

Cyber-Attack Detection using MTConnect Data

Zach DeSmit; Patrick Good

Virginia Tech

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.