The Internet of Things

What's it all about?

BILL POULSEN

The Internet of Things

What's It all About?

An Introduction to the Internet of Things by Bill Poulsen

First in a series of easy to understand explanations of various technologies and how they affect our everyday lives.

This book is based on a lifetime of experience as an engineer and entrepreneur using and developing technologies and solutions for multiple industries. The intent is to provide the reader with an overview and high-level understanding of a subject that allows them to intelligently discuss the topic in a social situation.

"To me, engineering projects are so much more than the technology. They represent the people and thousands of interactions between them that make a project successful. The innovation, collaboration and motivations of those people behind the effort are a tribute to society and mankind. That's why when I would see a Space Shuttle Launch or a fighter jet take off it would bring a tear to my eyes. Thousands of everyday people were behind those efforts, collectively creating something magnificent."

Bill Poulsen

Contents

The Internet of Things and How It's Changing Our Lives

The Internet of Things is fueling a revolution and that revolution is already upon us. As the Internet took the world by storm several decades ago and changed our lives forever by connecting people and breaking down communication barriers, the Internet of Things is now doing so for devices.

Billions of devices are already connected to the Internet and thousands more are being added each day. Soon they will affect everything we touch, do and engage with in our daily lives. Many of our homes, appliances, automobiles, and even ourselves are already connected to the IoT in one form or another. This advancement in technology is already helping to make our lives easier and will continue to do so for decades to come.

The vast number of connected devices are generally classified into two groups; *sensors* and *actuators*.

Sensors are devices that measure and detect what's happening in an environment. They check the status or condition of things in the world and provide quantitative measurements of parameters about those things. Think of these devices as substituting for a human's ability to sense touch, see, hear, taste and smell. Your "human" sensors are your ears, skin, taste buds, nose and eyes, and our inner ear which allows us to sense air pressure, acceleration, orientation and balance. Device sensors are temperature and humidity sensors, accelerometers, light sensors, cameras, motion detectors, sound level sensors, position sensors, switches and many others.

An example of a common sensor is the thermostat in your home that measures room temperature and communicates with your heating or cooling system, commanding those devices to turn on or shut off at specific temperature points. Other examples would be the IR motion detector in your home security system or the sensor in your smoke detector that monitors for signs of smoke or fire.

Actuators are things that move or do something physical. In human terms, think of the muscles that cause your arms and legs to move on command from your brain.

Examples of actuator devices might be the fan in your heating system that turns and moves the air throughout your home, or the mechanism that opens a gate at a parking garage after you pay. Another might be a valve in a nuclear power plant that opens remotely and allows liquid to flow and cool a reactor core to keep it from melting down.

So, we've mentioned sensors and actuators, is that all there is to it?

No, not hardly. There's much more to The Internet of Things, and it's all about data and being connected on a global scale. The power and value of IoT comes from the massive quantity of data available and the ability to analyze and utilize that data in a productive and immediate way.

IoT as a system

One of my favorite examples of a complete IoT system that many people are familiar with today is the SimpliSafe™ home security system. You hear it advertised frequently and it has become extremely popular.

This system consists of a central communications hub connected through the cellular phone system to the company's monitoring station. The various sensors you can purchase, such as key fobs, motion detectors, door and window sensors and others are wirelessly connected to the hub. Actuators, such as the alert siren are also wirelessly connected over a radio frequency link to the same communications hub.

Data is collected about the state of your system which contains the status of doors and windows, motion detectors and other sensors. The health of the system, such as battery levels, signal strength and quality of the cellular data connection is also monitored and reported.

When the alarm is triggered a wireless message is sent to the cellular hub in your home, which sends a message to the alert siren, causing it to activate. Then a message is sent over the cellular network and the internet to SimpliSafe's monitoring station. Depending on your subscription you will receive a call notifying you of the security breach or an alert on an app running on your smart phone. If that breach is confirmed, they then notify local police of the situation. In addition to receiving an alert, the app also allows you to monitor and control the system remotely from any location with cellular coverage.

The SimpliSafe™ security system is a great example of a widely deployed and practical IoT solution used by many people each day without ever giving thought to the Internet of Things.

Devices have been connected for decades, predominantly in factory and commercial settings. These devices were usually connected on closed networks, creating feedback loops that are used to control manufacturing processes within a system, building or complex. Thermostats have been controlling heating systems in homes for almost 100 years. Although comprised of a system of sensors and actuators, these examples alone are not the Internet of Things.

My first experience with the concept of IoT began long before the general population was using the Internet and personal computers were only on the desks of some of the most technologically advanced companies around. In the late 1980's I purchased a Commodore 64 computer. I could attach it to an early version of the internet using a cumbersome and slow modem connected through the phone lines. I belonged to an early Internet organization that allowed limited access into a variety of textual document files that were in the early stages of being digitized by many universities around the world. You could also get into IRC (Internet Relay Chat) rooms that allowed you to communicate in real time with others on the network. Some rudimentary email clients were also available and a few mail servers that allowed you to send and receive emails. We had none of the graphics, video or streaming video that we all take for granted today.

Eventually bored with the computer games of the day, I started thinking about ways to make the inexpensive and hobbyist focused C64 solve some real-world problems.

During that time-period energy prices were climbing exponentially, and electric utility companies were searching for ways to cut costs. A friend and I decided to attempt to design an automated electric meter reading system that we would eventually pitch to a large power company in New Jersey.

The system was simple, effective and could communicate back to a central point over an existing regional network (the telephone system). Data would be collected by sensors placed at each consumer's location to monitor energy usage and transmit that information to a C64 computer back at the energy company's office. This could now be accomplished without the need to periodically send someone out and physically read each meter.

The remote device was an optical sensor that could count the revolutions of the spinning aluminum disk still found in many electric utility meters connected to homes today. A digital counter would store that total, representing the energy consumed. The other part of the device was a touch tone encoder/decoder that generates and detects the tones used by the telecom system to connect to a phone number. The device was connected to the hardwire phone system at the customer's location.

The power company would collect the count using the C64 computer with a customized interface plugged into its game card slot. That interface contained the hardware needed to make calls and communicate using the phone system's touch tones. Controlled by a software application that we developed using the Commodore Basic programming language, the system could silently dial up the customer's location in the middle of the night and collect the count that represented the Kilowatt-Hour usage of the customer. In the time when everyone had a landline, there were attributes of the phone system that would allow our system

to dial a phone number, interrogate our device, collect the data and close the line well before the phone ever rang, thus our ability to collect the data without disturbing the customer.

The utility company now had a method to remotely monitor energy usage and use the data to automate and more accurately provide billing information. They quickly discovered that there was more to that data than they expected. Snapshots of average energy usage in near real-time could be gathered and analyzed to better manage the power grid and plan future infrastructure expansion or maintenance. This was arguably a first step in the direction of the Internet of Things using remote sensors and analytics, decades before anyone heard of IoT and only a few consumers had ever logged onto a personal computer.

My second exposure to the concept of the Internet of Things came years later, in the 2003 to 2005 timeframe, when passive RFID was first becoming a popular technology. Some smart people from MIT were talking about inexpensive and tiny RFID tags attached to every retail product distributed throughout the economy. The idea was that these tags could communicate with a network of interrogators placed throughout the supply chain and eventually in the consumer's hands. The benefit would start at the manufacturing plant where the item was produced and follow all the way to the customer and finally to disposal of the item. The items were identified as to not only what they were, but which unique one of those items it was. Every bottle of Coke would be identified as such, but also contain or reference information about which bottle was produced from which batch, even down to precisely when it was manufactured and perhaps even the source of the raw materials used to manufacture that batch. It could represent not only what kind of product it was, but also its specific DNA and history. This was a key difference between a simple barcode that identifies what something is, but

not its individual heritage and characteristics. An end user would be able to scan the tag and find out information about the life of that product, from cradle to grave. Customer feedback for items could occur easily to help improve products and product delivery, and even provide data not only about where the item was purchased, but where and when it was used. That data would be valuable to business in a myriad of ways, while customer satisfaction and participation in a product's lifecycle would create many benefits as well. Product recalls could be better managed, with improvements in both safety and costs. At the end of the product's life, you could trace the item to its point of recycle or disposal.

Manufacturers would gain valuable data, shippers would have better insight into the logistics flow, and customers would have more precise product information at their fingertips, all while improving efficiencies and having a positive effect on the environment.

The primary issues with the concept in that earlier timeframe had less to do with the RFID technology itself, but more to do with the data. Business had no clue at the time and many otherwise sensible projects were shelved because no one really knew how to handle that vast flow of data and how to utilize it in an effective manner. Today, those obstacles are no longer barriers to execution.

A few years back I commented to a colleague that I thought passive RFID tags would become the most prolific wireless sensors in the world. Today, that seems to be coming true, as thousands of internet-connected RFID interrogators are being added to an ever-growing infrastructure and millions of tags are being deployed in retail and logistics operations. Think of an RFID interrogator as a Wi-Fi hotspot for RFID tags, a gateway for

RFID tags to connect to the Internet of Things.

More Sensors

Earlier I introduced the idea of sensors, described by what sort of data they can monitor and collect. The simplest and least expensive sensor is an RFID tag, identifying an object and sensing where it is as a location or point in some process flow and connected to the internet via an interrogator. More costly and complex sensors exist that can connect to the internet through hardwire ethernet, Wi-Fi, cellular networks and satellite connections.

Most industrial and scientific sensors connected to the internet today are what I refer to as passive or "dumb" sensors. They measure some parameter and simply pass data over the network to a remote application that utilizes that data.

As hardware costs are dropping, some manufacturers have created smart sensors that can measure multiple parameter types. These sensors not only take measurements, but also autonomously process and make decisions about what to do with that combination of data before sending it. Low cost and low power consumption microcontrollers allow complex algorithms to be processed on the remote device, starting the task of analyzing that data right at the source. Some of these sensors can report data for years powered by a single battery.

A simple example would be a temperature and humidity sensor configured to only send data when those parameters exceed a certain limit. In-tolerance data may not be required on a regular basis, but an alert when that data is out of range is important. Sending only data when it is useful has the added advantages of conserving battery power and saving on data costs for cellular or satellite connected services.

An extension of this concept might be to send temperature data only when the *rate of change* of that data exceeds a threshold. This approach might alert that a temperature limit has not yet been exceeded but may be in danger of doing so. Based on the data the sensor has collected over time, it might also provide a probability percentage estimate of an out of tolerance condition occurring with a guess as to when that might happen. Although on a small scale, this could be considered predictive analytics happening right on the remote sensor. Extend that to thousands of smart sensors sending their individual predictions about temperature changes to a central point where that same sort of analysis could be performed over millions of data points. From that information you can envision some massively useful data trends being discovered that would allow action to be taken prior to a situation getting dangerous or out of control.

There are also fixed and mobile sensors. Fixed sensors may be permanently installed at a location and remain stationary. Mobile sensors can be installed on a moving vehicle or other conveyance, such as a shipping container, communicating through a cellular or satellite link and using GPS to monitor location.

As the cost of GPS hardware has decreased I have even seen a desire for fixed sensors to employ their own GPS receivers to automate the documenting of an installation's location, although that sensor may never be moved. For a fixed sensor which relies on knowing its exact installation location, consider that the cost of adding a GPS module to a device is about $10. The option of having that installation surveyed and identified might exceed many hundreds or even thousands of dollars. Go with the $10 GPS when you can.

Mobile and location aware sensors provide a host of other on-device intelligence possibilities. Devices that autonomously

know where they are can be configured to act differently and provide customized sets of data or alerts based on location and other measured parameters. The sensor could provide different data sets to different data endpoints or users. The manufacturer of a product being transported might get the data concerning temperature and humidity, while the logistics company doing the transport might only receive the location of the shipment as it progresses on its journey.

The concept that a sensor is self-aware of its surrounding environment and location and can be configured to act differently under various sets of conditions is extremely powerful. I believe that these types of intelligent sensors will become the next big leap forward for the Internet of Things. Taking that concept to its farthest point and adding appropriate actuators, you are now talking the technology you see depicted in the television shows Humans and West World. Much less of a stretch of the imagination than you might think.

The Sensor in Everyone's Hands

One massively prolific and intelligent sensor connected to the Internet of Things today is often overlooked. It is the iPhone, Android or other smart phone sitting in your pocket or purse. Perhaps one is in your hand right now and you are reading this from its screen.

This wirelessly connected device is filled with a myriad of built in sensors that include GPS, accelerometer, gyroscope, a camera, light, temperature and more. A device that almost everyone has in their pocket, continuously collecting data in the background wherever you are and reporting it over a cellular or Wi-Fi network to your cell company, Google or other app providers.

In addition to the sensors in your phone, the ability to download applications that run on the device and access these sensors provide an almost unlimited scope of capability. The fact that most everyone has one also provides the ability for companies like Google or Amazon to constantly monitor the location and activities of over a billion people and collect and analyze that data for various reasons on a real-time basis. Using machine learning and advanced predictive analytics allows these companies to essentially predict the future, knowing what you will do or purchase even before you know yourself.

Powering Sensors: Less is More

Many remote sensors have little or no access to external power or main lines. Some must be small, mobile and lightweight, perhaps even carried on your wrist, like a physical fitness watch used to track our workouts. Others may be placed in remote locations like in the desert or forest to measure and report environmental conditions. Or how about a space probe roaming around the surface of Mars for decades, the ultimate remote sensor?

Over the years, engineers have developed electronic components that require less voltage and less power to operate. IC's, semiconductors and microcontrollers with plenty of computing power and memory are available at low cost, making the prolific deployment of sensors possible and economically feasible.

Lithium-Ion batteries and small, inexpensive solar panels to provide power are commonplace and reliable. The combination of low power components and compact batteries has pushed the ability of sensors to be deployed forward at an accelerated pace.

The next step in powering sensors is the utilization of the electromagnetic energy already abundant in our environment from radio transmissions and AC power deployments to power our devices. This is called "Energy Harvesting", and the components to do so are becoming readily available with inexpensive development kits available for engineers to start integrating this technology into their new product designs.

The combination of low cost and low power components, along with the possibility of "free" harvested energy will surely help expand the deployment of sensors exponentially over the next

few years.

Actuators

Actuators are devices that do things. They provide the physical actions and indications needed to accomplish tasks in the physical world.

Actuators need special consideration, as some of them can cause dangerous conditions to occur if not properly controlled. The gate at a parking lot getting stuck or controlled improperly might cause you to get upset at not being able to exit a parking lot as quickly as you'd like, but the example of a remotely operated cooling valve at a nuclear power plant malfunctioning could conceivably cause a reactor meltdown.

Other actuators might be indicators like a traffic light or other warning sign, where improperly signaling can cause an accident and not just a traffic jam.

Large manufacturing machinery also contains mechanical actuators that are network connected, and improper control can cause not only financial impact on production, but also dangerous situations potentially resulting in death.

The security and reliability of controlling actuators must be taken into serious consideration before being deployed to ensure safe operation. And part of that security is ensuring that the data used to make decisions about how and when those devices operate is also secure and accurate.

Communications Protocols

There are several somewhat standardized communications protocols used in IoT, along with a myriad of custom protocols developed by individual companies.

Most communicate over some variant of TCP or UDP. Actual messages sent can be in the form of clear text, binary or encrypted and encoded information using various schemes.

MQTT, or Message Queued Telemetry Transport is a popular method. You can learn a lot more at www.mqtt.org.

MQTT It is a very lightweight protocol that lends itself well to battery powered and resource restricted devices. It can also be encrypted and password protected.

The concept is based on a relatively simple publisher-broker-subscriber structure.

This architecture allows sensors to send data to a single broker, where multiple devices or servers can subscribe to data flows from that broker. Think Twitter or Facebook here, where you can subscribe to data feeds from one or more sources or post your own tweets to those who subscribe to you. A one-to-many as well as a many-to-many relationship.

Connecting to the Internet

There are many ways to connect a device to the Internet of Things. Wireless devices using various protocols and RF frequencies are the most popular. Some examples are listed below.

Wi-Fi: Home, office and industrial

BlueTooth: Portable short-range connectivity to Smart Phones and BT Hubs

Cellular/GPRS/LTE: Mobile Cellular connectivity

Ethernet: Hardwired, usually in an industrial environment

ZigBee: Enhanced Bluetooth applications

LoRa: Long range radio link, indoors or outdoors

Mesh Networks: Self-healing and auto-expanding node to node communications

Satellite: Iridium, Orbcomm – Global connectivity where no cellular coverage exists

Data and Analytics

You have the data, now what?

Here is where it all gets interesting.

You can collect data from millions of sensors at locations around the world. The real value in IoT is in how you handle that data and what you do with it.

With so many sensors connected and so much data flowing, how you ingest that data and process it becomes critical.

Simply gathering that data in one location becomes a huge task. Old approaches to network data collection are slow and inefficient. Newer approaches such as utilizing a Hybrid/Lambda architecture are becoming popular because of their efficiency and ability to support an analytics approach. Systems like this can quickly store all the data and allow both immediate analysis in near real-time or post processing analysis for forensic and future research.

Assume the data is collected and available for analysis. A growing need is for data scientists that work at discovering new ways to analyze and correlate diverse data sources.

One area may be to utilize data and analytics to improve the efficiency of moving product across the global economy. Shipping containers could be fitted with sensors that both track the location and monitor the security of those goods throughout the shipping process. They may also report temperature, shock and other parameters associated with that shipment.

More than knowing where something is and what its condition is, it is valuable to be able to predict when a shipment will arrive at its destination. In addition to the sensor data, traffic data, weather data and even geo-political and crime data could be collectively used to accurately predict arrival times and safest routes, or even to adjust the travel route dynamically to optimize efficiency.

The possibilities are endless, and we are only beginning to utilize diverse data sources and machine learning to mine for not only data, but for unknown patterns in that data.

Data science and analytics is a growing and arguably the most important aspect of the Internet of things.

Security

Critical to any IoT system is security. There are several points in an IoT system where security is crucial to ensure safe and accurate operations.

Precautions must be taken to guarantee that data is protected both at rest (Data stored on a device or on a server) and in transit (Over the air, and over the internet).

Since the integrity of data is so important, we must work hard to ensure that it is authentic and accurate. Data can be used for nefarious purposes, so in addition to authentication, some form of encryption should be utilized throughout so that only the intended recipients of that data can have access to it.

In addition, systems should be protected against spoofing, where some third party may try to mimic a sensor on the network and send false data to your server.

Earlier I mentioned actuators, such as a valve used to control a process in a nuclear power plant. Protections must be implemented so that remotely controlled devices like this cannot be taken control of by any unauthorized actor.

Data Sharing

Data is critical to every decision we make every day of our lives. Some of that data may be current and received in real time, while other data may be historical and used to make judgements about a new situation.

Methods of sharing data need to be developed that can help society overall yet not take away our individual privacy.

The more we share data, the more valuable and useful that data becomes. At least I think so.

A concept that I have been working on is something like a Facebook for sensors.

In place of a profile for a person would be a profile describing a sensor and its location. "Friends" of that sensor would share in its data stream. Comments could be posted about the data which attest to the usefulness or reliability of that data. The person controlling that sensor could determine what parts of the data are shared and what are not, as well as to who that data is shared.

You could have several categories of sensor data providers. The hobbyist who sets up a backyard weather station, industrial participants, educational/universities, and government contributors.

This would make available great quantities of data for analysis.

As I see it, the sensors and flow of data will eventually become the commodity product, perhaps even given away free. The most valuable product of the Internet of Things will be the creative analytical algorithms and the applications that utilize those algorithms and data.

The Future of IoT

Although the concept of IoT has been around for decades, the real-world use of it is only in its infancy. The more data we collect and analyze allows us to discover new ways of using that data. As with anything, data can be used for good or evil purposes. And as always, technology out paces our ability to regulate and understand its implications in our lives. With platforms such as Facebook and Twitter we have already seen its effect on society. We need to keep a close eye on these things and make sure that we all understand how it works.

What does this mean to me?

Even now, IoT means many things for everyday life. The advent of security and remote security cameras has helped tremendously to identify and alleviate crime in many neighborhoods. Systems like Ring Door Bell, Simpli-Safe and others have very quickly advanced how millions of people handle home security.

Home appliances such as refrigerators and washing machines now connect to the manufacturer over the internet to report problems as well as allowing you to check on the contents of your refrigerator or status of your clothes from an app on your phone.

Products like the Nest™ thermostat allow you to control its settings from anywhere you have a cell connection.

As interesting as these applications are, they are only very basic and just touching the surface of possibilities.

Remote health monitoring is already becoming wide spread with the real possibility for the use of remotely controlled surgery becoming a near term reality. This could extend the care of skilled surgeons and doctors to places they could never be on an ongoing basis, like battle fields or other areas where skilled medical professionals may not be available.

The future of IoT is only limited by our imagination. We need the innovators of today to keep looking forward to bringing us the IoT of the future. The possibilities are great and can make our lives easier and potentially better.

Job Opportunities in IoT

The Internet of Things has created a whole world of opportunities for people with a background in technology. These jobs span the realm from business analysts, product managers to hardware engineers, programmers and data scientists.

Many of the jobs listed below are in high demand and pay well. These highlight just a few of the many available jobs in the industry.

Data Scientist: Analyzes data patterns and devises algorithms for machine learning programs

Programmer: Develops applications and user interfaces

Data Base Architect: Develops optimized data base structures

DevOps Experts: Develops and maintains operational systems

Data Security Experts: Creates secure environments for data collection and usage

Hardware Engineers: Designs the physical devices and sensors used to collect data

Embedded Systems Engineers: Designs the electronic sensor platforms and firmware to run on the sensors

Firmware Engineers: Writes the code that ruins on the devices

Product Managers: Develops and manages the product roadmaps for software applications and hardware devices

Systems Engineers: Architects the overall hardware/software system approach to a solution

Project Managers: Manage development and installation projects

There are many companies out there today working in the field of IoT who to provide innovative and useful solutions based on the underlying technology. Some of these have been around for years while others are new and in the startup phase.

They span the gap from sensors and hardware to software and analytics, as well as systems integrators.

Some of the most interesting are listed below.

Savi Technology: Provides analytics, sensors, tracking and asset solutions to the Department of Defense and commercial product manufacturers who need to monitor and secure their shipments on a global basis.

Orbcomm: Produces satellite-based asset tracking tags to monitor shipping containers on a global basis. They even launch their own satellites.

All Traffic Solutions: Provides traffic monitoring sensors, displays and analytics solutions to keep the flow of traffic running smoothly and safely on our roads.

Simply-Safe: Provides networked security systems for homes at a low cost.

Ring: Video and other security monitoring solutions for homes and business. The Ring Video Doorbell is their main product.

Impinj: Provides RFID hardware, tags and solutions to major industries for monitoring product flow throughout the supply chain and at retailers.

CalAmp: Manufactures a series of tracking and condition monitoring ruggedized sensors.

These are just a sample. Do a Google search on IoT and you will find many more, including all the large technology players such as IBM, Lockheed, General Electric and others.

Promote Tech Careers

Technology jobs are some of the highest paid and most interesting out there. Jobs in technology are currently in high demand and that demand is projected to increase into the future.

Try and get young people you know interested, especially girls. The first and best computer programmers were women. Today programming is a male dominated field. This needs to change.

There are many organizations that are tying to help. One that I know of that is doing great work getting girls interested in software engineering is called Boolean Girl. Please look for them on Facebook or at their website. https://booleangirl.org/

STEM, Science, Technology, Engineering and Math. Get the kids involved, it will be worth it for them.

Contact the Author

If you have any questions, thoughts or ideas about the Internet of Things, please contact Bill Poulsen via email at billrfid@gmail.com or on LinkedIn.

Learn More

If you are interested in learning more about IoT and DYI IoT projects, please check out our website at www.iot-techshop.com and join our Facebook group at https://www.facebook.com/groups/3188341227932417/