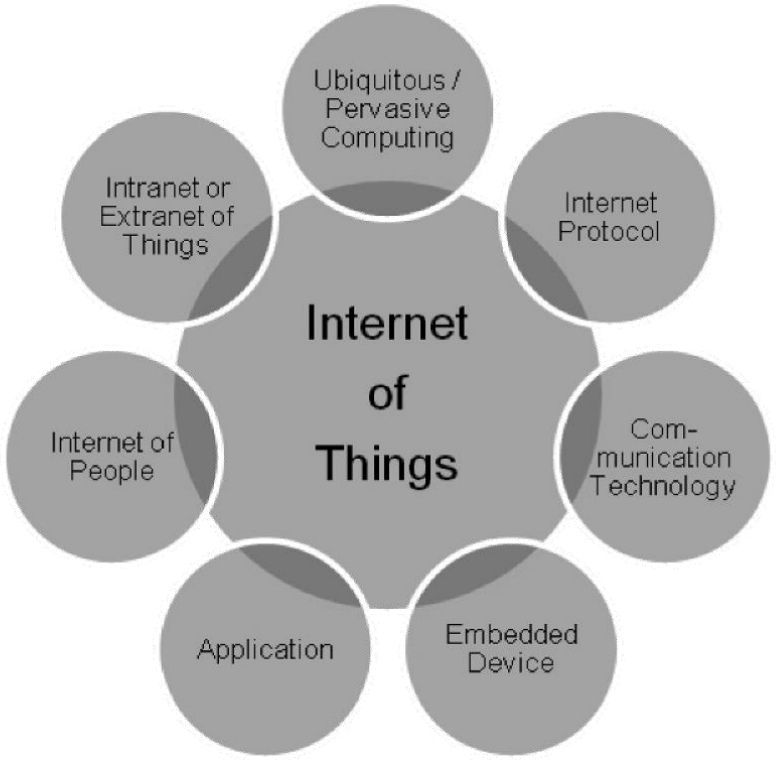
Architecting IoT
Notes, Concepts & Ideas

D. Vanderbist 24/03/2017

IoT: Definition

"Internet of Things (IoT) is an integrated part of future Internet and could be defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network"



- Definition is limited: not enough to distinguish from web 2.0
- What is IoT NOT:
  - Ubiquitous passive computing: this does not require object or internet infra
  - IP: not linked to a specific protocol
  - Communication technology: IoT requires communication but it not prescribes how it must be done
  - Embedded device (like RFID): there must be a information infrastructure backend
  - Applications: combination of hardware and software
  - The internet of people: objects are an important aspect
  - Intranet or Extranet of Things: not limited to a small group of stakeholders (=closed-loop in stead of open-loop)

IoT: Business Value

Operational Technology (OT):

- OT is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

Information technology (IT):

- IT is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise.

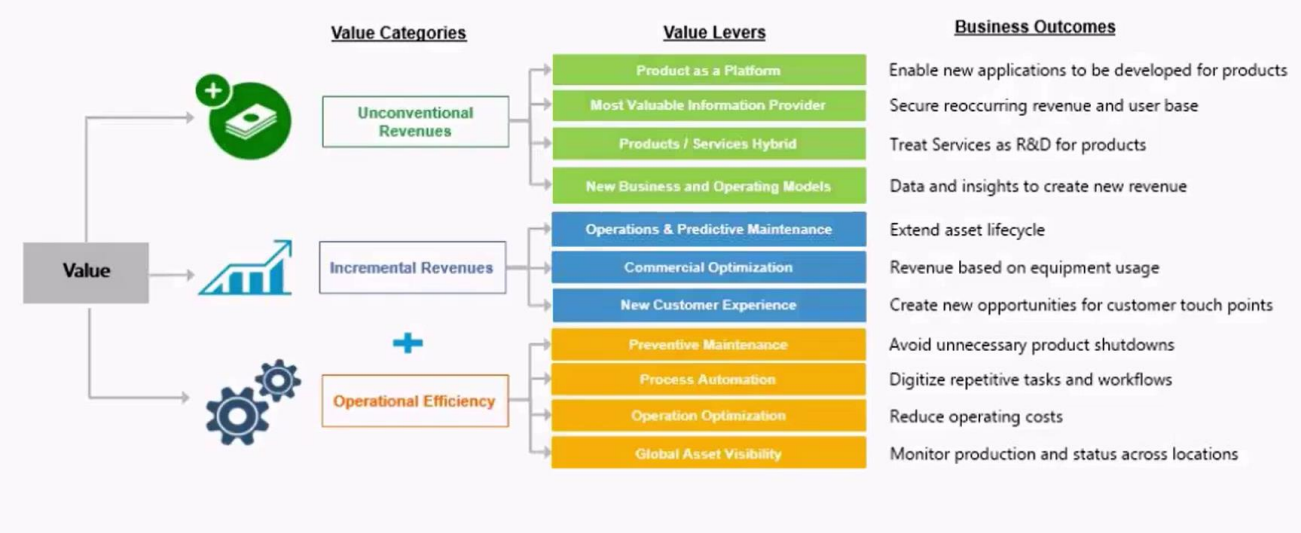
Future Technology (FT):

- FT are new emerging technologies like unmanned aerial vehicle (UAV) or Block Chain.

Business Value:

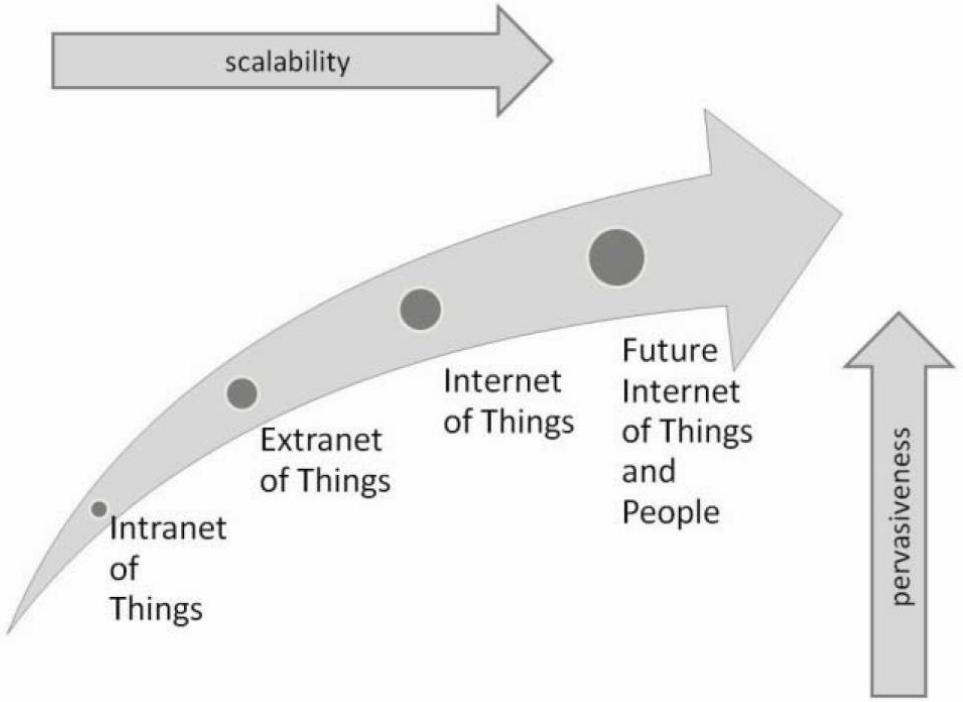
OT/IT + FT BV

IoT Outcome based value



IoT: Concepts

- Things:
  - Person to object and object to object communication
  - Digital twins: Combining the virtual world of data with the real world of things (objects)
  - From state sensing and real-time analysis to real-time intervention in the world
  - Possible because of reducing cost of RFID and NFC.
- Messaging:
  - From analogue to digital messaging
  - Broadcasting messaging & personalization via filtering
- Environment:
  - The environment will adapt us but we also have to adapt the environment to make it work: adapt building to make RF communication work
- Infrastructure:
  - From cost generating infrastructure to revenue generating infrastructure
  - Requires open, scalable, secure and standardized infrastructure



IoT: The Things

Things object is based at least in the following capabilities:

- A unique identity
- Ability to sense and store their condition. Condition is the status of an object obtained by interpreting the output of sensor transducers associated with it
- Ability to make their information (be it identification, condition or other attributes) available to external entities
- Ability to communicate with other objects
- Ability to take decisions about themselves and their interactions with other objects

IoT: Addressing

Internet of Things addressing:
scheme:

- Addresses must be unique inside a network
- Addresses must be reused when objects leave
- Addressing must be dynamic. Address assignation should be fully distributed
- Addressing must be scalable
- Support for network merge and split should be provided
- The protocol overhead must be minimized

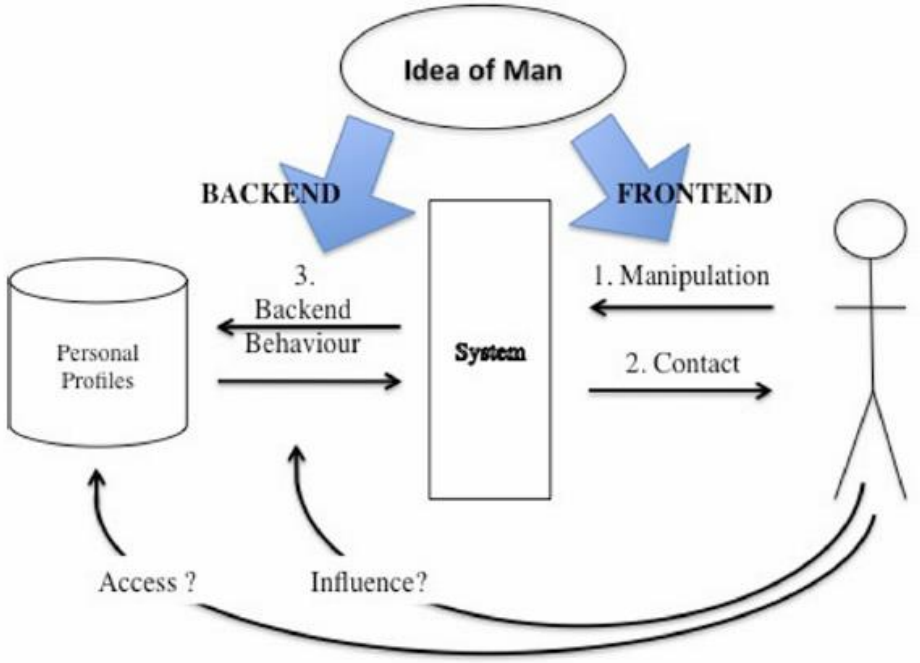
To meet this addressing:

- Hierarchical
- Distributed
- Scalable

IoT: Idea of man

Idea of man:

- Responsible and mature behavior, act rationally, moral autonomy, freedom of choice
- In a highly automated and networked environment how will people retain their self-determination “the ability to make decisions for themselves”
    - The right of privacy
    - The right to be calm
    - The right to make autonomous decisions
    - Accountability for action made to others
- Functional computing is replaced by human centric computing.
    - Ethical computing



IoT: Law of Information

Laws of information

- First Law of Information:
  - Information is (Infinitely) Shareable and Can Be Shared with Others Without a Loss of Value
- Second Law of Information:
  - The Value of Information Increases with Use and It Does Not Provide Any Value, If It Is Not Used at All
- Third Law of Information:
  - Information Is Perishable and It Depreciates Over Time
- Fourth Law of Information:
  - The Value of Information Increases with Accuracy
- Fifth Law of Information:
  - The Value of Information Increases When Combined with Other Information
- Sixth Law of Information:
  - More Information Is Not Necessarily Better, related / relevant information is important
- Seventh Law of Information:
  - Information Is Not Depletable

Providing the right information …

- Linked through a unique identifier to a physical product
  … in the right granularity …
- High information granularity, providing a new dimension of clarity and insight
  … and the right condition …
- High information accuracy
  - Aggregation of information from various sources, such as tags, sensors or embedded systems
  - Correlation, integration, and further analysis of information in a way that allows new insights to be derived
  - Defined syntax and semantics

  … at the right time …
- Timeliness of information
  - Access to real time information as well as to historical data for business analysis
  - Real-time analytics and business intelligence for high resolution management
  - Intelligent real-time decision-making capability based on real-time physical events · ... anywhere in the network …
  - Online access and possibly offline usage
  - Mobile access

  … at an appropriate price.
- Price transparency
  - Low premium for billing service, the price should be paid for the information rather than the infrastructure

IoT: Logistics

New opportunities for logistics:

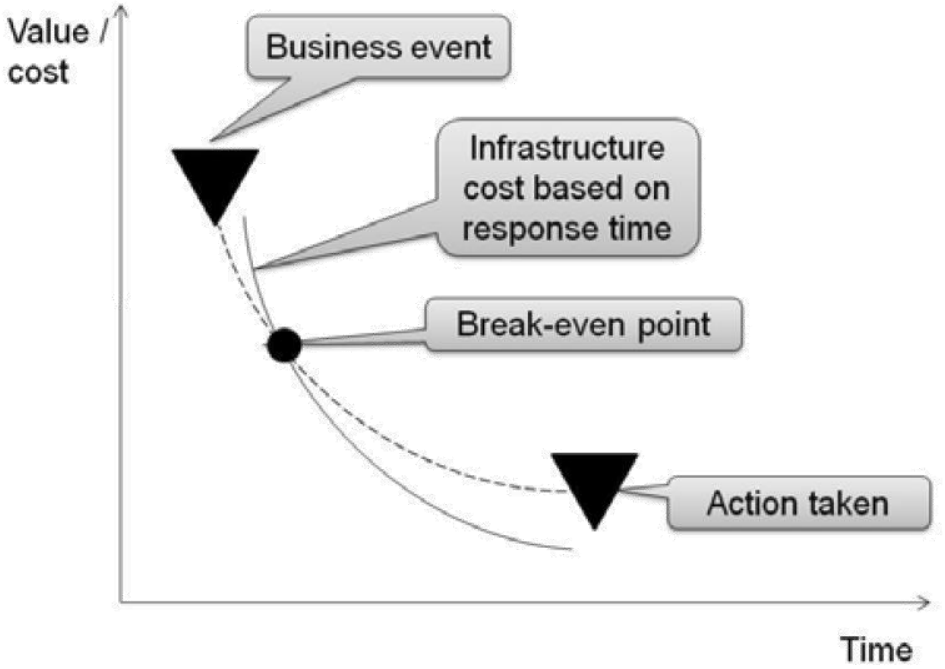
- Definition the right quantity, right time, right place, right condition, right price, right products
- IoT allows for real time logistics
  - Requires real time data and data processing
  - Reducing time between event and action for an acceptable price

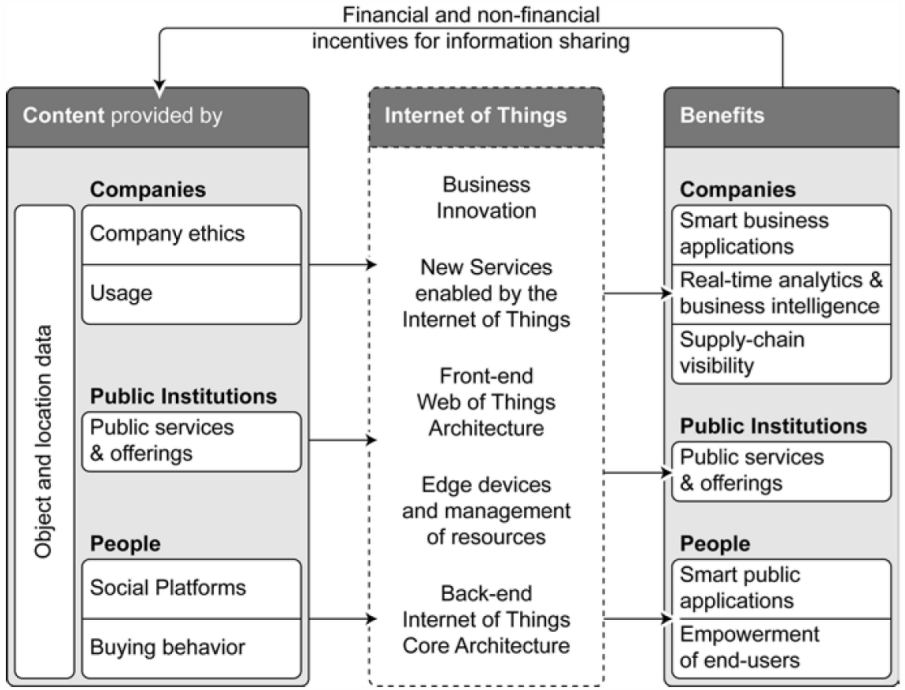
Information:

- The right balance: the cost of gathering information < the benefit gained from the additional information
- Information sharing

Privacy relies on context awareness:

- People need to opt in for privacy reasons but for context awareness this not always possible





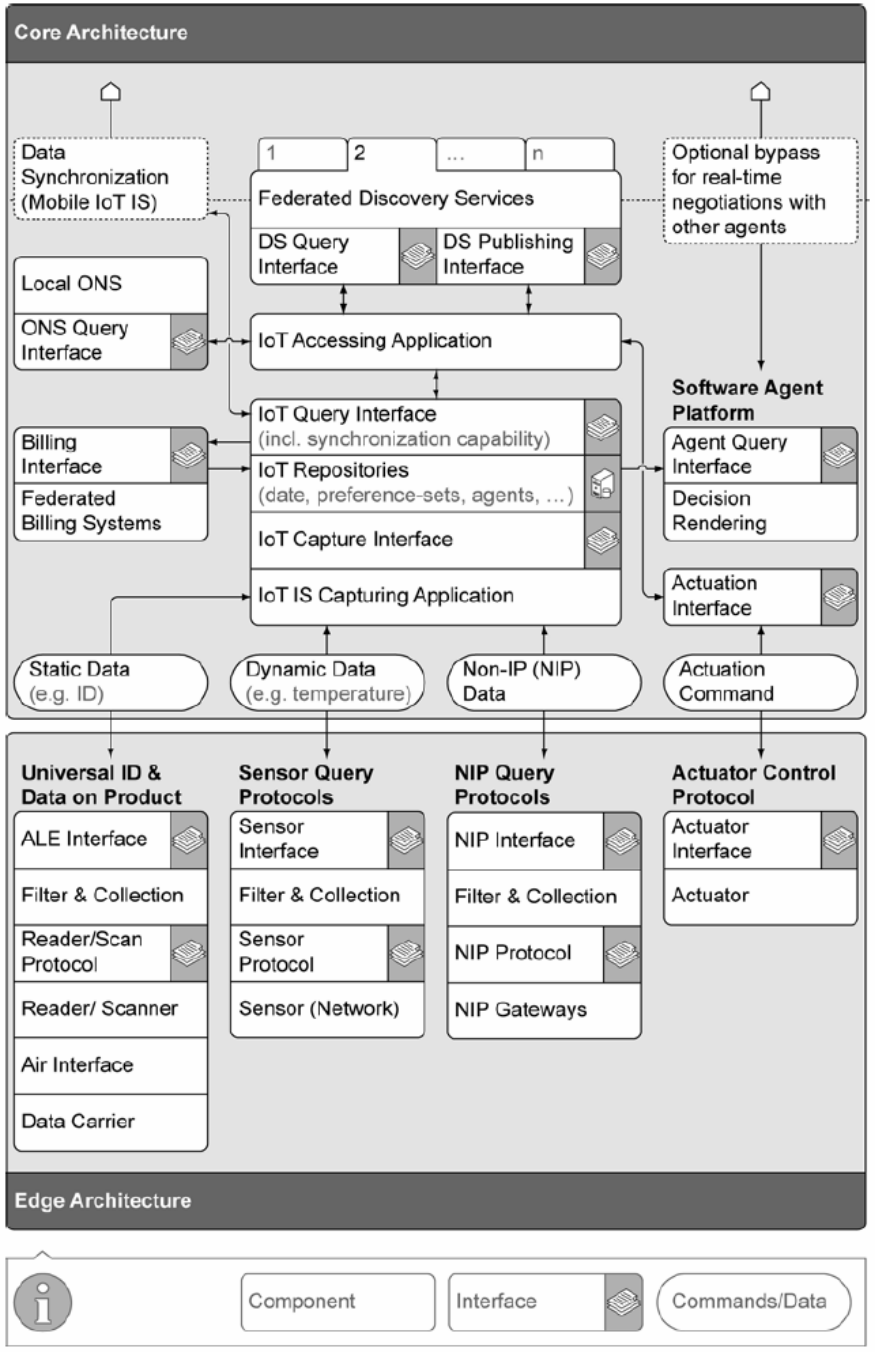
IoT: Costs

Cost level	Cost of tagging (Agarwal 2001)	Cost considerations for RFID (Feinbier et al. 2008)	Cost of Internet of Things adoption
1 Mobile devices	• Cost of the tag itself • Cost of applying tags to products	• Tags	• Cost of mobile technologies, such as data-carriers (e.g., tags), sensors, actuators or smart devices • Cost of applying mobile technologies to things
2 Aggregation devices and software	• Cost of purchasing and installing tag readers in factories and/or warehouses	• Readers • Antenna and cabling • Installation • Tuning • Controllers • Software platform (middleware)	• Cost of purchasing edge devices (e.g., readers, gateways, controllers, accessories) and edgeware for fixed and/or mobile environments • Installation and technical optimisation costs
3 Integration	• Systems integration costs	• Integration (to legacy systems)	• Systems integration costs including new interfaces as well as necessary updates, extensions, or replacements of existing systems
4 Training and reorganisation	• Cost of training and reorganisation	• Process (incl. redesign and human elements)	• Training cost • Reorganisation / business reengineering / business model innovation
5 Application	• Cost of implementing application solutions	• -	• Cost of implementing internal application solutions beyond existing applications
6 Networking (technical and organisational)	• -	• -	• Cost for networking in an open environment, including e.g., improved security, fine layered access control, multi-directional communication, product data contracts, service level agreements, standardised syntax and semantics, data conversion, synchronisation, trust concepts
7 Operational	• -	• Maintenance	• Cost for maintenance • Other operational costs for running (e.g., data storage and analysis), extending and improving the system

IoT: Core Architecture

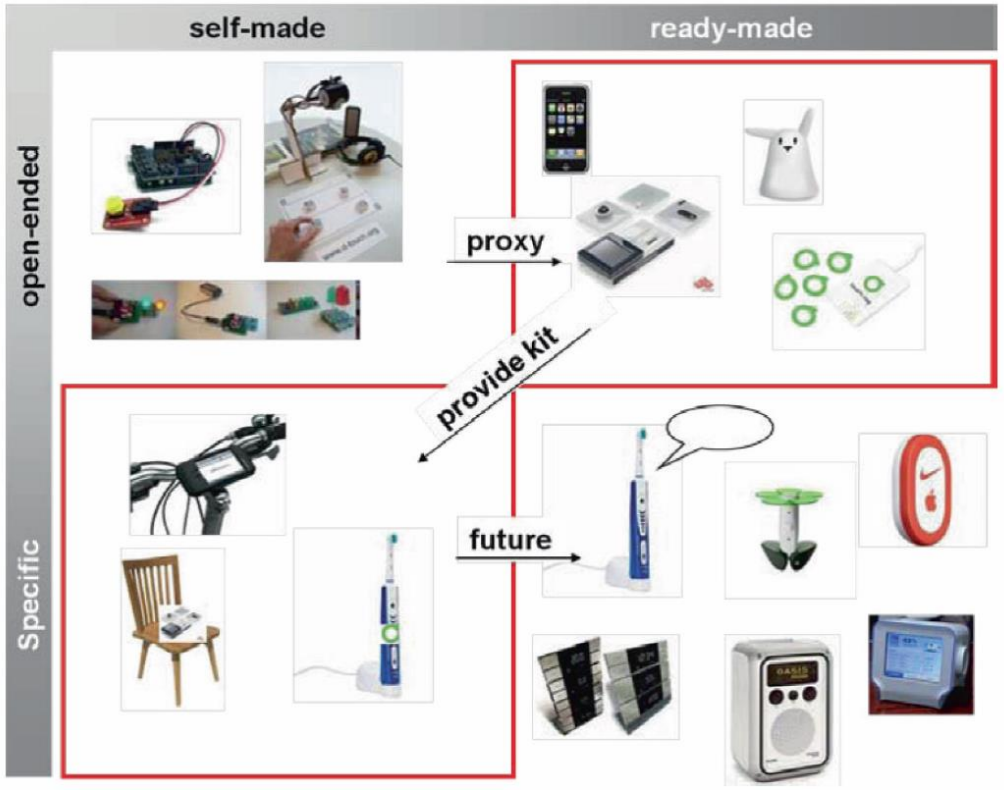
Some components:

- ID systems:
  - The need to support all existing unique ID system
  - Changing to another ID is just too costly
  - Object name service (ONS)
- Seasons:
  - Give info on the state of the real world
- Actuators:
  - Give control of thing to human or service
- Gateways:
  - To connect non-ip (NIP) devices
- Federated discovery
- Federated billing
- Off-line data support schemas
- Application Level Events (ALE)



IoT: DIY

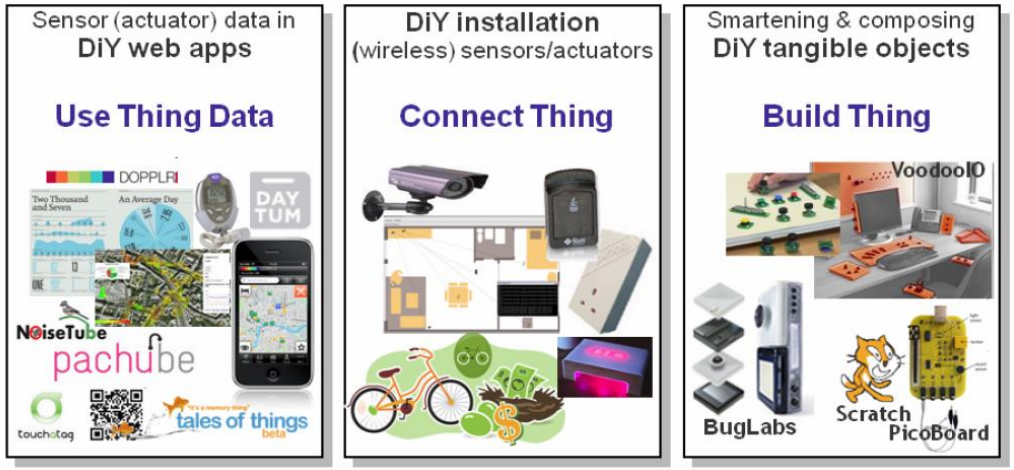
- Being your own boss
  - Garage DIY: working alone in a personal closed environment
  - Community DIY: a community of same thinking people
- DIY is about:
  - Connecting: people do self service
  - Taking control: openness of technologies and platforms
  - Diversification
- DIY rules:
  - Cases shall be easy to open not glued together
  - No special tools unless for a darn good reason
  - USB-power is good, proprietary adapters are bad
  - Ease to repair by design not as an afterthought
  - If it snap shut it shall snap open
  - "If you open it you shall not own it“-philosophies
- DIY in programming:
  - Open API's



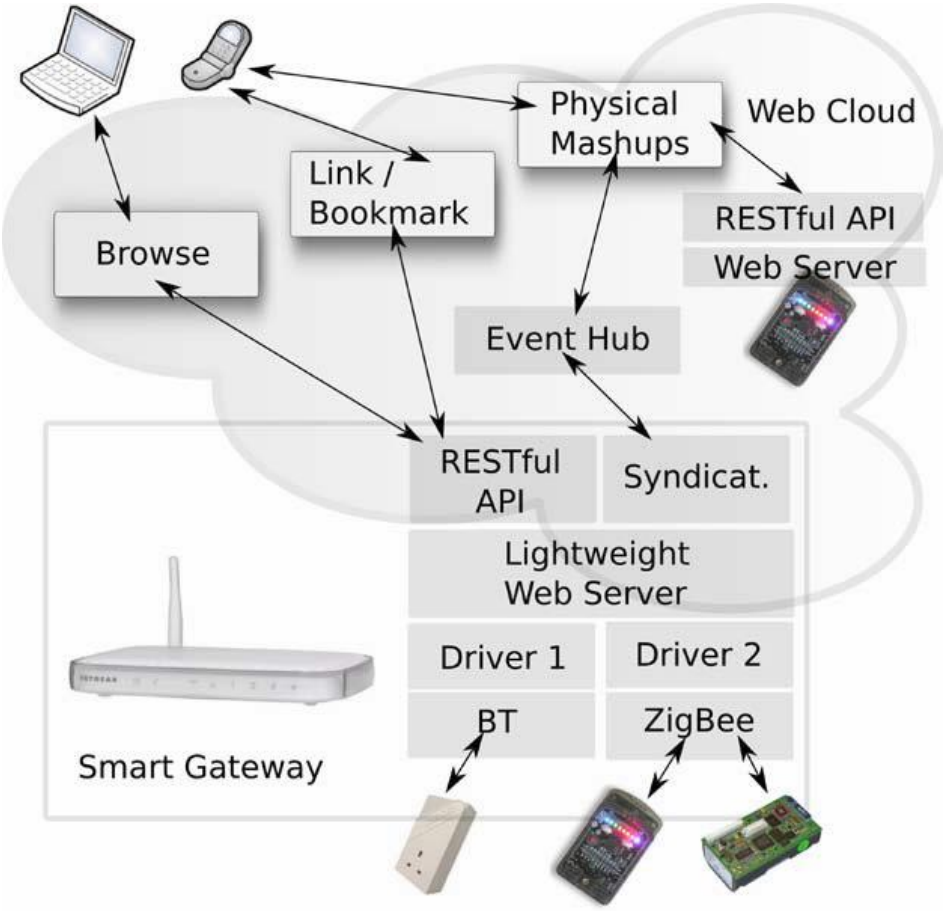
IoT: Context Awareness

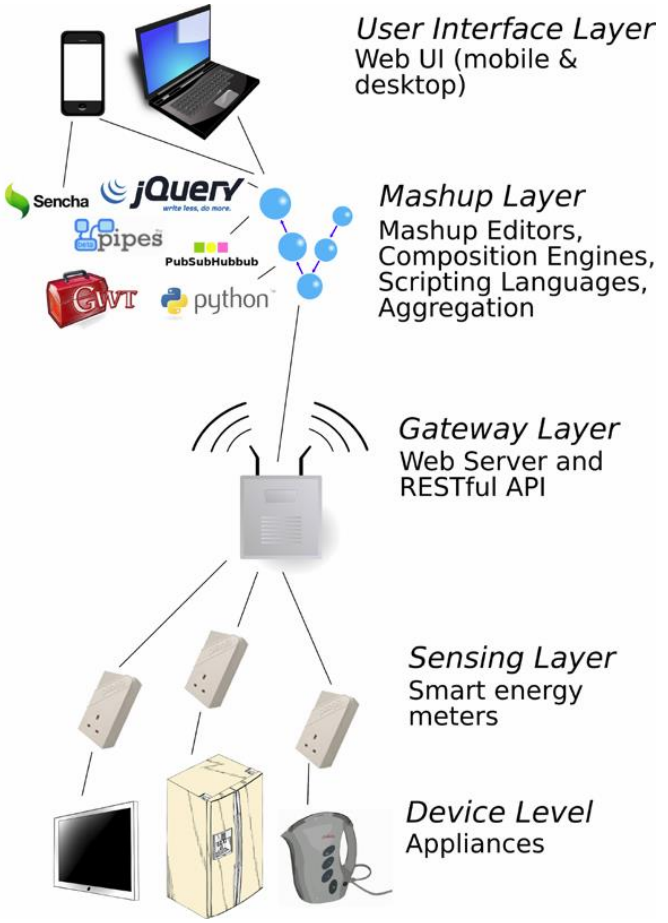
Context:

- Network of interconnected sensors & actuators:
  - Using the data on things
- Connection new sensors & actuators to the network:
  - Connecting new things
- Building smart objects:
  - Creating new things

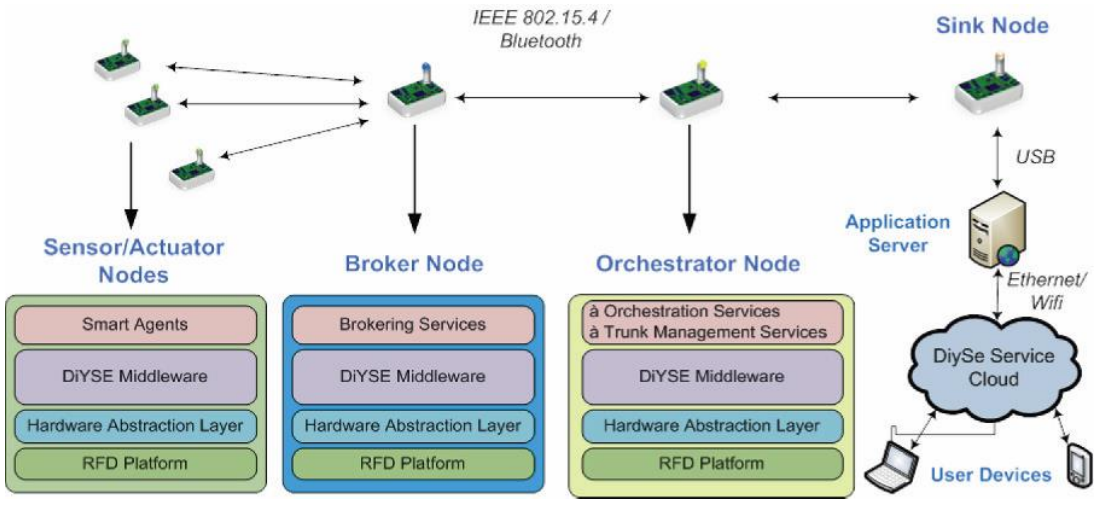


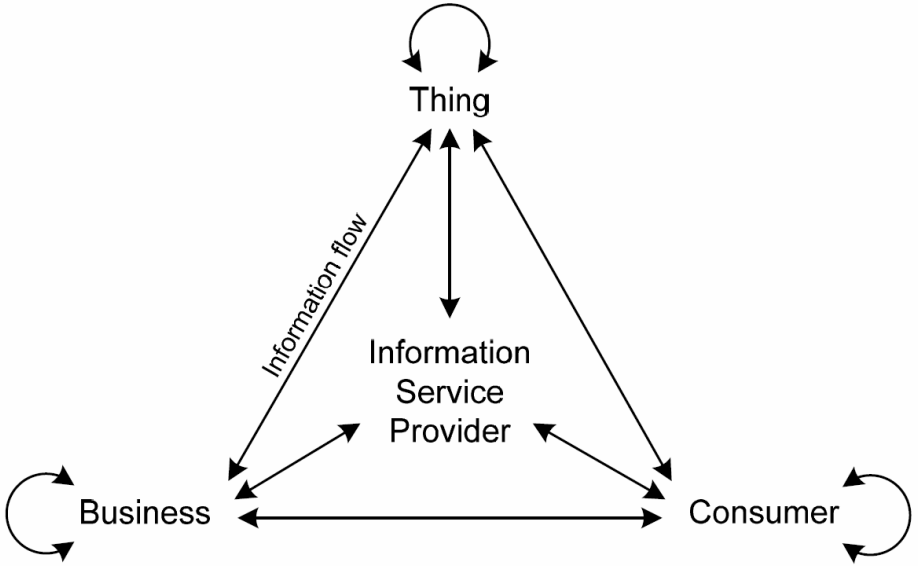
IoT: Architecture





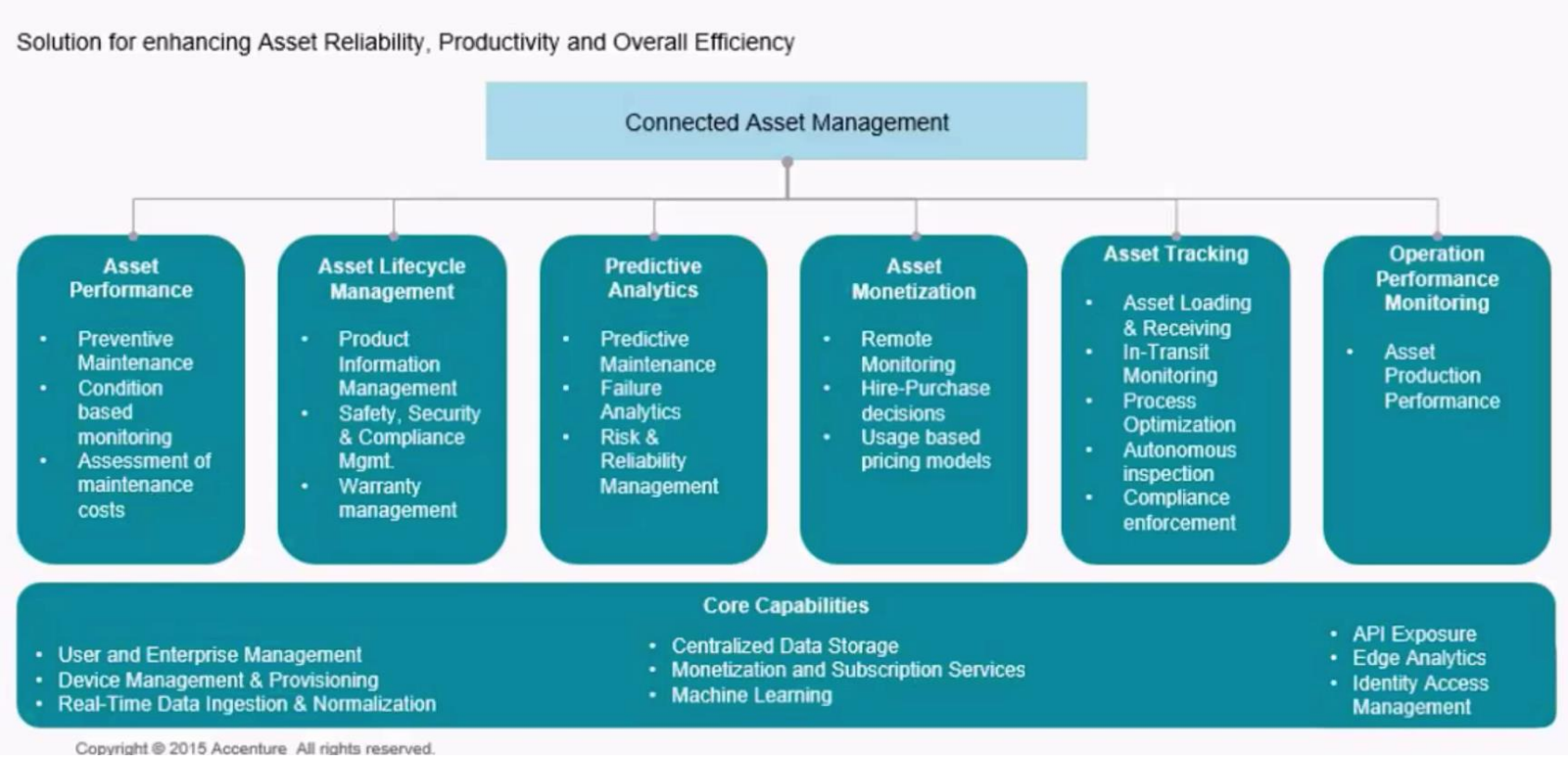
IoT: Architecture



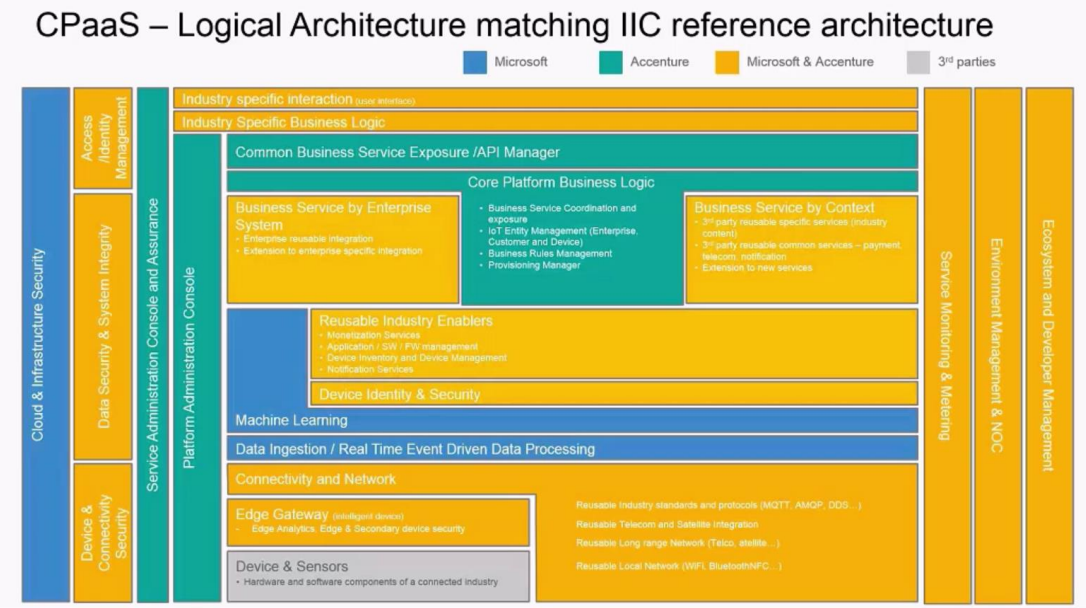


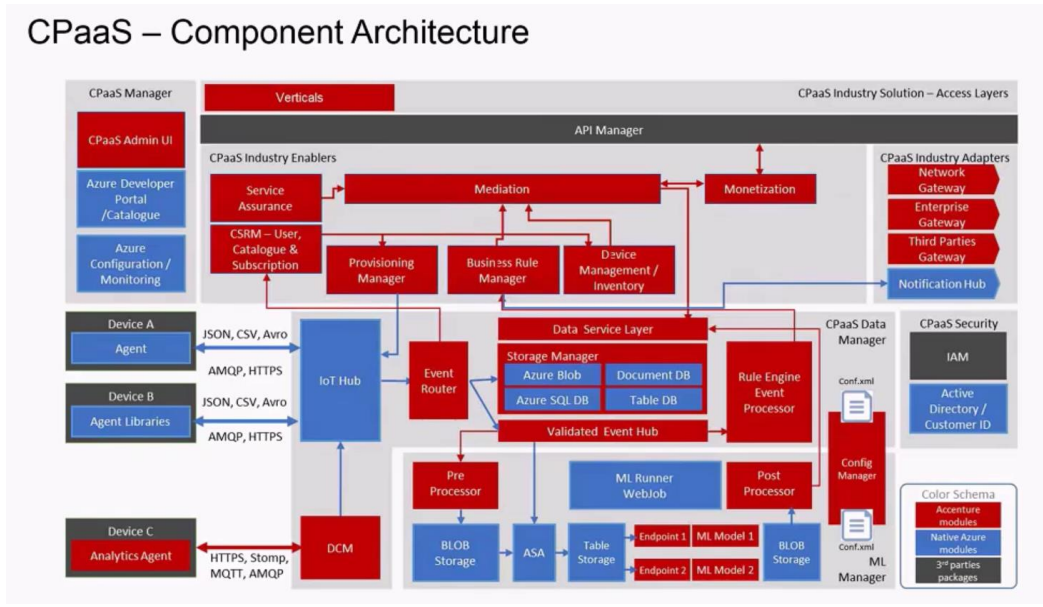
CPaaS: Communications Platform as a Service

Connected Asset Management:



CPaaS: Communications Platform as a Service





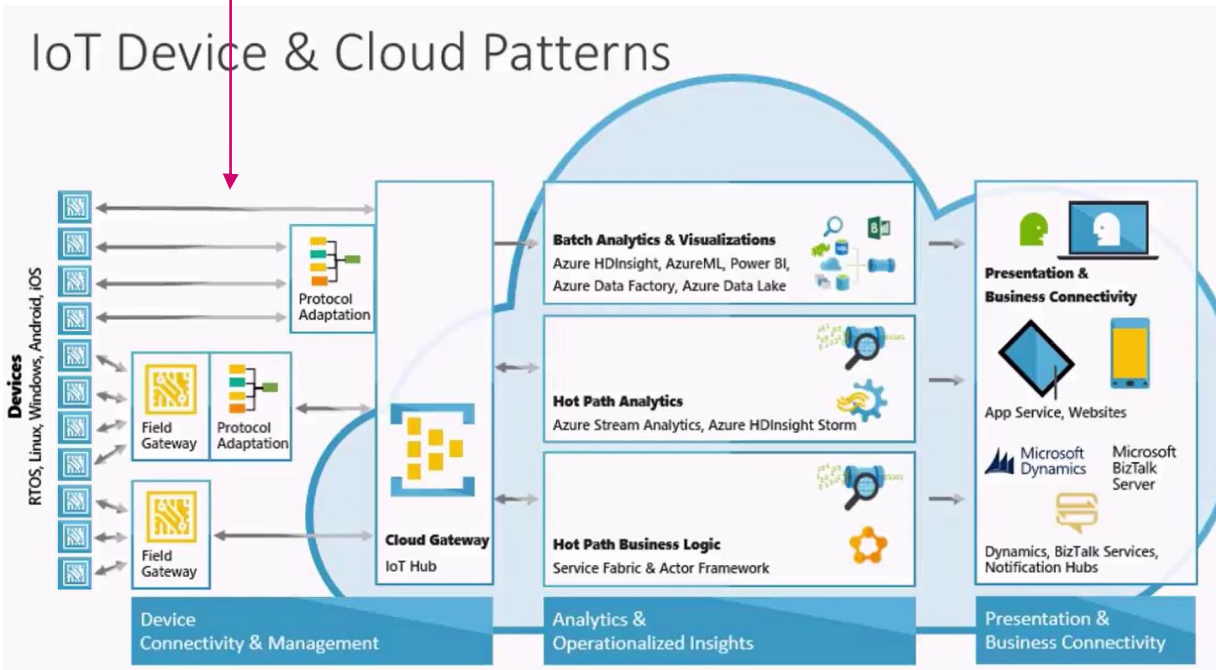
IoT: Azure Patterns

Connection Patterns

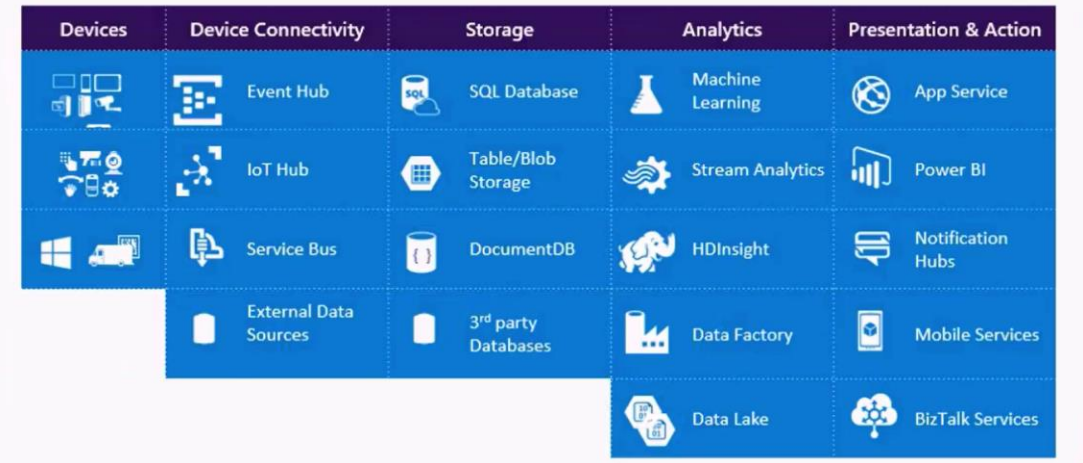
- Connect Direct Pattern:
  - Connected direct to cloud
- Field Gate Pattern = edge:
  - Fog vs. Cloud
  - Connected through a field gateway
- Protocol adaptation:
  - No direct connections
  - Field gateway translates = protocol conversion + integration

Service Patterns:

- Batch Analytics & Visualization
- Hot Patch Analytics: microsecond decisions
- Hot Path Busines Logic: seconds / minutes



IoT: Azure Components



Device-to-cloud messages

Interface

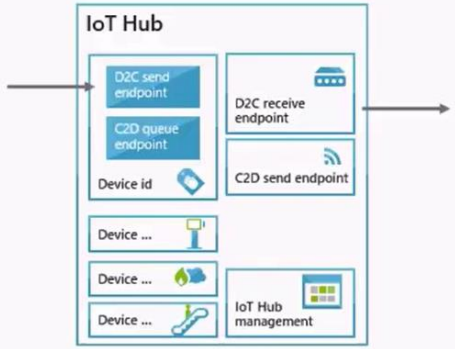
AMQP/S and HTTP/S device-side endpoint
AMQP service-side endpoint
Device and service SDKs

Compatible with Event Hubs

Partitioned receiver, client check-pointing
Integrations with Azure Stream Analytics, Storm, ...
100% compatible with Event Hubs receivers

IoT Hub services for D2C

Millions of simultaneously connected devices
Per-device authentication
Connection-multiplexing:
C2D and D2C traffic
Across multiple devices for gateway scenarios



Cloud-to-device messages

Interface

AMQP/S and HTTP/S device-side endpoint
AMQP service-side endpoint

At-least-once semantics

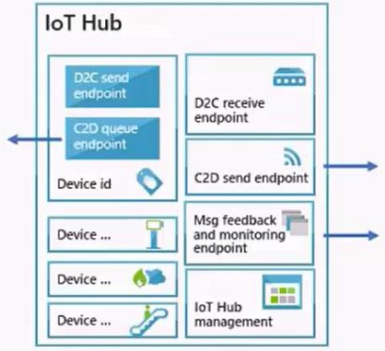
Durable messages
Device acknowledges receipt
(Send - Receive - Abandon OR Complete)

TTL and receipts

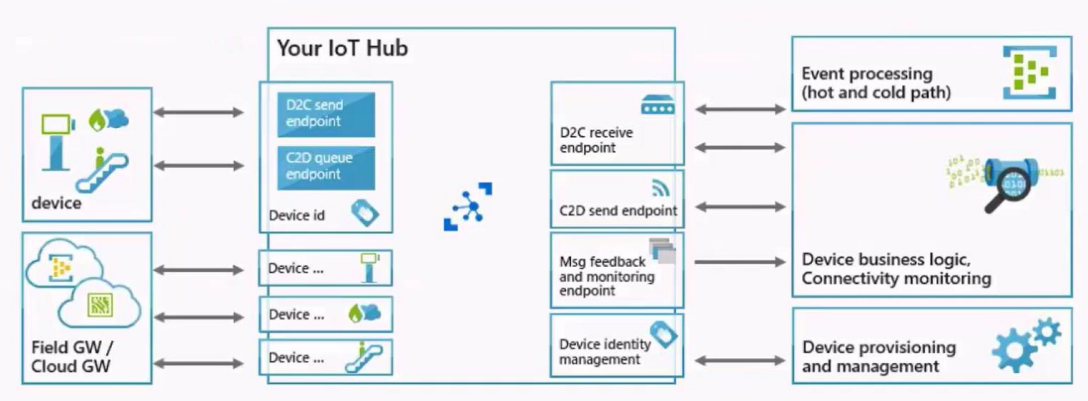
Per-message TTL
Per-message positive and negative receipts

Command lifecycle pattern

Use correlated D2C for responses
Use feedback information to retry
Store command state in command registry



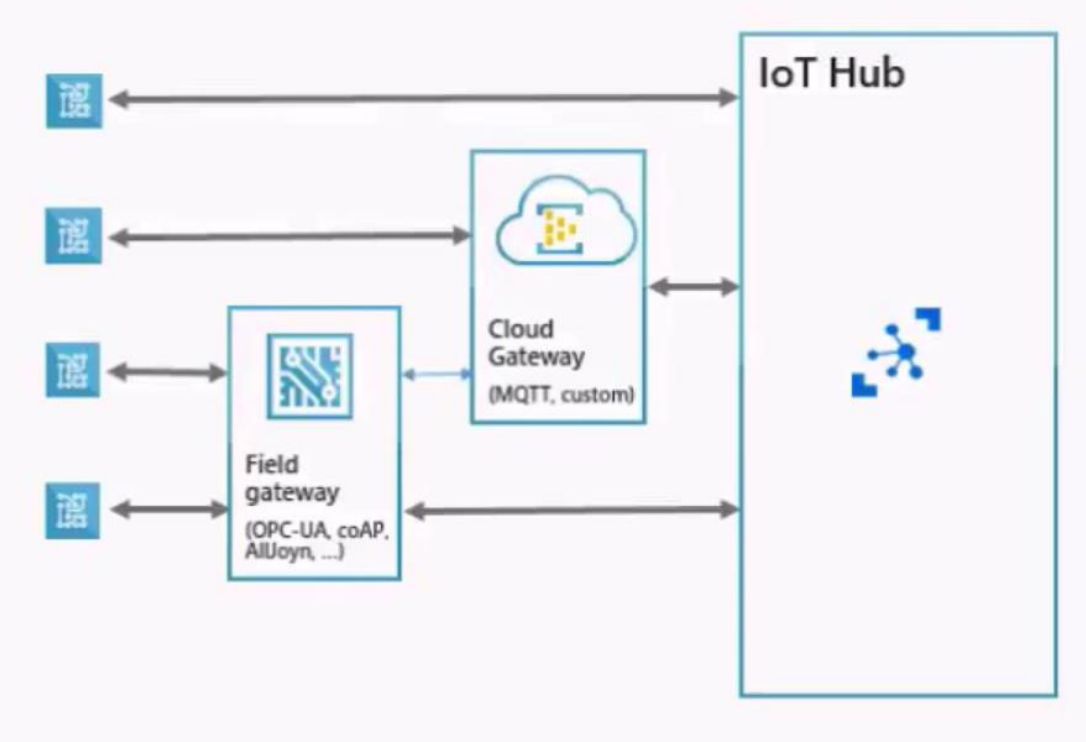
IoT: Azure Device Management



Device Management Capabilities in IoT Hub

- Register/un-register ✓
- Authenticate ✓
- Authorize ⊖
- Manage state (active/inactive/maintenance) ⊖
- Remote Configuration Update ✗
- Remote Firmware Update ✗

IoT: Azure Gateways



Cloud and field gateways

Use cases

PAN-IP access

Protocol translation

IoT Hub capabilities

Connection-multiplexing for multiple devices

Individual device identities through gateway

Extensible MQTT cloud gateway

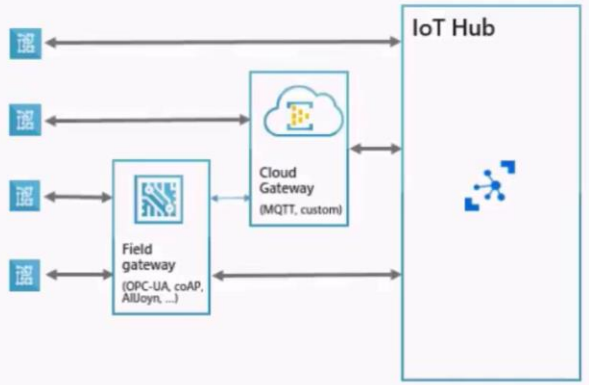
Patterns

Transparent vs opaque

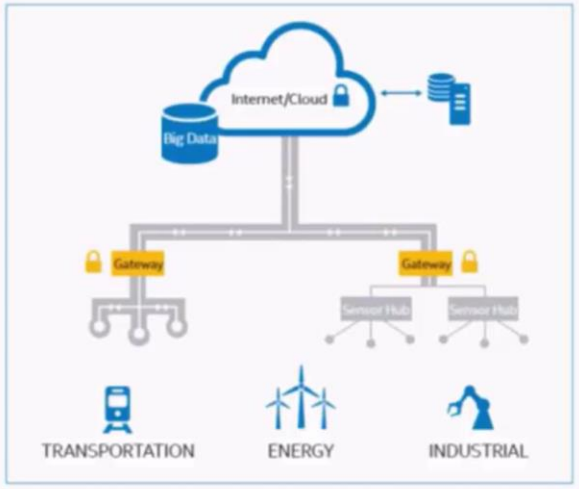
Individual identities known to hub or not

Pull vs push

Individual devices acts as servers or maintain persistent connection



Field Gateways



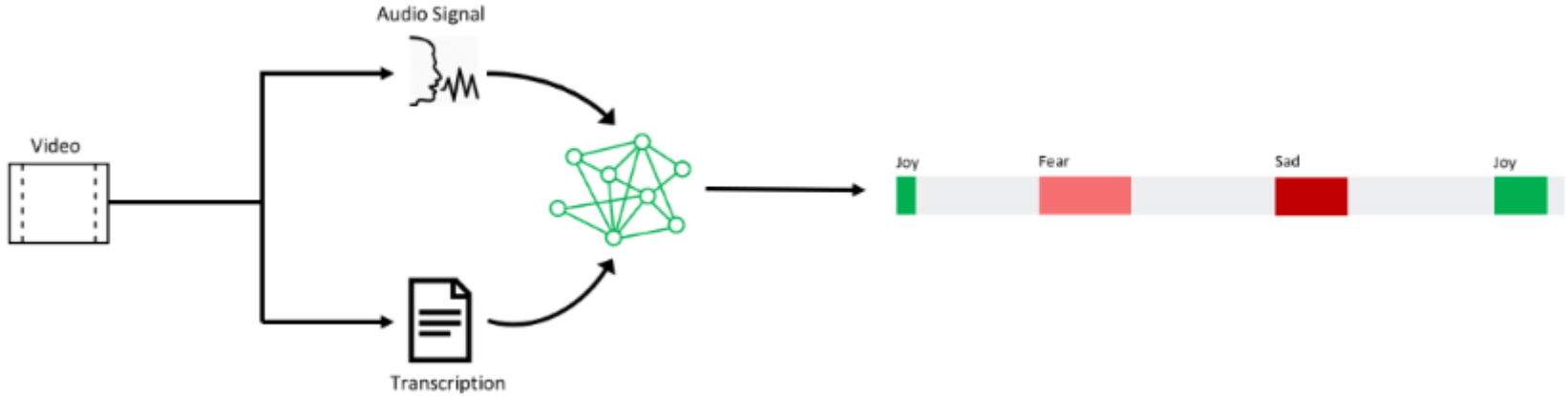
- Communication assistance
  - Secure data flows edge <-> cloud
  - Protocol translation
  - Data buffering
- Manage connectivity cost
  - Data filtering
  - Data batching/aggregation
- Device management
  - Provisioning
  - Updates

IoT: Azure Intelligent Cloud & Edge

The intelligent cloud is ubiquitous computing, enabled by the public cloud and artificial intelligence (AI) technology, for every type of intelligent application and system you can envision.

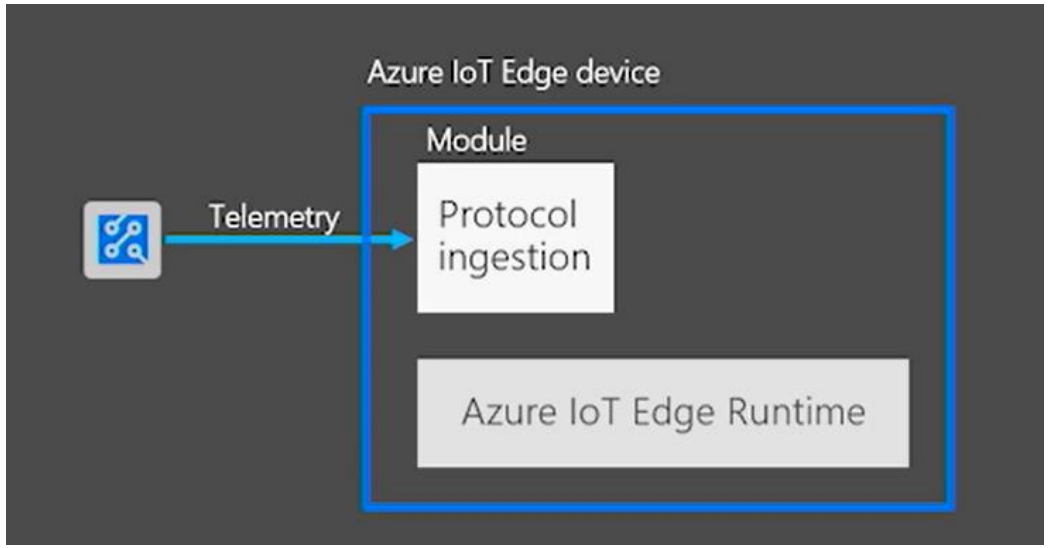
Together, they give you the ability to create a new class of distributed, connected applications and, ultimately, breakthrough business outcomes.

The intelligent edge is a continually expanding set of connected systems and devices that gather and analyze data—close to your users, the data, or both. Users get real-time insights and experiences, delivered by highly responsive and contextually aware apps.



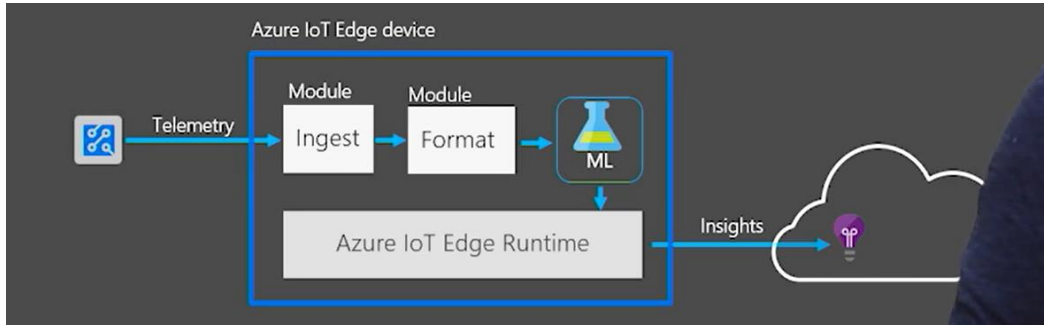
IoT: Azure Edge

- Data stays local
- Runtime on device:
  - Connectivity & security
    - Devices Backnet connected to the internet
    - Devices can be seen as unique devices with their own identity
    - Edge can store data event and forward it to the cloud
  - Runtime manage modules:
    - Add capabilities to the runtime
    - You create a processing pipeline
    - Modules are based on Docker container
    - You can write your customer modules



IoT: Azure Analytics

- Cloud offload:
  - Run cloud compute services on Edge
  - For example near real-time analytics
  - Azure functions
  - Edge Analytics 3d party Edge Services



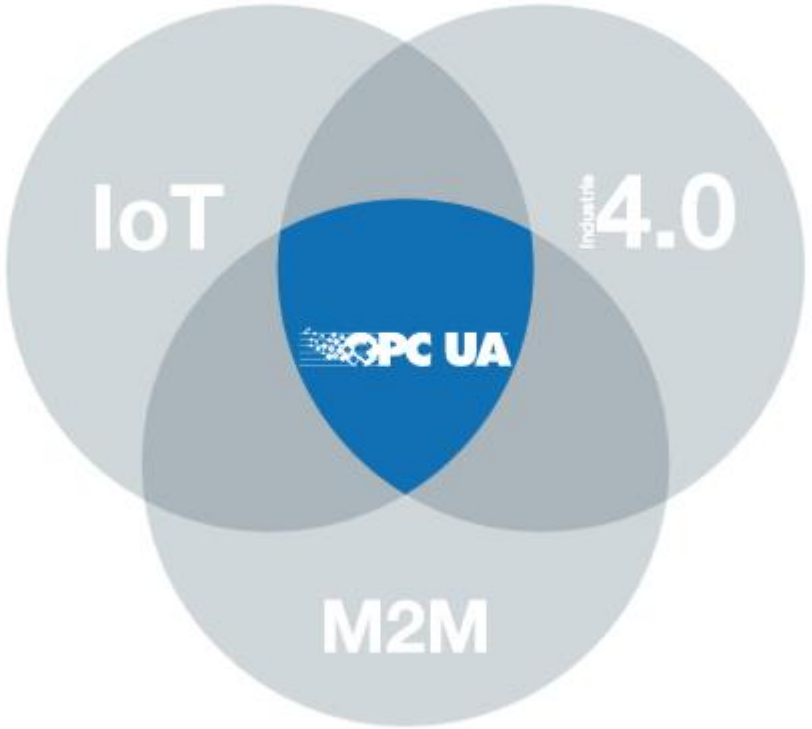
OPC-UA: Overview

OPC-UA:

- Open Platform Communication (OPC)
- Unified Architecture (UA)
- Composed of:
  - Internet of Things (IoT)
  - Web 4.0
  - Machine to Machine (M2M)

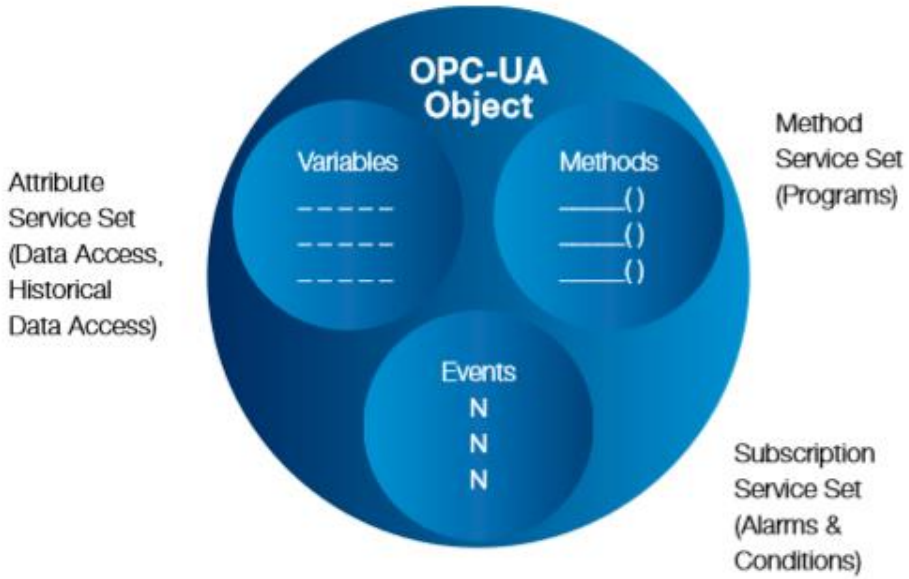
Industry 4.0 Requirements:

- Bridging communication protocols and devices
- Scalable networks (IoT)
- Secure communication
- Service according to standards
- Complex data objects
- Pull-Push and ad-hoc communication

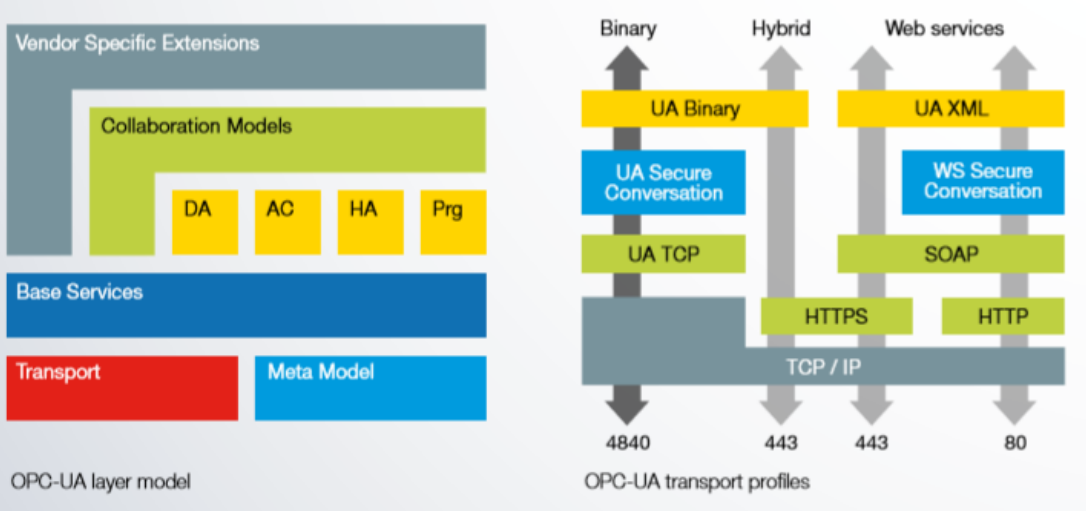


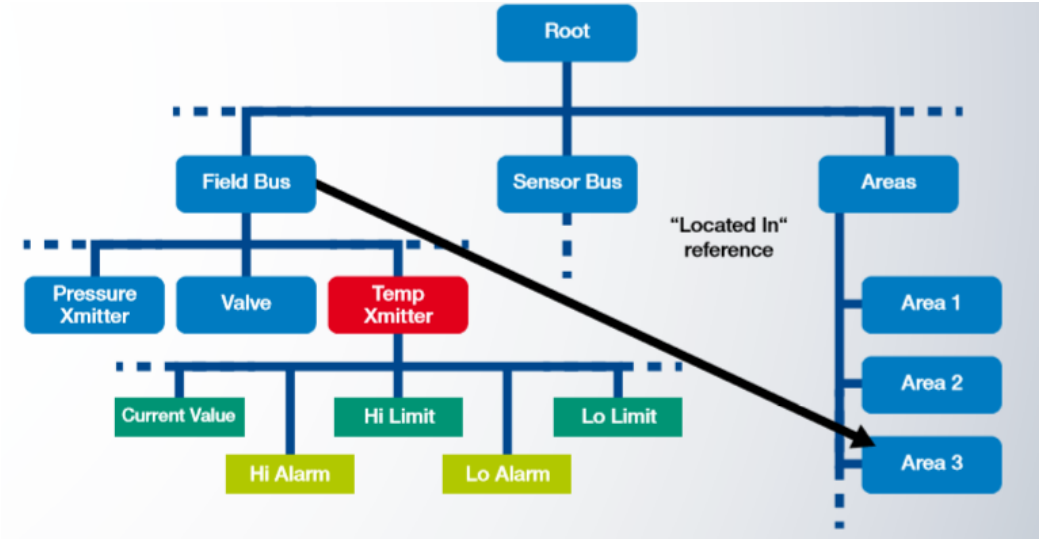
OPC-UA: Overview

Industrie 4.0 requirements	OPC-UA solution
Independence of the communication technology from manufacturer, sector, operating system, programming language	The OPC Foundation is a vendor-independent non-profit organization. Membership is not required for using the OPC-UA technology or for developing OPC-UA products. OPC is widely used in automation but is technologically sector-neutral. OPC-UA runs on all operating systems – there are even chip layer implementations without an operating system. OPC-UA can be implemented in all languages – currently stacks in Ansi C/C++, .NET and Java are available.
Scalability for integrated networking including the smallest sensors, embedded devices and PLC controllers, PCs, smartphones, mainframes and cloud applications. Horizontal and vertical communication across all layers.	OPC-UA scales from 15 kB footprint (Fraunhofer Lemgo) through to single- and multi-core hardware with a wide range of CPU architectures (Intel, ARM, PPC, etc.) OPC-UA is used in embedded field devices such as RFID readers, protocol converters etc. and in virtually all controllers and SCADA/HMI products as well as MES/ERP systems. Projects have already been successfully realized in Amazon and Microsoft Azure Cloud.
Secure transfer and authentication at user and application level	OPC-UA uses X.509 certificates, Kerberos or user/password for authentication of the application. Signed and encrypted transfer, as well as a rights concept at data point level with audit functionality is available in the stack.
SOA, transport via established standards such as TCP/IP for exchanging live and historic data, commands and events (event/callback)	OPC-UA is independent of the transport method. Currently two protocol bindings are available: optimized TCP-based binary protocol for high-performance applications and HTTP/HTTPS web service with binary or XML coded messages. Additionally Publish/Subscribe communication model can be integrated. The stacks guarantee consistent transport of all data. Besides live and real time data also historical data and their mathematical aggregation are standardized in OPC-UA. Furthermore method calls with complex arguments are possible, but also alarm and eventing via token based mechanism (late polling).
Mapping of information content with any degree of complexity for modelling of virtual objects to represent the actual products and their production steps.	OPC-UA provides a fully networked concept for an object oriented address space (not only hierarchical but full-meshed network), including metadata and object description. Object structures can be generated via referencing of the instances among each other and their types and a type model that can be extended through inheritance. Since servers carry their instance and type system, clients can navigate through this network and obtain all the information they need, even for types that were unknown to them before. This is a base requirement for Plug-and-Produce functionality without prior configuration of the devices.
Unplanned, ad hoc communication for plug-and-produce function with description of the access data and the offered function (services) for self-organized (also autonomous) participation in "smart" networked orchestration/combination of components	OPC-UA defines different "discovery" mechanisms for identification and notification of OPC-UA-capable devices and their functions within a network. OPC-UA participants can be located local (on the same host), in a subnet or global (within enterprise). Aggregation across subnets and Intelligent, configuration-less procedure (e.g. Zeroconf) are used to identify and address network participants.
Integration into engineering and semantic extension	The OPC Foundation already collaborates successfully with other organizations (PLCopen, BACnet, FDI, AIM, etc.) and is currently expanding its cooperation activities, e.g. MES-DACH, ISA95, MDIS (oil and gas industry), etc. A new cooperation initiative is with AutomationML, with the aim of optimizing interoperability between engineering tools.
Verification of conformity with the defined standard	OPC-UA is already an IEC standard (IEC 62541), and tools and test laboratories for testing and certifying conformity are available. Additional test events (e.g. Plugfest) enhance the quality and ensure compatibility. Expanded tests are required for extensions/amendments (companion standards, semantics). Additionally various validations regarding data security and functional safety are performed by external test and certification bodies.

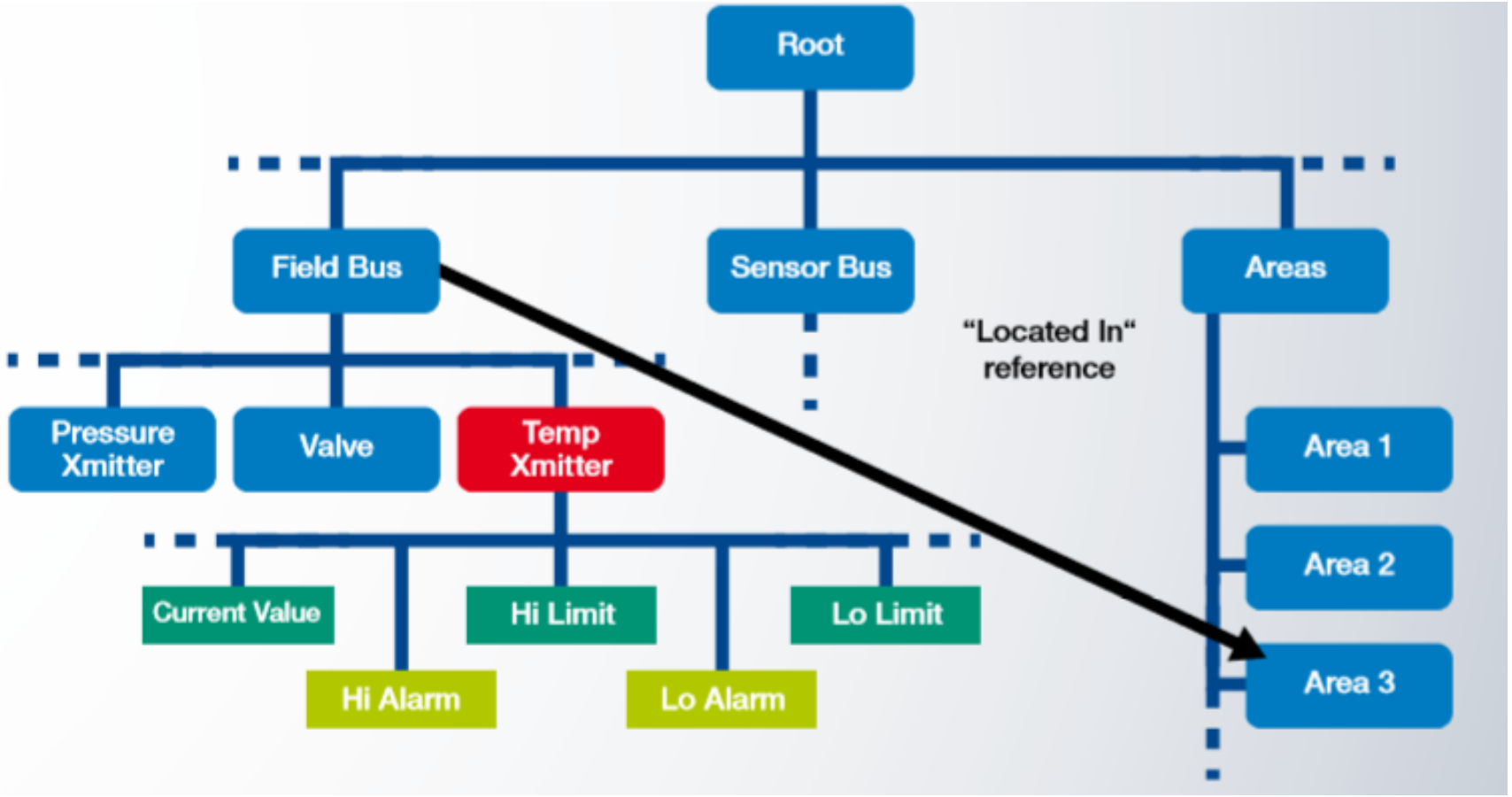


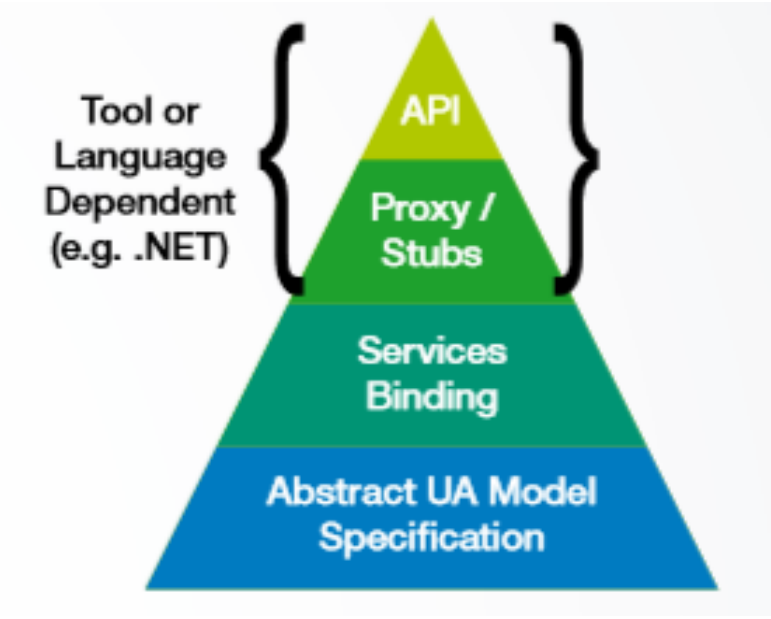
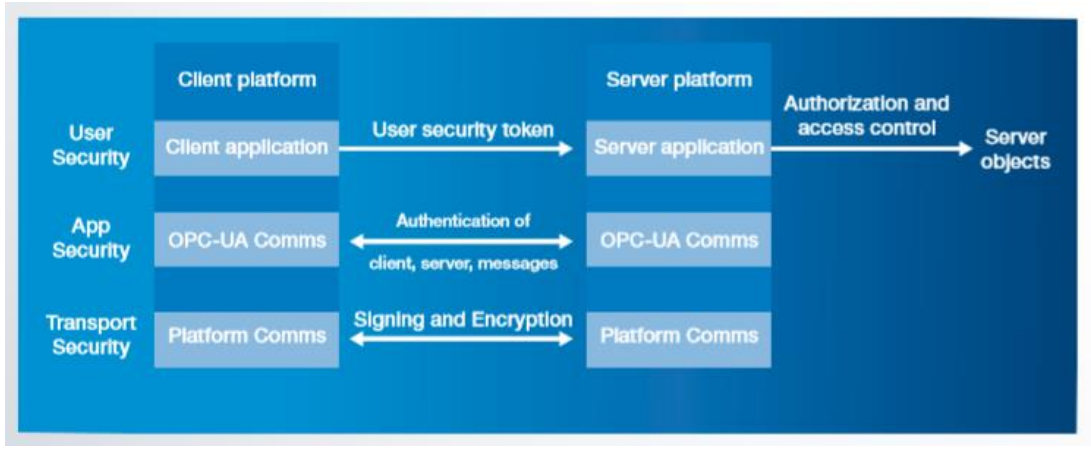
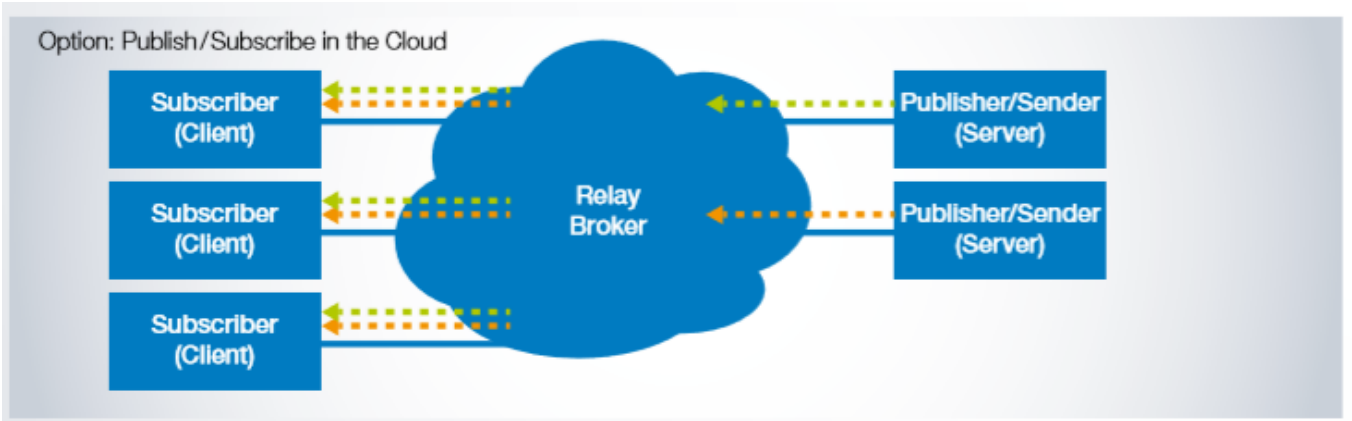
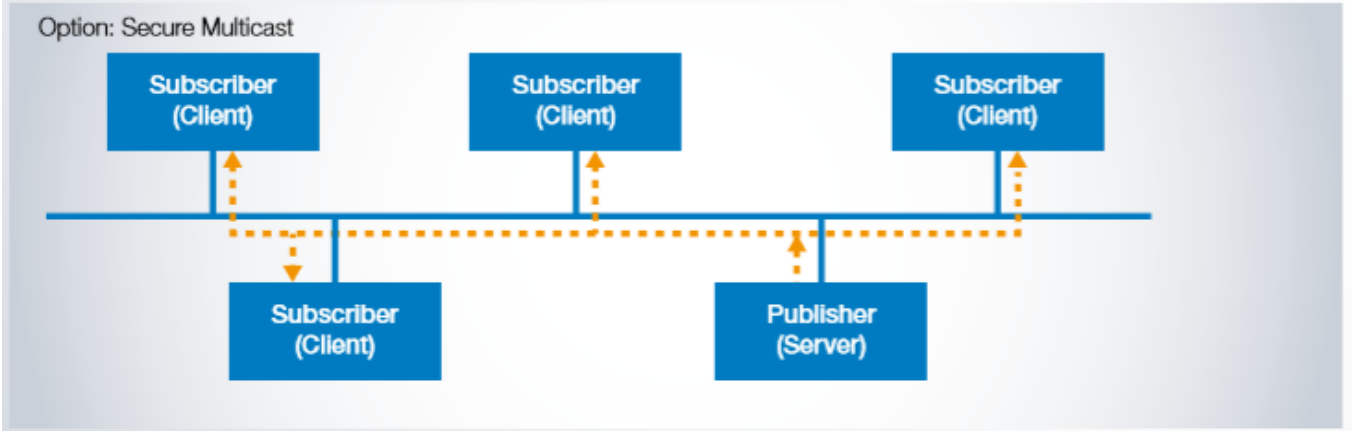
OPC-UA: Overview





OPC-UA: Overview





OPC-UA: Overview