RV College of Engineering®

UNIT-I
Introduction, and Architecture and Fundamentals

Prof. Narasimha Swamy S
Department of AIML
RV College of Engineering
Bengaluru-59

Go, Change the World

Content

→ Applications
- Asset Management
- Biometrics Identification
- Smart Home
- Bird Strike Avoidance Radar System
- River Navigation Safety System

→ Introduction to Internet of Things (IoT)
- IoT Concept
- Related Concepts of IoT
- The Intrinsic Characteristics of IoT
- IoT Development and Application
- Future IoT Vision

→ Architecture and Fundamentals
- Some Research on IoT Architecture
- Ubiquitous IoT (U2IoT) Architecture
- Some Layered Models for IoT
- Layered Model Proposed and Social Attributes
- IoT Development Phases Summary and Discussion
- Science Category and Supporting Technologies for IoT

Applications

- → Asset Management
- → Biometrics Identification
- → Smart Home
- → Bird Strike Avoidance Radar System
- → River Navigation Safety System

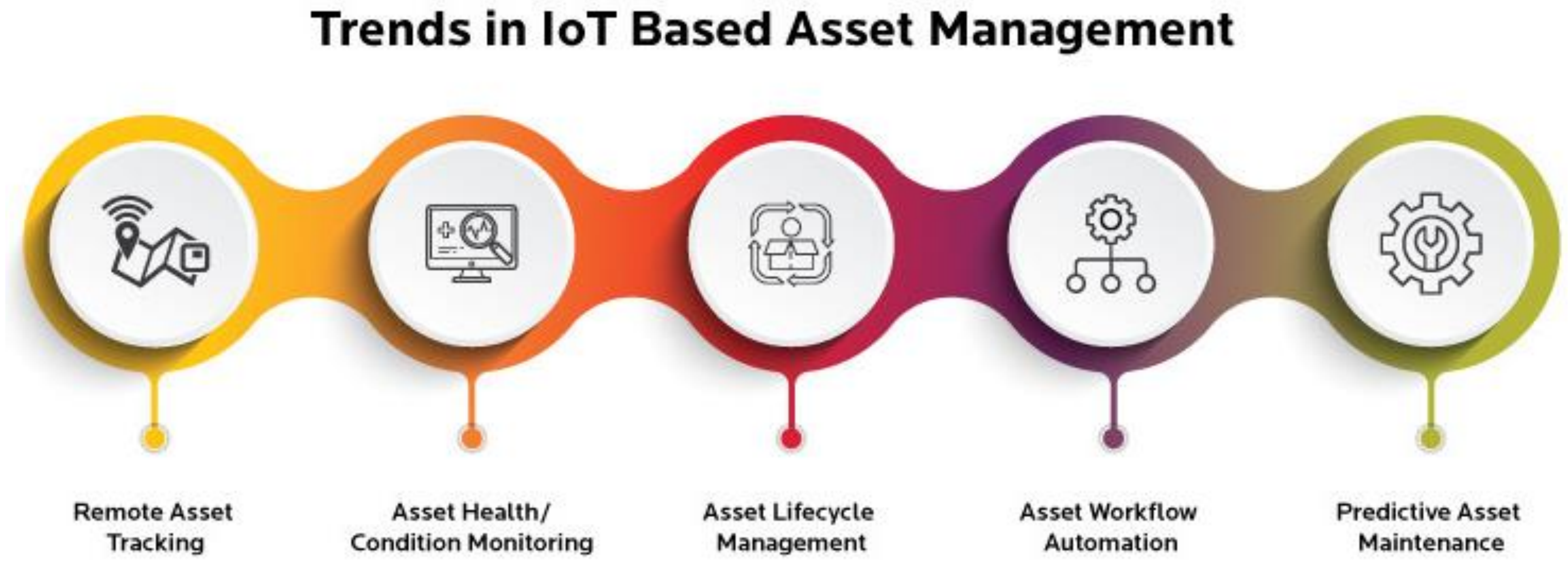
Applications

Asset Management System

- An asset management system is a process used by an organization to manage all of its assets across the business
- They can include personnel, buildings, software and hardware, inventory, monetary assets, and anything vital to the business's day-to-day running
- Asset can be tangible or intangible.
- Availability, Performance, and Quality are the three critical drivers for overall equipment effectiveness (OEE) for a manufacturing entity
- IoT-powered solutions will help monitor and detect specific problems, such as missing parts, faulty areas, and scope of improvement.
- With these improvements, the firm can achieve 80% OEE

Applications (Contd.)

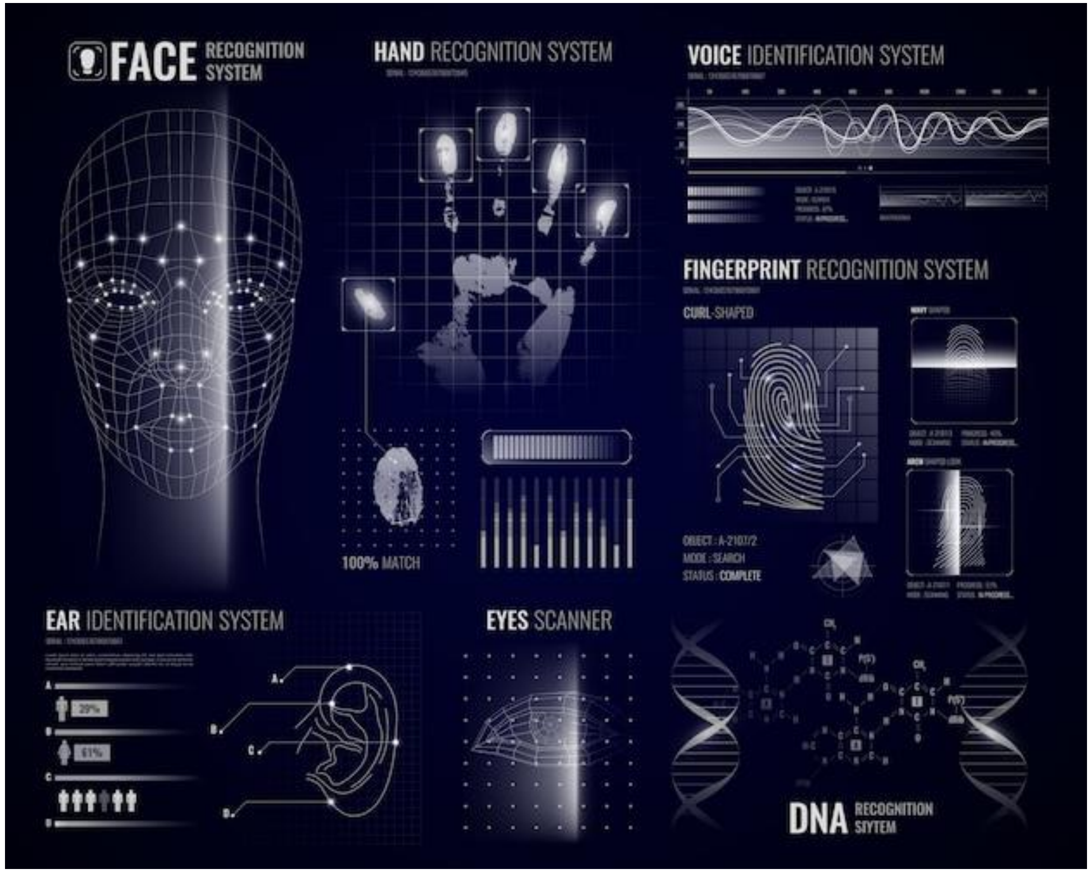
Asset Management System

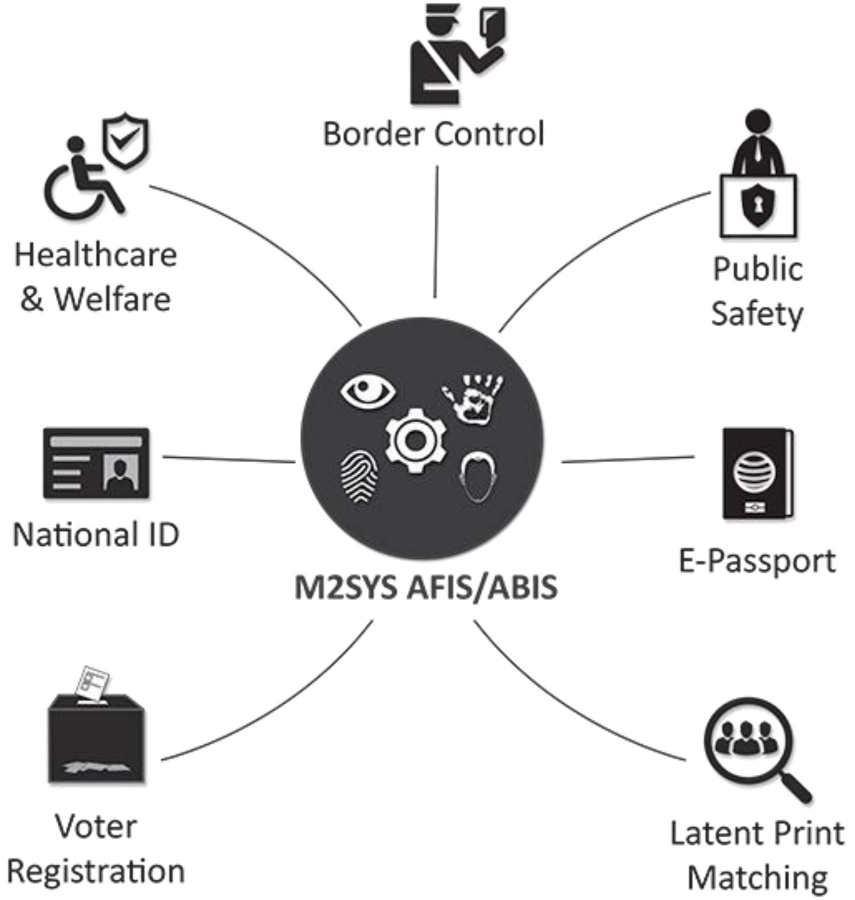


Applications (Contd.)

Biometrics Identification

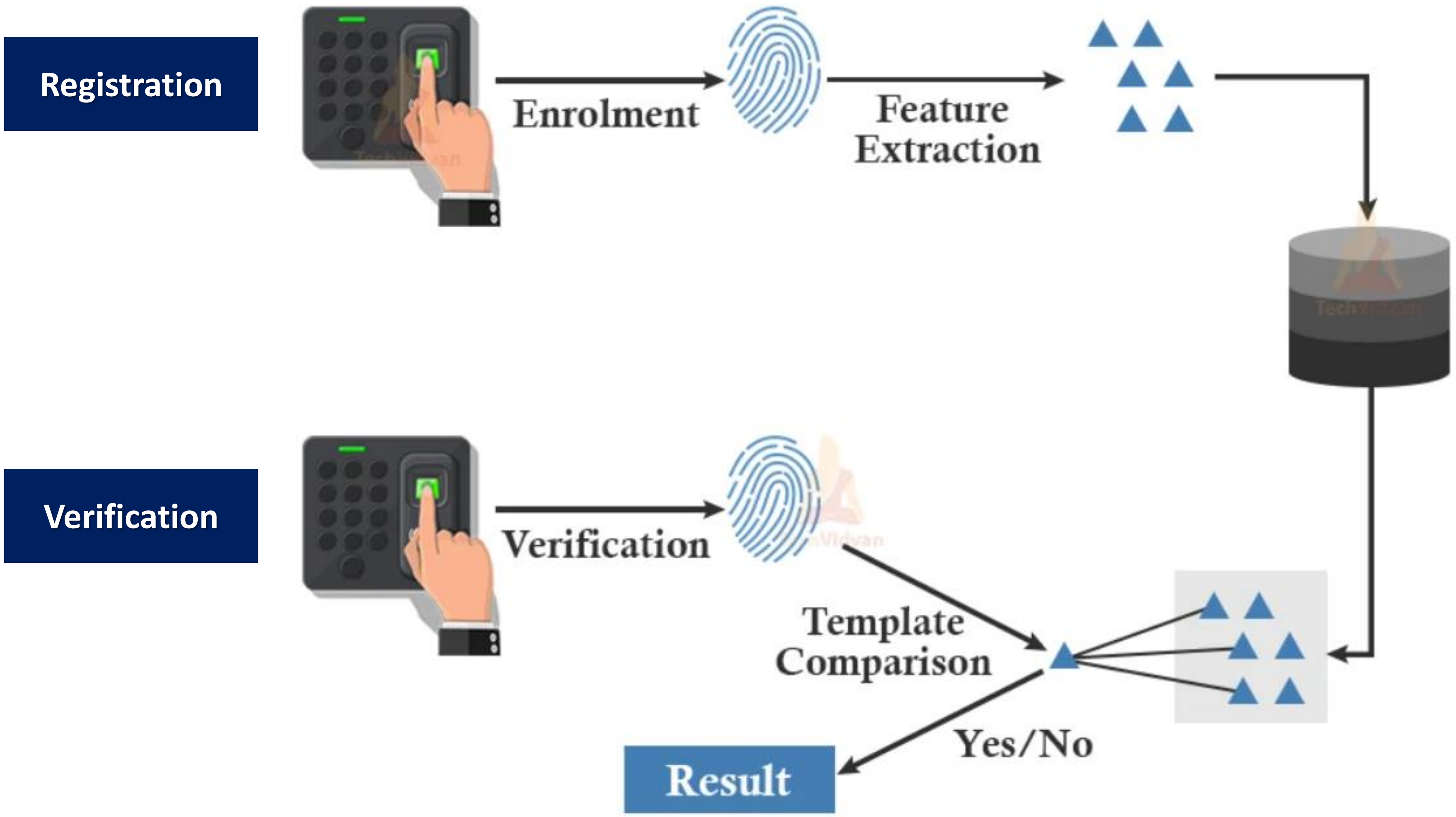
→ Biometric identification uses unique biological features to identify and verify an individual. These attributes include fingerprints patterns, facial features, eye structures, DNA, speech, and even handwriting.





Applications (Contd.)

Biometrics Identification

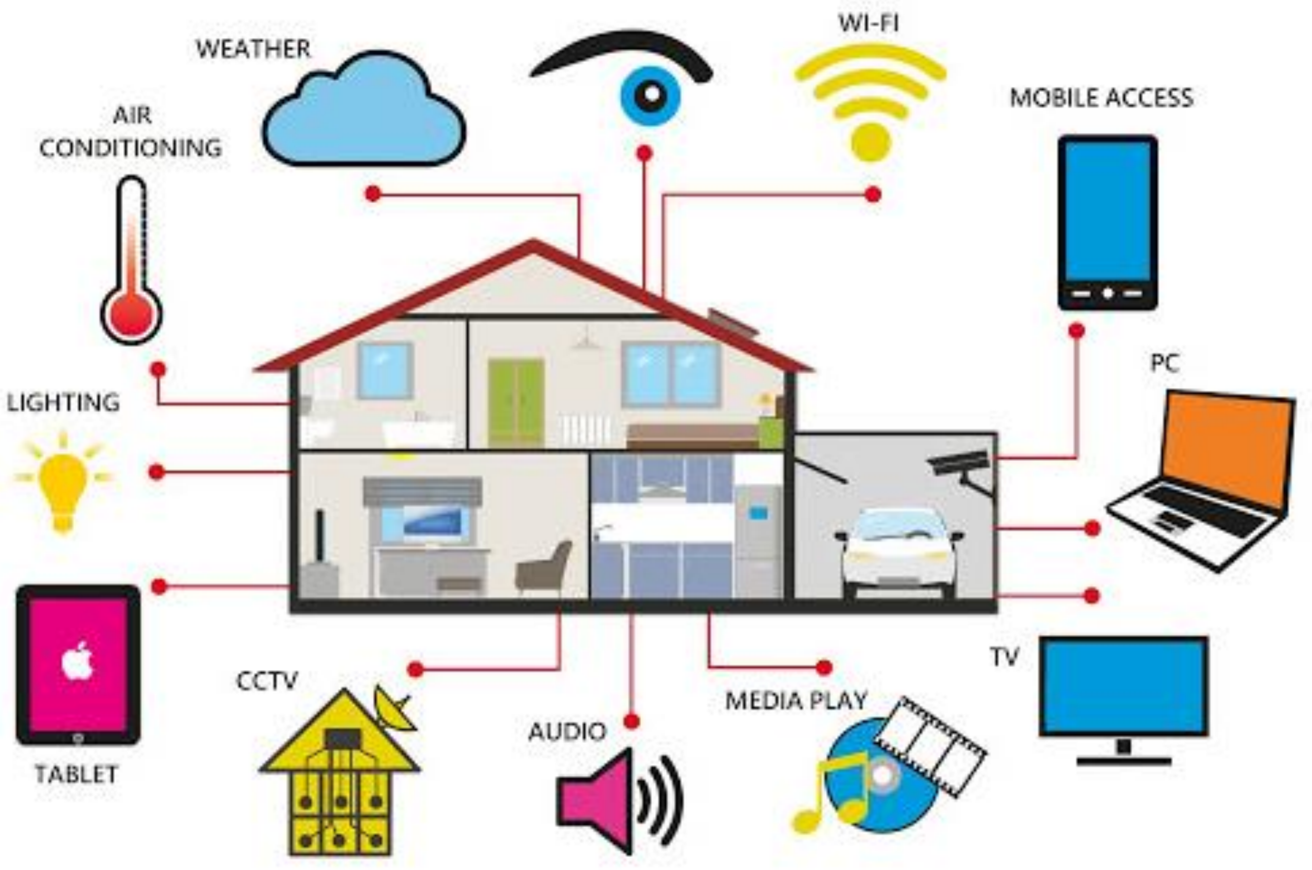


Applications (Contd.)

Smart Home

→ A smart home refers to as a concept where appliances and devices can be automatically controlled remotely from anywhere with an internet connection using a mobile or other networked device

→ Devices in a smart home are interconnected through the internet, allowing the user to control functions such as security access to the home, temperature, lighting, and a home theater remotely



Applications (Contd.)

Smart Home

Home Entertainment

- Smart TV
- Smart Speaker
- Smart Set Top Box
- Gaming Consoles
- Streaming Devices
- Audio Video Receiver
- XR Headset

Energy Management

- Smart Thermostat
- Smart Meters
- Smart Bulbs
- Smart Switches
- Smart Plugs
- Smart Lamps
- Smart Boilers

Safety and Security

- Smart Blinds/Shutters
- Alarm Systems
- Motion Sensors
- Smoke Detectors
- Gas Leak Detectors
- Security Camera
- Smart Locks
- Smart Video Doorbell
- Thermal Detectors
- Smart Baby Monitor

Comfort and Ease (Appliances)

- Smart AC
- Smart Fridge
- Smart Kettle
- Smart Coffee Maker
- Smart Washing Machine
- Smart Dryers
- Smart Robot/Cleaner
- Smart Oven
- Precision Cooker
- Smart Dish Washer
- Smart Water Purifier
- Smart Water Heater
- Smart Air Purifier

Lifestyle and Health

- Smart Toothbrush
- Smart Yoga Mat
- Smart Alarm Clock
- Smart Bed
- Smart Thermometer

Applications (Contd.)

Bird Strike Avoidance Radar System

→ Bird strike avoidance radar systems are crucial tools used in aviation to detect and avoid potentially hazardous bird movements

→ Bird Strike is common and can be a significant threat to aircraft safety

→ For smaller aircraft, significant damage may be caused to the aircraft structure and all aircraft, especially jet engine ones, are vulnerable to the loss of thrust which can follow the ingestion of birds into engine air intakes

→ Trends

- Real-time Data Collection: Monitors the weather conditions, bird migration patterns, and bird movement detection using various sensors
- Integration with Aircraft Systems: IoT integration can enable the bird strike avoidance radar systems to communicate with onboard aircraft systems.
- Collaborative Bird Strike Avoidance: With IoT, bird strike avoidance radar systems can connect with other radar systems and share data.
- Intelligent Alarming Systems: IoT can facilitate the implementation of intelligent alarm systems that prioritize alerts based on the severity of the bird strike risk.

Applications (Contd.)

River Navigation Safety System

→ River Navigation Systems enable

- Safety of the Ship and Lives
- Protection of Environment
- Protect of the Property
- Avoids Financial Losses and Time

→ Real-time Data Collection: IoT devices, such as sensors and cameras, are deployed along riverbanks, on vessels, and at key points in the river to collect real-time data

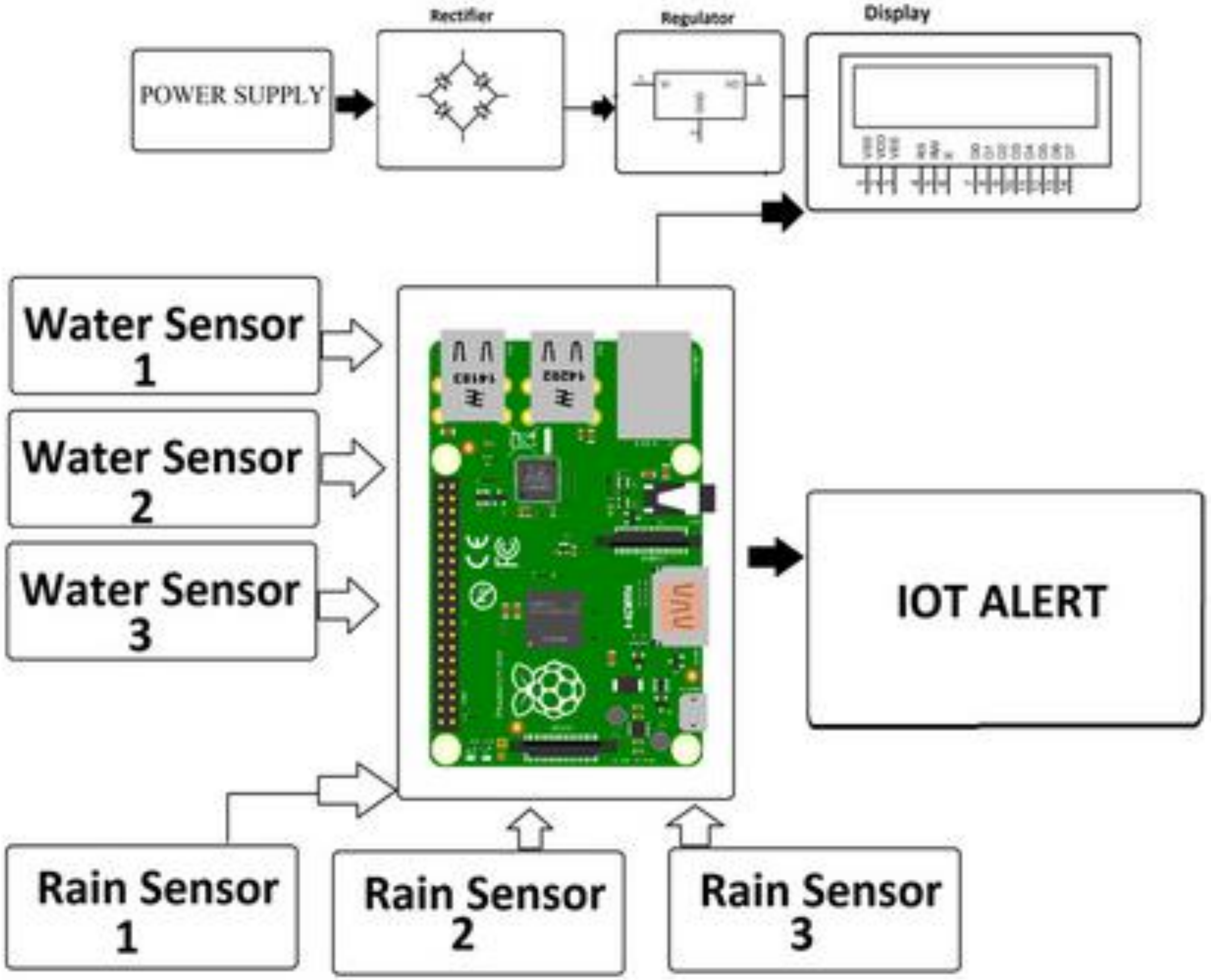
→ Safety Alerts and Warnings: IoT systems can issue real-time alerts and warnings to vessel operators and authorities. For instance, if water levels rise to dangerous levels or a vessel deviates from its planned course, automated alerts can be sent to relevant parties, ensuring timely responses to safety concerns

→ Vessel Tracking: To detect, identify, and monitor a ship's location, and map the full details of the entire route

→ Search and Rescue Operations

Applications (Contd.)

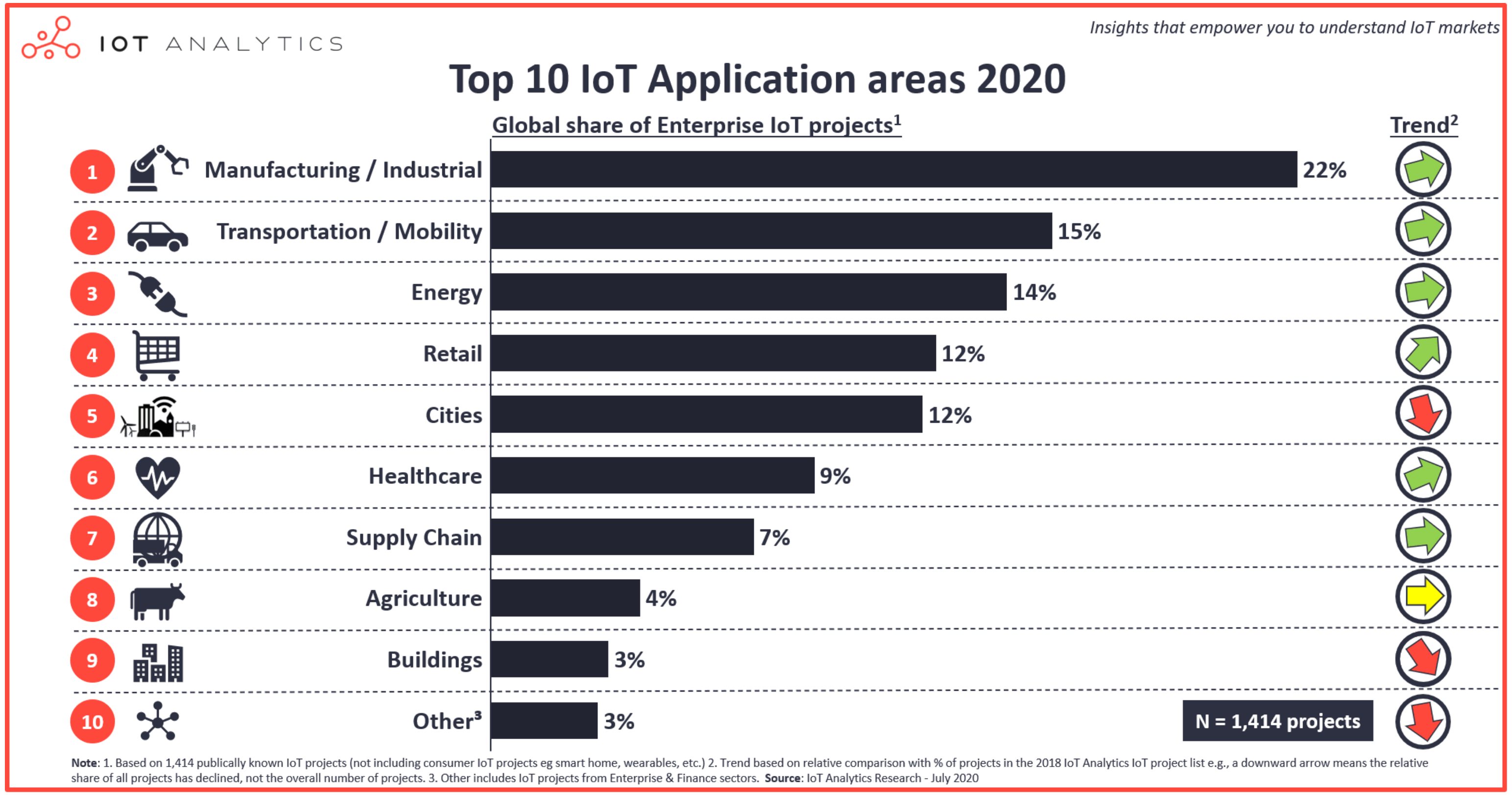
River Navigation Safety System



Introduction

→ Internet of Things (IoT) attracts great attention and brings with it promising opportunities and challenges.

→ Research on IoT has important economic and social value for the development of the next generation of information, network, and communication technologies.



Concept of IoT

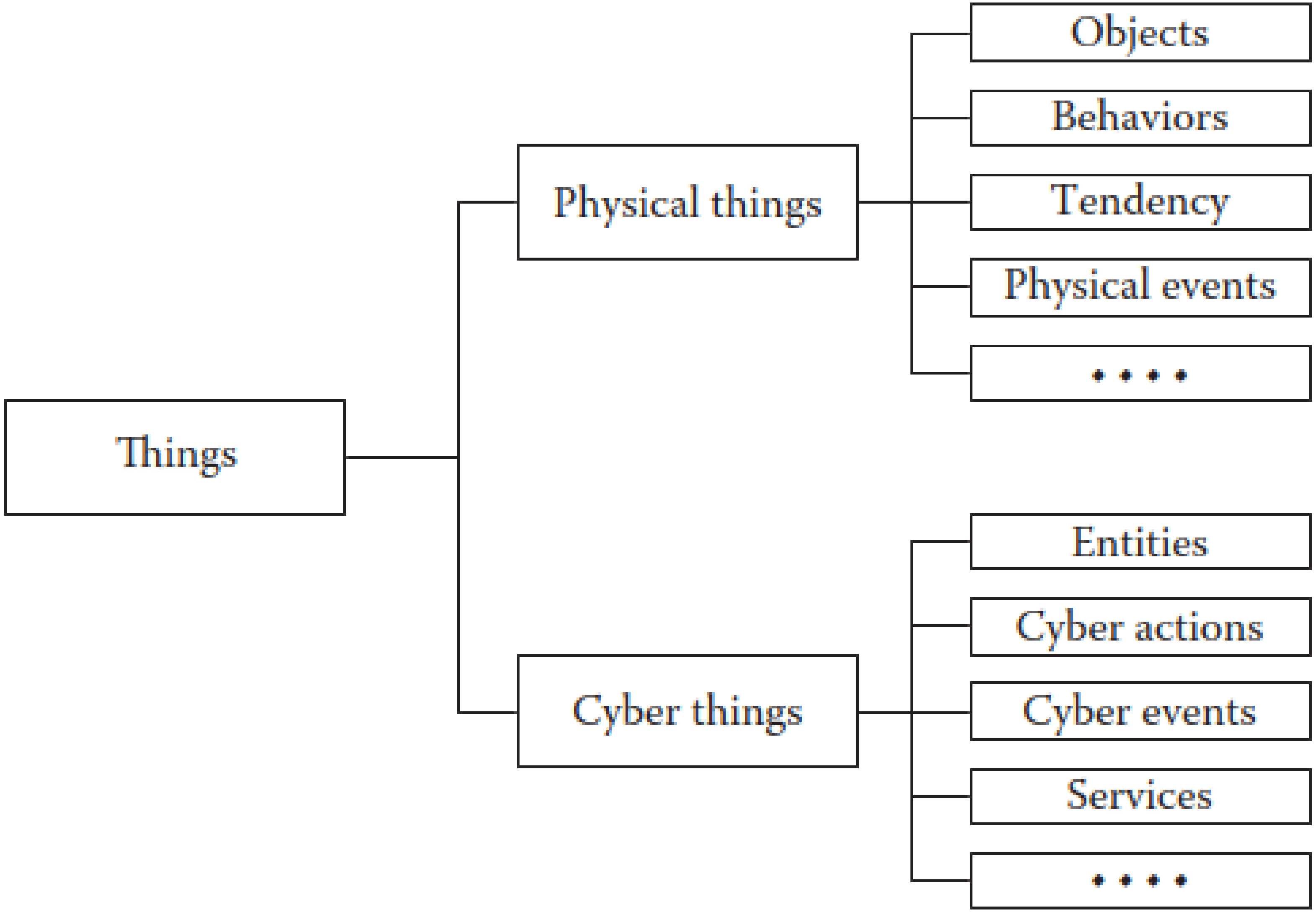
- → The phrase "Internet of Things" was proposed by MIT (Massachusetts Institute of Technology) Auto-ID Center in 1999.
- → Such an embryonic definition of IoT refers to constructing an Internet-based network covering all the things in the world by using related technologies
- → The Internet of Things, published by the International Telecommunications Union, pointed out the IoT concept and expanded its meaning, and indicated that RFID technology, sensor technology, nanotechnology, and intelligent embedded technology are the four core technologies to realize IoT.
- → In recent years, IoT has been redefined depending on different perspectives and application scenarios
- → The Cluster of European Research Projects on the Internet of Things Strategic Research Roadmap, announced by the European Union in 2009, stated that IoT is an integrated part of Future Internet and could be defined as

  "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocol"

- → In IoT, things refer to the ubiquitous things in the physical world and cyber world.

Concept of IoT (Contd.)

→ Things are classified into two types: Physical things and Cyber things



Concept of IoT (Contd.)

→ The physical things mainly include objects, behaviors, tendencies, and physical events

- **Objects** (e.g., a person, vehicle, table, and bird) indicate concrete things with tangible bodies.
- **Behaviors** (e.g., running, monitoring, eating, shouting, catching, and driving) indicate movements with certain motivations of certain objects.
- **Tendency** (e.g., weather is becoming clear, the traffic is becoming crowded, and communication is going to finish) indicates trends in the things of themselves or under a certain external environment.
- **Physical events** (e.g., a tornado happens in a certain place) generally consist of objects, behaviors, and certain causation, indicating things happening, which are triggered by certain conditions in the physical world.

Concept of IoT (Contd.)

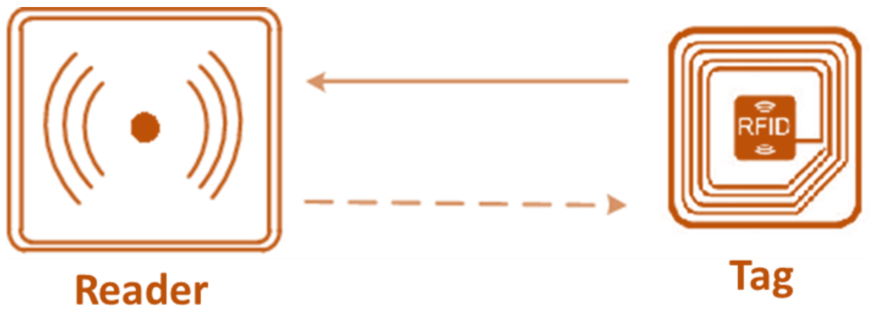
→ The cyber things include entities, cyber actions, cyber events, and services.

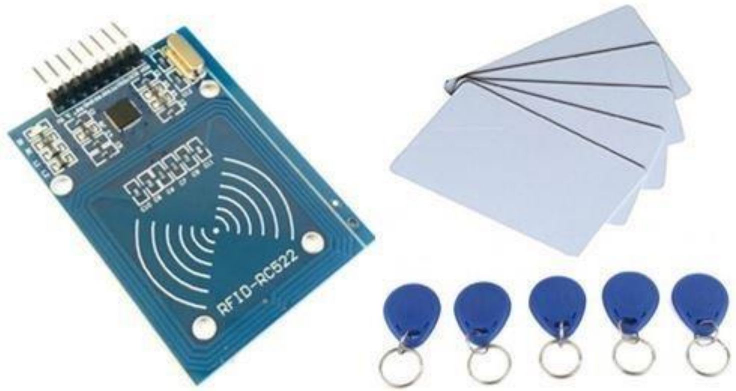
- **Entities** (e.g., Web page, software, codes, and data) indicate the abstract things in the cyber world.
- **Cyber actions** (e.g., things, coding, and data transmission) indicate the processing of virtual things.
- **Cyber events** (e.g., online payment is conducted) indicate the things consisting of entities, cyber actions, and certain causation in the cyber world.
- **Service** (e.g., the Domain Name System [DNS] query service) indicates the functions that a thing can offer or be offered for certain goals.

Related Concepts in IoT

→ As the concept of IoT is usually confused with other related concepts, such as Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), Electronic Product Code (EPC), Machine to Machine (M2M), Cloud Computing, and Cyber-Physical Systems (CPS), they are briefly introduced as follows:

- RFID is a wireless automatic identification technology, relying on the RF communication technology to identify objects attached with RFID tags by an RFID reader.





  - The identification can be performed to determine presence, location, Consistency, authentication, and other identity-related applications.
  - Currently, RFID has been widely applied in fields including transportation, logistics, etc.
  - It is an important sensing method for IoT

Related Concepts in IoT (Contd.)

→ EPC is a typical early IoT solution based on RFID technology for the global logistics applications proposed by EPC global (Standard)

- EPC standards are regarded as a special kind of RFID application standard, as the front-end sensing is RFID, while only two RFID frequency bands in ISO/IEC 18000 are involved
- In addition, it also includes EPC coding, Object Naming Service (ONS), and EPC Information Services (EPCIS), and is a global and systematic specification.

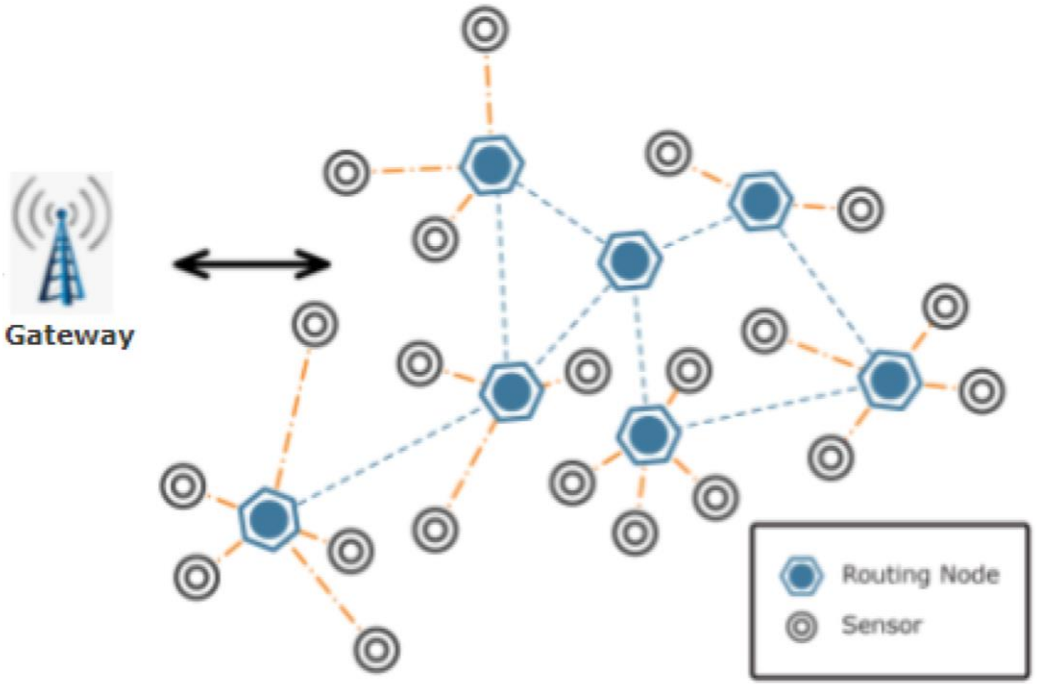
EPC Type	Manufacturer	Product Type	Unique Item
01	. 1234567	. 891011	. 001122DBC
Header 8-bits	EPC Manager 28-bits	Object Class 24-bits	Serial Number 36-bits
256 Combinations possible	268,435,456 Combinations possible	16,777,216 Combinations possible	68,719,476,736 Combinations possible

- Similarly, Ubiquitous ID (UID) proposed by Japan is another typical early IoT solution based on RFID technology, which is composed of ubiquitous code (Ucode), ubiquitous communication, a Ucode resolution server, and an information system server.

Related Concepts in IoT (Contd.)

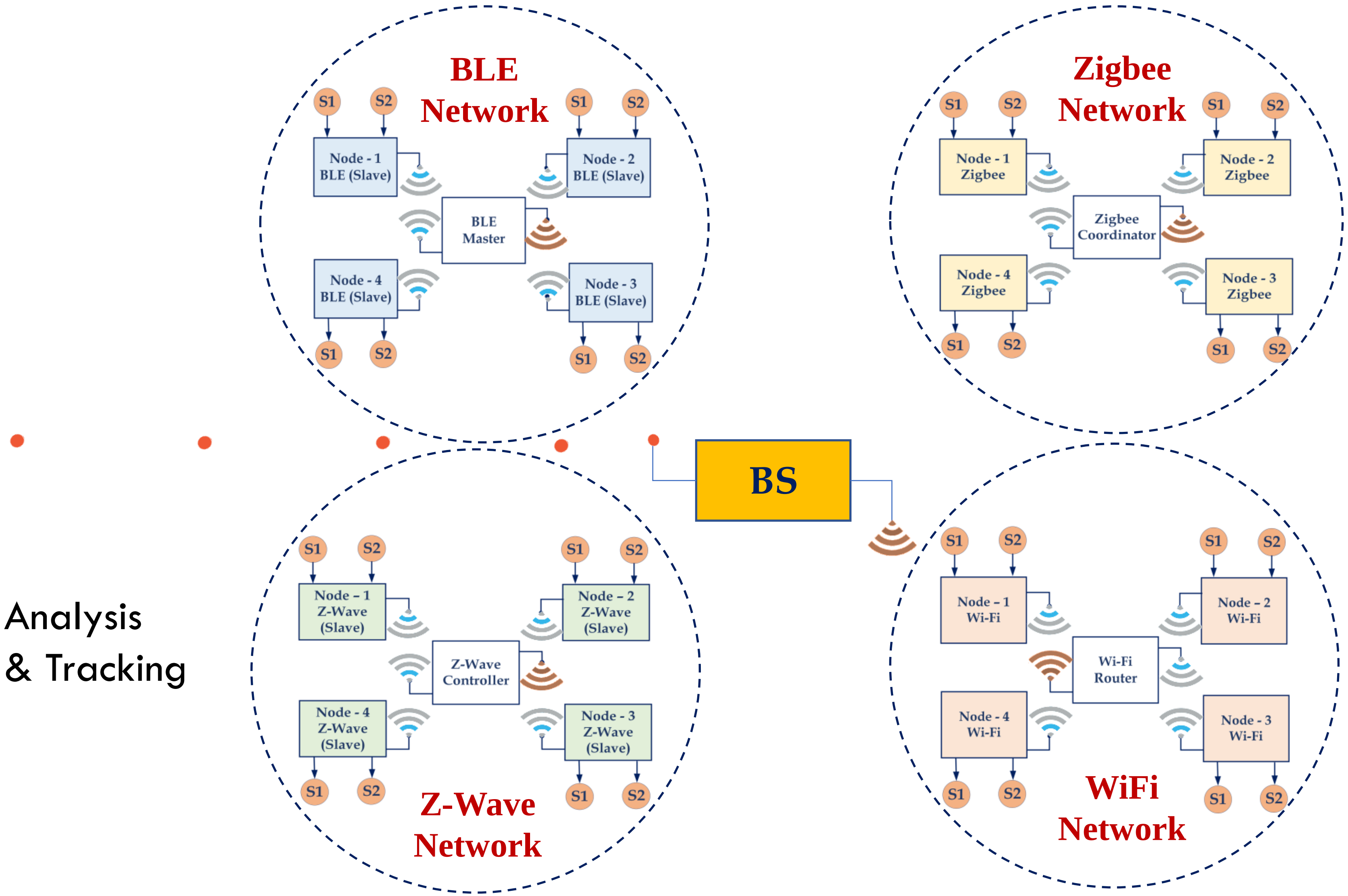
→ Wireless Sensor Networks is an integration sensing, computation, and communication

- It is a wireless network consisting of enormous distributed autonomous sensors to monitor an environment or object's information, and has low-power, low-cost, distributed, and self-organization characteristics.
- WSN belongs to a kind of access network for IoT.
- Thus far, main technologies used to realize WSN include Zigbee, Bluetooth, Wi-Fi, and so on.



Concept of IoT (Contd.)

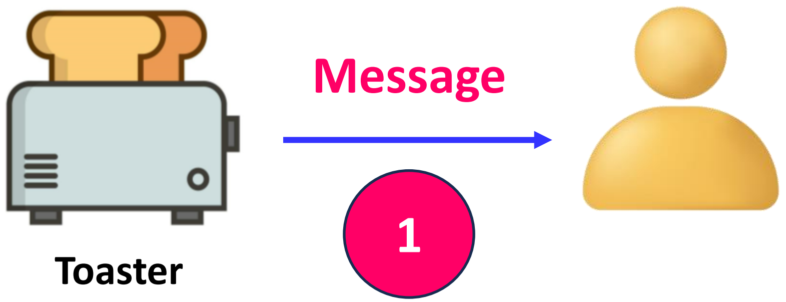
1. Data Storage
2. Data Processing and Analysis
3. Device Management & Tracking



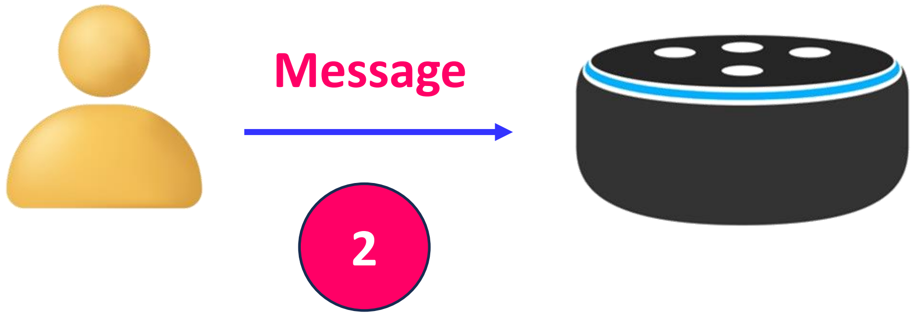
Related Concepts in IoT (Contd.)

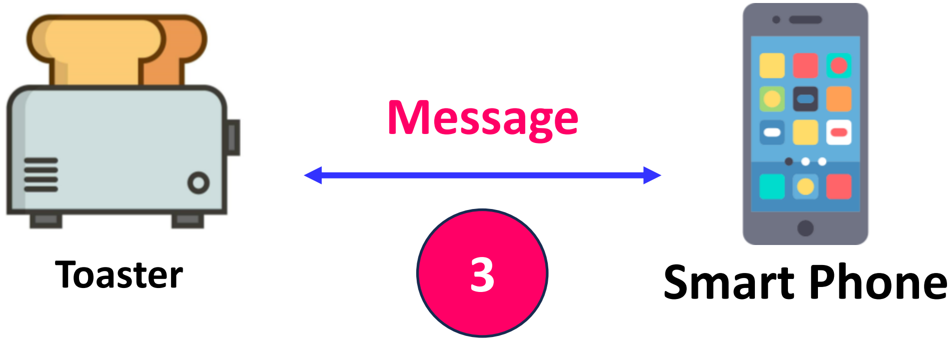
→ **M2M** - Machine-to-Machine (M2M) communication mode, to realize the connection of systems and remote devices

- With the expansion of the M2M concept, it also refers to the communication that transmits data to applications
- IoT involves various kinds of communication modes
  1. Thing-to-Human
  2. Human-to-Thing
  3. Thing-to-Thing communications



- M2M is thought to be a promising technology for IoT
- Meanwhile, M2M is also regarded as an application form of IoT





Related Concepts in IoT (Contd.)

→ Cloud Computing is a network application mode, providing services in a demand assignment and scalable way by the network

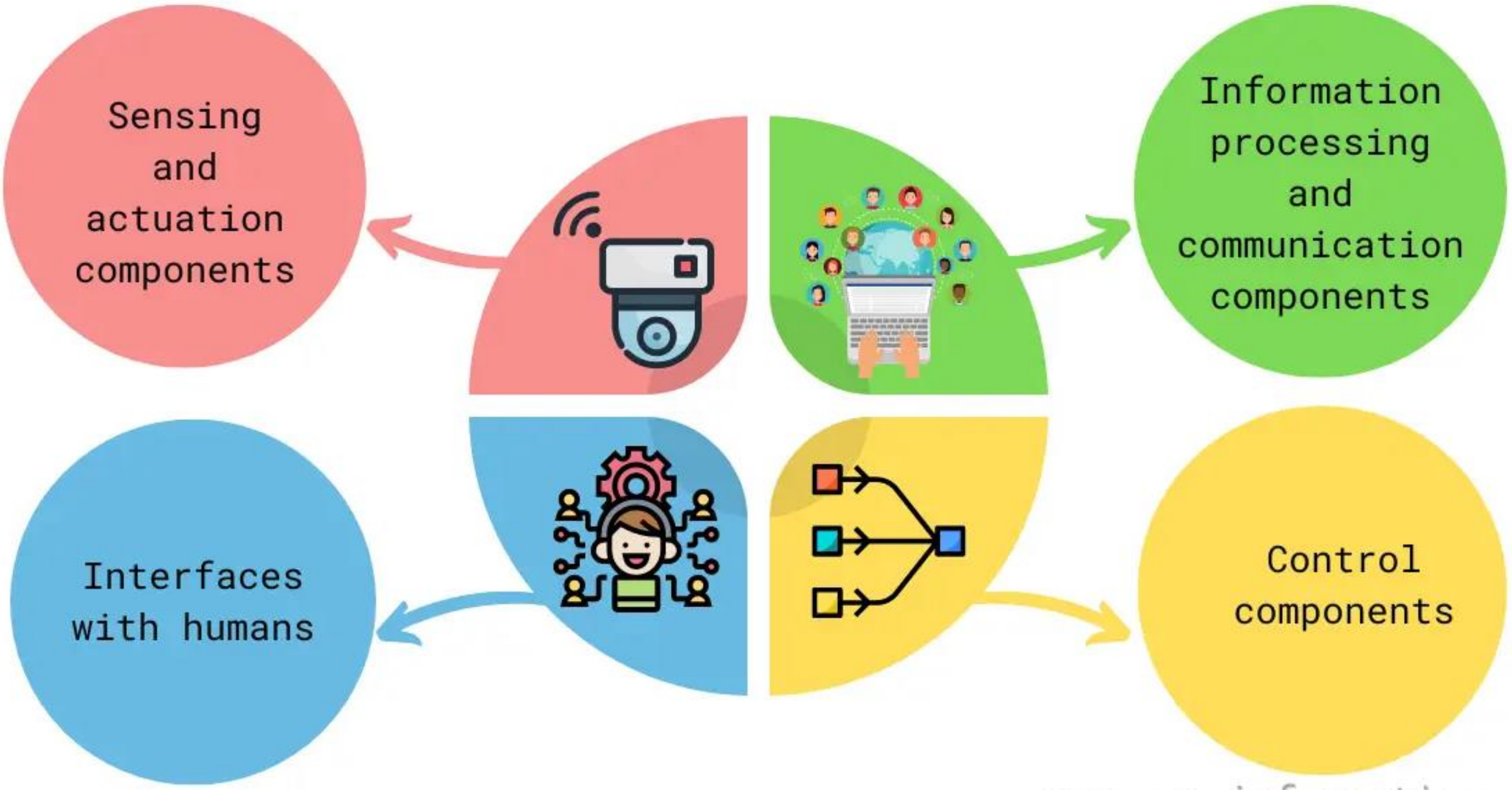
- It includes three fundamental types of models: Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS).
- Services are provided according to one type.
- The end users just need to focus on the required resources and access approaches.
- Cloud computing aims to solve the huge data storage and processing problems brought on by the Internet.
- Currently, companies such as Google, Amazon, IBM, and SUN have increased investment and research efforts in cloud computing.
- With IoT development, the huge data storage and computing need the support of cloud computing technology.
- In turn, cloud computing technology advancement will drive IoT development.

Related Concepts in IoT (Contd.)

→ CPS - CPS is the system that combines computing, network, and physical environment.

- It provides services such as real-time sensing, dynamic control, and information feedback to realize the interaction of the physical world and cyber world by integration and collaboration of computation, communication, and control (3C) technologies.
- CPS and IoT have many similarities, and both need sensing, computing, information transmitting, and interaction technologies to enhance the combination of the cyber world and physical world.
- Meanwhile, they also have some differences.
  - IoT emphasizes the connection of things with networks, while CPS emphasizes the integration of computational and physical elements information
  - Additionally, IoT involves the physical world, cyber world, and social world.
  - CPS has also recently been extended to cyber-physical-social systems.
  - In this perspective, the concepts of IoT and CPS are almost the same, as both highlight the social attributes.

Related Concepts in IoT (Contd.)



Ref: https://www.erp-information.com/cyber-physical-systems?expand_article=1

The Intrinsic Characteristics of IoT

→ Future IoT is highly unified with ubiquitous networks, services, and things, and it establishes the Internet of services, Internet of networks, and Internet of everything

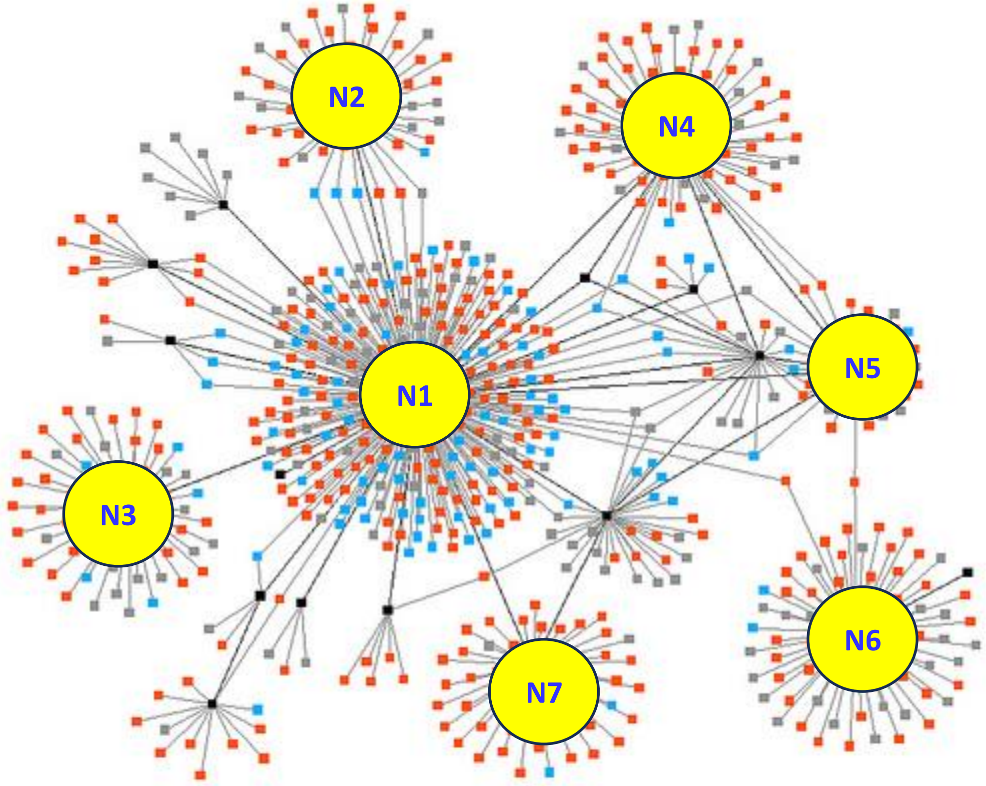
→ As mentioned, "things" covers both the Physical world and Cyber world

→ IoT has three main features:

- **Ubiquitous Sensing**
  - Beyond the sensing ability of humans to the physical world (e.g., vision, hearing, smell, and touch) and the specific sensing function of sensor networks, ideal sensing in IoT includes all the sensing technologies that realize things identification, named ubiquitous sensing
  - The sensing information can include a thing's identifier (i.e., ID), static attributes (e.g., size, color, and shape), dynamic attributes (e.g., behavior tendency and interactions), and environmental information (e.g., temperature, pressure, and humidity).
  - One important goal of future IoT is to unify the physical world and cyber world, and solve human-machine interface bottlenecks by using ubiquitous sensing technologies
  - In addition, along with more and more things mapping from the physical world to the cyber world, there is also increasing feedback from the cyber world to the physical world, and thus control of the physical world is also becoming wider.

The Intrinsic Characteristics of IoT (Contd.)

- **Networks of Networks**
  - IoT involves various kinds of networks.
  - On the one hand, there are many heterogeneous access networks in the sensor-actuator layer
  - On the other hand, heterogeneous communication networks, such as the Global System for Mobile Communications (GSM), code division multiple access (CDMA), and wideband code division multiple access (WCDMA), coexist
  - Future IoT should construct the network of networks, which is a crucial part of IoT development to connect things in both the physical world and cyber world.



The Intrinsic Characteristics of IoT (Contd.)

Intelligent Processing

- Intelligent processing is like human wisdom, but also beyond human wisdom in many aspects, such as it overcomes the shortcomings of the long amount of time needed for learning and the limited ability for parallel information processing.
- In IoT, processing should be realized intelligently.
- An ideal scene is that things can be sensed and controlled automatically with high intelligence
- Intelligent processing results in Real-time information management, flexible production scheduling, and accurate tracking can be achieved
- Intelligent processing capabilities is another goal of future IoT: freeing humans from the information explosion is another qualitative leap after the two industrial revolutions in history

IoT Development and Applications

- IoT is regarded as an emerging industry by some people and even the governments of some nations, while it is also thought to be a new stage in information technology (IT) development
- IoT has attracted great attention in many nations.
- The United States puts significant emphasis on IoT-related technologies, especially standards, architectures, security, and management, trying to possess dominance in the IoT field.
- In 2008, the U.S. National Intelligence Council announced IoT as one of the six technologies in Disruptive Civil Technologies—Six Technologies with Potential Impacts on U.S. Interests out to 2025.
- Meanwhile, many enterprises facilitate IoT development through technology, product, and application innovation.
- In the European Union, IoT research and development (R&D) has been supported by the European Commission (EC) and established as the strategic development plan of European information and communication technologies.

IoT Development and Applications (Contd.)

- In 2008, the EC developed a policy road map for European IoT, and four authoritative documents were announced in 2009, in which Internet of Things—An Action Plan for Europe indicates that the development of IoT has been upgraded to a higher level.
- In addition to the technology and standard aspects, relevant organizations, such as the European Telecommunications Standards Institute (ETSI) and IoT European Research Cluster (IERC), are committed to IoT research projects.
- Some enterprises are also gradually taking action to deploy applications.
- For example, Vodafone has cooperated with Alcart-lucent to develop solutions for the smart grid
- T-Mobile has cooperated with Sierra Wireless to focus on the automobile, shipbuilding, and navigation industries
- The United States, European Union, China, Japan, Korea, and some other nations place great emphasis on IoT research and rom the initial applications in commercial retail and logistics fields, applications are extended to other fields, such as environmental and biomedical monitoring.

IoT Development and Applications (Contd.)

- However, at the present stage, some central enterprises have more abilities to launch some large scale or ultra-large-scale industrial applications, and IoT promotion needs support from the government

Future IoT Vision

- The ideal IoT vision in the future may be an era of harmony of humans with nature, which means harmony, coordination, and coexistence of the physical world, cyber world, and social world.
- In future, IoT should incorporate information exploration, analysis, prediction to achieve a substantial leap to share the benefits brought on by IT technologies. (Efficient Use of IT Technologies)
- For instance, for IoT in the logistics industry, the flow of goods can be instantly monitored and automatically reported, instead of manual searching; for IoT in the power industry, generation, transmission, storage, and distribution of electricity can be arranged efficiently and dynamically;
- IoT in the public security field, intelligence monitoring can be achieved for significant security regions and action can be taken intelligently.
- Future IoT will bring changes in most fields and make things more intelligent to promote the revolution of production capability and modes.

Architecture and Fundamentals

- → Internet of Things (IoT) architecture is the cornerstone for future IoT.
- → It is a fundamental issue that provides a supporting platform for addressing other issues in IoT.
- → The rapid development of IoT around the world has triggered a wave of unprecedented expectation.
- → Several governments have launched massive projects even though the key technologies, including the fundamental architecture of IoT, are still open issues.
- → It becomes very much necessary to study future IoT architecture.

Some Research on IoT Architecture

→ There has been much research on IoT architecture.

- The Electronic Product Code (EPC) can be regarded as a representative earlier scheme for global logistics application.
- It is a vision that all physical objects can be connected by a radio frequency identification (RFID) transponder through a global unique EPC attached to RFID tags
- Japan also proposed a global application prototype—Ubiquitous ID (UID)
- SENSEI is a project in the European Union's Seventh Framework-Program to integrate the physical world with the cyber world
  - The architecture includes the system model, resource model, and information model, and provides services for users and applications for providers in the physical world via wireless sensor and actuator network (WSAN) systems.
- The PECES architecture provides a general software layer for global application devices.
- SemSorGrid4Env architecture also provides a software platform, and it includes a set of Web services as a service-oriented architecture

Some Research on IoT Architecture (Contd.)

→ The projects encourage research groups to fully consider social, economic and legal issues brought from interaction between the Internet and society, and to design and experiment with brand new Internet architecture and networking ideas

→ It tries to provide the direction for future IoT development and adapts to the development trend.

Definition

Unit IoT: Unit IoT refers to a single application

Ubiquitous IoT: Ubiquitous IoT refers to the collection of multiple IoT applications, including local IoT, industrial IoT, national IoT, and global IoT applications

U2IoT = Unit IoT + Ubiquitous IoT

Industrial IoT: It's a collection of sensors, actuators and associated networking technologies , that work together to collect, and analyse data from the Industrial operations

Local IoT: It is a unit IoTs within a certain region and management platforms

National IoT: It includes all unit IoTs that belong to one specific nation and management platform

Global IoT: Global IoT refers to the specific application on a global scale

Ubiquitous IoT (U2IoT) Architecture

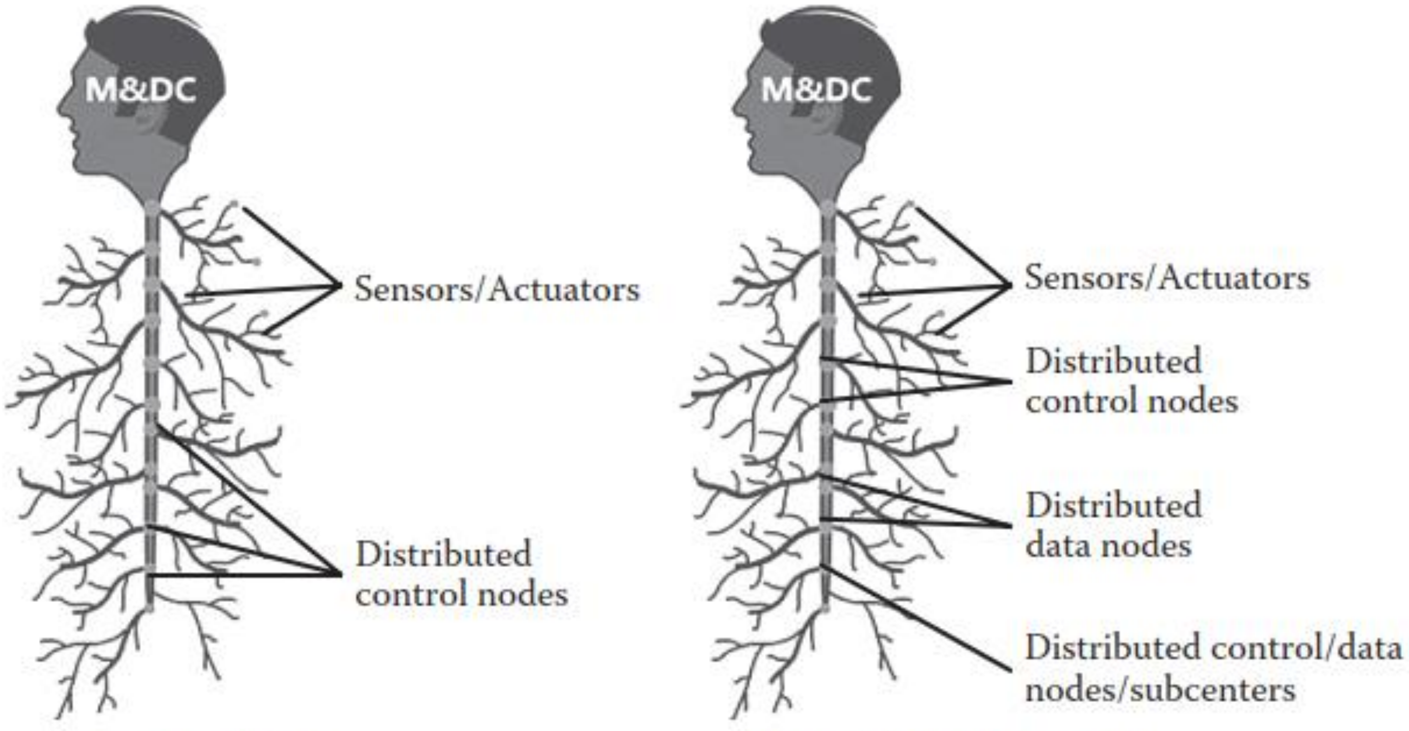
- IoT is the fusion of the physical world, cyber world, and social world.
- Things are sensed via ubiquitous sensors. Future IoT architecture should be ubiquitous.
- Meanwhile, the architecture shall help existing intelligent applications immigrate to IoT, and satisfy the requirements for the insufficiently developing infrastructure in the underdeveloped regions around the world
- The nervous system structure in the human body and social organization consisting of individuals are good examples for designing IoT architecture.
- In the human body, the nervous system is a kind of complicated intelligent system that can see, taste, feel, and control things, or even make decisions.
- Inspired by the human nervous system and the social organization framework, future IoT architecture will be introduced from two aspects: unit IoT and ubiquitous IoT (U2IoT) architecture.

Ubiquitous IoT (U2IoT) Architecture (Contd.)

Unit IoT Definition and Its Architecture Design

→ Unit IoT architecture is a Man-like Nervous System (MLN), which is a kind of complicated intelligent system that can sense and control things or make decisions.

→ It can be classified into two types
- One type works like the human nervous system with a centralized data center (a).
- It has three main components: the brain (management and data center [M&DC]), the spinal cord (distributed control nodes), and a network of nerves (IoT network, sensors, and actuators).



(a) MLN model (b) Modified MLN model

Ubiquitous IoT (U2IoT) Architecture (Contd.)

- In general, the IoT network transmits the data from sensors to the corresponding control nodes and M&DC, which receives, translates, and transmits messages to actuators to control the things.
- In unit IoT, M&DC is a centralized data center for processing and storing data and managing the whole networks.
- Although the working flow is similar to humankind's nervous system, there still remains an important difference:
  - The distributed control nodes are more capable of controlling or responding to external or internal stimulation in some cases.
- The other type of unit IoT is a modified MLN model.
  - Its distributed data center lies not only in the M&DC but also in some distributed cord nodes.
  - In this model, whether a distributed control node works as a distributed data node
  - One important issue is how the existing intelligent system prototypes can be integrated or immigrated into future IoT.

Ubiquitous IoT (U2IoT) Architecture (Contd.)

- → In general, these intelligent systems can retain their own structures while adding proper M&DCs as unit IoTs to access future IoT.
- → In some cases, revising or reorganizing is required.

Ubiquitous IoT Definition and Its Architecture Design

- → Ubiquitous IoT refers to the collection of multiple IoT applications, including local IoT, industrial IoT, national IoT, and global IoT applications, which are composed of multiple unit IoTs and management platforms with certain service goals.
- → Ubiquitous means coverage of different services in unit IoTs and provides the higher-level service by integration of various unit IoTs.
- → Local IoT includes the unit IoTs within a certain region and management platforms
- → The management platform is the local management and data center (IM& DC), which manages the covered local unit IoTs in the corresponding region.
- → Industrial IoT includes the unit IoTs that belong to a specific industry as well as management platforms.
- → The industry management and data center (IM& DC) for industry IoT is responsible for the management of covered unit IoTs in a particular industry (e.g., logistic, agriculture, and smart grid) and is managed by a specific industrial authority.
- → National IoT includes all unit IoTs that belong to one specific nation and management platform.

Ubiquitous IoT Definition and Its Architecture Design

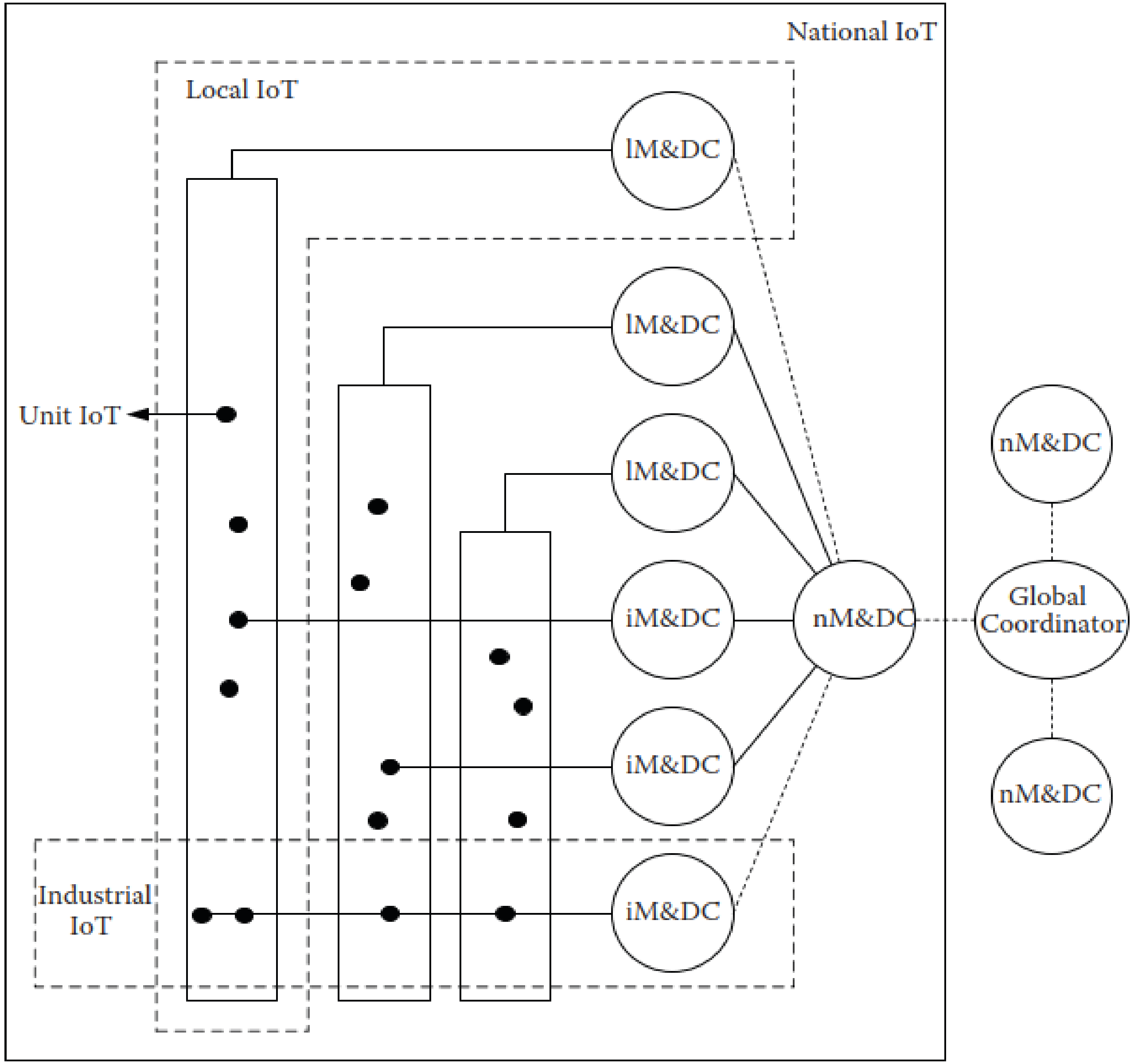
→ A national management and data center (nM&DC) is responsible for the management of national IoT.

→ It manages the corresponding nationwide unit IoTs, and controls IM&DC and IM&DC around the nation.

→ Global application IoT refers to the specific application on a global scale.

→ The global coordinator establishes the coordination mechanism when developing and applying IoT among nations, such as coordination and cooperation in terms of policy, standards, technology, and application.

→ It includes the current international organization, such as the International Telecommunications Union (ITU), as well as other possible future global coordination institutions.



Ubiquitous IoT Definition and Its Architecture Design (Contd.)

- nM&DC directly or indirectly manages iM&DCs and lM&DCs, which are also coordinated by the global coordinator.
- Solid dots denote unit IoT.
- iM&DC manages unit IoTs in the corresponding industry (solid dots in the rectangle connected to the iM&DC).
- lM&DC manages unit IoTs in its corresponding region (solid dots on the line connected to the lM&DC).
- It can be seen that industry IoT and local IoT overlap.
- Nationwide unit IoTs in different regions and industries construct national IoT.
- The global coordinator manages the cooperation for different nations.

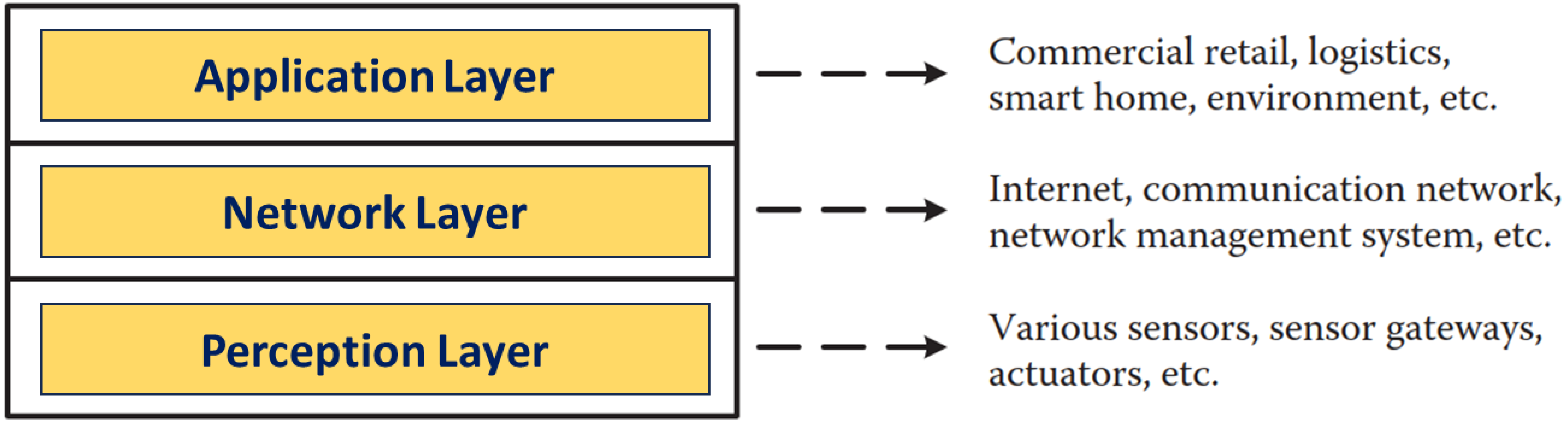
Some Layered Models for IoT

→ IoT can be layered according to different functional aspects. Thus far, various kinds of layered models have been raised.

→ Here, three models are mainly introduced, including the three-layer model, four-layer model, and IBM eight-layer model.

→ **Three-Layer Model**

- IoT is generally divided into three layers from the aspect of technologies, which are the perception layer (also called the sensing layer), the network layer, and the application layer



Some Layered Models for IoT (Contd.)

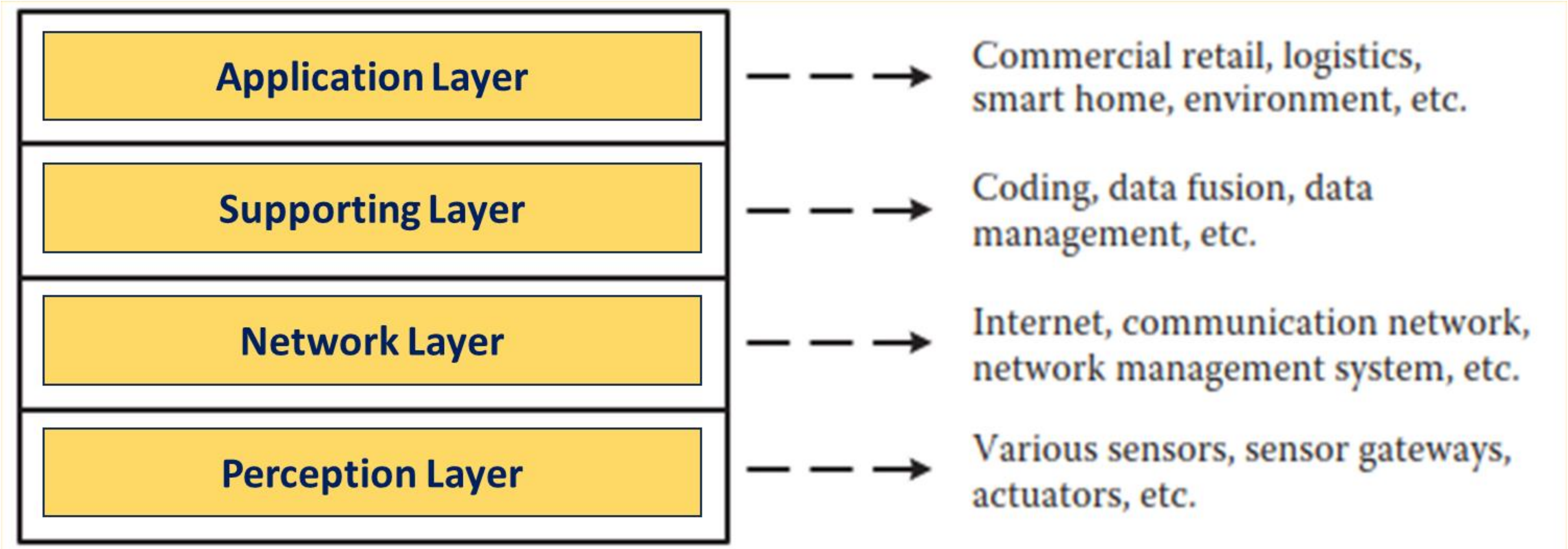
→ **Three-Layer Model**

- The perception layer consists of various sensors, sensor gateways, and actuators.
    - It is responsible for identifying things, collecting information, and controlling things.
- The network layer includes a variety of private networks, the Internet, mobile networks, the local area network, and the wide area network.
- The application layer is the interface of the IoT service and users.
- Combining IoT technologies with actual requirements, the intelligent application of IoT can be realized.

Some Layered Models for IoT (Contd.)

→ Four-Layer Model

- The four-layer model is like the three-layer model, as shown
- The difference is an additional supporting layer split from the application layer.
- The network layer utilizes networks to ensure secure and reliable data transmission.
- The supporting layer adopts unified coding, data fusion, data management, cloud computing, cloud storage technology, and so forth.



Some Layered Models for IoT (Contd.)

→ Eight-Layer Model

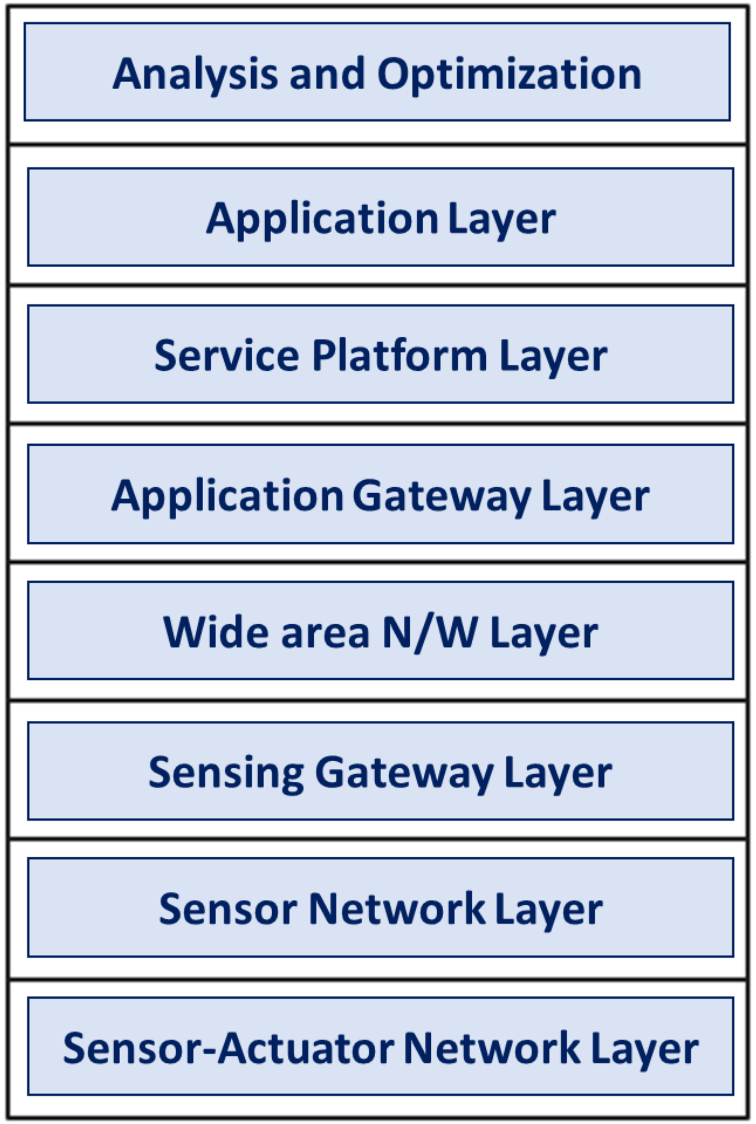
- The eight-layer model is proposed by IBM which includes the sensor-actuator layer, sensor network layer, sensing gateway layer, wide area network layer, application gateway layer, service platform layer, application layer, and analysis and optimization layer.
- Compared to the three-layer and four-layer models, more aspects about ubiquitous IoT are considered in the IBM eight- layer model
- In the above three IoT layered models, the three-layer and four-layer models are more suitable to describe unit IoT.
- Compared to them, the eight-layer model adds more content for multiple applications, and it considers characteristics in heterogeneous sensing, communications, and applications.

Analysis and Optimization
Application Layer
Service Platform Layer
Application Gateway Layer
Wide area N/W Layer
Sensing Gateway Layer
Sensor Network Layer
Sensor-Actuator Network Layer

Some Layered Models for IoT (Contd.)

→ Eight-Layer Model

- However, for ubiquitous IoT, there are still some limitations in the eight-layer model.
- Based on U2IoT architecture, a new layered model and the social attributes involved in IoT are discussed.



Some Layered Models for IoT (Contd.)

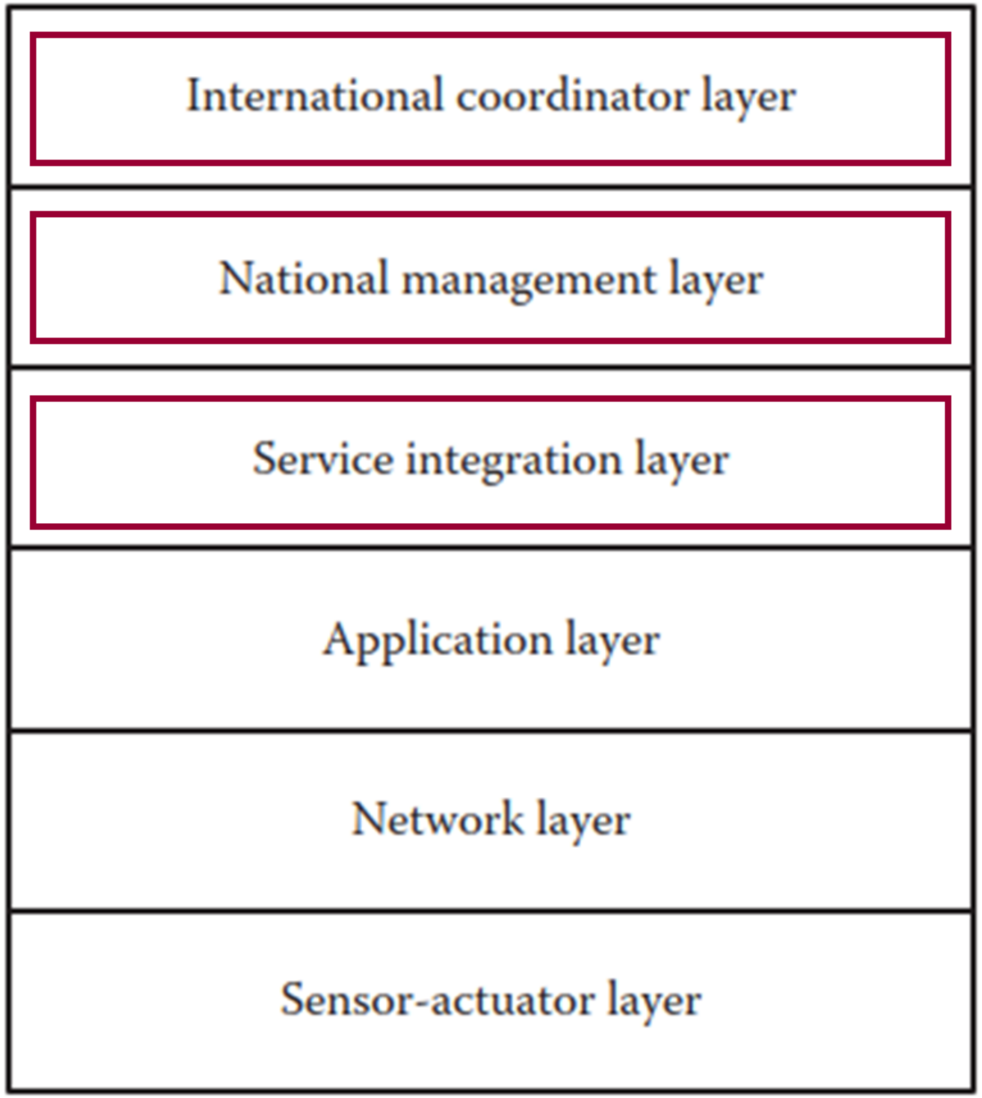
→ Discussion on the layer Models

- The In the above three IoT layered models, the three-layer and four-layer models are more suitable to describe unit IoT.
- Compared to them, the eight-layer model adds more content for multiple applications, and it considers characteristics in heterogeneous sensing, communications, and applications.
- However, for ubiquitous IoT, there are still some limitations in the eight-layer model.
- Based on U2IoT architecture, a new layered model and the social attributes involved in IoT are discussed.

Some Layered Models for IoT (Contd.)

→ **Layered Model Proposed and Social Attributes Discussion for U2IoT**

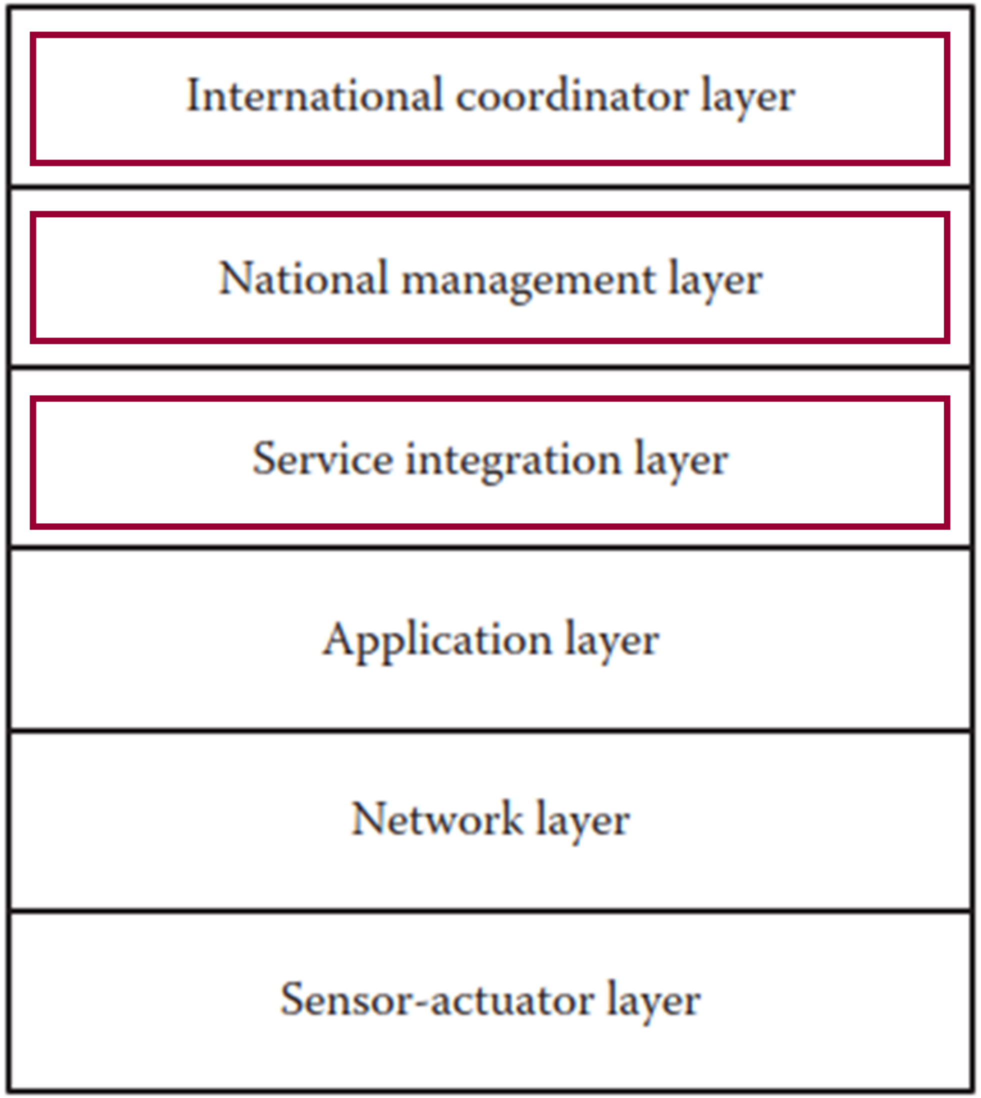
- Based on U2IoT architecture, a six-layer model is proposed as shown , including the sensor-actuator layer, network layer, application layer, service integration layer, national management layer, and international coordinator layer.
- The sensor-actuator layer, network layer, and application layer are like to those in the three-layer model.
- The upper three layers are designed for ubiquitous IoT.
- Concretely, the purpose of the service integration layer is to manage the set of different applications for service providing, such as iM&DC.



Some Layered Models for IoT (Contd.)

→ **Layered Model Proposed and Social Attributes Discussion for U2IoT**

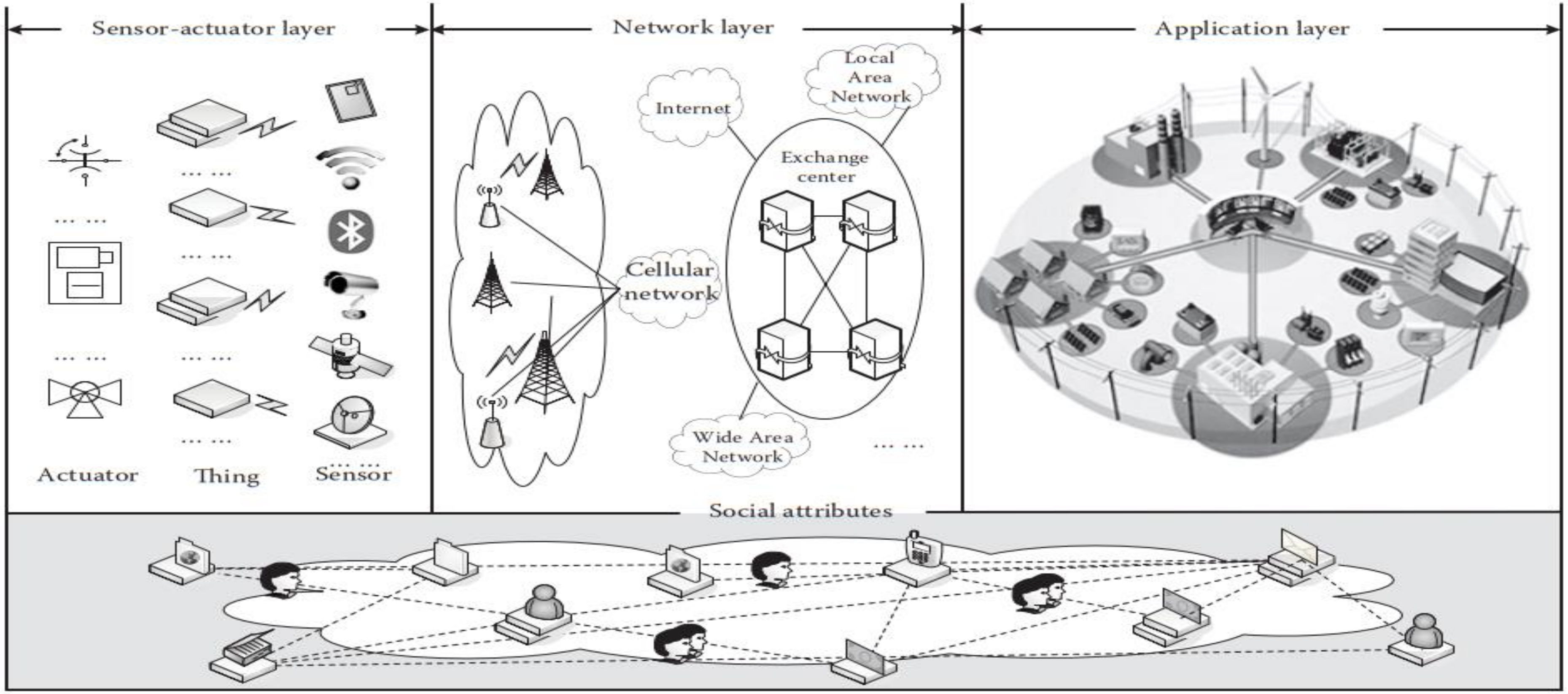
- The national management layer is responsible for the regulation of local IoT and industrial IoT, which is guided by the nation.
- The international coordinator layer is mainly responsible for the coordination of IoT applications and development and standards in different nations; it coordinates IoT development, regulations, and applications on a global scale.



Some Layered Models for IoT (Contd.)

→ Layered Model Proposed and Social Attributes Discussion for U2IoT

- As shown in figure, unit IoT has three layers with social attributes, including the sensor-actuator layer, network layer, and application layer.
- Note that the sensor-actuator layer and network layer in the figure only refer to those in a single application.



Some Layered Models for IoT (Contd.)

→ Sensor-actuator layer

- The sensor-actuator layer comprises sensors and actuators to perform things' identification, resource/service discovery, and execution control.
- It senses things to extract information and realize semantic resource discovery and performs actions to realize control.
- Sensing techniques in this layer include RFID, camera, Wi-Fi, Bluetooth, global positioning system (GPS), radar, and so on.

→ Network Layer

- The network layer includes the network interfaces, gateways, communication channels, and information management.
- A heterogeneous network existing in IoT mainly refers to communication networks such as the Internet and mobile networks, and access networks such as wireless sensor networks (WSNs), in which the hybrid network topologies are involved to assist in monitoring real-time network configuration.
- The network layer ensures reliable data transmission by applying the data coding, extraction, fusion, restructuring, mining, and aggregation algorithms.

Some Layered Models for IoT (Contd.)

→ Application Layer

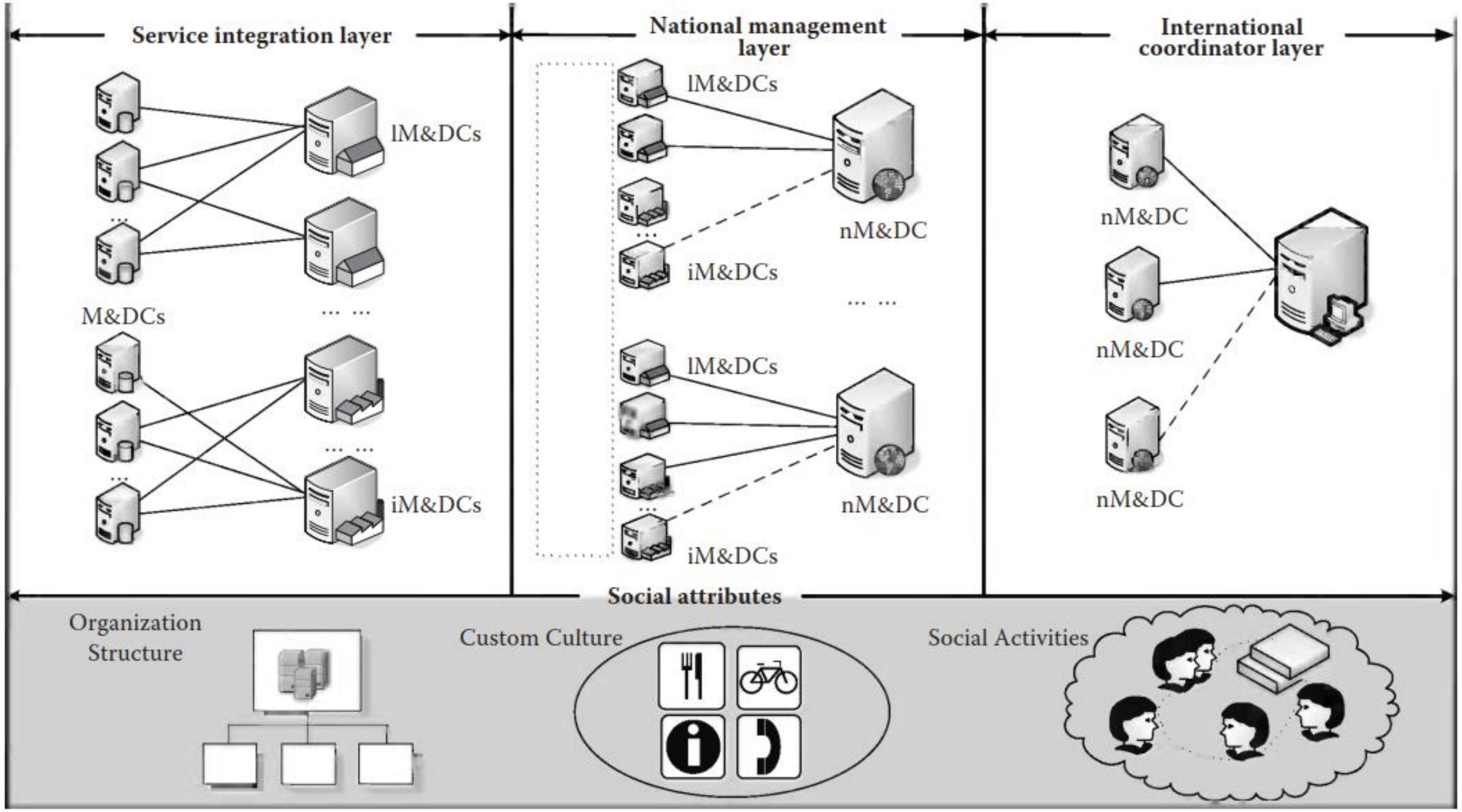
- The application layer supports embedded interfaces to provide diverse functionalities, realizing information aggregation and distribution and providing users with certain services.
- It includes different application processing systems.
- The systems process, analyze, and execute different functionalities and make decisions.
- This layer should fully consider the specific requirements for the application and provide a user-friendly interface for operation.

→ Social attribute

- The social attributes consider those throughout the three layers and are devoted to digging out social relationships among other things.
- The heterogeneous networks to which unit IoT applies, security and privacy, things involved in unit IoT, concrete local IoT, industrial IoT, or national IoT to which it belongs are all affecting factors.

Some Layered Models for IoT (Contd.)

- For example, if a local policy is established by the government and acts on one region, the unit IoTs in the region will be affected, while the effects on other unit IoTs may be small.



- Ubiquitous IoT includes the Service Integration Layer, National Management Layer, International Coordinator Layer, and Social Attributes as shown

RV College of Engineering

Some Layered Models for IoT (Contd.)

→ Service Management Layer

- The service integration layer is responsible for the coordination of various unit IoTs in the corresponding local IoT or industrial IoT.
- In many cases, unit IoTs need to be integrated to provide better and more comprehensive services.
- M&DCs in these unit IoTs are often managed by the lM&DC or iM&DC in this layer.
- An interface to integrate the services provided by different unit IoTs should be built in this layer, as well as local regulations or industrial standards.
- This layer provides approaches and platforms for various unit IoTs' integration.

Some Layered Models for IoT (Contd.)

→ **National management Layer**

- The national management layer is the regulation of local and industrial IoT, providing the industry planning and guidance functions (Cement Industry).
- In each nation, the industry and local development situation is dissimilar, so corresponding national management is needed for better construction of IoT, satisfying different cases and requirements.
- nM&DC manages lM&DC or iM&DC in this layer, and related regulations, laws, and platforms should be provided for coordination and supervision.
- It should be noted that national information security is especially important in this layer.

Some Layered Models for IoT (Contd.)

→ International Coordination Layer

- The international coordinator layer manages transnational IoTs, builds international standards, and coordinates interaction among IoTs in different nations.
- It is like the United Nations Organization (UNO), in which different nations participate, establishing standards and protocols, or the International Organization for Standardization (ISO), building international standards.
- In this layer, nM&DC in nations all over the world may not be coordinated by one centralized global coordinator only.
- Several international organizations can coordinate jointly.

Some Layered Models for IoT (Contd.)

→ Social Attributes

- Social attributes of ubiquitous IoT should also be mapped from the social world to the cyber world.
- For ubiquitous IoT, as a collection of unit IoTs, its social attributes include organization function and structure, geographical terrain and custom culture, security and privacy, and competition and cooperation among nations, industries, and regions, instead of the specific things involved in unit IoT.
- The organization function and structure
- It considers more about the organization form.
- How it is formalized should also be reflected in the cyber world.
- For instance, if the ubiquitous IoT is formalized by the region division, the corresponding characteristics, such as physiognomy of the region, will affect it as well.

Some Layered Models for IoT (Contd.)

→ **Social Attributes**

- The competition and cooperation among nations, industries, and regions influence ubiquitous IoT as well.
- In a certain IoT, there are features or requirements according to the corresponding requirements.
- So, when the competition and cooperation relationship emerges, compatible and interactive issues should be considered.

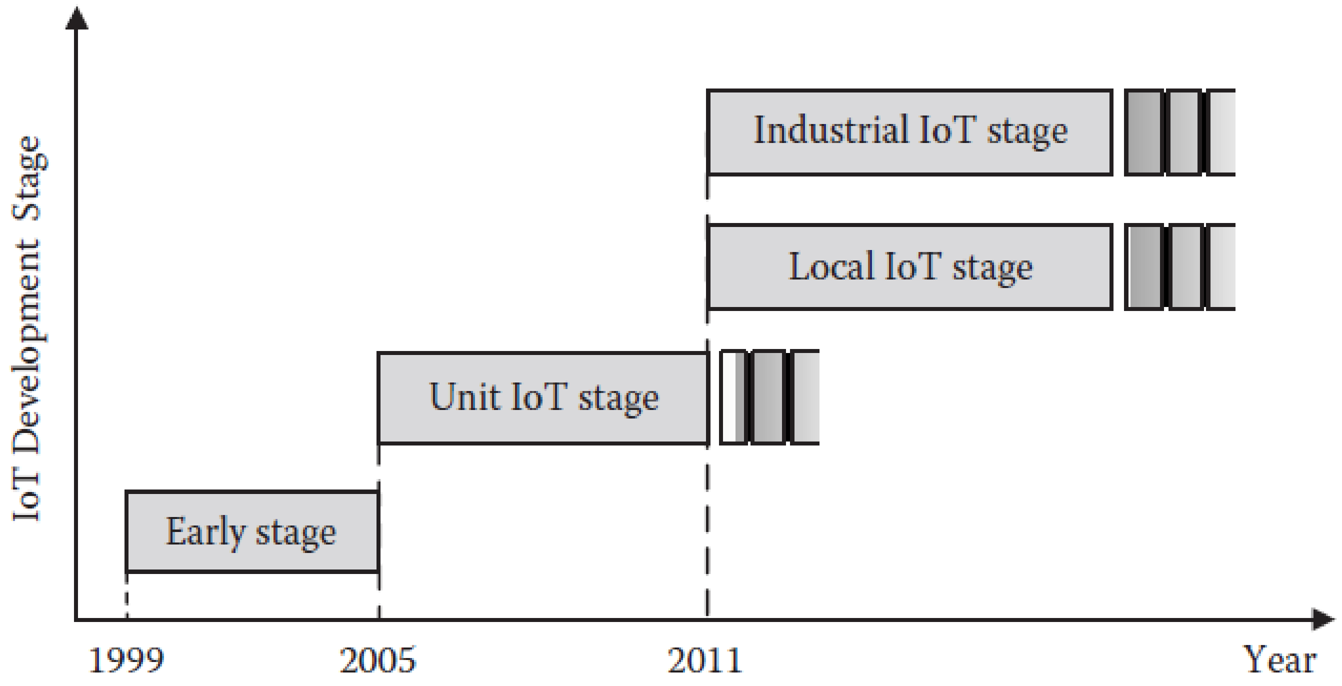
IoT Development Phases, Summary, and Discussion

- Despite IoT's development, IoT is still a blurred concept for the public.
- This is the result of disconnection of the academia and industries.
- Some industrialists have already taken hasty moves to informationize their applications to the IoT concept, while a distinct scientific and technological framework for future IoT has still not been established.
- Therefore, it is difficult to establish IoT standards in the real sense at this stage.
- Compared to the early stage, one of the significant differences is that involved sensing and networking technologies include RFID, WSN, ZigBee, Wi-Fi, and so on.
- Thus far, IoT development has experienced two stages: the early development stage and the unit IoT stage.

IoT Development Phases, Summary, and Discussion (Contd.)

- The ideal future IoT vision may be an era of harmony of humans with nature, which means harmony, coordination, and coexistence of the physical world, cyber world, and social world.
- Thus far, IoT development can be summarized as three stages before achieving the ideal IoT vision era: the early stage, unit IoT stage, and industrial/local IoT stage

→ **Early Stage**



- The early stage is the beginning of the IoT early development stage.
- In this stage, two typical schemes are the EPC system and UID.
- The EPC system realizes that all physical objects can be identified uniquely by assigning an EPC code carried by RFID tags.

IoT Development Phases, Summary, and Discussion (Contd.)

- The UID solution was proposed by Japan and identifies objects through ubiquitous code (Ucode).
- The main feature at this stage is using RFID technology to identify objects uniquely and trace them globally.

→ **Unit IoT Stage**

- The unit IoT stage focuses on a specific IoT application.
- It can be dated back to 2005 with its milestone—publishing of the IoT report by ITU followed by some important events: the U.S. government made a positive statement to develop IoT in 2008, the European Union launched cluster research on IoT and announced some reports and China announced that a sensor network would be developed as an important industry in 2009.
- One of the stage characteristics is the sensing method in IoT, which not only includes RFID identification, but also involves a variety of ubiquitous sensing methods (including sound, light, and electricity-based contact, contactless, and remote sensing methods).
- Another characteristic is the application of intelligence to IoT. For example, Smarter Planet proposed by IBM has already gained increasing popularity.

IoT Development Phases, Summary, and Discussion (Contd.)

→ Unit IoT Stage

- Therefore, it is difficult to establish IoT standards in the real sense at this stage.
- Compared to the early stage, one of the significant differences is that involved sensing and networking technologies include RFID, WSN, ZigBee, Wi-Fi, and so on.
- Thus far, IoT development has experienced two stages: the early development stage and the unit IoT stage.

IoT Development Phases, Summary, and Discussion (Contd.)

→ Industrial/ Local IoT Stage

- From 2011, industrial IoT and local IoT have simultaneously developed. They can be formalized gradually and in parallel.
- **Industrial IoT**
  - The beginning of 2011 saw a milestone when China announced a push in IoT development in 10 important application fields, namely, industrial IoT.
  - Though IBM had developed solutions such as Smart Bank in 2008, it is, after all, a corporation aiming at unit IoT other than establishing and operating an industrial IoT led by a nation.
  - Some national standards for industrial IoT will be formulated, and cross-field cooperation mechanisms will be established.
  - Some global industrial standards concerning transnational communication, such as global logistics, will emerge at this stage.

IoT Development Phases, Summary, and Discussion (Contd.)

→ **Local IoT**

- Local IoT is generated at this stage to coordinate and manage unit IoTs at the local place.
- Security and privacy are also significant for local IoT, and local customs and culture should be fully considered.
- For local IoT, permission rights among different local IoT may conflict, and coordination should be taken into consideration by the local government.
- Resource usage among different IoT applications in the same region may also be considered a priority.
- An agreement or coordinator is needed for negotiation in local IoT.

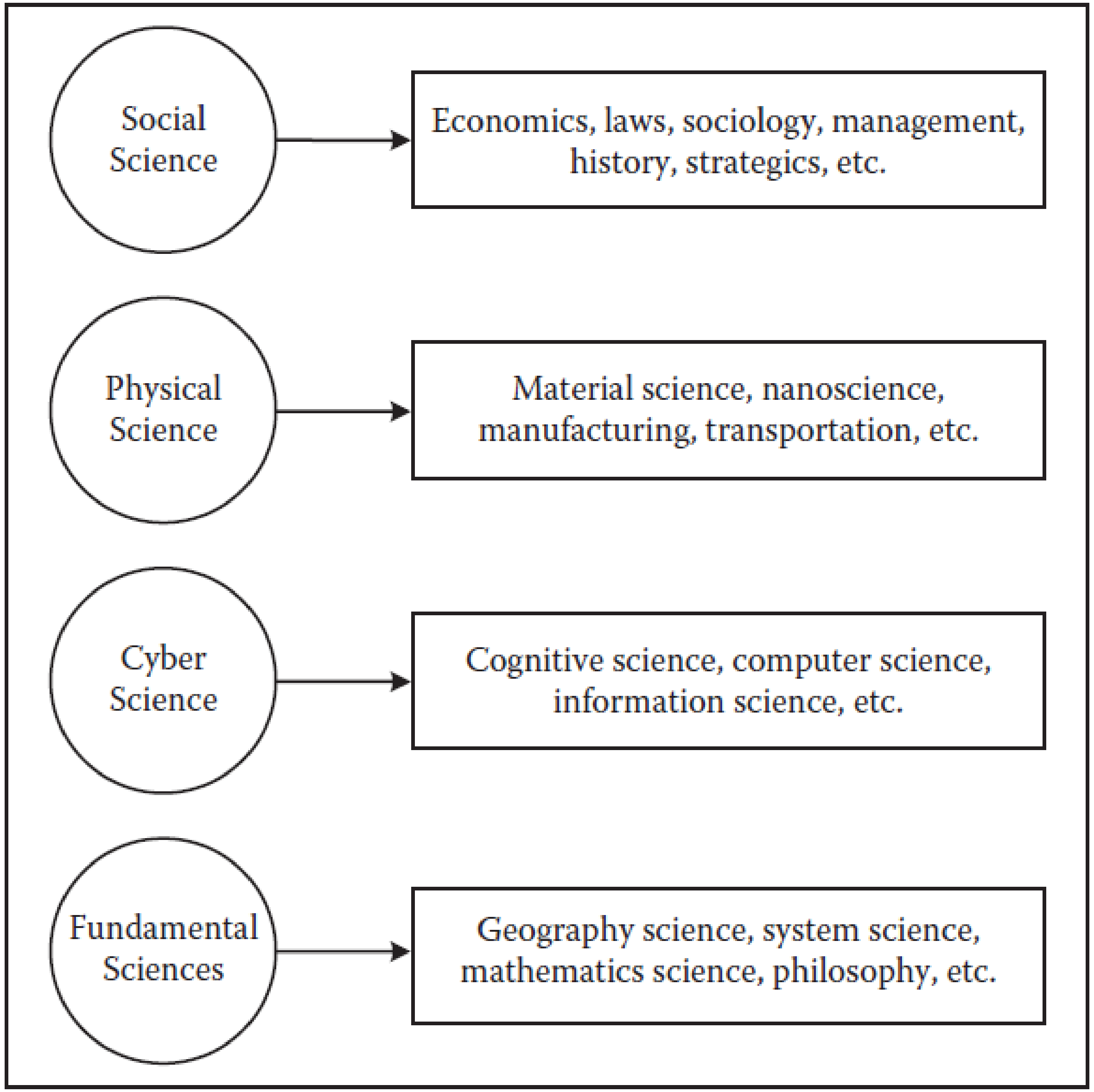
IoT Development Phases, Summary, and Discussion (Contd.)

→ National IoT

- When industrial IoT and local IoT maturely develop, national IoT that manages all IoT applications in the nation will be formed with relatively mature technologies, user consciousness and cultivation, laws, regulations, and security.
- Nations can independently control their information network and resources.
- Cross-disciplinary subjects such as science, technology, and engineering associated with IoT will be introduced, and IoT-relevant subjects and humanities and social science, such as economics, managing, sociology, the law, and philosophy, will also be considered in IoT.
- When national IoT connects and develops maturely, IoT covering different countries will be connective and the international cooperation mechanism will also be basically founded.
- Under the new information network, changes will occur in people's lifestyles, ideals, social organization structures, and government functions.

Science Category and Supporting Technologies for IoT

- IoT combines three worlds—the physical world, cyber world, and social world—and links all the things to achieve an ideal IoT.
- Correspondingly, we classify social science, physical science, and cyber science for IoT.
- Basically, from the aspect of study and IoT required knowledge, fundamental science is also involved, including geography science, system science, mathematics science, and philosophy, as shown in Figure



Science Category and Supporting Technologies for IoT (Contd.)

→ Social Sciences

- It is the study of society development, which covers economics, law, sociology, management, history, and strategies.
- It services humans and society, studying issues of social attributes, property rights transfer, markets, investments, organization, coordination, operation, management, supervision, law enforcement, privacy protection inter- and intra-applications, industries, regions, and nations.
- By studying the entire behavior of society, rules can be found and used to establish new regulations for future IoT development.
- Social science addresses the issues of IoT management and operation regulation.

Science Category and Supporting Technologies for IoT (Contd.)

→ Physical Sciences

- It studies things in the physical world, for example, material science, nanoscience, manufacturing, and transportation.
- This science is different from the current physics as a concrete subject.
- It means the study of things that exist objectively in the physical world, not only humans, but also other things.
- This science discusses aspects of materials, devices, equipment, networks, and their production, construction, operation, maintenance, energy consumption, and so forth

Science Category and Supporting Technologies for IoT (Contd.)

→ Cyber Sciences

- It focuses on things in the cyber world, including cognitive science, computer science, and information science, excluding the building of the physical devices that realize the cyber things' interaction.
- The range of this science covers electronic information, computers, networks, control, intelligence, systems management, information security, and collecting, processing, transmitting, storing, and utilizing procedures of information.

Science Category and Supporting Technologies for IoT (Contd.)

→ Fundamental Sciences

- It include geography science, system science, mathematics science, and philosophy.
- Geographical science studies the earth and society, and the mutual relationship and reciprocity of space objects. System science studies IoT from aspects of the whole and part, local and global, and the hierarchical relation, including the overall IoT-relevant system optimization, the relationship between system structure and function, the system stability, and so on. Mathematics science studies quantitative relations of quantity and quality, not considering the nature difference.
- Philosophy is the most abstract and basic level of all and guides IoT development. In addition, physics, chemistry, and spatial orientation are also basic parts of science.

Science Category and Supporting Technologies for IoT (Contd.)

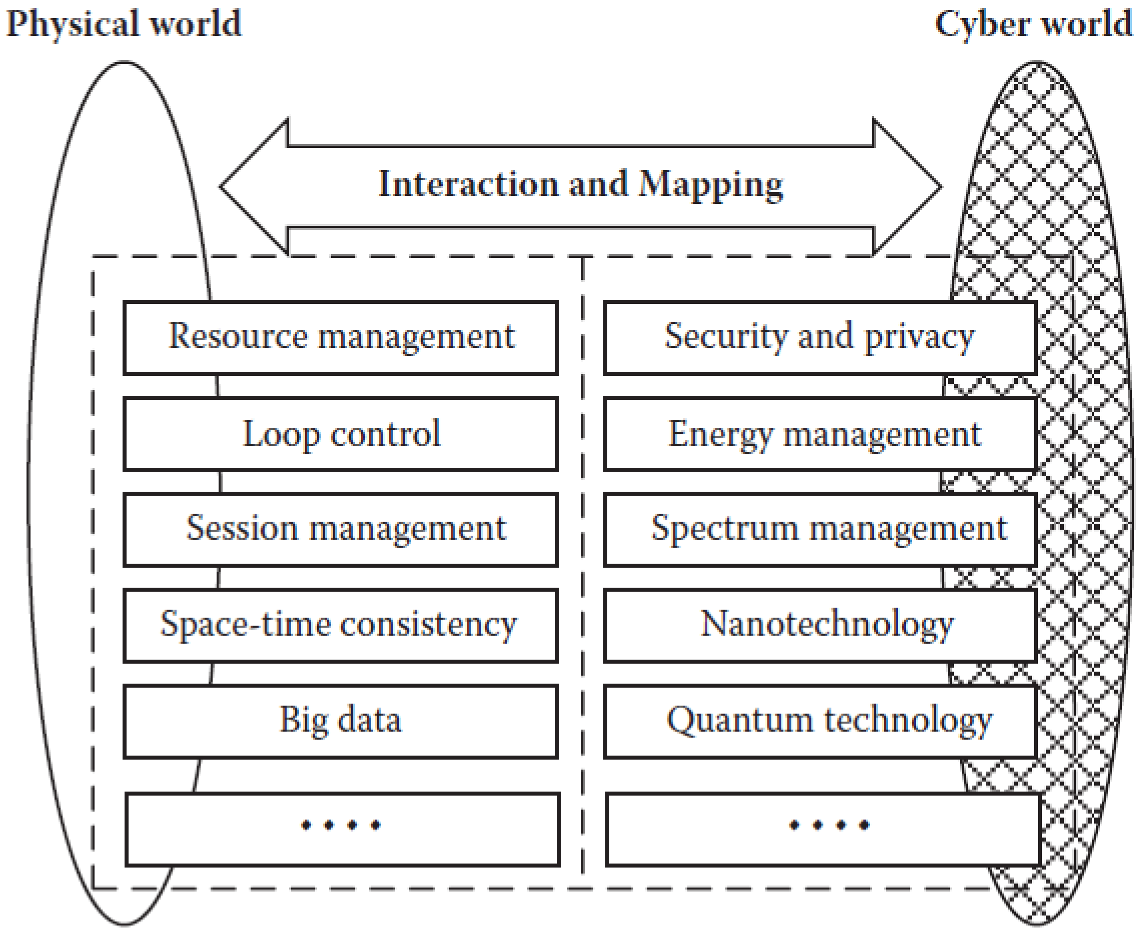
→ Supporting Technologies

- It IoT involves various kinds of supporting technologies, covering resource management, security and privacy, energy management, loop control, session management, space-time consistency, spectrum management, nanotechnology, and quantum technologies.
- There are different classification methods for these technologies.
- One is to classify them according to sensing, network, application, and intelligent processing
- The other is to classify them according to the IoT definition and meaning of mapping between the physical world and cyber world, as shown in Figure.
- These technologies are divided into two kinds.
- One is the supporting technologies based on the interaction between the physical world and cyber world, including resource management, loop control, session management, space-time consistency, and big data.

Science Category and Supporting Technologies for IoT (Contd.)

→ Supporting Technologies

- Resources exist in both the physical world and cyber-world, and are required to be managed to achieve resource-optimized utilization.
- Loop control is needed for the decision of the actuation loop's logic/components/process, and the maintenance of loop executing.
- Session management is also involved in IoT, as it is required to manage interactions between the ubiquitous resources and resource users.



Science Category and Supporting Technologies for IoT (Contd.)

→ Supporting Technologies

- Time and space are basic dimensions in the physical world, so when mapping things to the cyber world, space-time consistency should be taken as a supporting technology and researched with great attention.
- Big data is a data set that is beyond the common tool's ability to capture, manage, and process. It has become a contact bond of the physical world, cyber world, and social world.
- The other is the common supporting technologies, including security and privacy, energy management, spectrum management, nanotechnology, and quantum technology.
- As IoT involves a large amount of information about humans and human life, threats to security and privacy issues will become unprecedentedly serious.
- Therefore, security and privacy have to be considered when mapping information between the physical world and cyber world.

Science Category and Supporting Technologies for IoT (Contd.)

→ Supporting Technologies

- Energy consumption should be considered in concrete applications, which is a serious global problem because of energy limitation.
- Frequency management manages the procedures of planning, coordinating, and managing the spectrum utilization in IoT.
- Nanotechnology is a new emerging technology of controlling matter on the scale of 1 ~ 100 nm and affects many disciplines and technologies. Quantum technology brings us new materials, devices, communications, and computing mechanisms.
- These technologies are basically needed for IoT as common supporting technologies.


Thank you