Developing a Secure Manufacturing Industrial Internet of Things (IIOT) Environment

Andres Castillo

ICTN 6823: Information Security Management

Department of Technology Systems

ICTN 6823 East Carolina University

Dr. Phil Lunsford

July 11, 2018

Abstract

Technology advances constantly and in the process of developing new ways to collect data, new security concerns become more prevalent. In order to increase profit, manufacturing requires increased efficiencies in processes and procedures, data collection is essential to the environment as a whole. It also provides valuable information for improving quality, time, maintenance plans, environmental data, as well as providing archived information for future evaluations. Developing a secured infrastructure is paramount to ensuring the companies data does not become susceptible to virus attacks, ransomware or fall into the wrong hands. Within this paper we will address intrusion and detection security for IIOT devices and developing a secure data strategy to address securing data collection points, securing hardware and transmission paths, as well as determining risk and providing solutions.

Introduction

Manufacturing environments have evolved over the years while maintaining legacy equipment, processes and procedures in order to continually provide essential products to the world. Established hardware, software and automation devices can be costly and making any type of change can have an effect in multiple areas as well as the bottom line. The one consistency regarding the world of manufacturing, is change. Change has brought about increased efficiencies with automation, maintenance, environmental controls and data collection. Increasingly, data collection remains a critical aspect of upholding consistent standards, with regards to product, developing preventative maintenance programs with predictive analytics, and documenting the manufacturing process flow from receiving commodities to distributing final product, using real time information.

Industrial Internet of Things (IIoT) is the latest enhancement in the world of technology, used to describe a process to increase data intelligence and decision-making performance. One aspect of IIoT was described in a paper written by Bart Winters and Francois Leclerc; "The IIot enables plant operators to improve process reliability by capturing and analyzing data, and then identifying the warning signs of potential issues – predicting when process adjustment and equipment maintenance are needed, and preemptively servicing installed assets before problems arise." Winters (2017) With new improvements, comes new challenges with regards to integrating security into legacy equipment and software, in addition to enhancing the data collection processes.

Knowledge is power, is an old saying, and in the manufacturing environment, millions of data bits containing knowledge used to ensure products are produced consistently, and in government regulated environments, the same data is retained and archived as a part of the history of the production process, data integrity is especially essential in the pharmaceutical manufacturing world. There are several levels of the production process from the Programmable Logic Controller (PLC) to the application software used to analyze input data and the data historian used as a library of the collected information. IIoT is the next generation of data collection, information gathering and decision making and involves securing each level which is just as important as the data collection itself, network communication, secured access to switches, rooms, collection devices, servers and applications.

Industrial Internet of Things

The predecessor to IIoT, is The Internet of Things (IoT) which is described by Dr. Mohsen Attaran in a paper submitted to ProQuest in the following way; "The Internet of things (IoT) is emerging as the third wave in the development of the internet. IoT interconnects

devices, people, environments, virtual objects and machines." Attaran (2017) Identifying the IoT in this way, naturally leads to the eventual addition of the term Industrial. Understanding the IIoT includes broadening the scope of hardware, data collection, and the incorporating of legacy equipment. Cheryl Rocheleau wrote an article as part of a consortium, quotes an article written by Travis Hessman entitled 'The Dawn of the Smart Factory", describing the additional devices within the "Industry"; "Today's Industrial Revolution is being powered by the Industrial IoT. What are these "things"? They are a jam-packed assembly of sensors and controllers, devices and embedded components, all talking to one another – interconnected, machine to machine, in real time – the entire factory moving and producing in harmony." Rocheleau (2016)

Another point of reference within the article provides a brief paragraph regarding legacy equipment, the simple summary, upgrade it. Working in large manufacturing environments, you will inevitably find some equipment decades old, still working because it is well maintained, these can sometimes present a roadblock to improvements. Companies who have developed these sensors, controllers and other such hardware have greatly improved their products over time and integrated technology to allow network connections, whether hard wired or wireless connections.

Although these improved devices provide increased functionality such as greater abilities to improve process control, manage decision making remotely, develop maintenance programs based and data analytics. Often times the challenge to improvements are costs associated required to improve still functioning equipment. With this understanding some companies have found ways to increase efficiencies by evolving current equipment into the current generation of technology. In turn, recognizing the need for improvements and enhancing current assets, allows industries to use a gradual approach as opposed to an all at once capital layout.

Cyber-attacks

The industrial world is under constant attack from external sources and at times, internal rogue individuals, with the easiest examples to provide are disgruntled employees, and careless individuals. Industrial automation has been around for decades and though it has been crucial in increasing efficiencies, securing the intelligence has not been priority. One of the more recent examples of an attack was seen in the pharmaceutical industry with the company Merck. The attack crippled the company during the global cyberattack involving the WannaCry along with NotPetya ransomware. Resulting in more than a week of lost production time of key life-saving vaccines, in addition to the financial loss to the tune of over $300m. The primary cause was due to an exploited vulnerability with the Microsoft operating system, a patch was made available to close the hole, but had not yet been applied, according to an article written for Dynamic Strategies; "Many of these attacks worked due to a vulnerability in the Microsoft Operating system that was fixed earlier this year!" Dynamic Strategies (2017)

An essential tool in the battle for a secured environment is awareness. Unfortunately, when top executives have separated themselves from the world of Information Technology (IT) and how it is intertwined in the everyday aspect of every major corporation. There becomes less of a sense of urgency to incur a major expense related to technology, especially when it is discovered the costs associated with upgrading, developing and instituting a secured environment. According to an article written for The Hill online magazine; "Cybersecurity needs to become a deeply ingrained part of every manufacturing company's culture – embedded in management decisions, workforce training, and investment calculations." Kota (2017) The article goes on to discuss how Cyberattacks are on the rise and major corporations are under attack daily.

The Stuxnet virus was the first publicized virus in 2010, to cause actual physical damage to an Iranian Nuclear Plant. The virus was transmitted through a USB drive brought in through a trusted support vendor changing the commands on a Programmable Logic Controller (PLC). Kim Zetter, writing for an online magazine "Wired" states this about Stuxnet; "Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment the computers controlled." Zetter (2014) This event truly brought the light to a previously unrealized possibility of cyber attacks and the reality of the potential damage it can cause.

Cyber Attacks continue to be steadily on the rise, countries, corporations, and nefarious individuals constantly explore various avenues to exploit, either for obtaining intelligence or obstructing advancements. Seeking vulnerabilities is a full-time job for many in the world and it is not just in one area or medium. One example highlights an article submitted to IEEE Xplore Digital Library, the authors describe developing a framework with 3 primary layers for any IIoT production environment, to defend against Distributed Denial of Service (DDoS) attacks. The authors identify 3 layers; edge computing level, fog computing level and cloud computing level, each level contains multiple points in conjunction with the various applications and or intelligence. Yan (2018)

Securing the Edge IoT Devices

As previously discussed, the purpose of developing the IIoT framework is to increase data collection efficiencies, automating intelligent decisions based on the generated information and integrating optimizing the multiple input devices. A paper developed for I-Scoop a consulting company based in Belgium, consolidates an excellent breakdown of IIoT into an overview, which provides a framework of understanding the benefits, case studies, approaches to

adapting an industry as well as architecture. The paper references a survey performed by Morgan Stanley identifying the top five challenges to IIoT adoption: "1) cybersecurity (46 percent), 2) lack of standardization (35 percent), 3) the legacy-installed base (34 percent), 4) significant upfront investments (30 percent) and 5) the mentioned lack of skilled workers (24 percent)." I-Scoop (2018) The survey identified cybersecurity as the number one concern, in turn understanding the associations with IIoT, various examples of vulnerabilities and identifying the multiple benefits to process improvement and data analytics, we now move towards examining an approach to securing the framework and related hardware.

As stated earlier, awareness is the first level of developing a secure IIoT infrastructure. As of late, the news constantly makes reference to the cyber-security, almost on an hourly basis. You would think by sheer volume, individuals would begin to understand how integrated security is (or should be) into a company's network. Passwords have become more complex and increased the frequency to change them and should no longer be written on a piece of paper stuck to the bottom of your keyboard or on the side of the computer screen, or in this case, taped on or around the Human Machine Interface (HMI) device. Educating individuals on this important first line of defense will go a long way in ease of access.

Supervisory Control and Data Acquisition (SCADA) and HMI devices control or manage the PLC's and other data generating devices and generally are software applications installed on a computer operating system (OS), most of the time a Microsoft OS. In legacy manufacturing environments, when these devices where first installed, they had a default password, which was never changed due to convenience. Many times, as upgrades occur, devices are joined to the domain and become a vulnerable point of entry. While considering default passwords the physical security or access to these devices are also point of concern. As described in an article

written for Industry Week magazine quoting a strategic innovation group at Cisco “Security needs to be embedded in all of our systems, in all of our infrastructure, in all of our software, and at the architectural level.” LaWell (2016) Integrating PLC, HMI’s and other devices into the network environment, consider placing the control centers in a secure room, or command center with badge access. Networking equipment in a large plant, provides increased accessibility to managing, while increasing the response time to events.

Securing the FOG

Developing a framework to integrate legacy systems in addition to the addition of IIoT hardware such as those categorized as FOG devices is the next level of communication. Fog computing is a term to describe a new level of intelligence processing. In most current environments, data generated from line sensors, generally travels from an edge switch to a core network switch or router, moves on to another switch then to a server, possibly residing in a cloud data center. Data generated, contains multiple points of information requiring decision making responses in order to initiate necessary adjustments to the production process. Saturating the bandwidth from point to point with massive amounts of information fighting for space along the network backbone. Margaret Rouse described Fog environments this way; “In a fog environment, the processing takes place in a data hub on a smart device, or in a smart router or gateway, thus reducing the amount of data sent to the cloud.” Rouse (2016) Intelligent responses occurring at the next hop as opposed to traveling back and from the cloud, increases efficiency and reduces bandwidth utilization.

Most manufacturing facilities struggle to find space for a secured network closet or cabinet, in turn switching equipment would become situated in open areas vulnerable to the elements as well as insecure open physical access. Establishing the Fog node, physical security

such as locked or badge entry doors, reduces the opportunity of plugging any harmful device into the network without accountability and developing an access policy with routine audits is part of Sarbanes Oxley (SOX) requirements. Developing trust relationships between edge devices and the intelligent device, is critical to establishing communication between physical entities. According to the OpenFog consortium, a blockchain-based security fabric is considered the most effective manner of securing the communication within the framework, as stated;

> "A blockchain-based security fabric comprehensively satisfies the challenging requirements of a global industrial IoT by promoting autonomous operation at all points. Because it's redundant, tamper-proof, heterogeneous, peer-to-peer and distributed, such a blockchain fabric provides the exact type of security needed to realize a truly powerful industrial IoT." Susanto (2018)

Blockchain security is also used in the cryptocurrency world, the concept is described in a journal written for the MIT Technology Review, "What makes this system theoretically tamperproof is two things: a cryptographic fingerprint unique to each block, and a "consensus protocol," the process by which the nodes in the network agree on shared history." Orcutt (2018) Blockchain security in an environment where devices are open and accessible, provides a sense of limiting access by ensuring only allowed nodes are allowed to communicate data.

Cloud Security

Within the IIoT design, Fog computing is the intermediate layer between IoT and the Cloud, as the endpoint of the data delivery. The cloud is the data center containing applications and hardware for data processing, maintaining and analysis. Within an organization is also the point requiring the most interaction, users local and global will have the ability to access, review, manipulate and develop production decisions based on the information stored in history. This level is very critical as it contains proprietary information to the manufacturing process, maintenance information, and archived data for future verification and validation. Security will

vary based on the type of environment and application models in place, such as Software as a Service (SAAS), Platform as a Service (PaaS) and Infrastructure as Service (IaaS) as described in a journal written by Xun Xu submitted to ScienceDirect online magazine. Xu (2012)

There are some basic essentials required to develop a security framework without degrading the transmission rates and maintaining accessibility while utilizing either a paid for service or transmitting over an internal Wide Area Network (WAN). Rahul Pangam identifies 7 best practices for securing your cloud service starting with transmitting with Data Encryption, proceeding to then develop a vulnerability testing schedule, moving next to define and enforce data deletion policies, adding protective layers with user-level data security, obtaining a virtual private cloud and network, and finally insisting on rigorous compliance certifications such as PCI DSS or SOC 2 Type II. Pangam (2017)

AES-256 encryption, considered a highly secure method of transmission over the network, provides a level of confidence between originator and receiver. Within the server file and folder structure, where the data remains, should use the same level of encryption, in addition securing the folders with security groups provides the ability to control and audit access. Security groups should require ownership by a few individuals who have authority to grant or deny access to the material. The data retention policy as well as the backup policy should be defined and strictly adhered to in order to maintain current and relevant information, these policies are especially relevant in a government regulated industry. Although some small companies who choose to utilize a cloud service, they need to insist on securing hardware and software specifically for their company and not to be shared, such as a database server. Requesting certifications such as PCI DSS, is required when maintaining and processing financial transactions and may not be required for all environments.

Larger corporations with the ability to develop their own data centers, an article written for Forbes magazine provides a couple of major concerns regarding cyberattack and performance and “For these reasons, enterprises running mission-critical applications with high-availability needs and compliance or regulatory requirements may want to think twice about using a public or shared cloud.” Lesser (2017) Although to maintain such an environment, requires obtaining the individuals with skill sets, background checks as well as the hardware software applications, developing support models, and ensuring security policies and procedures are enforced and maintained.

Conclusion

In conclusion, within this paper we developed an understanding of what IIoT is and how it can be utilized to increase production efficiencies, improve maintenance and assist in proactive maintenance. We identified how manufacturing environments with legacy equipment can still advance their equipment into an IIoT framework using a phased upgrade approach. Several examples were given as to the potential security vulnerabilities with recent cyberattack experiences, further enhancing the need to develop a secure environment. A breakdown into 3 layers and suggestions on how to address each, layers are identified as Edge IoT devices, the Fog and the Cloud.

Examples of edge devices otherwise known as IoT devices, are SCADAs, HMIs, sensors, and other endpoints transmitting and receiving data. These devices are the most vulnerable as they generally are in the open and susceptible to open access to the hardware. Securing the Fog devices such as switches, routers and intelligence processing devices placed close to the edge devices require trust relationships with the various data input hardware. The OpenFog consortium suggested using a Blockchain security model as the best practice, because it’s

redundant, tamper-proof, heterogeneous, peer-to-peer and distributed, it is also the same model used for Cryptocurrency. Finally, the Cloud security involves several key decisions regarding using a cloud service or developing an internal data center. Either way AES-256 encryption should be used to transmit and maintain data, incorporate vulnerability tests to reduce potential threats and cyberattacks. Overall individuals within the field of IT security, understand it is a never-ending battle, which requires diligence, maintenance, upgrades, patching, establishing policies, procedures and password protection, the challenge is there to be met head-on, do not shy away and make the world less secure!

References

Winters, Bart; Leclerc, Francois (2017) IIot & Process reliability: A Real-World Approach to the IIot for Process Reliability, Retrieved from, http://go.galegroup.com.jproxy.lib.ecu.edu/ps/i.do?p=SCIC&u=ncliveecu&id=GALE%7CA516541742&v=2.1&it=r&sid=summon

Attaran, Mohsen, PhD (2017) The Internet of Things: Limitless Opportunities for Business and Society, Retrieved from, https://search-proquest-com.jproxy.lib.ecu.edu/docview/1987683834?pq-origsite=summon

*Rocheleau, Cheryl (2016) Smart Factories: a Symphonic Example of the Industrial Internet in Action, Retrieved from, http://blog.iiconsortium.org/2016/04/smart-factories-a-symphonic-example-of-the-industrial-internet-in-action.html#_ftn1

Dynamic Strategies Staff (2017) Merck Cyber Attack and What You Should Know, Retrieved from, https://www.ds-inc.com/merck-cyber-attack-know/

Kota, Sridhar (2017), A Plan for defending US Manufacturers From Cyberattacks, Retrieved from, http://thehill.com/opinion/cybersecurity/356377-a-plan-for-defending-us-manufacturers-from-cyberattacks

Zetter, Kim (2014) An Unprecedented Look at Stuxnet, the World's First Digital Weapon, Retrieved from, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

*Yan, Qiao; Huang, Wenyao; Luo, Xupeng; Gong, Qingxiang; Yu, F. Richard (2018) Journal Paper; A Multi-Level DDoS Mitigation framework for the Industrial Internet of Things, Retrieved from, https://ieeexplore-ieee-org.jproxy.lib.ecu.edu/document/8291111/

I-Scoop Staff (2018) The Industrial Internet of Things (IIoT): the Business Guide to Industrial IoT, Retrieved from https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/

LaWell, Matt (2016) Manufacturing Cybersecurity in an IIoT World, Retrieved from, http://eds.a.ebscohost.com.jproxy.lib.ecu.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=a24a1429-f6ae-4a49-a1a4-ee7d22e8b564%40sessionmgr4010

Rouse, Margaret (2016) Fog Computing (fog networking, fogging) Retrieved from, https://internetofthingsagenda.techtarget.com/definition/fog-computing-fogging

Susanto Irwan, Xage (2018) Redesigning Security for Fog Computing with Blockchain, Retrieved from, https://www.openfogconsortium.org/redesigning-security-for-fog-computing-with-blockchain/

*Orcutt, Mike (2018) How Secure is Blockchain Really? Retrieved from, https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/

*Xu, Xun (2012) From Cloud Computing to Cloud Manufacturing, Retrieved from, https://ac.els-cdn.com/S0736584511000949/1-s2.0-S0736584511000949-

main.pdf?_tid=e9f85e90-1a7c-42a4-aa77-ac5f54ff53d8&acdnat=1531958686_9d05f8e1ca4a967e0f63421e8d74afb9

Pangam, Rahul (2017) 7 Best Practices for Securing Your Cloud Service, Retrieved from, https://www.csoonline.com/article/3184623/cloud-security/7-best-practices-for-securing-your-cloud-service.html

Lesser, Alex (2017) The Cloud vs. In-House Infrastructure: Deciding Which Is Best For Your Organization, Retrieved from https://www.forbes.com/sites/forbestechcouncil/2017/07/25/the-cloud-vs-in-house-infrastructure-deciding-which-is-best-for-your-organization/#1c56482b20f6