1. Title: State of Industrial IoT 2017: Advances in Technology and Security

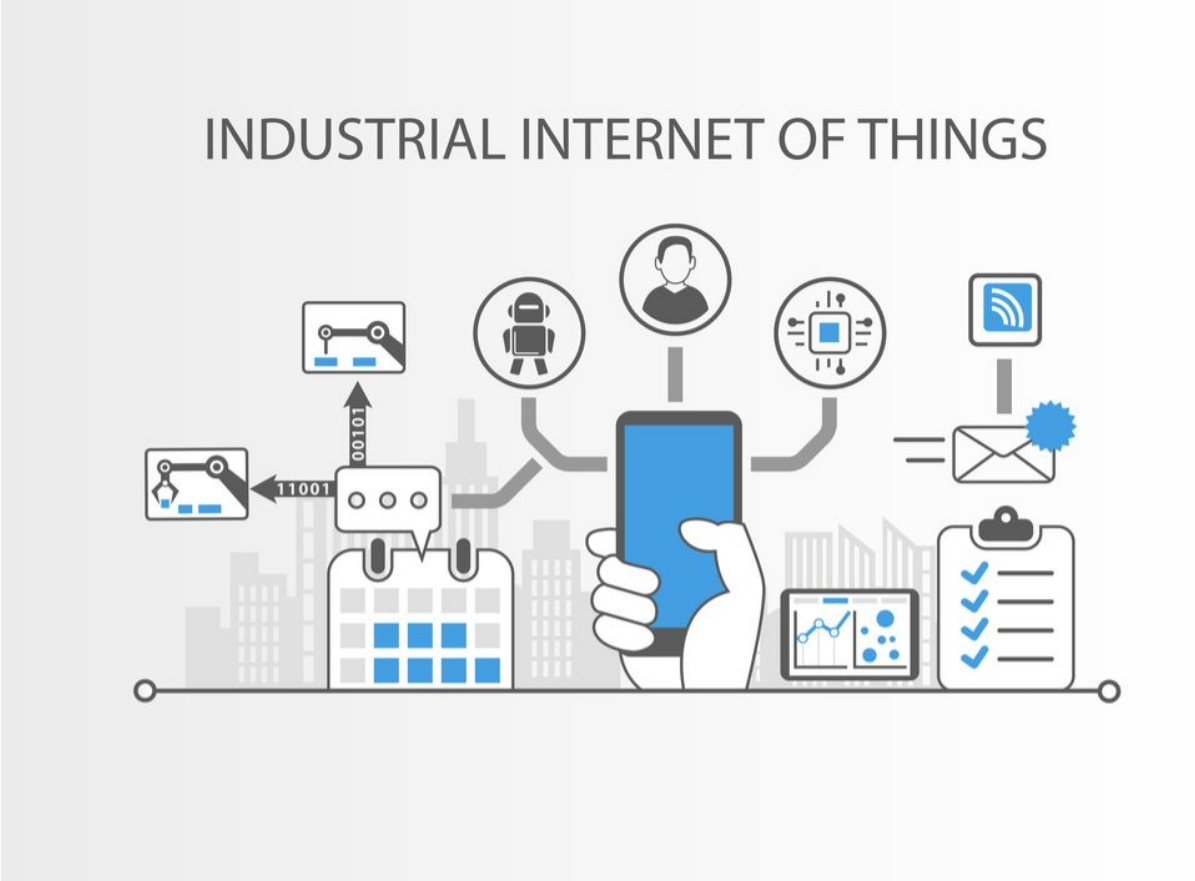
Subtitle: ***Where IIot is at and where it's headed***

2. Title: Advances in IIoT Technology and Security

Subtitle: ***State of IIoT with details on key developments in IIoT technology and security***

3. Title: IIoT 2017: Advances in IIoT Technology and Security

Subtitle: ***Details on innovations in IIoT devices, networks, and security***



"The IoT demands an extensive range of new technologies and skills that many organizations have yet to master. A recurring theme in the IoT space is the immaturity of technologies and services and of the vendors providing them. Architecting for this immaturity and managing the risk it creates will be a key challenge for organizations exploiting the IoT. In many technology areas, lack of skills will also pose significant challenges."

-- Nick Jones, VP Gartner

The industrial IoT landscape is complicated and confusing. A bewildering mix of IIoT service providers exists to provide everything from systems integration to custom IoT platforms that include security and analytics at every level. Network implementations run the gamut from wireless to cellular to NarrowBand IoT (NB-IoT).

Advances are being made in multiple areas, including improvements in IIoT devices, wide-area and short-range networks, and IoT operating systems. Data collection and analytics are also getting a lot of attention as IIoT engineers develop event stream processing and applications robust enough to handle the massive data some IIoT devices will generate. A general move toward standardization is also underway, to provide the interoperability and communications capabilities critical to IIoT systems.

However, IIoT networks present multiple security challenges. To be fair, security is improving, but it has a ways to go. Chip manufacturers have responded by developing IoT chips that integrate security at the hardware level, while the IIoT industry works on developing security protocols and standards that give organizations a consistent framework for developing their IIoT systems.

Join us as we explore in detail some key advances in IIoT technology and evaluate current IIoT security.

Improvements in IIoT Technology

Most new developments in IIoT technology fall into one of the following categories:

- IIoT processors
- IIoT device connectivity
- IIoT networks

IIoT has become far more complex than originally imagined. It is driven by multiple factors that include massive data collection. Processing that puts a strain on current technology. Hardware manufacturers and service providers are working hard to create the components necessary for efficient IIoT network operation and data processing.

IIoT Processors

IIoT device manufacturers have used off-the-shelf microcontrollers, but are finding them inadequate to device needs. Chip manufacturers have responded by developing IoT processors designed to work within specific categories of IoT devices. The categories break down something like this:

- **Smart Sensor --** A connected microcontroller with integrated analog interfaces for sensing.
- **Connected Audio and Video --** Provides processing and connectivity for audio and video devices.
- **High-performance Computing --** Provides processing and connectivity for devices that are used across a broad variety of processor-intensive applications, such as video analytics, automotive, and wearable technologies (AR headsets, proximity sensors, etc.).

The precise configuration of each chip is determined by factors that include IIoT device type, and the environment in which it will be used.

The chips developed for IIoT applications are being developed with hardware-level security, low energy consumption, and connectivity built into a single processor. The result is a robust, efficient processor that is future-proof and reliable.

IIoT Connectivity

IIoT connectivity is currently available in three fundamental ways: Bluetooth, low-power Wi-Fi, and low-power cellular. A host of protocols litters the connectivity landscape, making it a challenge to explore this area. Security and standardization are the two main areas of focus, each with its own challenges.

Security

IIoT system security needs to find ways to effectively block exploits aimed at vulnerabilities within each network type effectively. Some of these vulnerabilities, such as the Bluetooth vulnerability that allows a criminal to reboot security cameras, make it easy to break into a home undetected. While home

invasion is a serious crime, such a vulnerability can have disastrous results affecting large swaths of the population if successfully hacked in a power generation plant or other utility.

Standardization

Dozens of connectivity protocols exist. Getting even a few of them to work together toward a single standard is a major challenge. Competition between protocols and other factors have made standardization an uphill battle. One that will likely see difficulties for some time to come. While IIoT device manufacturers are building many protocols into their devices, the specifics vary widely from one manufacturer to another.

Wi-Fi

Conventional Wi-Fi consumes a lot of electricity. A new alternative, Low-power Wi-Fi (LP Wi-Fi) aims to reduce power consumption without any loss of capacity. Some LP Wi-Fi will operate in the 900MHz frequency range, with about double the range, and the ability to penetrate physical objects. This makes connectivity in industrial environments much easier than with current Wi-Fi, which has a limited ability to penetrate physical obstacles in the environment. Other improvements will include much-improved interoperability, government-grade security, and relatively easy setup. You will also be able to configure LP Wi-Fi networks to allow machine-to-machine (M2M) communications, an important factor in many manufacturing processes.

IIoT Networks

Two of the biggest challenges for the IIoT is capacity and security. Some IIoT devices generate massive amounts of data, placing a strain on the network as it struggles to handle the capacity. Both hardware and software need to be engineered to handle the enormous data transmission capacities required by some IIoT networks. Work in this area is making progress, albeit difficult. At the core of the challenges is the cloud-based, centralized IT model behind IIoT systems. Fog computing aims to change that by utilizing a distributed computing architecture that brings the benefits of the cloud closer to where data is generated and processed. This has huge implications for every IoT application from manufacturing to autonomous vehicles to healthcare, where the latency introduced by a round trip to the cloud-based server is eliminated.

To accomplish this, the fog layer mimics the cloud. It provides the computing capacity, storage, and networking at the edge while providing support for fast data processing. What is the “edge?” It is the optimal point in the network for managing data collection, processing, and analysis. But what about the security of all the IIoT technology that’s out there -- what’s happening with it?

[INSERT CTA]

IIoT Security

The single greatest challenge for IIoT is security. IIoT manufacturers are a mixed bag. Some emphasize security. Others take a more cavalier approach, producing devices with little, if any, security. Network security is an even bigger challenge.

“As industrial companies pursue IIoT, it’s important to understand the new threats that can impact critical operations. Greater connectivity with operational technology (OT) exposes operational teams to the types of attacks that IT teams are used to seeing, but with even higher stakes. The concern for a cyber attack is no longer focused on loss of data, but safety and availability. Consider an energy utility as

an example – cyber attacks could disrupt power supply for communities and potentially have impact to life and safety."

-- Robert Westervelt, Security Research Manager, IDC

Cyber threats are a serious issue that organizations cannot afford to take lightly. Most teams are acutely aware of IIoT security problems, but most lack the ability to detect and stop cyberattacks against IIoT systems. David Meltzer, CTO at Tripwire, says, "Either we change our level of preparation, or we experience the realization of these risks. The reality is that cyber attacks in the industrial space can have significant consequences in terms of safety and the availability of critical operations." What can you do to reduce your organization's IIoT security risks?

IIoT Security Risk Mitigation

To secure your IIoT systems, first, you need to perform a security risk assessment that identifies all possible attack vectors and assigns a risk level to each one. Create an IIoT security strategy that addresses each risk in order of priority.

Use the checklist below to help identify IIoT risks. Then prioritize based on your own risk assessment:

- Update/upgrade existing IT infrastructure and systems to take advantage of security improvements in both hardware and software
- Run IIoT networks through a firewall
- Actively monitor IIoT systems for unusual changes in network
- Secure network protocols as much as possible through the use of passwords and authorized user controls
- Closed ports are known to be in use by hackers (recently, port 445 for the WannaCry and other ransomware/malware)
- Use IIoT devices that have been hardened against exploitable memory
- Keep all software and firmware updated to the latest versions to benefit from the most recent security improvements

This list is only as a rough outline of what you will need to look for. Each IIoT environment will have many more factors to take into consideration.

Other than security, another major challenge is finding adequate IT talent.

IIoT Skills Shortage

"The internet of things is a multi-billion dollar industry and with it comes demand for employees with IoT skills. However, insufficient staffing and lack of expertise is hampering the IoT market..."

-- Sharon Florentine, Senior Writer for CIO magazine

Manufacturers are struggling to hire talent with the skill sets they need. Security, protocols, and microcontroller programming are among the top 10 skills in demand right now. On the IT side, organizations are having difficulty finding IT professionals with the skills and expertise necessary to manage IIoT systems. The solution may lie in tech companies partnering with colleges and universities to develop IIoT engineering and IIoT IT management programs to educate and train students.

A Peek at the Future of IIoT

The IIoT is still very young. A messy ferment of innovation and development are creating a heady mix of technologies, with some competing directly against each other. The frothy mix of IIoT service providers and their technologies will settle as smaller vendors are bought out by larger ones, and others fall out of sight.

We can expect standardization of the IIoT to continue, with standards that promote interoperability and simpler solutions. On the security front, we can look forward to more improvements in IIoT security at the connectivity and network levels as engineers find ways to improve hardware security. IoT-specific network protocols are also in the works to meet the unique needs of both consumer and industrial IoT.

It has become clear that the current operating systems in use are inadequate for IIoT applications. While operating systems designed specifically for IIoT applications are in the works, it is uncertain when they will be available for purchase.

The biggest challenges for IT departments will continue to be a severe shortage of adequately trained IT staff to work with the IIoT and its many complexities. Education and training must be increased to prepare IT staff for management of IIoT systems. Lacking adequate education and training, even the best IIoT systems will be left vulnerable to attack.