Procedia Manufacturing

Volume 5, 2016, Pages 1060–1074

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

# Cyber-Physical Vulnerability Assessment in Manufacturing Systems

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

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

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

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

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

**Abstract**

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

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

## 1 Background and Motivation

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

* Corresponding Author

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

doi:10.1016/j.promfg.2016.08.075

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

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

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

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

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

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

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

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

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