Journal of Strategic Management Studies
Vol. 10, No. 1, 19–28 (October 2018)
doi: 10.24760/iasme.10.1_19

Cyber Security in Industry 4.0: The Pitfalls of Having Hyperconnected Systems

MAURICE DAWSON
Assistant Professor, School of Applied Technology, Illinois Institute of Technology

Abstract

The fourth industrial revolution is referred to as Industry 4.0. The current trend with manufacturing is automation and unparalleled levels of data exchange. To bring this trend to realization requires integrating the Internet of Things, Internet of Everything cyber-physical systems, cloud computing technologies, and more into manufacturing. Industry 4.0 involves a hyperconnected system that includes the smarter use of robotics to effectively and efficiently move to manufacture to new heights. With the use of all these technological systems, it is imperative to ensure that cyber security plays a role during the rise of this digital industrial revolution. In the United Kingdom, more than eighty manufacturing plants were hit by cyber attacks while threats in this specific industry have risen. The pitfalls of having hyperconnected systems leave an entire industry even more vulnerable than the traditional enterprise system design.

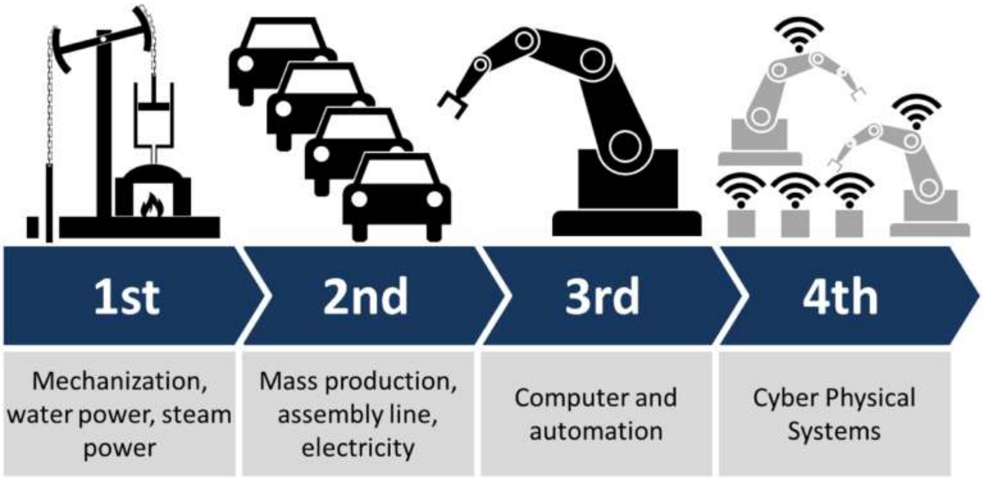
Keywords:
cyber security, risk management, internet of things, hyperconnectivity

INTRODUCTION

The landscape of manufacturing has changed, and this has allowed attackers unparalleled access to data unlike before. Nearly eighty-five participants in a survey reported falling victim to a cyber attack in the United Kingdom (U.K.) (Ambrose, 2018). The worry is that Russian hackers and other nation states are gaining entry into protected networks. Currently, there are well-documented attacks on Supervisory control and data acquisition (SCADA) systems throughout North America and Europe. A survey conducted by researchers shows the methods of operations, impact, and target sectors (Miller & Rowe, 2012). Essentially all incidents were classified with the following to include showing the year of the attack. Within the summary of incidents, you can see the earliest attack is 1982 on the Power of Siberia pipeline (Miller & Rowe, 2012). This shows that manufacturing has been a target for attackers for over two decades.

To understand the current state of manufacturing, it is vital to understand the history of the previous industrial revolutions. The First Industrial Revolution occurred in Britain over the century 1750–1850 (Deane, 1979). This was when the theory of economic development took root, and specialized activity for production for national and international markets rose. The Second Revolution is known as the technological revolution. This period was near the end of 19th century through the beginning of the 20th century. During this revolution, we received inventions such as airplanes, Henry Ford's Model T, light bulb, and telegram. This period introduced mass production which has been altered by experts in supply chain and logistics today to equip manufacturing companies to produce to meet supply and demand. The Third Industrial Revolution was from 1969 to 2000. These three industrial revolutions are depicted in **FIGURE 1**.

Manufacturing is undergoing another revolutionary change, and that is paving the way for systematical deployment of Cyber-Physical Systems (CPS) (Lee, Bagheri, & Kao, 2015). CPS is an integration of networking, physical processes, and embedded computers that are tightly integrated with the Internet. This change is known as the Fourth Industrial Revolution, and it does not arrive without cyber se-


1st
Mechanization, water power, steam power
2nd
Mass production, assembly line, electricity
3rd
Computer and automation
4th
Cyber Physical Systems

Reprinted from Industry 4.0, by Wikipedia, June 30 2018, retrieved from https://en.wikipedia.org/wiki/Industry_4.0. Licensed under CC Attribution-ShareAlike License.

FIGURE 1 Industrial Revolutions

curity with technological implementation. While technology is the United States (U.S.) has been years ahead of the laws providing protection and governance meanwhile the government are continuously playing catch up (March & Smith, 1995). Understanding the various technological architectures in this connected environments provides an insight into the issues surrounds this new revolution.

INTERNET OF THINGS

The Internet of Things (IoT) describes a world in which smart technologies enable objects with a network to communicate with each other and interface with humans effortlessly. This connected world of convenience and technology does not come without its drawbacks, as interconnectivity implies hackability. This new world of convenience calls for revolutionary protection strategies to reassess security. Risk management concepts and Information Assurance architecture similar to those practiced in the United States Department of Defense (DoD) should be used as guidelines for cyber security implementation. This new emerging market that is facilitating the exchange of services and goods requires understanding the associated laws for the implementation of an IoT architecture (Weber, 2010).

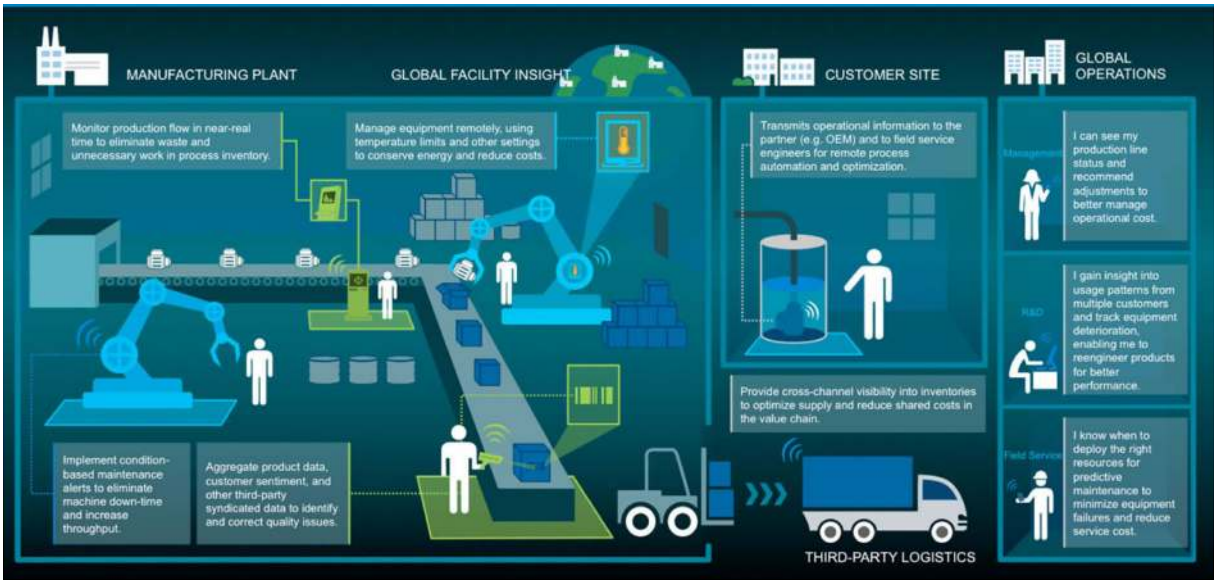
Researchers at Cisco Systems estimate that over 99 percent of physical devices are still unconnected and that there is a market of $14.4 trillion. This white paper urges business leaders to transform their organizations based on key learnings to be competitive for the future (Evans, 2012). As this new wave of Internet-enabled technologies arrives, it is imperative to understand the security and privacy concerns fully (Thierer, 2015). Understanding these concerns also means understanding how to apply security controls to systems appropriately. Addressing security objectives appropriately will allow for risks to be mitigated. This means following the principles of security to ensure cyber security posture is achieved.

All of these connected devices using proven standards, policies, and guidance can help with the ease of integrating these technologies into everyday life. Currently, there is a lack of guidance for securing IoT, Internet of Everything (IoE), and Web of Things (WoT) as a cohesive unit; however, there is appropriate documentation available through the National Institute of Standards and Technology (NIST), Federal Information Processing Systems (FIPS), Department of Defense (DoD), Institute of Electronic and Electrical Engineers (IEEE), International Organization for Standardization (ISO), Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and more. It is essential for the security engineer to understand how to protect these devices individually and then understand how the devices become more vulnerable when connected. Mobile devices would need to be hardened with appropriate security controls for compliance (Dawson, Wright, & Omar, 2015). Encryption would need to be on devices that have IoT capabilities such as refrigerators, televisions, or smart watches. This would allow the protection of data in transit and at rest. The recommended guidance would be to use an approved public algorithm and not a weak algorithm. The classification of weak and robust algorithm change over time thus it is essential to keep abreast of the changes in cartographic algorithms. Access controls would need to be placed to ensure that other users within the hyperconnected system to do not have the ability to elevate privileges through lateral movement within a network (Dawson, 2017).

INTERNET OF THINGS IN MANUFACTURING

IoT in manufacturing is part of this Industrial Revolution 4.0, and this concept has a significant impact. For the manufacturing plant, one can monitor production to apply lean principles for waste management while being able to see inventory changes in real time. The implementation of IoT allows for Built-In Test (BIT) alerts, maintenance alerts for downtime. Having embedded OS allows for devices to be transformed for computing functionality beyond essential functions. This would include the ability to capture more data that allows for managers to see production status, gain insight on usage patterns, and from this data make decisions. A manager could make decisions that allow them to make decisions based upon product performance in the assembly line such as replacement or the need to add additional equipment. The data would include information such as Global Positioning Systems (GPS) tags that provide the exact location of equipment that needs to be further examined to review point of origination.

FIGURE 2 displays how IoT looks in manufacturing and all the different situations where IoT can be applied. What is not displayed is the negative concerns around using IoT. Since all these systems are connected to so many other systems through Internet, Bluetooth, or another method of communication it is necessary to ensure the secure transmission of data. At the current time, there are a few documents that provides the guidance for securing the systems in the manufacturing environment. This is an issue as the industrial revolution is rapidly taking root in manufacturing.



Monitor production flow in near-real time to eliminate waste and unnecessary work in process inventory.

Manage equipment remotely, using temperature limits and other settings to conserve energy and reduce costs.

Implement condition-based maintenance alerts to eliminate machine down-time and increase throughput.

Aggregate product data, customer sentiment, and other third-party syndicated data to identify and correct quality issues.

Transmits operational information to the partner (e.g. OEM) and to field service engineers for remote process automation and optimization.

Provide cross-channel visibility into inventories to optimize supply and reduce shared costs in the value chain.

I can see my production line status and recommend adjustments to better manage operational cost.

I gain insight into usage patterns from multiple customers and track equipment deterioration, enabling me to reengineer products for better performance.

I know when to deploy the right resources for predictive maintenance to minimize equipment failures and reduce service cost.

Reprinted from *Internet of Things (IoT)*, by Andrej Tozon, 2015, retrieved from https://www.slideshare.net/andrejt/ntk-2015-internet-of-things-track-iot-smart-home. Licensed under CC Attribution-ShareAlike License.

FIGURE 2 Internet of Things in Manufacturing

Secure computing is essential as technological environments continue to become intertwined and hyperconnected. The policies to properly secure these new environments must also be explored as many of the security controls found within guidance such as the DoD focuses on singular systems and components (Dawson, Crespo, & Brewster, 2013). There needs to be the creation of new controls that review embedded sensors, body modifications, and devices that entirely take advantage of Internet-enabled technologies. With the emergence of these technologies, the possibilities are endless; however, there will be new vulnerabilities unexplored.

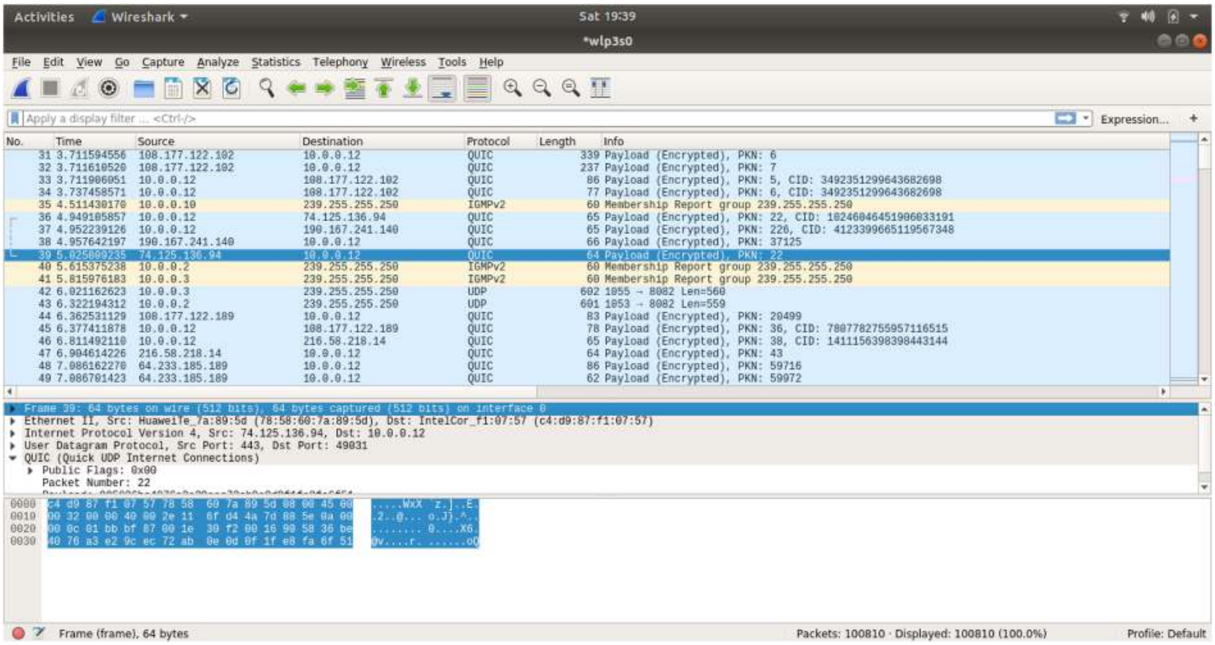
CYBER SECURITY ISSUES IN TECHNOLOGICAL DEVICES

As the next era of computing will be outside of the traditional desktop and into embedded systems and smaller devices are targets for attacks (Gubbi, Buyya, Marusic, & Palaniswami, 2013). When you consider, Bring Your Own Device (BYOB) as a radical step, imagine using a device such as a refrigerator that contains an embedded computing device to track the number of groceries within. This integrated device would allow access to email, weather, and other devices that enable connectivity through WiFi, or some Application Programming Interface (API) to a web-based application. Thus, the data collected would be weather, thermostat cooling patterns, foods purchased, the cost of items per month, average consumption, and more. This massive amount of data provides the ability for an attacker to gather intelligence unlike before. They can see schedules which allow for them to analyze behavioral patterns view dietary concerns that affect health, and more than give information once though genuinely personal. At the moment, organizations such as Cisco Systems and others are pushing for WoT and IoT, but no one has a plan for ensuring secured transmission is maintained during various modes of operation.

Additionally, the unknowing consumer of everyday products needs to be aware of what it means to have sensors, Radio Frequency IDentification (RFID), Bluetooth, and WiFi enabled products. What further needs be explored is how Availability, Integrity, and Confidentiality (AIC) can be applied to IoT, WoT, and IoE with consideration for the application of these architectures in the commercial sector. All these architectures allow for hyperconnectivity while at the same time it is critical to understand the changing threat landscape (Badonnel, Koch, Pras, Drašar, & Stiller, 2016).

When an organization allows BYOB being to be used in a manufacturing setting it must be realized that yet another device is going unchecked into the system, effects of various attacks such as Distributed Denial of Service (DDoS), replicating worms, and calculated virus that are activated based upon specific system configuration (Singh, 2012; Brooks, 2017). As the consequences of security problems ranging from personal injury to system downtime the need for secure environments (Chahid, Benabdellah, & Azizi, 2017). So having a manufacturing floor with multiple IoT devices means there are lots of data that can be captured with relative ease. With applications such as Wireshark, it is relatively easy to capture data on an unsecured network. Wireshark is a software application that not only a laptop but also a mobile device or RaspberryPi for penetration testing (Muniz & Lakhani, 2015). The amount of detailed captured through Wireshark is astounding and revealing much about the network (See **FIGURE 3**) .

In **FIGURE 4** displayed is 500,000 packets captured from one device on a network. Understanding the origination, destination, and types of network protocols are currently in use enable an attacker to know what to attack precisely. This scenario could also include knowing the destination as it could be used to develop man in the middle attacks. The data captured through a system can be revealing and help an attacker understand the attack surface in detail. Provided in network scans are the open ports and the closed ports, disabling, and identification of unpatched applications. This informs the attacker there was no system hardening done before the deployment of the system on the network and perhaps that the organization has a lack of security policies that address secure system configuration before going live (Creery & Byres, 2005).


Activities
Wireshark ▾
Sat 19:39
*wlp3s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time         Source           Destination      Protocol  Length Info
  31 3.711594556  108.177.122.102  10.0.0.12        QUIC         339 Payload (Encrypted), PKN: 6
  32 3.711610520  108.177.122.102  10.0.0.12        QUIC         237 Payload (Encrypted), PKN: 7
  33 3.711906051  10.0.0.12        108.177.122.102  QUIC          86 Payload (Encrypted), PKN: 5, CID: 3492351299643682698
  34 3.737458571  10.0.0.12        108.177.122.102  QUIC          77 Payload (Encrypted), PKN: 6, CID: 3492351299643682698
  35 4.511430170  10.0.0.10        239.255.255.250  IGMPv2        60 Membership Report group 239.255.255.250
  36 4.949105857  10.0.0.12        74.125.136.94    QUIC          65 Payload (Encrypted), PKN: 22, CID: 10246046451906033191
  37 4.952239126  10.0.0.12        190.167.241.140  QUIC          65 Payload (Encrypted), PKN: 226, CID: 4123399665119567348
  38 4.957642197  190.167.241.140  10.0.0.12        QUIC          66 Payload (Encrypted), PKN: 37125
  39 5.025809235  74.125.136.94    10.0.0.12        QUIC          64 Payload (Encrypted), PKN: 22
  40 5.615375238  10.0.0.2         239.255.255.250  IGMPv2        60 Membership Report group 239.255.255.250
  41 5.815976183  10.0.0.3         239.255.255.250  IGMPv2        60 Membership Report group 239.255.255.250
  42 6.021162623  10.0.0.3         239.255.255.250  UDP          602 1055 → 8082 Len=560
  43 6.322194312  10.0.0.2         239.255.255.250  UDP          601 1053 → 8082 Len=559
  44 6.362531129  108.177.122.189  10.0.0.12        QUIC          83 Payload (Encrypted), PKN: 20499
  45 6.377411878  10.0.0.12        108.177.122.189  QUIC          78 Payload (Encrypted), PKN: 36, CID: 7807782755957116515
  46 6.811492110  10.0.0.12        216.58.218.14    QUIC          65 Payload (Encrypted), PKN: 38, CID: 1411156398398443144
  47 6.904614226  216.58.218.14    10.0.0.12        QUIC          64 Payload (Encrypted), PKN: 43
  48 7.086162270  64.233.185.189   10.0.0.12        QUIC          86 Payload (Encrypted), PKN: 59716
  49 7.086701423  64.233.185.189   10.0.0.12        QUIC          62 Payload (Encrypted), PKN: 59972

▸ Frame 39: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
▸ Ethernet II, Src: HuaweiTe_7a:89:5d (78:58:60:7a:89:5d), Dst: IntelCor_f1:07:57 (c4:d9:87:f1:07:57)
▸ Internet Protocol Version 4, Src: 74.125.136.94, Dst: 10.0.0.12
▸ User Datagram Protocol, Src Port: 443, Dst Port: 49031
▾ QUIC (Quick UDP Internet Connections)
   ▸ Public Flags: 0x00
     Packet Number: 22

0000  c4 d9 87 f1 07 57 78 58  60 7a 89 5d 08 00 45 00   .....WxX `z.]..E.
0010  00 32 00 00 40 00 2e 11  6f d4 4a 7d 88 5e 0a 00   .2..@... o.J}.^..
0020  00 0c 01 bb bf 87 00 1e  30 f2 00 16 90 58 36 be   ........ 0....X6.
0030  40 76 a3 e2 9c ec 72 ab  0e 0d 0f 1f e8 fa 6f 51   @v....r. ......oQ

Frame (frame), 64 bytes          Packets: 100810 · Displayed: 100810 (100.0%)          Profile: Default
```

FIGURE 3 Wireshark Capture

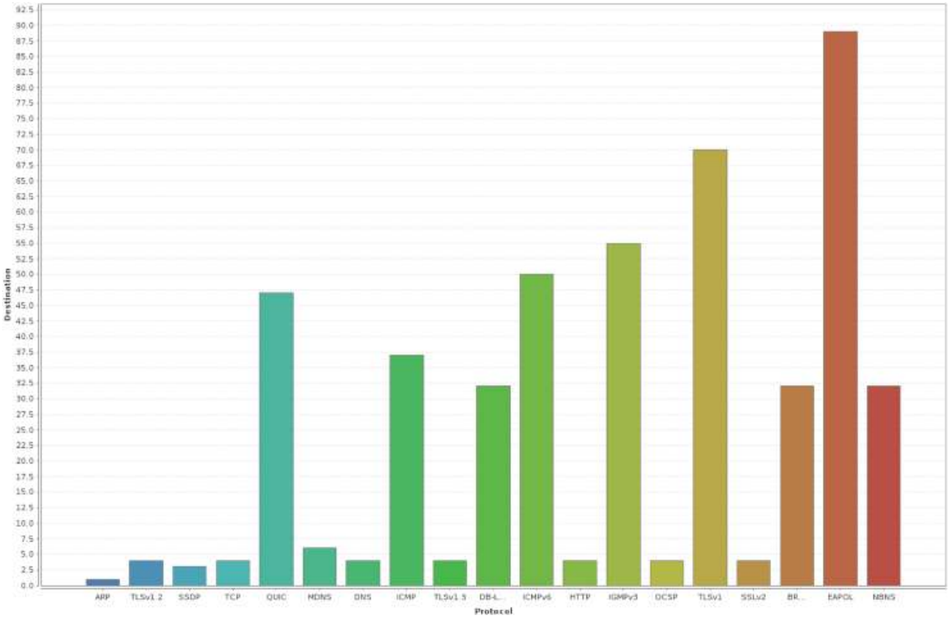


FIGURE 4 Group-by Column: Protocol and Value Column: Destination

MANUFACTURING SYSTEMS CERTIFICATION AND ACCREDITATION

For Industry 4.0 to survive, it is necessary to ensure security is being embedded into the system from the beginning of the lifecycle through a process (Aljawarneh, Alawneh, & Jaradat, 2017). Thus the implementation of policies, directives, and laws that systems undergo Certification and Accreditation (C&A) is mandatory. Implementing this allows for all these systems to be routinely checked and meet stringent initial cyber security controls before the system goes live. (Ross, 2009). Essentially the industry would be required to implement a bare minimum of controls to protect the facility from physical controls. In 2011, NIST published a Guide to Industrial Control Systems (ISC) Security that provides a baseline for precisely this (Stouffer, Falco, & Scarfone, 2011). Contained in the document is how the overall environment should be set up to maximize cyber security to include specific recommendations for ICS. These documented guidelines would mitigate attacks that are against the process, risk assessment, risk management, and the overall systems development life cycle (Cárdenas et al., 2011).

A framework such as the Risk Management Framework (RMF) should be used as a baseline to enable organizations to have already defined controls. This activity is possible as NIST 800-53 provides details about the RMF which is a framework created by the NIST to address risk management (NIST, 2013). The RMF uses the risk-based approach to security control selection and specification considering effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations. Six RMF categorization steps serve as the basis for this NIST guidance (NIST, 2013). Step 1: Categorize. The system is assessed and categorized based on an impact analysis. Step 2: Select. During the period the organization must identify, select, customize, and document the security and privacy controls required to protect the system and the organization commensurate with the risk to organizational operations and assets, individuals. These controls are to be addressed in the design and are a result of high-level requirements that are decomposed into lower level requirements. Step 3: Implement. During this step, the controls selected in step 2 are deployed within the system to include the associated environment of operation. Step 4: Assess. The controls implemented are assessed to see if they are working as intended, and that the desired outcome meets the security requirements for the system. Step 5: Authorize. Get authority for the system to operate based upon an acceptable decision upon the acceptable risk for the system. Step 6: Monitor. Continually assess the security control of the system on an ongoing basis. The process should include annual security checks to review compliance and reporting to a third party for compliance that does not have ties to the organization undergoing the C&A process. This process should be more of a regulatory body that issues the letter for accreditation. Roles similar to that in the former framework, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), should be implemented (Eller & Stauffer, 2000).

CYBER THREATS AND INTELLIGENCE GATHERING

With the potential threats of cyber terrorism affecting national and international security, the importance of security is elevated to greater heights (Dawson, Omar, & Abramson, 2015). New threats against national infrastructure and digital crime are making researchers consider new methods of handling cyber incidents (Dawson & Omar, 2015). It is imperative that if the government or commercial sectors want to make use of these new technological Internet and Web-enabled architectures that they are prepared to battle new threats. Countries could target the ability to manufacture products where it is for military or agriculture could significantly affect a country's Gross Domestic Product (GDP). Imagine numerous factories used for producing foods for an area known to have a significant amount of federal employees. The food has the incorrect levels of nutrients and some items bypassing proper checks. An entire county could be sick due to tampering of equipment in a manufacturing center. If you consider more high tech items, this tampering could lead to essential checks not occurring in vehicle production that degrades the quality of the car. The lacks of quality controls in the automatic process would have dangerous results such as no checks on breaks, power steering, windows, and onboard system diagnostics (Atamli & Martin, 2014; Amoozadeh et al., 2015). The manufacturing floor could serve as a place that allows an attacker not only to gather critical data from devices but inflict damage of any of the products being produced.

During the Stuxnet, attack operators thought the centrifuges were operating normally while the causing a meltdown and significantly slowing down the process of Uranium enrichment (Langner, 2011). The source code of this worm is available online and can be repurposed for an attack. Reviewing the attack on Natanz, the exact Program Logic Controller (PLC) had to be discovered and from this point, they had to identify the manufacturer. This facility was kept secret whereas a standard production facility it is easier to uncover the technological tools in the manufacturing facility to include methods to investigate the logistics of getting that device to the facility. Using Open Source Intelligence Tools (OSINT) and other forms of intelligence gathering such as Human Intelligence (HUMINT), it will not be far-fetched to say that an attacker could find out key manufacturers of machines used in the facility.

For an attacker, they could employ the techniques from the statecraft of intelligence, and use that to exploit the numerous devices that are connected to the network to create an intelligence report (Dulles, 2006; Andrews & Peterson, 1990). The first stage planning would occur and the determination of informational needs. These needs could be the types of information and requirements for the data needed. The second stage collection would be the process and tools used to collect the data. Earlier in this paper, the researcher showed half a million network packets captured in only 15 min using Wireshark. Data collection could be my means of OSINT, Signals Intelligence (SIGINT), or running an application to map out the network and vulnerabilities. The third stage, processing, and exploitation are performed with tools to automate the process. For the fourth stage, the use of the R programming language and Python could be used to perform data science on the massive amount of data collected to analyze data further. It can be everything from looking at the captured metadata on photos, analyzing machine behavior, and routing of information. In the final stage, dissemination, this could include many methods of providing information. **FIGURE 5** shows the entire Intelligence Cycle at a high level, however, these stages can be broken down further and tailed for the organization that is performing the tasks. For example, in the collection stage, it can be broken down to details the methods in which the collections occur. There could be an entire subprocess for

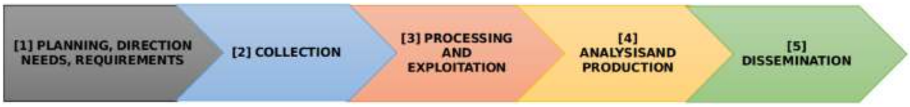
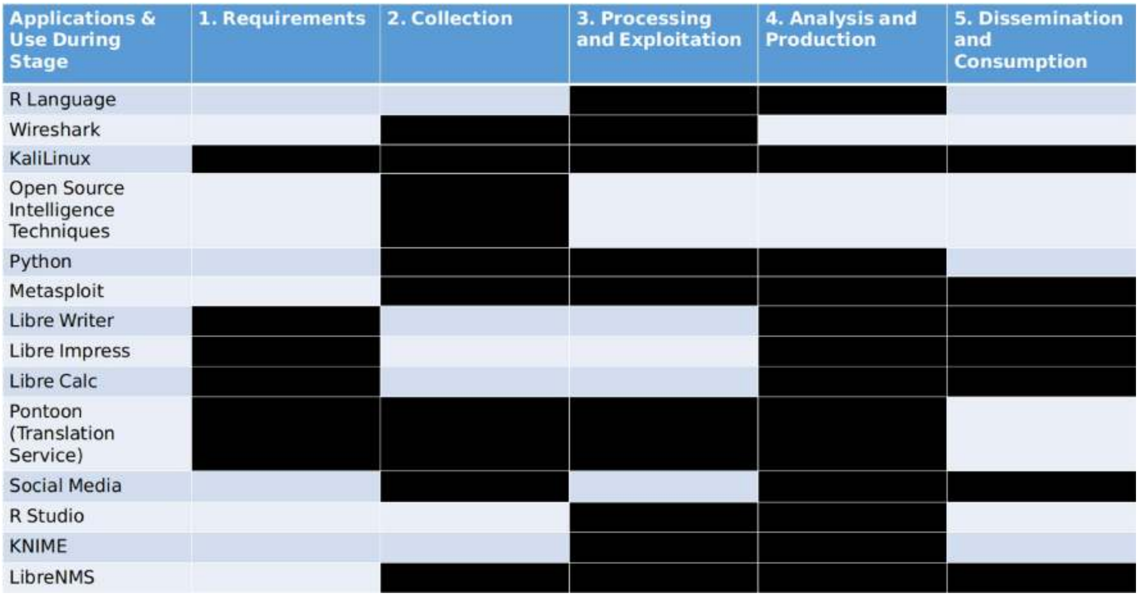

[1] PLANNING, DIRECTION NEEDS, REQUIREMENTS
[2] COLLECTION
[3] PROCESSING AND EXPLOITATION
[4] ANALYSISAND PRODUCTION
[5] DISSEMINATION

FIGURE 5 Intelligence Cycle



Applications & Use During Stage	1. Requirements	2. Collection	3. Processing and Exploitation	4. Analysis and Production	5. Dissemination and Consumption
R Language			■	■	
Wireshark		■	■		
KaliLinux	■	■	■	■	■
Open Source Intelligence Techniques		■			
Python		■	■	■	
Metasploit		■	■	■	■
Libre Writer	■			■	■
Libre Impress	■			■	■
Libre Calc	■			■	■
Pontoon (Translation Service)	■	■	■	■	
Social Media		■		■	■
R Studio			■	■	
KNIME			■	■	
LibreNMS		■	■	■	■

FIGURE 6 Open Source Applications to Use During Intelligence Cycle

OSINT collection which includes getting tagged in the next stage. The tools that are selected for use and in what sequence could be essential based upon the first stage. For example, an attacker could have some collections tools running first against the network, and then on individual components for identification. Once these components are identified, then the applications can be discovered. Once that has happened then the source code can be analyzed to show current Common Weakness Enumeration (CWE) (Martin & Barnum, 2008). In stage 4 the CWEs could be analyzed using their associated Common Vulnerability Scoring System (CVSS) scores and vulnerability types (Barnum, 2008). If a CWE is a top ten, then it is likely that this may be an unaddressed exploit from the CWE Top 10 List. Therefore the attacker could go down the list performing an array of attacks against the system as if they were doing black box vulnerability testing (Bau, Bursztein, Gupta, & Mitchell, 2010).

Some tools can be used to go through the entire intelligence cycle. In **FIGURE 6** listed are those tools and applicable stags of use. The majority of listed applications are Open Source Software (OSS) and licensed by the Gnu Public License (GPL). Out of all the tools for analysis, the R Language is one of the most powerful open source languages as it allows for statistical analysis and performing data science (RDC Team, 2004).

Illustrated in **FIGURE 6** the number of tools available that can be used to perform an array of intelligence tasks that gives further insight into the network environment. Briefly covered is the need for securing the system but provided are some applications that can quickly transform an attacker into an intelligence analyst.

CONCLUSION

As this new industrial revolution is taking ground it will be key to establish what a baseline secure configuration would be for this manufacturing plants. This will include a minimum set of security controls every organization will need to have before gaining an Approval to Operate (ATO). As the attacks continue to grow this will be the only path forward to ensuring that these attacks are lowered and that identified risks are brought to an accepted minimum level. This will include tighter regulatory polices, employee education, and hardened technology that is used within the boundaries of the network. The goal of this paper was to show the pitfall of having a hyperconnected system with improper cyber security implemented.

REFERENCES

Aljawarneh, S. A., Alawneh, A., & Jaradat, R. (2017). Cloud security engineering: Early stages of SDLC. *Future Generation Computer Systems*, *74*, 385–392.

Ambrose, J. (2018, April 23). Half of UK manufacturers fall victim to cyber attacks. Retrieved May 30, 2018, from https://www.telegraph.co.uk/business/2018/04/22/half-uk-manufacturers-fall-victim-cyber-attacks/

Amoozadeh, M., Raghuramu, A., Chuah, C. N., Ghosal, D., Zhang, H. M., Rowe, J., & Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, *53*(6), 126–132.

Andrews, P. P. & Peterson, M. B. (Eds.). (1990). *Criminal intelligence analysis*. Loomis, CA: Palmer Enterprises.

Atamli, A. W. & Martin, A. (2014, September). Threat-based security analysis for the internet of things. In *2014 International Workshop* on *Secure Internet of Things (SIoT)*, (pp. 35–43). IEEE.

Badonnel, R., Koch, R., Pras, A., Drašar, M., & Stiller, B. (2016). Management and security in the age of hyper connectivity. In *10th IFIP WG 6.6 International Conf. Autonomous Infrastructure, Management, and Security*, AIMS 2016.

Barnum, S. (2008). Common attack pattern enumeration and classification (capec) schema description. Cigital Inc, http://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1, 3.

Bau, J., Bursztein, E., Gupta, D., & Mitchell, J. (2010, May). State of the art: Automated blackbox web application vulnerability testing. In *2010 IEEE Symposium on Security and Privacy* (pp. 332–345). IEEE.

Brooks, T. T. (Ed.). (2017). *Cyber-assurance for the Internet of Things*. John Wiley & Sons.

Cárdenas, A. A., Amin, S., Lin, Z. S., Huang, Y. L., Huang, C. Y., & Sastry, S. (2011, March). Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM symposium on information, computer and communications security* (pp. 355–366). ACM.

Chahid, Y., Benabdellah, M., & Azizi, A. (2017, April). Internet of things security. In *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, (pp. 1–6). IEEE.

Creery, A. & Byres, E. J. (2005, September). Industrial cybersecurity for power system and SCADA networks. In *Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual* (pp. 303–309). IEEE.

Dawson, M. (2017). Exploring Secure Computing for the Internet of Things, Internet of Everything, Web of Things, and Hyperconnectivity. In M. Dawson, M. Eltayeb, & M. Omar (Eds.). *Security Solutions for Hyperconnectivity and the Internet of Things* (pp. 1–12). Hershey, PA: IGI Global. doi: 10.4018/978-1-5225-0741-3.ch001

Dawson, M. & Omar, M. (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 1–368). Hershey, PA: IGI Global. doi: 10.4018/978-1-4666-8345-7

Dawson, M. E. Jr, Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*(1), 1–22.

Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the Methods behind Cyber Terrorism. In M. Khosrow-Pour (Ed.). *Encyclopedia of Information Science and Technology* (3rd ed.) (pp. 1539–1549). Hershey, PA: IGI Global. doi: 10.4018/978-1-4666-5888-2.ch147

Dawson, M., Wright, J., & Omar, M. (2015). & Mobile Devices: The Case for Cyber Security Hardened Systems. In M. Dawson, & M. Omar (Eds.). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 8–29). Hershey, PA: IGI Global. doi: 10.4018/978-1-4666-8345-7.ch002

Deane, P. M. (1979). *The first industrial revolution*. Cambridge University Press.

Dulles, A. (2006). *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World.* Rowman & Littlefield.

Eller, M. M. J., & Stauffer, B. (2000). *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*. US-Department of Defense.

Evans, D. (2012). The internet of everything: How more relevant and valuable connections will change the world. *Cisco IBSG*, 1–9.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, *9*(3), 49–51.

Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, *3*, 18–23.

March, S. T. & Smith, G. F. (1995). Design and natural science research on information technology. *Decision support systems*, *15*(4), 251–266.

Martin, R. A. & Barnum, S. (2008). Common weakness enumeration (cwe) status update. *ACM SIGAda Ada Letters*, *28*(1), 88–91.

Miller, B. & Rowe, D. (2012, October). A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology* (pp. 51–56). ACM.

Muniz, J. & Lakhani, A. (2015). Penetration testing with raspberry pi (pp. 1–245). Packt Publishing Ltd.

NIST. (2013). Security and privacy controls for federal information systems and organizations. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

Omar, M. & Dawson, M. (2013, April). Research in progress-defending android smartphones from malware attacks. In *2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT)*, (pp. 288–292). IEEE.

RDC Team. (2004). R: A language and environment for statistical computing. Vienna: R Foundation for Statistical Computing. Available: http://www.R-project.org. Accessed 26 July 2018.

Ross, R. S. (2009). *Recommended Security Controls for Federal Information Systems and Organizations [includes updates through 9/14/2009]* (No. Special Publication (NIST SP)-800-53 Rev 3).

Singh, N. (2012). BYOD genie is out of the bottle–"Devil or angel". *Journal of Business Management & Social Sciences Research*, *1*(3), 1–12.

Stouffer, K., Falco, J., & Scarfone, K. (2011). *Guide to industrial control systems (ICS) security*. NIST special publication, 800(82), 1–255.

Thierer, A. D. (2015). The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. *Richmond Journal of Law and Technology*, *21*, 1–118.

Tozon, A. (2015, May 25). NTK 2015: Internet of things track (IoT)—Smart Home. Retrieved July 27, 2018, from https://www.slideshare.net/andrejt/ntk-2015-internet-of-things-track-iot-smart-home

Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer law & security review*, *26*(1), 23–30.

Wikipedia. (2018, June 19). Industry 4.0. Retrieved June 30, 2018, from https://en.wikipedia.org/wiki/Industry_4.0

Dr. Maurice Dawson is an Assistant Professor of Information Technology and Management within the School of Applied Technology at Illinois Institute of Technology. Additionally, he serves as Director and Distinguished Member of the IIT Center for Cyber Security and Forensics Education (C2SAFE) and responsible for working with the faculty who are members of this center. He has a Doctor of Computer Science from Colorado Technical University and a Doctor of Philosophy in Cyber Security from the Intelligent Systems Research Centre at London Metropolitan University. Additionally, he is the co-editor of Developing Next-Generation Countermeasures for Homeland Security Threat Prevention, and New Threats and Countermeasures in Digital Crime and Cyber Terrorism, published by IGI Global in 2017, and 2015 respectively. Dawson has received a Fulbright Scholar Grant to the School of Electrical Engineering and Computer Science at South Ural State University in Russia in 2015 for Business Intelligence and more recently an award to the College of Computer & Information Science of Prince Sultan University in Saudi Arabia for cyber security for the period of 2017–2018.
E-mail: maurice.dawson@ieee.org