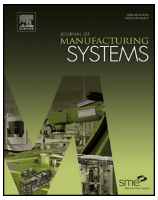
Journal of Manufacturing Systems 43 (2017) 339–351

Contents lists available at ScienceDirect

Journal of Manufacturing Systems

journal homepage: www.elsevier.com/locate/jmansys



An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems

Zach DeSmit[a,*], Ahmad E. Elhabashy[a,b], Lee J. Wells[c], Jaime A. Camelio[a]

[a] Grado Department of Industrial & Systems Engineering, Virginia Tech, Blacksburg, VA 24061, USA
[b] Production Engineering Department, Faculty of Engineering, Alexandria University, Alexandria 21544, Egypt
[c] Industrial and Entrepreneurial Engineering & Engineering Management Department, Western Michigan University, Kalamazoo, MI 49008, USA

ARTICLE INFO

Article history:
Received 9 November 2016
Received in revised form 8 March 2017
Accepted 15 March 2017
Available online 7 April 2017

Keywords:
Cyber-physical security
Decision tree analysis
Intelligent manufacturing systems
Vulnerability assessment

ABSTRACT

The rampant increase in frequency and complexity of cyber-attacks against manufacturing firms has motivated the development of identification and assessment techniques for cyber-physical vulnerabilities in manufacturing. While the field of cybersecurity assessment approaches is expansive, there is a gap in assessments for cyber-physical vulnerabilities in intelligent manufacturing systems. In response, this paper provides an approach for systematically identifying cyber-physical vulnerabilities and analyzing their potential impact in intelligent 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 vulnerabilities for each production process. The stoplight scale allows manufacturers to interpret assessment results in an intuitive way. Finally, a case study of the proposed approach at an applied manufacturing research facility and general recommendations to securing similar facilities from cyber-physical attacks are provided.

Published by Elsevier Ltd on behalf of The Society of Manufacturing Engineers.

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 1000 Iranian high-speed centrifuges used for uranium enrichment. Specifically, the life-spans of these centrifuges were significantly reduced by periodically changing their rotational speeds [1,2]. This attack was successful because it was able to display misleading equipment readings (readings indicated no problems) to operators [3].

Examples of other cyber-attacks are quite numerous, expanding across a variety of fields. Recent cyber-attacks include the Yahoo data breach of 2016 [4], the hacking of Sony Pictures Entertainment [5] in November 2014, and acquiring private customer information from Anthem Health Insurance in December 2014 [6]. In addition to the Stuxnet virus, other examples also involved cyber-attacks on physical systems, such as the “logic bomb” that was reportedly inserted in the Trans-Siberian pipeline’s control software. This attack changed pump and valve settings, causing a massive explosion in 1982 [7]; in 2016, there was an attack on a power grid which cut power to over 100,000 people [8]. These examples demonstrate that no system is beyond the reach by cyber-attackers, and intelligent manufacturing systems are no exception.

Over the last few years, manufacturing has been one of the most targeted sectors for cyber-attacks [9,10] by spear-phishing attacks.[1] 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 2015 [12]. Attacks such as these traditionally aim at gaining unauthorized access to information or valuable trade secrets [13]. 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 [14], including manufacturing. In addition, internet-based Computer Aided Engineering (CAE) support tools, such as cloud computing

* Corresponding author.
E-mail addresses: zachd1@vt.edu, zachdesmit@gmail.com (Z. DeSmit), habashy@vt.edu (A.E. Elhabashy), lee.wells@wmich.edu (L.J. Wells), jcamelio@vt.edu (J.A. Camelio).

[1] A *spear-phishing attack* is a targeted e-mail scam aiming to access sensitive data, steal valuable information, or install malware on compromised computers [11].

http://dx.doi.org/10.1016/j.jmsy.2017.03.004
0278-6125/Published by Elsevier Ltd on behalf of The Society of Manufacturing Engineers.

and software as a service (SaaS) are being adopted across manufacturing. This opens new unwanted "doors" for malicious attacks into current intelligent 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 [15], 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 [16]. 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 [15].

Recently, the median number of days between the onset of a cyber-attack was reported and its detection in an organization was over 200 days [17]. Additionally, 69% of these attacks were not discovered by the victims themselves, but by third parties such as law enforcement agencies and customers [17]. Currently, there is little emphasis placed on cyber-physical security in present manufacturing environments, as cybersecurity for manufacturing is commonly treated as a purely information technology concern. However, given the cyber-physical nature of intelligent manufacturing, attacks against these systems cannot be mitigated by traditional cybersecurity approaches [2,18]. 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 possible cyber-physical attacks.

There exists a need to develop a manufacturing specific approach to identify and assess cyber-physical vulnerabilities[2] within the manufacturing industry. 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 identifies those vulnerabilities through a systematic cyber-physical vulnerability assessment approach for intelligent manufacturing systems. In addition to identifying and analyzing vulnerabilities within the manufacturing environment, the proposed approach is the first of a five-step cyber-physical security protocol: identifying and assessing vulnerabilities, protection, attack detection, response strategy, and recovery protocol; proposed by the National Institute of Standards and Technology (NIST) [20]. The proposed approach provides manufacturing enterprises with a method to adhere to cybersecurity frameworks, such as NIST's [20]. 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 [21]; 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 [22]. Together, vulnerability assessments and risk analysis reports allow an organization to view their security stance at any given time.

There exists only limited research within the field of vulnerability assessment for cyber-physical systems. Baker developed a three-step process for cyber vulnerability assessment and risk analysis methods for cyber-physical systems [23]. The first step consists of understanding the organizational structure. Second, the organization determines failure modes and identifies potential consequences. Lastly, the organization implements improvements [23]. 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. developed a vulnerability assessment approach for industrial control systems, specifically, Supervisory Control and Data Acquisition (SCADA) Systems [24]. 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 [24]. 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 [24]. That NERC requirement is similar to a US manufacturing mandate by President Obama in 2013 [25]. However, the approach of Ten et al. [24] 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. expanded the risk management frontier for manufacturers to include cybersecurity risks and vulnerabilities. Hutchins et al. outlined a framework for identifying cybersecurity risks in manufacturing [26]. 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 [26]. While providing a structured approach to identifying cybersecurity risks in manufacturing, their approach does not consider cyber-physical security in its assessment, which includes the securing of products or processes that arise from the interconnectivity of the manufacturing enterprises.

A number of researchers have noted the inability to identify vulnerabilities within cyber-physical systems as a serious issue. These researchers have constructed systems and methodologies that attempt to identify attack vectors in cyber-physical systems. The majority of these approaches focus solely on the electric Smart Grid, such as Vellaithurasi et al. [27], Shi and Jian [28], Stefanov [29], and Guo et al. [30]. Other approaches, such as the one proposed by Xiaotian et al., attempted to identify critical components within a cyber-physical system based on network communication [31]. While, Liu et al. developed a security approach that is based on overlaying dependence analysis on a network matrix [32]. However, given the specific nature of manufacturing systems, none of these cyber-physical vulnerability assessments could be applied.

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. Some of the common tools are created at research institutions, such as Carnegie Mellon University's Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [33]. Others are created from government and federal agencies, such as the Federal Financial Institutions

[2] 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 [19].

Examination Council's (FFIEC) assessment tool [34] and the NIST Cybersecurity Framework [20].

The OCTAVE assessment strives to assist organizations in aligning their security activities with overall organizational goals [33]. 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 [34]. 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 an 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 [25]. The framework focuses primarily on cyber challenges, i.e. intellectual property concerns, leaving the questions related to cyber-physical vulnerabilities unanswered [20]. 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 Cybersecurity 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, methods exist for identifying cyber vulnerabilities within an organization, but they do not focus on the "physical" aspect; while the assessments accounting for the "physical" aspect are not well suited for intelligent manufacturing systems. Table 1 summarizes how the proposed approach compares to other currently existing methods.

The proposed approach is the first approach to translate cybersecurity vulnerability assessment techniques to cyber-physical manufacturing 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 motivate the creation of follow-up mitigation techniques and industry best practices, but is a step towards the creation and implementation of a comprehensive 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 idea 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 Fig. 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 this procedure would continue through every intersection in the manufacturing process.

The proposed approach starts with mapping intersections and analyzing the vulnerability impact at each intersection node; as shown in Fig. 2. However, better understanding of the process flow, transition of data/knowledge, and resource requirements for a given manufacturing system is first needed as a key input to the proposed approach. Hence, a comprehensive process mapping of the concerned production area is performed before the intersection mapping. Due to not being part of the proposed approach, the details of development of the process mapping are not discussed in this work. For a complete analysis, process maps and subsequent intersection maps need to be created for every part of the manufacturing process to ensure all intersections are included. After that, vulnerability impact analysis will be performed at each intersection node according to a set of specific metrics; as further discussed in Section 3.2. As an output of the approach, an overview of cyber-physical vulnerabilities existing in the system are made available to the manufacturer. Finally, leveraging the results of the proposed approach, appropriate mitigation strategies could be implemented by the manufacturers to better secure the compromised facilities.

It should be noted that the vulnerability assessment approach proposed here goes beyond malicious cyber-physical attack vulnerabilities and includes vulnerabilities from unintentional process

Table 1
Comparison of the different cyber-security assessment approaches and audit tools (adapted from [20,27–32,35]) with the proposed approach.

	Traditional Cyber-Security Audit	NIST Cyber-security Framework	FFIEC	OCTAVE	Cyber-physical Vulnerability Assessments	The Proposed Approach
Focus on Cyber-Physical Security					x	x
Protection of Intellectual Property	x	x	x	x		
Supports Enterprise Compliance Requirements				x		x
Produces Consistent Results Across Enterprise		x	x	x	x	x
Easy/Intuitive to Implement				x		x

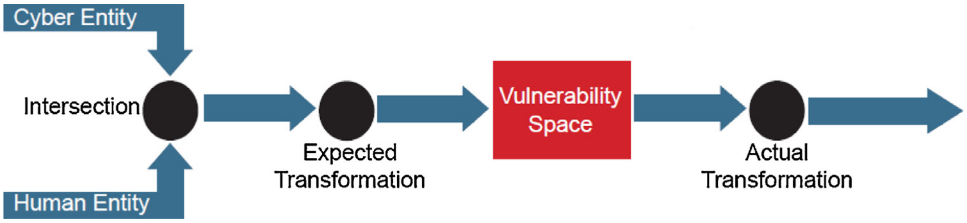


Fig. 1. An example of a cyber/human intersection.

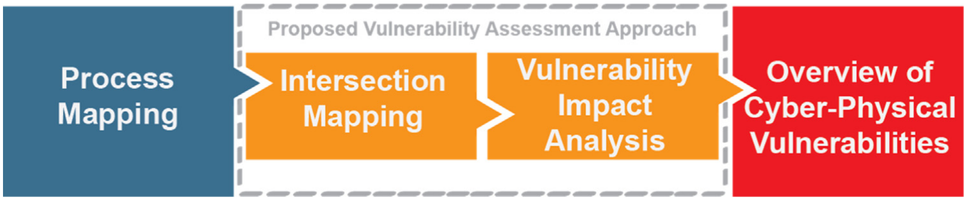

Process Mapping
Proposed Vulnerability Assessment Approach
Intersection Mapping
Vulnerability Impact Analysis
Overview of Cyber-Physical Vulnerabilities

Fig. 2. Outline of the proposed vulnerability assessment approach.

changes as well. It is a general approach to understanding 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 (listed next) 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, 3D printers, 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.

3.2. *Cyber-physical vulnerability impact analysis*

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 the 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; in a fashion similar to a stoplight scale to allow manufacturer to easily interpret the assessment approach results. 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. Details for trees corresponding to each of these metrics are discussed next.

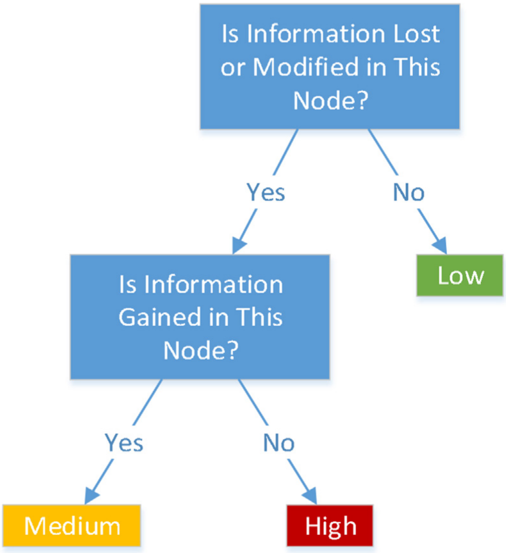

Is Information Lost or Modified in This Node?
Yes
No
Low
Is Information Gained in This Node?
Yes
No
Medium
High

Fig. 3. Loss of Information metric decision tree.

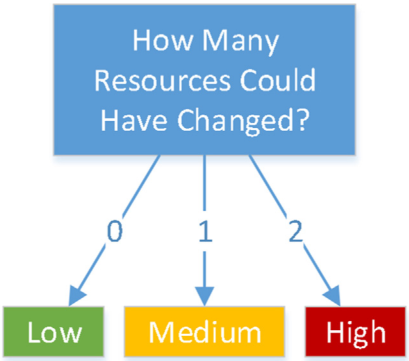


Fig. 4. Inconsistency metric decision tree.

3.2.1. *Loss of information metric*

The first question in the decision process for this metric determines if 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 only two inputs for each node,[3] 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 Fig. 3. For the Loss of Information 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.

3.2.2. *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, as shown in Fig. 4. An example of this would be a change in the operator of a physical machine or the changing of a tool or machine setup.

3.2.3. *Relative frequency metric*

The decision process for the vulnerability of a node with respect to the relative frequency metric can be seen in Fig. 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 approaching zero and results in a rating of low. Likewise, the Computer-Aided Manufacturing (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 approaching one, resulting in a high rating.

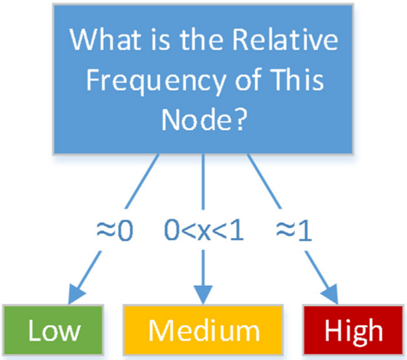


Fig. 5. Relative Frequency metric decision tree.

3.2.4. *Lack of maturity metric*

The fourth decision tree, shown in Fig. 6, answers the questions of lack of maturity of a specific node. The first question determines if the manufacturer considers the resource 100% trustworthy. An example of a non-trusted resource or factor would perhaps be a 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.

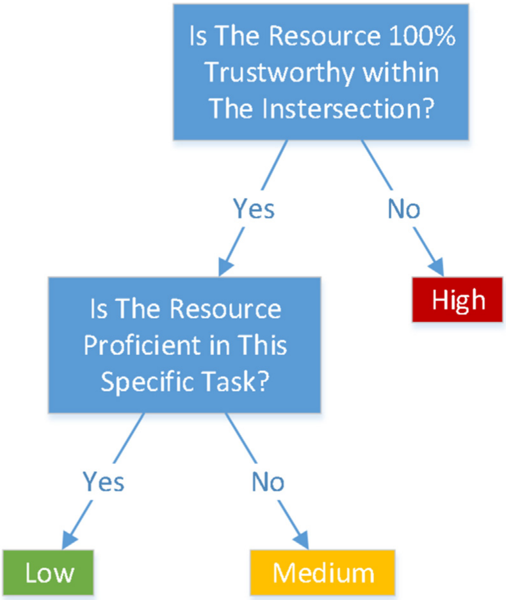

Is The Resource 100% Trustworthy within The Instersection?
Yes
No
High
Is The Resource Proficient in This Specific Task?
Yes
No
Low
Medium

Fig. 6. Lack of Maturity metric decision tree.

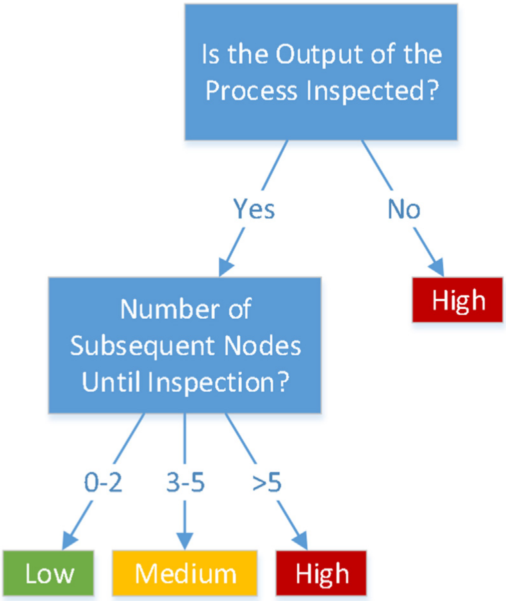

Is the Output of the Process Inspected?
Yes
No
High
Number of Subsequent Nodes Until Inspection?
0-2
3-5
>5
Low
Medium
High

Fig. 7. Time until Detection metric decision tree.

[3] During the intersection mapping step, the inputs of all intersection nodes are restricted to only 2 entities.

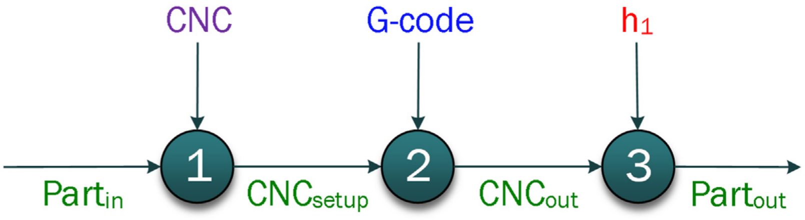


Fig. 8. An example of a vulnerability intersection map for a manufacturing process.

3.2.5. *Time until detection metric*

The time until detection metric questions if the output of the process will eventually be inspected and the details of the corresponding decision tree are shown in Fig. 7. If a process will never 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.

3.3. *Example*

An example is used to demonstrate more clearly how the proposed two-step approach is implemented. This example is of creating a metal blank on a CNC machine, as a representative of a process commonly seen in industry. 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 examined by an inspector (h_1) as a visual quality control inspection resulting in the finished part ($Part_{out}$).

The corresponding intersection map of this process can be seen in Fig. 8. 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.

Next, the results of applying the cyber-physical vulnerability impact analysis are summarized in Table 2; where the logic in the described decision trees is 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 all low. These results indicate a 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.

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 both the CNC machine fixture and the raw material are proficient, corresponding 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.

3.4. *Summary of proposed approach*

A more detailed presentation of the proposed two-step approach is shown in Fig. 9. As previously mentioned, exhaustive process maps for the entire manufacturing facility are the input for this approach. Intersection mapping is the first step of the approach, where all the interactions present in the process maps are converted into intersections. It is important to note that each intersection has only 2 inputs, and a single output.

Following the intersection mapping the vulnerability impact analysis evaluates the five metrics using the different decision trees discussed in Section 3.2 for each node. The five metrics can be analyzed in any order even though the arrows used in Fig. 9 show a sequential process. Finally, the output of the proposed approach is providing an overview of the cyber-physical vulnerabilities existing in the manufacturing facility under consideration. Such an overview should help in assessing the cyber-physical security status of the system and devising corresponding mitigation and prevention techniques.

4. Case study

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 working with both universities and companies to rapidly translate promising research innovation into commercial use [36]. The overall goal of the case study was to identify that cyber-physical vulnerabilities, which can be exploited by cyber-attacks, exist within a manufacturing facility. Also, those vulnerabilities can be identified through the careful assessment of a facility's production process.

Table 2
Vulnerability assessment for the metal blanking process in Fig. 8.

#	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

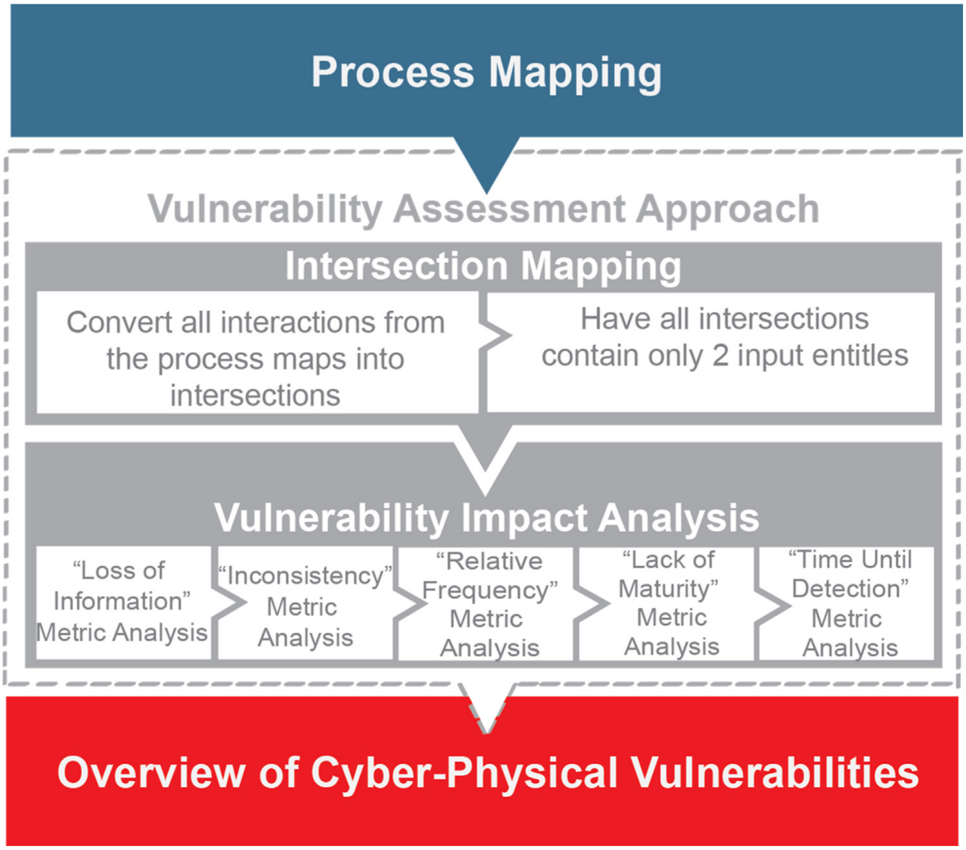

Process Mapping
Vulnerability Assessment Approach
Intersection Mapping
Convert all interactions from the process maps into intersections
Have all intersections contain only 2 input entitles
Vulnerability Impact Analysis
"Loss of Information" Metric Analysis
"Inconsistency" Metric Analysis
"Relative Frequency" Metric Analysis
"Lack of Maturity" Metric Analysis
"Time Until Detection" Metric Analysis
Overview of Cyber-Physical Vulnerabilities

Fig. 9. Details of the proposed approach.

Through the case study a part was manufactured at the CCAM facilities, going through various phases from the design intent to finishing and quality control. These phases included: product design, 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 ensure 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 it is possible for both the programmer and machinist to collaborate in these two steps. The machinist's input is often valuable and could cause the programmer to re-adjust the initial setup accordingly.

The other phase is the quality inspection phase, consisting 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 if the part is conforming to the required specifications.

4.1. 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, Fig. 10 shows the intersection map of the manufacturing process planning phase at CCAM. Each of the two previously mentioned steps are modeled

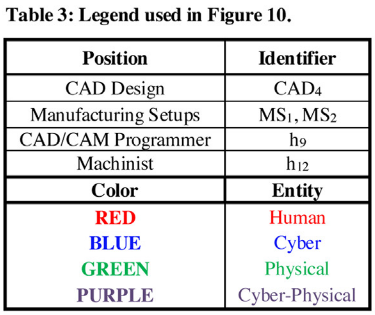


Table 3: Legend used in Figure 10.

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

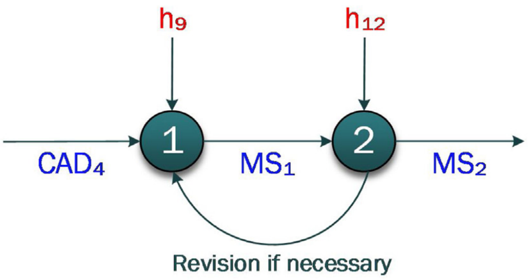


Fig. 10. Intersection map for the manufacturing process planning phase at CCAM.

as two separate nodes (nodes 1 and 2, respectively). Fig. 11 shows the intersection map for the CCAM's quality inspection phase, with three different nodes representing the different steps within this phase.

4.2. Cyber-physical vulnerability impact analysis

Upon completion of the intersection mapping, the decision trees are used to assess the vulnerability of each node. For the manufacturing process planning phase, the results are summarized in Table 5, where each of the two nodes has its resulting metric value (color-coded) from the cyber-physical vulnerability assessment approach. According to Table 5, 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 the remaining metric rating is low for both nodes.

As for the product quality inspection phase, the cyber-physical vulnerability assessment results are shown in Table 6. 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.

4.3. Interpreting the results

From the ratings obtained in both Tables 5 and 6, it can be concluded that vulnerabilities exist in the manufacturing environment used for this case study. More specifically, both nodes in the manufacturing process planning phase have at least 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 have varying patterns of vulnerabilities with the third node being slightly more vulnerable to cyber-physical attacks while the second node is 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 with intersections between cyber and physical entities are highly vulnerable to cyber-attacks. This insight 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.

4.3.1. Metric levels description for manufacturing process planning phase

To further understand the results seen in Tables 5 and 6, it may be helpful to step through the three different levels of cyber-physical vulnerability for each identified metric. The first node identified in Table 5, where the programmer creates the identified part setup for the previously designed part, can be used to further expand upon high, medium, and low levels of vulnerability related to the Relative Frequency metric. A low relative frequency would occur if the programmer designed a single machine setup for multiple parts within the production process. The vulnerability increases

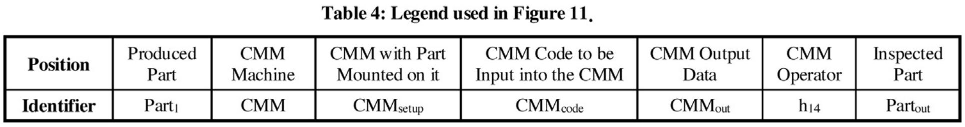


Table 4: Legend used in Figure 11.

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	$Part_I$	CMM	CMM_{setup}	CMM_{code}	CMM_{out}	h_{14}	$Part_{out}$

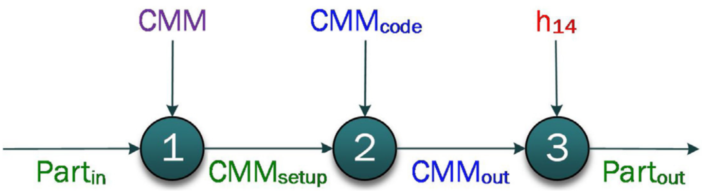


Fig. 11. Intersection map for the quality inspection phase at CCAM.

Table 5
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

Table 6
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
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

to medium if the programmer designs multiple machine setups that are used to secure the same part in the CNC machine. Finally, the vulnerability increases to high if the programmer designs a new manufacturing setup from scratch for every single part that is to be fixed in the CNC machine.

The second node identified in Table 5, where the machinist finalizes the manufacturing setup, can further demonstrate how Inconsistency can cause low, medium, or high levels of cyber-physical vulnerability. An example of low cyber-physical vulnerability during this process would be if neither the machinist nor the machine setup were allowed to change. The level of vulnerability would increase to medium if the machinist (or the machine setup) was changed prior to completion of the process for any reason. The increase in vulnerability comes from the inconsistencies present between two different machinists (or machine setups). Lastly, a high level of vulnerability could be reached if both the machinist and the manufacturing setup were changed.

4.3.2. Metric levels description for quality inspection phase

From the quality inspection phase vulnerability assessment in Table 6, the first node of creating the measurement setup on the CMM can be used to demonstrate low, medium, and high levels of vulnerability related to the Loss of Information metric. A low level of cyber-physical vulnerability can be obtained if the setup of the CMM is completely documented, thus transferring all information from the setup to the following processes. A medium value would be obtained if only a small amount of information were documented pertaining to the CMM setup. The medium value corresponds to only some information being documented, forcing a subsequent process to make guesses about the setup. Lastly, a high value could be achieved if the CMM setup is constructed without documentation, thus eliminating the ability to reproduce the setup exactly.

The second node in Table 6 can be used to demonstrate the low, medium, and high levels of vulnerability of the Time until Detection metric. A low value coincides with the immediate validation of the process. That is, if the measurement from the CMM is immediately confirmed by the machine, a low value would be given. A medium value would be assigned if the CMM measurement wasn't validated until a later time. Finally, a high value would be achieved if the measurements from the CMM were never validated or were not validated for an extended period of time.

Lastly, the final process listed in Table 6 can be used to demonstrate the Lack of Maturity metric and its relation to low, medium, and high levels of cyber-physical vulnerability. A low Lack of Maturity could be achieved if the CMM operator has been performing this job for many years and is well versed in the intricacies of the part being measured. The metric could be assessed as medium if the CMM operator has been performing this job for years, but is not well versed in the part that is being measured. Finally, a high value would be assigned if the CMM operator was new to this position and had little to no information about the part being measured. A more mature operator has a higher chance of noticing a potential cyber-physical attack.

4.4. Validating the results

This subsection describes the details of a proof-of-concept cyber-physical attack implemented within the case study at CCAM to validate the results from the vulnerability assessment. The attack was launched independent of obtaining the metrics attained from the vulnerability assessment approach. After the attack implementation, the approach results were then re-visited to evaluate if the information they had provided corresponds to the exploited vulnerabilities.

4.4.1. Selected part

The selected test part that is manufactured for this case study was actually the GE prototype jet engine bracket illustrated in Fig. 12. This design was a part of the "GE Jet Engine Bracket Challenge" [37] and was chosen for this case study for the following reasons: 1) publicly available design; 2) the part's significant structural importance; 3) good mixture of simple and complex geometrical features; and 4) known loading conditions (made available to challenge participants).

The GE Jet Engine Bracket Challenge used additive manufacturing as the production process. However, the part geometry illustrated in Fig. 12 was altered slightly as the geometry was not well suited for the machining resources available at CCAM. This modified geometry can be seen in Fig. 13 which includes: 1) altering the left side design and making the bracket symmetrical; 2) removing bottom and top draft angles from all sides and making the sides square; 3) removing angle on back side and making the back side parallel to the front side; 4) removing the current face transition and making it smoother; and 5) redesigning the cavity for symmetry. After that, a generic GD&T was performed as shown in Fig. 14. This GD&T was used as a baseline for developing the CMM program for quality control.

4.4.2. Details of the cyber-physical attack

The cyber-physical attack was carried out with coordination with CCAM personnel, as if an attacker has already penetrated

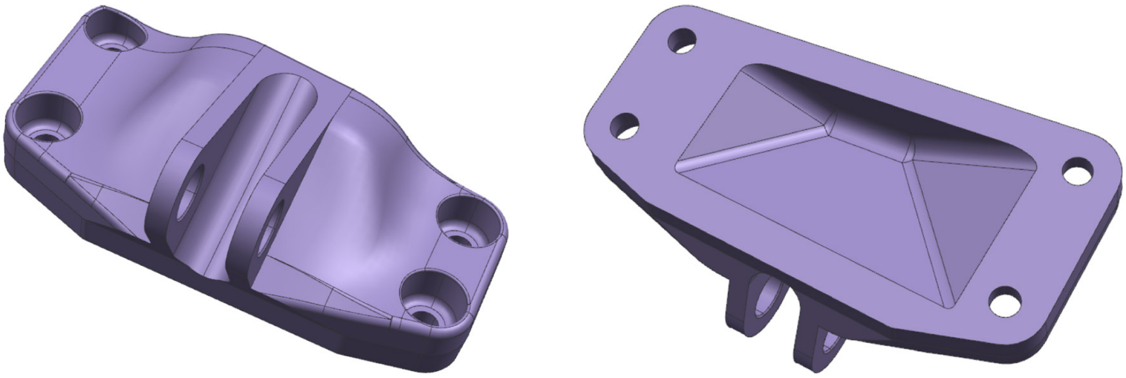


Fig. 12. GE prototype jet engine bracket.

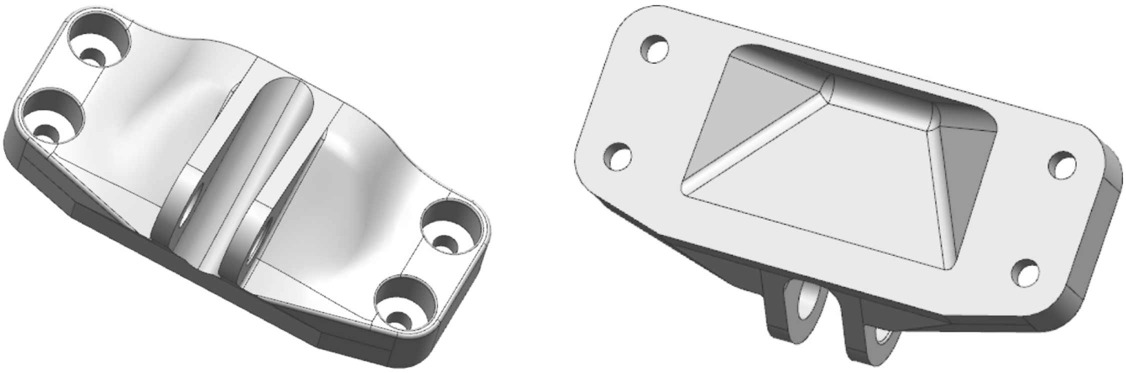


Fig. 13. GE prototype jet engine bracket modifications.

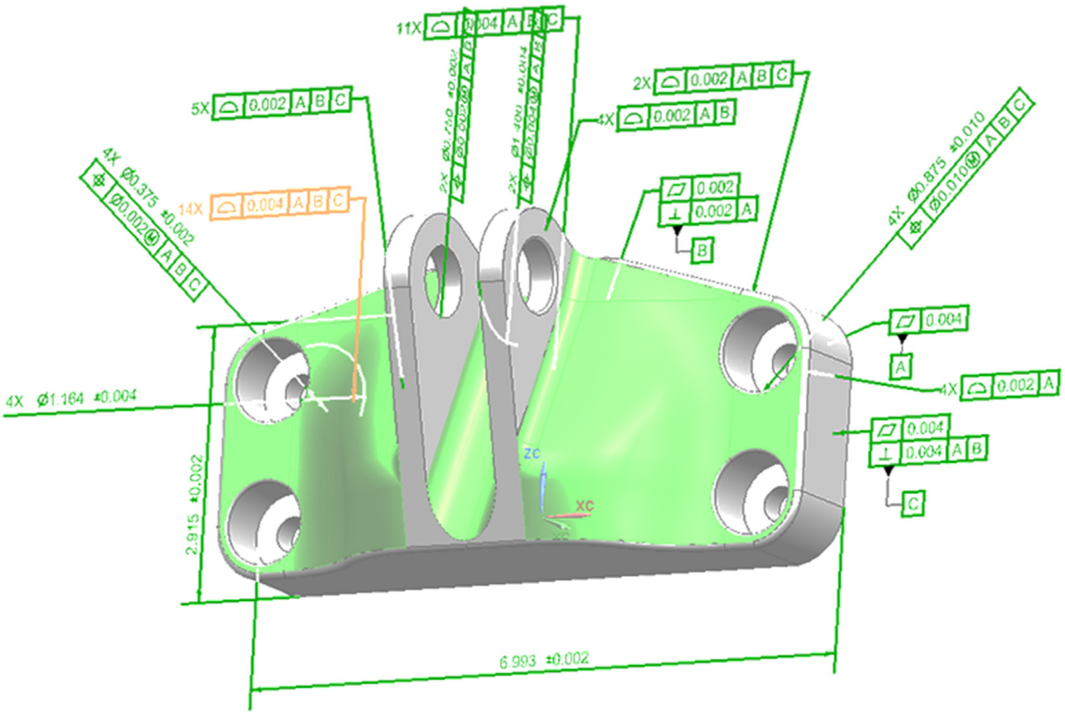


Fig. 14. Manufactured jet engine GD&T details.

the system and has access to the different resources in the facility. Therefore, this attack demonstrates what would occur as the result of a network penetration. With the different manufacturing phases at CCAM facilities, the attack altered the CAD file of the part. Specifically, three part features were targeted for the attack after reviewing the GD&T produced for the bracket. It is important to note that these attacks focused on simple features that could be

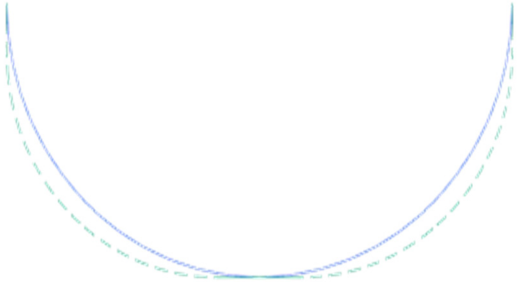


Fig. 15. Attacked feature #1.

easily adjusted in the CAM environment used. The details regarding these feature attacks are as follows.

4.4.2.1. Feature attack #1. The first feature attacked was the profile of the channel between the part's two lug plates. This profile was slightly modified to reduce the amount of material present. Fig. 15 illustrates this attack, where the blue line is the original profile and the green dashed line is the modified profile.

4.4.2.2. Feature attack #2. The second feature attacked was the angle of the channel between the part's two lug plates. This angle was slightly modified to reduce the amount of material present. Fig. 16 shows this attack, where the blue solid line is the original channel angle and the green dashed line is the modified channel angle.

4.4.2.3. Feature attack #3. The third feature attacked was the radius of one edge on the pocket that resides on the bottom of the part. The radius was slightly modified to reduce the amount of material present. Fig. 17 demonstrates this attack, the left image is the original pocket geometry and the right image is the modified pocket geometry.

By replacing the original CAD file with the one containing the three feature modifications, an altered part was manufactured at CCAM. The attack went unnoticed and the altered part was allowed to progress through the remainder of the manufacturing system. Not being able to detect the existence of the cyber-physical attack occurred for a number of reasons: 1) the attack was implemented after the product design has been completed and its CAD file sent to be machined; 2) neither the CAD/CAM programmer nor the machinist had any reason to doubt the accuracy of the CAD file; 3) the altered part didn't have an effect on the manufacturing setup or tools needed; 4) the features the CMM were programed to check were not affected by the attack; and 5) the changes made to the part were difficult to detect during visual inspection.

4.4.3. Proposed approach evaluation

Evaluating the proposed approach with regard to this cyber-physical attack shows the approach did indeed identify areas of

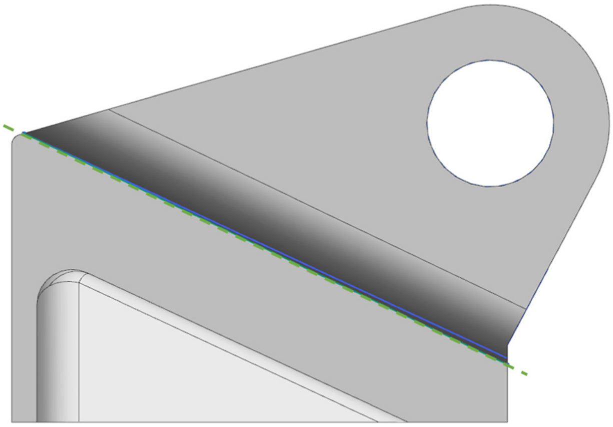


Fig. 16. Attacked feature #2.

vulnerabilities that were exploited by the attack. As discussed in Section 4.4.2, the executed cyber-physical attack maliciously altered the CAD file; making the manufacturing process planning phase the first phase to be entirely impacted. The altered CAD file was then loaded into the CNC machine and a flawed part was manufactured. The proposed approach categorized four of the five vulnerability analysis metrics for the first node of this phase in Table 5 to have a high value of cyber-physical vulnerability; and three out of the five for the second node.

This coincided with the successful exploitation and implementation of the attack on the cyber-physical system. More specifically, the approach exposed the high vulnerability with the Time until Detection metric in the manufacturing process planning phase. According to the results, it would take a while for an attack to be detected; which is exactly what happened. The attack was not detected in this phase nor in subsequent phases verifying the vulnerability assessments conclusion. Similarly, the Lack of Maturity metric had a low rating in the results; which wasn't a weakness exploited by the attacker, since the attack wasn't initially implemented at this phase.

On the other hand, the results of the approach indicated that the Time until Detection metric in Table 6 had a low value for all nodes within the quality inspection phase; yet, the actual attack was not detected there. The reason behind this is the fact that the attacked features were designed with the knowledge of the GD&T parameters used by the CMM in this phase. With that taken into account, there was no chance for the CMM to detect the attack; despite expecting this phase to capture any irregularities. It should be noted that a low rating means it is unlikely a vulnerability will be exploited by an attack. This behavior would likely be observed if the attack was not highly sophisticated. This outcome warrants perhaps revising the definition of this metric to make it more robust or including more metrics in the assessment approach to compensate for that. Nevertheless, similar arguments to those discussed for

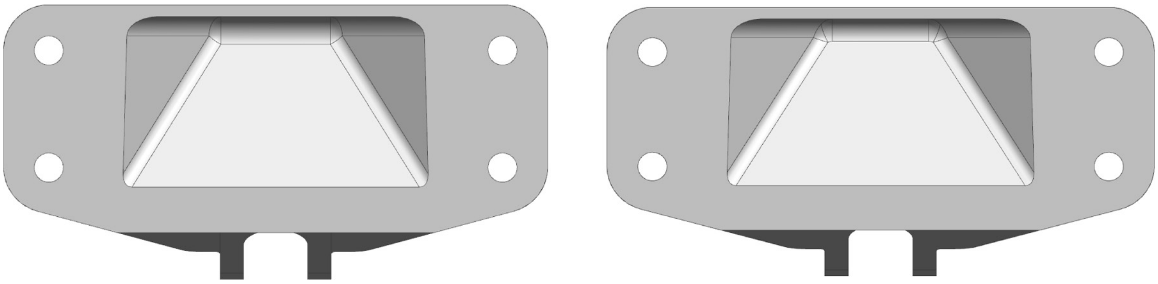


Fig. 17. Attacked feature #3, original (left) and modified (right).

the manufacturing process planning phase could be still be made for this phase.

The results for both the Inconsistency and Relative Frequency metrics from the case study were concerning. They indicated additional significant areas of vulnerability that need to be addressed. To mitigate these potential 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 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. Another suggestion is 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. These vulnerabilities pose a significant risk to their manufacturing production process if left unidentified. The proposed approach consists 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 analyzed. This assessment is a step in the right direction for manufacturers to begin to take cyber-physical security seriously. The literature has shown 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 processes used in the case study, many areas of improvement were identified. This motivates the further development of a more comprehensive full cyber-physical vulnerability assessment tool. Used to detect cyber-physical vulnerabilities within an intelligent 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.

Threat identification for cyber physical security in advanced manufacturing is a future research area. The proposed approach only identifies and assesses cyber-physical vulnerabilities. A natural extension is to determine the likelihood of each threat from previous data collected from customer discovery and through the analysis of threats seen commonly in industry. Risk analysis is another capability which could be developed from the vulnerability assessment tool. This capability would identify the likelihood of the cyber-physical vulnerability being exploited and combine that with the potential impact given by the manufacturer, providing them with an individualized risk assessment. Lastly, these capabilities should be incorporated into 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 serve as an audit based tool. The audit tool would be semi-automated requiring the manufacturer 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.

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 [38]. 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 [39]. 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.

Acknowledgements

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* (CPSSMFG) Group. The authors would also like to thank 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

[1] Albright D, Brannan P, Christina W. Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant? Institute for Science and International Security (ISIS); 2010.
[2] Vincent H, Wells L, Tarazaga P, Camelio J. Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. Procedia Manuf 2015;1:77–85.
[3] Cherry S. Sons of stuxnet. IEEE spectrum 2011.
[4] Fahey M, Wells N. Yahoo data breach is among the biggest in history. CNBC, cnbc.com; 2016.
[5] Lee TB. The Sony hack: how it happened, who is responsible, and what we've learned. Vox Media; 2014.
[6] Anthem. How to access & sign up for identity theft repair & credit monitoring services. Anthem, Inc.; 2015.
[7] Rost J, Glass RL. The dark side of software engineering: evil on computing projects. Wiley-IEEE Computer Society Press; 2011.
[8] Tuptuk N, Hailes S. The cyberattack on Ukraine's power grid is a warning of what's to come. The Conversation US, Inc.; 2016.
[9] Symantec. Symantec Corporation; 2014.
[10] Symantec. Symantec Corporation; 2015.
[11] Kaspersky. What is spear phishing? – definition. Kaspersky Lab; 2015.
[12] ICS-CERT. ICS-CERT monitor newsletters: November-December 2015. Department of Homeland Security; 2016.
[13] Deloitte. Global cyber executive briefing – manufacturing. Deloitte Touche Tohmatsu Limited; 2014.
[14] Evans D. The internet of things: how the next evolution of the internet is changing everything. Cisco Internet Business Solutions Group (IBSG); 2011.
[15] Wells LJ, Camelio JA, Williams CB, White J. Cyber-physical security challenges in manufacturing systems. Manuf Lett 2014;2:74–7.
[16] Sturm LD, Williams CB, Camelio JA, Parker WJR. Cyber-physical vulnerabilities in additive manufacturing systems. In: 25th Annual solid freeform fabrication symposium. 2014.
[17] M-Trends 2015: a view from the front line. Mandiant; 2015.
[18] Cybersecurity for advanced manufacturing. National Defense Industrial Association (NDIA); 2014.
[19] Sadowsky G, Dempsey JX, Greenberg A, Mack BJ, Schwartz A. Information technology security handbook. Washington, DC: World Bank; 2003.
[20] National Institute of Standards and Technologies (NIST). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology; 2014.
[21] Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system. IEEE Secur Privacy 2006;4:85–9.
[22] Cerullo MJ, Cerullo V. EDP risk analysis. Comput Audit Update 1994;1994:9–30.

[23] Baker GH. A vulnerability assessment methodology for critical infrastructure sites; 2005.
[24] Ten C-W, Liu C-C, Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems. IEEE Trans Power Syst 2008;23:1836–46.
[25] Obama B. In: Policy F, editor. Improving critical infrastructure cybersecurity. The White House; 2013.
[26] Hutchins MJ, Bhinge R, Micali MK, Robinson SL, Sutherland JW, Dornfeld D. Framework for identifying cybersecurity risks in manufacturing. Procedia Manuf 2015;1:47–63.
[27] Vellaithurai C, Srivastava A, Zonouz S, Berthier R. CPIndex: cyber-physical vulnerability assessment for power-grid infrastructures. IEEE Trans Smart Grid 2015;6:566–75.
[28] Shi L, Jian Z. Vulnerability assessment of cyber physical power system based on dynamic attack-defense game model. Dianli Xitong Zidonghua/Autom Electr Power Syst 2016;40:99–105.
[29] Stefanov A, Liu C-C, Govindarasu M, Wu S-S. SCADA modeling for performance and vulnerability assessment of integrated cyber-physical systems. Int Trans Electr Energy Syst 2015;25:498–519.
[30] Guo J, Han Y, Guo C, Lou F, Wang Y. Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties. Energies 2017;10:87.
[31] Xiaotian W, Davis M, Junjie Z, Saunders V. Mission-aware vulnerability assessment for cyber-physical systems. In: 2015 IEEE Trustcom/BigDataSE/ISPA, 20–22 Aug. 2015, IEEE Computer Society. 2015. p. 1148–53.
[32] Liu X, Zhang J, Zhu P. Dependence analysis based cyber-physical security assessment for critical infrastructure networks. Information technology, electronics and mobile communication conference (IEMCON), 2016 IEEE 7th Annual, IEEE 2016:1–7.
[33] Caralli RA, Stevens JF, Young LR, Wilson WR. The OCTAVE allegro guidebook, v1. 0. Software Engineering Institute; 2007.
[34] Federal Financial Institutions Examination Council (FFIEC). FFIEC Cybersecurity Assessment Tool Overview. In: Council F.F.I.E., editor. 2015.
[35] Caralli RA, Stevens JF, Young LR, Wilson WR. Introducing OCTAVE allegro: improving the information security risk assessment process. Carnegie Mellon University; 2007.
[36] CCAM. Commonwealth center for advanced manufacturing – about us, in, 2015.
[37] GrabCAD. GE jet engine bracket challenge. GrabCAD a STRATASYS solution; 2013.
[38] Bergvall J, Svensson L. Risk analysis review. Linköping, Sweden: Linköpings University; 2012.
[39] El Fray I. A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in information systems. In: IFIP international conference on computer information systems and industrial management. 2012. p. 428–42.