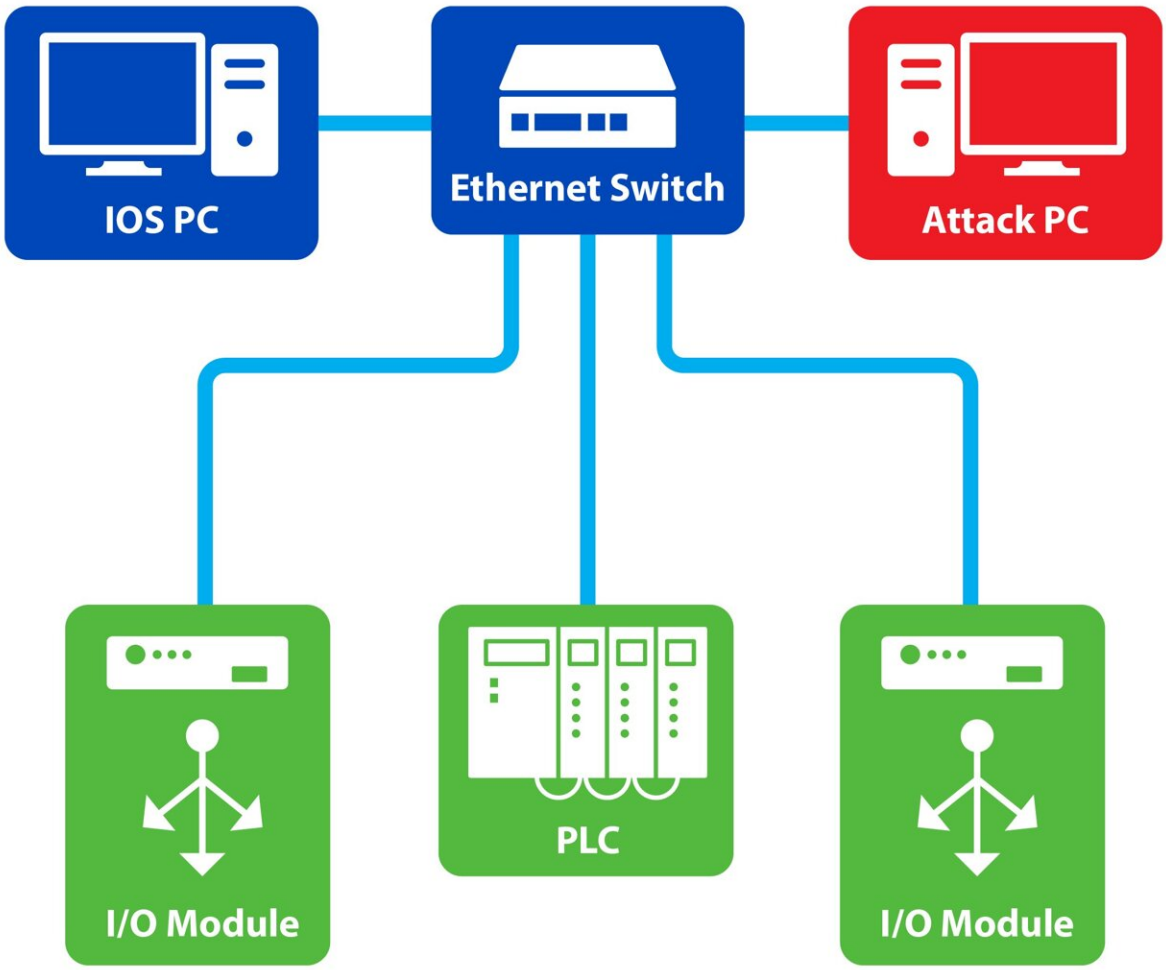
A cyber security intrusion detection system for industrial control systems

May 2 2022



SwRI designed an industrial network to detect cyberattacks from a malicious computer. The network utilized the Modbus/TCP protocol to transfer data packets between input/output (I/O) devices and programmable logic controllers (PLCs) connected via an Ethernet switch. Credit: Southwest Research Institute

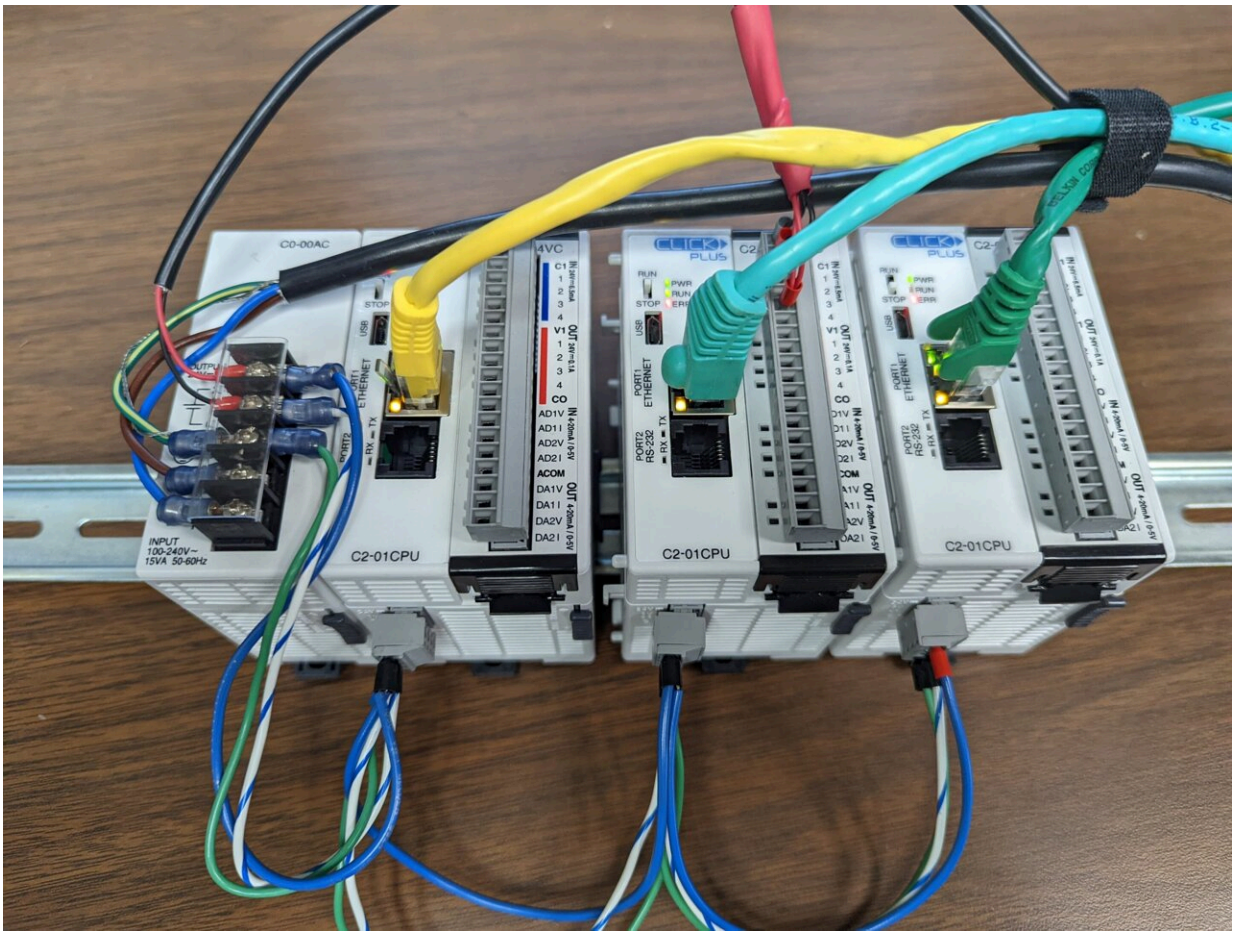
Southwest Research Institute has developed technology to help government and industry detect cyber threats to industrial networks used in critical infrastructure and manufacturing systems. SwRI funded the research to address emerging cyber threats in the rapidly evolving ecosystem for industrial automation.

The team used algorithms to scan for cyber threats across network protocols that transmit industrial control data for everything from natural gas pipelines to manufacturing robots. The research led to development of an intrusion detection system (IDS) for industrial control systems (ICS).

"Historically, industrial control systems were not designed with security in mind," said Ian R. Meinzen, an SwRI intelligent machines engineer who worked on the project. "They had the benefit of an 'air gap' where they could operate securely without a connection to IT networks."

Unplugging industrial networks from information technology (IT) networks, however, is no longer an option for modern automation systems that rely on the internet of things (IoT) to transmit vast amounts of data. IoT describes the network of physical objects embedded with sensors and software to connect and exchange data with other devices and systems via communications networks over the internet.

"Connecting IoT devices and other hardware exposes industrial networks to security vulnerabilities," said Peter Moldenhauer, an SwRI computer scientist specializing in cybersecurity. "Attacks can occur through an IoT device or even network protocols and outdated software."



SwRI used programmable logic controllers (PLCs) connected to input/output (I/O) modules to a test network. Algorithms scanned the network for cyberattacks through data packets transferred over the Modbus/TCP protocol. Credit: Southwest Research Institute

The SwRI team focused this research on scanning for cyberattacks over the Modbus/TCP protocol. Utilities and industry have used this Ethernet-based networking protocol for decades in supervisory controls and data acquisition (SCADA) systems equipment.

SwRI researchers originally developed the algorithms to scan Controller Area Network (CAN) bus networks used in automotive hardware. They

customized cybersecurity algorithms to scan a simulated network equipped with industrial devices before evaluating the new algorithms on a real-world industrial network. The test system used the Modbus/TCP protocol to send data packets over a network. The network featured an Ethernet switch that connected personal computers, programmable logic controllers (PLCs) and input/out (I/O) modules. Such industrial computing devices send commands and record data for automated robots and mechanized equipment.

"We had to customize the previous algorithms to recognize the different ways the Modbus/TCP protocol grouped data packets in sequences and time signatures," said Jonathan Esquivel, an SwRI computer scientist.

The newly developed algorithms applied to the test network recognized normal Modbus/TCP traffic and identified cyberattack vectors such as out-of-band timing, address probing and data fuzzing/manipulation. The algorithms classify data packets as "regular" if they come from an uncompromised industrial control device or "attack" if the source is an unexpected or compromised device.

The research team featured experts from SwRI's Critical Systems Department, which specializes in embedded systems and cyber security, and the Institute's Manufacturing Technologies Department, which specializes in software and hardware integration for robotics and industrial automation.

"Business trends and new technology—driven in part by a pandemic push toward automation—are revealing more cyber vulnerabilities across industrial systems," said Dr. Steven Dellenback, vice president of SwRI's Intelligent Systems Division. "We are proud to support government and industry with multidisciplinary expertise in cybersecurity and automation technologies."

Provided by Southwest Research Institute