هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

Guidelines for IoT

cst.gov.sa

First Edition
2023 July

Table of Contents

1 Introduction

The Communications, Space and Technology Commission (CST) is mandated, in accordance with the Telecommunications Act, Telecom Act Bylaw and CST Ordinance, to regulate the Telecommunications and IT sector in the Kingdom of Saudi Arabia (Kingdom), which also includes the Internet of Things (IoT).

In accordance with the Telecommunication and Information Technology Act (Act) –and its bylaw- issued under the Council of Ministers Resolution No. (592), dated 1443/11/01 H, approved pursuant to the Royal Decree No. (M/106), dated 1443/11/02 H. In accordance with Article Seven of the Cabinet Resolution No. (292), dated 1441/04/27 H, and in order to achieve the objectives stated in Article Two of the Act; the Communications, Space and Technology Commission (CST) is the entity mandated to regulate the telecommunications and information technology sector in the Kingdom; including the Internet of Things (IoT) technology.Accordingly, and based on CST strategy; CST aims to enable IoT market in the Kingdom. To further this objective; CST issued the Guidelines for IoT document (guidelines) with a goal to increase the adoption ofbest practices,administrative, and technical recommendations related to IoT technology.

CST confirms that this guideline document is non-binding and not a substitute for any controls, procedures, standards, rules, instructions or regulations issued by a regulatory decision of CST, and is is not in any way a reference to any of the legal procedures and responsibilities of the persons and parties concerned.

1.1 Definitions

The terms and expressions that are defined in the Act, its bylaw, and the regulations issued by CST will have the same meaning when used in this document. The following terms and expressions will also have the meanings associated with them unless the context requires otherwise:

Term	Definition
IoT	A network of devices capable of independently sensing, monitoring, or interacting with the surrounding environment, as well as collecting and transmitting data.
IoT Device	A device that is connected to a network, has the ability to transmit data, and can communicate with other devices or IoT platforms.
IoT Connectivity	Communication means that enable IoT devices to communicate and transfer data between each other, to platforms, or to the Internet.
IoT Service	It is a service that includes the provision of an IoT Device, IoT Connectivity, and IoT Platform Service, or IoT Device and IoT Platform Service, or IoT Connectivity and IoT Platform Service, or IoT Platform Service.
IoT Service Provider	Any entity that provides an IoT service.
IoT Device Manufacturer	Any entity that manufactures an IoT device.
IoT User	Any entity or individual using or benefiting from an IoT service.

1.2 Scope

The guidelines focus on non-binding guidenlines aiming to facilitate and support the adoptiong of IoT to the following IoT ecosystem players:

IOT
User

IOT
Device
Manufacturer

IOT
Service Provider

More over, the guidelines focuses on the following areas:

Securing the IoT environment from malicious actors

Protecting IoT User against data privacy breaches

Increasing the level of access to IoT services by ensuring portability of devices, data and applications across platforms

Enabling the seamless flow of data across devices and platforms by ensuring sufficient levels of interoperability among applications and devices across the entire IoT ecosystem regardless of connectivity protocols applied

1.3 About IoT

IoT refers to a network of devices that are independently capable of sensing, monitoring, or interacting with the surrounding environment, in addition to the ability to collect and transmit data.

The diagram below represents the entire IoT environment. Things being a part of the edge are a key part of the IoT environment. Devices attached to things stream data towards the core, which consists of platforms and applications. There are multiple IoT solutions, i.e. applications processing data at the edge and mainly at the core in order to achieve specific business goals.

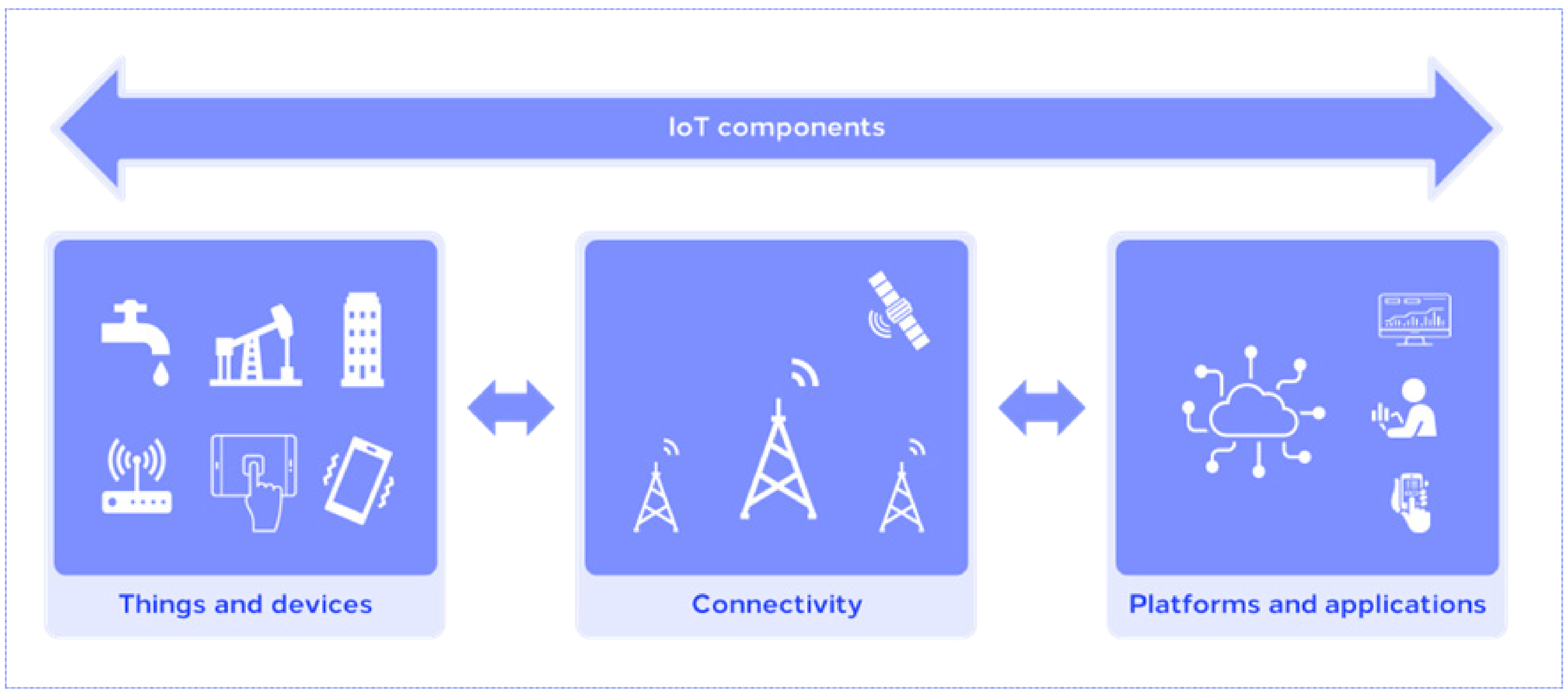


Figure 1: IoT Components

2 Related Laws and Regulations

Stakeholders must comply with the laws and regulations in force in the Kingdom and any regulations issued by the CST that apply to IoT solutions.This guide does not prejudice the competence of the National Cybersecurity Authority and the National Data Management Office with regulations related to cybersecurity, and data management and governance. The following list, is a non-exhaustive list of the most important regulations and mandatory regulations issued by the CST that may apply to IoT solutions, with an emphasis on the need to verify any updates to the documents mentioned below or any documents issued in the future that apply to IoT solutions.

#	Document title
1	**Cloud Computing Regulatory Framework (CCRF)**
2	**Cybersecurity Regulatory Framework (CRF)**
3	**IoT Regulatory Framework**
4	**Regulations for Importation and Licensing of Telecommunications and Information Technology Equipment**
5	**Technical Specification of Telecommunications and Information Technology Equipment**
6	**Regulations for Maintaining the Privacy of Personal Data Protection**
7	**Wireless Local Area Networks Regulations (WLAN/WiFi)**

3 Guidelines Summary

	Guideline	IoT Service Provider	IoT Device Manufacturer	IoT User
General	Choose an appropriate connectivity technology	✓	✓	✓
	Design and program devices to maximise battery life	✓	✓	–
	Check devices periodically to assure transmission when it is required	–	–	✓
Interoperability	Use available interoperability standards	✓	✓	–
	Design complex IoT solutions to be modular in compliance with service-oriented architecture	✓	✓	–
	Design IoT applications to use standardized APIs	✓	✓	–
	Create and apply an API framework	✓	–	–
	Build applications for a multi-domain IoT ecosystem using existing functions and APIs issued by individual IoT domains	✓	–	–
	Containerise and make IoT software components deployable in the Cloud, on-premise and at the edge	✓	–	–
	Identify, select, catalogue and follow adequate communication protocols while designing and developing an IoT environment	✓	✓	–
	Identify, select, catalogue and follow adequate data exchange protocols while designing and developing an IoT environment	✓	✓	–
	Common data models and ontologies should be applied	✓	✓	–
Data	Establish and follow a common metadata model	✓	✓	–
	Validate data incoming through user interfaces or transported by APIs	✓	–	–
	Create data backup plans	✓	–	–
	Establish and follow data retention rules	✓	✓	–
Security	Create and use a system to control access to resources of an IoT service domain	✓	✓	✓
	Ensure high availability of devices, platforms and applications	✓	✓	✓
	Establish and follow procedures for maintenance of IoT software	✓	–	–
	Apply security patches delivered over a secure channel periodically	✓	✓	✓
	Encrypt individuals-related and contextualised data	✓	–	–

4 General Guidelines

This section includes general guidelines for IoT applications, such as: connectivity choices and device power management and control..

4.1.1 Connectivity Choices

Choose an appropriate connectivity technology

Applies to:

IOT
User

IOT
Device
Manufacturer

IOT
Service Provider

Use the following dimensions to select the connectivity technology:

- SLA, including reliability, latency, mobility, etc.
- Device's design is fit for purpose
- Device support for current connectivity technologies
- Connectivity cost related to solution design, implementation and maintenance
- Density of devices per km^2 and planned communication frequency
- Current and future availability of local infrastructure and connectivity technology
- Market of currently available devices
- Device's power capabilities
- Average and peak transmission speed expected from devices

The following diagram represents connectivity methods. The horizontal axis shows the range span of a given technology, while the vertical axis shows data rate and energy consumption. The diagram also indicates the cost of network solution design, deployment and operation. Finally, it specifies whether the method operates within a licensed or unlicensed spectrum.

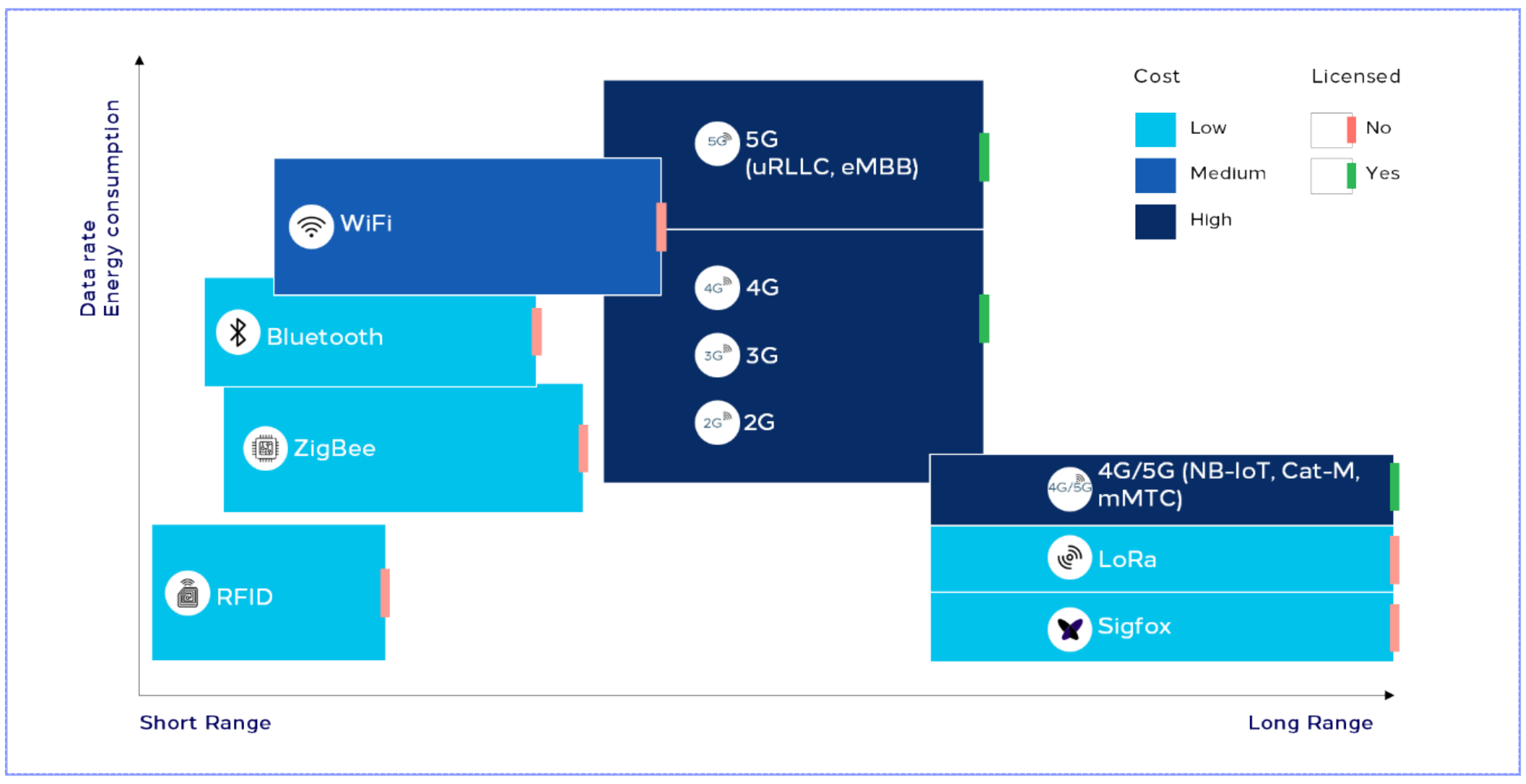


Figure 2: IoT Connectivity Methods

Below is a non-exhaustive list of connectivity methods, examples of IoT use cases, and application areas.

Connectivity	Areas of application	Use case examples
RFID	Physical proximity	Security, access control
ZigBee, Z-Wave	Indoor, close outdoor	Medical devices, smart buildings
Bluetooth, BLE	Close proximity	Short messaging, devices pairing
6E Wi-Fi and Wi-Fi	Indoor, close outdoor	Lighting, access points, hot spots
(4G / 3G / 2G) Mobile	Outdoor, metropolitan	Telemetry, international tracking
5G (uRLLC, eMBB)	5G high speed and reliability	Production, monitoring
NB-IoT, LTE-M, mMTC	distributed systems	Smart metering, assets tracking
LoRa	Fast deployment	Smart city, smart agriculture, tracking
Sigfox	Outdoor	Dispersed assets monitoring

4.1.2 Device Power Management and Control

Design and program devices to maximise battery life

Applies to:

IOT
Device
Manufacturer

IOT
Service Provider

Most devices are battery-operated and rely only on batteries. Therefore, it is essential to consider maximising battery life while designing, programming, and using IoT devices.

For examples, devices using LPWAN communication can last with two standard lithium LR6/AA batteries for more than ten years. However, it must be emphasised that to ensure prolonged battery life, the respective firmware of the device and the network should be compatible.

CST has specifications for devices using LPWAN with power limitations for specific parts of the device responsible for ensuring connectivity.

Check devices periodically to assure transmission when it is required

Applies to:

IOT
User

For example, smoke detectors remain in a sleeping mode for more than %99 of their lifetime and only wake up in case of fire.

The device should be switched from sleeping mode to an active mode periodically to verify whether the device and battery remain operational. Refer to the device manual for the battery verification period and method of changing modes.

5 Interoperability

When choosing an IoT solution or integrating a new solution to an existing one; users are recommended to take into account the compatibility between IoT devices, platform and data, in order to avoid the inability of new devices to communicate with the existing ones, and the inability to connect new devices with the platforms used in the solution.

Interoperability is the ability of two or more systems or applications to exchange information and mutually use the information exchanged.

This section includes recommendations that target interoperability within the IoT ecosystem, focusing on the following threes dimensions:

Device

Device ability to communicate with other devices or components within the IoT ecosystem

Refer to guidelines for Communication and Data Exchange Protocols.

Platform

Ability to communicate with / transport platform components

Refer to guidelines for Service-Oriented Architecture, API Framework, Architecture Designed for Portability and Hybridisation

Data

Ability to exchange and understand data communicated between two or more systems

Refer to guidelines for Usage of Data Models.

5.1.1 Interoperability Standards

Use available interoperability standards

Applies to:

IOT
Device
Manufacturer

IOT
Service Provider

Following interoperability standards for IoT devices, platforms, data, and systems increases their compatibility with other elements in the IoT environment, and there are standards for specific sectors such as smart cities and smart homes. One of the globally recognized standards for smart homes is the Matter Standard.

Source of the relevant standards:
ISO/IEC 1:2019-21823 Interoperability for IoT systems: Part 1: Framework
ISO/IEC 2:2020-21823 Interoperability for IoT systems: Part 2: Transport interoperability
ISO/IEC 3:2021-21823 Interoperability for IoT systems: Part 3: Semantic interoperability
ISO/IEC 4:2022-21823 Interoperability for IoT systems: Part 4: Syntactic interoperability
Matter Standard

5.1.2 Service-Oriented Architecture

Design complex IoT solutions to be modular in compliance with service-oriented architecture (SOA)

Applies to:

IOT
Device
Manufacturer

IOT
Service Provider

Service-Oriented Architecture (SOA) is an architectural style that supports service orientation. Service orientation is a way of thinking about services and service-based development and the outcomes of services.

An information technology environment built along Service-Oriented Architecture consists of multiple services, each responsible for executing a small range of functionality and collaborating through the integration layer. Independently managed modules should implement these services.

Service-orientation is needed to facilitate integration, thus contributing to interoperability.

Complex IoT solutions cover many applications, devices and networks working in combination, usually in real-time.

An IoT environment integration layer consists primarily of APIs - see guideline 4.2.3 API Framework - and message exchange – see guideline 4.2.8 Data Exchange Messaging. A rules-engine application responsible for events management orchestrates the collaboration of services to meet business objectives.

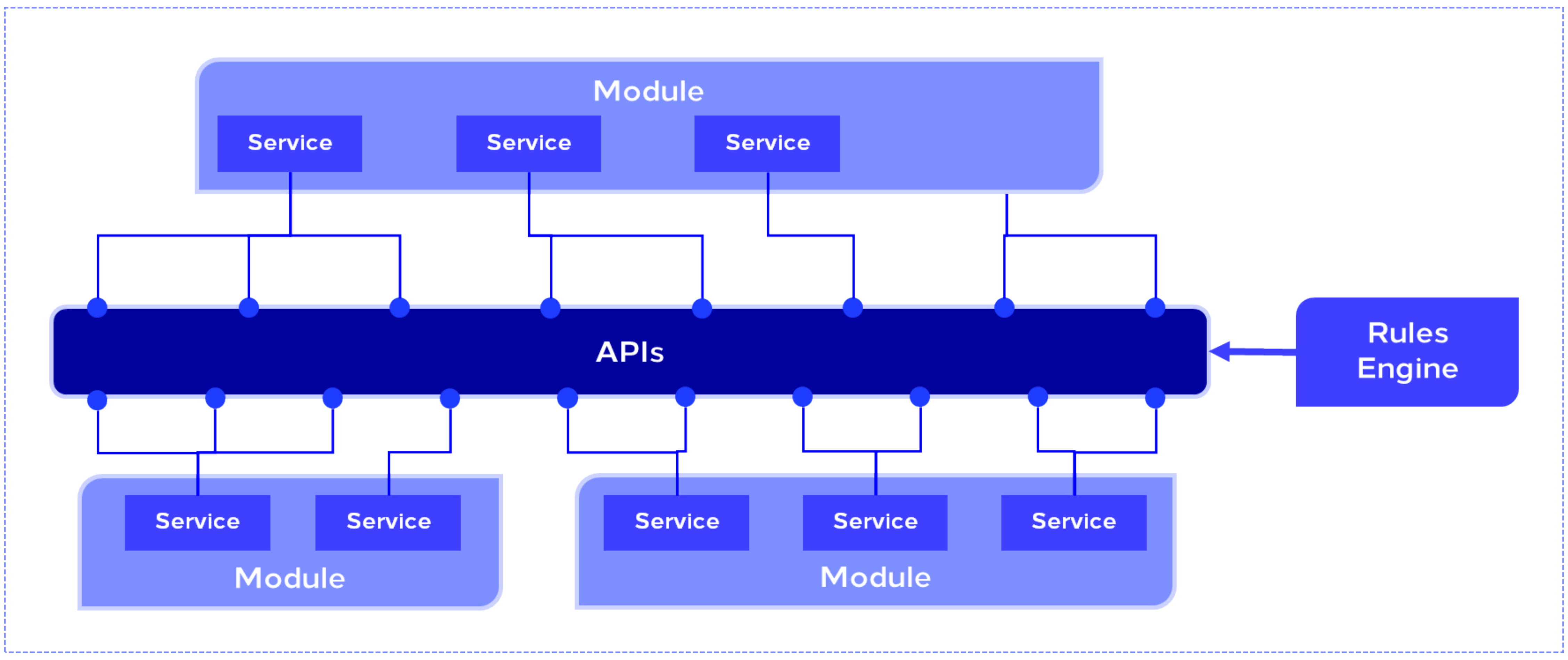


Figure 3: Service-Oriented Architecture for IoT

In the absence of SOA in an IoT system, the system becomes increasingly device-centric, with business logic tightly coupled with the devices. Such mesh architectures make it difficult for business owners to influence the system using business objectives. Furthermore, such a design is prone to operational errors, failures, and outages, which re§uces overall solution integrity and commercial value.

SOA implementation adds a layer of abstraction between business logic and devices, reducing the tight coupling between them. SOA makes the solution modular, allowing business owners to concentrate on specific parts of the system without having to worry about the whole. Thus, SOA empowers business owners to focus on business objectives instead of infrastructure.

Additionally, a rules engine enables for widening the functional scope of solutions compliant with SOA by adding new services and rules to the system without affecting existing services.

Finally, modularity assured by service orientation allows ease of scaling for an IoT system, enabling such capabilities as:

dynamic scaling

to handle spikes in the usage of particular functionality,

increasing the availability

of services by the ability to move a given module from one host to another

Source of the relevant standard:

3GPP TS 23.501 – System architecture for the 5G System (5GS)

5G; Management and orchestration; Architecture framework

5.1.3 API Framework

Design IoT applications to use standardised APIs

Applies to:

IOT
Device
Manufacturer

IOT
Service Provider

APIs are software components that enable data exchange between services. If standardised APIs were not utilised, various IoT components such as devices, gateways, clouds, IoT platforms and IoT applications would require additional integration efforts to exchange data, leading to a fractured IoT ecosystem

Source of the relevant standard:
Context Information Management (CIM); NGSI-LD API

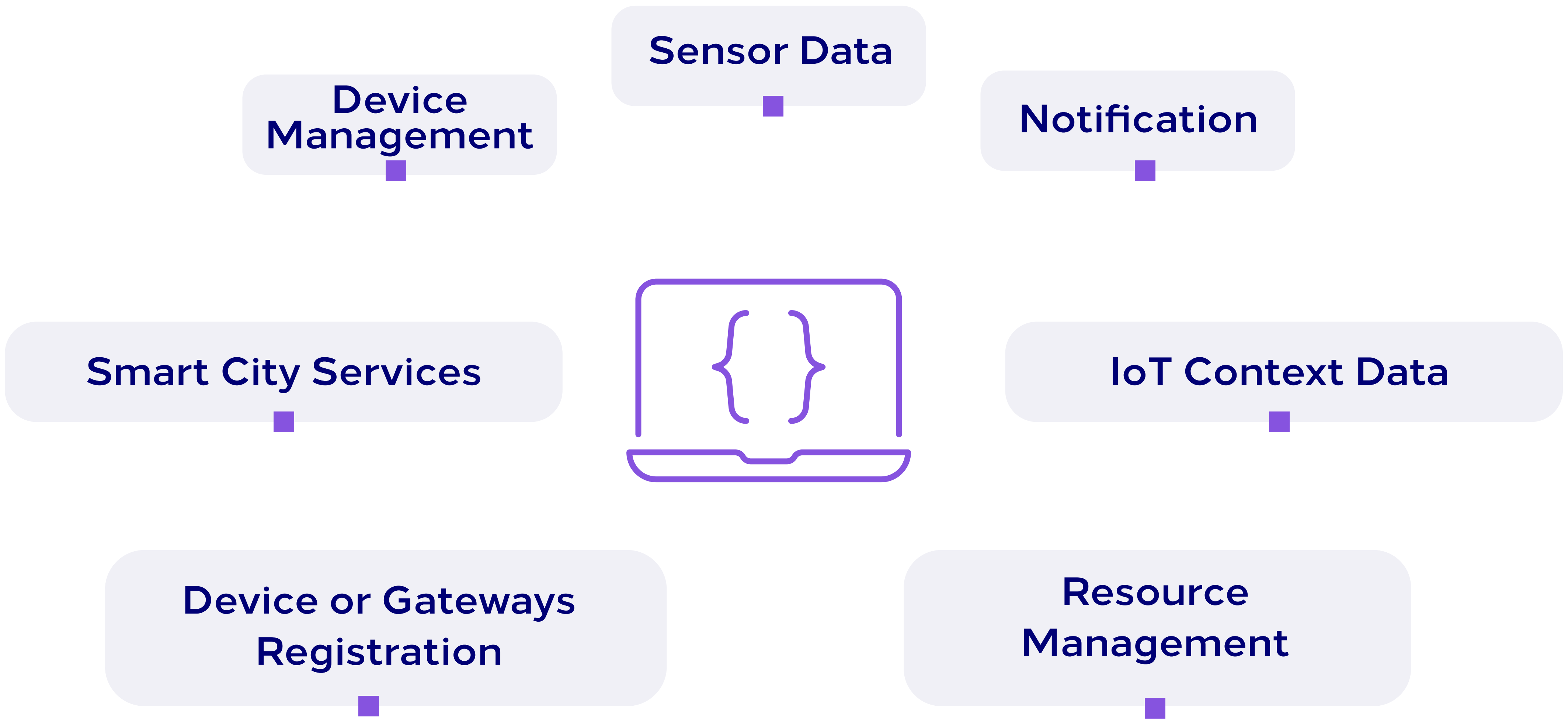
Create and apply an API framework

Applies to:

IOT
Service Provider

There are multiple API-related specifications. Therefore, developing a standard API framework that includes common aspects applicable to any IoT service APIs is necessary to avoid duplication, discrepancies, and inconsistencies between .different API specifications

API Framework might address the following aspects through APIs:



Device Management

Sensor Data

Notification

Smart City Services

IoT Context Data

Device or Gateways Registration

Resource Management

API framework also enables API access management governance.

An example of the 4G and 5G APIs of the API utilisation framework is presented in the standard below.

Source of the relevant standard:

Common API Framework for 3GPP Northbound APIs

Build applications for a multi-domain IoT ecosystem using existing functions and APIs issued by individual IoT domains

Applies to:

IOT
Service Provider

An example of a multi-domain IoT ecosystem is a Smart City, where utilities, transportation, air quality, natural disaster monitoring, surveillance, and security constitute separate domains.

5.1.4 Architecture Designed for Portability and Hybridisation

Containerise and make IoT software components deployable in the Cloud, on-premise and at the edge

Applies to:

IOT
Service Provider

The flexibility of an IoT solution's deployment allows for achieving the same business goal even in a different physical or business context. Additionally, it reduces the dependency on any particular cloud provider, allowing the service .provider to switch to another one

For example, connectivity is often a limiting factor in sectors with vast geographies due to the cost of high data traffic or the need for real-time analysis. Therefore, designing applications in a flexible way will allow processing raw data in edge devices and interacting with that data at the same time while the code is .stored centrally

Thus, it is recommended to design IoT applications with ability to deploy it in cloud, .on-premises or edge device

5.1.5 Communication and Data Exchange Protocols

Identify, select, catalogue and follow adequate communication protocols while designing and developing an IoT environment

Applies to:

IOT
Device
Manufacturer

IOT
Service Provider

A communication protocol is a set of rules allowing multiple devices or information systems can transmit information between themselves. Communication protocols define methods for:

- **Establishing** and maintaining a connection
- **Data exchange**
- **Transmission error** recovery and correction

For complex IoT ecosystems, such as Smart Cities, it is paramount to use a carefully curated set of communication protocols to ensure interoperability. Therefore, when designing a new IoT environment, the following actions need to be taken:

Identification of available and required communication protocols, depending on use cases and devices

Selection of a set of protocols to be used

Creation of a catalogue of protocols for implementation and future reference to choose from when expanding the scope of the IoT environment

Following the protocols from the established catalogue when implementing platforms and applications

Identify, select, catalogue and follow adequate data exchange protocols while designing and developing an IoT environment

Applies to:

IOT
Device
Manufacturer

IOT
Service Provider

Data exchange is the part of communication that enables information to flow through an IoT environment. Data exchange protocols define rules that allow the recipient of data to receive it correctly.

Data exchange protocols apply to sensor data, device management data (e.g., software update commands), and device authentication data.

Examples of data exchange protocols applicable in IoT are CoAP, LwM2M, mMTC and MQTT.

Sources of the relevant standard:
OMA LightweightM2M Overview
Constrained Application Protocol (CoAP)
3GPP TS 23.501 – System architecture for the 5G System (5GS)
Multi-access Edge Computing (MEC) Framework and Reference Architecture
Multi-access Edge Computing (MEC) MEC 5G Integration

5.1.6 Usage of Data Models

Common data models and ontologies should be applied

Applies to:

IOT Device Manufacturer

IOT Service Provider

Common data models that should be used are described in 4.3.1 Common Data Models.

6 Data

This section includes guidelines to facilitate data exchange between IoT components and transferring data securely.

6.1.1 Common Data Models

Establish and follow a common metadata model

:Applies to

IOT
Device
Manufacturer

IOT
Service Provider

Metadata is the data that describes other data. Metadata identifies:

- The name of the data set
- The description
- Update history
- Frequent updates
- Licensing
- The category or group to which the dataset belongs to
- Keywords or notices
- Explanations or formulas for how to extract data or their equations
- Quality specifications and related restrictions

Applications manipulate data described by metadata. Metadata offers a common reference point for all data within a specific information technology environment. The role of metadata is enhanced in IoT environments due to the complexity manifested in a significant number of applications, databases, and dataflows. A lack of a reference data description could result in IoT ecosystem malfunctions since data manipulation is reflected in the real world by affecting operations of different things like machines, vehicles and buildings.

One common malfunction occurs if particular data attributes are defined differently in two IoT applications, and thus, these two applications interpret that data differently. The lack of a common metadata model is often the cause of such situations. For example, a device attached to a thing, such as an oil pipeline, sends an alert message when there is a sudden rise of pressure in a pipeline's fragment towards an appropriate application in the core. The application receives this message, parses it and moves for further processing. However, suppose parsing and processing rules are built upon a data model which does not share the metadata model with the data model used by the device. In that case, it is highly likely that the original alert message will not be adequately interpreted, resulting in a life-threatening situation in the real world.

Specific ontologies are applied to build a metadata model. IoT is not an exception in this regard. Ontologies provide rudimentary definitions of the concepts and relations, capturing the knowledge of a particular domain. The diagram below shows the process of building data models, starting from selecting appropriate ontologies.

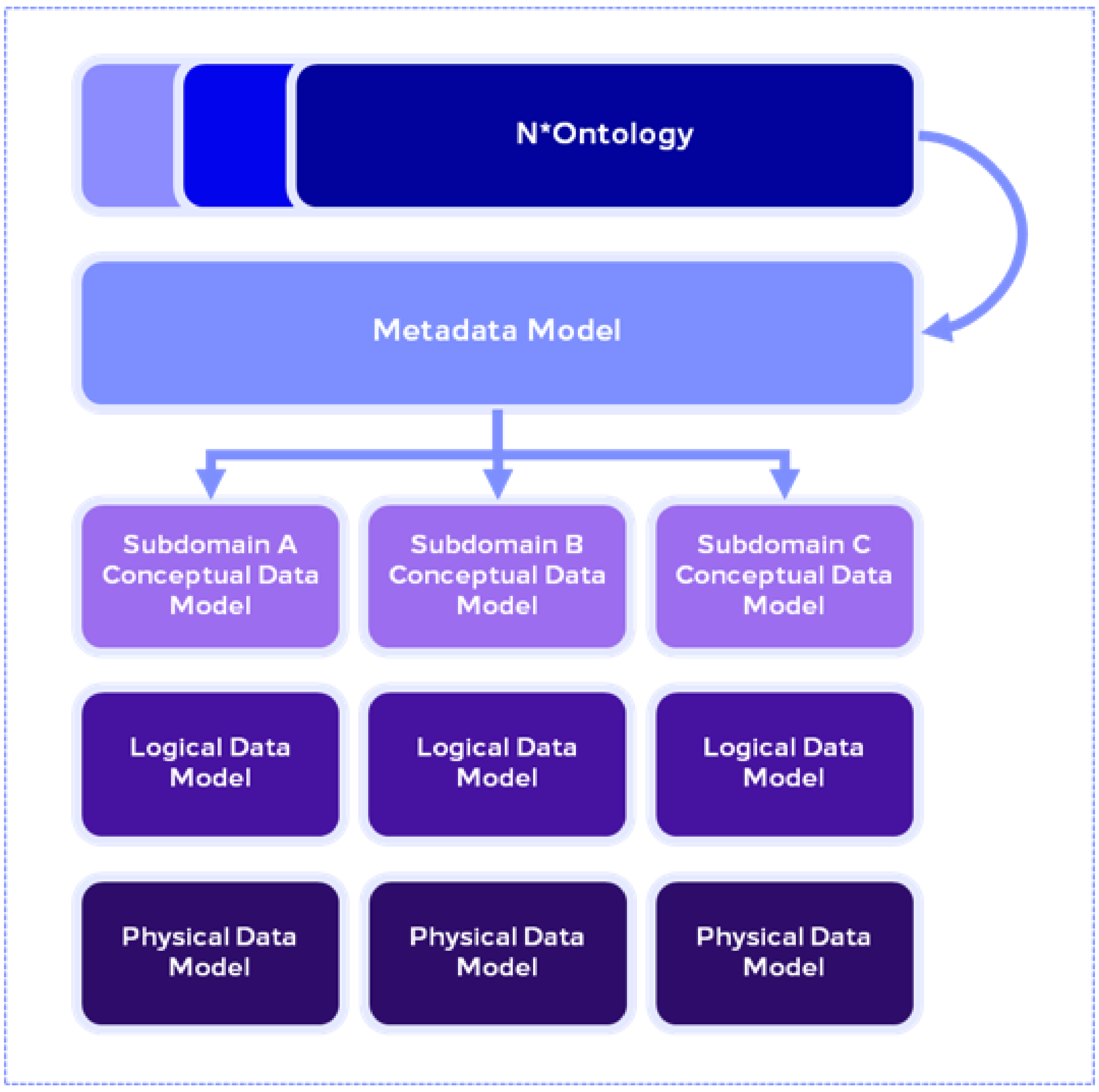


Figure 4: Applying ontology for data modelling scheme

Applying the metadata model in the way described above contributes to ensuring interoperability among applications inside the IoT environment.
There are other business domain-specific ontologies available. However, one of the most commonly used is a set of ontologies addressing Industry 4.0 specific departments such as aerospace, oil & gas etc.

Source of the relevant standard:

Context Information Management (CIM); NGSI-LD API

6.1.2 Input Data Validation

Validate data incoming through user interfaces or transported by APIs

Applies to :

IOT
Service Provider

Incorrectly formatted input data that is not fully validated can expose systems. Hackers employ tool that can snoop on such data and find potential gaps to send data that disrupts or attacks the system.

Examples include, though are not limited to, data:

- Instead of text, there is executable code
- Value out of range, for example, too high voltage
- Database command sent via the user interface because it lacked sanitisation

6.1.3 Backup Strategy

Create data backup plans

Applies to :

IOT
Service Provider

Data backup plans are necessary to prevent potential data loss.

Storing the backup copy in a different physical site prevents the backup from being impacted by the primary site's availability, and businesses can expect a quicker recovery of their operations.

6.1.4 Data Retention

Establish and follow data retention rules

Applies to:

IOT Device Manufacturer

IOT Service Provider

Data is the most valuable asset of IoT ecosystems. As such, it must be manageable and securely collected, stored, archived, and removed throughout its whole life cycle.

IoT players should follow KSA's data retention regulations that apply to the appropriate IoT sector.

7 Security

This section includes guidelines to increase security of IoT applications through domain access control, high availability, software maintenance, encryption.

7.1.1 Domain Access Control

Create and use a system to control access to resources of an IoT service domain

Applies to:

IOT
User

IOT
Device
Manufacturer

IOT
Service Provider

The Authentication, Authorisation and Accounting (AAA) systems can be employed to control access. The three concepts of AAA are:

Authentication **is the process of proving the identity of a person or application. Authentication happens at the start of the authorisation process, and the exchange of data**

Authorisation **refers to the process of specification and verification of the level of access,**

Accounting **refers to measuring the consumption of resources during service exchange**

AAA systems may vary from one domain to another. Thus, a software component capable of mapping real-time user access rights in one AAA system into user access rights in another should be added to the IoT ecosystem.

IoT domain is an IoT computing environment with users and resources subject to the same set of access control policies that concern AAA from the security perspective.

7.1.2 High Availability

Ensure high availability of devices, platforms and applications

Applies to:

IOT
Device
Manufacturer

IOT
Service Provider

Ensuring the high availability of IoT services protects IoT ecosystems from disruptions caused by outages and denial-of-service attacks.

To maintain high service availability, devices, platforms and applications in the IoT environment should possess resilience capability against network and power outages. They should also be capable of either identifying and rejecting malicious service requests or scaling up to handle a flood of requests sent by malicious actors.

In case an outage happens, the IoT environment should:

Not inflict any damage to its respective components, retaining the integrity of its data and the functionality of its devices, platforms and applications

Recover without disruption in a controlled manner while avoiding overloading the network

IoT devices should remain operational as much as possible. However, platforms and applications should be capable of handling a sudden influx of data generated during connectivity downtime from devices capable of storing it while disconnected.

7.1.3 Software Maintenance

Establish and follow procedures for maintenance of IoT software

Applies to:

IOT
Service Provider

IoT software is distributed on:

- Devices
- Platforms
- Applications

Maintenance procedures entail applying fixes, patches and updates to the software following the established rules.
An example of a maintenance procedure:

01 Periodically check for device firmware updates

02 When a new device firmware update is released, schedule a rollout to devices during the nearest period of low network traffic

03 Afterwards, check whether the update has been applied without errors

Maintenance procedures should be automated through IoT Platforms whenever possible.
Updates should be timely and should not negatively impact the system's functioning. As far as devices are concerned, an end-of-life policy should be published. The standard functions should continue to be operational while an update is underway.

Apply security patches delivered over a secure channel periodically

Applies to :

- IOT User
- IOT Device Manufacturer
- IOT Service Provider

Security patches prevent the IoT ecosystem from being subjected to unauthorised access or attacks from outside by using existing vulnerabilities or new attack methods. IoT Device Manufacturers and IoT Service Providers should provide and deliver these patches, and IoT User should install them without unnecessary delay.

7.1.4 Encryption

Encrypt indiviuals-related and contextualised data

Applies to:

IOT
Service Provider

It is essential to encrypt data. Encryption protects data during transfers and transformations. Furthermore, it reduces the risk of abuse as access is limited only to authorised people and systems.

In IoT, due to vast amounts of raw data, it is not economical to encrypt all data. However, context changes data into information. Information needs to be protected; hence only contextualised data should be encrypted.

For example, data containing the geographic location of vehicles used for traffic congestion tracking can be transmitted and processed unencrypted. However, the geographic location of a vehicle in the context of the vehicle's registration is the personal data of that vehicle's owner and should not be accessed unauthorised. Therefore, transmitting and processing geographic location coupled with vehicle identification data requires encryption to secure privacy.

References

1- CST Regulations

https://regulations.citc.gov.sa/en/pages/published-document.aspx#/published-document

2- Equipment Approval and Licensing | CST Statutes

https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/EquipmentApproval/Pages/default.aspx

3- Technical Specification Category of Telecommunications and Information Technology Equipment | CST Statuteshttps://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/EquipmentApproval/Pages/Technical_Specification.aspx

4- Maintaining the Privacy of Personal Data | CST Statutes

https://www.cst.gov.sa/en/RulesandSystems/privacy/Pages/default.aspx

5- Wireless Local Area Networks Regulation | CST Statutes

https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/OtherRegulatoryDocuments/Pages/CITCWirelessLocalAreaNetworksRegulations.aspx

6- Y.101 : Global Information Infrastructure terminology: Terms and definitions

https://www.itu.int/rec/T-REC-Y.200003-101-I/en

7- Matter Standard: Matter | Smart Home Device Solution

https://csa-iot.org/all-solutions/matter/

8- ISO/IEC 1:2019-21823 Interoperability for IoT systems: Part 1: Framework

https://www.iso.org/standard/71885.html

9- ISO/IEC 2:2020-21823 Interoperability for IoT systems: Part 2: Transport interoperability

https://www.iso.org/standard/80986.html

10- ISO/IEC 3:2021-21823 Interoperability for IoT systems: Part 3: Semantic interoperability

https://www.iso.org/standard/83752.html

11- ISO/IEC 4:2022-21823 Interoperability for IoT systems: Part 4: Syntactic interoperability

https://www.iso.org/standard/84773.html

-12 3GPP TS 23.501 – System architecture for the 5G System (5GS)

https://itectec.com/archive/3gpp-specification-ts-501-23/

-13 5G; Management and orchestration; Architecture framework

https://www.etsi.org/deliver/etsi_ts/60_15.00.00/128533/128599_128500/ts_128533v150000p.pdf

14- Context Information Management (CIM); NGSI-LD API

https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.03.01_60/gs_cim009v010301p.pdf

15- Common API Framework for 3GPP Northbound APIs
https://www.etsi.org/deliver/etsi_ts/60_15.02.00/123222/123299_123200/ts_123222v150200p.pdf

16- OMA LightweightM2M Overview

https://technical.openmobilealliance.org/Overviews/lightweightm2m_overview.html

17- IETF | Constrained Application Protocol (CoAP)

https://datatracker.ietf.org/doc/html/rfc7252

-18 3GPP TS 23.501 – System architecture for the 5G System (5GS)

https://itectec.com/archive/3gpp-specification-ts-501-23/

19- Multi-access Edge Computing (MEC) Framework and Reference Architecture

https://www.etsi.org/deliver/etsi_gs/MEC/60_02.02.01/003/099_001/gs_MEC003v020201p.pdf

20-Multi-access Edge Computing (MEC) MEC 5G Integration

GR MEC 031 - V2.1.1 - Multi-access Edge Computing (MEC) MEC 5G Integration (etsi.org)

CST

هيئة الاتصالات والفضاء والتقنية

Communications, Space &
Technology Commission