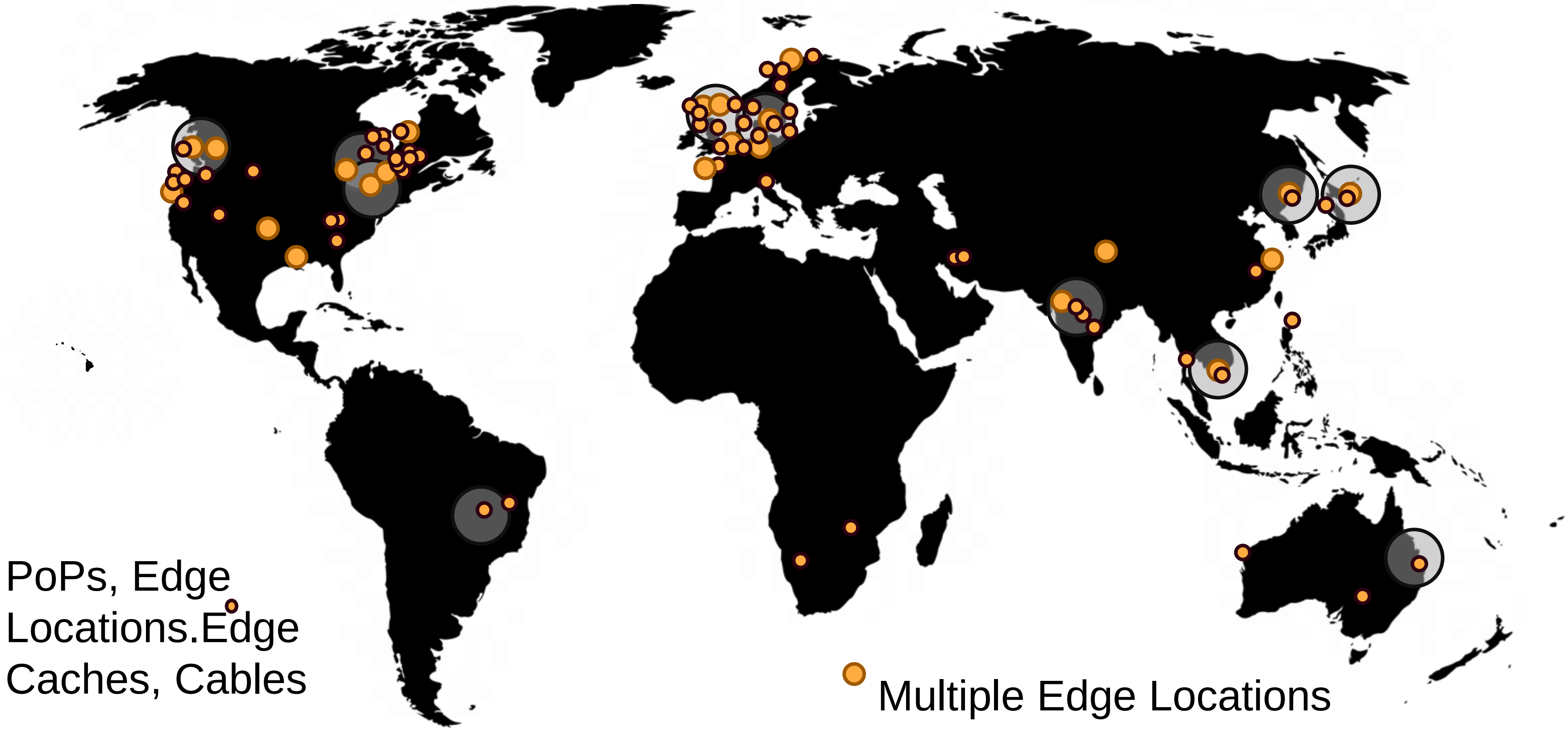
Key characteristics: Resource sharing, openness, scalability, concurrency, performance, reliability

Edge & Content Delivery Network

Content Delivery Network

- Speed up distribution of your static and dynamic web content, such as .html, .css, .js, image files, and streaming video, to your users
- Depending on your CDN architecture/provider, content can be cached all around the world
- Geographic proximity means lower latency and better user experience
- For CSP-hosted CDN, typically only data transfers and requests that you use are charged

Global Edge Network

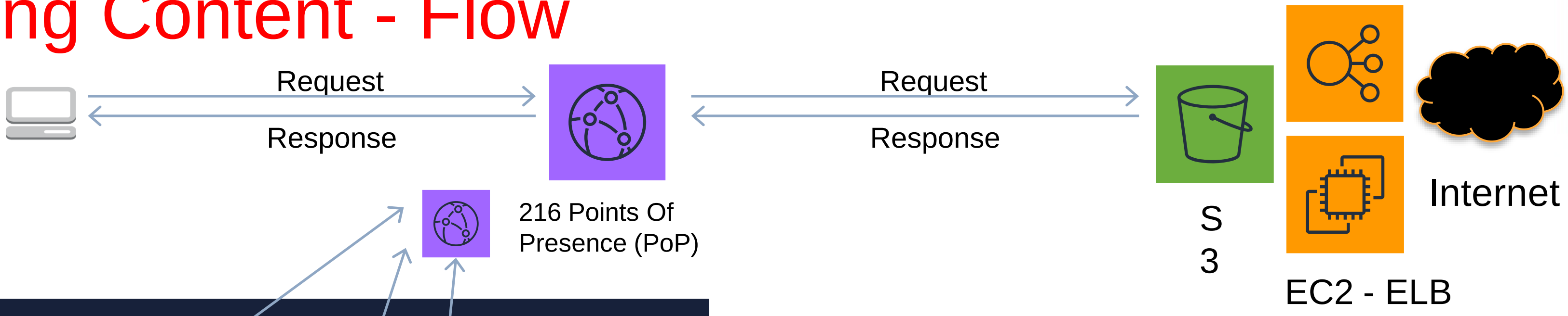


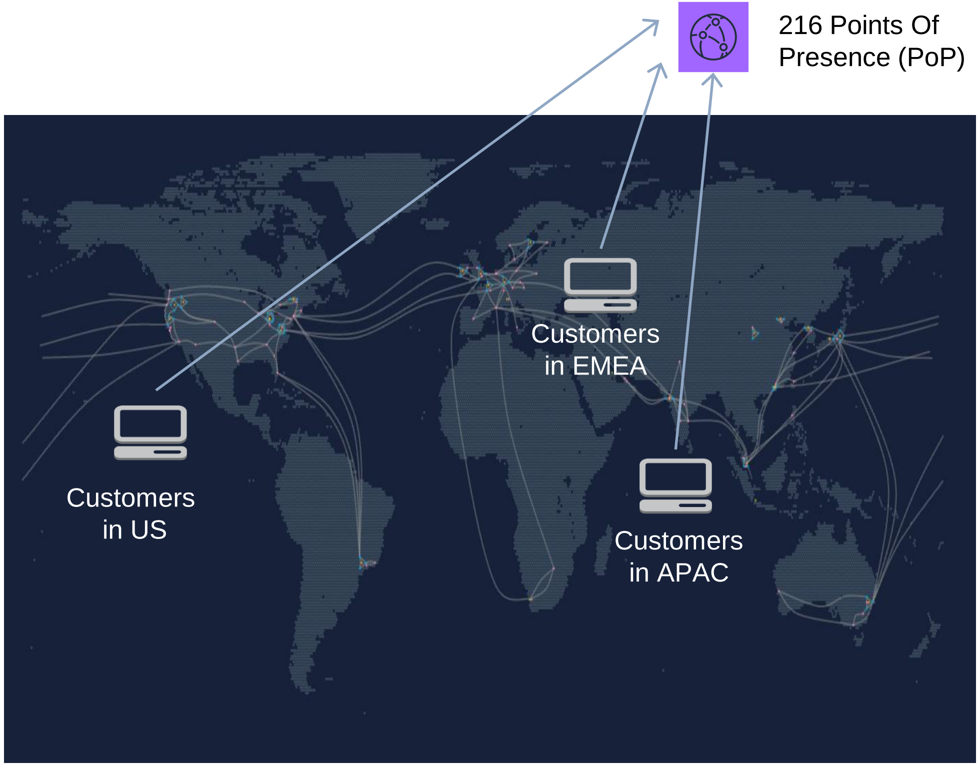
PoPs, Edge Locations.Edge Caches, Cables

Multiple Edge Locations

Edge Locations & Caches

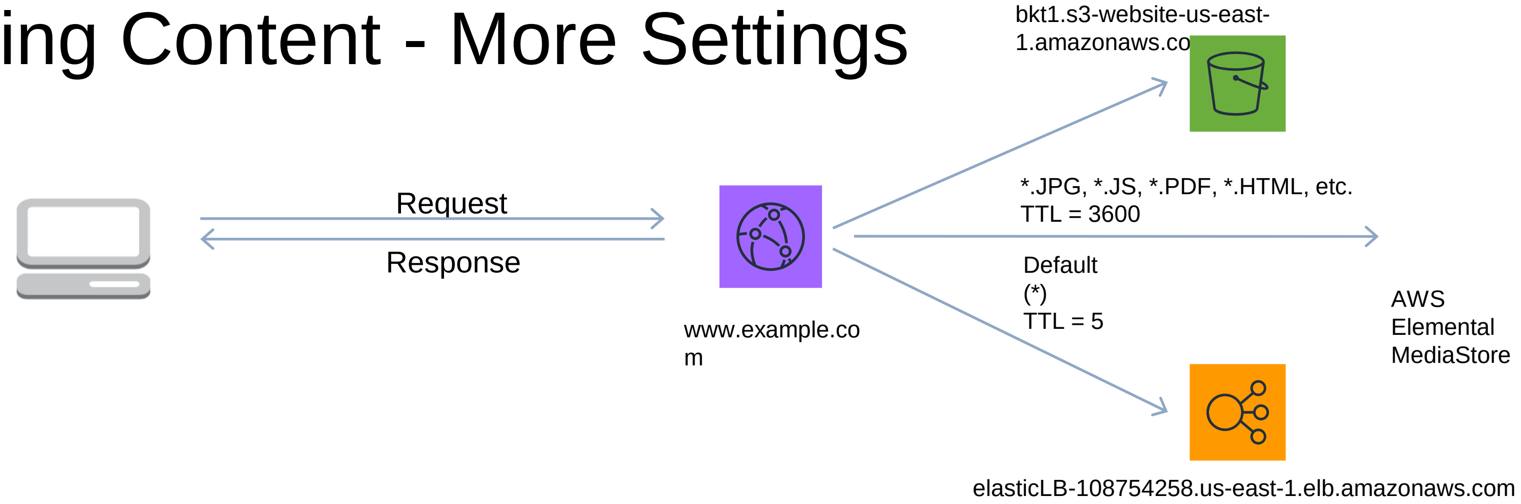
Serving Content - Flow





1. User Access Request to DNS
2. DNS routes the request to the POP
3. In the POP, check cache for the requested files. If in the cache, return to the user. If not :
   - ✓Gather from the origin server for the corresponding file type
   - ✓The origin servers send the files back to the edge location.
   - ✓Stream to user on arrival, store for subsequent

Serving Content - More Settings



- **Origin Servers** contain the static assets, videos, and are the source of truth
- **Viewer Protocol Policy** usually HTTP or HTTPS protocol.
- **Expiration Period** is set on your files (through cache control headers) to determine whether it needs to check the origin for an updated version of the file AKA time-to-live (TTL)
- **Query String** Parameters are often used to return customized content generated by a script running on the origin server.
- **Trusted Signers** create content for distribution

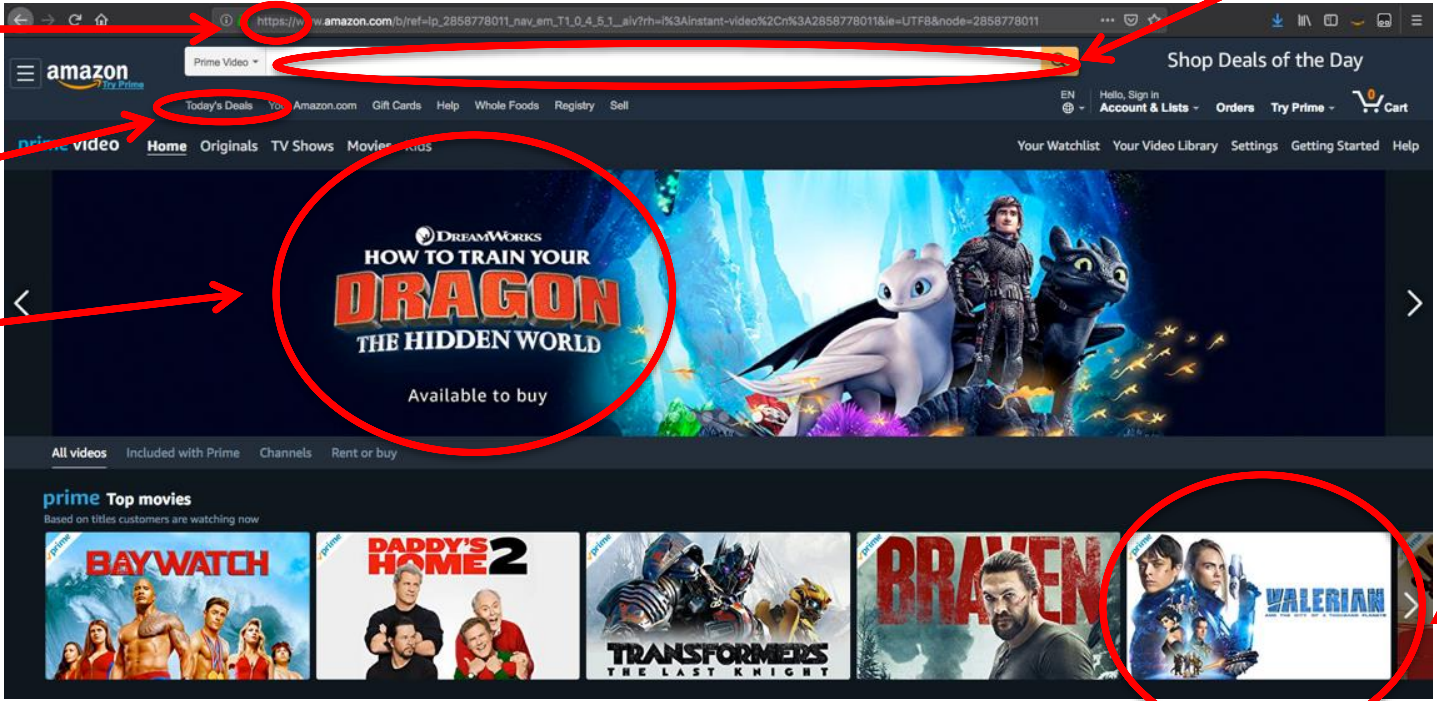
Deliver All of Your Content

User Input

SSL

Dynamic

Static



Video

Key CDN Features

Video Streaming

- Adaptive Bitrate Live & VOD Streaming (HLS, HDS, Smooth.
- MPEG-DASH)
- RTMP (Flash) and HTTP(S) delivery

Security

- Private Content
- Custom SSL Support
- Geo Restriction
- WAF Integration

Content Management

- Access through Dashboard, CLI, and SDKs
- Full control
- Programmatic Invalidation
- Access Logs
- Usage Charts

Dynamic Content Acceleration

Low Content Expiration Periods (TTL=0)
Device Detection
CORS Support
Geo Targeting
Multiple Cache Behaviors
Multiple Origin Servers
Zone Apex Support
Query String & Cookie Support
Put/Post HTTP Verb Support

Price Flexibility

Pay for Use
Price Classes
Reserved Capacity Pricing

Expiring Content

- TTL
  - Fixed period of time
  - Content owner configuration
  - Refreshes at that time without exception
  - Configurable Default TTL and a Maximum time-to-live (Max TTL) to specify how long objects are cached

- Change object name
  - Header-v1.jpg becomes Header-v2.jpg
  - New name forces refresh

- Invalidate object
  - Last resort – very inefficient
  - Wildcard operator make invalidation of multiple objects easier
  - Invalidating cached content is also supported (* per an amount of charge)

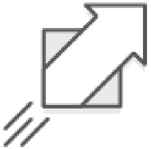
FaaS on the Edge

FaaS on the Edge

AWS Lambda + **Amazon CloudFront** = **Lambda@Edge**

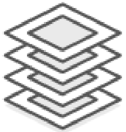
Lambda@Edge

No servers to provision or manage



Scales with usage

Never pay for idle

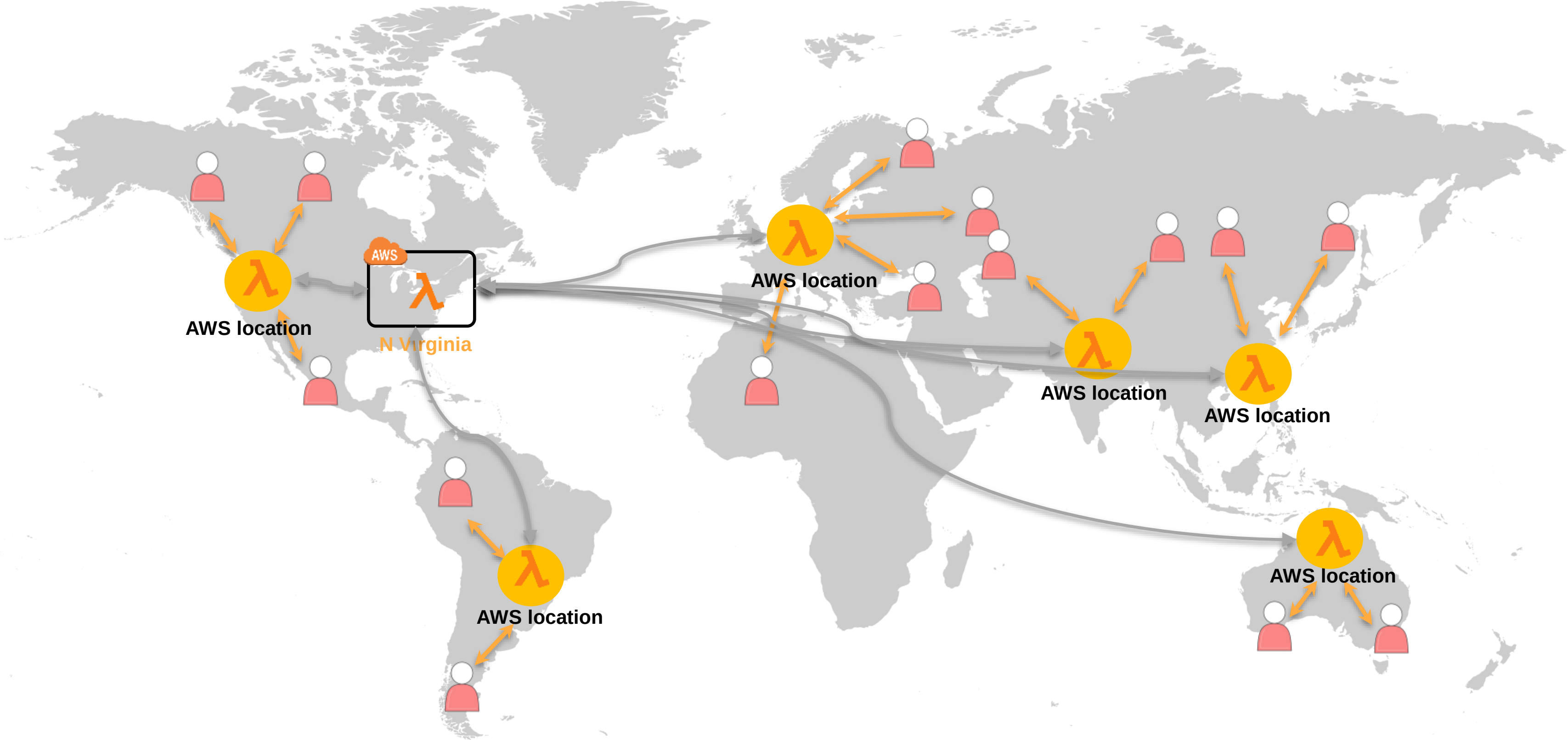


Built-in availability and fault tolerance

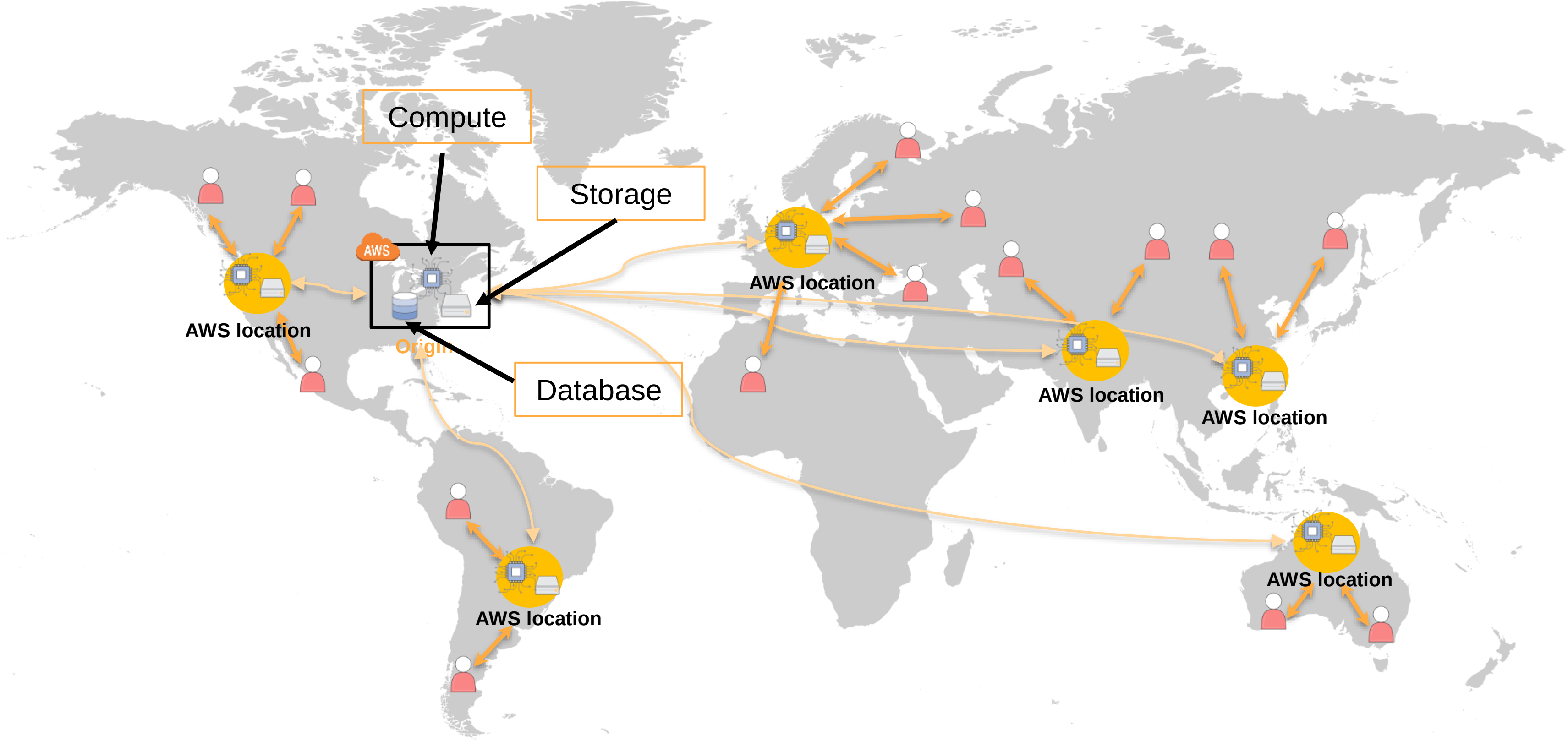
Globally distributed

Bring your own code to the edge to improve the user experience

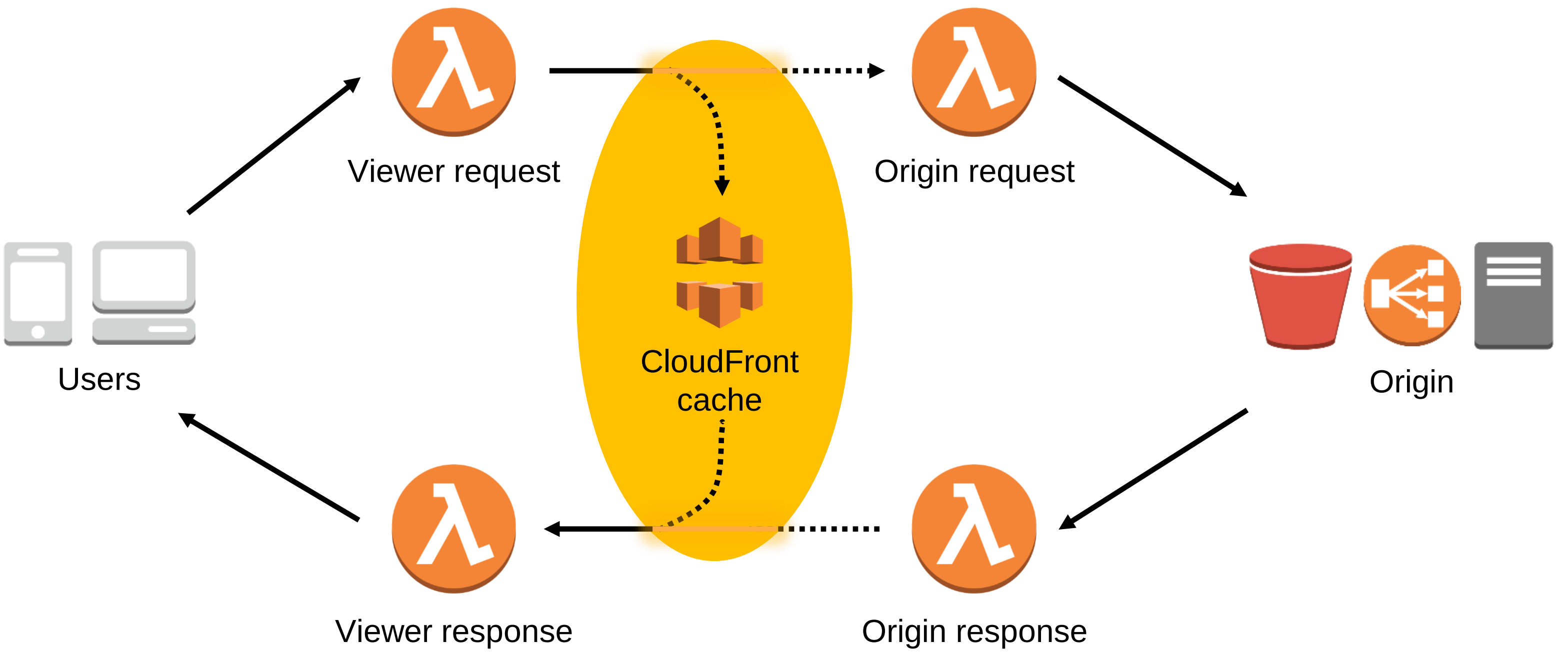
Write once, run FaaS globally



Lambda@Edge


Compute
Storage
Database
AWS
Origin
AWS location
AWS location
AWS location
AWS location
AWS location
AWS location

CloudFront triggers



Lambda@Edge

Response generation

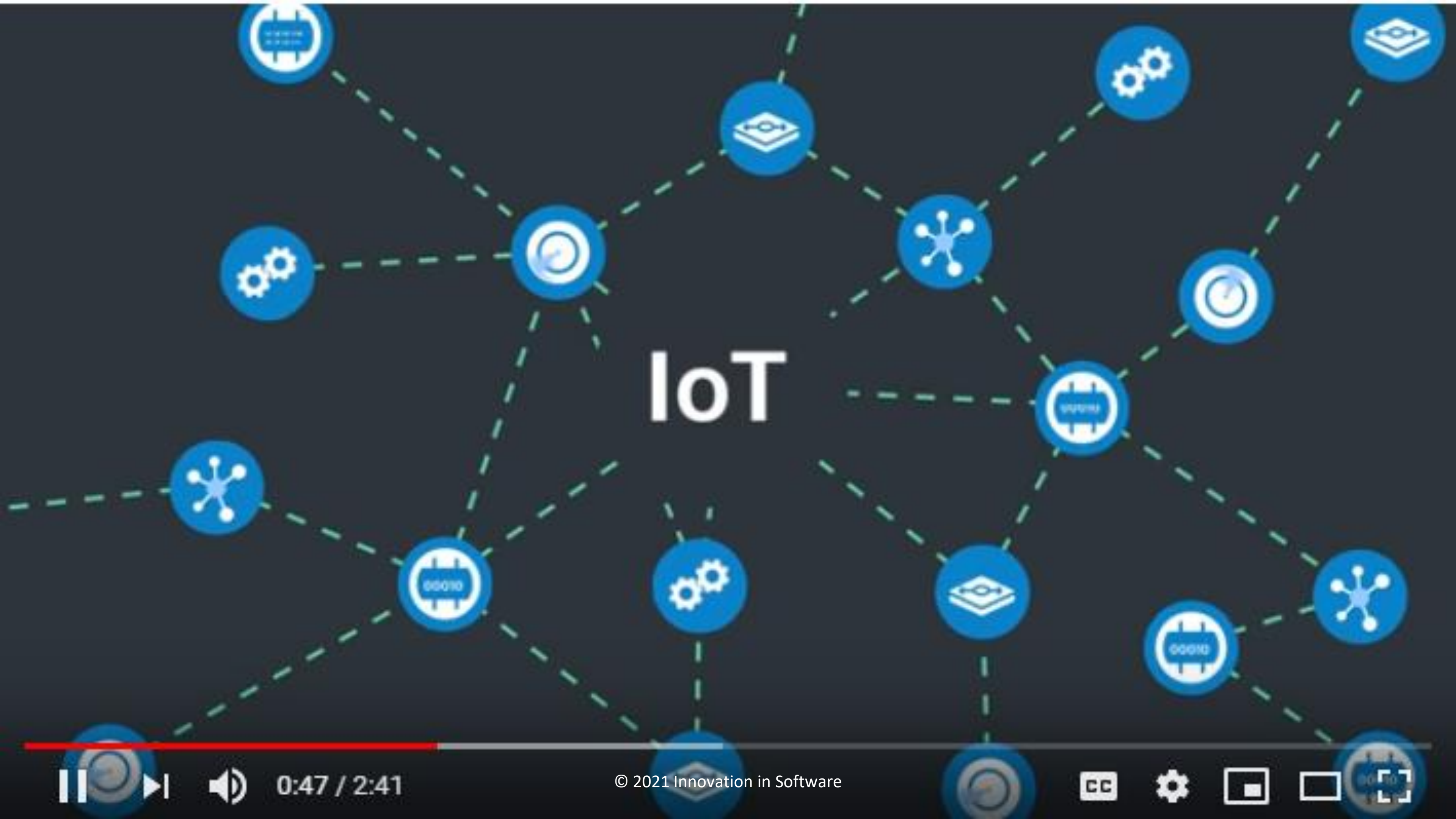
- Generate custom responses at the edge
- Read and write access to headers, query string, and cookies

Network calls

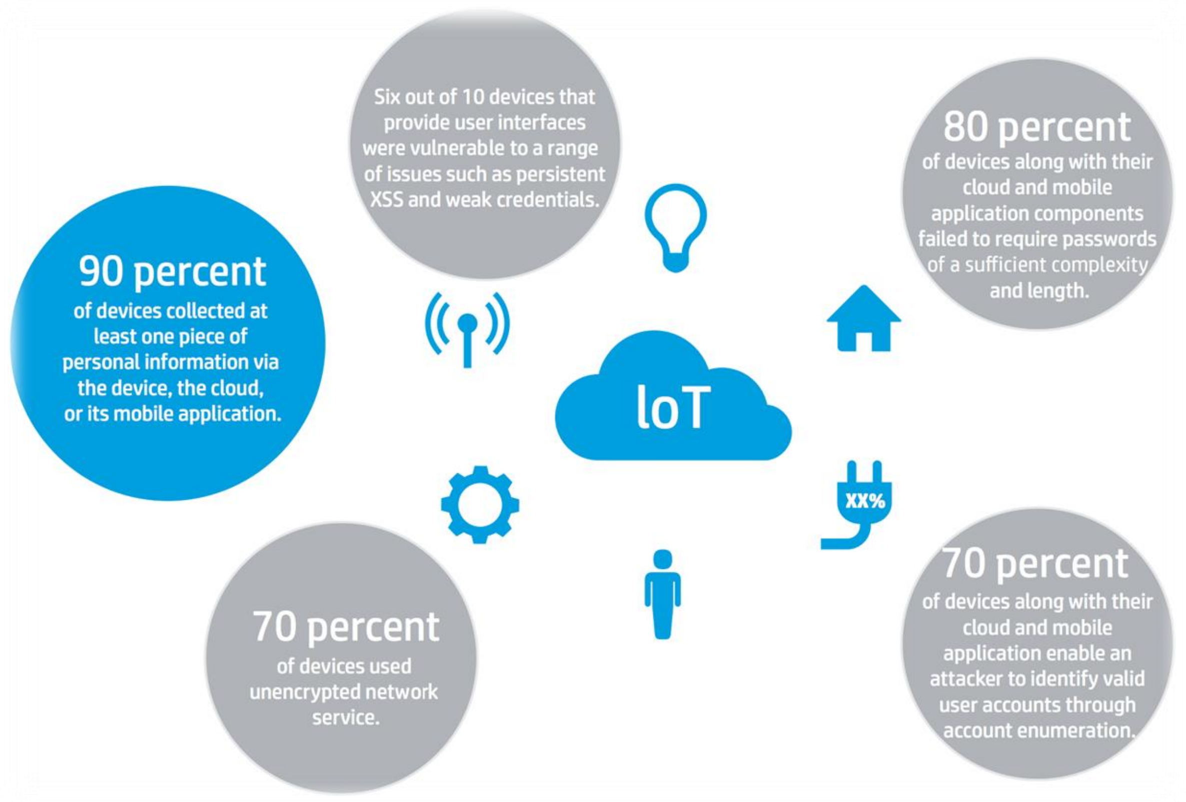
- Origin events
- Viewer events

Content-based routing to any origin

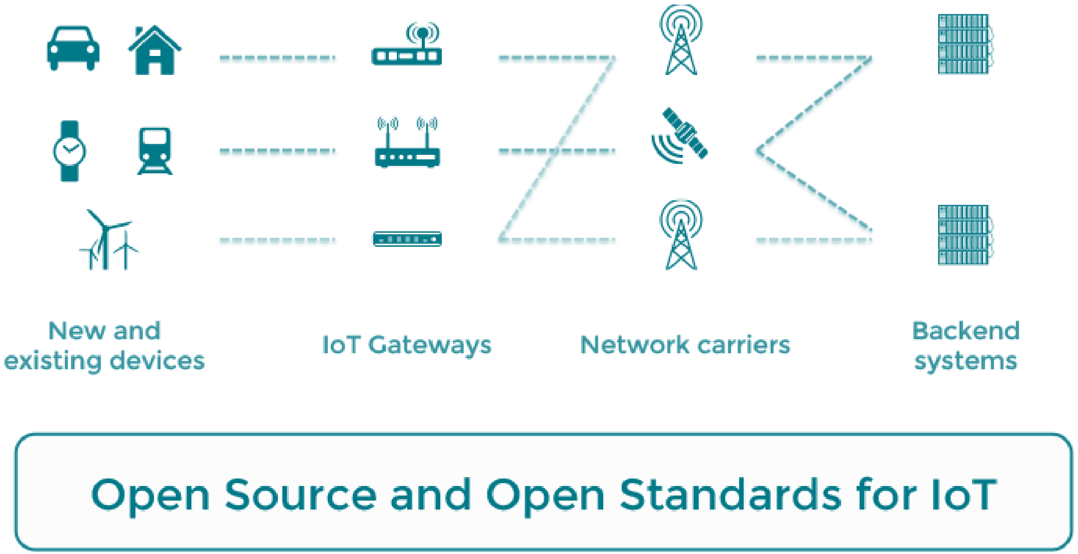
Challenges for Successful Edge & IoT


IoT
0:47 / 2:41

Challenges of Edge & IoT



Standards in Edge & IoT



Standards are developed and widely adopted in established areas

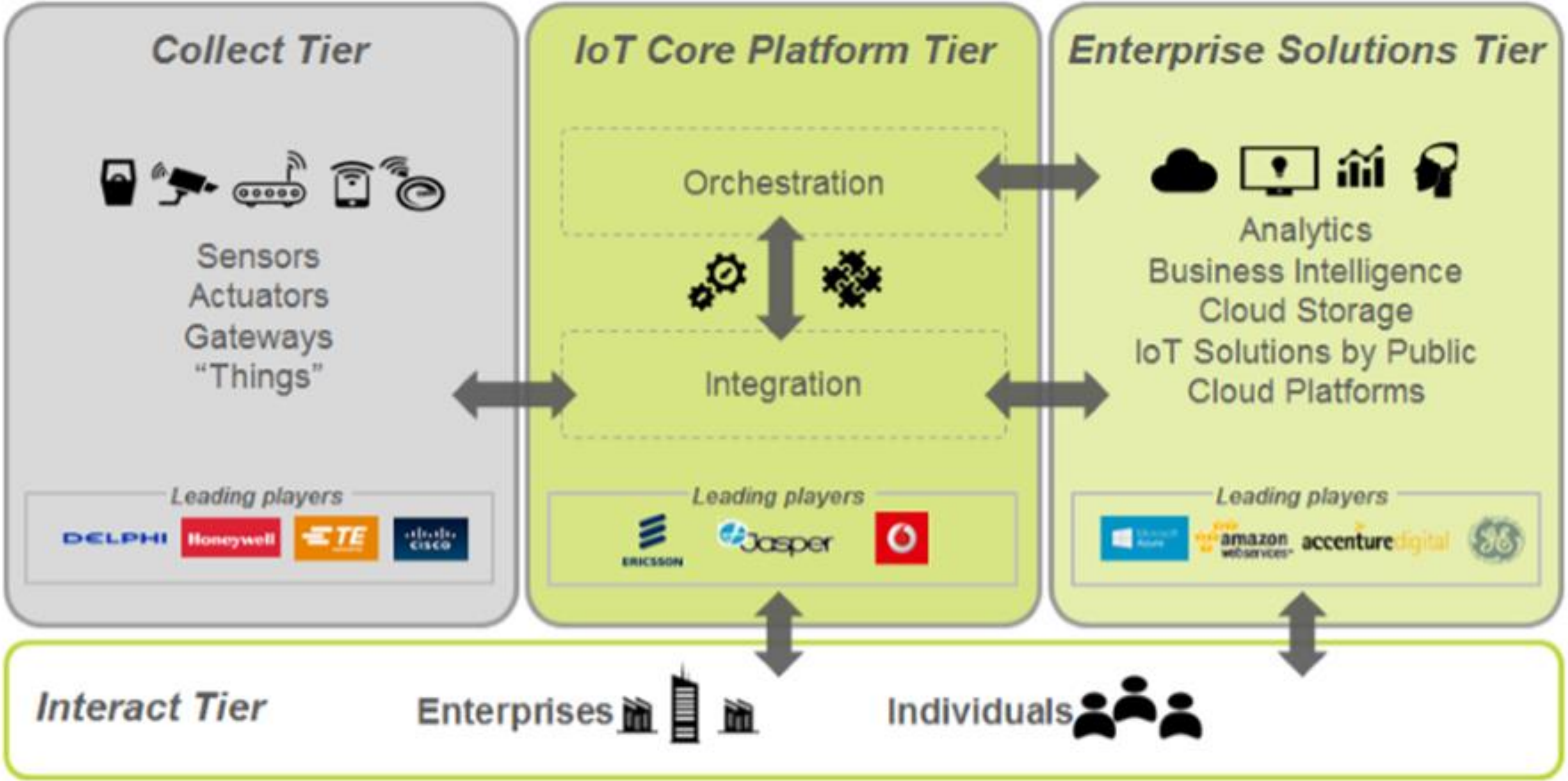
In new areas like M2M there are emerging standards and uncertainty

Open standards are the key to success for Edge & IoT

Capabilities used in equipment have standards and must have evaluations

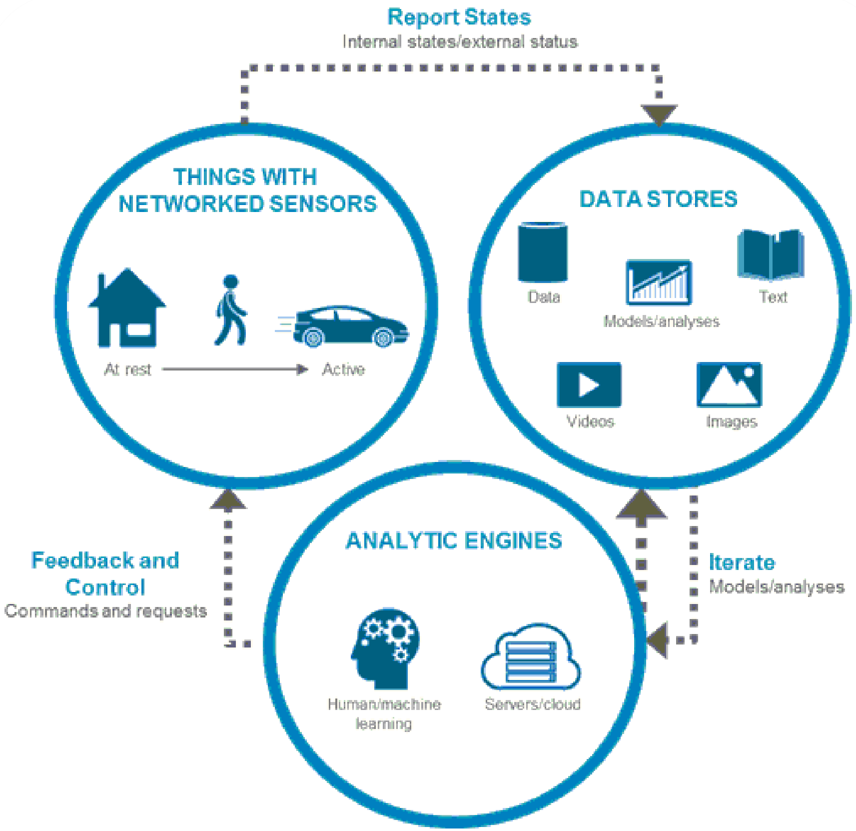
MatrixSSL is an example of a standard that requires security

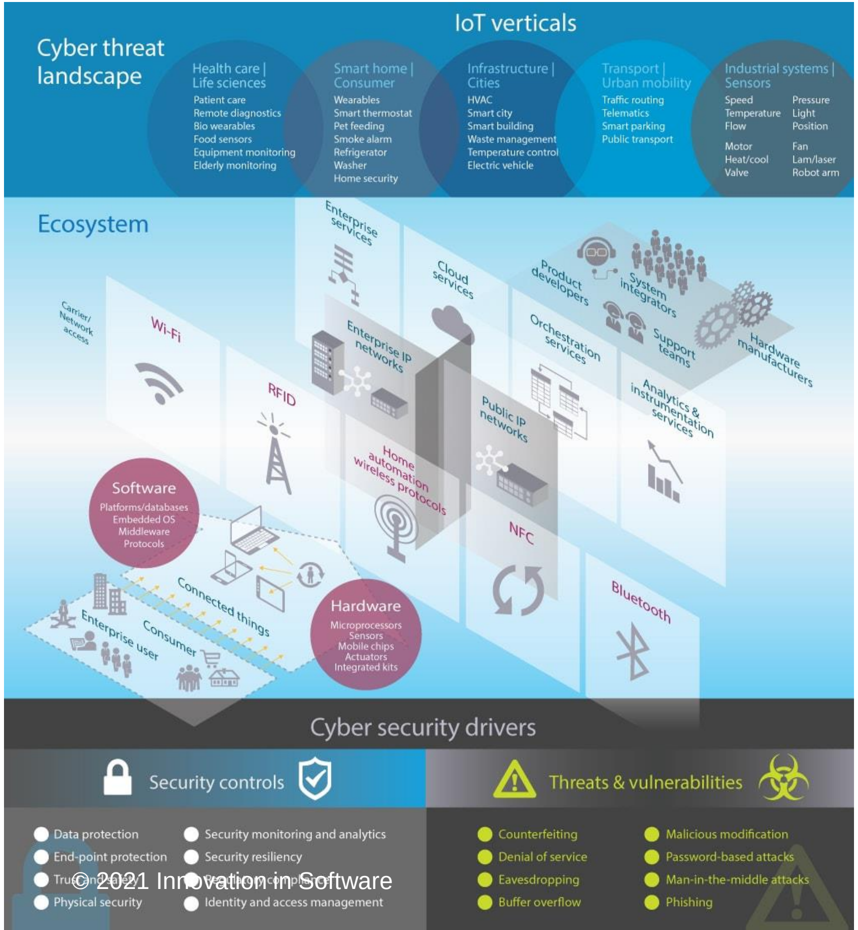
Edge & IoT: Tiered Complexity



Edge & IoT: Limitations

Data Storage and Analysis Challenges

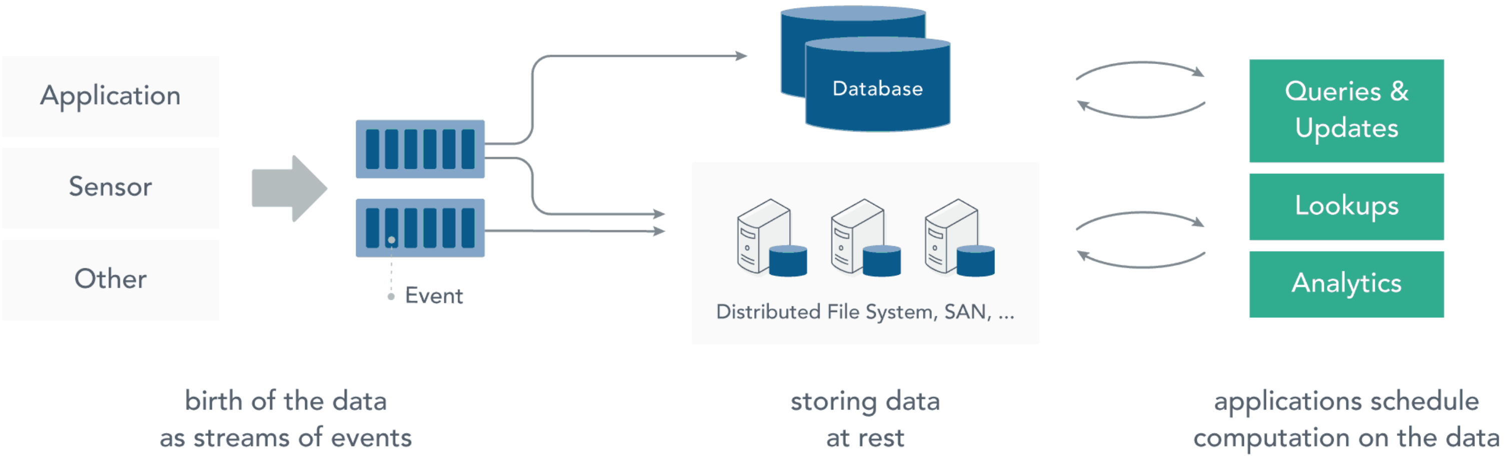




- In Edge & IoT, sensitive data is being shared so risks of security are very high
- More information and gateways creates more possibilities for hacking
- Companies face challenges when it comes to securing hardware that are part of Edge & IoT networks
- External threat: hacking
- Internal Threat: Employees rigging the system

Data Processing Challenges

- Steam processing is data in motion, or computing data directly as it is produced or received
- The application, analytics, and queries exist continuously and data flows through them continuously to large volumes of information in multiple data streams
- Stream processing decentralizes the infrastructure and models the timely nature of most data



Security, Flexibility, Scalability

Not only do applications have to be consolidated, the infrastructure has to **ensure security, flexibility and scalability**

Modern infrastructures are the foundation of an IoT Ecosystem

Security

- An IoT architecture exposes services / applications to the public Internet with all it's associated threats
- A consolidated infrastructure with top-notch security solutions and a coordinated security center allows to defend the companies' IT (data) from external and internal threats

Flexibility

- An IoT ecosystem requires the fast integration of new "things" and services together with the ability to leverage new technologies / frameworks
- A solution for a highly automated configuration and monitoring of infrastructure components together with an automated deployment pipeline has to be set-up

Scalability

- Customer facing services and "things" will have rapid exponential demand curves
- The infrastructure has to be prepared for that with a cloud-like structure and the ability to enhance the IT capacity by public cloud providers

Understanding threats to the IOT

Given the potential threats, IT and security executives need to focus on the security aspects of IoT and integrate them with processes and lifecycle schedules. Figure 3 depicts a high-level IoT architecture that connects what were once isolated technology components across domains.[11,12] The threat vectors that hackers use will depend on their motives, skills and the levels of difficulty they encounter. The following offers a simplified view of how an attacker could target each component in the IoT.[11]

Applications

The cyber-attacker can exploit a number of weaknesses in the application domain, many of which are the result of poor security awareness by the users. For instance, simple, easy-to-guess or default passwords make it easy to gain access to devices and accounts. Likewise, sending unencrypted confidential information makes it easy for an attacker to collect information through "sniffing" or eavesdropping. Increasingly, hackers are using sophisticated social engineering attacks to trick unsuspecting employees or users into revealing confidential information.

Network

Network domain attacks might focus on the core network infrastructure and the access network. Attacks could exploit vulnerabilities in protocols, impersonate devices or involve the insertion of rogue devices, leading to unauthorized network access. Attackers can also exploit the error information used by engineers to debug systems to identify what information technicians do and do not monitor, and to determine network topologies, device identities and information flows.

Devices and Equipment

Attacks typically target connected devices and equipment such as supervisory control and data acquisition (SCADA) systems, sensors or household appliances. Many such devices depend on hard-coded access keys, making them vulnerable to brute-force attacks and spoofing.

Figure 3: High-level IoT architecture

	Application Domain	Network Domain	Device Domain
Threats	Attacks can occur on the application domain. Passwords can be accessible in plain text. Eavesdropping or masquerading as a user can reveal data and identification tokens or identity data and personal user information.	Attacks on the network domain, including the core network infrastructure and access network, can occur by exploiting vulnerabilities in protocols such as Global System for Mobile communications (GSM), impersonating devices or inserting rogue devices to gain unauthorized network access, and making DoS attacks against network components.	At the device level, attacks can be targeted against end-user devices, such as televisions and household appliances, or industrial devices and systems, such as smart meters and control systems. Many devices depend on hard-coded access keys, making them vulnerable to brute-force attacks and spoofing. SCADA systems and IP Gateways tend to leave default passwords.
Examples	• Household heating and power units • Malicious software loaded on point-of-sale terminals to steal credit card and payment information and cause financial, privacy and confidentiality issues	• Medical devices such as insulin pumps and defibrillators with embedded web services connected to the Internet or hospital network • Universal Plug and Play (UPnP) protocol vulnerability	• Industrial control systems (SCADA) • Smart meters • Medical devices • Traffic flow sensors • Connected vehicle control systems

Assessing security readiness

To gauge their security readiness, company leaders need answers to the following questions.

Who is responsible for managing your security risk as your business accelerates toward connected products, equipment and services?

How do your governance practices integrate security with the business (decision-making) processes?

How are you protecting data collected in the field? Do your protection efforts extend from data collection to intermediate storage locations to the industrial data center?

Where is your data stored? Using the cloud may mean that data is not automatically stored in the region in which it was collected. Some countries have regulations relating to data usage that could limit cross-border transfers.

How valuable is the metadata associated with your secure data? What information could someone derive from it?

Who ultimately owns your big data? How do you protect against intentional or even inadvertent breaches of privacy and confidentiality? How do you even know when violations have occurred?

What happens to risk, governance and compliance activities when previously hard-wired OT that controls critical functions and agile IT systems converge into a unified platform? The consequences of failures in such a converged system can be severe and far-reaching.

What is the security model for mass-produced, mass-consumed connected products?

How do you failsafe thousands or millions of industrial system sensors or microelectromechanical systems (MEMS)? Organizations need to integrate and thoroughly test safety mechanisms for critical applications to ensure their robustness.

How do you stay ahead of attackers who are becoming more creative as they take advantage of the physical and digital "blur"?

How does your security organization embrace agile, resilient and reflex-like solutions that can be embedded in products and where threats and operational states are monitored in a way that operational decisions can be made before a cyber-attack causes damage?

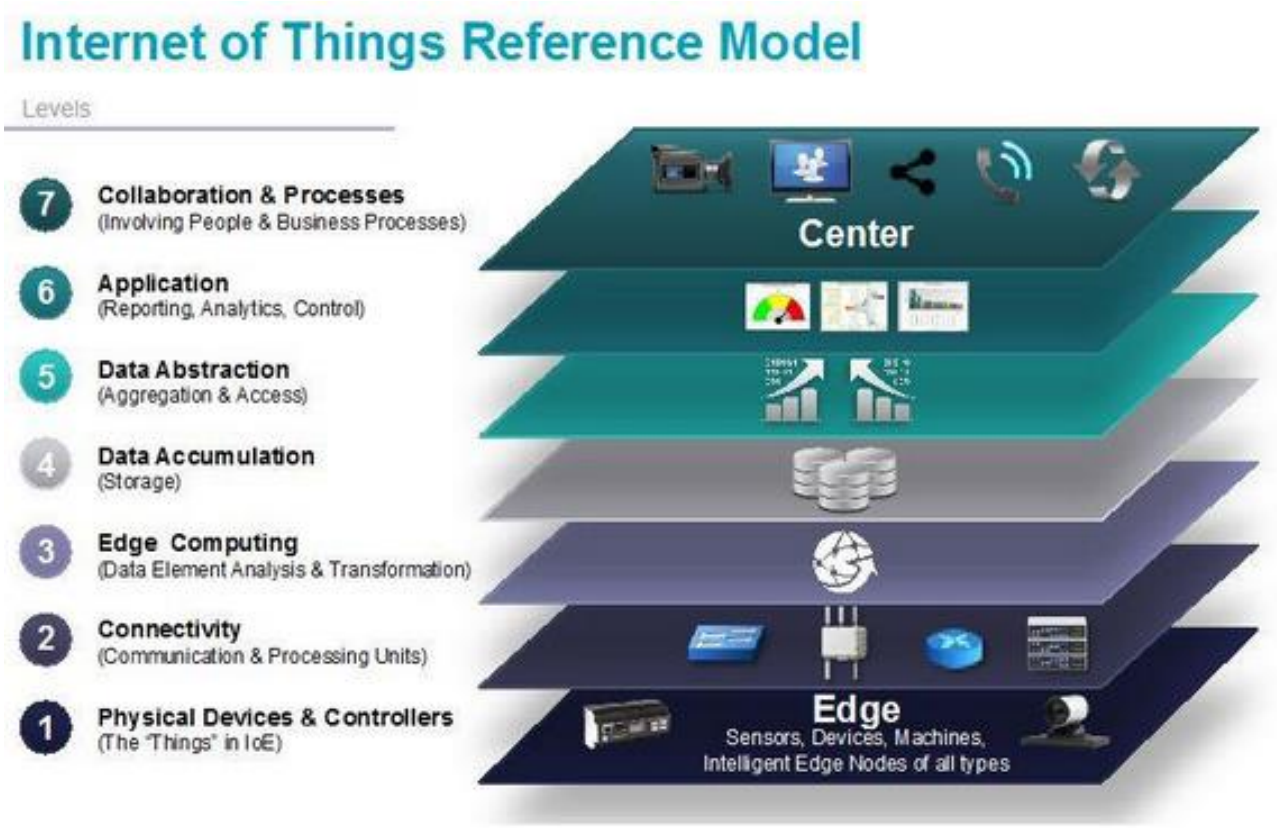
GSMA Edge & IoT Security Guideline

- https://www.gsma.com

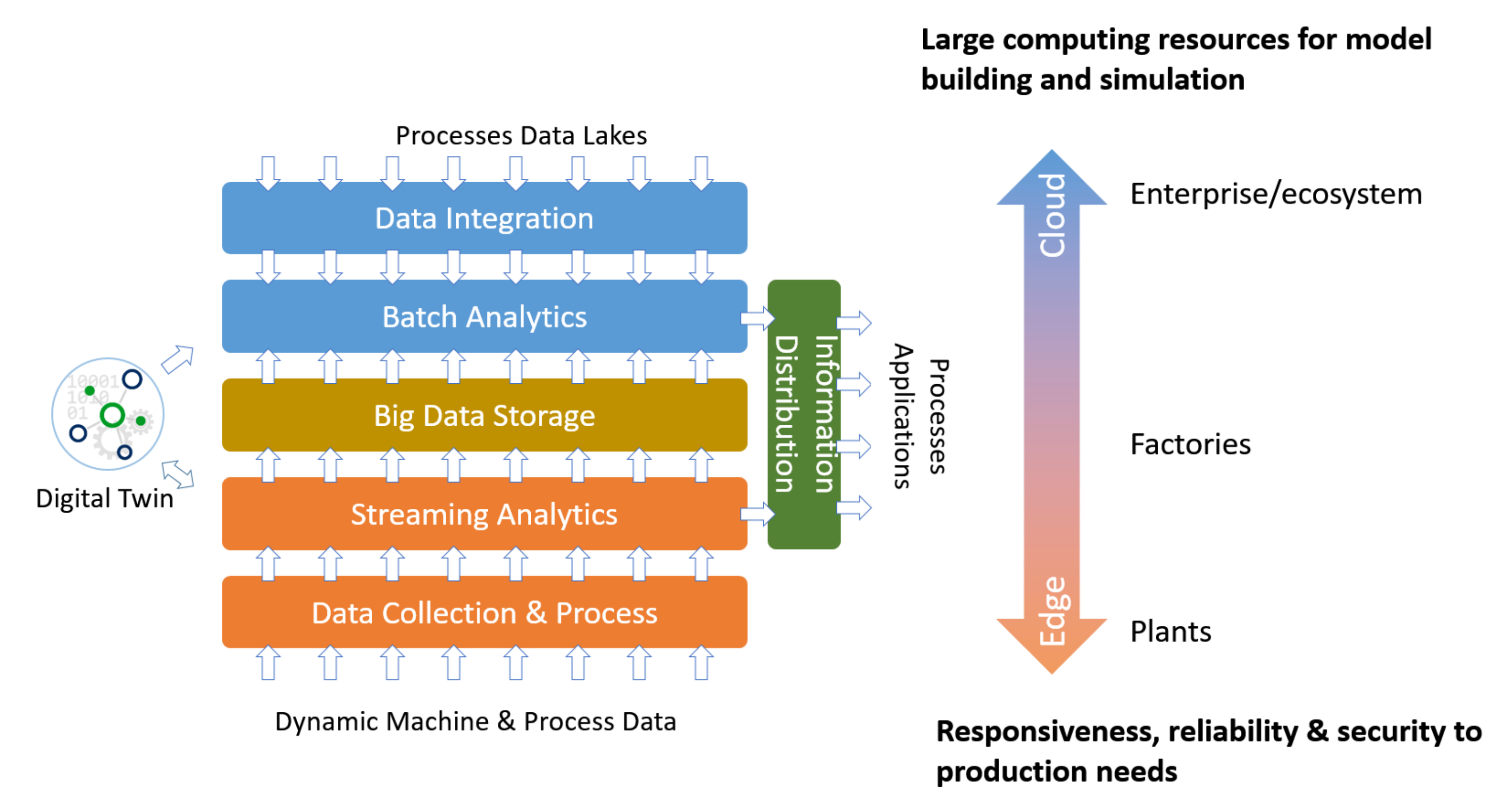
Steps a Digital Enterprise Should take in a Connected World

- Engineer “trust” into connected products
- Adopt a new operational mindset
- Develop contextualized threat models
- Adopt privacy by design principles
- Track emerging standards
- Educate system users

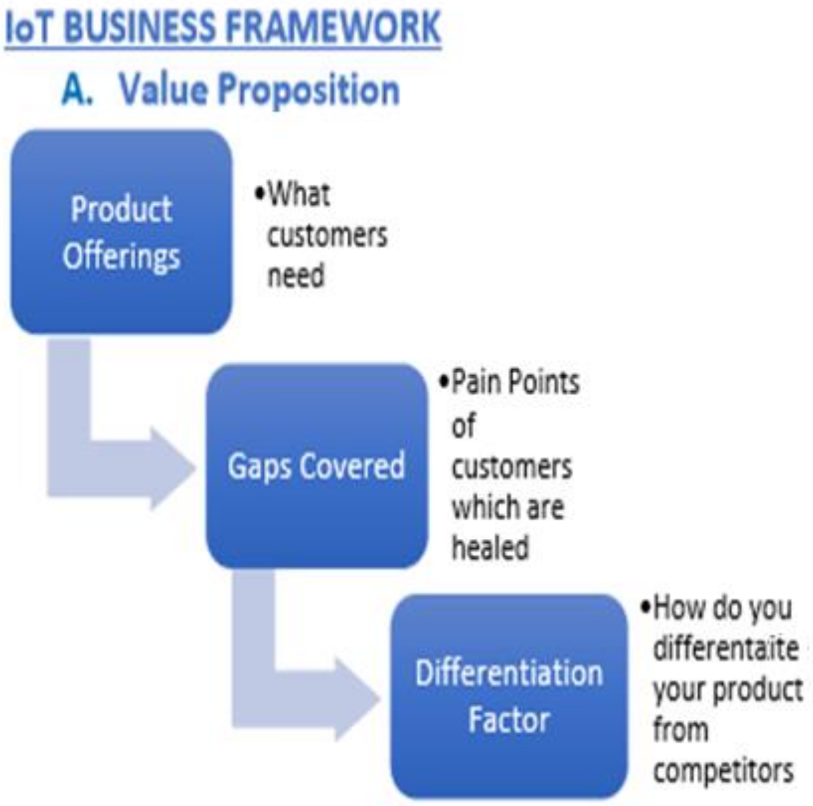
Edge & IoT Reference Model



Digitizing Infrastructure



Edge & IoT Business Framework



Edge & IoT Solution Landscape

Verticals (applications)

Consumer | Healthcare | Insurance | Manufacturing | Retail | Transportation | Utilities | Resource | Government

Platform & Enablement

Platforms

Interface

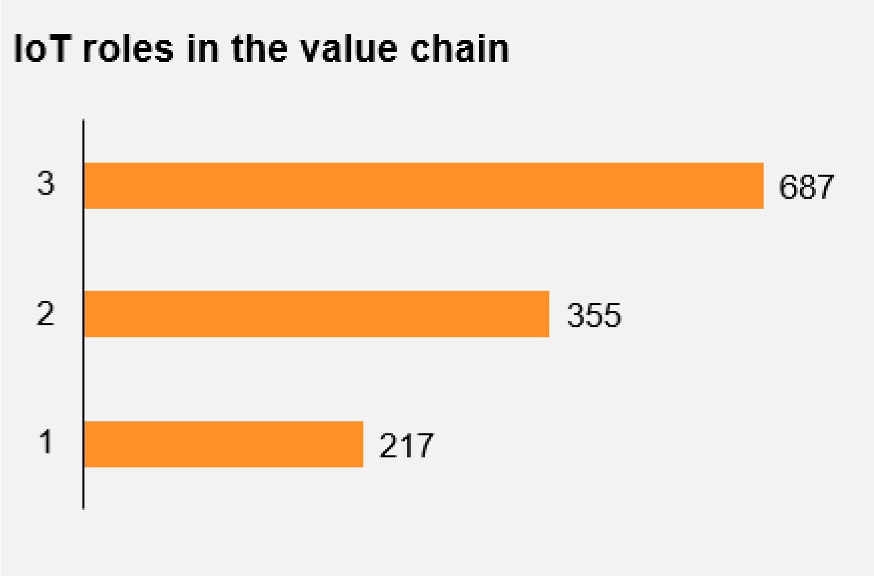
Building blocks

Hardware

Software

Connectivity

Edge & IoT Solution Fragmentation



- **Applications** - Vertical solutions and services
- **Platform & Enablement** – platforms, enabling capabilities, integration with 3rd party applications, analytics
- **Building blocks** – chipset, module, device hardware & software, connectivity providers, partners & consultancies

- That's over 1400 players currently and growing

Edge & IoT Risk Mitigation: Function, Components and Call to Action

Security challenges

- Data Management
- Security Strategy & Governance
- Identify Management
- Device and Cloud Integration

Components and considerations

- Edge & IoT Services, Devices, Applications & Platforms
  - Secure
  - Store
  - Orchestrate
  - Analyze

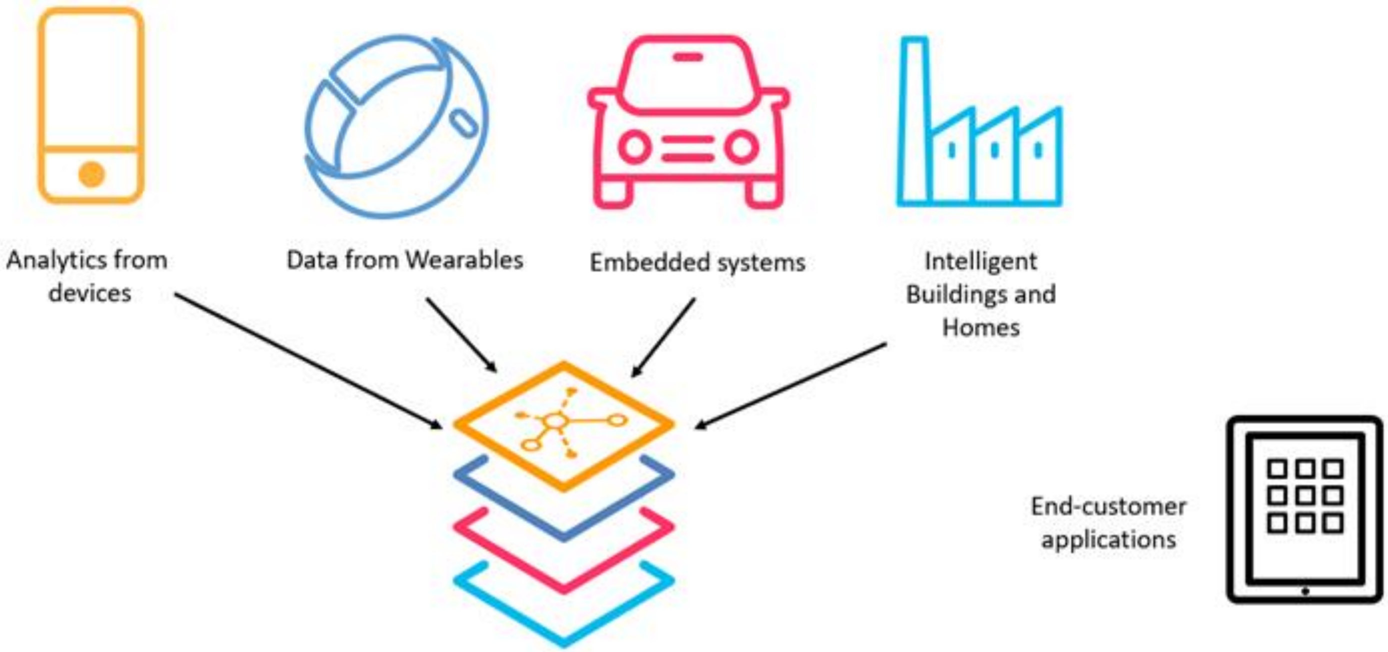
Security call to action

- Identity & Access Management
- S-SDLC
- Collaboration
- E2E Data Security
- Privacy by Design

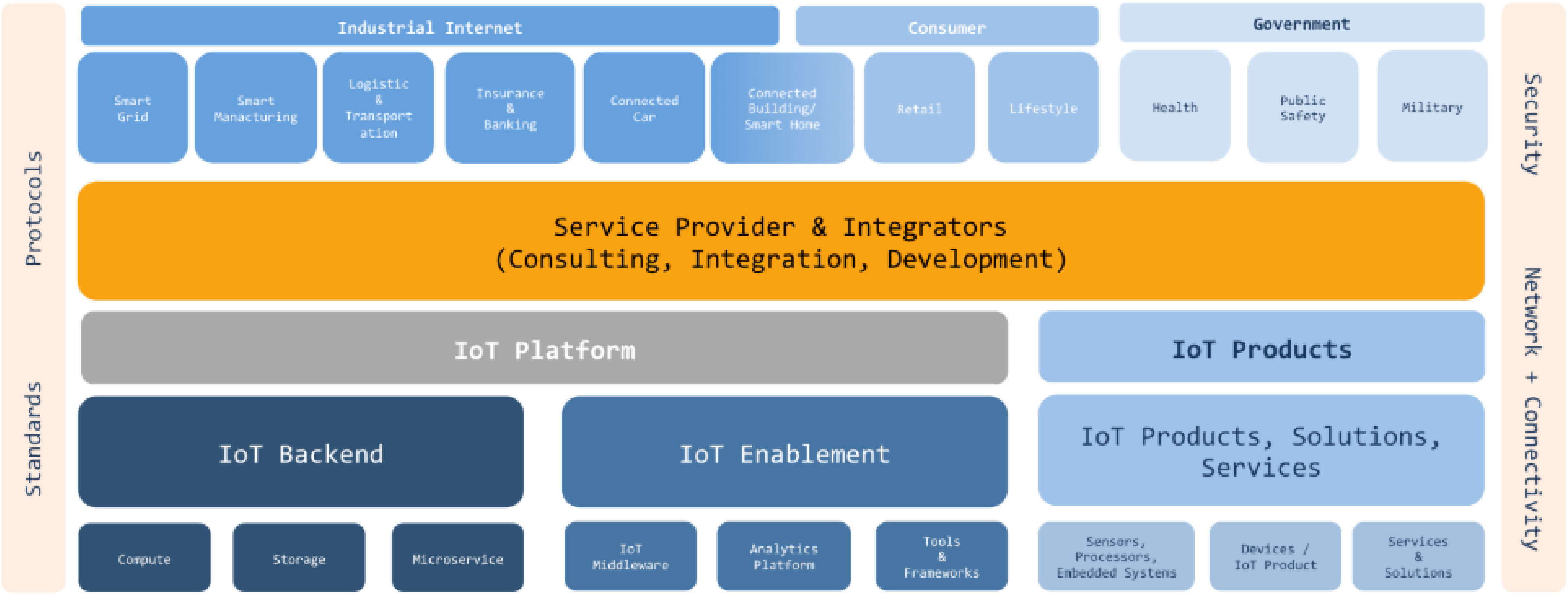
Edge & IoT Platforms


1:44 / 1:59
amazon
web services
YouTube
Amazon Web Services (AWS) IoT platf
made with

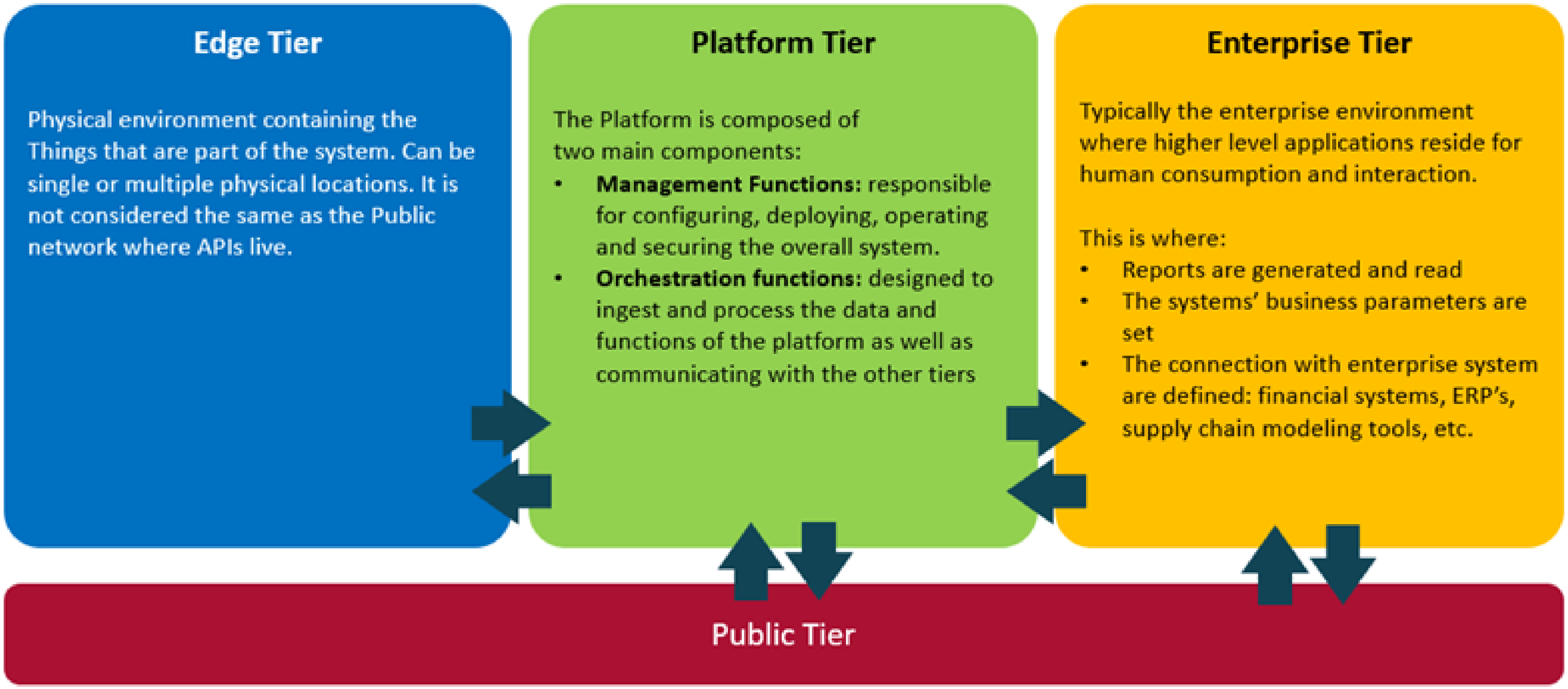
Edge Computing & IoT Convergence



Edge Computing & IoT – The Stack



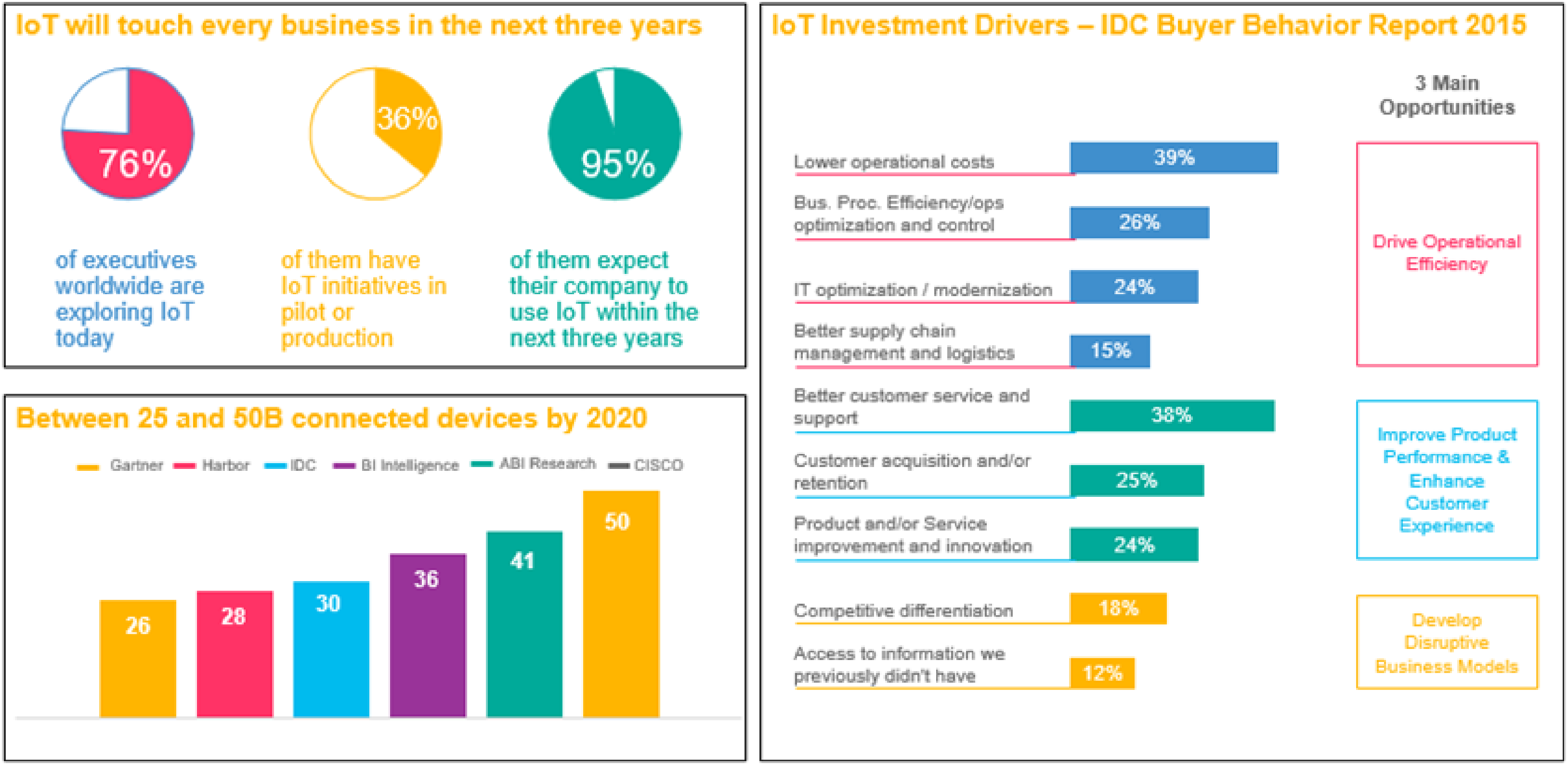
Single Platform Edge & IoT System Architecture



Platform Evaluation Criteria

Global Credibility and Scale • Global reach • Availability of capabilities, service providers and ecosystem partners • Strategic partnerships, their true meaning and value • Vendor lock considerations for technology and services • References of Edge & IoT platform implementations	**Platform Economy** • Software differentiation • Support for open app ecosystems • Developer friendliness • Convergence of Edge & IoT and AI for analytics and predictive maintenance • Alliances (IIC etc.)	**Service Creation** • Developer enablement • Develop-Build-Maintain • Availability of reusable business modules • Documentation • Operability • Security	**Technical Execution** • Device Communications • Service enablement • Edge analytics + hot, warm and cold data • Data Management • Enterprise integration • Industry solutions • Security
Industry Fit • Industry credibility for Organization • Industry relevant references	**Vendor Roadmap** • Partnerships • Developer engagement activities • Vendor vision and responsiveness	**Service Run** • Scalability • Licenses • Recoverability • Operability • Availability	**Commercial model** • Pricing models • Cost vs. value of reusable business modules • Cost vs. value of vertical applications • Service creation • Service run

Edge & IoT Dramatically Reshaping the World



Source: The Economist, Cisco, 3rd Party Research Firms, Ericsson, Programmableweb, GSMA

Platform Stats & Business Transformation

Platform is a business critical decision in the Product to Service Transformation journey

A well-designed IoT platform accelerates development of IoT applications through ease of discovery, reuse and configuration, and extension of a library of core data and service components. Implementation of IoT applications is an iterative process. It starts with a singular, sometimes relatively simple, use case which uses a discrete set of capabilities and data complete enough to imagine and capture the initial use case and generate new data. Once operational, it provides insights and knowledge which can be used to expand the use case or spawn new use cases. The platform differentiates itself through its ability to quickly create, capture, learn from, and rapidly adapt and optimize new applications.

Functional Areas of Edge & IoT Platforms

Industrial Internet of Things (IIoT)

Accenture Definition

"The Industrial Internet Of Things is a technical and business paradigm in which devices (things), equipped with contextual intelligence, interact on one end with their environment, either passively (sensing) or actively (actuating), and are networked to collaborate with other smart objects, humans or applications, to deliver a value that can be expressed as a service."

Growth Drivers

Pervasive Sensing — *Physical, chemical and biological sensors based on nano-materials such as conducting polymers and composites are rapidly evolving towards autonomous analytical devices that perform sophisticated analytical processes*

Platform Economics — *The steep decline in cost of electronic components, storage and data processing has led to emergence of platforms that bring together set of differentiated capabilities to deliver IoT solutions at scale*

Ubiquitous Connectivity — *The advances and standardization in network technologies allow rapid and low-cost promulgation of information from sensors to be combined with the avalanche of business process & consumer activity data*

Value networks — *Businesses and Governments are realizing that IoT applications and data driven insights can be used to optimize cost, support service led business models and create tangible value for ecosystem participants*

IoT platforms **market** trends and observations

#1 **Highly fragmented market with established players from various industry sectors are pursuing IoT platform strategies**

*There is **immense fragmentation** in the IoT platforms space, an increasing number of large, midsize and small vendors have been entering the market, ranging from IT megavendors to midsize providers incorporating IoT capabilities into existing product and service offerings, to proliferating IoT-centric startups.*

3 main drivers exist for continued diversification of the IoT platform vendor landscape:

- **unique requirements**
- **a plethora of vendors**
- **a plethora of buyer project types** *(Gartner, Jul 2016)*

~300
IoT platforms in operation currently

#2 **Consulting providers and SI's are rushing to build their IoT capabilities with own investments, partnerships, and acquisitions**

- **2016 is the year of the IoT message of the megavendors** (IBM, GE, IBM, Microsoft, Oracle and SAP) as *they seek to educate and influence enterprises. However, these megavendors have good roadmaps but are still building out their solutions and ecosystems – via investing, partnering or acquiring.*

Microsoft Azure
HCL
IoT Incubator

IBM Watson IoT.
$200M AI investment

IBM Watson IoT.

SAP
$2.2B investment in 5 years

In IIoT companies like Mocana

IoT platforms offering trends and observations [1/2]

#1 Software is emerging as a key differentiator, and firms are leveraging key strategies to drive this – in house development, collaborating and acquiring niche players

***Embedded software** is the foundation of **value and differentiation** in the fast-evolving connected devices that make up the IoT. However, IoT software is still **an emerging market with a broad set of buyers** across the enterprise — from the various lines of business (LOBs) to central IT. These buyers have different objectives, project types and success criteria. (Gartner, Jul 2016)*

Develop software testbeds/ simulation software/ digital enterprise software

SIEMENS Ingenuity for life → MindSphere

IBM software test automation for IoT

Collaborate with large firms to develop new technology/ optimization tools

ptc – vmware

Acquisition of innovative startups

ptc → kepware

Microsoft Azure → solair

#2 App ecosystems are emerging around open platform plays

*As a step towards **achieving adoption** across users, firms have started to **open their cloud platforms to create an ecosystem for third-party developers** to design, develop, and host applications which can be made available to end customers.*

GE

- ✓ Open platform
- ✓ Predix app marketplace
- ✓ Digital foundry

CLOUDFOUNDRY

intel Security – WIND RIVER

- ✓ Intel subsidiary Wind River announced a app store for the VxWorks IoT RTOS

ptc

- ✓ Open platform
- ✓ Thingworx launched the first marketplace for IoT apps and modules in 4Q 2013

IoT platforms **offering** trends and observations [2/2]

#3 IoT and AI are naturally converging in IoT platforms for predictive analytics/maintenance

Big data analytics tools are evolving from descriptive to predictive and prescriptive, which enables companies to use foresight rather than hindsight to improve business processes. IoT will be a huge generator of machine data. The predictive analytics market is expected to reach $18.5 billion by 2021.

- **Evidence**
  - **IBM** announced that it is investing USD200m in Watson IoT AI business
  - **Microsoft**'s Azure IoT Suite strongly leverages the Cortana Intelligence Suite, which is underpinned by Artificial Intelligence and Machine Learning for its analytics capabilities
  - **Siemens** has €1 billion allocated to 'Next47' which invests in IoT, artificial intelligence and other emerging technologies. Accenture is also building a suite of applications for Siemen's MindSphere to enable new digital services, such as predictive maintenance.
  - **PTC** acquired Coldlight, a ML and predictive analytics company for USD105m to complement its IoT application enablement capabilities.

#4 Extensive cyber security is an increasingly necessary capability for IoT platform vendors

We sense that there is rising demand from the market for hyper secure frameworks from IoT solution vendors. Security assurances should enable and encourage large organisations to transition from pilots and small scale IoT deployments to larger scale deployments.

- **Evidence**
  - **Siemens** and McAfee (an Intel subsidiary) have partnered on industrial cyber security
  - **GE** acquired the cyber security company Wurldtech
  - **Intel** has partnered with Honeywell to secure critical infrastructure and 'industrial Internet of things'
  - **Microsoft**'s Azure cloud is supported by the MS Digital Crimes Unit, MS Security Response Center, and MS Malware Protection Center.

Edge & IoT Paradigm Shift

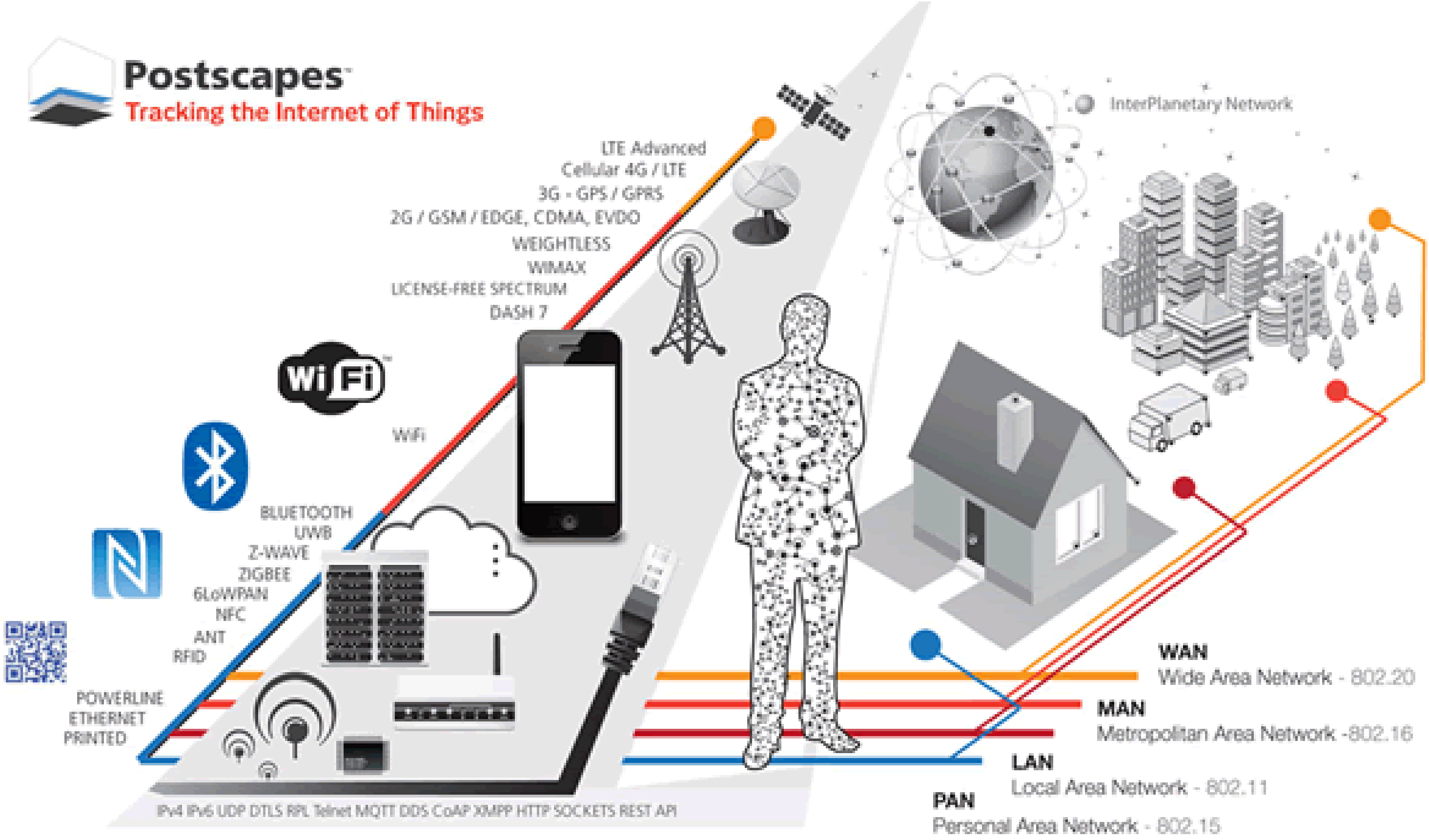
IoT helps businesses achieve unconventional revenue streams

	Traditional Business Model +	IoT Technologies/Solutions =	New Revenue Streams
The Weather Channel	Weather forecasts	Sensors, nanosatellites, autonomous marine vessels, drones	Granular weather insights as a business service to apparel, food, entertainment, travel, shipping and insurance companies
GE	Jet engine supplier	Sensor technology, embedded software, real-time analytics	Aircraft engine preventative maintenance and fleet optimization services
Virtual Radiologic	X-ray interpretation service	Teraradiology, real time data accumulation	SaaS and Analytics services

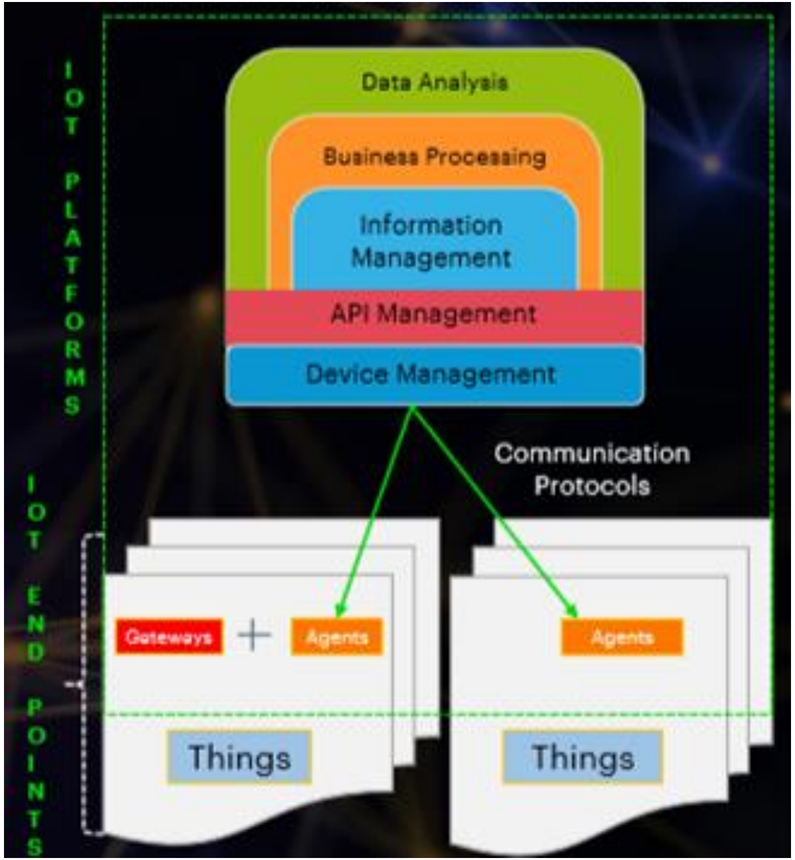
Platform Architecture Comparison Features

- Things and gateways provisioning and management.
- SDK, IDE, virtualization, containerization
- Reliable and secure bidirectional communication
- Identify and access management
- Connectivity - communication protocols
- Set of Edge & IoT hardware supported
- Event processing capabilities
- Decision processing
- Pricing plans
- DevSecOps - Security
- Integration via API or Adapters
- User Interface for end user and developers
- Advanced analytics
- Database
- Device management and Integration support

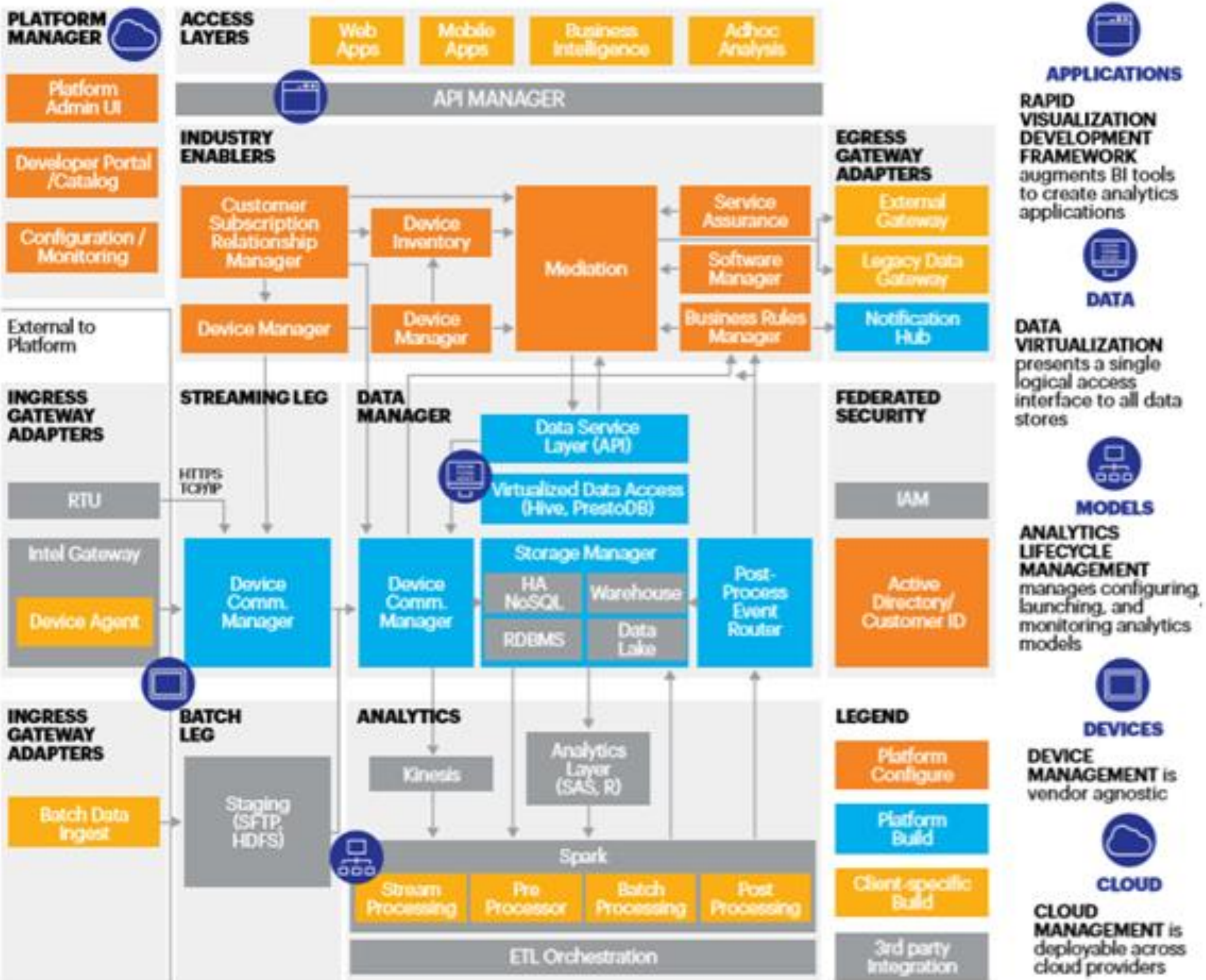
Networking Edge Computing & IoT



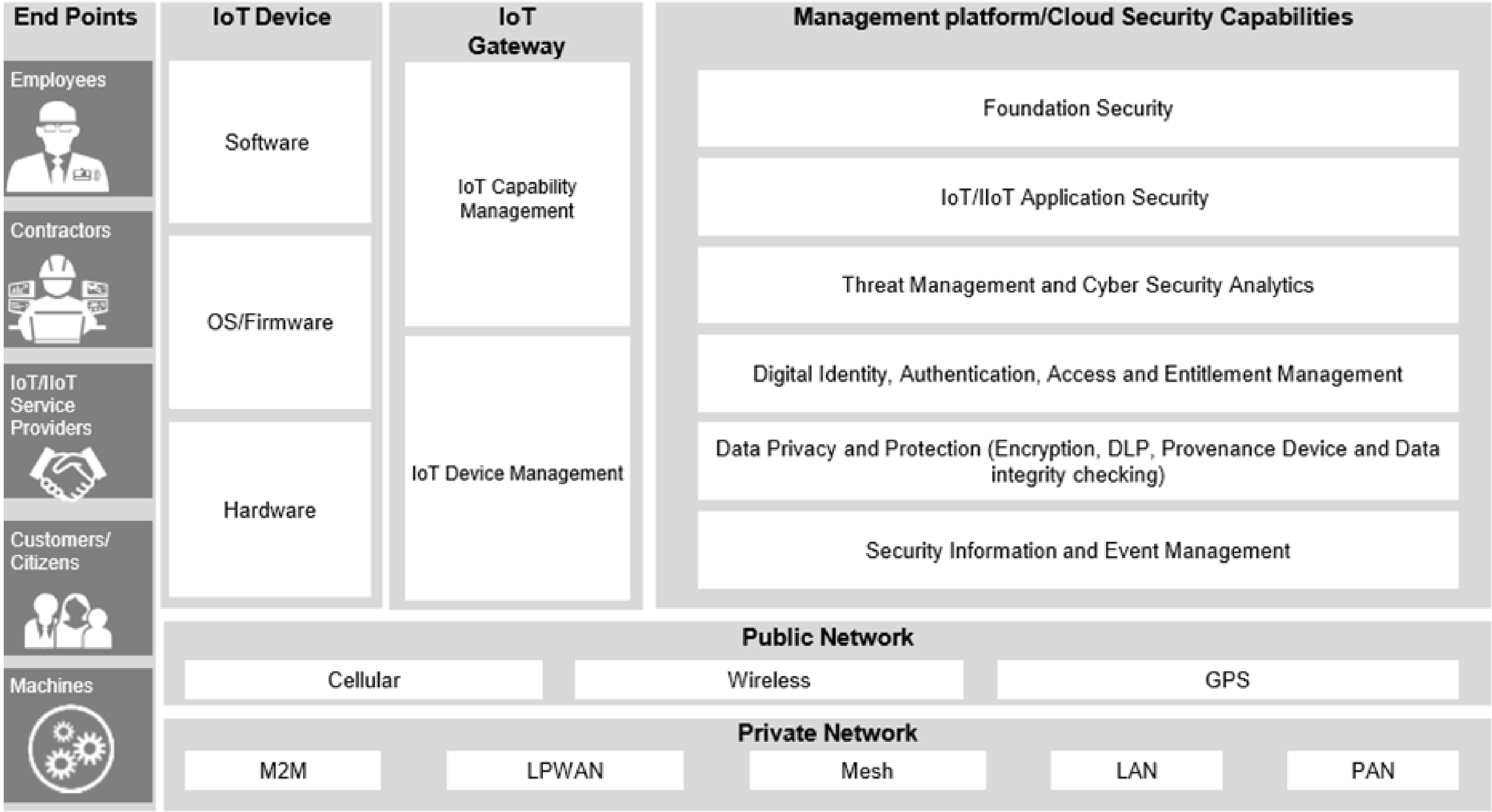
Edge & IoT Platform Functional Layers



Edge & IoT Platform Management End 2 End



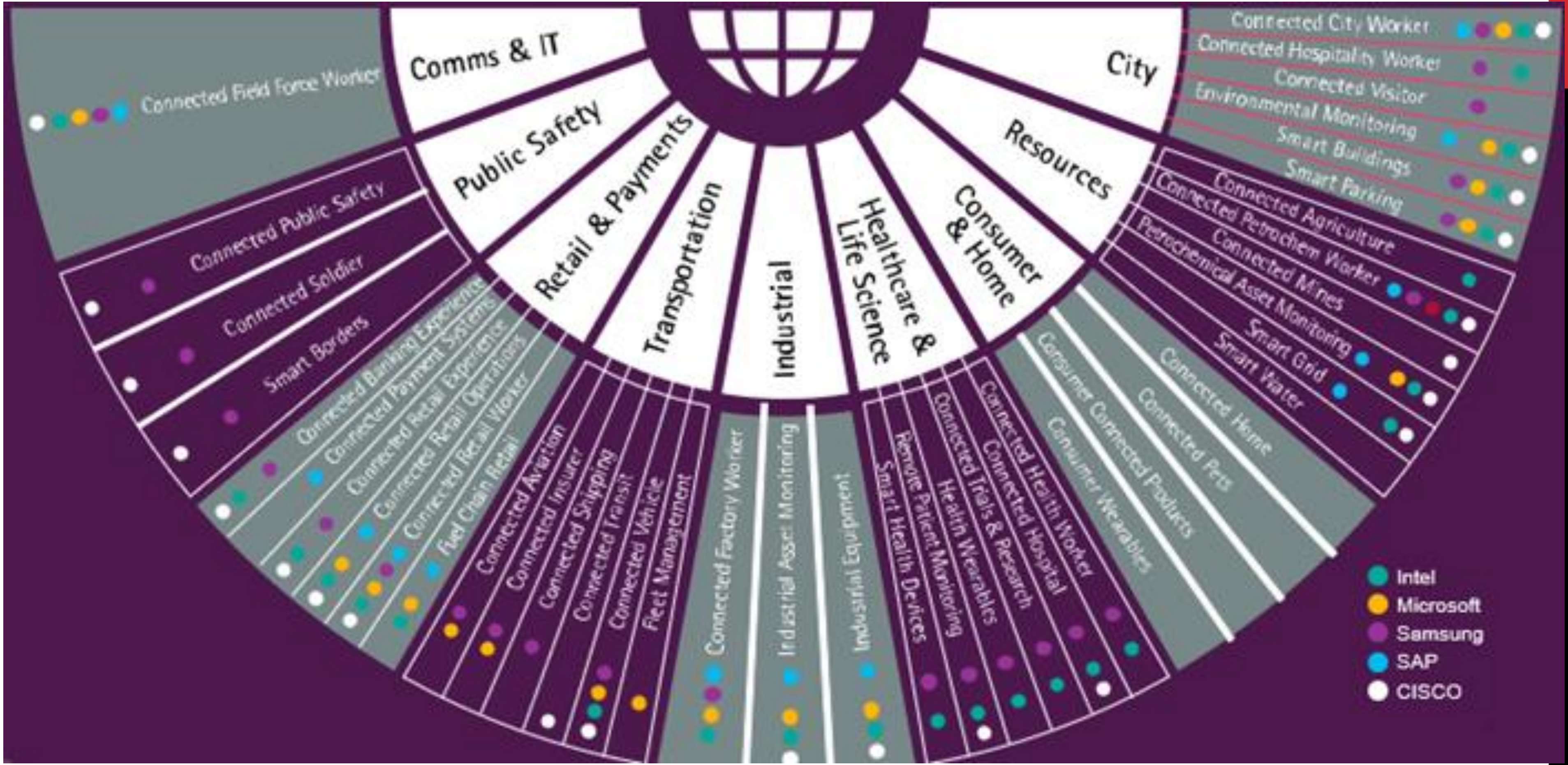
Edge & IoT Identify and Access Management



Edge & IoT Platform Security Controls

Security Area	Security Control	Description	Applicability
Identity & Access Management	Authoritative Identity Source	The IoT platform should integrate with XX as the authoritative identity source of all corporate records	TECOM Business Systems
	Least Required Access	A user should only have access to the systems that are of crucial importance for performing his business function	External and internal users
	Least Required Privilege	An authorized user should only have those application privileges required to perform his business function	External and internal users
		...	
Network Security	Network Architecture	The network should have a well defined DMZ, External and Internal perimeters	Platform network environment
	Network Zone Gateways	Every network zone should be separated from the other by a firewall	Platform network environment
	Secure Communications	Secure all communications between the I&AM system and other systems, applications and databases	Platform network environment
		...	
Encryption	Channels Security	Encryption is required or the following protocols: HTTP over SSL, LDAP over SSL and JDBC over SSL	Secure channels
	PII Classification	Identify key personal identifiable information and ensure classification of such attributes in a secure manner	Personal Identifiable Information
	Password Storage	Passwords should always be encrypted with approved algorithms and be stored using one-way hash algorithms	External and internal users

Edge & IoT Platform Industry Use Cases



Edge & IoT Platform Use Cases

Variety of use cases are enablers for X-Industry business

Connected Transport

Use Case Categories

- Connected Vehicle
- Connected Fleet
- Connected Transit Systems
- Connected Insurance
- Connected Freight

Connected Spaces

Use Case Categories

- Connected Home
- Connected Buildings
- Connected Cities

Connected Operations

Use Case Categories

- Connected Mine
- Connected Asset Mgmt
- Connected Worker
- Precision Agriculture

Connected Health

Use Case Categories

- Remote Patient Monitoring
- Wellness & Prevention
- Connected Pharma
- Intelligent Health Enterprise

Connected Commerce

Use Case Categories

- IoT Payment & Data Security
- Blockchain & Cryptocurrency
- Connected Contextual Commerce

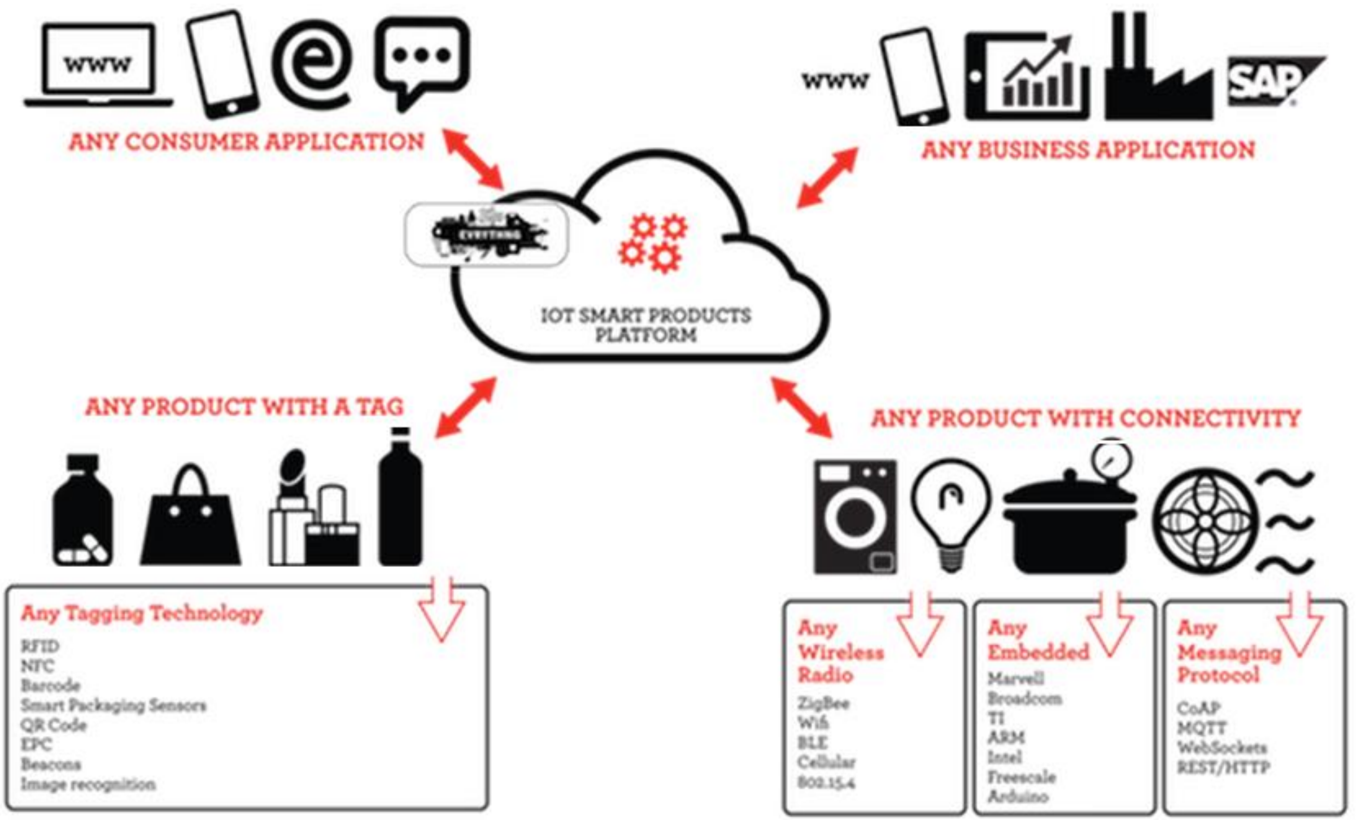
Edge & IoT Platform Infrastructure Requirements

Infrastructure Area	Infrastructure Requirement	Description
Servers & sizing	Core Platform Sizing	The core IoT platform should have a minimum of ## cores
	Vendor Standardization	The IoT platform should run on blades whenever possible
	Virtualization	The IoT platform's infrastructure should target 70% virtualization
		…
Network	Vendor Standardization	The IoT platform should use routers a minimum bandwidth of x GBps
	Physical Channels	The network should use cables of type x to support anticipated traffic
	Communication Protocols	The platform should communicate using built-in Web Services
		…
Storage & Backup	Storage Sizing	The platform should utilize a SAN of ## GB at a minimum
	Live Backup	The platform should support live backup for the following data sets
	Offline Backup	The platform should support daily backup for the following data sets
		…
Operating Systems and Clients	Operating System Standardization	The platform components should run on Windows Server 2008
	Thin Client Support	The platform should support a thin client running on IE 7+ or Chrome
	Thick Client Support	The platform should support xx thick client
		…
…		

Architectural Styles for Edge & IoT

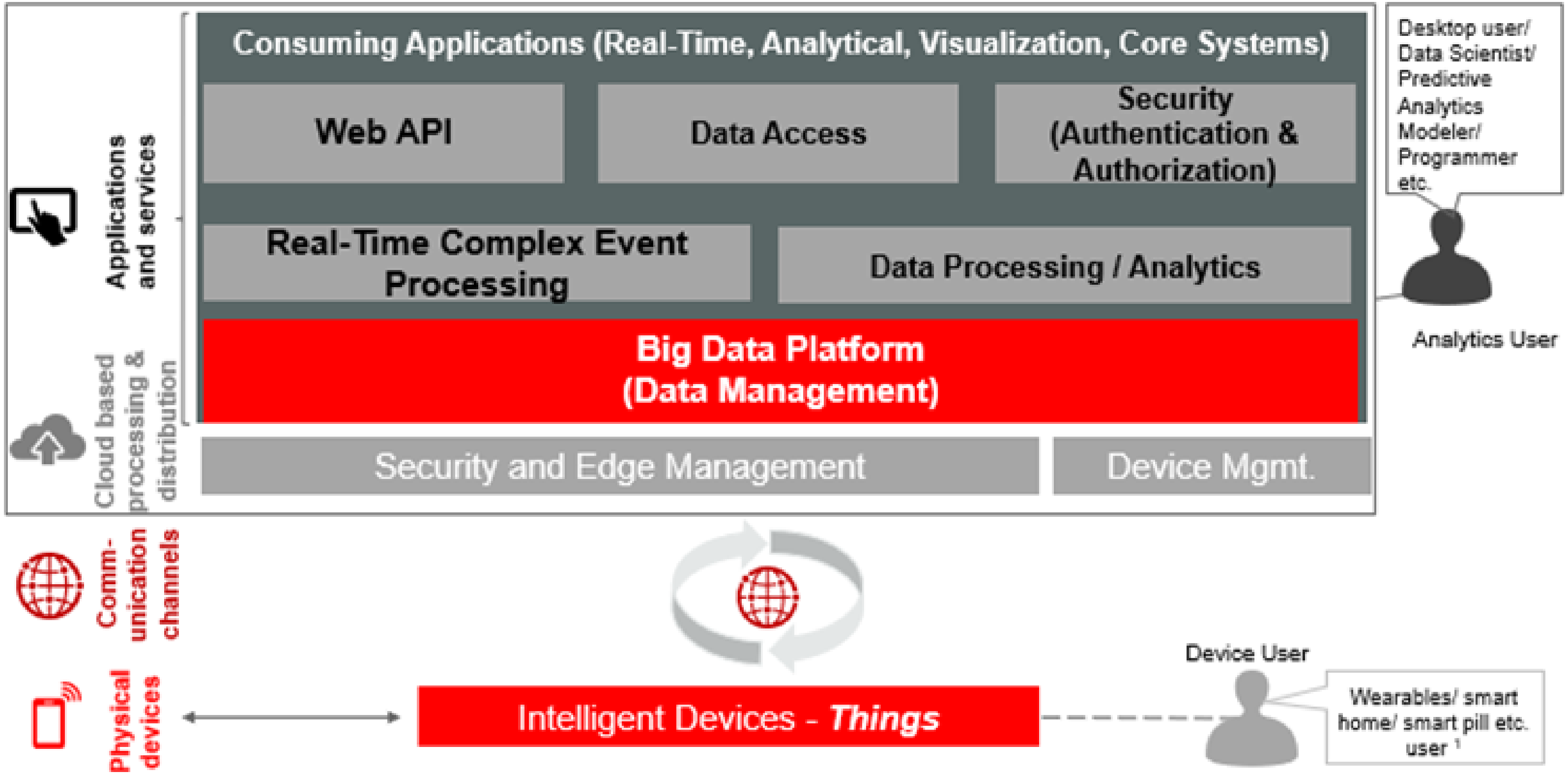
Thing-Centric	"Things" store most of their data on-board and are smart. They are self-sufficient and communicate to the Internet for centralized analysis and synchronization.
Gateway-centric	The gateway stores the application logic, data and communicates from the "things" connected to it. The gateway provides resources needed by the "things".
Mobile Device-centric	A mobile device houses the application logic, stores data and communicates with the "things" connected to it. The "things" do not need to be as smart, since the mobile device provides the resources.
Cloud-centric	The cloud acts as the connectivity center, powers analytics and provides data storage. The "things" do not need to be as smart, since the cloud provides the necessary resources.
Enterprise-centric	"Things" reside behind firewalls and are geographically collocated. There is little need to extend out to the extranet.

Architectural Styles for Edge & IoT

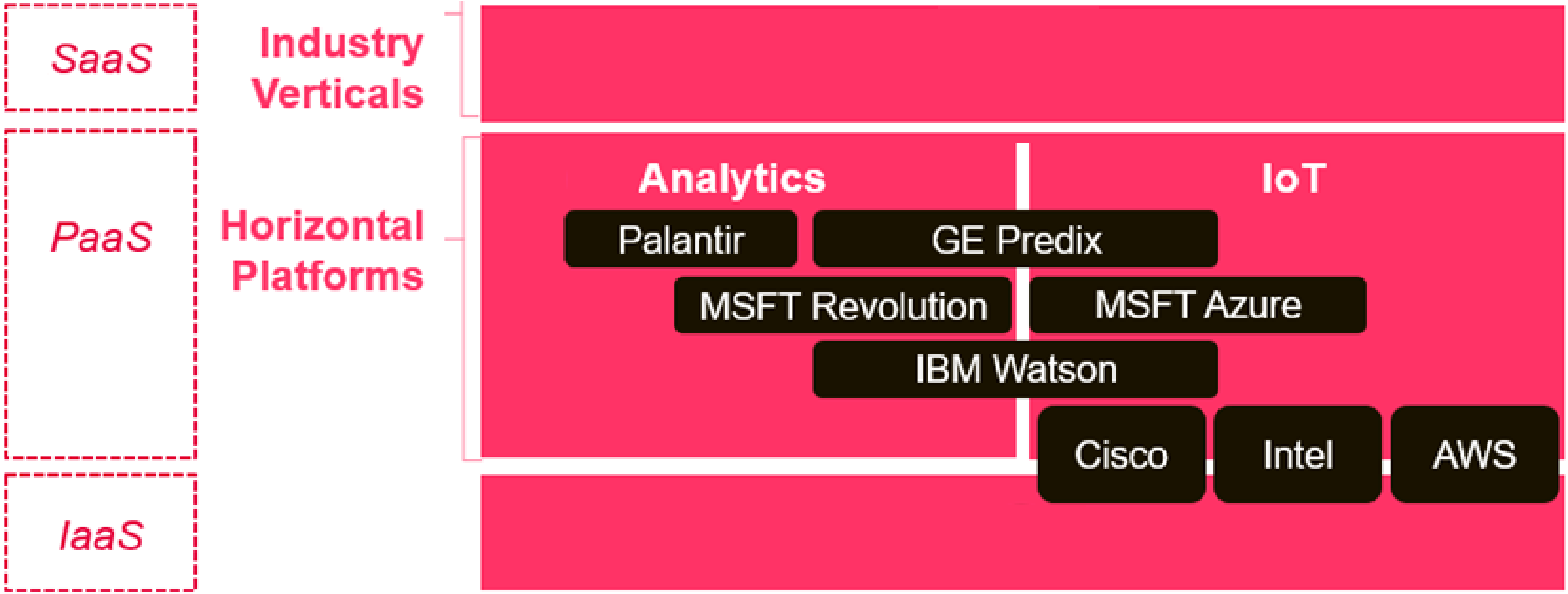


Big Data Edge & IoT Middleware

Big data is a **key element of the Middleware architecture** which ensures efficient collection and normalization of data sent by intelligent devices

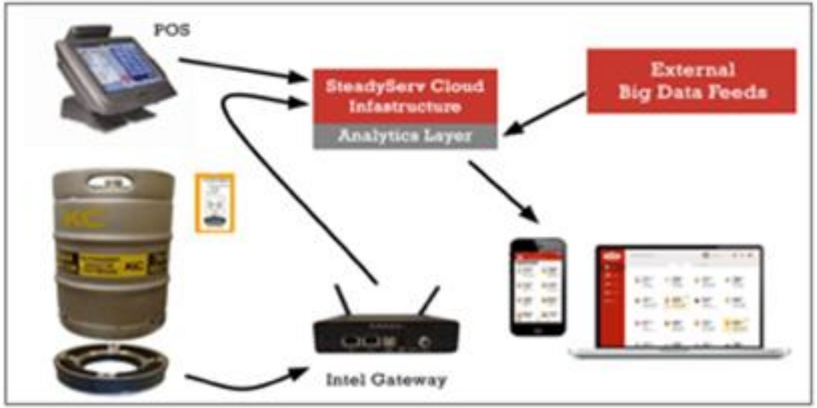


Edge & IoT Ecosystem



Edge & IoT Platform Products - Example

Connected Retail

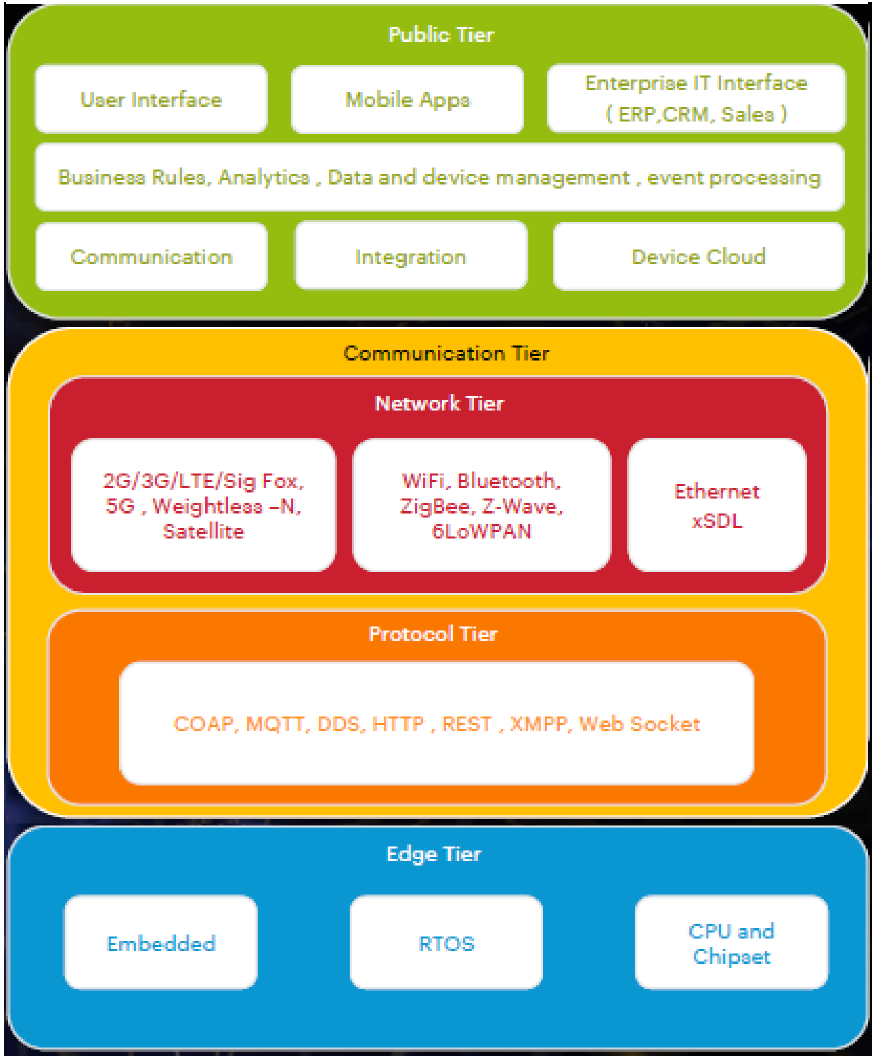


Connected Home

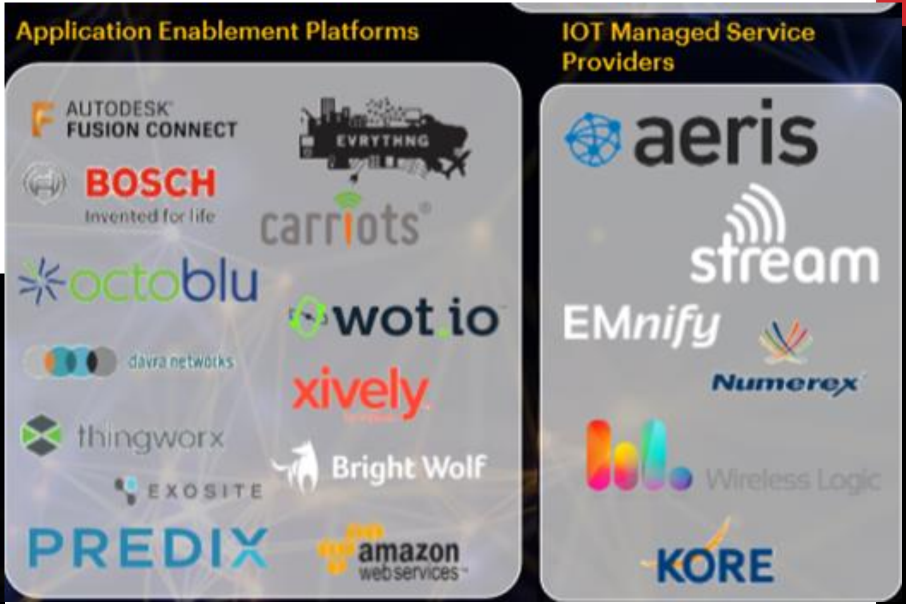
Key Challenges for Edge & IoT Platform Selection

- Multiple large and small vendors providing Edge & IoT platform and it's related technology stack elements. Hence vendor selection becomes confusing.
- No single Edge & IoT cloud platform has offering coverage of all technology stack. Enterprises are forced to get into long term contract with multiple vendors for building Edge & IoT project business requirements
- Enterprises getting into a Edge & IoT cloud platform usage agreement will see the center of Edge & IoT data processing and aggregation needs to be distributed as appropriate, with no relation on how platform capabilities distributed between cloud services and on-premises gateways or devices
- Edge & IoT devices are assets that must be managed along their 10+ years lifecycles. This introduces challenges regarding multiple versions of hardware/software/protocols to a larger scale.

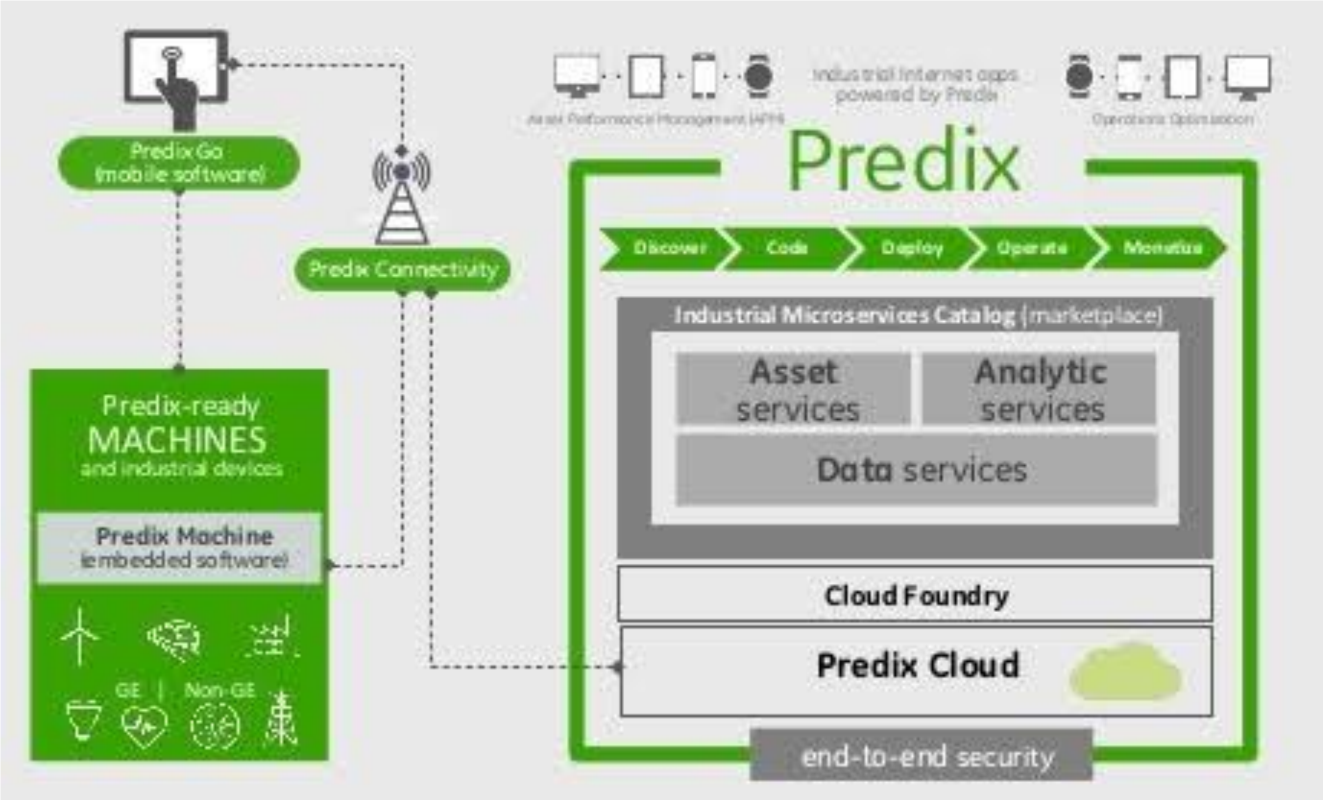
Edge & IoT Architecture Pattern



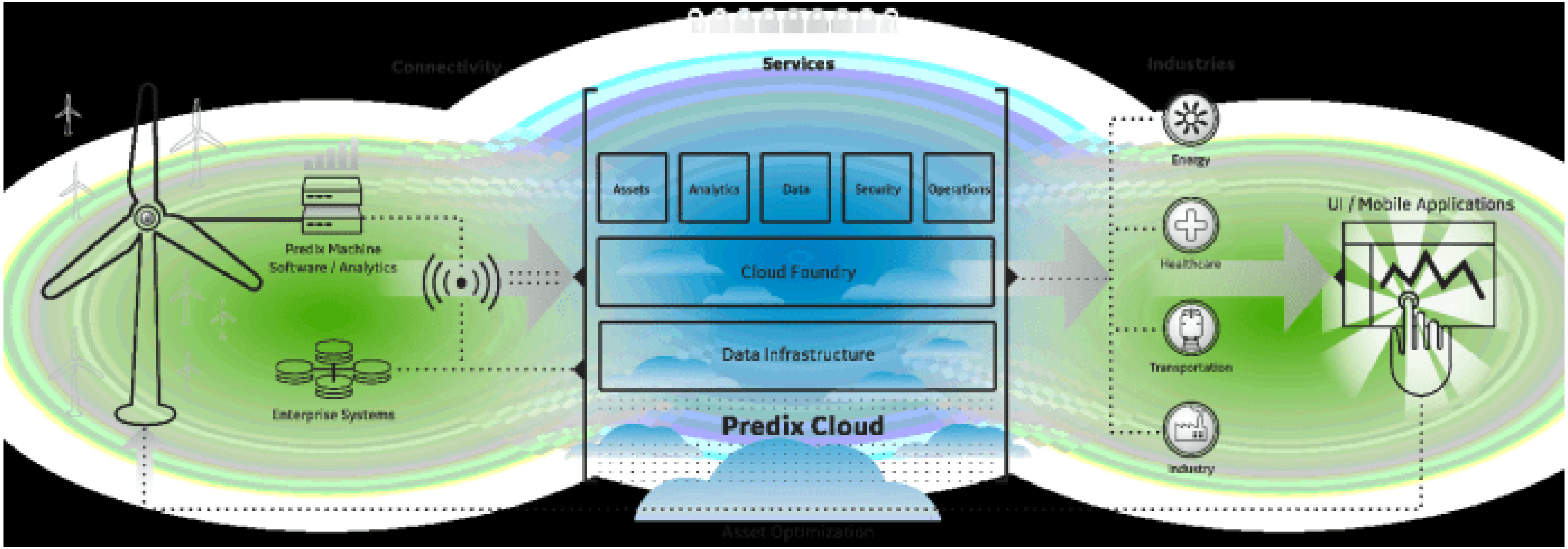
Edge & IoT Platform & Provider Categorization



Platforms: GE Predix DevOps Architecture



Platforms: GE Predix Cloud Architecture



Platforms: IBM Bluemix Edge & IoT

IBM continues to evolve its IoT offerings, from its 2014 launch of Bluemix IoT Foundation to its current Watson IoT portfolio. It has seminal experience in technologies, protocols and platforms, such as Node-RED, MQTT and Cloud Foundry, as well as a portfolio of applications. IBM sees that the IoT value for customers is a story of data analytics and cognition helping clients make better decisions.

IBM Bluemix – IBM's cloud platform-as-a-service (PaaS) launched in 2014 – is based on open source Cloud Foundry software running on IBM's Soft Layer infrastructure hosted in 46 data centers worldwide.

End users can leverage a local or cloud-based discrete portfolio of elements, which starts with the Bluemix IoT Zone and continues with options that include solutions for manufacturers (Product Line Engineering, Rhapsody and other apps); asset management solutions (for example, Maximo Asset Management and Tririga); and its cloud capabilities (SoftLayer, an IBM Company, for IaaS and IBM Watson for cognitive analytics).

Platforms: IBM Bluemix Edge & IoT – Where to Use

Platforms: IBM Bluemix Edge & IoT – Partnerships

Key partners include Cisco; Arrow Electronics and National Instruments for hardware; Orange and Verizon for communications; Cloud Foundry and Cisco Jasper for software; and IBM GBS, HCL Technologies and Deloitte for services.

Platforms: Azure Edge & IoT

Azure IoT Hub, available since February 2016, enables customers to connect, provision and manage IoT devices from the cloud, using open-source device SDKs for platforms including Linux, Windows and real-time operating systems.Microsoft's Azure IoT Suite is a collection of Azure services, including IoT Hub, Stream Analytics, several data stores and a dashboard service. Azure IoT Hub is the only service in the suite designed specifically for IoT; the other services are also available directly. Windows 10 IoT (formerly Windows Embedded) software enables development of local device management applications, as well as connectivity to the back-end cloud services, including Azure IoT services. Azure IoT SDK is open source software that enables devices and gateways to connect back to the Azure IoT Hub. Finally, the Azure Logic Apps provide integration between the Azure IoT Suite and back-end applications (including Microsoft Dynamics, Salesforce, SAP and Oracle), completing the end-to-end model.

Platforms: Azure Edge & IoT – Where to Use

Microsoft is focusing initially on remote monitoring, device management and predictive

- more than 50% Fortune enterprises are running ERPs and CRMs on Microsoft Dynamics AX platform, making Azure IoT the favored choice
- Azure IOT combined with Windows 10 IoT Enterprise brings the capabilities of Windows 10 Enterprise to a wide range of industry devices across retail, manufacturing, health, finance and other industries.
- Azure IOT integrated with Windows IOT core is optimized for smaller and lower cost industry devices ranging from IoT gateways to micro-kiosks.
- Microsoft existing eco system and cloud infrastructure (companies using Microsoft products) enables Azure IOT to get more deeper usage – As a public cloud platform

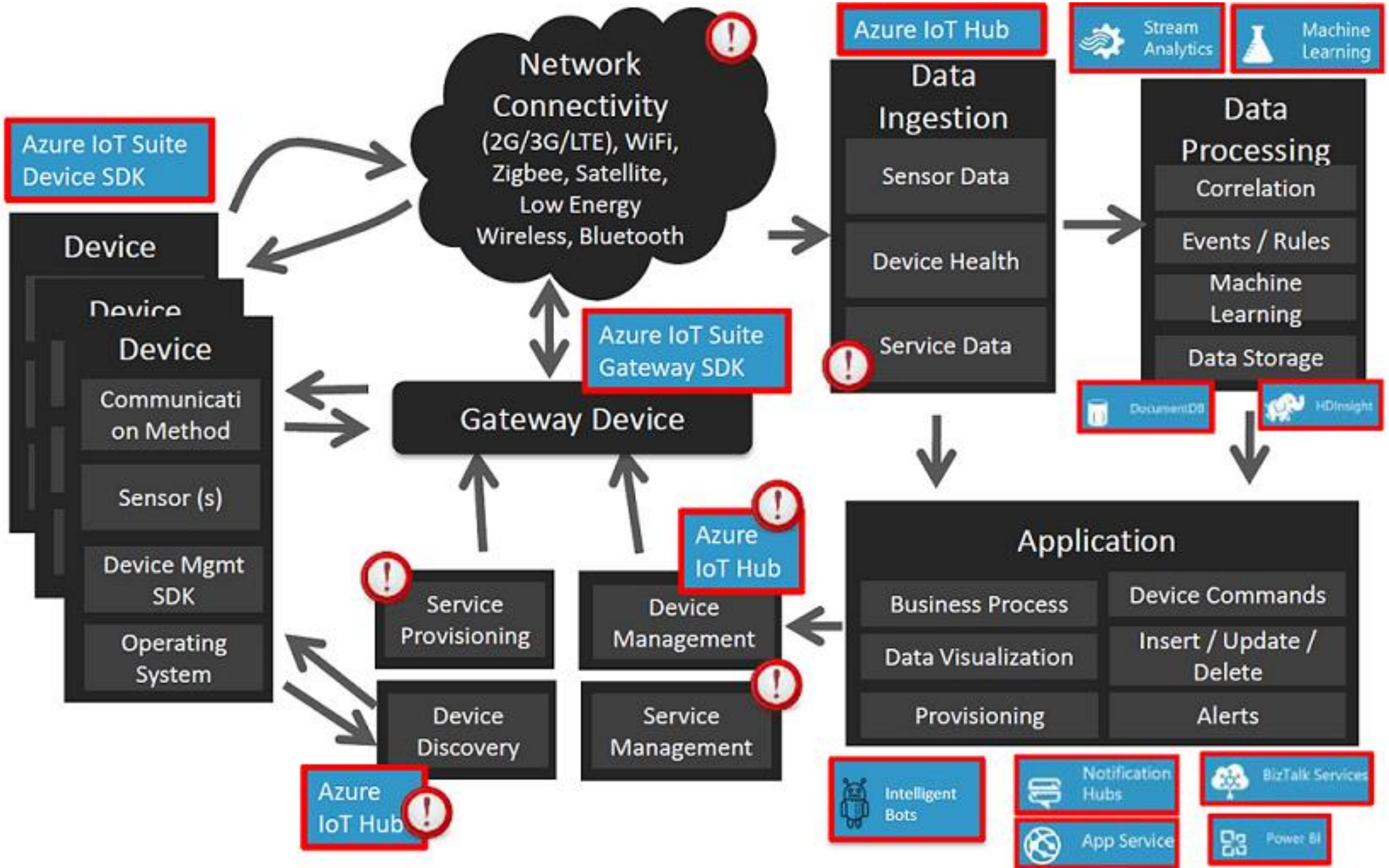
Platforms: Azure Edge & IoT – Partnerships

IIOT Platform vendors partners with Azure IOT to give leverage of both Commercial and Industrial solutions

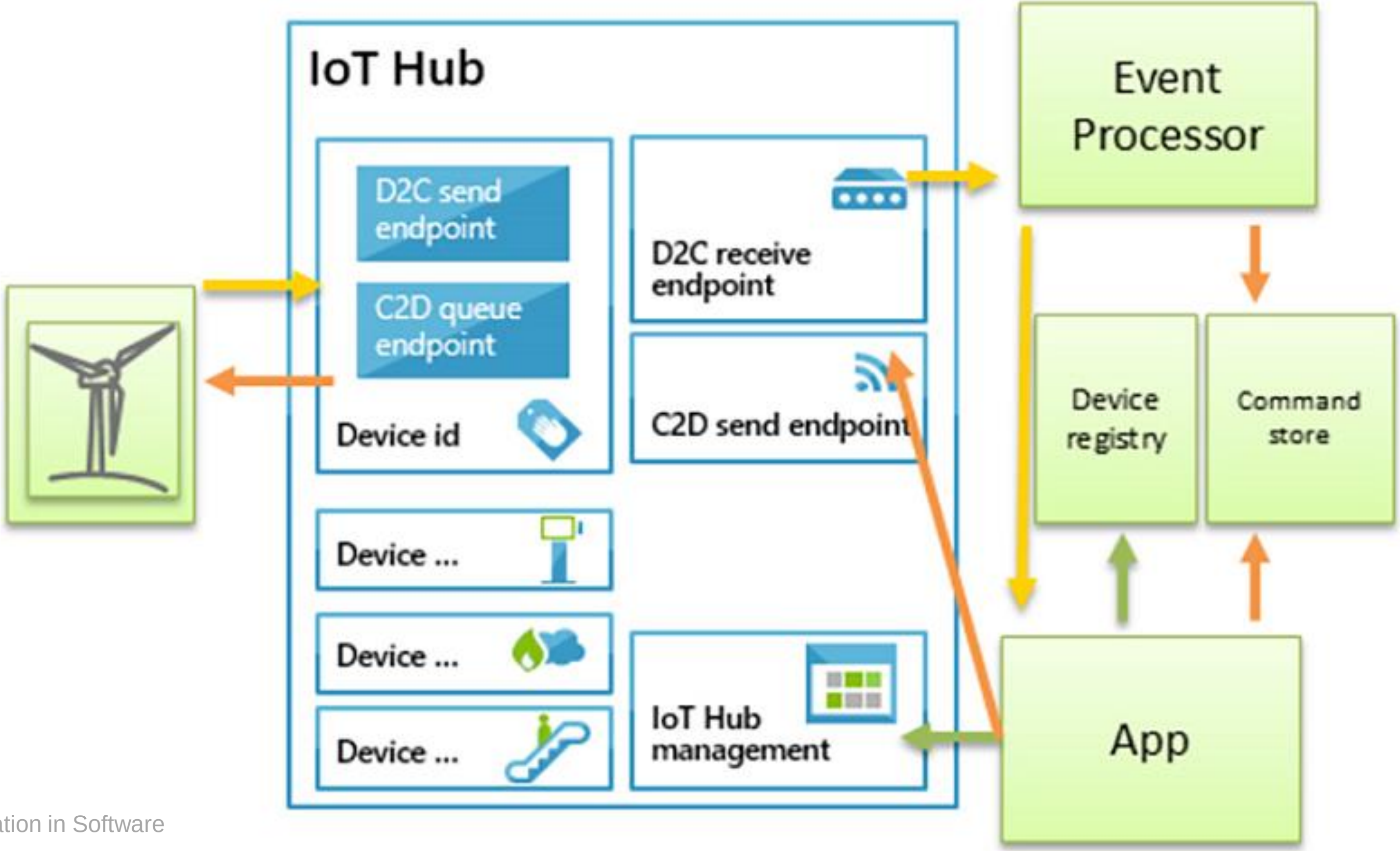
- GE Predix partners with Microsoft Azure Cloud
- PTC ThingWorx partners with Microsoft Azure cloud

Microsoft Edge & IoT Services and Patterns

Anatomy of Edge & IoT with Azure



Azure Edge & IoT Hub Platform Flow



Platforms: AWS Edge & IoT

Amazon Web Services (AWS) is a subsidiary of Amazon launched in 2006 that focuses on a wide variety of cloud computing services. AWS is the leading provider of cloud infrastructure services (IaaS).

- AWS IoT is a cloud-based process pipeline priced in proportion to the traffic. The services in the pipeline includes AWS IoT message broker (or Device Gateway), AWS IoT rules engine, Device Shadows, Device Registry and IoT Console services.
- The message broker is the device-facing portal point for IoT interactions; the rules engine directs processing of the incoming signals to a variety of AWS targets, including Device Shadows, Lambda, DynamoDB, Kinesis and so forth.
- The Device Shadows implements the "digital twin" architecture representation of the device state and encapsulates communications via REST APIs. The AWS IoT process is designed for mainly AWS's offering stack: for the edge, AWS offers only a communication SDK; back-end application and SaaS connectivity are possible only via Lambda functions and Kinesis data services..

Platforms: AWS Edge & IoT– Where to Use

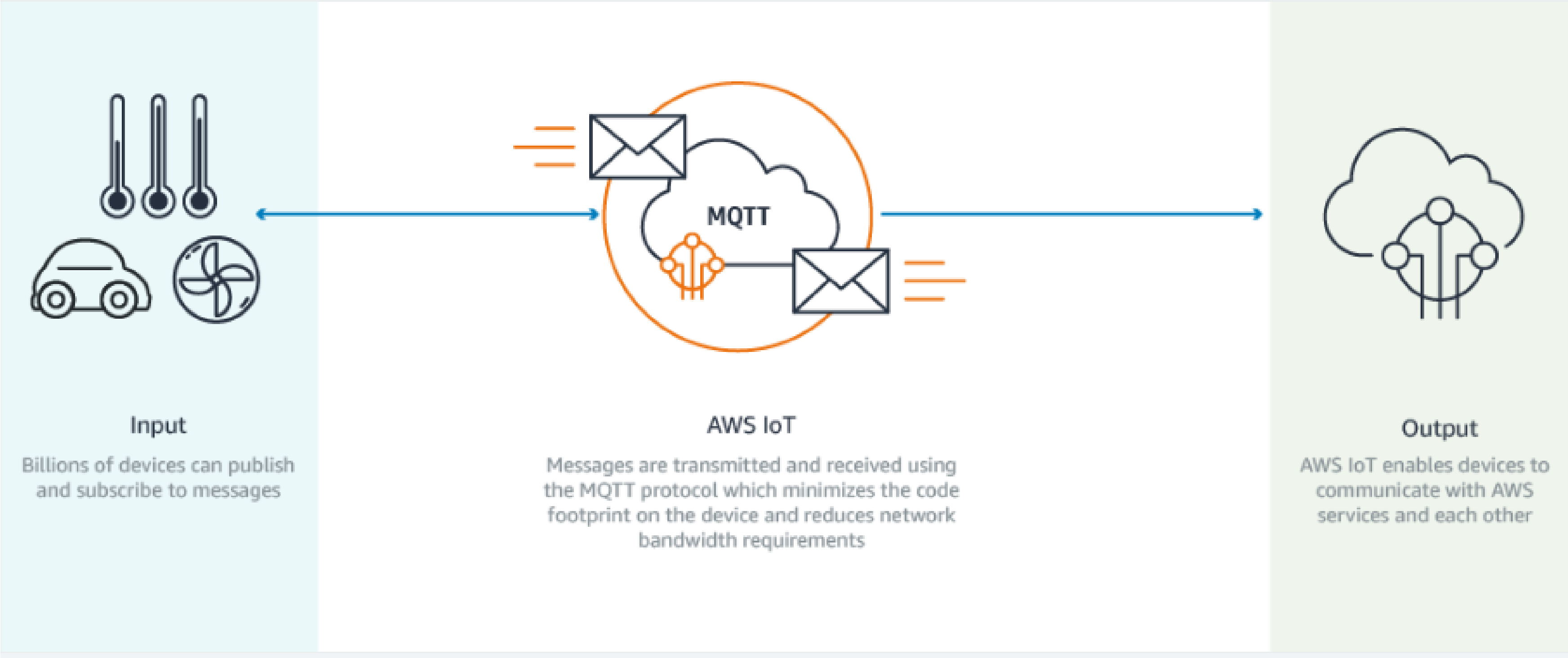
AWS IoT is a cloud centric platform for connecting devices to AWS Services, as well as other cloud services and devices.

- AWS IOT is mainly helps formed small and mid size companies to move farther and faster than they ever could before.
- Amazon is focused on generic computing services. It has enabled the creation of many applications and specialized services, but these all must be centrally located and offered over the network.
- AWS IOT device gateway scales automatically to support over a billion devices without provisioning infrastructure
- AWS IoT platform is very good for consumer and wearable applications, limited scope (still evolving) for predictive maintenance and optimization applications for wind farms, oil pumps, jet engines, or rotating equipment in general

Platforms: AWS Edge & IoT– Partnerships

- Partners include Intel, Microchip and Samsung for hardware,
- Splunk,PTC,C3IOT and Twilio for software,
- and Accenture and Deloitte for services.

Platforms: AWS Edge & IoT– Core



Platforms: Azure or AWS

MS Azure and AWS are highly rated and adaptable platforms among the many in the market today. Open and voluminous documentation, and a strong developer community make them platforms of choice among the developers for their application development.

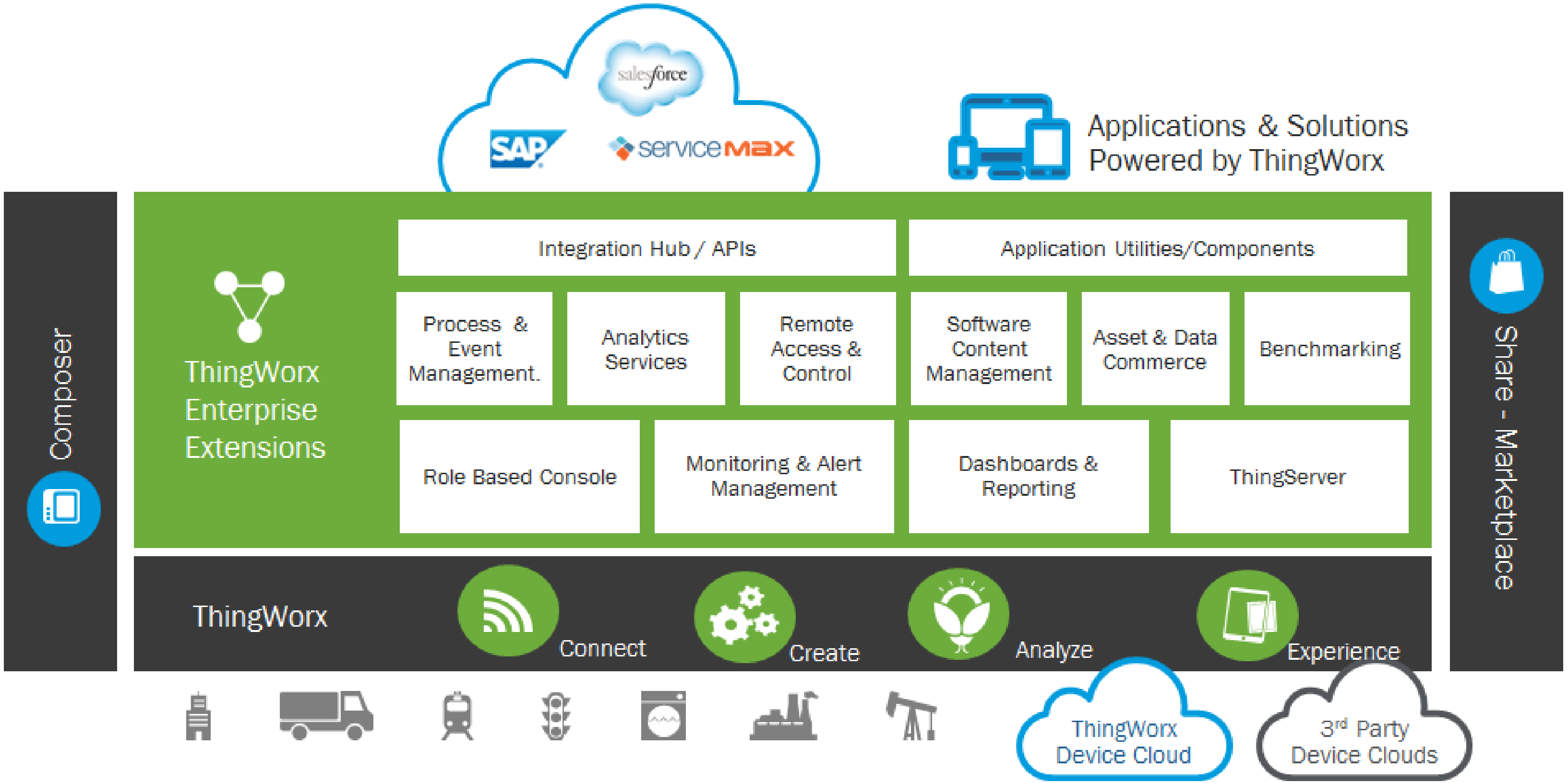
Most enterprise companies irrespective of size and start-ups are leveraging these platforms and hence adoption of a solution developed on Azure or AWS is seamless in comparison to other IoT platforms.

AWS has datacenters located in 14 geographical regions with 56 edge location and Azure has datacenters located in 30 geographical regions.

Another, very important and less obvious advantage of using either of these platforms, is the availability of skilled resources. In case of shortage of resources the turnaround time of recruiting and training for these platforms is shorter.

Platforms: PTC ThingWorx

Platforms: PTC ThingWorx Architecture



Platforms: ThingWorx – Where to Use

Platforms: ThingWorx – Partnerships

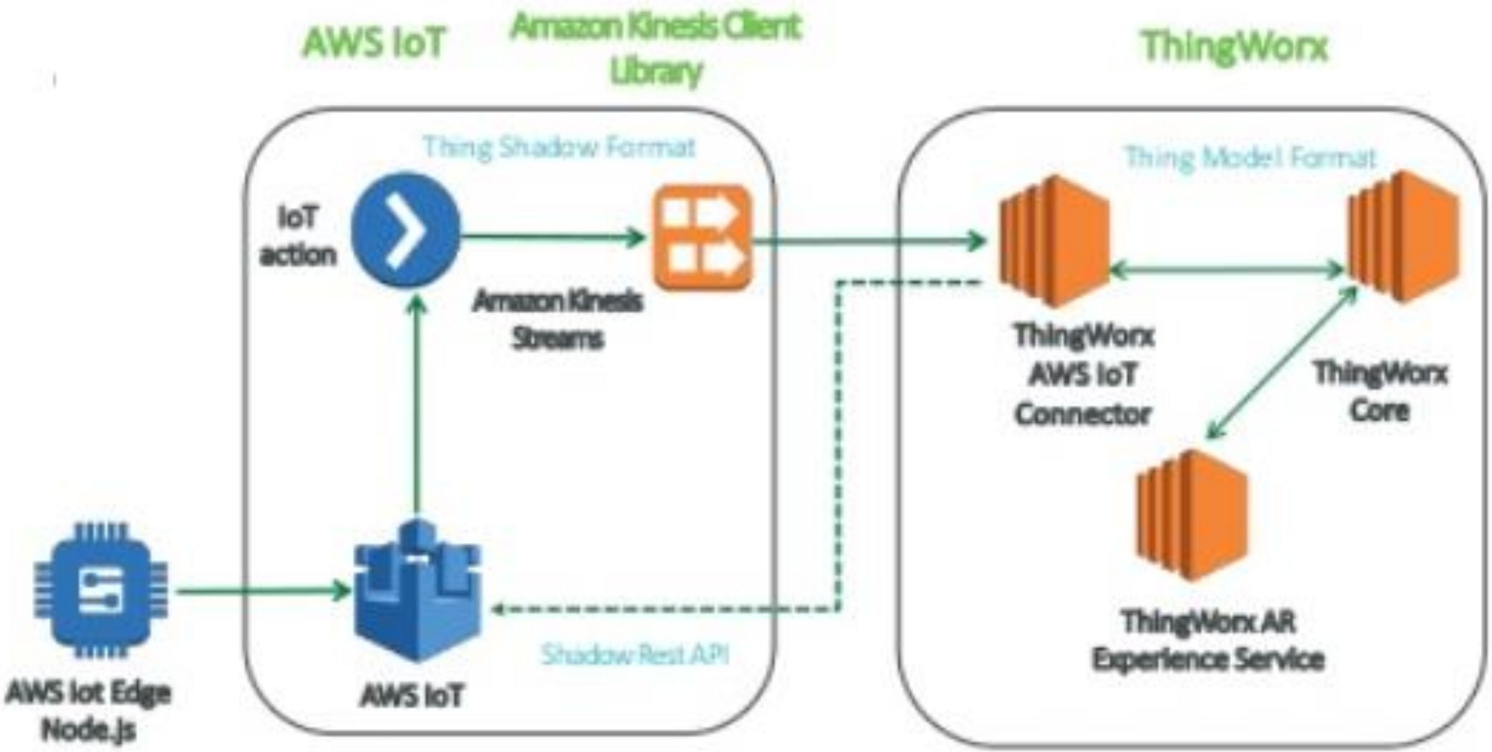
- ThingWorx platform integrates with Amazon Web Services (AWS) IoT, and also fully support Microsoft Azure IoT Hub.
- Independent software vendors like General Electric, ServiceMax and Salesforce use the ThingWorx platform to enhance their existing solutions
- PTC is working with leading communication service providers in all major regions including Altice Group, AT&T, Bell, Deutsche Telekom, Elisa, Etisalat, NTT Docomo, Tele2,Telenor, Telkomsel, Verizon Wireless, KORE Telematics and Stream Technologies.

Platforms: ThingWorx + Predix

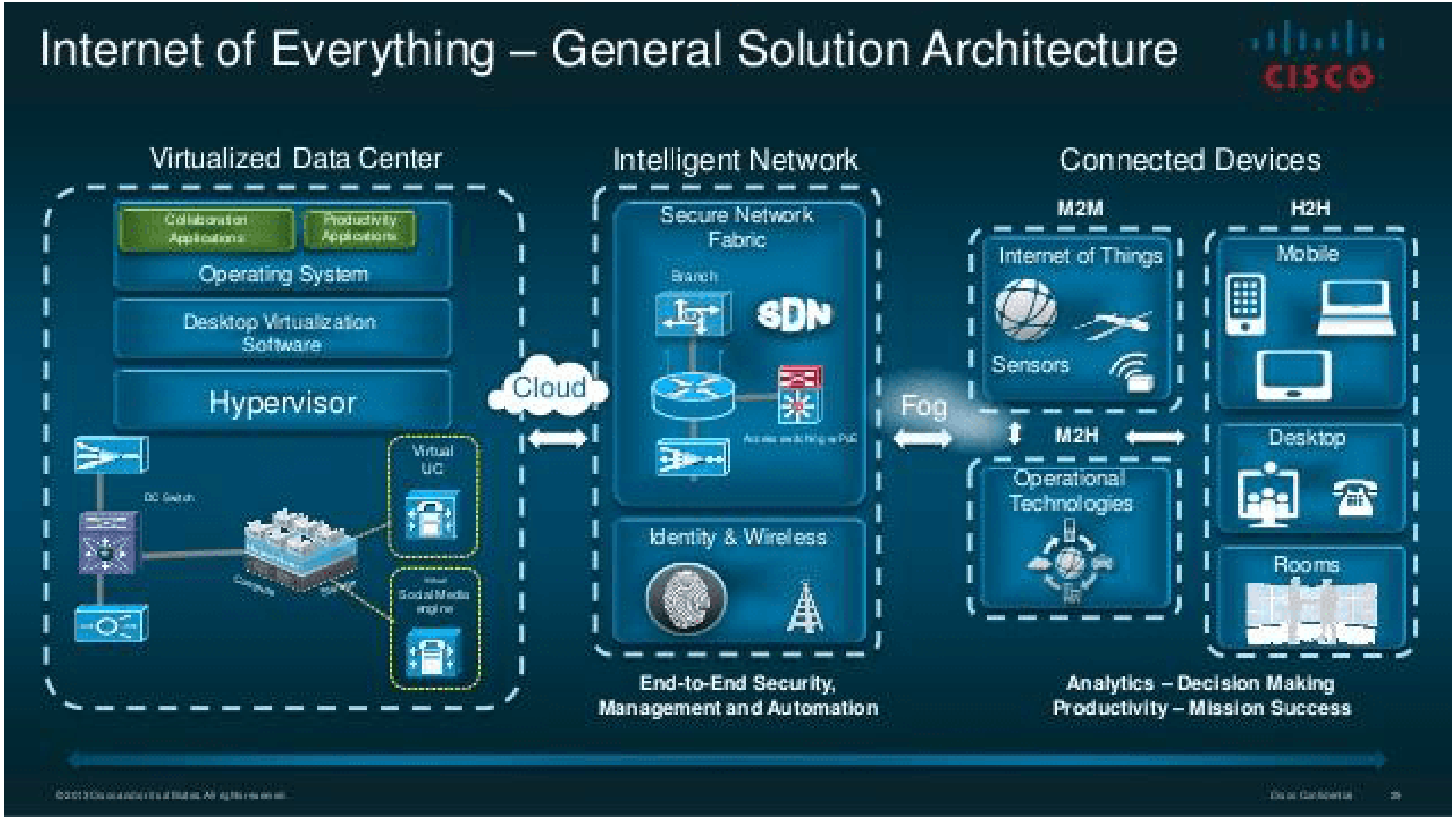
Working with GE, PTC plans to develop an optimized version with elements from its ThingWorx technology suite that would integrate closely with Predix, making it possible for customers to enjoy the full power of ThingWorx along with their Predix system. In turn, GE would deploy 'ThingWorx for Predix' together with Predix for its own internal manufacturing and service processes.

Asset centric industries will benefit with rapid drag-and-drop development of IoT solutions that readily incorporate industrial automation connectivity, machine learning and predictive analytics, remote service, and powerful augmented and virtual reality (AR/VR) experiences.

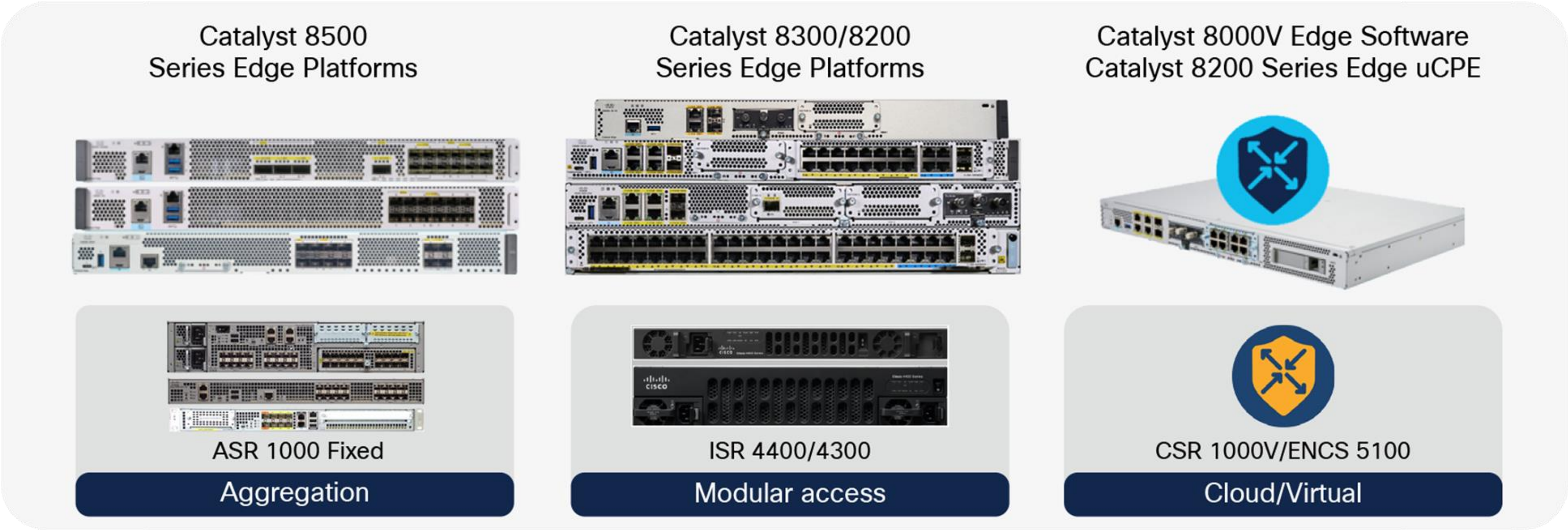
Platforms: ThingWorx + AWS



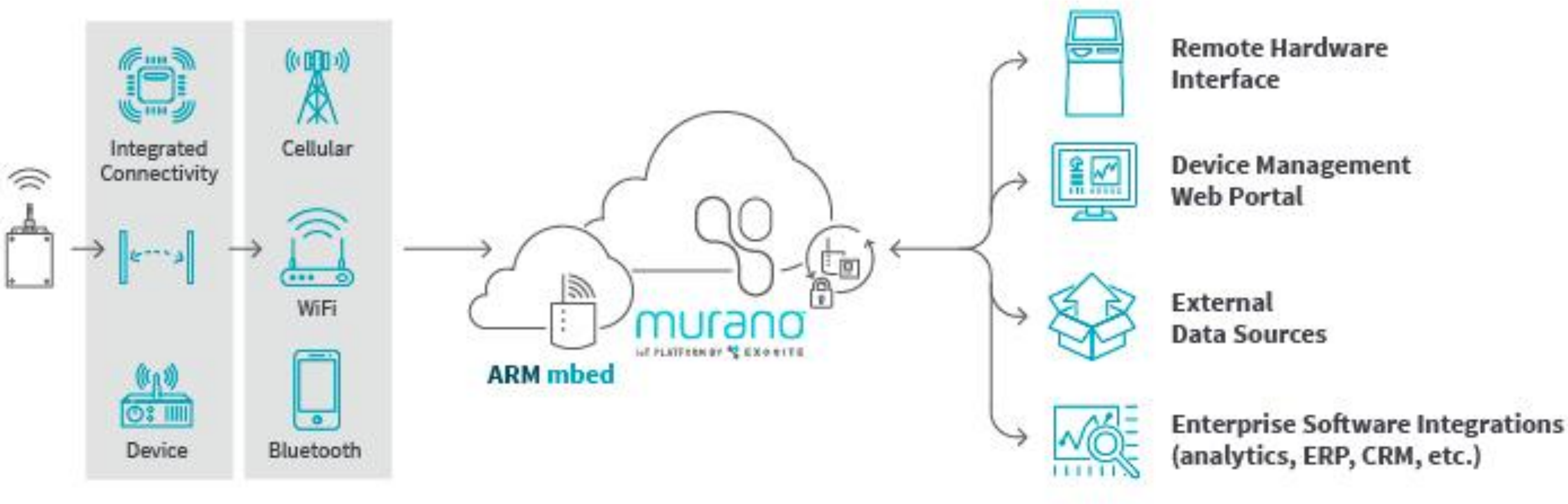
Platforms: Cisco Jasper Edge & IoT/IoE



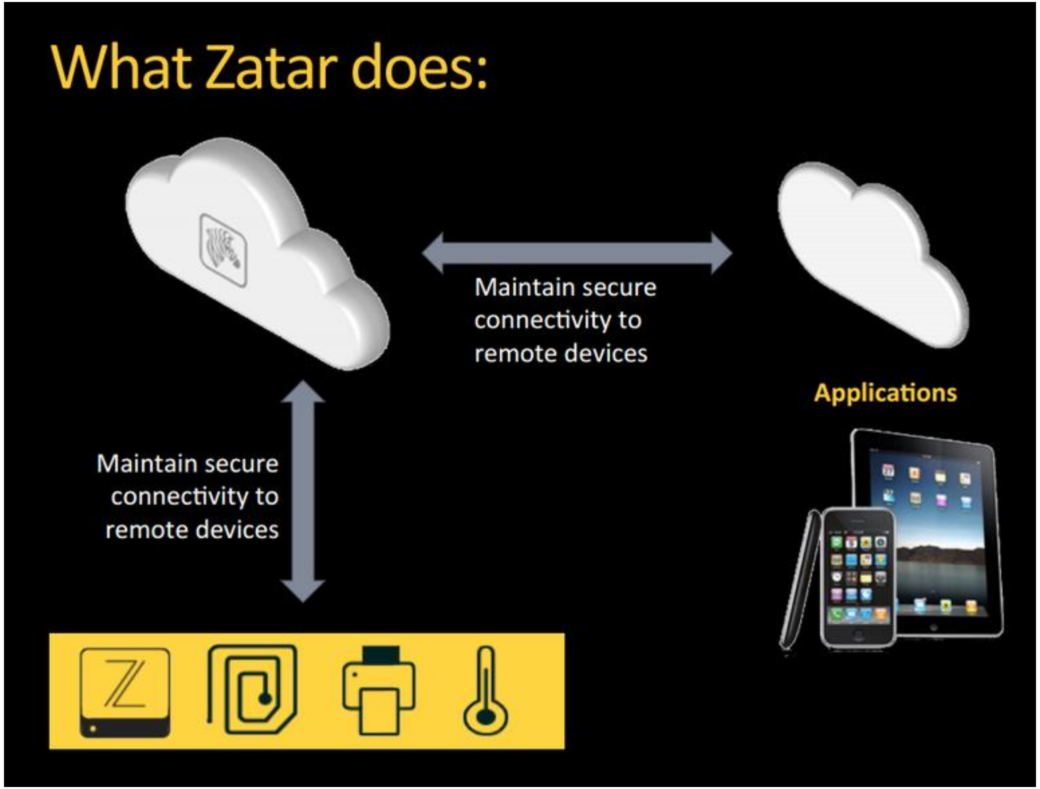
Platforms: Cisco Catalyst Edge



Platforms: Exosite Murano



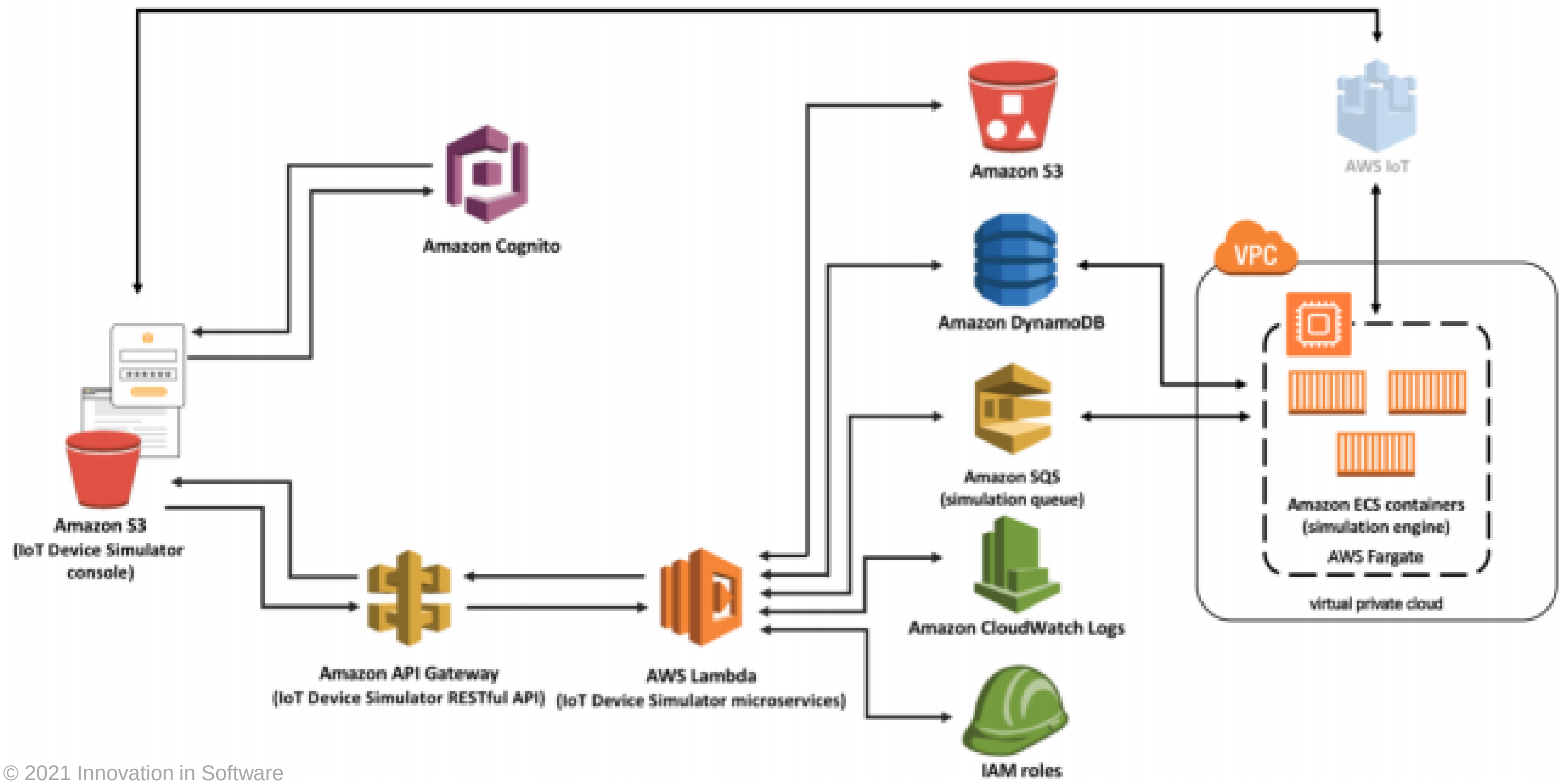
Platforms: Zebra + Zatar



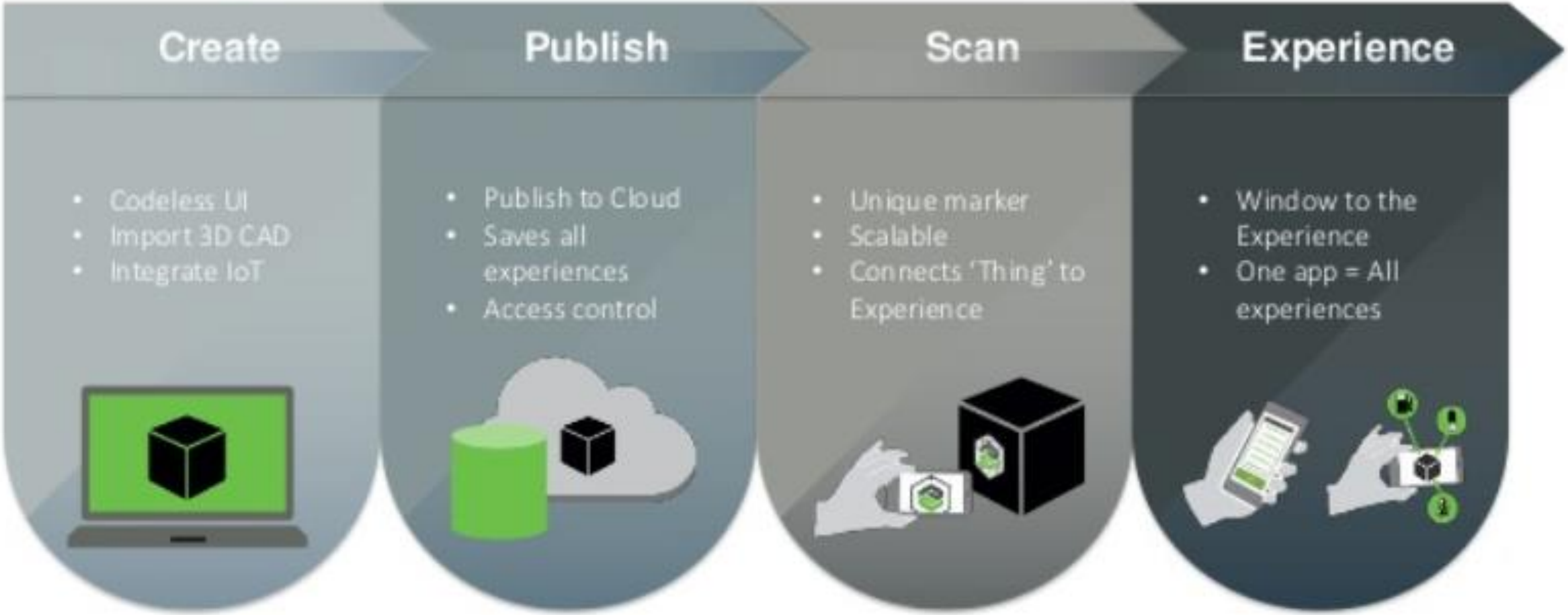
Platforms: Top 5 Edge Platform Companies

	“ Cisco IoT System helps you connect, manage, and control previously unconnected devices. Better secure your physical and digital assets and data. Innovate by creating and deploying IoT applications from fog to cloud. ”
IoT ONE Profile:	http://www.iotone.com/vendor/cisco/v24
	“ Google Cloud Platform gives you the tools to scale connections, gather and make sense of data, and provide the reliable customer experiences that hardware requires. ”
IoT ONE Profile:	www.iotone.com/vendor/google/v36
	“ IBM and its clients are ushering in a new cognitive era. IBM Watson IoT platform extends the power of cognitive computing to the billions of connected devices, sensors and systems that comprise the IoT. ”
IoT ONE Profile:	www.iotone.com/vendor/ibm/v41
	“ The Intel IoT Platform is an end-to-end reference model that works with third party solutions to provide a foundation for seamlessly and securely connecting devices, delivering trusted data to the cloud, and delivering value through analytics. ”
IoT ONE Profile:	www.iotone.com/vendor/intel/v44
Microsoft	“ Azure IoT Suite is a cloud-based offering with preconfigured solutions that address common Internet of Things scenarios, so you can capture and analyze untapped data to transform your business. ”
IoT ONE Profile:	www.iotone.com/vendor/microsoft/v59

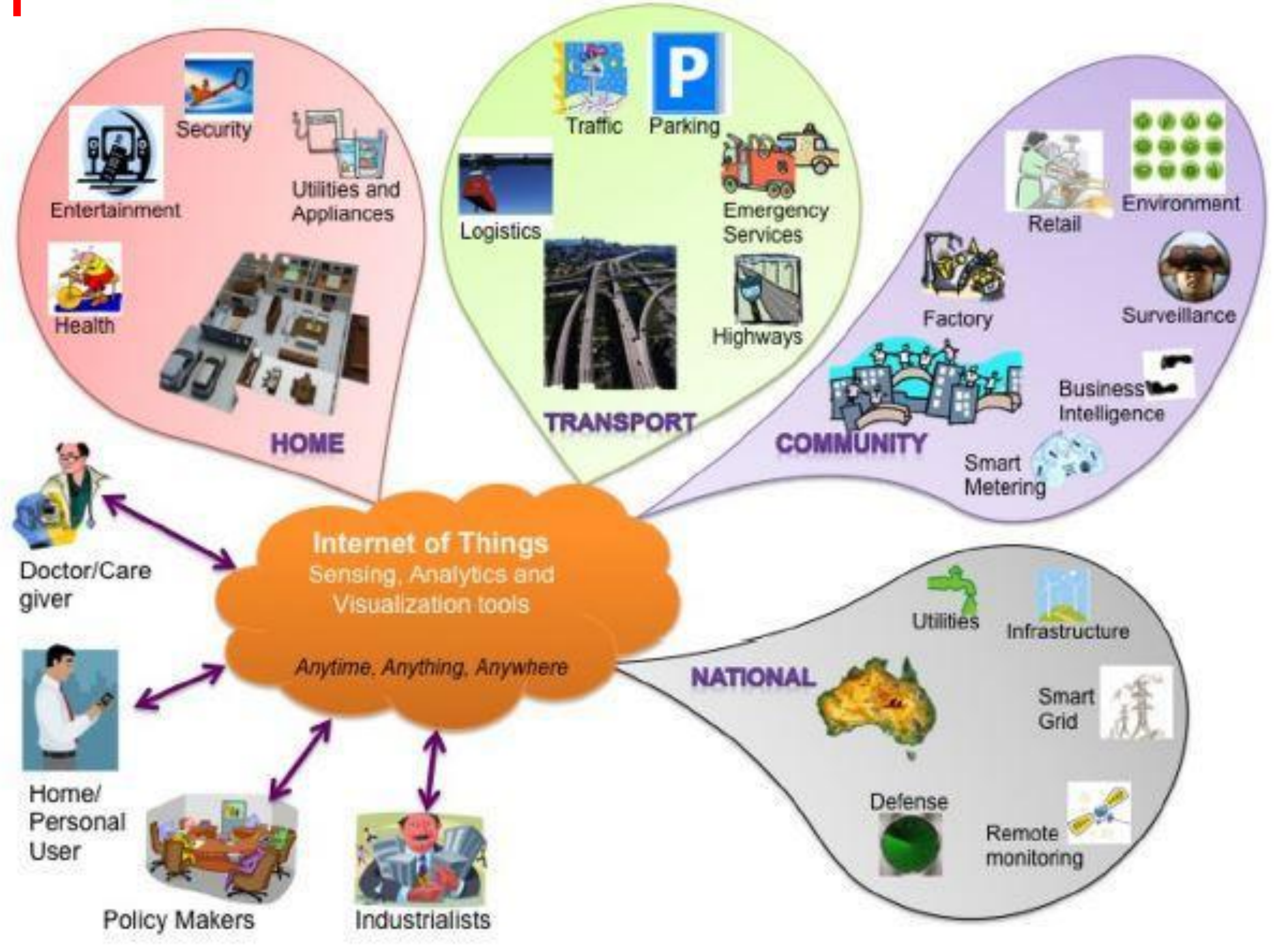
Edge & IoT Device Simulation



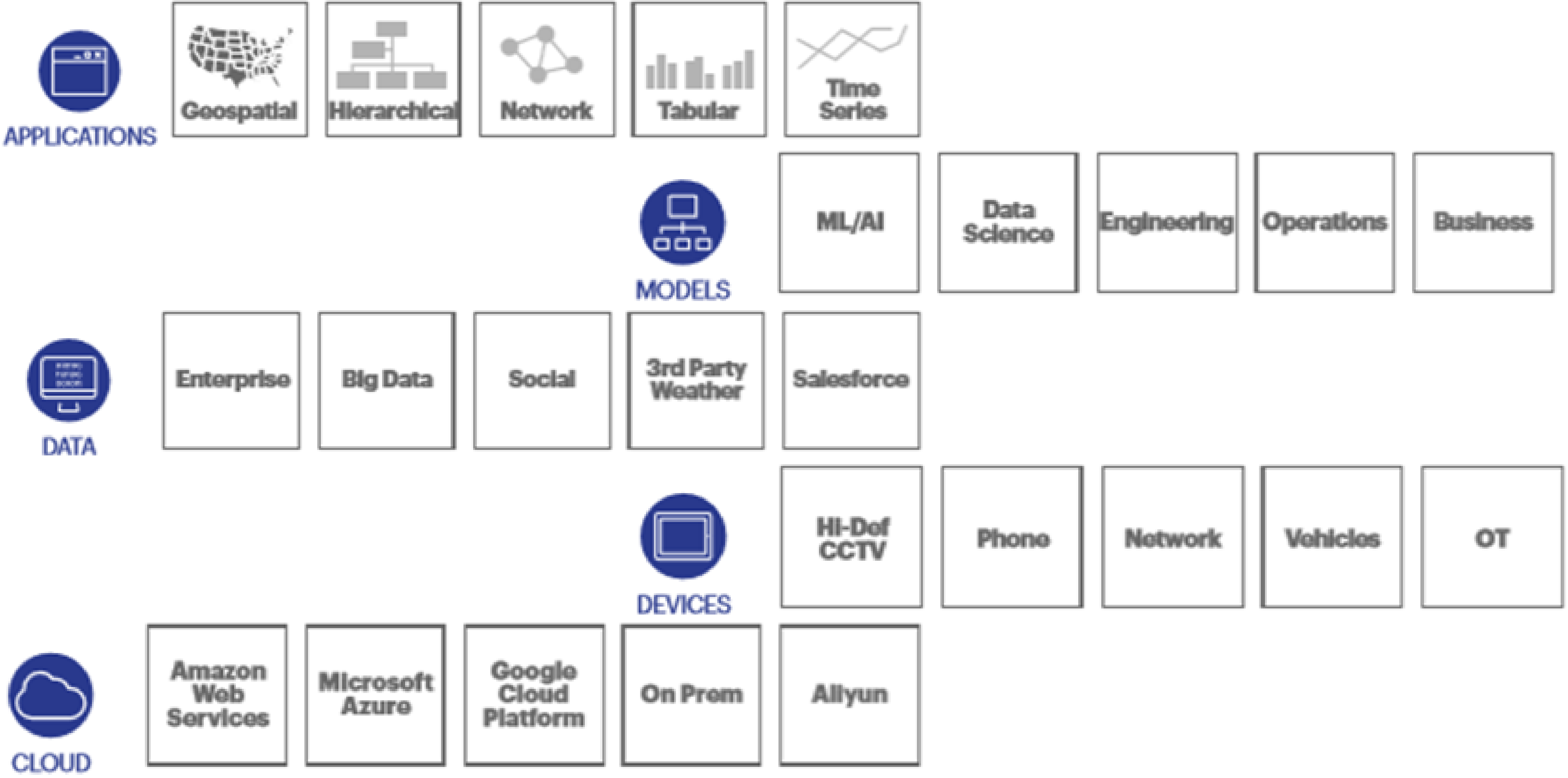
Monitoring, Dashboards, and Visualization



End-user application



Edge & IoT Platform Components

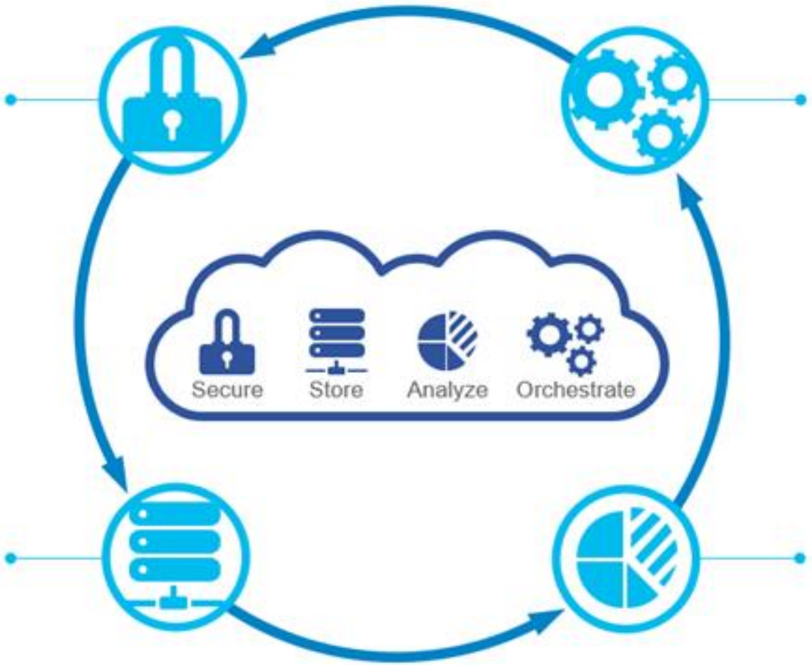


Is Cloud Required for Edge & IoT

A common source of confusion is the assumption that a platform is the same as cloud computing. While an IoT application may use cloud for compute and storage services, it also incorporates higher-level functionality like device management, data and analytical models, business logic, and visualizations, all of which need to work together in a secure and scalable fashion.

Edge & IoT Enabled through Cloud Services

- **Security** is a key consideration in distribution of sensors, devices, user & data management for Edge & IoT
- **Storage** considerations are put under increasing strain from the abundance of information generated and stored from Edge & IoT



- **Orchestration** in cloud is achieved through automated actions based on rule engine sets that include prevention and remediation of issues
- **Analytics** in cloud provide real time analysis of Edge & IoT and users data for identification of patterns that support AI and Machine Learning

Cloud & The Edge Computing & IoT

The cloud provides scalable and cost effective solutions for data storage, analytics, security and process orchestration, and is ideal for Edge & IoT use cases by enabling new business opportunities to be pursued without incurring the cost of licenses, hardware infrastructures or maintenance that conventional solutions entail.

USER

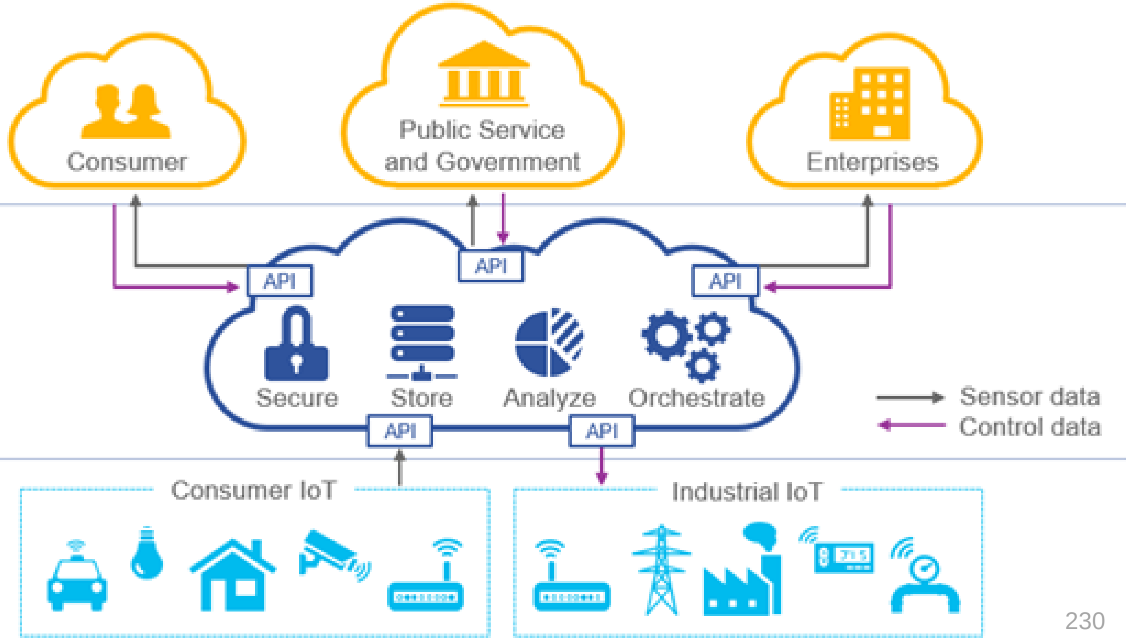
- Monitor
- Insight & awareness
- Control

CLOUD

- Security
- Storage
- Analytics
- Orchestration

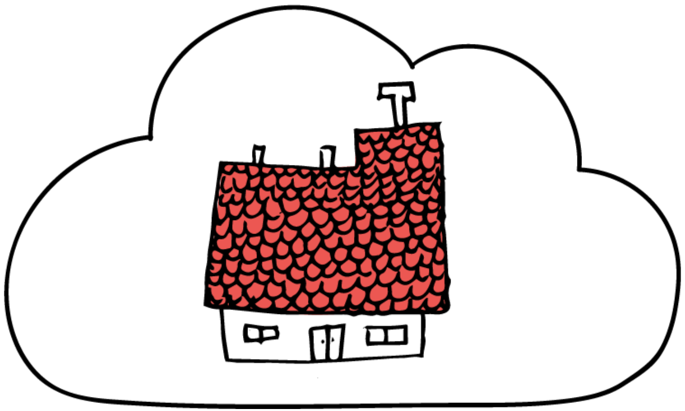
EDGE

- Generate data
- Limited storage and processing capabilities



Moving to the Cloud

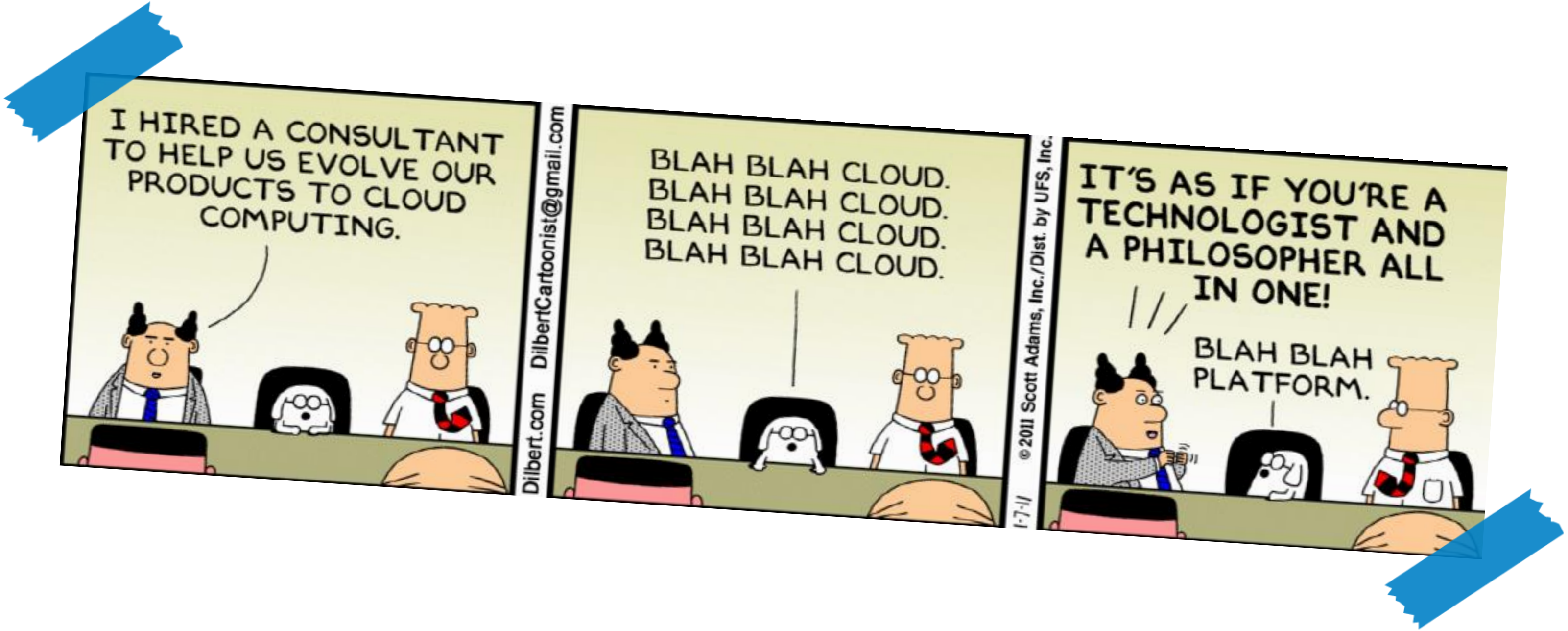
- While Cloud computing (using Cloud vendor's data centers) is, in many aspects, similar to what you do on-premise, there are nuances, however, that may make the process of moving to the cloud costly, if not frustrating
  - Moving to Cloud computing is a paradigm shift
  - It is also an opportunity to undertake application modernization initiatives
- You need to educate yourself about Cloud's intricacies, learn and adopt best practices for designing and implementing Cloud applications, and, of course, make the right technological choices
- Down the road, it is all about making your business successful and your technological choices must be aligned with the business objectives of your organization



Cloud Kickstart

- There are certain steps you need to follow in order to make moving to the Cloud as painless as possible
- It is not possible to touch on all the steps each organization, line of business or team would need to consider, but here are some of the more common first broad directions:
  - Create a Cloud app from scratch (Green field)
  - Migrate an existing on-premise app (Brown field)
- What are your priorities for Cloud-native application modernization
- What Cloud service models (IaaS, PaaS, or SaaS) are you already using to accelerate business value?
- What are your vendors and channel partners doing with Cloud?
- What is the current capabilities in the organization and have you created a Kaizen skills map?

Deep Thoughts on Cloud from Scott Adams



Agile Cloud Provisioning

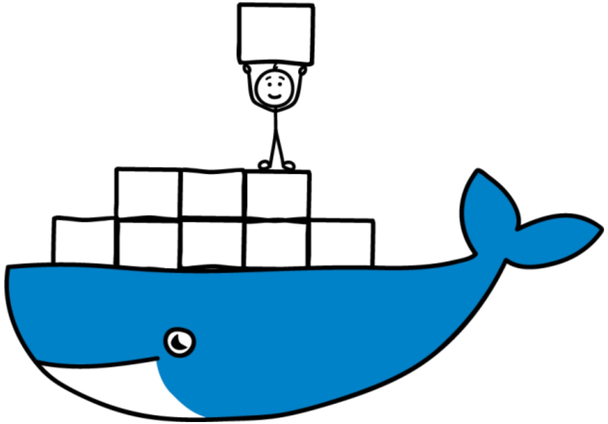
- There are evolving Cloud standards for platform, service, and infrastructure
- Organizations can adopt vendor-specific or vendor agnostic views of Cloud, e.g. “We use AWS”, or “We use a solution that makes us provider agnostic”
- To avoid the vendor lock-in situation (for both IaaS and PaaS deployments):
  - Try to use as much of the open and accepted standards to achieve and maintain system interoperability. For example, for web services use
    - Basic Profile 1.0 compliant web services
    - RESTful services (wherever practical, favor them over WS-*)
  - Wrap up native platform API in a generic and portable API with dependency injection to plug platform-specific implementation

Virtualization & Containerization: A Tale of Two Technologies

- Both offer multi-tenancy for guests (OSes and applications)
- Virtualization is about translating communication between the hosted OSes and hypervisor
- Containerization is "native" in that containers share the host OS's kernel
- Containers' OS is the same as the hosts' OS
- Virtualization allows to run multiple guest OSes on the same host, while containerization is limited to the OS type the host uses
- Traditional virtualization offers better protection from "rogue" tenants
- Containerization offers higher levels of scaling
- Some specialized systems, like Kubernetes [https://kubernetes.io/], introduce logical grouping of containers for intelligent resource management at massive scale

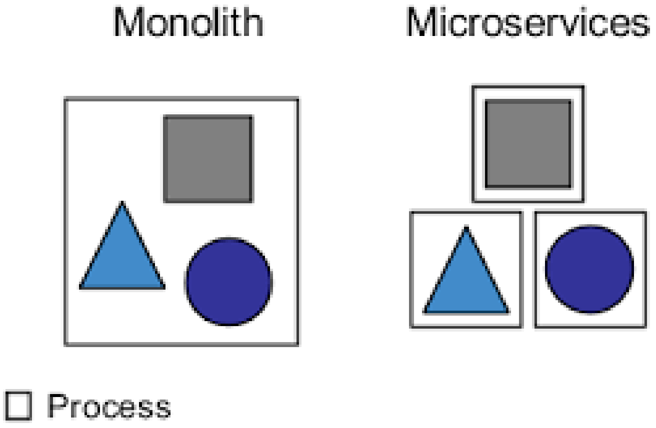
Containerization for Application Componentization and Modernization

- Containers are a lightweight alternative to full machine virtualization
  - It is often called virtualization environment, or OS-level virtualization
  - Docker is a very popular open-source system for creating virtual environments as containers
- A container encapsulates an application running inside its own operating environment which is derived from the underlying host OS
- Containerization has been popularized by cloud-like processing environments that require fast server boot-up time
  - Platform-as-a-Service (PaaS) vendors such as Heroku, OpenShift, and Cloud Foundry use Linux containerization



Microservices In a Nutshell

- Shift Left. Microservices go hand-in-hand with Agile software development methodologies and DevOps.
- Competitive Advantage. Clean, well managed services improve agility and velocity.
- Technology Enabled Business. Time to market and value is enabled by a componentized application, built on the principal of MVP.
- Gold Master. Every organization needs their reference architecture and working examples to simplify consistent adoption across the enterprise.



Dynamic Infrastructure Examples

- AWS CloudFormation service
  - Simplifies provisioning and management on AWS using templates
- Azure Resource Manager and Quickstart templates
  - Allows you to provision and manage your applications along with Quickstart template.
- Pivotal Cloud Foundry
  - Allows you to provision your applications along with their dependencies using a declarative template
- Terraform
  - Allows you to provision your applications along with their dependencies using IaC templates.
- Configuration Management Tooling
  - Chef, Puppet, Ansible and Salt all provide dynamic infrastructure creation.

Edge & IoT Sensors

History of Sensing

- Today sensors are everywhere. We take it for granted, but there are sensors in our vehicles, in our smart phones, in factories controlling CO2 emissions, and even in the ground monitoring soil conditions in farms.
- Research on wireless sensor networks (WSNs) started back in the 1980s, and was initially focused on military applications
- Edge & IoT applications using sensor networks for industrial and research perspectives, have put renewed emphasis on development of new technology and usages.
- Key to this growth has been the availability of inexpensive, low powered miniature components like processors, radios and sensors that were often integrated on a single chip (system on a chip (SoC))

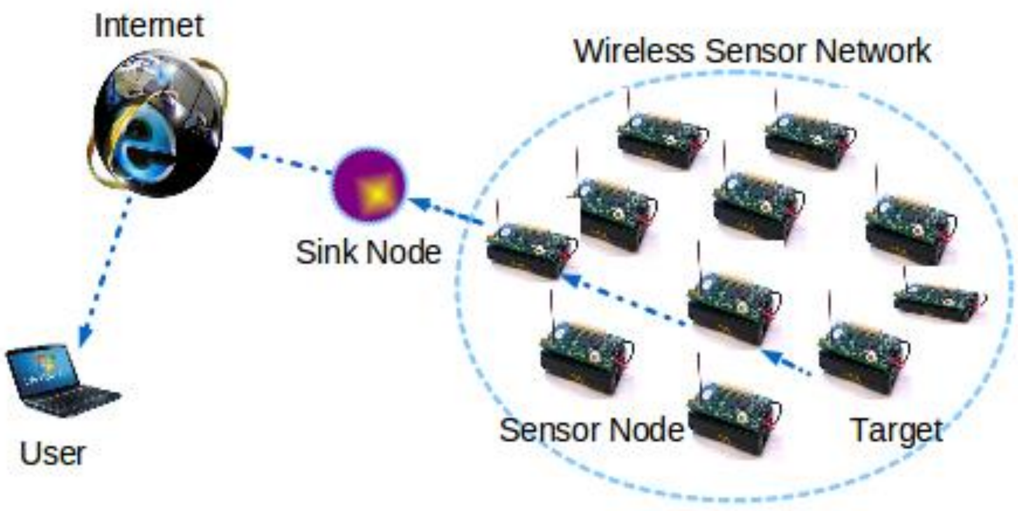
Sensor Technology

- The ability to detect changes in the physical status of things is essential for recording changes in the environment.
- Wireless sensor technology play a pivotal role in bridging the gap between the physical and virtual worlds, and enabling things to respond to changes in their physical environment. Sensors collect data from their environment, generating information and raising awareness about context.
- Sensor Market includes : Micro-electromechanical systems (MEMS) - based sensors, optical sensors, ambient light sensors, gesture sensors, proximity sensors, touch sensors, fingerprint sensors and more

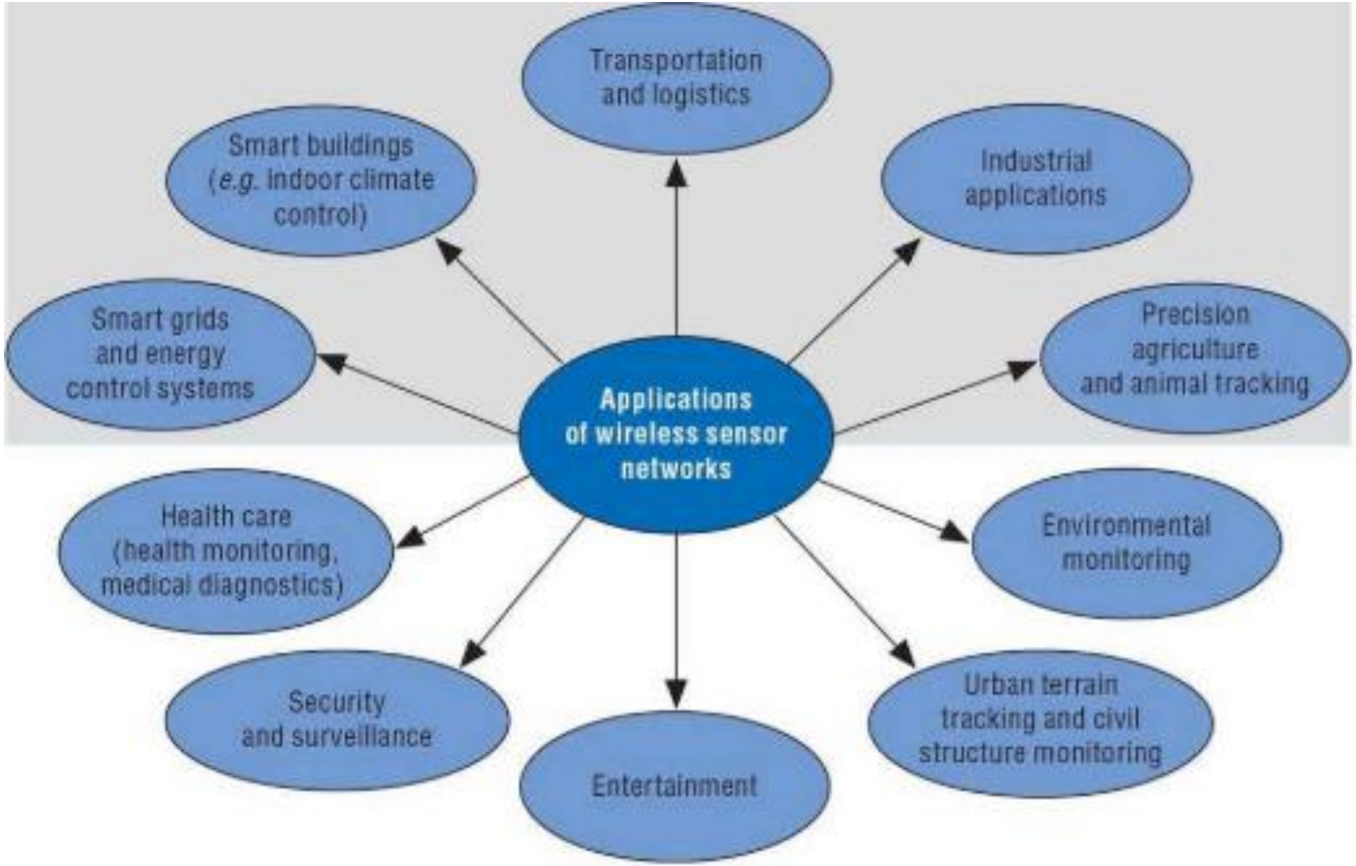
Example: ***sensors in an electronic jacket can collect information about changes in external temperature and the parameters of the jacket can be adjusted accordingly***

Wireless Sensor Networks (WSN)

- A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet.

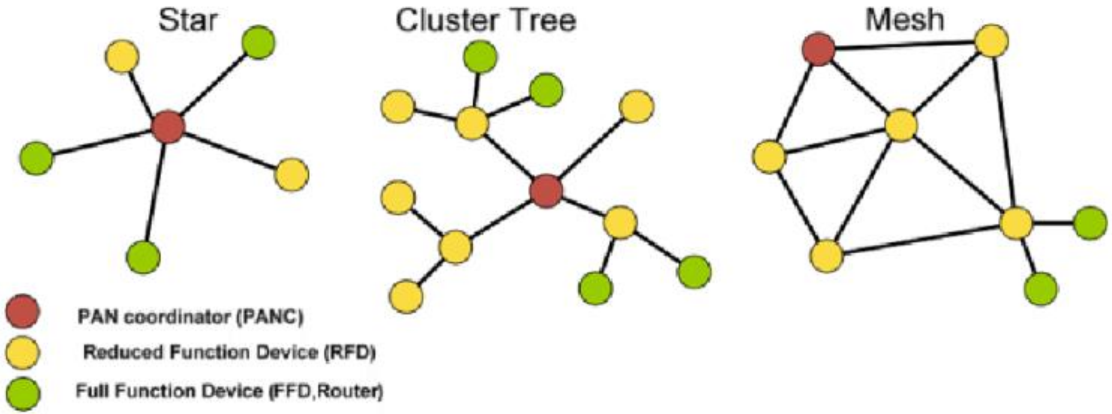


Wireless Sensor Applications



WSN Networking Topologies

- Star - each node connects directly to a gateway. A single gateway can send or receive a message to a number of remote nodes.
- Tree - each node connects to a node that is placed higher in the tree, and then to the gateway.
- Mesh - allows transmission of data from one node to another, which is part of it's broadcast or transmission range.



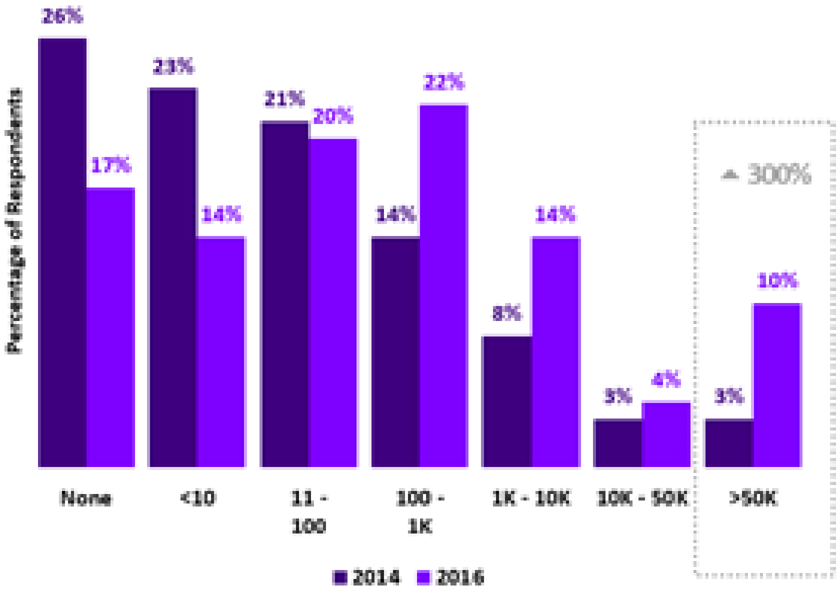
WSN Types

- Terrestrial - consist of hundreds to thousands of wireless sensor nodes deployed either in unstructured (ad hoc) or structured (Preplanned) manner.
- Underground - sensor nodes that are hidden in the ground to monitor underground conditions.
- Underwater - sensor nodes and vehicles deployed under water.
- Multimedia - tracking and monitoring of events in the form of multimedia, such as imaging, video, and audio.
- Mobile - networks consisting of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment.

Sensors in Manufacturing

THE VOLUME OF WIRELESS SENSOR DEVICES IN PLANTS HAS INCREASED DRAMATICALLY

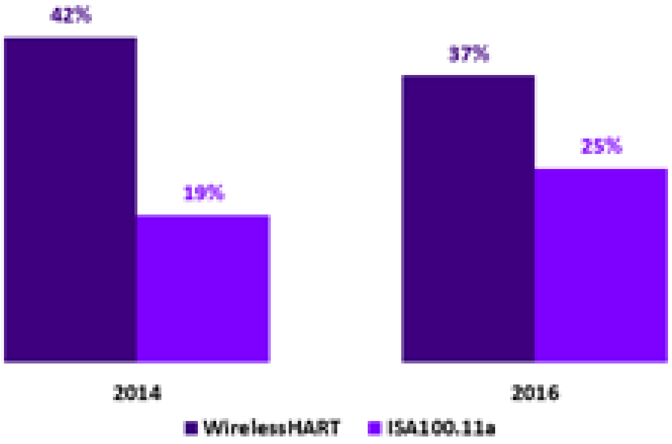
NUMBER OF WIRELESS SENSOR NETWORK DEVICES INSTALLED IN MANUFACTURING SETTINGS, 2017, N = 400



WIRELESSHART & ISA100 ARE THE MOST COMMON SENSOR MESH PROTOCOLS IN FACTORIES

- WirelessHART and ISA100.11a are short range mesh networking technologies based on IEEE 802.15.4 & specifically designed for field devices in industrial automation environments
- Organisations typically will deploy only one of these technologies. In most cases, preference is a direct result of the organisation's existing vendor alignment for their control system.

INDUSTRIAL WIRELESS MESH STANDARDS ADOPTION [N=400]

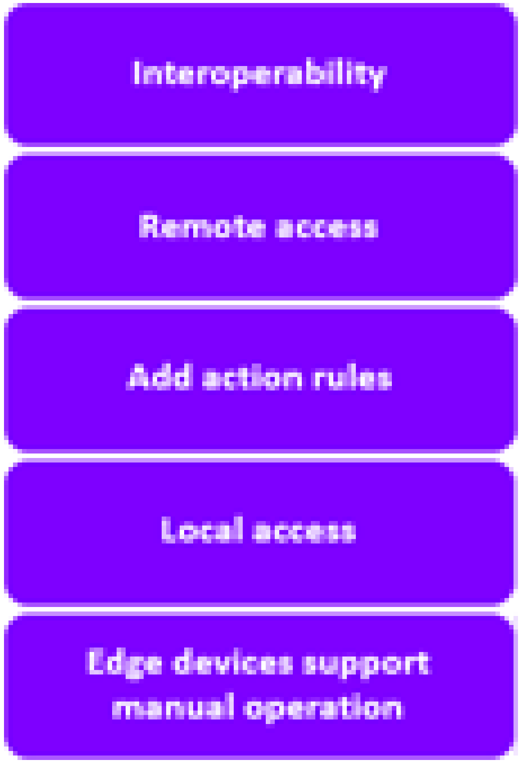


Edge & IoT Communication Protocols

- Protocols designed specifically for Edge Computing & IoT are:
  - CoAP (Constrained Application Protocol)
  - MQTT (MQ Telemetry Transport)
  - ZigBee
  - Z-Wave
  - Bluetooth LE

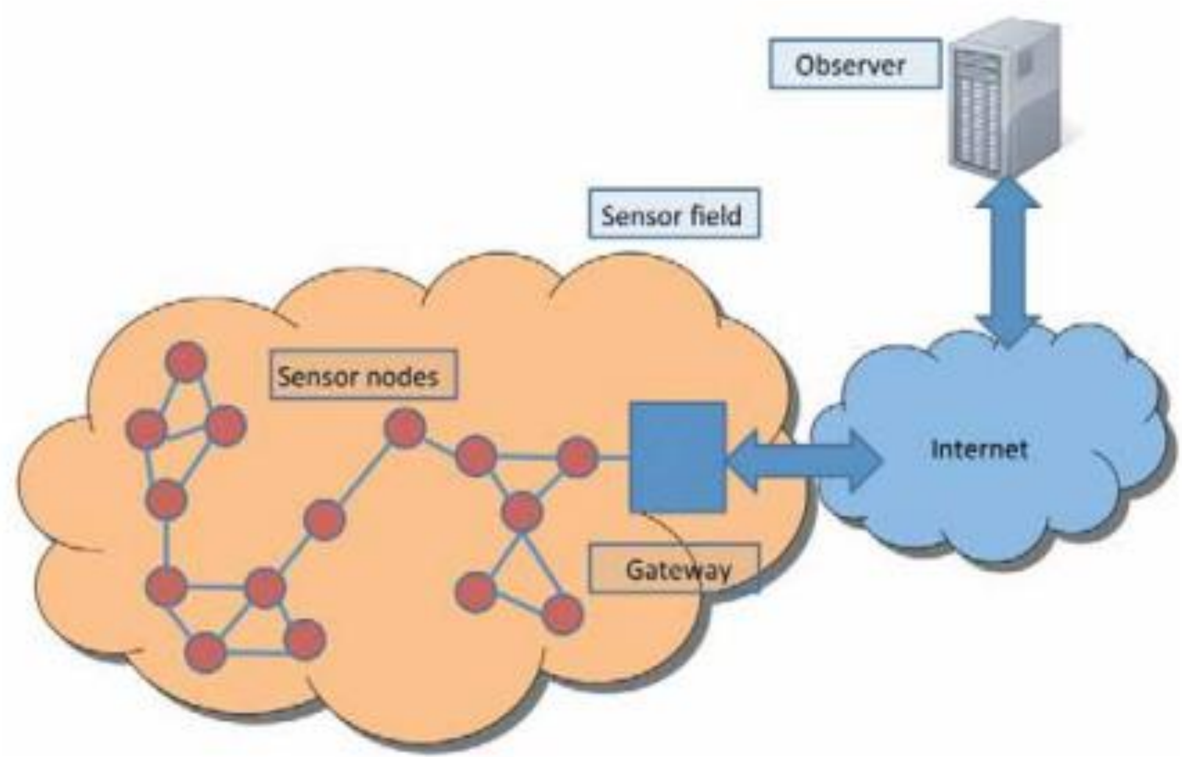
Edge & IoT requires a new Edge Layer which is responsible for being first line of connectivity for devices to connect. The edge Layer is responsible for handling outages and store and forward data.

Sensor Requirements



- The system must be able to interconnect various devices, potentially offered by different vendors and have specific integration
- End users must be able to view/control the state of all connected devices remotely, e.g. via apps running on mobile devices
- End users must be able to create rules to trigger actions based on the state (update) of their environment. e.g. turn off lights in a room when there is no movement by motion sensors in the room for 10 minutes
- End users must be able to control the connected devices within their local network if the connection to the Internet network is broken
- End users be able to operate all connected devices manually using their physical interfaces

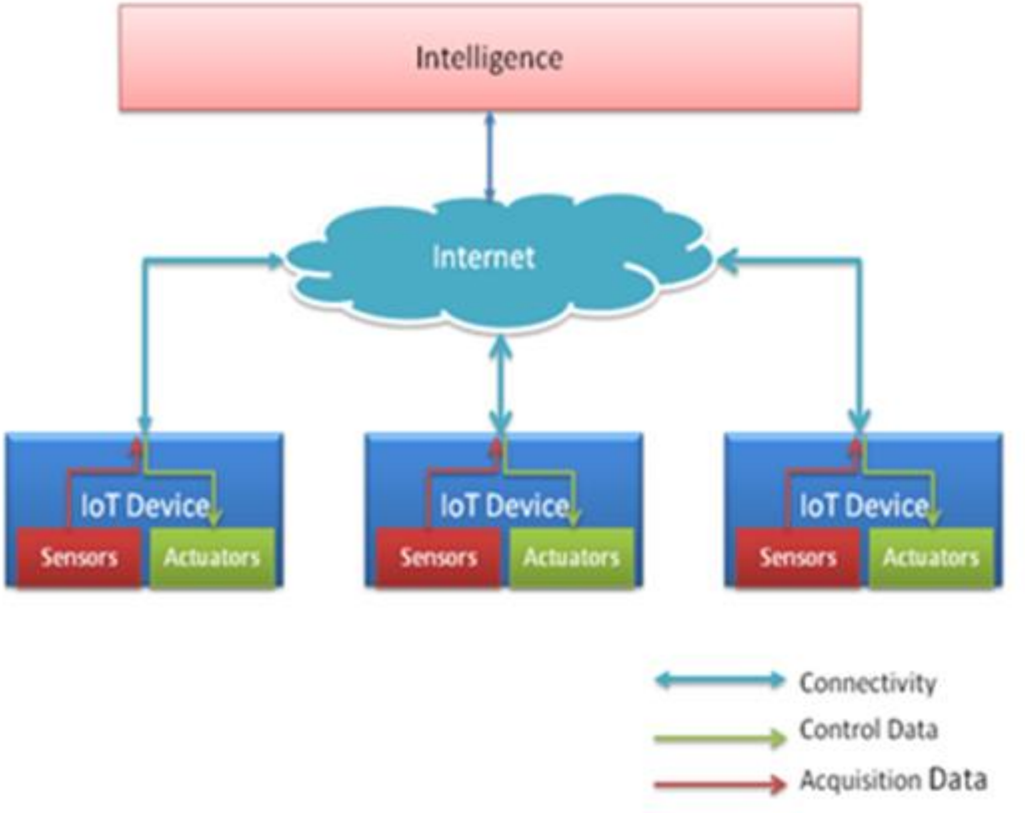
Sensor Architecture



Sensor Network Limitations

- Possess very little storage capacity – a few hundred kilobytes
- Possess modest processing power-8MHz
- Work in short communication range – consumes a lot of power
- Requires minimal energy – constrains protocols
- Have batteries with a finite life time
- Passive devices provide little energy

Edge & IoT Architecture



Edge & IoT Communication Architectures

- Device-to-device
- 2 or more Edge & IoT devices communicate directly with each other, without an intermediary used in traditional devices.

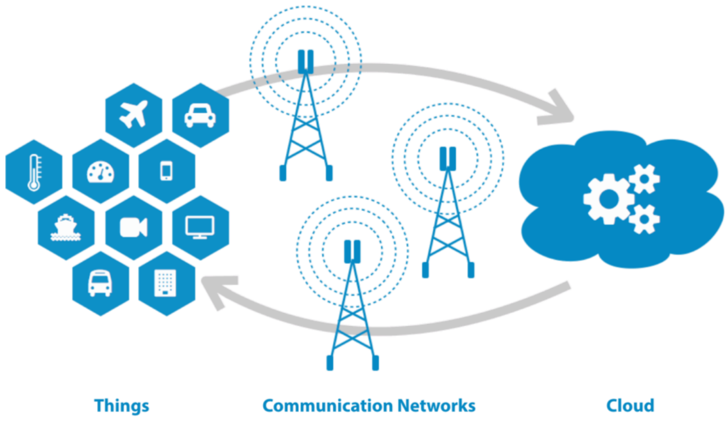
Device-to-cloud

- An Edge & IoT device directly communicates with an application server in the Internet (cloud) and exchanges messages like device status and control commands.

Device-to-gateway

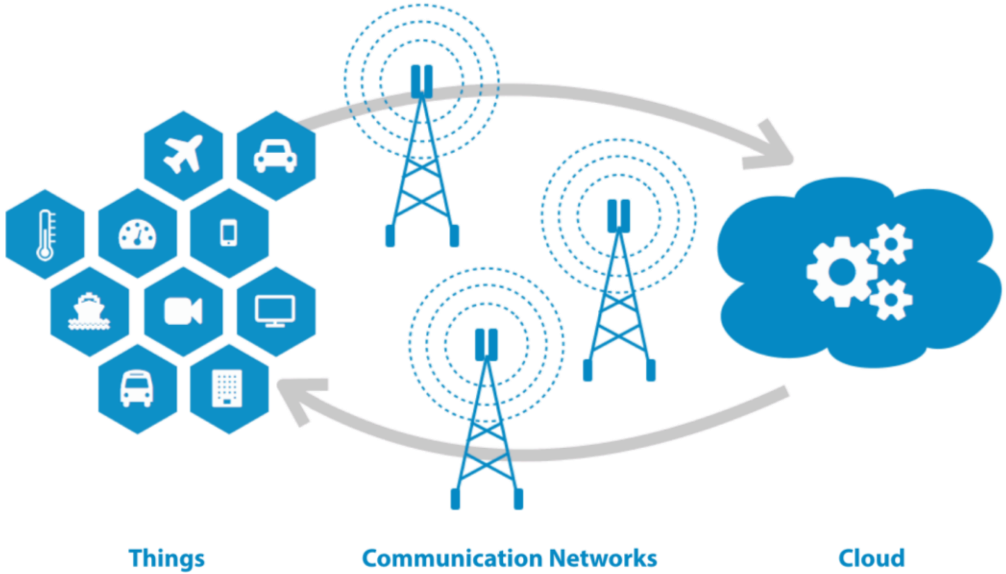
- An application layer gateway (ALG) is used, which is a computer system with 2 or more network interfaces. In this model, Edge & IoT devices are directly connected to an ALG that mediates between the Edge & IoT devices and an application server in the cloud.

Device 2 Device (D2D)



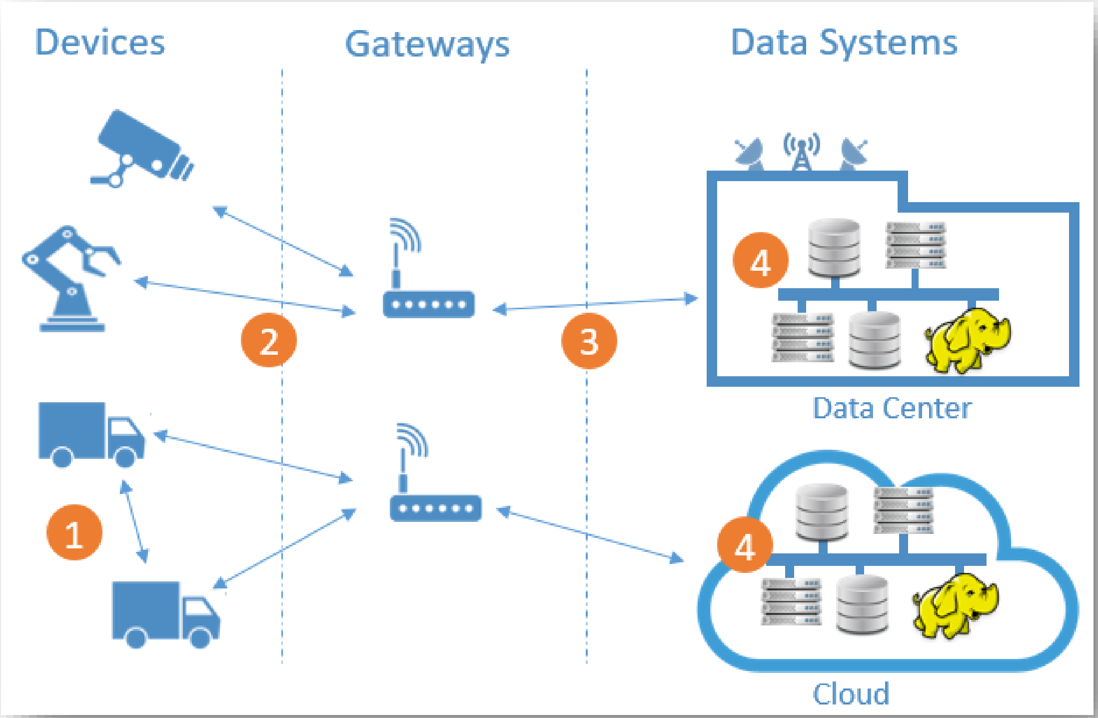
- Devices communicate with each other autonomously without any centralized control and collaborate to gather, share, and forward information.
- Ultimately, the quality of the information gathered depends on how smart the devices are.

Device 2 Cloud



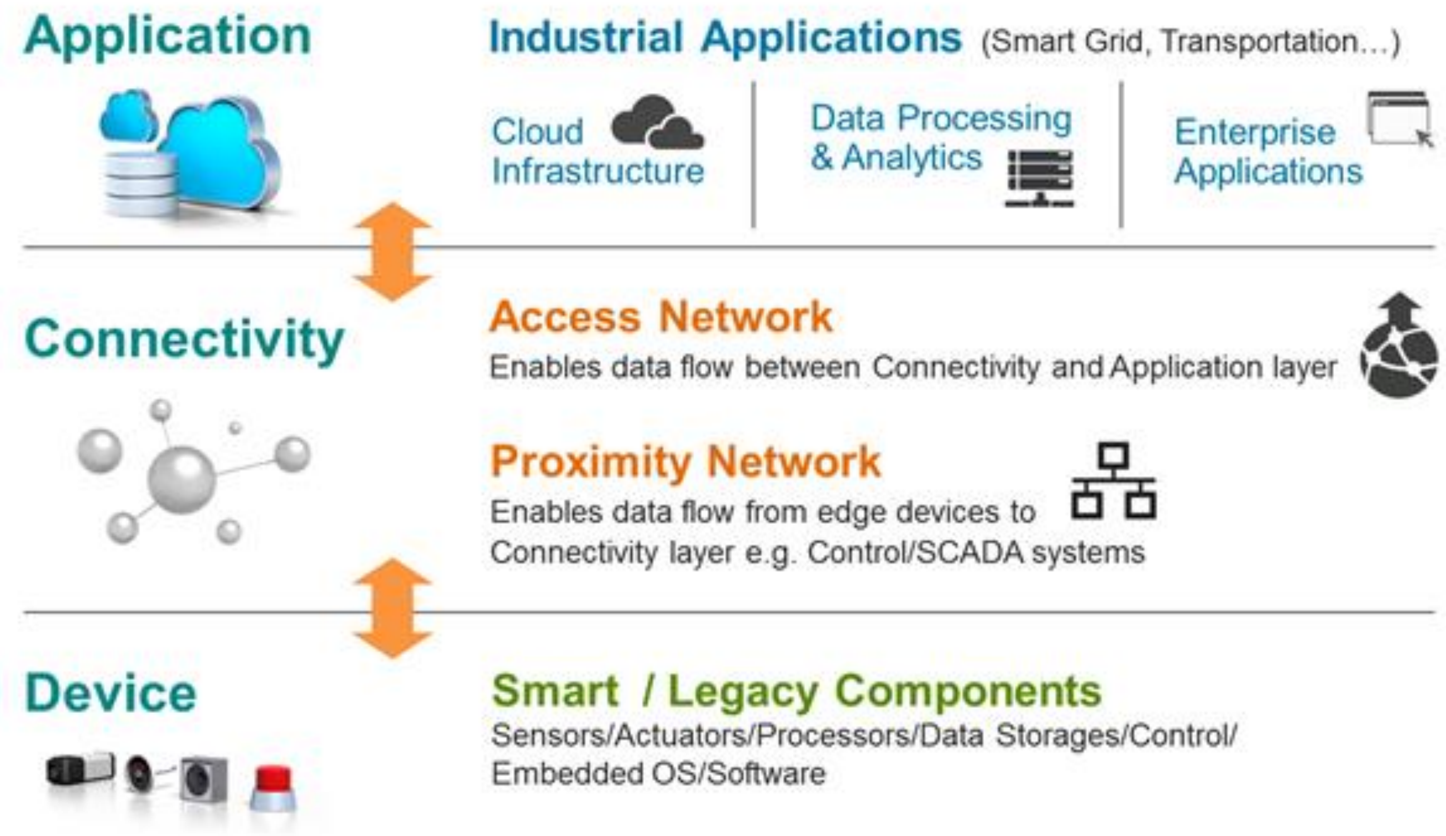
- Direct communication with cloud is the most crucial component
- Edge & IoT cloud platforms are used in application development, device and system management, research, visualization, analysis, monitoring, etc.

Device 2 Gateway (Edge & IoT-GW)

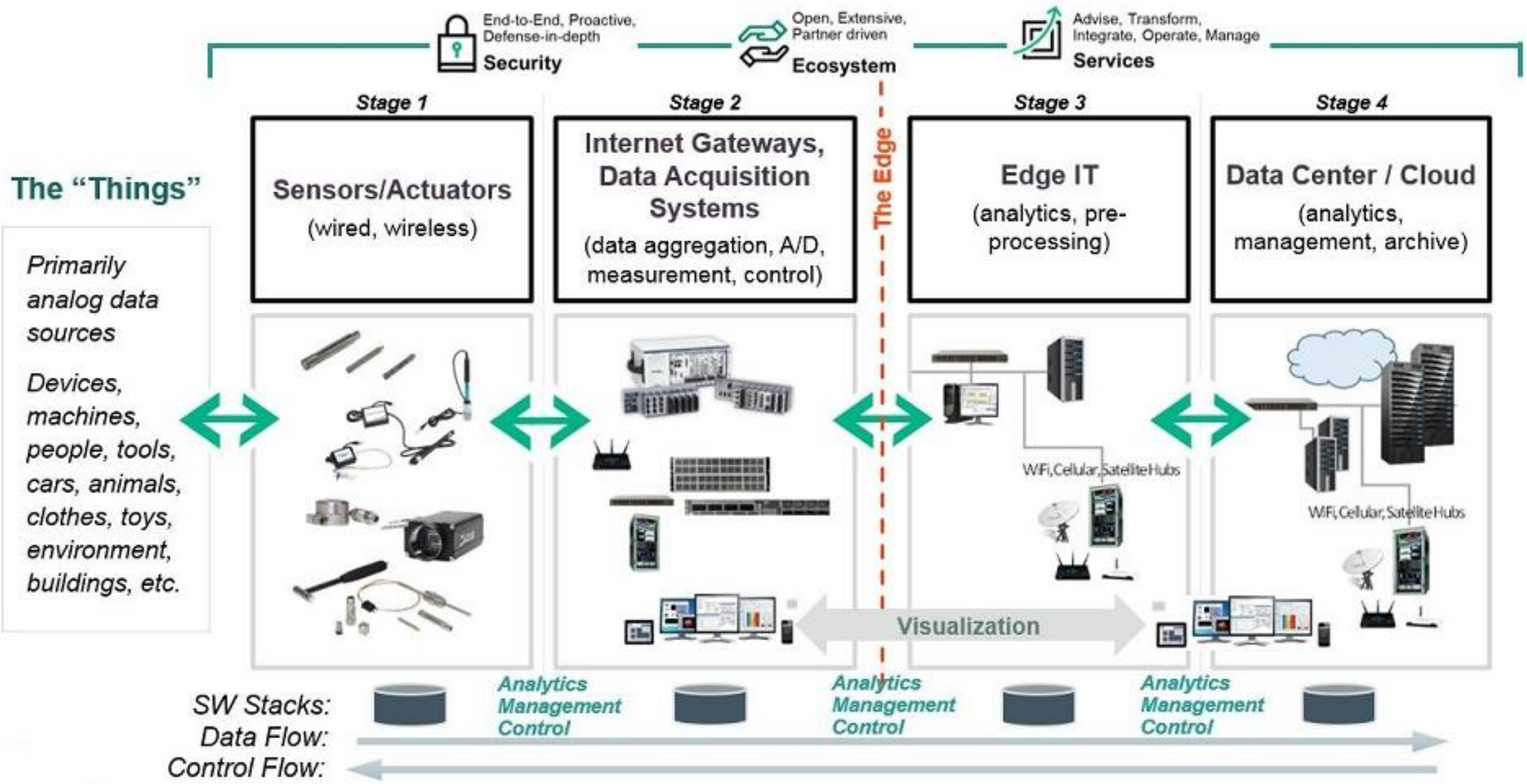


- Direct communication with gateway is the most crucial component
- Edge & IoT gateways are used as waypoints to Public, Private and Hybrid data management, analysis and visualization platforms

Connectivity: Binding Things to Insight



Edge & IoT Solution Sensor Architecture



Architecture Principles Example: Smart Homes

#	Architecture Principle	Description
1	Security first	Security breach into connected home system potentially brings a direct negative impact to end users' privacy. Connected home system collect information from sensors/devices that may reveal end users' day-to-day activities, interest, and preferences. Extra security precautions are needed to keep the potential impact of any security breach to end users' privacy minimum to none.
2	Integration at multiple level	Connected home technology brings more value with more connected devices. Thus, the design of a connected home system must also include multiple interfaces to third party devices and platforms. Also take into account that some devices are tightly coupled with their own platforms, thus can only be integrated via platform interfaces.
3	Design for User Experience	Connected home users may have little or no technical knowledge. Thus, do not rely on end users to perform complex maintenance operation. Always prioritize user experience and convenience for all technical decisions that being made. For example, integrating a popular device that is tightly coupled to a 3rd party platform may have an indirect consequence that the overall system needs to include an extra edge gateways – in this case, the addition adds functionality, but negatively impact customer experience as customers need to have multiple gateways.
4	Centralized Identity Management	The heterogeneous nature of interconnected sub-systems in connected home motivates the need to have a centralized identity management system to keep the overhead of integrating new systems at a minimal level.
5	Minimum lifestyle disruption	The ability to blend product usage into daily activity (i.e., without being too intrusive) is a key to success in the consumer market where Connected Home is considered in. Therefore, opt for architecture solutions that support minimum level of disruption to user lifestyle.
6	Power savings	Connected home users potentially include people with limited technical knowledge to perform system maintenance by their own after initial setup. Therefore, the system shall be designed to use power efficiently so it can work normally for long period.
7	Always connected	Connected home system shall never be completely disconnected from end-users. In the case where connectivity drops completely, each device in the system shall still be able to deliver its core functionality normally.

Edge & IoT Device Domain: Smart Home

Connected Home Sensors

NETWORK TOPOLOGIES

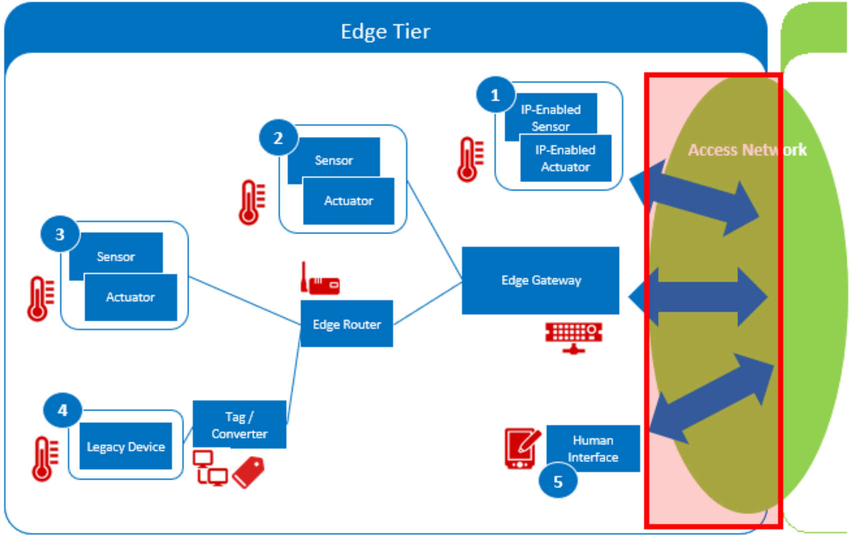
It is common to have all 5 types of network topologies altogether in a connected home system.

Despite the existence of communication standards, many edge devices provided by connected home vendors are built with either proprietary protocols with special edge gateway or dedicated platform.

Thus, the integration between edge devices made by different vendors is often implemented at the level of either **edge gateways** (i.e., multiple gateways in an internal network communicates with one another) or **platform tier** (i.e., connected home edge tier communicates with dedicated platforms of certain devices).

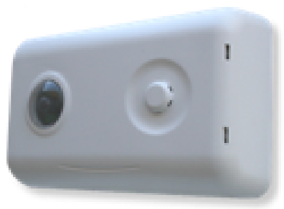
However, this typically leads to cost inefficiency, because 1) end users need to have (and pay for) multiple edge gateways, and 2) extra gateways and platforms shall introduce operational complexity (e.g., HW upgrade, patch, user federation).

Consider API management and IAM federation in the platform tier, exposed onto the access network to solve integration issues typically appears in connected home project.



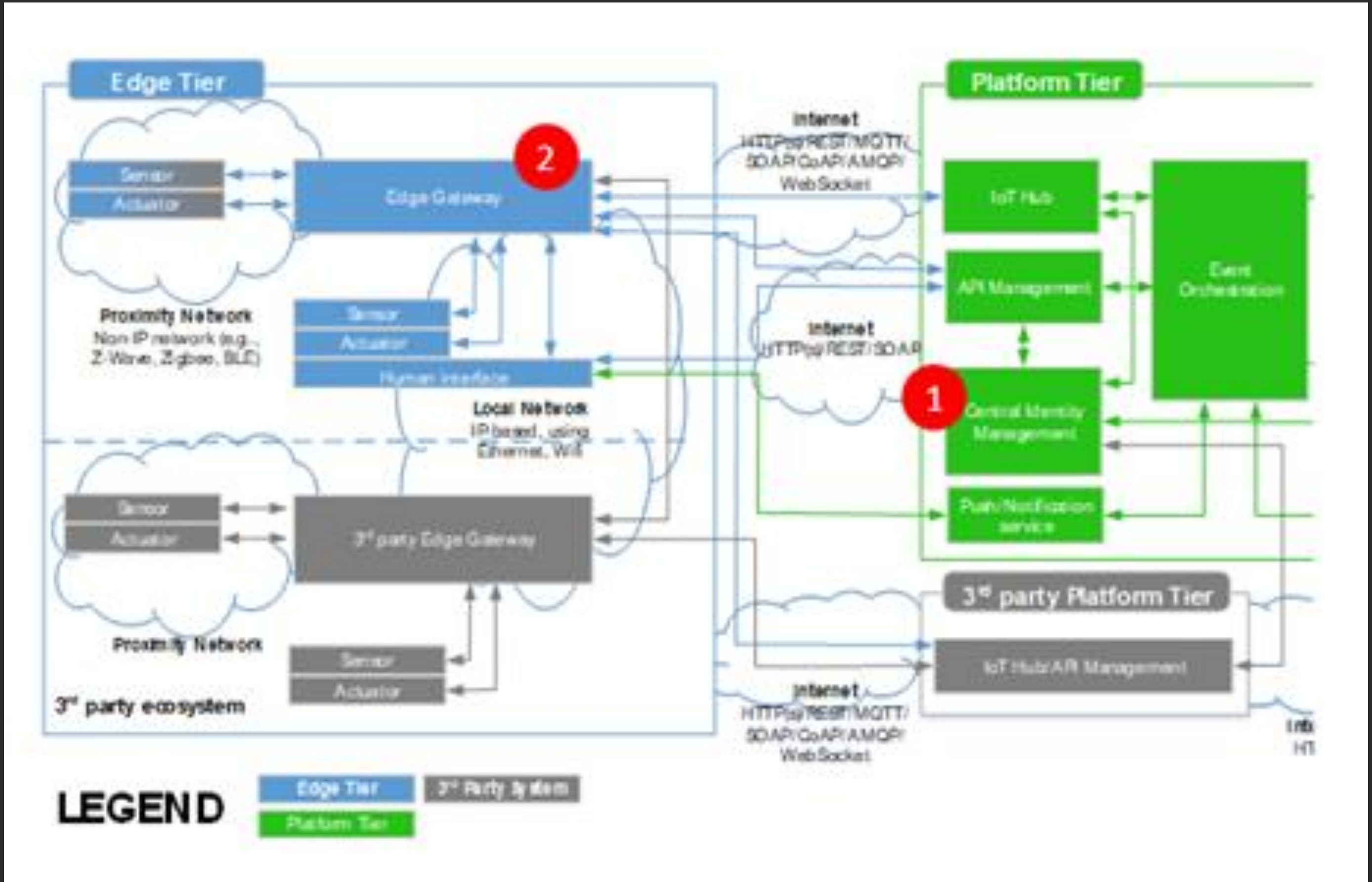
Common point of integration between for multiple vendors

Sensor Examples: Adjacent

	Product & story
	**Teddy the Guardian** This is a different take on connected medical devices or even quantified self devices. This teddy has embedded certified medical sensors that measure child's heart rate, oxygen saturation, and body temperature seamlessly during play, capturing and sending the data using wireless technologies to a pediatrician's app. The patient benefit is that data is non-skewed by a stressful situation. Pre-order pricing €XXX. http://teddytheguardian.com/
	Simpalarm: assisted living Reduced barriers to entry into the hardware market has enabled start-ups such as Simpalarm to enter the market with a service based on a smart device. The device monitors activity in the house and alerts relatives & carers if abnormal activity is detected. Targeting the UK market, it locks onto a standard UK power socket to prevent accidental disconnection. As with most connected devices, the required bandwidth is low, so it uses a GPRS modem to keep BOM (Bill of Materials) cost low. http://www.simpalarm.com/
	**Alzheimer's tracking device** – how not to roll-out device technology Here's an example of the importance of how to roll out device technologies. A police force in the UK has introduced a location tracking device for Alzheimers sufferers for when they go missing. Although intended as positive (find the sufferer faster and cheaper (£XX per month rental vs. a helicopter!)) this technology can be seen as negative as in this news report. News story: http://www.telegraph.co.uk/health/healthnews/10029205/GPS-tags-for-dementia-patients.html Devices: http://www.mindme.co.uk/ and/or http://www.gpsshoe.com/

Edge & IoT Sensors Connectivity

Sensor and Connectivity Security Concerns: Connected Home



Sensor & Connectivity Example: Digital Broom

A Digital Broom for public street cleaning service optimization.

Service contracts are not indexed to the number of resources anymore. Nowadays, new contracts are based on the quality of the services.

Companies have to face relevant penalties if they receive low quality or citizen complaints.

The solution includes a custom device to detect road sweeping activity (GPS and sweeping movement) and cart position.

Sigfox LPWAN is used to reduce communications cost and extend battery life with a Web portal to track real-time activity.

Twitter integration provides real time information to citizens: “We are cleaning Grand St. now”.

Sensor & Connectivity Example: Smart Waste Monitoring

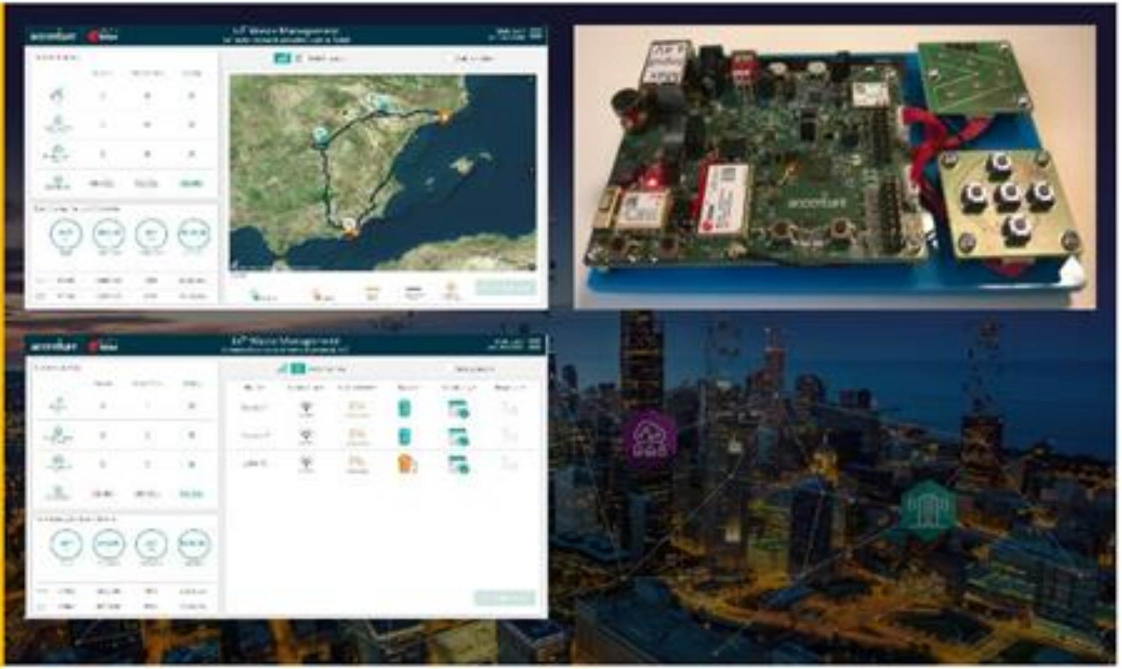
Accenture worked with Vodafone to showcase Narrow Band-IoT technology in an end-end vertical use case.

The Accenture IoT Development Platform (AIDP) incorporates a NB-IoT module used as sensor within a waste container.

The status of the waste container is communicated to Accenture's cloud-based service, using Vodafone's NB-IoT network.

The values demonstrated are:

- Auto Schedule bins for collection
- Optimal path calculation
- Analytics for reporting savings in terms of Fuel costs, Emissions, Duration and Distance.



RTLS Wireless Device Connectivity

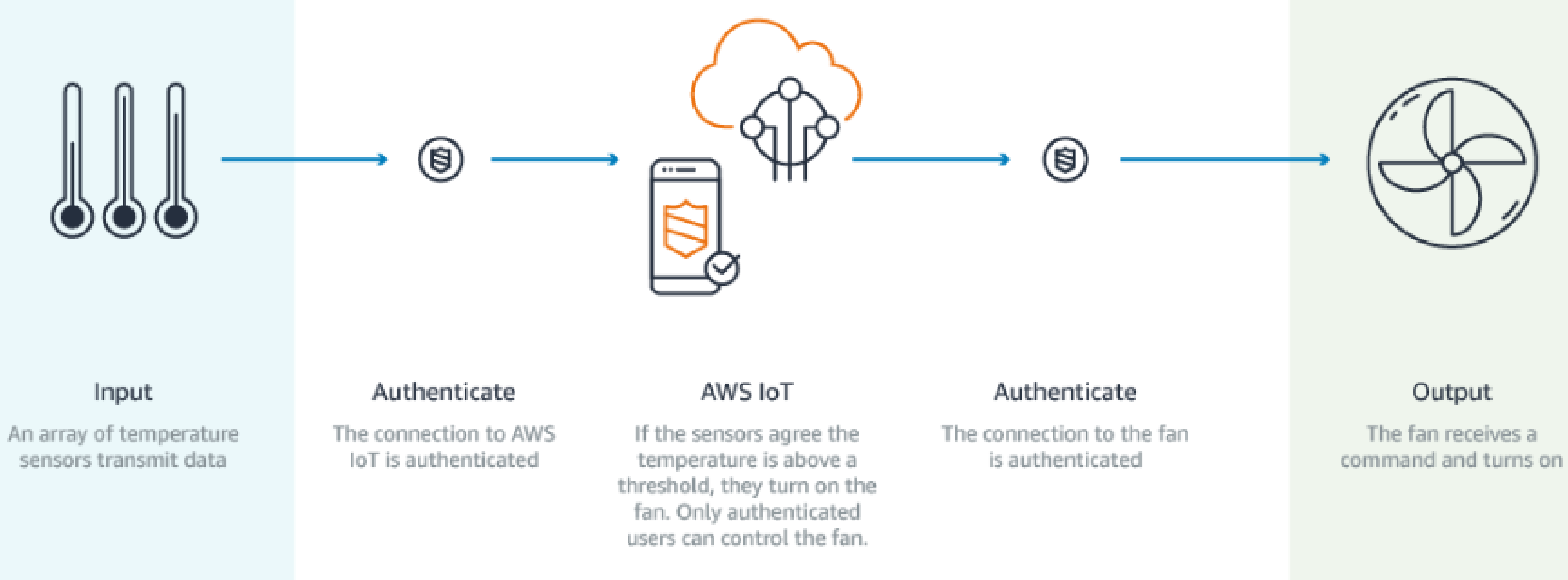
Options		Max range	Battery life	Example size/weight	Tracking unit cost*	Device operational cost
RFID	Passive	10m In-room	No battery required	Minimal, e.g. built into Octopus transit cards	<$X	Disposable
	Active	20-100m	Measured in years	Aeroscout T2 tag: 35g, 62x40x17mm	$XX-$XX	Battery replacement
Bluetooth LE (using beacons)		<100m In-room	Device: 1 year Beacon: up to 10 years	Guardian: Electronics core: 6g Bracelet: 12g, 225x35x12mm	$XX inc. bracelet (<$X electronics)	Battery replacement (device and beacon)
ZigBee/Z-Wave		10-100m In-room	Years	AwarePoint wearable tag: 46x33x13mm	<$XX	Battery replacement
Wi-Fi		100m In-building	Days	Sonitor P-tag: Unknown but expect smaller than Guardian as disposable	<$X	Battery replacement
Weightless (in development)		10km	Years	None in-market yet	<$X target	Battery replacement
Cellular		Global or 10m for femtocell	Days	Trax: Electronics core: 30g, 55x38x10mm Bracelet etc.: unknown	$XX's	SIM subscription

*Per-unit cost/price approximate as always built into solution price and dependent upon volume

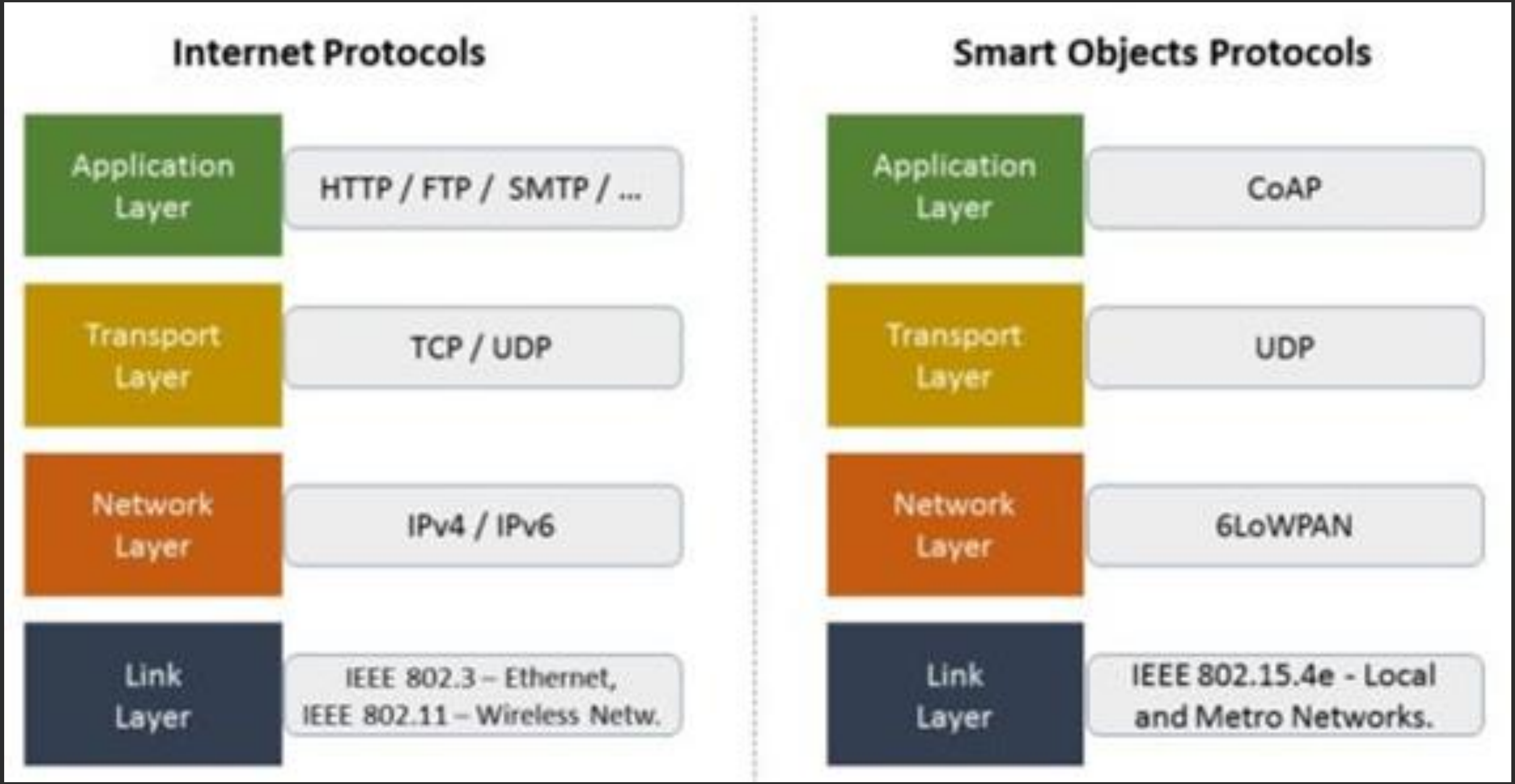
Sensor & Connectivity Examples: RTLS

	Supplier	Product	Technology
	Aeroscout / Stanley Healthcare	Hugs infant protection http://www.stanleyhealthcare.com/solutions/health-systems/security-protection/infant-protection	RFID exciters + Wi-Fi
	BeLuvv	Guardian http://beluvv.com/main/guardian	Bluetooth LE
	Awarepoint	Patient tracker http://www.awarepoint.com/solutions/rtls-technology	ZigBee (802.15.4)
	Sonitor	Safety / Patient Flow http://www.sonitor.com/	Wi-Fi (802.11) / **Ultrasound**
	Trax	GPS Tracker http://www.traxfamily.com/	GPS + GPRS Designed for external use, thus poor battery performance (Currently no roaming agreement in place for Client Location)

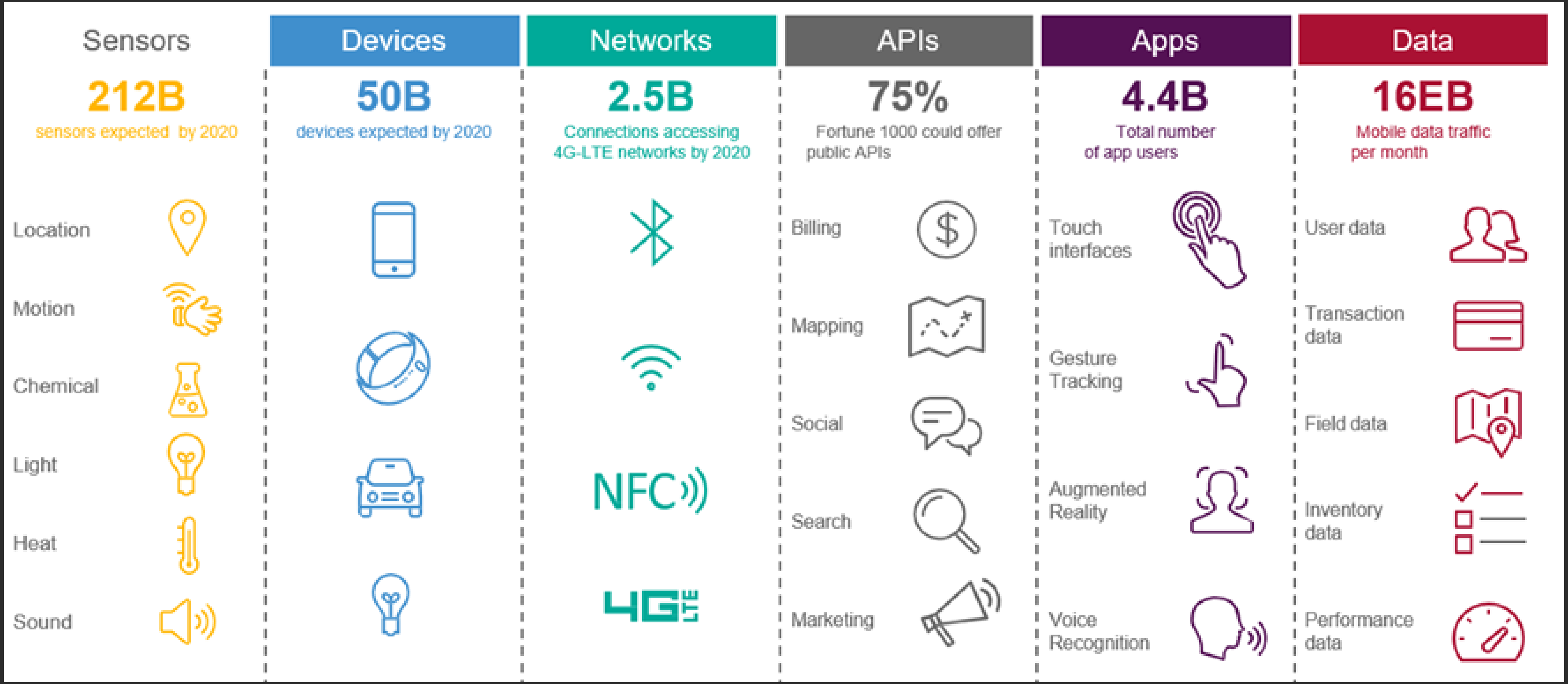
Sensor & Connectivity Examples: AWS Edge & IoT



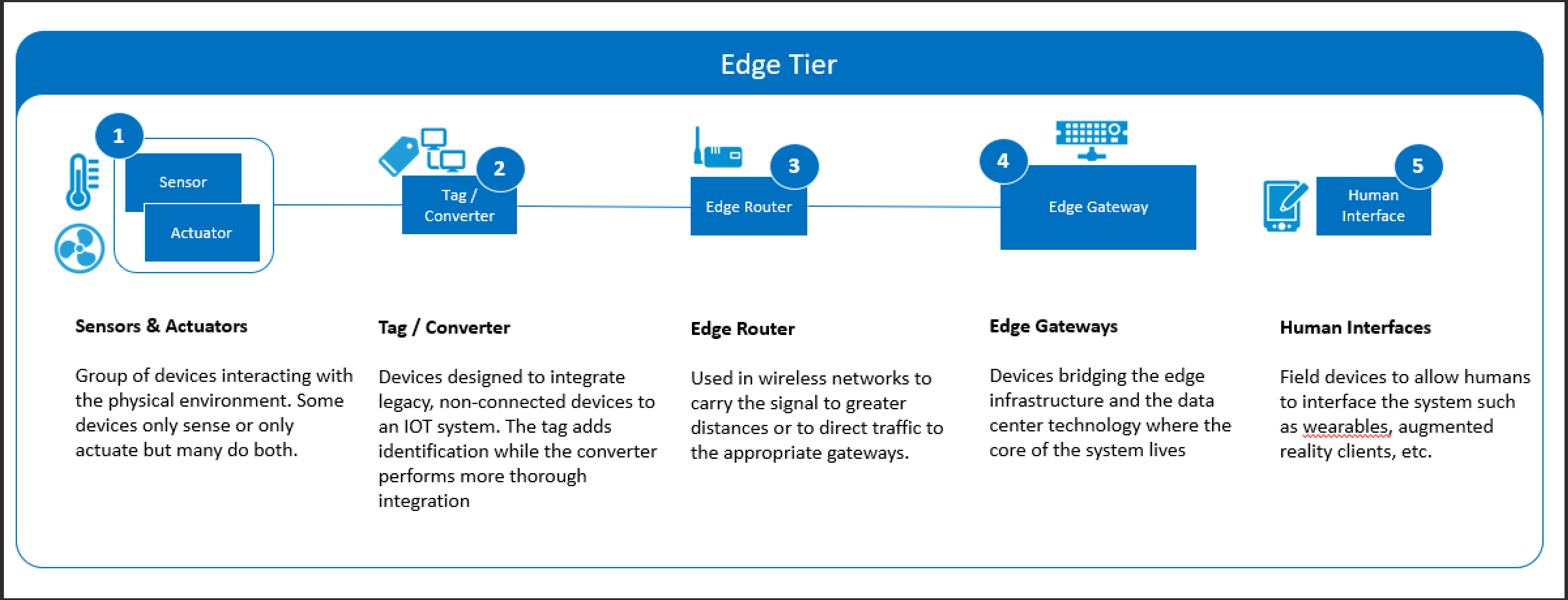
Connectivity Protocol Layers



Predictions for the next few years



Edge Tier


Edge Tier
1
Sensor
Actuator
2
Tag / Converter
3
Edge Router
4
Edge Gateway
5
Human Interface
Sensors & Actuators
Group of devices interacting with the physical environment. Some devices only sense or only actuate but many do both.
Tag / Converter
Devices designed to integrate legacy, non-connected devices to an IOT system. The tag adds identification while the converter performs more thorough integration
Edge Router
Used in wireless networks to carry the signal to greater distances or to direct traffic to the appropriate gateways.
Edge Gateways
Devices bridging the edge infrastructure and the data center technology where the core of the system lives
Human Interfaces
Field devices to allow humans to interface the system such as wearables, augmented reality clients, etc.

Wireless Connectivity Options

Technology	Range	Power consumption	Hardware cost	Operational cost
Bluetooth	• 100m • In-room / car	• 1-100mW tx	• <$5	• Maintenance costs only
Wifi	• 100m • In-room / in building	• 100mW tx	• <$5	• Maintenance costs only
Z-Wave	• 30m • In-room	• 1 mW	• <$10	• Maintenance costs only
Cellular	• 10's km • Wide area	• 1-2 W	• $10's	• On-going SIM costs per sensor
	Range allowing cost effective network rollout	Terminals able to optimise for long-term battery use	Low enough to incorporate in low cost devices	Low enough to support IoT scale proposition

Wired Connectivity

- Device to Device uses Bluetooth, Z-Wave or Zigbee as it involves transmitting small amounts of data.
- Device to Cloud uses WiFi or Cellular technology. Cloud connections allow users to obtain access to the device remotely.
- Device to Gateway uses the network of your smart device like a smart phone or a smart watch. Examples of this are fitness trackers that upload data into your mobile app.
- Backend Data Sharing extends the single device to cloud communications to authorized third parties. This can use any network connectivity like WiFi, Cellular or even satellite. It all comes down to the use case of your business.

Wireless Communication

Below are categorization that only applicable for sensors.

#	Category	Description	Example values
1	Energy in/out	Does the sensor consume, or produce energy?	**Active:** produce energy, typically require external power supply **Passive:** receive energy, typically require no external power supply.
2	Invasiveness	Does the sensor a part/external to environment its measure	**Invasive:** it is a part of the environment it measures. **Non-invasive:** it is external to the environment it measures.
3	Contacts	Does the sensor require physical contact?	**Contact:** Require physical contact **No-contact:** Does not require any contact
4	Relativity of measurements	Relativity of measurements	**Absolute:** Measure on absolute scale **Relative:** Measurements are based on difference with fixed/variable reference values
5	How sensor measure	The physical mechanism used to measure sensory input	Thermoelectric, electrochemical, piezoresistive, optic, electric, fluid mechanic, photoelastic
6	Measurement objects	Objects of measurements	Position, Occupancy and motion, velocity and acceleration, force, pressure, flow, acoustic, humidity, light, radiation, temperature, chemical, biosensors
7	Frequency bands	Which frequency bandwidth the devices are working on	Sub-GHz, 2.4 GHz

Frequency -> Bandwidth & Distance

The Concept

Not All Frequencies Are Created Equal

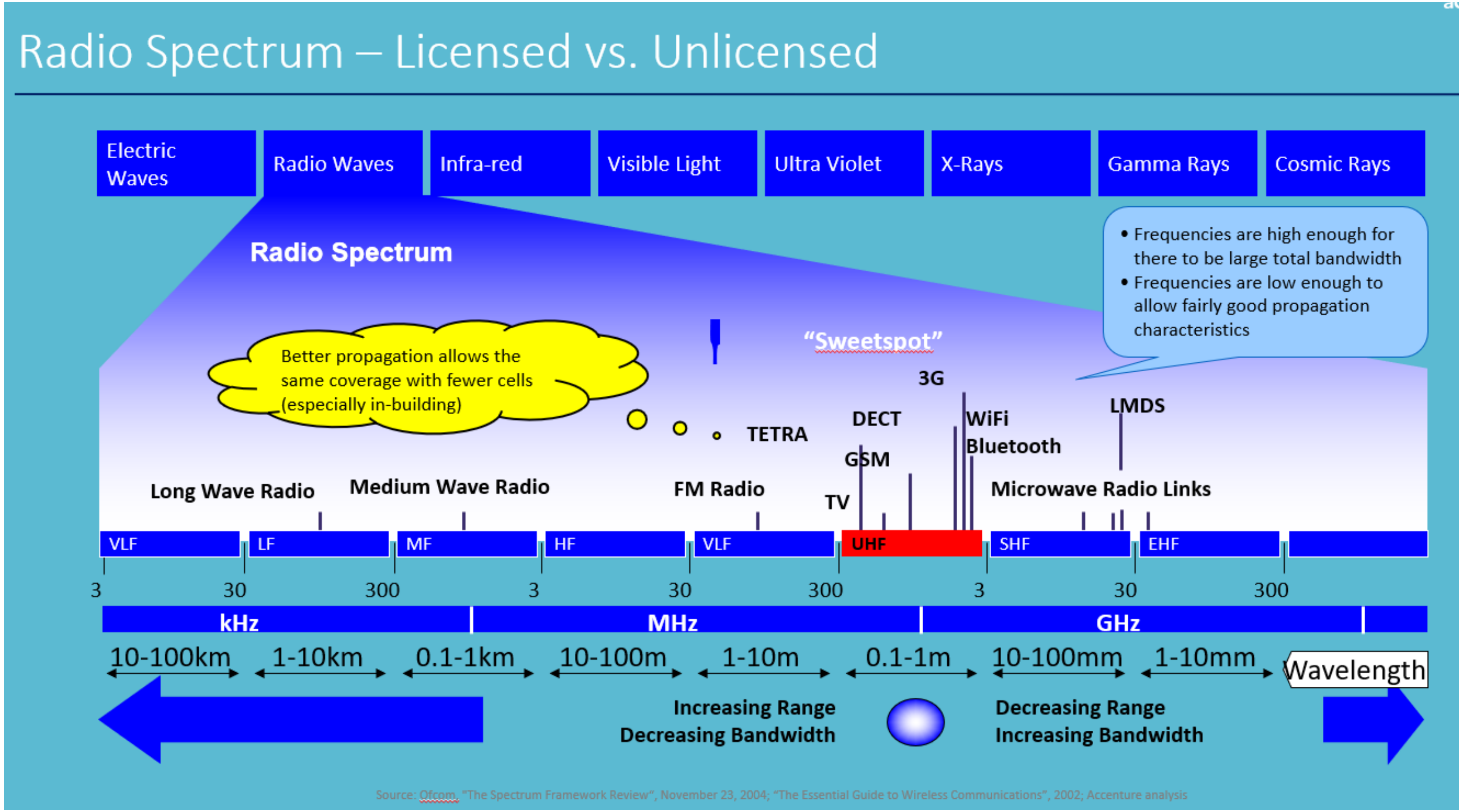
The **distance traveled** by the encoded sine wave **depends** on **its power, frequency & the environment it's travelling in.**

For the same amount of power **lower frequencies travel further and have better penetration:**

•i.e. penetrates through walls with more ease (key for in-building coverage).

However, **high frequencies bands can carry more information** since they can be wider.

WiFi in Context

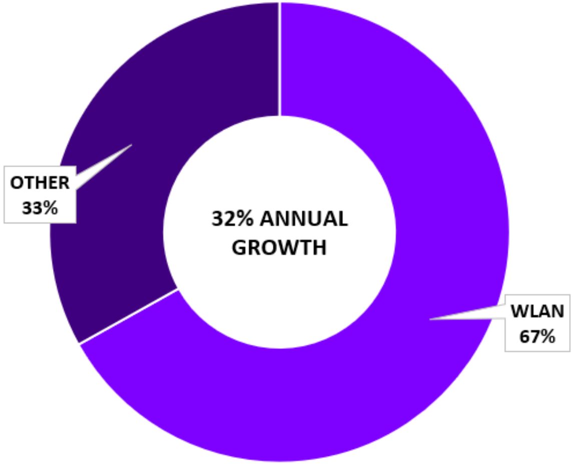


WiFi in Context

EXECUTIVE SUMMARY: WIRELESS SENSOR & LOCAL AREA NETWORKING

WI-FI IS A GROWING COMMUNICATIONS CHOICE FOR INDUSTRIAL NETWORKS

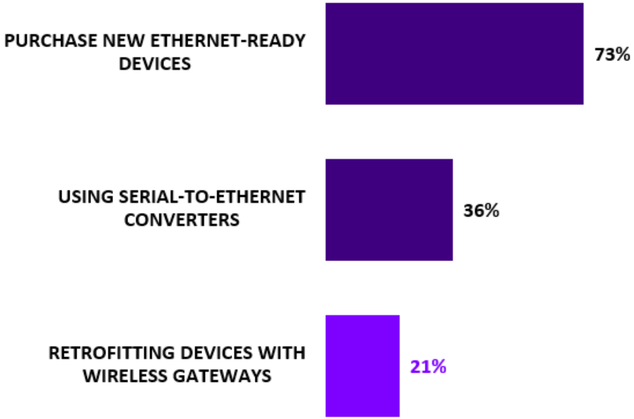
WIRELSS INDUSTRIAL NETWORKS MARKET SHARES [2018]



Source: HMS

IT IS A NATURAL CHOICE AS IT IS BASED ON THE SAME UNDERLYING PROTOCOLS AS INDUSTRIAL ETHERNET

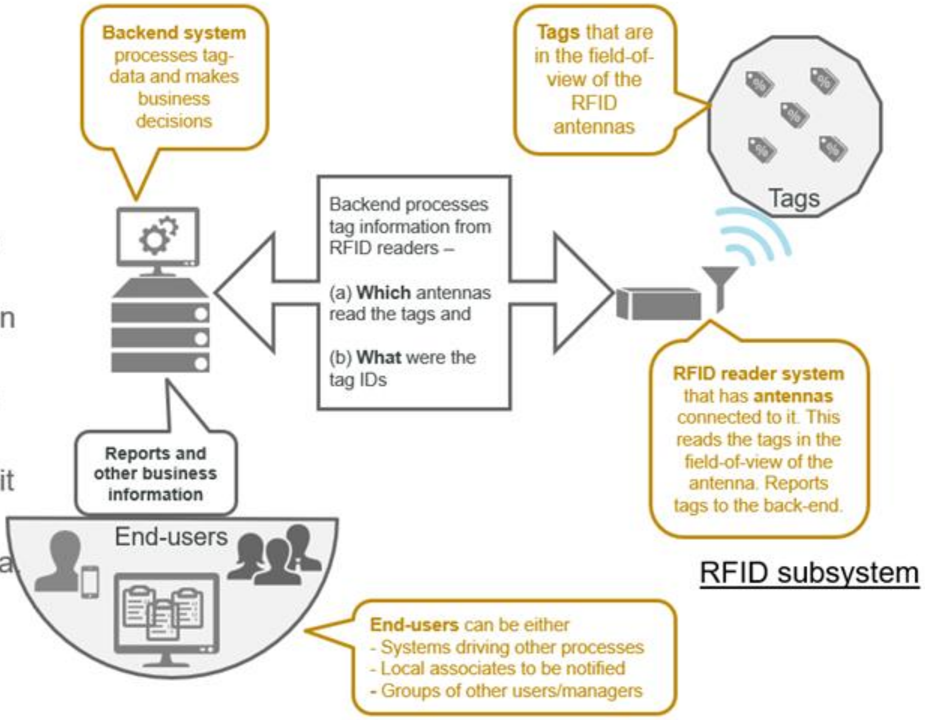
"WHEN UPGRADING LEGACY DEVICES TO ETHERNET, WHAT HAS BEEN YOUR APPROACH?" [2016]



Source: AutomationWorld

RF & RFID

- A basic RFID system consists of a
  - ***Tags*** *– on the products that are to be tagged*
  - ***RFID antenna*** *- to receive tag responses*
  - **RFID reader** *– to decipher tag signals received*
- The RFID reader constantly emits radio waves - Inquiring if any tags are present in front of the antenna.
- Tags that are within earshot respond with their IDs.
- RFID reader records the IDs and passes it on to the back-end system.
- The back-end system aggregates the data
- Thus feeds and enables other business analytics.



* Only if tags are encoded in the SGTIN format

* UHF Passive RFID – Ultra High Frequency RFID Solutions that operate in the ISM bands (*860 MHz-960MHz*). *The tags do not need batteries. They are powered by RFID antennas directly.*

Barcodes vs RFID

Barcode based

- Need the scanner to SEE the barcode.
- Cannot be used to locate/find a specific tag or tagged product.
- Tagged items need to be individually scanned.
- Mostly SKU based coding. So items are not serialized.
- Only store single string worth of data

Barcode scanner

RFID based

- Need the scanner and RFID tag to HEAR each other.
- Can be used to locate/find a specific tag or tagged product.
- Multiples of items can be scanned in a single pass. More than 300 items can be scanned in a single pass, at the same time.
- RFID IDs are serialized numbers and include SKU information*.
- Ability to store several bytes of data in RFID tag memory banks

RFID scanner **

RFID tag

- Micro chip with an antenna connected
- Gets excited and active when it walks into the field of view of a antenna that is transmitting
- Has 4 memory banks
  - EPC ID/ Tag ID of the tag
  - TID bank (Manufacturer info)
  - Reserved bank (Security info)
  - User bank (Optional memory bank)
- Upon getting excited, the tag replies initially with its ID and subsequently with other information as requested by the reader/interrogator.
- Tags come in several form factors

Type of RFID Tags

- The most common and cheapest tags are the paper tags. They are RFID tags on rolls of paper, plastic or apparel-type labels.
- There are several other specialty tags that can be used based on the use-case and location where the tags are being deployed
  - Metal mount tags – Used when a tag is being mounted on a metal surface
  - Large memory bank tags – Used when the user application wants to store large quantities of custom information on the tag memory / keep updating it depending on the situation.
  - Temperature sensor tags – Used to measure temperature at specific intervals of time and store them.
  - EAS tags – Used to track merchandize as it exits stores and use it as a way to identify sold/unsold merchandize.

Paper tag

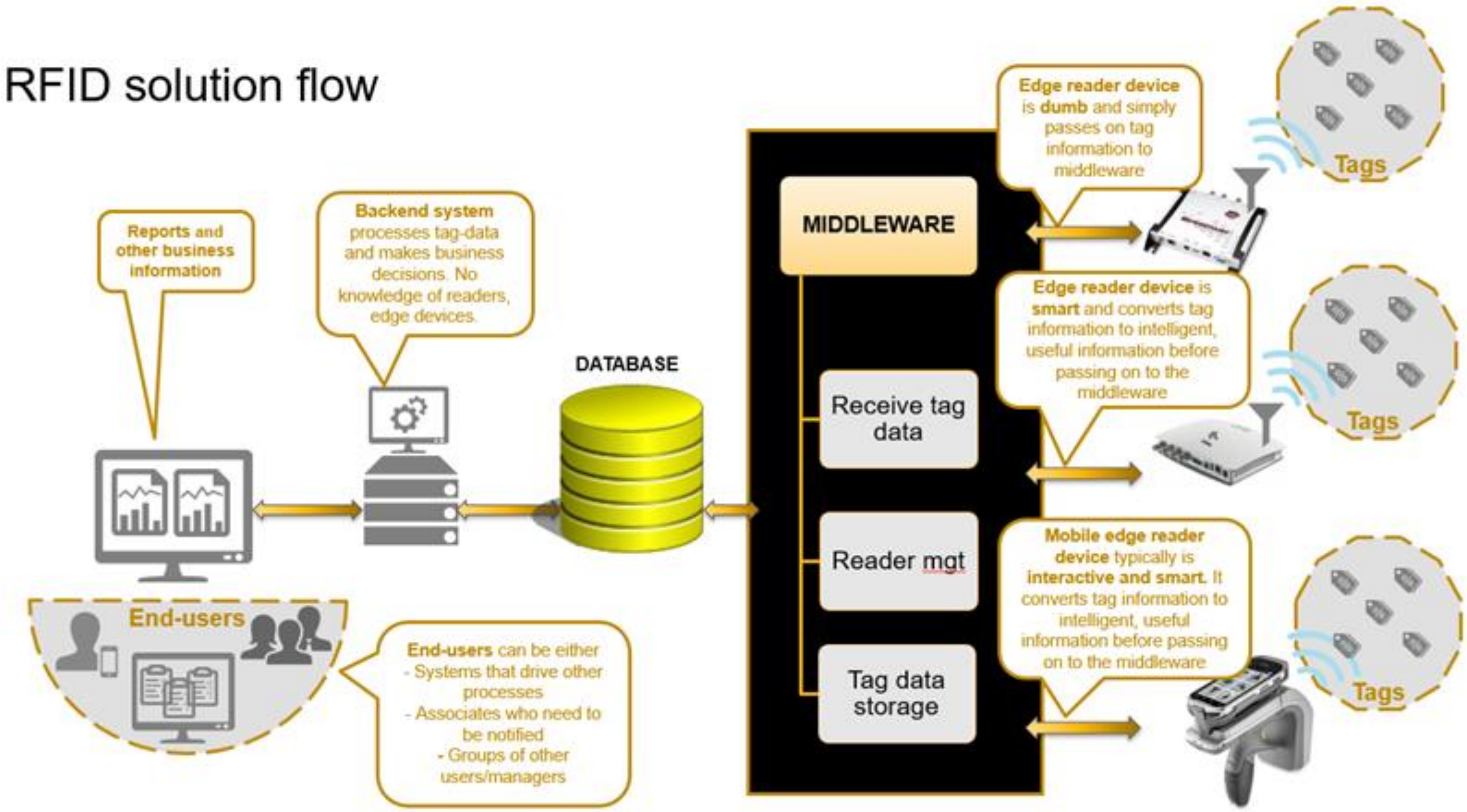
Temperature sensor tag

Large memory RFID tags

Conditions Impacting RFID

- Conditions directly impacting RFID efficiency
  - Liquid
    - Water, Blood and liquids absorb RFID energy and as a result, a tag that is shielded from the antenna by a liquid-filled body will not read very well … if at al
  - Metal
    - Metal shorts RF waves. So if the appropriate di-electric is not separating the tag from the metal backplane, there would be no signal transmission back to the tag.
  - Indoor v/s Outdoor
    - Walls, false ceilings and raised floors reflect RF waves. This multi-path helps with the RFID reading.
    - So a tag that only reads from a 5 ft distance outdoors will read from a 15 ft distance indoors
  - Adjacent readers
    - Multiple RFID readers/ interrogators in a close proximity will tend to talk ***over*** each other's query sessions and drown out the tag responses. This is ***INTERFERENCE***.
    - Multiple RFID readers can end up interrogating and recording each others tag populations .. Thus causing ***CROSS READS***.

RFID Solution Flow

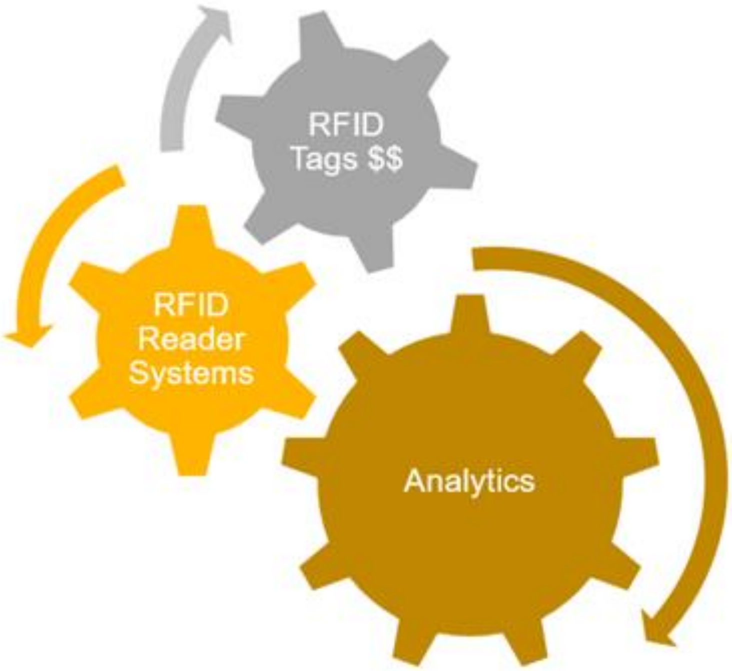


Enhancing RFID Logic

- Fixed mount RFID readers
  - Motion/Proximity sensors
    - To trigger start and stop of signal transmission/reading
    - To aid in processing received tag data.
    - Smart software / middleware is always notified of when an object arrived, departed
    - Also helps to determine direction of tag movement
  - Light stacks, Buzzers
    - To alert users when a *specific* event occurs
  - Canting of RFID antennas/ portals
    - To determine directionality of tag movement
- Mobile RFID readers
  - Handle triggers
    - Perform actions when a user wants to comments RFID transmission/reading
  - Beepers, LEDs
    - To alert users to specific events, Help them locate specific tags and other feedback

RFID Challenges

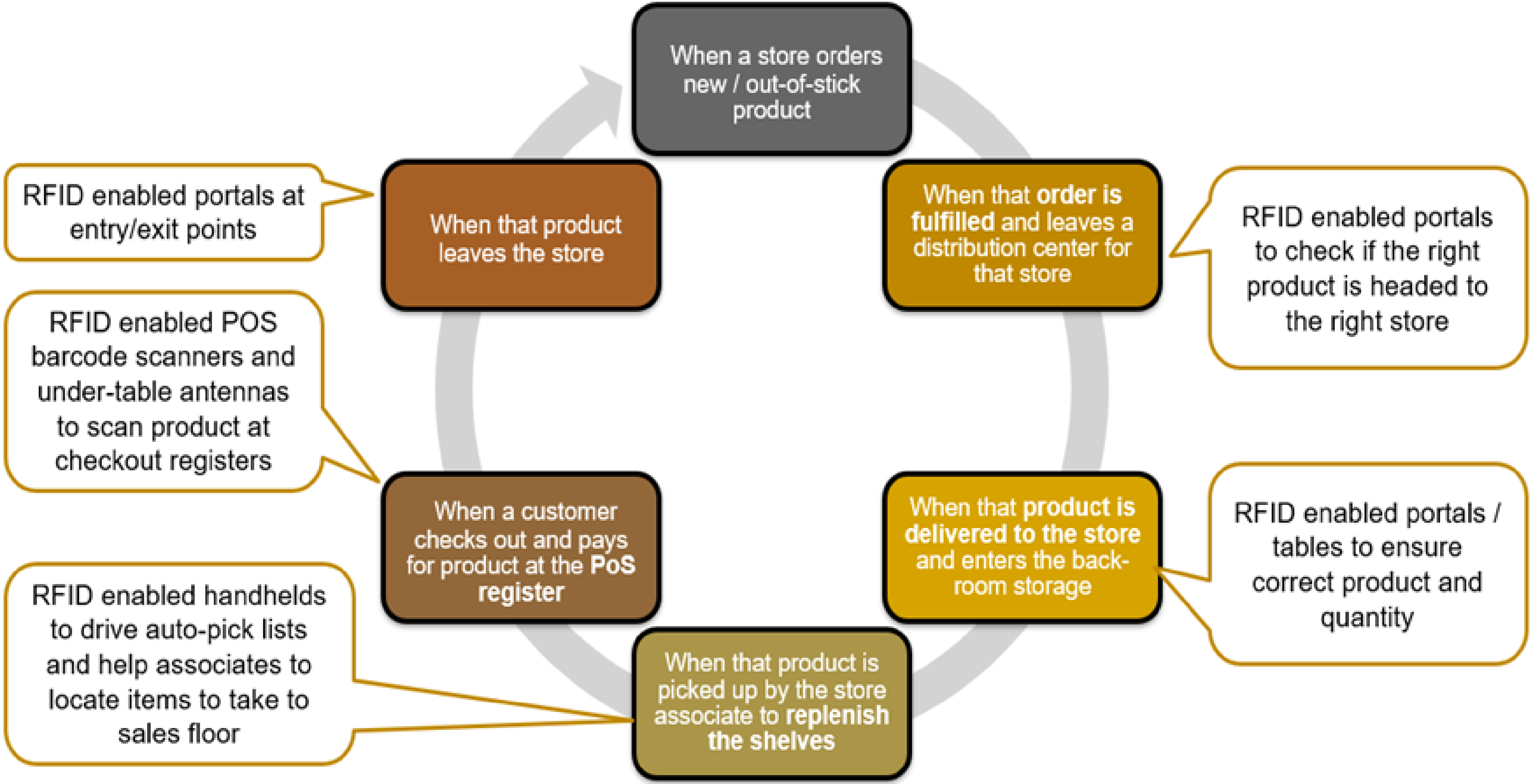
- RFID in Retail has been on the verge of ‘inflection point’ for several years now.
- All the hype has not translated to $$ due to lack of RoI visibility – Return on Investment
- Today
  - The tags are fairly cheap in the 10 cent and under range.
  - The edge devices – Readers are fairly accurate and efficient today
  - The back end is still inching towards maturity
    - Large quantities of data generated
    - Lacking - Analytics to drive conclusions and decisions
    - Lacking - Strong User interfaces to help the store associate derive benefits
- Strongest adopters today → Macys, Tesco, Inditex, Walmart.



RFID Keys to Success

Define simple use cases	• Reduce the number of read points under consideration • Reduce the necessity for tags information to be continuously updated in databases
Focus on ROI *visibility*	• Insert data points that a user-can-see • One approach is to give managers and associates visibility to RFID driven actions using email, message alerts
Negotiate associate business process	• Almost all interested entities want to INTEGRATE RFID without changes to existing processes • This may be practically possible .. Especially given the need to DEMONSTRATE ROI
Analytics at the back-end	• Most application architects may want Intelligent edge devices with high user-interactive abilities. **Not a great idea.** • Focus the analytics on the back-end. The end-user interface should pull data from the back-ends. • But this will lead to stability issues and the EDGE devices may be unable to provide reliability under such circumstances.
Visibility expectations	• Expecting real-time, down-to-the second visibility for overall inventory accuracy is unrealistic. Delays of a few seconds to a few minutes is required to allow algorithms to process data. • Enabling simple logic on the edge is acceptable to drive instant user-feedback is a smart approach .. As long as the edge is not loaded with other advanced activities.

Common RFID Capable Touchpoints



Shelf Replenishment

- Once a product enters a store, it can automatically get populated into the associate's pick-list for shelf replenishment
- Now the associate needs help to locate the items using mobile RFID readers and take them to replenish the shelf.
- Innovative solutions can be found for read-points above and below shelves to track individual items. They can be cost prohibitive if the right strategy is not in place.
- Portals at the transition points from backroom to store-sales floor can read the tags as they pass .. And determine that XYZ product that I received has now been moved to the store shelf.
- Phase and RSSI information can be used for locating tags in the crowded backrooms

Slim line portals

Shelf antenna read points

Point of Sale (POS)

- As an item is scanned at the Point-Of-Sale for checkout, internal systems are updated with the updated quantity of remaining products.
- Other things that can be done at this stage
  - Tag memory banks can be marked to indicated SOLD items
  - New product replenishment can be triggered
  - Tags can be killed so that they don't show up again in inventory systems

Point of Sale RFID+ Barcode scanners

Slim profile antennas for connecting below the POS/other table

IP V6

- It's still just an Internet Protocol (IP)
- IPv6 is not an upgrade from IPv4
- IPv6 is separate from IPv4
- As the name implies it is a different version of IP
- Both IPv4 and IPv6 packets will be like "ships in the night" passing through the network without affecting each other
  - Carful, there might be a hit on routers & switches CPU and memory
- IPv6 addresses are:
  - 128-bit length (vs. 32-bit in IPv4)
  - Uses hex (0 to F) instead of dotted decimal octets in IPv4
  - Uses Colon (:) as a separator instead of dot(.) in IPv4
  - The characters between colons : in IPv6 address called Hextet
  - The characters between the dots . in IPv4 address called Octets
  - Compression available if needed when writing IPv6 addresses
  - Using :: will mean the remaining hextets to the right of it; are all zeros

- In several ways similar to IPv4's.
- Much cleaner in some ways.
- The larger address space should allow environments to get single, larger allocations to enable better summarization.
- IANA represents the highest entity in this tree
  - Although one could argue that the IETF itself is one step higher.
  - IETF delegated 2000::/3 to IANA (out of the entire IPv6 address space).
  - The remaining are mostly reserved by IETF http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml

Communication for Connected Devices

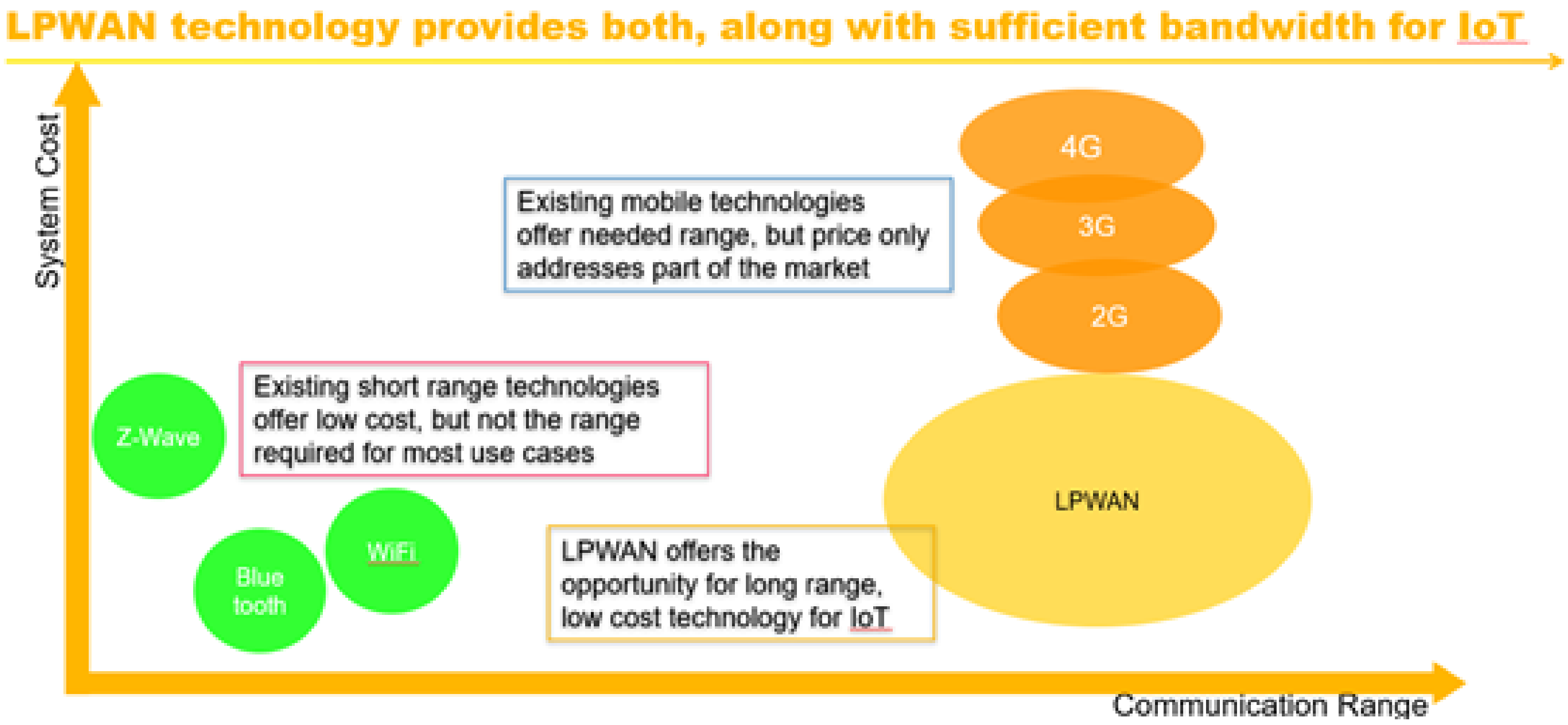
There are many connectivity options for connecting devices …

- Communications technology deals with the transfer of data from one device to another – although there is a vast range of differing requirements covering many diverse use cases
- Varied technologies exist for this purpose including wired, wireless and optical; in particular wireless which is increasingly being adopted for flexibility and mobility

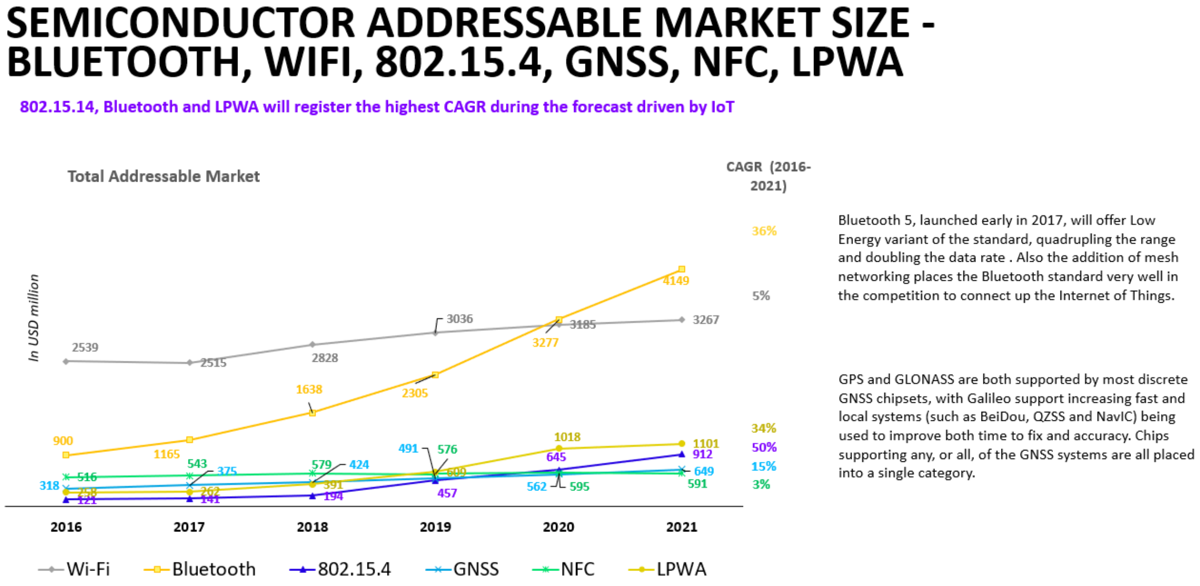
… but existing technology does not cover all IoT needs

- A specific focus has emerged in recent years on wireless networks designed from the ground up to support the specific requirements of IoT devices
- In particular addressing the key requirements of;
  - Long Range
  - Low Power
  - Low capital and operational cost

Many Current Technologies that Emphasize Bandwidth, Tradeoff Cost or Range



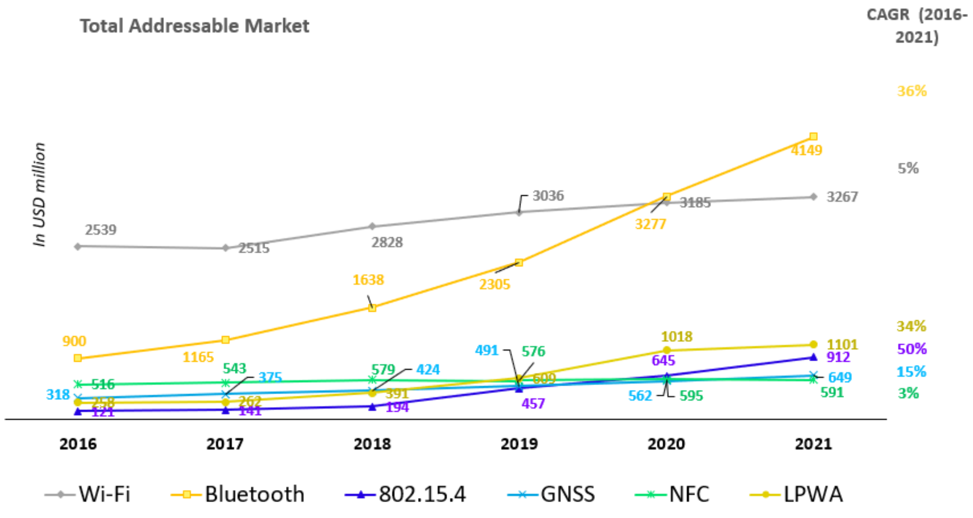
Zigbee (IEEE 802.15.4)



Bluetooth or Bluetooth Low Energy

SEMICONDUCTOR ADDRESSABLE MARKET SIZE - BLUETOOTH, WIFI, 802.15.4, GNSS, NFC, LPWA

802.15.14, Bluetooth and LPWA will register the highest CAGR during the forecast driven by IoT



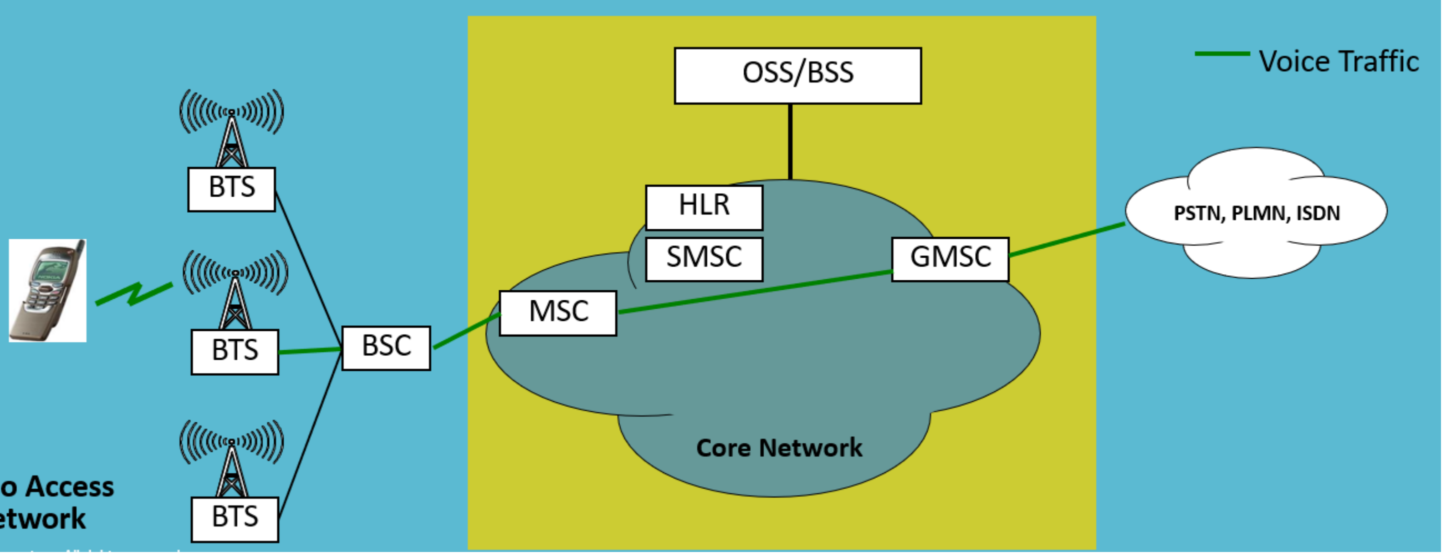
Bluetooth 5, launched early in 2017, will offer Low Energy variant of the standard, quadrupling the range and doubling the data rate . Also the addition of mesh networking places the Bluetooth standard very well in the competition to connect up the Internet of Things.

GPS and GLONASS are both supported by most discrete GNSS chipsets, with Galileo support increasing fast and local systems (such as BeiDou, QZSS and NavIC) being used to improve both time to fix and accuracy. Chips supporting any, or all, of the GNSS systems are all placed into a single category.

GSM(2G/3G/LTE)

2G GSM Architecture

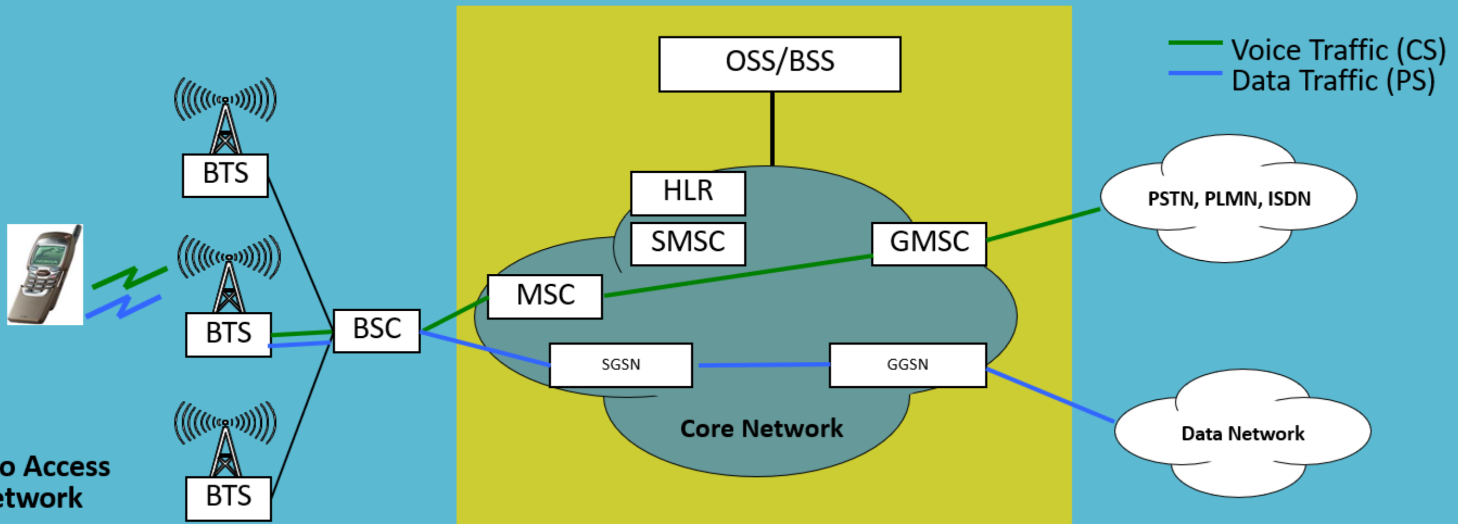
- GSM – originally a European standardization collaboration effort, forms the foundation of global 3GPP standardization body tha governs 3G WCDMA and 4G LTE.
- GSM was conceived intentionally modular to allow for interworking of various vendor elements, practice lived on in newer technologies.
- The major change from 1G to **2G was the introduction of “digitized voice”** and used TDMA.
- 1G networks used an analog air interface over which data was not supported.



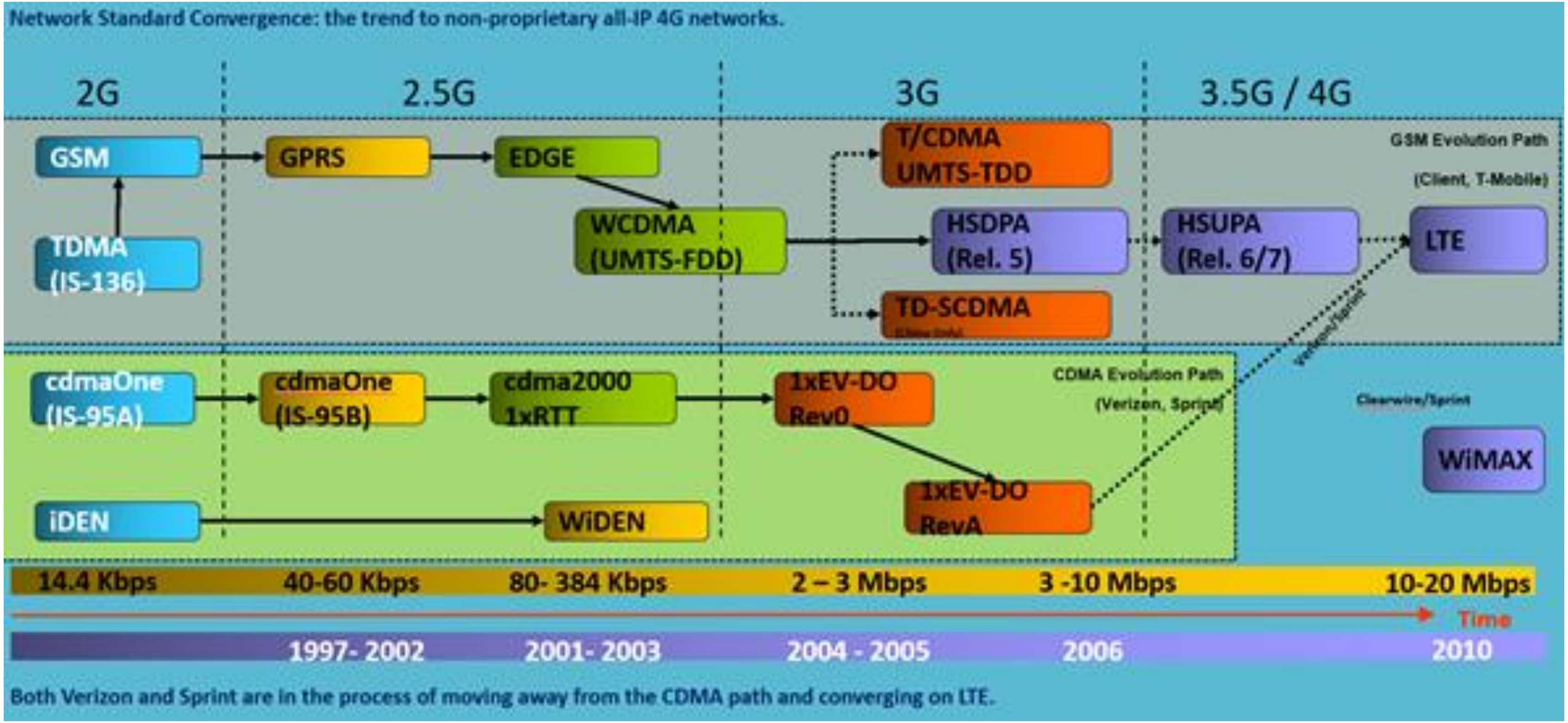
GSM(2G/3G/LTE)

2.5G GSM Architecture

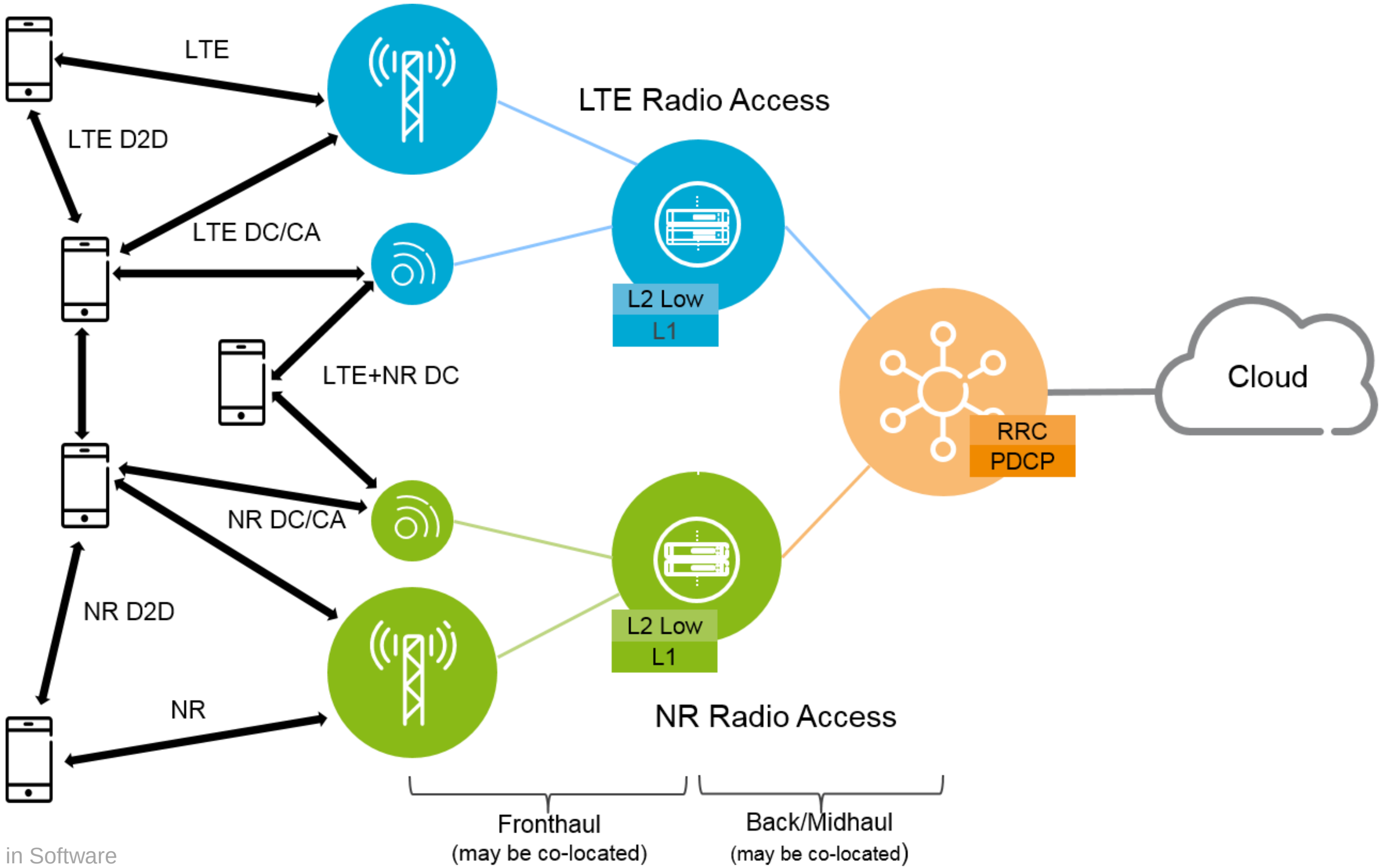
- **Packet data functionality** ((GPRS (2.5G), EDGE (2.75G)) **was “bolted on” to 2G** networks and added new elements to the network
- This created **two separate paths** in the network:
  - The **Circuit Switched (CS) Voice Path**
  - and the **Packed Switched (PS) Data Path**
- Data use required the use of multiple “voice channels” and was TDMA based.



GSM, CDMA, WiMAX Evolution



5G and the Future



5G and the Future

PRIVATE 4G/5G NETWORKS ARE INCREASINGLY PROMOTED BY VENDORS AS A HIGH-PERFORMANCE CHOICE FOR INDUSTRIAL APPLICATIONS

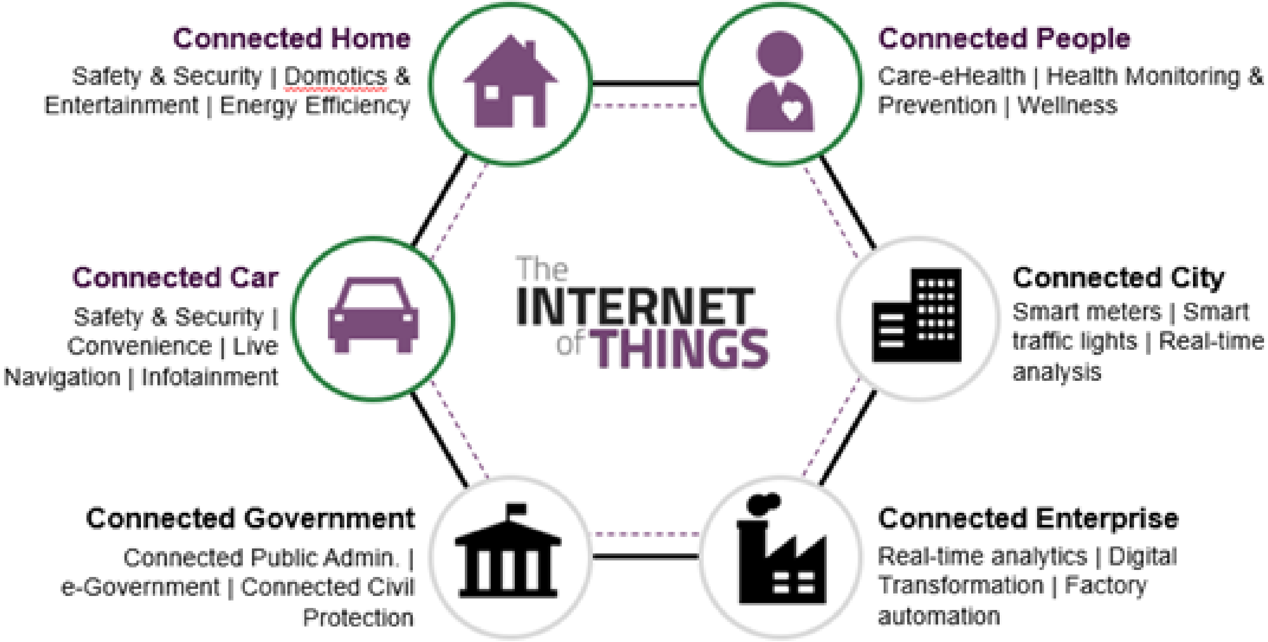
- A wide array of production environments are potentially addressable by private 4G and 5G networks. In particular, significant opportunities for ultra low latency 5G may exist in factories that rely on precision instruments

- 5G network slicing also enables a telco-driven 5G private network approach of 'A network within a network'.

5G Market Drivers

Internet of Things

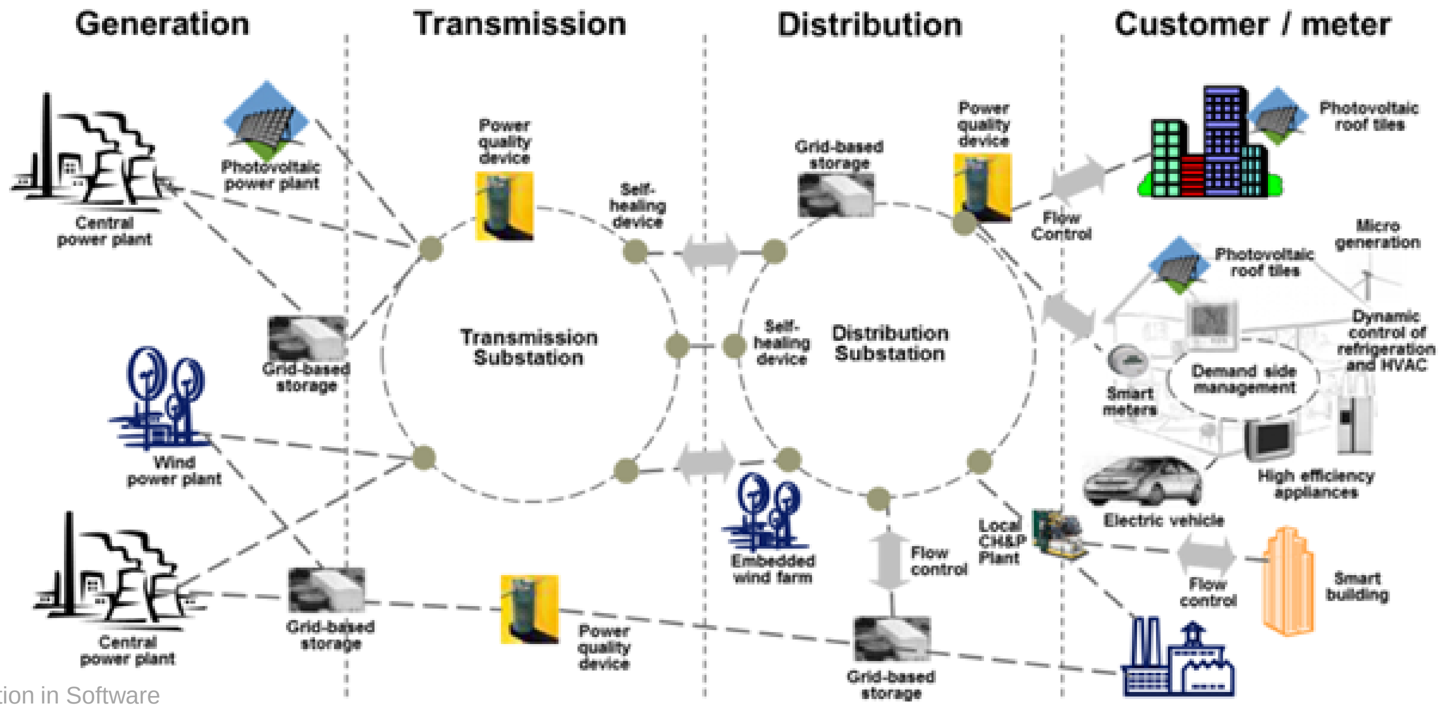
- Predicted to grow at a faster rate than current networks can handle
- Service/context sensitive information transfer: mobility, latency, reliability, resilience



5G Market Drivers

Smart Grid and Critical Infrastructure Monitoring

- Malfunction or damage leads to major financial impacts, quality of living or loss of life
- Infrastructure context determines system functions: electricity distribution, structural monitoring, intelligent transportation systems.



5G Market Drivers

Extreme Video, Virtual/Augmented Reality

Public Safety
- Emergency/Catastrophe broadcast

PSTN Sunset

Prototype AR Contact Lens

LoRa and LoRaWAN

STANDARD

LoRa is an LPWAN standard managed by the LoRa Alliance. LoRa is the physical radio interface (using radios from semiconductor vendor SemTech), and LoRaWAN is the overall communications

DEVICES

LoRaWAN supports a range of devices via three device classes (Sensors, Actuators and Powered Actuators). LoRaWAN is a spread-spectrum technology covering a range of data rates from 0.3kbps to 200

DEPLOYMENT

There are both private and managed network options – users are able to build their own networks, but there are also telco operators building managed national networks (Eg KPN in the Netherlands).

GLOBAL

LoRaWAN has global variants for the various international ISM frequencies and different modes to maximise performance within regulatory restrictions. Additionally LoRaWAN

NB-Edge & IoT

CELLULAR STANDARD

There are now several LPWAN-like standards emerging from the 3GPP standardisation group as part of the LTE family. These standards have evolved through a number of names (Cellular IoT, NB-IoT, LTE cat MTC).

LICENSED SPECTRUM

These standards differ from the other LPWAN technologies in that they operate in the licensed bands used for other cellular communications and thus will be provided by existing (or new) cellular operators as part of their overall connectivity offering

TECHNOLOGY

Cat M1 is a higher bandwidth (1Mbit) standard for higher demand IoT devices such as cameras

NB-IoT is more directly comparable to other LPWANs with a 200kbit narrowband architecture, simplified modems, and can exist in guard bands and re-farmed cellular spectrum

NB-IOT

NB-IoT is particularly interesting, as now that standardisation is complete it should be possible to roll out widely and quickly as the telco operators integrate it into their existing infrastructure – which can be as simple as a software update. Vodafone launched commercially in Spain in February and are preparing in other countries

SigFox

TECHNOLOGY

Sigfox technology is a proprietary Ultra Narrowband (UNB) wireless protocol operating in the various international ISM bands. It therefore does not require licensing, but also must coexist with other

PERFORMANCE

Bandwidth is very low and is best considered in terms of messages per day: A maximum of 140 12byte messages per day uplink, and 4 8byte messages per day downlink are allowed to meet Duty Cycle restrictions.

ECOSYSTEM

An ecosystem of silicon and module vendors offer Sigfox compliant components suitable for building into or retrofitting onto equipment. Terminal equipment is inexpensive and available from numerous vendors

CLOUD

Messages from devices are managed by the Sigfox cloud, which provides management and data access through both a web portal and APIs for integration into back end systems

Weightless

SIG

The Weightless Special Interest Group develops a set of technical standards for LPWAN networks. Implementations are provided by member companies. Over time Weightless has developed a number of specifications for networks in different forms from TV Whitespace to Ultra Narrowband

WEIGHTLESS-W

Weightless-W is the original technology specification and covered operation in TV Whitespace. This standard has not yet been fully implemented largely due to global regulatory complexity and inconsistency and the rise of UNB technologies

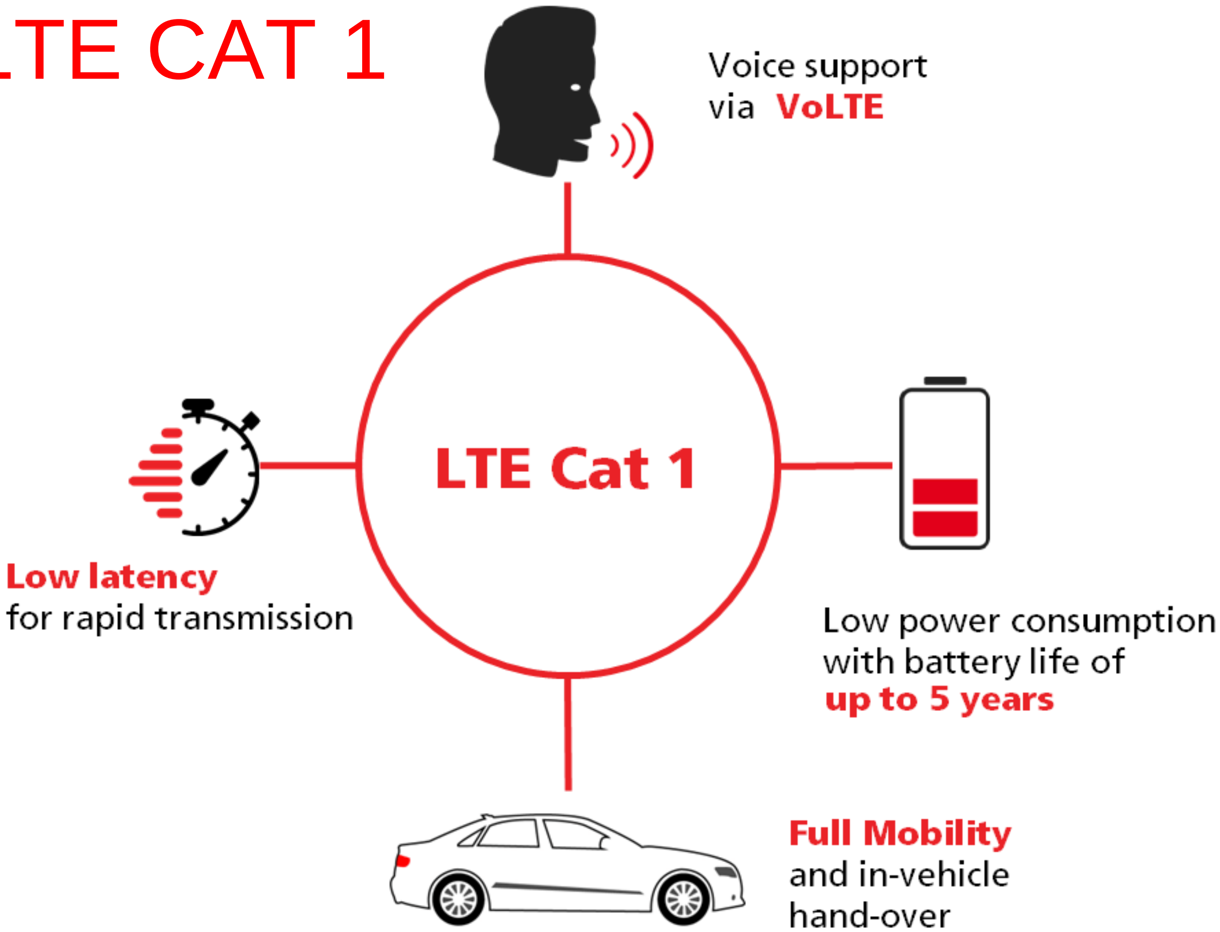
WEIGHTLESS-N

Weightless-N is a Narrowband variant of the specification published in May 2015. It operates in the sub-1GHz ISM bands. Weightless-N is being commercialised by NWave

WEIGHTLESS-P

Weightless-P is the most recent variant covering all sub 1Ghz ISM bands with narrowband protocol offering between 200bps and 100kbps over bidirectional links.

LTE CAT 1


Voice support
via VoLTE
LTE Cat 1
Low latency
for rapid transmission
Low power consumption
with battery life of
up to 5 years
Full Mobility
and in-vehicle
hand-over

LTE for Edge & IoT

	LTE Cat-1 (Today)	LTE Cat-M1 (Rel-13)	LTE Cat-NB1 (Rel-13)
Peak data rate	DL: 10 Mbps UL: 5 Mbps	DL: 1 Mbps UL: 1 Mbps	DL: ~20 kbps UL: ~60 kbps
Bandwidth	20 MHz	1.4 MHz	200 kHz
Rx antenna	MIMO	Single Rx	Single Rx
Duplex mode	Full duplex FDD/TDD	Supports half duplex FDD/TDD	Half duplex FDD only
Transmit power	23 dBm	20 dBm[1]	20 dBm[1]

Higher throughput, lower latency, full mobility

LTE CAT-M1/Cat-M/LTE-M

Cat-M (officially known as LTE Cat-M1) is often viewed as the second generation of LTE chips built for Edge & IoT applications.

It completes the cost and power consumption reduction for which Cat-0 originally set the stage.

By capping the maximum system bandwidth at 1.4 MHz (as opposed to Cat-0's 20 MHz), Cat-M has specific use cases for LPWAN applications like smart metering, in which only small amount of data transfer is required.

NB-Edge & IoT/Cat-M2

NB-Edge & IoT (also called Cat-M2) has a goal similar to that of Cat-M; however, it uses DSSS modulation instead of LTE radios.

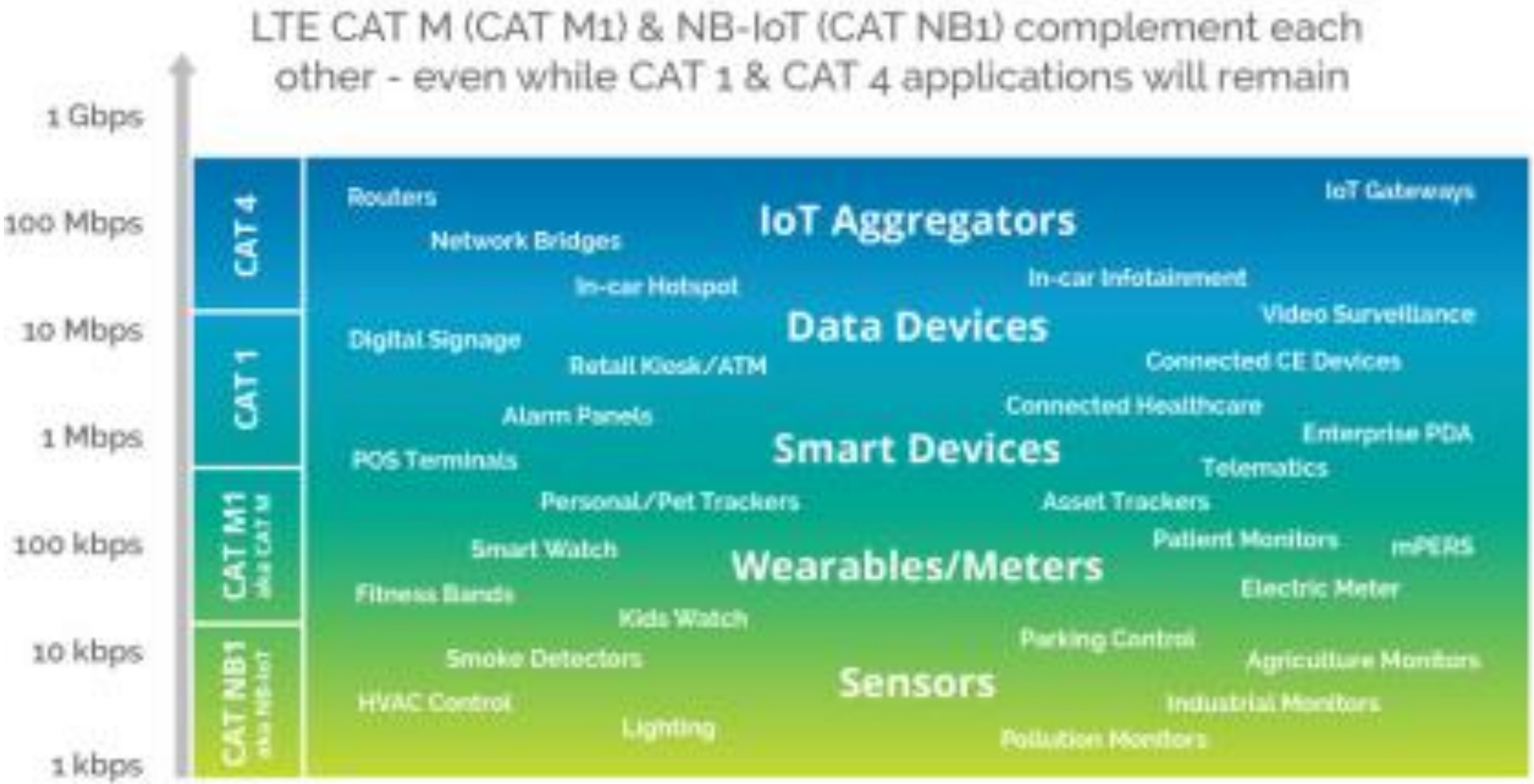
Therefore, NB-Edge & IoT doesn’t operate in the LTE band, which means that providers have a higher upfront cost to deploy NB-Edge & IoT.

Nonetheless, NB-Edge & IoT is being touted as the **potentially less expensive option**, because it eliminates the need for a gateway.

EC-GSM (formerly EC-EGPRS)

EC stands for Extended Coverage. EC-GSM is the Edge & IoT-optimized GSM network, the wireless protocol 80 percent of the world's smartphones use. As the name suggests, EC-GSM can be deployed in existing GSM networks—a huge advantage in terms of practicality and modularity, since a simple piece of software enables EC-GSM connectivity within 2G, 3G, and 4G networks.

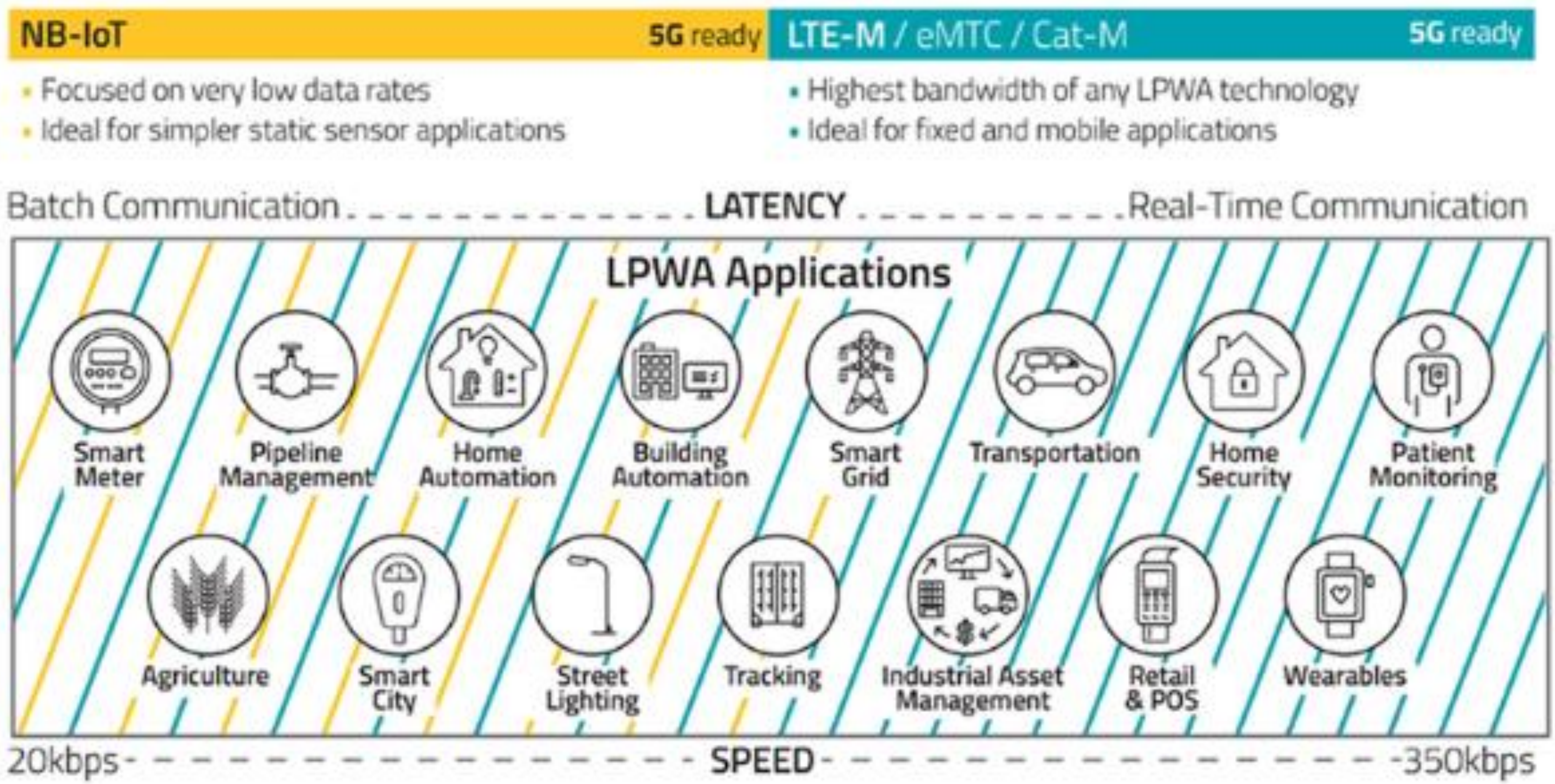
Edge & IoT Applications by LTE Category



5G Cellular Edge & IoT

Unlike the cellular Edge & IoT options above, 5G has yet to be officially defined. Next Generation Mobile Networks Alliance (NGMN) is pushing for specs for it to be 40 times faster than 4G while supporting up to 1 million connections per square kilometer. 5G is already enabling high-bandwidth, high-speed applications for Ultra-HD (4k) streaming, self-driving car connectivity, or VR/AR applications, such as Verizon and Samsung showcased at the Superbowl and Olympics respectively. What will the future hold?

LPWA Applications



Cellular Technology

CELLULAR STANDARD

There are now several LPWAN-like standards emerging from the 3GPP standardisation group as part of the LTE family. These standards have evolved through a number of names (Cellular IoT, NB-IoT, LTE cat MTC).

LICENSED SPECTRUM

These standards differ from the other LPWAN technologies in that they operate in the licensed bands used for other cellular communications and thus will be provided by existing (or new) cellular operators as part of their overall connectivity offering

TECHNOLOGY

Cat M1 is a higher bandwidth (1Mbit) standard for higher demand IoT devices such as cameras

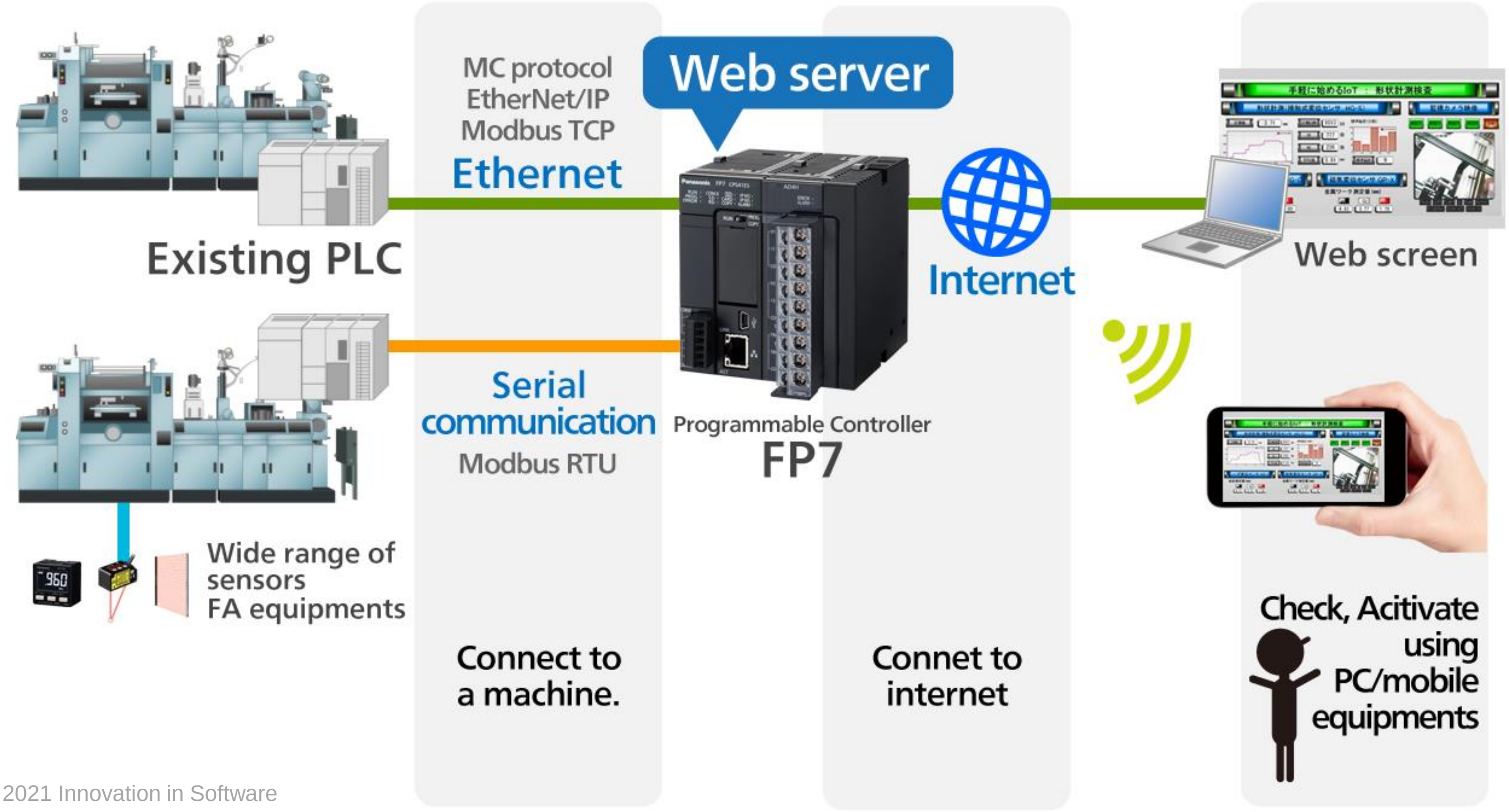
NB-IoT is more directly comparable to other LPWANs with a 200kbit narrowband architecture, simplified modems, and can exist in guard bands and re-farmed cellular spectrum

NB-IOT

NB-IoT is particularly interesting, as now that standardisation is complete it should be possible to roll out widely and quickly as the telco operators integrate it into their existing infrastructure – which can be as simple as a software update.

Edge & IoT Sensor Arch Concerns

End to End Communication

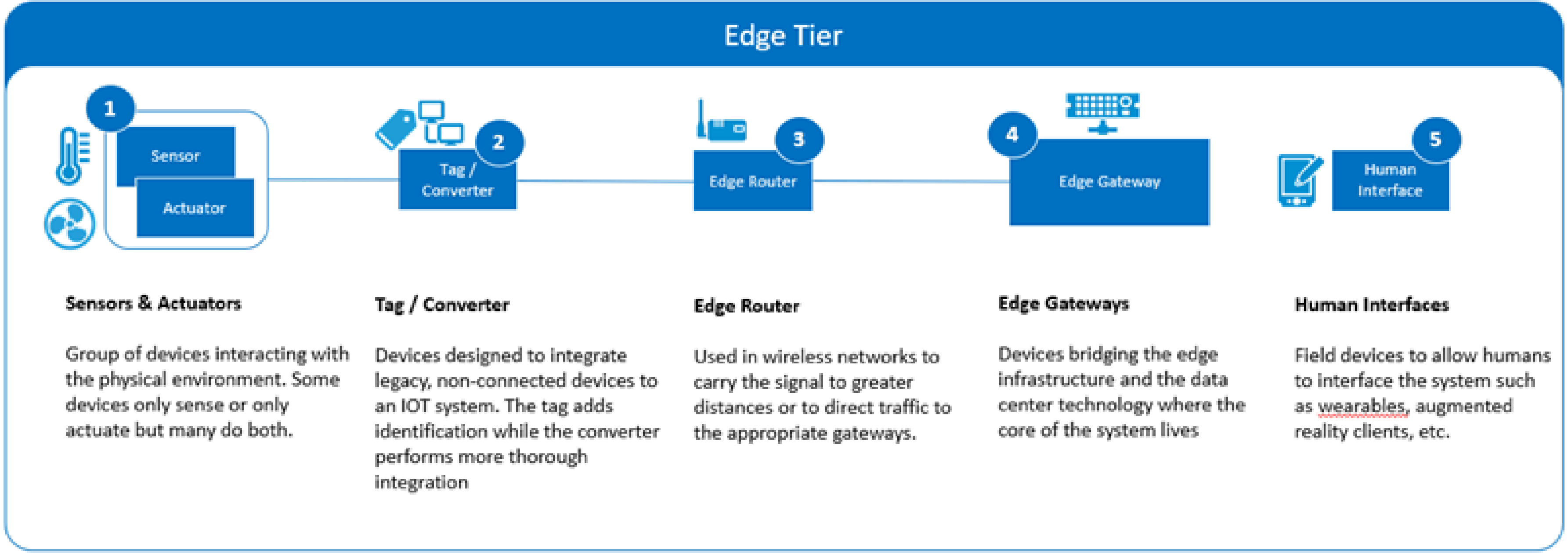


Thing -> Fog -> Cloud

Gateways act as bridges between sensors/devices and the cloud. Many sensors/devices will “talk” to a gateway and the gateway will then take all that information and “talk” to the cloud.

But why the extra step? Power consumption, bandwidth, security, latency, and filtering

Edge Tier Component Architecture



Powering Considerations

- *Things/nodes/gateways need an energy source, and ambient energy harvesting from external sources are used to power small autonomous sensors such as those based on MEMS* (microelectromechanical systems) *technology.*

Constrained Device Nodes

Category	Characteristics	Example
Class 0	• Severely constrained • Less than 10 KB RAM and 100KB of flash (ROM) • Typically battery-powered • Limited computation power to implement IP stack and associated security mechanism	Push button that sends 1 byte of information when changing its status
Class 1	• Approximately 10 KB RAM and 100 KB flash (ROM) • Cannot implement full IP stack, but can implement optimized stack (e.g., to support CoAP) • Can engage in meaningful conversations with network without gateway • Support limited set of security functions	Environmental sensors
Class 2	• Running full implementations of IP stack on embedded devices • Approximately 50 KB RAM and 250 KB flash (ROM)	Smart power meter

- *Constrained nodes have limited resources that impact their networking feature set and capabilities. Therefore, some classes of Edge & IoT nodes do not implement an IP stack. The network that build upon these devices often called low-power lossy networks (LLNs).*

Best Practices for Building Sensor Networks

- Pay for what you need
- Identify each sensors role
- Understand each sensors capabilities
- Consider testing and monitoring
- Define connectivity
- Identify replay scenarios
- Physical and virtual security
- Consider multiple vendors
- Sensor expiration timing
- Data transfer timing
- Send deltas
- Consider performance
- POC, POV, FlashBuild, Start Small

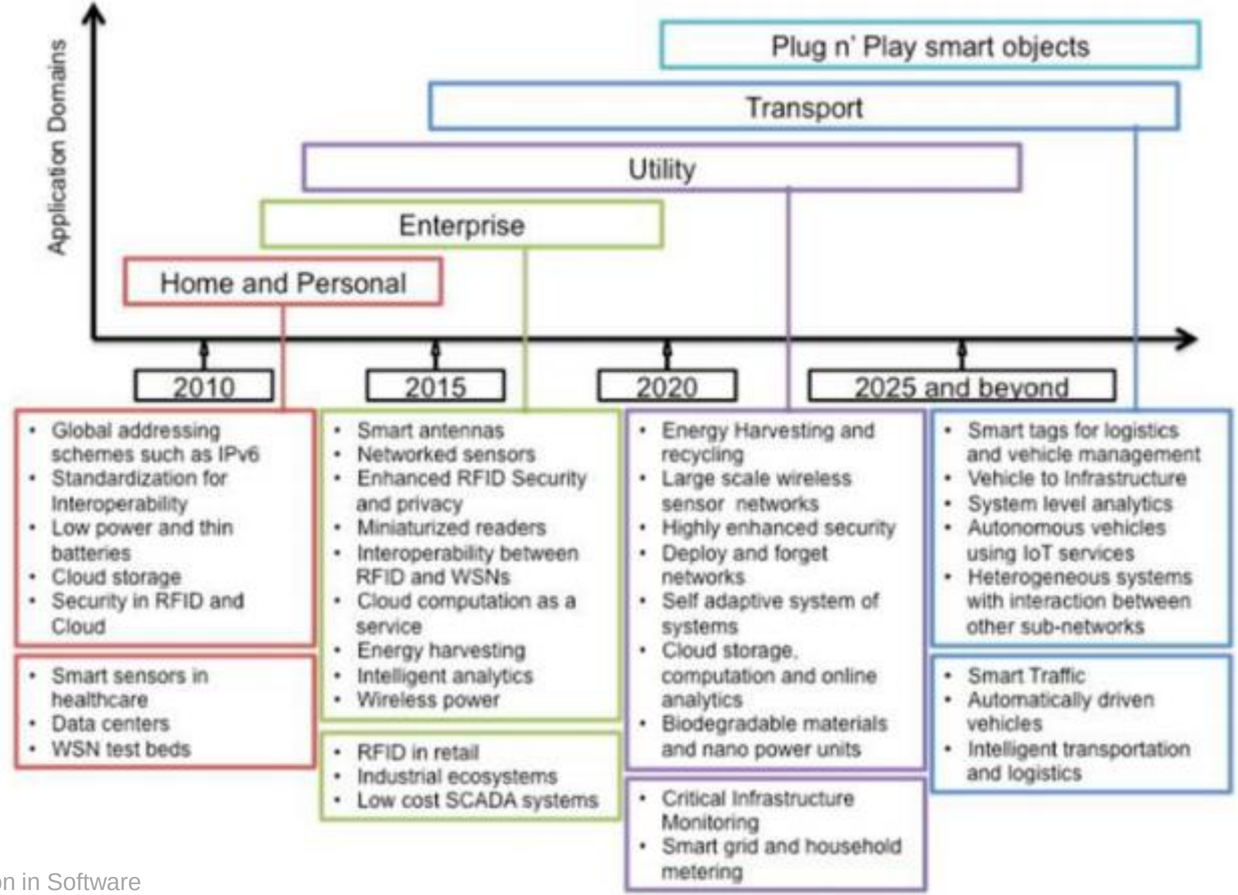
Application of Edge & IoT


FEATURED VIDEO
1:31 / 1:31
CC
YouTube

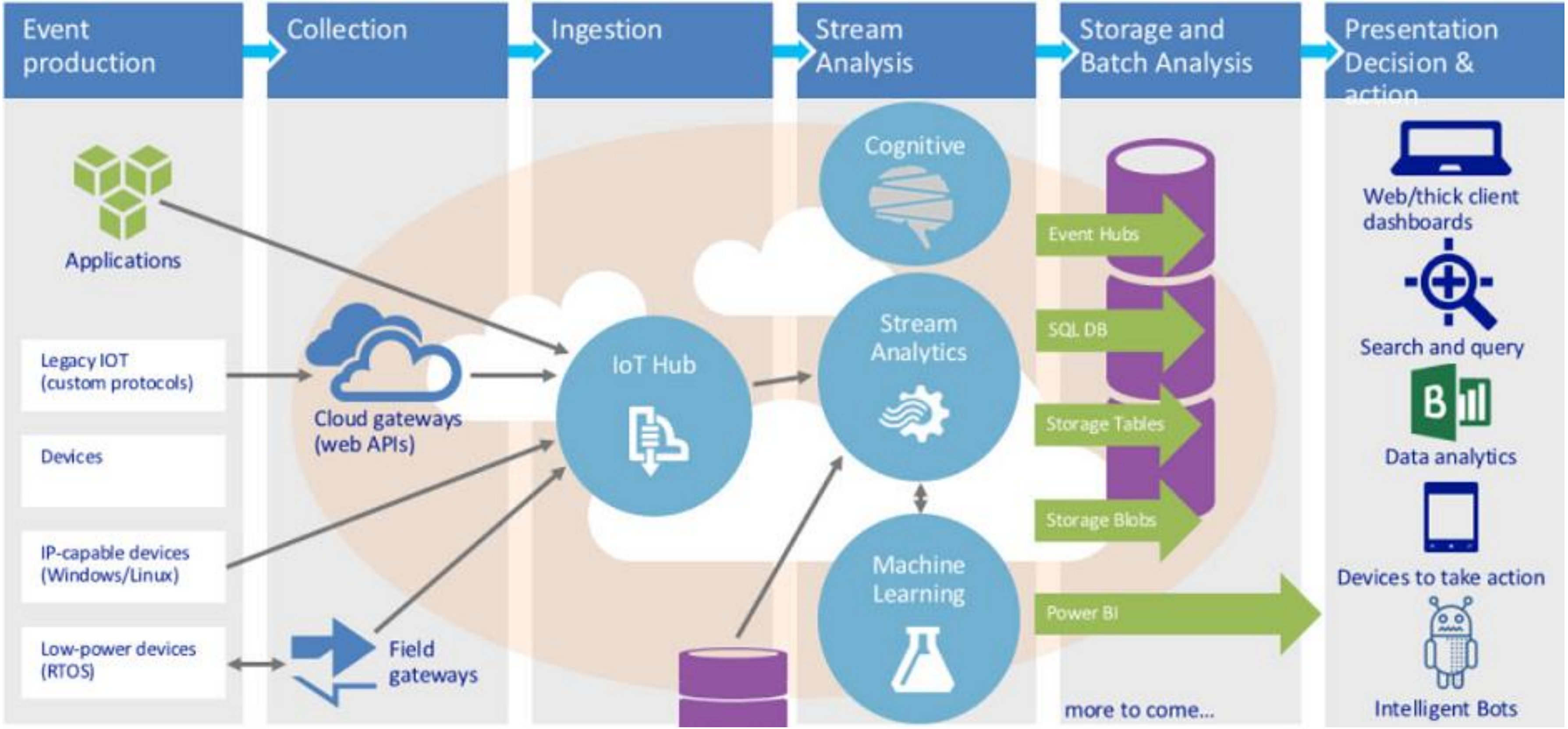
Fundamental Assumptions of Edge & IoT Applications

- Various wireless connections will be used
- Devices will range from tiny MCUs to high performance systems with the emphasis on small MCUs
- Security is a core requirement
- Operation may not be continuous
- Data will be stored in the cloud and may be processed in the cloud, whether private, public or hybrid
- Connections back to the data storage are required
- Routing of information through wireless and wired connections to the data storage is required

Edge & IoT Application Domains



Edge & IoT Application Patterns

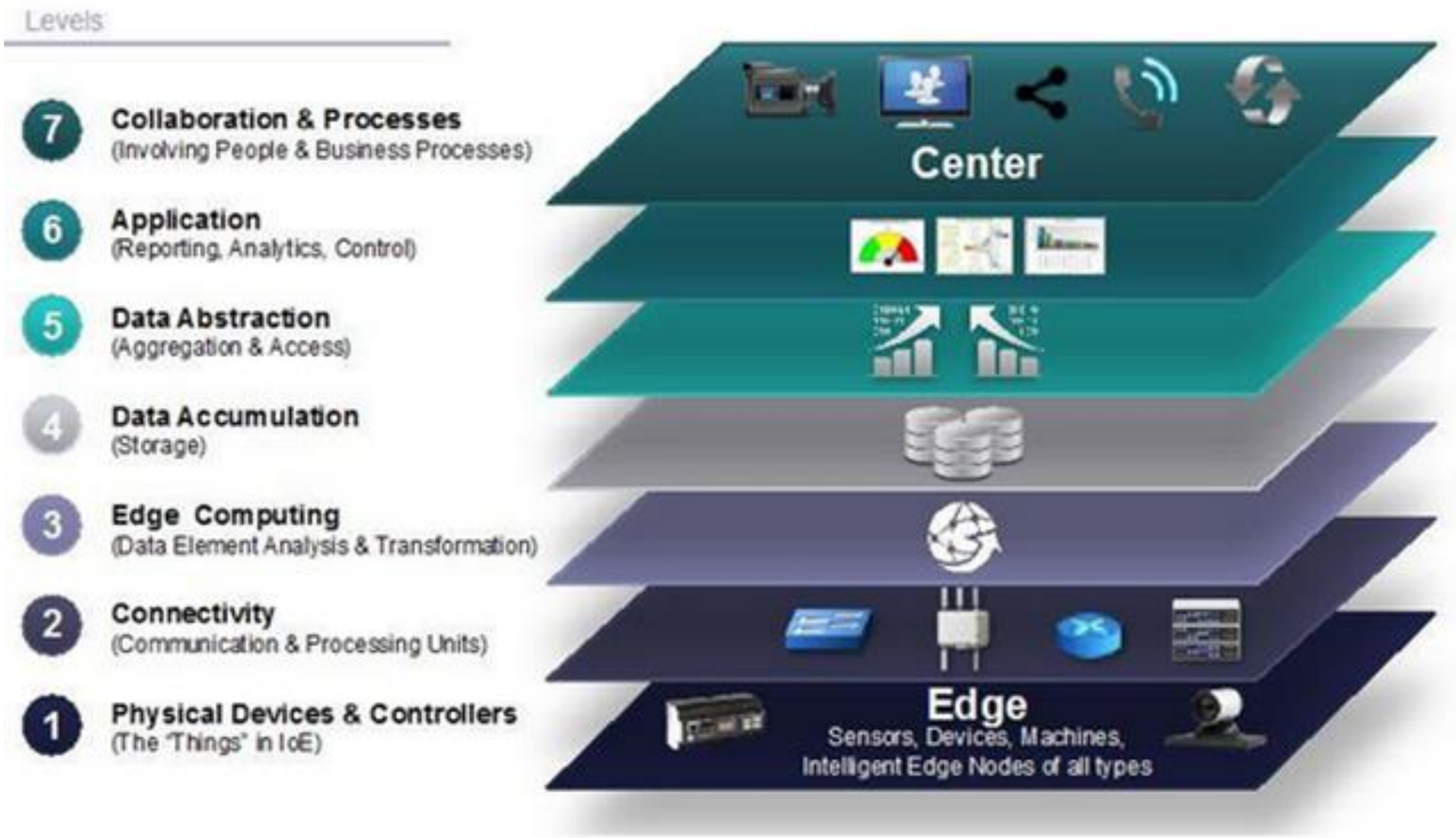


Fundamental Areas of Edge & IoT Applications

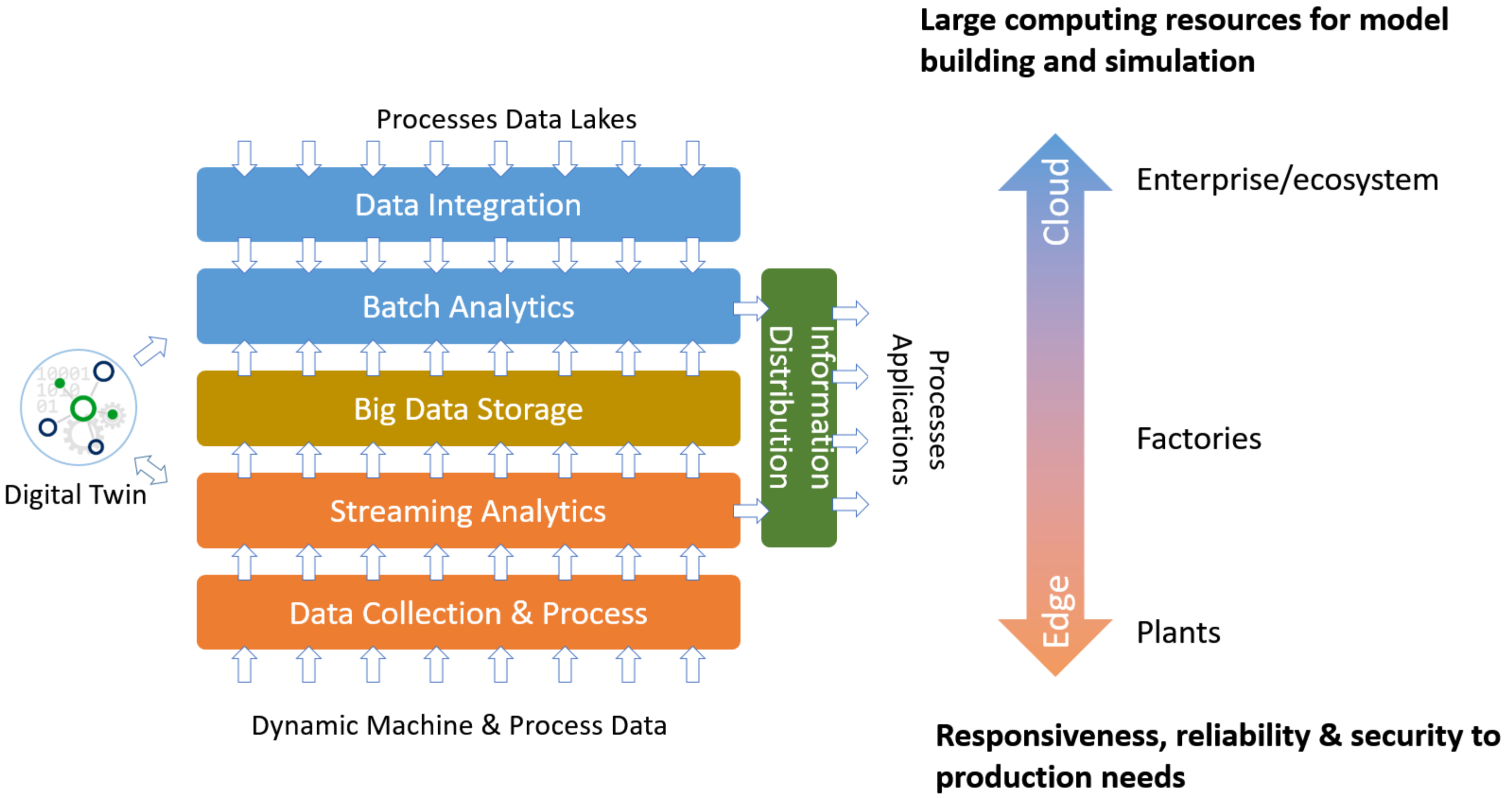
- Event production
- Data collection
- Data ingestion
- In-motion stream analysis
- Data storage
- Batch analysis
- Visualization
- Actionable insight

Edge & IoT Service Provider Application Architecture

Edge & IoT Reference Model



Digitizing the Physical World



Consumer Application of Edge & IoT

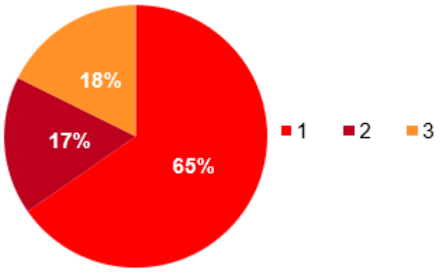
Consumer vertical trends

- One of the potentially largest IoT markets is consumer and home applications of IoT
- Some of the most common IoT consumer applications include the use of the Internet to control smart appliances at home or office, remote monitoring and control of heating and lighting, improving appliance performance through automated error reports, security systems and fire and burglar alarm systems, as well as other inventory tracking, food temperature monitoring, and tank level gauging (beer, other liquids)

Identified use cases

- Home security & home monitoring
- Personal wellness
- Smart appliance and gadgets

Number of identified use cases



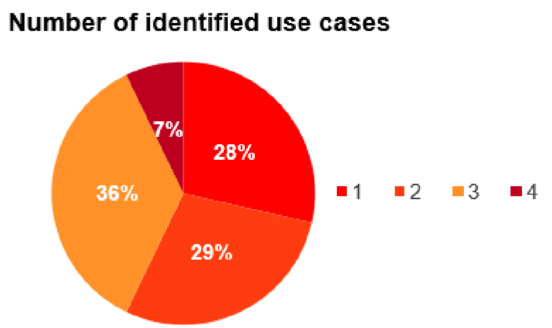
Government Application of Edge & IoT

Government vertical trends

- IoT will also advance government processes for public safety, traffic management, asset monitoring, surveillance, and toll collection, etc. Many large IT vendors are already looking to use IoT to automate and monitor important government functions
- Some of the most common IoT government solutions include automation of public transit, management and control of emergency services, public safety/surveillance, and public infrastructure asset management (bridges, roads, tunnels)

Identified use cases

- Environmental monitoring detection
- Intelligent transportation systems (parking management, traffic management, traveler info etc.)
- Public infrastructure asset management
- Public safety and emergency response



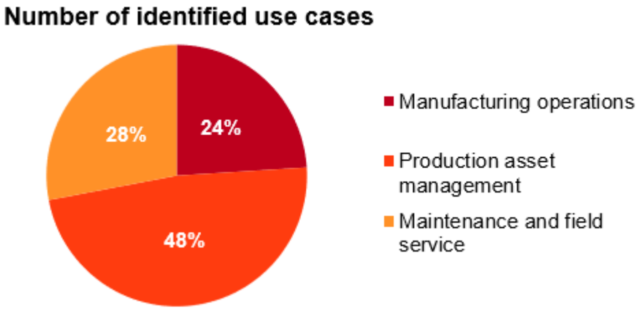
Manufacturing Application of Edge & IoT

Manufacturing vertical trends

- Manufacturing will be the largest IoT industry for the next few years. IoT has already been employed by many manufacturers in both discrete and process manufacturing. This trend will accelerate with increasing pressure to automate and drive out inefficiency in the manufacturing process, to develop new revenue streams with remote services, and to improve production uptime
- Some of the most common IoT solutions include production asset management, manufacturing operations control and measurement, remote diagnostics of industrial equipment and vehicles, remote maintenance, plant floor communications to programmable logic controllers, next-generation supply chain management and inventory management

Identified use cases

- Maintenance and field service
- Manufacturing operations
- Production asset management



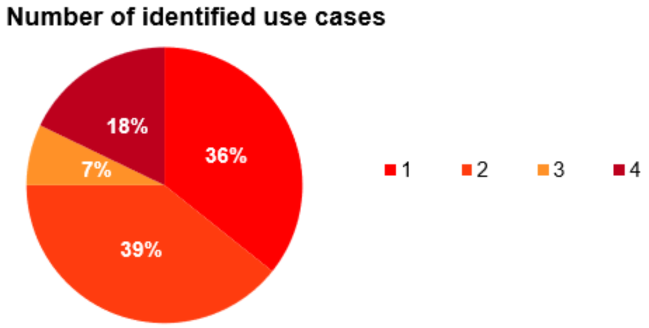
Retail Application of Edge & IoT

Retail vertical trends

- IoT is already impacting the retail industry, whether it's through product tracking from distribution through the warehouse, in-store customer kiosks, in-store promotion, or business process automation. The potential of IoT in the retail industry is huge. IoT solutions can optimize inventory, personalize in-store promotions, or even handle payment services
- Some of the most common IoT retail solutions include real-time inventory data, customer in-store kiosks designed to make individual special offers, digital signage, telemetry for vending machines, wireless payment solutions, RFID tag-based warehousing

Identified use cases

- Digital signage
- In-store contextualized marketing
- NFC payment/shopping
- Omni-channel operations



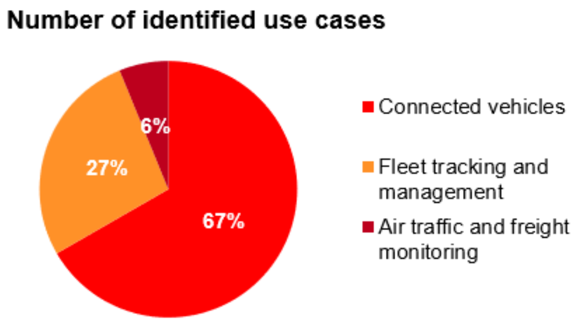
Transportation Application of Edge & IoT

Transportation vertical trends

- The transportation sector also shows tremendous IoT opportunity. IoT will help transportation and logistics companies to maximize capacity and improve efficiencies as well as to meet increasing governmental regulation and compliance. With IoT solutions, transportation and logistics companies are able to monitor their workforce and asset utilization in real time, transport goods and people more safely and efficiently and, in turn, increase end-customer satisfaction
- Some of the most common IoT transportation solutions include vehicle tracking, freight monitoring, automated monitoring of air traffic, connected fleets/asset management

Identified use cases

- Air traffic and freight monitoring
- Connected vehicles
- Fleet tracking and management



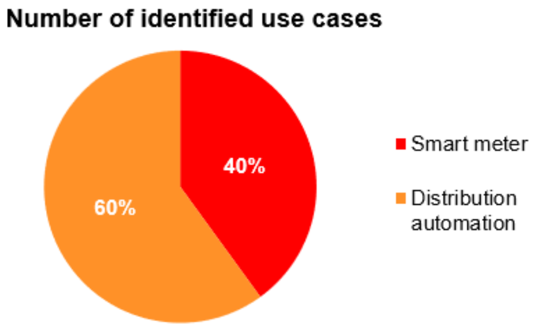
Utilities Application of Edge & IoT

Utilities vertical trends

- The utilities vertical will see changes through IoT solutions for intelligent power networks, offering utilities efficient load sharing, monitoring and reporting. The consumer side of utilities such as smart metering and smart homes are included in the Consumer sector
- Some of the most common IoT energy/utility solutions include smart grids/smart metering, detection of power network losses or theft, and pipeline monitoring

Identified use cases

- Smart meter
- Distribution automation



Other Application of Edge & IoT

Trends for other industries

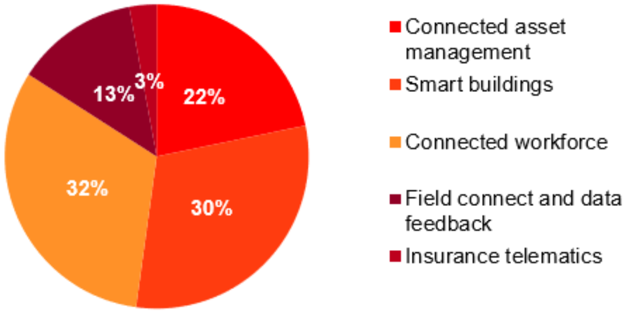
This includes IoT solutions in other industries, such as:

- Smart building including heating, lighting controls, security systems and analytics-based energy management and maintenance, staff communications and connection
- Insurance telematics using driving behavior to offer differentiated insurance packages and improve road safety
- Resources solutions including connecting remote assets on the field with real-time or periodic feedback on status for data collection, emergency incidents and change prediction, GPS-based seeding, watering, fertilization, pesticide, and yield management, as well as supervisory control and data acquisition systems in oil production

Identified use cases

- Connected asset management
- Smart buildings
- Connected workforce
- Insurance telematics
- Field connect and data feedback

Number of companies in the identified use cases



Edge & IoT Application: Drive Through Payments

The opportunity

- Everything becomes drive-through with a connected car that communicates with financial service providers.
- Road taxes, insurance, parking tickets and fines can all be dealt with on the go.
- Leveraging this type of IoT enabled features will greatly help car manufacturers get ahead of the competition.

The threat

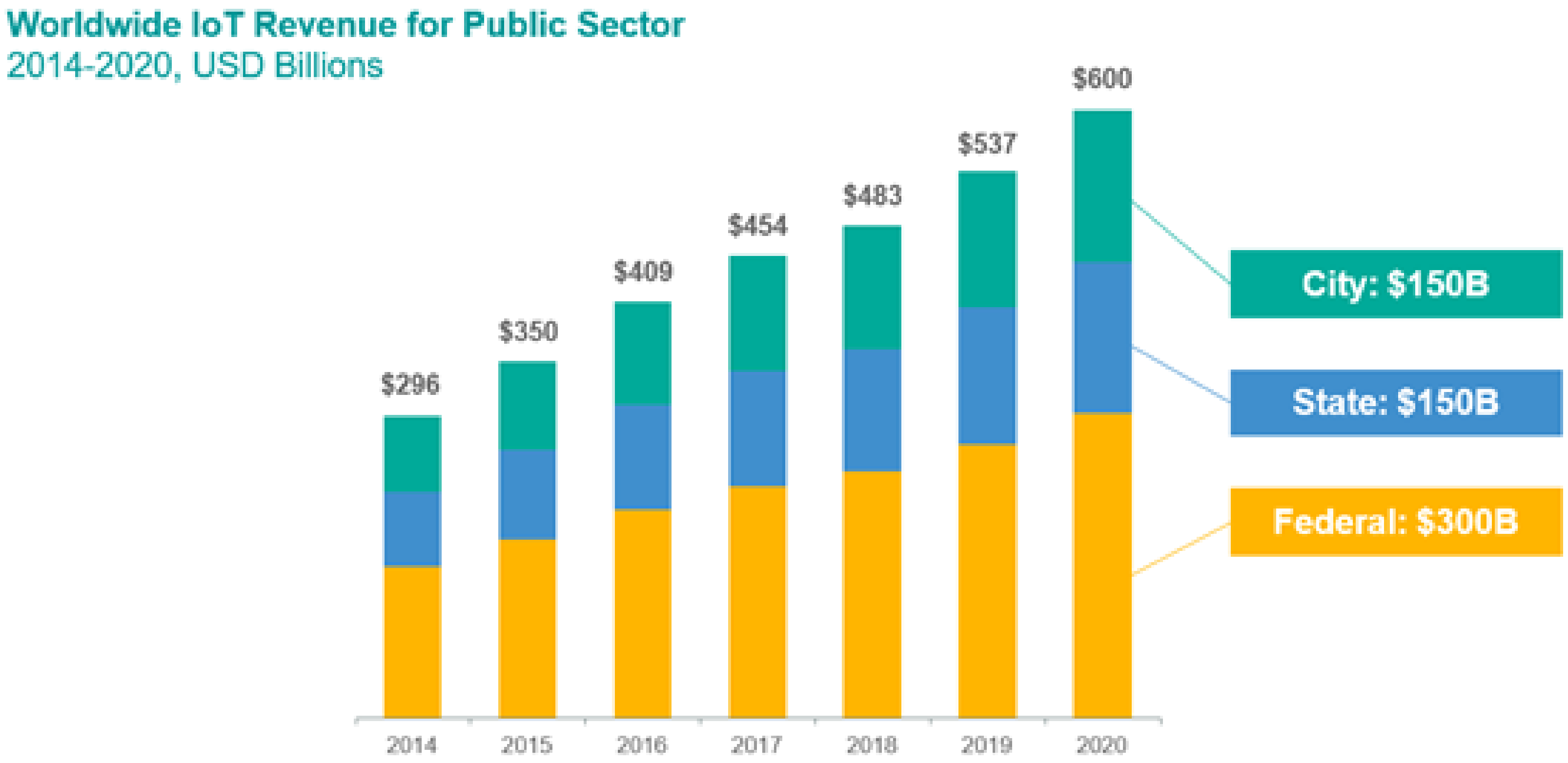
- Confidentiality and privacy are on top of the concerns list when dealing with financial credentials and PII.
- Security flaws in this type of scenario can lead to identity theft, financial frauds and privacy breaches with serious consequences on both users and service providers.
- Compliancy with data protection and PCI regulations must be thoroughly managed to avoid fines and penalties.

Edge & IoT Application: Localized Routing

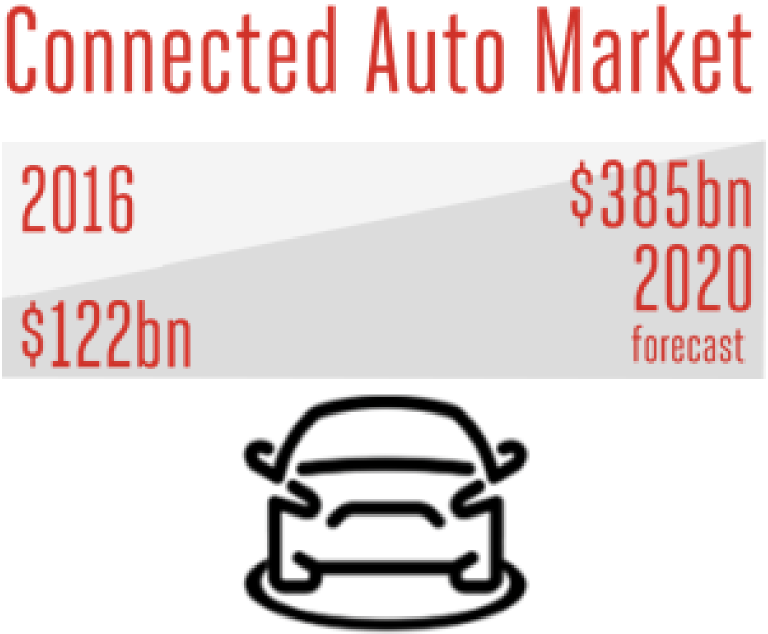
Indoor localization Technology Comparison

IEEE 802.11 n [67] **802.11 ac 802.11 ad**	250 m outdoor 35 m indoor couple of meters	600 Mbps 1.3 Gbps 4.6 Mbps	Moderate Moderate Moderate	Widely available, high accuracy, does not require complex extra hardware	Prone to noise, requires complex processing algorithms
UWB [68]	10-20m	460 Mbps	Moderate	Immune to interference, provides high accuracy,	Shorter range, requires extra hardware on different user devices, high cost
Acoustics	Couple of meters		Low-Moderate	Can be used for proprietary applications, can provide high accuracy	Affected by sound pollution, requires extra anchor points or hardware
RFID [69]	200 m	1.67 Gbps	Low	Consumes low power, has wide range	Localization accuracy is low
Bluetooth [70]	100m	24 Mbps	Low	High throughput, reception range, low energy consumption	Low localization accuracy, prone to noise
Ultrasound [71]	Couple-tens of meters	30 Mbps	Low-moderate	Comparatively less absorption	High dependence on sensor placement
Visible Light [72]	1.4 km	10 Gbps [73]	Relatively higher	Wide-scale availability, potential to provide high accuracy, multipath-free	Comparatively higher power consumption, range is affected by obstacles, primarily requires LoS
SigFox [43]	50 km	100 bps	Extremely low	Wide reception range, low energy consumption	long distance between base station and device, sever outdoor-to-indoor signal attenuation due to building walls
LoRA [43]	15 km	37.5kpbs	Extremely low	Wide reception range, low energy consumption	long distance between base station and device, sever outdoor-to-indoor signal attenuation due to building walls
IEEE 802.11ah [43]	1km	100 Kbps	Extremely low	Wide reception range, low energy consumption	Not thoroughly explored for localization, performance to be seen in indoor environments
Weightless	2 km for P, 3 km for N, and 5 km for W	100 kbps for N and P, 10 Mbps for W	Extremely low	Wide reception range, low energy consumption	long distance between base station and device, sever outdoor-to-indoor signal attenuation due to building walls

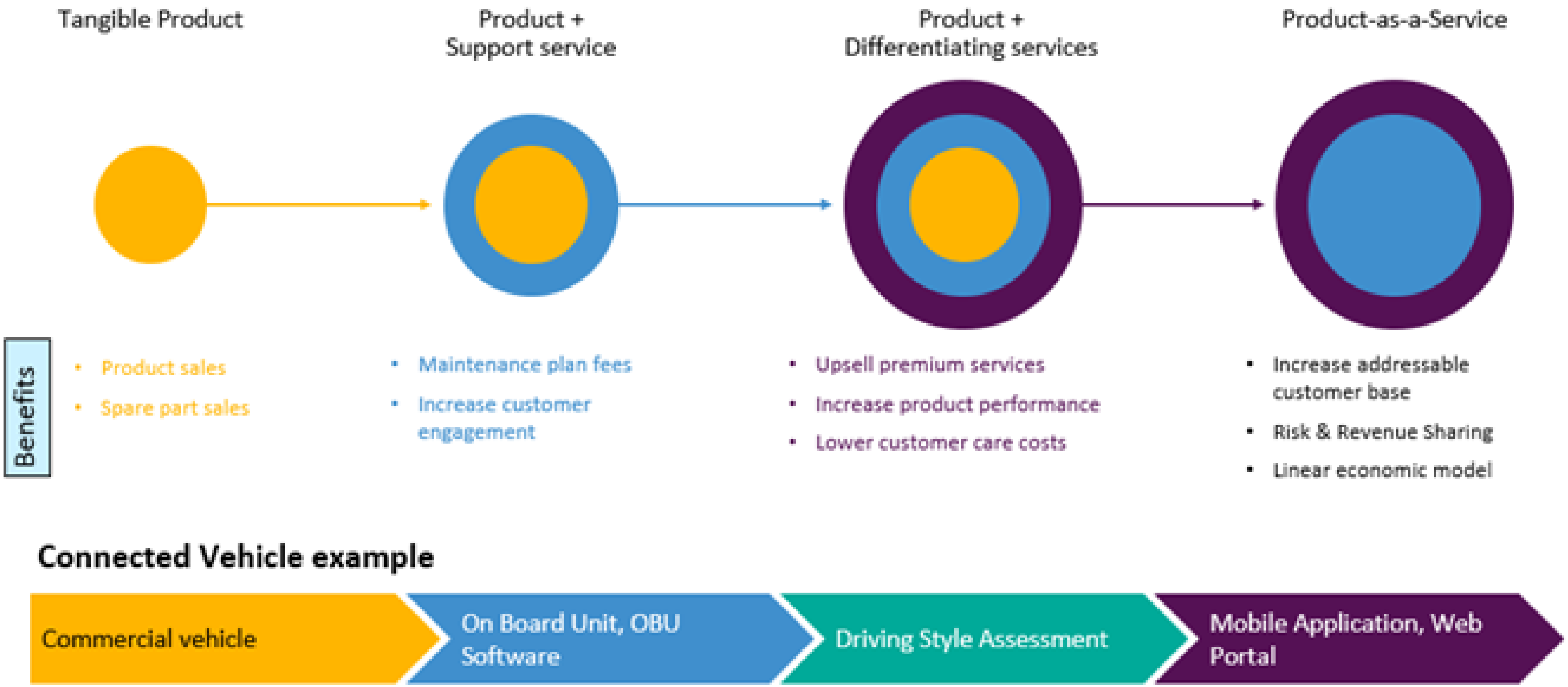
Edge & IoT Application Investment: Smart Cities



Edge & IoT Application Investment: Vehicles



Shifting from Product to Service Models with Edge & IoT



Edge & IoT Application Infrastructure Requirements

Infrastructure Area	Infrastructure Requirement	Description
Servers & sizing	Core Platform Sizing	The core IoT platform should have a minimum of ## cores
	Vendor Standardization	The IoT platform should run on blades whenever possible
	Virtualization	The IoT platform's infrastructure should target 70% virtualization
		...
Network	Vendor Standardization	The IoT platform should use routers a minimum bandwidth of x GBps
	Physical Channels	The network should use cables of type x to support anticipated traffic
	Communication Protocols	The platform should communicate using built-in Web Services
		...
Storage & Backup	Storage Sizing	The platform should utilize a SAN of ## GB at a minimum
	Live Backup	The platform should support live backup for the following data sets
	Offline Backup	The platform should support daily backup for the following data sets
		...
Operating Systems and Clients	Operating System Standardization	The platform components should run on xxxxx Server
	Thin Client Support	The platform should support a thin client running on Chrome
	Thick Client Support	The platform should support xx thick client
		...

- Edge & IoT Solutions World Congress
- AWS re:Invent
- Industry of Things World
- Smart Cities Summit
- Edge & IoT World
- IEEE World Forum on Edge & IoT

Consumer Edge & IoT Application Patterns

	Est. Market size 2020	Applications & Uses		Example players
Connected Home	\$75bn - \$95bn	• Home security • Connected furniture	• Home automation • Smart metering	
Connected Health	\$300bn - \$360bn	• Patient monitoring • Healthcare devices	• Emergency rescue information • Remote diagnosis	
Connected Cars	\$55 bn - \$65 bn	• Usage-based insurance • Predictive maintenance	• Built-in connectivity • Enhanced safety features	
Connected Retail	\$220bn - \$260bn	• Payments & promotions • Connected wearables	• Supply chain efficiency • Vending machines & automation	
Connected Cities	\$700bn - \$860bn	• Smart metering • Intelligent transport	• Waste management • Air quality monitoring	

6 Critical Areas for Edge & IoT Applications

Access & Secure

Implement connected devices to enable secure access **into a space** such as a home or building

Find & Track

Use real-time location data to track the people and assets **within a space** e.g. improve positioning of displays in a retail store using foot traffic data from video analytics software

Enable & Manage

Integrate software and hardware of a space such that **better experiences can be delivered** to the guests e.g. a hotel room is conditioned to the guest's preferred temperature before the guest enters the room

Diagnose & Treat/Service

Analyze data from assets (e.g. HVAC equipment) in a space to **diagnose problems** that might affect the performance of that asset

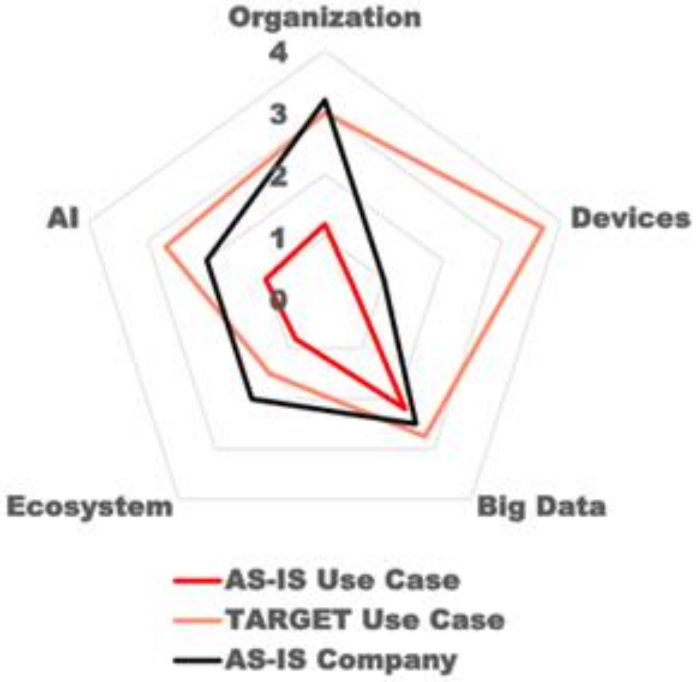
Automate, Predict

Develop software and algorithms that **predict anomalies** in the energy use and comfort of a space and **automatically adjust** the settings of the facility equipment to correct for the anomalies

Monetize

Collect and deliver sensor data (both data about a space's assets and the people who reside/visit the space) needed for clients to deliver **new services for homes, buildings, and cities**

Measuring Edge & IoT Maturity Level



DIMENSIONS

ORGANIZATION – Strategic and organizational foundation for IoT use cases

ARTIFICIAL INTELLIGENCE – Ability to leverage AI methods on data present in the company

DEVICES – Access to suitable devices and ability to manage these, ensuring a reliable information flow

ECOSYSTEM – Ability to connect with third parties to enable cross-company service delivery and value creation

BIG DATA – Ability to aggregate, handle, store, analyze large amounts of data within required time constraints (near real-time, real-time)

Funding Edge & IoT

Government Smart Cities Initiative

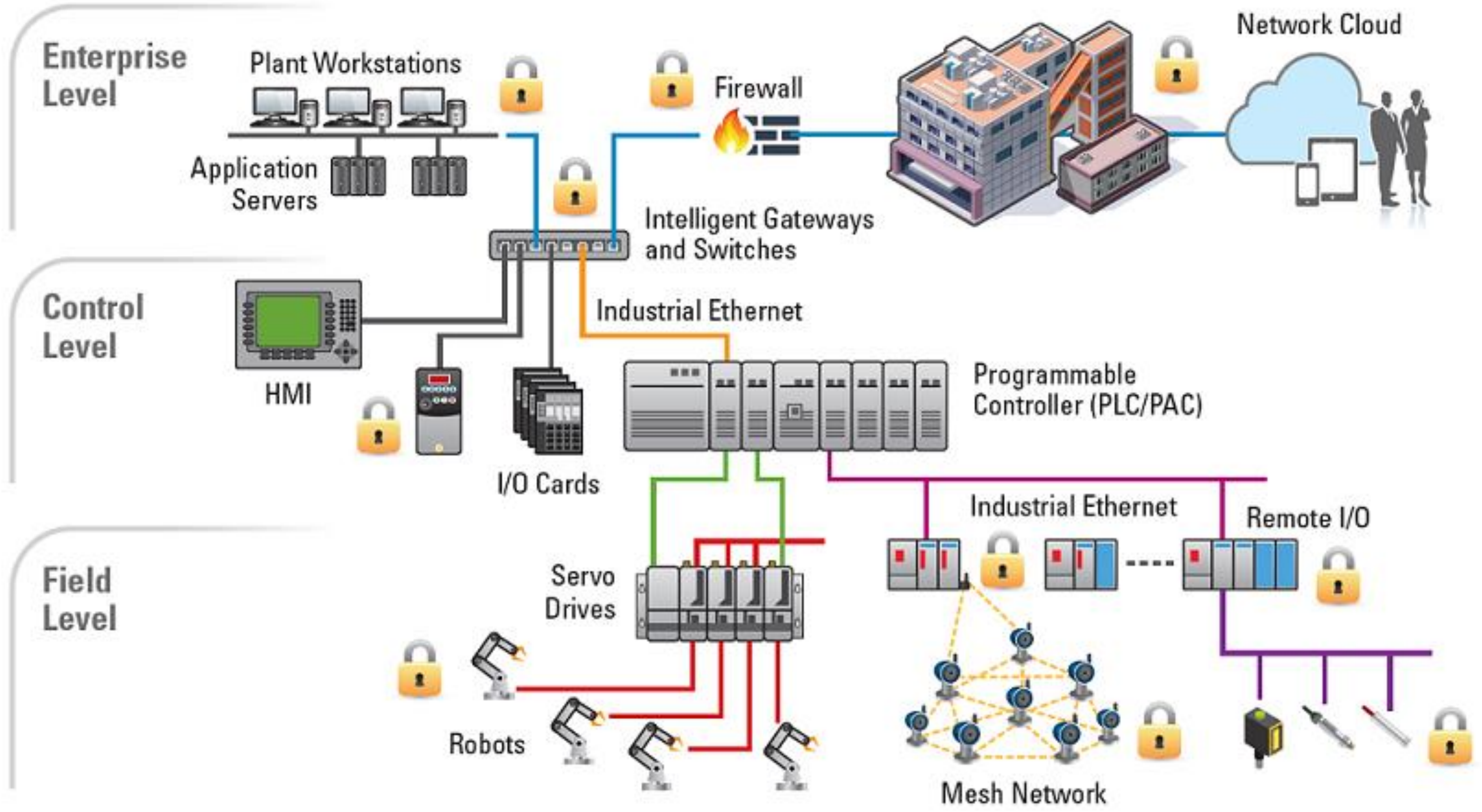
On September 14, 2015 the White House announced a new “Smart Cities” initiative to help communities solve public problems and improve city services.

> *“Every community is different, with different needs and different approaches. But communities that are making the most progress on these issues have some things in common. They don't look for a single silver bullet; instead they bring together local government and nonprofits and businesses and teachers and parents around a shared goal.”*

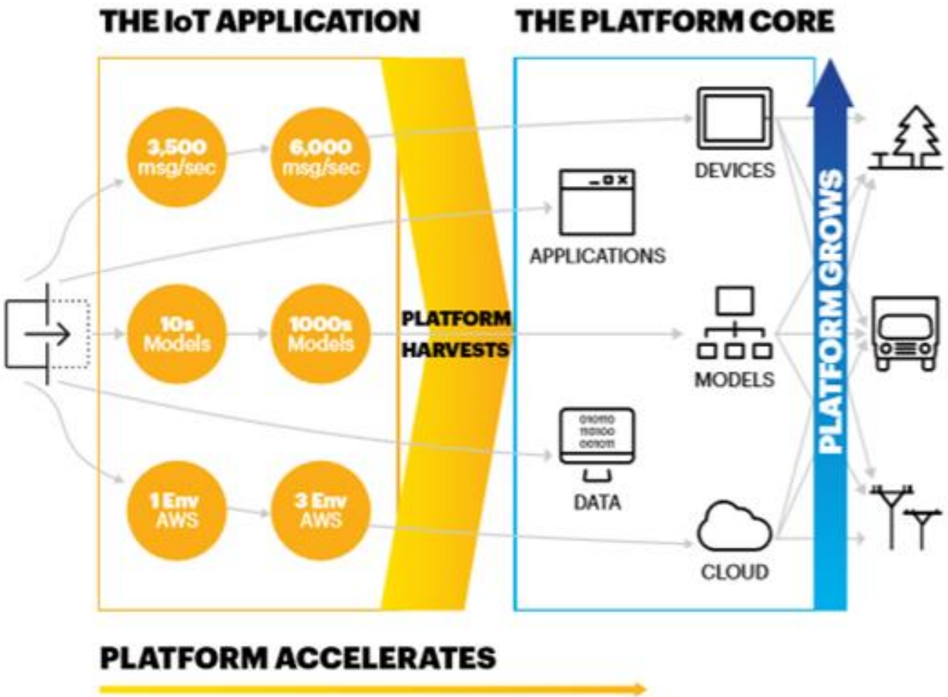
– **President Barack Obama**

The Administration will invest $160 million in federal programs and leverage new technology collaborations to assist local communities.

Industrial Edge & IoT (IEdge & IoT) Design and Practices



Platforms Accelerate Edge & IoT Application Delivery



PLATFORM ACCELERATES DEVELOPMENT

Agility to rapidly develop and evolve use case.

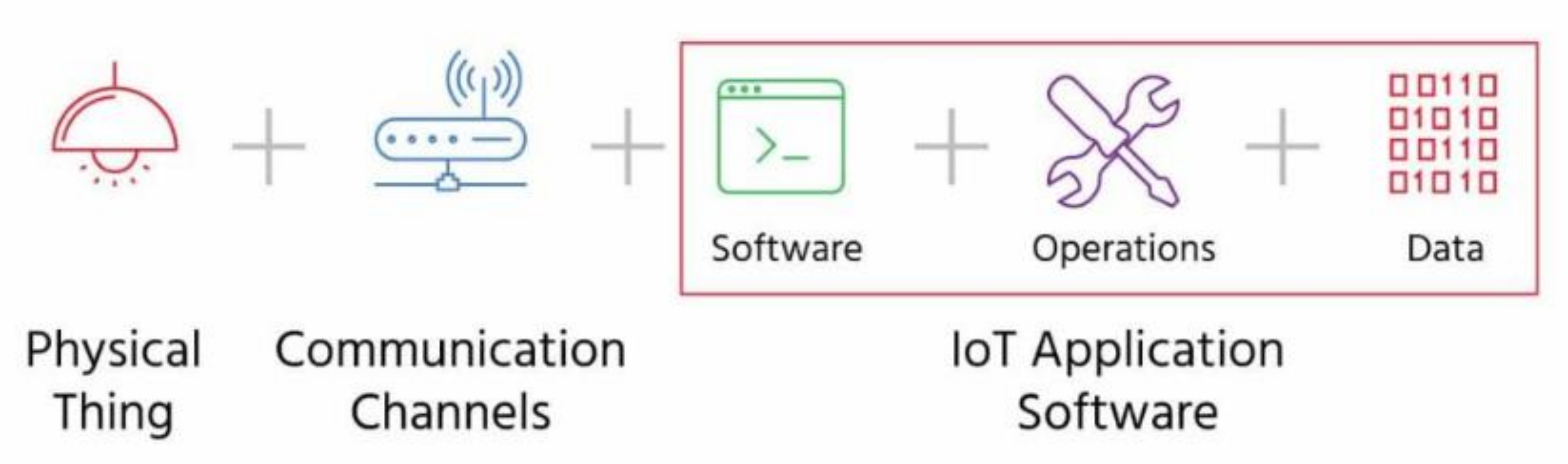
Scale number of devices, volumes of data, analytical models.

PLATFORM GROWS NEW USE CASES

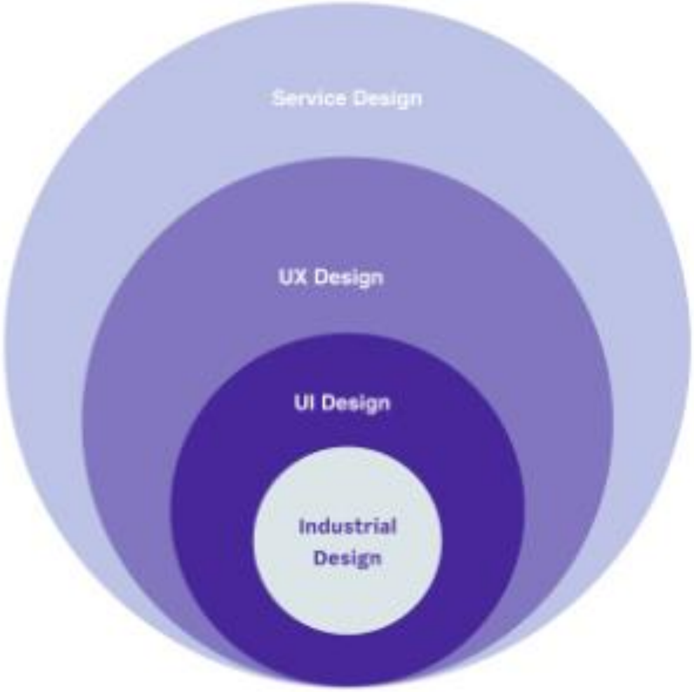
Agility to harvest, discover, and reuse IoT components.

Scale horizontal components to scale across verticals.

Developing an Enterprise Edge & IoT Solution



Edge & IoT Design Principles



- Don’t believe the hype
- Ensure SW & HW lifespans align
- Empower users over their information e.g. GDPR
- Information flow transparency
- Collect useful data
- Design for privacy
- Security in layers
- Improve lives through Edge & IoT

Metro-Lab Network Edge & IoT Partnership

The network was launched by 20 city-university partnerships across the United States.

The **Goals of the Network** are:

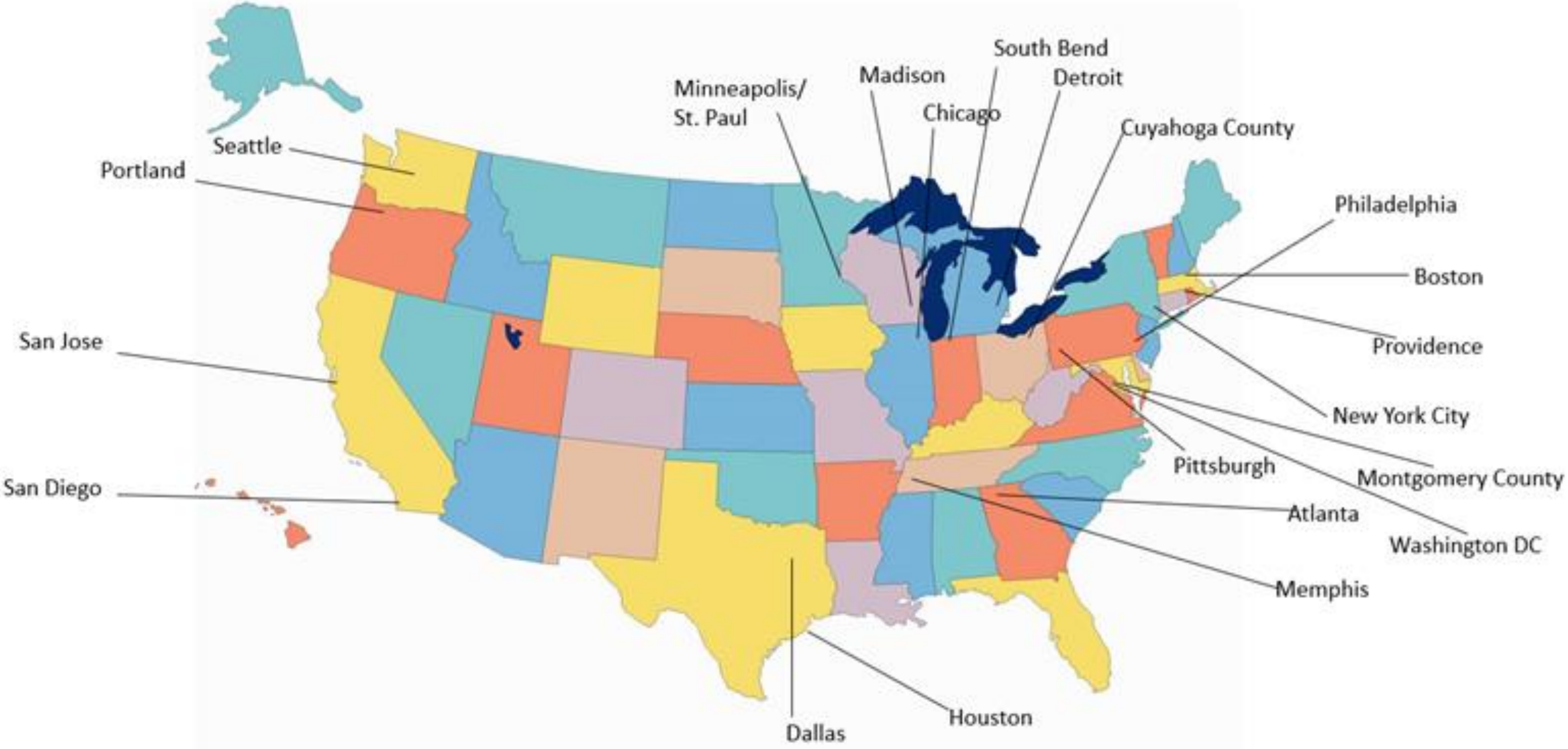
- Enable the City-University Partnerships to share their projects and ensure broad adoption of tools
- Identify common problems shared by metro areas
- Create a platform of the Network members to jointly plan and seek resources

The **Scope of the Network** is:

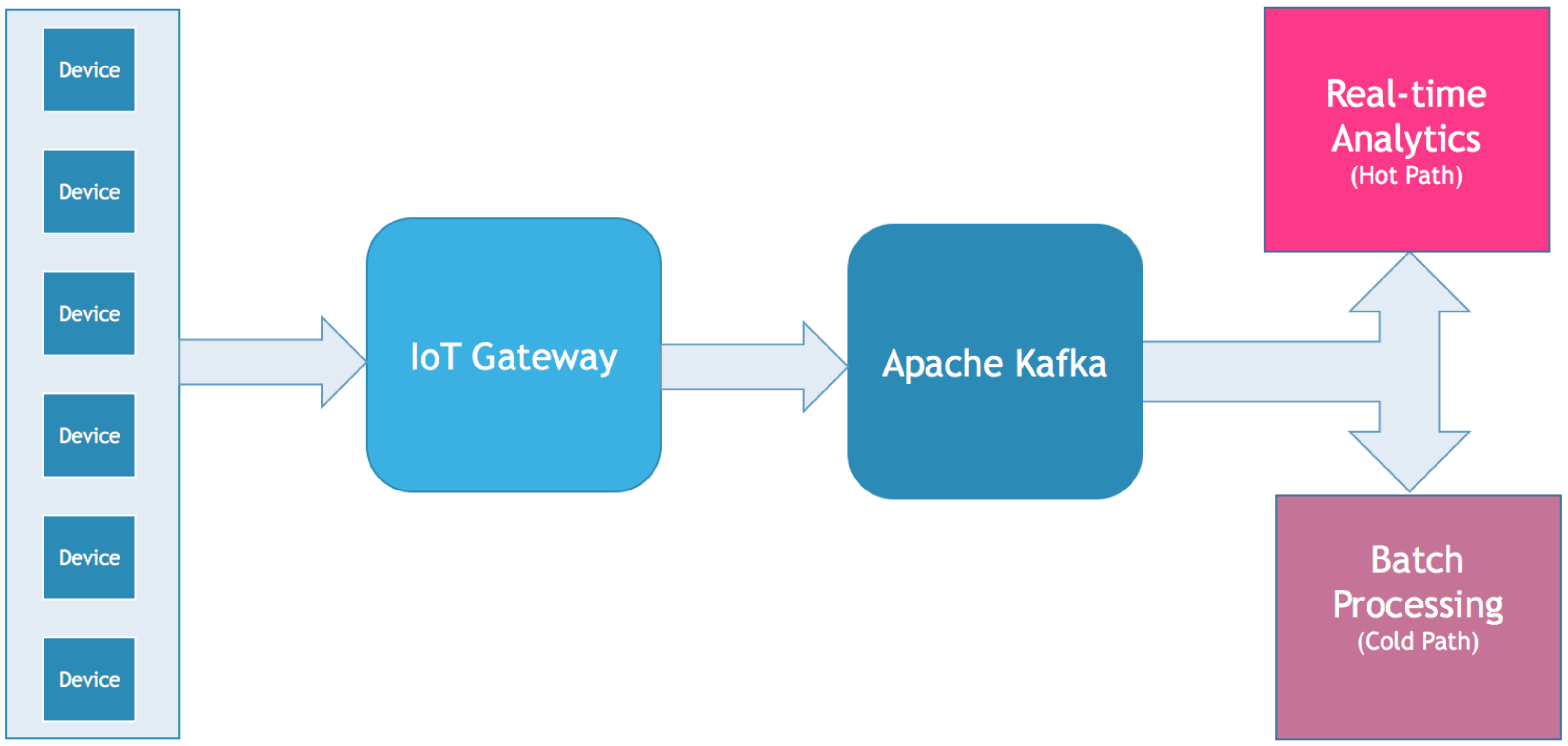
- *Public Private Infrastructure:* This may include water, sewer, communication, transportation, land and buildings
- *Public-Private Services, emphasizing underserved populations:* This may include public safety, education, energy, health, human services, parks and recreation, economic development and arts organizations.
- *Democratic Governance:* This may include planning, equity and citizen participation.
- *Public Policy and Management:* Projects will focus on data driven decision making.

Project design will result in 4 broad areas – Multi-city projects outcomes, network outcomes, single-city project outcomes, urban science outcomes

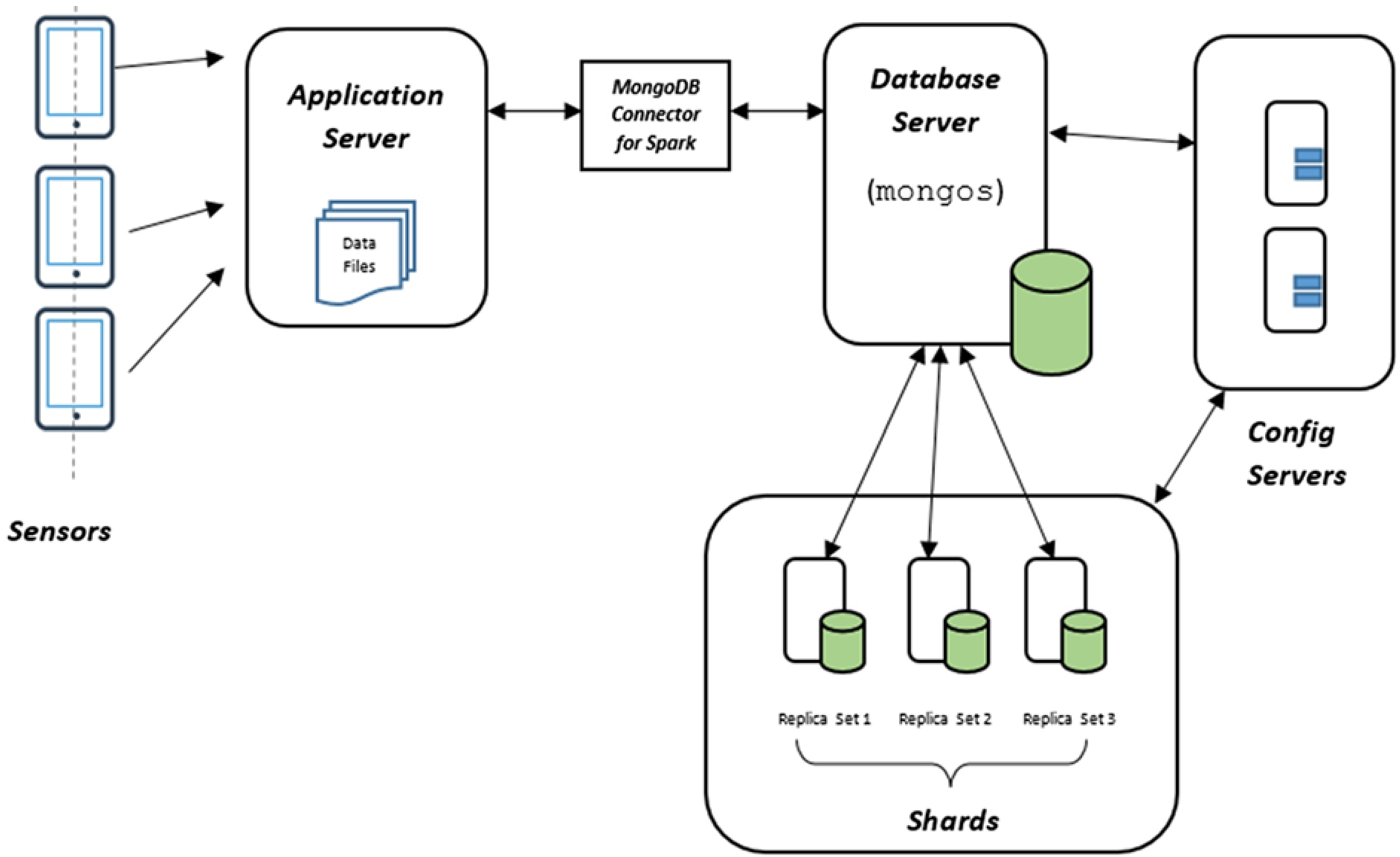
Metro-Lab Network Edge & IoT Partnership



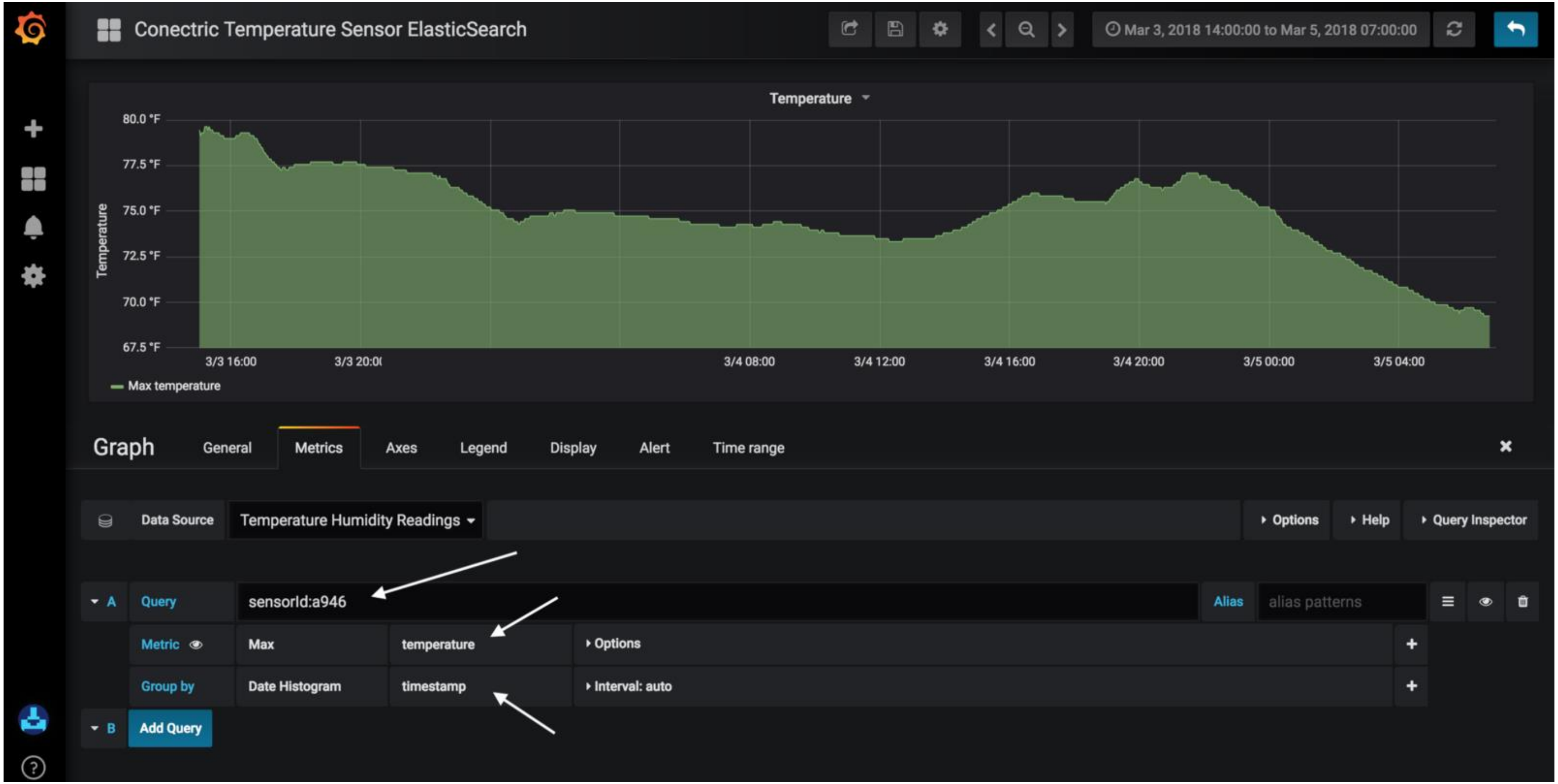
Managing and Processing High Performance Edge Data



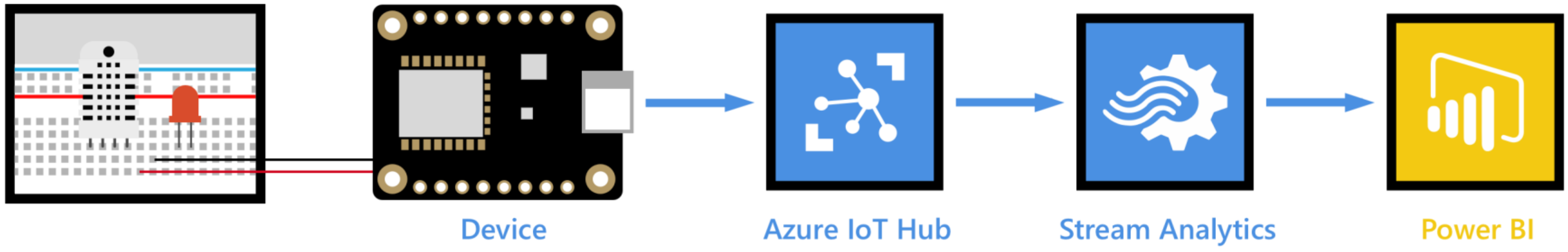
Managing and Processing High Performance Edge Data



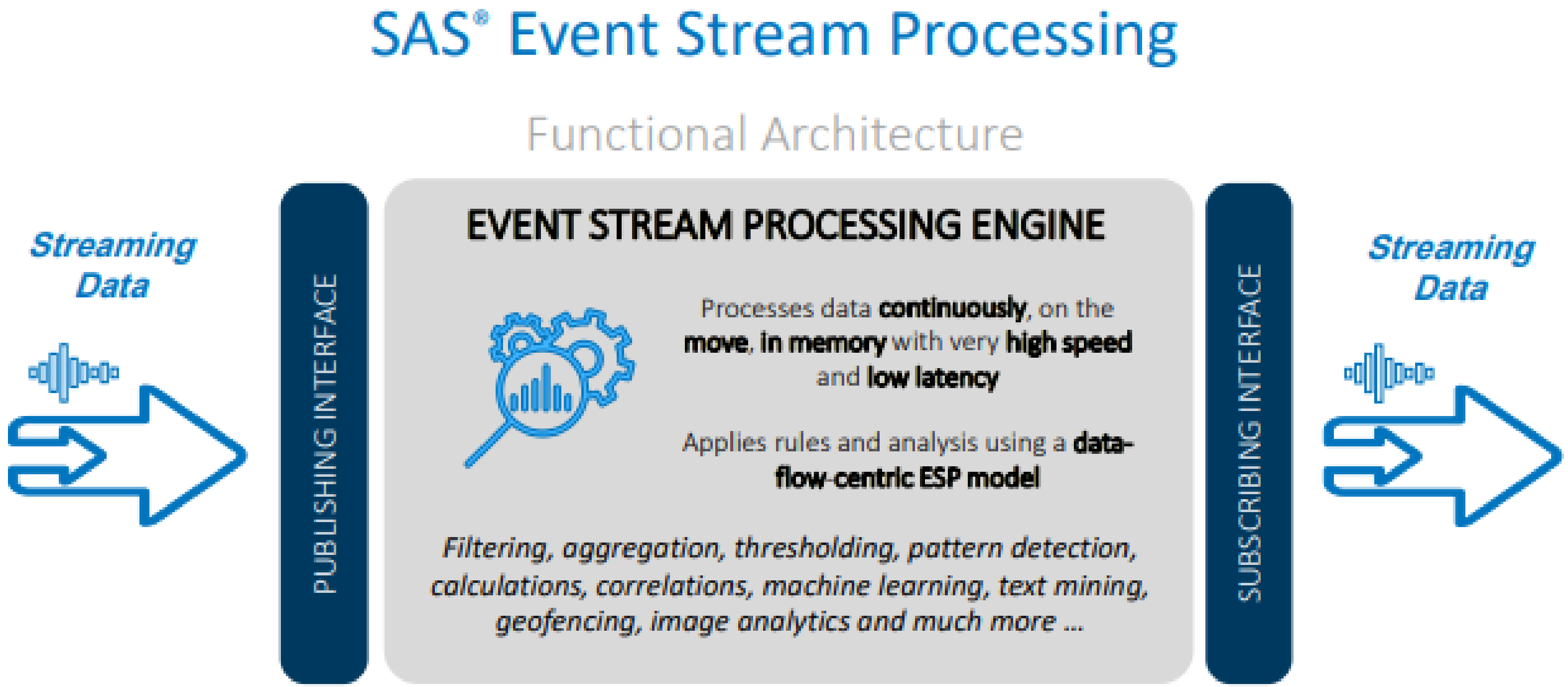
Visualizing Sensor Data



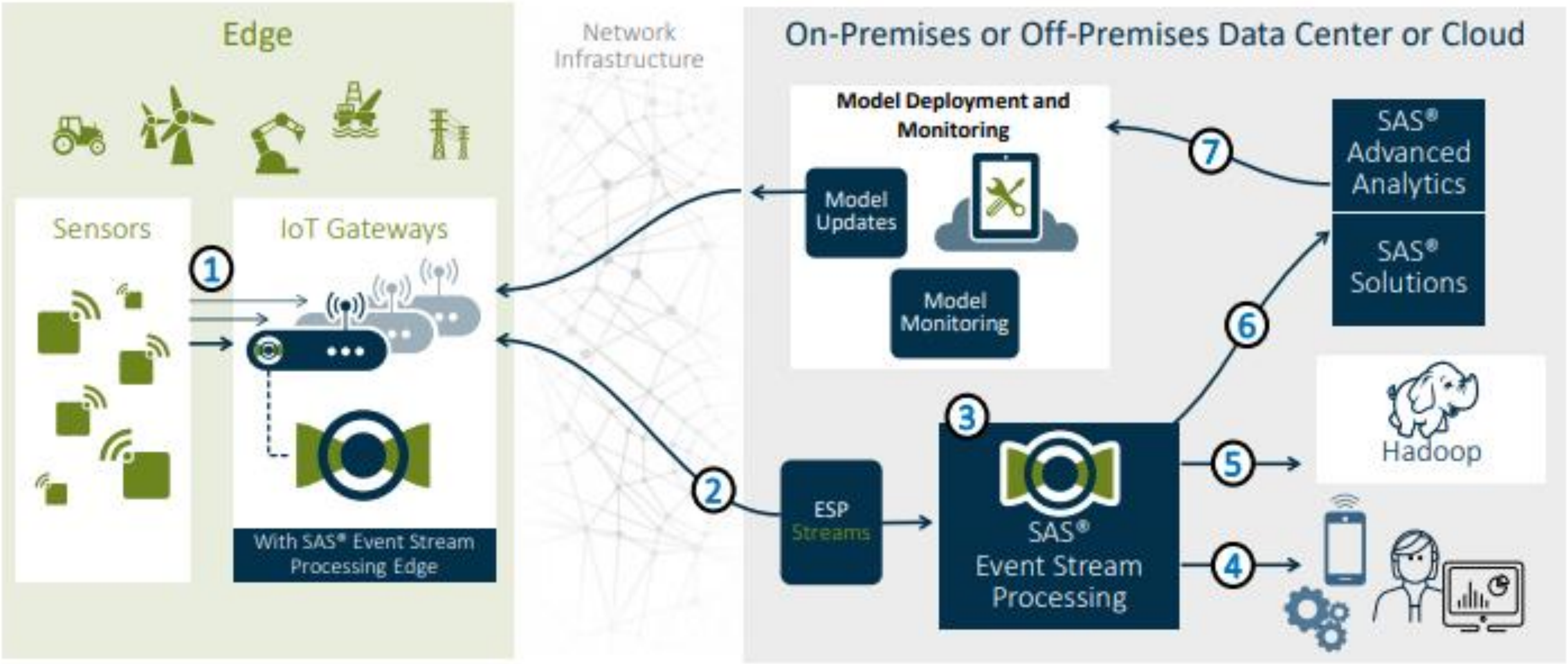
Visualizing Sensor Data



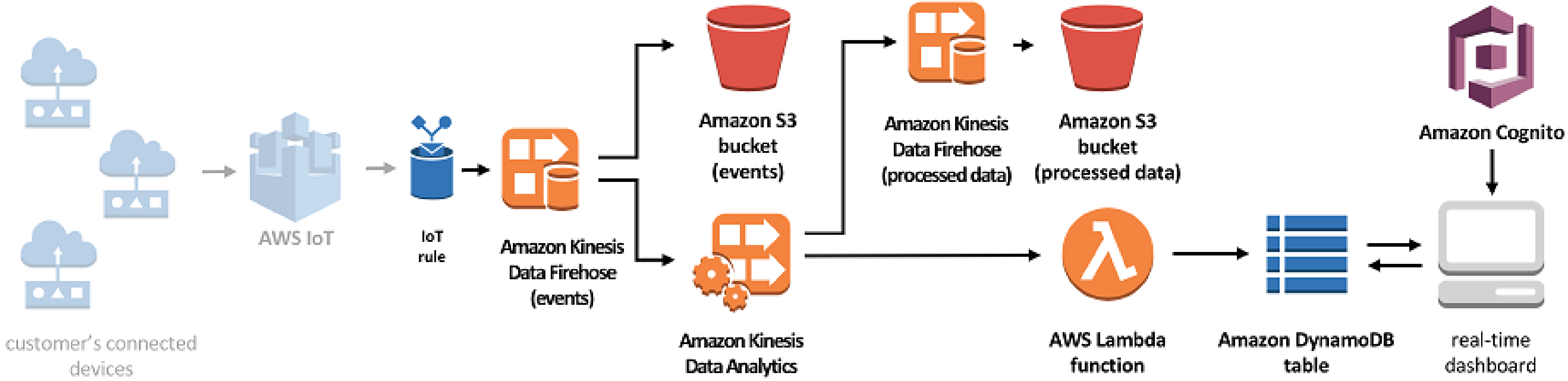
Processing data streams



Processing data streams



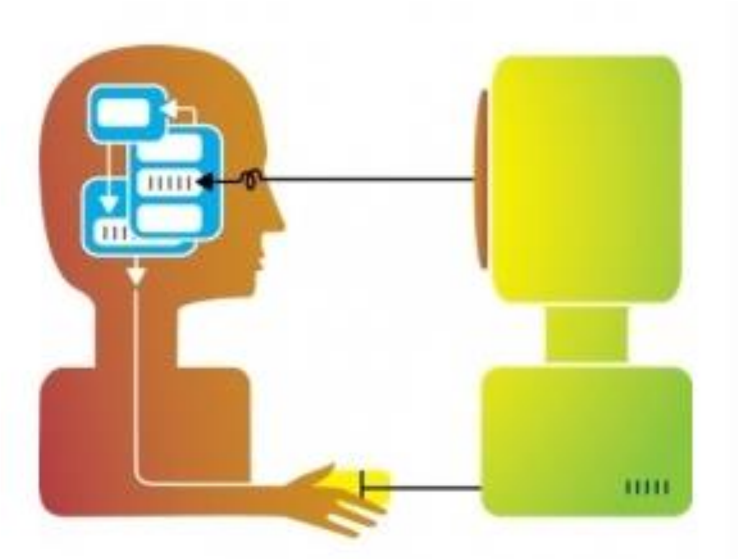
Processing data streams



Data Consistency in an Intermittently Connected or Disconnected Environment

- **Trust** is the foundation of an Edge & IoT system. It means that you know you are talking to the right device and the device knows it is talking to the correct end system.
- **Identity** refers to the association of incoming data with the correct time series history and addressing messages to the correct device.
- **Time** is an accurate date and time stamp for each event and data point. In Edge & IoT, it can be a challenge for devices operating across time zones and where users can make manual adjustments to clocks, for example.
- **Chain of custody** refers to understanding the complete history of each data point, including details about the devices and software that processed the data.

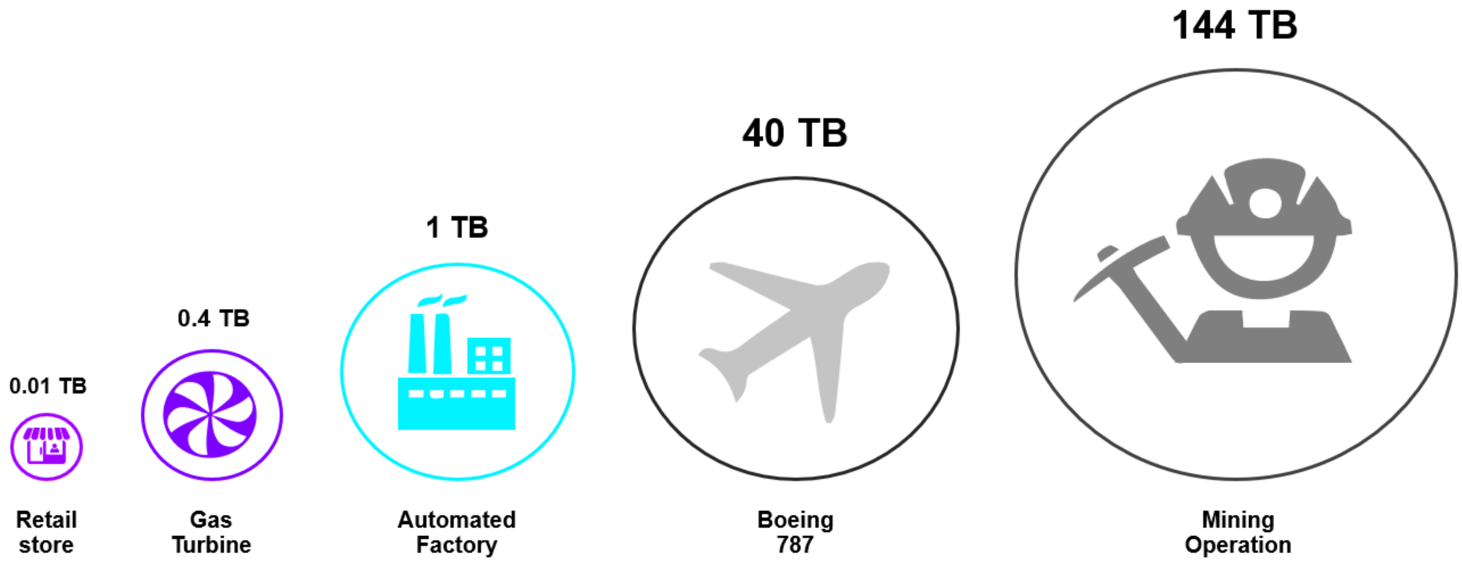
Human computer interaction



Data ingestion, storage and transformation

THE AMOUNT OF DATA GENERATED BY IOT IS OVERWHELMING AND IS INCREASING OVER THE YEARS EXPONENTIALLY

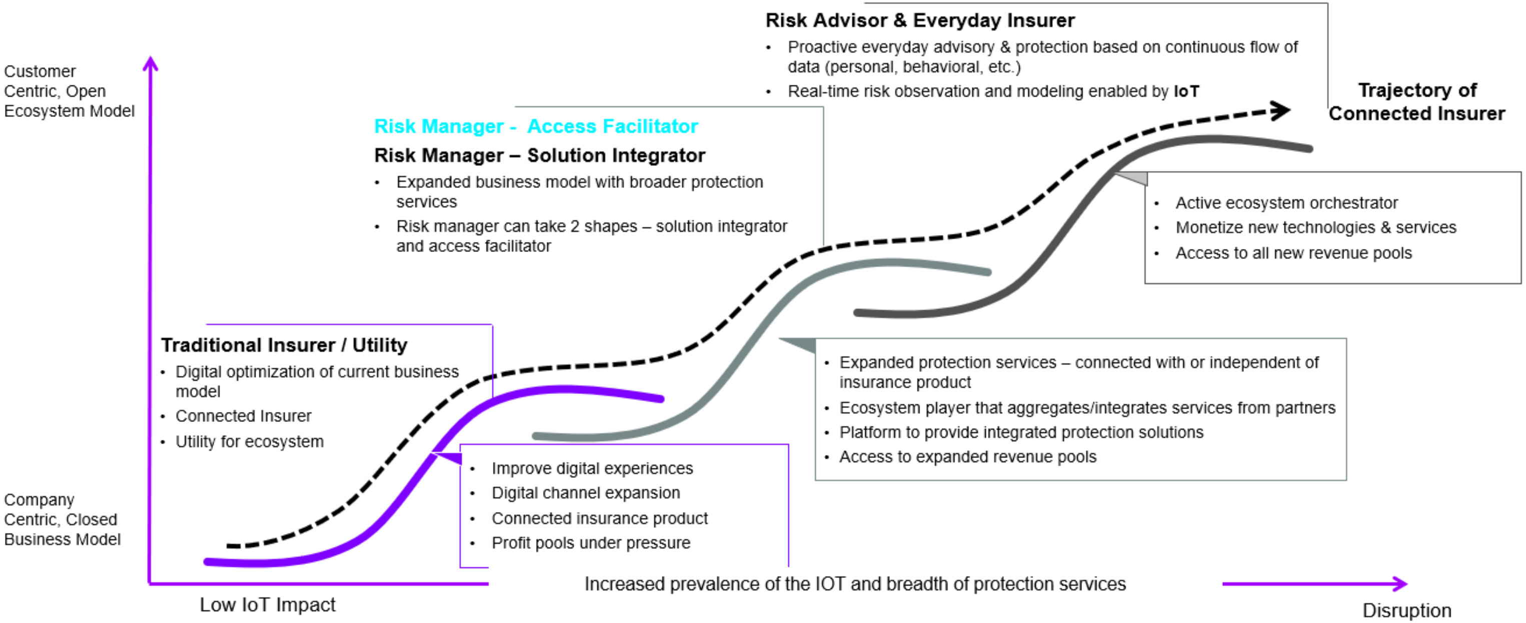
AMOUNT OF DATA GENERATED IN ONE HOUR BY...



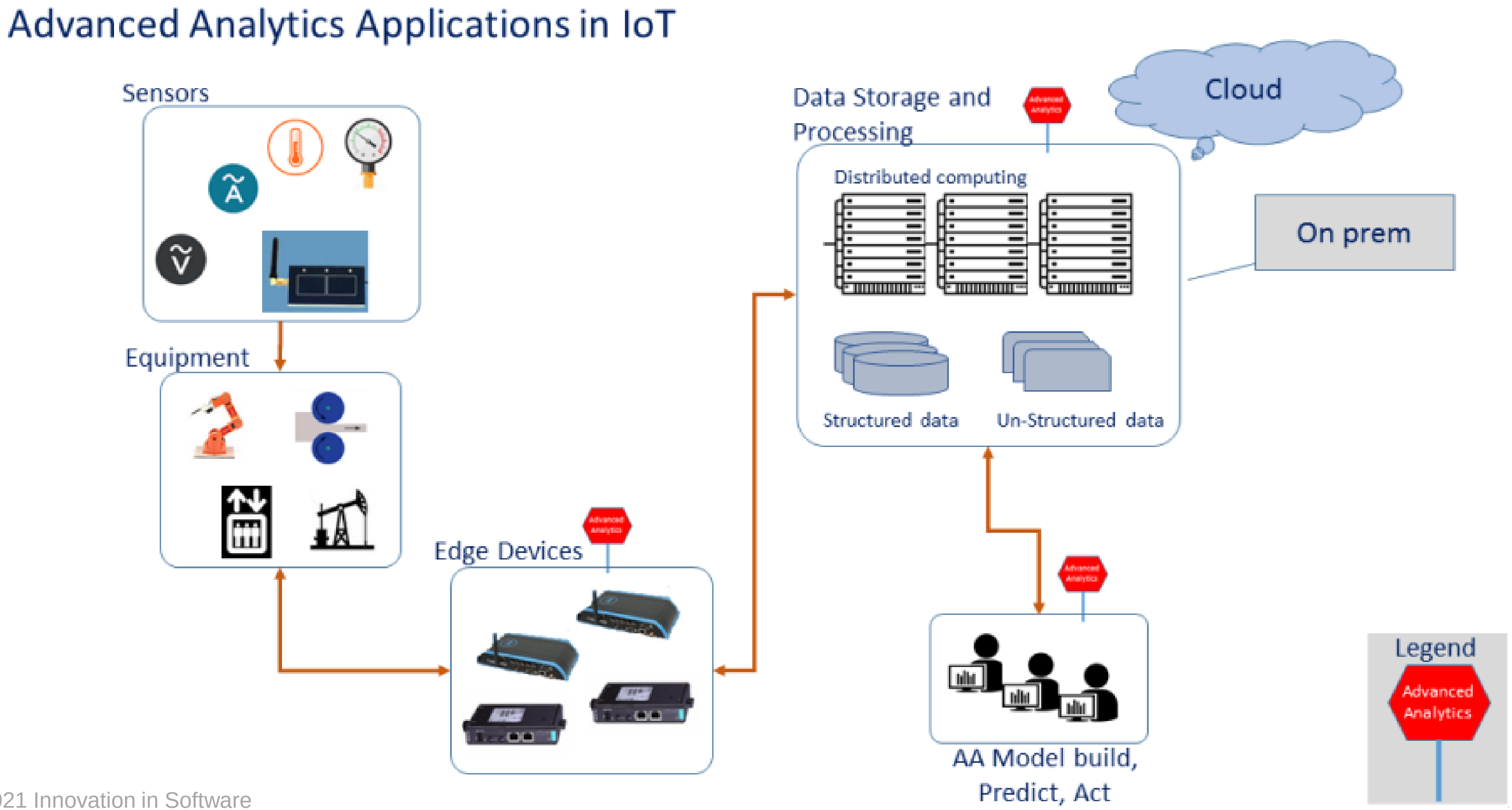
Data ingestion, storage and transformation

TO COMPETE IN THE FUTURE, PROTECTION PROVIDERS NEEDS TO BE ABLE TO OPERATE OPEN BUSINESS MODELS AND DELIVER AN EXPANDED SET OF PRODUCTS AND SERVICES

FUTURE PROTECTION PROVIDER ROLES



Edge & IoT Advanced Analytics



Government Smart Cities Initiative

Government is **slow to adopt change**. City governments will likely pilot smart city programs prior to adopting them more broadly. In the long run there would be benefit to creating an identity as a key player in the early stages of Smart Cites in America.

Collaboration is key. The White House announcement emphasized collaboration across a broad eco-system of players. Private and public players are working together throughout all of the programs highlighted.

While some funds have been awarded they point to priorities and players. It is likely that **additional funds** will be awarded in the future.

US Ignite is a non-profit that is partnering with public, non-profit and private players. The National Science Foundation was instrumental to their creation and is targeting much of their Smart Cities funding through this non-profit. They will likely play a key role in driving the agenda in the future.

Edge & IoT Credential Dashboard – US Smart Cities Initiative

Edge & IoT Credential Dashboard – US Smart Cities Initiative

An Emphasis on Collaboration and Public Private Partnerships

- Several private sector initiatives were showcased as part of the White House Smart Cities announcement
- These partnerships are spread throughout the country and involve public and private players
- Client, IBM, Microsoft, Qualcomm, Cisco and Siemens were also involved in initiatives

Edge & IoT Adaptive Risk Model

- “To identify a potential threat based on the context, the behavior and the average information related to similar cases that are provided in real-time or almost real-time by other ‘things’ and produce a global risk index re-usable from every actor in the ecosystem to: assess, determine, reduce the risk and prioritize the action needed to avoid the threat.”

Edge & IoT Adaptive Risk Assessment

- An optimal adaptive solution for Edge & IoT will have the following behaviors

Real Time
Constantly watches the security posture of individual and collection of devices

Actionable IoT Intelligence
Leverages existing network and security infrastructure

Trusted Behavior
Enforces acceptable behavior consistent with each device's service profile

Security Posture
Identifies, Classifies, Actively Manages IoT Inventory

Self-Learning
Uses AI and Sophisticated Deep Learning Algorithms

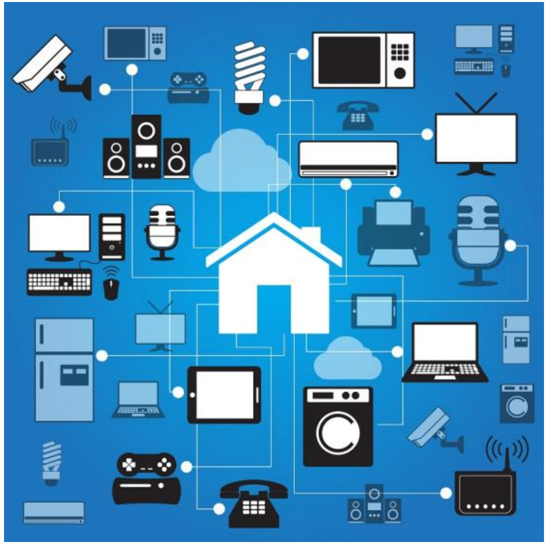
Non-Disruptive
Agentless, Seamless

Device Personality
Learns every device's unique personality and profile

Deep Learning
"Unsupervised" Deep Learning

Risk Exposure
Organization-level risk assessment

Connected Home Vision



- An ideal connected home system shall…
- Orchestrate the state of interconnected home appliances, either automatically or based on predefined user configuration, to maximize user experience at home,
- Allow its users to remotely monitor the state of environment via sensors and change the state of actuators, and
- Blends into human natural lifestyle. System must be operable effectively without any need for dedicated devices (e.g., smartphone). For example, using gestures, face expression, and biometric properties.

Connected Home Edge Tier Devices

- Connected home is a container term used mainly to describe a system with connected devices that serves domestic use cases at home. Some typical use cases on connected home includes security monitoring, personalized entertainment, and home healthcare.

Home security

Home Comfort

Smart lighting

Home automation

Connected kitchen

Personalized Entertainment

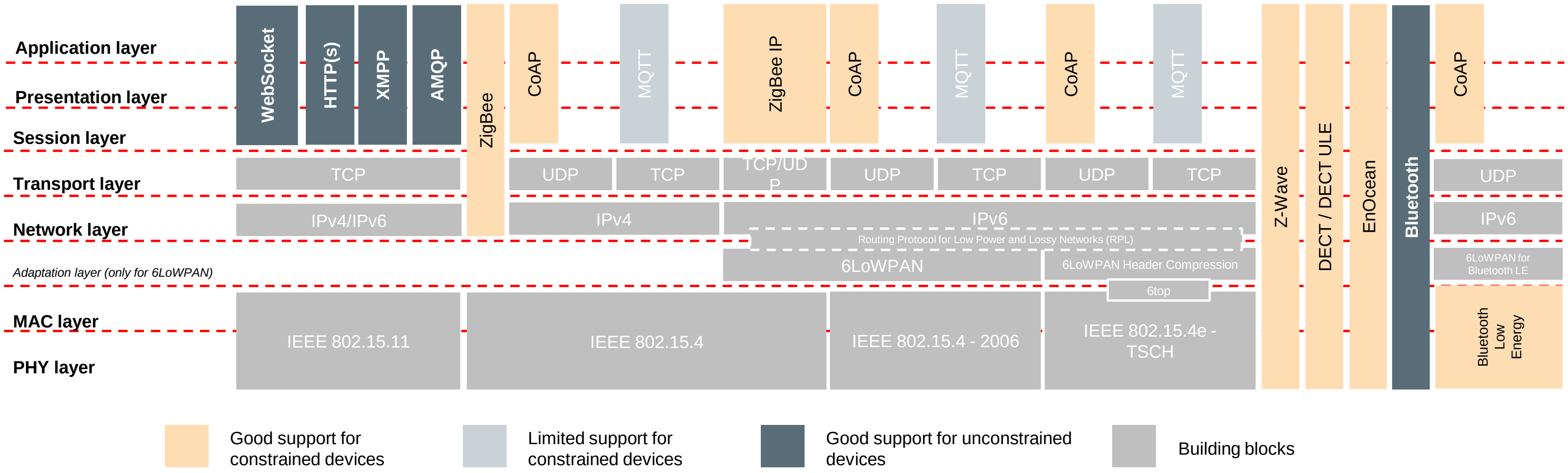
Connected Car

Healthcare, Fitness, and Wellness

Energy management

Connected Home Edge & IoT Application Connectivity

- Below are some Edge & IoT protocols commonly used in connected home use case, mapped to the supported devices. The selection of protocols need to be aligned with other requirements such as desired security level, data frequencies, and data size.



Architecture Principles

#	Architecture Principle	Implications
1	Security first	• Storage and access to personally identifiable information has to be secured using state-of-the art approaches. • All data communication from proximity to access network needs to go via secure channel. • All information shared to 3rd party platforms need to be sufficiently anonymized. • The system must implement data access/privacy management capability at edge tier, where end user may override all settings pushed remotely from central system. • Mitigation strategies for security breach at multiple tiers must be designed, i.e., edge tier (both physical and virtual), platform tier, enterprise tier, and public tier.
2	Integration at multiple level	Provide integration interfaces in both edge and platform tier.
3	Design for User Experience	• Prefer architecture solutions that minimize the number of extra hardware needed. • Adopt implementation framework that allows for remote device/software updates with minimal end user involvement. • Adopt data transmission/power management strategy that are sufficiently good for target users' experience • Design mitigation action for scenario where access network is not reachable • Move computation as much as possible to edge tier to improve responsiveness and avoid platform bottlenecks
4	Centralized Identity Management	Platform needs to have a publicly accessible central identity management system.
5	Minimum lifestyle disruption	Platform needs to be able to support modern I/O devices that blends with common user lifestyle (e.g., smart-watch, personal assistant with voice-command support)

Architecture Principles

#	ARCHITECTURE PRINCIPLE	DESCRIPTION
6	Power savings	Connected home users potentially include people with limited technical knowledge to perform system maintenance by their own after initial setup. Therefore, the system shall be designed to use power efficiently so it can work normally for long period.
7	Always connected	Connected home system shall never be completely disconnected from end-users. In the case where connectivity drops completely, each device in the system shall still be able to deliver its core functionality normally.

Typical Requirements

- Requirements describe how application must do and are often project-specific. Nevertheless, some typical requirements of connected-home systems are listed below:

Interoperability	The system must be able to interconnect various devices, potentially offered by different vendors and have specific integration requirements.
Remote access	End users must be able to view/control the state of all connected devices remotely, e.g. , via apps running on mobile devices, websites.
Add action rules	End users must be able to create rules to trigger actions based on the state (update) of their environment, e.g., turn off lights in a room when there is no movement identified by motion sensors in the room for 10 minutes.
Local access	End users must be able to control the connected devices within their local network if the connection to Internet network is broken.
Edge devices support manual operation	End users must be able to operate all connected devices manually using their physical interfaces, e.g., users must be able to set the target temperature of a thermostat in a connected home system manually using physical configuration buttons provided by the thermostat.

Device Characteristics

- A typical edge tier of a connected home comprises of devices with very different characteristics. Both constrained and non-constrained are typically co-exists.

#	Characteristic*	Camera	Magnetic door/window sensor
1	**Power source**	**Power connected**	**Battery-powered**
2	Mobility	Static	Static
3	**Reporting frequency**	**Very High**	**Low**
4	**Transferred data complexity**	**Rich data**	**Simple data**
5	Report range	Depends on cable length (wired), or wireless technology used (wireless)	5-10 m
6	Object density per cell	Typically < 5	5-20 devices/cell
7	**Processing capability**	**Medium**	**Low**
8	Communication device	Wired, wireless	Wireless
9	**Constrained device**	**No**	**Yes**
10	Energy in/out	Active	Active
11	Invasiveness	Non-invasive	Non-invasive
12	Contacts	No-contact	Contact (with magnet)
13	Relativity of measurements	Absolute	Absolute
14	How sensor measure	Optic, accoustic	Electric
15	Measurement objects	Occupancy and motion, acoustic, light	Position

Camera is a popular device typically used to support home security, healthcare use cases (e.g., monitoring the state of a room/person). It has typically medium processing capability and able to perform basic up to advanced data pre-processing. Most cameras are power connected and support very high reporting frequency of rich data (e.g., image, audio).

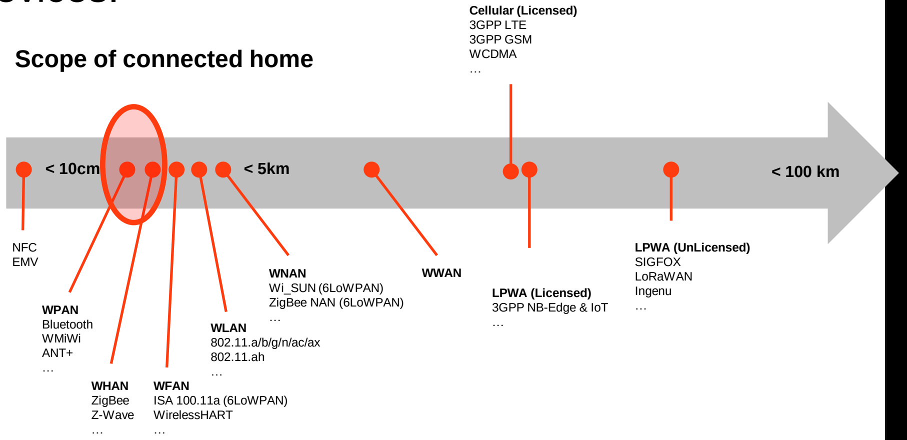
Magnetic door/window sensor is a device used to identify the state of doors/windows (i.e., opened/closed) based on the power of magnetic field around it. The device is typically used to support home security and comfort use cases. Most door/window sensors have relatively small physical dimension, very limited processing capability, and battery-powered.

* Contrasting device characteristics are highlighted.

Proximity Networks for Edge & IoT Applications

- All devices in connected home use cases are typically separated within **short range** wireless network*. Within short range wireless network, the first filter towards choosing a wireless network technology is the data rate requirements of the devices – derived from reporting frequency and transferred data complexity of devices.

#	Device category	Reporting frequency	Transferred data complexity	Device example	Potential access network
1	Require high data-throughput	High/medium	High/medium	Camera, Smart TV, smart speakers	802.11a/b/g/n/ac/ax
2	Does not require high data-throughput	Low	Low	Magnetic door/window sensors, motion sensors, smoke detectors, Smart plugs, remote-controlled lights	Zigbee 2.4 GHz, Zigbee 868 MHz, BTLE, Z-Wave, DECT ULE



WPAN: Wireless Personal Area Network
WHAN: Wireless Home Area Network
WFAN: Wireless Field (or Factory) Area Network
WLAN: Wireless Local Area Network
WNAN: Wireless Neighborhood Area Network
WWAN: Wireless Wide Area Network
LPWA: Low Power Wide Area

* Despite falling under category of WLAN wireless network (802.11.ac), many predicted that 5G technology will provide crucial features necessary to support future Edge & IoT use cases.