Available online at www.sciencedirect.com

ScienceDirect

Manufacturing Letters 2 (2014) 74–77

www.elsevier.com/locate/mfglet

Research Letters

# Cyber-physical security challenges in manufacturing systems

Lee J. Wells [a], Jaime A. Camelio [a,*], Christopher B. Williams [b], Jules White [c]

[a] Grado Department of Industrial and Systems Engineering, Virginia Tech, United States
[b] Department of Mechanical Engineering, Virginia Tech, United States
[c] Electrical Engineering & Computer Science, Vanderbilt University, United States

Received 22 August 2013; received in revised form 29 January 2014; accepted 29 January 2014
Available online 12 February 2014

**Abstract**

As technology progresses, cyber-physical systems are becoming susceptible to a wider range of attacks. In manufacturing, these attacks pose a significant threat to ensuring products conform to their original design intent and to maintaining the safety of equipment, employees, and consumers. This letter discusses the importance of research and development of cyber-security tools specifically designed for manufacturing. A case study of a cyber-attack on a small-scale manufacturing system is presented to (i) illustrate the ease of implementing attacks, (ii) highlight their drastic effects and (iii) demonstrate the need for educating the current and future manufacturing workforce.

*Keywords:* Cyber security; Manufacturing; Quality control; Cyber attacks

## 1. Background and motivation

Cyber-attacks have drastically increased since their infancy in the early 1980's with operations such as the suspected 'Logic Bomb' that exploded the Trans-Siberian Pipeline [1]. As the number of attacks grows, their visibility decreases and maliciousness increases (Fig. 1). Over the past decades, this has been seen in aerospace [2], control systems [3], financial systems [4], and presidential campaign offices [5]. Attackers have repeatedly shown that no system is off-limits or out-of-reach. In addition, opportunities for attacks are increasing with the Internet of Things (IoT) [6], where the number of networked devices is rapidly expanding across every sector, including manufacturing.

While enhanced manufacturing system connectivity provides significant analytical and supply-chain management capabilities, it also opens the door for attacks against cyber-physical components. An attack can alter design files or process parameters (e.g. tool paths) to bring a part out of specification. In addition, this attack could also modify the quality control (QC) system to avoid proper quality assessment. Such attacks can disrupt the product/system design process and/or adversely affect a product's design intent, performance, or quality. The results of which could delay a product's launch, ruin equipment, increase warranty costs, or reduce customer trust. More importantly, these attacks pose a risk to human safety for operators and consumers.

## 2. Cyber-security weaknesses in manufacturing systems

The first step towards preventing, detecting, and mitigating the effects of cyber-attacks in manufacturing is to understand and overcome the current weaknesses in areas, such as design systems, production control, QC, and manufacturing cyber-security research and education. This section briefly describes these weaknesses. Here a weakness

* Corresponding author. Address: Virginia Tech, 250 Durham Hall, Blacksburg, VA 24061, Unites States. Tel.: +1 540 231 8976; fax: +1 540 231 1831.
*E-mail address:* jcamelio@vt.edu (J.A. Camelio).

http://dx.doi.org/10.1016/j.mfglet.2014.01.005
2213-8463/© 2014 Society of Manufacturing Engineers (SME). Published by Elsevier Ltd. All rights reserved.

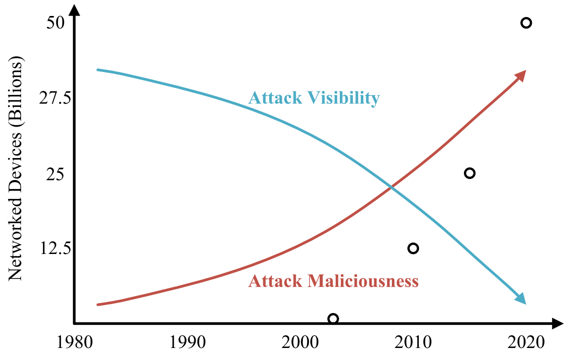

Fig. 1. Growth of Networked Devices [6] and Cyber-Attack Visibility and Maliciousness Trends, Adapted from [7,8].

refers to anything that impedes the development of cyber-security solutions.

### 2.1. Concerns of industry

One of the most important barriers for cyber-security in manufacturing is that industry is more concerned with attacks aimed at intellectual property (IP) theft. This is warranted as computer security has traditionally focused on protecting information [9]. As manufacturing systems have evolved into an IoT that rely on Softwares as a Service and cloud computing; attack opportunities now extend beyond IP theft. As industrial needs often drive research, it is vital that industry becomes aware of cyber-attack threats and the full extent of their consequences.

In addition, CAE software developers often maintain that their products are encrypted and 100% protected, which gives industry a false sense of security. Given enough time and computational resources, all encryptions can be broken. Moreover, a single poor cryptographic decision can put a system at risk, as recently seen with Android mobile devices. However, whether or not a system can be hacked is irrelevant considering that the majority of attacks on cyber-physical systems have come from insiders (e.g. disgruntled employees) [10–14].

### 2.2. Current research efforts

While cyber-security for manufacturing is not novel, current research efforts focus on high-level security issues, such as vulnerabilities in Supervisory Control and Data Acquisition Networks [15–18]. Here manufacturing is grouped with critical infrastructures [19] such as electrical power generation and distribution, water and waste management, and transportation systems. While manufacturing shares similarities with critical infrastructures, they have distinctly different requirements for cyber-security. Manufacturing systems are more than a collection of control systems; they are highly integrated with the product lifecycle. Hence, a manufacturing system can be attacked anywhere from initial design to final inspection, and anywhere in the supply chain. In order to develop efficient security measures for manufacturing requires a manufacturing specific research area within cyber-security.

### 2.3. Quality control

Since cyber-physical systems affect the physical world, they offer an additional avenue for detecting attacks beyond traditional cyber-security [9]. In manufacturing, QC is used to ensure a process' stability by measuring key product/process characteristics. However, current QC approaches are not designed to detect the effects of cyber-attacks. Specifically, QC approaches are based upon assumptions (sustained system shifts, rational sub-grouping, feature-based monitoring, etc.) that are no longer valid under the presence of an attack. In fact, these assumptions can be used against a QC system to create undetectable attacks. Additionally, QC systems can be compromised as they are often integrated into the digital manufacturing network.

Furthermore, the purpose of QC extends past detection and focuses on recovering from process disturbances. Current diagnostic procedures do not consider cyber-attacks as possible root-causes. Therefore, if the effect of an attack is detected; a significant amount of time, effort, and money would be wasted in unsuccessfully determining the cause. In this context, QC approaches need to be fundamentally re-evaluated to ensure protection.

### 2.4. Education

Modern engineering curriculums focus heavily on the development of CAE skills. However, outside of modeling errors (e.g. Finite Element Analysis), these tools are considered and taught as infallible. It is vital that future engineers and designers become exposed to the threats cyber-attacks pose on cyber-physical systems.

Curriculums focused on security for cyber-physical systems have been proposed and implemented [20–22]. However, they focus on control systems and do not consider manufacturing-specific issues, such as compromised CAE software. It is fundamental that manufacturing workforce development has a focus in increasing awareness of potential cyber-attacks, as education is the first step towards defending against attacks.

## 3. Case study

A case study was performed to demonstrate the feasibility of a cyber-attack on a simple manufacturing system and to understand the diagnostic capabilities of engineers who do not anticipate cyber-attacks. This section briefly describes the experiment and resulting observations.

### 3.1. Experiment

In this experiment sophomore-level engineering students, at a large land-grant university, were challenged to