MTConnect Student Challenge: Idea creation

Cyber-Physical Attack Detection using MTConnect Data

Zach DeSmit; Patrick Good

Organization: Virginia Tech

Phone Number: (540)-383-5873

Email Address: zachd1@vt.edu; goodp55@vt.edu

Date of Proposal: 12/15/15

# Abstract

The evolution of manufacturing systems from loose collections of cyber and physical components into true cyber-physical systems has expanded the opportunities for cyber-attacks against manufacturing (Evans, 2011). Attackers aren’t always attempting to create a catastrophic incident, possibly seeking instead to negatively impact part quality within the boundary of traditional quality control limits. This dangerous form of attack can adversely affect a product’s design intent, performance, quality, or perceived quality. The results could be financially devastating to a manufacturer by delaying a product's launch, ruining equipment, increasing warranty costs, or eroding the trust of the customer. The goal of this idea is to leverage machine generated MTConnect Data to detect cyber-attacks from within the very system being targeted while simultaneously revolutionizing the process by which major manufacturers control quality. MTConnect Data will be used to establish a new part feature, known as a signature. A system will be created to monitor relevant components of this signature, providing a digital certification to dimensional quality control systems. In essence, the proposed system supplements current quality control approaches which currently focus only on discrete pre-determined features, an approach easily exploited by cyber-attacks. In doing so, this proposed system has the potential to overcome current cyber-attack vulnerabilities in the deployment and use of quality control tools for manufacturing systems.

# Proposed Idea

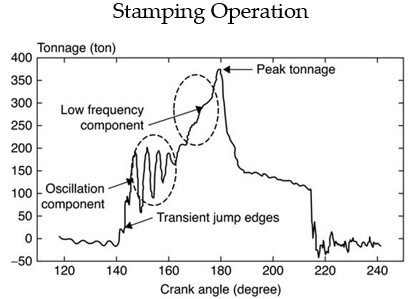
The proposed project consists of a signature based system rooted in the MTConnect protocol that will aid in detecting cyber-attacks targeting physical elements within a manufacturing system. Recently, James Comey, the director of the Federal Bureau of Investigation said, “There are two kinds of big companies in the United States. There are those who have been hacked … and those who don’t know they have been hacked …” (Cook, 2014). Symantec agrees and stated that the manufacturing industry is one of the most targeted, placing the odds of a phishing attack at 1 in 3.0 (Symantec Corporation, 2014). This constant threat is not currently being addressed by manufacturers leaving facilities and entire supply chains increasingly vulnerable to a barrage of cyber-physical attacks.

These attacks, which can be nearly impossible to detect, can negatively impact product quality and even long-term revenue. More importantly, attacks pose a risk to human safety as operators and consumers could be using both faulty equipment and products that deceitfully passed current dimensional quality control checks.

In 2013, as part of Executive Order 13636, President Obama stated that “The cyber threat to critical infrastructure represents one of the most serious national security challenges we must confront.” With its own unique set of cyber-security risks that manifest themselves in the physical world through cyber-physical attacks, manufacturing has been identified as a critical infrastructure sector by the Department of Homeland Security (Obama, 2013). This concept is being created in direct response to that executive order.

Expanding upon current quality control concepts, the proposed approach is intended to fit into manufacturers existing quality controls systems. At this stage the purpose is to generate a concept for detecting when a cyber-attack has occurred on a physical manufacturing system to avoid or significantly reduce its overall effect. Therefore, the assumption will be made that all incidents which alter the physical manifestation of a part from its original design, outside of normal variation, are the result of intentional meddling and not a simple quality incident. The proposed system will ultimately alert a quality engineer to a problem which would have to be diagnosed as a cyber-attack, machine-related quality incident, or human error. The intention is to conduct future research which will supply this quality engineer with a root cause of this defect, whether cyber or otherwise. However, the current goal is to increase awareness that hackers are attacking manufacturing systems, then both catch and derail these attacks from the production system itself.

The proposed MTConnect-based signatures will address cyber-physical security vulnerabilities while leveraging the quality control process known as statistical profile monitoring. Many processes or products can be characterized and summarized by a functional relationship between a response variable and one or more explanatory variables. Profile monitoring can check the stability of this relationship over time by sampling data points to create a profile, which is represented by a curve, and used for the purpose of quality control (Noorossana, Saghaei, & Amiri, 2011). Figure 1below displays this approach showing how required tonnage changes as a function of crank angle in a stamping operation.



*Figure 1. Statistical Profile of Stamping Operation (Woodall, 2008)*

Similar to third party digital certificates issued to secure websites, a manufacturing signature will be issued to secure physical processes within a manufacturing supply chain. The concept of this unique signature is driven by the combination of these statistical profiles. During a stamping operation like the one shown above, this could include tonnage as a function of crank angle, but could also focus on tool positions, total cutting time, feed rates etc. Layering these different profiles may be a difficult concept to visually display as it is the compilation of many very different features of process, but the created system will be simultaneously monitoring all specified machine parameters. Baseline signatures will be generated for different types of products as they undergo different machine processes. A disruption to the machining process of a particular part will be exposed through a deviation from the baseline, potentially exposing an otherwise undetectable cyber-attack on the physical manufacturing system.

This project would be nearly impossible to implement with any scalability if it were not for the process knowledge that can be quickly gained using MTConnect data. The proposed detection system will gather read-only data in real time delivering these machine parameters using extensible markup language (xml). Industry experts have already spent time identifying which elements of traditional manufacturing processes are critical to parts’ integrity when creating the framework meaning a signature should be inclusive to all data contained in the MTConnect Standard. This open source data can be obtained by applying an agent to most traditional manufacturing equipment and the schema structure is specified in the standard. This means a common output design exists for all manufacturers in all industries allowing for a cyber-detection strategy to be easily implemented. After design and manufacturing engineers develop a baseline signature for a part, the system will alert quality personnel to any deviation which we associate with a cyber-physical attack.

# Technical Requirements

Implementing this solution will require establishing and storing generated signatures for each manufacturing process. First, a graphical user interface (GUI) will be created which will compile the read-only MTConnect data into a product signature. A product signature is a cyber-representation of the successful completion of a physical manufacturing process.

The MTConnect protocol collects read-only process data output by the manufacturing equipment. Each variable that the protocol collects will act as a single layer that when combined with the others, creates a unique signature identifying the produced part. In Figure 2 the layer of the process signature detailing power consumption is shown as an example. This part, which utilizes a CNC machining process to precisely cut four holes, is a physical manifestation of the power signature shown. The machine will collect MTConnect data on power consumption over time as well as all other data industry experts have built into the Standard. Combining all these unique features of the process, a very specific process signature is formed. The GUI will track all similarly machined parts and, by comparing to the baseline signature, can be used to alert the quality control engineer to a deviation in the manufacturing process which indicates the part was not produced or machined as designed. This will trigger a thorough investigation and give manufacturers a necessary resource to identify that they are the target of a cyber-physical attack.

|  |  |
| --- | --- |
| Picture2  *Figure 2a. Nominal Part Drawing* | *Figure 2b. Nominal Part Power Consumption Profile* |

*Figure 2. Nominal Part Drawing and Profile*

Figure 3 outlines the use of MTConnect as a certification system to detect cyber-attacks. In this example, the manufactured part seen in Figure 2 has been attacked causing the tool to cut a channel in the work piece instead of four clean holes. Depending on the how this part fits into a larger subassembly, this attack could compromise the final product, the CNC Machine, or the operators. The power consumption graph demonstrates that the identified features (holes) in both the original and attacked parts align perfectly which will allow the part to pass a dimensional quality control test. However, because the attacker has caused the tool to cut a channel instead of returning the tool entirely out of the work piece the process signatures vary significantly. This example, although trivial, highlights the effectiveness of the proposed certification system to detect cyber-attacks on manufacturing processes.

|  |  |
| --- | --- |
| Picture1  *Figure 3a: Attacked Part Drawing* | *Figure 3b: Attacked Part Vs. Nominal part Signature* |

*Figure 3: Attacked Part Drawing and Profile*

Once the signature has been established, the quality control engineer views the signature through the GUI located at an inspection station. Graphs associated with the specific profile, similar to the one shown in Figure 3, will be generated for each process and differences will be calculated. Any layer or compiled product profile which deviates outside set tolerances will be highlighted as a possible attack and a recommendation will be made by the system as to whether the part is compliant or not. The quality control engineer will make the final judgement as to whether the parts can be used and as to whether a cyber-physical attack is occurring.

Due to the expansive nature of manufacturing and production, many manufacturing facilities do not use 100% inspection. This novel approach will aid facilities who do not inspect every part by highlighting work pieces that need to be inspected. By informing the quality control engineer that a part has significantly deviated from the established process signature, the system certifies the manufacturing process thereby securing it from the successful exploitation of cyber-attacks.

# Benefits and Impact

The largest and most obvious benefit to implementing a certification system to dimensional quality control is the security and ability to both accurately and rapidly detect a cyber-attack within a manufacturing facility. However, the benefits extend beyond that of securing a single process. The outlined approach will flow seamlessly into a manufacturer’s preexisting quality control standard while simultaneously increasing the security of the identified process. Since MTConnect data is constructed using a common schema, this approach can quickly move from a pilot facility across a multi-corporation supply chain. In the proposed approach scalability and ease of implementation have been regarded as extremely important as an organization is only as strong as the weakest link in its supply chain.

The proposed idea will provide a significant benefit to the quality control realm. By design, dimensional quality control systems tend not to measure every feature of a manufactured part, leaving the unmeasured features vulnerable to cyber-attacks. Using the signature based approach as a certification system will significantly reduce if not eliminate the number of exploitable vulnerabilities within a manufacturing system. This reduction in vulnerabilities will allow manufacturers to mitigate and secure entire supply chains from the onslaught of cyber-physical attacks they are currently experiencing. By eliminating these vulnerabilities, which as previously stated pose a very significant threat to manufacturing, resources are made available for other more beneficial business decisions.

Due to the open source nature of the MTConnect protocol, the proposed idea has an extremely large potential impact to the current manufacturing industry as no regulations are barring individuals from contributing or participating in the signature based approach. By flowing seamlessly into current quality control practices, this approach becomes simple to implement and use for small manufacturers and large conglomerates alike. The real time availability of read-only data from the MTConnect protocol allows manufactures to immediately detect the perturbation of a part within a process, eliminating the possibility of producing batches of incorrect or out-of-control parts.

Implementing this system using the MTConnect protocol will allow manufacturers to secure facilities from cyber-attacks on both the manufacturing and quality control systems. These attacks can prove devastating to an organization’s revenue, wellbeing, and customer goodwill. It is the responsibility of American manufacturers to protect their employees and consumers from harmful products as well as their stockholders from the financial consequence of a successful cyber-physical attack. This signature approach, if developed and implanted, will protect this segment of critical infrastructure from its newest and fastest growing threat.

# References

Cook, J. (2014, October 6). *FBI Director: China Has Hacked Every Big US Company*. Retrieved 10 19, 2015, from Business Insider: www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10

Evans, D. (2011). *The Internet of Things: How the Next Evolution of the Internet is Changing Everything.* Cisco Internet Business Solutions Group (IBSG).

Noorossana, R., Saghaei, A., & Amiri, A. (2011). *Statistical Analysis of Profile Monitoring.* Hoboken, NJ: John Wiley and Sons Inc.

Obama, B. (2013). *Executive Order 13636: Improving Critical Infrastructure Cybersecurity.* District of Columbia: The White House.

Symantec Corporation. (2014). *Internet Security Threat Report 2014, Volume 19.* Symantec Corporation.

Woodall, W. H. (2008). Profile Monitoring. *Encyclopedia of Statistics in Quality and Reliability, Volume III*.