# Module 3

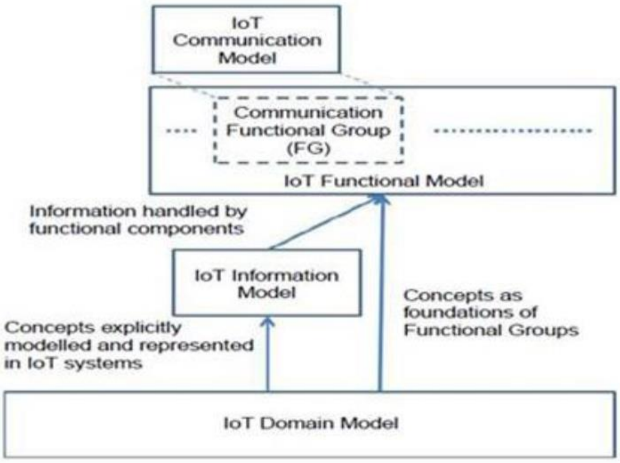
## Architecture reference model in IoT

An Architecture Reference Model (ARM) is divided into two main parts:

Reference model and Reference architecture.

-----------------------------------------------------------------------------------------------------------------------------

### 1] Reference Model


IoT Communication Model
Communication Functional Group (FG)
IoT Functional Model
Information handled by functional components
IoT Information Model
Concepts as foundations of Functional Groups
Concepts explicitly modelled and represented in IoT systems
IoT Domain Model

**1. Domain Model:**

1. The domain model captures the basic attributes of the main concepts and the relationship between these concepts.
2. The domain model is an important part of any reference model since it includes a definition of the main abstract concepts (abstractions), their responsibilities, and their relationships.
3. Based on the IoT Domain Model, the IoT Information Model, Functional Model and Communication Model has been developed.

**2. Information Model:**

1. The Information Model is derived from the IoT domain model and focuses on capturing and processing information about the main entities and their interactions within the IoT system.
2. It defines the structure, attributes, and relationships of the information that flows within the system.
3. The Information Model helps in understanding the data requirements, data formats, and data flows within the IoT system.

**3. Functional Model:**

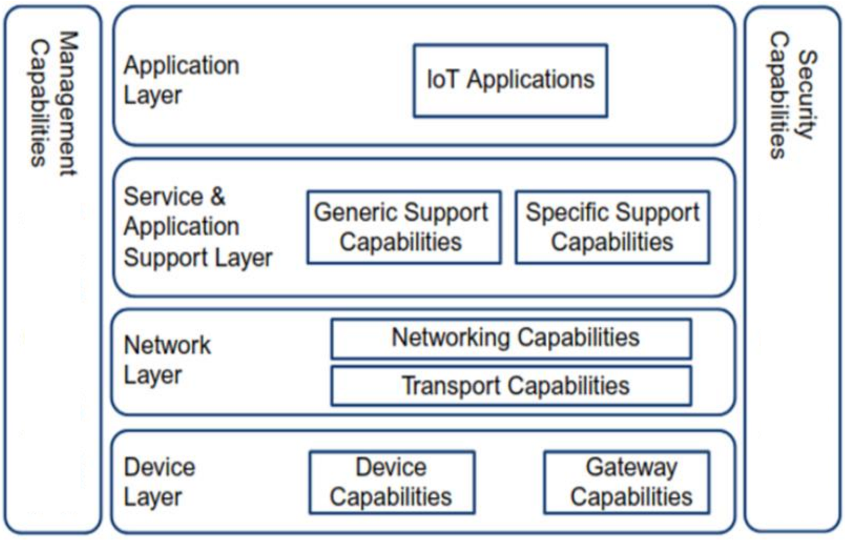
1. The Functional Model describes the concepts and entities specific to the working system or application within the IoT domain.
2. It identifies the functions, capabilities, and operations that the IoT system needs to perform to achieve its objectives.
3. The Functional Model focuses on the behavior and functionality of the system, including how it interacts with the entities defined in the Information Model.

**4. Communication Model:**

1. The Communication Model captures the communication interactions between the entities within an IoT system.
2. It defines the protocols, messaging formats, communication patterns, and technologies used for communication between devices, sensors, gateways, and other components.
3. The Communication Model ensures that the IoT system's entities can exchange information effectively and reliably

--------------------------------------------------------------------------------------------------------------------------------

**2] Reference architecture**



**1. Device Layer:**

1. Includes physical devices and sensors that collect data or interact with the physical world.
2. Examples include temperature sensors, cameras, smart appliances, and wearable devices.
3. Acts as the foundation for data collection and physical interaction.

**2. Network Layer:**

1. Handles communication between devices and the rest of the IoT system.
2. Utilizes communication protocols such as Wi-Fi, Bluetooth, Zigbee, and cellular networks.
3. Enables data exchange between devices, gateways, and cloud platforms.

**3. Application Layer:**

1. Hosts software applications that process and use data collected from IoT devices.
2. Provides insights, automation, and control functionalities based on the data.
3. Includes user interfaces such as dashboards, alert systems, and control panels.

**4. Service Layer:**

1. Focuses on providing IoT-related services to end users and businesses.
2. Leverages IoT data to create value through data analytics, predictive maintenance, and automation.
3. Helps achieve business goals and improve user experiences.

**5. Management Layer:**

1. Provides tools for monitoring, configuration, and maintenance of the IoT system.
2. Ensures smooth operation and performance of the IoT infrastructure.
3. Includes firmware updates, device management, and resource provisioning.

**6. Security Layer:**

1. Spans all other layers, ensuring data and device confidentiality, integrity, and availability.
2. Incorporates encryption, authentication, and access control mechanisms.
3. Protects the IoT system from threats and unauthorized access.