Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems

[1]Yao Pan, [1]Jules White, [1]Douglas C. Schmidt, [2]Ahmad Elhabashy, [2]Logan Sturm, [2]Jaime Camelio, and [2]Christopher Williams

[1]*Vanderbilt University, USA*
[2]*Virginia Tech, USA*

***Abstract* — The Internet of Things (IoT) has transformed many aspects of modern manufacturing, from design to production to quality inspection. In particular, IoT and digital manufacturing technol-ogies have substantially accelerated product development-cycles and manufacturers can now create products of a complexity and precision not heretofore possible. However, new threats to supply chain security have arisen from connecting machines to the In-ternet and introducing complex IoT-based systems controlling manufacturing processes. By attacking these IoT-based manufacturing systems and tampering with digital files, attackers can manipulate physical characteristics of parts and change the dimensions, shapes, or mechanical properties of the parts, which can result in parts that fail in the field. These defects increase manufacturing costs and allow silent problems to occur only under certain loads that can threaten safety and/or lives. To understand potential dangers and protect manufacturing system integrity, this paper presents two taxonomies: one for classifying cyber-physical attacks against manufacturing processes and another for quality inspection measures for counteracting these attacks. We systematically identify and classify possible cyber-physical attacks and connect the attacks with variations in manufacturing processes and quality inspection measures. Our taxonomies also provide a scheme for linking emerging IoT-based manufacturing system vulnerabilities to possible attacks and quality inspection measures.**

***Keywords* — Cyber-physical attack, Computer-aided Manufacturing, Cyber-physical system, Internet of Things.**

I. Introduction

THE Internet of Things (IoT) embeds electronics, software, and sensors into physical objects that collect and exchange data via network connections. IoT technologies have made manufacturing smarter by enabling manufacturing systems to evolve from loose collections of largely disjoint cyber and physical components into synergistic cyber-physical systems. The Internet-connected sensors, tooling, and control systems forming these IoT-based manufacturing systems enable the manufacturing and refinement of parts that previously were hard to produce cost-effectively.

The IoT plays an important role in improving the efficiency and productivity of manufacturing systems. For example, by connecting digital manufacturing technologies and Computer-Aided Engineering (CAE) tools, designers and manufacturing engineers can substantially accelerate the product development-cycle. The use of IoT-based manufacturing systems, however, also expands opportunities for cyber-physical attacks against these systems. In particular, older pre-IoT equipment was not Internet-accessible and thus not exposed to cyber-attack like newer IoT-based manufacturing equipment.

For instance, with IoT-based manufacturing systems, critical manufacturing files are stored in computers connected to the Internet, as shown in Fig. 1. It is possible for an attacker across the Internet to remotely intercept and alter design files or machine configurations to create undetectable changes in a part that adversely affect a product's design intent, performance, or quality [1], [2], [3], [4]. Since the parts being attacked are installed in automobiles, jet engines, or artificial heart valves, the results could financially devastate manufacturers, *e.g.*, by damaging equipment, incurring property losses, increasing warranty costs, losing customer trust, or threating human safety if these altered parts function improperly and fail in the field [2].

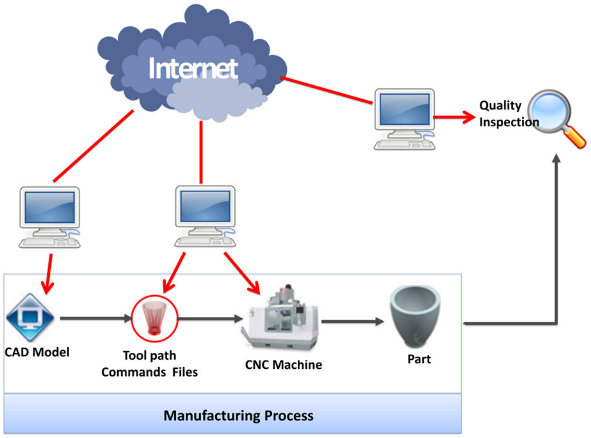


Fig. 1. Computers with Internet Connection in Manufacturing Systems.

A fundamental concern with IoT-based manufacturing systems is that they enable the monitoring and control of previously non-remotely accessible physical systems. If these Internet-connected IoT devices are not protected, the physical systems that they influence, such as the parts that a manufacturing facility produces, may be damaged. A famous example of critical IoT-based infrastructure being attacked is the Stuxnet malware that damaged nearly one-fifth of Iran's nuclear centrifuges [5]. The Stuxnet malware targeted programmable logic controllers and forced physical equipment to operate outside its design tolerances and led to centrifuge failures.

Past IoT security research has explored cyber-vulnerabilities in industrial control systems, such as Supervisory Control and Data Acquisition (SCADA) controllers [6], which can force physical systems to operate outside of their safety tolerances. While these control systems are a crucial area of research, IoT-based manufacturing systems are also vulnerable to silent attacks that result in a manufactured part's physical characteristics no longer matching their design specifications, which could lead to critical and/or pre-mature failures in the field. Similar research has looked at flaws injected into computer hardware and software logic [7], [8]. Much less research, however, has focused on flaws injected into the physical parts themselves, which have no computational logic.

DOI: 10.9781/ijimai.2017.437

In contrast to traditional cyber-security, IoT-based manufacturing systems use physical equipment, which generates measurable phenomena (e.g., temperatures and vibrations) to produce physical products that can be inspected and tested to determine if they meet their requirements. In addition, a particularly vexing challenge of IoT-based manufacturing systems is that their underlying software and hardware is rarely updated [1], [2], [3]. This lack of updates leaves complex IoT-based manufacturing equipment exposed and vulnerable to attack on the Internet. Moreover, this update problem cannot be easily addressed, as IoT-based manufacturing equipment is often extremely costly to purchase, amortized over decades, and very expensive to take out of production operation. Techniques and tools are therefore needed to help protect the physical parts that IoT-based manufacturing systems produce, while recognizing that these systems will always be at risk of cyber-attacks.

Fortunately, cyber-physical attacks against an IoT-based manufacturing system are unique in having correlated cyber *and* physical manifestation of the attack in the manufactured part. This correlation can be used to model and predict the relationships between attacks, process data, product quality observations, and side-channel impacts for the purpose of attack detection and diagnosis.

Hence, the work presented in this paper helps answer the following questions:

- What types of attacks are particular IoT-based manufacturing system processes vulnerable to?
- What facets of a part can be attacked in a given IoT-based manufacturing system?
- What quality inspection mechanisms could be put in place to lower risk in IoT-based manufacturing systems?
- How can quality inspection and side channel measurements mitigate cyber-vulnerabilities in IoT-based manufacturing system?
- How does a newly disclosed cyber vulnerability impact a particular IoT-based manufacturing process?

To answer these questions, we have created two taxonomies: one for classifying cyber-physical attacks against IoT-based manufacturing processes and another for quality inspection measures for counteracting these attacks. These taxonomies catalog IoT-based manufacturing processes, attacks, and quality inspection measures, as well as model the relationship between specific attack types, vulnerabilities, equipment, processes, and quality inspection measures. They also help to bridge the gap between (1) the IoT *cyber domain*, where the research subjects are cyber infrastructure and software vulnerabilities, and (2) the *physical domain*, which includes manufacturing processes and quality inspection measures.

Our taxonomies provide a framework that researchers and practitioners from both cyber-security and IoT-based manufacturing can use and augment to understand the scope of cyber vulnerabilities, how these vulnerabilities impact different processes, the types of cyber attributes that these attacks express, and their impacts on the physical properties of both the process execution and physical part outputs. This framework makes it easier to make decisions on cyber-physical security in manufacturing, catalog attacks and vulnerabilities as they emerge, and understand the relationship between specific attack types, equipment, processes, and side-channel impacts.

The remainder of this paper is organized as follows: Section II describes the taxonomies for the manufacturing process, cyber-physical attacks, and quality inspection measures; Section III explores a case study of a manufacturing industry partner using the proposed taxonomy; Section IV compares our research with related work; and Section V presents concluding remarks and future work.

II. Taxonomies

Our overarching goal is to connect vulnerabilities, IoT-based manufacturing processes, cyber-physical attacks and quality inspection measures all together, as we show in Fig. 2. The characteristics of the IoT-based manufacturing processes reveal the vulnerabilities that could be exposed, which would then determine what cyber-physical attacks could be launched. Each cyber-physical attack has its effects either in the physical domain or the cyber domain. We can choose the quality inspection measures that could capture the provisioned attack effects, thereby enabling better defenses against cyber-physical attacks in IoT-based manufacturing systems.

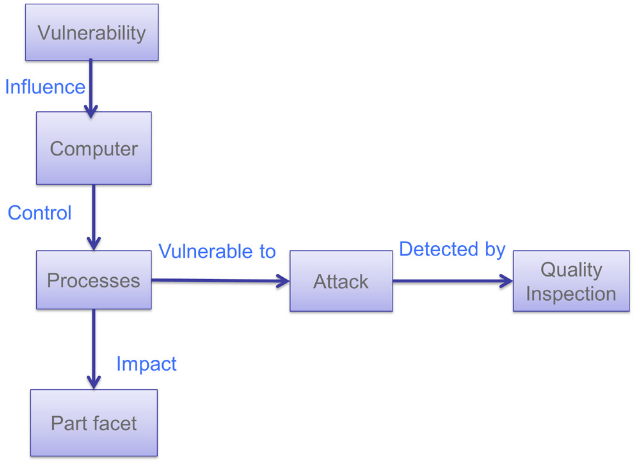


Fig. 2. Logic Flow in Manufacturing Processes.

A. Overview of Manufacturing Processes

Manufacturing systems are rarely the same for different types of manufactured products, but most of these systems share a similar workflow. A manufacturing system typically starts with product design, then procures raw material, goes through various manufacturing processes, followed by assembly and inspection for quality control, and finally distribution of the products, as shown in Fig. 3. Our taxonomies focus on the chain of process steps ranging from design to manufacturing with its different operations to inspection only, without considering other steps such as raw material procurement and distribution.

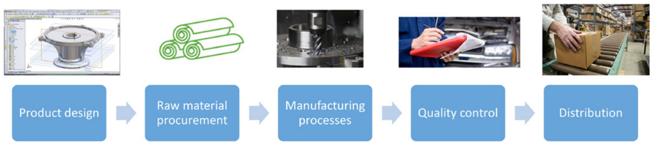


Fig. 3. Workflow of Manufacturing System.

A key differentiator between IoT-based manufacturing systems and traditional systems is that the former operate more like distributed software-reliant systems than the latter. Traditional manufacturing systems use significant numbers of manual steps and closed/locally managed control systems. Newer IoT-based manufacturing systems are remotely accessible and monitorable by designers, reconfigurable, and capture volumes of sensor and tool actuation data during operation. Moreover, these systems are driven by computer instructions that coordinate their constituent IoT sensors and tooling to produce a given part.

Since IoT-based manufacturing processes perform the set of steps through which raw materials are transformed into a finished product, this sub-section summarizes the basic and most commonly used manufacturing processes in industry today. In production systems, a combination of several processes may be required to manufacture a product, but understanding the characteristics of the essential and most common processes is important to build accurate taxonomies.

There are several methods [9], [10] [11] to classify the different manufacturing processes involved in production, such as dividing them into the two main groups shown in Fig. 4:

1. ***Processing operations***, which add value to materials by transforming them from one state to another. Process operations can be further divided into *solidification processes* (such as casting that pours material in a cavity to fill when it cools down), *deformation processes* (such as forming that changes the shape of the material, without usually changing its original volume), *subtractive processes* (such as machining that changes the shape of the material through removing some of it, thereby decreasing its volume), *additive processes* (such as 3D printing that builds the shape of the material progressively by accumulating thin layers one on top of the other), *surface processing* (such as surface finishing done as a final step to improve the quality of the surface of the current product), and others (such as heat treatment, which enhances the property of the material itself, and particulate processing, where particles are consolidated together).
2. ***Joining operations***, which bring two or more components together. Joining operations can be split into permanent joining processes (such as welding) and joining via mechanical components (such as fasteners).

An overview of such grouping can be seen in Fig. 4, along with some (non-exhaustive) examples for each sub-group. These sub-groups are not necessarily mutually exclusive, *e.g.*, a subtractive process may also be performed during surface processing operations.

Another concept we define is "part facet", which is a specific aspect or geometric structure of a part that is important to its performance. The facet type includes dimension (*e.g.*, length, width, height, radius, etc.), weight, center of gravity, color, magnetism, surface roughness, tensile strength, yield strength, etc. Each manufacturing process is restricted by its characteristics, so it can only affect a subset of the part facets. For example, a turning process can change the dimensions of the part. Likewise, a heat treatment can change the yield strength of the part.

B. Design Artifacts to Code

An interesting facet of IoT-based manufacturing is that design files, such as solid geometry representations of parts, are eventually translated into computer instructions, such as G-Code, for a set of IoT machines indicating how to manufacture the part [12]. This process is a form of model-driven engineering, which is also used in software development [13]. Many of the attacks are analyzed based on the instruction set limitations of manufacturing equipment, which are directly connected to the physical capabilities of the equipment, and provide cyber-physical bounds on attacks.

Due to the wide range of IoT-based manufacturing processes, this paper only concentrates on subtractive and additive processes, which serve as representatives of a larger group due to the fact that they are currently being used heavily in IoT environments. For example, in Computer Aided Manufacturing (CAM) the products within these processes are created through Computer Aided Design (CAD) software. The design is then realized by coordination of Computer Numerically Controlled (CNC) machines or 3D printers through a network and driven by computer programmed commands, rather than being controlled by hand. Such extensive use and reliance on IoT devices and software systems invites new cyber-physical threats. Due to the wide range of IoT-based manufacturing processes, this paper only concentrates on subtractive and additive pro-cesses, which serve as representatives of a larger group due to the fact that they are currently being used heavily in IoT environments[1].

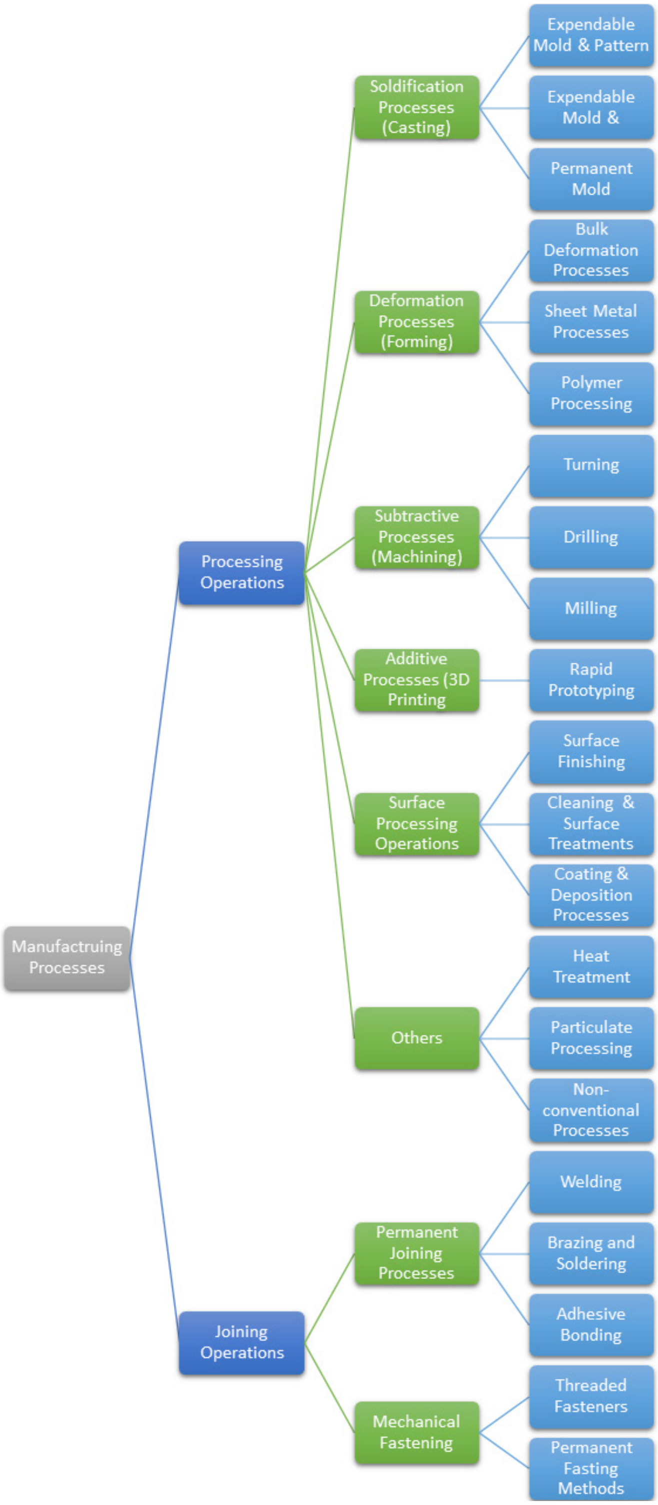

Manufactruing Processes
Processing Operations
Joining Operations
Soldification Processes (Casting)
Expendable Mold & Pattern
Expendable Mold &
Permanent Mold
Deformation Processes (Forming)
Bulk Deformation Processes
Sheet Metal Processes
Polymer Processing
Subtractive Processes (Machining)
Turning
Drilling
Milling
Additive Processes (3D Printing
Rapid Prototyping
Surface Processing Operations
Surface Finishing
Cleaning & Surface Treatments
Coating & Deposition Processes
Others
Heat Treatment
Particulate Processing
Non-conventional Processes
Permanent Joining Processes
Welding
Brazing and Soldering
Adhesive Bonding
Mechanical Fastening
Threaded Fasteners
Permanent Fasting Methods

Fig. 4. Manufacturing Processes Classification with Examples.

While subtractive and additive processes are significantly different, their integration into an IoT-based manufacturing system is relatively

[1] The attack taxonomy presented in Section II.C can also be applied to other manufacturing processes.

similar. Fig. 5 shows modern process chains for both an additive and a subtractive process, respectively. The process chain starts with a 3D CAD model, which is the digital representation of the shape and dimensions of an artifact.

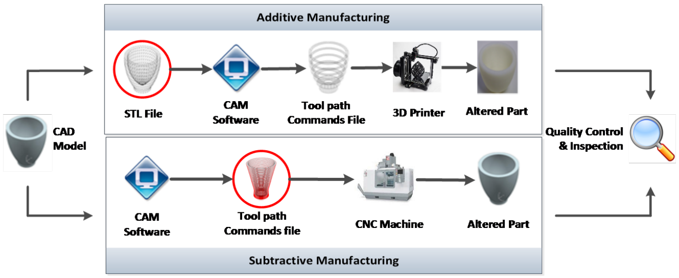


Fig. 5. Process Chains for Subtractive and Additive Manufacturing.

For subtractive manufacturing, the 3D CAD model goes directly to CAM software as modern CAD/CAM systems are integrated. After the CAM step is completed, a generic toolpath file is generated and sent to the IoT machine's controllers. In the process chains shown in Fig. 1, users have ready access to the toolpath, which provides a set of instructions for the tool regarding its direction, speed, and path.

In additive manufacturing, the CAD model is usually translated into an intermediary file format called an "STL" file, which represents the solid geometry with a list of triangu-lar facets that define a part's surface. Using machine-specific CAM software, this STL file is virtually sliced into layers that will be printed. Another algorithm generates commands (such as G-Code) that determine the additive manufacturing machine-specific toolpath to process each layer. This toolpath is generated locally on the machine or sent to a 3D printer's controllers across a network. These IoT systems allow designers to remotely print and monitor progress of different parts across the Internet.

In IoT-based manufacturing, each component of these process chains are linked through the IoT infrastructure, which poses potential risks of external cyber-physical attacks. In fact, two case studies [2], [3] conducted recently at Virginia Tech showed how to target a different component in each chain, as highlighted red in Fig. 5. In the case of the additive manufacturing process, a cyber-physical attack modified the STL file to create a part with an internal void [3]. In the case of the subtractive manufacturing process commands in the machine toolpaths were altered, thereby producing an incorrect part [2].

Examining the process chains of both additive and subtractive manufacturing demonstrates how vulnerable modern manufacturing is to cyber-physical attacks, *e.g.*:

- Both the STL and toolpath files are plain text without any encryption or encoding, which means these files can be intercepted and tampered/replaced. By modifying these files, attackers can bring parts out of specifications, add undesired part features, or alter part mechanical properties.
- An attack can propagate through an entire process chain. For example, altering a CAD file in transit across a network between IoT components will result in changes in the translated STL/toolpath file. If attacks cannot be prevented in previous processes, any quality inspection measures in later processes are meaningless.

C. A Taxonomy of Cyber-physical attacks against Manufacturing Processes

In this sub-section, we describe possible types of cyber-physical attacks against manufacturing system processes in IoT environments. An attack can be characterized by an *attack flow* where attackers first probe for a cyber vulnerability within the system, then exploit it with an appropriate attack vector to target a specific component within the manufacturing environment, producing a corresponding impact in form of a resulting attack. An example of an attack vector can be seen highlighted in red in Fig. 6, which also shows they key elements within an attack flow that could be described as follows:

(1) **Vulnerabilities** in the IoT-based manufacturing system can include a com-promised worker, OS/Software vulnerability, or weak authen-tication mechanism.

(2) **Attack Vectors** refer to paths where attackers can gain unauthorized access to the IoT system. Possible attack vectors include social engineering, malware like viruses or Trojans, insufficient authentication (attackers can get permission by brute force or bypass authentication), etc.

(3) **Attack Targets** are the actual assets (cyber or physical) being targeted by the attack. They can be manufactured products, the IoT machines used for manufacturing, or intellectual property, such as CAD design files or specifications.

(4) **Attack Impacts** result in different possible attack types, depending on the attack target. Those can be classified into three categories:

- **Confidentiality attacks** compromise the intellectual property of files, such as design model files. Design models may be highly confidential since they represent valuable business secrets for manufacturing companies. If these files are stolen by competitors and are used to reproduce similar products, substantial economic loss can be incurred for the company.
- **Availability attacks** affect the availability of manufacturing resources as they target manufacturing machines and tools. These attacks could deliberately slow down manufacturing processes by breaking down the controlling computers or damaging the manufacturing machines.
- **Integrity attacks** tamper with design models or configuration files of a manufacturing product line, thereby changing the geometric dimensions or mechanical properties of a part so it does not meet its designed requirements.

Based on the attack target, *integrity attacks* can be further categorized into *material attacks* and *structure attacks*, which are all shown in Fig. 6.

Material attacks are attacks that change the physical properties, such as material strength, surface roughness, color or magnetism of the manufacturing parts.

Structure attacks can change the following four types of geometric dimensions of manufacturing parts, as illustrated in [3]:

1. Scaling: a part is scaled up or down in one or more dimensions, resulting in various outcomes. For example, the part may no longer fit into other components or the part's mechanical properties may change by decreasing its strength.
2. Vertex movement: Some vertexes of a part have moved, which may not always change the part's external dimensions but alters the coordinates of certain vertexes internally. Vertex movement could result in fit issues or a change of mechanical properties.
3. Indents/protrusions: small indents or protrusions can be created on the surface of a part, resulting in fit issues or rough surface finish.
4. Internal void: a small volume created inside a part is not easily detectable by visual inspection since the void is completely enclosed. The void does not change the dimensions of a part. The void can impact a part's mechanical properties, e.g., if placed in a load bearing location, the void can make the part fail more easily. Additive manufacturing can create internal voids due to its layer-by-layer building process, but subtractive

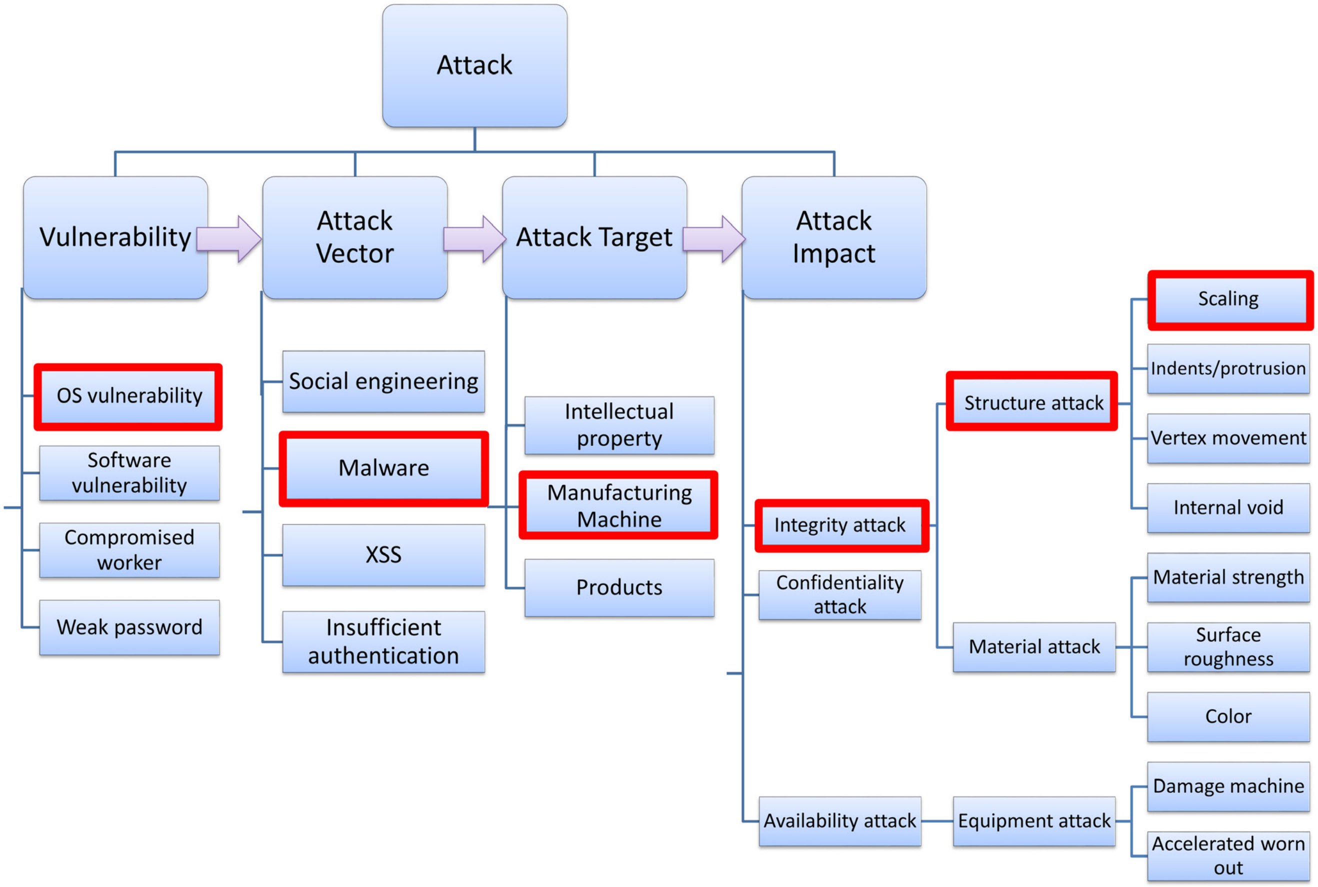


Fig. 6. Taxonomy of Cyber-Physical Attacks on Manufacturing Systems.

manufactur-ing cannot create internal voids.

Availability attack include *Equipment attacks* that aimed at IoT-based manufacturing equipment. For example, attackers can change machine configurations to force the equipment to operate outside its tolerance, causing damage to the machine, or accelerating wear and tear on the machine.

As shown with the red path in Fig. 6, an attack exploiting a vulnerability within the operating system, can apply a malware to target a manufacturing machine used in the facility. For instance, a structure attack could then affect the integrity of the machine through scaling the final product dimensions.

There is a relation between IoT-based manufacturing processes and cyber-physical attacks. Some attacks are only possible with the presence of certain manufacturing processes. For example, as previously mentioned, subtractive manufacturing processes, such as milling or turning generally, cannot create internal voids in manufactured parts. In contrast, 3D printing's flexibility makes it vulnerable to many kinds of at-tacks, including internal void attacks.

Table I presents a mapping between common manufacturing processes and their corresponding potential attack types. These relationships enable us to narrow down the possible attack types based on the manufacturing processes being used. In other words, after the desired attack type is determined, we can identify which specific manufacturing process would be affected; or we might even realize that the chosen attack type would not be possible and needs to be altered.

TABLE I. MANUFACTURING PROCESSES AND THEIR POTENTIAL ATTACKS.

Manufacturing Process	**Vulnerability to Attack Types**
Milling	Scaling, indents/protrusion, vertex movement, surface roughness
Turning	Scaling, surface roughness
Drilling	Scaling, indents/protrusion, vertex movement, surface roughness
3D printing	Scaling, indents/protrusion, vertex movement, internal void, material strength, color
Soldering	Material strength
Heat treatment	Material strength
Surface finishing	Color, surface roughness

D. A Taxonomy of Quality Inspection in IoT-based manufacturing Processes

We now present a second taxonomy of the quality inspection measures for manufacturing processes. Quality inspection "are measures aimed at checking, measuring, or testing of one or more product characteristics and to relate the results to the requirements to confirm compliance" [35]. It is an indispensable component in modern manufacturing to ensure products meet their quality requirements. Various quality inspection measures exist, each with its own pros and cons. For example, dimension measurement can detect scaling attacks, though it is ineffective against mechanical property attacks. It should just be noted that this quality inspection taxonomy has been developed assuming that the digital quality inspec-tion tools are not victims of cyber-physical attacks themselves; cyber-physical attacks compromising quality inspec-tion tools are beyond the scope of this paper.

Fig. 7 shows our taxonomy of quality inspection for manufacturing processes. These quality inspection measures can be applied to either the physical or the cyber domains of IoT-based manufacturing. The measures applied to the phys-ical domain usually measure the physical or mechanical properties of manufacturing parts to assess whether the de-sired requirements have been met. Based on the measured properties, quality inspection measures are usually non-destructive and can be classified into three groups: phys-ical characteristics, mechanical properties, and side-channel impacts. quality inspection measures for physical characteristics include visual inspection, dimension measure, weight measure, 3D laser scanning, X-rays, and CTs.

Mechanical properties refer to how parts behave under load. Mechanical properties include, but not limited to, strength (the resistance of a material to deformation from an external load), elasticity (the ability of a material to return to its original shape after the load is removed), and hardness (the ability of a material to resist indentation and scratching) [14]. These properties cannot be visually inspected, so tests must be run with specialized equipment to analyze these aspects of a part.

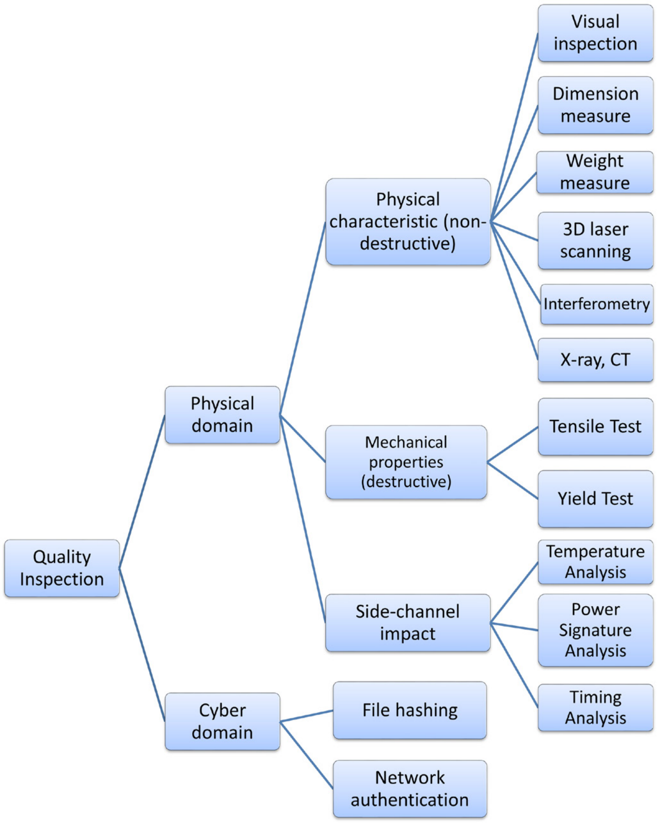


Fig. 7. A Taxonomy of Quality Inspection in Manufacturing Processes.

Side-channel impacts are mostly discussed in cryptography and refer to cases where attackers do not leverage information from plaintext or ciphertext, but from physical characteristics of cryptosystems. For instance, hardware has varying power consumption when doing different computations, such as adding and multiplying. By observing the power consumption of a cryptosystem, it is possible to deduce the key bits of RSA [19] or even to break the key [20]. Some other side-channel impacts include timing delays [20], electromagnetic leaks [21], temperature [22], or radiation [21]. Quality inspection in IoT-based manufacturing can measure side-channel impacts as well, to determine if a manufacturing process deviates from its designed specifications.

Quality inspection measures could be also combined with statistical analysis techniques since these tests may be expensive, destructive, or time consuming. Typical statistical analysis techniques are employed based on statistical models, in-cluding Statistical Process Control (SPC) [15], Six Sigma [16], acceptance sampling (where samples are chosen and analyzed in place of every part) [17], [18], etc.

In a way, the characteristics being measured are the parts facets, since it relates to its performance. Depending on such characteristics, linking quality inspection measures with the attack types described in Section II. C is important and can help determine which measures are effective against different attack types. A subset of the correspondences is shown in Table II. Again, cyber-physical attacks on quality inspection tools are not considered here.

TABLE II. CYBER-PHYSICAL ATTACK TYPES AND THEIR QUALITY INSPECTION MEASURES.

Attack Type	Effective Quality Inspection Measure
Scaling	Dimension Measure - Coordinate measure machine
Vertex movement	Dimension Measure - Coordinate measure machine
Indents/protrusion	Visual inspection
Internal void	X-ray, CT, side-channel information
Material strength	Tensile/yield strength test

E. *Deducing Attack Threats from Software Vulnerabilities*

A common misconception in the cyber-security community is that attacks can be avoided by simply employing the latest software versions and best practices. However, many IoT systems such as manufacturing equipment have long lifetimes, prohibitively high upgrade costs and need to remains operational continuously, and therefore cannot be migrated to the latest operating systems or manufacturing software versions. A key challenge, therefore, is to protect a complex IoT-based manufacturing process built on equipment with buggy or outdated software that cannot be easily upgraded to newer and more secure versions.

The cyber infrastructure refers to the computing equipment controlling physical manufacturing processes. Each computer equipment has several characteristics, such as operating system version (Windows XP, Windows 7, etc.), manufacturing software version (CAD, CAM software), and network connectivity status (Internet, LAN or None). The characteristic of the computers can be mapped to the exploitability vectors of vulnerabilities. A vulnerability with an access vector of “Internet” will only affects computers with an Internet connection.

To determine what attacks could be launched with known cyber vulnerabilities within the cyber infrastructure and what quality inspection measures should be taken to detect possible attacks, we have connected our attack taxonomy with the National Vulnerability Database (NVD) [23]. The NVD is a U.S. government repository of vulnerability management data, which uses the Common Vulnerability Scoring System (CVSS) [24] to evaluate the severity of vulnerabilities. The CVSS defines a set of metrics to describe the characteristics of vulnerabilities. The metrics includes six vectors that are described below. The first three of these vectors in CVSS are organized in terms of exploitability:

- **Access Vector** (AV) measures an attacker’s ability to successfully exploit a vulnerability based on how remote an attacker can be from a networking perspective [25]. There are three possible values for Access Vector: Local, Adjacent Network, and Network. An Access Vector of value “Network” (AV: N) means the vulnerability must be exploitable without requiring physical (*i.e.*, local) or adjacent network access. Often, AV: N vulnerabilities can be exploited from IP addresses on the Internet. An Access Vector of value "Adjacent Network" means the vulnerability must be exploitable through a broadcast or collision domain. An Access Vector of value "Local" means the vulnerability must only be exploitable via physical access, such as proximity to a device or local shell access.

- **Access complexity** measures the complexity of the attack required to exploit the vulnerability after the attacker gained access to the target system already [25].
- **Authentication** measures the number of times an attacker needs to authenticate to the target system to exploit a vulnerability [25].

The Access Complexity and Authentication vectors describe the degree of difficulty, but not possibility of an attack, which are not relevant to our taxonomy, so we omit their discussions here.

Three other vectors in CVSS are organized in term of impact:

- The **Confidentiality Metric** measures the attacker's ability to obtain unauthorized access to information from an application or system [25]. If no information or data is exposed due to exploitation, the Confidentiality metric receives a value of "None". If only partial information is disclosed due to exploitation (the attacker cannot control what is obtained), the Confidentiality metric receives a value of "Partial". If an attacker has complete read access to all information and data on a system, the Confidentiality metric receives a value of "Complete". The compromise of confidentiality metric means the vulnerability can help attackers gain "read" access to the system. The "read" access will make it possible to launch confidentiality attacks that are discussed in Section II.C.
- The **Integrity Metric** measures an attacker's ability to manipulate or remove data from a product or system [25]. There are three possible values for this metric: None (I: N), Partial (I: P), and Complete (I:C). "None" is used when vulnerability exploitation cannot manipulate data. For example, an information leak only exposes information but unauthorized modification is not possible. A "Partial" impact to Integrity implies limited or uncontrolled modifications to files are possible by exploiting a vulnerability. An Integrity metric of "Complete" means an attacker is able to modify any system files or data in the system. The compromise of integrity metric means the vulnerability can help attackers gain "write" access to the system. The "write" access will make it possible to launch integrity attacks. Integrity attacks usually need to change the critical part of design files or machine configurations, a "partial" impact is not sufficient because attackers cannot make predictable changes. The partial value is therefore treated the same as no value.
- The **Availability Metric** measures an attacker's ability to disrupt or prevent access to services or data [25]. Vulnerabilities can impact availability by affecting hardware, software, and network resources. For example, vulnerabilities can make it possible for attackers to flood network bandwidth, exhaust CPU or system memory. There are three possible values for this metric: None (A: N), Partial (A: P), and Complete (A: C). The compromise of availability metric means it is possible to launch availability attacks.

We now examine some vulnerabilities from the NVD to see how they can be connected to our proposed taxonomy. As shown in Table III, CVE-2014-7268 is a vulnerability whose description is "*Buffer overflow in AClient in Symantec Deployment Solution 6.9 and earlier on Windows XP and Server 2003 allows local users to gain privileges via unspecified vectors*." As shown in Table III, the prerequisites of vulnerability CVE-2014-7268 are installations of Symantec Deployment Solution on Windows XP or Server 2003 operation systems and local access to the computers involved in the IoT-based manufacturing process. If these prerequisites are met, this vulnerability can be exploited to launch attacks that result in "complete" confidentiality, integrity, and availability impacts, which means all the attacks in our taxonomy shown in Fig. 6 could be launched by exploiting this vulnerability.

TABLE III. EXAMPLE VULNERABILITY AND METRICS.

Vulnerability	Metric	Value
CVE-2014-7286	Vulnerable software	Symantec Deployment Solution 6.9 or earlier on Windows XP or Windows server 2003
	Access vector	Local
	Confidentiality	Complete
	Integrity	Complete
	Availability	Complete
CVE-2015-2453	Vulnerable software	Windows vista, 7, 8, 8.1, server 2008, 2012
	Access vector	Local
	Confidentiality	Complete
	Integrity	None
	Availability	None

Table III also shows the metrics for vulnerability CVE-2015-2453, which is documented as "*The Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to obtain sensitive information via a crafted application that continues to execute during a subsequent user's login session, also known as "Windows CSRSS Elevation of Privilege Vulnerability"*." This vulnerability just impacts confidentiality, so only confidentiality attacks can be launched and manufacturers need not prepare for integrity attacks or availability attacks. Moreover, manufacturers need not do anything if the manufacturing design files are publically available, *i.e.*, intentionally not confidential.

III. Case Study

An increasing number of manufacturing companies have embraced the Internet of Things to revolutionize the way they manufacture. Information technology infrastructure has been used extensively in design, manufacturing processes and quality inspection for accessing the information of physical objects and for manipulating them. The tight integration of hardware and software enables a more efficient production management. While modern manufacturing companies are enjoying the benefits the IoT brings, most of them are unaware of the potential cyber-security risks they may face.

To demonstrate how our taxonomies can be applied to modern manufacturing systems to assess cyber-security risks, we visited an industry partner to collect related information and map them to our approach. This company provides additive manufacturing services that allow customers to submit their own parts designs to facilitate production.

The general process flow of this company is shown in Fig. 8. A customer submits parts through a web portal or directly through email to a product engineer, who then coordinates with the customer to determine the printability and best material/process. The part files (in CAD or STL format) will be saved to the network drive. The process engineer checks the file for common problems, such as thin walls or extra shells, and adjusts the files if necessary. Machines will also be checked before printing. After that, the parts will be printed (along with witness bars) and will go through quality inspection measures. If the parts pass inspection, they will be shipped to customers; otherwise, they will be scrapped or reworked.

The Information Technology (IT) infrastructure in this manufacturing company consists of three categories of computers: engineers' computers, 3D printer computers, and inspection station computers. Files are stored on a networked server connected to all computers. There are no restrictions on USB drives and all computers have USB access. No personal computers are allowed, but work laptops can be taken home and can remotely access the server. Many computers run outdated operating systems, including Windows XP and Windows 7. Most computers are connected with the Internet to access the design files from network drive. For computers without the need to access design files, many cannot be unplugged due to the restriction of Digital Rights Management (DRM) systems or software activation.

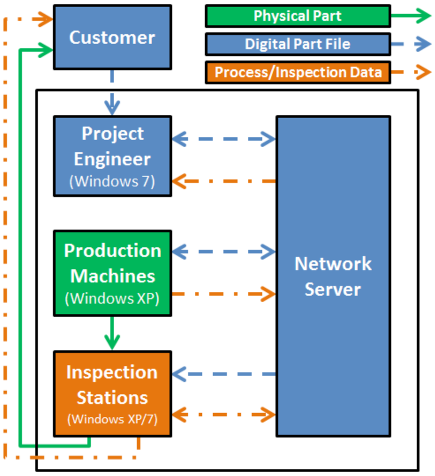

Customer
Physical Part
Digital Part File
Process/Inspection Data
Project Engineer (Windows 7)
Production Machines (Windows XP)
Inspection Stations (Windows XP/7)
Network Server

Fig. 8. General Process Layout of the Manufacturing Company.

This company applies many quality inspection measures, including digital file checks, machine process checks, material quality checks, and part quality checks. Digital file checks verify the STL file and determine if there are any inverted normals, holes, or non-closed shells. Machine process checks include assessing laser power, IR sensor, or O2 sensor to ensure the machine is operating normally. Material quality checks includes checking the powder mix ratio and the melt flow index to see the powder batch being used meet the requirements. Part quality checks include dimension measure, visual inspection, and tensile test. Dimension measures are performed with Faro Arm (a portable coordinate measuring machine) and manually by calipers.

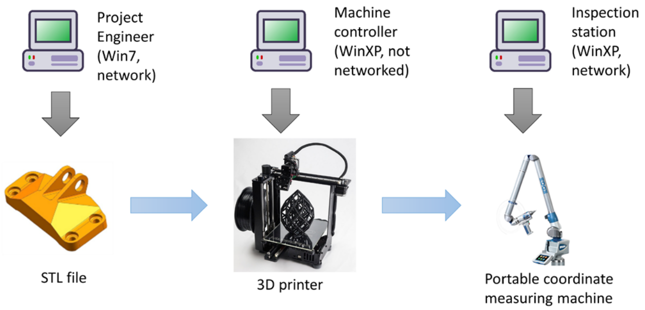

Project Engineer (Win7, network)
Machine controller (WinXP, not networked)
Inspection station (WinXP, network)
STL file
3D printer
Portable coordinate measuring machine

Fig. 9. An Example Product Line.

We applied our taxonomies to conduct a systematic risk assessment for this manufacturing company. Fig. 9 shows an example product line that consists of a single process: *3D printing*. Vulnerability "CVE-2015-2453" presented in Section II.D is an operating system vulnerability that will impact all computers running Windows 7 with "complete" confidential impact. Since the project engineer's computer is running Windows 7 and the STL file is stored in this computer, the vulnerability will allow attackers to launch confidentiality attacks to steal the design files.

Vulnerability CVE-2014-7268 will impact all the computers running Symantec Deployment Solution 6.9 or earlier on Windows XP with "complete" confidentiality/integrity/availability impact, which means attackers could launch integrity attacks by gaining write access to computers controlling 3D printer and inspection station.

IV. Related Work

Prior work has explored various types of security issues in cyber-physical systems. For example, Cardenas et al. [26] discuss key challenges for securing cyber-physical systems and Sridhar et al. [27] model the security risks for the Electric Power Grid. However, they do not consider the domain knowledge of manufacturing in their security models.

Taxonomies have been proposed for cyber-attacks in Information Technology (IT) systems [28], [29]. While the taxonomies are useful for manufacturing systems to defend traditional cyber-attacks, these taxonomies do not capture the physical effects of the attacks on IoT-based manufacturing systems. In IoT-based manufacturing systems, the attacks on the controlling systems can directly impact the physical world.

Taxonomies have also been proposed for cyber-attacks in the IoT systems. For example, Zhu et al. [6] analyze the cyber-attacks on Supervisory Control and Data Acquisition systems. No equivalent taxonomy has been proposed, however, to systematical classify possible cyber-physical attacks in manufacturing systems. However, no equivalent taxonomy has been proposed in manufacturing.

Integrated circuit manufacturing faces similar security challenges as cyber-physical manufacturing systems [30]. Taxonomies have been developed for hardware Trojans [7], [8], [30], which are maliciously injected logic in integrated circuits. Tehranipoor et al. [7] survey the design and taxonomy of hardware Trojan. Detection methodologies for hardware Trojans are also discussed in their survey. Jin et al. [8] present different implementations of hardware Trojans and show that traditional functional testing can be useless in detecting hardware Trojans.

Quality inspection in integrated circuits aims to detect if a manufactured circuit matches its original design [8]. Since circuits cannot be easily deconstructed for testing, side-channel detection is widely used as a quality inspection measure for defending against hardware Trojans. Researchers have developed various side-channel methods including timing delays [31], power analysis [32] for detecting hardware Trojans. Cyber-physical attacks in manufacturing systems differ from hardware Trojan in that the manufactured parts are not electronic in nature and there is no computational logic to verify the functions; yet some similarities could still exist as discussed in [33].

Hence, taxonomies to systematical classify possible cyber-physical attacks in manufacturing systems and provide a framework to reason about the relationship between attack types, processes, equipment and quality inspection measures were needed.

V. Concluding Remarks

The Internet of Things (IoT) has transformed many aspects of modern manufacturing. IoT-based manufacturing systems, however, are much more vulnerable to cyber-physical attacks than traditional manufacturing systems. Given the importance of IoT-based manufacturing systems throughout the supply chains in modern economies, identifying and remediating these vulnerabilities is of paramount importance [34].

To understand potential dangers and protect manufacturing system safety, this paper presents two taxonomies: one for classifying cyber-physical attacks against IoT-based manufacturing processes and another for quality inspection measures for counteracting these attacks. These taxonomies provide guidance for evaluating IoT-based manufacturing system security by delineating the research space and helps to codify and relate research approaches to one another. These taxonomies also build connections between IoT-based manufacturing processes, attacks, and quality inspection measures.

Based on creating our taxonomies and applying them in the context of the case study in Section III, we have identified the following lessons learned:

- Manufacturing companies can benefit from these taxonomies to reason more effectively about what possible attacks could happen to their IoT-based manufacturing process chains, as well as ascertain which quality inspection measures are needed to detect defects resulting from cyber-attacks on IoT-based manufacturing infrastructure.
- Ensuring the security of IoT-based manufacturing systems is a cross-disciplinary problem that can be solved most effectively by collaborative efforts of researchers from both cyber-security and mechanical engineering domains. Moreover, knowledge of cyber-security should be explained in manufacturing terms to enable meaningful reasoning.
- There is a tradeoff between quality inspection measure coverage and the costs. Enforcing more quality inspection measures can examine more aspects of the products, but with a higher cost. Our taxonomies can help eliminate quality inspection measures that are not necessary and prioritize quality inspection measures that ensure quality attributes that requirements manufacturers value the most.

Now that we have created these taxonomies, our next step is to develop an analysis tool to emulate current IoT-based manufacturing systems. Given IoT-based manufacturing process structures, system configurations, and budgets, this analysis tool will provide quality inspection recommendations on where and how to test. We also plan to explore what side-channel information can be utilized to detect attacks and develop algorithms to detect attacks by processing side-channel data in IoT-based manufacturing processes.

ACKNOWLEDGE

This work was supported in part by the National Science Foundation and Department of Homeland Security through Grant #CNS1446303.

References

[1] H. Turner, J. White, J. A. Camelio, C. Williams, B. Amos, and R. Parker, “Bad parts: Are our manufacturing systems at risk of silent cyberattacks?” *IEEE Security & Privacy,* no. 3, pp. 40–47, 2015

[2] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, “Cyber-physical security challenges in manufacturing systems,” Manufacturing Letters, vol. 2, no. 2, pp. 74–77, 2014.

[3] L. Sturm, C. Williams, J. Camelio, J. White, and R. Parker, “Cyberphysical vulnerabilities in additive manufacturing systems,” 25th Annual Solid Freeform Fabrication Symposium, vol. 7, p. 8.

[4] S. Hurd, C. Camp, J. White, Quality Assurance in Additive Manufacturing Through Mobile Computing, The 7th EAI International Conference on Mobile Computing, Applications and Services, Nov 12-13, 2015, Berlin, Germany.

[5] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” Security & Privacy, IEEE, vol. 9, no. 3, pp. 49–51, 2011.

[6] B. Zhu, A. Joseph, and S. Sastry, “A taxonomy of cyber attacks on scada systems,” in Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing. IEEE, 2011, pp. 380–388.

[7] M. Tehranipoor and F. Koushanfar, “A survey of hardware trojan taxonomy and detection,” 2010.

[8] Y. Jin, N. Kupp, and Y. Makris, “Experiences in hardware trojan design and implementation” IEEE International Workshop on Hardware-Oriented Security and Trust. IEEE, 2009, pp. 50–57.

[9] M. P. Groover, Fundamentals of modern manufacturing: materials processes, and systems. John Wiley & Sons, 2007.

[10] E. P. De Garmo, J. T. Black, and R. A. Kohser, DeGarmo’s materials and processes in manufacturing. John Wiley & Sons, 2011.

[11] S. Kalpakjian and S. R. Schmid, Manufacturing, Engineering and Technology 7th Edition. Pearson Education, Inc., 2014.

[12] Oberg, Erik, et al. Machinery's handbook. Vol. 200. New York: Industrial Press, 2004.

[13] Schmidt, Douglas C. "Model-Driven Engineering." IEEE Computer, 39.2 (2006): 25.

[14] R. W. Messler and R. W. Messler Jr, The essence of materials for engineers. Jones & Bartlett Publishers, 2010.

[15] J. S. Oakland, Statistical process control. Routledge, 2007.

[16] M. J. Harry and R. R. Schroeder, Six Sigma: The breakthrough management strategy revolutionizing the world’s top corporations. Broadway Business, 2005.

[17] E. G. Schilling, Acceptance sampling in quality control. CRC Press, 1982.

[18] Montgomery, Douglas C. Introduction to statistical quality control. John Wiley & Sons, 2007.

[19] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” in Advances in cryptology. Springer, 1985, pp. 10–18.

[20] P. C. Kocher, “Timing attacks on implementations of Diffie-hellman, RSA, DSS, and other systems,” in Advances in CryptologyCRYPTO96. Springer, 1996, pp. 104–113.

[21] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, “Side channel cryptanalysis of product ciphers,” in Computer Security ESORICS 98. Springer, 1998, pp. 97–110.

[22] M. Hutter and J.-M. Schmidt, “The temperature side channel and heating fault attacks,” in Smart Card Research and Advanced Applications. Springer, 2014, pp. 219–235.

[23] “Nist vulnerability database,” https://nvd.nist.gov/

[24] P. Mell, K. Scarfone, and S. Romanosky, “Common vulnerability scoring system,” Security & Privacy, IEEE, vol. 4, no. 6, pp. 85–89, 2006.

[25] J. Franklin, C. Wergin, and H. Booth, “CVSS implementation guidance,” National Institute of Standards and Technology, NISTIR-7946, 2014.

[26] Cardenas, Alvaro, et al. "Challenges for securing cyber physical systems."Workshop on future directions in cyber-physical systems security. 2009.

[27] Sridhar, Siddharth, Adam Hahn, and Manimaran Govindarasu. "Cyber–physical system security for the electric power grid." Proceedings of the IEEE 100.1 (2012): 210-224.

[28] Hansman, Simon, and Ray Hunt. "A taxonomy of network and computer attacks." Computers & Security 24.1 (2005): 31-43.

[29] Killourhy, Kevin S., Roy A. Maxion, and Kymie Tan. "A defense-centric taxonomy based on attack manifestations." 2004 International Conference on Dependable Systems and Networks. IEEE, 2004.

[30] Wang, Xiaoxiao, Mohammad Tehranipoor, and Jim Plusquellic. "Detecting malicious inclusions in secure hardware: Challenges and solutions." Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on. IEEE, 2008.

[31] Y. Jin and Y. Makris, “Hardware Trojan detection using path delay fingerprint,” in IEEE International Workshop on Hardware-Oriented Security and Trust (HOST 2008), 2008, pp. 51– 57.

[32] R. Rad, J. Plusquellic, and M. Tehranipoor, “A sensitivity analysis of power signal methods for detecting hardware Trojans under real process and environmental conditions,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 18, no. 12, pp. 1735–1744, 2010.

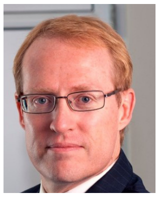
[33] Vincent, Hannah, et al. "Trojan Detection and Side-channel Analyses for Cyber-security in Cyber-physical Manufacturing Systems." Procedia Manufacturing 1 (2015): 77-85.

[34] CERT-UK, “Cyber-security Risks in the Supply Chain,” available from https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supplychain.pdf.

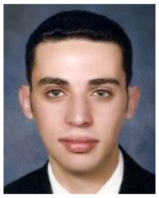
[35] CEOPEDIA, https://ceopedia.org/index.php/Quality_inspection, 2016.

Yao Pan received the B.S. degree in Computer Science in June 2012, from Zhejiang University in China. He is currently working toward the Ph.D. degree under the supervision of Dr. Jules White, at the Department of Electrical Engineering and Computer Science, Vanderbilt University. His research interests include cyber security, distributed systems, cloud computing and mobile computing.

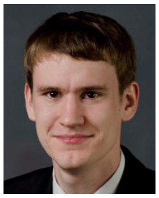
Jules White is an Assistant Professor of Computer Science in the Department of Electrical Engineering and Computer Science at Vanderbilt University. He is a National Science Foundation CAREER Award recipient. Dr. White's research focuses on securing, optimizing, and leveraging data from mobile cyber-physical systems. His mobile cyber-physical systems research spans four key focus areas: (1) mobile security and data collection, (2) high-precision mobile augmented reality, (3) mobile device and supporting cloud infrastructure power and configuration optimization, and (4) applications of mobile cyber-physical systems in multi-disciplinary domains, including energy-optimized cloud computing, smart grid systems, healthcare/manufacturing security, next-generation construction technologies, and citizen science. His research has been licensed and transitioned to industry, where it won an Innovation Award at CES 2013, attended by over 150,000 people, was a finalist for the Technical Achievement at Award at SXSW Interactive, and was a top 3 for mobile in the Accelerator Awards at SXSW 2013.



Douglas C. Schmidt is a Professor of Computer Science at Vanderbilt University. His research covers a range of software-related topics, including patterns, optimization techniques, and empirical analyses of object-oriented middleware frameworks for distributed real-time embedded systems and mobile cloud computing applications. Dr. Schmidt received B.S. and M.A. degrees in Sociology from the College of William and Mary in Williamsburg, Virginia, and an M.S. and a Ph.D. in Computer Science from the University of California, Irvine (UCI) in 1984, 1986, 1990, and 1994, respectively.



Ahmad Elhabashy rreceived B.S. and M.Sc. degrees in Production Engineering in 2009 and 2012 respectively, from Alexandria University, Egypt. He is currently working towards a Ph.D. degree under the supervision of Dr. Jaime Camelio at the Grado Department of Industrial and Sys-tems Engineering, Virginia Tech. His research interests include Quality control, production planning and control, modeling of industrial systems and optimization particularly in manufacturing context.



Logan Sturm graduated from Virginia Tech with a Bachelor of Science in Mechanical Engineer in 2013. As an undergraduate he performed research in the MicrON Lab on BacteriaBots, and served as captain and mechanical team lead for the Autonomous Underwater Vehicle Team. While in school Logan completed two years as a manufacturing engineering intern at Federal Mogul. For his senior capstone design project, Logan programed the software and user interface for a Mask Projection Micro-Stereolithography 3D Printer that he and his team designed and built. The team's final project received the award for "Best Design Project" from among 40 mechanical engineering capstone projects. Logan joined the DREAMS Lab in 2013 as an undergraduate researcher and is now pursuing a Ph.D. degree in Mechanical Engineering. Logan's current research is in Cyber-Physical Security for AM systems. This involves identifying current vulnerabilities in AM machines and in the process chain, and determining ways to detect and mitigate attacks.

Jaime Camelio is the Rolls-Royce Commonwealth professor for advanced manu-facturing at the Grado Department of Industrial and Systems Engineering at Virginia Tech. He leads the Virginia Tech Cyber-Physical Systems Security Manufacturing Group, which along with its industry partners and alliance with government agencies, is looking to improve the resiliency of the critical infrastructure of the United States, specifically the manufacturing related segments. Dr. Camelio holds a Ph.D. in Mechanical Engineering and a M.S. in Industrial Engineering from the University of Michigan and a B.S. and M.S. degrees in Mechanical Engineer-ing from the Universidad Catolica de Chile. His research interests are in assembly systems, intelligent manufacturing, process moni-toring and control, and cyber-physical security in manufacturing. He has authored or co-authored more than 70 technical papers and holds one patent.

Christopher Williams is an Associate Professor and the Electro-Mechanical Corporation Senior Faculty Fellow in the Department of Mechanical Engineering at Virginia Tech. He is the Director of the Design, Research, and Education for Additive Manufacturing Systems (DREAMS) Laboratory (DREAMS Lab), and the Associate Director of Virginia Tech's Macromolecules & Interfaces Institute. He holds affiliate faculty appointments in the Department of Engineering Education and the Department of Material Science & Engineering. His Additive Manufacturing (AM) expertise is focused in innovations in (i) AM processes and materials; (ii) design methodologies and tools to guide AM use; and (iii) AM workforce development initiatives. Dr. Williams has authored over 100 peer-reviewed articles and has presented 30+ invited talks. Dr. Williams is also a recipient of a National Science Foundation CAREER Award (2013). His research contributions have been recognized by eight Best Paper awards at international design, manufacturing, and engineering education conferences. Dr. Williams holds a Ph.D. and M.S. in Mechanical Engineering from the Georgia Institute of Technology and a B.S. with High Honors in Mechanical Engineering from the University of Florida.