The Internet of Things

By Jim Daggon, senior product engineer of emerging technologies

The Internet of Things, or IoT, is one of the biggest emerging technologies in place today. We all know what the Internet is, but what are these "things?" Basically, they are any device that can connect to the Internet, usually using the TCP/IP network protocol for data transmission and/or exchange.

The IoT can be understood as the global connection of sensors and other devices to a hosted service and/or each other. However, this leaves a lot of room for interpretation and application. To make matters possibly more confusing, the Internet of Things is also known by another name: Industry 4.0. This term illustrates a change in the way machines can be utilized.

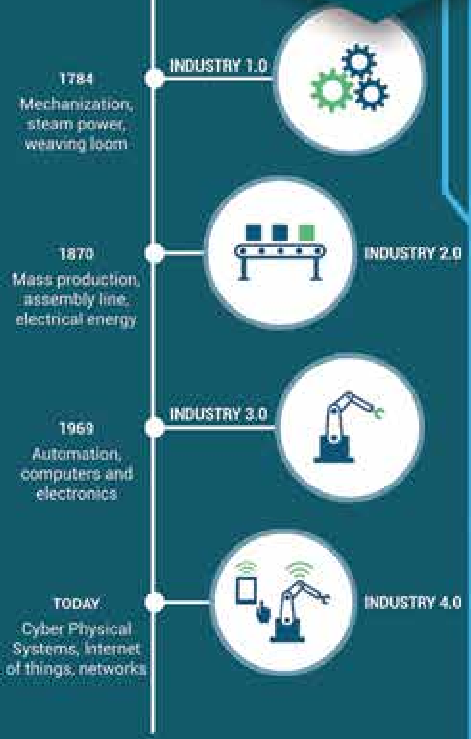
Here is the history behind the "4.0" part: Just as software increments a version number with each major release, industry has undergone major changes throughout recent history.

Industry 1.0 – There was a major influence on industry when James Watt invented the Watt steam engine. He introduced the concept of a separate condenser and rotary motion to the Newcomen steam engine, meaning a machine could now be harnessed to provide power for many different tasks that had previously needed to be accomplished by humans. A basic unit of power, the Watt, was named after him.

Industry 2.0 – Henry Ford originated the idea of a moving assembly line and the mass production of automobiles.

Industry 3.0 – Computerization of records, then calculations, diagnostics and operations.

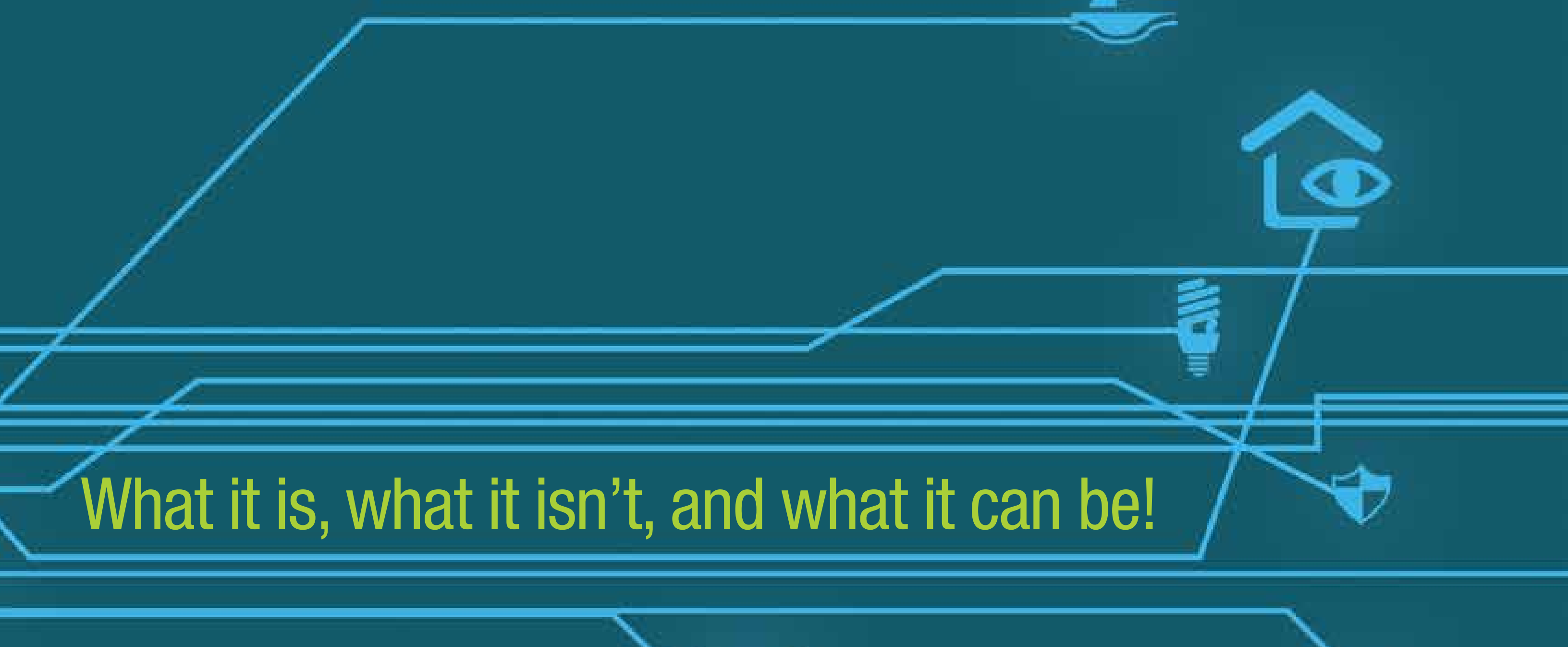
Industry 4.0 – Cyber and the Industrial Internet of Things. Now, machines are not only performing tasks, but also controlling one another and amassing data between themselves. In cases where deemed necessary, this occurs with no human intervention.


INDUSTRY 1.0
1784
Mechanization, steam power, weaving loom
INDUSTRY 2.0
1870
Mass production, assembly line, electrical energy
INDUSTRY 3.0
1969
Automation, computers and electronics
INDUSTRY 4.0
TODAY
Cyber Physical Systems, internet of things, networks

Although the advancement of technology has inspired dire predictions of gloom and doom—from the uprising of machines, to a singular super computer taking over the world and mankind (as seen in "The Matrix" and "Terminator"), this is not realistic (at least not in the foreseeable future). Rather, the Internet of Things has a goal of being able to collect sensor data from various sources, with the additional goal of making intelligent decisions based on the data. A simple example, which is actually in use today, is the use of a large network of sensors on a farm to collect the moisture and mineral content of the soil. Water is dispersed only where and when it is needed. Fertilization is customized to soil conditions and spread only where it is required. This type of technology usage will become more widespread as it increases efficiency and profitability.

According to SAP Systems, a provider of digital systems: The Internet of Things is not merely a step along the path to digital transformation; it is the driving force. By 2025, the IoT's economic impact could reach $11 trillion, or 11% of global economic value, and by 2030 the IoT could influence nearly the entire economy.

How did we get here? In the past 10 years, sensor costs have lowered to less than half of what they were, bandwidth (the ability to send data) costs are 1/40th of what they were and the cost of processing all that data has plummeted to 1/60th of what



What it is, what it isn't, and what it can be!

it was. This has created a perfect storm of technology to make this cost-effective and easy to implement. Many companies are spending massive amounts of money, time and resources to implement the IoT on, and for, their equipment.

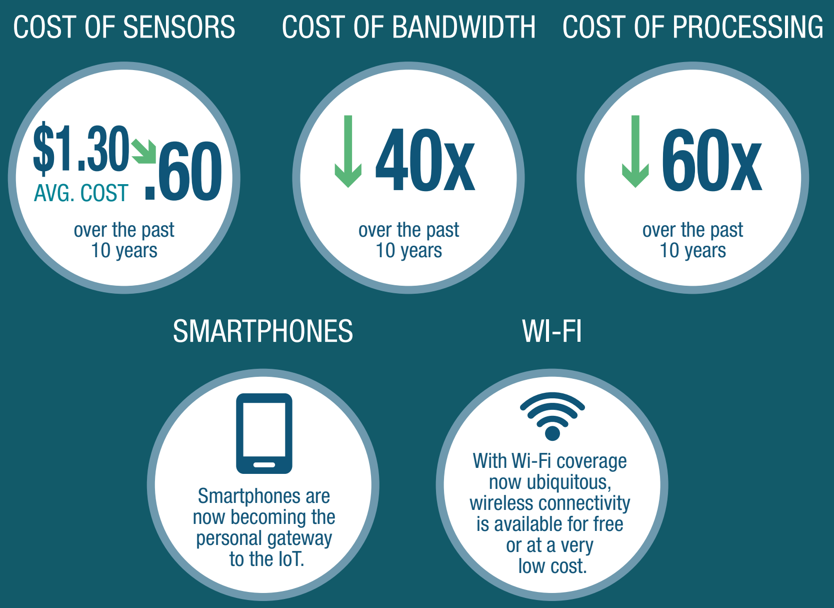
Although the Internet has been in existence for a while, the Internet of Things is relatively new. Total worldwide spending on the IoT is predicted to reach $1.29 trillion by 2020. That represents a compound annual growth rate of 15.6 percent over the 2015-2020 forecast period!

Much of that will go toward hardware (the largest spending category throughout the forecast), followed by services, software and connectivity. Hardware spending is estimated to approach $400 billion by 2020, the bulk of which is represented by modules and sensors that connect endpoints to networks.

But there is more to the IoT than sensors. These sensors need to be connected to the Internet in some way. Many of these sensors will be self-powered through batteries and wireless protocols such as Zigbee®, Bluetooth® and even Wi-Fi. The data will then be collected and, after the data is analyzed, there will be decisions made to control the systems that are being monitored. However, the latest concern is in the security of these systems that are connected to the Internet.

Implementing IoT

There are five areas that need to be addressed for a successful and beneficial IoT implementation. Let's look at each of these with respect to capabilities and some practical application.


COST OF SENSORS
$1.30 .60
AVG. COST
over the past 10 years
COST OF BANDWIDTH
40x
over the past 10 years
COST OF PROCESSING
60x
over the past 10 years
SMARTPHONES
Smartphones are now becoming the personal gateway to the IoT.
WI-FI
With Wi-Fi coverage now ubiquitous, wireless connectivity is available for free or at a very low cost.

Sensors

The capabilities of sensors have increased by orders of magnitude in the past few years and, due to new technologies such as MEMS (Micro Electro-Mechanical Systems), costs have been reduced dramatically. Although there are several sensors for determining weight such as resistive load cells, vibrating wire, piezo electric, tuning fork and force-restoration, today there are sensors for temperature, pressure, humidity, positioning, acceleration, direction, vibration, light intensity, level and fluid properties, just to name a few. Most of these sensors are easily integrated into systems using analog (or even digital) outputs. Accuracy is within a percent or two, if not greater, and mechanical mounting is simple with a clip, screw or even an adhesive mount. Connection to a high-tech programmable controller, such as the 1280 Enterprise™ Series allows the data to be collected and aggregated for decision-making.

Communication

The sensors involved in an IoT system need to communicate with the Internet in some way. This may involve wired, wireless or a combination of the two technologies. Since there are a number of technologies available, their individual strengths need to be considered.

The environment the sensor is exposed to needs to be taken into account. Temperature, humidity and exposure to outside conditions are factors. Can the communication be sent over wires from a fixed position? Does the sensor need to be mobile and still maintain connectivity? How critical is the timing of the information?

Continued on page 22

The Internet of Things continued from page 21

Security

This is an area that has been surprisingly overlooked in many implementations of an IoT solution. Even though there may only be a sensor transmitting information to a server over the Internet, there is still cause for concern. Any device connected to the Internet will be sending (and possibly receiving) data from one or more networks. This data is unencrypted, so it is readable by anyone that can get a connection. Rule number one for security on an IoT implementation (or any other connection to the internet) is: Never connect anything to the Internet without data security measures and encryption. This can be done relatively easily by using a VPN or firewall.

Data Aggregation

Once the data is being collected, then the decision has to be made regarding trends and how long to archive data. Much of this will be determined by the application and the goals set for that application. For instance, if the temperature of a tank is being monitored for out of tolerance high and low temperatures, then perhaps if the temperature stays within tolerance over the course of a month or two, the old data can be purged. If it goes out of tolerance a few times, the data should be kept to analyze the possible reasons why, and to correlate the temperature with other data to determine the cause. This is a big reason why IoT implementations fail (or succeed) to develop a return on investment (ROI): There is no preset goal or metric to collect the data in a way that allows the next section of IoT systems. Taking the time for setting goals and metrics before beginning an IoT solution will be time very well spent.

Decision making

You have the sensors in place, and the security in place. You are collecting data at a rapid rate and see some trends. What do you do about it? First, determine what decision you *can* make based on the data you have. The simple ones, such as temperature and humidity data can tell you if your process is taking those variables into effect (or if you need to). Does the temperature and humidity need to be controlled? Does the process need to be tweaked to account for these changes?

Now, think a step further—how about predictive maintenance? If the vibration of a motor is steadily increasing, at what point can/should the motor be rebuilt or replaced before it fails? Why is it drawing more power than usual? Should the filter in the heat exchanger be changed to allow the air to move more freely? Is the bearing in the motor failing? Is the load increasing for an unknown reason?

Here is where the true value of an IoT system becomes apparent. However, there are caveats. For instance, consider a warehouse that is mostly staffed with conveyors, robotic handlers and packaging-machines for shipments. Only a handful of personnel are there to monitor the system and correct problems that may arise. A network of strategically placed sensors with infra-red to detect people and control the lights/temperature are designed mostly for the benefit of the 15 human employees. The decisions made by the system are:

1) Keep the lights off, unless a person is in the area.

2) If a person is in the area, regulate the temperature to be between 65 and 80 degrees.

Sounds simple, right? Well, one day there are a few people sensed in the corner of the warehouse and the temperature is 93 degrees. The system turns on the lights in that corner and starts the air conditioning with the fan on low. Then, the system detects more people in the corner and the temperature is up to 104 degrees. The system turns on more lights and puts the air conditioner fan and cooling on high. There are now 35 people sensed in the corner and the temperature is now 128 degrees! The system now turns on more lights and puts the air conditioning on maximum.

Actually, there is a fire in the corner of the warehouse, no one is there, and we are fanning the flames with lots of cold, dense air! One of the first decisions in planning an Internet of Things, is to determine what decisions will be made autonomously and which decisions will require someone to get the information, verify whether something is abnormal and investigate. In this case, the fact that there were more people sensed than actual employees and the rapid rise of the temperature, despite the cooling system activation, should have activated an alarm.

In decision-making planning, all possible outcomes need to be addressed, even if it is simply "if *this* happens, then do *that*. However, if *this* is over a certain amount, then send an alert or shut down the process." ■

McKinsey Global Institute, The Internet of Things: Mapping the Value Beyond the Hype (McKinsey & Company, June 2015),

Danger lurks in the IoT

Security has become a major issue and is gaining visibility in the IoT. The need for Internet security has been known for years, with banks and other entities being "hacked" to get data. However, in the Internet of Things, now systems are being controlled based on data collected. Without the proper safeguards, the control can easily be taken over and in some cases, can result in serious damage to systems and even physical harm or death to people. A few steps that can be taken to provide additional security for the IoT include:

All IoT devices should be segmented into their own network and have access restricted using strong passwords containing at least seven characters (more is better) and use uppercase, lowercase, numbers and other characters (!@#$%^&*()_+=) in the same password.

Make it mandatory to change passwords on a regular basis! Do not allow the use of a previously used password. Although this may seem onerous to the users, it will provide additional protection even if one or more passwords are leaked.

If the data is only outbound and not inbound under any circumstances, at least implement a Virtual Private Network (VPN). This will add encryption to the data and require a secure sign in (hopefully using a strong password as noted above).

If the data is both inbound and outbound, a firewall should be required at both the sending network and the receiving network. This basically does what the name implies; it keeps out anyone without the previous allowed credentials. This additional level of security can be both software and hardware and is used as another level of protection when combined with a VPN and additional software such as anti-virus, anti-spam filters and anti-spyware.

Be sure your operating systems and other software is up to date with all the issued patches and updates. Many malware attacks are simply taking advantage of "holes" or vulnerabilities that have been discovered and patched, but if the patches have not been applied, then they are an open invitation to hackers. ■