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.