Procedia Manufacturing

Volume 5, 2016, Pages 1060–1074

44th Proceedings of the North American Manufacturing Research Institution of SME http://www.sme.org/namrc

Cyber-Physical Vulnerability Assessment in Manufacturing Systems

Zach DeSmit[1*], Ahmad E. Elhabashy[1,2], Lee J. Wells[3] and Jaime A. Camelio[1]

[1]*Grado Department of Industrial & Systems Engineering, Virginia Tech, Blacksburg, VA 24061, USA*

[2]*Production Engineering Department, Faculty of Engineering, Alexandria University, Alexandria 21544, Egypt*

[3]*Industrial and Entrepreneurial Engineering & Engineering Management Department, Western Michigan University, Kalamazoo MI 49008, USA*

zachd1@vt.edu, habashy@vt.edu, lee.wells@wmich.edu, jcamelio@vt.edu

Abstract

The rampant increase in frequency and complexity of cyber-attacks against manufacturing firms, has motivated the development of identification and mitigation techniques for cyber-physical vulnerabilities in manufacturing. While the field of cybersecurity assessment approaches is expansive, there is no literature aimed at assessing cyber-physical vulnerabilities for manufacturing systems. In response, this paper provides a framework for systematically identifying cyber-physical vulnerabilities in manufacturing systems. The proposed approach employs intersection mapping to identify cyber-physical vulnerabilities in manufacturing. A cyber-physical vulnerability impact analysis using decision trees then provides the manufacturer with a stoplight scale between low, medium, and high levels of cyber-physical vulnerability for each analyzed production process. The stoplight scale allows manufacturers to interpret assessment results in an intuitive way. Finally, the paper provides a case study of the proposed approach at an applied manufacturing research facility and provides general recommendations to securing similar facilities from cyber-physical attacks.

Keywords: Cyber-physical security, Decision tree analysis, Manufacturing systems, Vulnerability assessment

1 Background and Motivation

With advancements in networking and internet technologies, cyber-attacks on physical systems are becoming a growing phenomenon. Perhaps the most infamous cyber-attack on a physical system was the “Stuxnet” virus. Between late 2009 and early 2010, Stuxnet allegedly destroyed as many as 1,000 Iranian high-speed centrifuges used for uranium enrichment. Specifically, the life-spans of these centrifuges were significantly reduced by periodically changing their rotational speeds (Albright et al.,

* Corresponding Author

 Selection and peer-review under responsibility of the Scientific Programme Committee of NAMRI/SME

doi:10.1016/j.promfg.2016.08.075

2010; Vincent et al., 2015). This attack was successful because it was able to display misleading equipment readings (reading indicated no problems) to operators (Cherry, 2011).

Examples of other cyber-attacks are quite numerous, expanding across a variety of fields. Recent cyber-attacks include the Target data breach in December 2013 (Target, 2014), the hacking of Sony Pictures Entertainment (Lee, 2014) in November 2014, and acquiring private customer information from Anthem Health Insurance in December 2014 (Anthem, Inc., 2015). Other examples also involved cyber-attacks on a physical system, such as the "logic bomb" that was reportedly inserted in the Trans-Siberian pipeline's control software to abnormally change the pumps and valves settings, causing a massive explosion in 1982 (Rost & Glass, 2011). These examples demonstrate that no system is beyond the reach by cyber-attackers, and manufacturing systems are no exception.

Over the last few years, manufacturing has been one of the most targeted sectors for cyber-attacks (Symantec, 2014; Symantec, 2015) by spear-phishing attacks[†]. In addition, the critical manufacturing sector accounted for the most security incidents reported to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in the past year (ICS-CERT, 2015). Attacks such as these traditionally aim at gaining unauthorized access to information or valuable trade secrets (Deloitte, 2014). However, with the evolving nature of manufacturing systems, the threat of cyber-physical attacks (cyber-attacks affecting physical systems) against manufacturing is of significant concern.

The opportunities for these cyber-physical attacks are also exacerbated by the Internet of Things (IoT), which has resulted in a rampant expansion of networked devices across every sector (Evans, 2011), including manufacturing. In addition, internet-based Computer Aided Engineering (CAE) support tools, such as cloud computing and software as a service (SaaS) are being adopted across manufacturing. This opens new unwanted "doors" for malicious attacks into manufacturing systems.

Recent case studies, conducted at Virginia Tech, have shown the ease in which such cyber-physical attacks can be executed. In the first case study (Wells et al., 2014), tool path files were modified in a subtractive manufacturing operation, while the design files for an additive manufacturing process were altered in the second case study (Strum et al., 2014). Examples of the undetected outcome of cyber-physical attacks can include defective products as well as not meeting required design specifications. In addition, the financial consequences of such an attack could be devastating due to delaying a product's launch, ruining equipment, increasing warranty costs, losing customer trust, or causing physical harm to an employee or end user.

Recently, it was reported that the median number of days between the onset of a cyber-attack and its detection in an organization was over 200 days (Mandiant, 2014). Additionally, 69% of these attacks were not discovered by the victims themselves, but by third parties such as law enforcement agencies and customers (Mandiant, 2014). Currently, there is little emphasis placed on cyber-physical security in present manufacturing environments, as cybersecurity for manufacturing is commonly treated through pure information technology. However, given the cyber-physical nature of advanced manufacturing, attacks against these systems cannot be mitigated by traditional cybersecurity approaches (National Defense Industrial Association (NDIA), 2014; Vincent et al., 2015). The threat of cyber-physical attacks on manufacturing is not being addressed in the manufacturing industry leaving facilities and entire supply chains vulnerable to a barrage of cyber-physical attacks.

There exists a need to develop a manufacturing specific approach to identifying cyber-physical vulnerabilities. As a first step, manufacturers need to understand how their systems could be compromised by cyber-physical attacks; in order to better secure them. Accordingly, this paper aims to identify those vulnerabilities through a systematic cyber-physical vulnerability[‡] assessment approach for manufacturing systems. In addition to identifying and assessing vulnerabilities within the manufacturing environment, the proposed approach is the first of a five-step cyber-physical security

[†] A *spear-phishing attack* is a targeted e-mail scam aiming to access sensitive data, steal valuable information, or install malware on compromised computers. (Kaspersky, 2015)

[‡] A *vulnerability* is defined as any flaw, weakness, or gap in a system's design, implementation, or operation that can be exploited by an intruder to violate the system's security policy (Sadowsky et al., 2003)

protocol: identifying and assessing vulnerabilities, protection, attack detection, response strategy, and recovery protocol (NIST, 2014). The proposed approach provides manufacturing enterprises with a method to adhere to cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) (NIST, 2014). Finally, implementing a vulnerability assessment approach will raise awareness among industry practitioners regarding the existence of malicious cyber-physical attacks and their potentially serious consequences.

The remainder of this paper is organized as follows. Section 2 discusses related work in the field of vulnerability assessment and relevant commercial tools for cyber-physical systems. Section 3 presents the details of the proposed cyber-physical vulnerability assessment approach. Section 4 implements the proposed approach in a case study within an applied research facility. Finally, Section 5 provides our conclusions and future work.

2 Literature Review

This section discusses related efforts of assessing cyber-physical system vulnerabilities within the academic and commercial realms. A vulnerability assessment presents a common framework to assess and quantify the impact a vulnerability may have on a system (Mell et al., 2006); it should not be confused with risk analysis. A traditional risk analysis approach involves an investigative audit to verify the presence of security systems and to validate their usefulness (Cerullo & Cerullo, 1994). Together, vulnerability assessments and risk analysis reports allow an organization to view their security stance at a given time.

There exists only limited research within the field of vulnerability assessment for cyber-physical systems. Baker (2005) developed a three-step process for cyber vulnerability assessment and risk analysis methods for cyber-physical systems (Baker, 2005). The first step consists of understanding the organizational structure. Second, the organization determines failure modes and identifies potential consequences. Lastly, the organization implements improvements (Baker, 2005). The main issue of this approach is the lack of clarity on how to correctly identify vulnerabilities, which results in a pure risk analysis method rather than a vulnerability assessment and risk analysis method.

Ten et al. (2008) developed a vulnerability assessment approach for industrial control systems, specifically, Supervisory Control and Data Acquisition (SCADA) Systems (Ten et al., 2008). Their assessment was motivated by a requirement passed by the North American Electric Reliability Corporation (NERC) to identify cyber vulnerabilities in electrical power systems. Adhering to the NERC requirement has proven difficult due to the increasing level of interconnectedness in electrical power and SCADA systems (Ten et al., 2008). The goal of their approach was to provide a systematic vulnerability assessment at the system, scenario, and access point levels, fulfilling the requirements of the NERC standard (Ten et al., 2008). That NERC requirement is similar to a US manufacturing mandate by President Obama in 2013 (Obama, 2013). However, the approach of Ten et al. (Ten et al., 2008) cannot identify vulnerabilities within the manufacturing system as it focuses solely on industrial control (SCADA) systems which make up only a small portion of the entire manufacturing landscape.

More recently, Hutchins et al. (2015) expanded the risk management frontier for manufacturers to include cybersecurity risks and vulnerabilities. Their paper outlined a framework for identifying cybersecurity risks in manufacturing (Hutchins et al., 2015). Their approach is motivated by the inability to identify and assess cyber-risk in manufacturing through existing risk management approaches. Their paper deals strictly with the cyber domain, specifically with the flow and transfer of data through interconnected processes and machines (Hutchins et al., 2015). While providing a structured approach to identifying cybersecurity risks in manufacturing, their paper does not consider cyber-physical security in its assessment approach, which includes the securing of products or processes that arise from the interconnectivity of the manufacturing enterprise.

With respect to the commercialization of vulnerabilities assessments and audits, the current cybersecurity market is rich in varying methods and approaches for identifying cybersecurity vulnerabilities within an organization. Many of the common tools are created at research institutions, such as Carnegie Mellon University's Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Caralli et al., 2007). Others are created from government and federal agencies, such as the Federal Financial Institutions Examination Council's (FFIEC) assessment tool (FFIEC, 2015) and the NIST Cybersecurity Framework (NIST, 2014).

The OCTAVE assessment strives to assist organizations in aligning their security activities with overall organizational goals (Caralli et al., 2007). This approach uses a multidisciplinary team from within the organization to complete a series of survey-based asset related questions to assess the current levels of cybersecurity within the organization. The FFIEC Cybersecurity Assessment Tool acts more as a reference guide to an organization's level of security from cyber-attacks and can be repeated as needed to assess progress (FFIEC, 2015). The FFIEC tool focuses on defining and assessing the cybersecurity risks an organization might experience and brings together board members and shareholders to agree upon the level of security and risk the company is willing to incur.

The NIST Cybersecurity Framework was developed in response to the executive order that mandated NIST to proceed in implementing a cybersecurity framework that would assist the nation's industries with fortifying their infrastructure in order to be more resilient to cyber-attacks (Obama, 2013). The framework focuses primarily on cyber challenges, i.e. intellectual property concerns, leaving the questions related to cyber-physical vulnerabilities unanswered (NIST, 2014). Therefore, manufacturing vulnerabilities are left open to cyber-physical attacks, as there is little to no work being done to connect the methodology in the NIST framework to manufacturing facilities.

Even with the wealth of commercially available cybersecurity assessments and approaches, cyber-physical security for the manufacturing realm cannot be addressed by these assessments. This paper's proposed approach builds upon the characteristics adopted by the NIST Framework, while focusing on concerns that are pertinent to the cyber-physical domain rather than the cyber-domain alone. As highlighted in the literature review, there currently exist methods for identifying cyber vulnerabilities within an organization. The proposed approach breaks new ground by applying cybersecurity vulnerability assessment techniques to cyber-physical systems while providing manufacturers with the tools necessary to objectively assess their production processes.

Using the proposed approach, manufacturers can assess their production facility and identify the cyber-physical vulnerabilities inherent to their specific system. The proposed approach will not only introduce mitigation techniques and industry best practices, but also towards the creation and implementation of a cyber-physical vulnerability assessment tool.

3 Approach

With the goal of identifying cyber-physical vulnerabilities within a manufacturing process, the proposed vulnerability assessment approach is based upon the principle that vulnerabilities in manufacturing systems occur at intersections (and intra-sections, referred to collectively as intersections) of cyber, physical, cyber-physical, and human entities that embody a manufacturing system. A visual representation of how these entities and vulnerabilities interact within the vulnerability space can be seen in Figure 1, where intersections should result in an expected transformation. However, the actual transformation could differ from the expected one, even when considering nominal variability within the production process; due to the existence of some type of vulnerability. This transformation would then act as input to the next intersection and so on.

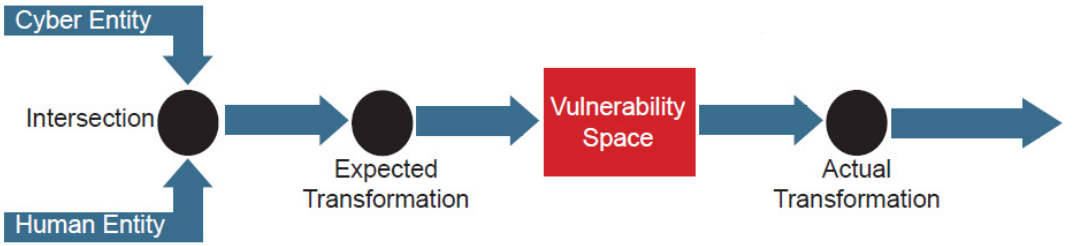

Figure 1: An example of a cyber/human intersection.

In essence, the developed approach starts by mapping intersections, then assessing the vulnerability impact at each intersection node. For complete analysis of a production facility, intersection maps need to be created for every part of the manufacturing process to ensure all intersections are accounted for. It should be noted that the vulnerability assessment approach proposed here goes beyond malicious cyber-physical attack vulnerabilities and includes vulnerabilities from unintentional process changes. It is a general approach to understand cyber, physical and cyber-physical vulnerabilities existing within a system.

3.1 Intersection Mapping

The first step of the proposed assessment approach is to track the four different entity types through the entire production process. For this purpose, intersection maps are used to identify each entity as it progresses through the production process creating a string of related entities that could be easily traced. Not only does this step allow the manufacturer to trace these four entities through their production process, more importantly it highlights the intersections where cyber-physical vulnerabilities most likely occur. The four entities listed below are, cyber, physical, cyber-physical, and human.

- **Cyber:** The cyber entity is used for pre-processing, saving, transferring, managing, or post-processing of digital information. Examples of cyber entities include: Material Requirements Planning (MRP) systems, Product Lifecycle Management (PLM) platforms, Enterprise Resource Planning (ERP) systems, CAE tools, data management systems, data-mining software, and quality control/inspection reporting systems.
- **Physical:** A physical entity is one that is tangible in nature and whose role in the manufacturing system is not completely governed by automated systems. Examples of physical entities include: manufactured parts, manually operated machines, raw/intermediary materials, and manually operated inspection equipment.
- **Cyber-Physical:** Cyber-physical entities are traced through the production process as well and are defined as any entity comprised of cyber and physical elements that autonomously interact together, with or without human supervision. Examples of cyber-physical entities include: Computer Numerical Control (CNC) machines, Coordinate Measurement Machines (CMMs), data acquisition (DAQ) systems, and SCADA networks.
- **Human:** In the vulnerability space, a human is defined as any person who has an opportunity to interact with other entities within the manufacturing system. Examples of human entities include: Information Technology (IT) support staff, designers, manufacturing engineers, machinists, quality engineers, maintenance crew members, shipping and handling personnel, and visitors.

An example of an intersection map can be seen in Figure 2. The example was created to highlight the related intersections; but is representative of a process commonly seen in industry, creating a metal blank on a CNC machine. The process begins with the interaction between the raw material ($part_{in}$) and

the CNC machine (CNC). It is assumed that the raw material has previously been placed onto the machine, outputting an entity (CNC_{setup}) that would be used as an input for the next node. Once fixed in the machine, the machine control language is loaded (G-code) and executed to create the blank part (CNC_{out}). Finally, the blank part is reviewed by an inspector (h_1) as a visual quality control inspection resulting in the finished part ($Part_{out}$).

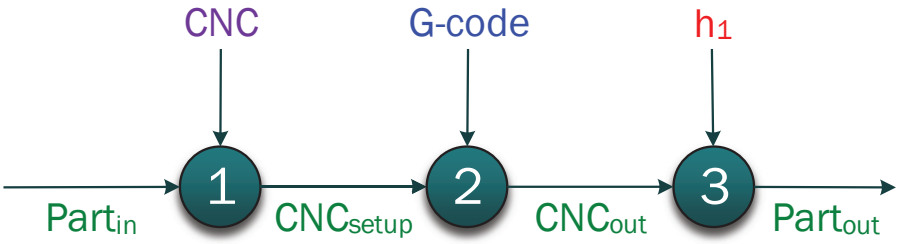

Figure 2: An example of a vulnerability intersection map for a manufacturing process.

Note that each node only consists of two inputs, which allows for a generic analysis of the system. The inputs have also been color coded to later identify trends or levels of significance occurring within specific types of inputs. Green represents a physical entity in the system, blue represents a cyber-component, purple represents a cyber-physical component, and finally red represents a human entity.

3.2 Cyber-Physical Vulnerability Impact Assessment

For each node within an intersection, its characteristics would then be evaluated to assess its corresponding vulnerabilities. These characteristics are used as metrics to determine the impact of exploiting this vulnerability. Such intersection characteristics would include:

a. *Loss of Information:* The information lost or modified during the completion of a node. For example, all of the CAD designer's information or knowledge of a manufactured part cannot be accounted for in the validation of the CAD file; therefore, some information is lost or modified when transitioning away from the node with the intersection of the CAD file and the human.
b. *Inconsistency:* The level of intersection variability, which can occur due to operator changes, re-tooling, machine set-ups, etc. For example, a simple operation could be performed in numerous ways across different machine and/or operators configurations, resulting in a large range in the variation of that certain intersection.
c. *Relative Frequency:* The number of times an exact intersection is repeated during the manufacturing process. This metric refers to the recurring specific intersection with identical details.
d. *Lack of Maturity:* The amount of time an intersection has not been in operation. In the case of human entities, it could be thought of as the lack of experience or trust; since a novice machinist is expected to be less mature than one who has been machining parts for ten years, for example.
e. *Time until Detection:* The amount of time elapsed between a node perturbation and its possible detection; not necessarily referred to in terms of time, but could be with reference to the distance in the process.

It should be noted that each metric will be ranked low, medium, or high. Low values represent a low vulnerability impact and a more secure intersection than one receiving a higher value. Decision trees for each of these metrics are created to allow for an easily repeated assessment. Each decision tree for a metric poses a question (or a set of questions); it is through answering these different questions that the impact level of cyber-physical vulnerabilities is determined. What follows are the details for trees corresponding to each of these metrics.

Loss of Information Metric:

The first question in the decision process for this metric asks whether or not information is lost or modified in the node. The modification of information or data has the potential of a significant negative impact on the cyber-physical system. Considering the two inputs, has all the information from the previous node been carried to this node? Then, the next question asks as to whether or not information has been gained in this node; as shown in Figure 3. For this particular metric, each type of intersection (human/human, human/cyber, cyber/physical, etc.) should be represented by its own unique decision tree. However, for the sake of brevity, the decision tree for the intersection of only cyber and physical entities is presented here.

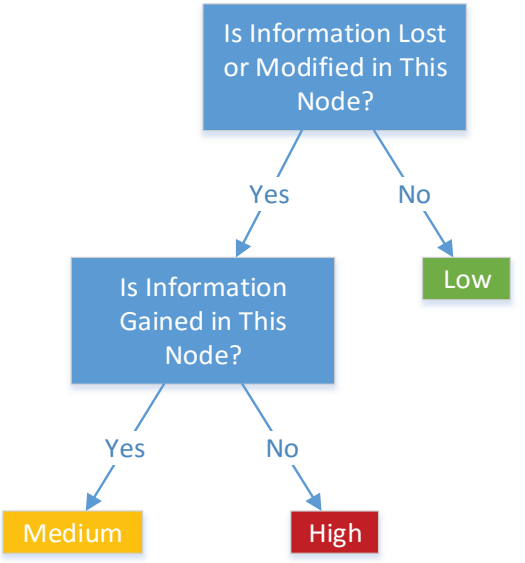

Figure 3: Loss of Information metric decision tree.

Inconsistency Metric:

Considering that each node of the process map would represent an intersection of two entities or resources, the decision here is to determine how many inputs could have changed. An example of this would be a change in the operator of a physical machine or the changing of a tool or machine setup; as shown in Figure 4.

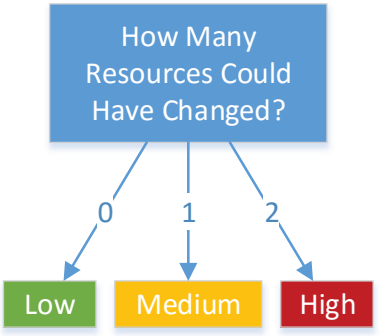

Figure 4: Inconsistency metric decision tree.

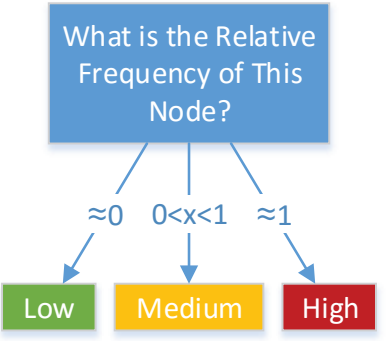

Figure 5: Relative Frequency metric decision tree.

Relative Frequency Metric:

The decision process for the vulnerability of a node with respect to the relative frequency metric can be seen in Figure 5. The metric looks into how many times the specific node is repeated relative to the manufacturing process. For example, if a company manufactures only one product, and they produce

one part a day for an entire year, the frequency of the CAD file creation will be 1/365, which would correspond to a relative frequency close to 0 and results in a rating of low. Likewise, the CAM node will have a frequency of 1/365. The manufacturing node, however, will have a frequency of 365/365 due to the daily manufacturing of the part and the relative frequency of the manufacturing node would be ≈1, resulting in high rating.

Lack of Maturity Metric

The fourth decision tree, shown in Figure 6, answers the questions of lack of maturity of a specific node. The first question is whether or not the manufacturer considers the resource 100% trustworthy. An example of a non-trusted resource or factor would perhaps be a brand new machine that one is not 100% comfortable with or fully knowledgeable about. The second question is related to the proficiency of this specific resource.

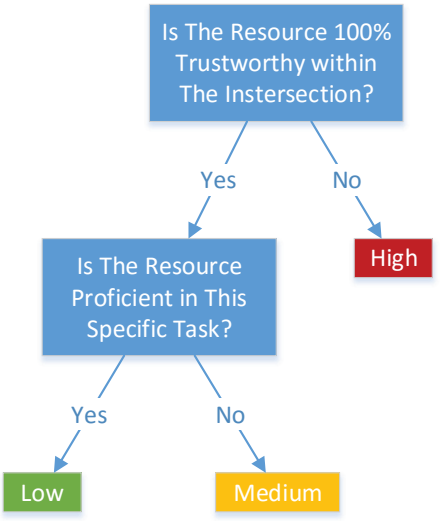

Figure 6: Lack of Maturity metric decision tree.

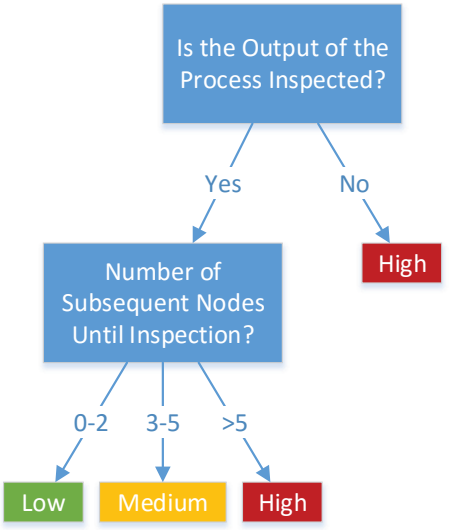

Figure 7: Time until Detection metric decision tree.

Time until Detection Metric

For the time until detection, it is asked whether or not the effects of the process will eventually be inspected. If a process is never going to be inspected, the resulting time until detection results in a high level of vulnerability. Second, a question is asked as to how many subsequent nodes until an inspection occurs, which determines the amount of time a vulnerability could be exploited; details of this tree are shown in Figure 7.

3.3 Example

Going back to the example shown in Figure 2, the results of the cyber-physical vulnerability impact analysis is summarized in Table 1; where the logic in the described decision trees have been applied to yield these results. For instance, it can be seen that the Inconsistency metric for the second node and the Loss of Information in the third node show a high rating; while the Relative Frequency metric for all three nodes has a high rating. Whereas, the Inconsistency metric for the first node and the Lack of Maturity for the second node resulted in a rating of medium. The ratings for the remaining nodes were low. These results indicate that there seems to be high variability in the second node, a significant

amount of important information is lost in the third node, and an issue with the repeatability in all nodes, representing potential exploits for cyber-physical attacks within these nodes.

Table 1: Vulnerability assessment for the metal blanking process in Figure 2.

#	Description	Loss of Information	Inconsistency	Relative Frequency	Lack of Maturity	Time until Detection
1	The CNC (CNC) is loaded with the raw material ($part_{in}$)	**Low**	**Medium**	**High**	**Low**	**Low**
2	The actual manufacturing operation (blanking) on the CNC machine.	**Low**	**High**	**High**	**Medium**	**Low**
3	Resulting product quality is assessed by an inspector.	**High**	**Low**	**High**	**Low**	**Low**

For the sake of clarity, details of the ratings of each metric for the first node, which contains the intersection of the part and the CNC machine to create the production setup, are as follows:

- **Loss of information**: This metric assesses the vulnerability of the node based on how much information is lost or modified during the completion of the node. The first question asks whether information is lost or modified when the raw material is fixed into the CNC machine. Since the material is information-less and the fixture remains static there is no loss of information, resulting in an assessment value of low.
- **Inconsistency:** This metric assesses the variability of the node. The first question is whether or not the raw material could have changed prior to fixing it in the CNC machine. In this case, it is not possible that the raw material was altered. It is asked again, whether or not the CNC machine fixture could have changed and the answer is yes (i.e. only one resource could have changed), giving the node a medium rating.
- **Relative Frequency:** This metric asks whether or not the process is repeated. In this example, the process of fixing the raw material into the machine happens every time the production process is started, resulting in a high level of relative frequency.
- **Lack of Maturity:** This metric assesses the vulnerability of the node, based on the time it has not been in operation. It is asked whether or not the resources are trusted, which in this case, are the raw material and the CNC machine fixture. It is assumed that they are 100% trustworthy. Secondly, it is asked if the resources are proficient in their tasks. We assume that both the CNC machine fixture and the raw material are proficient, which corresponds to a lack of maturity rating of low.
- **Time Until Detection:** This metric measures the distance to an inspection point, which for this node is less than two nodes, resulting in a rating of low.

4 Case Study

4.1 Overview

The approach outlined in Section 3 was implemented at the Commonwealth Center for Advanced Manufacturing (CCAM) as a case study. CCAM is an applied research center that works with both universities and companies to rapidly translate promising research innovation into commercial use (CCAM, 2015). The overall goal of the case study was to identify that cyber-physical vulnerabilities

exist within a manufacturing facility, which can be exploited by cyber-attacks. Also, those vulnerabilities can be easily identified through the careful assessment of a facility's production process.

Hence, a part was manufactured at CCAM facilities, going through various phases from the design intent to finishing and quality control. These phases included: manufacturing process planning, Geometric Dimensioning and Tolerencing (GD&T) and CMM programming, raw material preparation, CAM programming, manufacturing, and quality inspection. However, for the purpose of this case study, only a select few phases were considered for the implementation of the cyber-physical vulnerability assessment. The phases considered are the manufacturing process planning and product quality inspection stages.

Particularly, a phase such as manufacturing process planning consists of two main steps. First, a manufacturing setup is created for the part to be produced by the CAD/CAM programmer. The programmer's main job is to make sure the part location, blank geometry, datums, and other process characteristics are accurate. The second step is creating a similar setup for the work holding device. This is done by a machinist, who finalizes the whole manufacturing setup and selects the suitable work area. It should be noted that it is possible for both the programmer and the machinist to collaborate in these two steps. The machinist's input is often valuable and would cause the programmer to re-adjust the initial setup accordingly.

The other phase is the quality inspection phase which consists of three main steps. The first is creating a suitable measurement setup on a CMM for the part to be measured. After the measurement setup is ready, the part is inspected automatically via the CMM using a pre-specified measurement procedure (referred to as the CMM code). Finally, the resulting output data of the CMM is evaluated by a CMM operator, to determine whether the part is conforming to the required specifications or not.

4.2 Intersection Mapping

As stated in Section 3, the first step was to track the four identified entities (cyber, physical, cyber-physical, and human) through the production process. This was accomplished through creating intersection maps representing different phases within the manufacturing environment at CCAM. For instance, Figure 8 shows the intersection map of the manufacturing process planning phase at CCAM, where each of the two previously mentioned steps are modeled as two separate nodes (nodes 1 and 2, respectively). Figure 9 shows the intersection map for the CCAM's quality inspection phase, with three different nodes representing the different steps within this phase.

Table 2: Legend used in Figure 8.

Position	Identifier
CAD Design	CAD_4
Manufacturing Setups	MS_1, MS_2
CAD/CAM Programmer	h_9
Machinist	h_{12}
Color	**Entity**
RED	Human
BLUE	Cyber
GREEN	Physical
PURPLE	Cyber-Physical

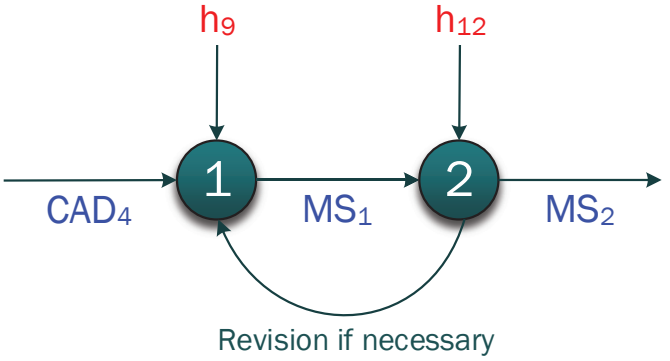

Figure 8: Intersection map for the manufacturing process planning phase at CCAM.

Table 3: Legend used in Figure 9.

Position	Produced Part	CMM Machine	CMM with Part Mounted on it	CMM Code to be Input into the CMM	CMM Output Data	CMM Operator	Inspected Part
Identifier	$Part_1$	CMM	CMM_{setup}	CMM_{code}	CMM_{out}	h_{14}	$Part_{out}$

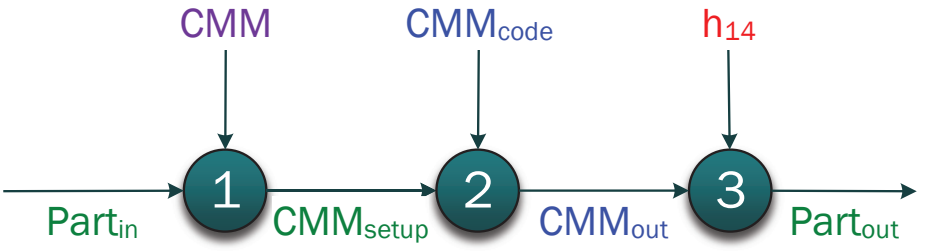

Figure 9: Intersection map for the quality inspection phase at CCAM.

4.3 Cyber-Physical Vulnerability Impact Assessment

Upon completion of the intersection mapping, the next step is to apply the logic in the different decision trees to assess the vulnerability of each node. For the manufacturing process planning phase, the results are summarized in Table 4, where each of the two nodes has its resulting metric value (color-coded) from the cyber-physical vulnerability assessment approach. According to Table 4, there are three metrics that show high ratings for both of the nodes in this stage: Inconsistency, Relative Frequency, and Time until Detection. In addition, the Loss of Information metric for the first node has a high rating. Only one other metric provides a medium rating for the second node, which is the Loss of Information metric, while all the remaining metrics' rating is low for both nodes.

Table 4: Vulnerability assessment for the manufacturing process planning phase.

#	Description	Loss of Information	Inconsistency	Relative Frequency	Lack of Maturity	Time until Detection
1	Programmer (h_9) creates part (CAD_4) setup (MS_1).	**High**	**High**	**High**	**Low**	**High**
2	Machinist (h_{13}) finalizes the setup (MS_1).	**Medium**	**High**	**High**	**Low**	**High**

As for the product quality inspection phase, the cyber-physical vulnerability assessment results are shown in Table 5. It seems that the Relative Frequency metric is always yielding a high rating, regardless in which node, while the Inconsistency metric has a rating of medium in both the first and third nodes. Other than another medium rating for the Loss of Information metric in the third node, all the remaining metrics provide low ratings for all remaining nodes.

Table 5: Vulnerability assessment for the quality inspection phase.

#	Description	Loss of Information	Inconsistency	Relative Frequency	Lack of Maturity	Time until Detection
1	Creating a measurement setup (CMM_{setup}) on the CMM.	**Low**	**Medium**	**High**	**Low**	**Low**

#	Description	Loss of Information	Inconsistency	Relative Frequency	Lack of Maturity	Time until Detection
2	Actual part measurement, resulting in (CMM_{out}).	Low	Low	High	Low	Low
3	Inspection results evaluation by a CMM operator.	Medium	Medium	High	Low	Low

4.4 Interpreting the Results

From the ratings obtained in both Table 4 and Table 5, it can be concluded that there exists vulnerabilities in the manufacturing environment used for this case study. More specifically, both nodes in the manufacturing process planning phase have three out of five metrics with a high rating. Moreover, the first node shows an additional high rating metric, while the second node also shows a metric with a medium rating. The situation is somewhat better for the product quality inspection phase from a vulnerability assessment standpoint. Only one metric yields a high rating in all three stages. The results also show that the nodes for this phase seem to be having a varying pattern of vulnerability risks with the third node being slightly more vulnerable to cyber-physical attacks and the second node being the least vulnerable.

This implies that the identified production process contains nodes that are vulnerable to cyber-physical attacks. Nodes earning a high ranking denote a portion of the production process that is extremely vulnerable to exploitation through cyber-physical attacks and could compromise an entire production system if not mitigated. Such an assessment indicates that processes within this facility that are comprised of the intersection between cyber and physical entities are highly vulnerable to cyber-attacks. The phenomenon seen here highlights the need for cyber-physical vulnerability assessment in manufacturing.

Using the vulnerability assessment tool to highlight these intersections and overall level of cyber-physical vulnerability will aid manufacturers in securing their production systems from attack. The vulnerability assessment performed for CCAM's manufacturing facility outlines the need for cyber-physical security to be a more widely discussed topic in manufacturing. The proposed vulnerability assessment highlights areas of potential improvement to better secure the production system from cyber-physical attacks.

The largest vulnerability areas from the case study are the Inconsistency and Relative Frequency metrics. To mitigate these risks, CCAM needs to decrease the number of resources that could be altered within a node and the number of times the node is repeated. To decrease the number of resources that could have changed within a node, the authors suggest that version control be implemented with a chain of certification for files. This would allow the necessary individuals to alter the files while providing a chain of certification as to who has changed which attributes within the files. Altering the manufacturing production process is required to decrease the number of times a node is repeated, eliminate redundancies, and to only allow the necessary operations to occur once. It was suggested to produce blank parts in batches to reduce the number of potential attack opportunities on the CNC machine. This can also be accomplished through designing parts only once, and not altering design files after a process setup has been created.

5 Discussion and Future Work

The proposed cyber-physical vulnerability assessment approach provides manufacturers with a detailed outline to identify cyber-physical vulnerabilities. Where identified vulnerabilities are instances that pose a significant risk to their manufacturing production process if left unidentified. The proposed approach mainly consisted of two steps. First, representing various processes within a manufacturing

setting as intersection maps of different entity types. Then, using decision tree analysis to evaluate the impact of vulnerabilities in each of the resulting intersection nodes is assessed. This assessment is a step in the right direction for manufacturers to begin to take cyber-physical security seriously. The literature has shown that this area of risk is left untouched by other assessments, while the number and complexity of attacks on manufacturers continues to increase.

Upon applying the proposed vulnerability assessment approach to the production process used in the case study many areas of improvement were identified that would allow this approach to be developed further into a full cyber-physical vulnerability assessment tool. Used to detect cyber-physical vulnerabilities within a manufacturing system, the proposed tool would also provide manufacturers with a detailed plan including mitigation strategies to secure the identified production process from cyber-physical attacks.

The first area identified for future work is the area of threat identification. The proposed approach only identifies cyber-physical vulnerabilities. It is expected to extend this approach to determine the likelihood of each threat from previous data collected from customer discovery and through the analysis of threats seen commonly in industry. The second area aims to equip the assessment approach with risk assessment capability. This capability would allow the assessment to identify the likelihood of the cyber-physical vulnerability being exploited and multiplying that number by the potential impact given by the manufacturer, providing them with an individualized risk assessment. Lastly, the main goal is to eventually incorporate all of these ideas into one package creating an easy-to-use cyber-physical vulnerability assessment tool to identify vulnerabilities within manufacturing production processes by analyzing input from manufacturers.

The incorporation of the vulnerability assessment tools into a single package would best be served as an audit based tool. This audit tool would be semi-automated in that the manufacturer would be required to input certain information regarding their production processes and the tool would do the analysis, significantly reducing the amount of time and effort required of the manufacturer. The aim would be asking the minimum amount of manual input from the manufacturers, to be able to provide them with a complete assessment, along with areas of higher risks that require more attention.

As previously mentioned, in addition to the NIST Framework, other organizations have also embarked on alternate solutions to cybersecurity such as creating audit tools that protect critical infrastructure by allowing companies to secure their critical assets from cyber-attacks (Bergvall & Svensson, 2012). However, most of their work has been directed towards securing assets and proprietary information, which has resulted in their expertise and contributions being relegated solely to the cybersecurity market, leaving the cyber-physical market untouched (Fray, 2012). Contributing to the cyber-physical market requires a more robust approach that includes working with industry partners, gaining insights into the limitations of manufacturing enterprises, and developing an organization-specific assessment approach that caters to the needs of the various manufacturing enterprises. The future work aims to bridge the gap between assessment tools and cyber-physical security for manufacturing by creating a cyber-physical vulnerability assessment tool.

6 Acknowledgments

This research work was partially supported by the National Science Foundation (NSF) grants CNS 1446804 and CMMI-1436365, the Commonwealth Center for Advanced Manufacturing (CCAM), and Virginia Tech's *Cyber-Physical Security Systems Manufacturing Group*. The authors would also like to thank graduate student members of the Center for Innovation-based Manufacturing (CIbM) lab at Virginia Tech, for their help with reviewing the manuscript, Samantha Roscher for aiding with some of the figures, and the staff at CCAM for their assistance in the case study.

References

Albright, D., Brannan, P. & Christina, W., 2010. *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* [Online] Institute for Science and International Security (ISIS) Available at: isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ [Accessed 14 December 2014].

Anthem, Inc., 2015. *How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services*. [Online] Available at: www.anthemfacts.com [Accessed 28 October 2015].

Baker, G.H., 2005. A Vulnerability Assessment Methodology for Critical Infrastructure Sites. In *DHS Symposium*. Boston, Massachusetts, 2005. Department of Homeland Security.

Bergvall, J. & Svensson, L., 2012. *Risk Analysis Review*. Master's Thesis. Linköping, Sweden: Linköpings University.

Caralli, R.A., Stevens, J.F., Young, L.R. & Wilson, W.R., 2007. The OCTAVE Allegro Guidebook, v1.0. *Software Engineering Institute*.

CCAM, 2015. *Commonwealth Center For Advanced Manufacturing - About Us*. [Online] Available at: www.ccam-va.com/about-us/ [Accessed 24 November 2015].

Cerullo, M.J. & Cerullo, V., 1994. EDP Risk Analysis. *Computer Audit Update*, pp.9-30.

Cherry, S., 2011. *Sons of Stuxnet*. [Online] Available at: spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet [Accessed 15 December 2014].

Deloitte, 2014. *Global Cyber Executive Briefing - Manufacturing*. [Online] Available at: www2.deloitte.com/global/en/pages/risk/articles/Manufacturing.html# [Accessed 16 August 2015].

Evans, D., 2011. *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*. White Paper. Cisco Internet Business Solutions Group (IBSG).

FFIEC, 2015. *FFIEC Cybersecurity Assessment Tool Overview*. Federal Financial Institutions Examination Countil.

Fray, I.E., 2012. A Comparative Study of Risk Assessment Methods, MEHARI & CRAMM with a New Formal Model of Risk Assessment (FoMRA) in Information Systems. In *Proceedings of the 11th IFIP TC 8 international conference on Computer Information Systems and Industrial Management*. Venice, Italy, 2012. Springer-Verlag.

Hutchins, M.J. et al., 2015. Framework for Identifying Cybersecurity Risks in Manufacturing. *Procedia Manufacturing*, 1, pp.47-63.

ICS-CERT, 2015. *ICS-CERT Monitor Newsletters: November-December 2015*. [Online] Department of Homeland Security Available at: ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT%20Monitor_Nov-Dec2015_S508C.pdf [Accessed 26 January 2016].

Kaspersky, 2015. *What is Spear Phishing? - Definition*. [Online] Available at: usa.kaspersky.com/internet-security-center/definitions/spear-phishing#.VlIcL3arQgs [Accessed 22 November 2015].

Lee, T.B., 2014. *The Sony Hack: How it Happened, Who is Responsible, and What we've Learned*. [Online] Available at: www.vox.com/2014/12/14/7387945/sony-hack-explained [Accessed 15 December 2014].

Mandiant, 2014. *M-Trends 2015: A view from the front line*. Threat Report. Mandiant, a FireEye Company.

Mell, P., Scarfone, K. & Romanosky, S., 2006. Common Vulnerability Scoring System. *Security & Privacy, IEEE*, 4(6), pp.85-89.

National Defense Industrial Association (NDIA), 2014. *Cybersecurity for Advanced Manufacturing*. White Paper. NDIA.

NIST, 2014. *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology.

Obama, B., 2013. *Improving Critical Infrastructure Cybersecurity*. Executive Order. Federal Register.

Rost, J. & Glass, R.L., 2011. *The Dark Side of Software Engineering: Evil on Computing Projects*. Wiley-IEEE Computer Society Press. Available at: http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470597178.html [accessed 14 December 2014].

Sadowsky, G. et al., 2003. *Information Technology Security Handbook*. Washington, DC, United States of America: The World Bank.

Strum, L.D. et al., 2014. Cyber-physical Vulnerabilities in Additive Manufacturing Systems. In *Proceedings of the 25th Annual International Solid Freeform Fabrication Symposium*. Austin, TX, 2014.

Symantec, 2014. *Internet Security Threat Report 2014, Volume 19*. Annual Threat Report. Symantec Corporation.

Symantec, 2015. *Internet Security Threat Report 2015, Volume 20*. Annual Threat Report. Symantec Corporation.

Target, 2014. *Data Breach FAQ*. [Online] Available at: corporate.target.com/about/shopping-experience/payment-card-issue-faq [Accessed 28 October 2015].

Ten, C.-W., Liu, C.-C. & Manimaran, G., 2008. Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Transactions on Power Systems*, 23, pp.1836-46.

Vincent, H., Wells, L., Tarazaga, P. & Camelio, J., 2015. Trojan Detection and Side-channel Analyses for Cyber-security in Cyber-physical Manufacturing Systems. *Procedia Manufacturing*, 1, pp.77-85. Available at: http://www.sciencedirect.com/science/article/pii/S2351978915010653.

Wells, L.J., Camelio, J.A., Wiliams, C.B. & White, J., 2014. Cyber-physical Security Challenges in Manufacturing Systems. *Manufacturing Letters*, 2(2), pp.74-77.