MSiTEC

CYBER SECURITY SOLUTIONS FOR SAFER IIOT INITIATIVES

HOW SAFE IS YOUR IIOT INITIATIVE FROM THE PUBLIC INTERNET?

WHITE PAPER

JANUARY 2019

MSI TEC, INC.

AUTHORS:

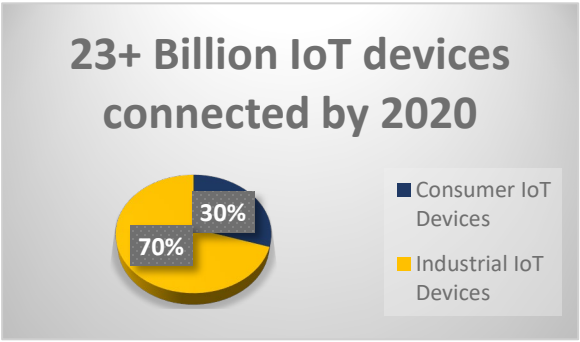
MIKE BARRETT
JAMES TURNER
BRIAN COSPER

INDUSTRIAL INTERNET OF THINGS

The age of the Industrial Internet of Things (IIoT) is upon us. It comes with a long and varied past, commonly referred to as Machine to Machine (M2M), Pervasive Computing, Industry 4.0, and many other buzzwords used across a wide range of industries. One thing is certain - the term IIoT is here to stay.

Cybersecurity is a growing concern in the Industrial IOT space and will continue to be at the forefront of discussions on the topic for decades to come. According to IT consulting firm, Gartner, there will be anywhere between 20 and 30 billion connected devices by 2020. Without a sound strategy for securing the connection and data transmission between these devices, we will find these installations with massive security vulnerabilities.

The myriad of options out there to address cybersecurity can be over whelming, and don't typically come at a reasonable entry point or with a clear path forward. In this white paper, we offer a strategy to reduce exposure to cyber security threats.



The Industrial Internet of Things (Industrial IoT or IIoT) is the application of IoT technology within the non-consumer physical world.

It ties together networked sensors and software with complex physical machinery.

It captures and analyzes data from machines (mostly in real-time).

It allows for remote control capabilities, deeper performance insights, operational optimization and efficiency.

DEVICE CONNECTIVITY CONUNDRUM

Most industrial devices were created without the capability or intent to be online, many created even before the invention of the internet. These devices lack basic network security features, such as firewalls, that we take for granted with modern devices like computers. Because of this, these devices are inherently insecure when installed in a network on their own.

Focusing on the Industrial Internet of Things (IIoT), we find ourselves connecting industrial devices such as PLC's (Programmable Logic Controllers), VFD's (Variable Frequency Drives), Industrial Controllers, HMI's (Human-Machine Interfaces), Industrial Edge Gateways to the public internet. These connections are being made in order to gather useful data from these industrial devices and send them to online analysis services from the industry giants like Azure IoT, AWS, IBM Bluemix, and the list goes on. There are also connections from these Industrial devices to online databases, MQTT brokers, OPC (Open Platform Communications) Servers, etc. These devices are also being used to connect directly to online SCADA software, again over the public internet.

With multiple devices connecting on the same network, they can be vulnerable to unauthorized access. Many industrial protocols weren't designed with internet security in mind and may not support encryption or user authentication.

Graphic by macrovector

WHAT ARE THE RISKS?

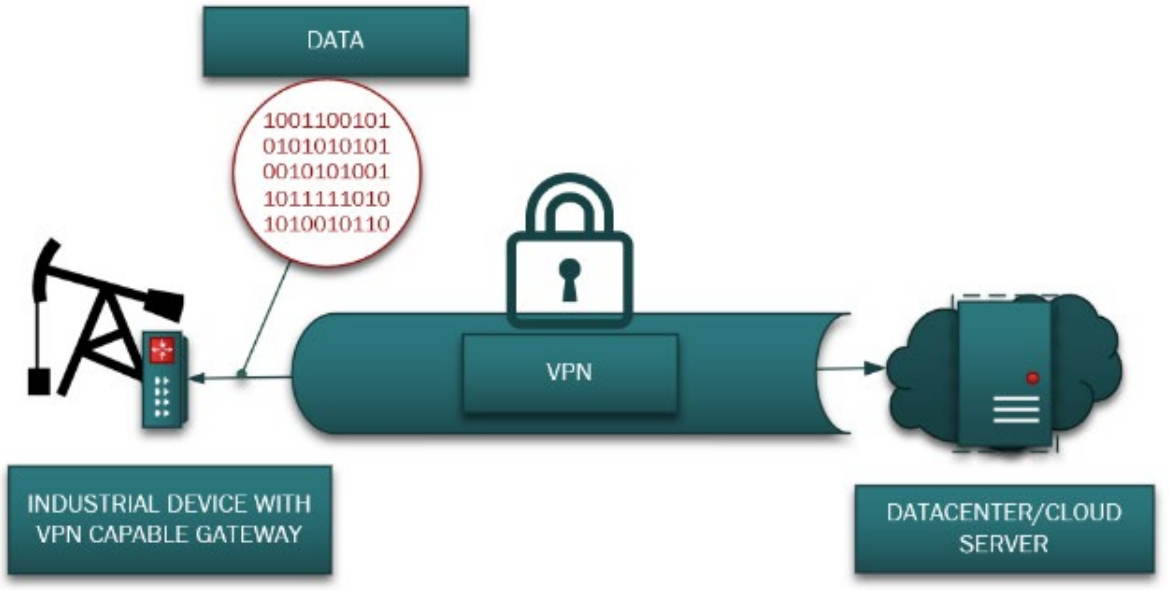
Most people think of IIoT cyber threats as attackers gaining unauthorized access to systems with the intent to steal data. But, it's much broader – and more serious – than that.

- DDOS (Denial of Service) attacks can take down the connection resulting in loss of data, or control of remote devices
- Botnets like Mirai can infect devices like industrial cellular modems, and send unsolicited traffic resulting in massive data overages, and fees.
- If the industrial devices are connected to business networks and are not secured, sensitive company data can be at risk.
- Unsecured Devices can serve as a mount point to launch attacks on other areas of the network, or even remote networks.
- Modbus/TCP being the most widely used industrial protocol, and typically using port 502, leaves a large opening for a potential hacker to get to for unwanted machine or device control, or data breach.

Critical infrastructure cyber attacks have increased by 24% in the past 3 years*. Whether it is wired or wireless, there are potential security risks across factory cells, zones, and fields.

*ICS-CERT

THE SOLUTION



Virtual Private Networks (VPNs) and specially designed hardware can be used to protect the network from unauthorized connections.

A Virtual Private Network (VPN) addresses most of the risks listed above. By connecting the industrial devices to an industrial edge gateway, or firewall/router with VPN technology available, a secure tunnel (using authentication and encryption) can be established between the devices and the applications. This could apply locally, in an application where industrial devices are connected to the business network, or remotely where the devices are reporting data back to a cloud service. A VPN uses a server/client architecture, offers authentication ("who is connecting") and encryption ("encoded/decoded data"). It provides a means to create secure communication on an untrusted network.

VPN solutions are just one strategy to create secure communication and mitigate the risk of attack. There are other strategies that we will cover in future material that explore cellular only connections, and how to secure those connections.

GLOSSARY OF TERMS

IIoT	The Industrial Internet of Things. Applying IT (networking and data-collection) practices from the commercial “Internet of Things” to industrial processes and machines.
Industry 4.0	The fourth industrial revolution (ongoing), focused on intelligent production, cloud technology, “big data” analytics, and machine learning to allow for cyber-physical systems.
SCADA	Supervisory Control And Data Acquisition. A high-level software application that monitors a process, machines, or systems in the field and displays relevant information to users. Commonly this application will also provide database/historian, alarming, and reporting functions.
MQTT	Message Queuing Telemetry Transport. A lightweight data protocol that uses publish/subscribe messaging with a broker, useful for sending data efficiently over cellular and low-bandwidth TCP/IP networks. It was first introduced in 1999 and is now an ISO standard, supported by many companies such as IBM for IoT applications.
VPN	Virtual Private Network. A VPN extends a private network across a public network (such as the internet) to allow for secure and encrypted communications. Commonly a VPN server will be cloud-hosted, and the endpoint in the field will be a VPN client. Applications such as OpenVPN allow for scalable deployment and management.
PLC	Programmable Logic Controller. The “brains” of a machine, programmed to perform logic functions based on physical inputs such as sensors, to perform actions with outputs to devices such as motors or valves.
HMI	Human-Machine Interface. This is commonly a touchscreen local on a machine, where a user monitors production and controls some process. It can also be a web browser or app interface to a remote SCADA system.
Data Concentrator	A device that connects a number of data channels with a similar destination. For example, instead of having 10 devices sitting in the same area all with their own cellular plans, you could point the 10 devices at a Data Concentrator, and have it manage sending a single outgoing message to a SCADA system.

RESOURCES:

Gartner, 2017, Leading the IoT, Gartner Insights on how to lead in a connected world

Moxa, 2018, The Industrial IoT is Here

ICS-CERT, 2018, https://ics-cert.us-cert.gov/

PR News Wire, 2016, The Internet of Things Hearlds New IT Service Opportunities

Gartner, 2017, The Industrial IoT Opportunity Infographic

eWon, 2018, https://ewon.biz/

FOR UPCOMING CLASSES, INDUSTRY NEWS, PRODUCT UPDATES & MORE,
SUBSCRIBE TO OUR MAILING LIST.

VISIT OUR WEBSITE: WWW.MSITEC.COM

SHOP ONLINE AT STORE.MSITEC.COM.

MSiTEC
PRODUCTIVITY THROUGH TECHNOLOGY

8925 E. NICHOLS AVE CENTENNIAL, CO 80112 720-875-9835

EMAIL: INFO@MSITEC.COM WEBSITE: WWW.MSITEC.COM