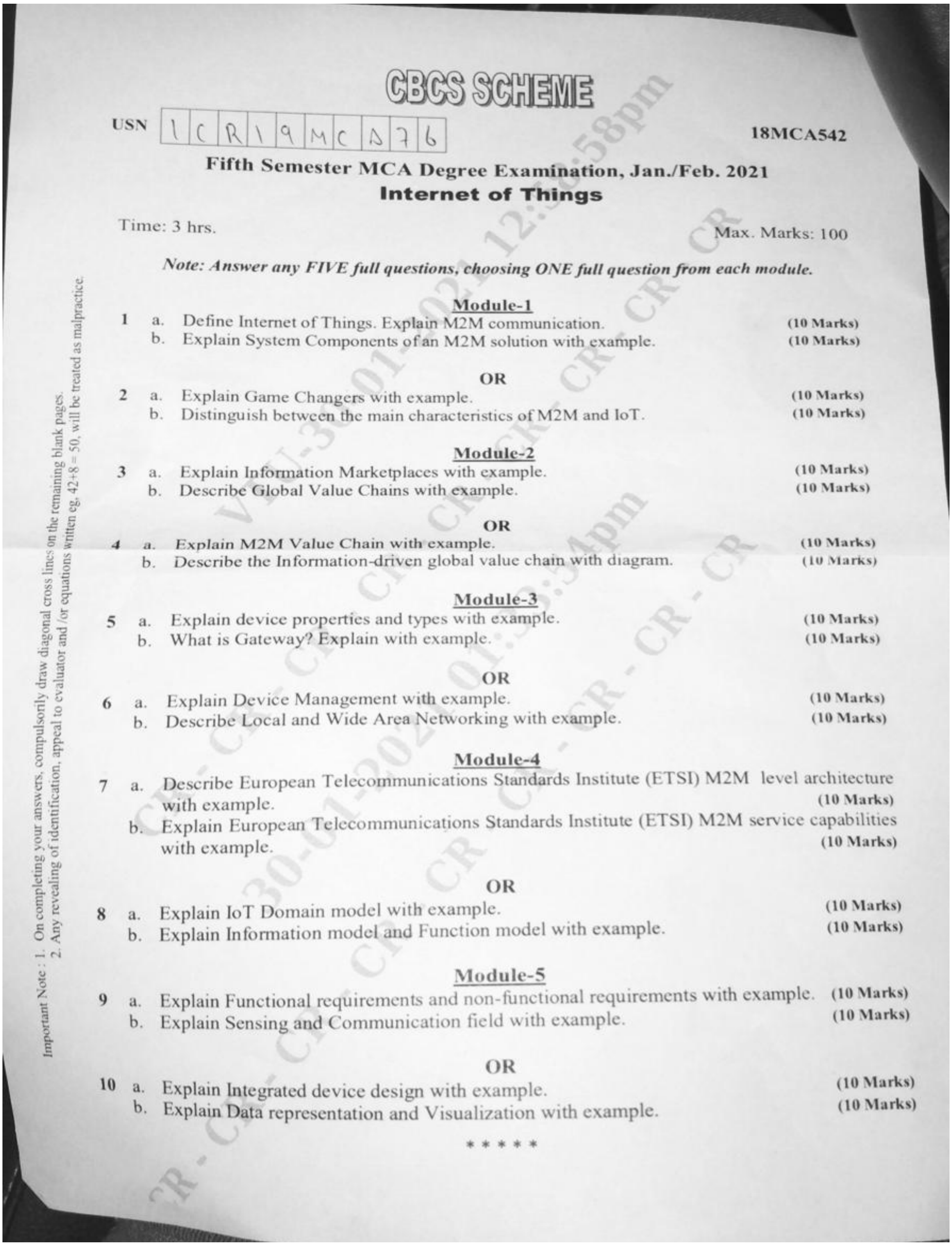
VTU MCA DEGREE EXAMINATION Jan/Feb 2021
INTERNET OF THINGS



CBCS SCHEME

USN 1CR19MCA76

18MCA542

Fifth Semester MCA Degree Examination, Jan./Feb. 2021

Internet of Things

Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

Module-1

1 a. Define Internet of Things. Explain M2M communication. (10 Marks)
b. Explain System Components of an M2M solution with example. (10 Marks)

OR

2 a. Explain Game Changers with example. (10 Marks)
b. Distinguish between the main characteristics of M2M and IoT. (10 Marks)

Module-2

3 a. Explain Information Marketplaces with example. (10 Marks)
b. Describe Global Value Chains with example. (10 Marks)

OR

4 a. Explain M2M Value Chain with example. (10 Marks)
b. Describe the Information-driven global value chain with diagram. (10 Marks)

Module-3

5 a. Explain device properties and types with example. (10 Marks)
b. What is Gateway? Explain with example. (10 Marks)

OR

6 a. Explain Device Management with example. (10 Marks)
b. Describe Local and Wide Area Networking with example. (10 Marks)

Module-4

7 a. Describe European Telecommunications Standards Institute (ETSI) M2M level architecture with example. (10 Marks)
b. Explain European Telecommunications Standards Institute (ETSI) M2M service capabilities with example. (10 Marks)

OR

8 a. Explain IoT Domain model with example. (10 Marks)
b. Explain Information model and Function model with example. (10 Marks)

Module-5

9 a. Explain Functional requirements and non-functional requirements with example. (10 Marks)
b. Explain Sensing and Communication field with example. (10 Marks)

OR

10 a. Explain Integrated device design with example. (10 Marks)
b. Explain Data representation and Visualization with example. (10 Marks)

* * * * *

1. Define internet of things. Explain M2M Communication 10M

The **Internet of Things** (**IoT**) is the network of physical devices embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect and exchange data

□ The IoT is a widely used term for a set of technologies, systems, and design principles associated with the emerging wave of Internet-connected things that are based on the physical environment
□ IoT also refers to the connection of such systems and sensors to the broader Internet, as well as the use of general Internet technologies b) With the diagram, Discuss IoT and its emerging applications.

M2M refers to those solutions that allow communication between devices of the same type and a specific application, all via wired or wireless communication networks.
□ M2M solutions allow end-users to capture data about events from assets, such as temperature or inventory levels.
□ M2M is deployed to achieve
o productivity gains,
o reduce costs, and
o increase safety or security.
□ M2M has been applied in many different scenarios, including the remote monitoring and control of enterprise assets, or to provide connectivity of remote machine type devices.
□ Remote monitoring and control has generally provided the incentive for industrial applications, whereas connectivity has been the focus in other enterprise scenarios such as connected vending machines or point-of-sales terminals for online credit card transactions. □ M2M solutions, however, do not generally allow for the broad sharing of data or connection of the devices in question directly to the Internet.
1.b) Explain system components of an M2M solution with example
A typical M2M system solution consists of
o M2M devices
o communication networks that provide remote connectivity for the devices,
o service enablement, application logic,
o Integration of the M2M application into the business processes provided by an Information Technology (IT) illustrated in the below figure 1.1

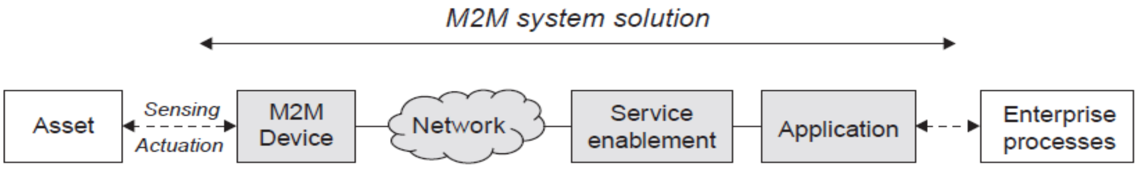


FIGURE 2.1
A generic M2M system solution.

The M2M system solution is used to remotely monitor and control enterprise assets of various kinds, and to integrate those assets into the business processes of the enterprise in question. The asset can be of a wide range of types (e.g. vehicle, freight container, building, or smart electricity meter), all depending on the enterprise.
The system components of an M2M solution are as follows:
o ***M2M Device***. This is the M2M device attached to the asset of interest and provides sensing and actuation capabilities. The M2M device is here generalized, as there are a number of different realizations of these devices, ranging from low-end sensor nodes to high-end complex devices with multimodal sensing capabilities.
o ***Network***. The purpose of the network is to provide remote connectivity between the M2M device and the application-side servers. Many different network types can be used and include both Wide Area Networks (WANs) and Local Area Networks (LANs). Examples of WANs are public cellular mobile networks, fixed private networks, or even satellite links.
o ***M2M Service Enablement***. Within the generalized system solution outlined above, the concept of a separate service enablement component is also introduced. This component provides generic functionality that is common across a number of different applications. Its primary purpose is to reduce cost for implementation and ease of application development.

o ***M2M Application***. The application component of the solution is a realization of the highly specific monitor and control process. The application is further integrated into the overall business process system of the enterprise. The process of remotely monitoring and controlling assets can be of many different types, for instance, remote car diagnostics or electricity meter data management.

2a) explain Games changers with example

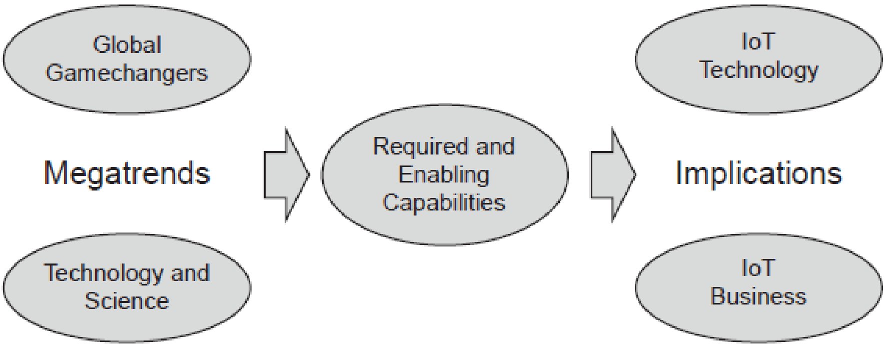


FIGURE 2.5

Megatrends, capabilities, and implications.

The game changers come from a set of social, economic, and environmental shifts that create pressure for solutions to address issues and problems, but also opportunities to reformulate the manner in which our world faces them.

 There is an extremely strong emerging demand for monitoring, controlling, and understanding the physical world, and the game changers are working in conjunction with technological and scientific advances.

 The transition from M2M towards IoT is one of the key facets of the technology evolution required to face these challenges.

 Some of the global significant game changers

o Natural Resource Constraint

 The world needs to increasingly do more with less, from raw materialsto energy, water or food, the growing global population and associated economic growth demands put increasing constraints on the use of resources. The use of IoT to increase yields, improve productivity, and decrease loss across global supply chains is therefore escalating.

o Economic Shifts

 The overall economy is in a state of flux as it moves from the post- industrial era to a digital economy. One example of this is found in the move from product-oriented to service-oriented economies

o Changing Demographics

 Many countries will need to deal with an aging population without increasing economic expenditure. As a result, IoT will need to be used, for example, to help provide assisted living and reduce costs in healthcare and emerging “wellcare” systems.

o Socioeconomic Expectations

 Lifestyle and convenience will be increasingly enabled by technology as the same disruption and efficiency practices evident in industries will be applied within people’s lives and homes as well.

o Climate Change and Environment Impacts

 The impact of human activities on the environment and climate has been long debated, but is now in essence scientifically proven. Technology, including IoT, will need to be applied to aggressively reduce the impact of human activity on the earth’s systems.

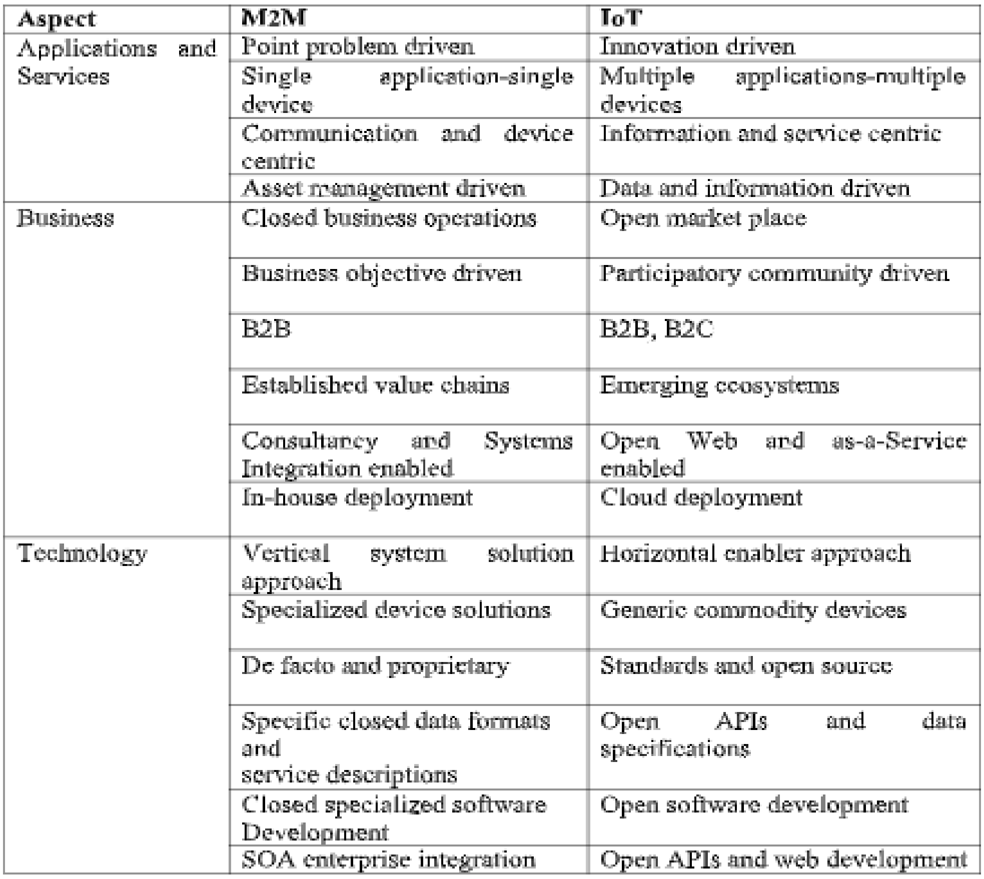
o Safety and Security

 Public safety and national security becomes more urgent as society becomes more advanced, but also more vulnerable. This has to do both with reducing fatalities and health as well as crime prevention, and different technologies can address a number of the issues at hand

o Urbanization

 Urbanization creates an entirely new level of demands on city infrastructures in order to support increasing urban populations. IoT technologies will play a central role in the optimization for citizens and enterprises within the urban realm, as well as providing increased support for decision-makers in cities.

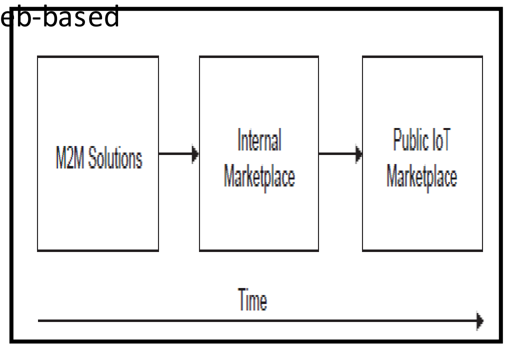
2.a) Distinguish between the main characteristics of M2M and IOT



Aspect	M2M	IoT
Applications and Services	Point problem driven	Innovation driven
	Single application-single device	Multiple applications-multiple devices
	Communication and device centric	Information and service centric
	Asset management driven	Data and information driven
Business	Closed business operations	Open market place
	Business objective driven	Participatory community driven
	B2B	B2B, B2C
	Established value chains	Emerging ecosystems
	Consultancy and Systems Integration enabled	Open Web and as-a-Service enabled
	In-house deployment	Cloud deployment
Technology	Vertical system solution approach	Horizontal enabler approach
	Specialized device solutions	Generic commodity devices
	De facto and proprietary	Standards and open source
	Specific closed data formats and service descriptions	Open APIs and data specifications
	Closed specialized software Development	Open software development
	SOA enterprise integration	Open APIs and web development

3.a) Explain information marketplace with example

- A key aspect to note between M2M and IoT is that the technology used for these solutions may be very similar they may even use the same base components but the manner in which the data is managed will be different.
- In an M2M solution, data remains within strict boundaries it is used solely for the purpose that it was originally developed for.
- With IoT, however, data may be used and reused for many different purposes, perhaps beyond the original intended design, thanks to web-based technologies.
- Data can be shared between companies and value chains in internal information marketplaces. Alternatively, data could be publicly exchanged on a public information marketplace is as shown in figure 2.1



3.b) Describe Global value chains with example

A value chain describes the full range of activities that firms and workers perform to bring a product from its conception to end use and beyond, including design, production, marketing, distribution, and support to the final consumer.

A simplified value chain is illustrated in Figure 2.2; it is comprised of five separate activities that work together to create a finalized product.

These activities may be contained within a single firm or divided among different firms.

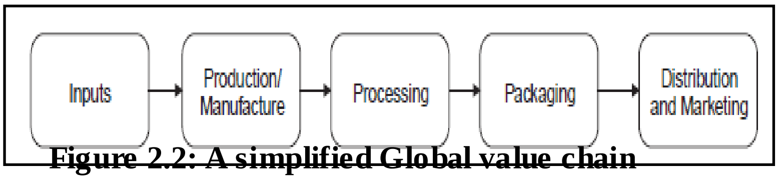


Figure 2.2: A simplified Global value chain

4.a) Explain M2M value chain with example

M2M value chains are internal to one company and cover one solution.

Let us consider **Figure 2.2,** let's take a look at the inputs and outputs of an M2M value chain. **Inputs:** Inputs are the base raw ingredients that are turned into a product. Examples could be cocoa beans for the manufacture of chocolate or data from an M2M device that will be turned into a piece of information.

Production/Manufacture: Production/Manufacture refers to the process that the raw inputs are put through to become part of a value chain. For example, cocoa beans may be dried and separated before being transported to overseas markets.

Processing: Processing refers to the process whereby a product is prepared for sale. For example, cocoa beans may now be made into cocoa powder, ready for use in chocolate bars. For an M2M solution, this refers to the aggregation of multiple data sources to create an information component _ something that is ready to be combined with other data sets to make it useful for corporate decision-making.

Packaging: Packaging refers to the process whereby a product can be branded as would be recognizable to end-user consumers. For example, a chocolate bar would now be ready to eat and have a red wrapper with the words "KitKatt" on it. For M2M solutions, the data will have to be combined with other information from internal corporate databases, for example, to see whether the data received requires any action. This data would be recognizable to the end-users that need to use the information, either in the form of visualizations or an Excel spreadsheet.

Distribution/Marketing: This process refers to the channels to market for products. For example, a chocolate bar may be sold at a supermarket, a kiosk, or even online. An M2M solution, however, will have produced an Information Product that can be used to create new knowledge within a corporate environment examples include more detailed scheduling of maintenance based on real-world information or improved product design due to feedback from the M2M solution

4. b) Describe the information driven global value chain with example

There are five fundamental roles within the I-GVC that companies and other actors are forming around, illustrated in Figure 2.5

- Inputs:
  - Sensors, RFID, and other devices.
  - End-Users.
- Data Factories.
- Service Providers/Data Wholesalers.
- Intermediaries.
- Resellers.

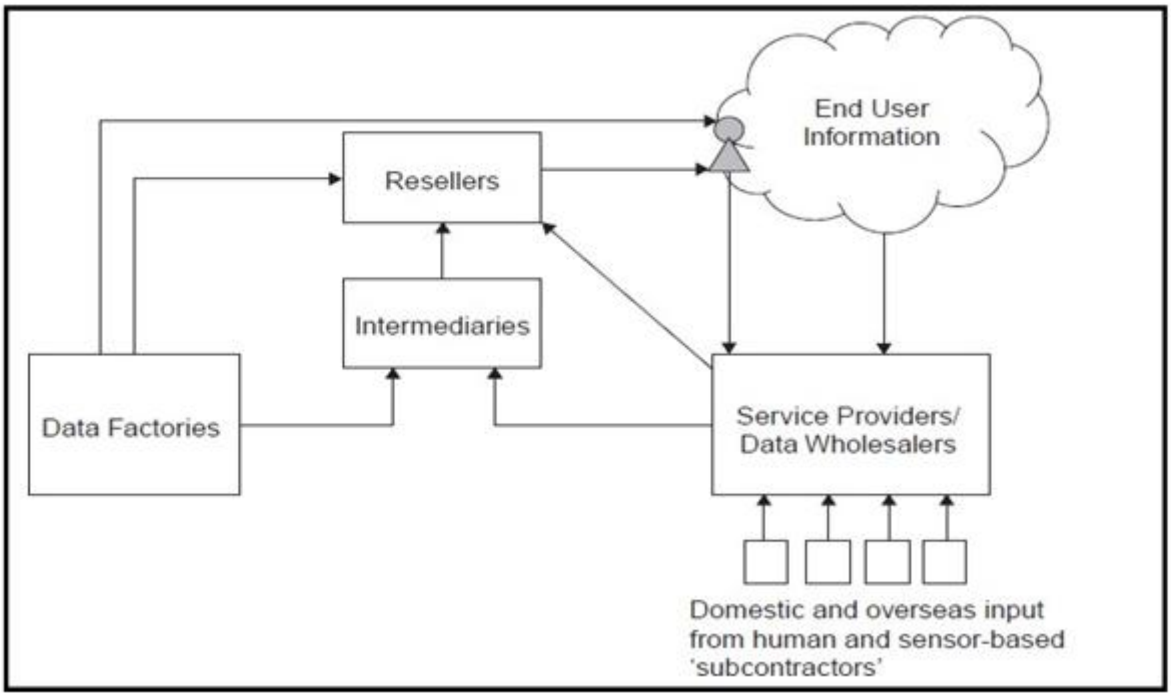

End User Information
Resellers
Intermediaries
Data Factories
Service Providers/ Data Wholesalers
Domestic and overseas input from human and sensor-based 'subcontractors'

Figure 2.5: The Information Driven Global Chain

2.5.1.1 Inputs to the information driven global commodity chain

There are two main inputs into the I-GVC:

1. Sensors and other devices (e.g. RFID and NFC).
2. End-users.

Both of these information sources input tiny amounts of data into the I-GVC chain, which are then aggregated, analyzed, repackaged, and exchanged between the different economic actors that form the value chain. As a result, sensor devices and networks, RFIDs, mobile and consumer devices, Wi-Fi hotspots, and end-users all form part of a network of "subcontractors" in the value chain.

- Sensors and Radio frequency identification

Sensors and RFID are already found in a multitude of different applications worldwide, helping to smooth supply and demand in various supply chains worldwide and gathering climate and other localized data that is then transmitted back to a centralized information processing system.

Smartphone's have also been developed that allow mobile devices to interact with sensors and RFID. This allows for a two-way interaction between a mobile terminal and the sensor technology. In this sense, the sensor networks, and NFC and RFID technologies may be viewed as subcontractors to the I-GVC, workers that constantly gather data for further processing and sale.

- End-Users

The second main inputs to the I-GVC are the end-users. Due to the convergence of the computing and mobile broadband platforms, end-users are no longer passive participants in the digital economy, with a role only to purchase those physical products that companies develop and market to them. End-users that choose to use and participate within the digital world are now deeply embedded into the very process of production.

In fact, the creation of the I-GVC would not be possible without the contribution of many millions of individuals worldwide. This is perhaps the most unique aspect of the I-GVC there is no national boundary for the contribution of humans to the I-GVC, the data about individuals can be collected from any person in any language, in almost any data format.

Every person worldwide that has to use digital technologies to do their banking, their taxes, their information searches, and to communicate with friends and colleagues, are constantly working on behalf of the I-GVC, contributing their individual profile data and knowledge to the value chain.

2.5.1.2 Production processes of the information driven global value chain-Data Factories

- Data factories are those entities that produce data in digital forms for use in other parts of the I-GVC. Previously, such data factories would create paper-based products and sell them to end-users via retailers. With the move to the digital era, however, these companies now also provide this data via digital means; for example, OS now makes maps and associated data available in digital format. For example, maps from OS can be combined with other data from travel services such as TFL to provide detailed travel applications on mobile devices.

- Service Providers/data wholesalers

Service Providers and Data wholesalers are those entities that collect data from various sources worldwide, and through the creation of massive databases, use it to either improve their own information products or sell information products in various forms. Many examples exist several well-known ones are Twitter, Facebook, Google, etc. Google “sells” its data assets through the development of extremely accurate, targeted, search-based advertising mechanisms that it is able to sell to companies wishing to reach a particular market.

- Intermediaries

In the emerging industrial structure of the I-GVC, there is a need for intermediaries that handle several aspects of the production of information products.

For example, I may happily share my personalized information about my tastes with a clothing company or music store in order to receive better service, while I may not be happy for my credit rating or tax data to be shared freely with different companies. I would therefore allow an intermediary to act on my behalf, tagging the relevant information in some form to ensure that it was not used in a manner that I had not previously agreed to.

Another reason for an intermediary of this nature is to reduce transaction costs associated with the establishment of a market for many different companies to participate in.

- Resellers

Resellers are those entities that combine inputs from several different intermediaries, combine it together, analyze, and sell it to either end-users or to corporate entities. These resellers are currently rather limited in terms of the data that they are able to easily access via the converged communications platform, but they are indicative of the types of corporate entities that are forming within this space.

5a) Explain device properties and types with example

Basic Devices: Devices that only provide the basic services of sensor readings and/or actuation tasks, and in some cases limited support for user interaction. LAN communication is supported via wired or wireless technology, thus a gateway is needed to provide the WAN connection.

- These devices are often intended for a single purpose, such as measuring air pressure or closing a valve. In some cases several functions are deployed on the same device, such as monitoring humidity, temperature, and light level.
- The requirements on hardware are low, both in terms of processing power and memory.
- The main focus is on keeping the bill of materials (BOM) as low as possible by using inexpensive microcontrollers with built-in memory and storage, often on an SoC-integrated circuit with all main components on one single chip(Figure 3.1)

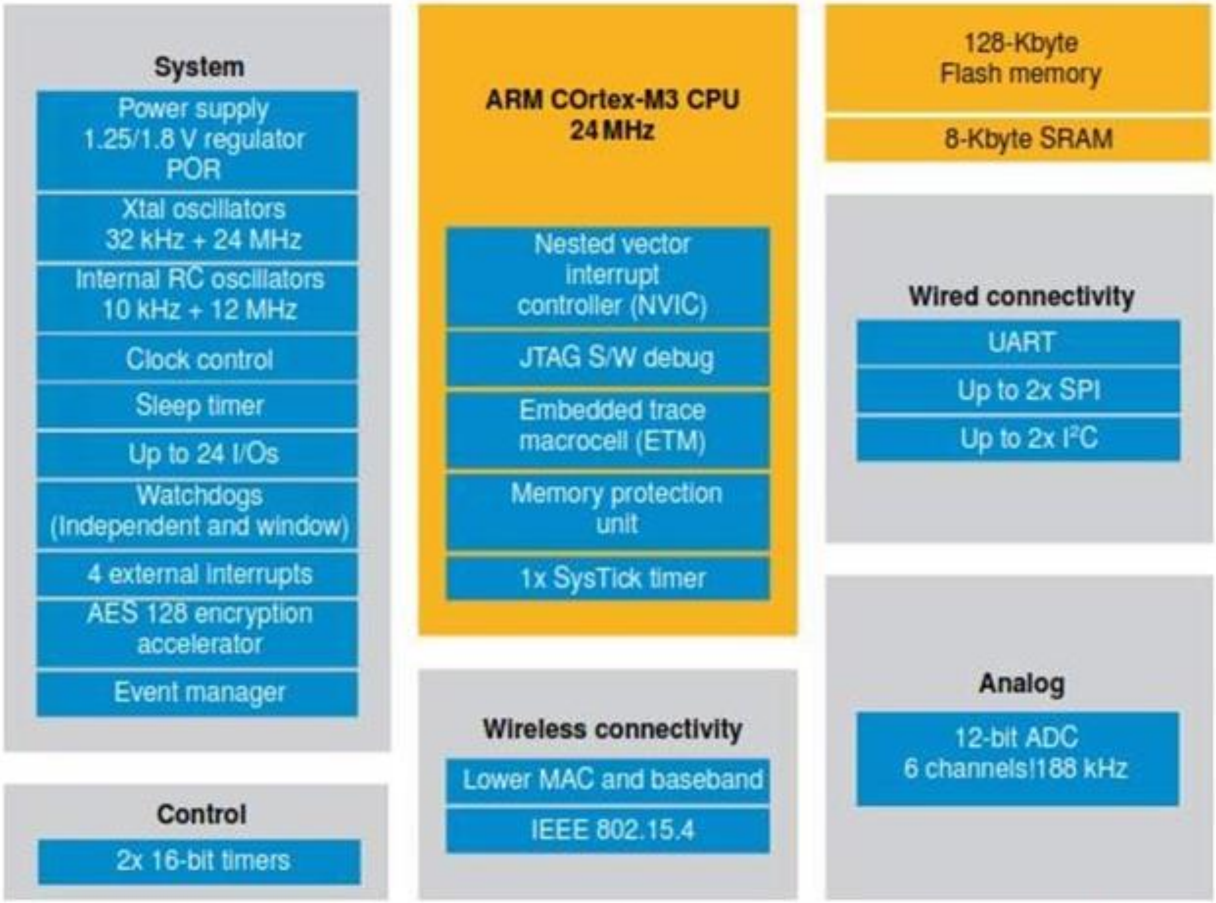


Figure 3.1 Example of a microcontroller with integrated STM32W-RFCKIT.

Advanced Devices: In this case the devices also host the application logic and a WAN connection. They may also feature device management and an execution environment for hosting multiple applications. Gateway devices are most likely to fall into this category.

- A powerful CPU or microcontroller with enough memory and storage to host advanced applications, such as a printer offering functions for copying, faxing, printing, and remote management.
- A more advanced user interface with, for example, display and advanced user input in the form of a keypad or touch screen.
- Video or other high bandwidth functions.

5b) What is Gateway? Explain with example

3.1.2 Gateways

- A gateway serves as a translator between different protocols, e.g. between IEEE 802.15.4 or IEEE 802.11, to Ethernet or cellular.
- There are many different types of gateways, which can work on different levels in the protocol layers. Most often a gateway refers to a device that performs translation of the physical and link layer, but application layer gateways (ALGs) are also common. The latter is preferably avoided because it adds complexity and is a common source of error in deployments.
- Some examples of ALGs include the ZigBee Gateway Device (ZigBee Alliance 2011), which translates from ZigBee to SOAP and IP, or gateways that translate from Constrained Application Protocol (CoAP) to Hyper Text Transfer Protocol/Representational State Transfer (HTTP/REST).

- For some LAN technologies, such as 802.11 and Z-Wave, the gateway is used for inclusion and exclusion of devices.
- This typically works by activating the gateway into inclusion or exclusion mode and by pressing a button on the device to be added or removed from the network.
- For very basic gateways, the hardware is typically focused on simplicity and low cost, but frequently the gateway device is also used for many other tasks, such as data management, device management, and local applications. In these cases, more powerful hardware with GNU/Linux is commonly used.

6a) Explain device management with example

Device Management

- Device management (DM) is an essential part of the IoT and provides efficient means to perform many of the management tasks for devices:
  - **Provisioning**: Initialization (or activation) of devices in regards to configuration and features to be enabled.
  - **Device Configuration**: Management of device settings and parameters.
  - **Software Upgrades**: Installation of firmware, system software, and applications on the device.
  - **Fault Management**: Enables error reporting and access to device status
- In the simplest deployment, the devices communicate directly with the DM server. This is, however, not always optimal or even possible due to network or protocol constraints,

e.g. due to a firewall or mismatching protocols.

- In these cases, the gateway functions as mediator between the server and the devices, and can operate in three different ways:
  - If the devices are visible to the DM server, the gateway can simply forward the messages between the device and the server and is not a visible participant in the session.
  - In case the devices are not visible but understand the DM protocol in use, the gateway can act as a proxy, essentially acting as a DM server towards the device and a DM client towards the server.
  - For deployments where the devices use a different DM protocol from the server, the gateway can represent the devices and translate between the different protocols (e.g. TR-069, OMA-DM, or CoAP). The devices can be represented either as virtual devices or as part of the gateway

6b) Describe Local and wide area networking with example

- A network is created when two or more computing devices exchange data or information. The ability to exchange pieces of information using telecommunications technologies has changed the world, and will continue to do so for the foreseeable future, with applications emerging in nearly all contexts of contemporary and future living.
- Basic networking requirements have become explicit. It is essential to uniquely identify each node in the network, and it is necessary to have cooperating nodes capable of

linking nodes between which physical links do not exist. In modern computing, this equates to IP addresses and routing tables.

- Beyond the basic ability to transfer data, the speed and accuracy with which data can be transferred is of critical importance to the application. Irrespective of the ability to link devices, without the necessary bandwidth, some applications are rendered impossible.
- Consider the differences between streaming video from a surveillance camera, for example, and an intrusion-detection system based on a passive sensor.
- A Local Area Network (LAN) was traditionally distinguishable from a Wide Area Network (WAN) based on the geographic coverage requirements of the network, and the need for third party, or leased, communication infrastructure. In the case of the LAN, a smaller geographic region is covered, such as a commercial building, an office block, or a home, and does not require any leased communications infrastructure.
- WANs provide communication links that cover longer distances, such as across metropolitan, regional, or by textbook definition, global geographic areas. In practice, WANs are often used to link LANs and Metropolitan Area Networks (MAN) _ where LAN technologies cannot provide the communications ranges to otherwise interconnect _ and commonly to link LANs and devices (including smart phones, Wi-Fi routers that support LANs, tablets, and M2M devices) to the Internet. Quantitatively, LANs tended to cover distances of tens to hundreds of meters, whereas WAN links spanned tens to hundreds of kilometers.
- There are differences between the technologies that enable LANs and WANs. In the simplest case for each, these can be grouped as wired or wireless. The most popular wired LAN technology is Ethernet. Wi-Fi is the most prevalent wireless LAN (WLAN) technology.
- Wireless WAN (WWAN), as a descriptor, covers cellular mobile telecommunication networks, a significant departure from WLAN in terms of technology, coverage, network infrastructure, and architecture. The current generation of WWAN technology includes LTE (or 4G) and WiMAX.
- Considering M2M and IoT applications, there are likely to exist a combination of traditional networking approaches. The need exists to interconnect devices (generally integrated microsystems) with central data processing and decision support systems, in addition to one another. The business logic and requirements for each embodiment will differ on a case-by-case basis.
- The “Internet of Things,” as a term, originated from Radio Frequency Identification (RFID) research, wherein the original IoT concept was that any RFID-tagged “thing” could have a virtual presence on the “Internet.” In reality, there is little conceptual dissimilarity between RFID and bar codes, or more recently, QR codes _ they simply use different technological means to achieve the same result (i.e. an “object” has an online presence).
- WANs are typically required to bridge the M2M Device Domain to the backhaul network, thus providing a proxy that allows information (data, commands, etc.) to traverse heterogeneous networks. This is seen as a core requirement to provide communications services between the M2M service enablement and the physical deployments of devices in the field. Thus, the WAN is capable of providing the bi-directional communications links between services and devices. This, however, must be achieved by means of physical and logical proxy.

- The proxy is achieved using an M2M Gateway Device. Depending on the situation, there are, in general, a number of candidate technologies to select from. As before, the M2M Gateway Device is typically an integrated microsystem with multiple communications interfaces and computational capabilities. It is a critical component in the functional architecture, as it must be capable of handling all of the necessary interfacing to the M2M Service Capabilities and Management Functions.
- This device is now capable of acting as a physical proxy between the LR-WPAN, or M2M Device Domain, and the M2M Network Domain
- The Access and Core Network in the ETSI M2M Functional Architecture are foreseen to be operated by a Mobile Network Operator (MNO), and can be thought of simply as the "WAN" for the purposes of interconnecting devices and backhaul networks (Internet), thus, M2M Applications, Service Capabilities, Management Functions, and Network Management Functions.
- The WAN covers larger geographic regions using wireless (licensed and un-licensed spectra) as well as wire-based access. WAN technologies include cellular networks (using several generations of technologies), DSL, WiMAX, Wi-Fi, Ethernet, Satellite, and so forth.
- The WAN delivers a packet-based service using IP as default. However, circuit-based services can also be used in certain situations.

In the M2M context, important functions of the WAN include:

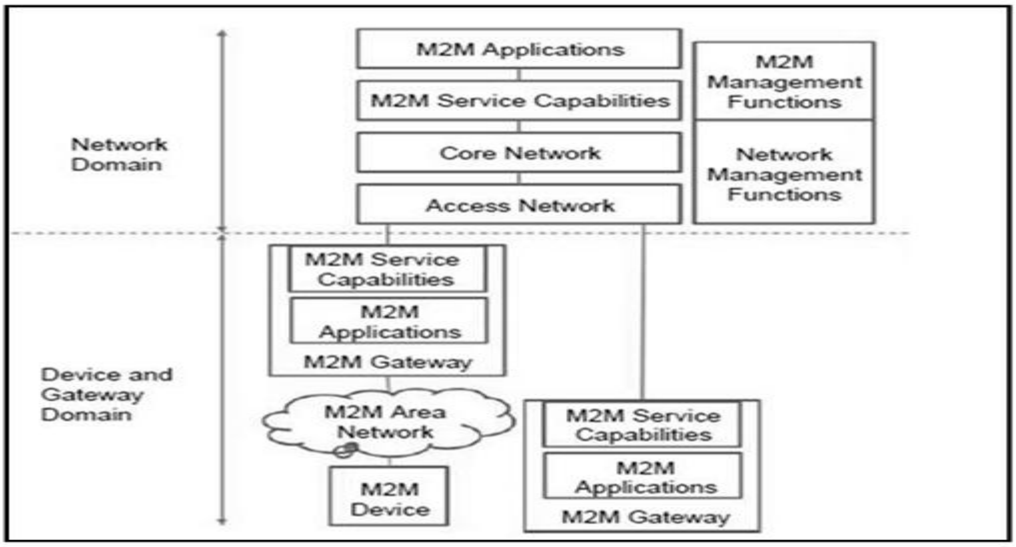
- The main function of the WAN is to establish connectivity between capillary networks, hosting sensors, and actuators, and the M2M service enablement. The default connectivity mode is packet-based using the IP family of technologies.

  Many different types of messages can be sent and received. These include messages originating as, for example, a message sent from a sensor in an M2M Area Network and resulting in an SMS received from the M2M Gateway or Application (e.g. by a relevant stakeholder with SMS notifications configure ed for when sensor readings breach particular sensing thresholds.).
- Use of identity management techniques (primarily of M2M devices) in cellular and non-cellular domains to grant right-of-use of the WAN resource.
- The following techniques are used for these purposes:
  - MCIM (Machine Communications Identity Module) for remote provisioning of SIM targeting M2M devices.
  - xSIM (x-Subscription Identity Module), like SIM, USIM, ISIM.
  - Interface identifiers, an example of which is the MAC address of the device, typically stored in hardware.
  - Authentication/registration type of functions (device focused).
  - Authentication, Authorization, and Accounting (AAA), such as RADIUS services.
  - Dynamic Host Configuration Protocol (DHCP), e.g. employing deployment- specific configuration parameters specified by device, user, or application- specific parameters residing in a directory.
  - Subscription services (device-focused).
  - Directory services, e.g. containing user profiles and various device (s) parameter(s), setting(s), and combinations thereof. M2M-specific considerations include, in particular:
  - MCIM (cf. 3GPP SA3 work).
  - User Data Management (e.g. subscription management).

- Network optimizations (cf. 3GPP SA2 work).

- There may be many suppliers of WAN functionality in a complete M2M solution. It follows that an important function in the M2M Service Enablement domain will be to manage westbound business-to-business (B2B) relations between a number of WAN service providers.

7a) describe European Telecommunication standards Institute (ETSI) M2M level architecture with example



- **M2M Device:** This is the device of interest for an M2M scenario, for example, a device with a temperature sensor. An M2M Device contains M2M Applications and M2M Service Capabilities. An M2M device connects to the Network Domain either directly or through an M2M Gateway:
  - Direct connection: The M2M Device is capable of performing registration, authentication, authorization, management, and provisioning to the Network Domain. Direct connection also means that the M2M device contains the appropriate physical layer to be able to communicate with the Access Network.

  Through one or more M2M Gateway: This is the case when the M2M device does not have the appropriate physical layer, compatible with the Access Network technology, and therefore it needs a network domain proxy. Moreover, a number of M2M devices may form their own local M2M Area Network that typically employs a different networking technology from the Access Network. The M2M Gateway acts as a proxy for the Network Domain and performs the procedures of authentication, authorization, management, and provisioning. An M2M Device could connect through multiple M2M Gateways.
- **M2M Area Network:** This is typically a local area network (LAN) or a Personal Area Network (PAN) and provides connectivity between M2M Devices and M2M Gateways. Typical networking technologies are IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee, IETF 6LoWPAN/ROLL/CoRE), MBUS, KNX (wired or wireless) PLC, etc.
- **M2M Gateway:** The device that provides connectivity for M2M Devices in an M2M Area Network towards the Network Domain. The M2M Gateway contains M2M Applications and M2M Service Capabilities. The M2M Gateway may also provide services to other legacy devices that are not visible to the Network Domain. The Network Domain contains the following functional/topological entities:
- **Access Network**: this is the network that allows the devices in the Device and Gateway Domain to communicate with the Core Network. Example Access Network Technologies are fixed (xDSL, HFC) and wireless (Satellite, GERAN, UTRAN, E-UTRAN W-LAN, WiMAX).
- **Core Network:** Examples of Core Networks are 3GPP Core Network and ETSI TISPAN Core Network. It provides the following functions:

- IP connectivity.
- Service and Network control.
- Interconnection with other networks.
- Roaming.

- **M2M Service Capabilities:** These are functions exposed to different M2M Applications through a set of open interfaces. These functions use underlying Core Network functions, and their objective is to abstract the network functions for the sake of simpler applications. More details about the specific service capabilities are provided later in the chapter.
- **M2M Applications:** These are the specific M2M applications (e.g. smart metering) that utilize the M2M Service Capabilities through the open interfaces.
- **Network Management Functions:** These are all the necessary functions to manage the Access and Core Network (e.g. Provisioning, Fault Management, etc.).
- **M2M Management Functions:** These are the necessary functions required to manage the M2M Service Capabilities on the Network Domain while the management of an M2M Device or Gateway is performed by specific M2M Service Capabilities. There are two M2M Management functions:
- **M2M Service Bootstrap Function (MSBF):** The MSBF facilitates the bootstrapping of permanent M2M service layer security credentials in the M2M Device or Gateway and the M2M Service Capabilities in the Network Domain. In the Network Service Capabilities Layer, the Bootstrap procedures perform, among other procedures, provisioning of an M2M Root Key (secret key) to the M2M Device or Gateway and the M2M Authentication Server (MAS).
- **M2M Authentication Server (MAS):** This is the safe execution environment where permanent security credentials such as the M2M Root Key are stored. Any security credentials established on the M2M Device or Gateway are stored in a secure environment such as a trusted platform module.

7b) Explain ETSI M2M Service capabilities with example

4.2.1.1 ETSI M2M service capabilities

All the possible Service Capabilities (where "x" is Network, Gateway, and Device are shown in Figure 4.3:

1. Application Enablement (xAE). The xAE service capability is an application facing functionality and typically provides the implementation of the respective interface: NAE implements the mIa interface and the GAE and DAE implement the dIa interface.The xAE includes registration of applications (xA) to the respective xSCL; for example, a Network Application towards the NSCL.

2. **Generic Communication (xGC).** The NGC is the single point of contact for communication towards the GSCL and DSCL. It provides transport session establishment and negotiation of security mechanisms, potentially secure transmission of messages, and reporting of errors such as transmission errors. The GSC/DSC is the single point of contact for communication with the NSCL, and they both perform similar operations to the NGC (e.g. secure message transmissions to NSCL). The GSC performs a few more functions such as relaying of messages to/from NSCL from/to other SCs in the GSCL, and handles name resolution for the requests within the M2M Area Network.
3. **Reachability, Addressing, and Repository (xRAR).**
   This is one of the main service capabilities of the ETSI M2M architecture. The NRAR hosts mappings of M2M Device and Gateway names to reachability information, and scheduling information relating to reachability, such as whether an M2M Device is reachable between 10 and 11 o'clock.

- It provides group management (creation/update/deletion) for groups of M2M

Devices and Gateways,stores application (DA, GA, NA) data, and manages subscriptions to these data, stores registration information for NA, GSCL, and DSCL,and manages events (subscription notifications).

- The GRAR provides similar functionality to the NRAR, such as maintaining mappings of the names of M2M Devices or groups to reachability information (routable addresses, reachability status, and reachability scheduling),storing DA, GA, NSCL registration information, storing DA, GA, NA,GSCL, NSCL data and managing subscriptions about them, managing groups of M2M Devices, and managing events. Similar to NRAR and GRAR, the DRAR stores DA, GA, NA, DSCL, and NSCL data and manages subscriptions about these data, stores DA registration and NSCL information, provides group management for groups of M2M Devices and event management.

4. **Communication Selection (xCS):** This capability allows each xSCL to select the best possible communication network when there is more than one choice or when the current choice becomes unavailable due to communication errors. The NCS provides such a selection mechanism based on policies for reaching an M2M Device or Gateway, while the GCS/DCS provides a similar selection mechanism for reaching the NSCL.
5. **Remote Entity Management (xREM)**
   - The NREM provides management capabilities such as Configuration Management (CM) for M2M Devices and Gateways (e.g. installs management objects in device and gateways), collects performance management (PM) and Fault Management (FM) data and provides them to NAs or M2M Management Functions, performs device management to M2M Devices and Gateways such as firmware and software (application,SCL software) updates, device configuration, and M2M Area Network configuration.
   - The GREM acts as a management client for performing management operations to devices using the DREM and a remote proxy for NREM to perform management operations to M2M Devices in the M2M Area Network. Examples of proxy operations are mediation of NREM-initiated software updates, and handling management data flows from NREM to sleeping M2M Devices.The DREM provides the CM, PM, and FM counterpart on the device (e.g. start collecting radio link performance data) and provides the device-side software and firmware update support.

6. **SECurity (xSEC).** These capabilities provide security mechanisms such as M2M Service Bootstrap, key management, mutual authentication,and key agreement (NSEC performs mutual authentication and key agreement while the GSEC and DESC initiate the procedures), and potential platform integrity mechanisms.
7. **History and Data Retention (xHDR).** The xHDR capabilities are optional capabilities, in other words, they are deployed when required by operator policies. These capabilities provide data retention support to other xSCL capabilities (which data to retain) as well as messages exchanged over the respective reference points.
8. **Transaction Management (xTM).** This set of capabilities is optional and provides support for atomic transactions of multiple operations.

An atomic transaction involves three steps:

(a) propagation of a request to a number of recipients

(b) collection of responses, and

(c) commitment or roll back whether all the transactions successfully completed or not.

9. **Compensation Broker (xCB).** This capability is optional and provides support for brokering M2M-related requests and compensation between a Customer and a Service Provider. In this context a Customer and a Service Provider is an M2M Application.

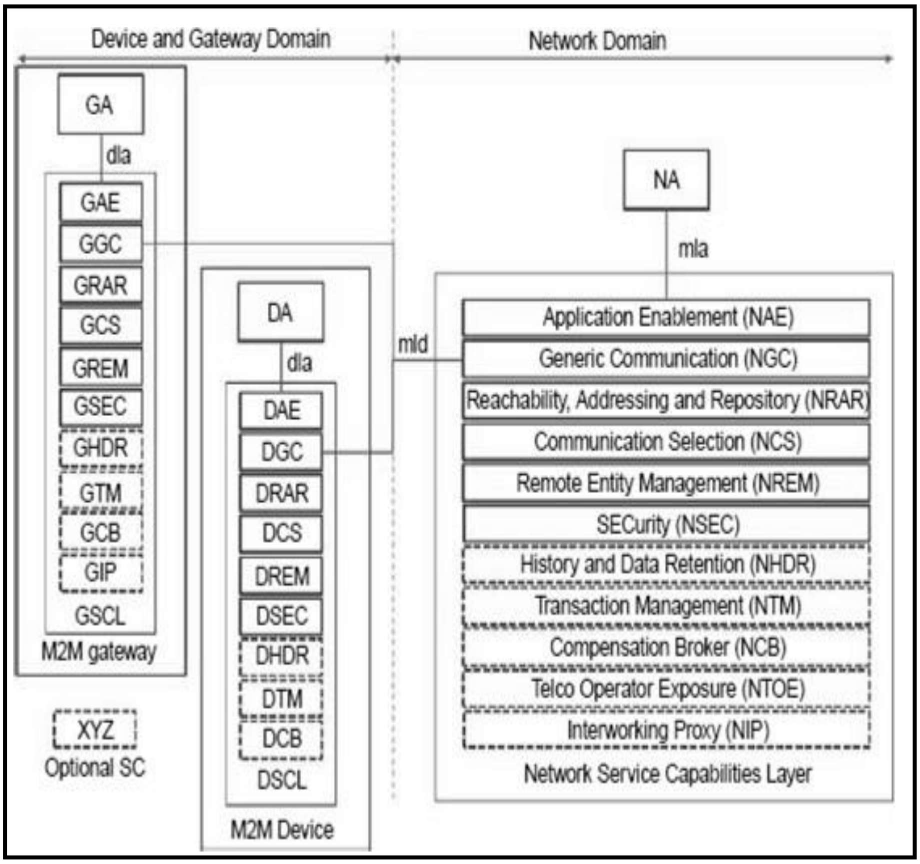

Device and Gateway Domain
Network Domain
GA
dIa
GAE
GGC
GRAR
GCS
GREM
GSEC
GHDR
GTM
GCB
GIP
GSCL
M2M gateway
XYZ
Optional SC
DA
dIa
DAE
DGC
DRAR
DCS
DREM
DSEC
DHDR
DTM
DCB
DSCL
M2M Device
mId
NA
mIa
Application Enablement (NAE)
Generic Communication (NGC)
Reachability, Addressing and Repository (NRAR)
Communication Selection (NCS)
Remote Entity Management (NREM)
SECurity (NSEC)
History and Data Retention (NHDR)
Transaction Management (NTM)
Compensation Broker (NCB)
Telco Operator Exposure (NTOE)
Interworking Proxy (NIP)
Network Service Capabilities Layer

Figure 4.3: M2M Capabilities for different M2M Nodes.

10. **Telco Operator Exposure (NTOE).** This is also an optional capability and provides exposure of the Core Network service offered by a Telecom Network Operator.

11. **Interworking Proxy (xIP).** This capability is an optional capability and provides mechanisms for connecting non-ETSI M2M Devices and Gateways to ETSI SCLs. NIP provides mechanisms for non-ETSI M2M Devices and Gateways to connect to NSCL while GIP provides the functionality for non-compliant M2M Devices to connect to GSCL via the reference point dIa, and the DIP provides the necessary mechanisms to connect non-compliant devices to DSCL via the dIa reference point.

8a) Explain information model and function model with example

4.1 Information Model

Similar to the IoT Domain Model, the IoT Information Model is presented using Unified Modeling Language (UML) diagrams. As mentioned earlier, each class in a UML diagram contains zero or more attributes.These attributes are typically of simple types such as integers or text strings, and are represented with red text under the name of the class (e.g.entityType in the Virtual Entity class in Figure 4.18).

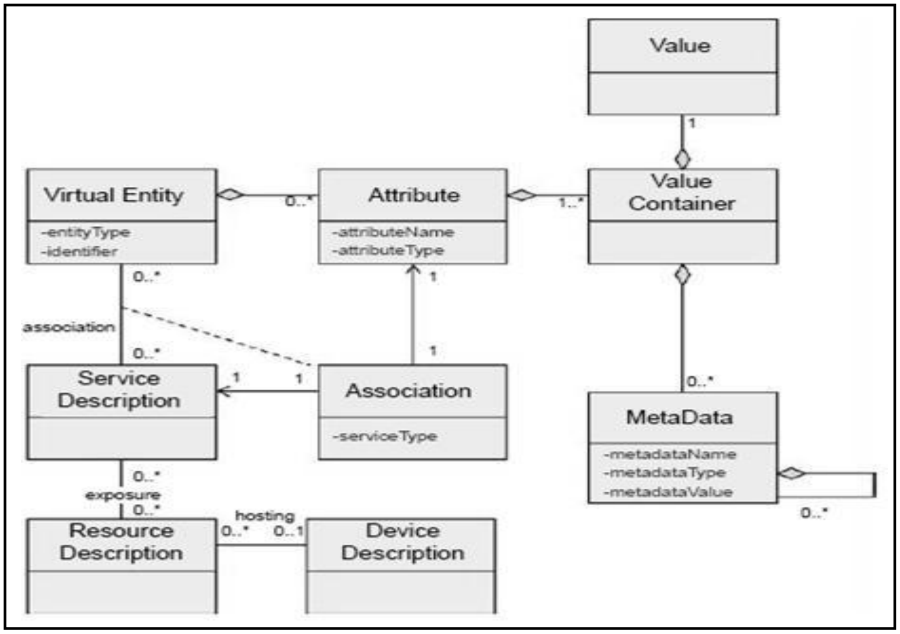


Figure 4.18: High –level Information Model

High level information model

- A more complex attribute for a specific class A is represented as a class B, which is contained
- in class A with an aggregation relationship between class A and class B.Moreover, the UML diagram for describing the IoT Information Model contains additional notation not presented earlier.
- On a high-level, the IoT Information Model maintains the necessary information about Virtual Entities and their properties or attributes. These properties/attributes can be static or dynamic and enter into the system in various forms, e.g. by manual data entry or reading a sensor attached to the Virtual Entity.
- Virtual Entity attributes can also be digital synchronized copies of the state of an actuator as mentioned earlier: by updating the value of an Virtual Entity attribute, an action takes place in the physical world.
- In the presentation of the high-level IoT information model, we omit the attributes that are not updated by an IoT Device (sensor, tag) or the attributes that do not affect any IoT Device.

IoT information Model example

The IoT Information Model describes Virtual Entities and their attributes that have one or more values annotated with meta-information or metadata. The attribute values are updated as a result of the associated services to a Virtual Entity. The associated services, in turn, are related to Resources and Devices as seen from the IoT Domain Model.

A Virtual Entity object contains simple attributes/properties:

(a) entityType to denote the type of entity, such as a human, car, or room (the entity type can be a reference to concepts of a domain ontology, e.g. a car ontology);

(b) a unique identifier; and

(c) zero or more complex attributes of the class Attributes.

The class Attributes should not be confused with the simple attributes of each class. This class Attributes is used as a grouping mechanism for complex attributes of the Virtual Entity. Objects of the class Attributes, in turn, contain the simple attributes with the self- descriptive names attributeName and attributeType.

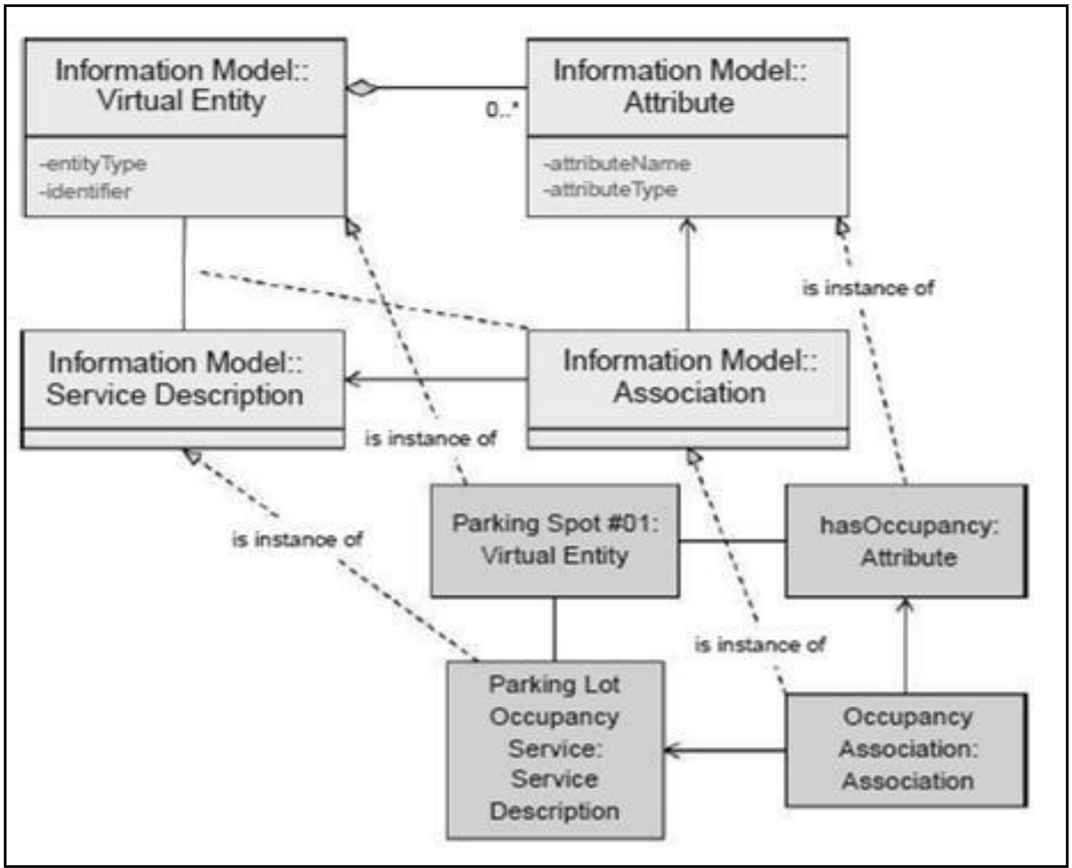
As seen from the IoT Domain Model, a Virtual Entity is associated with Resources that expose Services about the specific Virtual Entity. This association between a Virtual Entityand its Services is captured in the Information Model with the explicit class called Association.

Because the class Association describes the relationship between a Virtual Entity and Service Description through the Attribute class, there is a dashed line between Association class and the line between the Virtual Entity and Service Description classes.

The attribute serviceType can take two values:

(a) "INFORMATION," if the associated service is a sensor service (i.e.allows reading of the sensor), or (b) "ACTUATION," if the associated service is an actuation service

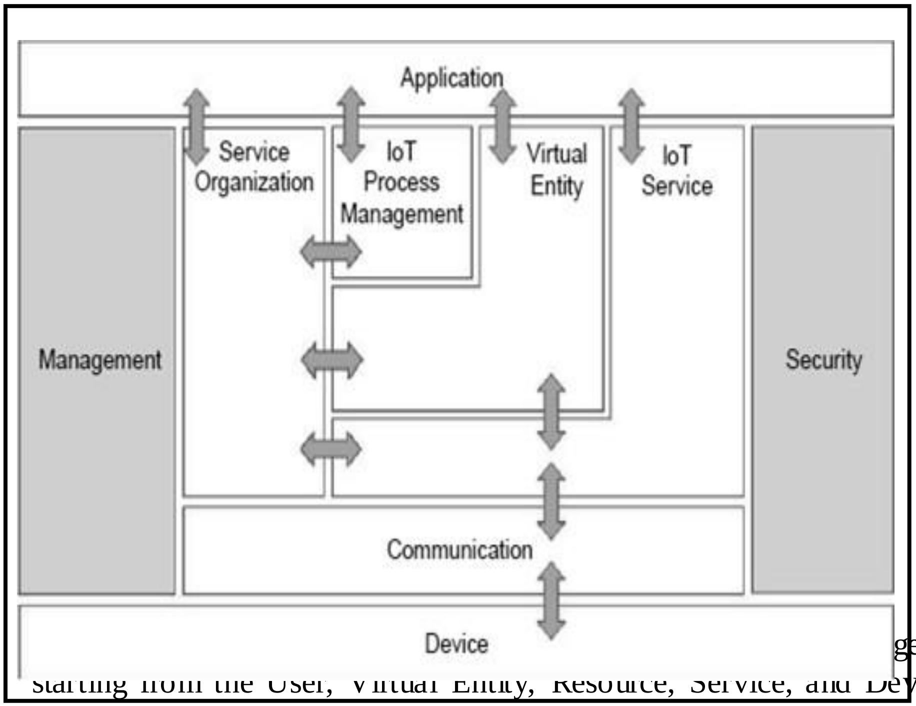
Figure 4.19 : IoT Information Model example



An example of an instantiation of the high-level information model is shown in **Figure 4.19**
following the parking lot example presented earlier.
Here we don’t show all the possible Virtual Entities, but only one corresponding to one parking spot. This Virtual Entity is described with one Attribute (among others) called hasOccupancy. This Attribute is associated with the Parking Lot Occupancy Service Description through the Occupancy Association. The Occupancy Association is the explicit expression of the association (line) between the Parking Spot #1 Virtual Entity and the Parking Lot Occupancy Service. model, as opposed to the Realization relationship for the IoT Domain Model.

4.2 Functional model

The IoT Functional Model aims at describing mainly the Functional Groups (FG) and their interaction with the ARM, while the Functional View of a Reference Architecture describes the functional components of an FG,interfaces, and interactions between the components. The Functional View is typically derived from the Functional Model in conjunction with high-level requirements. The IoT-A Functional Model is as shown in figure 4.21



generated by starting from the User, Virtual Entity, Resource, Service, and Device classes from the IoT Domain Model. The need for communicating Devices and digital artifacts was the motivation for the Communication FG.

- The need to compose simple IoT services in order to create more complex ones, as well as the need to integrate IoT services (simple or complex)with existing Information and Communications Technology (ICT) infrastructure,is the main driver behind the introduction of the Service Organization and IoT Process Management FGs respectively.

- The figure shows the flow of information between FGs apart from the cases of the Management and Security FGs that have information flowing from/to all other FGs, but these flows are omitted for clarity purposes.

4.2.1 : Device management group

The Device FG contains all the possible functionality hosted by the physical Devices that are used for instrumenting the Physical Entities. This Device functionality includes sensing, actuation, processing, storage, and identification components, the sophistication of which depends on the Device capabilities.

4.2.2 : Communication functional group

The Communication FG abstracts all the possible communication mechanisms used by the relevant Devices in an actual system in order to transfer information to the digital world components or other Devices. Examples of such functions include wired bus or wireless mesh technologies through which sensor Devices are connected to Internet Gateway Devices.

4.2.3 IoT Service functional group

The IoT Service FG corresponds mainly to the Service class from the IoT Domain Model, and contains single IoT Services exposed by Resources hosted on Devices or in the Network (e.g. processing or storage Resources).Support functions such as directory services, which allow discovery of Services and resolution to Resources, are also part of this FG.

4.2.4 Virtual Entity functional group

The Virtual Entity FG corresponds to the Virtual Entity class in the IoT Domain Model, and contains the necessary functionality to manage associations between Virtual Entities with themselves as well as associations between Virtual Entities and related IoT Services, i.e. the Association objects for the IoT Information Model.

Associations between Virtual Entities can be static or dynamic depending on the mobility of the Physical Entities related to the corresponding Virtual Entities.

A major difference between IoT Services and Virtual Entity Services is the semantics of the requests and responses to/from these services.

4.2.5 IoT Service Organization functional group

The purpose of the IoT Service Organization FG is to host all functional components that support the composition and orchestration of IoT and Virtual Entity services.

Moreover, this FG acts as a service hub between several other functional groups such as the IoT Process Management FG when, for example, service requests from Applications or the IoT Process Management are directed to the Resources implementing the necessary Services. Simple IoT or Virtual Entity Services can be composed to create more complex services,e.g. a control loop with one Sensor Service and one Actuator service with the objective to control the temperature in a building.

4.2.6 IoT Process Management functional group

The IoT Process Management FG is a collection of functionalities that allows smooth integration of IoT-related services (IoT Services, Virtual Entity Services, Composed Services) with the Enterprise (Business) Processes.

4.2.7 Management Functional group

The Management FG includes the necessary functions for enabling fault and performance monitoring of the system, configuration for enabling the system to be flexible to changing User demands, and accounting for enabling subsequent billing for the usage of the system.

4.2.8 Security functional group

The Security FG contains the functional components that ensure the secure operation of the system as well as the management of privacy. The Security FG contains components for Authentication of Users (Applications, Humans), Authorization of access to Services by Users, secure communication (ensuring integrity and confidentiality of messages) between entities of the system such as Devices, Services, Applications, and last but not least, assurance of privacy of sensitive information relating to Human Users.

4.2.9 Application functional group

The Application FG is just a placeholder that represents all the needed logic for creating an IoT application. The applications typically contain custom logic tailored to a specific domain such as a Smart Grid.

4.2.10 Modular IoT functions

The Functional Model, as well as the Functional View of the Reference Architecture, contains a complete map of the potential functionalities for a system realization. The functionalities that will eventually be used in an actual system are dependent on the actual system requirements The bare minimum functionalities are Device, Communication, IoT

Services, Management, and Security (Figure 4.22a). With these functionalities, an actual system can provide access to sensors, actuators and tag services for an application or backend system of a larger Enterprise. The application or larger system parts have to build the Virtual Entity functions for capturing the information about the Virtual Entities or the “Things” in the IoT architecture.

Often the Virtual Entity concept is not captured in the application or a larger system with a dedicated FG, but functions for handling Virtual Entities are embedded in the application or larger system logic; therefore, in Figures 4.22a_c, the Virtual Entity is represented with dashed lines.

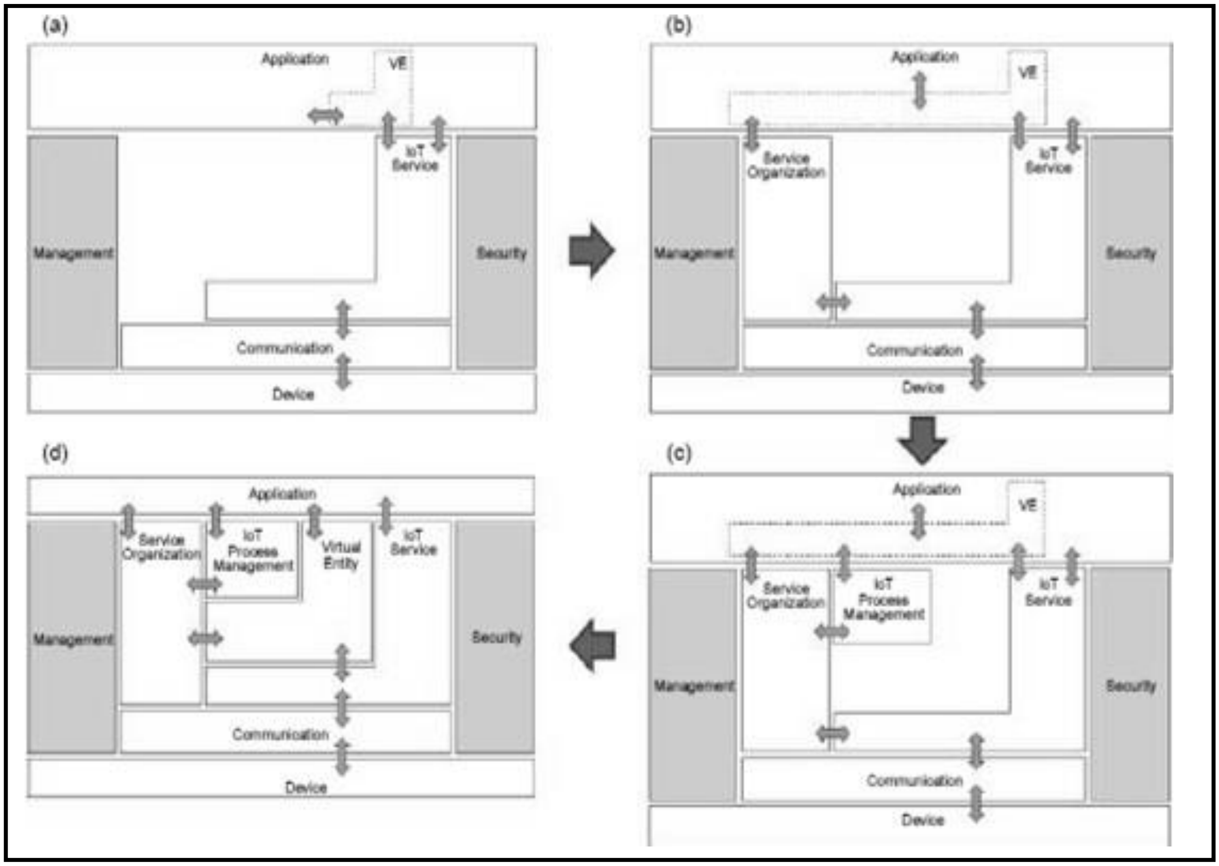


Figure 4.22: Building Progressively complex IoT Systems

8b) IOT domain model with example

IOT DOMAIN MODEL

- The domain model captures the basic attributes of the main concepts and the relationship between these concepts.
- A domain model also serves as a tool for human communication between people working in the domain in question and between people who work across different domains.
- A domain model also serves as a tool for human communication between people working in the domain in question and between people who work across different domains.

Model notation and semantics

- For the purposes of the description of the domain model, we use the Unified Modeling Language (UML).Class diagrams in order to present the relationships between the main concepts of the IoT domain model.
- The Class diagrams consist of boxes that represent the different classes of the model connected with each other through typically continuous lines or arrows, which represent relationships between the respective classes.
- Each class is a descriptor of a set of objects that have similar structure, behavior, and relationships.

- A class contains a name (e.g. Class A in Figure 4.14) and a set of attributes and operations.

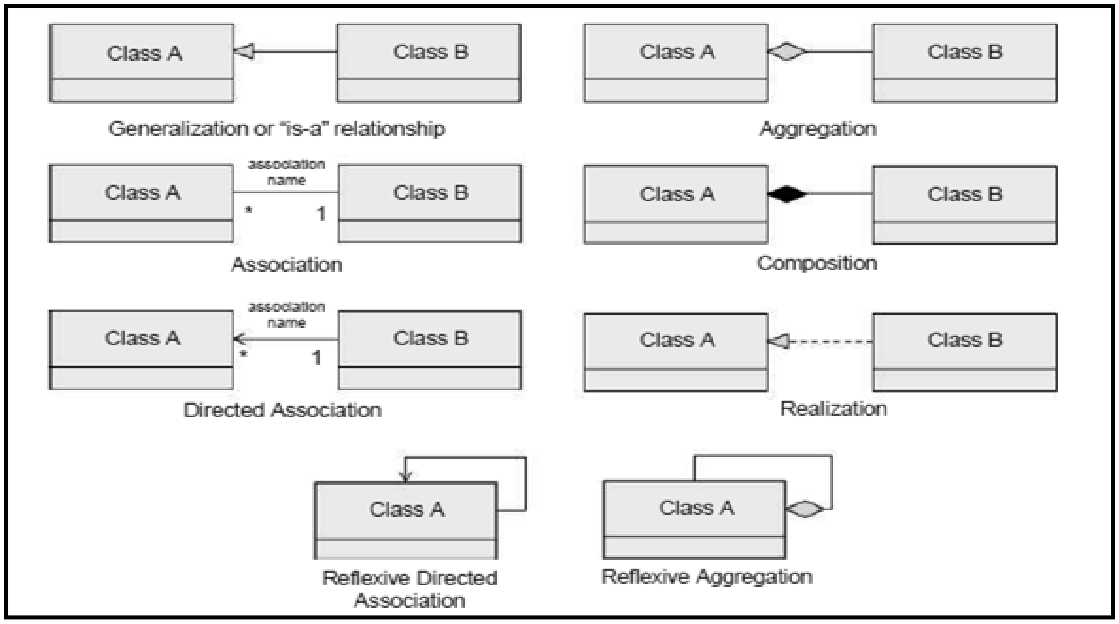


Figure 4.14: UML Class diagram main modeling concepts.

- For the description of the IoT domain model, we will use only the class name and the class attributes, and omit the class operations.
- Notation-wise this is represented as a box with two compartments, one containing the class name and the other containing the attributes. However, for the IoT domain model description, the attribute compartment will be empty in order not to clutter the complete domain model.
- The following modeling relationships between classes (Figure 4.14) are needed for the description of the IoT Domain Model: Generalization/ Specialization, Aggregation and Reflexive Aggregation, Composition, Directed Association and Reflexive Directed Association, and Realization.
- The Generalization/Specialization relationship is represented by an arrow with a solid line and a hollow triangle head. Depending on the starting point of the arrow, the relationship can be viewed as a generalization or specialization.
- The Aggregation relationship is represented by a line with a hollow diamond in one end and represents a whole-part relationship or a containment relationship and is often called a "has-a" relationship. The class that touches the hollow diamond is the whole class while the other class is the part class.
- The Composition relationship is represented by a line with a solid black diamond in one end, and also represents a whole-part relationship or a containment relationship. The class that touches the solid black diamond is the whole class while the other class is the part class.

Main concepts

The IoT is a support infrastructure for enabling objects and places in the physical world to have a corresponding representation in the digital world.The reason why we would like to represent the physical world in the digital world is to remotely monitor and interact with the physical world using software.

Let's illustrate this concept with an example (Figure 4.15).Imagine that we are interested in monitoring a parking lot with 16 parking spots. The parking lot includes a payment station for drivers to pay for the parking spot after they park their cars. The parking lot also includes an electronic road sign on the side of the street that shows in real-time the number of empty spots.

Frequent customers also download a smart phone application that informs them about the availability of a parking spot before they even drive on the street where the parking lot is

located. In order to realize such a service, the relevant physical objects as well as their properties need to be captured and translated to digital objects such as variables, counters, or database objects so that software can operate on these objects and achieve the desired effect,

i.e. detecting when someone parks without paying, informing drivers about the availability of parking spots, producing statistics about the average occupancy levels of the parking lot, etc.

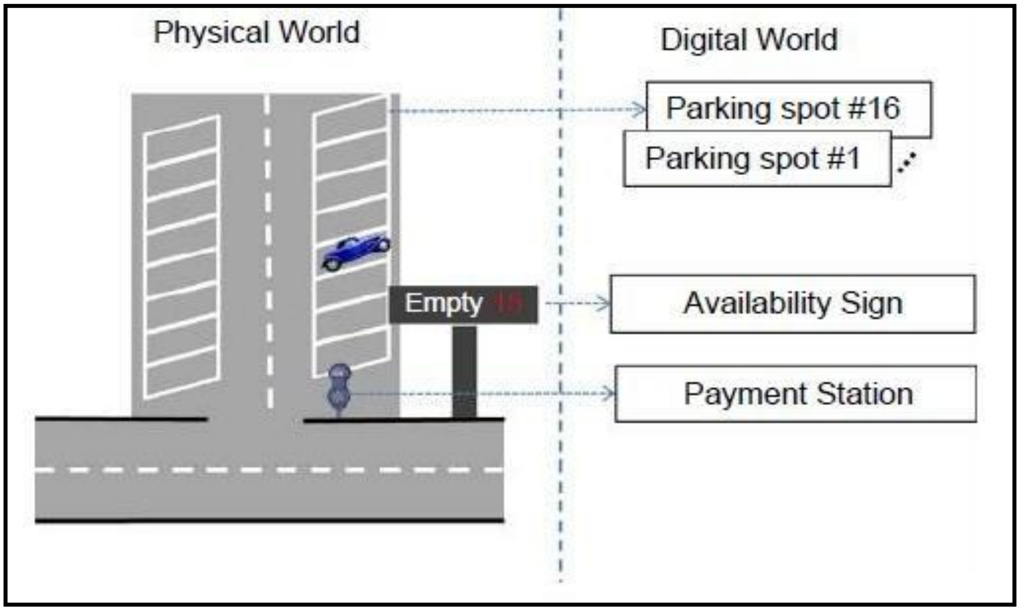


Figure 4.15: Physical vs. Virtual World.

For these purposes, the parking lot as a place is instrumented with parking spot sensors (e.g. loops), and for each sensor, a digital representation is created (Parking spot #1_#16). In the digital world, a parking spot is a variable with a binary value ("available" or "occupied"). The parking lot payment station also needs to be represented in the digital world in order to check if a recently parked car owner actually paid the parking fee. Finally, the availability sign is represented to the digital world in order to allow notification to drivers that an empty lot is full for maintenance purposes, or even to allow maintenance personnel to detect when the sign is malfunctioning.

As interaction with the physical world is the key for the IoT; it needs to be captured in the domain model (Figure 4.16). The first most fundamental interaction is between a human or an application with the physical A User can be a Human User, and the interaction can be physical (e.g. parking the car in the parking lot).

The physical interaction is the result of the intention of the human to achieve a certain goal (e.g. park the car). In other occasions, a Human world object or place. Therefore, a User and a Physical Entity are two concepts that belong to the domain model.

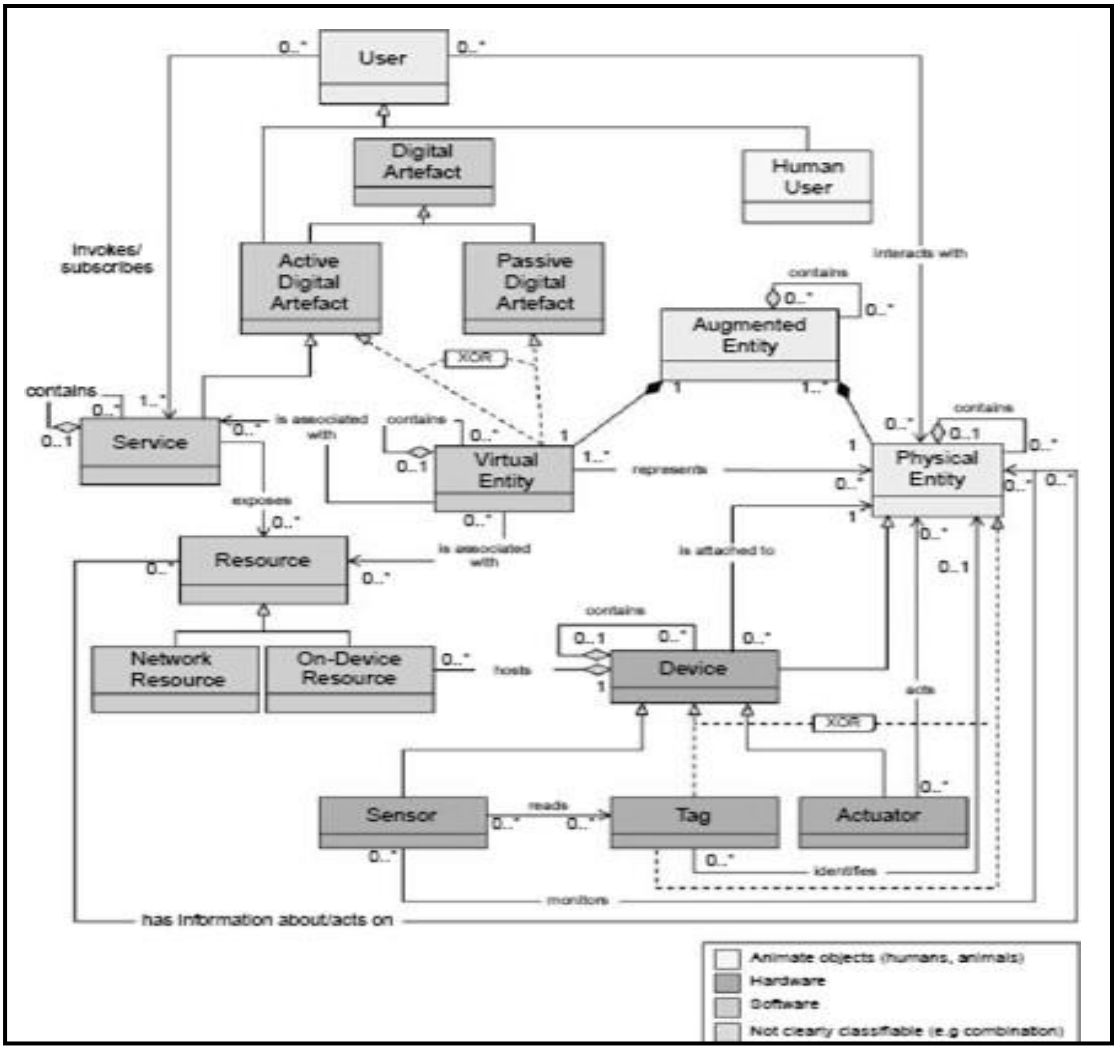


Figure 4.16: IoT Domain Model.

A Physical Entity, as the model shows, can potentially contain other physical entities; for example, a building is made up of several floors, and each floor has several rooms.

The objects, places, and things represented as Physical Entities are the same as Assets mentioned earlier in the book. According to the Oxford Dictionary, an Asset .is an item or property that is regarded as having value”; therefore, the term Asset is more related to the business aspects of IoT. Because the domain model is a technical tool, we use the term Physical Entity instead of Asset.

- A Physical Entity is represented in the digital world as a Virtual Entity.
- A Virtual Entity can be a database entry, a geographical model (mainly for

places), an image or avatar, or any other Digital Artifact.

- One Physical Entity can be represented by multiple Virtual Entities, each serving a different purpose, e.g. a database entry of a parking spot denoting the spot
availability,and an (empty/full) image of a parking spot on the monitor of the parking lot management system.
- Each Virtual Entity also has a unique identifier for making it addressable among other Digital Artifacts. A Virtual Entity representation contains several attributes that correspond to the Physical Entity current state.
- The Virtual Entity representation and the Physical Entity actual state should be synchronized whenever a User operates on one or the other, if of course that is physically possible.

For the IoT Domain Model, three kinds of Device types are the most important:

1. **Sensors:** These are simple or complex Devices that typically involve a transducer that converts physical properties such as temperature into electrical signals. These Devices include the necessary conversion of analog electrical signals into digital signals, e.g. a voltage level to a 16-bit number, processing for simple calculations, potential storage for intermediate results, and potentially communication capabilities to transmit the digital representation of the physical property as well receive commands.
2. **Actuators:** These are also simple or complex Devices that involve a transducer that converts electrical signals to a change in a physical property (e.g. turn on a switch or move a motor). These Devices also include potential communication capabilities, storage of intermediate commands, processing, and conversion of digital signals to analog electrical signals.
3. **Tags:** Tags in general identify the Physical Entity that they are attached to. In reality, tags can be Devices or Physical Entities but not both, as the domain model shows. An example of a Tag as a Device is a Radio Frequency Identification (RFID) tag, while a tag as a Physical Entity is a paper-printed immutable barcode or Quick Response (QR) code.

- As shown in the model, Devices can be aggregation of other Devices e.g. a sensor node contains a temperature sensor, a Light Emitting Diode (LED, actuator), and a buzzer (actuator). Any type of IoT Device needs to (a) have energy reserves (e.g. a battery), or (b) be connected to the power grid, or (c) perform energy scavenging (e.g. converting solar radiation to energy).
- The Device communication, processing and storage, and energy reserve capabilities determine several design decisions such as if the resources should be on-Device or not.
- Resources are software components that provide data for, or are endpoints for, controlling Physical Entities. Resources can be of two types,on-Device resources and Network Resources. An on-Device Resource is typically hosted on the Device itself and provides information, or is the control point for the Physical Entities that the Device itself is attached to. The Network Resources are software components hosted somewhere in the network or cloud.

- A Virtual Entity is associated with potentially several Resources that provide information or control of the Physical Entity represented by this Virtual Entity.
- The Virtual Entities that are associated with Physical Entities instrumented with Devices that expose Resources are also associated with the corresponding resource Services.

It is important to note that IoT Services can be classified into three main classes according to their level of abstraction:

1. Resource-Level Services typically expose the functionality of a Device by exposing the on-Device Resources. In addition, these services typically handle quality aspects such as security, availability, and performance issues.
2. Virtual Entity-Level Services provide information or interaction capabilities about Virtual Entities, and as a result the Service interfaces typically include an identity of the Virtual Entity.
3. Integrated Services are the compositions of Resource-Level and Virtual Entity-Level services, or any combination of both service classes.

9a) Explain functional requirements and non – functional requirements with example

There are a number of nonfunctional requirements that need to be satisfied for every application. These are technical and non-technical:

- Regulations
  - For applications that require placing nodes in public places, planning permission often becomes an issue.
  - Radio Frequency (RF) regulations limit the power with which transmitters can broadcast. This varies by region and frequency band.
- Ease of use, installation, maintenance, accessibility
  - Simplification of installation and configuration of IoT applications is as yet unresolved beyond well-known, off-the-shelf systems. It is difficult to conceive a general solution to this problem. This relates to positioning, placement, site surveying, programming, and physical accessibility of devices for maintenance purposes.
  - Physical constraints (from several perspectives)
  - Can the additional electronics be easily integrated into the existing system?
  - Are there physical size limitations on the device as a result of the deployment scenario?
  - What kind of packaging is most suitable (e.g. IP-rated enclosures for outdoor deployment)?
  - What kind and size of antenna can I use?
  - What kind of power supply can I use given size restrictions (relates to harvesting, batteries, and alternative storage, e.g. supercapacitors)?

9 b) Explain sensing and communication field with example

The sensing field is of importance when considering both the phenomenon to be sensed (i.e. Is it local or distributed?) and the distance between sensing points. The physical environment has an implication on the communications technologies selected and the reliability of the system in operation thereafter. Devices must be placed in close enough proximity to communicate. Where the distance is too great, routing devices may be

necessary.
Devices may become intermittently disconnected due to the time varying, stochastic nature of the wireless medium. Certain environments may be fundamentally more suited to wireless propagation than others. For example, studies have shown that tunnels are excellent environments for wireless propagation, whereas, where RF shielding can occur (e.g. in a heavy construction environment), communication range of devices can be significantly reduced.

10.a) Explain Integrated device design with example

- Integrated Device Design: Once the energy, sensors, actuators, computation, memory, power, connectivity, physical, and other functional and nonfunctional requirements are considered, it is likely that an integrated device must be produced. This is essentially going to be an exercise in Printed Circuit Board (PCB) design, but will in many cases require some consideration to be paid to the RF front-end design. This means that the PCB design will require specific attention to be paid to the reference designs of the RFIC manufacturer during development, or potentially the integration of an additional Integrated Circuit (IC) that deals with the balun and matching network required.

10. b) Explain data representation and visualization with example

Data Representation

Each IoT application has an optimal visual representation of the data and the system. Data that is generated from heterogeneous systems has heterogeneous visualization requirements. There are currently no satisfactory standard data representation and storage methods that satisfy all of the potential IoT applications.

Data-derivative products will have further ad hoc visualization requirements. A derivative in these terms exists once a function has been performed on an initial data set _ which may or may not be raw data. These can be further integrated at various levels of abstraction, depending on the logic of the integrator. New information sources, such as those derived from integrated data streams from various logically correlated IoT applications, will present interesting representation and visualization challenges.