6NTCM009W Internet of Things

- **Lecture 2 - Objectives**
- Professional and regulatory bodies
- IoT Network Design and Architectures
  - oneM2M model
  - IoTWF model
  - IoT Reference model
- Edge computing vs cloud computing
- Smart IoT gateway

The need for an IoT architecture

- IoT was not “designed”, it “happened”
- Multiple specialised solutions
- Multiple sensor types
- Multiple protocols
- Multiple requirements
- Multiple applications

Differences between IT and IoT

- The key difference between IT and IoT is the data.
- IT systems are mostly concerned with reliable and continuous support of business applications such as:
  - email, web, databases, Customer Relationship Management (CRM) systems
- IoT is all about the data generated by sensors and how that data is used.
- The essence of IoT architectures thus involves how the data is transported, collected, analysed, and ultimately acted upon.

Professional bodies and standardisation

- Strong interest in developing IoT solutions lies within the Third Generation Partnership Project (3GPP) for 2G/3G/4G/5G technologies
  https://www.etsi.org/committee/3gpp
- Forums such as OneM2M and IoT World
  https://www.onem2m.org/
  https://iotforum.org/about-iot-forum/
- The Industry IoT Consortium is a global not-for-profit partnership of industry, government, and academia
  https://www.iiconsortium.org/iira/
- Internet Research Task Force (IETF) Working Groups
  https://www.ietf.org/
- IEEE 802.15 Working Group for Wireless Specialty Networks (WSN)
- IEEE 802.11 WIRELESS LOCAL AREA NETWORKS - The Working Group for WLAN Standards

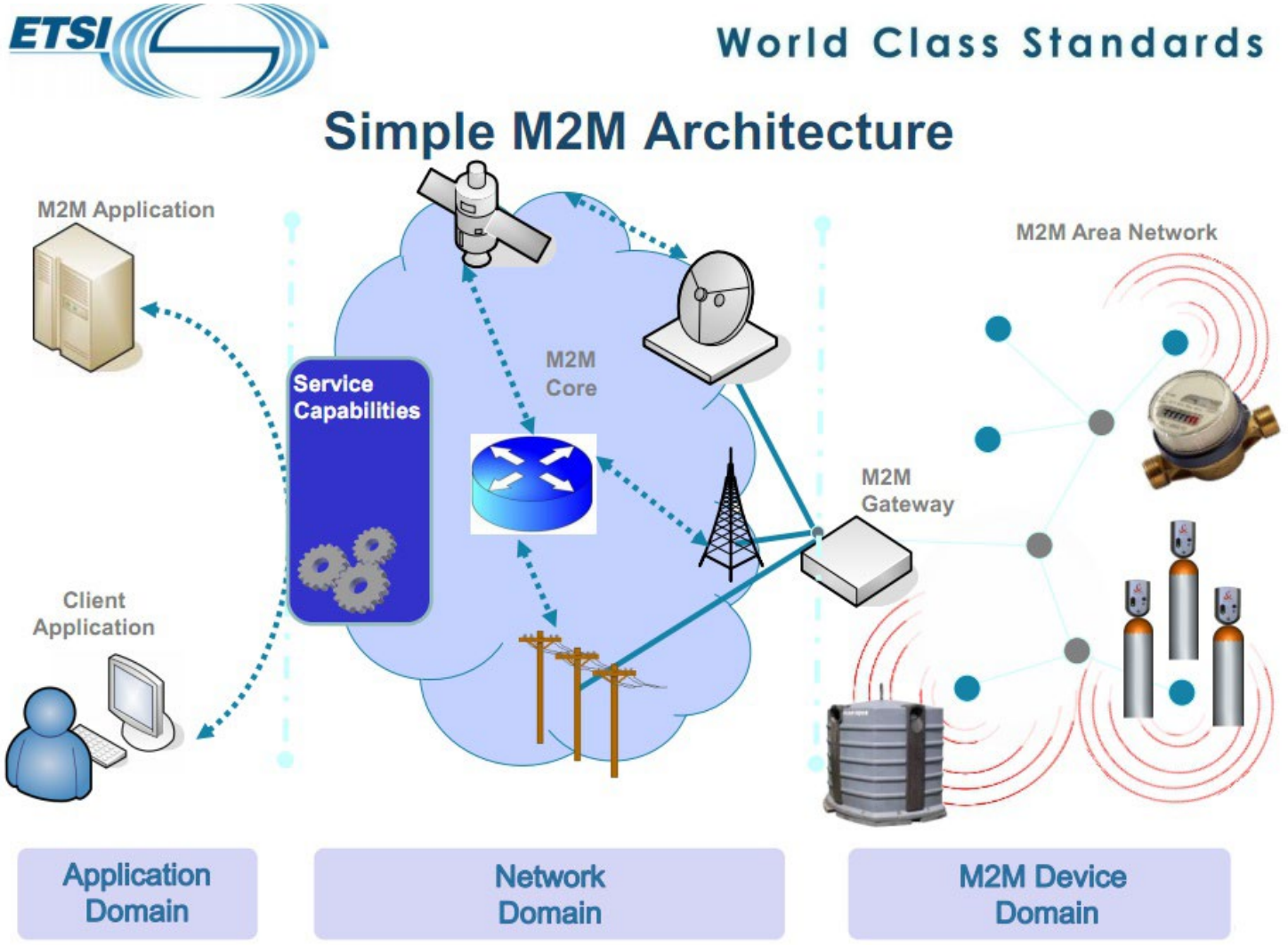
Architecture models

- Many available such as
  - European Telecommunications Standards Institute (ETSI) M2M and
    - oneM2M IoT Standardised Architecture
  - IoT World Forum (IoTWF)
    - World Forum (IoTWF) Standardised Architecture
  - Purdue Model for Control Hierarchy
  - Industrial Internet Reference Architecture (IIRA) by Industrial Internet Consortium (IIC)
  - Internet of Things Architecture (IoT-A)

ETSI M2M Standardised Architecture

- 2008: European Telecommunications Institute (ETSI) forms M2M Technical Committee
  - -> goal to accelerate the adoption of M2M applications and devices which later expanded to include IoT
- 2012: ETSI forms oneM2M as a global initiative
  - -> to create a common Services Layer which can be embedded within field devices to allow communication with application servers
- ETSI model includes 3 “domains” each leveraging multiple existing protocols

ETSI model – M2M Architecture



https://www.etsi.org/technologies/internet-of-things

IoT World Forum (IoTWF) Standardised Architecture

- 2014: IoTWF committee by Cisco, IBM, Rockwell automation and others published a seven-layer IoT architectural reference model
- Simplified perspective on IoT
- It follows the 7-layer OSI architecture

IoTWF architecture model

L7. Collaboration & Processes
(involving people & business processes
L6. Application
(reporting, analytics, control)
L5. Data abstraction
(aggregation & access)
L4. Data accumulation
(storage)
L3. Edge Computing
(Data element analysis & Transformation
L2. Connectivity
(communication & Processing Units)
L1. Physical Devices & Controllers
(the “things” in IoT)

IoTWF Layer 1: Physical devices

- The first layer is concerned with the physical devices and controllers.
- “Things”: sensors, actuators, microcontrollers and power
- Devices send data
- Data include a description of the device status or information from the sensors.

IoTWF Layer 2: Connectivity layer

- Sets up a connection with the Layer 1 devices
- Ensures reliable delivery of information throughout the network
- Implements different device compatible protocols
- Performs switching and routing
- Translates protocols
- Provides network level security (provides protection against security threats)
- Provides network analytics
- Example: Wi-Fi Access point for home applications

IoTWF L3 - Edge Computing layer

- Filters data to reduce traffic at higher level processing
- Cleans up data
- Aggregates data
- Evaluates and validates data so that they can be processed by Layer-4
- Reformats data for further processing at higher levels
- It takes place at a location not very far from the sensors
- It is used to generate events for any alerts

IoTWF L4 – Data accumulation layer

- Data go to the cloud
- Data may be raw or processed
- Data are maintained in a format that is extremely accessible
- Data can be examined, and intelligence can be obtained

IoTWF L5 – Data abstraction layer

The objective of this layer is to render data along with its storage with such a strategy that can help developers to write easier applications.

- Reuse the data to create abstracted data
- Reconcile multiple data formats
- Establish semantics from various sources

IoTWF L6 – Applications layer

- Process data to ensure that it is accessible for everyone
- It is used for data interpretation to create reports for monitoring and control of the application
- Business intelligence tools are used.

IoTWF L7 – Collaboration & Processes layer

- It offers action or response that can help against the provided data.
- It enables collaboration on communicating IoT information for business decision making.

IT and OT processing for IoT

Layers 4 -7 : Information Technology (IT) processing

- Query based
- Data at rest
- Non-real time

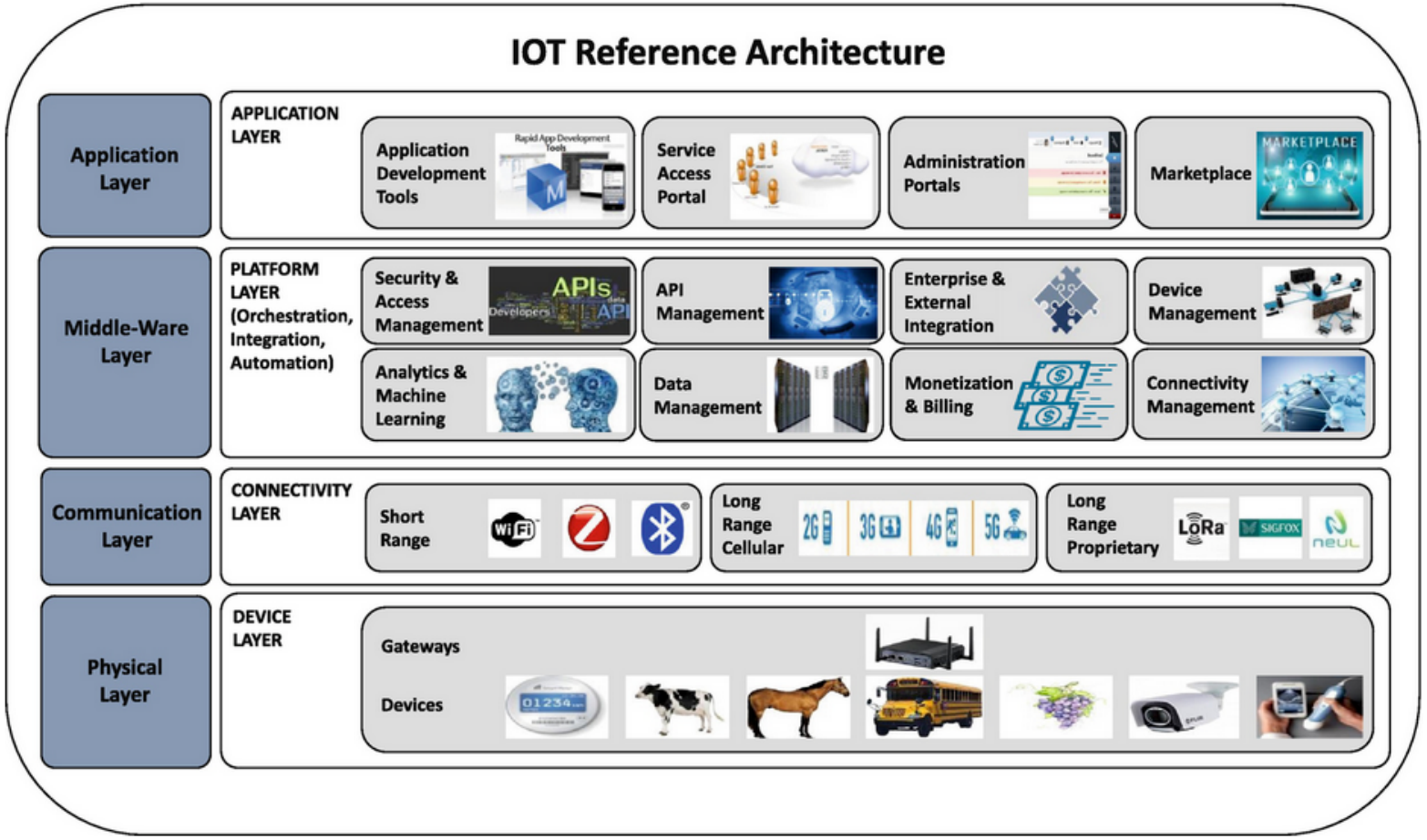
Layers 1-3 : Operation Technology (OT) processing

- Event based
- Data in motion
- Real-time

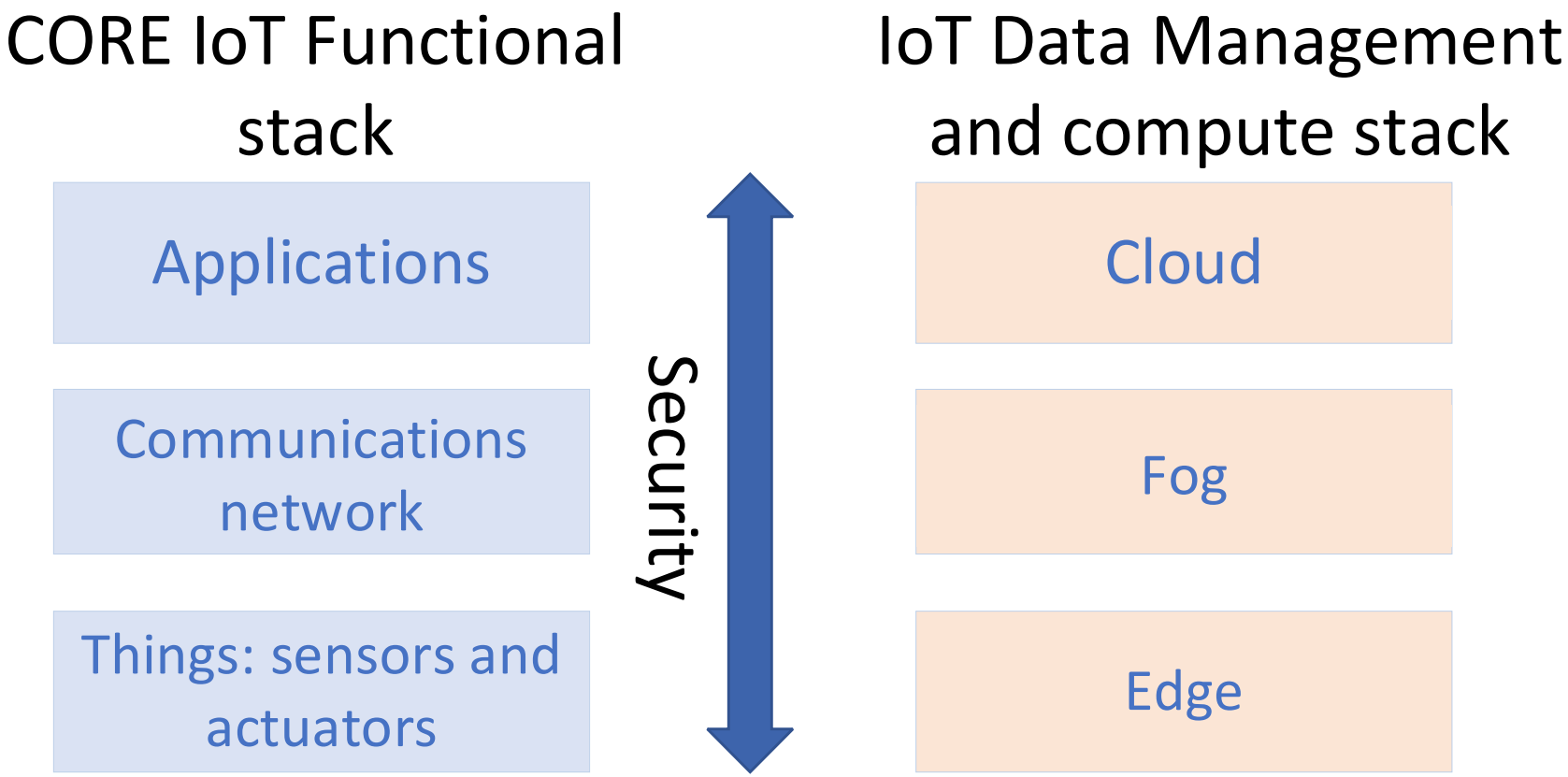
Commonalities between models/layers

- All models are built on layers
- Layers are usually independent with different functions and roles
- Multiple protocols at each layer
  - Some protocols appear at several layers
- Multiple possible parallel domains
- Objective: objects to connect to a network and communicate with applications

IOT Reference Architecture – four layered model



Functional stack and data management stack



Edge computing

- Edge computing acts on data at the source and brings applications closer to data sources such as IoT devices or gateways.
- The growth of IoT devices has resulted in unprecedented volumes of data.
  - Expectation for further growth with 5G networks
- Cloud services and Artificial Intelligence (AI) require all device-generated data to be in a centralized data centre or to the cloud, causing bandwidth and latency issues.
- Edge computing offers a more efficient alternative; data is processed and analysed closer to the point where they are created
  - data does not traverse over a network to a cloud or data centre to be processed hence latency and power are significantly reduced

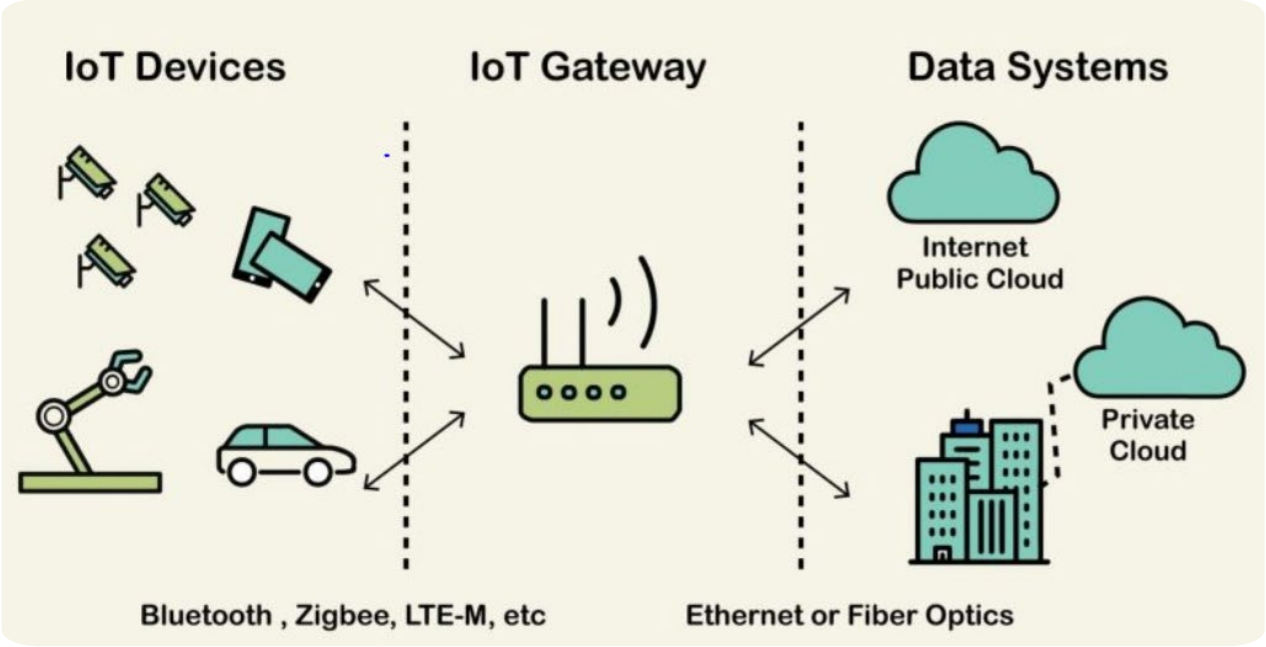
Fog computing

- Fog computing or fog networking uses edge devices (gateways) to carry out a substantial amount of computation, storage, and communication locally and routing over the Internet backbone
- Fog computing is intended for distributed computing where numerous "peripheral" devices connect to a cloud.
- Fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-centre.
- The word "fog" refers to its cloud-like properties, but closer to the "ground", i.e. IoT devices
- These days, fog computing tends to be amalgamated with edge computing

Cloud computing

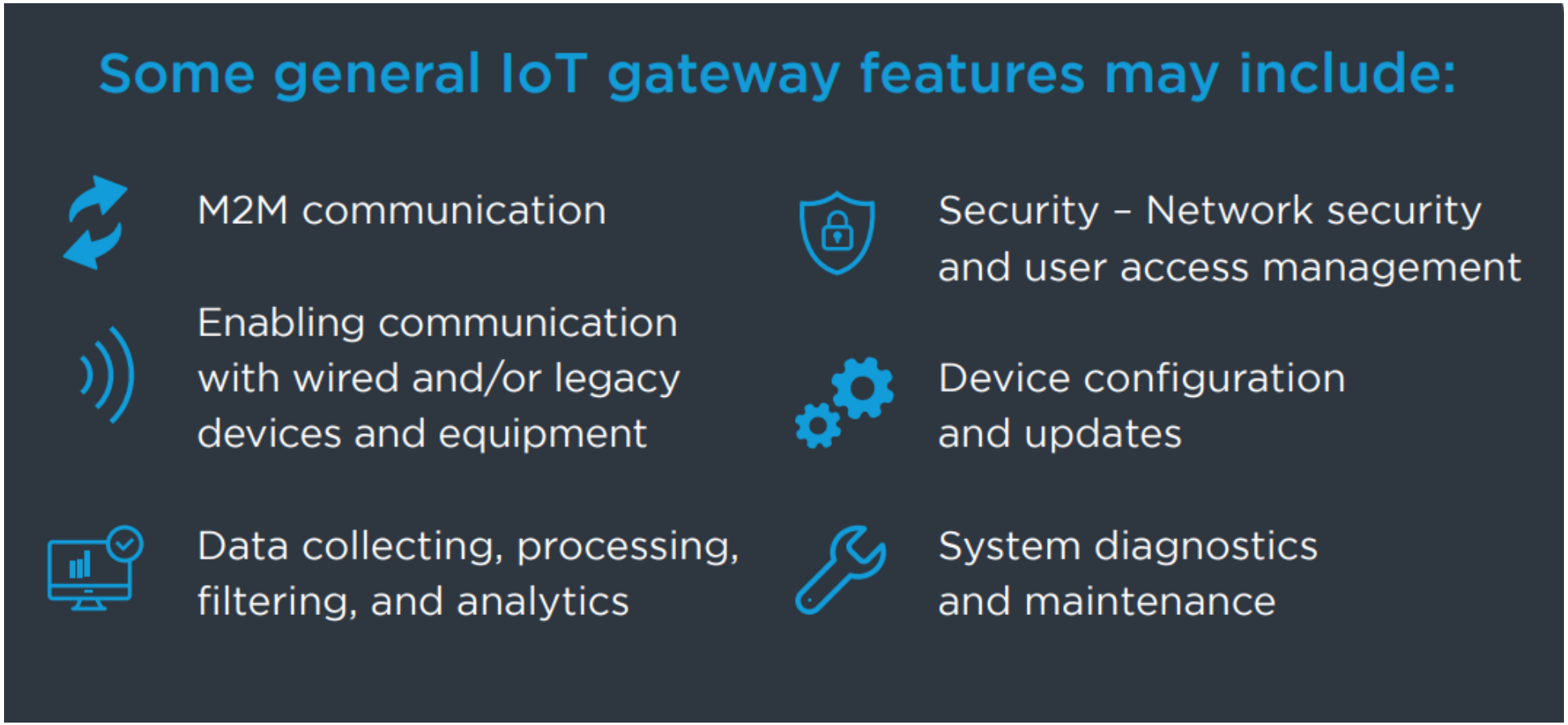
- Cloud computing offers on-demand availability of computing resources as services over the internet.
- It eliminates the need for enterprises to procure, configure, or manage resources themselves, and they only pay for what they use.
- It is flexible, efficient, secure, cost effective and offers strategic value.
- The cloud – the brain centre – in the IoT system provides a resource for the collection, storage, and analysis of the data outside the internal network.
- **Advantage:** frees up space and lowers workload, decreases the monetary investment for internal IoT system equipment and upgrades, and allows for much simpler and realistic scalability.
- **Challenge:** transferring all this data from an internal system to the cloud.

IoT gateway



- a gateway is a hardware device that contains application software capable of performing required tasks for IoT communication whether it involves device-to-device or device-to-cloud interactions.
- A gateway may include many integrated technologies such as Bluetooth 5, 802.11ac MU-MIMO Wi-Fi, and Hardware Root of Trust.
- Utilizing a gateway for IoT monitoring systems can simplify, secure, and enhance the performance of critical IoT systems.

IoT gateway features



IOT gateway challenges

- **Objective:** to connect to the internet and transfer data to the cloud using a method that is both efficient and secure.
- Reliable network connections can be threatened by
  - security concerns
  - high data costs
  - proprietary and other varying protocols
  - the critical need for real-time requirements
  - tough wireless conditions
  - existence of out-of-date and/or wired legacy equipment
  - connectivity is complicated
- The use of an IoT gateway addresses and mitigates many of these challenges.

Potential Challenges with IoT Gateways

- Transferring data from a single sensor to the cloud is easy but when faced with the need for scalability, gateways may be necessary between the sensors and the cloud.
- Security
- Computational needs
- Filtering out unnecessary data
- Establish connectivity between differing technologies, devices and protocols

Smart IoT gateway

- A smart gateway is an IoT gateway that incorporates the capabilities of edge computing.
- Using a smart gateway allows for more computing to take place at the edge.
- Rather than sending directly to the cloud every packet of data from every connected sensor in the IoT network, the sensors instead deliver data to the gateway.
- The gateway then analyses the data and only sends to the cloud essential data and/or data that requires additional analysis or action.
- Considering that IoT systems can be made up of hundreds of thousands or more individual sensors, gateways and edge computing help distribute the data processing burden.
- With a smart IoT gateway, full intelligence is not required at each connected sensor or device
- Remember: edge computing refers to any computing that occurs before the data is delivered to the cloud.

Smart IoT gateway offers reduced latency

- Latency refers to how much of a delay occurs when sending information from one device to another.
- When utilizing a cloud-based IoT system, latency can be a significant issue.
- With edge computing and a smart gateway, data does not need to be sent to the cloud to be acted upon. The gateway itself can act locally on the data it receives which enables nearly real-time responses.
- Example: use case of a hospital or warehouse setting where the workers use badges to log or scan their work hours. During a shift change of many employees, the gateway can receive and process the data locally and only then transfer the information to the cloud, if necessary.

Smart IoT gateway offers improved availability

With a smart gateway and edge computing, the gateway itself can

- collect,
- process,
- store, and
- act on data internally even when there is no internet connection.

Once the system is back online, the gateway can then synchronize the data between the sensors and the cloud service.

- It can be suitable for applications where loss of internet is critical.

Examples of IoT applications and availability

Example 1: consider a hospital setting where health monitoring equipment tracks patients and acts upon the information as needed.

- A life-critical setup like this must be able to operate offline when necessary.
- If there is a disruption in the internet connection, healthcare workers must be confident that the equipment will continue to function effectively.

Example 2: retail stores rely on their POS systems to be available the entire time their store is open to customers.

- For areas that suffer with unreliable internet connections, this could be an issue and could potentially affect their sales.

SOLUTION: develop software in the gateways for specific functions which can be executed locally:

- gateways to manage their connected sensors without disruption even when an internet connection is not available.
- down-time caused by internet disruptions are expensive, but using IoT gateways in this manner reduces operating costs.

Smart IoT gateway offers centralised network management

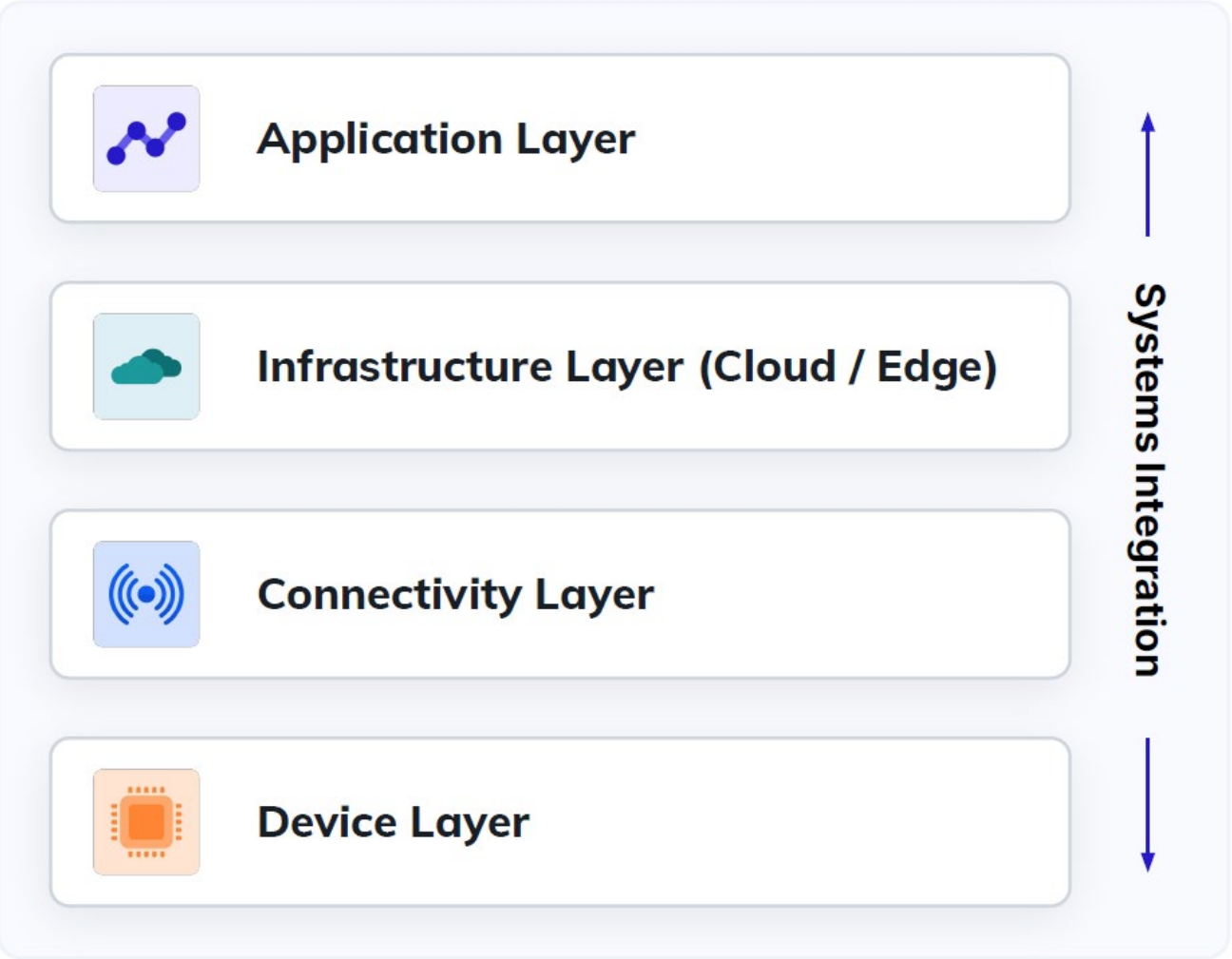
- By creating a centralized system, those responsible for the operation and maintenance of the sensors can manage the sensors as a whole rather than individually.
- This applies to firmware upgrades and the configuration of new sensors and devices, both of which can be done remotely over-the-air (OTA) once initiated by the gateway.
- This method also generates cost savings.
  - When uploading data to the cloud via the internet, you need a data plan.
  - When uploading data to the cloud from a lot of different sensors, you'd need a lot of individual data plans.
  - The ability to complete this via a single gateway (a single data plan) eliminates many of these operational costs.

Smart IoT gateway offers security

- A reliable system provides encryption and authentication for communications between a gateway and its associated sensors as well as between the gateway and the cloud.
- With these protections in place, an IoT gateway can relay security tools (such as firmware updates and patches from the cloud to all sensors at one time.

IoT system deployment

- An IoT system is ready to be deployed only when all four layers are seamlessly integrated together.
- All four layers are secure.



Summary

- Keep in mind the various models and layers
- The 4-layered reference architecture model
- Core IoT functional stack and data management stack
- Edge computing, cloud computing, IoT gateways