NISTIR 8316

Internet of Things (IoT) Component Capability Model for Research Testbed

Eric Simmon

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8316

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8316

Internet of Things (IoT) Component Capability Model for Research Testbed

Eric Simmon
Software and Systems Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8316

September 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8316
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8316, 20 pages (September 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8316

Abstract

Internet of Things (IoT) is the product of the worlds of information technology (IT) and operational technology (OT) converging. IoT combines the ability to observe the physical world with distributed computing systems that can combine and analyze the resulting data, using the results to better inform decision making, alter the physical environment, and predict future events.

While the basic ideas related to IoT are understood, a precise understanding of the IoT concept is lacking, with different groups (including standards development organizations, private companies, consortium, and even government agencies) providing varying definitions for IoT, which results in confusion among stakeholders.

This document describes a component capability model for IoT that is being used to develop an IoT research testbed in the Information Technology Laboratory's Software and Systems Division at NIST.

It will also be used to facilitate discussion and conversation around IoT. It describes several key terms and core concepts related to IoT and explains how those terms and concepts relate to each other. The model provides a common language that can be used to communicate, specify, review, analyze, and reason about IoT definitions, documents, architectures, components, and systems.

Key words

Complex systems; cyber-physical systems; Internet of Things (IoT)

Table of Contents

List of Tables

List of Figures

1. Document Purpose and Usage

This document describes a component capability model for the Internet of Things (IoT) that is being used to develop an IoT research testbed in the Information Technology Laboratory's (ITL) Software and Systems Division (SSD) at NIST. The models serve a variety of purposes including; communication internally and externally about the research testbed, as a basis for defining the requirements and capabilities of individual IoT components and IoT systems within the testbed, and as a model for developing the IoT components themselves.

This paper provides a common language that can be used to discuss, review, analyze, and reason about IoT definitions, documents, architectures, components, and systems. The model can also be used to assist in the categorization of testbed components, systems, and applications. It is intended that this model be extended by providing specializations of this model for different categories of IoT systems as research in the testbed continues. These categories could be based on application domains, system types, and other types of constraints.

Although these IoT models were developed for use in the testbed they can be used by other IoT stakeholders. For example, IoT system builders can leverage the model to help match IoT component capabilities with requirements, and to make it easier to combine IoT components into IoT systems by combining capabilities to create a system that achieves a set of goals. Acquisition professionals and contracting officers can use terminology from the model when specifying procurement requirements; manufacturers and vendors can use the same terminology when explaining what their products are capable of doing. Other stakeholder groups—ranging from software developers and system administrators to IoT system users and operators—can also benefit from using the IoT general model.

The models presented here have been used in other NIST documents including NISTIR 8200 "Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)," as well as in international standards including Institute of Electrical and Electronic Engineers (IEEE) P2413 "IEEE Standard for an Architectural Framework for the Internet of Things (IoT)." NIST security experts are currently applying the models to various security scenarios to better understand the composition of the IoT systems under review.

2. The Evolution of IoT

Since the first computers were created, people have been thinking about harnessing their computing power to observe and change the world around us. Long before the term "Internet of Things" existed, there were IoT systems – networked computing resources combined with sensors and actuators. One of the first examples was in the early 1980s, when students at Carnegie Mellon University added a network interface to a vending machine [1]. Students connected through the network to the vending machine to see if drinks were available and cold before walking over to buy one. The origin of the term "Internet of Things" is credited to Kevin Ashton, a Massachusetts Institute of Technology researcher working at Proctor & Gamble [2]. In 1999 he was studying Radio Frequency IDentification (RFID) technology for identifying physical objects ("things") and adding data about the 'things' to RFID tags that could then be scanned by connected RFID readers and accessed through a network. Kevin referred to this network of tags and readers as the "Internet of Things."

Since that time, IoT has evolved into something much greater. IoT today is more aligned with the world Mark Weiser envisioned in his seminal paper "The Computer for the 21st Century" where ubiquitous computing resources, combined with sensors and actuators (forming the edge between the cyber and physical worlds) seamlessly support our goals and activities [3]. Today computing networks are ubiquitous and inexpensive, and people are always connected to these networks through desktops, laptops, and mobile devices. This new connected world is challenging our approach to building complex systems [4].

IoT is the result of combining the worlds of information technology (IT) and operational technology (OT). Many IoT systems have become feasible only recently due to the advances in cloud computing, mobile computing, embedded systems, big data, low-cost hardware, and other technologies. IoT can provide computing functionality and network connectivity for equipment that previously lacked these features, enabling remote control (e.g., monitoring, configuration, troubleshooting, etc.) among other features. IoT also adds the ability to collect and analyze data regarding the physical world and use the results to better inform decision making, alter the physical environment, and predict future events. The desire to collect data from IoT often drives system design choices, and the data itself may be more valuable to IoT product manufacturers than the sales of the IoT products themselves.

IoT is based on many complementary technologies, ranging from the Transmission Control Protocol/Internet Protocol (TCP/IP)-based Internet to cellular communication networks and from microelectromechanical systems (MEMS) and embedded systems to inexpensive sensors and actuators to cloud computing services and artificial intelligence. Even the most basic sensors can provide vast amounts of real-world data that requires large scale cloud computing services to process.

An incredible variety of applications fall within the scope of IoT, ranging from smart buildings and smart manufacturing to connected vehicles and smart roads. Virtually every imaginable consumer device (many of which are also present in business and industrial facilities) has become "IoT enabled"—kitchen appliances, thermostats, home security cameras, door locks, light bulbs, TVs, and other consumer electronics, and intelligent personal assistants. There are also many IoT systems specific to a particular sector—for example, there is an enormous IoT presence in healthcare, including hospital equipment and supplies, implantable medical devices, and wearable health monitoring equipment and fitness trackers.

IoT transducing components (with sensors and/or actuators) are connected to the same networks as conventional computing resources, providing the capability to observe, analyze, and affect the physical world. Traditional fields of automation (including the automation of buildings and homes), wireless networking, electromechanical sensing, satellite navigation systems, and control systems are now part of IoT.

Today the term "Internet of Things" itself is a source of confusion. IoT is no longer limited to the "Internet," and the term "Things" is very general and ambiguous. IoT means so many different things to different people because it is such a cross-cutting concept; IoT is applicable to many different application domains and use cases, each with its own specific set of goals and requirements. IoT also does not define one specific, implementable

architecture; IoT systems and environments may be implemented differently depending on the specific requirements to be met.

While the basic ideas related to IoT are known, a precise understanding of the IoT concept is lacking, with many different groups (including standards development organizations, private companies, consortium, and even government agencies) providing varying definitions for IoT, which results in confusion among stakeholders. Because of this fragmentation, the NIST ITL SSD team building the IoT research testbed created the following models to have consistency within the project. This paper addresses this gap by providing a description of the essential concepts of IoT and foundational models that can be applied to all IoT systems, components, and environments.

3. Basic IoT Concepts and Terminology

IoT created a paradigm shift combining two domains that traditionally have been separated. In this new paradigm Information Technology (IT) and Operational Technology (OT) are merged to form systems composed of networked entities (which can include IoT devices, information resources, and people) that can interact (observing and changing) with the physical world. This section defines key terms and concepts for understanding this new paradigm.

3.1. Essential IoT Concepts

There are two essential concepts for IoT:

- The capacity to support many-to-many networked relationships between components (these digital network capabilities may or may not be TCP/IP based and the many-to-many relationship may or may not be utilized)
- The presence of sensors and/or actuators that allow the components to interact with the physical world (only one sensor and/or actuator is required, but often systems have more)

3.2. Components, Systems, and Environments

IoT can be broken down into three important architectural concepts (**Figure 1**): the IoT environment containing all the components, systems, and related infrastructure, the IoT system that provides benefit to the stakeholders, and the IoT components that interact together to form the IoT system.

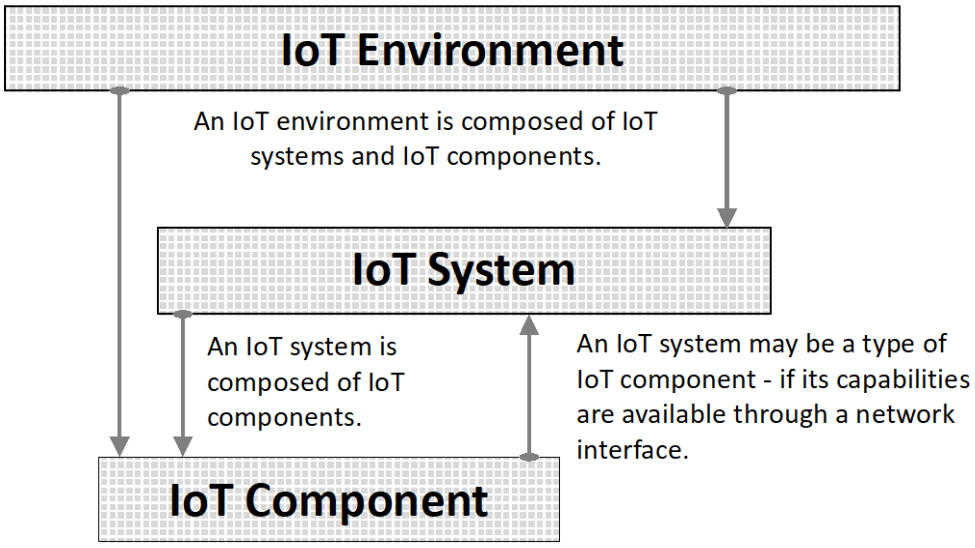

Figure 1 - The relationships between IoT component, IoT system, and IoT environment

3.2.1. IoT Components

IoT components are the basic building blocks of IoT systems. IoT components interact with other IoT components to form a system and achieve one or more goals. Each IoT component provides some function that is necessary within the system so it may achieve its goal(s).

All IoT components have at least one network interface that provides the ability to participate in a many-to-many network, although a given IoT component doesn't need to communicate with more than one other IoT component in a given system (e.g., limiting communication between two static IP addresses). Most IoT components also have an application interface that provides the capacity for application-level interactions between IoT components. The data flow between IoT components may be bidirectional, but individual components may only transmit while others may only receive data.

Each IoT component offers one or more IoT capabilities for use by other IoT components. Network interfaces and sensing are two examples of IoT capabilities. Section 4 examines IoT capabilities in detail. Security is a concern regardless of the capabilities of a given IoT component [5][6].

Components that have sensing and/or actuating categories are a special class of IoT component as they are on the boundary (the 'edge") between the physical world and the digital information systems. These components are often referred to as "IoT devices" [7].

3.2.2. IoT Systems

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15288:2015 [8] defines a *system* as "a combination of interacting elements organized to achieve one or more stated purposes." For a system to be considered an *IoT system*, it must be composed of networked IoT components, and it must interact with a

physical entity of interest through one or more sensors and/or actuators that are within the IoT components. IoT systems differ from conventional IT systems in their ability to directly interact with the physical world.

IoT systems range from the very simple, such as an Internet-enabled thermometer, to the extremely complex, such as a city management system, and everything in between. IoT components can be assembled into many different systems, and a single IoT component may be part of more than one system at a time if the component has that ability. An IoT system can also act as an IoT component within another IoT system if it has a network interface that allows it to be used that way.

IoT systems do not have specific security, privacy, reliability, cost, or functional requirements. It does not stop being an IoT system if these criteria are not met. However, it might not be a "good" IoT system for a specific use case if the IoT system cannot meet the use case requirements. In other words, "goodness" is purely in the eyes of the system stakeholders and dependent on the goals and requirements of the particular application.

People are an important aspect of IoT and may take on one or more of three roles during the operation of an IoT system:

- people may be end users of an IoT system (intentionally using the system to gain benefit)
- people may participate as part of an IoT system (providing capabilities such as sensing, processing, or actuating and interacting with other components through a networked device such as a smart phone or tablet)
- people may be physical entities of interest (that may be observed or acted upon).

3.2.3. IoT Environments

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*. Although an IoT environment contains the IoT components that can be used to create IoT systems, it does not necessarily contain any functioning IoT systems (if no IoT components have been instructed to interact together as a system). On a similar note, an IoT environment can be used to create non-IoT systems (conventional IT systems) by excluding IoT components that have sensing or actuating capabilities. In its current state, the Internet can be considered an IoT environment.

Figure 2 is an example of an IoT environment containing IoT systems and components. It shows numerous IoT components within the environment, and four IoT systems formed by two or more IoT components interacting with each other. Note that one IoT component is shown as being part of two IoT systems and one of the IoT systems is an IoT component within another IoT system. Each IoT component has a set of capabilities (not shown) which are described in section 4.

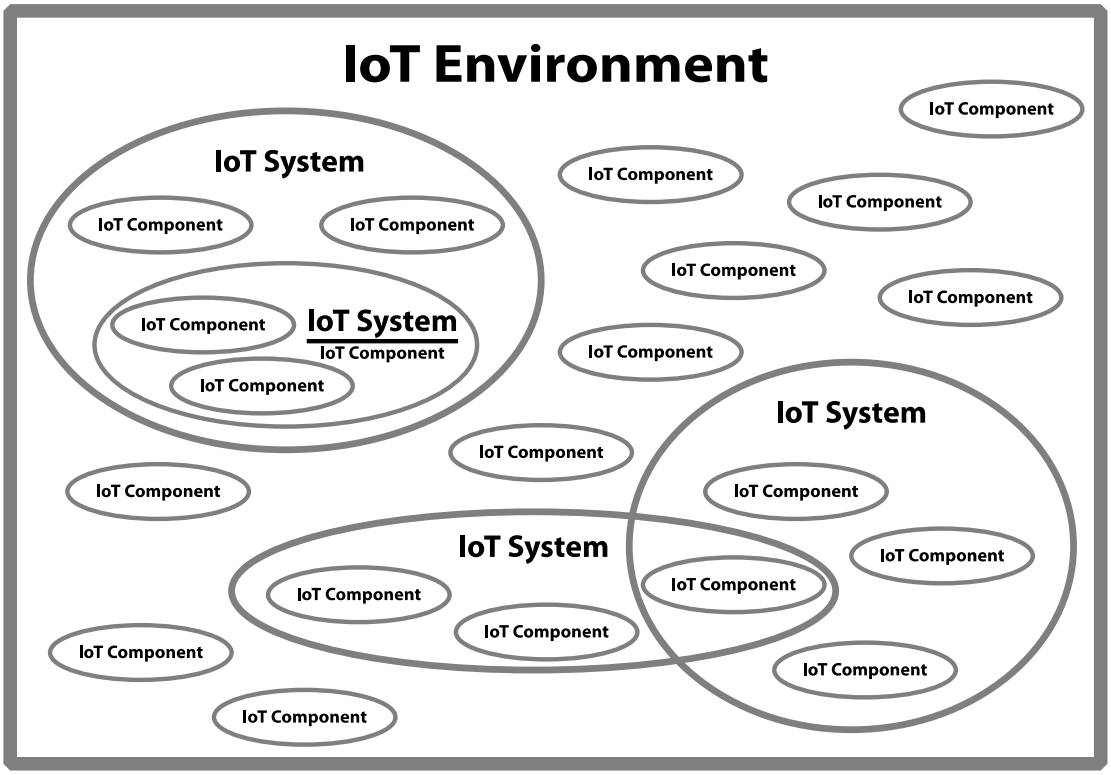

Figure 2 - Example of an IoT environment

3.3. Interaction with the Physical World

IoT systems are digital systems that interact directly with the physical world. Therefore, the relation between the cyber (digital) and the physical is important. From an IoT perspective, interactions can be grouped into three types: logical, physical, or logical-physical. *Logical* (or *cyber*) *interactions* are exchanges of symbols (representing information) and affect the logical state of the system [L_1, …, L_n], while *physical interactions* are exchanges of matter or energy and affect the physical state of the system [P_1, …, P_m]. *Physical-logical* (sensing and actuating) *interactions* convert physical energy to logical information (or logical information to physical energy) as shown in **Figure 3**.

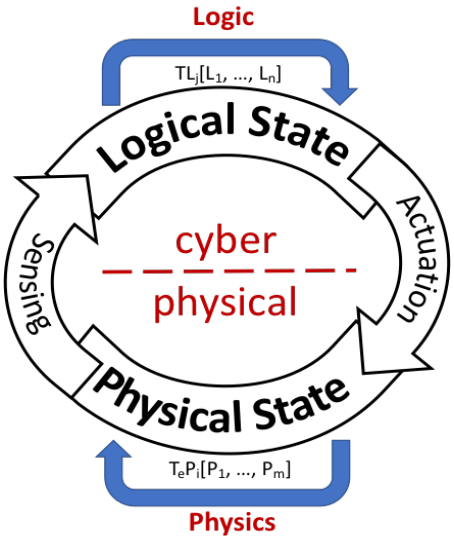

Figure 3 - Interactions Between the cyber and the physical

The sensors and actuators in IoT systems link the logical state of information technology systems (governed by logical constructs), with the physical state of an entity (or entities) of interest [**Figure 3**]. Individual interactions and compositions of both sorts operate on the overall state of the combined systems, ($TL_i[L_1, \ldots, L_n]$ and $T_eP_i[P_1, \ldots, P_m]$ represent the combined logical and physical state descriptions). The understanding of both cyber and physical interactions and the interplay between the two is essential to the success of any IoT system and is also referred to as the study of Cyber Physical Systems (CPS). For more information on CPS, see the NIST Framework for Cyber-Physical Systems [8].

4. IoT Component Capability Model (IoT CCM)

Understanding the set of capabilities of a given IoT component is essential to being able to use the component in an IoT system with confidence. A simple definition of *capability* is "the quality of being able to perform a given function."

Many IoT components are black boxes, meaning the organizations acquiring, using, and administering them have little or no access to information about their internal workings, including the capabilities they offer. For white box IoT components, where detailed information about the internal workings is available, there are often no standardized mechanisms employed to expose, access, and configure capabilities.

Regardless of whether IoT components are white or black boxes, it is useful to have a standardized approach to describing an IoT component's capabilities. This model uses a black box approach to focus on the functionality that a given IoT component can provide to a system. Functionality that is internal to an IoT component is not visible using this model.

The diagram shown in **Figure 4** provides a model of the capabilities an IoT component can provide. The large grey box represents an IoT component and the remaining boxes represent capabilities types for an IoT component. Each IoT component can then be characterized by the set of capabilities it provides. A given IoT component may have more than one of any

given capability type (e.g., sensors, network interfaces, actuators) but it must have at least one network interface capability and one additional capability that is provided through the network interface. This model can also be used to describe a set of IoT components and relationships formed into a given IoT system or it can be used to describe the capabilities of an IoT system.

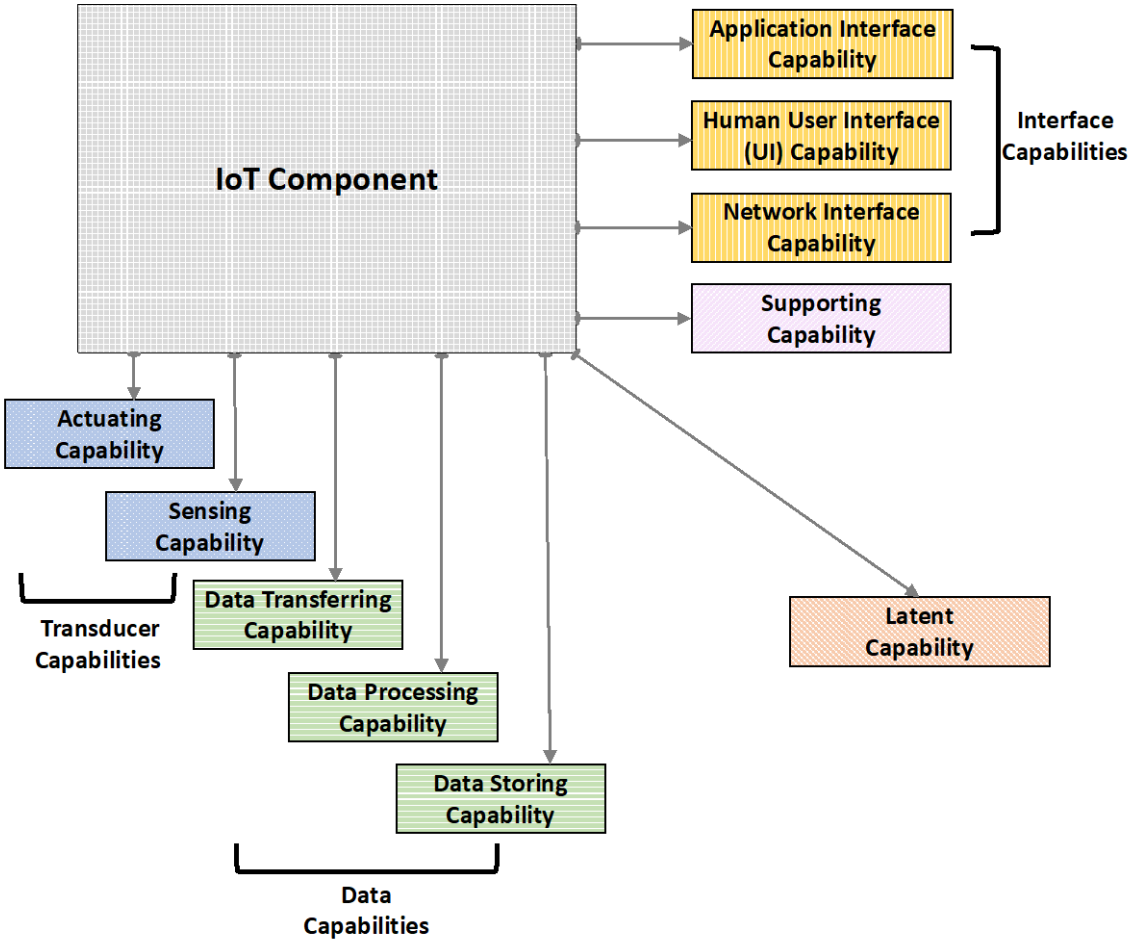

Figure 4 - Capabilities of an IoT component

The IoT capabilities can be grouped into several categories:

- *Transducer capabilities* interact with the physical world. These capabilities, prevalent in OT, serve as the boundary (edge) between the digital and physical environments. Transducer capabilities provide the ability for computing systems to interact directly with physical entities of interest.
- *Data capabilities* are directly involved in providing functionality to the system. These capabilities—data storing, transferring, and processing—are commonly associated with conventional IT systems, and are critical to IoT systems.
- *Interface capabilities* provide the component the ability to interact with other IoT components (including people using a connected device to interact with the other system components).

- *Supporting capabilities* are indirectly involved in providing functionality to the system, such as monitoring, management, security, or orchestration.
- *Latent capabilities* are transducer, data, interface, or supporting capabilities that are not currently enabled and accessible outside the IoT component. These capabilities can potentially be enabled either by a trusted actor or a bad actor with malicious intent.

The subsections below provide additional information on each capability category.

4.1. Transducer Capabilities

4.1.1. Actuating

An *actuating capability*, provided by an *actuator*, offers the ability to make a change in the physical world based on information given as input to the component.

Errors may be introduced in the digital logic, the digital to analog converter, the analog electrical circuit, and the actuator transducer. There is a time delay between the input data arriving at the component and the change being made to the environment.

Examples of actuating capabilities include heating coils (heating capability), electric shock delivery (cardiac pacing), electronic door locks (lock/unlock capability), unmanned aerial vehicle operation (remote control), servo motors (motion/movement capability), and robotic arms (complex motion/movement capability).

An important type of actuator is a black box control system that accepts a desired outcome as an input and internally uses sensors, actuators, and processors to make the physical changes. This is considered an actuating capability in this model since the sensors and processors are not directly usable from outside the component.

4.1.2. Sensing

A *sensing capability* (provided by a *sensor*) offers the ability to provide an observation of an aspect of the physical world in the form of measurement data. Information from sensor observations may be provided to other IoT components through the component's network interface for processing and storage.

Sensing is "read only"; any change to the physical state is a side effect. Measurement errors may be introduced by the physical environment between the physical system and the sensor transducer, in the sensor transducer itself, in the analog electrical circuit, in the analog to digital (A/D) converter, and in the digital logic of the sensor. There is also a time delay between the sensing and the data becoming available at the component output.

Examples include temperature sensing (temperature measurement capability), computerized tomography (CT) scans (radiographic imaging), spatial sensing (accelerometers, gyroscopes), optical sensing, and audio sensing.

4.2. Data Capabilities

4.2.1. Data Storing

A *data storing capability* provides the ability to store and retrieve data and information over time. The intent is to store data for use at some later time. Data persists for a finite period. Data may be published by the component or provided in response to an external request. There is a time delay between the input and output, i.e. between a data request and the data response.

Examples of data storing capabilities include databases, data brokers (such as a Message Queuing Telemetry Transport (MQTT) broker [10]), and any other type of component that stores input data for later use.

4.2.2. Data Transferring

A *data transferring capability* provides the ability to transmit data from one physical or logical location to another. The data transferring capability provides the ability to 'black box' a network and provide information about the network without having to understand the specific network topology.

As the interactions of an IoT system with the physical world require the data transferring network to meet latency, reliability, and security requirements, it is useful to be able to describe the network characteristics in this manner, so the capability is explicitly called out by the IoT general model.

Examples of specific data transferring capabilities include data networks based on Ethernet, Institute of Electrical and Electronics Engineers (IEEE) 802.11 (also known as WiFi) [11], and Long-Term Evolution (LTE) [12].

4.2.3. Data Processing

A *data processing capability* provides the ability to transform data based on an algorithm. The intent of processing is to transform input data and provide output data. There is a time delay between the input and output that should be accounted for. The transformation may be very simple, with a single input variable and a single output, or it may be complex with multiple inputs and outputs.

Control algorithms are an important type of processing that take the output of sensor(s) and actuator(s) or pre-processor(s) and provide an output that can be fed into an actuator or post-processor. These control algorithms often are used within negative feedback loops, but not always. A proportional-integral-derivative (PID) control algorithm is an example of such a control algorithm.

Some examples of processing include data aggregation, binary (Yes/No) analysis, big data analytics, machine learning, and predictive analysis.

4.3. Interface Capabilities

4.3.1. Application Interface

An *application interface capability* provides the ability for other IoT components (components, systems, etc.) to communicate with a given IoT component through an IoT component application. A widely used type of application interface is an application programming interface (API).

4.3.2. Human User Interface

A *human user interface (UI) capability* provides the ability for the component to communicate directly with people. Not all IoT components have a human UI capability (i.e., a dedicated processing component). Any effect on the physical environment is a side effect of the interface (the purpose being information exchange) and as such is not considered to be sensing or actuating. Examples of human UI capabilities include keyboards, mice, microphones, cameras, scanners, monitors, touch screens, touch pads, speakers, and haptic devices.

4.3.3. Network Interface

A *network interface capability* provides the ability to interface with a digital communication network for the purpose of communicating data from one component to another. Every IoT component must have at least one network interface capability and may have more than one. While the network interface capability allows for a component to be connected to a communication network, it does not provide the communication (data transferring) capability. Some examples of network interface capabilities include Ethernet adapters, LTE radios, ZigBee radios, and WiFi dongles.

4.4. Supporting Capabilities

Supporting capabilities provide additional functionality that supports the IoT system. Examples of supporting capabilities include time synchronization, data encryption, authentication, orchestration, and remote component management. Note that some IoT components may only provide a supporting capability such as orchestration and not offer any transducer or data capabilities.

4.5. Latent Capabilities

The *latent capabilities* are capabilities that the IoT component could potentially provide but are not currently enabled for access externally from the IoT component. For example, a component may have an empty USB port with nothing plugged into it. In that state, the USB port is considered a latent capability. It has the potential to be used at any time, and if someone attaches something to it, that could enable any of the other capabilities — if someone plugs a WiFi adapter into the USB port, the IoT component would then have an additional network interface capability. USB ports and other communication interfaces, such as serial, High-Definition Multimedia Interface (HDMI), Digital Visual Interface (DVI), DisplayPort, and External Serial Advanced Technology Attachment (eSATA), often change their state and thus may switch from being a latent capability to an active capability and back.

5. Key Capability Transformations

To provide value or benefit to an IoT system, an IoT component may perform some type of transformation. Key capabilities and their respective transformations are listed in **Table 1**.

Table 1 - Key capability transformations

Capability Type	Input Type	Transform Input	Transform Output	Output Type
Sensing	Physical energy	Property of physical system state	Representation of property of physical state	Digital data
Actuating	Digital data	Representation of desired change in aspect of physical state	Changed property of physical system state	Physical energy
Data Processing	Digital data	Set of information	New set of information	Digital data
Data Storing	Digital data	Set of information	Set or subset of information available over time	Digital data
Data Transferring	Digital data	Set of information	Same set of information available over distance	Digital data

6. Implications of IoT

Although every IoT system in its IoT environment has a unique set of characteristics, we can generalize some implications of how IoT differs from conventional networked IT. IoT has several important implications for the usage, management, and maintenance of IoT components and systems compared to conventional IT.

- **Diversity of primary capabilities.** IoT offers a larger range of primary capabilities, and IoT components and systems are much more heterogeneous in terms of the capabilities each provides.
- **Interactions with the physical world.** IoT sensor data, being based on the physical world, always has uncertainty. IoT systems with actuators introduce the possibility of physically damaging equipment and facilities, as well as harming people.
- **People.** People plus a networked device (e.g., smartphone, tablet, computer) can potentially participate in an IoT system as an IoT component, providing one or more of the transducing or data capability types (actuating, data storing, data transferring, data processing, and sensing) to an IoT system. However, they will do so fundamentally differently than an electronic device would. Additionally, people can be the physical entity an IoT system is interacting with, and people can also be the end user of an IoT system. The roles of people should be well understood for a given IoT system.
- **Access.** Networking of IoT components may allow remote access to IoT systems from anywhere on the network (which, in the case of the Internet, is effectively the entire world). This access often reflects heterogeneous ownership: an IoT system may have components owned by third parties, who may have access to data from the system or even access to and control of the system itself for monitoring, maintenance,

and troubleshooting purposes. In addition, IoT components and systems may not have local user and administrator interfaces, or the interfaces may exist but lack the features offered by conventional networked IT systems.

- **Modularity.** IoT components are modular, so they can be quickly and easily assembled into IoT systems in new and different ways. This supports reuse of components and dynamic system building and modification, as well as advanced system of systems.

- **System of systems (of systems).** Because an IoT system can also be an IoT component for another IoT system, an IoT system can become extremely complex, with many levels of nesting (e.g., system of systems of systems of systems). Such an IoT system may exist at an enormous scale, even over much of the world.

7. Using the IoT CCM to Develop an IoT Testbed

The model discussed in this paper will be evaluated and tested with a new IoT testbed that is focused on building IoT systems using IoT components within an IoT environment. The testbed will be designed around the model's characteristics and component-system-environment as a basis for scoping out the testbed's design and architecture.

The testbed team will create a set of IoT components using the IoT component capability model as a template. The IoT CCM will then be used to create a description of each IoT component. The testbed will use a TCP/IP based network built using off the shelf equipment. It will be expanded to support additional networking technologies at a later date. Standard protocols will be used for the application interface capabilities allowing off the shelf IoT components to be used along with the custom built IoT components giving great flexibility in the creation of a wide variety of IoT systems. Internal and external communications about the testbed will use the language laid out in this document.

In addition to evaluating the model, the testbed will be used to research different aspects of IoT systems [13]. This includes researching how to test and evaluate IoT systems with a focus on the understanding of each IoT component and the relationships between components. How do these components interact with each other to form a new system with new capabilities and other emergent properties? Of particular interest is; quantitatively measuring and evaluating the capabilities of an IoT component, accurately expressing those capabilities so the component can be used in a system, calculating the capabilities of a given system based on the capabilities of its constituent components and evaluating systems to verify the performance of the system.

Acknowledgments

Thanks to Karen Scarfone, Bill Fisher, Danna Gabel O'Rourke, and the other experts in the NIST Information Technology Laboratory (ITL) and Engineering Laboratory (EL) for all their input.

References

[1] *The 'Only' Coke Machine on the Internet*. https://www.cs.cmu.edu/~coke/history_long.txt

[2] Gabbia A (2015) *Kevin Ashton Describes "The Internet of Things"* Smithsonian Magazine, January. https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/

[3] Weiser M (1991) The Computer for the 21st Century. *Scientific American Special Issue on Communications, Computers, and Networks.* 91(09). 94-104.

[4] Simmon E, Kim K, Subrahamanian E, Lee E, de Vaulx F, Murakami Y, Zettsu K, and Sriram R (2013) *A Vision of Cyber-Physical Cloud Computing for Smart Networked Systems*. NIST IR 7951. https://doi.org/10.6028/NIST.IR.7951

[5] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, Gabel O'Rourke D, Scarfone K (2019) *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. NIST IR 8228. https://doi.org/10.6028/NIST.IR.8228

[6] Fagan M, Megas K, Scarfone K, Smith M (2020) *Foundational Cybersecurity Activities for IoT Device Manufacturers*. NIST IR 8259. https://doi.org/10.6028/NIST.IR.8259

[7] *The Industrial Internet of Things Vocabulary*. https://www.iiconsortium.org/pdf/Vocabulary-Report-2.3.pdf

[8] *ISO/IEC/IEEE 15288:2015 Systems and software engineering -- System life cycle processes*. https://www.iso.org/standard/63711.html

[9] Griffor ER, Greer C, Wollman DA, Burns MJ (2017) *Framework for Cyber-Physical Systems: Volume 1, Overview*. NIST SP 1500-201. https://doi.org/10.6028/NIST.SP.1500-201

[10] *MQ Telemetry Transport*. http://mqtt.org

[11] *IEEE 802.11*. http://www.ieee802.org/11/

[12] *LTE*. http://www.3gpp.org/technologies/keywords-acronyms/98-lte

[13] Sriram RD, Sheth A (2015) *Internet of Things Perspectives*. IT Professional, *17* (3), 60-63.