1. Introduction
The Internet of Things (IoT) is a term that both draws our attention and captures our imagination, but often escapes a definitive meaning. One person may say that IoT is all about connecting devices to the Internet, including cell phones, washing machines, watches, and anything else, while another person may say that IoT is connecting everyday things embedded with computing devices to the Internet so they can exchange data. Both definitions speak truth to one degree or another, but are somewhat lacking, because they do not fully describe an important and powerful subset of IoT technology, the Industrial Internet of Things (IIoT). What sets apart the IIoT from the broad category of IoT? The answer to this question is the topic of this learning module.

To answer the question, we will first briefly tour the history of automation, and then explore traditional machine-to-machine (M2M) communication technology, which is the immediate predecessor of the IIoT, to give context to the topic. Then we will explain the key benefit of the IIoT: how data collected by the "things" can help drive better business decisions for enterprises.

This learning module will also cover the great technological expanse of the Industrial IoT by examining its building blocks, systems, and technologies, including an example of a purpose-built IIoT platform—EcoStruxure™—to see how complex automation systems can be built to deploy Smart Enterprise Control.

2. Objectives
Upon completion of this module, you will be able to:

- Discuss the relationship between the IIoT and operational and information technology
- Name the primary differences between traditional M2M and IIoT systems
- Define the building blocks of an Industrial IoT system
- Explain the difference between a reference and an applied IIoT architecture
- Define an IIoT platform and describe its benefits
- Describe the three layers of the EcoStruxure™ IIoT platform

3. Definitions
Industrial IoT has many terms and concepts with which some readers may not be familiar. So, let’s start this learning module by defining important terms. These definitions will help you build a vocabulary for understanding the concepts presented herein.

**Abstraction**: A technique for dealing with complexities in software development by separating the non-important characteristics of the things from the important characteristics. It’s a technique used in IoT solutions development.
- **Asset Performance Management (APM):** Software applications used to improve the reliability and availability of physical assets while forming intelligent asset strategies.
- **Backhaul Network:** The links between the core network and the edge network.
- **Big Data:** The large volume of data generated by IoT sensors, both structured and unstructured, that can be analyzed for business insights.
- **Breaker:** An automatically operated electrical switch that protects a circuit from damage caused by overloads, overcurrents, or short circuits. See Essential Circuit Protection I.
- **CANopen:** An application layer protocol for industrial automation that connects devices via peer messaging.
- **Customer Relationship Management (CRM):** Software applications that assist enterprises in managing business processes such as customer data, retention, acquisition, and sales.
- **Drive:** An electronic controller used to control and vary AC motor speed and torque by varying motor input frequency and voltage.
- **Edge Control:** Intelligent controls located as close as possible to a sensor, actuator or other remote device.
- **Enterprise Resource Planning (ERP):** Software applications that help manage business processes such as planning, purchasing, inventory, sales, marketing, finance, and human resources.
- **EtherNet/IP:** An open industrial networking standard, used in industrial automation; it allows the deployment of standard Ethernet technology (IEEE 802.3 with the TCP/IP Suite) while enabling Internet and enterprise connectivity.
- **Evolvability:** The capacity to efficiently change a solution to serve new objectives, functions, or purposes. Functional Layers: The hierarchy of functions of a network.
- **Heterogeneities:** Devices and systems that operate on different communication protocols.
- **Internet of Things (IoT):** A set of devices and systems that interconnect sensors and actuators that interface with the physical environment to the Internet.
- **Industrial Internet of Things (IIoT):** A network of industrial control systems and devices, connected to the Internet by communication technology, to transfer and communicate data to a cloud platform for use in analytics, services, and applications, resulting in frameworks that can determine business insights to drive better decision-making for enterprises.
- **IoT Applied Architecture:** A framework for the specification of a network's physical components and their functional organization, operational principles, and data formats.
- **IoT Platforms:** An intelligent layer that connects the sensing and actuating devices to the network and abstract applications from the IoT devices with the goal of enabling services development. Platforms provide a framework for developing IoT applications.
- **Machine-to-machine (M2M) Communication:** Point-to-point communication between devices using wired or wireless communications.
- **Modbus TCP/IP:** Uses TCP/IP and Ethernet to carry data using the Modbus message structure between compatible devices.
- **Operational Technology (OT):** Hardware and software that process operational data from industrial processes. OT frequently uses industrial control systems, SCADA, and PLCs.
- **Product Lifecycle Management (PLM):** The process of managing the lifecycle of a product from ideation through development, production, service, and end-of-life elimination.
- **Programmable Logic Controller (PLC):** An industrial computer used for the control of manufacturing processes, such as assembly equipment, robots, motors, or industrial processes.
- **Scalability:** The ability of a system or network to be enlarged for growth.
- **Smart Enterprise Control:** The tight integration of intelligent machines and manufacturing assets across an entire enterprise.
- **Supervisory Control and Data Acquisition (SCADA):** A control system architecture that uses computers, networked data communications, and graphical user interfaces for high-level supervisory management of industrial processes.
- **Supply Chain Management (SCM):** The management of the flow of parts, raw materials, finished products, and services, including transportation, storage, and inventory of materials.
- **Technology Silo:** The control of a specific industrial process or machine for which it was originally designed. Traditional M2M communication systems are siloed technologies, while open IIoT systems are not.
- **Uninterruptible Power Supply (UPS):** An electronic system that provides emergency power to a load when the input power source or mains power fails.
4. Industrial Automation to Industrial IoT

As a technology solution, the IIoT is the outcome of earlier versions of information, operational, and automation technology. To better appreciate the beginnings of the IIoT, let us begin this section by briefly touring the history of automation. Then, we will explore the immediate predecessor of the IIoT, machine-to-machine communication (M2M), and explain how M2M communication systems are transitioning into the IIoT.

- 4.1 History of Automation

![Figure 2: The Stages of Automation](image)

It's hard to pinpoint an exact date when the field of automation began. Some claim that one of the earliest "automation" inventions was a feedback control mechanism used in a water clock for accurate timekeeping around 250 B.C. Dutch inventor Cornelis Drebbel invented an incubator and a thermostat during the 1620s which automatically kept the incubator at a constant temperature. In the 1930s, radar and sonar were invented, both of which are considered the dawn of automation technology in the modern era. Shortly after World War II, General Motors opened an automation department, which is considered by many a milestone for the industrial use of automation.

But it wasn't until the 1960s that automation was deployed in a form that we understand today. This was when machine-to-machine communication (M2M) was painstakingly invented by Theodore G. Paraskevakos for a caller line identification system, what we now refer to as Caller ID.

In the late 1960s, the first programmable logic controllers (PLCs) were rolled out to replace electromechanical relay logic. Instead of using hardwired relays wired in such a manner to turn on and off equipment using timing relays, interlocks, and electromechanical sensors, PLCs could be programmed to perform the same functions with more flexibility.

While not directly related to industrial automation per se, the invention of the Transmission Control Protocol (TCP) and the Internet Protocol (IP) by Vint Cerf and Bob Kahn in the 1970s had a major impact on industrial automation in subsequent decades. These technologies set in place the possibilities of IIoT by enabling network communication: TCP transport could be used to deliver data across IP networks. The rollout of Global System for Mobile communication (GSM) in the early 1990s led to cellular M2M communication, which has been used in point-of-sale (POS) terminals, in-vehicle telematics, remote monitoring and tracking, and tracing applications. The limitations of traditional M2M-based automation spearheaded the development of the IIoT.

- 4.2 M2M Communication

The development of machine-to-machine communication (M2M) was an important step in realizing the IIoT. M2M is point-to-point communication, typically with fixed lines using different/proprietary protocols or mobile networks, between devices of the same type and a particular application. In this manner, M2M systems are closed systems, meaning the data they generate cannot be widely shared with other equipment or used for purposes for which it was not designed. Today, the control of M2M communication systems is typically accomplished with programmable logic controllers (PLCs).
Programmable logic controllers are an important part of supervisory control and data acquisition (SCADA), which is a supervisory control system with applications for managing large-scale, automated industrial operations. It’s a software package of applications that gathers data in real-time from remote locations in order to control equipment and conditions. While M2M systems using SCADA work quite well in the control of process automation equipment, M2M systems in the context of IIoT are considered to have limitations. Traditional M2M systems are often proprietary and not connected to the Internet. As such, they do not have the broader services, analytics, and applications that would be typical of an IIoT system. This is why M2M systems are called dedicated, single-use, or "siload" technology. Siload technologies work well at controlling a specific industrial process, but they typically do not have the capability to share data with the ERP, PLM, or SCM systems of a business enterprise.

### 4.3 M2M to IIoT

The terms M2M and IIoT have common roots because, in some respects, they refer to the same thing: the interconnection of different devices (sensors or actuators) into an industrial control system to achieve a tangible result or output. M2M is the more technical term since it defines the connections between devices that are managed and monitored, not with direct human operation, but independently via the devices’ messaging capabilities and programming. But IIoT offers important capabilities that traditional M2M systems do not. Let’s explore the differences between M2M and IIoT in this section.

Previously, we touched upon the difference between M2M and IIoT systems in terms of siloed/closed and data-sharing/open technologies, respectively. That is, an M2M system is built to control a dedicated process, typically an industrial machine or group of interconnected machines, via wired or cellular connectivity, using point-to-point communications and embedded hardware modules that run a dedicated application. IIoT systems use the Internet as an interconnection means in order to send device data to the cloud, where multiple applications and/or services can be made available.
IIoT systems enable the ability to share data across an enterprise in order to obtain business intelligence to manage operations better. Transitioning from closed silo deployments to open, multi-functional IIoT technologies allows the integration of device and sensor data with Big Data, analytics, and other enterprise applications. M2M systems solve problems through service improvement at the device or machine level, while IIoT systems use analytics and Big Data to realize enterprise-wide improvements.

M2M systems often focus on reducing service-related costs with remote diagnostics, remote troubleshooting, updates and other remote capabilities that reduce the need to send out field service engineers to far flung sites. IIoT systems, on the other hand, emphasize obtaining improvements in operations and offering information products as a service via the cloud. To put it another way, IIoT is a transition from hardware (devices and connectivity) to software (services, data, and actionable knowledge) in order to improve operations.

- **4.4 IIoT to Smart Enterprise Control**

The development of the IIoT has created the possibility of integrating information technology (IT) systems used to manage business processes for an enterprise with operational technology (OT) used to monitor and control physical equipment and industrial processes. This integration, called the convergence of IT and OT systems, can enhance the overall performance of the enterprise.

The IIoT makes the IT/OT convergence possible because of its ability to share data gathered by the OT systems with the IT systems via the Internet, which is sent to the cloud and applied to analytics to derive the knowledge for better decision-making. The IT/OT convergence, enabled by IIoT, creates the prospect of Smart Enterprise Control. Smart Enterprise Control is the tight integration of smart connected machines and smart connected manufacturing assets within the wider enterprise. One of the biggest potential benefits of IIoT systems is the breakdown of enterprise silos. These technologies allow for closer integration of production systems and Enterprise Resource Planning (ERP) systems, Product Lifecycle Management (PLM) systems, Supply Chain Management (SCM) and Customer Relationship Management (CRM) systems.

Some of the benefits derived from Smart Enterprise Control include:

- Mass customization and lot sizes of one
- Reducing the size of product recalls
- Detection of defective products earlier
- Modification of product design to eliminate root causes
5. IIoT Building Blocks

As suggested by section 3 of this learning module, the Industrial IoT has lots of new terms, equipment, systems, and so on with which an IoT project builder, or even an engineer of another domain of expertise on the element14 Community, may be unfamiliar. This statement may very well apply to the hardware, equipment, and software typically used in IIoT systems. So, let's use this section to get familiar with the hardware and software building blocks of a generic IIoT system to aid the understanding of the system as a whole.

- 5.1 Connected Devices

Located on the edge of an IIoT system, connected devices are the "things" of an industrial application that perform a sensing or actuating function for the industrial control process, system, machinery, or other ancillary equipment. They generate the raw data that will ultimately be accessed by the wider enterprise once it is pushed to a cloud platform or some form of data repository. There are a wide range of devices. Typical examples include breakers, drives, UPSs, motor starters, energy monitors, smart instrumentation, relays, sensors, flow metering devices, intelligent on/off valves, and other smart-connected devices. Some devices have data processing capabilities. These devices are connected to a gateway via wired, wireless, or cellular connectivity. Another option is the use of wireless sensor networks, which include sensor and actuator nodes, along with gateways and clients.

Figure 7: Some Examples of Connected Devices

- ZigBee® Wireless Limit Switch
- Wireless, Pushbutton Harmony XB5R
- Variable Speed Drive, Altivar Machine ATV320 Series
- TeSys T Motor Management (Starter) System
- Ultrasonic Sensor, OsiSense™
- Remote Control Station, Harmony™ eXLhoist
- 5.2 Operational Technology
Operational Technology (OT) consists of computing systems that control industrial operations, and equipment such as process machines, production equipment, and remote monitoring systems. Industrial control systems (ICS) are part of OT and use PLCs for process control, and Supervisory Control and Data Acquisition (SCADA) systems to monitor and manage the process control system.

![TM241CE24TPLC Modicon ™ M241 Series](image1)

![TM251MESCPLC Modicon ™ M251 Series](image2)

![Modicon TM4 I/O Module](image3)

*Figure 8: Some examples of controllers and I/O modules used in an OT System*
- **5.3 Gateways and Networking Infrastructure**

Gateways are hardware and software that support edge computing and serve as a connection point between the edge connected devices and the cloud platform. They perform connectivity consolidation by taking device data of different communication protocols and translating them into a single protocol before sending it upstream. Advanced gateways can process data and/or perform computations before transferring it to the cloud; the benefit to this is it limits the data transferred, providing response improvements and data transmission cost savings. Gateways can also provide storage and security functions.

Networking infrastructure provides the means of connecting devices to cloud applications and services using wireless networks. LANs cover small areas such as a home, building, or an office. WANs provide communication links to the backhaul network; they cover large areas, from cities, regions, to larger geographical areas. Gateways, switches, routers, and multiplexers are common types of networking devices.

*Figure 9: Examples of gateways and networking devices*
- **5.4 Industrial Communication**
A communication protocol is an agreed upon way for devices or machines to communicate with one another. There are many different industrial communication protocols for the interconnection of connected devices and I/O modules. The main ones include: serial communication (RS232, RS422 and RS485), DeviceNet, ControlNet, Modbus, ModBus-TCP, FieldBus, Profibus, EtherNet/IP™, EtherCAT, Profinet, PowerLink, and Sercos III.

- **5.5 Data Management**
Data management systems handle the essential functions of data acquisition, validation, storage, and the availability of critical information. IIoT systems use a wide variety of devices for data generation, and thus IIoT data is heterogeneous, spanning temporal, spatial, polymorphic, and proprietary data types. Massive amounts of data will be generated as well, with predictions already of 1 petabyte of data for a smart factory. Managing this level of data will require using a massive data / Big Data technology.

- **5.6 IIoT Analytics**
IIoT analytics uses data analysis tools to obtain insights and actionable operational intelligence from the data produced by the connected devices. Analytics includes real-time or edge computing and batch analysis. Analytics can be behavioral, descriptive, predictive, or prescriptive. Visualization solutions use dashboards, alerts, events, maps, and other tools to present easily comprehensible data to end users. Analyzing data from operational technology can provide insights for reducing maintenance costs, obtaining predictive failure analyses, and implementing overall improvement strategies for business operations.

- **5.7 Information Technology: Business Processes**
Business processes are a series of activities within an enterprise that lead to achieving specific business objectives. The IIoT enables business processes by acquiring very detailed data about real-time operations and making it available to the enterprise's IT systems in a timely manner. As a result, better business intelligence and more informed decision-making can be realized. Typical IT business process applications include ERP, PLM, SCM, etc.

- **5.8 IIoT Platform**
IIoT platforms are a stack of intelligent layers that connect the sensing and actuating devices to the network and abstract applications from the IoT devices with the goal of enabling services development. Platforms provide a framework for developing IoT applications. Key benefits of IIoT platforms include the facilitation of communication, data flow, device management, and application functionality across the IIoT system. As a result, they enable enterprises to bring IIoT solutions rapidly to the market.

**Figure 10:** A simplified Block Diagram of the EcoStruxure™ IIoT Platform. (Sections 6.2 and 6.3 have a detailed description.)

---

1 **Industrial Software Subcategories:** Process Engineering, Planning & Scheduling, Operations Management, Enterprise Asset Performance Management, Information Management, & Operations Control

2 **Industrial Automation Management Subcategories:** Modicon, PES, Foxboro, Triconex
6. IIoT Architecture: Reference and Applied

An IoT architecture represents the various layers of technologies and their functionalities in an IIoT system and illustrates how they relate to one another. There are two types of IoT architectures: reference and applied. A reference architecture is a set of guidelines for developing an applied IIoT architecture, with respect to the system’s objectives, design principles, and desired elements. An applied architecture is a blueprint for the development of an actual system.

- 6.1 Developing a Reference Architecture

To develop a model for an IoT reference architecture, one needs to first establish the overall objectives and design principles. Design principles that support the objective could include, but are not limited to:

- Provide services across different business domains of the wider enterprise
- Ensure trust, security, and privacy
- Offer scalability, performance, and effectiveness
- Possess the characteristics of evolvability, scalability, and simplicity of integration
- Be capable of different service delivery models
- Possess lifecycle support

- 6.2 Applied Architecture: EcoStruxure™ Platform

An applied IIoT architecture is the embodiment of the objectives and principles delineated by the reference architecture. In this section, let’s look at an applied IIoT architecture and platform developed by Schneider Electric, EcoStruxure™. Enabling IT/OT system convergence, EcoStruxure is an open, scalable, and interoperable IIoT and energy management platform serving the business domains of building control, data center, industrial and infrastructure. It connects the three core layers of Schneider Electric’s technology stack:

- **Connected Products**: IoT-enabled connected products with embedded intelligence, including sensors, circuit breakers, variable speed drives, UPSs, relays, sensors, and process instrumentation. This layer provides the link to real-time data that is essential to higher-level control and decision-making. It also offers local control and firewall protection.

- **Edge Control**: This layer enables local control at the edge, protecting system safety and uptime. Real-time and runtime control systems are connected to field devices and collect data from them, analyzing current conditions against goals and past performance, and making autonomous control decisions (or helping in operator decision-making) to improve process performance.

- **Applications, Analytics, And Services**: This layer enables a wide range of applications, analytics, and services for seamless integration with the wider enterprise. At the highest level of the EcoStruxure architecture, it handles sophisticated problem-solving and analysis on an enterprise-wide basis to optimize business operations and maximize results. On this level, a wide variety of software and services are provided, including: (i) advanced predictive analytics for process and equipment, (ii) virtual and augmented reality for operators and maintenance personnel, (iii) energy/process optimization and simulation, (iv) and integrated operations, planning and supply chain management.

![Figure 11: The Three Technology Layers of the EcoStruxure Platform](image-url)
Microsoft’s Azure IoT cloud is the backbone of EcoStruxure, using Azure’s digital services, apps and analytics. The platform includes options to deploy on the cloud and/or on-premise and has the ability to scale up from medium to large, multisite-facility enterprises. Additionally, it employs advanced cybersecurity and supports industry standard and IP-based open protocols to facilitate the secure exchange of data and analytics.

- 6.3 Real-World Application of EcoStruxure

We have thus far discussed the building blocks and fundamentals of *generic* Industrial IoT systems. So, let’s go a step deeper in our discussion, and describe an IIoT system that is more closely aligned to real-world applications.

Refer to Figure 12 for the remaining part of our discussion. It illustrates a detailed view of an Industrial IoT system, from the machinery/plant floor all the way up to the enterprise ERP system. The diagram is an automation process and control interconnection diagram for an industrial application. Given the number of motor starters, variable speed and servo drives, and motion controllers, the diagram applies to a variety of applications ranging from building automation to material handling to smart factory operations.
The entire system is running on EcoStruxure, which serves as the digital backbone of the entire system. This system is an interconnected Industrial Ethernet architecture, allowing transparent communication among field, process, plant and the enterprise. By combining EtherNet/IP, Modbus TCP, and standard protocols, the entire system is interoperable, easily adapting to the evolution of technology, and allowing for the easy integration of legacy equipment. Industrial Ethernet/IP also gives the system flexibility in terms of what topologies (e.g., Star, Daisy Chain, Daisy Chain Loop, Ring, Wi-Fi, etc.) and what networks (e.g., Ethernet, PROFIBUS, CANopen) can be run on it.

Another benefit of Industrial Ethernet is that it can manage different kinds of data types and media with different protocols simultaneously. In addition, since Industrial Ethernet is based on Internet Technologies, it lends itself easily to web interfaces.

This real-world EcoStruxure platform is divided into three technology layers: enterprise, operation, and control. Let's discuss each of these layers:

**Control Level:**
The control level is where the smart-connected equipment is installed, housing the connected devices (circuit breakers, motor starters, variable speed drives, servo drives, safety logic controllers, etc.). This level also contains the machine controllers (drive, logic, and motion controllers). Some of the devices are hardwired, while others are connected via different network protocols (CANopen/CANmotion, Ethernet and Sercos). Since industrial equipment is often run on different protocols, interoperability is an important benefit of the system. The smart machine controls themselves were built utilizing MachineStruxure, which is a building block of EcoStruxure. It’s a software-based machine-building platform used to control a machine application.

**Operation Level:**
The operation level is the process automation system with combined energy management that controls the industrial processes for the entire system. The automation systems themselves were built utilizing PlantStruxure, which is a building block of EcoStruxure; it is a collaborative and integrated automation architecture for industrial and infrastructure applications. It combines data from process and power systems to give valuable and new insights into plant operations, allowing for the ability to improve overall efficiencies. PlantStruxure connects the control, operation, and enterprise levels. It uses the Modicon 580 ePAC (Ethernet programmable automation controller) to connect all field devices, such as variable speed drives, HMI, motor starters, electrical distribution, and energy management functions into a single and open system. With a built-in Ethernet backbone, the M580 architecture interconnects all the devices and provides continuous communication flow to obtain IIoT benefits. Legacy Ethernet-enabled devices or systems can be integrated with ePAC. Network technologies and web services provide efficient sharing and distribution of information between sensors, instrumentation, devices, controllers, operator work stations, and other third party systems. It also brings together Telemetry, PLC/SCADA and DCS with lifecycle services.

**Enterprise Level:**
The top of the diagram is the enterprise level. It connects operational technology with IT technology (i.e., Enterprise Resource Planning) to share data, analyze information, and create knowledge to improve decision-making and enhance value. EcoStruxure Resource Advisor is an enterprise-level, cloud-based sustainability and energy management application. It manages enterprise monthly energy and sustainability data, and detailed site interval data.

*Trademark. Schneider Electric is a trademark of Schneider Electric Corp. Other logos, product and/or company names may be trademarks of their respective owners.

**Test Your Knowledge**

Are you ready to demonstrate your Industrial IoT knowledge? Then take a quick 15-question multiple choice quiz to see how much you’ve learned from this Industrial IoT Learning Module. To earn the Industrial IoT Badge, read through the module to learn all about Industrial IoT, attain 100% in the quiz at the bottom, leave us some feedback in the comments section, and bookmark this page.

Take Quiz