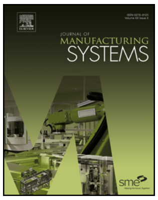
Contents lists available at ScienceDirect

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 xxx

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].