MINTZ

Internet of Things Strategies for the Energy Sector

September 18, 2019 | Blog | By

VIEWPOINT TOPICS

- Sustainable Energy & Infrastructure

RELATED PRACTICES

- Technology, Communications & Media

RELATED INDUSTRIES

- Technology
- Energy & Sustainability
- Clean Tech / Renewables
- Artificial Intelligence

Whether thinking about managing oil and gas, water or other infrastructure facilities, or considering industrial efficiency, robotics and automation, you may be pondering how the Internet of Things (IoT) can be used to leverage resources. Forward thinking strategies include not just staying on top of regulatory changes that affect the IoT ecosystem, but also influencing them.

The Internet of Things involves the collection of data by sensors and other devices that is then sent to a processor for analysis and decision making. IoT is not a completely new concept in the energy sector, as systems for wireless automatic meter reading, obtaining tank measurements, tracking industrial assets, and Smart Grid monitoring have been in use for decades to manage and control systems. But today's IoT is now much more advanced and complex.

All Internet of Things systems have in common three aspects: 1) hardware, such as devices, sensors and tags, which collect the data, and perhaps communicate with each other; 2) networks, whether fiber, licensed 4G (and soon 5G) wireless networks, unlicensed technologies like Wi-Fi and Bluetooth, or even satellite; and 3) a means to process information for decision making and action, which can occur at the device level or in the Cloud.

What is new? Advances in chip technologies and lower chip costs now allow for faster, more powerful processing of larger amounts of collected data. Faster and more nimble wireless networks provide connectivity at greater speeds. And, advents in machine learning and other forms of artificial intelligence can analyze and process all this data in faster and more intelligent ways.

The one-two punch of processing + connectivity will allow for the proliferation of sensors and devices far beyond what we see now, all collecting more information and transmitting greater amounts of data. This raises concerns about issues such as privacy and the protection of the information (whether contained on the devices or sent over the networks), as well as potential cybersecurity risks to the devices and networks, to include unauthorized access and control. The growth of IoT also drives the need for more wireless spectrum.

What does this mean? Business decisions should consider cybersecurity risks – especially when building "critical infrastructure;" developing a supply chain that may include parts from China; or considering sales to the Federal government. Right now, industry best practices in network and device security are being developed by the Administration (led by the Departments of Homeland Security and Commerce). As part of a broad cybersecurity risk analysis, Federal agencies are focusing on managing the integrity of the U.S. supply chain to ensure that devices sold in the U.S. are manufactured with components that are "safe" from cyber risks. Proposals being considered for "best practices" may at best become de facto standards of conduct, or could even become law or regulation. If the business community wants to successfully self-regulate, it needs be a part of these discussions to shape policy.

At the Federal Communications Commission, new spectrum has and is being made available for IoT, and spectrum auctions are ongoing. One of the most important decisions in selecting IoT technology is the frequency band(s) on which it is deployed, especially considering whether it is licensed or unlicensed. Though the lines between these operations are becoming blurred (with some new technologies using both), there are important differences in operational control and performance that should be understood. Other important considerations include the type of network being used; the rules for siting wireless infrastructure; and the operating characteristics of a given frequency band.

One final important consideration relates to the use Artificial Intelligence in analyzing and using data collected, and in particular the risk that bias may pose to many companies. Biased predictions or decisions can occur intentionally or accidentally because of problems with data, the algorithm or both. While recent concerns relating to bias in AI concern credit or employment decisions, any company that relies on AI should understand the potential for bias in decisions being made with AI. While AI is not yet regulated, Congress has been holding hearings and considering legislation, raising the potential that at least some AI activity may be regulated in the future.

Keeping abreast of, and even participating in, the shaping of IoT policy in Washington, will help guide better business decisions, whether in risk analysis, due diligence, or the development of business plans.

Authors