CSE 425: Internet of Things

Dept. of CSE, BUBT| Summer 2021

Md. Hasibur Rahman

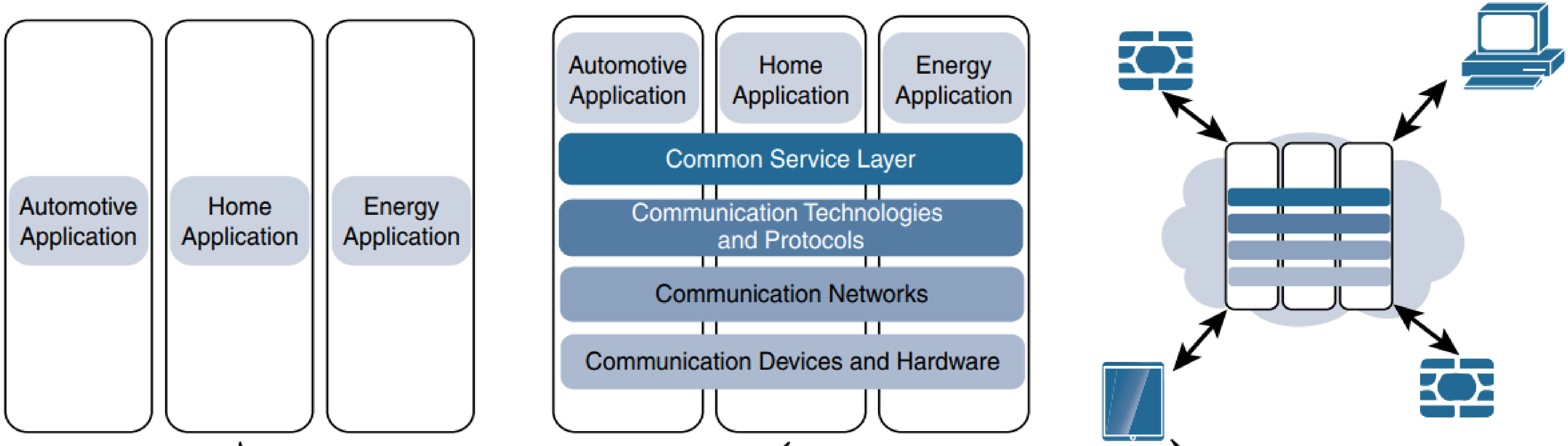
IoT Network Architecture and Design

IoT Architecture: oneM2M

One of the greatest challenges in designing an IoT architecture is dealing with the heterogeneity of devices, software, and access methods. By developing a horizontal platform architecture, oneM2M is developing standards that allow interoperability at all levels of the IoT stack. For example, you might want to automate your HVAC system by connecting it with wireless temperature sensors spread throughout your office. You decide to deploy sensors that use LoRaWAN technology (discussed in Chapter 4, “Connecting Smart Objects”). The problem is that the LoRaWAN network and the BACnet system that your HVAC and BMS run on are completely different systems. This is where the oneM2M common services architecture comes in. oneM2M’s horizontal framework and RESTful APIs allow the LoRaWAN system to interface with the building management system over an IoT network, thus promoting end-to end IoT communications in a consistent way, no matter how heterogeneous the networks.

IoT Architecture: oneM2M Main Elements

In 2012 ETSI and 13 other founding members launched oneM2M.



Applications Layer:

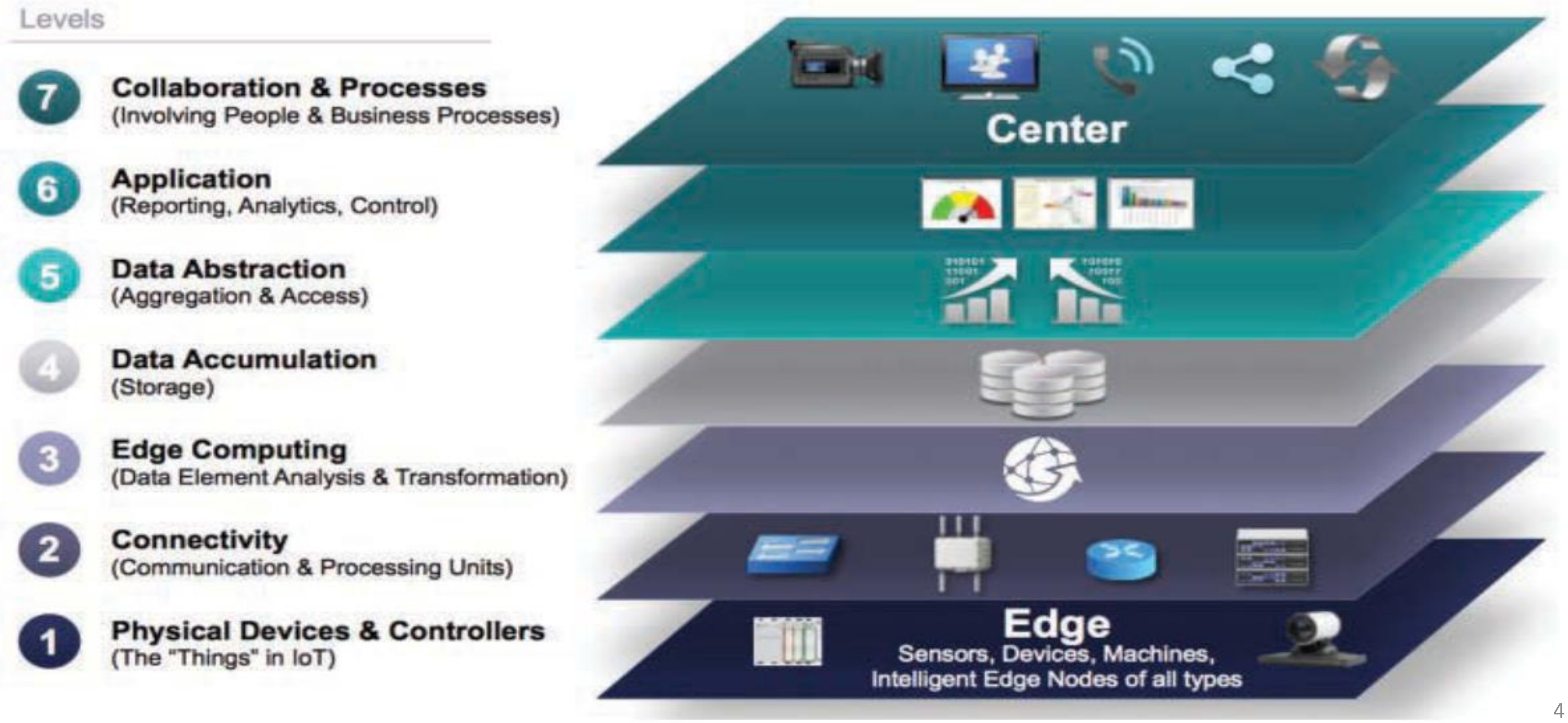
- Smart Energy
- Asset Tracking
- Fleet Management

Services Layer:
oneM2M includes a common services horizontal framework supporting Restful APIs

Network Layer:
Applications talk to the APIs to communicate to sensors

The IoT World Forum (IoTWF) Standardized Architecture

In 2014 the IoTWF architectural committee (led by Cisco, IBM, Rockwell Automation, and others) published a seven-layer IoT architectural reference model.


Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types

The IoT World Forum (IoTWF) Standardized Architecture

Using the above reference model, we are able to achieve the following:

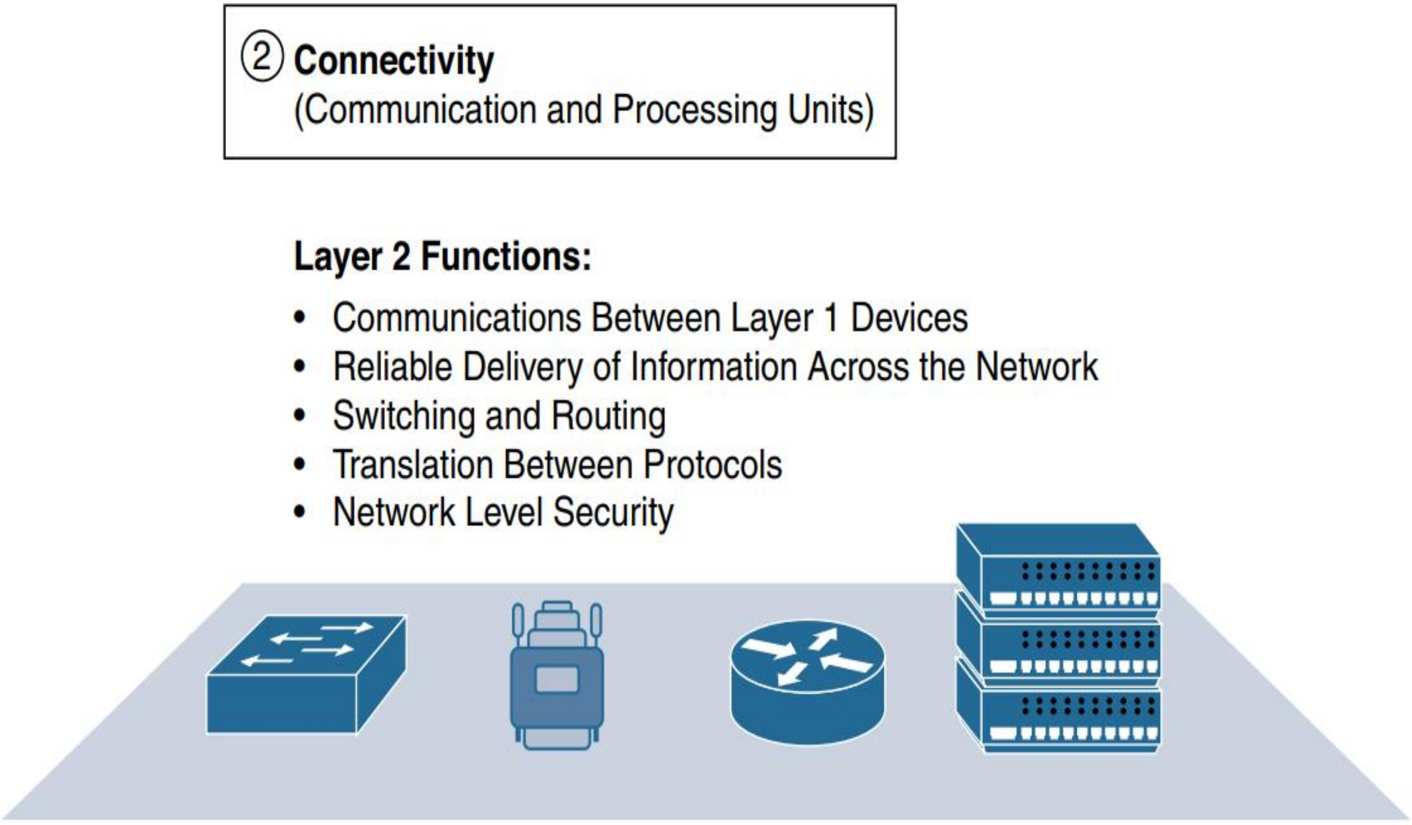
- Decompose the IoT problem into smaller parts
- Identify different technologies at each layer and how they relate to one another
- Define a system in which different parts can be provided by different vendors
- Have a process of defining interfaces that leads to interoperability
- Define a tiered security model that is enforced at the transition points between levels

Closer Look at the Layers

Layer 1: Physical Devices and Controllers Layer

The first layer of the IoT Reference Model is the physical devices and controllers layer. This layer is home to the *“things”* in the Internet of Things, including the various *endpoint devices* and *sensors that send and receive information*. The size of these “things” can range from almost microscopic sensors to giant machines in a factory. Their primary function is generating data and being capable of being *queried and/or controlled over a network*.

Closer Look at the Layers



② **Connectivity**
(Communication and Processing Units)

Layer 2 Functions:

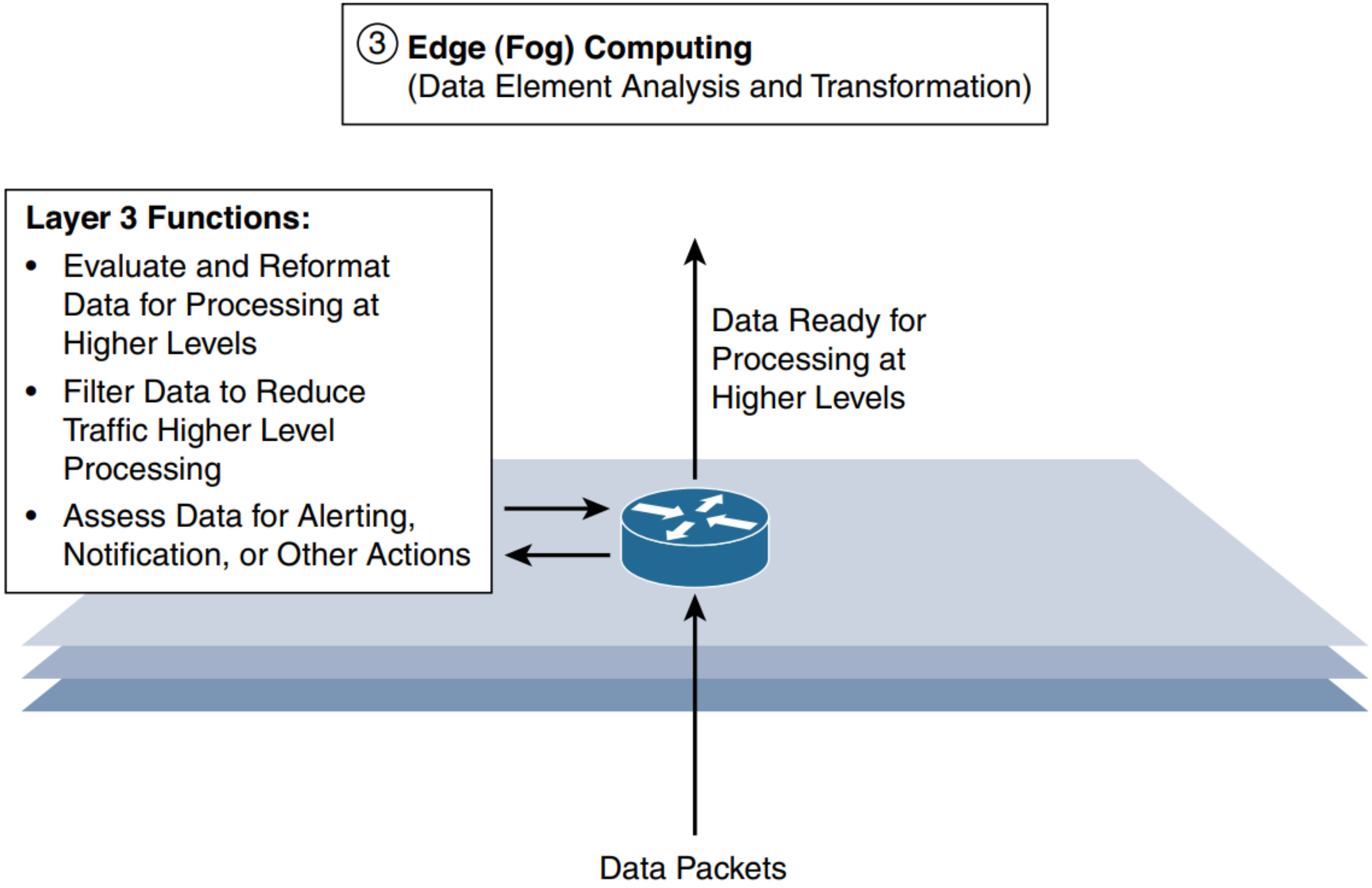
- Communications Between Layer 1 Devices
- Reliable Delivery of Information Across the Network
- Switching and Routing
- Translation Between Protocols
- Network Level Security

Layer 2: Connectivity Layer

this includes transmissions between Layer 1 devices and the network and between the network and information processing that occurs at Layer 3 (the edge computing layer).

Closer Look at the Layers

Layer 3: Edge Computing Layer



③ **Edge (Fog) Computing**
(Data Element Analysis and Transformation)

Layer 3 Functions:

- Evaluate and Reformat Data for Processing at Higher Levels
- Filter Data to Reduce Traffic Higher Level Processing
- Assess Data for Alerting, Notification, or Other Actions

Closer Look at the Layers

Upper Layers: Layers 4–7

Layer	Functions
Layer 4: Data accumulation layer	Captures data and stores it so it is usable by applications when necessary. Converts *event-based data to query-based* processing.
Layer 5: Data abstraction layer	*Reconciles multiple data formats* and ensures consistent semantics from various sources. Confirms that the data set is complete and *consolidates data into one place or multiple data stores using virtualization*.
Layer 6: Applications layer	Interprets data using software applications. Applications may monitor, control, and provide reports based on the analysis of the data.
Layer 7: Collaboration and processes layer	Consumes and shares the application information. Collaborating on and communicating IoT information often requires multiple steps, and it is what makes IoT useful. This layer can change business processes and delivers the benefits of IoT.

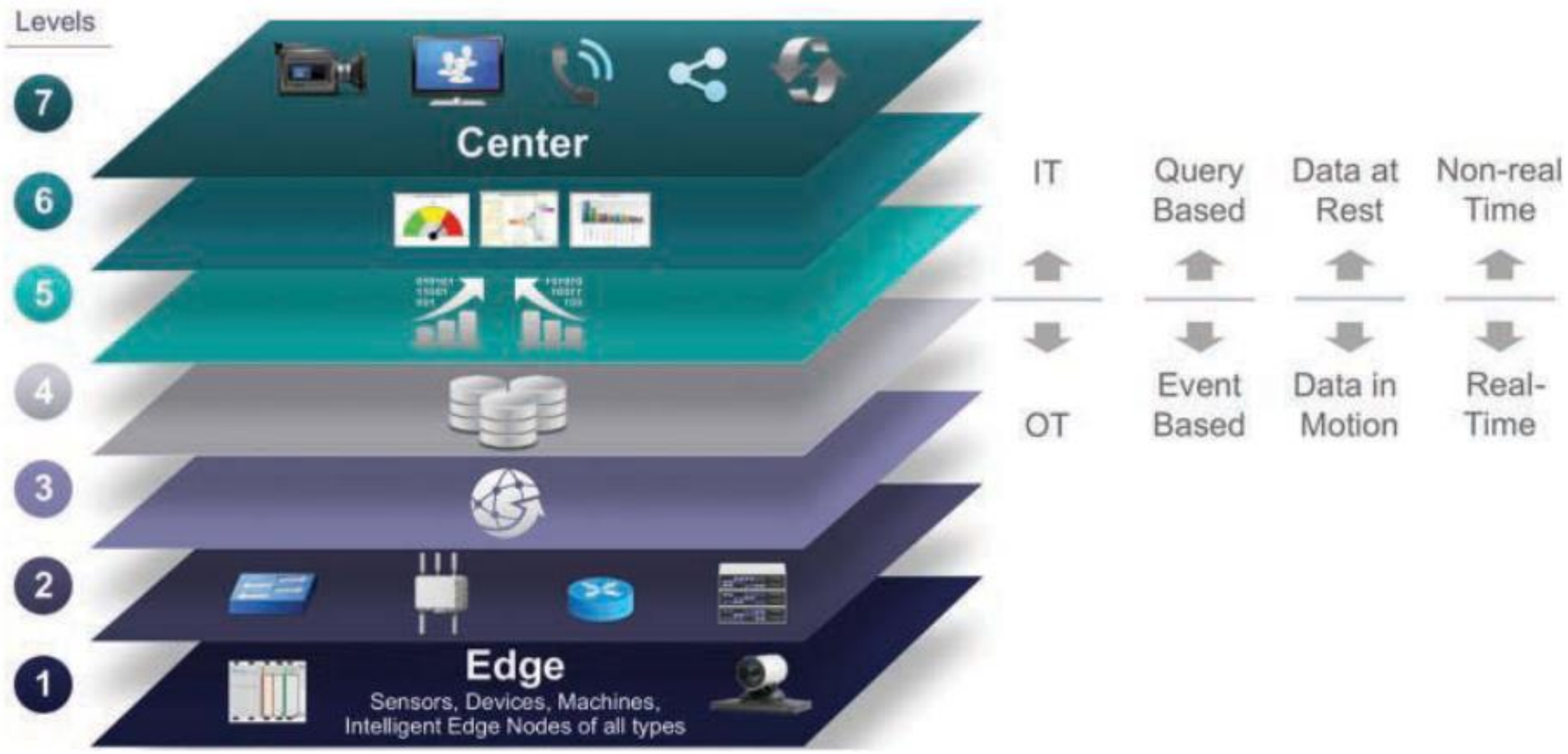
IT and OT

IT organization is responsible for the information systems of a business, such as email, file and print services, databases, and so on.

OT is responsible for the devices and processes acting on industrial equipment, such as factory machines, meters, actuators, electrical distribution automation devices, SCADA (supervisory control and data acquisition) systems, and so on.

Management of *OT is tied to the lifeblood* of a company. For example, if the *network connecting the machines in a factory fails*, the machines cannot function, and production may come to a standstill, negatively impacting business on the order of millions of dollars. On the other hand, if *the email server (run by the IT department) fails* for a few hours, it may irritate people, but it is unlikely to impact business at anywhere near the same level.

Convergence of IT and OT, and IoTWF Architecture



IT vs OT in Industrial Application

Criteria	OT	IT
Operational focus	Keep the business operating 24x7	Manage the computers, data, and employee communication system in a secure way
Priorities	1. Availability 2. Integrity 3. Security	1. Security 2. Integrity 3. Availability
Types of data	Monitoring, control, and supervisory data	Voice, video, transactional, and bulk data
Security	Controlled physical access to devices	Devices and users authenticated to the network
Implication of failure	OT network disruption directly impacts business	Can be business impacting, depending on industry, but workarounds may be possible
Network upgrades (sw or hw)	Only during operational maintenance windows	Often requires an outage window when workers are not onsite; impact can be mitigated
Security vulnerability	Low: OT networks are isolated and often use proprietary protocols	High: continual patching of hosts is required, and the network is connected to Internet and requires vigilant protection

Alternative IoT Reference Model

- Purdue Model for Control Hierarchy:

  www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG/ch2_EttF.pdf

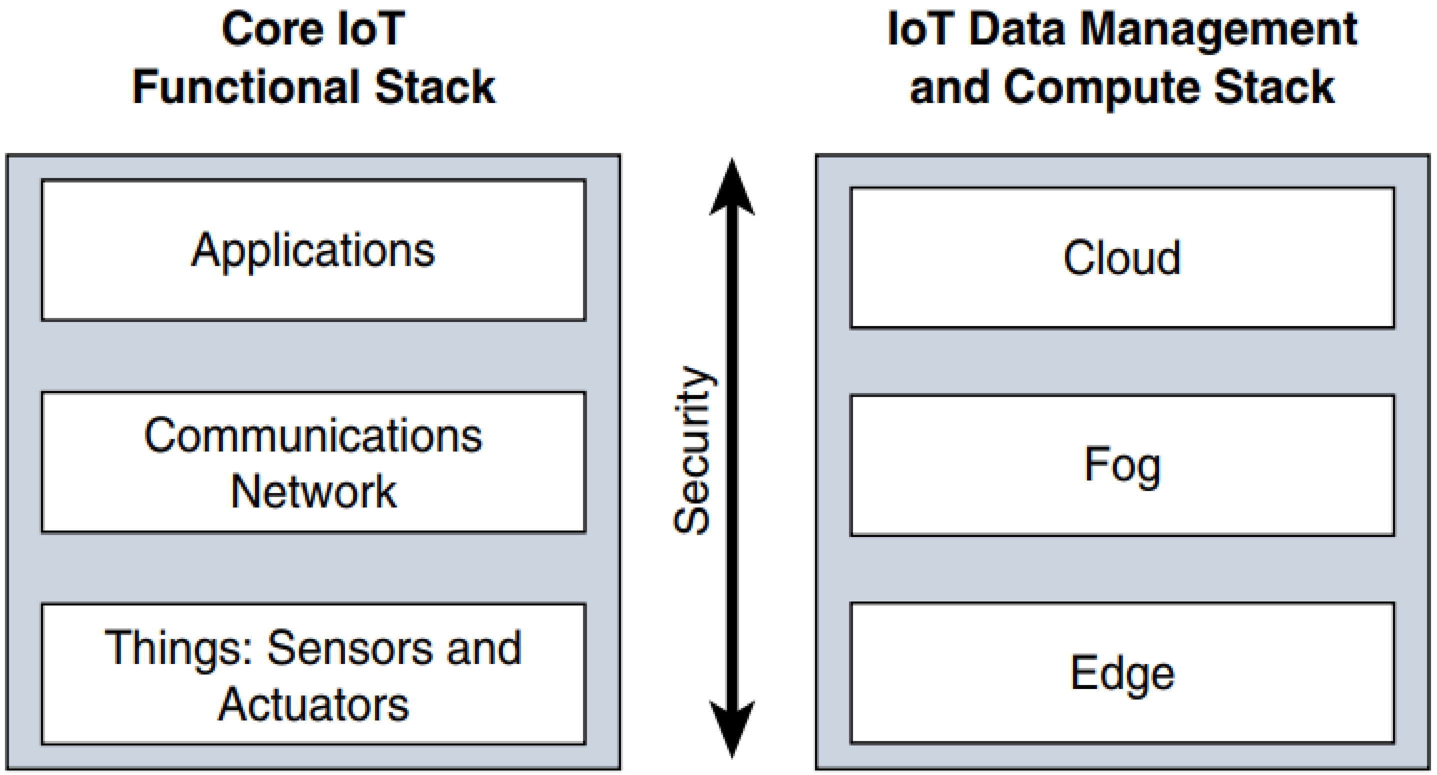
- Industrial Internet Reference Architecture (IIRA) by Industrial Internet Consortium

  www.iiconsortium.org/IIRA.htm

- Internet of Things– Architecture (IoT-A)

  https://vdivde-it.de/en

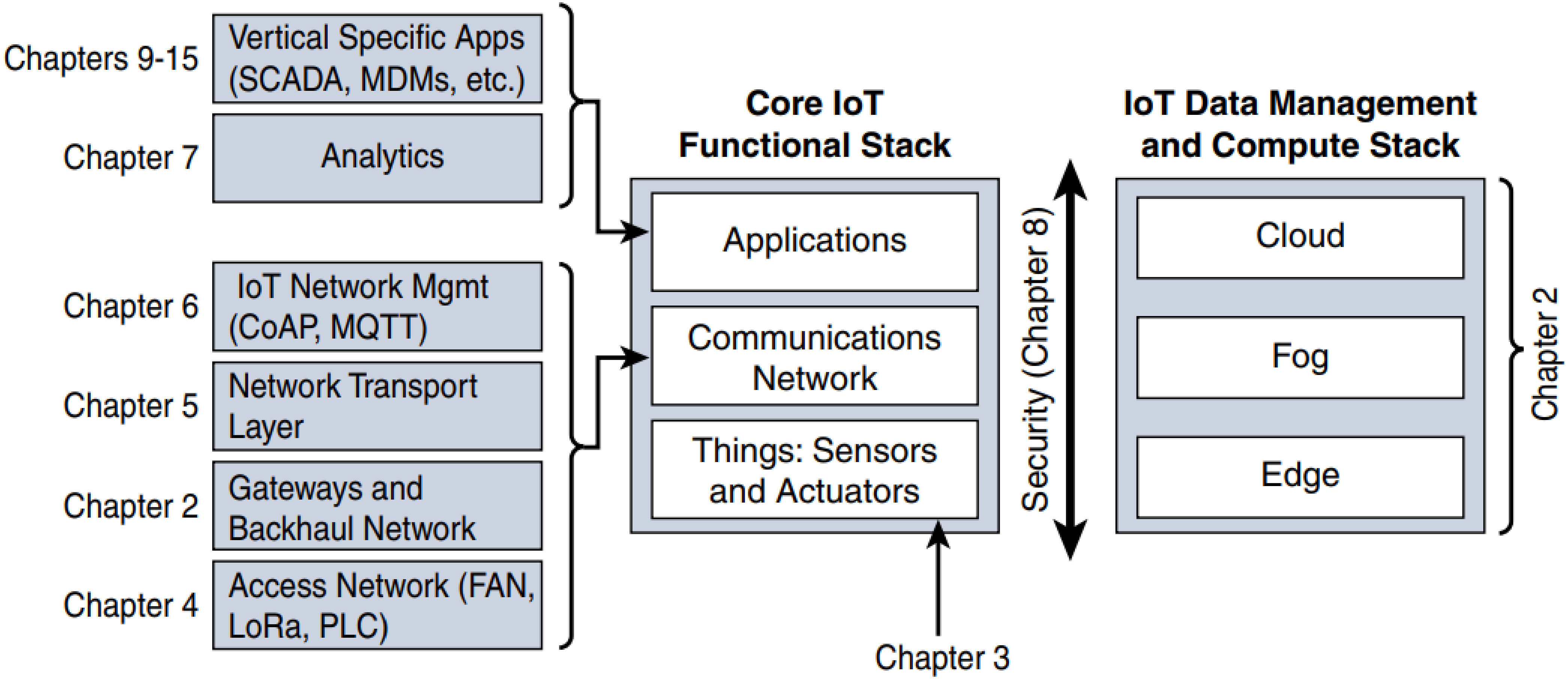
A Simplified IoT Architecture



Although differences exist between the aforementioned reference models, interconnection of the IoT endpoint devices to a network that transports the data where it is ultimately used by applications, whether at the data center, in the cloud, or at various management points throughout the stack.

This framework is presented as two parallel stacks: The IoT Data Management and Compute Stack and the Core IoT Functional Stack. Though it lacks detail necessary, our intention is to simplify the IoT architecture into its most basic building blocks. All the layers will still cover but they are grouped here in functional blocks that are easy to understand.

A Simplified IoT Architecture: Expanded View


Chapters 9-15
Vertical Specific Apps (SCADA, MDMs, etc.)
Chapter 7
Analytics
Chapter 6
IoT Network Mgmt (CoAP, MQTT)
Chapter 5
Network Transport Layer
Chapter 2
Gateways and Backhaul Network
Chapter 4
Access Network (FAN, LoRa, PLC)
Core IoT Functional Stack
Applications
Communications Network
Things: Sensors and Actuators
Chapter 3
Security (Chapter 8)
IoT Data Management and Compute Stack
Cloud
Fog
Edge
Chapter 2

The Core IoT Functional Stack

IoT networks are built around the concept of "things," or smart objects performing functions and delivering new connected services. These objects are "smart" because they use a combination of contextual information and configured goals to perform actions. Actions can be self contained or interaction with an external system to report information that the smart object collects.

From an architectural standpoint, several components have to work together for an IoT network to be operational:

1. **"Things" layer:** physical devices need to fit the constraints of the environment in which they are deployed in which they are deployed while being able to provide the information needed.
2. **Communications network layer:** When smart objects are not self-contained, they need to communicate with an external system. In many cases, this communication uses a wireless technology. This layer has four sublayers:

The Core IoT Functional Stack

2. **Communications network sub layers:**

   a) **Access network sublayer:** The last mile of the IoT network is the access network. This is typically made up of wireless technologies such as 802.11ah, 802.15.4g, and LoRa. The sensors connected to the access network may also be wired.

   b) **Gateways and backhaul network sublayer:** The role of the gateway is to forward the collected information from smart objects through a longer-range medium (called the backhaul) to a headend central station where the information is processed.

   c) **Network transport sublayer:** For communication to be successful, network and transport layer protocols such as IP and UDP must be implemented to support the variety of devices to connect and media to use.

   d) **IoT network management sublayer:** Additional protocols must be in place to allow the headend applications to exchange data with the sensors. Examples include CoAP and MQTT.

The Core IoT Functional Stack

3. Application and analytics layer:

At the upper layer, an application needs to process the collected data, not only to control the smart objects when necessary, but to make intelligent decision based on the information collected and, in turn, instruct the "things" or other systems to adapt to the analyzed conditions and change their behaviors or parameters.

> "When something is important enough, you do it even if the odds are not in your favor."
>
> -Elon Musk

Layer 1: Things: Sensors and Actuators Layer

- **Battery-powered or power-connected:** This classification is based on whether the object carries its own energy supply or receives continuous power from an external power source.

  Issues: moving, lifetime

- **Mobile or static:** This classification is based on whether the "thing" should move or always stay at the same location. A sensor may be mobile because it is moved from one object to another (for example, a viscosity sensor moved from batch to batch in a chemical plant) or because it is attached to a moving object (for example, a location sensor on moving goods in a warehouse or factory floor).

  Issues: frequency of the movement, range of mobility

- **Low or high reporting frequency:** This classification is based on how often the object should report monitored parameters. A rust sensor may report values once a month. A motion sensor may report acceleration several hundred times per second.

  Issues: higher frequencies drive higher energy consumption

Layer 1: Things: Sensors and Actuators Layer

- **Simple or rich data:** This classification is based on the quantity of data exchanged at each report cycle. A humidity sensor in a field may report a simple daily index value (on a binary scale from 0 to 255), while an engine sensor may report hundreds of parameters, from temperature to pressure, gas velocity, compression speed, carbon index, and many others.

  Issues: Richer data typically drives higher power consumption

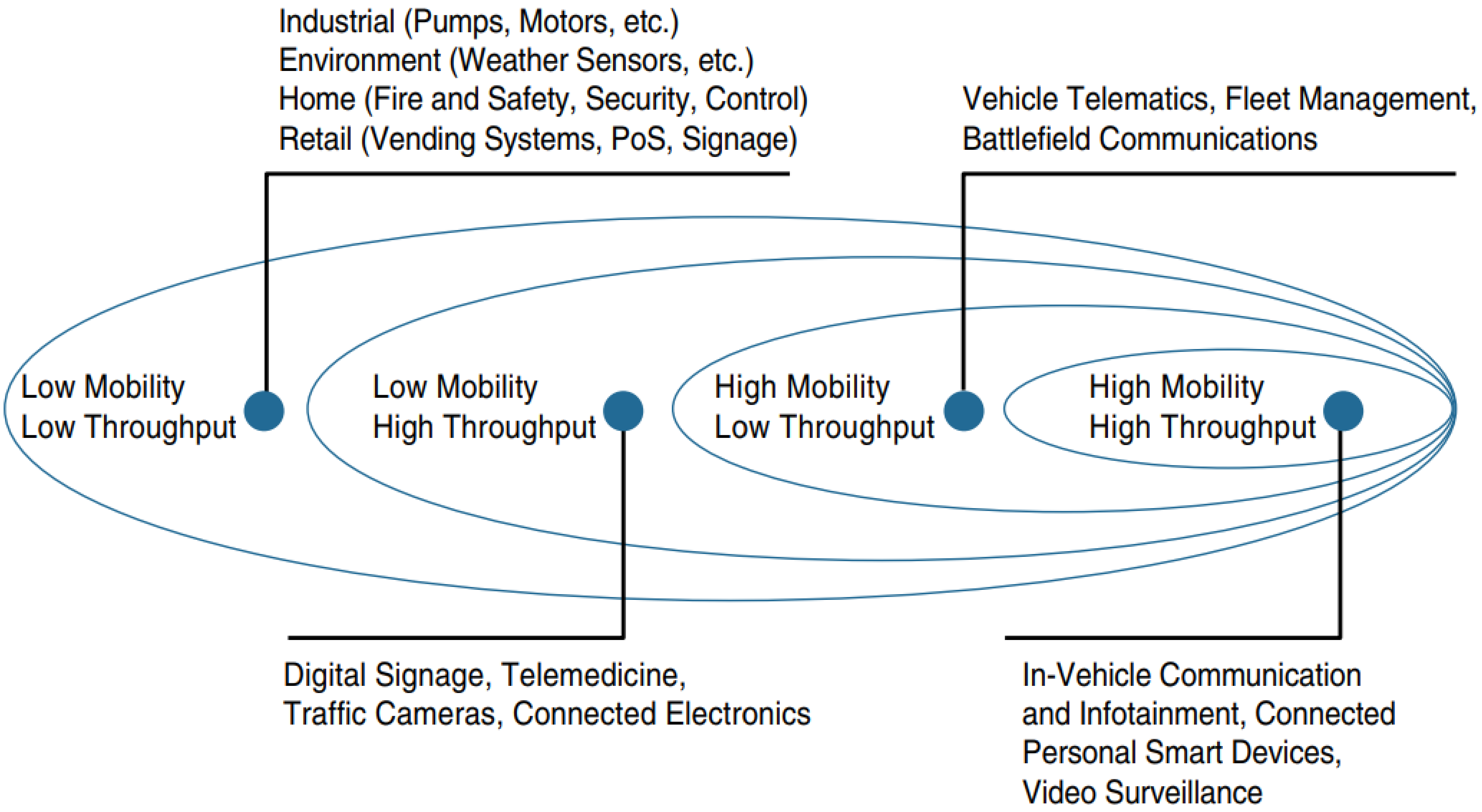
- **Report range:** This classification is based on the distance at which the gateway is located. Imagine amazon alexa in your home and a moisture sensor in the asphalt of a road may need to communicate with its reader several hundred meters or even kilometers away.

- **Object density per cell:** This classification is based on the number of smart objects (with a similar need to communicate) over a given area, connected to the same gateway. An oil pipeline may utilize a single sensor at key locations every few miles. By contrast, telescopes like the SETI Colossus telescope at the Whipple Observatory deploy hundreds, and sometimes thousands, of mirrors over a small area, each with multiple gyroscopes, gravity, and vibration sensors.

What should be in your head during IoT design

- Determine which technology should be used to allow smart objects to communicate. This determination depends on the way the "things" are classified.
- The categories used to classify things can influence other parameters and can also influence one another.
- **Example 1:** A battery-operated highly mobile object (like a heart rate monitor, for example) likely has a small form factor. A small sensor is easier to move or integrate into its environment. At the same time, a small and highly mobile smart object is unlikely to require a large antenna and a powerful power source. This constraint will limit the transmission range and, therefore, the type of network protocol available for its connections.
- **Example 2:** The criticality of data may also influence the form factor and, therefore, the architecture. missing monthly report from an asphalt moisture sensor may simply flag an indicator for sensor (or battery) replacement. A multi-mirror gyroscope report missing for more than 100 ms may render the entire system unstable or unusable. These sensors either need to have a constant source of power (resulting in limited mobility) or need to be easily accessible for battery replacement (resulting in limited transmission range).

Example of Sensor Applications Based on Mobility and Throughput



Industrial (Pumps, Motors, etc.)
Environment (Weather Sensors, etc.)
Home (Fire and Safety, Security, Control)
Retail (Vending Systems, PoS, Signage)

Vehicle Telematics, Fleet Management,
Battlefield Communications

Digital Signage, Telemedicine,
Traffic Cameras, Connected Electronics

In-Vehicle Communication
and Infotainment, Connected
Personal Smart Devices,
Video Surveillance