Procedia Manufacturing

Volume 1, 2015, Pages 77–85

43rd Proceedings of the North American Manufacturing Research Institution of SME http://www.sme.org/namrc

Trojan Detection and Side-Channel Analyses for Cyber-Security in Cyber-Physical Manufacturing Systems

Hannah Vincent[1], Lee Wells[1,*], Pablo Tarazaga[2], and Jaime Camelio[1]

[1]*Grado Department of Industrial and Systems Engineering, Virginia Tech*

[2]*Mechanical Engineering, Virginia Tech*

Blacksburg, VA, U.S.

hannahev@vt.edu, leejay@vt.edu, pablot@vt.edu, and jcamelio@vt.edu

Abstract

As the maliciousness and frequency of cyber-attacks continues to grow, the safety and security of cyber-physical critical infrastructures, such as manufacturing, is quickly becoming a significant concern across the globe. Outside of traditional intellectual property theft, attacks against manufacturing systems pose a threat to maintaining a product's design intent. More specifically, such attacks can alter a manufacturing system to produce a part incorrectly; resulting in impaired functionalities or reduced performance. Manufacturing systems rely heavily upon the use of quality control systems to detect quality losses and to ensure the continued production of high-quality parts. However, quality control systems are not designed to detect the effects of malicious attacks and are ill-suited to act as a cyber-security measure for many manufacturing systems. Therefore, this paper presents a novel product/process design approach to enable real-time attack detections to supplement the shortcomings of quality control systems. The proposed approach, inspired by side-channel schemes used to detect Trojans (foreign malicious logic) in integrated circuits, aims at detecting changes to a manufactured part's intrinsic behavior through the use of structural health monitoring techniques.

Keywords: Cyber-Attack detection, Cyber-Physical manufacturing systems, Quality control, Side-Channel analyses, Structural Health Monitoring, Trojans

1 Introduction

The evolution of manufacturing systems from disjoint mechanical processes to interconnected cyber-physical systems has introduced many opportunities for cyber-attacks against advanced manufacturing systems. The recent increase in the reliance on digital technologies has introduced new

* Corresponding Author

Peer-review under responsibility of the NAMRI Scientific Committee

doi:10.1016/j.promfg.2015.09.065

vulnerabilities that occur from taking trusted parts from untrusted sources [Rizzo, 2010], and in securing the current manufacturing cyber infrastructures [DMDI Institute, 2013]. In general, these vulnerabilities can be categorized as: 1) Technical data theft, 2) Data alteration, and 3) Process control [NDIA, 2014].

The categories described above provide an overview of the current cyber-security situation for cyber-physical systems. While most companies and manufacturers have instituted methods to protect their solely digital systems and information; manufacturing security requirements are significantly different than those of traditional business IT systems [NDIA, 2014]. Typical cyber-security focuses solely on digital systems, whereas current manufacturing technologies apply both cyber and physical components. As a "first line of defense", traditional cyber-security techniques are used to protect against cyber-attacks aimed at manufacturing. However, as stated by FBI Director James Comey, "There are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked." [Cook, 2014]. This statement exemplifies the growing mentality in the cyber-community that 100% security can never be guaranteed and that all cyber-enabled systems can be exploited.

Given that cyber-attacks against manufacturing systems can result in a physical manifestation allows for the possibility of a "second line of defense". In the information technology industry, this "second line of defense" has a long history in identifying flaws placed into computer hardware and software logic. Unfortunately little to no research has focused on cyber-enabled attacks on manufactured components. Therefore, this paper presents a novel product/process design approach to enable real-time attack detection of compromised parts. The rest of the paper is organized as follows; in Section 2 we will discuss cyber-attacks in manufacturing systems and how traditional QC techniques are not necessarily capable of detecting the effects of cyber-attacks. Next, in Section 3, we will introduce the field of Trojan (malicious foreign logic) detection in integrated circuits. Finally, in Section 4, we will introduce an approach, based upon current Trojan detection strategies, to detect the effects of cyber-attacks on manufactured parts through the use of structural health monitoring techniques.

2 Cyber-Attacks Against Manufacturing Systems

Between late 2009 and early 2010 the infamous Stuxnet virus was responsible for destroying as many as 1,000 Iranian high-speed centrifuges used for uranium enrichment [Albright et al., 2010]. The core attack used by Stuxnet was to periodically change the rotational speeds of the centrifuges, drastically shortening their life-spans. While very successful, the attack would have been futile if not for the man-in-the-middle exploit used on the system's programmable logic controller (PLC) that presented false equipment readings to operators [Cherry & Constantine, 2011]. Currently, manufacturing systems are evolving into highly integrated cyber-physical systems that rely on their cyber components as much as they do their physical ones. This begs the question, "Is it possible to attack a cyber-physical manufacturing system to produce flawed parts, and if so, can the quality control (QC) system be exploited to hide the effects of the attack?"

Recently, two case studies were performed at Virginia Tech [Wells et al., 2014; Strum et al., 2014] to answer the first part of this question by demonstrating the ease in which cyber-physical manufacturing systems can be attacked to produce flawed parts with drastically reduced performance. In addition, these attacks was accomplished without visually alerting the system's operators to any signs of treachery. Figure 1 illustrates the different manufacturing process chains that were involved in these two studies and indicates the location in this chain where the attack was implemented.

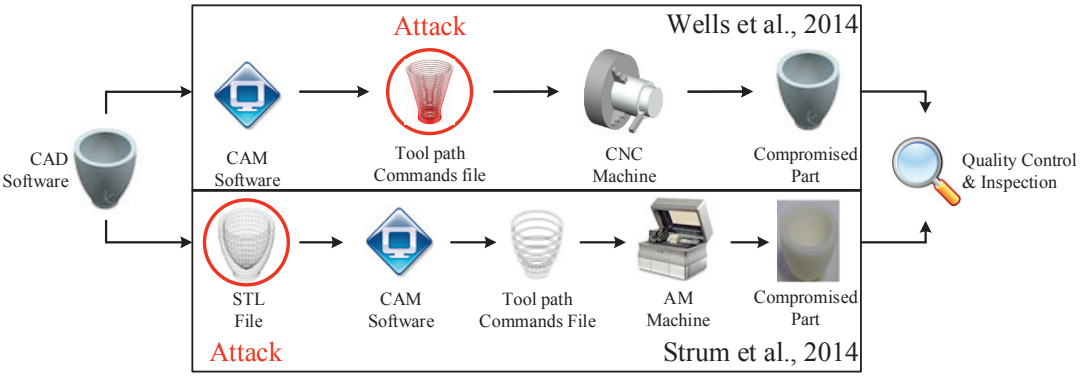

Figure 1: Manufacturing Process Chains used in the Attacks Implemented in the Studies by Wells et al., 2014 and Strum et al., 2014

In the first case study [Wells et al., 2014] an attack interfered with the transfer of digital design files used to manufacture a part. Participants were tasked to: 1) Design a tensile test specimen using computer-aided design (CAD) software, 2) Generate tool-paths using (computer-aided manufacturing) CAM software, and 3) Machine the specimen. The tool-path file was transferred to a computer that controlled a computer numerical control (CNC) milling machine. During this file transfer, a malicious software intercepted and altered the tool-path files, resulting in the manufacturing of an incorrect part. If this part had been used as intended, the end-product would have prematurely failed. Furthermore, participants were unable to determine the cause for producing incorrect parts as they were unaware of potential attacks against manufacturing.

In the second study [Strum et al., 2014] a malicious software was designed to modify STL files used in additive manufacturing. STL files are the standard CAD format used to manufacture parts using additive manufacturing technologies. In this experiment, an internal defect (void) was introduced within the part causing it to fail prematurely when tested. It should be noted that the malicious software analyzed the STL file to determine an optimal (with respect to causing the largest increase in stress concentrations) location to place the void. Similar to the results of [Wells et al. 2014], participants were unable to determine the cause of these incorrect parts, and concluded that the problem was due to an error in the printing process.

While the aforementioned study demonstrated that cyber-attacks against manufacturing systems are indeed feasible, the question still remains, “Can the QC system be exploited to hide the effects of the attack?" Over the past century, QC strategies have been vital for manufacturing to detect quality losses and in ensuring the continued production of high-quality parts. However, QC approaches are not designed to detect the effects of cyber-attacks. QC methods are based upon assumptions (sustained system shifts, rational sub-grouping, feature-based monitoring, etc.) that may no longer be valid under the presence of an attack. In fact, these assumptions can be exploited to make an attack undetectable. For instance, QC approaches generally focus on a product’s key quality characteristics (KQCs). Any attack that alters a non-KQC will most likely go undetected, especially for high-volume, complex parts. To illustrate this concept, a very simple and highly plausible example of a cyber-attack against a real-world manufacturing system is described in the remainder of this section.

Consider a manufacturer (Manufacturer A) that produces commercial trucks. The side frame rails for these trucks are being produced by Manufacturer B. Manufacturer B produces a wide range of rails for several commercial truck manufacturers through an almost completely automated process. The design specifications provided to Manufacturer B for these rails include the thickness, length, and cross-sectional geometry. In addition, Manufacturer B is provided with the size, location, and number of holes (bolts, wiring, brake-lines, etc.) required for the rails. For each rail that Manufacturer B produces, a simple text file that contains the locations and sizes for all necessary holes are uploaded to

a punching machine's controller. In addition, typical rails range from 30 to 40 ft. long and can easily have upwards of 100 required holes.

For QC purposes, Manufacturer B has an automated inspection system to test the hardness (indirectly measure the strength) of each rail they produce. In addition, two rails are inspected using a coordinate measuring machine (CMM) each day (out of more than 100 produced in a day). It should be noted that due to the large variety of rails being produce, not every rail model can be inspected. This inspection process ensures dimensional accuracy of the rail's cross-section and the quality of the holes (i.e. determine if a punch is worn or broken) being punched. Any holes that are missing (broken punch) are sent to rework.

Imagine that this system was attacked by altering the text file used by the punching machine's controller to produce a rail for Manufacturer A. This simple attack adds an additional hole (by adding one line of text) to the rail in a location of significantly high stress. Given that not all rail models are inspected on a given day could result in this attack going unnoticed. However, even if this rail model was inspected, detecting the addition of one hole would be nearly impossible. The CMM is programmed to measure KQCs, namely the location and size of holes that are supposed to exist and a view discrete points for measuring the rails cross-section. In addition, the probability of the CMM operator noticing an addition hole is incredible unlikely considering: 1) the overall length of the part, 2) the large number of holes that already exist, 3) the fact that numerous rail models are produced in the facility, and 4) the simple fact that (from the CMM operator's point of view) the occurrence of an additional hole is impossible.

After the frame rails for Manufacturer A have been produced they are shipped and delivered. At Manufacturer A's assembly plant, line operators begin to assemble these rails to other frame components, the suspension system, and the drive-train. During this process it is highly unlikely that the additional hole would be noticed considering: 1) cycle times for assembly stations in the automotive industry tend to be less than a few minutes, 2) line operators are responsible for very specific tasks that focus on a small section of the entire frame, 3) unoccupied/unused holes are common as they are required for subsequent assembly operations, and 4) the simple fact that (from the line operator's point of view) the occurrence of an additional hole is impossible.

Unoccupied/unused holes exist throughout the assembly process until the body is finally assembled to the frame. During this process, the body is lowered unto the frame and joined at discrete locations, which will aid in concealing the hole for the remainder of the assembly process. It could be argued that over time the effects of this attack will be noticed. However, by this time the damage would have already been done and dozens if not hundreds of trucks could have been produced with compromised side frame rails. In addition, the attack could have been implemented for only a short period of time. If this were the case, the attack may not be detected until the rail fails in-use.

From this example, it has been shown that current QC strategies cannot be relied upon to detect the effects of the malicious cyber-attack against manufacturing. Therefore, a more holistic approach to attack detection for manufacturing systems is desperately needed.

3 Integrated Circuits and Trojans

An area that parallels the current state of cyber-physical security for manufacturing systems is in the detection of "Trojans" placed in integrated circuits (ICs) produced by untrusted overseas manufacturers [Jin et al., 2009; Banga et al., 2009; Wang et al., 2008]. Trojans are extraneous malicious logic introduced into ICs in order to perform a specific task unrelated to the original intent of the IC. Once inserted, the Trojan's extra code within the IC reacts to specific triggers or situations, which activates the Trojan's harmful nature. Identifying these Trojans is difficult because the circuits cannot be easily tested for the presence of Trojans nor their effects. Traditional testing fails because the unanticipated behavior introduced by the Trojan is not necessarily on the IC's fault list [Jin et al.,

2009]. Sifting through millions of lines of code or logic gates is inefficient, and destructively testing ICs is undesirable. In addition, natural variations that arise from the manufacturing process make it difficult to detect extraneous and malicious logic, burying the attack under inherent process noise within the IC. All these factors combine to create challenges very similar to those in current manufacturing systems; where inspection costs, system variability, and quality control/inspection limitations make it difficult to ensure absolute product integrity.

In order to battle these limitations and to develop new detection strategies, a taxonomy describing Trojans and their effects on ICs has been created. Current Trojan taxonomy breaks Trojans down according to three broad categories: payload, activation type (or trigger), and "physical" characteristics [Chakraborty et al., 2009]. The payload of a Trojan is the event or action enacted by the Trojan. Activation type or triggers focus on how the Trojan is activated, whether this is through internal or external means. Physical characteristics include characteristics such as type, size, and structure. This taxonomy allows for a full description of both the intent and characteristics of a Trojan. For additional information regarding this taxonomy, readers are referred to [Wang et al., 2008]. This paper will focus primarily on Trojan payloads and the events triggered by the activation of a Trojan within an IC. Payloads can be classified by three functions: 1) retrieving and/or relaying data back to the attacker, 2) compromising IC functionality, and 3) destroying the IC [Jin et al., 2009]. Given the intent and repercussions of each of these payload categories, Trojans pose a high risk to those producing and using ICs within their systems. Trojans can induce a wide variety of faults within ICs, including reduced functionalities and premature failures.

The creation of different techniques for detecting the presence of a Trojan has been widely explored [Chakraboarty et al., 2009; Tehranipoor et al., 2009]. These detection approaches can be roughly categorized into side-channel, Trojan activation, and architecture-level detection. The methods using Trojan activation and architecture-level for Trojan detection rely heavily on the purely digital aspects of the Trojan, and make use of the idea that Trojans can be activated [Agrawal et al., 2007; Lin et al., 2009] and have inputs and outputs that can be monitored.

Of these methods, side-channel detection approaches provide the strongest link to manufacturing. These approaches rely solely on measuring side-channels, and use external characteristics of the Trojan for detection. Side-channel detection of Trojan uses non-destructive testing of the IC to create a "fingerprint" or characterization of the IC [Agrawal et al., 2007; Lin et al., 2009; Du et al., 2010; Narasimhan et al., 2010]. Side-channels have used timing delays, leakage measurements, and temperature to build IC operational models. Through the careful selection of IC characteristics for model generation, attackers have little information on the side-channel measurements being used. This makes the process of engineering an undetectable Trojan much more difficult [Agrawal et al., 2007]. The ultimate challenge lies in creating a comprehensive model that is not impractical in the number of tests required. If this can be accomplished, side-channel analysis allows for detection of Trojans without having to exhaustively search through all IC logic gates or code, using a more hollistic approach to identifying Trojans.

4 IC Trojan Detection Approaches for Manufacturing

The current research into detecting Trojans within ICs has significant applications in developing strategies for detecting for attacks against cyber-physical manufacturing systems. Natural system variation, limitations in measurement techniques, inspection costs, and other limitations to ensure that a part matches its intended design difficult and costly. For instance, several non-destructive techniques can be used to analyze a manufactured part for alteration, such as; 3D laser scanning, interferometry, etc. However, the cost and time associated with these would be detrimental to a manufacturing environment, especially when considering the need to capture the entire 3D surface. This cost increases when considering internal attacks against 3D printed parts, which would require X-Ray

images or CT scans. In addition, these techniques often require significant training to classify data as healthy or unhealthy.

The aforementioned limitations may be overcome by integrating IC Trojan detection approaches into manufacturing. The similarities between manufacturing cyber-attacks and Trojans are most clearly seen in their respective intentions or payloads, described in Section 3. Compromising a manufactured part can be done by simply adding an additional hole or changing the shape of a part, much like a Trojan can be introduced by simply adding an additional logic gate. This can result in a part performing sub-optimally or performing a different function entirely. For example, if a gas pedal on a car was made longer than specified, it may stick causing uncontrolled acceleration or accidents. Premature or catastrophic failures can also be induced by changing part characteristics, such as altering a part's shape to result in higher stress concentrations or changes in mechanical properties. In addition, alterations to the part design or intentional flaws can be hidden from view, making detection schemes similar to those for hidden Trojans a necessity for manufacturing.

In the IC world, side-channel detection schemes do not attempt to discover the effects a possible Trojan has on a system nor do they test for changes in system functionality. Side-channel approaches operate at a more fundamental level, as they rely on the fact that any change to the system will perturb its intrinsic behavior. Therefore, side-channels in manufacturing should capture intrinsic part behaviors and should not necessarily focus on detecting specific attacks (design alterations) or changes to a part's functionality.

It could be argued that a physical part's intrinsic behavior can be captured by its dynamic properties, which is a unique function of both the part's mass, stiffness, and damping. A cyber-attack that alters a part's design will affect these characteristics; resulting in a different dynamic response. However, testing the dynamic behavior of a physical part, through modal analysis, is extremely time consuming, expensive, and not very robust.

Over the past several decades, the field of structural health monitoring (SHM) has made significant progress in detecting structural degradation. One of the crucial technologies behind the success of SHM is piezoelectric materials [Ciang et al., 2008]. Piezoelectric transducers (PZTs) have been used significantly in SHM due to their ability to quickly and accurately determine a system's dynamic response (impedance) through coupled electrical-mechanical analysis [Liang et al., 1994]. This paper proposes that SHM techniques, specifically PZT augmented impedance based SHM [Peairs et al. 2007], could be applied as a side-channel attack detection approach for manufactured parts. It should be noted that piezoelectric-based SHM has already been successfully applied to manufacturing for the purpose of detecting damage accumulation in assembly fixtures [Rickli and Camelio, 2009]. However, until now there has been little need to apply SHM technology to detecting changes to manufacturing parts. SHM technologies cannot be used to accurately measure specific part features without substantial modeling efforts [Albakri et al., 2014] nor can they be used for diagnosis, both of which are crucial for traditional QC.

For any attack detection strategy to be a realistic solution for manufacturing, it should 1) not substantially interfere with the manufacturing system, 2) not require significant additional processing to be implemented, and 3) be relatively quick. To satisfy these requirements, the SHM attack detection approach proposed in this paper is based upon a removable "antenna" to connect a PZT with a host structure (manufactured part). An example of this concept is provided in the subsequent paragraph.

Consider the GE jet engine bracket [GE, 2013] illustrated in Figure 2a. In order to implement the proposed approach, the bracket would need to be redesigned to accommodate the antenna, as shown in Figure 2b. During the manufacturing process the antenna/PZT assembly is joined to the bracket (Figure 2c). Then the PZT is excited and the resulting impedance signature would be acquired. It is worth noting that impedance based SHM techniques use a very high frequency measurement range (10k*Hz* and up) which allow for the measurements to be taken in micro-seconds and do not pose any risk on the systems integrity (e.g., in many cases this is done during operational conditions). This signature is then analyzed to determine if the part has been altered. The measured signature is

compared against a previously measured part that has no defect (i.e., a baseline measurement). This deviation can be bound by manufacturing and material tolerances providing a measure that would allow the detection of damage or in this case the incipient intrusion and part modification. Finally the antenna/PZT is removed from the bracket and the manufacturing process would continue.

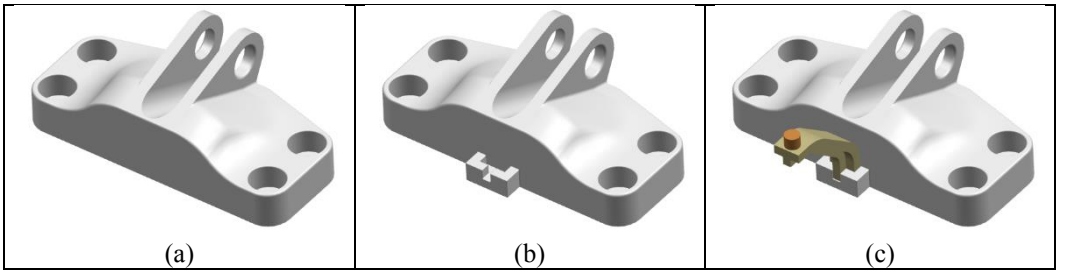

Figure 2: SHM Attack Detection Concept Illustrating a) Original Part to be Manufactured (adapted from GE, 2013), b) Modified Part to Accommodate Testing "Antenna", and c) Testing "Antenna" and Manufactured Part Assembly

For this proposed detection approach to be an acceptable solution for manufacturing, an SHM detection system must exhibit two traits: 1) the system must be robust to inherent system variability and 2) the system must be highly sensitive to non-inherent changes to the physical product. These two requirements can only be achieved by considering the SHM system during the product and process design stages. A manufactured product is typically designed with respect to its form, fit, function, and cost. While a manufacturing process is typically designed with respect to cost, quality, throughput, and safety. As discussed by Ravi et al. (2004), when dealing with embedded computing systems, security considerations should be a mainstream system (hardware/software) design issue rather than an afterthought. Given the current state of cyber-attacks against critical infrastructures, such as manufacturing, it is becoming imperative that security considerations need to be made during the design of these systems.

The proposed SHM detection system allows for a new form of physical security to be instilled into manufacturing during both the product and process design stages. In order to design an optimal (robust to inherent variability and highly sensitive to product alterations) SHM system, the product and process design must simultaneously consider all factors that will affect the system's impedance. These considerations include but are not limited to: 1) part geometries, 2) part materials, 3) boundary condition between the part and the testing station, 4) boundary conditions between the antennae and the part, 5) antennae geometries, 6) boundary conditions between PZT(s) and their respective antennae, and 7) excitation signature(s). If successful, the use of SHM for attack detection would provide a quick and cost effective approach for detecting attacks on manufactured parts.

5 Conclusion

In this paper, we have explored cyber-physical manufacturing systems and their vulnerabilities to cyber-attacks. We have demonstrated the need for new methods for detecting attacks beyond traditional quality control techniques. It is clear that current manufacturing systems can be exploited to allow compromised parts to pass both quality control and visual inspections. Therefore, it is essential to develop new manufacturing specific approaches for detecting cyber-attacks that incorporate the physical nature of the manufacturing systems. In response to this need, this paper adapted the key principles of state-of-the-art approaches for detecting Trojans in integrated circuits to detect physical changes in manufactured parts. More specifically, the approach proposed in this paper incorporates the use of structural health monitoring techniques to detect changes in a part's intrinsic behavior. If successful, the proposed approach has the potential to quickly detect compromised manufactured parts

without significantly disrupting the manufacturing process flow. In addition, the proposed approach brings manufacturing cyber-security considerations to the product/process design stages. This transition is of the utmost importance as cyber-security for manufacturing should not be considered as an after-thought, but as a key consideration throughout the product/process design chain.

6 Acknowledgement

This research was partially supported by NSF grant CMMI-1436365.

References

Albakri, M., and Tarazaga, P.A. Impedance-Based Structural Health Monitoring Incorporating Frequency Shifts for Damage Identification. In: *IMAC XXXII A Conference and Exposition on Structural Dynamics,* 2014.

Albright, D., Brannan, P., and Walrond, C. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? *Institute for Science and International Security* 2010.

Agrawal, D., Baktir, S., Karakoyunlu, D., Rohatgi, P., and Sunar, B. Trojan detection using IC fingerprinting. *In: IEEE Symposium on Security and Privacy*, 2007, pp. 296–310.

Banga, M., Chandrasekar, M., Fang, L., and Hsiao, M. S. Guided test generation for isolation and detection of embedded Trojans in ics. In: *Proceedings of the 18th ACM Great Lakes symposium on VLSI*, 2008, pp. 363–366.

Chakraborty, R.S., Narasimhan, S., and Bhunia, S. Hardware Trojan: Threats and emerging solutions. In: *High Level Design Validation and Test Workshop, 2009 IEEE International*, 2009, pp. 166–171.

Cherry S. and Constantine L. (2011). "Sons of Stuxnet", *IEEE Spectrum*.

Cook, J. (2014). "FBI Director: China Has Hacked Every Big US Company," *Business Insider*. Accessed Oct. 10, 2014 from http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10.

Digital Manufacturing and Design Innovation (DMDI) Institute (2013). "Overview - Digital Manufacturing and Design Innovation (DMDI) Institute." Retrieved from *http://www.manufacturing.gov/docs/dmdi_overview.pdf*.

Du, D., Narasimhan, S., Chakraborty, R.S., and Bhunia, S. Self-referencing: a scalable side channel approach for hardware Trojan detection. In: *Cryptographic Hardware and Embedded Systems, CHES,* 2010, pp. 173–187.

GE (2013). "GE jet engine bracket challenge," *GE*. Accessed on Jan. 5, 2015 from https://grabcad.com/challenges/ge-jet-engine-bracket-challenge

Jin, Y., Kupp, N., and Makris, Y. Experiences in hardware Trojan design and implementation. In: *IEEE International Workshop on Hardware-Oriented Security and Trust*, 2009, pp. 50–57.

Liang, C., Sun, F.P., and Rogers, C.A. Coupled electromechanical analysis of adaptive material systems - Determination of the actuator power-consumption and system energy-transfer. *Journal of Intelligent Material Systems and Structures*, 1994, 5: 12–20.

Lin, L., Kasper, M., Güneysu, T., Paar, C., and Burleson, W. Trojan side-channels: Lightweight hardware Trojans through side-channel engineering. In: *Cryptographic Hardware and Embedded Systems-CHES 2009*, 2009, pp. 382–39.

Narasimhan, S., Du, D., Chakraborty, R.S., Paul, S., Wolff, F., Papachristou, C., Roy, K., and Bhunia, S. Multiple-parameter side-channel analysis: a non-invasive hardware Trojan detection approach. In: *Hardware-Oriented Security and Trust, 2010 IEEE International Symposium*, 2010, pp. 13–18.

National Defense Industrial Association (2014). "Cybersecurity for Advanced Manufacturing." Retrieved from *http://www.ndia.org/Advocacy/LegislativeandFederalIssuesUpdate/Documents/Cyber_for_Manufacturing_White_Paper_5May14.pdf*

Peairs, D., M., Tarazaga, P.A., and Inman, D.J. Frequency Range Selection for Impedance-Based Structural Health Monitoring. *Journal of Vibration and Acoustics*, 2007; 129(6): 701-709.

Ravi, S., Raghunathan, A., Kocher, P., and Hattangady, S. Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems (TECS)*, 2004; 3(3): 461-491.

Rickli, J.L. and Camelio, J.A. Damage detection in assembly fixtures using non-destructive electromechanical impedance sensors and multivariate statistics. *The International Journal of Advanced Manufacturing Technology*, 2009; *42*(9-10): 1005-1015.

Rizzo, J. (2010). "Industry experts: Less 'made in usa' puts security at risk." Retrieved from *http://edition.cnn.com/2010/US/09/21/manufacturing.security/index.html*

Strum, L.D., Williams, C B., Camelio, J., White, J., and Parker, R. Cyber-physical Vulnerabilities in Additive Manufacturing Systems. In: *International Solid Freeform Fabrication Symposium*, 2014, Austin, TX.

Tehranipoor, M. and Koushanfar, F. A survey of hardware Trojan taxonomy and detection. 2009.

Wang, X., Tehranipoor, M., and Plusquellic, J. Detecting malicious inclusions in secure hardware: Challenges and solutions. In: *Hardware-Oriented Security and Trust, 2008 IEEE International Workshop*, 2008, pp. 15–19.

Wells, L.J., Camelio, J.A., Williams, C.B., and White, J. Cyber-Physical Security Challenges in Manufacturing Systems. *Manufacturing Letters*, 2014; 2(2): 74-77.