Manufacturing Network Strategy Considerations with Industrial Internet of Things (IIoT) and Fog Computing

Andres Castillo

ICTN 6885: Network Management Technology

Department of Technology Systems

ICTN 6880 East Carolina University

Dr. John Pickard

March 30, 2019

ABSTRACT

Manufacturing in today's world is changing from the standard methodology of communicating between devices. Due to the various levels of vulnerability and attack patterns, businesses require a more intricate evaluation of data patterns and application process flow. Introducing new technology and network configurations are necessary for creating increased efficiencies and security layers as a part of the overall network security plan. The Industrial Internet of Things (IIoT) is an additional layer within the environment, which introduces various new device end points, connecting to the wireless network and providing data used in the decision-making process.

In addition to IIoT devices, Fog computing is emerging as a method to reduce data traffic as well as decreasing network latency while increasing decision response time with regards to Programmable Logic Controllers (PLCs), and other data collection devices within the controller network, used during the manufacturing process. These devices are used to determine multiple responses dependent on the data input received from data sensors, PLCs or other data collection hardware. While integrating the latest developed technology appeals to those who monitor and manage the manufacturing process, there are several considerations to review as due diligence, in order to provide a safe, efficient and secure infrastructure.

This paper will discuss the benefits and challenges of developing an environment of IIoT and Fog computing within a manufacturing environment. Identifying security concerns to include attack points and defending against black hats in their quest to infiltrate or introduce damaging software. We will discuss benefits and concerns of establishing these new environments, as well as examples of attacks, their consequences and how to protect against such attacks. As a result, the paper will provide several considerations in the overall development of a layered manufacturing network.

INTRODUCTION

Networked environments within the manufacturing industries are some of the more difficult to upgrade or introduce new technology. Generally, in a majority of facilities, the production equipment used to produce product has been in service for well over a decade due to the high cost of replacement. As technology rapidly changes, vendors have been developing ways to integrate new technology with legacy applications and equipment. As a result, areas such as; automation, engineering, maintenance, and environmental controls are integrating into the 21st century applications and infrastructure. An article written for "Pharmaceutical Manufacturing" online magazine, sums up how businesses must change with the times while maintaining profitability; "the manufacturing industry is facing business challenges centered on improving performance of applications and infrastructure while controlling the cost of doing business." (Singit, 2015)

The Internet of Things (IoT) is a phrase used to identify any device connected to the Internet as described by an article in "Forbes" magazine "Simply put, this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other)." (Morgan, 2014) Incorporating the term IIoT into an industrial infrastructure opens a new specialized area of networking now phrased as Industrial Internet of Things (IIoT). Working in conjunction with ever changing technology, new areas of increased efficiencies are developed constantly within infrastructure, software, and hardware, Fog Computing is one example of optimizing automation. As the next phase of the industrial evolution continues to increase network presence, so does the need to develop a secure atmosphere to deter any wrong doers.

INDUSTRIAL INTERNET OF THINGS

As described earlier IoT is basically any device connected to the internet for example; cell phones, home appliances, OnStar, televisions or anything with an Internet Protocol (IP) address. IIoT goes a step further as a means to further define a specific subset of devices connected to an industrialized network as described in article written by Hugh Boyes;

> "The Industrial Internet of Things (Industrial IoT) is made up of a multitude of devices connected by communications software. The resulting systems, and even the individual devices that comprise it, can monitor, collect, exchange, analyze, and instantly act on information to intelligently change their behavior or their environment – all without human intervention." (Boyes, 2018)

By reducing human intervention, IIoT increases the efficiency of automated networks, while decreasing the overall human errors, latency issues and provides increased productivity.

Those who operate the manufacturing line will be enabled, with the help of IIoT infrastructure, to most importantly, analyze data, which will allow them to predict potential problems and respond proactively to address issues or perform maintenance. Within a production environment, IIoT can also be described physically as controllers, sensors, embedded components communicating in real time. Examples of potential IIoT devices are Programmable Logic Controllers (PLCs), which are devices used to read input signals from a source, then transmit information to a motor, valve or some other automated machine and these devices can be configured to automate the reactions of the connected device function. An article written for PharmTech.com "the Industrial Internet of things (IIoT), similarly, is a network of equipment with sensors that collect data in real time and communicate them to other machines or people using the cloud or internal company systems." (Markarian, 2016)

When considering IoT in comparison to IIoT, there are major differences as to the level of technical complexity within each area. IoT is represented by devices such as cell phones, kitchen appliances, TV's or any other wirelessly connected device. IoT devices are created primarily for end user convenience, where, due to the market competition, it is better to get product on the shelf as quickly as possible, rather than to ensure it meets certain communication and security standards. The approach taken for IIoT devices address several aspects of how the device communicates, security, reliability, adaptiveness and data analytics. Manufacturing plants are slow to progress when it comes to the rapid change and growth of technology, due in part, to major impacts financially and on production.

The image below reflects a typical illustration of an IIoT environment, there are physically and wirelessly connected devices communicating across network infrastructure. Data is transmitted from end devices such as PLC's within the production network which is collected and managed in SCADA configuration and then interfaced by external mobile devices, computers or other devices, in order to analyze the data.

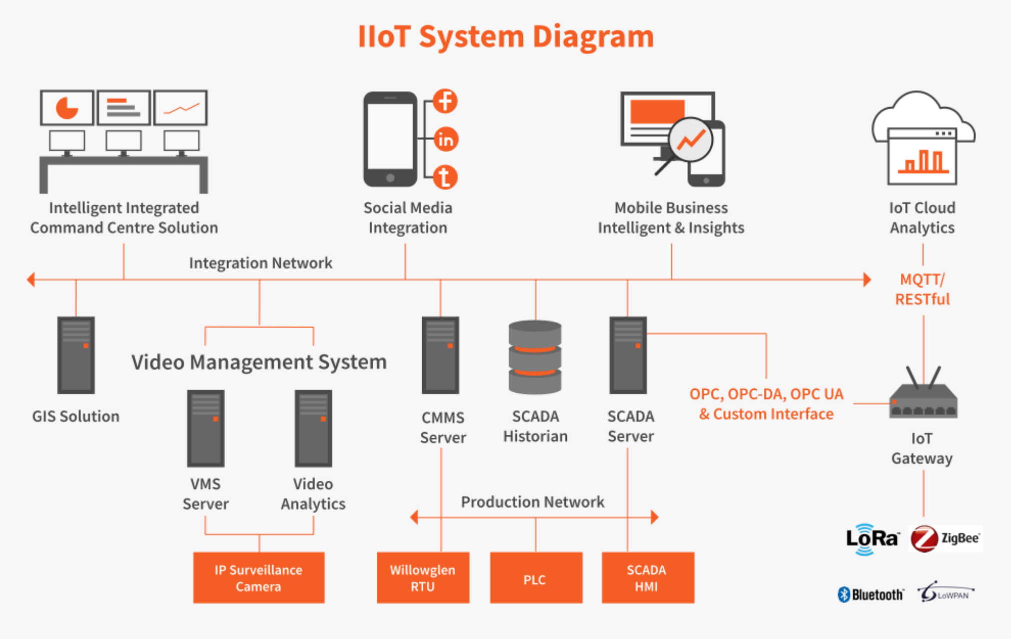


Image retrieved from: https://www.willowglen.com.my/product-and-service/iiot

With reference to factories legacy equipment, a paper written by Cheryl Rocheleau relates the approach of developing a smart factory to composing a symphony. She provides four movements; Becoming a Good Listener, Second Movement: Retrofitting – Ode to Joy, Third movement: Recognizing the Benefits, and the Fourth Movement: The Power of collaboration. Within the second movement, she describes the approach to legacy systems; "Today, sensor technology costs have decreased to the point where operations of every size have the means to revamp, upgrade, retrofit, and prepare for digital automation. The process to becoming a Smart Factory is a journey." (Rocheleau, 2016)

Assisting in the integration of the vast amounts of legacy systems currently in production, an organization was developed called OneM2M, working in conjunction with several partners to establish standards for the Internet of Things as well as the Industrial Internet of Things. An excerpt from their website: "The purpose and goal of oneM2M is develop technical specifications which address the need for a common M2M service layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices I the field with M2M application servers worldwide." (OneM2M, 2018) An IoT architect named Peter Niblett reinforces the need for standardization and recognizes OneM2M's agenda:

> "OneM2M's platform provides a security architecture to ensure the trustworthy, safe and secure handling of the data collected or processed by these IIoT devices – which is particularly important within industrial environments, where security

> glitches, could present safety concerns that have never been contemplated before, with a breach potentially resulting in a life-threatening situation" (Niblett, 2018)

The need to develop and maintain standards are paramount to any area of technology, without providing that type of consistency would not only fall into chaos, but would also become a costly adventure. Integrating devices relating to Fog Computing and IIoT require an understanding of each and how they will provide the required enhancements.

FOG COMPUTING

Companies around the world both large and small are constantly seeking out ways to improve the bottom line especially in the area of technology and the high costs associated with building infrastructure. Information technology and the associated computing power has been decades in the making primarily with large corporations leading the way in first developing their own data centers along with the required support staff. Businesses also began to realize the need to incorporate into the budget, the ever-changing improvements to hardware technology. Increased processing power and data storage space have become essential for any business to develop an efficient baseline to support the business needs.

The Greek philosopher Plato once said that "Necessity is the mother of invention" which rings true especially in the area of Info Tech. The Internet and the ability to create Wide Area Networks (WAN) through Internet Service Providers (ISPs), provided opportunity for the development of off-site server rooms or data center facilities while transmitting over secured connections between sites. New industries were birthed and are able to provide to some extent, a relief to industries growing hardware, application and software needs, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) in addition to supported hardware redundancies.

In order to understand the concept of Fog Computing, it is necessary to first understand the concept of Cloud Computing. Global and domestically wide spread companies found ways to reduce infrastructure costs by centralizing access to data centers through Cloud Computing. Cloud computing offers businesses the access to scalable resources, increased processing power and in some cases, reduces hardware support costs. Eric Knorr wrote an article for "InfoWorld" magazine with his interpretation, "more precise meaning of cloud computing: The virtualization and central management of data center resources as software-defined pools." (Knorr, 2017)

Centralized Data Centers are increasingly becoming the standard for major industries such as pharmaceutical manufacturing. The ability to centralize access to applications globally using virtualized or hardware servers improved the bottom line in reducing the need to license and maintain the same application and hardware at different plants around the world. Reduced costs in licensing, hardware, infrastructure support, application support as well as improving the overall customer experience. Corporations can return to focusing on their primary business and not becoming mini IT companies as well. From personal experience, when the CEO of a major pharmaceutical corporation was once asked why the manufacturing plant was experiencing issues with regard to support, his response was, "We are not an IT company, so I can't answer that" Businesses are moving out of a local data center and towards the centralized model to reduce the redundant models around the world.

The image below provides an example of a centralized data center:

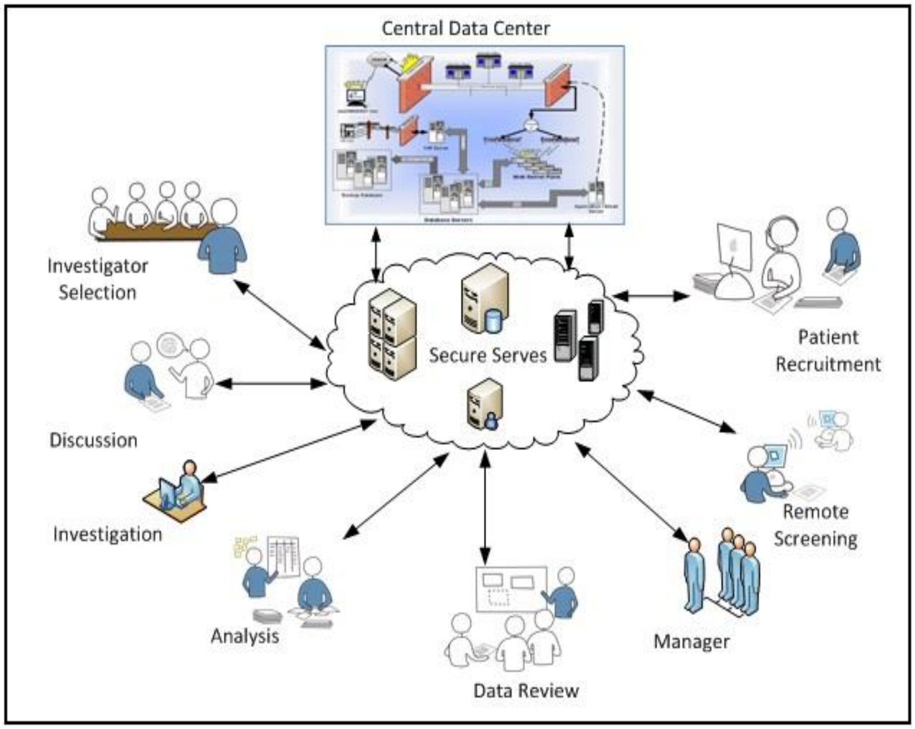


Image retrieved from: http://www.pharmamanufacturing.com/assets/Media/2015/1510/PM1511-CloudComputing-Small.jpg

Although utilizing data centers continues to be a viable centralized data solution, manufacturing is one industry where reducing latency and increasing the ability to process commands more efficiently requires less access to data centers for certain functions. Fog Computing is gaining ground along with IoT and IIoT within various applications from wireless connections on the highway monitoring traffic patterns to the world of manufacturing. The term Fog Computing is a reference to changing the infrastructure paradigm from Cloud computing, which is sending data to data center over Wide Area Network (WAN) connection, to bringing the processing of data closer to the ground. A paper covering the topic of Fog Computing and security, provides the following description: “As Fog Computing is implemented at the edge of the network, it provides low latency, location awareness and improves quality-of-services (QoS) for streaming and real time applications. Typical examples include industrial automation, transportation and networks of sensors and actuators.” (Stoimenovic, 2015)

Jakub Pizon and Jerzy Lipski wrote an article for “Applied Science” which provided the following description: “Fog computing is a highly virtualized platform that provides compute, storage, and networking services between end devices and the traditional Cloud Computing data centers, typically, but not exclusively located at the edge of the network.” (Pizon) 2016 As shown in the previous quotes, Fog computing is primarily focusing on developing an efficient methodology for computing collected data into decision making activities and developing data analytics.

As a result, another new organization was created so that method of standardizing the new-found technology, the new organization is called OpenFog Consortium. The consortium consists of originating members; Cisco, Dell, Intel, Microsoft, ARM and Princeton University. The website for the consortium provides this definition: “fog computing is a system-level horizontal architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from the Cloud of Things.” (Consortium, 2017) The group of members continually work to improve the technology as it rapidly becomes integrated into businesses around the world.

PLC’s and other endpoint devices constantly process input and respond according to pre-configured instructions. Within standard infrastructure, data is transmitted through the network to multiple devices, the WAN and eventually to a data center where the servers will process and store the data and, in some cases, provide response actions. With considerations to legacy systems, the “Journal of Manufacturing Systems” published an article addressing this concern; “From a hardware perspective, there exists a continued lack of affordable sensing technologies that can be readily integrated into both legacy and modern manufacturing systems.” (Wu, 2017) The need to increase efficient response times and overcome latency issues due to the number of devices throughout the data path is addressed by Fog Computing.

Latency issues occur when data is initiated from a point on the network and due to various circumstances, such as a switch not possessing enough processing power to handle the multitude of inputs, causes a delay the receiving of the data on the other end. Another side effect could be data loss, which in some industries, can cause a loss of product, due to lack of evidence the product was manufactured within standards. Reducing the data path by placing an intelligent device as part of the infrastructure closest to the data input device addresses this concern as described by Margaret Rouse “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)

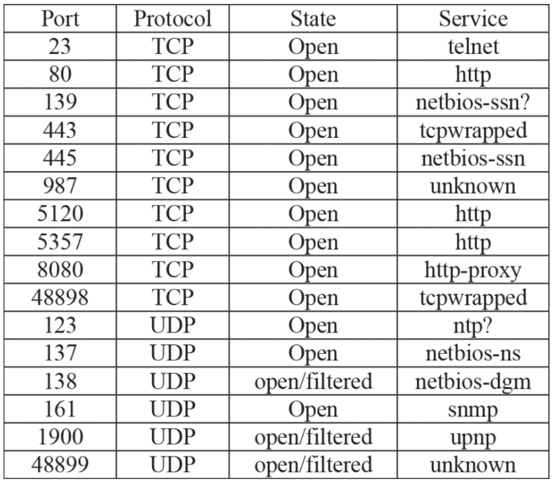
MANUFACTURING NETWORK INFRASTRUCTURE

Within manufacturing facilities most everything is on the same network with little to separate the overall traffic on a flat network, thus creating the challenges of traffic patterns and high latency issues. Separating automation traffic from day to day business traffic is the first step in developing a more efficient infrastructure. Unfortunately developing a separate physical network is costly, creating a new infrastructure with cabling, switches, core redundancies and disaster recovery plans is an expensive endeavor. The next question is what is the cost of production loss due to a network issue that could have been prevented by having a separate environment?

A separate physical network connecting only the automation network is preferred and if possible is necessary for controlling the type of traffic allowed. Consider separating the network into a minimum of 3 layers of communication; Business network, Control (or manufacturing) network, and Wide Area network (WAN). To provide greater distinction, divide the subnets in such a way as to make it easier to separate during time of troubleshooting. For example, the business IPv4 network can use 10.x.x.x, the manufacturing network can use 192.168.x.x and the WAN can use 172.x.x.x or if using IPv6 use fe80, fd00 or fc00 respectively. When designating the subnets, be sure to provide for growth.

Introducing a firewall to the physical and virtual infrastructure, with a Demilitarized Zone (DMZ) to create separate traffic, allowing only certain paths between the 2 (or more) zones, will greatly reduce over saturated data traffic. The authors of an article written for "Industrial Control Networks" states: "Any equipment that requires communication with both the business and industrial networks is placed between the two firewalls, within the DMZ." (Galloway, 2013) Although this will create additional administrative tasks, it will also provide for a more secure and efficient data flow.

Separating the data traffic physically and/or virtually, is the first step to developing a secure manufacturing network, protecting the network is a continuous process. As default there are standard ports open on every system, access to the internet (port 80) should be strictly controlled as it provides the greatest vulnerability to the engineering\automation network. Although there are applications requiring access to the vendor's website to download patch updates for security, it must be restricted with firewall settings allowing access to certain ports on the site only and with restricted times. A paper written to identify certain security concerns conducted a port security analysis on a typical PLC and the following results were documented as open shown on the graph below (Bonney, 2015):



Port	Protocol	State	Service
23	TCP	Open	telnet
80	TCP	Open	http
139	TCP	Open	netbios-ssn?
443	TCP	Open	tcpwrapped
445	TCP	Open	netbios-ssn
987	TCP	Open	unknown
5120	TCP	Open	http
5357	TCP	Open	http
8080	TCP	Open	http-proxy
48898	TCP	Open	tcpwrapped
123	UDP	Open	ntp?
137	UDP	Open	netbios-ns
138	UDP	open/filtered	netbios-dgm
161	UDP	Open	snmp
1900	UDP	open/filtered	upnp
48899	UDP	open/filtered	unknown

Table 1: Port Scanning Result Source: ICS/SCADA security analysis of a Beckhoff CX5020 PLC

As shown, the graph reflects several open TCP/UDP ports, not all ports are high risk, but identifying the potential vulnerabilities should be every administrator's priority, then reduce the risk as much as possible.

By physically or virtually separating the manufacturing network, the possibility of interference is greatly reduced as well as reducing the number of dropped packets between devices. Data historians are a major contributor, data is received and archived and used to develop an audit trail of the manufacturing process. By maintaining two separate servers, one on the business side and the second on the manufacturing network, will reduce the bandwidth utilization of those who are reviewing or querying the data and forecasting future decisions. Response times from the device to the historian, become much more efficient, in turn, reducing possible product loss due to inaccurate or incomplete information.

Implementing IIoT and Fog computing within the infrastructure will require vendor input in determining the compatibility of legacy systems. Certain systems may only connect using legacy connection speeds of 10-megabyte (10mb) and half duplex and still run on Category 3 (Cat3) cable or Category 5 (Cat5) cable. Cat3 can only connect at 10mb speeds and Cat5 can connect up to 100mb, both will need to upgrade to a minimum of Cat5e, the lowest category for minimum 1gigabit (1gb) connection speed. When determining the cost of upgrading equipment to incorporate them into the network with an IIoT connection, be sure to consider the current infrastructure and whether it will be compatible with the newer hardware.

LOGIN CREDENTIALS

As with any planning for the addition of or upgrade to a current environment, Security should always be a part of the planning. The world is constantly under attack over the network, whether by an individual, group or nation, someone is always looking for ways to infiltrate any system possible. Within this section we will cover; Passwords, Control systems, Fog Computing devices, Infrastructure and IIoT considerations.

Passwords are considered the first line of defense with any form of security administration, it is the fastest way to access any device by know the default login credentials. Over the last few years, the news has constantly reported of another breach into some major corporation, through a cyber-attack, Phishing or using default login credentials. In years past, users were less concerned about security and would keep a written copy under the keyboard, taped to the front of the monitor or in an unlocked drawer. As businesses large, medium and small continue to hear about and see the repercussions of poor ID management, they realize it’s not just that simple anymore to allow users to keep the same default password.

Security policies have become more prevalent and establishing strict adherence to required characters, password length, as well as how frequent the passwords must be changed. These can be controlled on a network domain with enforced policies, but for those devices not authenticating to the domain, it is necessary to take additional steps for securing devices such as PLC’s, Human Machine Interfaces (HMI) and Supervisory Control and Data Acquisition (SCADA) devices. Most devices on the network came with default credentials for the initial configuration and had never been updated, changing the login and password should be the first step in the process. As stressed in an article written for the Cisco Strategic Innovation group “Security needs to embedded in all of our systems, in all of our infrastructure, in all of our software, and at the architectural level." (LaWell, 2016) As a side note, when firmware or software has been updated on these devices, verify the ID and Password have not reverted back to default.

ANTI-VIRUS

As discussed previously, IIoT is any device placed on an Industrial Network, to include PC's, HMIs and SCADA that access wirelessly. A book called; *Plant IT: Integrating Information Technology into Automated Manufacturing*, tackles the question of putting Anti-Virus (AV) on a manufacturing PC and the answer is "yes", then followed with "However, if the applications involve real-time control or guaranteed response times, such as HMIs, DCS systems, or PC-based control systems, then the answer is not so easy." (Brandl, 2012) Although every effort should be made to hard cable devices, there are instances where there are physical constraints which prevent wired and are replaced with wireless access.

The book also references a study performed by the National Institute of Standards and Technology (NIST) and Sandia National Laboratories, under the guidance and sponsorship of the Department of Energy's Office of Electricity Delivery and Energy Reliability and it's National SCADA Test Bed (NSTB) program. The study reviewed how Anti-Virus software affected the performance levels of a SCADA device, here are the major findings:

1. Manual scanning, also known as "on-demand" scanning, has a major effect on control processes, in that they take CPU time needed by the control process (sometimes close to 100% of the CPU time). Minimizing the antivirus software throttle setting lessens, but does not remove this effect.
2. Active scanning, also known as "on-access" scanning, has little or no effect on control processes.
3. Signature updates can also take up to 100% of CPU time, but for a much shorter length of time than a typical manual scanning process.
   (Brandl, 2012)

The conclusion of the test reflects yes, based on the processing power of the SCADA or HMI, AV does have an effect on data transmitted from a PLC. When either device is wireless that will add an additional layer of complexity, possibly hindering the data collection. PLC's can collect data many times every second, in some cases up to 100 times per second. In those cases, dropped packets will cause gaps in the data analytics and require an investigation.

FOG COMPUTING SECURITY

As stated previously, Fog Computing is bringing the power to make decisions closer to the data input device or moving from the cloud closer to the ground/device. Cisco is primarily related to Fog Computing Gateway (FCG) as they took part in coining the phrase. Examples of Fog Computing devices are devices acting as Gateways dividing the Edge device and the rest of the network, in turn providing an additional layer of security. One aspect of security is the ability to remove personally identifiable information before sending the data across the local area network (LAN).

In a manufacturing environment removing some of the data prior to transmitting across the LAN and WAN reduces traffic and vice versa, reduced traffic and controlled access on the Control side of the FCG. The FCG also provides another layer of authentication within the infrastructure which would reduce compromising data collection devices. Also, by implementing an FCG, data collection devices on the Control network would not be affected by a business network outage, as they would continue to communicate from PLC to SCADA devices. By using encryption, the FCG can also secure communications between the network and the Control network and in the event one FCG is hacked, the others will continue to operate, thereby reducing the outage impact to just a few devices. As a side note, by physically separating the FCG from the rest of the network, users no longer have the ability to easily obtain ALL the accumulated metadata which may be necessary for investigations.

Another aspect of considering the implementation of a Fog Computing Gateway, it is necessary to remember that it is also a physical device and should be located in a secure location. Although edge devices are generally in the open, the cabling connecting to the FCG, can extend into a network closet or secure access room. This will ensure controlled access to the device and reduce the possibility of a bad character gaining easy access and causing damage to the process. Reducing physical exposure as well as potential electromagnetic interference is only one part of the security process when introducing new hardware.

IIOT SECURITY

Within large manufacturing facilities, it is easy to find legacy equipment, some are decades old yet the still work due in part to the craftsmanship as well as scheduled maintenance. Over time the vendors who created these devices conducted research, trial and error in developing the next level device. Keeping up with the latest trends in order to integrate into the paperless and wireless society, developing new products either to replace or enhance current hardware. Companies as a whole agree the need for improvements are a constant anywhere in a plant, to add to the project planning is to add security to the project as well.

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 the number one concern as Cybersecurity, which is definitely the buzzword of the day, at work, in the news and social media all have stories of negative cyber activity. Working from the control network, devices such as PLC's, temperature gauges, SCADA's and HMI's should all operate in as secure environment as possible. Access should be restricted by application login credentials, PC domain credentials, physical location and if possible, badge access to the room. The objective is to provide security from as points of view as possible, while maintaining Cybersecurity as the primary concern.

CYBER ATTACKS AND SOLUTIONS

As previously discussed, Cybersecurity is essential when developing any type of a networked infrastructure. Daily, there are news events identifying another breach of security, whether it was someone who fell prey to a fishing attack, or man in the middle or any number of scenarios. It is paramount for users and businesses to be aware of the potential vulnerabilities, especially when the virus may be installed by someone who was thought to be trustworthy, such as the case of the first Stuxnet virus.

Within the Penn State College of engineering website, a document presents the details of the first virus attack causing actual physical damage to a nuclear power plant in Iran. The paper is called "Real world example: Stuxnet Worm" and it lays out the scenario of how the nuclear facility called Natanz was infiltrated by the worm. (Daniels, 2016) The breakdown goes as follows; Unknowingly a Siemens technician used a Universal Serial Bus (USB) to transfer code from a PC within the Siemens plant in order to perform standard maintenance at the Natanz nuclear plant.

When the person plugged the USB into the module it immediately activated the worm to install and take control of specific devices the Siemens SIMATIC WinCC/Step 7 controller software. Only when the worm found the specific software did it activate otherwise it would lie dormant. The worm caused significant damage to the centrifuges at the plant, essentially incapacitating the facility. According to the paper, the worm has affected over 70,000 hosts worldwide, with over 60,000 in Iran alone. It is believed this work was created by a government and is identified as the first casualty of cyberwarfare.

From the example above, we understand the need for defending against any outside (or inside) attack is paramount to protecting the business environment. In the Stuxnet example several precautionary procedures would have helped to identify and or prevent the worm. To prevent unauthorized access, USB can either be disabled or use locking devices which can be installed on every open USB port. As a precaution, require the vendor to use an encrypted USB drive previously scanned with Anti-Virus software. Next prior to installing the USB into the PLC, the local site must have a safe PC used to scan any incoming devices, this PC would be disconnected from the network. Not every attack will cause physical damage, primarily attacks will involve data, websites, Malware, Denial of service attacks or Application specific attacks.

Understanding the multiple network layers of a manufacturing environment, such as the business layer, Manufacturing layer and Control Layer, each should involve a firewall to segregate the traffic. In addition, each layer of firewalls along include an Intrusion detection\Intrusion Prevention (IDS\IPS) systems to be used for preventing attackers from drilling down to the Control layer. As improvements are made and new technology is incorporated, each Information Technology dept need to take the additional steps to research the latest strategies to secure their companies infrastructure, both physical and virtual.

CONCLUSION

In conclusion, we identified and defined IIoT and Fog Computing and how they integrate into a manufacturing environment. During the discussion, we covered some of the benefits and challenges with integrating legacy systems into an upgraded network infrastructure. A recommended layout of establishing a Business layer, Manufacturing layer and Control layer network, which allows for greater control, distribution of network management and security. Some examples were provided of particular cyber attacks as well as suggested defensive measures. Overall introducing newer technology into a manufacturing facility, requires research, knowledge of the environment and planning in order to provide a secure and high performing solution. As every IT person should be aware, no environment is 100% protected from attacks or always the best performing, it is a constant battle, but definitely one worth working towards.

REFERENCES

Singit, Raju and Murthy, Sridhar (2015) Cloud Computing in Pharma, quote and image Retrieved from http://www.pharmamanufacturing.com/articles/2015/cloud-computing-in-pharma/

Morgan, Jacob (2014) A Simple Explanation of 'The Internet of Things', Retrieved from https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#64066d9a1d09

Boyes, Hugh; Hallaq, Bil; Cunningham, Joe; Watson, Tim (2018) The Industrial Internet of Things (IIoT): An Analysis Framework, Retrieved from; https://www-sciencedirect-com.jproxy.lib.ecu.edu/science/article/pii/S0166361517307285#bib0155

Markarian, Jennifer (2016) The Internet of things for Pharmaceutical Manufacturing, Retrieved from http://www.pharmtech.com/internet-things-pharmaceutical-manufacturing

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

OneM2M staff (2018); OneM2M – Standards for M2M and the Internet of Things, Retrieved from: http://www.onem2m.org/about-onem2m/why-onem2m

Niblett, Peter (2018) IIoT Hills to Climb, Retrieved from: https://internetofthingsagenda.techtarget.com/tip/IIoT-standards-have-yet-to-keep-pace-with-IoT-protocols

Stojmenovic, Ivan; Wen, Sheng; Huang, Xinyi; Luan, Hao (2015) An Overview of Fog Computing and its Security Issues, Retrieved from; https://onlinelibrary-wiley-com.jproxy.lib.ecu.edu/doi/full/10.1002/cpe.3485

Pizon, Jakub; Lipski, Jerzy (2016) Applied Computer Science: Perspectives for Fog Computing in Manufacturing, Vol 12 No. 3, pp 37-46, Retrieved from, https://docs.google.com/viewerng/viewer?url=http://www.acs.pollub.pl/pdf/v12n3/4.pdf

Fog Computing Consortium (2017) Definition of Fog Computing, Retrieved from https://www.openfogconsortium.org/resources/#definition-of-fog-computing

Wu, Dazhoung; Liu, Shaopeng; Zhang, li; Terpenny, Janis; Gao, Robert X.; Kurfess, Thomas; Guzzo, Judith A. (2017) Journal of Manufacturing Systems: A Fog computing-based Framework for Process Monitoring and Prognosis in Cyber-Manufacturing, Vol 43, Part 1, pp 25-34, Retrieved from: http://www.sciencedirect.com/science/article/pii/S0278612517300237

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

Galloway, Brendan and Hancke, Gerhard P. (2013) Introduction to Industrial Control Networks, Retrieved from http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/stamp/stamp.jsp?tp=&arnumber=6248648&isnumber=6512259

G. Bonney, H. Höfken, B. Paffen and M. Schuba, "ICS/SCADA security analysis of a Beckhoff CX5020 PLC," *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, Angers, France, 2015, pp. 1-6. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7509940&isnumber=7509852

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

Brandl, Dennis L., Brandl, Donald E. (2012) Plant IT: Integrating Information Technology into Automated Manufacturing, Retrieved from http://site.ebrary.com.jproxy.lib.ecu.edu/lib/eastcarolina/reader.action?docID=10629651

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/

Daniels, Stacie (2016) Real World Example: Stuxnet Worm, Retrieved from http://www.cse.psu.edu/~trj1/cse443-s12/slides/cse443-lecture-22-stuxnet.pdf