**IEEE P802.24**

**Vertical Applications Technical Advisory Group**

|  |  |
| --- | --- |
| Project | IEEE P802.24 Vertical Applications Technical Advisory Group |
| Title | **Internet of Things White Paper** |
| Date Submitted | 2025-09-17 |
| Source | Allen JonesChris DiMinicoAnn KriegerBen RolfeTim GodfreyPhil Beecher |   |
| Re: | N/A |
| Abstract | This contribution provides draft the Internet of Things White Paper. It will be updated (along with this Abstract) as the content materializes and is included. |
| Purpose | Draft of the IoT White Paper (Changes accepted, closed comments deleted for 2025) |
| Notice | This document has been prepared to assist the IEEE P802.24. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.24. |

# Background and Introduction

This white paper is to consider the applications related to the Internet of Things

# References

[1] [Gartner](https://www.gartner.com/en/information-technology/glossary/internet-of-things) Gartner Glossary: Internet Of Things (IoT)

[2] [ITU](https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx) Internet of Things Global Standards Initiative

[3] [Techopedia](https://www.techopedia.com/definition/28247/internet-of-things-iot) What Does Internet of Things (IoT) Mean?

[4] [IBM](https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/) What is the Internet of Things (IoT)?

[5] [ISO/IEC 20924:2024](https://www.iso.org/standard/88799.html) Internet of Things (IoT) and digital twin — Vocabulary

[6] [IEEE 2413-2019](https://ieeexplore.ieee.org/document/8672168) IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT)

[7] [SAS](https://www.sas.com/en_us/insights/big-data/internet-of-things.html) Internet of Things (IoT) What it is and why it matters

# What is the Internet of Things?

The term Internet of Things is widely used, often with varying definitions. An “Internet” does not always mean the public Internet. There are different kinds of internets - public and private. Many vertical applications connect over a non-public network but retain other characteristics of IoT. The common thread is the use of Internet Protocol (IP).

1. The network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. [1] Gartner.
2. A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. [2] ITU
3. The Internet of Things (IoT) is a computing concept that describes the idea of everyday physical objects being connected to an internet and being able to identify themselves to other devices and send and receive data. [3] Techopedia
4. The Internet of Things is the concept of connecting any device (so long as it has an on/off switch) to the Internet and to other connected devices. The IoT is a giant network of connected things and people – all of which collect and share data about the way they are used and about the environment around them. [4] IBM.

These definitions from the industry provide an introduction to considering the Internet of Things to begin the investigation.

The International Standards Organization and the International Electrotechnical Commission [5] ISO/IEC also provide definitions of an “IoT Device”, the Internet of Things and many other components which contribute to the Internet of Things. The definition of an “IoT Device” emphasizes the idea that new IoT Devices are Sensors and/or Actuators.

The IEEE also provides definitions in their Draft Standard for an Architectural Framework of the Internet of things [6] IEEE Std 2413-2019.

“It is important to understand what the Internet of Things is and what the difference is between the IoT environment and an IoT system. A simple definition of an Internet of Things system is “a system of entities (including cyber-physical devices, information resources, and people) that exchange information and interact with the physical world by sensing, processing information, and actuating.”

The set of IoT components available to be composed into IoT systems, the networks connecting the components, and any associated services that provide the mechanisms for discovery, composition, and orchestration can be called an IoT environment.

Core to the idea of IoT is this interaction with physical entities. An entity of interest is a physical entity that is of interest to a human or organization for the completion of a goal. A physical entity is a discrete, identifiable part of the physical environment. Physical entities can be any physical object: humans; animals; cars; store or logistics-chain items; mechanical devices; computing devices; etc.”

The comprehensive descriptions above include the major components when contemplating the concepts comprised in the Internet of Things. Many of the definitions above mention common elements such as data sharing over a communication path. Most are very inclusive of a broad range of “things” including people and hardware. Some emphasize Sensors and Actuators.

# Things used in IoT – Sensors and Actuators

Many common definitions of the Internet of Things are based on the concept that IoT things are primarily new devices based on Sensors and Actuators. Sensors and Actuators are an important device class for the IoT. To aid in the understanding of Sensors and Actuators, common definitions for these devices are provided below.

In a general sense, a sensor measures something in the real world and converts it to a digital value. It can also be defined as a device that responds to any change in physical phenomena or environmental variables like heat, pressure, humidity, movement etc. and turns that into to a form usable in a digital system.

For example, a sensor may contain a transducer, a device that converts energy from one form to another.

An actuator is a device that is responsible for moving or controlling a mechanism or system. It is operated by a source of energy, which can be mechanical force, electrical current, hydraulic fluid pressure, or pneumatic pressure, and converts that energy into motion.

A great example of a Senor/Actuator device is a fire sprinkler, these have been around for over a hundred years. The Sensor detects excess heat, and the Actuator turns on the water to the sprinkler. A useful IoT device, however, modern systems take this closer to the value of the Internet of Things by including additional data. The system monitors the health of the Sensors and Actuators and the water delivery system to determine if it is in working order and to communicate alerts if the system needs maintenance.

# Another perspective

Another definition provides a further perspective on concept of the Internet of things.

The Internet of Things (IoT) refers to a vast number of “things” that are connected to the internet so they can share data with other things – IoT applications, connected devices, industrial machines and more. Internet-connected devices use built-in sensors to collect data and, in some cases, act on it. IoT connected devices and machines can improve how we work and live. Real-world Internet of Things examples range from a smart home that automatically adjusts heating and lighting to a smart factory that monitors industrial machines to look for problems, then automatically adjusts to avoid failures. [7] SAS.

So, it should not be about the definition of IoT devices.

The IoT includes **ALL** devices, examples included below:

New IoT things (sensors and actuators) such as

* + Video doorbells
	+ Smart thermostats
	+ IP Security cameras
	+ Health & Activity trackers
	+ Lighting & Electrical
	+ Blinds & Shades
	+ Smart Speakers
	+ Irrigation
	+ Fire Sprinklers
	+ Motion detectors
	+ Plumbing Leak Detectors
	+ Etc.

But traditional computing devices play a role and should not be excluded from the ecosystem:

* + PCs
	+ Mobile Phones
	+ Smart TVs
	+ Game consoles
	+ Printers
	+ Etc.

Certainly, this is not a complete list, although it attempts to make the point that all addressable connected things can provide data that contributes to the IoT ecosystem.

So maybe “what is a thing” should not be the focus?

If a

Device is connected

Able to communicate

Provides data and/or a useful function

Able to be configured, monitored and provide status

Then

It may be considered part of the IoT ecosystem

# Smart Home

A major class of IoT devices live in the Smart Home and are gaining adoption and popularity.

Smart devices are interesting; however, it is debatable whether these individual devices create an Internet of Things?

Today, in many cases, each Smart Device includes its own App and performs a limited Smart function. Typically, the Smart Device connects to the manufacturer’s cloud service using the local Wi-Fi. The App also connects to the manufacturer’s cloud service using the local Wi-Fi (or cellular if the phone is away from the home)

 

When the Smart Home devices communicate with each other and work together, the system begins to approach a greater Internet of Things concept. In the example below the Smart Home can implement a system that attempts to coordinate and control when the house needs services such as heating, air conditioning and hot water to increase efficiency. The IoT App could know when the home is vacant and deploy an “Away” mode to reduce energy consumption. Further, it could contribute to the “Smart City’ concept by reducing energy usage during peak hours.

This scenario has been challenging in multi-vendor environment. Lack of interoperability between smart home device vendors has limited the ability of smart home devices from different vendors to directly communicate with each other. Initiatives such as CSA Matter are improving interoperability for devices that support their standard.

Local Power Company

Lower power consumption

during energy peak hours

IoT App Controls a system of devices





Smart Devices talk to each other

68

Wi-Fi



# Smart City and Utilities

Smart City use cases enable automation, control, sensing, and reduction of power consumption for systems used in cities. Examples include smart streetlights that reduce power consumption without compromising safety, parking management systems to reduce vehicle congestion, traffic control and signage, management of water use for irrigation and sprinkler systems.

Electric utilities use IoT for a variety of uses. Advanced Metering Infrastructure (AMI) is a widely used application, with millions of wirelessly communicating smart meters deployed in North America. Wi-SUN provides an interoperable network specification AMI and other utility IoT use cases. In addition to AMI, utility IoT use cases include line sensors, fault current indicators, pole tilt sensors, transformer health monitoring, environmental monitoring, security monitoring, and many others.

(Placeholder for Diagram 1 – Streetlght smart city network)

Placeholder for AMI smart metering electric/gas/sensors. (National Grid) Diagram



Figure 7‑1 Neighborhood Area Mesh Network

# Vertical Applications

While Smart Home is an early target including any other verticals are also making progress such as healthcare, agriculture, manufacturing, automotive, public transportation, utilities and energy, environmental, smart cities, and others.

Special cases for automotive IoT – use of Single Pair Ethernet. <Chris D to insert section here> also new work on automotive in 802.11.

DALI for architectural lighting.

KNX Building Automation’

Placeholder for protocol architecture diagram (Hourglass diagram)

Include certificate based enterprise class security. IEEE 2857

Reference IETF work on 6LoPAN and other standards

For vertical use cases that require high reliability, changes in the communication network, and enhanced cyber security are employed. Reliability includes both the delivery of consistent performance of data with adequate bandwidth and limited latency, as well as availability of the communication system, and freedom from failures and service outages. Vertical IoT use cases will often use a private wireless network, to ensure predictable performance and availability. The network may operate in private wireless spectrum, since unlicensed spectrum is subject to interference and congestion and is less able to provide predictable performance. The private spectrum could be a commercial cellular network, or a private cellular network built for the vertical use case.

Many vertical use cases employ intelligence at the edge device, and do not involve a public “cloud” service. They often have an internal, private data center for gathering data and controlling edge devices.

Some use cases do not require any centralized facility at all. For example, some electric utility protection use cases involve direct communication between two devices, without involving a server, cloud, or any Internet connection. A single point to point connection serves the function, which can be implemented with wired or wireless technology.

# It is about the Data

Things are important, it’s in the name. The ultimate value of all of the things could be the data that these things collect and communicate.

Information

Data

Knowledge

Wisdom

Intelligence

& Analytics

People make better Decisions

With an abundance of data, intelligence and analytics can be applied to that data to create superior information which contributes to knowledge and greater wisdom. This will allow people and information systems to make better decisions. The abundance of data may also result in issues related to data security, privacy, and use (and mis-use) of personal information. Economic incentives exist to control and monetize data, resulting in “one-way” flows from users and their devices to the ecosystem owner. This can result in “walled garden” scenarios where the ecosystem owner gains substantial value from the data, but prevents the users that provided the data from sharing in that value, and establishes barriers to prevent the user from leaving the ecosystem.

# Connectivity Technologies for IoT

IEEE 802 Technologies

Wireless

802.15.4 – DSSS

802.15.4 SUN

802.15.4 LPWA

 802.11 Frequency ranges and applicable PHYs

|  |  |  |
| --- | --- | --- |
| **Start frequency (MHz)** | **End frequency (MHz)** | **PHY name** |
| 863 | 928 | S1G (Sub 1 GHz) |
| 2400 | 2483.5 | HE (High Efficiency) |
| Extended Rate |
| HT (High Throughput) |
| EHT (Extreme High Throughput) |
| 2401 | 2423 | WUR (Wake-Up Radio) |
| 2471 | 2497 | Extended Rate  |
| 5150 | 5895 | HE (High Efficiency) |
| EHT (Extreme High Throughput) |
| VHT (Very High Throughput) |
| Orthogonal Frequency Division Multiplex (OFDM) |
| HT (High Throughput) |
| 5190 | 5575 | WUR (Wake-Up Radio) |
| 5850 | 5925 | Orthogonal Frequency Division Multiplex (OFDM) |
| NGV - Next Generation V2X PHY |
| 5945 | 7125 | HE (High Efficiency) |
| EHT (Extreme High Throughput) |

802.11 is widely used as “backhaul” to connect phones and other devices that control IoT to the Internet, ultimately communicating with a gateway device, which may use a different technology (or technologies) for connectivity to the IoT device.

Wired – Ethernet (including Single Pair Ethernet)

Other technologies

 3GPP LTE / 5G / 6G / NB-IoT

 LoRa

# Closing

As noted throughout, IoT does not stand for one specific technology or application. This is not unusual as IoT means different things to different people.  The definitions of what is considered IoT, including the items used in IoT show the particular interest in Smart areas of Home, City and Utilities. And while the hardware sensors are important, what the hardware collects, the data, is the ultimate value.  This data can be used to help us make decisions on how efficiently we run our homes or find the best parking places.

The variety of IEEE 802 standards address the different requirements for different tiers of an IoT network (performance, range, latency, etc.)  A unified architecture enables integration across the network. The architecture and design principles of IEEE 802 have been extended into other standards that have IoT applications.

In summary, IEEE 802 standards provide a platform to support the communication requirements of diverse applications across the range of utility operations, and other devices in support of the Smart Grid, eHealth industry, intelligent transportation systems, smart city applications, and general IoT.