NEWS RELEASE

Contacts

Jerry Poling, Marketing Communications, 715-232-2384

Marketing Communications 715-232-2381

News Center

Smart manufacturing pilot project receives $149,000 Dept. of Defense grant

Initiative aimed at helping regional companies develop secure, high-tech manufacturing systems

Story Link

Photos attached

FOR IMMEDIATE RELEASE
Dec. 3, 2020

Menomonie, Wis. — Smart manufacturing, a key to the future of manufacturing, is moving to the head of the class in west-central Wisconsin thanks to a federal grant awarded to University of Wisconsin-Stout.

The university, a Center of Academic Excellence for Cyber Defense, has received a $149,000 cybersecurity grant from the U.S. Department of Defense and National Security Agency for a proposal to develop a smart and secure manufacturing pilot project.

Smart manufacturing integrates computer technology into the production process and products. It builds on the industrial internet of things — IIoT — using cloud computing, network segmentation, secure authentication, 5G technology for broadband networks, industrial robots, big data analysis, artificial intelligence and more.

“A lot of small and medium-size manufacturing firms are facing challenges of understanding the benefits of smart manufacturing and developing a smart manufacturing roadmap,” said Professor Holly Yuan. “Our test bed will give them the means to experiment, validate and explore the benefits and challenges of smart manufacturing solutions for their business uses.”

The test bed, a testing lab, is expected to begin operating in May 2021.

Smart manufacturing systems can respond in real time to market demand. Cybersecurity risks and vulnerability to hacking, however, are heightened with smart manufacturing, Yuan said. A secure system includes software upgrades and security patches and isolates rogue devices.

“Attackers may use the same skill sets in the field of information security and extend it to the IoT devices, industrial control systems and automated production processes,” Yuan said.

In a recent test, for example, a security research firm hacked into a smart light bulb and took control of the device in less than an hour.

Common products already using smart manufacturing, which is expected to grow by 19% the next seven years, include electric vehicles with internal and external software support systems; and home appliances and security systems that use IoT to communicate with other devices, such as cell phones.

Collaborative effort to benefit regional manufacturers

Taking part in the pilot project could help regional manufacturers incorporate:

- Machine automation, using robotics and automated guide vehicles to reduce dependence on labor
- Machine monitoring and maintenance, using sensors to collect data in real time to predict maintenance and increase productivity
- Factory environmental monitoring, using dust, temperature and motion sensors
- Inventory and asset tracking, using smart devices to trace production efficiency and inventory levels.

Yuan is director of the university’s cyber defense center, designated in 2017 by the Department of Defense. The designation, the first in the UW System, helps higher education institutions with computer-related programs prepare the U.S. against cybersecurity threats.

The center will work with the university’s Manufacturing Outreach Center, the computer and electrical engineering undergraduate program and other academic programs.

Larry Blackledge, director of the Manufacturing Outreach Center, said small and midsize manufacturers often overlook cybersecurity. “It is not well understood and is sometimes seen as a distraction from just getting the work done. With this test bed we will be able to demonstrate to manufacturers the need and implementable solutions for cybersecurity issues,” he said.

“Just raising awareness will be a big step forward. This project helps to provide prepared, experienced, graduates who will be able to properly design solutions for the companies they work for throughout their careers,” Blackledge added.

The Manufacturing Outreach Center specializes in helping small manufacturers improve their operations. It is part of UW-Stout’s Discovery Center, the university’s primary outreach and engagement organization.

Wei Shi, director of the computer and electrical engineering program, is excited that students can be involved in the multidisciplinary project. "Our students will apply what they learn in class to design and implement a secure, smart manufacturing test bed. With undergraduate students involved in the project, we also hope to integrate faculty-student applied research

into teaching with up-to-date technologies and applications in the classroom," said Shi, an associate professor.

UW-Stout has a program in computer networking and information technology along with many scientific, technical and managerial disciplines related to cybersecurity. Students at Center of Academic Excellence institutions like UW-Stout can receive a national cybersecurity certification by taking 13 required courses as part of their undergraduate degree program.

Additional grant for scholarship

Along with the $149,000 grant, UW-Stout received a $55,000 federal grant for a student scholarship. The award will cover a student's tuition and fees for a year; provide a $25,000 stipend; and pay for expenses to attend a national cybersecurity conference.

In 2018, UW-Stout received two other Department of Defense grants, $200,000 for a cybersecurity symposium held in April 2019 and $105,000 for three student scholarships.

UW-Stout is Wisconsin's Polytechnic University, with a focus on applied learning, collaboration with business and industry, and career outcomes.

###

Photos

Professor Holly Yuan, director of UW-Stout's Center of Academic Excellence for Cyber Defense

Larry Blackledge, UW-Stout Manufacturing Outreach Center director

Wei Shi, director of UW-Stout's computer and electrical engineering program