

# IoT BIZ™ (Exam IOZ-110)

# IoT BIZ™ (Exam IOZ-110)

Part Number: CNX0004

Course Edition: 1.1

## Notices

### DISCLAIMER

While CertNexus, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The name used in the data files for this course is that of a fictitious company. Any resemblance to current or future companies is purely coincidental. We do not believe we have used anyone's name in creating this course, but if we have, please notify us and we will change the name in the next revision of the course. CertNexus is an independent provider of integrated training solutions for individuals, businesses, educational institutions, and government agencies. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with CertNexus. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). CertNexus is not responsible for the availability of, or the content located on or through, any External Site. Please contact CertNexus if you have any concerns regarding such links or External Sites.

### TRADEMARK NOTICES

CertNexus and the CertNexus logo are trademarks of CertNexus, Inc. and its affiliates.

All other product and service names used may be common law or registered trademarks of their respective proprietors.

Copyright © 2019 CertNexus, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. This publication, or any part thereof, may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, storage in an information retrieval system, or otherwise, without express written permission of CertNexus, 3535 Winton Place, Rochester, NY 14623, 1-800-326-8724 in the United States and Canada, 1-585-350-7000 in all other countries. CertNexus' World Wide Web site is located at [www.certnexus.com](http://www.certnexus.com).

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. Do not make illegal copies of books or software. If you believe that this book, related materials, or any other CertNexus materials are being reproduced or transmitted without permission, please call 1-800-326-8724 in the United States and Canada, 1-585-350-7000 in all other countries.

# IoT BIZ™ (Exam IOZ-110)

Lesson 1: Planning an IoT Implementation.....	1
Topic A: Defining IoT.....	2
Topic B: IoT Infrastructure.....	12
Topic C: Business Benefits and Challenges.....	19
Lesson 2: Undertaking an IoT Project.....	31
Topic A: Real-World Applications for IoT.....	32
Topic B: The IoT Development Lifecycle.....	54
Solutions.....	63
Glossary.....	67
Index.....	71



# About This Course

The Internet of Things (IoT) promises a wide range of benefits for industry, energy and utility companies, municipalities, healthcare, and consumers. Data can be collected in extraordinary volume and detail regarding almost anything worth measuring, such as public health and safety, the environment, industrial and agricultural production, energy, and utilities. New data analysis tools have been optimized for the massive amounts of data that IoT produces, enabling well-informed decisions to be made quickly.

Business professionals often have little or no foundation for understanding of the components and design decisions that go into an IoT project. They may have a traditional understanding of information technology (IT) or operational technology (OT) solutions, which may include knowledge of networks, cloud computing, and applications running on servers, desktop computers, and mobile devices. With IoT technology embedded in 95 percent of all new electronics, awareness of how IoT will impact your organization will better enable you to derive solutions to generate revenue, leverage customer data, and reduce costs.

But putting IoT systems into place can be a complicated proposition with unique considerations distinctly different from traditional IT or OT solutions. Before you can successfully manage, sell, or plan an IoT solution, you must understand the various factors that will drive an organization's decisions.

## Course Description

### Target Student

This 4-hour course is intended for business leads in project management, marketing, and sales who are seeking to grow their organization through IoT technology solutions. This course also prepares students for taking the CertNexus® IoT BIZ™ credential (IOZ-110).

### Course Prerequisites

To ensure your success, you should have a general understanding of IT business needs and your organization's strategic goals.

### Course Objectives

This half-day course and associated credential (IOZ-110) will validate a participant's knowledge of IoT terminology and their ability to understand the components of IoT infrastructure, uncover challenges for consideration, and determine the impact that IoT has on their organization.

Successful participants will be able to identify what IoT can do for their organizations and recognize the various business and technical challenges to address.

Participants will:

- Plan an IoT implementation.
- Manage an IoT prototyping and development project throughout the development lifecycle.

## The CHOICE Home Screen

Logon and access information for your CHOICE environment will be provided with your class experience. The CHOICE platform is your entry point to the CHOICE learning experience, of which this course manual is only one part.

On the CHOICE Home screen, you can access the CHOICE Course screens for your specific courses. Visit the CHOICE Course screen both during and after class to make use of the world of support and instructional resources that make up the CHOICE experience.

Each CHOICE Course screen will give you access to the following resources:

- **Classroom:** A link to your training provider's classroom environment.
- **eBook:** An interactive electronic version of the printed book for your course.
- **Files:** Any course files available to download.
- **Checklists:** Step-by-step procedures and general guidelines you can use as a reference during and after class.
- **Spotlights:** Brief animated videos that enhance and extend the classroom learning experience.
- **Assessment:** A course assessment for your self-assessment of the course content.
- Social media resources that enable you to collaborate with others in the learning community using professional communications sites such as LinkedIn or microblogging tools such as Twitter.

Depending on the nature of your course and the components chosen by your learning provider, the CHOICE Course screen may also include access to elements such as:

- LogicalLABS, a virtual technical environment for your course.
- Various partner resources related to the courseware.
- Related certifications or credentials.
- A link to your training provider's website.
- Notices from the CHOICE administrator.
- Newsletters and other communications from your learning provider.
- Mentoring services.

Visit your CHOICE Home screen often to connect, communicate, and extend your learning experience!

## How to Use This Book

### As You Learn

This book is divided into lessons and topics, covering a subject or a set of related subjects. In most cases, lessons are arranged in order of increasing proficiency.

The results-oriented topics include relevant and supporting information you need to master the content. Each topic has various types of activities designed to enable you to solidify your understanding of the informational material presented in the course. Information is provided for reference and reflection to facilitate understanding and practice.

Data files for various activities as well as other supporting files for the course are available by download from the CHOICE Course screen. In addition to sample data for the course exercises, the course files may contain media components to enhance your learning and additional reference materials for use both during and after the course.

Checklists of procedures and guidelines can be used during class and as after-class references when you're back on the job and need to refresh your understanding.

At the back of the book, you will find a glossary of the definitions of the terms and concepts used throughout the course. You will also find an index to assist in locating information within the instructional components of the book. In many electronic versions of the book, you can click links on key words in the content to move to the associated glossary definition, and on page references in the index to move to that term in the content. To return to the previous location in the document after clicking a link, use the appropriate functionality in your PDF viewing software.

## As You Review






Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

## As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

## Course Icons

Watch throughout the material for the following visual cues.

<i>Icon</i>	<i>Description</i>
	A <b>Note</b> provides additional information, guidance, or hints about a topic or task.
	A <b>Caution</b> note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.
	<b>Spotlight</b> notes show you where an associated Spotlight is particularly relevant to the content. Access Spotlights from your CHOICE Course screen.
	<b>Checklists</b> provide job aids you can use after class as a reference to perform skills back on the job. Access checklists from your CHOICE Course screen.
	<b>Social</b> notes remind you to check your CHOICE Course screen for opportunities to interact with the CHOICE community using social media.





# 1

# Planning an IoT Implementation

**Lesson Time:** 1 hour, 55 minutes

## Lesson Introduction

Before you can successfully plan and implement an Internet of Things (IoT) solution, you must understand the various factors that will drive your decisions, such as identifying what IoT can do for your organization, and the various business and technical challenges you'll need to address.

In this lesson, you will examine the wide range of possibilities that IoT offers, and you will develop an understanding of the components and design decisions that go into an IoT project by creating a simple IoT device from parts.

## Lesson Objectives

In this lesson, you will:

- Define IoT and its components.
- Describe common elements within the IoT ecosystem.
- Identify benefits and challenges of IoT.

# TOPIC A

## Defining IoT

A good place to start with an IoT project is to determine what you intend to accomplish, the various components you'll need to bring together to meet your requirements, and to identify the benefits and challenges that you'll encounter on such a project.

### Dawn of a New Day

Consider the following scenario as you use IoT technologies to start your day.

- **6:34 A.M.**—Your alarm clock has been monitoring your sleep cycles, and awakens you at the optimal time, when you'll feel completely rested.
- **6:52 A.M.**—Your refrigerator door shows a recommended breakfast, with nutritional information based on your food preferences, weight goals, and what is in your kitchen.
- **6:53 A.M.**—Your smart speaker informs you of all the meetings and appointments you have today. Traffic is congested on your normal route, so the speaker tells you that your autonomous car has prepared an alternate route that will save you 10 minutes but take two minutes longer than your normal route.
- **7:12 A.M.**—Your electric car warmed up its interior just in time for you to get in. A speaker in the car informs you that your work colleague has signed the contracts, and will have them delivered to you before your first meeting.
- **8:50 A.M.**—Your smartwatch reminds you of your 9:00 A.M. meeting.
- **8:51 A.M.**—A delivery drone enters your office, bearing a package containing signed contracts for the meeting.

Not too long ago, this scenario may have seemed to be science-fiction hype, but each of the technologies described is available today through the *Internet of Things* (IoT).

## IoT

IoT refers to the ability to connect everyday things to the cloud, which leads to many possibilities for collecting, sharing, and interpreting data, and control of remote devices. IoT's potential applications are widespread, and have the potential to increase global food production, promote safety and security, improve the quality of life in our cities, create new markets and opportunities for business, and improve our conservation of natural resources.

Kevin Ashton, who coined the expression "Internet of Things" in 1999, wrote "if we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. Radio-frequency identification (RFID) and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data."

## IoT Ingredients

Many different technologies come together to provide the ingredients for the IoT. These include:

- **IoT devices** that are:
  - **Sensing:** Able to measure the world around them, such as local temperature, humidity, or water level, or number of cars passing by

- **Active:** Able to take local action as necessary, such as turning off a light, opening a valve, or sounding an alarm
- **Connected:** Able to share data with other systems in the cloud
- **Smart:** Able to:
  - Perform initial processing and filtering of sensor data
  - Determine whether immediate (real time) action should be taken in response to locally acquired data
  - Take action based on remote instructions from the cloud
- **The Cloud,** where powerful cloud applications can:
  - Collect data from IoT devices
  - Combine IoT device data with other data sources
  - Perform data analytics to reveal trends, identify problems, predict the future
- **Client applications** that enable users to:
  - Access and view data processed in the cloud
  - Issue commands to remote IoT devices



**Note:** Smart devices alone are not IoT. Connected devices alone are not IoT. The cloud alone is not IoT. IoT becomes possible when all three of these aspects are combined, enabling IoT devices and IoT client applications to work together, data to be stored and analyzed, and cybersecurity to be maintained.

## IoT Devices

IoT devices (the *things* in the Internet of Things) take many forms, providing many possibilities for automation and data collection. IoT devices may be geared toward home and consumer use, industry, agriculture, or various other domains. Some devices are geared toward *remote sensing*, while others are geared toward *process automation* or *remote control*.

Devices may be intended to be seen, manipulated, and handled by users (like a fitness watch), or they may be intended to function completely behind the scenes, out of sight, with very little direct contact by end users, such as a basement flooding monitor or weather sensors. Devices may be very specialized toward supporting a specific feature, or they may be much more general in purpose.

## Examples of IoT Devices

The diversity of IoT devices makes it difficult to articulate an all-encompassing description of the typical device. Examples may provide a better sense of the scope encompassed by the phrase *IoT device*.

- **Agricultural sensors:** Based on measurements of soil quality and geographic location, controls the application of chemicals and amendments to the soil in real time.
- **Air quality monitor:** Monitors air quality in a room and sends alerts via the smartphone app, providing useful data for people with allergies or who otherwise have a need to monitor air quality in their living or working environment.
- **Augmented reality (AR) headset:** Wearing the headset, can look around and see the local view augmented with data from the Internet, which could be useful in tourism and travel, real estate sales, museums, and many similar situations.
- **Connected universal remote control:** Televisions and home audio have long been controllable through remote controls, but with many other devices in the smart home now accessible through the home network, a universal remote control can control much more than entertainment devices. Likewise, devices like smart speakers can also be used to control functions that previously were the domain of the universal remote.
- **Dash button:** A single-purpose connected button. The concept is named after a device sold by Amazon that automatically places an order for a consumable product like detergent when

pressed. The concept has been expanded to perform tasks such as starting a car, opening a garage door, and enabling users to create their own custom tasks, such as sending an email or activating a remote buzzer.

- **Home systems monitor:** Monitor home systems such as heating, cooling, and drainage to alert the user when there are problems, when systems need to be tuned or maintained, and so forth.
- **Industrial control:** Sensors and actuators in production equipment enable operations staff to monitor and control production and implement process automation.
- **Remote-controlled mood lighting:** Enables users to define various lighting schemes involving numerous lights throughout their home. With a single command and through pre-programmed scripts, lights can be set in a combination of light intensities and colors.
- **Scientific instruments:** Scientists can monitor and control instruments in remote locations, including places that people can't easily reach, such as the poles, the ocean, other planets, within living organisms, and so forth.
- **Smart battery:** Smart batteries can transform your conventional devices into IoT devices. For example, a smart battery in a smoke or carbon monoxide alarm could warn you through text messages and other notifications when the power is getting low. The smart battery could also immediately notify you if the alarm sounds and you're not at home to hear it.
- **Smart door lock:** Enables users to use an electronic device such as a smartphone or fob as a key, eliminating having to fumble for a key. Also enables an owner to lock and unlock a door from a remote location using a smartphone app (to enable someone without a physical key to enter under the owner's control, for example). The device can monitor and log activity at the door, activating cameras and alerting the owner through a notification on their smartphone that someone is at the door.
- **Smart home appliance** (refrigerator, range, coffee maker, etc.): Smart appliances can notify you if there is a problem or maintenance need (to change a water filter in a refrigerator, for example, or warn that spoiling food has been detected), help you monitor energy consumption, and provide remote access to the device. For example, from the grocery store, you could use a camera in the refrigerator to check if you're out of milk.
- **Smart speaker:** A cloud-connected speaker that responds to a wide range of voice commands, enabling the user to control music streaming, command home automation devices (such as smart thermostats and smart outlets), communicate with other smart speakers (like an intercom), order products online, and perform web searches using voice and audio.
- **Smart thermostat:** Monitors and controls home heating, cooling, and air flow functions, enabling remote control and data logging through other devices, automatically sensing when users are at home and adjusting the home environment accordingly, logging use of heating and cooling systems, and suggesting ways to reduce energy costs.
- **Traffic monitoring:** Traffic patterns on roads, highways, sidewalks, and hallways can be monitored to provide data related to safety, civil engineering, and timing of traffic.
- **Wireless breath analyzer:** People tend to think of breath analyzers that detect levels of alcohol consumption, and certainly there are IoT applications for such devices, but breath analyzers can also be used to monitor various health-related conditions, such as dangerous ketone levels in diabetes patients, airway inflammation in asthma patients, and many other potential health problems.
- **Wearable device:** Wearable devices can monitor for conditions such as heart irregularities, low blood oxygen levels, and so forth, to provide users with early warning of impending medical problems. They can also be used to monitor babies, patients, pets, and others who require a caretaker. Caretakers can be alerted if their charge leaves a particular area, and the device can provide data on the wearer's health and well-being.
- **Weather sensors:** Sensors mounted outdoors can monitor local weather conditions, such as temperature, humidity, and air pressure. The user can read and analyze their weather data on a mobile or desktop application. Using a [crowdsourcing](#) approach, data from weather stations owned by many different individuals can be aggregated to provide detailed weather data on a global scale, as done by Weather Underground (<https://www.wunderground.com>).

Consumer

Industry



Figure 1-1: IoT devices take many forms.

IoT in Industry

Many of the general concepts of IoT, such as the ability to measure and control processes from afar, have been used in manufacturing for decades, and, in fact, manufacturers have been quick to adopt various new IoT technologies into their own process control applications. The following is a brief history of process automation in industry.

Time Period	Description
1970s	<ul style="list-style-type: none"><li>• Programmable logic controllers (PLCs) were integrated into manufacturing facilities, enabling process automation and robotics, which transformed the way many products were manufactured. PLCs were revolutionary because they were relatively simple to program, optimized for process automation, and very reliable.</li><li>• Early machine to machine (M2M) data communication capabilities were developed, based on telephone protocols, enabling computers to communicate with manufacturing equipment. This provided limited command and control (C2) capabilities from remote locations, in ways that resemble IoT capabilities of today.</li><li>• The first iteration of Supervisory Control and Data Acquisition (SCADA), an industrial control system architecture typically used in industrial, energy, and utility companies is introduced, starting as a system for mainframe computers, with limited interoperability and networking capabilities.</li></ul>

Time Period	Description
1980s	<ul style="list-style-type: none"> <li>The advent of inexpensive personal computers (PCs) and client-server networking (using Ethernet, for example) made it possible for desktop computers in the production office to interface with PLCs on the manufacturing floor.</li> <li>SCADA is expanded to interface with PCs, local area networks (LANs), and control through PC applications. Interfacing between SCADA systems from different vendors was not supported.</li> </ul>
1990s	<ul style="list-style-type: none"> <li>Following the advent of the worldwide web, PLCs were enabled to connect to the Internet, providing a relatively simple way to expand the connection between office and manufacturing systems on an enterprise level, beyond a single location or campus.</li> <li>SCADA evolved to use an open architecture and communication protocols. Over common network protocols such as Ethernet, systems from different vendors were able to communicate.</li> <li><b>Open Platform Communications (OPC)</b>, based on Microsoft standards such as <b>Object Linking and Embedding (OLE)</b> and <b>Component Object Model (COM)</b>, was created to provide open standards and specifications for communication of real-time plant data between control devices from different manufacturers.</li> </ul>
2000s	<ul style="list-style-type: none"> <li>The development of cloud technologies and ubiquitous connected computing devices (smartphones and tablets) provided a means for those monitoring and managing manufacturing processes to become more mobile and connected than ever before.</li> </ul>
2010s	<ul style="list-style-type: none"> <li>Inexpensive and pervasive web technologies, combined with low-cost microcontrollers, sensors, and high-performing batteries, resulted in new capabilities for data acquisition and process automation on a huge scale.</li> <li>In terms of spending, industry has been the primary driver of IoT, investing more in IoT technologies than any other sector.</li> </ul>

## Industry Evolution

Industry 4.0 refers to the state of process automation, data collection, analysis, and communication in today's "smart factories." Modern industry is described as being in the fourth industrial revolution.

- Industry 1.0:** Hydro and steam-powered mechanization of production.
- Industry 2.0:** Mass production through assembly lines, and the introduction of electrical power.
- Industry 3.0:** Automation of individual manufacturing processes through computers and robotics.
- Industry 4.0:** Massive automation and interconnection of global manufacturing systems, using:
  - Sensors** to collect extensive process data.
  - Software** to accurately model physical processes based on that data.
  - Smart production machines** that can interpret data, and adjust operations in real time.
  - Global networking** to enable extensive cooperation and coordination among the various machines, devices, sensors and people involved.

Because of the way in which Industry 4.0 uses software (*cyber* systems) to model production processes (*physical* systems), the technologies used in this approach are often called **cyber-physical systems (CPS)**.





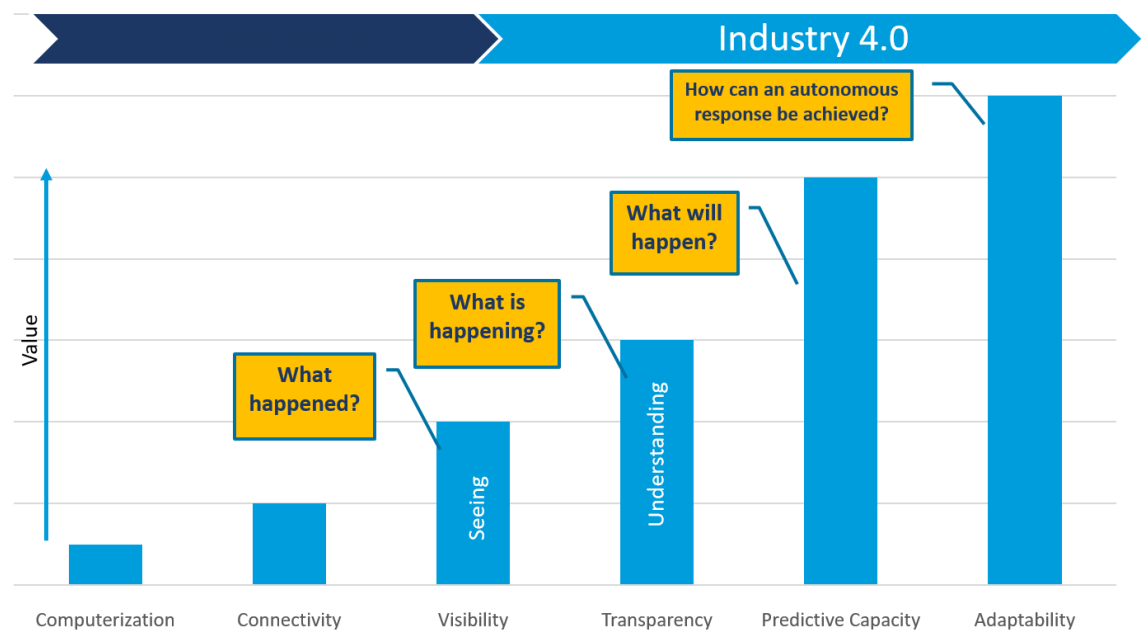
**Note:** Some people refer to Industry 4.0 as the *Industrial Internet of Things (IIOT)*. However, one might argue that Industry 4.0 preceded IoT, and has produced concepts and ideas that have subsequently been adopted by IoT, so it is not accurate to consider Industry 4.0 as a subset or derivative of IoT.

## Enabling Technologies

Various developments in technology provide the basis for IoT.

<i>Enabling Factor</i>	<i>Description</i>
Miniaturization	Significant processing power is available in a small package, with relatively powerful processors embedded in compact devices such as smart phones, smart watches and other wearable devices, home appliances, and other everyday things.
Connectivity	The ability to wirelessly connect devices, even those in remote locations, through a wide variety of technologies such as cellular data, Wi-Fi, Bluetooth®, RFID, and others, enable them to share data and respond to remote control.
Advanced power sources and power management	The ability to operate on very small amounts of electrical energy, using rechargeable batteries or harvesting energy from the surrounding environment, enable devices to function in mobile applications or remote locations, away from the power grid.
Inexpensive processors, sensors, and actuators	Relatively inexpensive components enable the proliferation of small, capable devices that can measure their local environment, process data, and respond accordingly.
Cloud-based processing	The ability to delegate data collection and analysis tasks to more powerful computers in the cloud enable IoT devices to remain compact and operate on minimal power.
Ubiquitous computing	More than ever before, people are often just an arm's length away from a computing device, whether it be a smartphone, tablet, desktop computer, wearable device, smart appliance, or some other device that provides a user interface through which users can receive notifications and run applications to control or pull information from remote devices and services.

## Industry 4.0 Promise



**Figure 1–2: The promise of Industry 4.0.**

Enabling new capabilities can help businesses add value for their customers. We can now see (and measure) not only what is happening in real time, but also even predict, with a high degree of accuracy, and respond (or actuate) in a prescriptive way. This is a powerful new capability that we did not have in the past.

An excellent article that describes this phenomenon is *Industry 4.0 and the digital twin*, which you can find at <https://www2.deloitte.com/insights/us/en/focus/industry-4-0/digital-twin-technology-smart-factory.html>

As manufacturing processes become increasingly digital, the digital twin is now within reach.

By providing companies with a complete digital footprint of products, the digital twin enables companies to detect physical issues sooner, predict outcomes more accurately, and build better products.

## Four Ps of Planned Maintenance

Early maintenance practices were *reactive*. When a component in the production system failed, causing production systems to come to a halt, the necessary repairs and maintenance would be performed, and production would then resume. This approach is sometimes called *run to failure (RTF)*.

Such unplanned downtime is costly, so manufacturers have long looked for ways to anticipate problems and prevent them by replacing components at a convenient time, before they fail. Listed in the following are four methods for planned maintenance that have been developed over the years to provide improved proactive approaches.

- **Preventive maintenance** was an early take on planned maintenance. It is driven by recommendations of the manufacturer who produces the component. Based on the estimated mean time between failure (MTBF) for a particular component, companies attempt to replace components before they are expected to go bad. This provides an advantage over reactive maintenance, as it helps to avoid many instances of downtime.
- **Predictive maintenance** relies on the ability of highly trained maintenance technicians to routinely inspect components for performance factors such as vibration, overheating, and so



forth to predict when they are nearing their end of life. Components are monitored while they are running, and fairly reliable indicators are used to detect when components are about to fail, so maintenance can be planned for a time when there will be minimal disruption to production.

- **Proactive maintenance** builds upon predictive maintenance, looking to also control the problems that lead to wear-and-tear. Remediations identified through this process include such things as training operators in best practices, identifying sources for better components, lubricants, and so forth.
- **Prescriptive maintenance** takes these approaches even further by using Industry 4.0 tools to automate measurement and analysis functions, so the system itself can spot the need for maintenance and prescribe mitigations or repair, even prioritizing those tasks among other tasks that need to be performed on the system.

## Three Key IoT Business Strategy Steps to Follow

Before you dive into IoT solutions, business leaders need to solve for these three focus areas, *in this order*:

1. **Value:** What new or incremental value does your idea provide to your customers?
2. **Insights:** What information will you need to be able to provide to support this new or incremental value?
3. **Data:** How is IoT a possible solution for you to obtain the data needed to enable these new insights?

# ACTIVITY 1–1

## Understanding Value, Insights, and Data

### Data File

C:\CNX0004Data\Planning an IoT Implementation\Understanding Value Insights and Data.docx

### Scenario

In this course, you will evaluate an IoT system to monitor the environment within agricultural greenhouses operated by Greene Organix. Greene Organix produces fresh roses for the northeast U.S. regional distributors florist market. Your goal is to see if you can identify some key areas of value that we must provide in order to deliver the best quality and freshest roses we can produce to our regional distributors.

The IoT system will collect data, analyze that data, and control the greenhouse environment as necessary to ensure all plants are subjected to optimal growing conditions. In this activity, you will identify the value of producing high quality products, what insights are needed to support that value, and what data is required. Finally, you will determine the capability of IoT to accomplish these objectives.

In the spaces provided, write your ideas regarding requirements for the IoT devices key areas of value for this scenario. (If you'd prefer to type your ideas in a Word document, a worksheet is provided in C:\CNX0004Data\Planning an IoT Implementation\Understanding Value Insights and Data.docx.)

1. **A) Identify New/Incremental Value: What elements of value would be important to produce year-round, high-quality fresh flowers for Greene Organix's distributors?**
2. **B) Understand Insights needed to support value: What information may be needed to drive down production costs so you can continue to deliver best-in-class flowers at improved competitive prices?**
3. **C) Data: What data do you need to collect to support these insights?**
4. **D) Identify data-collection capabilities you need to include in your IoT solution.**  
**Sensors — What useful information might an IoT device measure in this environment?**

5. D) Identify data-collection capabilities you need to include in your IoT solution.

**Actuators — What actions might an IoT device need to perform in this environment?**

6. D) Identify data-collection capabilities you need to include in your IoT solution.

**Other sources — What external data might be of use to support the insights?**

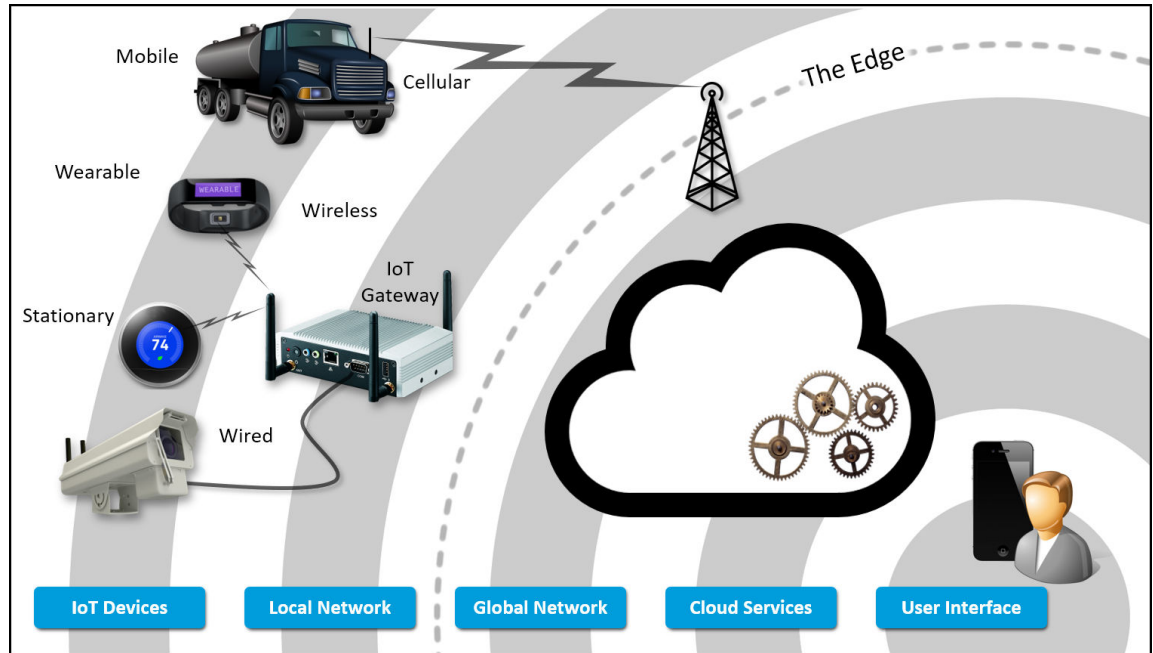
---

# TOPIC B

## IoT Infrastructure

The IoT ecosystem is typically complex. In reality, it is many systems operating under a broader ecosystem. In the previous topic, you explored the diversity of IoT devices. The IoT ecosystem can be just as diverse; however, there are common elements within the ecosystem, regardless of options.

## IoT Infrastructure



**Figure 1–3: General components of IoT architecture.**

Just as IoT devices are quite diverse, the infrastructure in which they operate may vary significantly from one system to another. However, common elements of IoT infrastructure include:

- **IoT devices**, including hardware and software that directly interacts with the world and measures local data (called *telemetry*, meaning "measurements from far away").



**Note:** Borrowing terminology from industrial automation, people sometimes refer to IoT devices as *field devices*.

- **A network connection** using wireless or wired communication.
- **An IoT gateway** that serves as an intermediary between local networks of IoT devices and the cloud, enabling local IoT devices to communicate with each other, and to an external network. The IoT gateway might be a discrete piece of hardware, or its functionality might be built-in to one of the IoT devices in the local network, such as a thermostat in a home network, or an industrial machine in a factory.
- **The edge**, defined by various points where traffic leaves (or enters) the local network; for example, a router providing access to an Internet carrier. A router that conveys network traffic between the local area network and the wider network beyond the control of the local organization is described as an *edge* device.
- **Global network**, which provides the long-haul connection to the cloud.

- **Cloud services** that collect data from devices, combine it with data from other devices and data sources, and analyze resulting data sets, which can become quite large when combined from hundreds or thousands of IoT devices. Massive data processing capabilities, known as *big data*, may be necessary, requiring the use of *artificial intelligence (AI)* and *machine learning (ML)* strategies and technologies.
- **User interface** that provides a user with the ability to view and analyze IoT data, issue commands and control IoT devices, and perform related tasks. The user interface may be provided through a mobile app, web application, or desktop application.

## IoT Gateway

An IoT gateway might perform tasks such as the following:

- **Support local communication and messaging** on a local network that is optimized or well-suited for IoT devices with limited data processing and communication capabilities.
- **Aggregate and store data from IoT devices temporarily** to take advantage of off-hour data rates or to deal with intermittent connections.
- **Forward data acquired from IoT devices to cloud services**, providing the increased security, routing capabilities, and electrical power requirements that communication across the Internet requires.
- **Perform local data analysis** where a fast turnaround is required, and sending data to the cloud for analysis would take too long.
- **Prepare data for cloud services** by filtering, compressing, or performing other processing tasks on it.
- **Translate between IPV6 and IPV4.**
- **Serve as a local cache for software updates** sent to IoT devices.
- **Receive device commands from the cloud** and send to IoT devices.

A wide variety of devices may be used as an IoT gateway, and they vary by industry. For example, many consumer-oriented IoT products (smart thermostats, smart speakers, and so forth) include built-in IoT gateways, although they're marketed by other names, such as *smart home hubs*.

For business implementations, IoT gateways may be constructed by installing the necessary software on an industrial or rack-mounted computer, or by using products specifically marketed as IoT gateways. Such systems are commonly sold by companies that traditionally have sold business computers and networking devices.

## Cloud Services

Cloud services provide a central point where massive amounts of data from IoT devices and other sources can be stored and analyzed, and where other systems and solutions can be integrated, such as enterprise applications, cloud services on other platforms, and so forth.

Cloud services may operate on cloud platforms such as Amazon Web Services, Microsoft Azure, Google Cloud Platform™, OpenShift, or Cloud Foundry. They may also be hosted within an enterprise's own data center using commercial, open source, and custom-developed software.

Cloud services can be scaled as needed to meet increased demand (e.g., more IoT devices are connected or more users need to access the system), and to support an increasing variety of different services.

## User Interface

*IoT client applications* provide users with access to view IoT data and issue commands.

For consumer IoT, client applications often include smartphone, tablet, or desktop computer apps that enable users to control remote devices, or to view data they have accumulated, such as exercise statistics from a smartwatch or fitness band.

In business applications, *business intelligence (BI)* applications may include *data dashboards* and similar visualization tools that enable users to view collected business data in graphic form and possibly issue commands to manage business processes.

Various other user interfaces may be provided as well. For example, administrative applications enable administrators to set up and configure the various IoT devices, IoT gateways, and other systems supporting the IoT infrastructure.

Software Stacks

Some software capabilities are typically required by all hardware involved in IoT. Clearly, cybersecurity is a requirement for any piece of hardware involved in collecting, processing, and presenting sensitive data. Furthermore, since much of the software involved in IoT is not running directly on the user's computer, remote management capabilities are required to set up, configure, and maintain IoT devices, gateways, and cloud applications. However, the requirements for the different types of hardware used in IoT are generally very different based on the role played.

This figure and the following table describe the typical layers of software (*stacks*) used by IoT devices, IoT gateways, and cloud services that support IoT.

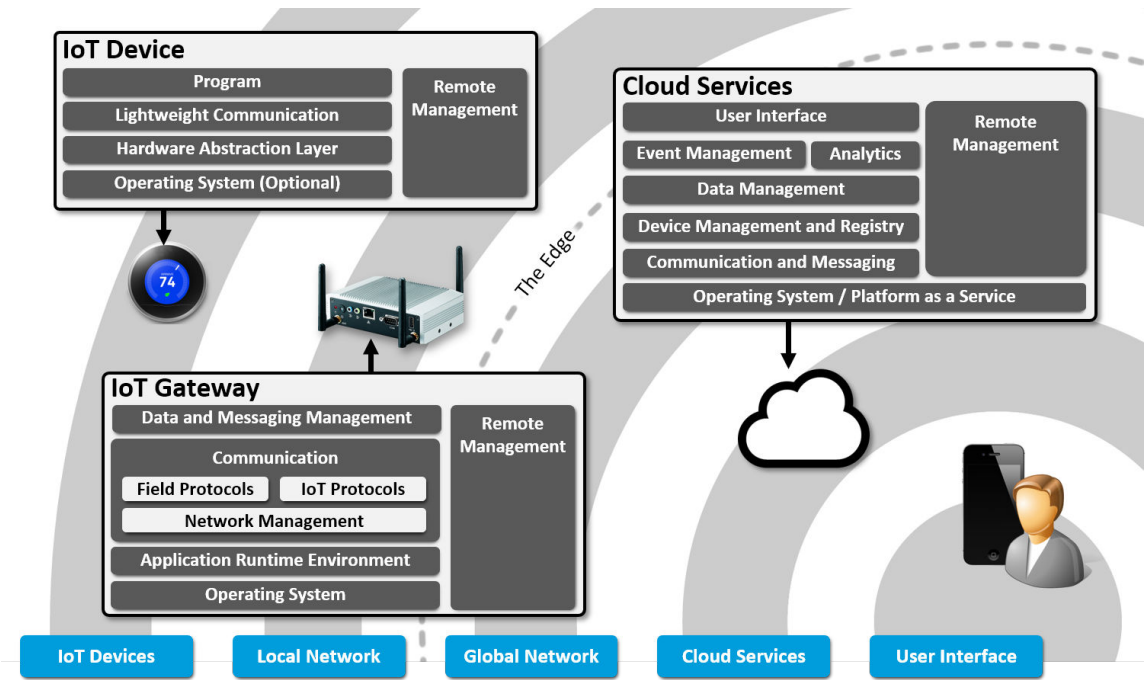


Figure 1–4: Types of software required based on role within the infrastructure.

IoT Hardware	Software Layers
IoT Devices	<p data-bbox="386 197 1221 327">IoT devices are often <i>constrained devices</i>, meaning they are purposely designed to function with little processing power, memory, energy requirements, physical size, and so forth. So the software on these devices must be very lean and oriented to the required tasks.</p> <p data-bbox="386 338 1221 434"><b>Operating System:</b> A very lightweight operating system is used, which may be customized to support only essential tasks. If possible, no operating system may be used at all.</p> <p data-bbox="386 445 1221 575"><b>Hardware Abstraction Layer (HAL):</b> Programmers may be provided with a programming interface that can perform operations on the device hardware using relatively simple code, without having to directly program the hardware.</p> <p data-bbox="386 585 1221 779"><b>Communication:</b> Capabilities include protocols the device needs to communicate with other devices and the IoT gateway. To conserve power, unused radios are typically disabled, and lightweight communication protocols optimized for constrained devices may be used to minimize the processing, memory, and power required. Encryption capabilities may be limited in these devices.</p> <p data-bbox="386 789 1221 852"><b>Program:</b> Typically a single program that starts running when the device is powered on provides the functionality of the device.</p>
IoT Gateways	<p data-bbox="386 873 1221 970"><b>Operating System:</b> IoT gateways generally have much more processing power than IoT devices, so they can run conventional operating systems, such as Linux or Windows.</p> <p data-bbox="386 980 1221 1144"><b>Application Runtime Environment:</b> IoT gateways may perform many different tasks to collect data and perform initial processing before forwarding data on to cloud services. Typically, this is accomplished using programs written for Node.js, Python, Java, or a similar application runtime environment, which must be installed on the IoT gateway.</p> <p data-bbox="386 1155 1221 1377"><b>Communication:</b> The role of a gateway in general is to serve as the go-between across two different types of networks. In the case of IoT gateways, these are the local network of IoT devices and the global network (the Internet), typically running TCP/IP. So IoT gateways must be able to support two types of communication, using lightweight protocols with local IoT devices and normal protocols (such as TCP/IP with TLS transport layer security) with the network at large.</p> <p data-bbox="386 1388 1221 1478"><b>Data and Messaging Management:</b> Because IoT gateways serve as a communication hub, they must provide the ability to manage communications between IoT devices and external network connections.</p>

IoT Hardware	Software Layers
Cloud Services	<p>The cloud services that support IoT typically perform heavy processing and analytics on data from IoT devices, and provide a central point for interfacing IoT with end users and enterprise applications.</p> <p><b>Operating System/Platform as a Service:</b> Cloud services typically run on virtual machines that can be scaled up or down as needed to meet demand, so operating systems that can function in this way, such as customized versions of Linux and Windows, are used.</p> <p><b>Communication and Messaging:</b> Cloud services must manage two-way communication and messaging with all devices, gateways, and clients they interact with, and must ensure that communications and transactions occur in proper sequence, even when dealing with huge numbers of devices scattered throughout the world.</p> <p><b>Device Management and Registry:</b> IoT cloud services must be able to identify devices and gateways they communicate with, and provide a means to manage those devices and securely provide them with software updates.</p> <p><b>Data Management:</b> The volume of aggregated data may become massive in scale. IoT cloud services must provide a way to manage this data, and handle it in ways that are economical, efficient, and secure.</p> <p><b>Event Management:</b> Event management software enables the system to detect when certain conditions exist, log them, and perhaps trigger a response. This supports a variety of other capabilities, such as security monitoring, data management, and so forth.</p> <p><b>Analytics:</b> Analytics software enables IoT data to be processed in light of business rules to provide insights that might not be readily apparent from just visually scanning the data. Analytics programs use advanced data processing techniques and artificial intelligence to reveal significant patterns of data.</p> <p><b>User Interface:</b> IoT cloud services can present information in highly visual and structured ways, such as charts, reports, and dashboards that can be viewed from a web browser or client application.</p>



# ACTIVITY 1–2

## Selecting an IoT Infrastructure

### Data File

C:\CNX0004Data\Planning an IoT Implementation\Selecting an IoT Infrastructure.docx

### Scenario

Now that we have some exposure to the complexity within the IoT Infrastructure, let's have a little fun again with our Greene Organix project. Automation will require that we both monitor (sense) important physical elements within the greenhouse, analyze the data we are collecting, and respond with control actions (actuate) to maintain optimal operating conditions within the greenhouses. Let's look at what a typical system would require from an IoT Infrastructure and also consider some of the real-world constraints that may limit our options.

The system will:

- Collect data
- Analyze the data
- Control the greenhouse environment to ensure all plants have optimal growing conditions
- Report data as needed

Identify the basic IoT infrastructure you will need to include in your IoT solution for:

- Data Collection and Control
- Local Connectivity
- Remote Connectivity
- Remote Data Ingestion, Analytics, Backend Applications
- Operational Constraints

In the spaces provided, write your ideas regarding requirements for the IoT infrastructure you would use in this scenario. (If you'd prefer to type your ideas in a Word document, a worksheet is provided in C:\CNX0004Data\Planning an IoT Implementation\Selecting an IoT Infrastructure.docx.)

---

### 1. A) What would be a typical IoT Infrastructure setup for our greenhouses?

2. B) What are some constraints we may be dealing with within our greenhouse operation?

---

# TOPIC C

## Business Benefits and Challenges

Industry has long benefited from process automation. With the advent of IoT, other business processes are now being automated on a greater scale than ever before. However, while IoT brings new capabilities that can benefit business and society as a whole, it also brings new challenges.

### Business Benefits

Applied effectively, IoT can enable organizations and businesses in many different sectors to transform how they operate, improving performance by providing abundant, accurate data that can help them make more informed decisions, reduce the need for "feet on the ground," and provide higher levels of situational awareness than they could manage previously.

IoT technologies have the potential to help businesses:

- Improve competitive position by providing information that leads to improvements to products, processes, and services.
- Anticipate and avoid expensive, time-consuming, and hazardous problems before they occur, reducing operational costs and the harmful impact of operations on the natural environment, while increasing safety and improving customer experience.
- Identify possibilities for new and enhanced revenue streams and markets by revealing previously unidentified problems that can be solved and areas in which products and services can be improved.
- Reduce operational costs and natural resources usage by identifying sources of waste and inefficiency.
- Reduce transportation and lodging expenses, and potentially reduce the impact on the environment by enabling some tasks to be performed from remote locations that previously had to be performed on site.
- Reduce waste and defects and increase productivity, agility, and product quality by improving product testing and manufacturing telemetry.
- Provide better tracking of logistics and transportation.

### Business Considerations

Organizations fall into the trap of building IoT solutions that capture lots of new data but put little thought into how this new data will add business value. Focus first on what value your company or your organization provides and how to improve that value. If you focus on the data first, the result may end up being that your incremental costs exceed your incremental value created.

There are three items to consider when trying to determine when your organization is evaluating an IoT implementation.

- *What incremental value are you trying to capture?*
- *What new information (insights) will you need to be able to deliver on this new value?*
- *What data will you need to capture to help facilitate and support this new information?*

### Business Challenges

Although many businesses may benefit from IoT, it also presents numerous challenges. For example, many organizations have invested heavily in existing infrastructure. Implementing IoT systems and adapting business processes to use them can be disruptive. Provisioning and tracking of additional devices, potentially numbering in the thousands for a single organization, will be

challenging for some organizations. Significant cost may be associated with just the hardware and software, not to mention setup, configuration, and interfacing the new components with legacy systems. Data networks will have to be reconfigured to add new network nodes for IoT devices, gateways, analytics tools, and support for IoT protocols. There may be some disruption to current systems as all these changes are implemented.

Security, privacy, and safety concerns may be associated with the new types of data being collected and the systems used to secure the data. The organization may be exposed to new standards and regulations associated with the data they are capturing. For some situations, the cost and disadvantages of IoT automation may outweigh benefits, and it may be more beneficial to utilize people or traditional technology.

Traditionally, *information technology (IT)* and *operational technology (OT)* have been managed by separate groups within organizations. IT typically managed the company's information systems, geared toward collecting, storing, and sending data, whereas OT focuses on measuring and controlling production and operations. With IoT, the distinctions between these two groups is blurring, with IT becoming more involved in measurement and control, and OT providing expertise in that area, while looking to take greater advantage of the information systems supported by IT.

Of course, IoT will drive change, and there may be some resistance within the organization. Some jobs will change, as more information can be collected automatically, and new skillsets will be required. To ensure a good transition, it is helpful to get buy-in and participation from all levels of the organization—particularly from those groups given the task of implementing and supporting the new technology.

## Technical Challenges

A variety of factors make it challenging to design, develop, implement, and maintain an IoT system.

<i>Factor</i>	<i>Description</i>
Device constraints	The constraints on IoT devices can make it challenging to provide robust features and capabilities. Those who design IoT devices and systems must manage the tradeoff between low power consumption and features the device needs to support, such as data processing, communication with other devices, and consistent, reliable data sensing.
Data communication	<p>IoT devices often use wireless (rather than cabled) connections to support remote or mobile use, and may have an unreliable, low-bandwidth, or intermittent connection, and their limited memory and storage may make it challenging to move large amounts of data quickly.</p> <p>The lack of standards and emergence of new standards makes it difficult to select technologies that will last over time. Organizations are working toward open standards, but the process takes time. Vendors are quite competitive in this new technology domain and trying to establish technology advantages over their competitors. While single-vendor, proprietary solutions are often quite good, they lead to interoperability issues, data silos, and security problems when products from different vendors are introduced into the mix.</p>

Factor	Description
Interoperability	<p>Integrating products from different vendors into a unified solution for the customer can be challenging.</p> <p>Industrial systems have traditionally been highly customized and based heavily on legacy systems that use proprietary communication and messaging protocols. It is difficult to connect industrial systems between organizations using products from a different vendor, and to interface systems with new technologies that were not part of the original system.</p> <p>In the consumer space, IoT products have forced customers into assembling systems like home automation using only products from a particular product line, or else risk having systems that are awkward to use or unable to support all of the product's features.</p> <p>Even when interoperability standards are supported, the solution is often clumsy, involving various proprietary apps and complicated processes to link the devices. For example, to set up a smart outlet from one vendor to respond to voice controls through a smart speaker by another vendor, the user may have to download a smartphone app for the smart outlet, an app for the smart speaker, and numerous steps within both applications to link the devices. If the user buys another smart outlet from a different vendor, yet another app may be required, as well as a different complicated linking operation.</p>
Real-time operations	<p>Determining where to perform processing within the IoT infrastructure is a primary concern for the IoT designer. Some IoT devices must be able to measure and detect certain events within a fraction of a second, and take local action immediately. This type of processing is called a real-time operation.</p>
Security and Privacy	<p>The Internet of Things brings new security challenges. IoT devices are often located in remote or public locations, where it may be more challenging to provide <i>physical</i> protection from attackers. They may be located on the edges of network infrastructure and exposed to Internet traffic, where it may be more challenging to provide <i>logical</i> protections through firewalls and other forms of network security.</p> <p>It may be easy to use radio devices to jam communication on low power wireless devices.</p> <p>Encryption is a common approach to protecting data when it is in transit across data networks or at rest in storage. But in many cases, encryption requires more capability than constrained devices can spare. So devices may have minimal or no encryption to protect the data they send and receive.</p> <p>IoT has introduced concerns about privacy and data provenance. It may be unclear who owns data collected by IoT processes. Consumers may be skeptical about IoT products and concerned they won't be able to control who can use their data.</p>
Usability	<p>Because of the limited storage and data communication capabilities on an IoT device, it may be challenging to provide security and functionality updates.</p> <p>In some cases, high security may be at odds with usability. Tasks such as pairing, configuration, and authentication may require multiple forms of authentication and multiple devices to complete, causing some frustration for users.</p>

Factor	Description
Updates	It may be challenging to provide security and functionality updates to IoT devices. They may have an unreliable, low-bandwidth, or intermittent connection, and their limited memory and storage may make it difficult for them to manage updates.

Designing systems around constrained devices can be challenging, and when security requirements are added to the mix, the challenge is even greater.

Security Challenges

There is a famous Twitter joke about IoT that is attributed to a guy named Tim Kadlec (@tkadlec): “The S in IoT stands for security.” Think about that for a second, as you say, “Wait, there is no S in IoT.” That is exactly the point of Tim’s statement. IoT manufacturers have been slow to build more needed security in their respective products

Beecham Research's IoT Security Threat Map displays the full set of threat and vulnerability analyses that Beecham uses to help its clients shape their strategies.

This downloadable summary includes many of the top 5 features from each of those analyses.

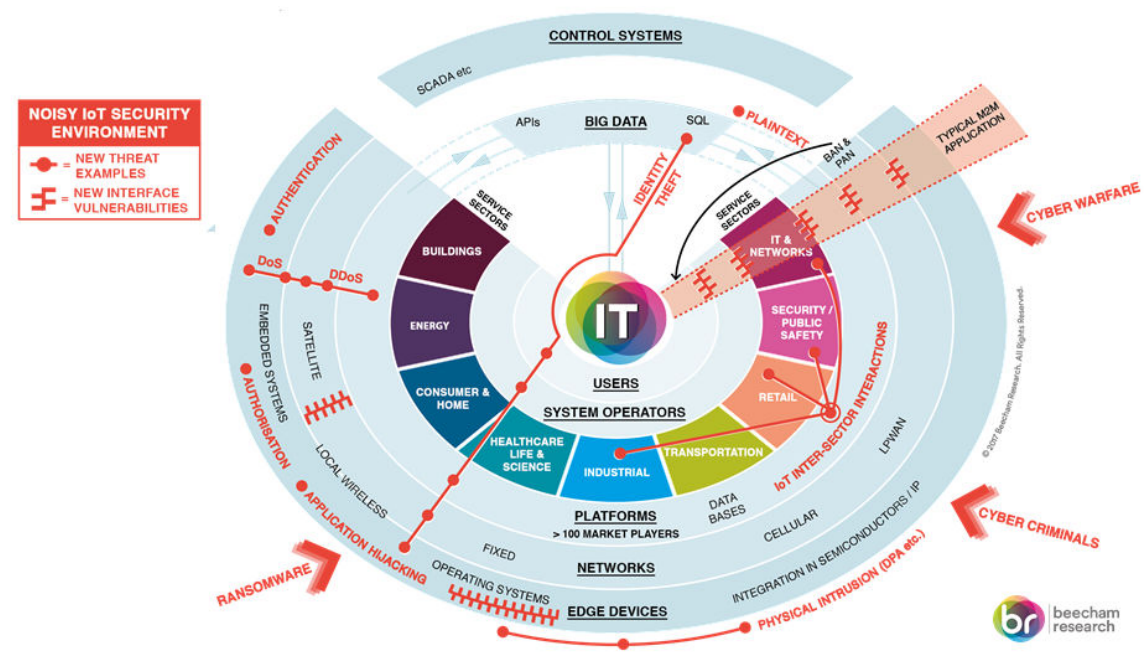


Figure 1–5: IoT Security Threat Map.

Traditional M2M (Machine to Machine) applications are typically very focused, using specific edge devices, a single network and custom platform, making it relatively easy for security professionals to secure to the acceptable level. IoT cuts across different sectors and embraces multiple devices and networks—from satellite to cellular—along with a growing number of IoT platforms and Big Data systems, which present threats on many different levels and fronts. Wherever there is a new interface between devices, networks, platforms, and users, there is the potential for a new weak link.

IoT Contributes to the Threat Landscape

According to the IDC, in 2016 there were 11 billion devices connected to the Internet, with an expansion to 30 billion expected by 2020. IoT contributes to the threat landscape primarily because of all the new devices that are added daily. IoT is the primary possible culprit in an additional 20 billion devices.

## The Dyn Attack

The 2016 Dyn cyberattack was a series of three distributed denial-of-service (DDoS) attacks that were launched on October 21, 2016. The attack targeted systems operated by former Domain Name System (DNS) provider Dyn. The attack left millions of users in Europe and North America without access to major Internet platforms and services. Although the groups Anonymous and New World Hackers, among others, claimed responsibility for the attack, no definitive evidence was provided.

As a DNS provider, Dyn provided end-users with the service of mapping an Internet domain name to its corresponding IP address. The DDoS attack was caused by bogus DNS lookup requests from tens of millions of IP addresses. It is believed that the requests were executed through a botnet consisting of millions of IoT devices that had been infected with the Mirai malware.

## Why IoT is Lacking Fundamental Security

Three reasons why IoT is lacking fundamental security are: lack of industry knowledge, rapid time to market, and lack of developer knowledge.

- **Lack of industry knowledge.** Products are being added with IP interfaces that existed previously in a network-less world. Companies such as Cisco, Microsoft, and HPE have decades of security experience. Most of the IoT startups do not. This lack of security knowledge results in products that repeat the same problems of the previous two decades. IoT startups need to learn from industry's past mistakes.
- **Rapid Time to Market.** The age-old argument between time to market vs. securing the customer's environment. Startups are focused on deploying products and features with a velocity that catches the eye of investors and new customers.
- **Lack of Developer Knowledge.** IoT is lacking fundamental security in that the developers do not understand security. A perfect example of this is the Mirai botnet, and specifically the XM cameras that made up a large portion of that botnet.

The solution to this problem is to build security into everything that is created on the IoT, by using a Secure Development Lifecycle (SDL). Also, many embedded security chipmakers and cryptography specialists are taking the matter of embedded security for IoT into their own hands and building security at the hardware chip level.

## Societal Impact

As with technologies that have preceded it, IoT has immense potential to disrupt and change the way things are done. Our history shows that some changes brought about through technology may benefit society, while others may cause harm. And different people may be affected differently. There may also be unintended side effects—new problems may be created while solving old problems. Technologists should consider the potential impact of IoT solutions they design and implement on their organization, people, and the environment.

For example, as machines gain new abilities to sense the world around them, process the data they take in, and take action based on that data, it will be possible for jobs previously performed by people to be performed by machines. There are clear societal benefits to having machines perform tasks that are dangerous, risky, or mundane. And, in some cases, machines may perform those tasks more efficiently and effectively than people. However, eliminating someone's job is disruptive—not only to that individual, but it may also have a significant negative impact on an entire family that can affect them for years.

IoT technologies may reduce manufacturing waste and the use of natural resources, and may significantly help to reduce pollution of the environment. But there are significant environmental costs for using those technologies, such as the mining operations needed to obtain raw materials for lithium batteries and other components; the energy, natural resources, and toxic chemicals used in their manufacture; and challenges associated with properly recycling or disposing of IoT hardware once it becomes damaged, obsolete, or worn out. These factors should all be included in evaluations of the benefits of IoT.

## Organizational Skills Impact

IT staff may need to develop new skills or combine efforts with OT groups to leverage the skills and experience of both groups. New skillsets for IT might include:

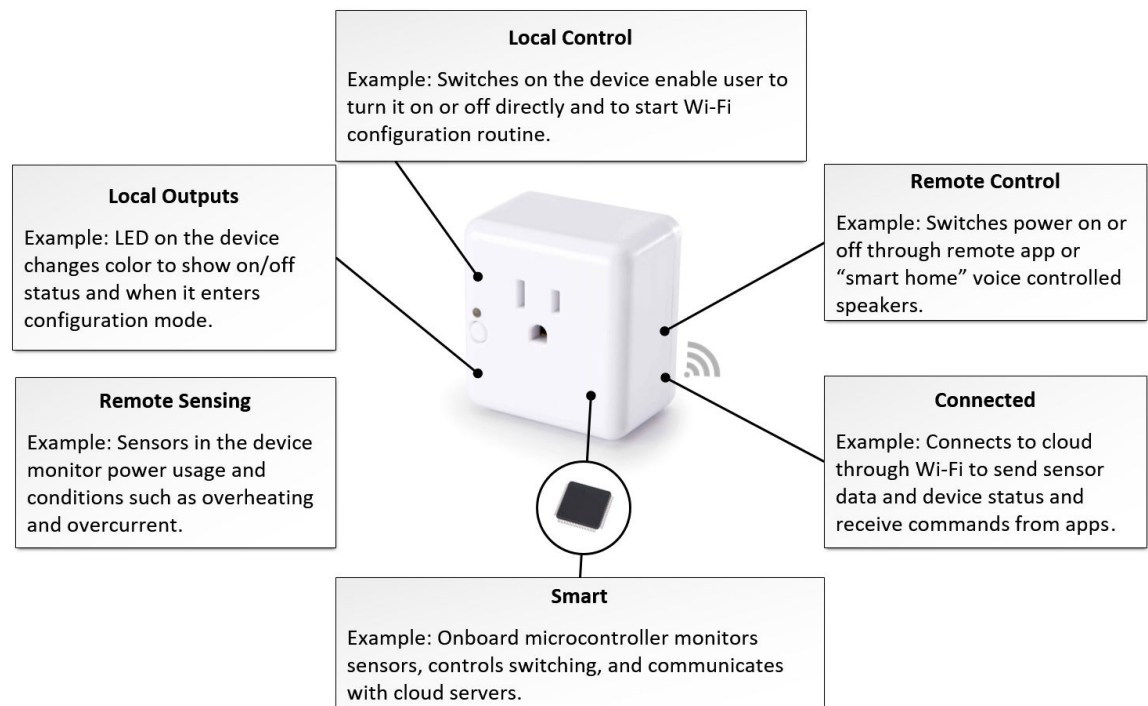
- Embedded devices
- Sensors and actuators
- Real-time data processing and networking
- Edge computing
- New methods of data processing and analysis

The key is to effectively merge industry domain knowledge with the new technical knowledge required (OT and IT) to accomplish the new goals.





## Case Study: Smart Outlet



**Figure 1–6: Common features of IoT devices, as exemplified in a smart outlet.**

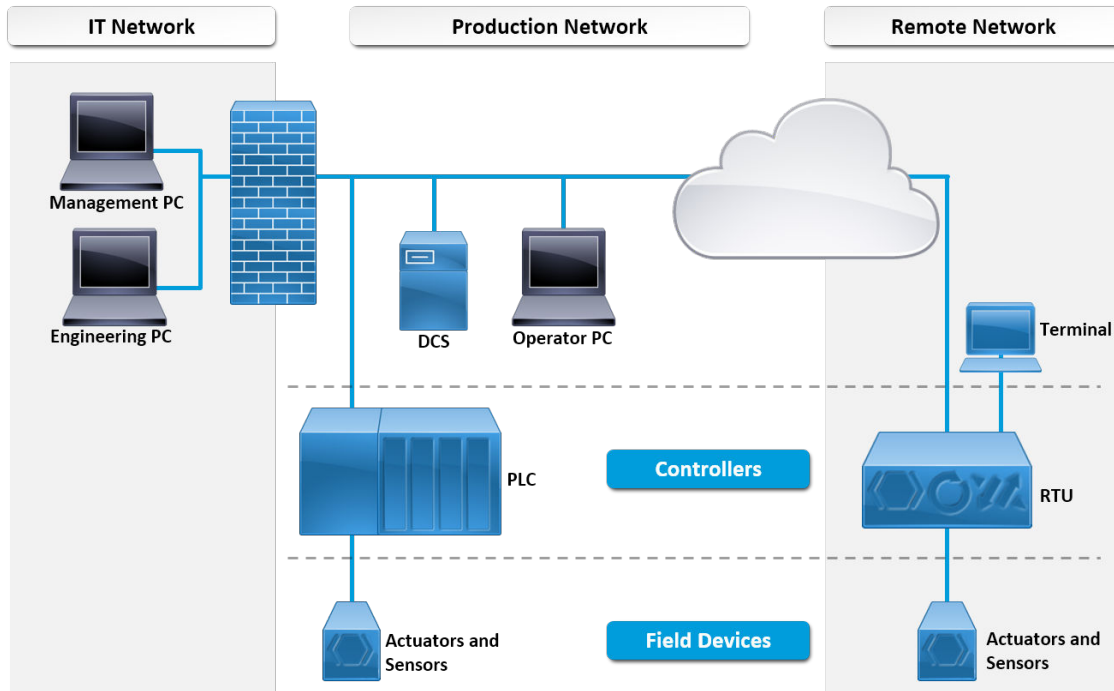
A smart outlet has attributes you might find in a typical consumer-oriented IoT device. Following setup and configuration, a user can plug in a normal electrical appliance such as a light or fan, and can switch the appliance on or off through a smartphone app or by issuing a voice command through a smart speaker such as Amazon Echo or Google Home. The outlet might also perform other tasks, such as monitoring and logging electrical flow (when the switch was on, how much current it drew, and safety monitoring for overheating and overcurrent). The device uses Wi-Fi to connect with the applications that collect its usage data and enable the user (through other devices) to switch it on and off.

IoT devices like this can be purchased for less than \$25 US, but even a relatively inexpensive and limited device like this would have attributes such as:

- **Local controls and user interface:** Controls may be provided directly on the device to enable the operator to set it up, turn it on and off, and perform other tasks.
- **Remote controls and user interface:** A remote user interface may be provided through a smartphone app, desktop application, or through verbal commands issued to a smart speaker. A relay in the device enables it to switch power on or off under remote control. (Other types of IoT devices must include motors, servos, valves, and other types of actuators to local action to take place using remote control.) Some local controls, such as buttons or switches, may be provided locally for setup and configuration of the device, or as an alternative to remote controls, but local controls are often quite limited.
- **Remote sensing:** A heat sensor and electrical current sensor in the device measure local information that can be locally processed (for example, automatically switching the device off and sending a notification to the remote user if an overcurrent or overheating condition occurs). Data produced locally can be sent to a remote system for logging and analysis.
- **Connected:** Wi-Fi, Bluetooth®, Bluetooth Low Energy®, Zigbee®, or other data communication capabilities enable the device to communicate locally with other devices or with cloud-based applications over the Internet.
- **Smart:** Processing capabilities embedded in the device enable it to process local inputs and outputs (switch, LED), remote inputs and outputs (commands from a remote user, sending data

logs to a server or gateway in the cloud). Some (typically small) amount of data storage might be present on the device, where it can be stored until it can be uploaded to a remote system for logging and analysis.

## Industrial Controllers



**Figure 1-7: Industrial controllers and related devices.**

Various systems and devices are used for industrial control, as described in the following table.

Item	Description
PLC	<p>Industrial control traditionally has been based on programmable logic controllers (PLCs). A PLC is comparable in some ways to a desktop computer or rackmount server in that it is a box containing a CPU and supporting components (e.g., motherboard, memory, storage). However, PLCs are optimized for use in industrial control applications. PLCs may be configured for rack mounting in a control room or in other form factors for standalone installation out on the factory floor or industrial complex. They are designed for durability in demanding environments, including resistance to electrical noise, vibration, smoke, humidity, and impact.</p> <p>The software on PLCs has been optimized to model traditional hardwired electronic controls, such as relays, which control motors, valves, lights, and so forth, using relatively simple programming schemes, such as ladder diagrams.</p>

Item	Description
RTU	<b>Remote terminal (or telemetry) units (RTUs)</b> monitor and control a remote asset (such as an oil well or water pump). Because they are often located in remote locations, these devices often need capabilities such as network communication (communicating with a centralized control system through radio, cellular telephony, and so forth), low power consumption, data logging and short term storage, ability to operate in adverse conditions (such as weather extremes), and so forth.
PC	<p>Personal computers (PCs) provide a user interface for viewing data and controlling industrial systems.</p> <p>Initially, PCs had required special adapter cards to communicate with industrial control systems, but as industrial control systems have incorporated PC networking standards, a common network connection (such as cabled Ethernet or Wi-Fi) is sufficient to make the connection, and other end-user devices, such as smartphones and tablets, can often be used to access control applications.</p>
DCS	PLCs were initially developed to control single manufacturing processes and continue to be used as a basic building block for automating a single line or process. But <b>distributed control systems (DCS)</b> have been developed to control manufacturing on a larger scale, integrating production across multiple processes and locations. Often, a DCS will incorporate multiple PLCs and PCs.
PAC	<p>Both PLCs and DCSes have evolved substantially over time, so, in many cases, it has become difficult to pinpoint precisely where one category begins and ends.</p> <p><b>Programmable automation controllers (PACs)</b> combine functions found on DCSes, RTUs, and PCs. This makes them suitable for operations requiring coordination among multiple processes (like a DCS), while providing fine control over specific processes (features traditionally performed by a PLC and RTUs).</p>
IPC	Another component that blurs the distinctions among industrial control systems is the industrial PC (IPC). In the 1990s, software for personal computers was developed to emulate functions of a PLC. Some manufacturers have developed IPCs, essentially "ruggedized" PCs adapted for industrial I/O tasks, to build upon this capability. IPCs can cost-effectively perform many of the tasks as a PLC and PC combined, making them well-suited for small automation projects and applications where space is limited.

While traditional programming tools continue to provide backward support, more advanced programming tools are now available, including instruction sets specifically geared toward specific industries, such as brewing, oil, gas, and nuclear power plants.

## Summary

In this lesson, you identified components of a successful IoT project, including a general architecture that enables those components to work together. You also identified benefits of IoT and challenges you might encounter in implementing an IoT system.

IoT has the ability to transform both old and new businesses. How well you both understand and apply IoT and your industry domain knowledge before you dive in, will determine to a large extent how successful your path will be.



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.



# 2

## Undertaking an IoT Project

**Lesson Time: 2 hours, 5 minutes**

### Lesson Introduction

Your organization is sold on the benefits of Internet of Things (IoT), has a healthy respect for the risks, and is prepared to undertake its first IoT project. To pull the project off successfully will require careful planning.

### Lesson Objectives

In this lesson, you will:

- Identify problems in your organization, and determine how you can use IoT technologies to help resolve them.
- Identify issues you'll need to consider throughout the IoT development lifecycle.

# TOPIC A

## Real-World Applications for IoT

Implementing IoT within your organization may have numerous costs in terms of hardware, software, setup, configuration, integrating it into other systems, maintenance, and acquiring the skills needed to work with it. Before you undertake a project, you should identify where it has the greatest potential to benefit your organization.

### IoT Market Sectors

According to IoT Analytics (<https://iot-analytics.com>), in 2018, the global share of IoT projects was distributed among various market sectors as follows:

- Smart City - 23%
- Connected Industry - 17%
- Connected Buildings - 12%
- Connected Cars - 11%
- Smart Energy - 10%
- Connected Health - 6%
- Smart Supply Chain - 5%
- Smart Agriculture - 4%
- Smart Retail - 4%

Other sectors accounted for an additional 8 percent of the global share of IoT projects.

### Smart City

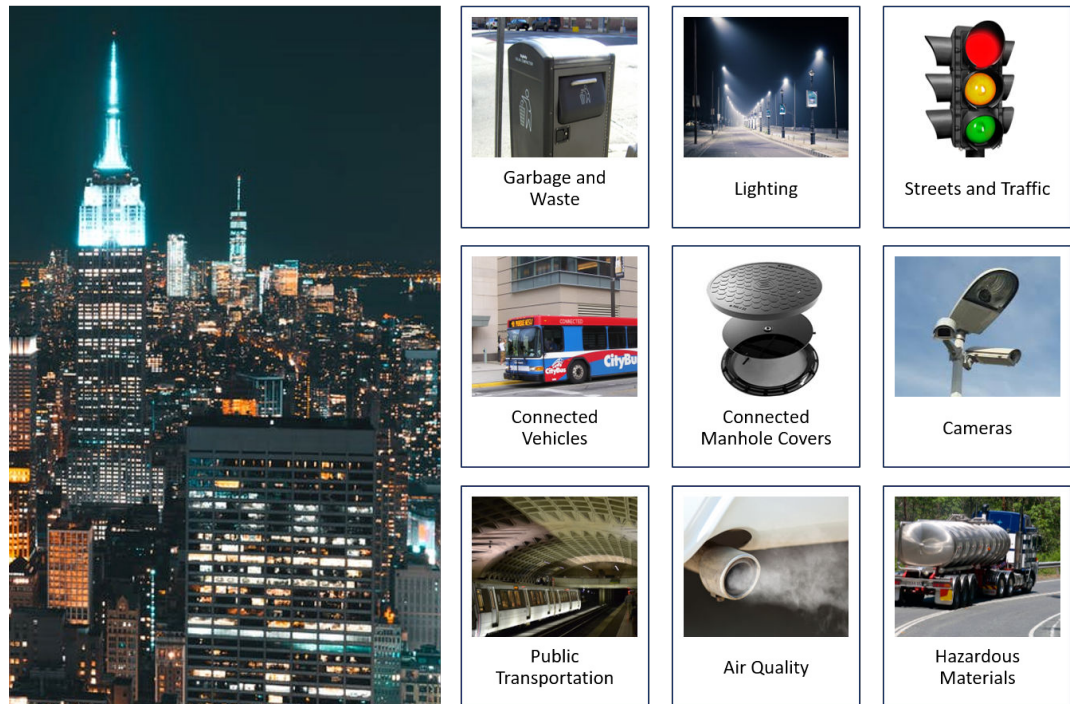


Figure 2-1: IoT automation in a smart city.



With increasingly large concentrated populations, there is significant pressure on the limited resources and space within cities and other municipalities. IoT-based innovations can help them make better use of resources and provide a high quality of life to their occupants. A **smart city** uses sensors distributed throughout the environment and connected to a network in conjunction with applications that support data collection, analysis, and remote control to solve problems in real time or near real time, coordinate complex urban systems, provide efficiency, reduce costs and adverse environmental impact, and improve public services and safety.

The following are examples of ways that IoT technology may be applied in smart cities.

## Garbage and Waste

Waste bins can be monitored so pickup routes can be optimized based on demand, saving operational costs, improving timeliness of collection, and reducing unnecessary traffic. Similar concepts can be applied to sewage systems, adjusting the flow of water pumps based on need and reducing water usage when demand for water increases elsewhere within the municipality.

## Streets and Traffic

Sensors can measure traffic patterns of pedestrians, cyclists, automobiles, and public transportation through pressure sensors in walkways, turnstiles, and so forth, which can be used to improve long-term planning of city layouts. Smart parking meters can monitor parking, enabling apps and smart signs to direct drivers to open parking spaces through smartphone apps, GPS units, and smart cars. Inputs from traffic sensors throughout a city can be analyzed in real time and coordinated with messaging sent to street signals, signs, and directly to citizens' IoT devices (smart phones, smart cars) to efficiently coordinate traffic flow out of the city during emergencies or other high-traffic situations.

## Lighting

Based on reduced need as measured by sensors measuring automobile and foot traffic, ambient light, and other inputs (such as scheduled sports events, festivals, etc.), street lamps can reduce or increase their light levels appropriately.

## Public Transportation

Digital signs in train stations, bus stops, and smartphone apps can provide real-time updates on estimated arrival times and suggest alternate routes when appropriate, to keep riders informed, improve the public transportation experience, and encourage wider use of public transportation. Based on real-time data such as air quality (smog levels from automobiles), available parking spaces, and so forth, temporary discounts on public transportation prices can be offered to provide citizens with incentive to avoid driving. Real-time data regarding traffic flow, road closings, working accidents, number of people waiting at bus stops, number of seats already filled, and so forth can be used to dynamically optimize routes and the number of vehicles in service, to make the best use of resources while meeting demand.

## Safety and Security

Sensors strategically located throughout the city can detect specific types of risks, such as the presence of chemical, biological, explosive, or radioactive devices, and authorities can be alerted. Sensors can monitor for impending natural disasters such as earthquakes, tsunamis, and landslides. Early warnings to citizens, road closures, evacuations, and other measures can be taken. Personal IoT devices such as smartphones and wearables can be used to send timely alerts to users as a supplement to traditional warning and messaging systems. In situations that unfold quickly, such as floods, landslides, and active shooting situations, the ability to quickly inform the public can save lives. Security and safety services, such as police presence and active visual monitoring, can be better coordinated based on sensor data that identifies such things as traffic patterns. While targeted tracking of individuals raises privacy issues, general tracking of numbers of people, noise levels, and so forth is less controversial. Analysis of ambient noises within a city can identify gunshots, car crashes, and other noise signatures that can alert authorities to an active situation in real time.

## Environment

Air quality in cities varies widely based on weather conditions, traffic, industrial processes, the operation of heating and power plants, and other factors. Various microclimates based on terrain, buildings, and other factors result in uneven air quality throughout the city on a given day. Sensor data from municipal systems and citizen-owned devices can be collected and analyzed to enable appropriate countermeasures to be taken as needed, such as coordinating the use of alternate energy sources, rerouting traffic, and so forth.

## Infrastructure

The structural integrity of bridges, roads, tunnels, dams, levees, and other infrastructure can be monitored through sensors that measure stress, vibration, erosion, position, and so forth to support predictive maintenance, reduce inspection costs, and prevent dangerous and costly failures. Connected manhole covers can detect and report abnormal, costly, and dangerous events like theft, vandalism, and dislocation due to storm surges, enabling timely replacement. Sensors within manhole covers can also be used to detect sewer levels and flow, chemical and biological conditions, temperature, and other factors that can be analyzed in real time to identify sewer management problems.

## Case Studies

Case studies describing various smart city IoT projects may be found at the following URLs.

- Berkeley County Case Study for smart meters  
[https://smartcitiescouncil.com/system/tdf/main/public\\_resources/Berkeley%20County%20Case%20Study\\_Final\\_0.pdf?file=1&type=node&id=4087](https://smartcitiescouncil.com/system/tdf/main/public_resources/Berkeley%20County%20Case%20Study_Final_0.pdf?file=1&type=node&id=4087)
- Seoul Waste Management Case Study  
[https://smartcitiescouncil.com/system/tdf/main/public\\_resources/Ecube%20city%20of%20seoul.pdf?file=1&type=node&id=2845](https://smartcitiescouncil.com/system/tdf/main/public_resources/Ecube%20city%20of%20seoul.pdf?file=1&type=node&id=2845)

## Industry



*Figure 2-2: IoT automation in industry.*

Traditional industrial automation has been accomplished through industrial control systems, such as Programmable Logic Controllers (PLCs), Process Automation Controllers (PACs), motor drives, robots, and so forth. The following are examples of additional ways in which IoT technology may be applied in industry.

## Transportation and Distribution

Logistics, the detailed coordination of people, facilities, and supplies involved in manufacturing, production, and fulfillment, is often the primary difference between businesses that succeed and those that fail. Tracking of goods from their source to their destination has usually required someone scanning a barcode at each junction. However, using devices like radio-frequency identification (RFID) tags, this process can be automated. Goods in transit can connect to the cloud and share data on their status and location, eliminating most human intervention. The status of the entire supply chain can be evaluated and communicated at any time. This includes raw materials, components, production machinery, finished products, material handling equipment, packaging, transportation vehicles, other means of transport, delivery, and distribution.

## Wearables

Wearable IoT devices such as watches, vests, jackets, and shoes can monitor workers operating in dangerous environments. They can detect exposure to chemicals, radiation, or other agents. They can sense when the wearer has lost consciousness or mobility (due to a cave-in in a mine, medical conditions like apoxia, stroke, or heart attack). They can detect falls from heights, and attempts to lift excessively heavy loads. Actuators in wearable devices can notify workers when someone nearby is in distress, through an audible alarm or through vibrations when the environment is loud or hearing protection is in use.

## Environment

IoT devices can be used to monitor the quality of air, water, and soil in areas where contamination is a risk to provide early detection of leakage or contamination. Natural disasters such as tornadoes, floods, earthquakes, tsunamis, avalanches, mudslides, and forest fires can be detected. Early detection enables problems to be quickly identified and remediated. Affected systems can be quickly shut down to minimize the impact, and personnel can be notified.

## Inspection and Quality

Data regarding quality parameters can be analyzed in real time, before the manufacture of a part is even completed, and necessary adjustments can be made. Quality control data from individual machine tools can be collected and sent to the cloud, where it can be analyzed remotely.

Quality inspections commonly involve visual confirmation that components are correctly assembled and have no defects. With the massive number and variety of products being manufactured today, traditional computerized scanning techniques are not practical, as they require extensive programming, testing, and refinement. However, by presenting machines with examples of defects, IoT systems can be trained quickly using artificial intelligence to recognize even subtle defects.

## Maintenance

Predictive maintenance is forecasted to be one of the fastest growing and most profitable applications of IoT over the next five years. IoT can improve the ability to predict when production equipment and machinery requires preventive maintenance, with its ability to measure overall equipment effectiveness in real time.

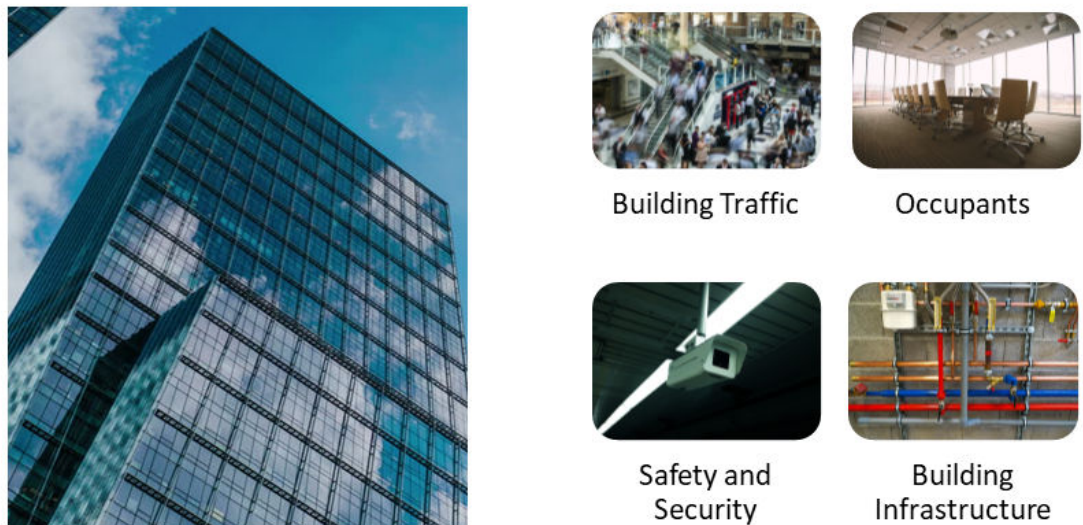
## Case Studies

Case studies describing various industrial IoT projects may be found at the URLs provided.

- IoT Central - IoT in Transportation and Logistics  
<https://www.iotcentral.io/blog/iot-in-transportation-and-logistics>
- Internet of Business - Maersk and Ericsson collaborate for IIoT success story

- <https://internetofbusiness.com/maersk-ericsson-iot-success/>
- MIT Sloan Management Review - GE's Big Bet on Data and Analytics  
<http://marketing.mitsmr.com.s3.amazonaws.com/PDF/57380-MITSMR-EY-GE-Case.pdf>
- Cisco - Leading Tools Manufacturer Transforms Operations with IoT  
[https://www.cisco.com/c/dam/en\\_us/solutions/industries/docs/manufacturing/c36-732293-00-stanley-cs.pdf](https://www.cisco.com/c/dam/en_us/solutions/industries/docs/manufacturing/c36-732293-00-stanley-cs.pdf)
- Hirotec Launches IoT Initiative  
<https://www.ptc.com/en/case-studies/hirotec>

## Buildings



**Figure 2-3: IoT automation in a smart building.**

Large buildings with extensive mechanical, HVAC, electrical, security, and fire alarm systems are often controlled through smart building software called a building management system (BMS). This software may also be called a building automation system (BAS). The BMS may control other systems as well, such as turnstiles, access doors, and elevators that control who is allowed passage, as well as monitoring for security through closed circuit TV and motion detectors.

The software may be proprietary, or may use open standards. The systems connected to a BMS might control up to 70 percent of the energy used in a building, so the BMS is an important tool for managing energy usage in smart cities. It is believed that 8 percent of the world's energy usage could be eliminated through better control of building management systems, which IoT technologies could support.

Building management systems are useful in the event of emergencies. For example, in a fire, the system can be used to locate occupants and shut HVAC dampers to limit the spread of smoke and fire.

IoT technologies support and extend the capabilities of building management systems to improve the experience of occupants, make better use of resources and building space, and improve safety and security. The following are examples of ways in which IoT technology may be applied to smart buildings.

## Building Traffic

Traffic into, within, and out of the building can be monitored and controlled through doorways, gates, toll gates, elevators, and escalators. Various types of keys associated with an individual can be used to track and control traffic, such as key cards, fobs, cipher locks, facial recognition, and other biometric scanners.

## Occupants

Smart buildings can monitor how many people are in the building and determine where they are located. There are numerous applications for this capability. For example, it can be used to locate people during an emergency such as a fire. It can be used to help manage consumption of resources such as heating, cooling, and lighting. It can be used for billing tenants for actual usage of the building and to identify underutilized spaces and facilities.

## Safety and Security

In an emergency, data showing who is currently in the building and where they are located, the locations where hazard and intrusion alarms have been triggered, and other factors, can provide first responders with extremely useful information to help guide a targeted and appropriate response.

## Building Infrastructure

Buildings can be "self-aware" — actively monitoring themselves and making adjustments as needed to improve their status, such as adjusting air balance and control of HVAC systems, rather than blindly following pre-programmed routines that are outdated when conditions within the building change over time. Some building management functions can be monitored and controlled remotely. These features can provide building owners with greater flexibility in staffing, and can reduce the need for on-site specialists, while providing better service to tenants.

Inside and outside environmental sensors monitor factors such as occupancy, lighting levels, temperature, humidity, air quality, and weather, and systems make adjustments as needed to ventilation controls such as vents, louvers, and window blinds, as well as heating and air conditioning. Resources such as power and water can be obtained and stored during times when demand and costs are lower, to be used when demand and costs are higher. Similarly, waste disposal can be more efficient—for example, retaining waste such as greywater until periods when it is most ecological to release into the sewage system. Power from the electrical grid can be supplemented with renewable power from on-building sources, such as wind power, solar, and geothermal. IoT capabilities within the building enable it to balance power generated on site with power from the grid, enabling it to be distributed and used, or sold back to the power company.

Data from machinery such as HVAC systems, elevators, water pumps, and other equipment can be analyzed to support predictive maintenance of equipment.

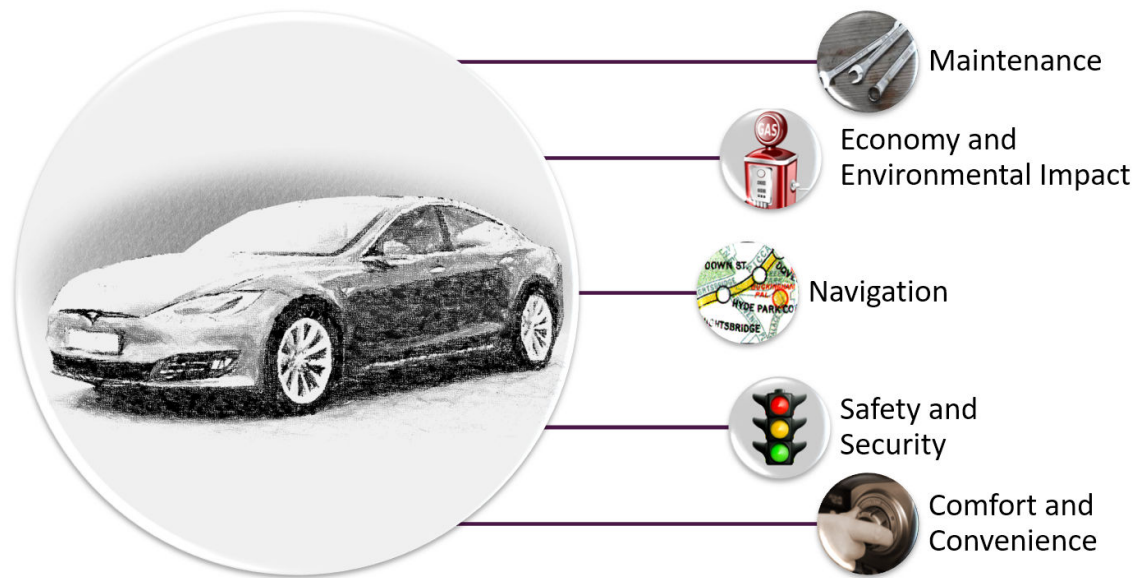
## Case Studies

Case studies describing various smart building IoT projects may be found at the following URLs.

- Intel - Intel Creates Smart Building Using IoT  
<https://www.intel.com/content/dam/www/public/us/en/documents/case-studies/smart-building-using-iot-case-study.pdf>
- Bradford Networks - From Concept to Reality: Designing Security Automation and Orchestration Technology into a Smart Building  
<https://www.bradfordnetworks.com/resources/concept-reality-designing-security-automation-orchestration-technology-smart-building/>



## Connected Cars



**Figure 2-4: IoT automation in a connected car.**

A single connected car may have the processing equivalent of 20 desktop computers onboard. Connected cars typically include a wireless Internet connection through cellular connections such as 3G, 4G LTE, and 5G. Onboard Wi-Fi enables passengers to route their smartphones or other personal devices through the car's cellular Internet connection.

The following are ways that IoT technology may be applied to connected cars.

### Maintenance

Information such as location, fuel level, fuel consumption, maintenance data, load, and weight can be tracked for individual vehicles within a fleet. Analytics tools can be used to correlate that information for the entire fleet, facilitating scheduling, routing, and planned maintenance. Based on fleet data and local fuel/energy costs, and using connected cars, smartphones, or other onboard communication, drivers can be provided with information on where to find optimal refueling locations on their route. Connected cars can monitor driving patterns and assess the wear and tear on a vehicle. Insurance companies can monitor this information and calculate fairer premiums that are based on usage and maintenance of the vehicle. Service stations can use the diagnostic information to perform predictive analysis and contact vehicle owners to schedule a proactive service appointment.

### Economy and Environmental Impact

Connected cars enable the driver to travel quickly, safely, and cost effectively. When vehicles can communicate with traffic signals and other infrastructure, they manage the accelerator better, slowing down before reaching a signal, and the highway infrastructure can also adjust the timing of lights to reduce unnecessary stops. These features will reduce fuel consumption and save drivers time.

### Navigation

Many modern cars are equipped with GPS navigation systems, but connected cars will take this further, combining smart navigation features with services based on location and the car's servicing requirements, such as prompting you to stop and refuel. The car could determine the distance to the nearest fueling station and automatically guide you there using the navigation system.

A connected car could integrate with your personal calendar to help you take the best route to your next meeting, based on real-time traffic and weather conditions. Based on your travel history, your current bearing, and traffic conditions, a connected car might figure out where you are headed and offer suggestions on alternate routing if you're approaching an accident, construction work, or other delay.

## Safety and Security

When connected cars and infrastructure such as smart roads are able to communicate, traffic flow can be coordinated better, not only reducing stops and saving fuel, but also potentially reducing traffic accidents. Connected cars can avert collisions by tracking the speed and the proximity with other vehicles. Vehicles can provide drivers with real-time alerts regarding road and weather conditions and nearby accidents. A connected car can track its location and coordinate with owner data to inform customers when their vehicle may have been stolen and support its safe retrieval. A vehicle could capture the state of the driver through cameras and sensors, and warn them when they suffer from fatigue and tiredness. The system can even optimize the temperature, music, and seat functions to ensure the driver remains alert.

The U.S. Department of Transportation (DOT) has proposed a legal requirement that cars be able to communicate with each other using vehicle-to-vehicle (V2V) technology. If two vehicles are on a collision course, the vehicles could prevent an accident by applying brakes, slowing down, or taking other appropriate actions. The cars would coordinate regarding their movement and speed, and could provide evasive actions before drivers are even aware of the problem.

## Comfort and Convenience

"Keyless" door locks can be accessed using key fobs, smartphones, or other tokens. Preferences for cabin climate and seat positions can be set for each driver and passenger. The power management system enables the car to be "awakened" under remote control to take readings or operate the car. Self-driving vehicles are already on the road. A common feature is automatic parallel parking, which automatically performs a task that some drivers find difficult.

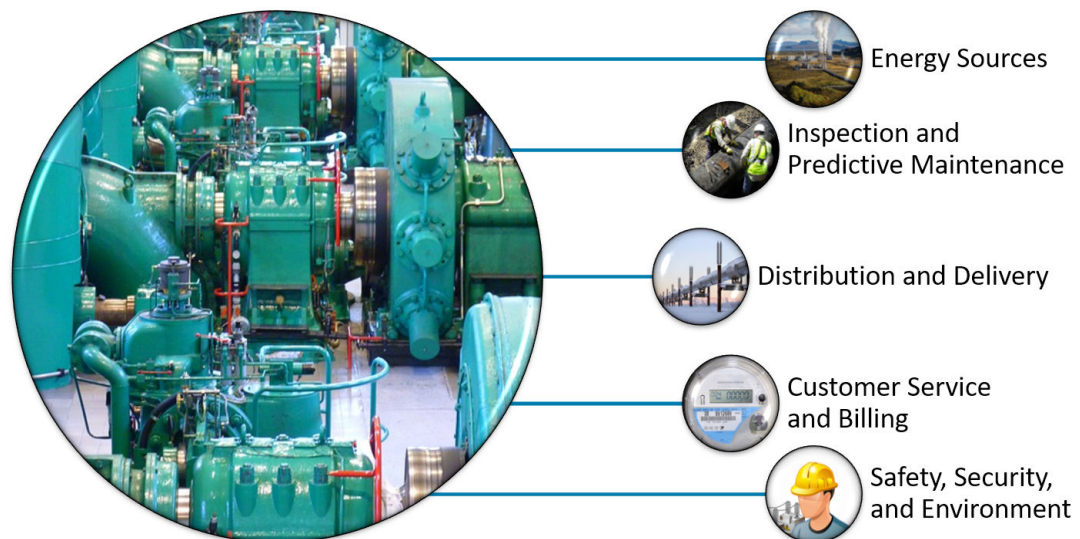
Mobile payment systems are already in use. Digital wallets operating on smartphones enable consumers to safely and securely conduct transactions electronically, such as "paying at the pump." Automobile companies will enable similar electronic payment schemes directly through smart vehicles, enabling the customer to pay at toll gates, fueling stations, parking meters, parks, and campgrounds using a digital wallet embedded in the car dashboard.

## Case Studies

Case studies describing connected car IoT projects may be found at the URLs provided.

- Digital Doughnut - The IoT-Connected Car of Today Case Studies  
<https://www.digitaldoughnut.com/articles/2017/march/the-iot-connected-car-of-today-cases>
- Cisco - Connected Cars  
<https://www.jasper.com/industry/connected-cars>
- IDC - Connected Cars: How Jaguar Land Rover Works With BearingPoint to Benefit Drivers  
[https://www.bearingpoint.com/files/IDC\\_buyer\\_case\\_study-Connected\\_cars-Jaguar\\_Land\\_Rover\\_BearingPoint-1.pdf&download=0&itemId=5158](https://www.bearingpoint.com/files/IDC_buyer_case_study-Connected_cars-Jaguar_Land_Rover_BearingPoint-1.pdf&download=0&itemId=5158)

## Energy and Utilities



**Figure 2-5: IoT automation in energy and utilities.**

The rationale for implementing IoT solutions in public utilities primarily derives from three needs: to make the most efficient use of energy, to minimize and eliminate adverse environmental impacts, and to reduce the cost of producing and delivering it. IoT can provide a wide range of benefits to customers, utility company employees, investors, and the environment. By providing two-way communication between a power utility and its customers, combined with sensing along power transmission lines and smart electrical meters, it is possible to create a **smart grid**, providing numerous benefits to customers, utility companies, and the environment. Many aspects of the smart grid will be managed through **energy management** applications that enable pipeline operators and energy managers to precisely monitor and control their systems, and make well-informed decisions that optimize energy efficiency, increase profits, and reduce greenhouse gas emissions. As with other industry, there are also potential benefits in the form of improved maintenance, safety, and security.

The following are ways that IoT technology may have applications in energy and utility industries.

### Energy Sources

Oil well flow rate, pressure, and temperature data collection can be done every minute, enabling production to be monitored and optimized in near real time. Customer-owned power generation systems and smaller commercial power plants, including solar, wind, bio-gas, and other renewable energy systems, can be controlled and monitored remotely, enabling better integration with the grid, improving power buyback mechanisms, distribution, and use of customer-provided energy sources. Oversupplies during peak production hours can be diverted to short-term storage, such as pump-storage hydropower plants, as needed. With careful monitoring and rules for automatic trading, **energy trading** can be performed in real time.

### Inspection and Predictive Maintenance

Sensors in oil and gas pipelines can monitor pressure, flow, compressor condition, temperature, density, and other variables. Acoustic sensors can detect a breach by a variation in the acoustic signature. Fiber optic sensors can detect deformations in pipe walls. Pinhole leaks can be detected before they can become large ruptures. Sensors can be sent inside pipes for inspection using a **smart pig**, a drone that can detect cracks, defects, and corrosion using magnetic and ultrasound detection. Aerial drones can perform similar inspections outside a pipe. Cameras in remote power stations can use various wavelengths of light (e.g., infrared, visual light) to provide inspection and monitoring.



## Distribution and Delivery

Power outages can be detected and corrected faster, and small outages can be quickly isolated to contain them before they become large-scale blackouts. Gas, oil, and water pipelines can be monitored to identify leaks, enabling prompt detection and shutdown, reducing adverse environmental impact, loss of resources, and cleanup costs. Monitoring of oil pipelines and tank trucks can help to reduce theft, detecting ruptures and instantly alerting personnel when distribution and delivery systems have been compromised.

## Customer Service and Billing

Automatic meter reading capabilities provide up-to-the-minute, accurate readings of power usage. Analytics can help customers visualize how they are using energy over time, to help them plan their use of power more strategically, during less expensive times of day, for example.

## Safety, Security, and Environment

During outages, power restoration can be conducted strategically—such as routing electricity to emergency services first, and taking greater advantage of customer-owned power generation. Water consumption and water quality can be monitored. Rain water and grey water can be harvested and recycled intelligently—particularly in arid climates—to identify water suitable for cleaning, irrigation, and so forth.

## Case Studies

Case studies describing energy and utility company IoT projects may be found at the following URLs.

- AWS - Power & Utilities Customer Case Studies  
<https://aws.amazon.com/power-and-utilities/case-studies/>
- Internet of Business - 10 real-life examples of IoT powering the future of energy  
<https://internetofbusiness.com/10-examples-showcasing-iot-energy/>
- Silver Spring Networks - Smart Grid Makes Restoration Faster, Easier for Utilities  
<https://www.silverspringnet.com/wp-content/uploads/SilverSpring-ExecutiveOverview-Outage.pdf>
- Three oil and gas IoT case studies  
<https://enterpriseiotinsights.com/20170515/channels/fundamentals/20170515channelsfundamentalsthree-iot-case-study-oil-gas-industry-tag23-tag99>

## Health, Medical, and Life Science



**Figure 2-6: IoT automation in health, medical, and life sciences.**

The healthcare industry has already begun using connected devices in a big way. As of 2018, the majority of healthcare organizations are using IoT for maintenance and monitoring of medical equipment and are leading business in adoptions of IoT technology. Patient monitoring equipment is the leading use case, but a variety of other applications are emerging. Consumer-oriented devices such as fitness watches have become commonplace. The following are various ways in which IoT technology is used in health, medical, and life science organizations and by consumers.

### Personal Health and Welfare

Wearable devices such as smart watches can measure a user's physical activity, heart rate, and body temperature. Better techniques for unobtrusively monitoring blood pressure, irregular heart rhythms, blood glucose levels, body chemistry, and so forth continue to be developed. Patients' use of prescription medicines can be monitored through devices such as connected pill boxes, injection devices, and inhalers. At-risk patients can wear devices that monitor them for medical issues or falls, and automatically alert care-providers when there is a problem and provide germane data, such as where the patient is currently located.

### Medical Devices

Home-use medical devices such as **continuous positive airway pressure (CPAP)** devices (which facilitate a patient's healthy breathing while sleeping), defibrillators, cardiac monitoring devices, and insulin pumps are now commonly designed to be connected devices that can be set up and monitored by clinicians in a remote location using a Wi-Fi or cellular data connection.

### Hospital Logistics

Safety is a primary concern for healthcare organizations. A critical component of safety is the ability to track assets such as medical staff, patients, and equipment throughout the medical campus, and to know the status of all devices and instruments. IoT and real-time location systems facilitate asset tracking, making it possible to know the location and status of the people and things involved in any healthcare scenario.

IoT's ability to track logistics—the location and status of goods—in real time has been demonstrated through retail industries like Amazon. Logistics capabilities can help solve the

problem of verifying the chain of custody in the pharmaceutical supply chain. New regulations require organizations to ensure that drugs have been protected from tampering by tracking the global path of a pharmaceutical product from raw material to end consumer.

## Medical Services

Cost reduction is a major benefit of IoT in healthcare. Telemedicine, sleep studies, cardiac monitoring, and other tasks that used to be performed in clinics are now often performed outside the clinic, as patients wear small devices that perform the monitoring tasks and go about their normal lives. This reduces the workload of healthcare providers, and frees up space in clinics, reducing overall costs.

Telemedicine can be very beneficial in countries and locations where health facilities are unavailable or inaccessible. The portability of these devices makes them very useful in areas with limited resources such as floods, earthquakes, and war zones.

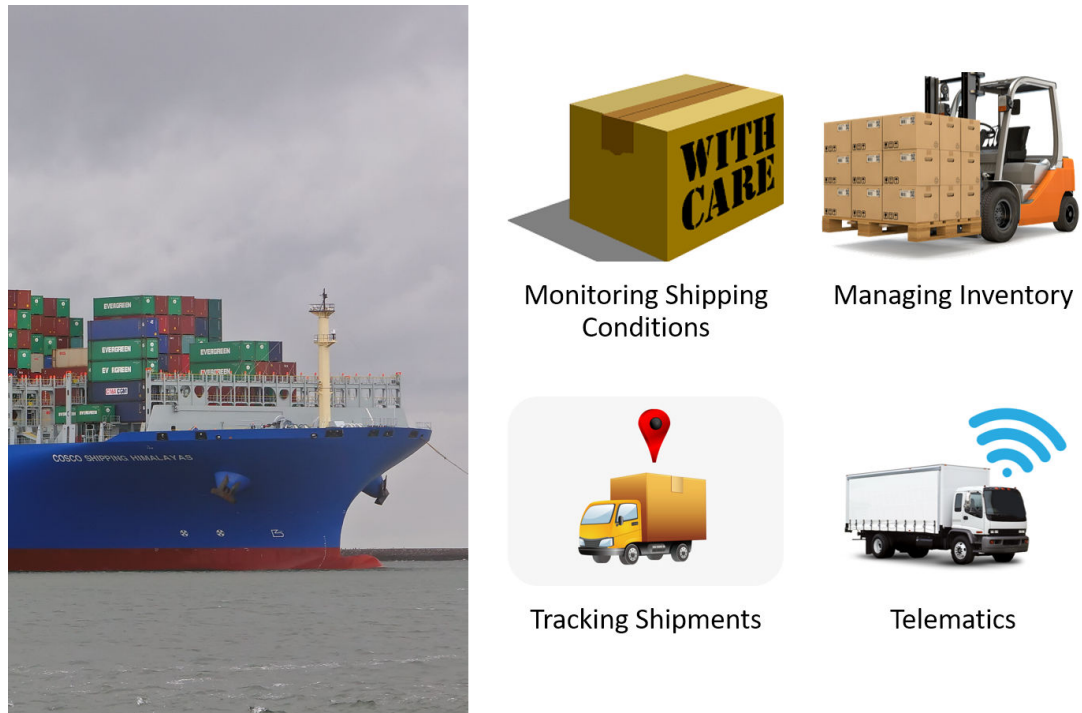
Robotic surgery provides a number of potential benefits. Robots may be able to perform certain operations with precision exceeding that of a human surgeon. And because robots can be autonomous or controlled from a distance, robotic surgery may have applications in telemedicine as well, enabling procedures to be performed in remote locations that can't easily be reached by a surgeon, and enabling surgeons to extend their coverage. Another type of surgery involves using miniature robots that can perform surgery inside the body, minimizing incisions and exposure to pathogens, and making possible various types of surgery that would previously have been impossible or dangerous to perform.

## Case Studies

Case studies describing IoT projects in health, medical, and life science organizations may be found at the following URLs.

- IoT News - Internet of Things case study: Boston Children's Hospital and smarter healthcare  
<https://www.iottechnews.com/news/2017/feb/28/internet-things-case-study-boston-childrens-hospital-and-smarter-healthcare/>
- Microsoft - 365mc improves the efficiency and safety of Liposuction with data analysis based on Microsoft Azure IoT solution accelerators and Machine Learning  
<https://customers.microsoft.com/en-us/story/365mc-azure-iot-suite-machine-learning-korea-en>
- Microsoft - Roche Diagnostics Case Study  
<https://customers.microsoft.com/en-us/story/roche-diagnostics>
- Fujitsu - Panasonic and Fujitsu Begin Joint Testing of an In-Home Monitoring Service for the Elderly  
<http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0625-01.html>

## Supply Chain



**Figure 2-7: IoT automation in supply chain management.**

IoT sensors can be made small, rugged, and self-supporting, so they can follow goods along for the ride as they make their way through the supply chain. IoT devices can relentlessly track and report details about the world around them while requiring minimal human intervention, making them ideal for tracking shipments and the status of inventory.

The following are various ways in which IoT technology is used in supply chain management.

### Monitoring Shipping Conditions

IoT devices at the source can provide measurements of conditions in which inventory is shipped, from the source to the destination. Products like pharmaceuticals, paint and chemicals, food, and so forth require special handling to ensure quality is maintained during shipping. Sensors can measure conditions such as ambient temperature, humidity, and air pressure, and either prevent operations or re-route if the conditions fall outside required parameters.

### Managing Inventory

In the past, managing inventory involved numerous counts, recounts, and/or paperwork as products were used or sold. With IoT, the process is automated through RFID tags on each item, which communicate with sensors to provide real-time data on the location of inventory. As inventory is depleted, sensors can monitor the count, weight, or volume of the remaining inventory, automatically ordering or replenishing as needed. Connected devices, tags, and sensors help to eliminate guesswork, thereby reducing risk.

### Tracking Shipments

Tracking shipments have been handled similar to inventory. As a package moves from one hub to another, a bar-code scan is performed to keep shipper and receiver informed about the package's location. The bar-code scan was an improvement over manual accounting, but in the IoT model, tracking information can be acquired from tags that automatically check in when they reach a hub.

Other sensors can report on shipping conditions, such as pressure, jolts, vibrations, noise, temperature, and so forth. If an item is damaged in transit, the cause and location can be pinpointed through this data. IoT can ensure that perishable products such as food have been kept in a controlled temperature during the entire shipping process, verifying what is called a "cold chain." Lab samples en route for testing can be tracked in a similar way. These are the sorts of tasks for which IoT is ideal.

To provide customers with transparent reporting of cold chain and other tracking data, companies are using blockchain to record the various data points as products are shipped from their source.

## Telematics

**Telematics** uses telecommunications technology to monitor the location, movements, status, and behavior of a vehicle or fleet of vehicles. A company's fleet might include vehicles such as ships, vans, and trucks.

## Case Studies

Case studies describing IoT projects involving supply chain management may be found at the following URLs.

- Enterprise IoT Insights - Orbcomm launches new cold chain monitoring solution  
<https://enterpriseiotinsights.com/20170816/internet-of-things/orbcomm-launches-new-cold-chain-monitoring-solution-tag23>
- Greening Supply Chains with the IoT  
<https://www.ulehssustainability.com/blog/supply-chain/greening-supply-chains-with-the-iot/#sthash.JvzCzbAn.dpbs>
- Virtualization of food supply chains with the Internet of Things  
<https://www.sciencedirect.com/science/article/pii/S026087741530056X>

## Agriculture



**Figure 2-8: IoT automation in agriculture.**

Large farms have already seen significant productivity gains through IoT. Improvements in the measurement and analysis of weather, the condition of soil, plants, and livestock, and market data combined with effective analytics enable farmers to improve their yields while making more efficient use of land, water, fertilizer, and other resources, and reducing environmental impact. These improvements help farmers obtain a higher return on investment.

Better information can also help farmers provide consumers with greater transparency, enabling them to more accurately monitor how much water and chemicals were used, and when and how the food was harvested.

Large investments in sensors and equipment may cost more than small farmers can afford. But some small farmers have figured out how to take advantage of IoT on a smaller scale, and are experiencing productivity gains. IoT can improve the efficiency of small farms, making them more viable and resilient to adverse conditions.

The following are examples of various ways in which IoT technology may be applied in agriculture.

### **Crops and Livestock**

IoT sensors can monitor plants for signs of stress, and make adjustments or recommendations to the farmer as needed. IoT analytics can evaluate crop data, weather conditions, and market data to determine the best timing for harvest. Biosensors on and around livestock can be used to acquire data that will help make better decisions regarding feeding, breeding, and the use of antibiotics.

### **Soil and Environment**

Soil chemistry can be monitored in very small areas, enabling precise adjustments of fertilizer and amendments to conserve on their use while improving soil quality. Local weather can be monitored and forecasted, adjustments to irrigation and drainage can be made as needed, and spraying and application of fertilizer can be scheduled. Aerial drones provide a closer, more accurate, affordable, and continuous view of farms, enabling them to be divided into manageable zones. Soil and crops can be managed on an extremely local basis, accounting for different microclimates within a single field, for example.

### **Equipment**

Tractors, harvesters, planters, sprayers, and other equipment can be tracked and monitored to support predictive maintenance. Fuel use can be managed by monitoring equipment use, and making adjustments or recommendations. GPS-connected tractors can plow furrows more accurately and use land more efficiently. Water, fertilizer, and amendments can be applied more precisely under machine control, and refer to soil and location data.

### **Irrigation Systems**

Data such as soil humidity, temperature, groundwater levels, weather forecast, and recently applied fertilizer or chemical interventions can guide where irrigation is needed to conserve water while improving results. Actuators can use GPS to determine the current position of fertilization and chemical apparatus, and can precisely adjust the amount being applied as determined by previously acquired data and analysis.

### **Drainage and Waste Systems**

Chemical sensors can determine the composition of animal waste and prioritize its use for fertilization, or energy production through bio-gas processing.

### **Case Studies**

Case studies describing IoT projects involving agriculture may be found at the following URLs.

- IoT Central - Can A Cow be an IoT Platform?  
<https://www.iotcentral.io/blog/can-a-cow-be-an-iot-platform>
- Internet of Business - Farming and shipping first to power IIoT revolution



<https://internetofbusiness.com/farming-and-shipping-first-to-power-iiot-revolution/>

- Drones in Precision Agriculture

<https://medium.com/@Unfoldlabs/drones-in-precision-agriculture-331c23cefc0b>

## Retail



**Figure 2–9: IoT automation in retail businesses.**

IoT technologies provide new ways to manage retail operations and provide store security, market products to customers, and manage sales transactions.

The following are ways in which IoT technology may have applications in retail businesses.

### Inventory Management and Distribution

Retail involves significant logistics operations that can be assisted through IoT, including the distribution of products to warehouses, from warehouses to stores, the transfer of inventory between stores, and shipping products to customers.

### Customer Traffic and Presence

IoT can be used to monitor customer traffic and presence in stores. This includes the use of floor sensors or light beams to track foot traffic, detecting the presence of mobile phones (through beacon or Wi-Fi triangulation functionality), and other types of sensors. Monitoring in-store traffic patterns can help to inform where products should be placed along popular routes. Combined with demographic data, traffic patterns can be more deeply analyzed to reveal how different types of customers move through the store, further informing product placement.

### Advertising

Analysis of in-store traffic patterns can be correlated to advertising in digital signs and store loudspeakers to determine their impact in real time. Online stores target their marketing based on customer's previous purchases or patterns of products they have looked at. Similar approaches can be used in bricks-and-mortar stores by detecting the customer's presence and location, identity (whenever possible), and using digital signs, self-serve kiosks, smartphone apps, wearable devices, and other methods to deliver advertising messages. Based on data provided by the customer's smart home appliances (such as smart refrigerators and thermostats), the customer can be reminded to purchase needed consumables (such as milk or furnace filters).

## Security

Using sensors such as RFID and smart cameras, IoT systems can track unpurchased items being removed from the store. Using infrared cameras, chemical and metal detectors, people entering or leaving the shopping facility can be scanned for weapons and dangerous materials. When security events occur, the system can trigger appropriate interventions.

## Vending and Payment

A wide variety of mobile payment systems and digital wallets (using smartphones or other devices) can be used to enable customers to safely and securely conduct electronic transactions. Wireless technologies such as Bluetooth® Low Energy (BLE) and near field communication (NFC) beacons make it unnecessary for customers to retrieve their devices or wallets to conduct transactions. Self-serve kiosks can be provided to help customers locate products in the store, request human assistance, bag items, and check out.

## Case Studies

Case studies describing IoT projects involving retail businesses may be found at the following URLs.

- Information Week - Amazon Robotics: IoT In The Warehouse  
<https://www.informationweek.com/strategic-cio/amazon-robotics-iot-in-the-warehouse/d/d-id/1322366>
- IBM - The New Retail Revolution: Connected Store  
<https://www.slideshare.net/IBMIoT/watson-iot-for-retail>
- IBM MetroPulse unlocks purchasing behavior insights, block by block  
<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=02013902USEN>
- Leading from the front: Digital Reinvention in retail  
<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03873USEN&>

## Defense



Matériel



Connected Warfighter



Logistics

**Figure 2–10: IoT automation in defense.**

Military organizations, in many ways, have many of the same information management needs as business and industry. The armed forces support their own medical facilities, have buildings and



vehicles to maintain, an enormous and complicated supply chain to manage, and even operate their own publishing, broadcasting, and retail facilities. As it does for the private sector, IoT has much to offer these sorts of operations.

But military organizations also have special needs. And IoT presents special risks to the military as well, as evidenced by recent reports that a hidden military base was revealed by a fitness app innocently used by a soldier who frequently jogged on and around the base.

To be fit for military use, IoT must be implemented with some differences from infrastructure supporting IoT in the private sector. Hacking is always a threat. Military IoT should not depend on centralized, publicly accessible clouds. Secure networks are essential. The U.S. has already created a classified data network that spans 48,000 miles. Using consumer-oriented devices will be unacceptable for many military scenarios. Such devices are not made to support protocols used in the military, and are not up to its stringent standards.

Nonetheless, the special needs of military organizations can be served by IoT technologies, even if they're not always provided in the same form as they are for consumer products.

## Matériel

Matériel such as tanks, aircraft, drones, ships, submarines, and satellites may be computer-controlled and network-connected. Vehicles can form a peer-to-peer network within seconds of forming a convoy. Data can be communicated between vehicles on the ground, in the air, and at sea, and with bases of operation throughout the world.

## Logistics

IoT has already improved the military's logistics and supply chain management. In war situations, IoT's logistics capabilities enable tracking of supplies and equipment from their source to where they are needed on the battlefield.

## Connected Warfighter

Soldiers in combat can wear devices to enable them to communicate and coordinate with each other. The small size and low power requirements of IoT sensing and communications devices makes them ideal for use in forward situations. Soldiers are provided with enhanced situational awareness. Combined with aerial drones, satellite images, and night vision, soldiers literally have a birds-eye view across hostile terrain. Internetworking capabilities enable information to be relayed from soldier's sensors and communication channels back to command and support facilities.

The armed forces collect data from a range of different platforms, including aircraft, weapon systems, ground vehicles, and troops in the field. Through IoT analytics, the military can increase the effectiveness of their intelligence, surveillance, and reconnaissance systems, enabling armed forces to identify key threats faster and with more accuracy.

## Case Studies

Case studies describing IoT projects involving security and public safety may be found at the following URLs.

- IBM - Military Cloud – Case Studies  
<https://www.ibm.com/blogs/insights-on-business/government/military-cloud-case-studies/>
- IoT for Military Asset Management  
<https://www.tapestry-solutions.com/2017/12/19/esi-and-the-iot-in-the-military-part-i-problems-from-the-past-and-how-the-internet-of-things-is-transforming-dod-supply-chain-management/>
- A systemic and cognitive vision for IoT security: a case study of military live simulation and security challenges  
<https://hal.archives-ouvertes.fr/hal-01478323/document>

- A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges  
[https://www.researchgate.net/publication/320637095\\_A\\_systemic\\_and\\_cognitive\\_vision\\_for\\_IoT\\_security\\_A\\_case\\_study\\_of\\_military\\_live\\_simulation\\_and\\_security\\_challenges](https://www.researchgate.net/publication/320637095_A_systemic_and_cognitive_vision_for_IoT_security_A_case_study_of_military_live_simulation_and_security_challenges)

## Connected Services

Suppose you buy a watch. Your relationship with the store that sold you the watch and the company that manufactured the watch may end the moment you leave the store. Of course, you might contact them if you have a problem with the watch. And some day, you might want to buy a new watch. If you had a good experience with the previous watch, you might buy your new watch from the same store or company. It's hard to get new customers, so many organizations look for ways to retain customers and build loyalty by establishing a relationship that goes beyond the sales transaction.

Connected devices can "phone home" to services provided by their manufacturer, so the device literally maintains a connection between the manufacturer and the customer. Of course, there must be a benefit—some sort of services provided—for customers to allow the connection. This is what is known as **connected services**.

In the case of a connected fitness watch, connected services might include such things as:

- A dashboard for viewing data collected by the watch over several months, such as your heart rate statistics, steps walked, calories burned, and so forth.
- Social networking with other watch users, such as competitions to see who gets the most exercise.
- Access to an app store, from which you can download apps and custom clock faces to the watch.
- Recommendations on exercise.
- The ability to examine watch data on other devices, such as computers, tablets, and smartphones.

Products that include connected services help to establish a relationship with customers, and provide more value to customers than a physical product alone. They also enable companies to learn more about their customers, which can help them make improvements to products and services over time.

## Guidelines for Using IoT to Solve Problems

Follow these guidelines to use IoT to solve problems.



**Note:** All of the Guidelines for this lesson are available as checklists from the **Checklist** tile on the CHOICE Course screen.

### Identify Goals for an IoT Implementation

When identifying your goals for your IoT project, look for opportunities to accomplish the following:

- Improve decision-making.
- Understand customers better.
- Deliver new value to customers.
- Make operations more efficient and effective.
- Reduce adverse impact on the natural environment.
- Improve the bottom line and increase business value.

### Identify Problems in Your Business that IoT Can Help to Solve

When planning an IoT solution, start by identifying problems your business needs to solve. Then consider which of the following questions apply to each problem. If the question applies to the problem, record your answer, which may become part of the requirements for your IoT solution.

- Can we obtain real-time data that would help us respond to this problem faster or better?
- Would it help if we could accomplish work in remote locations with less human intervention? (If "yes," then ask the following questions to determine what sorts of work should be accomplished.)
  - Is there data we should collect?
  - Is there data that should be analyzed immediately at the collection point to enable corrective actions to be taken using process automation?
  - Is there data that should be forwarded to the cloud for deeper analysis?
  - Are there automated processes that should be guided by a person in a different location (remote control)?
  - Are there automated processes that should be performed by a robot or process automation (autonomous)?
- Would it help to collect and analyze data about any of the following? (If "yes," then note which of the following information areas would be useful to have.)
  - Location and status of raw materials throughout the entire supply chain
  - Operations performed in your organization
  - Your equipment, assets, and inventory
  - How your operations impact the natural environment
  - How your customers interact with products
  - Customer shopping behavior

## Use Models to Design a Solution

Use a good reference architecture as a general model for your own projects, such as:

- Internet of Things Architecture (IoT-A): <https://docs.iota.org>
- IEEE P2413 Standard for an Architectural Framework for the Internet of Things (IoT): <https://standards.ieee.org/develop/project/2413.html>
- Industrial Internet Reference Architecture (IIRA): <https://www.iiconsortium.org/IIRA.htm>

## Use Vendor References to Guide Your Design

When basing an IoT solution on a particular vendor's platform, take time to learn the practices vendors recommend for their platform. Examples of vendor-specific guides include:

- Amazon Web Services Pragma Architecture: <https://aws.amazon.com/blogs/startups/iot-a-small-things-primer/>
- IBM IoT reference architecture: <https://www.ibm.com/cloud/garage/architectures/iotArchitecture>
- Intel® IoT platform Reference Architecture: <https://www.intel.com.au/content/www/au/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html>
- Microsoft Azure IoT Architecture: <https://azure.microsoft.com/en-au/blog/azure-iot-reference-architecture-update/>

# ACTIVITY 2–1

## Using IoT to Solve Problems

### Data File

C:\CNX0004Data\Undertaking an IoT Project\Using IoT to Solve Problems.docx

### Scenario

**Best Elevator** specializes in elevators with a reputation for high quality and dependable customer service. Competition is on the rise and the company is constantly at risk of losing market share to competitors.

### The Problem Areas

The company has identified several areas that have been a problem for them in the past. They are hoping to address these problem areas through IoT. They have expressed the problems as goals for improvement.

- Increase customer loyalty
- Improve service maintenance and predictive maintenance
- Manage spare parts inventory more efficiently
- Improve product design and technician training
- Improve uptime and field service efficiency
- Allocate scarce service technicians more efficiently
- Communicate more effectively with suppliers

In the spaces provided, write your ideas regarding ways that an IoT solution might address these problems. (If you'd prefer to type your ideas in a Word document, a worksheet is provided in C:\CNX0004Data\Undertaking an IoT Project\Using IoT to Solve Problems.docx.)

---

1. How might IoT help Best Elevators increase customer loyalty?

2. How might IoT help Best Elevators improve service maintenance and predictive maintenance?

3. How might IoT help Best Elevators manage spare parts inventory more efficiently?
  
  
  
  
  
  
  
  
  
  
  4. How might IoT help Best Elevators improve product design and technician training?
  
  
  
  
  
  
  
  
  
  
  5. How might IoT help Best Elevators improve uptime and field service efficiency?
  
  
  
  
  
  
  
  
  
  
  6. How might IoT help Best Elevators allocate scarce service technicians more efficiently?
  
  
  
  
  
  
  
  
  
  
  7. How might IoT help Best Elevators communicate more effectively with suppliers?
-

# TOPIC B

## The IoT Development Lifecycle

Your organization has decided to undertake an IoT project. To avoid the risks inherent in such a project, the organization should be sure to implement effective project management and development methodologies throughout the process.

### Complexity of IoT Projects

According to a Cisco survey (<https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1847422>), a majority of IoT projects get bogged down at the Proof of Concept stage, with only 26 percent of completed IoT projects considered a success by those who implement them. IoT projects are often complex. IoT projects converge different technologies from different vendors involving different platforms. Some of the products involved in a solution may target consumers, while others target business or industry, and even custom electronic components may be involved.

Furthermore, those implementing IoT solutions often need to learn new approaches to network design, security, and business strategies. They may need to work with new business or technology partners. And they may be exposed to regulations and standards they never had to deal with before.

There may be significant payback on IoT projects, but there are also significant risks. Because of this, organizations should be careful to employ systematic development processes when working on IoT projects.

### The IoT Development Lifecycle

Various models have been defined to describe essential phases in the *system development life cycle (SDLC)* of an IT system or project. While different models exist, they all tend to promote the idea of following a methodology to ensure no important steps are left out at any phase, with the goal of ensuring quality (including cybersecurity, privacy, and safety), operating efficiently, and reducing costs.

The models tend to encompass some form of the following phases.

- **Initiate:** A need is identified, initial goals are set, and the project is initially staffed with those responsible for planning it.
- **Plan:** Planning may include preliminary analysis and development of a system concept. Alternative solutions are examined along with a prediction of costs and benefits. The preliminary analysis may include clarification of the problem and objectives. A decision may be made to leave the system as is, improve it, or develop a new system.
- **Analyze requirements:** Facts are gathered through documentation, interviews, observation, questionnaires, examination of existing systems, and other sources. These facts are interpreted to translate project goals into functional and quality ("non-functional") requirements for the project, with a focus on describing the desired outcomes, rather than the design of the solution.
- **Design:** Based on requirements, a solution is identified and recorded in documentation such as screen layouts, business rules, process diagrams, data flow diagrams, and pseudocode to describe the desired features and operations in detail to those who will develop them.
- **Develop:** Based on requirements and design documents, code is written and other resources (data, images, etc.) are developed for use in the solution.
- **Integrate and test:** All of the pieces are brought together in an environment where they can be tested and checked for errors, bugs, security, privacy, safety, and interoperability with other systems. This phase ends when requirements have all been met, the project is accepted by

stakeholders, and development is considered complete. The system is authorized for implementation.

- **Implement:** The system is installed and deployed. It is put into production, and actual business begins operation on the system.
- **Operate and maintain:** The system is monitored and periodically assessed to ensure it maintains proper functioning and performance, continues to meet requirements, and does not become obsolete. Periodic updates must be performed.
- **Dispose:** In this phase, plans are developed for discarding system information, hardware, and software in making the transition to a new system. The purpose here is to properly move, archive, discard, or destroy information, as well as hardware and software that is being replaced, in a manner that prevents any possibility of unauthorized disclosure of sensitive data. The disposal activities ensure proper migration to a new system. Particular emphasis is given to proper preservation and archiving of data processed by the previous system. All of this should be done in accordance with the organization's security requirements.

As part of the initial planning process, all of these phases should be planned. For example, the planning process might identify potential problems that could occur when the system is eventually retired or replaced. By identifying these problems upfront, the system can be designed so that these problems don't occur in the first place, which is much better than having to come up with a solution later on.

## Return on Investment

One of the greatest challenges reported by enterprises planning and deploying IoT projects is demonstrating a return on investment. IoT presents a wide array of interesting use cases for business, but it can be difficult to estimate the economic value of these benefits. Likewise, it can be hard to estimate the cost of numerous challenges that need to be addressed, such as network design, cybersecurity, aggregating data from many sources and data formats, and bringing them all together to allow complex analytics and decisions to be made.

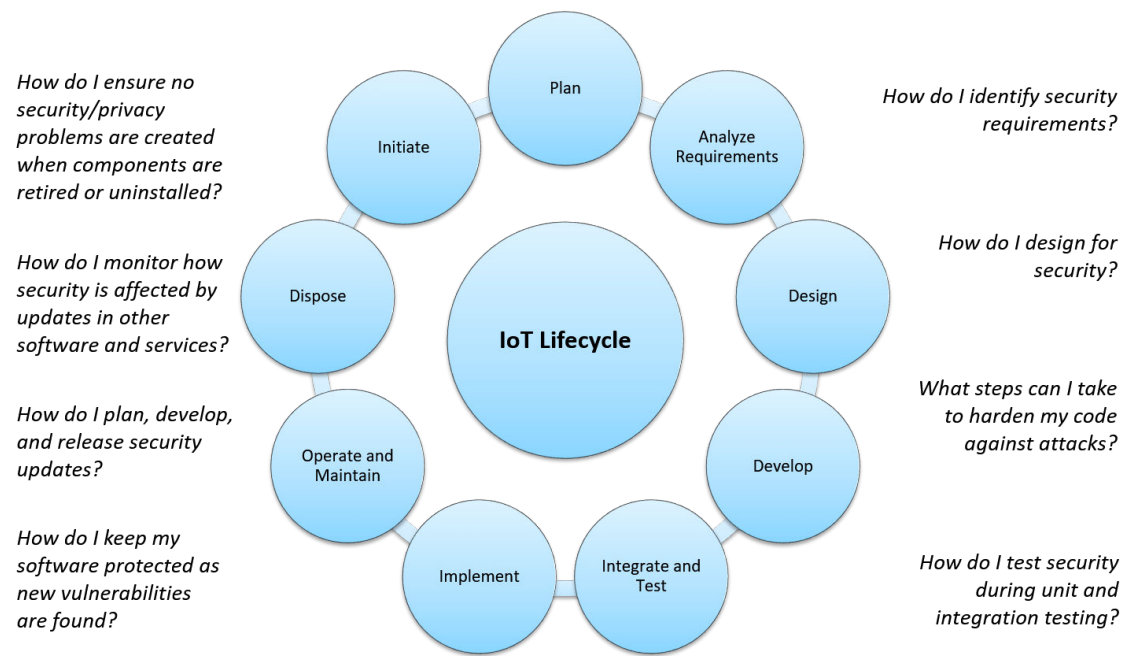
## Focus on Business Goals

IoT is transformative. Numerous organizations have already implemented IoT solutions and are reporting their successes with it. It is easy to get tempted by the hype, focusing on the interesting possibilities of IoT and looking for ways to shoehorn them into your business process, when instead you should focus on specific problems your organization needs to address, and then consider how IoT and other key technologies might help you address the issues you have identified.

## Cybersecurity Throughout the IoT Lifecycle

Unfortunately, in many IT projects, cybersecurity may be dealt with as an afterthought. But when security problems are late in development or after the system is deployed, security problems may have expensive consequences and at the very least are more expensive to correct than if they are found and corrected early in the project.

As with any aspect of software quality, to ensure successful implementation, security should be dealt with in every phase of the development lifecycle. From the very start, as you plan and identify requirements, security requirements should be identified. Those requirements should be designed and developed into the solution, and testing should verify that the requirements have been met. As you deploy and maintain the system over time, security should be monitored and necessary updates applied as needed to maintain security.



**Figure 2–11: Cybersecurity throughout the IoT lifecycle.**

## Guidelines to Prepare for an IoT Initiative

Follow these guidelines to prepare for an IoT initiative.

### Prepare for an IoT Initiative

Even before your organization commits to undertaking a major IoT project, there are steps you can take to prepare the organization, and by starting small, you can minimize risks and help to ensure the successful adoption of IoT.

- **Understand the organization's current state:** An early part of the planning process is to identify the results you're looking for. This requires that you understand the current state of the organization's business processes, know where there is need for improvement, and what type of information and process deficits are involved. This will help to reveal where new information flows and process automation provided by IoT can help.
- **Perform pilot projects and experimentation:** Starting small can help the organization to avoid risks involved in climbing a learning curve on a major project. Consider developing a proof of concept to test ideas first on a small scale. You can use small pilot projects to minimize risk, develop and improve your internal processes, evaluate vendors and products, and refine integration with your other systems. As you gain successes on smaller projects, you can scale them up over time. Pilot projects give you better data regarding costs and benefits, which you can use to estimate your return on investment on larger projects.
- **Manage change and corporate culture:** As you plan your IoT project strategy and pilot small projects, you can identify and eliminate gaps in your infrastructure, core skills, tools, and resources. By avoiding large failures, you can gain acceptance of IoT throughout the organization. As the use of IoT increases, involve more groups and individuals, sharing successes and lessons learned.

### Follow Best Practices for IoT Development

To help ensure your success in your IoT projects:

- Work with project stakeholders to define business goals and identify requirements for IoT projects that will help the organization reach those goals.



- Build security and privacy into every phase of development, rather than treating them as an afterthought. For example, include threat modeling early in the design process to plan countermeasures and defenses in advance.
- Employ a dedicated IoT architect to provide central coordination of IoT projects and provide guidance on design and best practices. Update skill sets and job descriptions as needed throughout the organization to distribute responsibility for supporting IoT systems.
- Include the IoT architect, information technology (IT), operational technology (OT), and business groups within the organization when identifying, planning, and documenting the organization's target architecture for IoT.
- Honestly appraise the organization's legacy infrastructure to determine whether it can meet the fundamentally different requirements of IoT, and if not, where it needs to be upgraded or replaced.
- Honestly appraise the organization's capabilities, and do not try to implement IoT projects relying solely on existing internal resources and IT generalists. Provide staff with training opportunities and add staff as needed. Work with trusted partners or vendors who can fill in your organization's gaps in IoT expertise.
- Utilize staff and resources from the organization's IT, OT, and business groups when evaluating potential IoT partners, vendors, and products.
- Design the entire solution as a system. Ensure the team understands the capabilities of all components within the system, and configure them as required to keep the overall solution as simple as possible, and configured correctly to meet performance, security, and other requirements.

## ACTIVITY 2–2

### Preparing for an IoT Initiative

#### Scenario

Working with your colleagues at Best Elevators, you have identified how you will address various problem areas within the company's operations. The following is a summary of the solution.

#### The Solution

As for the first problem, *increasing customer loyalty*, the company wants to establish a closer relationship with customers, provide services to help customers meet their own needs, and provide them with peace of mind that they associate with using Best Elevator products and services.

They plan to achieve this goal by quickly moving to a *connected services* strategy for their elevator product lines. When a company chooses to use Best Elevators, they will not only buy a high-quality product that provides good value for the money spent, but they will also invest in services that make Best Elevators a better choice than its competitors.

Each elevator will come with services that include:

- **Continuous monitoring of elevator safety and performance factors**, with data viewable through applications provided by Best Elevator.
- **Comprehensive data dashboards** to show the status of all elevator systems in real time, including usage reports and other information facility managers will find useful.
- **Faster maintenance and repairs**, made possible through better information, and the ability to anticipate problems before they occur and before they lead to other problems.
- **Reduced elevator downtime**, made possible through continuous monitoring and real-time notifications when problems are anticipated.

As IoT systems are installed and used, the other problem areas will be addressed in phases, as follows.

Problem Areas	How Addressed through IoT
<ul style="list-style-type: none"> <li>• Improve service maintenance and predictive maintenance</li> </ul>	Initially, Best Elevator wants to provide its customers with data collection from sensors, and analytics to improve service maintenance and predictive maintenance. The IoT solution must provide early-warning data and remote diagnostics to enable the organization to dispatch technicians promptly, ensuring they are equipped with the necessary information, tools, and parts to restore the equipment to safe operating conditions quickly.
<ul style="list-style-type: none"> <li>• Manage spare parts inventory more efficiently</li> </ul>	IoT can be very helpful for keeping spare part inventories in warehouses and service vehicles stocked appropriately, which is normally a notoriously difficult task to manage cost-effectively. On the supply side, inventory can be tracked using typical IoT devices such as RFID tags. On the demand side, elevator equipment can be monitored and analyzed using data analytics and Best Elevators' own domain expertise to predict future needs. Combining historical data of part failure rates with analytic algorithms, Best Elevator can optimize their part stocks in the warehouse and technicians' service vehicles, reducing inventory costs and improving repair time.

<b>Problem Areas</b>	<b>How Addressed through IoT</b>
<ul style="list-style-type: none"> <li>• Improve product design and technician training</li> <li>• Improve uptime and field service efficiency</li> <li>• Allocate scarce service technicians more efficiently</li> <li>• Communicate more effectively with suppliers</li> </ul>	<p>Once IoT systems are in place, the system will be able to collect and analyze usage patterns over time. This information can be used to improve product design and technician training, which will further improve uptime and field service efficiency, and allow more efficient allocation of scarce service technicians.</p> <p>Parts distributors and value-added resellers will also see additional opportunities to leverage the insight garnered from the IoT connected service solution. Best Elevator can share its experience and knowledge with equipment manufacturers, creating a value-based competitive advantage in a market that is highly cost-driven with pricing volatility.</p>

At this point, Best Elevator has identified the problems they need to address and have set goals for the project. Staff have been identified to carry out the project. A preliminary analysis has been performed, and a general system concept has been described (summarized previously). After much deliberation, costs and benefits have been identified, and the team has decided to proceed with the IoT implementation.

**1. What would need to be done next in this project?**

**2. What sorts of change management issues might arise as the company shifts from primarily selling physical goods to selling services?**

## Summary

In this lesson, you examined how IoT technologies can help to resolve real-world problems, and you identified issues you'll need to consider throughout the IoT development lifecycle.

**Where does IoT have the greatest potential to benefit your organization?**

**What steps should your organization take to ensure its success in IoT projects?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# Course Follow-Up

Congratulations! You have completed the *IoTBIZ™ (Exam IOZ-110)* course. You have gained knowledge to guide business decisions for implementing and managing IoT projects.

You've also gained knowledge that will prepare you for the CertNexus® *IoTBIZ™ (IOZ-110)* credential. If you combine this class experience with review, private study, and hands-on experience, you will be prepared to demonstrate your IoT management expertise both through professional certification and with solid competence on the job.

## What's Next?

For IT project managers and engineers, please consider attending the CertNexus® *Certified Internet of Things (IoT) Practitioner (Exam ITP-110)* course.

You are encouraged to explore the Internet of Things further by actively participating in any of the social media forums set up by your instructor or training administrator through the **Social Media** tile on the CHOICE Course screen.



# Solutions

---

## ACTIVITY 1–1: Understanding Value, Insights, and Data

---

1. **A) Identify New/Incremental Value: What elements of value would be important to produce year-round, high-quality fresh flowers for Greene Organix's distributors?**

**A:** Answers may vary, but should include: cost, real-time availability, consistency and quality of product, freshness, unique varieties, year-round availability, longevity, and others.

2. **B) Understand Insights needed to support value: What information may be needed to drive down production costs so you can continue to deliver best-in-class flowers at improved competitive prices?**

**A:** Answers will vary, but should focus on specific ways to drive down operational costs. Information required for this goal might include: investigating the feasibility of introducing additional automation into the operational process.

3. **C) Data: What data do you need to collect to support these insights?**

**A:** A local area network could be implemented through cabled connections, such as Ethernet, although a wireless network would make it easier to relocate sensors as needed.

4. **Sensors — What useful information might an IoT device measure in this environment?**

**A:** Answers may vary, although a greenhouse operator might be interested in CO<sub>2</sub> levels, humidity, temperature, light exposure, soil moisture, nutrients concentration, airflow, plant imaging, and liquid level detection.

5. **Actuators — What actions might an IoT device need to perform in this environment?**

**A:** Actuators in a greenhouse environment might include CO<sub>2</sub> generators, air blowers and vents, irrigation pumps and valves, plenum or shade actuators, artificial lighting controls, heaters, and air conditioners.

6. **Other sources — What external data might be of use to support the insights?**

**A:** Answers may vary, but might include: weather data, material supplier data, logistics data, inventory data, and commodities market pricing information.

---

## ACTIVITY 1–2: Selecting an IoT Infrastructure

---

### 1. A) What would be a typical IoT Infrastructure setup for our greenhouses?

**A:** Answers will vary, but should include: Sensors, actuators, gateways, and connectivity between; remote connectivity for our gateway to communicate to the cloud; a process to configure (add, delete, and move) sensors and actuators within our solution (provisioning and tracking); the ability to supply power to sensors, actuators, and gateways; a remote user connectivity application; a cloud IoT platform to ingest all the data and a streaming analytics process to analyze the data; and access to external data sources (weather data, market commodities data, etc.) to merge with our collected data.

### 2. B) What are some constraints we may be dealing with within our greenhouse operation?

**A:** Answers will vary, but should include: the cost to implement and maintain (the incremental cost must be less than the incremental value created); security; remote locations of warehouses and extreme conditions where internal equipment may not be reliable; greenhouse sites may be too remote for Wi-Fi-based communications from the hub to the cloud (the solution might need to be cellular or satellite based); safety-related parameters that must be considered first, and possibly an extra layer of security for this data and control; any data that must be analyzed and processed locally to ensure rapid response and no reliance on remote network connection issues; and whether or not to limit the amount of data sent to the cloud (more data means more cost, both for transmission and for storage).

---

## ACTIVITY 1–3: Identifying Potential Challenges of IoT

---

### 1. A) Challenges — What challenges might your organization encounter in implementing an IoT solution?

**A:** The answer depends on the nature of the proposed implementation and unique challenges within the organization. However, several themes are common, such as cost and possible disruption to current operations. Because IoT implementations may lead to automation and changes in job responsibilities, there may be challenges related to change management, such as getting buy-in, retraining staff, updating documentation, and so on.

### 2. B) Countermeasures and Remediations — How might you address the challenges you identified?

**A:** Identifying what might go wrong is an important part of the design process. If you identify potential problems at the start of the project, you can design a solution that will prevent them from occurring. Various countermeasures and remediations to common IoT challenges are described throughout the remainder of this course.



---

## ACTIVITY 2–1: Using IoT to Solve Problems

---

### 1. How might IoT help Best Elevators increase customer loyalty?

**A:** If IoT can provide improvements in all of the other problem areas, then presumably customer satisfaction will increase, and customers will be less likely to explore competitive options. Also, implementing a *connected services* strategy will improve the customer experience, and will provide customers with a sense that Best Elevator is a trusted partner in their daily operations, which should also contribute to increased customer loyalty.

### 2. How might IoT help Best Elevators improve service maintenance and predictive maintenance?

**A:** Data collection from sensors combined with analytics can be used to inform Best Elevators and their customers when maintenance is required. Early-warning data and remote diagnostics would enable the organization to dispatch technicians promptly, ensuring they are equipped with the necessary information, tools, and parts to restore the equipment to safe operating conditions quickly.

### 3. How might IoT help Best Elevators manage spare parts inventory more efficiently?

**A:** IoT can be very helpful for keeping spare part inventories in warehouses and service vehicles stocked appropriately, which is normally a notoriously difficult task to manage cost-effectively. On the supply side, inventory can be tracked using typical IoT devices such as RFID tags. On the demand side, elevator equipment can be monitored and analyzed using data analytics and Best Elevators' own domain expertise to predict future needs. Combining historical data of part failure rates with analytic algorithms, Best Elevator can optimize their part stocks in the warehouse and technicians' service vehicles, reducing inventory costs and improving repair time.

### 4. How might IoT help Best Elevators improve product design and technician training?

**A:** Once IoT systems are in place, the system will be able to collect and analyze usage patterns and maintenance requirements over time. This information can be used to improve product design and technician training.

### 5. How might IoT help Best Elevators improve uptime and field service efficiency?

**A:** The solutions described in the previous questions will help improve uptime and field service efficiency.

### 6. How might IoT help Best Elevators allocate scarce service technicians more efficiently?

**A:** If product design, elevator uptime, and field service efficiency are improved (as described in the previous two answers), then this will reduce the demand on service technicians. Improvements in technician training should make technicians more efficient and effective.

### 7. How might IoT help Best Elevators communicate more effectively with suppliers?

**A:** Parts distributors and value-added resellers will also see additional opportunities to leverage the insight garnered from the IoT connected service solution. Best Elevator can share its experience and knowledge with its equipment manufacturers, creating a value-based competitive advantage in a market that is highly cost-driven with pricing volatility.

---

## ACTIVITY 2–2: Preparing for an IoT Initiative

---

### 1. What would need to be done next in this project?

**A:** Answers will vary, depending on the development methodologies your organization follows. You've already initiated the project and developed a system concept. There may be more planning to do, and requirements have not been completely identified yet. So it seems that the project is in the late planning stage. The next phase would be identifying requirements. Typically, before delving into design and development, the team would translate the general concept into formal requirements so all project stakeholders can agree on specifically what the project should accomplish.

### 2. What sorts of change management issues might arise as the company shifts from primarily selling physical goods to selling services?

**A:** Best Elevator is currently focused on manufacturing and maintenance operations. The new system will establish a new branch of operations focusing on software services. This will have some impact on staffing and organization structure. The payment model may change, as the company's orientation shifts from primarily selling physical goods to selling services. This will have numerous effects on the organization. You will also have some change management issues with customers. While many customers will welcome the improvements Best Elevator is proposing, some will be suspicious and may resist becoming more dependent on Best Elevator. You'll need to ensure that customers understand how the improvements will benefit them and their tenants, and may even save them money on maintenance costs. Planning the technical aspects of an IoT project is complex enough, but to ensure the success of the project you should also carefully consider the impact on personnel, contractors, customers, business operations, and the financial bottom line.

# Glossary

## **AI**

(artificial intelligence) The capability of a machine to imitate intelligent human behavior.

## **BI**

(business intelligence) Strategies and technologies used by enterprises for the analysis of business data, which transforms that data into useful information.

## **big data**

Data collections that are so large and complex that they are difficult for traditional database tools to manage. Businesses are often prompted to restructure their existing architecture to handle it.

## **C2**

(command and control) A set of organizational and technical attributes and processes that use human, physical, and information resources to solve problems and accomplish missions to achieve the goals of an organization or enterprise.

## **COM**

A standard for software components introduced by Microsoft in 1993, which provides a language-neutral way of implementing objects that can be used in environments different from the one in which they were created, even across machine boundaries, and which provides the basis for several other Microsoft technologies and frameworks.

## **connected services**

A service relationship between a customer and a product vendor made possible through network connections provided in the vendor's product.

## **constrained device**

A product that contains a processor whose capabilities are limited by low power usage requirements, low memory, low processor speed, compact size, and so forth.

## **CPAP**

(continuous positive airway pressure device) A machine that facilitates a patient's healthy breathing while sleeping.

## **CPS**

(cyber-physical systems) A system in which software (cyber) technologies model and control physical production equipment and processes.

## **crowdsourcing**

The act of outsourcing work and services to a group of people, such as an online community, who aren't internal employees of the organization.

## **data dashboard**

A visualization tool that provides users with a way to view key performance indicators and status for an enterprise.

## **DCS**

(distributed control system) A device used in industrial control that can control multiple manufacturing processes and

locations, perhaps performing the role of multiple PLCs and PCs.

**edge**

Refers to the boundary where the public Internet (the cloud) meets local networks and devices owned by customers.

**energy management**

Controlling how a device operates to conserve energy when it is not needed so it is available when it is needed—for example, putting a processor into sleep mode when there is no data for it to process.

**energy trading**

The buying, selling, and moving of bulk energy (electricity and natural gas) from where it is produced to where it is needed.

**IIoT**

(Industrial Internet of Things) The use of IIoT technologies to extend the traditional capabilities of industrial control systems. Also called Industry 4.0.

**IIoT**

(Internet of Things) A network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity that enables these things to connect and exchange data, integrate the physical world with computer-based systems that can use advanced techniques to process the data that is obtained, resulting in efficiency improvements, economic benefits, and reduced human exertions.

**IIoT client application**

An application that enables end users to view and analyze data obtained through IIoT devices, and control IIoT devices.

**IT**

(information technology) The use of computers to store, retrieve, transmit, and manipulate data or information.

**M2M**

(machine to machine) Communication between computers, embedded devices, or other machines.

**ML**

(machine learning) A subset of artificial intelligence that typically uses statistical techniques to enable computers to progressively improve performance on a specific task without being explicitly programmed.

**OLE**

(Object Linking and Embedding) A proprietary technology developed by Microsoft that allows embedding and linking to documents and other objects.

**OPC**

(Open Platform Communications) An industrial standard for interprocess communication initially based on Microsoft's standards for distributed computing.

**OT**

(operational technology) Hardware and software used to detect or cause changes in physical processes through direct monitoring and control of physical devices such as valves and pumps, typically used for industrial control. Often contrasted with IT (information technology) to point out technological and functional differences between two types of technology operations performed in businesses and manufacturing concerns.

**PAC**

(programmable automation controller) A type of industrial automation controller that combines attributes of a programmable logic controller and a personal computer.

**PLC**

(programmable logic controller) An industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity

that requires high reliability control and ease of programming and process fault diagnosis.

### **predictive maintenance**

Techniques that help determine the condition of in-service equipment in order to predict when maintenance should be performed, potentially saving costs over routine or time-based preventive maintenance because tasks are performed only when warranted.

### **prescriptive maintenance**

An approach to predictive maintenance in which required maintenance is predicted by systems, and a course of action is prescribed. Essentially, it is preventive maintenance with built-in intelligence.

### **preventive maintenance**

A statistical approach to periodic maintenance that requires maintenance at standard intervals, determined by the frequency with which parts have failed in the past.

### **proactive maintenance**

Any approach that attempts to schedule maintenance before a problem occurs, hopefully preventing a run to failure (RTF) situation.

### **RTF**

(run to failure) Waiting until a component fails before replacing it.

### **RTU**

(remote terminal unit) A microprocessor-controlled electronic device used in industrial control systems to monitor and control a remote asset.

### **SCADA**

(Supervisory Control and Data Acquisition) A control system architecture typically used in industrial, energy, and utility companies to support machine to machine communication.

### **SDLC**

A software development process that divides software development work into distinct phases to improve design, product management, and project management.

### **smart city**

A municipal area that uses various types of electronic data collection sensors and actuators to supply information used to manage assets and resources efficiently, and to control remote resources.

### **smart grid**

An electrical grid that includes a variety of operational and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficient resources.

### **smart pig**

An embedded device that can be sent into a pipeline to perform maintenance tasks such as cleaning or detecting leaks.

### **stack**

An implementation of a computer networking protocol suite or protocol family.

### **telematics**

Using telecommunications technology to monitor the location, movements, status, and behavior of a vehicle or fleet of vehicles.

### **telemetry**

An automated communications process by which measurements and other data are collected at remote or inaccessible points and transmitted to receiving equipment for monitoring.

### **thing**

In the context of IoT, an object that is network connected, includes an embedded processor, and may include sensors and actuators that interact with the physical world around the device.



# Index

## A

artificial intelligence [13](#)

## B

big data [13](#)

business benefits [19](#)

business challenges [19](#)

business considerations [19](#)

business intelligence  
definition [14](#)

business strategy steps [9](#)

## C

client applications  
definition [13](#)

cloud services  
overview [13](#)

COM [6](#)

command and control [5](#)

Component Object Model, *See* COM

connected services [50](#)

connectivity [7](#)

constrained devices [15](#)

continuous positive airway pressure, *See*  
CPAP

CPAP [42](#)

CPS [6](#)

crowdsourcing [4](#)

cyber-physical systems, *See* CPS

cybersecurity  
throughout IoT lifecycle [55](#)

## D

data dashboards [14](#)

DCS [28](#)

devices

examples [3](#)

overview [3](#)

things  
overview [3](#)

distributed control systems, *See* DCS

## E

edge [12](#)

enabling technologies [7](#)

energy management [40](#)

energy trading [40](#)

## G

gateway

smart home hubs [13](#)

gateways

overview [13](#)

global network [12](#)

## I

IIOT [6](#)

Industrial Internet of Things, *See* IIOT

industrial PC, *See* IPC

Industry 4.0 [6](#), [8](#)

information technology, *See* IT

infrastructure [12](#)

Internet of Things, *See* IoT

IoT

business goals [55](#)

- connected cars [38](#)
- energy and utilities [40](#)
- healthcare industry [42](#)
- in agriculture [46](#)
- in industry [35](#)
- in military [48](#)
- in retail [47](#)
- market sectors [32](#)
- overview [2](#)
- return on investment [55](#)
- smart buildings [36](#)
- supply chain management [44](#)

IoT development lifecycle [54](#)

IoT ingredients [2](#)

IoT projects  
complexity [54](#)

IPC [28](#)

IT  
definition [20](#)

## M

M2M [5](#)

machine learning [13](#)

machine to machine, *See* M2M

maintenance  
predictive [8](#)  
prescriptive [9](#)  
preventive [8](#)  
proactive [9](#)

miniaturization [7](#)

## O

Object Linking and Embedding, *See* OLE

OLE [6](#)

OPC [6](#)

Open Platform Communications, *See* OPC

operational technology, *See* OT

organizational skills impact [24](#)

OT [20](#)

## P

PACs [28](#)

PC [28](#)

personal computer, *See* PC

PLCs  
overview [27](#)

process automation [3](#)

programmable automation controllers, *See*  
PACs

programmable logic controllers, *See* PLCs

## R

remote control [3](#)

remote sensing [3](#)

remote terminal (or telemetry) units, *See*

RTUs

RTF [8](#)

RTUs [28](#)

run to failure, *See* RTF

## S

SCADA [5](#)

SDLC [54](#)

security challenges [22](#)

smart city [33](#)

smart grid [40](#)

smart outlet [26](#)

smart pig [40](#)

societal impact [23](#)

software layers [14](#)

software stacks [14](#)

Supervisory Control and Data Acquisition,  
*See* SCADA

system development life cycle, *See* SDLC

## T

technical challenges [20](#)

telematics [45](#)

telemetry [12](#)

## U

user interface [13](#)





CNX0004S rev 1.1  
ISBN-13 978-1-4246-3899-4  
ISBN-10 1-4246-3899-2

