Industrial and Systems Engineering
Vol. 1, No. 1, 2016, pp. 27-36
http://www.aiscience.org/journal/ise

Big Data Analytics and Cybersecurity for Advanced Manufacturing

Lidong Wang[1, *], Cheryl Ann Alexander[2]

[1]Department of Engineering Technology, Mississippi Valley State University, Itta Bena, Mississippi, USA
[2]Technology and Healthcare Solutions, Inc., Itta Bena, Mississippi, USA

Abstract

Many advanced manufacturing systems are based on industrial control systems (ICSs). Manufacturing systems are being facilitated by Internet of Things (IoT), cyber-physical systems (CPSs), and cloud platforms; however, the security risks due to these advanced technologies and platforms are increasing greatly. Cybersecurity in manufacturing is not the same as general IT security. There are many challenges in cybersecurity for advanced manufacturing. Big Data analytics is a powerful tool for analyzing complicated data with high volume, high variety, and high velocity, etc. It has the potential to improve cybersecurity in advanced manufacturing. This paper presents the progress of cybersecurity in IT, ICSs, CPSs and advanced manufacturing. Challenges in these areas are also discussed.

Keywords

Big Data Analytics, Advanced Manufacturing, Cybersecurity, Industry 4.0, Additive Manufacturing (AM), Cyber-Physical System (CPS), Internet of Things (IoT), Cloud Computing, Industrial Control System (ICS)

Received: August 6, 2016 / Accepted: August 15, 2016 / Published online: August 25, 2016

1. Introduction

A globally-interconnected digital information and communications infrastructure may be referred to as "cyberspace". Manufacturing is not exempt from many cybersecurity challenges faced by other critical infrastructure sectors. Cyber threats have the potential to affect confidentiality, integrity, and availability in a manufacturing setting as well. Manufacturing is at risk for spear phishing attacks, directed attacks that embed malware in target computers, which may be delivered via email or other targeted means [1].

As systems migrate to open systems like Windows and TCP/IP, the security risks are greatly increasing. Cyber security in a live production system has challenges. Basic security practices like strong authentication and encryption are not available in most systems. There is a common misunderstanding that a firewall and antivirus software will protect systems. Companies should ensure they have good firewalls, antivirus, patch management, tape backup, remote access, authentication, and physical security in place [2].

Three key concepts form the core of cyber security problems are vulnerabilities, threats, and attacks. A vulnerability is any weakness contained within a computing or networking system that can be exploited. A threat is defined as any process that can potentially violate the security policies of a system. An attack is considered to be any active process that deliberately seeks to violate the security polices of a system. Fire walls are security mechanisms that control the flow of network traffic (i.e., communication packets), into or out of a communication system. Intrusion detection is a process performed by an intrusion detection system (IDS) where events within a cyber environment are analyzed via audit data and sequences of events [3]. Many intrusion detection systems (IDSs) are signature based. When deploying IDSs in a control system, the ability to add unique signatures must be

* Corresponding author
E-mail address: lwang22@students.tntech.edu (Lidong Wang)

used. It is also commonplace to remove some of the default signatures and response capability as it may have no relevance to a control system network. When IDSs on control system networks are used, it is imperative that rule sets and signatures unique to that domain be used [4].

A survey was independently conducted by Ponemon Institute, LLC. Seven hundred six (706) IT and IT security practitioners in financial services, manufacturing, and government with an average of 10 years' experience were surveyed. Different perceptions and practices in financial services (FS), manufacturing (Manf), and government (Gov) were analyzed and published. The survey results are shown in Table 1 [5].

Table 1. Difficulties with Anomalous Traffic (Very difficult and difficult response combined).

Difficulties	FS	Manf	Gov
Difficulty in reducing the number of false positives in the analysis of anomalous traffic	74%	83%	87%
Difficulty in seeing anomalous traffic entering networks	69%	67%	80%

For today's plant floor, there are often the following phenomena: 1) a large installed base of proprietary networks, 2) protocol converters prevalent, 3) limited plant-floor segmentation or security, 4) insecure remote access solutions, 5) single point of failure being common-place, and 6) no process for patching or endpoint anti-virus protection with negative impact on production [6].

The Internet of Things (IoT) are often at security risks. The Cloud is not only a key pillar of ubiquitous computing, but also of the IoT. Besides the ever growing market for public cloud computing, private clouds are also on the rise since companies are realizing that they need to migrate in business-critical areas in order to protect their digital valuables. Cloud service providers will increasingly have to face the question of how resilient their own cloud-based security architectures actually are against cyberattacks. For Industry 4.0, security enforcement is not optional. Germany's manufacturing industry still has little confidence in the security of innovative solutions. Germany will be able to keep pace with the global economy during the fourth Industrial Revolution only if it manages to further strengthen confidence in the cybersecurity of fundamental technologies like the IoT and cloud computing [7].

Design, manufacturing, and product support operations are driven by a "digital thread" of technical data -- product and process information -- that can be shared throughout the supply chain and must be protected. The Department of Defense (DoD) in the USA and its industry have not taken enough action to improve the protection of technical data in factory floor networks and control systems that are increasingly subject to cyber threats. Cyber threats to manufacturing enterprises may be motivated by espionage, financial gain, or other reasons to compromise data confidentiality, integrity or availability – the C-I-A concerns. These concerns are translated as [8]:

- Theft of technical data, including critical national security information, and valuable commercial intellectual property. This is a confidentiality concern.
- Alteration of data, thereby altering processes and products. This is an integrity concern.
- Impairment or denial of process control, thereby damaging or shutting down operations. This is an availability concern.

Better practices and technical solutions are needed to protect against theft of technical data transiting or residing in manufacturing systems, alteration of the data (thereby compromising the physical parts produced), or interference with reliable and safe operation of a production line [8].

Advanced manufacturing often relies on ICSs. More and more manufacturing systems are being based on the IoT, cyber-physical systems (CPS), and cloud computing. The organization of the paper is as follows: the next section introduces general IT security; Section 3 introduces cybersecurity for industrial control systems and cyber-physical systems; Section 4 introduces cybersecurity in advanced manufacturing; Section 4 introduces Big Data analytics for cybersecurity in advanced manufacturing; and the final section is a conclusion.

2. General IT Security

Common vulnerabilities are in password practices and privileged access such as use of shared administrator accounts. In addition, there are the following vulnerabilities [9]:

(1) Access control: use of unsecure ports and protocols, use of prohibited ports and protocols, anonymous File Transfer Protocol (FTP) allowed, unsecure network services enabled on network devices and systems, and lack of Access Control Lists (ACLs) implemented on border router.

(2) Computer network defense service provider monitoring and operations: data exfiltration not detected, host-based security services misconfiguration, misconfigured intrusion detection systems (IDS), inadequate detection of insertion of removable media, unauthorized software installed on workstations not detected, and unauthorized (rogue/malicious) devices installed on network not detected.

(3) Workstations and server configurations: unsecured

sharepoint server, unpatched server and workstation vulnerabilities, misconfigured services/servers and vulnerable drivers, unauthorized data manipulation due to weak data protections, web application vulnerable to Standard Query Language (SQL) injection attack, network credentials/system configurations and network diagrams stored insecurely, insecure configurations for hardware and software on mobile devices/workstations and servers, and operational information stored insecurely (no authentication or encryption used).

(4) Infrastructure: physical security of critical components, exploitation of two-way trust relationship between domains, no wireless intrusion detection (WIDS) devices implemented, and logging for infrastructure (network) devices not implemented.

Security is also a major concern for wireless sensor networks (WSNs) applications in process industry. Attacks vary from eavesdropping on transmissions, including traffic analysis or disclosure of message contents, to modification, fabrication, and interruption of the transmissions through node capturing, routing attacks, or flooding. When designing the security mechanisms, both low-level (key establishment and trust control, secrecy and authentication, privacy, robustness to communication denial-of-service, secure routing, resilience to node capture) and high-level (secure group management, intrusion detection, and secure data aggregation) security primitives should be addressed. AES-128 (Advanced Encryption Standard, with 128-bit keys and 128-bit block size) symmetric-key cryptography algorithm is used in the IEEE 802.11 and IEEE 802.15.4 standards. The ZigBee protocol defines methods for implementing security services such as cryptographic key establishment, key transport, frame protection, and device management [10].

WSNs are vulnerable to various types of attacks. These attacks consist mainly of three types: attacks on secrecy and authentication; attacks on network availability; and stealthy attack against service integrity [11]. The possible DoS attacks and the corresponding countermeasures are listed in Table 2 [12].

Table 2. Attacks on WSNs and Countermeasures.

Attacks	Layers	Countermeasures
Jamming	Physical	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
Collision	Link	Error-correction code
Exhaustion	Link	Rate limitation
Unfairness	Link	Small frames
Spoofed Routing Information & Selective Forwarding	Network	Egress filtering, authentication, monitoring
Sinkhole	Network	Redundancy checking
Sybil	Network	Authentication, monitoring, redundancy
Hello Flood	Network	Authentication, packet leashes by using geographic and temporal information
Ack. Flooding	Network	Authentication, bi-directional link authentication verification
Wormhole	Network	Authentication, probing
Flooding	Transport	Client puzzles
De-synchronization	Transport	Authentication

Security mechanisms for WSNs lie in [11] cryptography in WSNs and key management protocols. For cryptography in WSNs, selecting the most appropriate cryptographic method is vital. Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated by code size, data size, processing time, and power consumption. As for key management protocols, key management is a core mechanism to ensure security in network services and applications in WSNs.

The challenges of security in cloud computing environments can be categorized into network level, user authentication level, data level, and generic issues. The challenges of the network level deal with network protocols and network security, such as distributed nodes, distributed data, and internode communication. The challenges of the authentication level deal with encryption/decryption techniques, authentication methods such as administrative rights for nodes, authentication of applications and nodes, and logging. The challenges of the data level deal with data integrity and availability such as data protection and distributed data. The challenges of generic issues are traditional security tools and use of different technologies [13].

Industrial Agents (IA) are considered as a key enabler for industrial applications. However, there are the following agent threats [14]:

(1) Misuse of agent(s) by the host --- Some example attack scenarios may include: masquerading, denial of service, eavesdropping, cloning/replacement, and agent manipulation by a malicious host.

(2) Misuse of the host by agent(s) --- Malicious agents may scan and identify security weaknesses in the host environment. Subsequently attacks may be performed once the possibilities are analyzed. They might include: masquerading, security breach, denial of service, and damage such as disk files and network access.

(3) Misuse of an agent by another agent--- Malicious agents may pose a threat for other agents executing in multi-agent systems. Examples include: repudiation, denial of service, and masquerading and misinformation.

(4) Misuse of agent(s) or host by underlying infrastructure --- Although the most common attacks involve the agents and the host, attacks could also happen outside the agent environments e.g. in the underlying network infrastructure. Typical examples include monitoring of communication, replay attacks, cloning of agents and host in order to study their behaviors/strategies, modification of agent system data and state etc.

(5) Complex attacks --- More complex attacks are usually collaborative and distributed. Two or more entities are working together towards common goals. Such entities might be agents or a combination of agents, malicious hosts and other services.

Industrial agent solutions will also need to be largely aware of the operational context and this includes multiple security considerations such as: data security, network security, hardware security, user security, and agent-based security (both agent and agent host execution environment relevant aspects) [14].

3. Cybersecurity for Industrial Control Systems and Cyber-Physical Systems

Modern control systems use the same underlying protocols that are used in IT and business networks, introducing security threats. For example, mobile code in the form of viruses, worms, and parasitic code, can manifest itself in network-enabled control system environments easily. Critical cybersecurity issues that need to be addressed include those related to the following: backdoors and holes in the network perimeter, vulnerabilities in common protocols, attacks on field devices, and communications hijacking and "man-in-the-middle" attacks. Key security issues arising from assumed trust are the ability of an attacker to re-route data that is in transit on a network, capture and analyze open critical traffic that is in plaintext format, and reverse engineer any unique protocols to gain command over control communications [4].

As for plant security, today's challenges include an increasing trend of disrupting critical infrastructure controls, cloud and secure remote access need driving the need for new security models, and today's control environments with "soft" middles and today's solutions not being geared to protect against threats like APTs. Solution capabilities lie in [15]: identity and policy, a new class of industrial focused security solutions, and in-line protection of critical machines via deep packet inspection of application traffic. In connecting these networks, and introducing IT components into the control system domain, security problems arise due to a number of aspects. They are: insecure connectivity to external networks, usage of technologies with known vulnerabilities, control system technologies with limited security, increasing dependency on automation and control systems, control system communications protocols being absent of security functionality, and considerable amount of open source information being available regarding control system configuration and operations [4].

Highly-privileged access to equipment sensors and controllers is a serious threat. Control systems are increasingly becoming remotely accessible and linked to the corporate networks or to other factories through the manufacturing grid. It is easy for malicious users, potentially from a business/manufacturing partner, to launch their attacks and compromise equipment sensors or controllers. For example, an attacker may develop Stuxnet-like malware, featuring zero-day exploits, rootkits, anti-virus evasion techniques, and process injection and hooking code, to target a specific process step within the entire chip manufacturing process. Techniques for detecting tampering, and validating the inputs provided by the sensors are of paramount importance [16]. Some examples of adversarial incidents are listed in Table 3 [17].

Table 3. Example Adversarial Incidents.

Threat Event	Description
Malware on Control Systems	Malicious software (e.g., virus, worm, Trojan horse) introduced into the system.
Control Logic Manipulation	Control system software or configuration settings modified, producing unpredictable results.
Safety Systems Modified	Safety systems operation are manipulated such that they either (1) do not operate when needed or (2) perform incorrect control actions that damage the ICS.
Spoofed System Status Information	False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators.
Denial of Control Action	Control systems operation disrupted by delaying or blocking the flow of information, denying availability of the networks to control system operators or causing information transfer bottlenecks or denial of service by IT-resident services (such as DNS).
Control Devices Reprogrammed	Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, alarm thresholds changed, or unauthorized commands issued to control equipment, resulting in possible damage to equipment and premature shutdown of processes, etc.

Factory floor technology includes networks, servers and end point computers, but it also includes cyber-physical systems. ICSs typically run specially designed operating systems and communications protocols and can have catastrophic physical safety consequences if they are compromised [8]. An ICS consists of combinations of control components that act together to achieve an industrial objective such as manufacturing. Traditional information technology (IT) security policies focus primarily on confidentiality with network availability being the lowest security priority. In contrast, ICSs, especially those considered critical infrastructure, must maintain a high level of system availability and operational resilience for many reasons including economic, environmental, human safety, and national security. Indeed, ICSs security must include elements of resilient physical design (redundancy and physical adaptability) in additional to network security to maintain acceptable system availability. Security devices should be deployed throughout the network. Firewalls also have the capability to perform device authentication, encryption, and deep packet inspection [18]. Table 4 [19] shows some typical differences between IT systems and control systems.

Table 4. Some Typical Differences between IT Systems and Control Systems.

Security Topics	Information Technology Systems	Control Systems
Anti-virus/Mobile Code	Common, widely used	Uncommon/Impossible to deploy effectively
Component Lifetime	2-3 Years, diversified vendors	Up to 20 years, single vendor
Outsourcing	Common, widely used	Operations are often outsourced, but not diverse to various providers
Application of Patches	Regular, scheduled	Rare, unscheduled, vendor specific
Change Management	Regular, scheduled	Highly managed and complex
Time Critical Content	Generally delays accepted	Delays are unacceptable
Availability	Generally delays accepted	24x7x365 (continuous)
Security Awareness	Moderate in both private and public sector	Poor except for physical
Security Testing/Audit	Part of a good security program	Occasional testing for outages
Physical Security	Secure (server rooms, etc.)	Remote/Unmanned Secure

Major security objectives for an ICS implementation should include the following: restoring the system after an incident, maintaining functionality during adverse conditions, protecting individual ICS components from exploitation, restricting physical access to the ICS network and devices, and restricting logical access to the ICS network and network activity. Some of the common technologies include: logical network separation enforced by encryption or network device-enforced partitioning, physical network separation to complete prevent any interconnectivity of traffic between domains, and network traffic filter which can utilize a variety of technologies at various network layers to enforce security requirements and domains. Boundary protection devices help protect the ICS against malicious cyber adversaries. They include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, encrypted tunnels, managed interfaces, mail gateways, and data diodes [17].

Cyber-physical systems (CPSs) are complex, multi-disciplinary, physically-aware next generation engineered systems that integrate embedded computing technology (cyber part) into the physical phenomena by using transformative research approaches. CPSs must operate in real-time. Integrity refers to the property of a system to protect itself or information within it from unauthorized manipulation or modification to preserve correctness of the information. High integrity is one of the important properties of a CPS. CPSs need to be developed with greater assurance by providing integrity check mechanisms on several occasions (such as data integrity of network packets, distinguishing malicious behaviors from the ambient noise, identifying false data injection and compromised sensor/actuator components etc.) [20]. Differences between corporate IT security and CPSs security are [21]:

- Software patching and frequent updates are not well suited for control systems. For example, upgrading a system may require months of advance in planning of how to take the system offline; it is, therefore, economically difficult to justify suspending the operation of an industrial computer on a regular basis to install new security patches.
- Control systems are autonomous decision making agents which need to make decisions in real time. Real-time availability provides a stricter operational environment than most traditional IT systems.
- By comparison to enterprise systems, control systems exhibit comparatively simpler network dynamics. Implementing network intrusion detection systems may be easier than in traditional enterprise systems.

4. Cybersecurity in Advanced Manufacturing

4.1. General Cybersecurity in Manufacturing

The equipment necessary for manufacturing can be rendered unavailable through cyber-attacks such as Stuxnet. Stuxnet is a computer worm that has been found in industrial control systems worldwide. Manufacturing systems are more than a collection of control systems. Therefore, manufacturing enterprises must be cognizant of cyber threats from initial design through final inspection to product use. While there are many opportunities to create new efficacies by harnessing the power of big data in manufacturing, there are also substantial risks. We distinguish vulnerabilities in the context of manufacturing cyber security as intrusive and interceptive. Intrusion refers to physical or remote (cyber) entrance into a system. Interception refers to data being compromised while flowing from one node to another along an edge. Interception may occur as information and physical data move through a supply chain. The key aspects to address are the requirement of data identification, tracking, and encryption during any of the data exchanges. The information a manufacturer gathers about its cyber risk (i.e., threats, vulnerabilities, and consequences) needs to be included in its existing risk management processes [1].

IT solutions don't always fit the manufacturing sector. Manufacturers often have a mix of old and new equipment. The new can be secured, but securing the old is much more difficult, and the old has to work with the new. Interconnected supply chains with a lot of data sharing may be especially vulnerable if they use small company suppliers who don't recognize cybersecurity risks in manufacturing [30]. For Industry 4.0, the radical digitization of production and products makes manufacturing companies even more vulnerable to cyber-assaults [22].

Manufacturing network requirements include the following aspects [23]: 1) industrial protocols; 2) topologies, resiliency, and industrial environments; 3) determinism, latency, and jitter, etc.; 4) motion control and safety; and 5) IP addressing (static). Manufacturing and enterprise security design deals with the following [23]:

- Physical security – limit physical access to authorized personnel: areas, control panels, devices, cabling, and control room.
- Network security – infrastructure framework, e.g. firewalls with intrusion detection and intrusion prevention systems (IDS/IPS), and integrated protection of networking equipment such as switches and routers.
- Computer hardening – patch management, antivirus software as well as removal of unused applications, protocols, and services.
- Application security – authentication, authorization, and audit software.
- Device hardening – change management and restrictive access.

4.2. Cloud-Based Design and Manufacturing

Cloud-based design and manufacturing (CBDM) is a product realization model. Because of the diversity of cyber resources constituting CBDM systems and because CBDM systems are Internet-enabled and rely on cyber-physical platforms. Traditional cyber defense is no longer applicable on many levels. CBDM systems will require sophisticated cybersecurity infrastructures to protect their highly sensitive and valuable assets. One particular trend, as evidenced by standards being developed such as TAXII, STIX, and CyBEX, is the development of cyber threat information exchanges that can be used for automated and active response to real-time cyber-attacks. These standards and the resultant technologies are likely to play a key role in securing CBDM systems [3].

A challenge for adopting CBDM is how to address cyber security threats including malicious activity, made possible by the provision of shared computing resources as well as inadvertent loss of confidentiality or integrity resulting from negligence or mismanagement. For enhancing cyber security, it was suggested that service providers must offer capabilities including 1) a test encryption schema to ensure the shared storage environment safeguards all data; 2) stringent access controls to prevent unauthorized access to the data; and 3) scheduled data backup and safe storage of the backup media [24]. Table 5 shows the strengths, weaknesses, opportunities, and threats of CBDM.

Table 5. SWOT Analysis for CBDM [24].

Strengths	Weaknesses
• Pay-per-use	
• Resouce pooling	• Reliability
• Agility and scalability	• Data ownership
• Ubiquitous data access	• Less control over data
• On-demand self-service	
Opportunities	**Threats**
• Low upfront cost	
• Collective innovation	• Outage
• Enhanced collaboration	• Security
• Shorter time-to-market time	

4.3. Cybersecurity for Hardware and Software in Manufacturing

The following are some cyber-physical vulnerabilities in manufacturing processes [25]:

(1) Attacks on cyber-physical systems (CPS): CPS are systems that integrate physical hardware with software systems, often with the use of a network. With the growth of the Internet of Things (IoT), the number of CPS systems on networks continues to increase. Cyber-attacks have become more prevalent, increasing in maliciousness and decreasing in visibility.

(2) Cyber-attacks on manufacturing: attacks on CPS are even more alarming when the increasing amount of networked devices are connected to machines in manufacturing. An attack could be designed to cause a process to produce faulty parts.

As for hardware attacks, chip hardware generally can't be changed after the chip leaves the factory. Thus, malicious hardware can only be inserted by someone who can access and alter the design for a chip before it is manufactured and placed in a product. Once malicious hardware has been built into a chip, a hardware attack can be initiated and act in a lot of ways. Insertion of malicious hardware during manufacturing is very difficult because the insertion process itself will possibly lead to impairments that would be detected during post-manufacturing testing. One possibility is that a company performing outsourced design services could intentionally provide a corrupted design. Alternatively, the design services company could store the designs on weakly secured networks, enabling the designs to be accessed and altered by an outside party. It is also possible for one or more individuals within the design services company to corrupt a design without the knowledge of their colleagues or managers. As for the challenge of testing, the testing procedures are very good at identifying accidental design flaws, but are poorly suited to ferreting out intentionally hidden malicious circuitry [26]. The following steps could reduce the likelihood and impact of hardware attacks [26]:

- A change in design practices within the semiconductor industry: a designer working on a portion of a chip devoted to receiving wireless data does not need access to the internal details of a portion of the chip that processes video for display on the screen.
- Establishment of a national-level capability to coordinate a quick response to an attack
- Improved testing procedures to detect corrupted chips before they are placed into products
- Inclusion of built-in defenses into chips to identify and thwart attacks as they occur.

Manufacturing security is a key component of global assurance programs of Huawei Company in China. To address manufacturing security risk and ensure the integrity of hardware and software, Huawei implements end-to-end processes to prevent tampering, including such risks as unauthorized hardware replacement, software implantation or tampering, and virus infection [27]. Huawei uses key software security management methods and software is treated as confidential data within Huawei [27]:

(1) R&D personnel release software only via a secure internal system and all software information is managed as confidential data within the company, with only designated personnel being allowed to receive software update information.

(2) Designated authorized personnel download the software from the R&D software library Product Data Management System (PDM) to the Cooperation-Manufacturing Execution System (C-MES), a secure manufacturing distribution system. The software is verified by other authorized personnel. The C-MES server automatically verifies and records changes to the server on a daily basis and releases corresponding reports.

(3) Robust physical security processes are implemented for the equipment room and production preparation management.

4.4. Cybersecurity in Direct Digital Manufacturing and Additive Manufacturing

Direct digital manufacturing (DDM) involves fabricating physical objects from a data file using computer-controlled processes with little or no human intervention. It includes additive manufacturing (AM), 3D printing, and rapid prototyping [28]. Digitization of manufacturing increases the risks for theft, disruption, and sabotage. There are vulnerabilities in preproduction software, data storage and data transfers, the Stereo Lythography (STL) file format, and printer components, etc. The risks for an industrial DDM system can be theft (processes and property), disruption (slowing or stopping the DDM process), and sabotage (inserting unforeseen time-delayed failures) [29]. The following recommendations were given [29]:

- Mandatory scanning of system prior to deploying to the network and disable all unneeded communications/system processes.
- Review of user accounts/groups on the system including their level of privilege and adjust accordingly.
- Removal of all unneeded applications installed on the system (browsers, readers, games, etc.).
- Enable host-based firewall to allow communication via secure ports to know IP addresses for manufacturer communications (disable this connectivity when not in use).
- Processes developed for system updates/upgrades.

Additive manufacturing techniques have been described by different terms with slightly different meanings such as three-dimensional (3D) printing and solid free-form fabrication. Advances in cybersecurity are needed to address additive manufacturing issues such as theft due to portability of designs and ease of replication [31].

One of the key advantages of AM is its digital thread. This also presents opportunities for cyber-attacks. For example, voids can be placed inside of a part and the material properties of internal layers can be changed without affect the exterior layers. There is a need to look at AM systems to determine what vulnerabilities exist and how to prevent and mitigate the threat of cyber-attacks. The digital nature of the additive manufacturing process chain, shown in Figure 1, provides an opportunity for a cyber-attack. There are four main steps on the process chain where an attack could take place: the CAD model, the.STL file, the toolpath file, and the physical machine itself. The.STL file was the most vulnerable attack vector due to its universality and ease of editing [25].

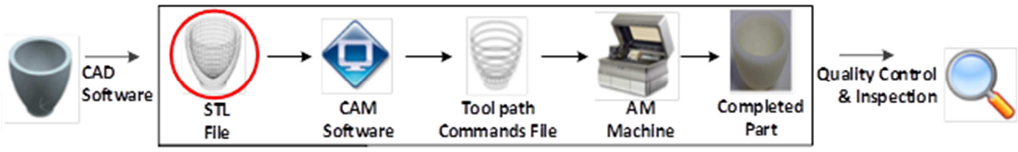

Fig. 1. Additive Manufacturing Process Chain [25].

Better monitoring systems and procedures should be developed to detect attacks. The following recommendations were given [25]: 1) improved software checks, 2) hashing/secure signing – allowing users to check that the file they receive is the same as the one that was sent, and 3) improved process monitoring by observing physical parameters such as the melt pool temperature indirectly from machine settings such as laser power, attacks are more likely to be discovered.

Manufacturing presents a unique set of problems combining cyber plus industrial control system (ICS) vulnerabilities. Existing cybersecurity controls may not be sufficient in a DDM environment. The problem is not unique to AM, but AM presents a significant opportunity to build security in [30].

5. Big Data Analytics for Cybersecurity in Advanced Manufacturing

Compared with traditional attacks, advanced persistent threats (APT) have unique characteristics [32]:

- APTs make frequent use of zero-day exploits or modify/obfuscate known ones and, thus, are able to evade the majority of signature-based end points and network intrusion detection solutions.
- Attackers focus on a specific target and are willing to spend significant time and explore all possible attack paths until they manage to subvert its defenses.
- For major APT attacks, some perpetrators are supported by nation-states that have significant enabling capabilities for cyber-attacks.
- APTs are highly selective. Only a small and carefully selected number of victims are targeted, usually in nontechnical departments, as they are less likely to identify.

Due to these characteristics, current cyber security solutions cannot provide an effective defense against such threats. Big data analytics facilitates APT detection by supporting [32]:

- Dynamic and managed collection, consolidation, and correlation of data from diverse data sources, such as network traffic, operating system artefacts, and event data. This holistic view of the infrastructure enables defenders to correlate sporadic low-severity events as a result of an ongoing attack.
- Anomaly detection, based on correlation of recent and historical events. The ability of Big Data analytics to correlate data from a wide range of data sources across significant time periods will result in a lower false positive rate and allow the APT signal to be detected in the noise of authorized user activities.

Big data has no clear definition, but it isn't wholly about size. Rather, it's defined based on at least three primary characteristics, also known as the 3Vs: volume, variety, and velocity. Variety refers to different types of data and their sources (sensors, devices, social networks, the Web, mobile phones, and so on) [33].

Real-time control in manufacturing generates big data. The manufacturing sector generates more big data than many other sectors. Table 6 [5] shows the perceptions about prevention & detection of anomalous & malicious traffic that is the survey conducted by Ponemon Institute LLC.

Table 6. Perceptions about Prevention & Detection of Anomalous & Malicious Traffic (Strongly agree and agree response combined).

Perceptions	FS	Manf	Gov
A strong defense against hackers and cyber criminals requires a quick containment of anomalous and malicious traffic in networks	66%	60%	55%
Big data analytics in cyber defense is considered very important	53%	48%	41%
Insufficient in-house personnel or expertise to analyze anomalous and potentially malicious traffic in networks	40%	52%	59%

The challenge in manufacturing is the integration of the equipment such that all levels of production may communicate. CPS shows the promise of potential applications in manufacturing. Big data is relevant to non-technical systems and IT systems, but becomes even more interesting when applied in the context of CPS due to the implications of physicality in terms of capabilities, technical risks and costs [34].

6. Conclusion

Factories in the future are of high-level in customization and quality, of high-level in communication and data storage via cloud, and rapidly adaptable to production lines. Advanced manufacturing and production systems are intelligent and digitizing systems with remote monitoring. Industrial control systems (ICSs) use some underlying protocols that are used in IT and business networks, introducing security threats. However, there are some differences between IT systems and industrial control systems. ICSs, especially critical infrastructure, must maintain a high level of system availability and operational resilience. There are also some differences between IT systems and CPSs in cybersecurity. High integrity is one of the important properties of a CPS.

Manufacturing systems are more than a collection of industrial control systems. Manufacturing enterprises must be cognizant of cyber threats from initial design through final inspection to product use. For ensuring the integrity of hardware and software and reduce manufacturing security risk, sometimes it is necessary to implement end-to-end processes to prevent tampering. CBDM systems require sophisticated cybersecurity infrastructures to protect their highly sensitive and valuable assets. Cybersecurity in direct digital manufacturing and additive manufacturing are an important area. Big Data analytics helps correlate data from a wide range of data sources. This holistic view of Big Data analytics facilitates APT detection and improves cybersecurity in advanced manufacturing.

References

[1] M. J. Hutchins, R. Bhinge, M. K. Micali, S. L. Robinson, J. W. Sutherland, D. Dornfeld (2015). Framework for Identifying Cybersecurity Risks in Manufacturing. *Procedia Manufacturing*, 1, 47–63.

[2] Honeywell (2011). Cyber Security in Manufacturing & Production, Whitepaper, Honeywell International Inc., August 2011.

[3] J. L. Thames (2014). Chapter: Distributed, Collaborative, and Automated Cybersecurity Infrastructures for Cloud-based Design and Manufacturing Systems. *Cloud-Based Design and Manufacturing (CBDM): A Service-Oriented Product Development Paradigm for the 21st Century*, Springer International Publishing, 17 June 2014, 207-229.

[4] M. Fabro, T. Nelson (2007). Control Systems Cyber Security: Defense-in-Depth Strategies. Idaho National Laboratory (INL), Technical Report: INL/CON-07-12804, USA, October 2007.

[5] Ponemon (2013). Big Data Analytics in Cyber Defense. Ponemon Institute Research Report.

[6] A. Ballard (2014). Network & Security Services, Lecture, Rockwell Automation.

[7] B. Haan (2015). Cybersecurity Trends 2015, Whitepaper, TÜV Rheinland i-sec GmbH.

[8] NDIA (2014). Cybersecurity for Advanced Manufacturing, White Paper, prepared by National Defense Industrial Association's Manufacturing Division and Cyber Division, May 5, 2014.

[9] S. J. Hutchison (2013). Cybersecurity: Defending the New Battlefield, Defense AT&L, November–December 2013, 34-39.

[10] G. Zhao (2011). Wireless Sensor Networks for Industrial Process Monitoring and Control: A Survey. *Network Protocols and Algorithms*, *3*(1), 46-63.

[11] J. Sen (2009). A Survey on Wireless Sensor Network Security. *International Journal of Communication Networks and Information Security*, *1*(2), 55-78.

[12] Y. Wang, G. Attebury, and B. Ramamurthy (2006). A Survey of Security Issues in Wireless Sensor Networks. *IEEE Communications Surveys and Tutorials*, *8*(2), 2-23.

[13] V. N. Inukollu1, S. Arsi1 and S. R. Ravuri (2014). Security Issues Associated with Big Data in Cloud Computing. *International Journal of Network Security & Its Applications (IJNSA), 6*(3), 45-56.

[14] S. Karnouskos (2015). Industrial Agents Cybersecurity, Chapter 6, in *Industrial Agents: Emerging Applications of Software Agents in Industry*, Elsevier, 109-120.

[15] T. Long, J. McGill (2014). Securing manufacturing networks and data from cyber attacks, Lecture, Cisco.

[16] M. B. Salem (2012). Security Challenges and Requirements for Control Systems in the Semiconductor Manufacturing Sector. *NIST Workshop on Cyber-Security for Cyber-physical Devices*, April 23rd, 2012.

[17] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, A. Hahn (2014). Guide to Industrial Control Systems (ICS) Security. *NIST Special Publication* 800-82, National Institute of Standards and Technology, Gaithersburg, MD, USA, May 2014.

[18] R. Candell, D. M. Anand, and K. Stouffer (2014). A Cybersecurity Testbed for Industrial Control Systems. *2014 Process Control and Safety Symposium*, Houston, TX, October 6-9, 2014.

[19] D. Kuipers, M. Fabro (2006). Control Systems Cyber Security: Defense in Depth Strategies. Idaho National Laboratory (INL), Technical Report: INL/EXT-06-11478, USA, May 2006.

[20] V. Gunes, S. Peter, T. Givargis, and F. Vahid (2014). A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems. *KSII Transactions on Internet and Information Systems*, *8*(12), 4242--4268.

[21] A. A. C´ardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry (2009). Challenges for Securing Cyber Physical Systems. *Workshop on Future Directions in Cyber-physical Systems Security*, DHS, July 2009.

[22] H. Brauser, F. Hammermeister, G. Schmidt, C. Krohn (2015). Cyber-security: managing threat scenarios in manufacturing companies. Technical Report, Roland Berger Strategy Consultants, Germany, March 2015.

[23] B. Barnes, G. Wilcox (2009). Manufacturing & IT Network Convergence. Lecture, Cisco.

[24] D.-Z. Wu, D. W. Rosen and D. Schaefer (2014). Cloud-Based Design and Manufacturing: Status and Promise, Springer International Publishing, Switzerland.

[25] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, R. Parker (2014). Cyber-physical vunerabilities in additive manufacturing systems. Technical Report, Virginia Polytechnic Institute and State University, 2014.

[26] J. D. Villasenor (2011). Ensuring Hardware Cybersecurity. *Issues in Technology Innovation*, Number 9, The Center for Technology Innovation, Washington, DC, USA, May 2011, 1-9.

[27] J. Suffolk (2013). Cyber Security Perspectives: Making cyber security a part of a company's DNA -A set of integrated processes, policies and standards. Technical Report, 2013 Huawei Technology Co., Ltd.

[28] C. Paulsen (2015). Reports on Computer Systems Technology. *Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium*, National Institute of Standards and Technology, Gaithersburg, MD, USA, April 2015, pp. iii-v.

[29] S. Zimmerman, D. Glavach (2015). Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing Systems. *Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium*, National Institute of Standards and Technology, Gaithersburg, MD, USA, April 2015, 51-54.

[30] M. F. McGrath (2015). Cybersecurity for Advanced Manufacturing – Securing the Digital Thread. *Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium*, National Institute of Standards and Technology, Gaithersburg, MD, USA, April 2015, 65-66.

[31] S. S. Shipp, N. Gupta, B. Lal, J. A. Scott, C. L. Weber, M. S. Finnin, M. Blake, S. Newsome, S. Thomas (2012). Emerging Global Trends in Advanced Manufacturing. IDA Paper P-4603, Institute for Defense Analyses, Virginia, USA, March 2012.

[32] N. Virvilis, O. Serrano, L. Dandurand (2014). Big Data Analytics for Sophisticated Attack Detection. *Isaca Journal*, 3, 1-5.

[33] C. Perera, R. Ranjan, L. Wang, S. U. Khan, A. Y. Zomaya (2015). Big Data Privacy in the Internet of Things Era. *IT Professional*, May/June 2015, 32-39.

[34] L. Wang, M. Törngren and M. Onori (2015). Current Status and Advancement of Cyber-Physical Systems in Manufacturing. *Procedia Manufacturing, Journal of Manufacturing Systems*, 37, 517–527.

Biography

Dr. Lidong Wang is an Associate Professor in the Department of Engineering Technology at Mississippi Valley State University, USA. He worked at Ohio State University, Mississippi State University, and the University of South Carolina; and conducted projects supported by the Department of Defense (DoD), the National Science Foundation (NSF), and the National Aeronautics and Space Administration (NASA). His current research interests include Big Data, cybersecurity, cyber-physical systems, and Industry 4.0, etc. He has published over 70 papers in various journals. He was the President of the Electricity, Electronics & Computer Technology (EECT) Division of the Association of Technology, Management, and Applied Engineering.