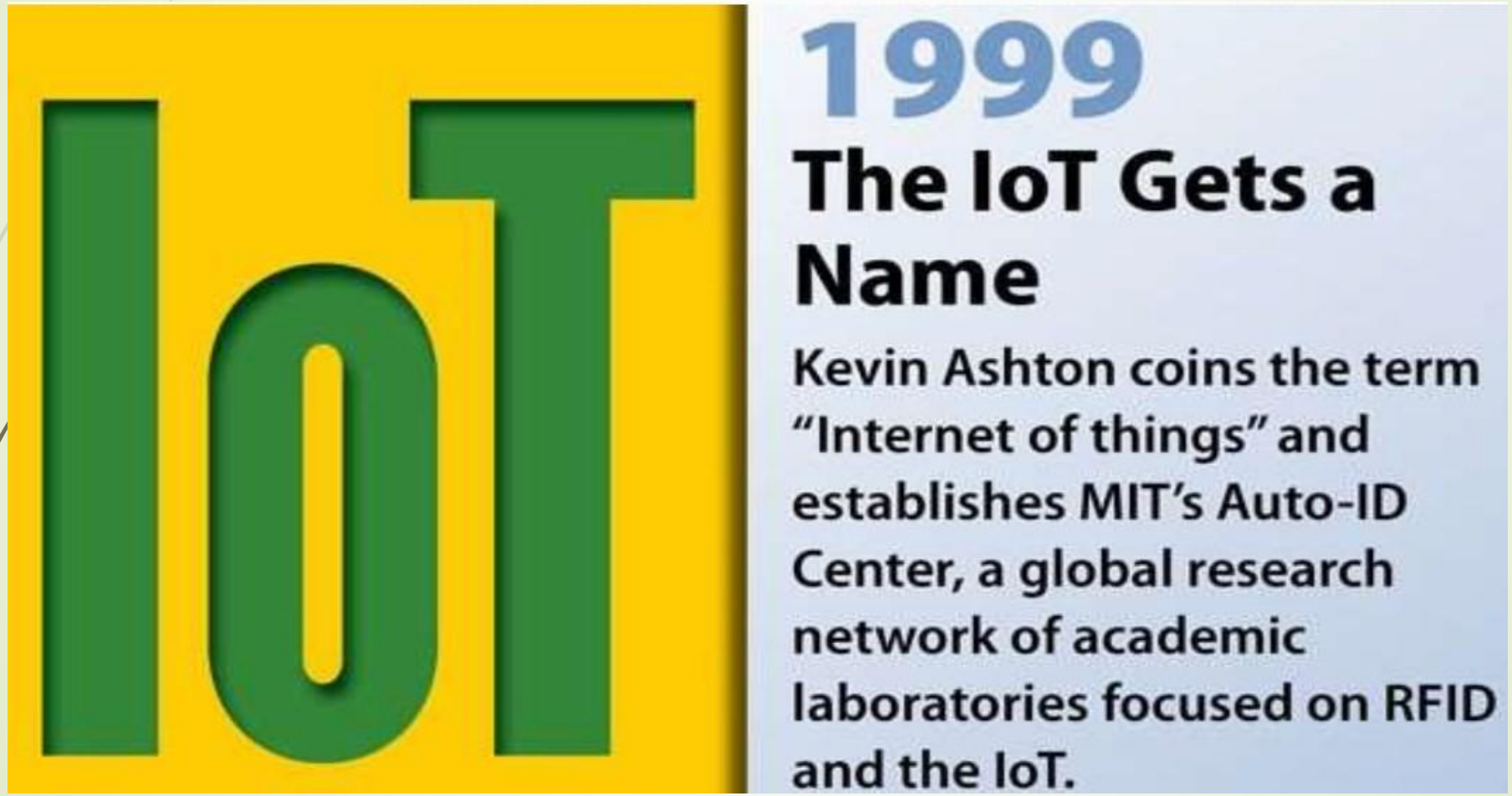
Module 1: IOT Introduction

- Goal of IoT:
  - Connect the unconnected
  - Objects that are not currently joined to a computer network-Internet, will be connected so that they can communicate and interact with people and other objects.
- IoT is a technology transition in which the devices will allow us to sense and control the physical world by making objects smarter and connecting them through an intelligent network.
- When objects and machines can be sensed and controlled remotely by across a network, a tighter integration between physical world and computers are enabled. This allows enablement of advanced applications.

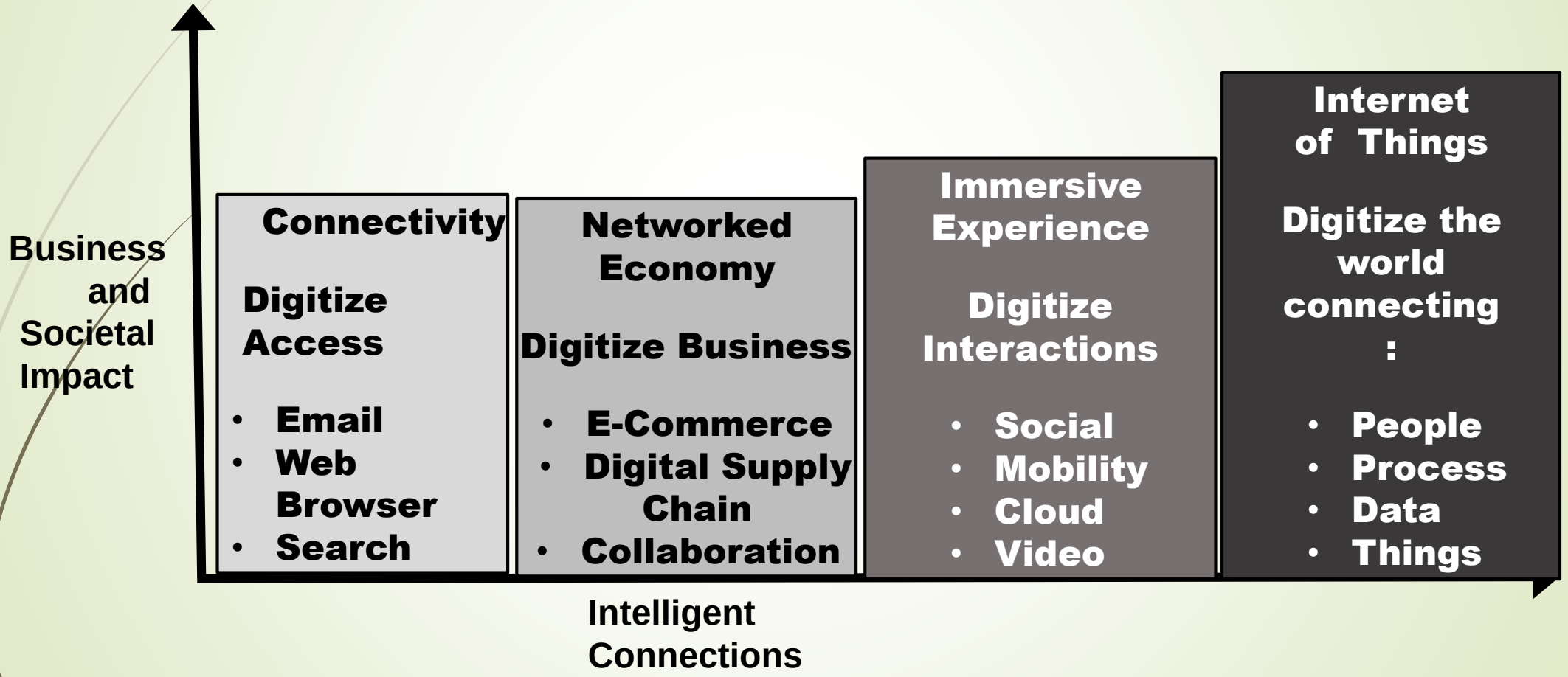
IOT Introduction

- **History: IoT involves the addition of senses to computers.**



IOT Introduction

- Evolutionary Phases of the Internet



IOT Introduction

Evolutionary Phases of the Internet

Internet Phase	Definition
Connectivity (Digitize Access)	This phase connected people to email, web services and search, so that information is easily accessed.
Networked Economy (Digitize Business)	This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business.
Immersive Experiences (Digitize Interactions)	This phase extended the Internet Experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved to Cloud.
Internet of Things (Digitize the World)	This phase is adding connectivity to Objects and machines to the world around us to enable new services and experiences. It is connecting the unconnected.

IOT Introduction

Evolutionary Phases of the Internet

Internet Phase: first Phase	Connectivity(Digitize Access)

- Began in the mid 1990s.
- Email and getting Internet were luxuries for universities and corporations.
- Dial-up modems and basic connectivity were involved.
- Saturation occurred when connectivity and speed was not a challenge.
- The focus now was on leveraging connectivity for efficiency and profit.

IOT Introduction

Evolutionary Phases of the Internet

Internet Phase: Second Phase	Networked Economy (Digitize Business)

- E-Commerce and digitally connected supply chains become the rage.
- Caused one of the major disruptions of the past 100 years.
- Vendors and suppliers became closely interlinked with producers.
- Online Shopping experienced incredible growth .
- The economy become more digitally intertwined as suppliers, vendors and consumers all became more directly connected.

IOT Introduction

Evolutionary Phases of the Internet

Internet Phase: Third Phase	Immersive Experiences (Digitize Interactions)

- Immersive Experiences, is characterized by the emergence of social media, collaborations and widespread mobility on a variety of devices.
- Connectivity is now pervasive, using multiple platforms from mobile phones to tablets to laptops and desktop computers.
- Pervasive connectivity enables communications and collaboration as well as social media across multiple channels via email, texting, voice and video.
- Person to person interactions have become digitized.

IOT Introduction

Evolutionary Phases of the Internet

Internet Phase: Forth(last) Phase	Internet of Things (Digitize the World)

- We are in beginning of the IoT phase.
- 99% of “things” are still unconnected.
- Machines and objects in this phase connect with other machines and objects along with humans.
- Business and society are using and experiencing huge increase in data and knowledge.
- Increased automation and new process efficiencies, IoT is changing our world to new way.

IOT Introduction

IoT and Digitization

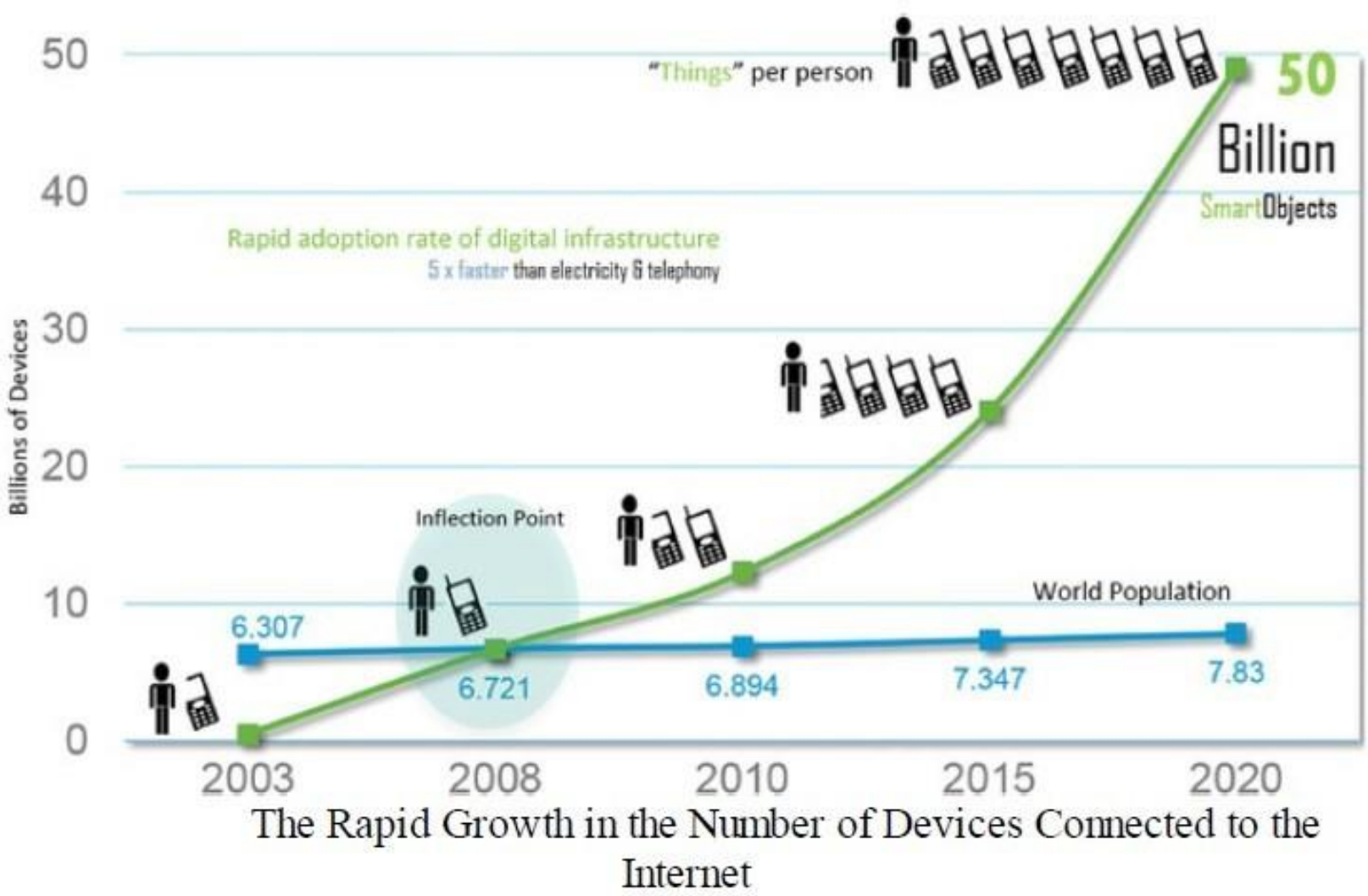
- At a high level, IoT focuses on connecting “things” such as objects and machines, to a computer network, such as the Internet.
- Digitization encompasses the connection of “things” with the data they generate and the business insights that result.
- Example: Wi-Fi devices in Malls detecting customers, displaying offers.
- Digitization: It is the conversion of information into a digital format.

IoT Impact

IoT Impact

- About 14 billion or 0.06% of “things” are connected to the internet today.
- Cisco predicts in 2020 , it may go upto 50 billion and says this new connection will lead to $19 trillion in profit and cost savings.
- UK government says 100 billion objects may connected
- Managing and monitoring smart objects using real –time connectivity enables a new level of data-driven decision making.
- This results in optimization of systems and processes and delivers new services that save time for both people and business while improving the overall quality of life.

IoT Impact



The Rapid Growth in the Number of Devices Connected to the Internet

IOT Impact on Connected Roadways

- **Connected Roadways- Google's Self Driving Car**
- **Connected Roadways is a term associated with both the drivers and driverless cars fully integrating with surrounding transportation and infrastructure.**
- **Basic sensors reside in cars monitor oil Pressure, tire pressure, temperature and other Operating conditions, provide data around Core car functions.**

Google's Self-Driving Car

➢ Connected Roadways

Current challenges being addressed by Connected Roadways

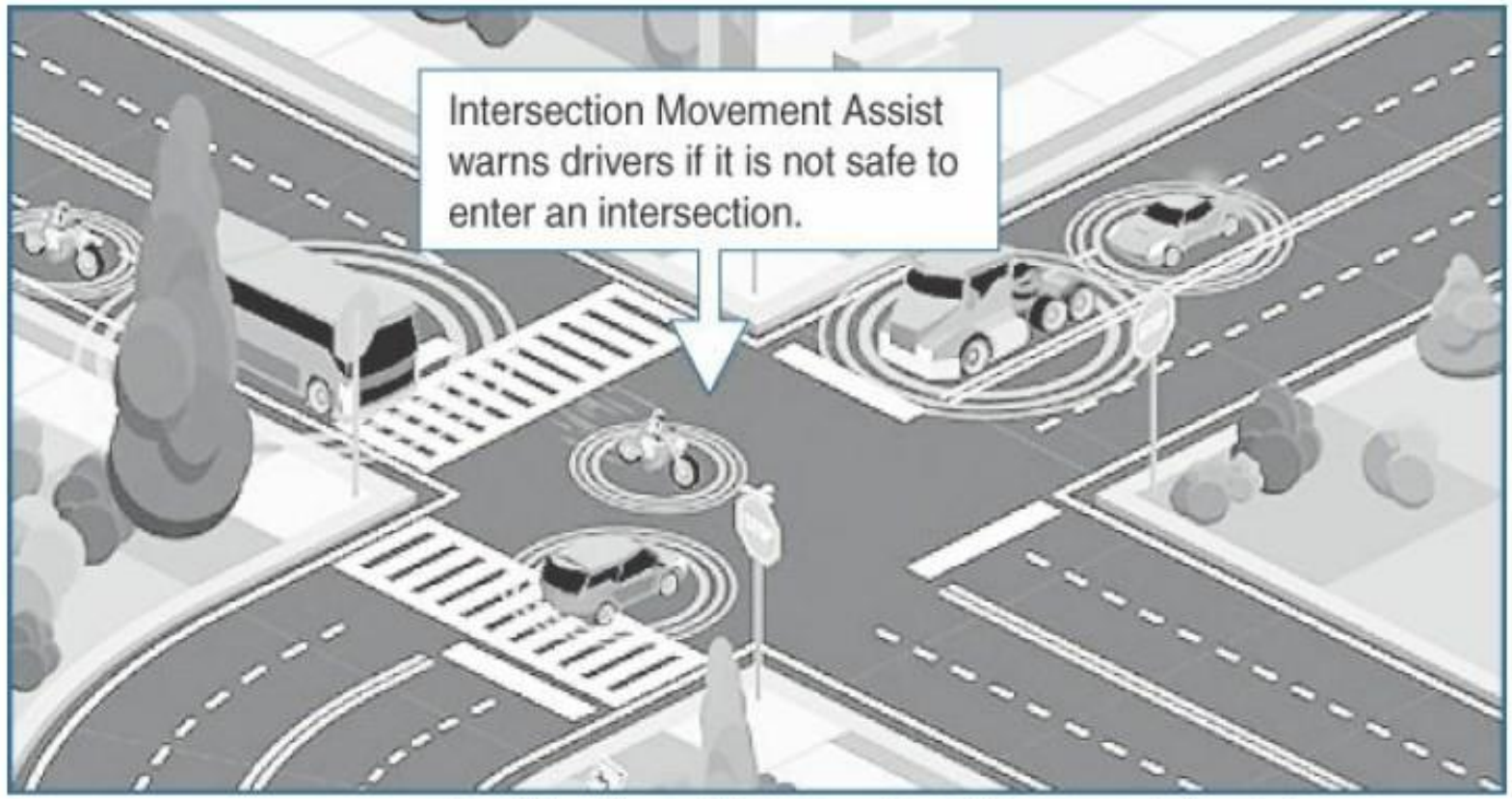
Challenge	Supporting Data
Safety	• 5.6 million crashes in 2012, 33,000 fatalities – US department of Transportation • IoT and enablement of connected vehicle technologies significantly reduces the loss of lives each year.
Mobility	• More than a billion cars on road worldwide. • Connected vehicle mobility application will give drivers more informed decisions which may reduce travel time. • Communication between mass transit, emergency response vehicle and traffic management help optimizing the routing of vehicle resulting in reducing in travel delays further.

➢ Connected Roadways

Current challenges being addressed by Connected Roadways

Challenge	Supporting Data
Environment	• Each year, Transit System will reduce CO_2 emission s by 16.2 million metric tons by reducing private vehicle miles- American Public Transportation Association • Connected Vehicle Environmental Application will give all travels the real time information to make “green transportation” choice.

- **Connected Roadways- IoT connected Roadways**
- **Intersection Movement Assist(IMA) This App warns the Driver when it is not Safe to enter an Intersection due to high Possibility of collision.**



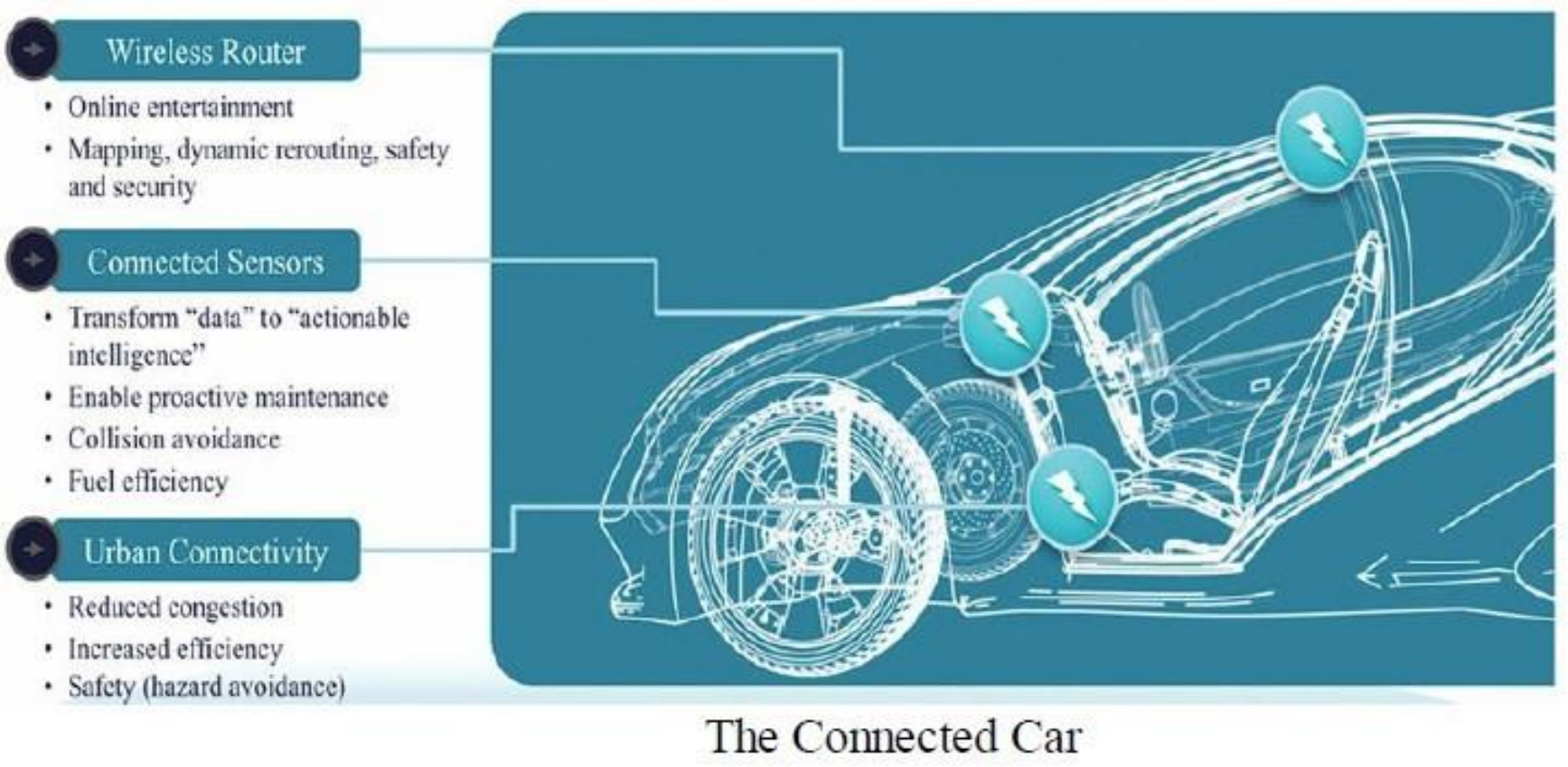
Application of Intersection Movement Assist

➢ **The Connected Car**

With automated vehicle tracking, a vehicle ‘s location is used for notification of arrival times, theft prevention or high way assistance.

-Cargo Management

-fully connected car will generate >25GB data/hour



The Connected Car

- **The Connected Roadways – creates another area where third party uses the data generated by car.**
- **Example- tyre company can collect data related to use and durability of their product in arrange of environments in real time.**
- **GPS/Map – to enable dynamic rerouting to avoid traffic, accidents and other hazards.**
- **Internet based Entertainment can be personalized and customized to optimize road trip.**
- **Data will be used for advertisement**
- **IoT Data Broker –provides Business opportunity**
- **Fiber optic sensing able to record how many cars are passing , their speed and type .**

IoT Impact Connected Facotry

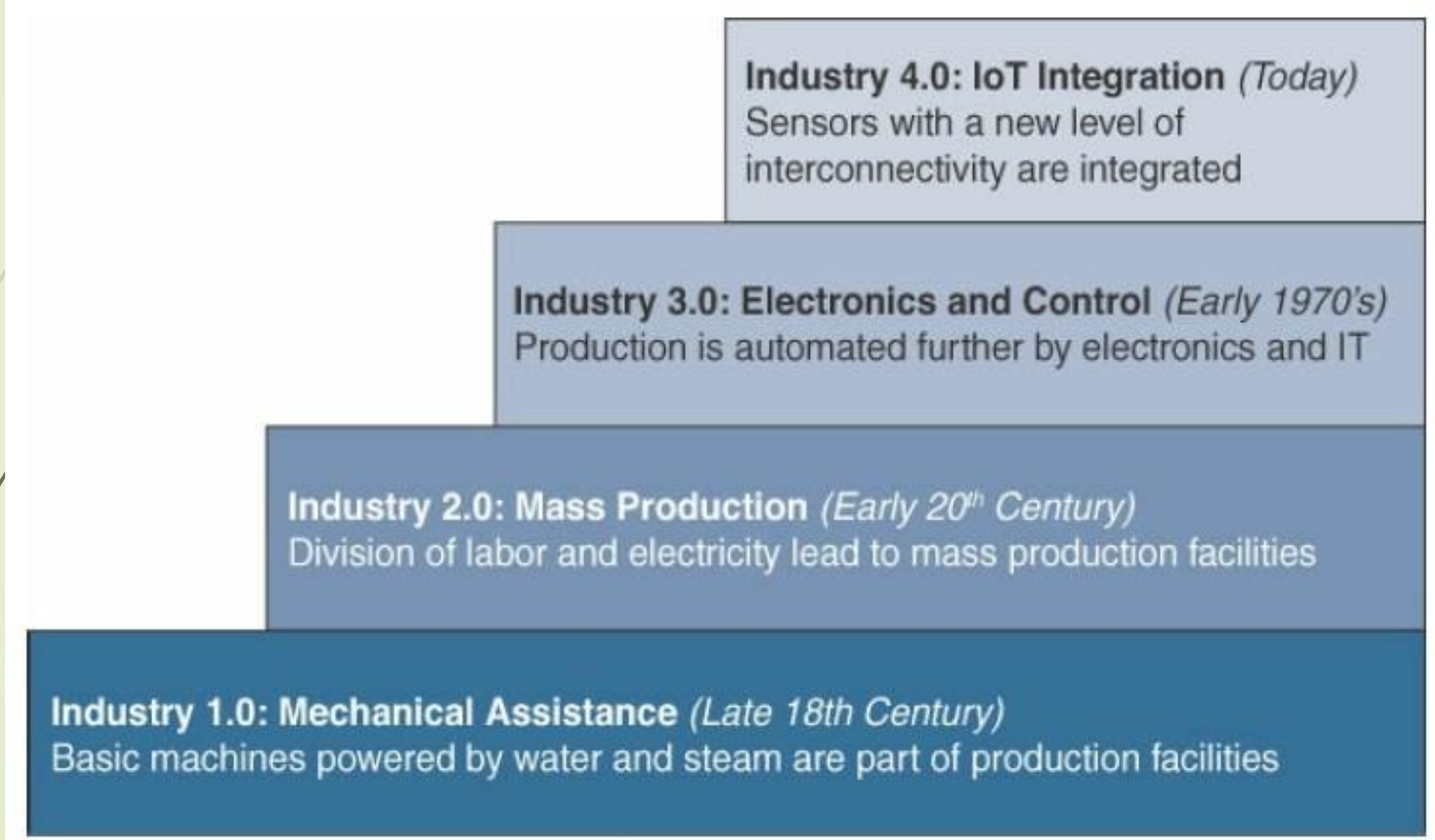
The Connected Factory

The main challenges facing manufacturing in a factory environment today:

- **Accelerating new products and service introduction to meet customer and market opportunities.**
- **Increasing plant productions, quality and uptime while decreasing cost.**
- **Mitigating unplanned downtime**
- **Securing factories from cyber threads**
- **Decreasing high cabling and re-cabling costs**
- **Improving worker productivity and safety.**
- **Example- In the ore melting process, control room will be far off from the unit resulting in multiple trips and controlling becomes difficult.**
- **With IoT and Connected factory – "machine to people " connections are implemented to bring sensor data directly to operator on the floor via mobile devices. Time is no longer wasted in moving.**
- **Real time location system (RTLS) attached Wi-fi RFID tag to locate the real time location and status of product.**

IoT Impact Connected Facotry

- **The Four Industrial Revolution**



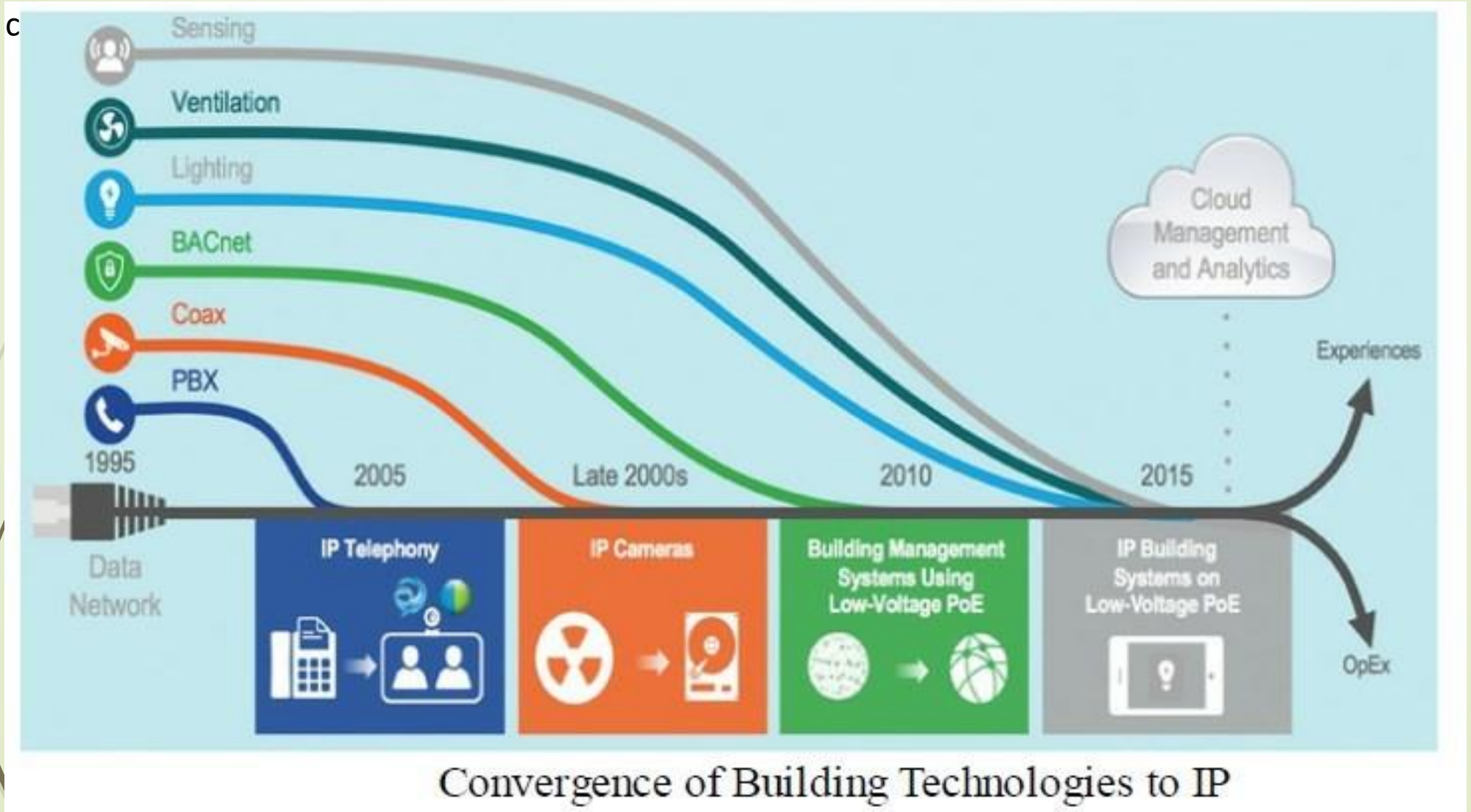
The Four Industrial Revolutions

IoT Impact on Smart Connected Buildings

- **The Smart Connected Buildings**
- **The function of a building is to provide a work environment that keeps the worker comfortable, efficient and safe.**
- **Physical Security alarm –fire alarm and suppression system to keep worker safe.**
- **Sensors to detect occupancy in the building.**
- **Lights are off automatically when no one is there.**
- **Sensors are used to control the heating, ventilation and air-conditioning (HVAC) system**
- **Temperature sensors are spread throughout the building and are used to influence the building management system(BMS) control of air flow into the room.**
- **Building Automation System(BAS) provides a single management system for HVAC, lighting, alarm and detection system.**
- **Defacto communication protocol for building automation is known as BACnet (Building Automation and Control Network)**

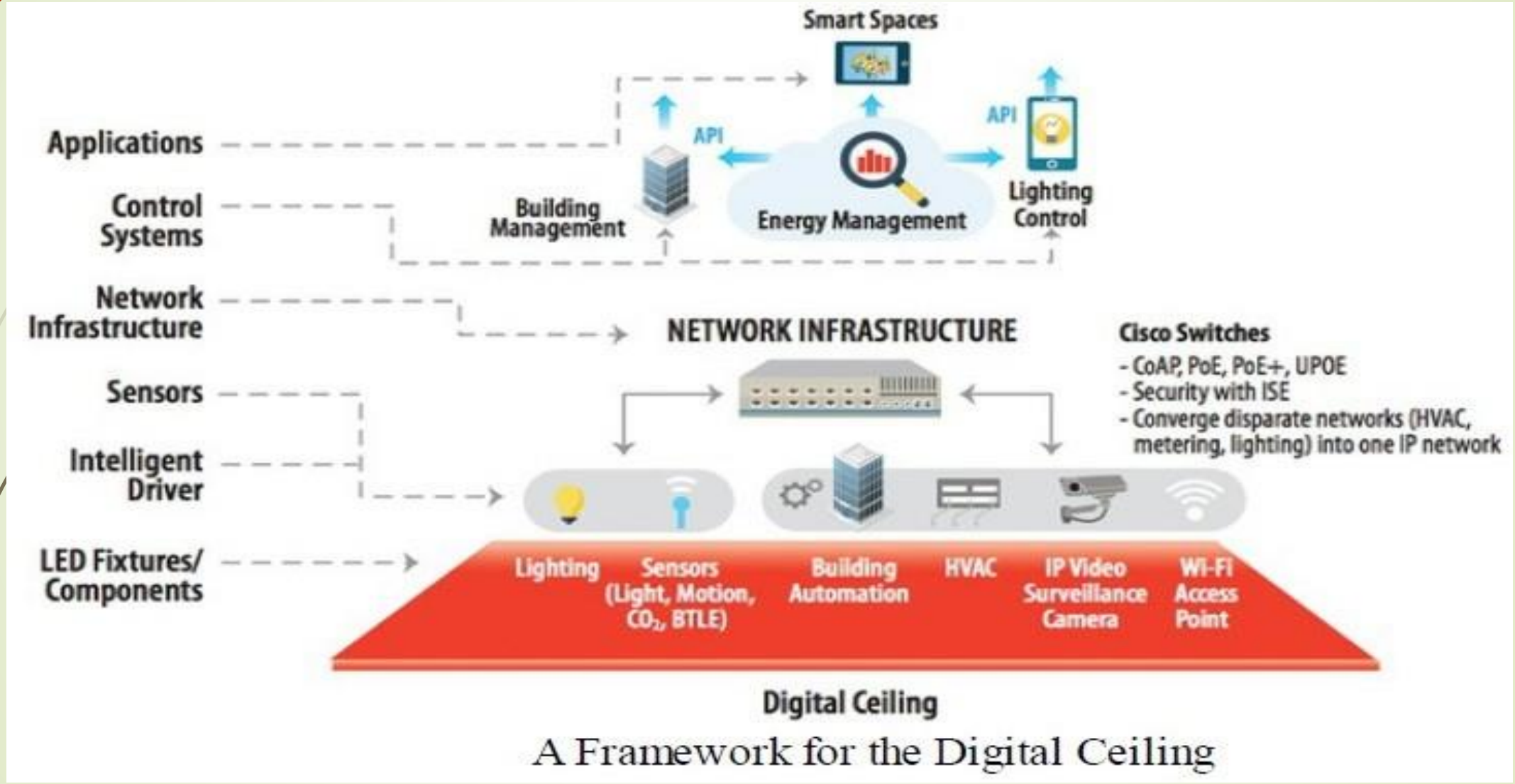
Smart Connected Buildings- Convergence of Building Technologies to IP

C

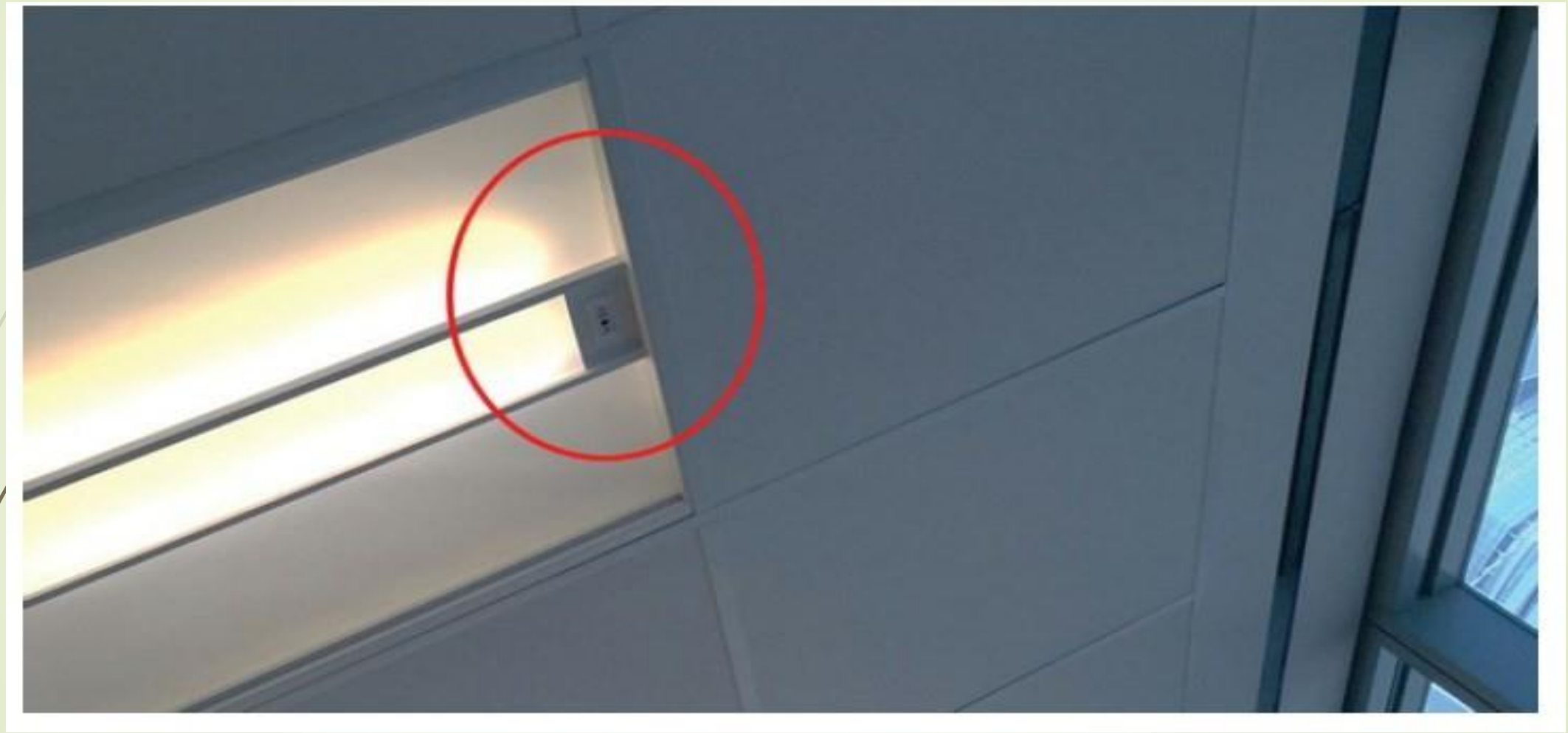


Convergence of Building Technologies to IP

Smart Connected Buildings- A Framework for the Digital Ceiling



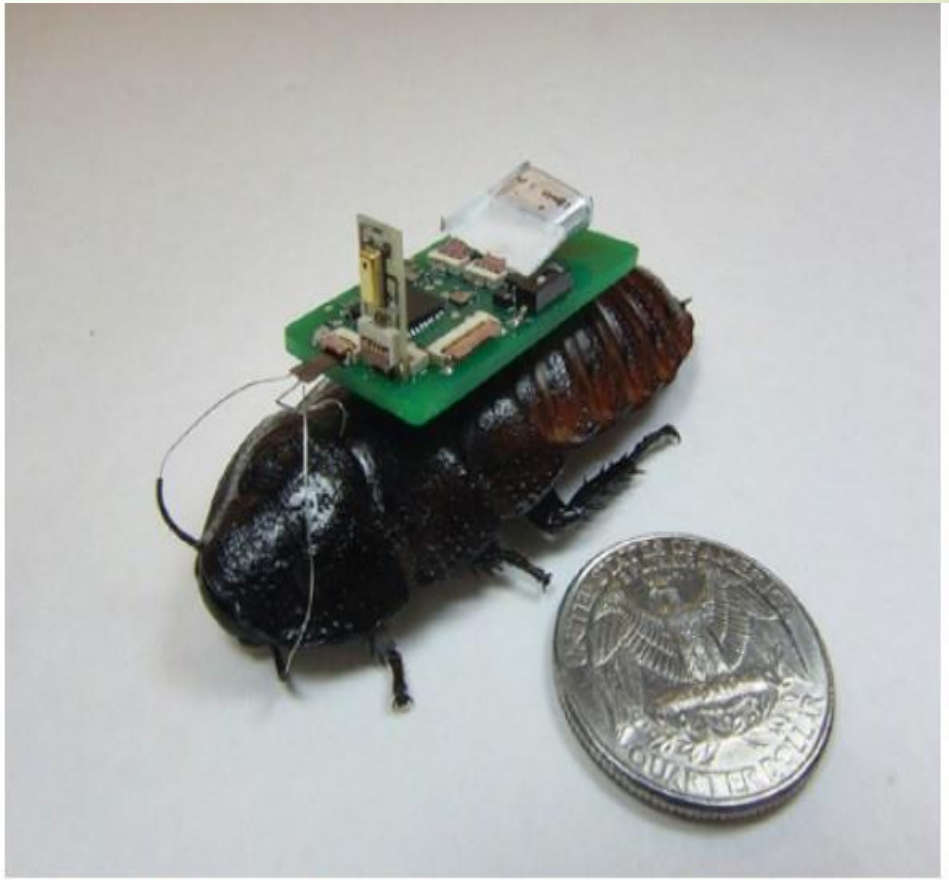
Smart Connected Buildings- An LED Ceiling with Occupancy Sensor



IoT Impact Smart Creatures

- **Smart Creatures-IoT Enabled Roach to find survivors**

- **IoT provides the ability to connect living things to the Internet.**
- **Sensors can be placed on animals and insects.**
- **Connected cow-sensors on cow's ear.**
- **IoT enables roaches to save life in disaster situations.**



IoT-Enabled Roach Can Assist in Finding Survivors After a Disaster (Photo courtesy of Alper Bozkurt, NC State University)

Convergence of IT and IoT

- **Comparing Operational Technology(OT) and Information Technology(IT)**

Criterion	Industrial OT Network	Enterprise IT Network
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

Convergence of IT and IoT

- **Comparing Operational Technology(OT) and Information Technology(IT)**

Criterion	Industrial OT Network	Enterprise IT Network
Implication of failure	OT network disruption directly impacts business	Can be business impacting, depending on industry, but workarounds may be possible
Network upgrades (software or hardware)	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

IoT challenges

Challenge	Description
Scale	• IT networks scale is larger, The scale of OT is several orders of magnitude larger. • Example: Electrical Company has deployed tons of millions meters in service area where they employed tens of thousands of employees for acting as IP Node using IP v6. • i.e the scale of network, the utility is managing has increased by more than 1000 fold.
Security	• With more “things” connected with other “things” and people security is an increasingly complex issue for IoT. Threat surface is greatly expanded and if device gets hacked, its connectivity is a major concern. • A Compromised device can serve as a launching point to attack other devices and systems.
Privacy	• A sensor become more prolific in every day lives, the data what they gather will be specific to individuals and their activities. • Example: Health information , Shopping patterns, transactions at retail establishments. • For Businesses, the data has monetary value. • Organization discusses about who owns the data and how individuals can control whether it is shared and with whom.

IoT challenges

Challenge	Description
Big Data and Data Analytics	• IoT and large number of sensors are going to trigger deluge of data that must be handled. • This data will provide critical information and insights if it can be processed in an efficient manner. • Challenge is evaluating massive amounts of data arriving from different sources in various forms and doing so in a timely manner.
Interoperability	• As with nascent technology, various protocols and architectures are jockeying for market share and standardizations within IoT. • Some of these protocols and architectures are based on proprietary elements and others are open. • Recently IoT Standards are helping minimize this problem, but there are often various protocols and implementations available for IoT networks.

Drivers Behind New Network Architecture

- The key difference between IT and IoT is the Data.
- IT systems are mostly concerned with reliable and continuous support of business application such as email, web, database, CRM systems and so on.
- IoT is all about the data generated by sensors and how that data is used.
- The essence of IoT architectures involve how data is transported, collected, analyzed and acted upon.

➢ IoT Architectural Drivers.

Challenges	Description	IoT Architectural Changes required
Scale	The massive scale of IoT endpoints (sensors) is far beyond that of typical IT networks.	• The IPv4 address space has reached exhaustion and is unable to meet IoT's scalability requirements. • Scale can be met only by IPv6. • IT networks continue to use IPv4 through features like Network Address Translation.
Security	IoT devices, especially those on wireless sensor networks(WSNs) are often physically exposed to the world.	• Security is required at every level of the IoT network. • Every IoT endpoint node on the network must be part of the overall security strategy and must support device level authentication and link encryption. • It must also be easy to deploy with some type of a zero – touch deployment model.

Challenges	Description	IoT Architectural Changes required
Devices and networks constrained by power, CPU memory and link speed	Due to the massive scale and longer distances, the networks are often constrained, lossy and capable of supporting only minimal data rates (10s of bps to 100s of kbps)	• New-last mile wireless technologies are needed to support constrained IoT devices over long distances. • The network is also constrained, i.e modifications need to be made to the traditional network-layer transport mechanisms.
The massive volume of data generated	The sensors generate the massive amount of data on daily basis, causing network bottlenecks and slow analytics in the cloud.	• Data analytics capabilities need to be distributed throughout the IoT network, from the edge to the cloud. • In traditional IT networks, analytics and applications typically run only in the cloud.

Challenges	Description	IoT Architectural Changes required
Support for legacy systems	An IoT network often comprises a collection of modern, IP capable end points as well as legacy , non-IP devices that rely on serial or proprietary protocols.	• Digital transformation is a long process that may take many years , and IoT networks need to support translation and / or tunneling mechanisms to support legacy protocols over standards-based protocols, such as Ethernet and IP.
The need for data to be analyzed in real time	Where as Traditional IT networks perform scheduled batch processing of data, IoT data needs to be analyzed and responded to in real – time.	• Analytics software need to be positioned closer to the edge and should support real-time streaming analytics. • Traditional IT analytics software (such as relational database or even Hadoop), are better suited to batch-level analytics hat occur after the fact.

Drivers Behind New Network Architecture

The requirements driving specific architectural changes for IoT.

➢ Scale

- **The scale of a typical IT network is on the order of several thousand devices typically printers, mobile wireless devices, laptops, servers and so on.**
- **The traditional 3 layer campus networking model supports access, distribution and core.**
- **IoT introduces a model where a average-sized utility, factory, transportation system or city could easily support a network of million of routable IP endpoints.**
- **Based on scale requirements of this order, IPv6 is the natural foundation for the IoT network layer.**

The requirements driving specific architectural changes for IoT.

➢ Security

- It world war 3, it would be for cyberspace. Targeted malicious attacks using vulnerabilities in networked machines such as out break of of the stuxnet worm, which specifically affected Siemens Programming Logic Controller (PLC) systems.
- Protecting Corporate Data from intrusion and theft is the main function of IT department.
- IT departments protect servers, applications and cyber crown jewels of the corporation.
- In IT, first line of defense is perimeter firewall.
- Placing IP endpoints outside the firewall is critical and visible to anyone.
- IoT endpoints are located in WSN that use unlicensed spectrum and are visible to world through spectrum analyzer and physically accessible and widely distributed in the field.

The requirements driving specific architectural changes for IoT.

➢ Security

- For optimum security , IoT systems must:
  - Be able to identify and authenticate all entities involved in the IoT service(i.e Gateways, endpoint devices, home networks, roaming networks, service platforms)
  - Ensure that all user data shared between the endpoint device and back-end applications is encrypted.
  - Comply with local data protection legislation so that all data is protected and stored correctly.
  - Utilize an IoT connectivity management platform and establish rules-based security policies so immediate action can be taken if anomalous behavior is detected from connected devices.
  - Take a holistic , network- level approach to security,

The requirements driving specific architectural changes for IoT.

➢ Constraint devices and Networks

- Most IoT devices are designed for a single job, they are small and inexpensive.
- This results in that they have limited power , CPU and memory.
- They transmit only when there is something important.
- Large amount of this small devices, large and uncontrolled environents where they are deployed, the network that provide tends to be very lossy and support very low data rates where as in IT networks provides multi-giga bit connections speed and endpoints with powerful CPUs.
- For faster network, VLAN may be considered but If too many devices are in VLAN, it affects performance.
- So, IoT needs new bread of connectivity technologies that meet boththe scale and constraint limitations.

The requirements driving specific architectural changes for IoT.

Data

- IoT devices generate a mountain of data.
- In IoT, data is like Gold, they enable business to deliver new IoT services that enhance the customer experience, reduce cost and deliver new revenue opportunities.
- IoT generated data is unstructured but insights it provides through analytics will provide new business models.
- Example: A smart city with few 100 thousands smart street lights , all connected through an IoT network. Lights ON/OFF, replacement, operational expense.

COMPARING IoT Architecture

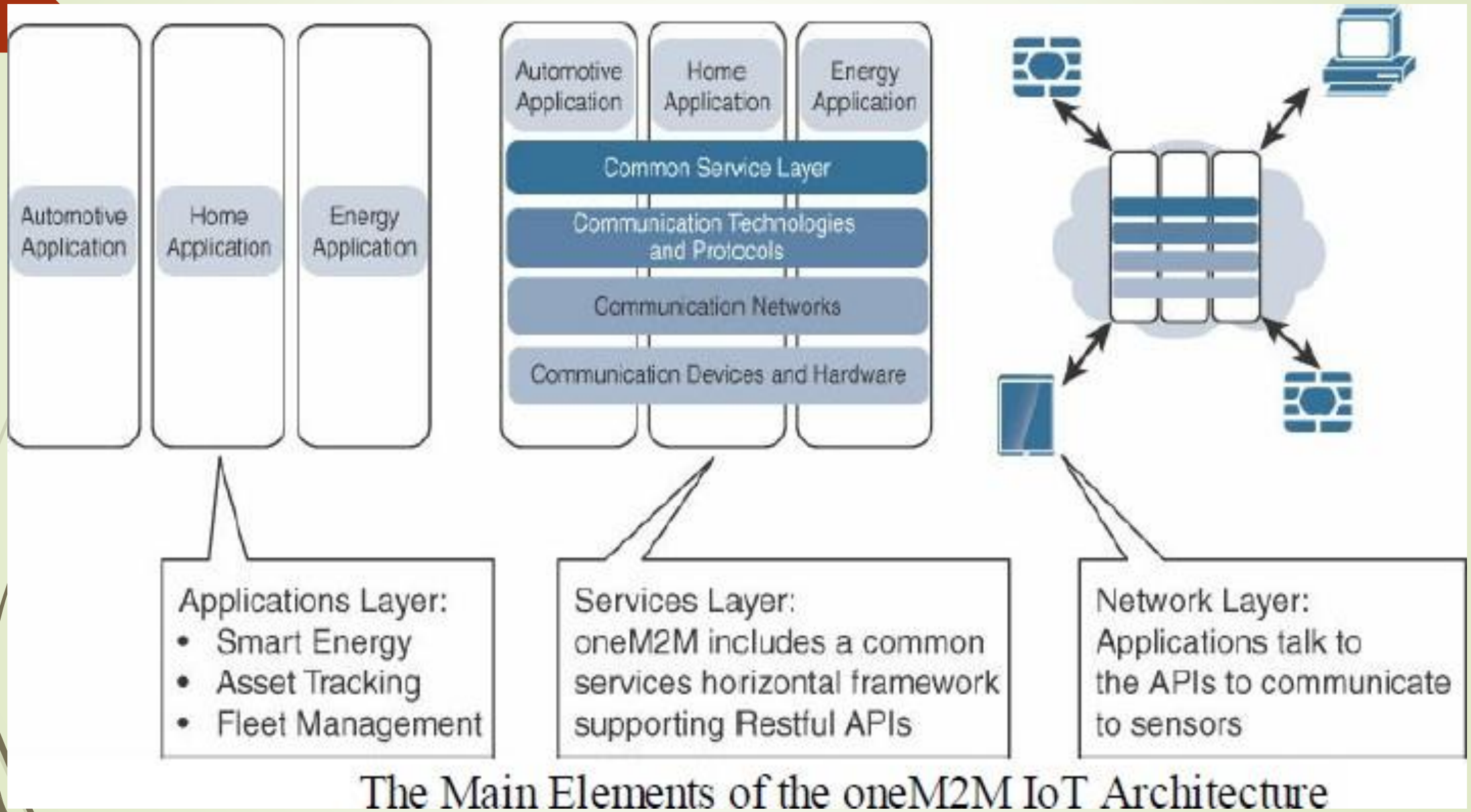
- **The foundational concept in all these architecture is supporting data, process and the functions that end point devices perform.**
- **Two of the best known architectures are**
- **1. One M2M IOT Standardized Architecture**
- **2. IOT World Forum (IOTWF)**

The oneM2M Standardized Architecture

- To standardize the rapidly growing field of machine-to-machine(M2M) communications, the European Telecommunications standards Institute (ETSI) created the M2M Technical Committee in 2008.

- The goal of the committee was to create a common architecture that would help accelerate the adoption of M2M application and devices and extended to IoT.
- Similar, in 2012 ETSI and 13 other funding members launched oneM2M as a global initiative to promote efficient M2M communication system and IoT.
- The goal of one M2M is to create a common services layer which can be readily embedded in the field devices to allow communication with application servers.
- OneM2M's framework focuses on IoT services, applications and platforms. These include smart metering applications, smart grid, smart city, automation, e-health and connected vehicles.
- One of the greatest challenges in designing an IoT architecture is dealing with the heterogeneity of devices, software and access methods.

The oneM2M Standardized Architecture



The Main Elements of the oneM2M IoT Architecture

The oneM2M Standardized Architecture

- **The OneM2M IoT standardized Architecture divides IOT functions into 3 major domains:**
  - **1. Application Layer**
  - **Service Layer**
  - **Network Layer**
- **Application Layer**
  - **OneM2M architecture gives more attention to connectivity between devices and their applications.**
  - **This domain includes the application-layer protocols and attempts to standardize northbound API definitions for interactions with Business intelligent (BI) systems.**
  - **Application tend to be industry specific and have their own sets of data models, thus they are shown as vertical entities.**

The oneM2M Standardized Architecture

- **Services Layer**

  - **Shown as horizontal framework across the vertical industry applications.**
  - **Horizontalmodules include the physical network that the IoT application run on, the underlying management protocols and the hardware.**
  - **Example: Backhaul communications via cellular, MPLS networks, VPNs and so on.**
  - **Riding on Top is the common service layer.**
  - **This conceptual layer adds APIs and middle ware supporting third party services and applications.**

The oneM2M Standardized Architecture

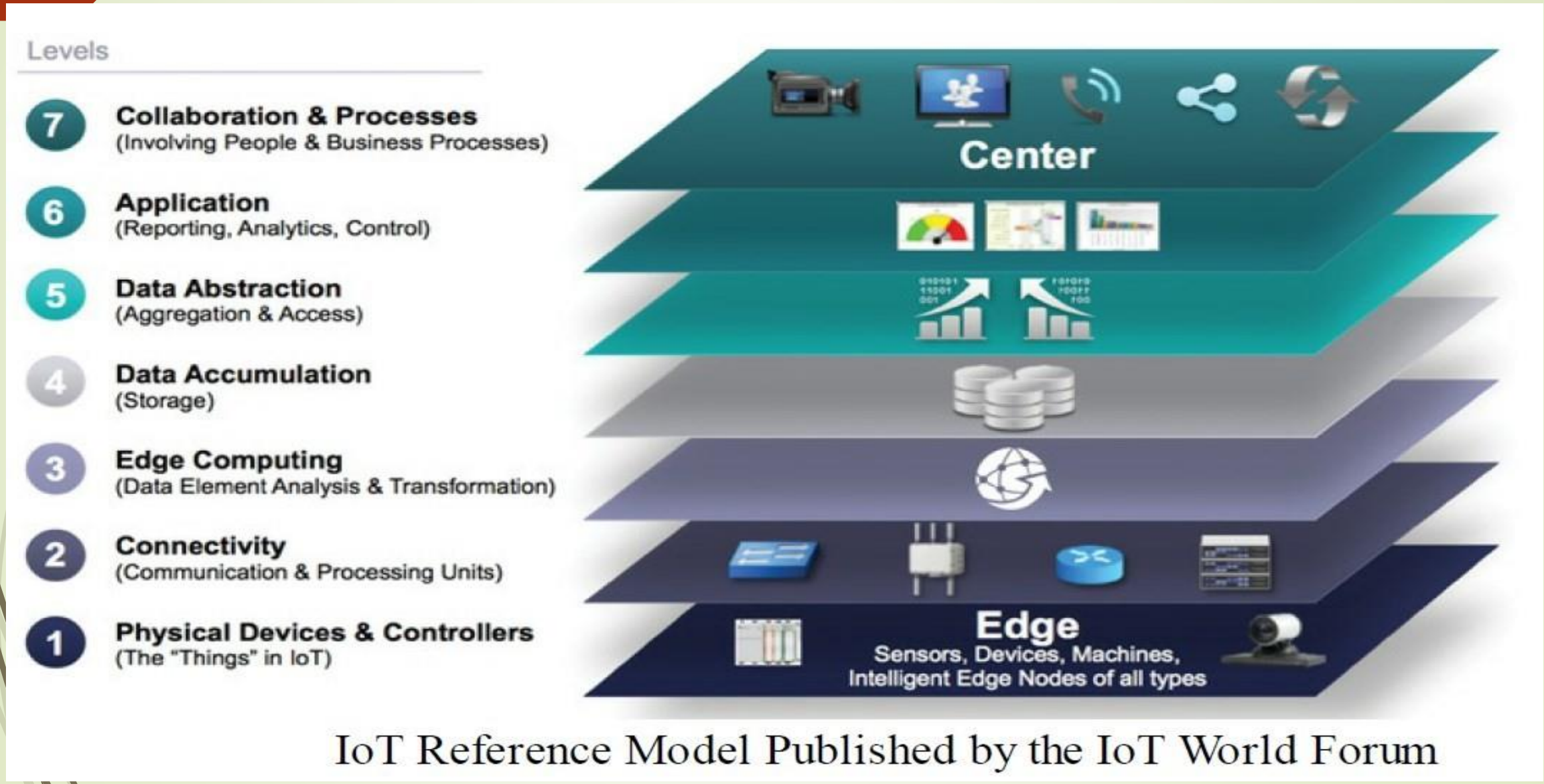
➢ **Network Layer**

- **Applications talk to API's to communicate to sensors.**
- **This is the communication domain for the IoT devices and endpoints.**
- **It includes the devices themselves and the communication network that links them.**
- **Includes Wireless mesh technologies such as IEEE 802.15.4 and wireless point-to-multipoint systems such as IEEE 801.1.11ah.**
- **It also includes wired device connections such as IEEE 1901 power line communications.**
- **In many cases, the smart (and sometimes not-so-smart) devices communicate with each other.**
- **In other cases, machine-to-machine communication is not necessary, and the devices simply communicate through a field area network (FAN) to use-case-specific apps in the IoT application domain.**
- **Therefore, the device domain also includes the gateway device, which provides communications up into the core network and acts as a demarcation point between the device and network domains.**

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.
- IoT World Forum Model offers a clean, simplified perspective on IoT and includes edge computing, data storage, and access. It provides a clean way of visualizing IoT from a technical perspective.
- Each of the seven layers is broken down into specific functions, and security encompasses the entire model.
- The IoT Reference Model defines a set of levels with control flowing from the center to the edge, which includes sensors, devices, machines and other types of intelligent end nodes.
- In general, data travels up the stack, originating from the edge, and goes to the center.
- Using this 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

The IoT World Forum (IoTWF) Standardized Architecture:



IoT Reference Model Published by the IoT World Forum

The IoT World Forum (IoTWF) Standardized Architecture:

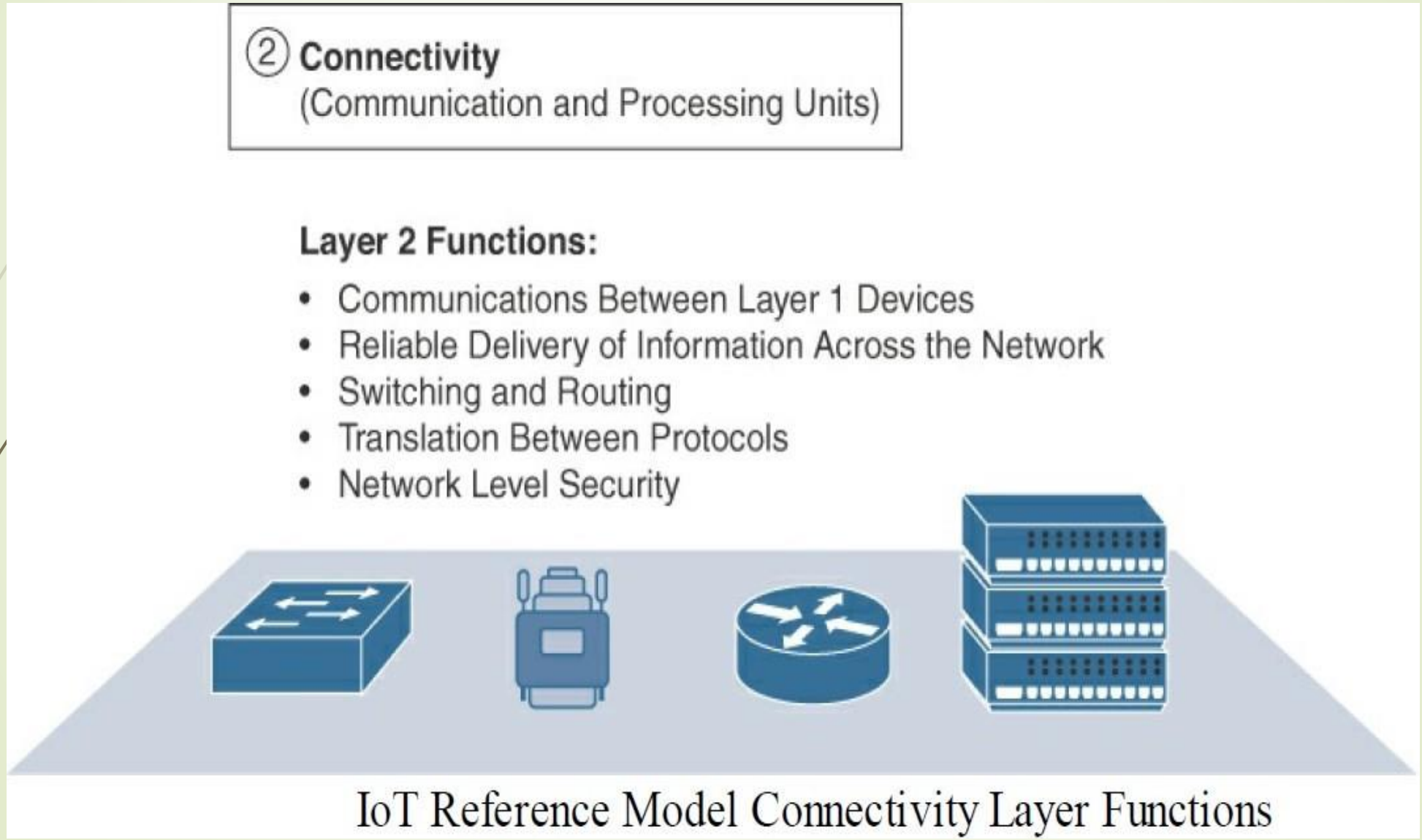
- **Layer 1: Physical Devices and Controllers Layer**
  - **The first layer of the IoT Reference Model is the physical devices and controllers layer.**
  - **This layer is home to the “things” in the Internet of Things, including the various endpoint devices and sensors that send and receive information.**
  - **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.**

The IoT World Forum (IoTWF) Standardized Architecture:

- **Layer 2: Connectivity Layer**
  - **In the second layer of the IoT Reference Model, the focus is on connectivity.**
  - **The most important function of this IoT layer is the reliable and timely transmission of data.**
  - **More specifically, 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).**
  - **The connectivity layer encompasses all networking elements of IoT and doesn't really distinguish between the last-mile network, gateway, and backhaul networks.**

The IoT World Forum (IoTWF) Standardized Architecture:

- **Layer 2: Connectivity Layer**

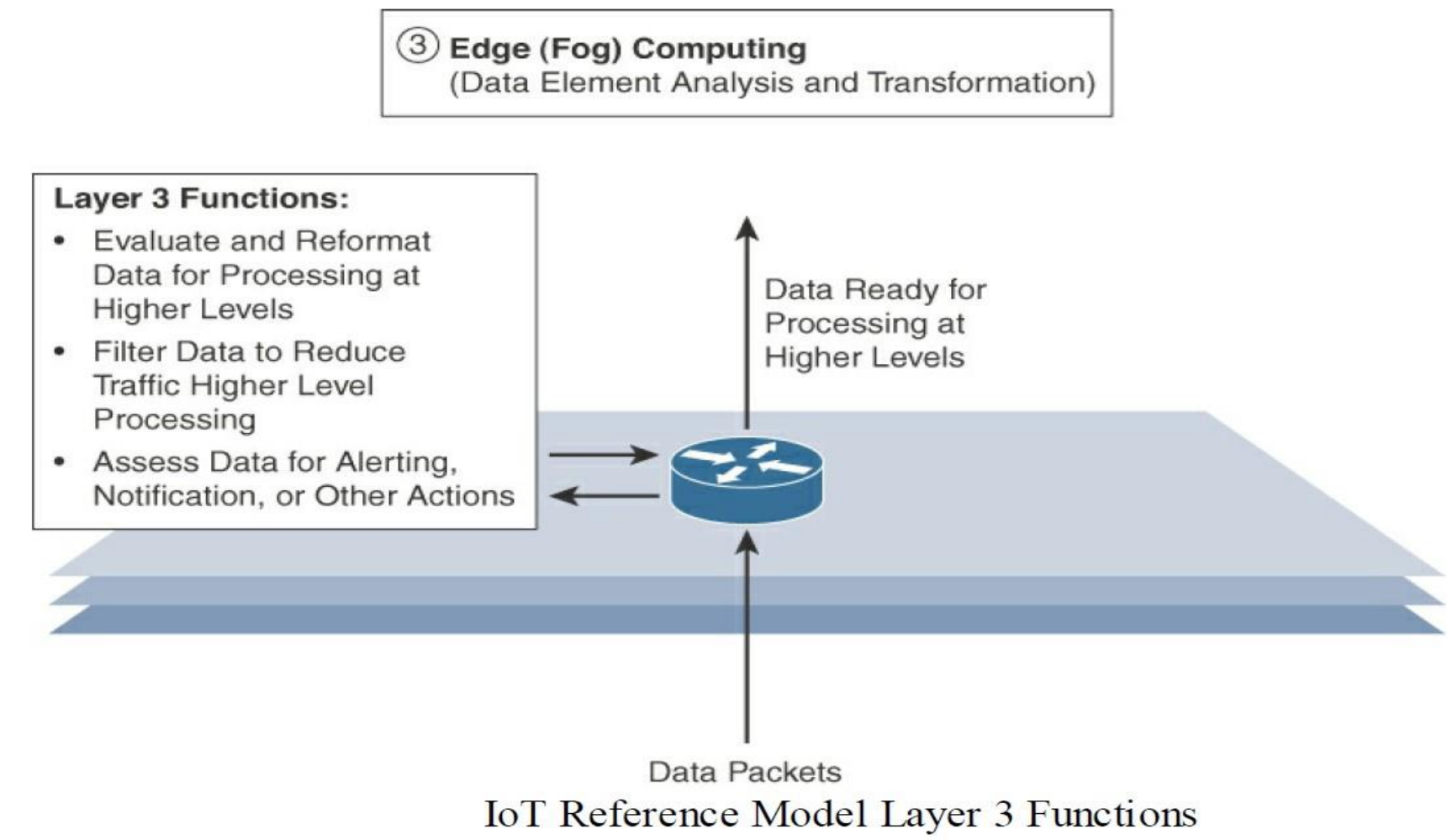


The IoT World Forum (IoTWF) Standardized Architecture:

- **Layer 3: Edge Computing Layer**
  - **Edge computing is the role of Layer 3.**
  - **Edge computing is often referred to as the “fog” layer .**
  - **At this layer, the emphasis is on data reduction and converting network data flows into information that is ready for storage and processing by higher layers.**
  - **One of the basic principles of this reference model is that information processing is initiated as early and as close to the edge of the network as possible.**
  - **Another important function that occurs at Layer 3 is the evaluation of data to see if it can be filtered or aggregated before being sent to a higher layer.**
  - **This also allows for data to be reformatted or decoded, making additional processing by other systems easier.**
  - **Thus, a critical function is assessing the data to see if predefined thresholds are crossed and any action or alerts need to be sent.**

The IoT World Forum (IoTWF) Standardized Architecture:

- **Layer 3: Edge Computing Layer**



IoT Reference Model Layer 3 Functions

The IoT World Forum (IoTWF) Standardized Architecture:

- **Layer 4-7: Upper Layers**

- **The upper layers deal with handling and processing the IoT data generated by the bottom layer. Layers 4–7 of the IoT Reference Model are summarized in the following Table.**

IoT Reference Model 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.

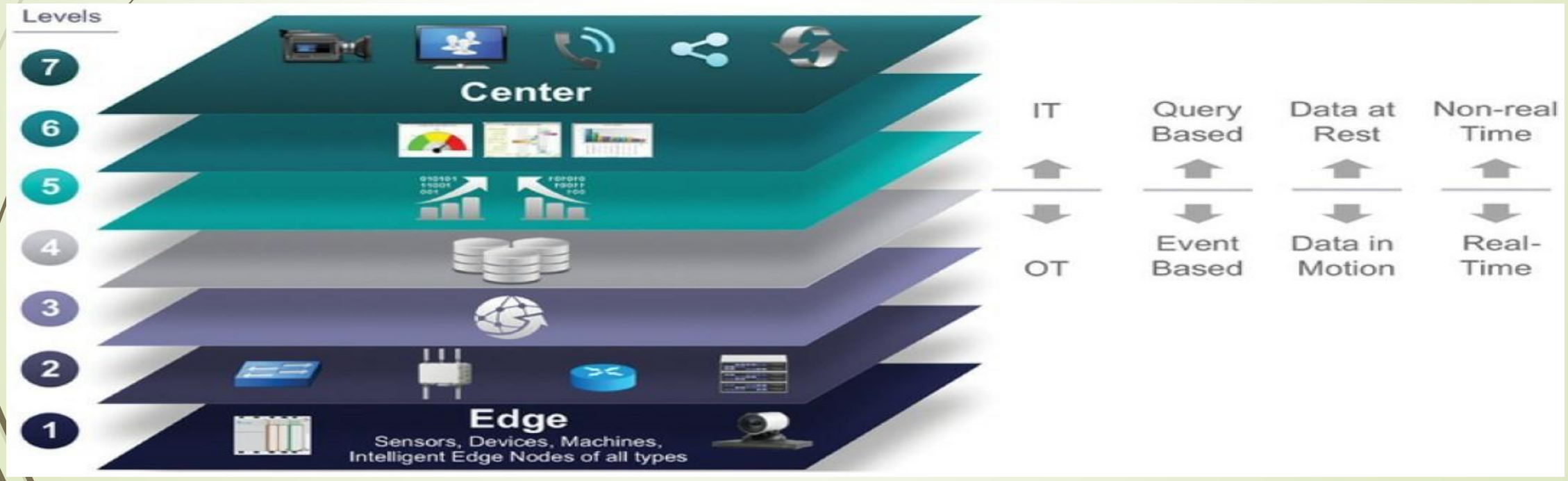
Summary of Layers 4–7 of the IoTWF Reference Model

The IoT World Forum (IoTWF) Standardized Architecture:

- **IT and OT Responsibilities in the IoT Reference Model**

- **An interesting aspect of visualizing an IoT architecture this way is that we can start to organize responsibilities along IT and OT lines.**
- **Following Figure illustrates a natural demarcation point between IT and OT in the IoT Reference Model framework.**

IOT Reference Model Separation of IT[7]a[5] nd OT



The IoT World Forum (IoTWF) Standardized Architecture:

IT and OT Responsibilities in the IoT Reference Model

- As demonstrated in Figure, IoT systems have to cross several boundaries beyond just the functional layers.
- The bottom of the stack is generally in the domain of OT.
- For an industry like oil and gas, this includes sensors and devices connected to pipelines, oil rigs, refinery machinery, and so on.
- The top of the stack is in the IT area and includes things like the servers, databases, and applications, all of which run on a part of the network controlled by IT.
- In the past, OT and IT have generally been very independent and had little need to even talk to each other. IoT is changing that paradigm.
- At the bottom, in the OT layers, the devices generate real-time data at their own rate—sometimes vast amounts on a daily basis.

The IoT World Forum (IoTWF) Standardized Architecture:

IT and OT Responsibilities in the IoT Reference Model

- Not only does this result in a huge amount of data transiting the IoT network, but the sheer volume of data suggests that applications at the top layer will be able to ingest that much data at the rate required.
- To meet this requirement, data has to be buffered or stored at certain points within the IoT stack.
- Layering data management in this way throughout the stack helps the top four layers handle data at their own speed.
- As a result, the real-time “data in motion” close to the edge has to be organized and stored so that it becomes “data at rest” for the applications in the IT tiers.
- The IT and OT organizations need to work together for overall data management.

Additional IoT Reference Models:

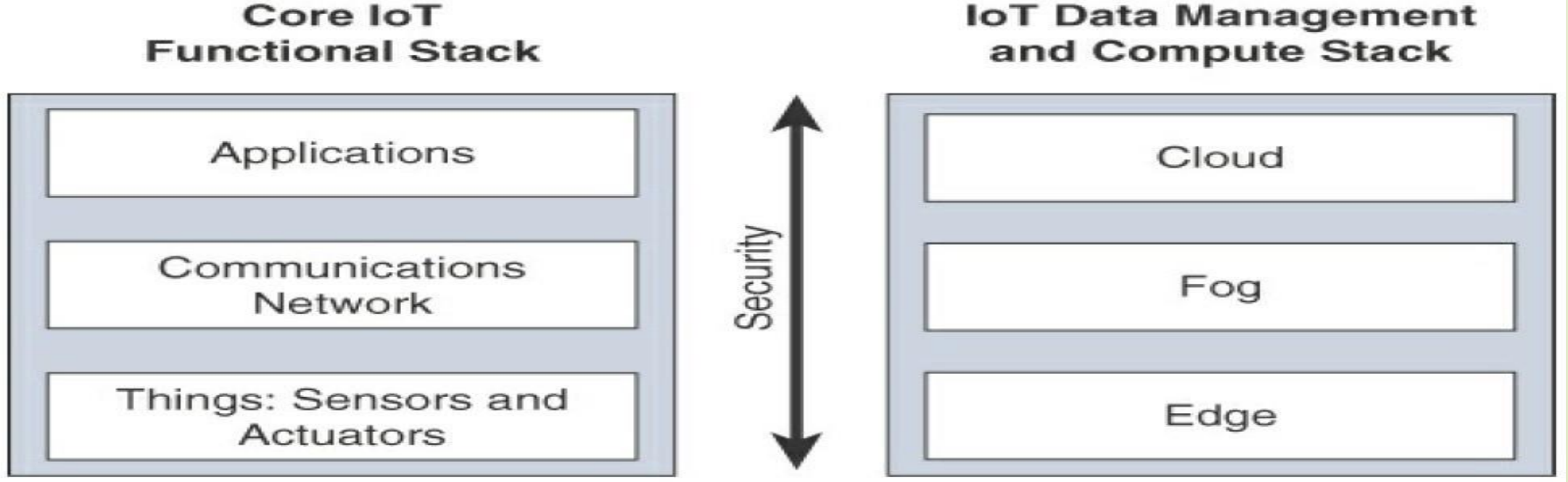
IoT Reference Model	Description
Purdue Model for Control Hierarchy	The Purdue Model for Control Hierarchy (see www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG/ch2_EttF.pdf) is a common and well-understood model that segments devices and equipment into hierarchical levels and functions. It is used as the basis for ISA-95 for control hierarchy, and in turn for the IEC-62443 (formerly ISA-99) cyber security standard. It has been used as a base for many IoT-related models and standards across industry.

IoT Reference Model	Description
Industrial Internet Reference Architecture (IIRA) by Industrial Internet Consortium (IIC)	The IIRA is a standards-based open architecture for Industrial Internet Systems (IISs). To maximize its value, the IIRA has broad industry applicability to drive interoperability, to map applicable technologies, and to guide technology and standard development. The description and representation of the architecture are generic and at a high level of abstraction to support the requisite broad industry applicability. The IIRA distills and abstracts common characteristics, features and patterns from use cases well understood at this time, predominantly those that have been defined in the IIC.

IoT Reference Model	Description
Internet of Things–Architecture (IoT-A)	IoT-A created an IoT architectural reference model and defined an initial set of key building blocks that are foundational in fostering the emerging Internet of Things. Using an experimental paradigm, IoT-A combined top-down reasoning about architectural principles and design guidelines with simulation and prototyping in exploring the technical consequences of architectural design choices.

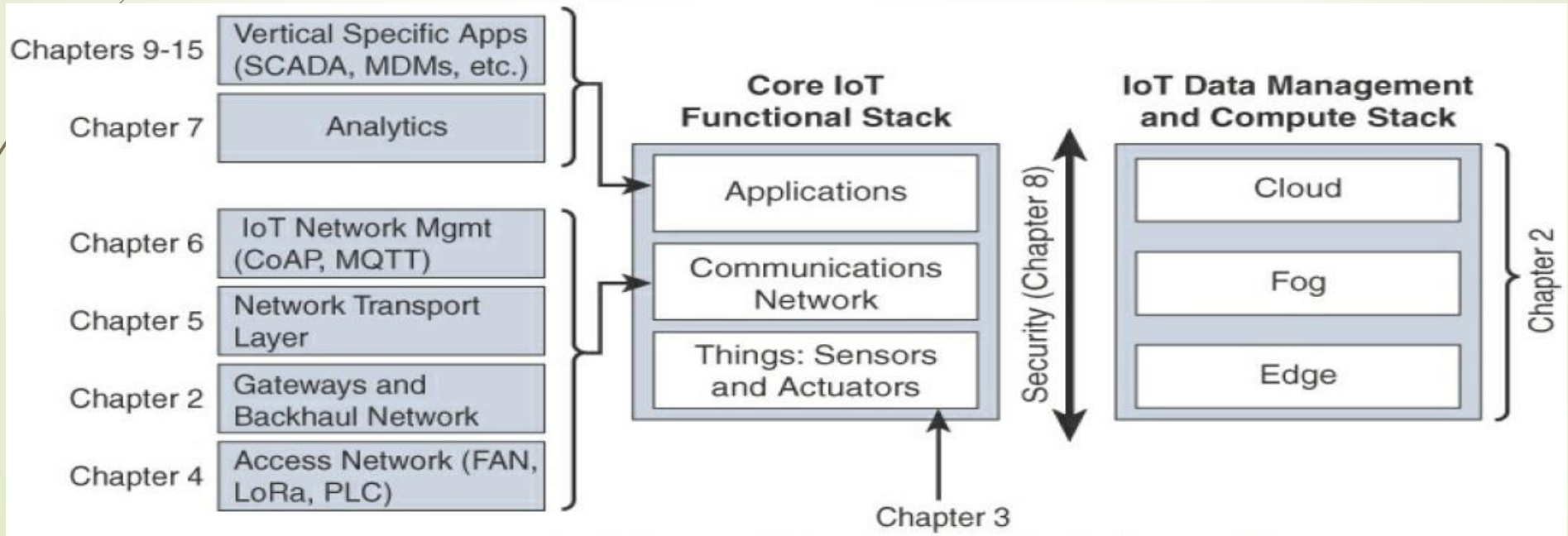
A Simplified IoT Architecture:

- All IOT models include Things, Communications Network and Applications. The framework separates the core IoT and data management into parallel and aligned stacks, allowing us to carefully examine the functions of both the network and the applications at each stage of a complex IoT system.
- This separation gives us better visibility into the functions of each layer.
- The network communications layer of the IoT stack itself involves a significant amount of detail



A Simplified IoT Architecture:

- In the model presented, data management is aligned with each of the three layers of the Core IoT Functional Stack.
- The three data management layers are the edge layer (data management within the sensors themselves), the fog layer (data management in the gateways and transit network), and the cloud layer (data management in the cloud or central data center).



Expanded View of the Simplified IoT Architecture

A Simplified IoT Architecture:

- The Core IoT Functional Stack can be expanded into sublayers containing greater detail and specific network functions.
- For example, the communications layer is broken down into four separate sublayers: the access network, gateways and backhaul, IP transport, and operations and management sublayers.
- The applications layer of IoT networks is quite different from the application layer of a typical enterprise network.
- IoT often involves a strong big data analytics component.
- IoT is not just about the control of IoT devices but, rather, the useful insights gained from the data generated by those devices.
- Thus, the applications layer typically has both analytics and industry-specific IoT control system components.

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.**
- **There are several components which have to work together for an IOT network to be operational.**

1. **“Things” layer**
2. **Communications network layer**
    1. **Access network sublayer**
    2. **Gateways and backhaul network sublayer**
    3. **Network transport sublayer**
    4. **IoT network management sublayer**
3. **Application and analytics layer**

The Core IoT Functional Stack

1. **“Things” layer:**

- **At this layer, the physical devices need to fit the constraints of the environment in which they are deployed while still 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:

- 2.1 Access network sublayer
- 2.2 Gateways and backhaul network sublayer
- 2.3 Network transport sublayer
- 2.4 IOT network management sublayer

The Core IoT Functional Stack

2.1 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.

The Core IoT Functional Stack

2.2 Gateways and backhaul network sublayer:

- A common communication system organizes multiple smart objects in a given area around a common gateway.
- The gateway communicates directly with the smart objects.
- The role of the gateway is to forward the collected information through a longer-range medium (called the backhaul) to a headend central station where the information is processed.
- This information exchange is a Layer 7 (application)function, which is the reason this object is called a gateway.
- On IP networks, this gateway also forwards packets from one IP network to another, and it therefore acts as a router.

The Core IoT Functional Stack

2.3 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.

2.4 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.**

The Core IoT Functional Stack

Layer -1 Things: Sensors and Actuators Layer

- Most IoT networks start from the object, or “thing” that needs to be connected.
- From an architectural standpoint, the variety of smart object types, shapes, and needs drive the variety of IoT protocols and architectures.
- There are many ways to classify smart objects.
- One architectural classification could be:
  1. Battery-powered or power-connected
  2. Mobile or static
  3. Low or high reporting frequency
  4. Simple or rich data
  5. Report range
  6. Object density per cell:

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.
  - Battery-powered things can be moved more easily than line-powered objects.
  - However, batteries limit the lifetime and amount of energy that the object is allowed to consume, thus driving transmission range and frequency.
- **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).
  - The frequency of the movement may also vary, from occasional to permanent.
  - The range of mobility (from a few inches to miles away) often drives the possible power source.

Layer -1 Things: Sensors and Actuators Layer

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.**
- **Higher frequencies drive higher energy consumption, which may create constraints on the possible power source (and therefore the object mobility) and the transmission range.**

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.**
- **Richer data typically drives higher power consumption.**
- **This classification is often combined with the previous to determine the object data throughput (low throughput to high throughput).**
- **A medium throughput object may send simple data at rather high frequency (in which case the flow structure looks continuous), or may send rich data at rather low frequency.**

Layer -1 Things: Sensors and Actuators Layer

Report range:

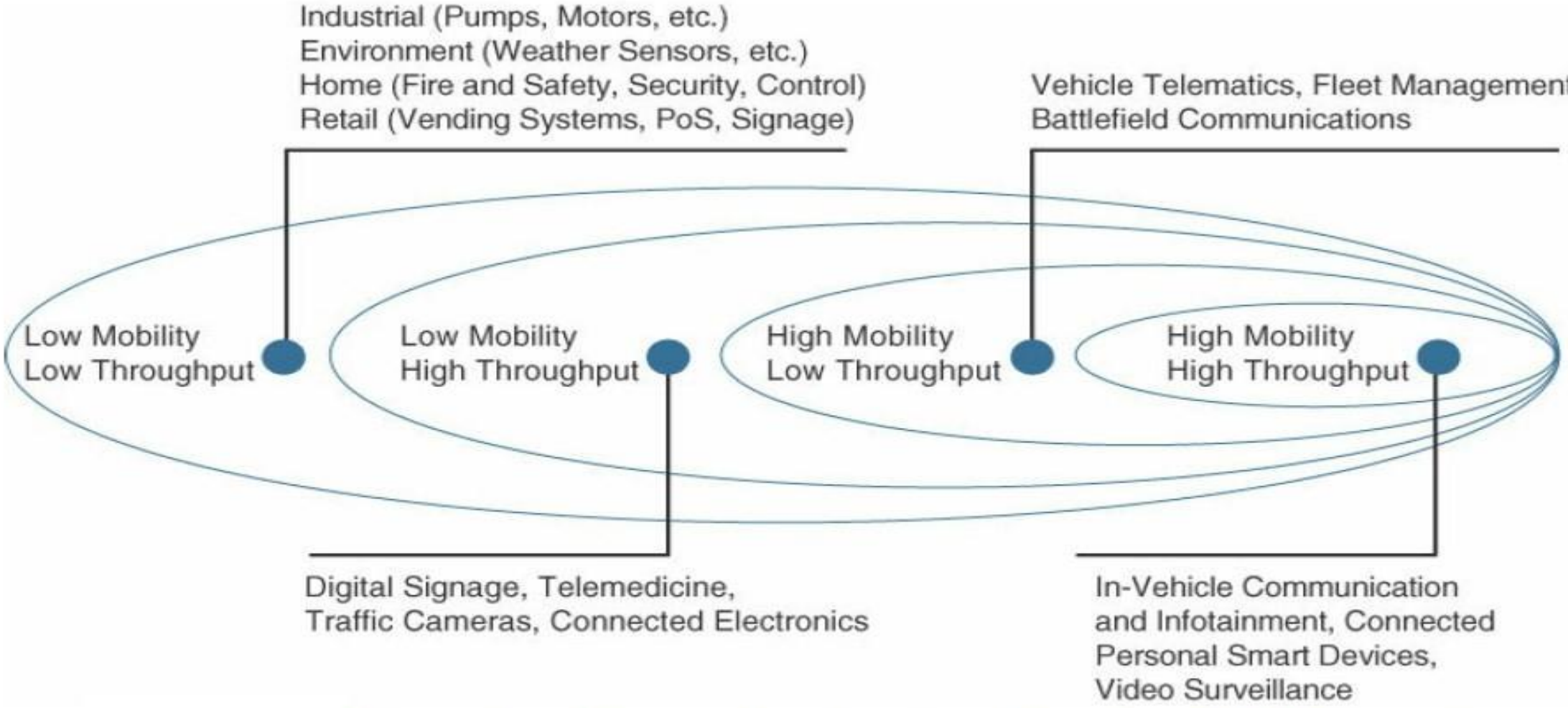
- **This classification is based on the distance at which the gateway is located.**
- **For example, for your fitness band to communicate with your phone, it needs to be located a few meters away at most.**
- **The assumption is that your phone needs to be at visual distance for you to consult the reported data on the phone screen.**
- **If the phone is far away, you typically do not use it, and reporting data from the band to the phone is not necessary.**
- **By contrast, a moisture sensor in the asphalt of a road may need to communicate with its reader several hundred meters or even kilometers away.**

Layer -1 Things: Sensors and Actuators Layer

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.**

Layer -1 Things: Sensors and Actuators Layer



Example of Sensor Applications Based on Mobility and Throughput

Layer -1 Things: Sensors and Actuators Layer

- The categories used to classify things can influence other parameters and can also influence one another.
- For example, 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.
- The criticality of data may also influence the form factor and, therefore, the architecture.
- For example, a 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).
- A first step in designing an IoT network is to examine the requirements in terms of mobility and data transmission (how much data, how often).

Layer -2 Communications network layer

- The categories used to classify things can influence other parameters and can also influence one another.
- 1. Access Network Sublayer
    1. PAN (Personal Area Network)
    2. HAN (Home Area Network)
    3. NAN (Neighborhood Area Network)
    4. FAN (Field Area Network)
    5. LAN (Local Area Network)
- 2. Gateways and backhaul network sublayer
- 3. Network transport sublayer
- 4. IoT network management sublayer

Layer -2 Communications network layer

- Once we have determined the influence of the smart object form factor over its transmission capabilities (transmission range, data volume and frequency, sensor density and mobility), we are ready to connect the object and communicate.
- Compute and network assets used in IoT can be very different from those in IT environments
- The difference in the physical form factors between devices used by IT and OT is obvious even to the most casual of observers.
- The operational differences must be understood in order to apply the correct handling to secure the target assets.
- Temperature variances are an easily understood metric.
- The cause for the variance is easily attributed to external weather forces and internal operating conditions.
- Remote external locations, such as those associated with mineral extraction or pipeline equipment can span from the heat of the Arabian Gulf to the cold of the Alaskan North Slope.

Layer -2 Communications network layer

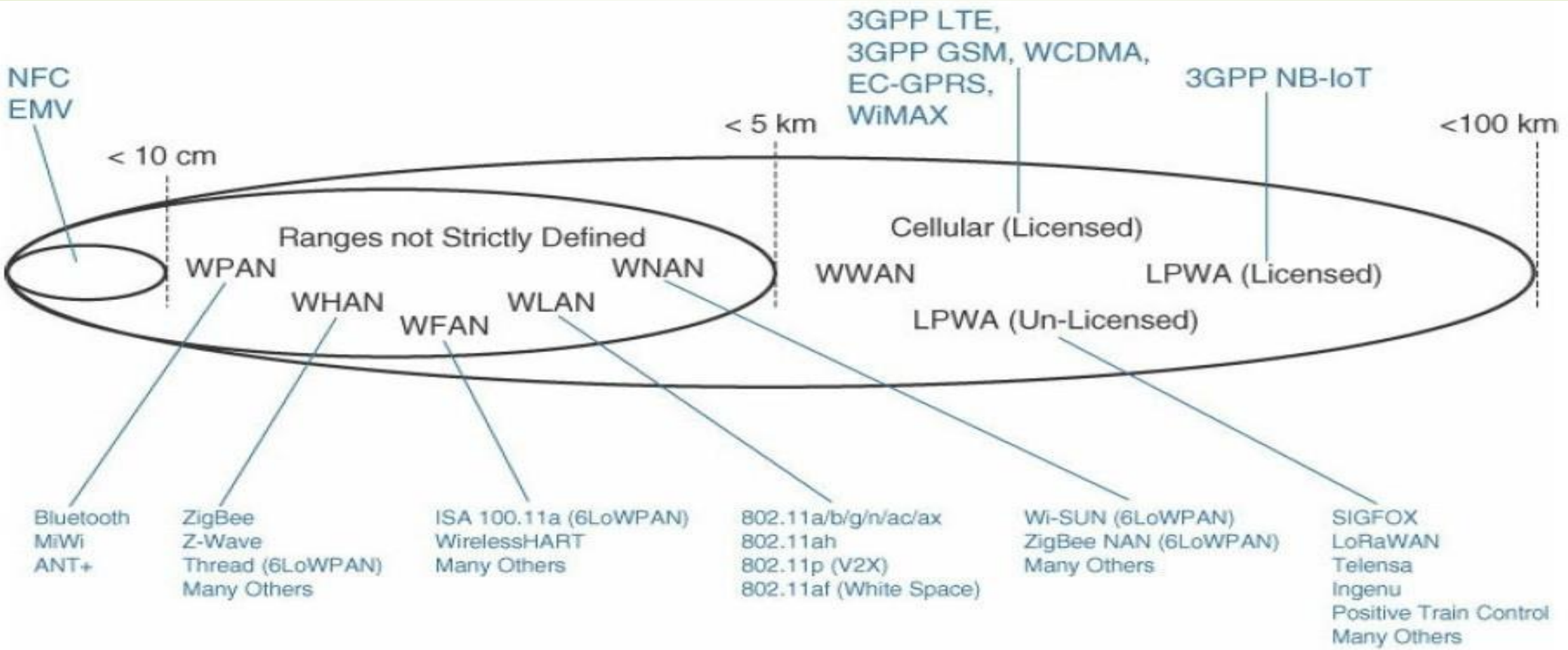
- Controls near the furnaces of a steel mill obviously require heat tolerance, and controls for cold food storage require the opposite.
- Humidity fluctuations can impact the long-term success of a system as well.
- Hazardous location design may also cause corrosive impact to the equipment.
- Caustic materials can impact connections over which power or communications travel. Furthermore, they can result in reduced thermal efficiency by potentially coating the heat transfer surfaces.
- In some scenarios, the concern is not how the environment can impact the equipment but how the equipment can impact the environment.
- For example, in a scenario in which volatile gases may be present, spark suppression is a critical design criterion.
- DC power sources are also common in many environments.

Layer -2 Communications network layer

Access Network Sublayer:

- Direct relationship exists between the IoT network technology and the type of connectivity topology this technology allows.
- Each technology was designed with a certain number of use cases in mind (what to connect, where to connect, how much data to transport at what interval and over what distance).
- These use cases determined the frequency band that was expected to be most suitable, the frame structure matching the expected data pattern (packet size and communication intervals), and the possible topologies that these use cases illustrate.
- IoT sometimes reuses existing access technologies whose characteristics match more or less closely the IoT use case requirements.
- Whereas some access technologies were developed specifically for IoT use cases, others were not.
- One key parameter determining the choice of access technology is the range between the smart object and the information collector.
- The following Figure lists some access technologies you may encounter in the IoT world and the expected transmission distances.

Access Network Sublayer:



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

Access Technologies and Distances

Layer -2 Communications network layer

Access Network Sublayer:

- **Cellular is indicated for transmissions beyond 5 km, but you could achieve a successful cellular transmission at shorter range (for example, 100 m).**
- **By contrast, ZigBee is expected to be efficient over a range of a few tens of meters, but would not expect a successful ZigBee transmission over a range of 10 km.**
- **Range estimates are grouped by category names that illustrate the environment or the vertical where data collection over that range is expected.**

Layer -2 Communications network layer

Access Network Sublayer:

- **Common groups are as follows:**

1. **PAN (personal area network):**
    1. **Scale of a few meters.**
    2. **This is the personal space around a person.**
    3. **common wireless technology for this scale is Bluetooth.**
2. **HAN (home area network)**
    1. **At scale of few tens of meters.**
    2. **At this scale, common wireless technologies for IoT include ZigBee and Bluetooth Low Energy (BLE).**
3. **NAN (neighborhood area network):**
    1. **Scale of a few hundreds of meters.**
    2. **The term NAN is often used to refer to a group of house units from which data is collected.**

Layer -2 Communications network layer

Access Network Sublayer:

- **Common groups are as follows:**

4. **FAN (field area network):**
    1. **Scale of several tens of meters to several hundred meters.**
    2. **FAN typically refers to an outdoor area larger than a single group of house units.**
    3. **The FAN is often seen as “open space” (and therefore not secured and not controlled).**
    4. **A FAN is sometimes viewed as a group of NANs, but some verticals see the FAN as a group of HANs or a group of smaller outdoor cells.**
    5. **FAN and NAN may sometimes be used interchangeably.**
    6. **In most cases, the vertical context is clear enough to determine the grouping hierarchy.**

Layer -2 Communications network layer

Access Network Sublayer:

- **Common groups are as follows:**

5. **LAN (local area network):**
    1. **Scale of up to 100 m.**
    2. **This term is very common in networking, and it is therefore also commonly used in the IoT space when standard networking technologies (such as Ethernet or IEEE 802.11) are used.**
    3. **Other networking classifications, such as MAN (metropolitan area network, with a range of up to a few kilometers) and WAN (wide area network, with a range of more than a few kilometers), are also commonly used.**

Layer -2 Communications network layer

Access Network Sublayer:

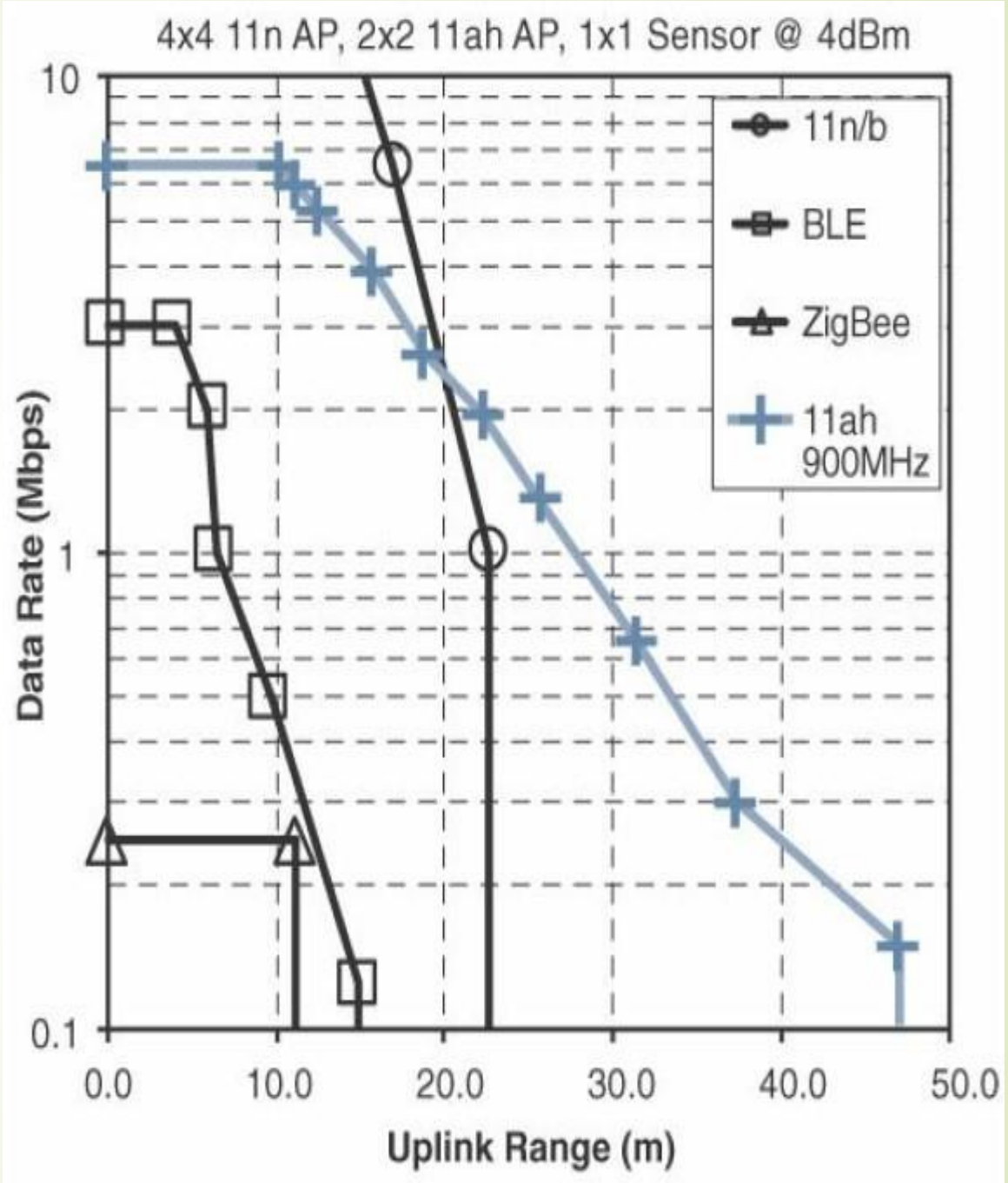
- **In the IoT network, a “W” can be added to specifically indicate wireless technologies used in that space.**
- **For example, HomePlug is a wired technology found in a HAN environment, but a HAN is often referred to as a WHAN (wireless home area network) when a wireless technology, like ZigBee, is used in that space.**

Access Network Sublayer:

Simulation Assumptions: 1% PER, 4dB NF,
32 Bytes, D-NLOS Fading, Indoor-to-Outdoor
PL Model. 900MHz has12dB propagation gain.

Sensor Antenna Gain: 11ah (-6.5dB)
and 11n (-4dB). AP antenna gain = 2dB.
* BT Long Range Adds 125 kbps and 500 kbps Modes

Range Versus Throughput for Four WHAN to WLAN Technologies



Layer -2 Communications network layer

Access Network Sublayer:

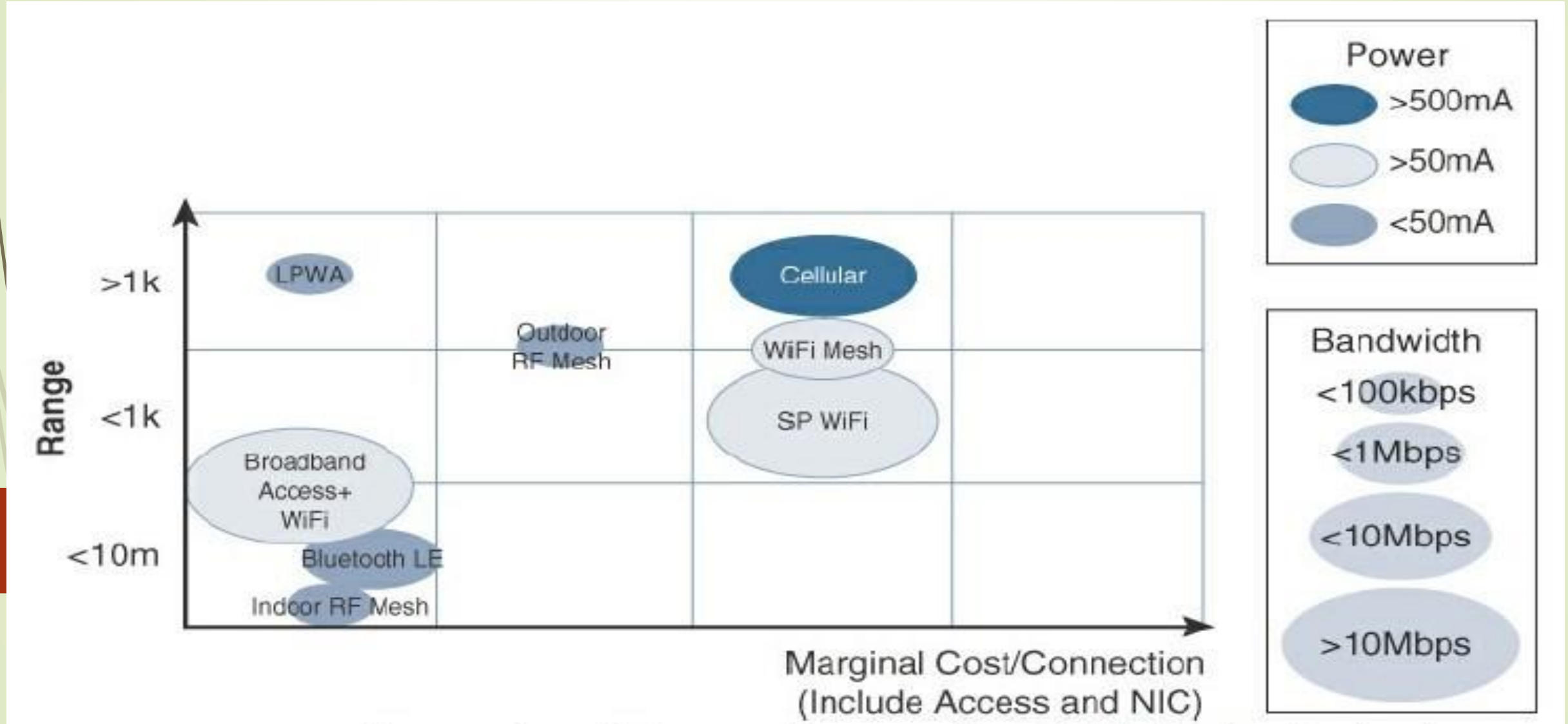
- Each protocol uses a specific frame format and transmission technique over a specific frequency (or band). These characteristics introduce additional differences.
- For example, above Figure demonstrates four technologies representing WHAN to WLAN ranges and compares the throughput and range that can be achieved in each case.
- Figure supposes that the sensor uses the same frame size, transmit power, and antenna gain.
- The slope of throughput degradation as distance increases varies vastly from one technology to the other.
- This difference limits the amount of data throughput that each technology can achieve as the distance from the sensor to the receiver increases.

Layer -2 Communications network layer

Access Network Sublayer:

- Increasing the throughput and achievable distance typically comes with an increase in power consumption.
- Therefore, after determining the smart object requirements (in terms of mobility and data transfer), a second step is to determine the target quantity of objects in a single collection cell, based on the transmission range and throughput required.
- This parameter in turn determines the size of the cell.
- It may be tempting to simply choose the technology with the longest range and highest throughput. However, the cost of the technology is a third determining factor.

Access Network Sublayer:



Comparison Between Common Last-Mile Technologies in Terms of Range Versus Cost, Power, and Bandwidth

Layer -2 Communications network layer

Access Network Sublayer:

The amount of data to carry over a given time period along with correlated power consumption (driving possible limitations in mobility and range) determines the wireless cell size and structure.

Technologies offer flexible connectivity structure to extend communication possibilities:

1. Point-to-point topologies:

- These topologies allow one point to communicate with another point.
- In this topology, a single object can communicate only with a single gateway.
- Several technologies are referred to as “point-to-point” when each object establishes an individual session with the gateway.

Layer -2 Communications network layer

Access Network Sublayer:

2. **Point-to-multipoint topologies:**

- **This topologies allow one point to communicate with more than one other point.**
- **Most IoT technologies where one or more than one gateways communicate with multiple smart objects are in this category.**
- **Some nodes (for example, sensors) support both data collection and forwarding functions, while some other nodes (for example, some gateways) collect the smart object data, sometimes instruct the sensor to perform specific operations, and also interface with other networks or possibly other gateways.**
- **For this reason, some technologies categorize the nodes based on the functions (described by a protocol) they implement.**

Layer -2 Communications network layer

Access Network Sublayer:

- To form a network, a device needs to connect with another device.
- When both devices fully implement the protocol stack functions, they can form a peer-to peer network.
- In many cases, one of the devices collects data from the others.
- For example, in a house, temperature sensors may be deployed in each room or each zone of the house, and they may communicate with a central point where temperature is displayed and controlled.
- A room sensor does not need to communicate with another room sensor.
- In that case, the control point is at the center of the network.
- The network forms a star topology, with the control point at the hub and the sensors at the spokes.
- In such a configuration, the central point can be in charge of the overall network coordination, taking care of the beacon transmissions and connection to each sensor.

Layer -2 Communications network layer

Access Network Sublayer:

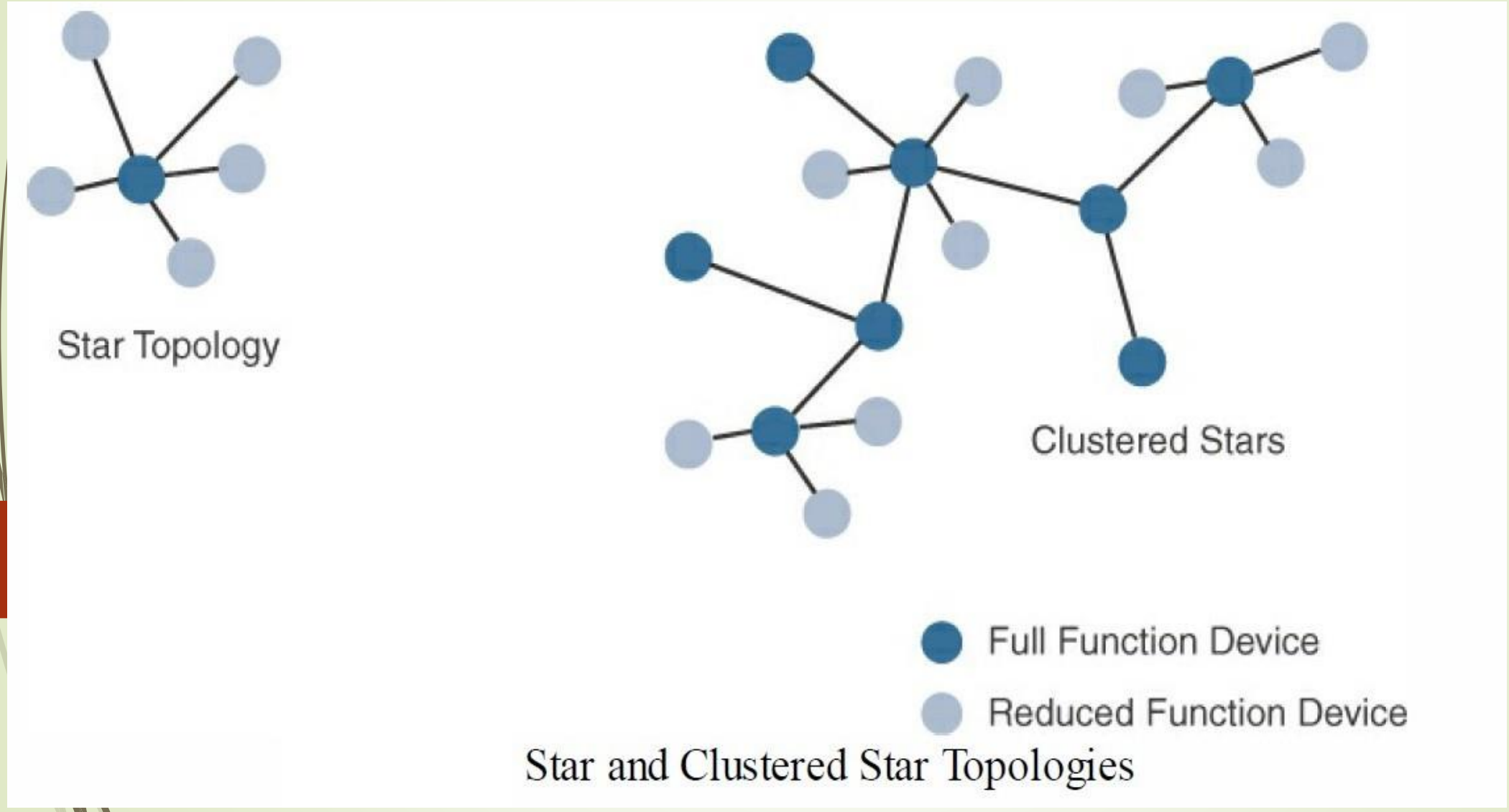
- In the IEEE 802.15.4 standard, the central point is called a coordinator for the network.
- With this type of deployment, each sensor is not intended to do anything other than communicate with the coordinator in a master/slave type of relationship.
- The sensor can implement a subset of protocol functions to perform just a specialized part (communication with the coordinator). Such a device is called a reduced-function device (RFD).
- An RFD cannot be a coordinator. An RFD also cannot implement direct communications to another RFD.

Layer -2 Communications network layer

Access Network Sublayer:

- The coordinator that implements the full network functions is called, by contrast, a full- function device (FFD).
- An FFD can communicate directly with another FFD or with more than one FFD, forming multiple peer-to-peer connections.
- Topologies where each FFD has a uniquepath to another FFD are called cluster tree topologies.
- FFDs in the cluster tree may have RFDs, resulting in a cluster star topology.
- The next Figure illustrates these topologies.

Access Network Sublayer:



Star and Clustered Star Topologies

Layer -2 Communications network layer

Access Network Sublayer:

- Other point-to-multipoint technologies allow a node to have more than one path to anothervnode, forming a mesh topology.
- This redundancy means that each node can communicate with more than just one other node.
- This communication can be used to directly exchange information between nodes (the receiver directly consumes the information received) or to extend the range of the communication link.
- In this case, an intermediate node acts as a relay between two other nodes.

Layer -2 Communications network layer

Access Network Sublayer:

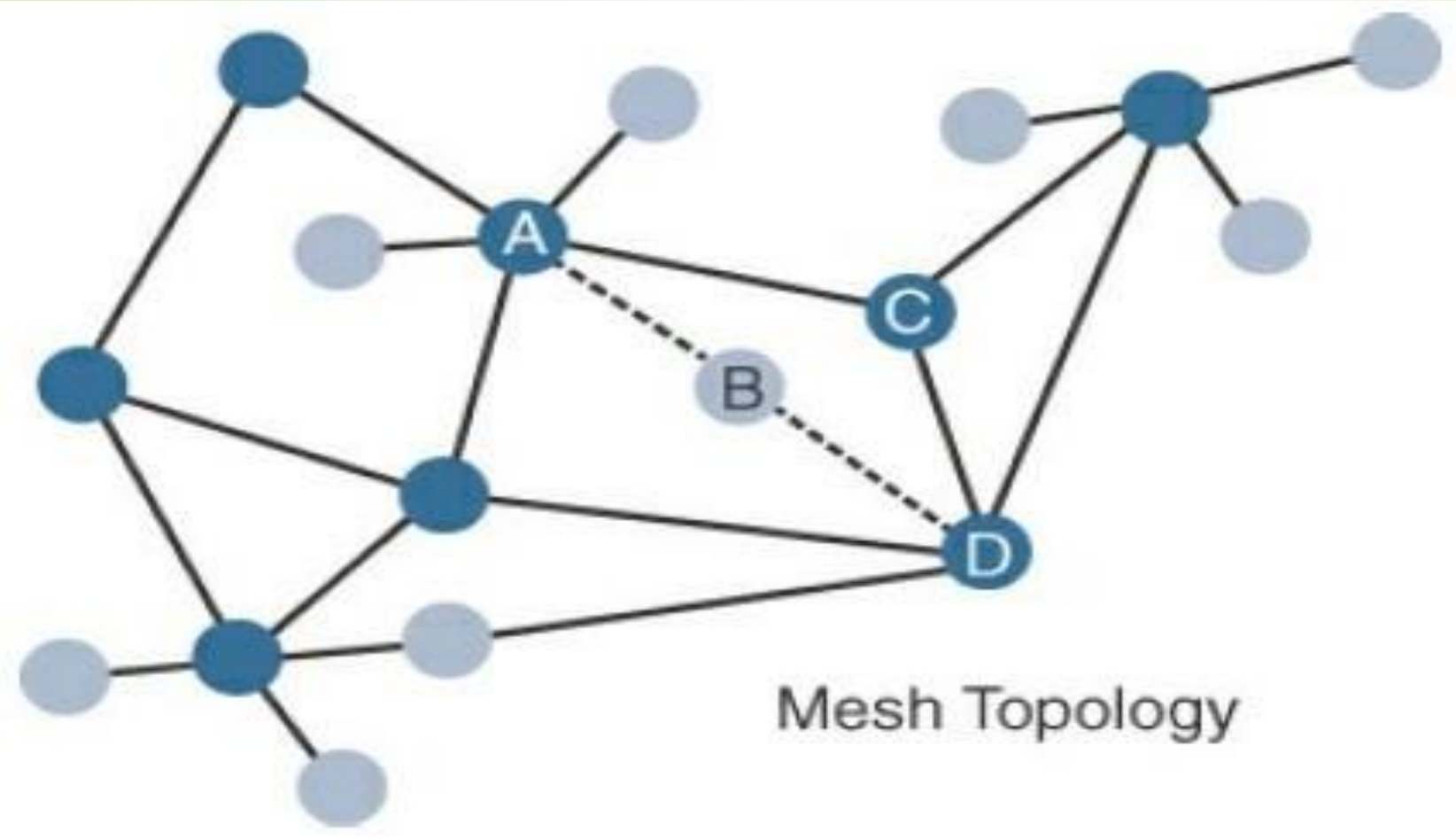
- These two other nodes would not be able to communicate successfully directly while respecting the constraints of power and modulation dictated by the PHY layer protocol.
- Range extension typically comes at the price of slower communications (as intermediate nodes need to spend time relaying other nodes' messages).
- An example of a technology that implements a mesh topology is Wi-Fi mesh.
- Another property of mesh networks is redundancy.
- The disappearance of one node does not necessarily interrupt network communications.
- Data may still be relayed through other nodes to reach the intended destination.

Layer -2 Communications network layer

Access Network Sublayer:

- Next Figure shows a mesh topology.
- Nodes A and D are too far apart to communicate directly.
- Communication can be relayed through nodes B or C. Node B may be used as the primary relay.
- The loss of node B does not prevent the communication between nodes A and D.
- Here, communication is rerouted through another node, node C.

Access Network Sublayer: Mesh Topology



Layer -2 Communications network layer

Access Network Sublayer:

- Figure shows a partial mesh topology, where a node can communicate with more than one other node, but not all nodes communicate directly with all other nodes.
- In a full mesh topology each node communicates with each other node.
- In the topology shown in previous Figure, which has 17 nodes, a full mesh structure would mean that each node would have 16 connections (one to each other node).
- Full mesh structures are computationally expensive (as each node needs to maintain a connection to each other node).

Layer -2 Communications network layer

Gateways and Backhaul Sublayer:

- Data collected from a smart object may need to be forwarded to a central station where data is processed.
- As this station is often in a different location from the smart object, data directly received from the sensor through an access technology needs to be forwarded to another medium (the backhaul) and transported to the central station.
- The gateway is in charge of this inter-medium communication.
- In most cases, the smart objects are static or mobile within a limited area. The gateway is often static.
- However, some IoT technologies do not apply this model.
- For example, dedicated short-range communication (DSRC) allows vehicle-to-vehicle and vehicle-to-infrastructure communication.
- In this model, the smart object's position relative to the gateway is static.
- The car includes sensors and one gateway.

Layer -2 Communications network layer

Gateways and Backhaul Sublayer:

- Communication between the sensors and the gateway may involve wired or wireless technologies.
- Sensors may also be integrated into the road infrastructure and connect over a wired or wireless technology to a gateway on the side of the road.
- A wireless technology (DSRC operates in the upper 5 GHz range) is used for backhaul communication, peer-to-peer, or mesh communication between vehicles.
- In the DSRC case, the entire “sensor field” is moving along with the gateway, but the general principles of IoT networking remain the same.
- The range at which DSRC can communicate is limited.
- Similarly, for all other IoT architectures, the choice of a backhaul technology depends on the communication distance and also on the amount of data that needs to be forwarded.
- When the smart object’s operation is controlled from a local site, and when the environment is stable (for example, factory or oil and gas field), Ethernet can be used as a backhaul.

Layer -2 Communications network layer

Gateways and Backhaul Sublayer:

- In unstable or changing environments (for example, open mines) where cables cannot safely be run, a wireless technology is used.
- Wi-Fi is common in this case, often with multiple hops between the sensor field and the operation center.
- Mesh is a common topology to allow communication flexibility in this type of dynamic environment.
- Throughput decreases as node-to-node distance increases, and it also decreases as the number of hops increases.
- In a typical Wi-Fi mesh network, throughputhalves for each additional hop.
- WiMAX (802.16) is an example of a longer-range technology.

Layer -2 Communications network layer

Gateways and Backhaul Sublayer:

- WiMAX can achieve ranges of up to 50 kilometers with rates of up to 70 Mbps.
- The choice of WiMAX or a cellular technology depends on the vertical and the location (local preferences, local costs).

Layer 2: Communications Network Layer

Technology	Type and Range	Architectural Characteristics
Ethernet	Wired, 100 m max	Requires a cable per sensor/sensor group; adapted to static sensor position in a stable environment; range is limited; link is very reliable
Wi-Fi (2.4 GHz, 5 GHz)	Wireless, 100 m (multipoint) to a few kilometers (P2P)	Can connect multiple clients (typically fewer than 200) to a single AP; range is limited; adapted to cases where client power is not an issue (continuous power or client battery recharged easily); large bandwidth available, but interference from other systems likely; AP needs a cable
802.11ah (HaloW, Wi-Fi in sub-1 GHz)	Wireless, 1.5 km (multipoint), 10 km (P2P)	Can connect a large number of clients (up to 6000 per AP); longer range than traditional Wi-Fi; power efficient; limited bandwidth; low adoption; and cost may be an issue
WiMAX (802.16)	Wireless, several kilometers (last mile), up to 50 km (backhaul)	Can connect a large number of clients; large bandwidth available in licensed spectrum (fee-based); reduced bandwidth in license-free spectrum (interferences from other systems likely); adoption varies on location
Cellular (for example, LTE)	Wireless, several kilometers	Can connect a large number of clients; large bandwidth available; licensed spectrum (interference-free; license-based)

Gateways and Backhaul Sublayer: Architectural Considerations for WiMAX and Cellular Technologies

Layer -2 Communications network layer

Network Transport Sublayer:

- communication structure may involve peer-to-peer (for example,meter to meter), point-to-point (meter to headend station), point-to-multipoint(gateway or head-end to multiple meters), unicast and multicast communications (software update to one or multiple systems).
- In a multitenant environment (for example, electricity and gas consumption management), different systems may use the same communication pathways.
- This communication occurs over multiple media (for example, power lines inside your house or a short-range wireless system like indoor Wi-Fi and/or ZigBee), a longer-range wireless system to the gateway, and yet another wireless or wired medium for backhaul transmission.
- To allow for such communication structure, a network protocol with specific characteristics needs to be implemented.

Layer -2 Communications network layer

Network Transport Sublayer:

- The protocol needs to be open and standard-basedto accommodate multiple industries and multiple media.
- Scalability (to accommodate thousands or millions of sensors in a single network) and security are also common requirements.
- IP is a protocol that matches all these requirements.
- The flexibility of IP allows this protocol to be embedded in objects of very different natures, exchanging information over very different media, including low-power, lossy, and low-bandwidth networks.
- For example, RFC 2464 describes how an IPv6 packet gets encapsulated over an Ethernet frame and is also used for IEEE 802.11 Wi-Fi.
- Similarly, the IETF 6LoWPAN working group specifies how IPv6 packets are carried efficiently over lossy networks, forming an “adaption layer” for IPv6, primarily for IoT networks.

Layer -2 Communications network layer

IoT Network Management Sublayer:

- IP, TCP, and UDP bring connectivity to IoT networks.
- Upper-layer protocols need to take care of data transmission between the smart objects and other systems.
- Multiple protocols have been leveraged or created to solve IoT data communication problems.
- Some networks rely on a push model (that is, a sensor reports at a regular interval or based on a local trigger), whereas others rely on a pull model (that is, an application queries the sensor over the network), and multiple hybrid approaches are also possible.
- IP logic, some IoT implementers have suggested HTTP for the data transfer phase.
- HTTP has a client and server component.
- The sensor could use the client part to establish a connection to the IoT central application (the server), and then data can be exchanged.

Layer -2 Communications network layer

IoT Network Management Sublayer:

- One example is WebSocket. WebSocket is part of the HTML5 specification, and provides a simple bidirectional connection over a single connection.
- Some IoT solutions use WebSocket to manage the connection between the smart object and an external application.
- WebSocket is often combined with other protocols, such as MQTT (described shortly) to handle the IoT-specific part of the communication.
- With the same logic of reusing well-known methods, Extensible Messaging and Presence Protocol (XMPP) was created.
- XMPP is based on instant messaging and presence.
- It allows the exchange of data between two or more systems and supports presence and contact list maintenance.
- It can also handle publish/subscribe, making it a good choice for distribution of information to multiple devices.
- A limitation of XMPP is its reliance on TCP, which may force subscribers to maintain open sessions to other systems and may be a limitation for memory-constrained objects.

Layer -2 Communications network layer

IoT Network Management Sublayer:

- To respond to the limits of web-based protocols, another protocol was created by the IETF Constrained Restful Environments (CoRE) working group: Constrained Application Protocol (CoAP).
- CoAP uses some methods similar to those of HTTP (such as Get, Post, Put, and Delete) but implements a shorter list, thus limiting the size of the header.
- CoAP also runs on UDP (whereas HTTP typically uses TCP).
- CoAP also adds a feature that is lacking in HTTP and very useful for IoT: observation.
- Observationallows the streaming of state changes as they occur, without requiring the occur, without requiring the changes.

Layer -2 Communications network layer

IoT Network Management Sublayer:

- Another common IoT protocol utilized in these middle to upper layers is Message Queue Telemetry Transport (MQTT).
- MQTT uses a broker-based architecture.
- The sensor can be set to be an MQTT publisher (publishes a piece of information), the application that needs to receive the information can be set as the MQTT subscriber, and any intermediary system can be set as a broker to relay the information between the publisher and the subscriber(s).
- MQTT runs over TCP. A consequence of the reliance on TCP is that an MQTT client typically holds a connection open to the broker at all times.
- This may be a limiting factor in environments where loss is high or where computing resources are limited.

The Core IoT Functional Stack

3. Application and analytics layer/ Layer 3: Applications and Analytics Layer

1. Analytics Versus Control Applications
    1. Analytics application
    1. Control application
2. Data Versus Network Analytics
    1. Data Analytics
    2. Network Analytics
3. Data Analytics Versus Business Benefits

Layer 3: Applications and Analytics Layer

- **Once connected to a network, smart objects exchange information with other systems.**
- **As soon as IoT network spans more than a few sensors, the power of the Internet of Things appears in the applications that make use of the information exchanged with the smart objects.**

1. Analytics Versus Control Applications:

- **Multiple applications can help increase the efficiency of an IoT network.**
- **Each application collects data and provides a range of functions based on analyzing the collected data.**
- **It can be difficult to compare the features offered.**

1.Analytics Versus Control Applications:

- From an architectural standpoint, one basic classification can be as follows:

1. Analytics application:

   - This type of application collects data from multiple smart objects, processes the collected data, and displays information resulting from the data that was processed.
   - The display can be about any aspect of the IoT network, from historical reports, statistics,or trends to individual system states.
   - The important aspect is that the application processes the data to convey a view of the network that cannot be obtained from solely looking at the information displayed by a single smart object.

2. Control application:

- This type of application controls the behavior of the smart object or the behavior of an object related to the smart object.
- For example, a pressure sensor may be connected to a pump.
- A control application increases the pump speed when the connected sensor detects a drop in pressure.
- Control applications are very useful for controlling complex aspects of an IoT network with a logic that cannot be programmed inside a single IoT object, either because the configured changes are too complex to fit into the local system or because the configured changes rely on parameters that include elements outside the IoT object.

Analytics Versus Control Applications:

- Many advanced IoT applications include both analytics and control modules.
- In most cases, data is collected from the smart objects and processed in the analytics module.
- The result of this processing may be used to modify the behavior of smart objects or systems related to the smart objects.
- The control module is used to convey the instructions for behavioral changes.
- When evaluating an IoT data and analytics application, we need to determine the relative depth of the control part needed for our use case and match it against the type of analytics provided.

2.Data Versus Network Analytics

Analytics is a general term that describes processing information to make sense of collected data . In the world of IoT, a possible classification of the analytics function is as follows:

1.Data analytics:

- **This type of analytics processes the data collected by smart objects and combines it to provide an intelligent view related to the IoT system.**
- **At a very basic level, a dashboard can display an alarm when a weight sensor detects that a shelf is empty in a store.**
- **In a more complex case, temperature, pressure, wind, humidity, and light levels collected from thousands of sensors may be combined and then processed to determine the likelihood of a storm and its possible path.**
- **In this case, data processing can be very complex and may combine multiple changing values over complex algorithms.**

1. Data analytics:

- Data analytics can also monitor the IoT system itself.
- For example, a machine or robot in a factory can report data about its own movements.
- This data can be used by an analytics application to report degradation in the movement speeds, which may be indicative of a need to service the robot before a part breaks.

2. Network analytics:

- Most IoT systems are built around smart objects connected to the network.
- A loss or degradation in connectivity is likely to affect the efficiency of the system.
- Such a loss can have dramatic effects.
- For example, open mines use wireless networks to automatically pilot dump trucks.
- A lasting loss of connectivity may result in an accident or degradation of operations efficiency (automated dump trucks typically stop upon connectivity loss).
- On a more minor scale, loss of connectivity means that data stops being fed to your data analytics platform, and the system stops making intelligent analyses of the IoT system.
- A similar consequence is that the control module cannot modify local object behaviors anymore.

Most analytics applications employ both data and network analytics modules

3. Data Analytics Versus Business Benefits

Almost any object can be connected, and multiple types of sensors can be installed on a given object.

Collecting and interpreting the data generated by these devices is where the value of IoT is realized.

From an architectural standpoint, we can define static IoT networks where a clear list of elements to monitor and analytics to perform are determined.

Data Analytics Versus Business Benefits

Almost any object can be connected, and multiple types of sensors can be installed on a
given object.

Collecting and interpreting the data generated by these devices is where the value of IoT is realized.

From an architectural standpoint, we can define static IoT networks where a

clear list of elements to monitor and analytics to perform are determined.

An example of a flexible analytics and control application is Cisco Jasper, which provides a turnkey cloud-based platform for IoT management and monetization.

Data Analytics Versus Business Benefits

An example of a flexible analytics and control application is Cisco Jasper, which provides

a turnkey cloud-based platform for IoT management and monetization.

Example:

Vending machines deployed throughout a city. At a basic level, these machines can be connected, and sensors can be deployed to report when a machine is in an error state. A repair person can besent to address the issue when such a state is identified. This type of alert is a time saver and avoids the need for the repair team to tour all the machines in turn when only one may be malfunctioning

4. Smart Services:

- The ability to use IoT to improve operations is often termed “smart services.”
- Fundamentally, smart services use IoT and aim for efficiency.
- For example, sensors can be installed on equipment to ensure ongoing conformance with regulations or safety requirements.
- This angle of efficiency can take multiple forms, from presence sensors in hazardous areas to weight threshold violation detectors on trucks.

Smart Services:

- Smart services can also be used to measure the efficiency of machines by detecting

  machine output, speed, or other forms of usage evaluation.

- Entire operations can be optimized with IoT.

- In hospitality, for example, presence and motion sensors can evaluate the number of guests in a lobby and redirectpersonnel accordingly.

- Movement of people and objects on factory floors can be analyzed to optimize the production flow.

- A sensor can turn a light on or off based on the presence of a human in the room.

IoT Data Management and Compute Stack:

- The data generated by IoT sensors is one of the single biggest challenges in building an IoT system.
- In modern IT networks, the data sourced by a computer or server is typically generated by the client/server communications model, and it serves the needs of the application.
- In sensor networks, the vast majority of data generated is unstructured and of very little use on its own.
- For example, the majority of data generated by a smart meter is nothing more than polling data; the communications system simply determines whether a network connection to the meter is still active.
- This data on its own is of very little value.
- The real value of a smart meter is the metering data read by the meter management system

IoT Data Management and Compute Stack:

As data volume, the variety of objects connecting to the network, and the need for more efficiency increase, new requirements appear, and those requirements tend to bring the need for data analysis closer to the IoT system.

These new requirements include the following:

1. Minimizing latency:

Milliseconds matter for many types of industrial systems, such as when we are trying to prevent manufacturing line shutdowns or restore electrical service.

Analyzing data close to the device that collected the data can make a difference between averting disaster and a cascading system failure.

2. Conserving network bandwidth:

- Offshore oil rigs generate 500 GB of data weekly.
- Commercial jets generate 10 TB for every 30 minutes of flight.
- It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the cloud. Nor is it necessary because many critical analyses do not require cloud-scale processing and storage.

3. Increasing local efficiency:

- Collecting and securing data across a wide geographic area with different environmental conditions may not be useful.
- The environmental conditions in one area will trigger a local response independent from the conditions of another site hundreds of miles away.
- Analyzing both areas in the same cloud system may not be necessary for immediate efficiency

Fog Computing

- The solution to the challenges in IoT is to distribute data management throughout the IoT system, as close to the edge of the IP network as possible.
- The best-known embodiment of edge services in IoT is fog computing.
- Any device with computing, storage, and network connectivity can be a fog node.
- Examples include industrial controllers, switches, routers, embedded servers, and IoT gateways. Analyzing IoT data close to where it is collected minimizes latency, offloads gigabytes of network traffic from the core network, and keeps sensitive data inside the local network.

Fog Computing:

- An advantage of structure is that the fog node allows intelligence gathering (such as analytics) and control from the closest possible point, and in doing so, it allows better performance over constrained networks.
- This introduces a new layer to the traditional IT computing model, one that is often referred to as the “fog layer.”

Fog Computing

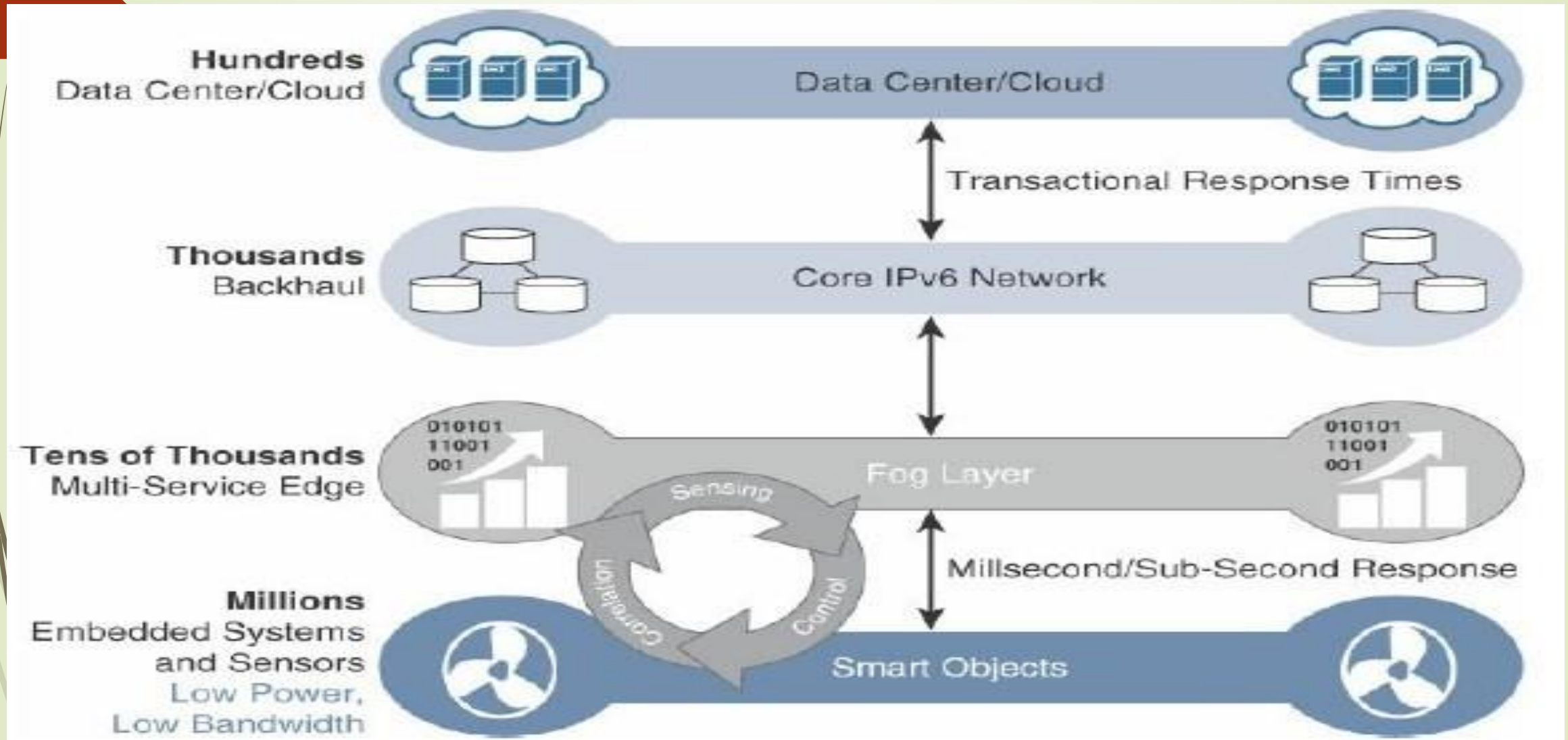


Figure shows the placement of the fog layer in the IoT Data Management and Compute Stack.

Fog Computing

- Fog services are typically accomplished very close to the edge device, sitting as close to the IoT endpoints as possible.
- One significant advantage of this is that the fog node has contextual awareness of the sensors it is managing because of its geographic proximity to those sensors.
- For example, there might be a fog router on an oil derrick that is monitoring all the sensor activity at that location.
- Because the fog node is able to analyze information from all the sensors on that derrick, it can provide contextual analysis of the messages it is receiving and may decide to send back only the relevant information over the backhaul network to the cloud.
- In this way, it is performing distributed analytics such that the volume of data sent upstream is greatly reduced and is much more useful to application and analytics servers residing in the cloud.

Fog Computing:

- In addition, having contextual awareness gives fog nodes the ability to react to events in the IoT network much more quickly than in the traditional IT compute model, which would likely incur greater latency and have slower response times.

- The fog layer thus provides a distributed edge control loop capability, where devices can be monitored, controlled, and analyzed in real time without the need to wait for communication from the central analytics and application servers in the cloud

Fog Computing:

- For example, tire pressure sensors on a large truck in an open-pit mine might continually report measurements all day long.
- There may be only minor pressure changes that are well within tolerance limits, making continual reporting to the cloud unnecessary.
- With a fog node on the truck, it is possible to not only measure the pressure of all tires at once but also combine this data with information coming from other sensors in the engine, hydraulics, and so on.
- With this approach, the fog node sends alert data upstream only if an actual problem is beginning to occur on the truck at affects operational efficiency.

Module – 1 Fog Computing

Fog Computing:

- IoT fog computing enables data to be preprocessed and correlated with other inputs to produce relevant information.
- This data can then be used as real-time, actionable knowledge by IoT-enabled applications.
- Longer term, this data can be used to gain a deeper understanding of network behavior and systems for the purpose of developing proactive policies, processes and responses.

Module – 1 Fog Computing

Fog Computing:

The defining characteristic of fog computing are as follows:

1. Contextual location awareness and low latency:

- **The fog node sits as close to the IoT endpoint as possible to deliver distributed computing.**

1. Geographic distribution:

- **In sharp contrast to the more centralized cloud, the services and applications targeted by the fog nodes demand widely distributed deployments.**

2. Deployment near IoT endpoints:

- **Fog nodes are typically deployed in the presence of a large number of IoT endpoints.**
- **For example, typical metering deployments often see 3000 to 4000 nodes per gateway router,which also functions as the fog computing node.**

Module – 1 Fog Computing

Fog Computing:

The defining characteristic of fog computing are as follows:

4. Wireless communication between the fog and the IoT endpoint:

- **Although it is possible to connect wired nodes, the advantages of fog are greatest when dealing with a large number of endpoints, and wireless access is the easiest way to achieve such scale.**

5. Use for real-time interactions:

- **Important fog applications involve real-time interactions rather than batch processing.**
- **Preprocessing of data in the fog nodes allows upper-layer applications to performbatch processing on a subset of the data.**

Module – 1 Edge Computing

Edge Computing:

- **The natural place for a fog node is in the network device that sits closest to the IoT endpoints, and these nodes are typically spread throughout an IoT network.**
- **In recent years, the concept of IoT computing has been pushed even further to the edge, and in some cases it now resides directly in the sensors and IoT devices.**
- **Edge computing is also sometimes called “mist” computing.**

Module – 1 Edge Computing

Edge Computing:

- **Some new classes of IoT endpoints have enough compute capabilities to perform at least low-level analytics and filtering to make basic decisions.**
- **For example, consider a water sensor on a fire hydrant.**
- **While a fog node sitting on an electrical pole in the distribution network may have an excellent view of all the fire hydrants in a local neighborhood, a node on each hydrant would have clear view of a water pressure drop on its own line and would be able to quickly generate an alert of a localized problem.**

Module – 1 Edge Computing

Edge Computing:

- **Another example is in the use of smart meters.**
- **Edge compute–capable meters are able to communicate with each other to share information on small subsets of the electrical distribution grid to monitor localized power quality and consumption, and they can inform fog node of events that may pertain to only tiny sections of the grid.**
- **Models such as these help ensure the highest quality of power delivery to customers.**

Module – 1 The Hierarchy of Edge, Fog, and Cloud

The Hierarchy of Edge, Fog, and Cloud:

- **Edge or fog computing in no way replaces the cloud but they complement each other, and many use cases actually require strong cooperation between layers.**
- **Edge and fog computing layers simply act as a first line of defense for filtering, analyzing, and otherwise managing data endpoints.**
- **This saves the cloud from being queried by each and every node for each event.**
- **This model suggests a a hierarchical organization of network, compute, and data storage resources.**

Module – 1 The Hierarchy of Edge, Fog, and Cloud

The Hierarchy of Edge, Fog, and Cloud:

- **At each stage, data is collected, analyzed, and responded to when necessary, according to the capabilities of the resources at each layer.**
- **As data needs to be sent to the cloud, the latency becomes higher.**
- **The advantage of this hierarchy is that a response to events from resources close to the end device is fast and can result in immediate benefits, while still having deeper compute resources available in the cloud when necessary.**

Module – 1 The Hierarchy of Edge, Fog, and Cloud

The Hierarchy of Edge, Fog, and Cloud:

- **heterogeneity of IoT devices also means a heterogeneity of edge and fog computing resources.**
- **While cloud resources are expected to be homogenous, it is fair to expect that in many cases both edge and fog resources will use different operating systems, have different CPU and data storage capabilities, and have different energy consumption profiles.**

Module – 1 The Hierarchy of Edge, Fog, and Cloud

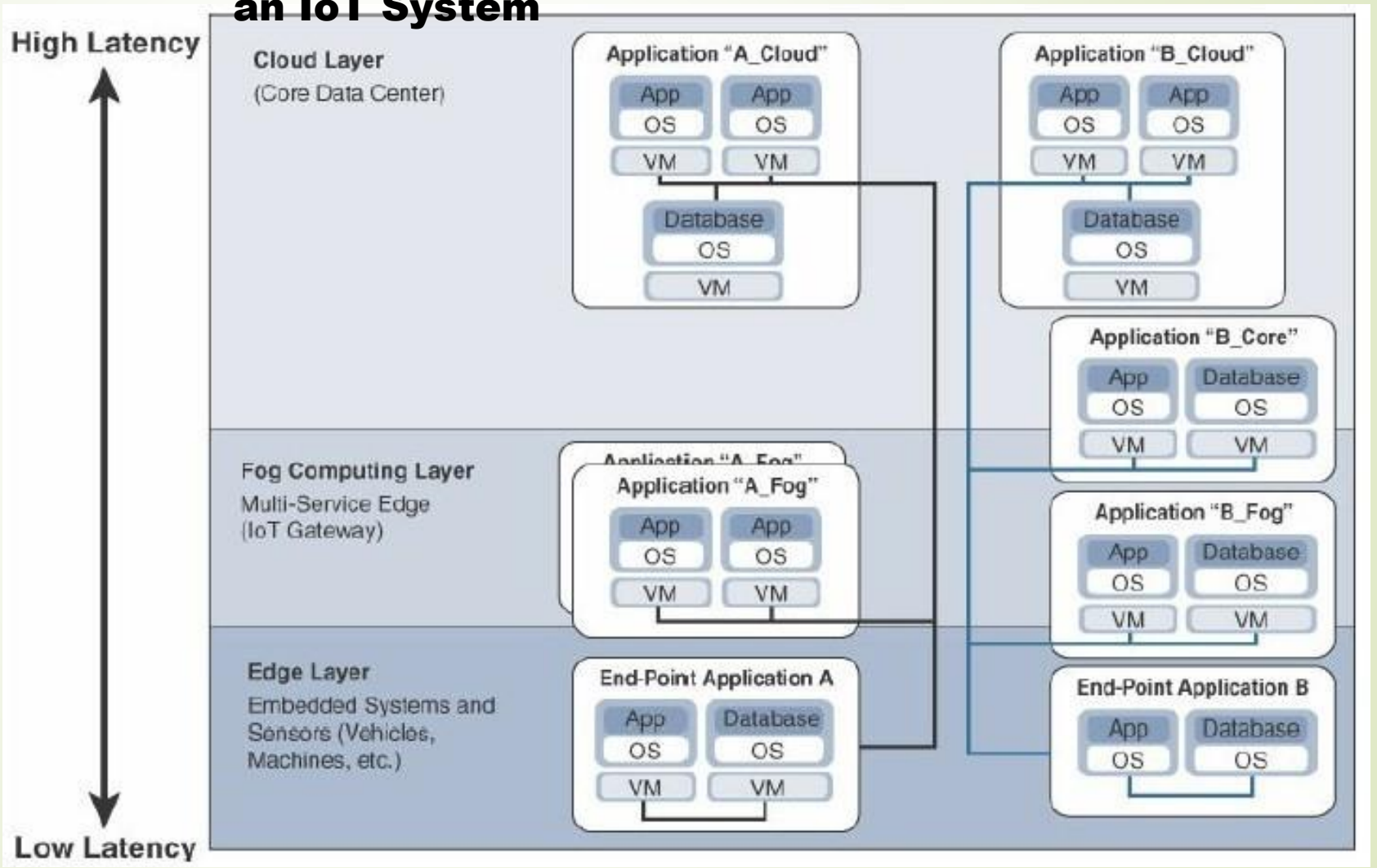
The Hierarchy of Edge, Fog, and Cloud:

- **Edge and fog thus require an abstraction layer that allows applications to communicate with one another.**
- **The abstraction layer exposes a common set of APIs for monitoring, provisioning, and controlling the physical resources in a standardized way.**
- **The abstraction layer also requires a mechanism to support virtualization, with the ability to run multiple operating systems or service containers on physical devices to support multitenancy and application consistency across the IoT system.**

Module – 1 The Hierarchy of Edge, Fog, and Cloud

Figure illustrates the hierarchical nature edge, fog, and cloud computing across an IoT system.

Distributed Compute and Data Management Across an IoT System



Module – 1 The Hierarchy of Edge, Fog, and Cloud

The Hierarchy of Edge, Fog, and Cloud:

From an architectural standpoint, fog nodes closest to the network edge receive the data from IoT devices. The fog IoT application then directs different types of data to the optimal place for analysis:

- **The most time-sensitive data is analyzed on the edge or fog node closest to the things generating the data.**
- **Data that can wait seconds or minutes for action is passed along to an aggregation node for analysis and action.**
- **Data that is less time sensitive is sent to the cloud for historical analysis, big data analytics, and long- term storage.**
- **Forexample, each of thousands or hundreds of thousands of fog nodes might send periodic summaries of data to the cloud for historic storage**