Detecting and correcting factory faults, cyberattacks in real time

September 7 2016, by Nicole Casal Moore

Varsha Venkatesh, Robotics & Autonomous Vehicles Mechanical Engineering Graduate Student, learns how to program and use an industrial manipulator robot arm. Credit: Joseph Xu, Michigan Engineering

Spotting a glitch on the factory floor in real time—and reconfiguring around it—are the goals of a new $4 million project led by University of

Michigan engineering researchers.

The project, which also involves researchers from the University of Illinois and Cornell University, aims to increase factory productivity and American competitiveness.

Modern advanced manufacturing plants hold hundreds of software and hardware components. Their robots, conveyer belts, sensors, control systems and communication networks have intricately choreographed roles in a sector that yields 12 percent of the nation's GDP.

But machine failures, operators' mistakes and, increasingly, cyberattacks can halt production—leading to expensive unscheduled downtime or potentially dangerous situations. In 2015, for example, hackers breached the control system in a steel mill in Germany and made it impossible for operators to properly shut down a blast furnace. News accounts described the damage as "massive."

The new project—made possible by a grant from the National Science Foundation—will yield "a revolutionary methodology for controlling manufacturing systems," the researchers say. They call the methodology "software-defined control."

Central to the new approach is a continuous, full simulation of the manufacturing plant. The team will produce this simulation and develop software that compares a plant's actual operation to what they'd expect based on the simulation.

"The idea is you have the physical manufacturing plant and the simulated model of the plant so if there's a difference between the two, you can detect a fault or a cyber-intrusion," said project principal investigator Dawn Tilbury, associate dean for research and professor of mechanical engineering at the U-M College of Engineering. "The goal is to develop

control systems for manufacturing systems that are secure and reconfigurable automatically."

Such systems could reprogram how parts flow through the plant to avoid a faulty piece of equipment.

"Our work aims to develop the science and enabling technologies to transform manufacturing systems from the current paradigm of low efficiency and high susceptibility to system disruptions to a new era of system-level anomaly detection, classification and action," said Kira Barton, U-M assistant professor of mechanical engineering. "This will lead to less downtime, faster responses to disruptions and a more efficient manufacturing system."

Indeed, the rise of automation calls for a better way to keep tabs on plant operation, Tilbury said.

Students learn how to program and use an industrial manipulator. Credit: Joseph Xu, Michigan Engineering

"Automation may increase efficiency and raise quality, but it brings with it vulnerabilities," she said.

Robots are networked, and the companies that produced them can often log in remotely to make repairs. These are legitimate endeavors, but they can also be weak links in the cybersecurity of the system.

As manufacturing systems become more complex and digitally connected, they become increasingly susceptible to disruptions that can cause significant financial losses.

The U.S. Department of Homeland Security investigated 97 cyberattacks at critical manufacturers during the fiscal year ending in June 2015, according to a report by its Industrial Control Systems Cybersecurity Emergency Response Team.

Cyberattacks to manufacturing plants are a relatively new phenomenon. The FY 2015 number that federal officials examined was double the previous year. A more clear and present risk—and this one to the nation's economy—is that of unscheduled factory downtime. It's one of the most prevalent causes of inefficiency in manufacturing, the researchers say. When a cyberattack or a broken machine stops a factory in its tracks, the cost can run tens of thousands of dollars a minute.

"Manufacturing systems produce the vast majority of products in the modern world—automobiles, computers, textiles and toys, to name just a few," said Sibin Mohan, U of I research assistant professor of computer science. 'Improvements in the design and operation of manufacturing systems will have a huge financial and social impact on companies and consumers, and that's crucial to economic competitiveness."

While the project focuses on discrete part manufacturing, the researchers say it translates well to semiconductor manufacturing and batch processes.

"The work will combine techniques from multiple disciplines, spanning control theory, modeling of physical properties, machine learning, and cybersecurity, to detect and deter such attacks. The collaboration will be exciting as well as challenging," said Elaine Shi, associate professor of computer science at Cornell.

This grant is one of three announced today through NSF's Frontier program, which aims to advance the state of the art in cyber-physical systems.

"NSF has been a leader in supporting research in cyber-physical systems, which has enabled and accelerated multidisciplinary research in a number of application domains," said Jim Kurose, NSF's head of computer and information science and engineering directorate. "We look forward to the results of this new award, which expands our Frontier projects portfolio into the area of cyber-manufacturing."

Provided by University of Michigan

Citation: Detecting and correcting factory faults, cyberattacks in real time (2016, September 7) retrieved 22 May 2024 from https://phys.org/news/2016-09-factory-faults-cyberattacks-real.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.