INTRO TO HOUSTON'S OT CYBER FUSION CENTER

VIDEO TRANSCRIPT

Control system cyber incidents are a real threat – with potentially devastating results. A strong Operational Technology Security posture can reduce the impact, but how do you realize the right solution for your organization?

Our Operational Technology Cyber Fusion Center is a risk-free environment in which to innovate, stage, and test the security solutions that protect industrial control systems and assets from cyber-attacks. It features fully functioning field controllers and security tools, already configured and deployed with Accenture's leading practices.

Our control system mimics real-world operations by manipulating the flow of water between several tanks. We interact with the control system using a touch screen called a Human Machine Interface, or HMI. The Programmable Logic Controller, or PLC, turns on pumps and opens valves.

The HMI and PLC communicate over the networks, except the messages they use are almost always unsecured.

When everything works correctly, we control the flow of water from tank to tank.

But what happens when this system is attacked?

Since network security was never a consideration during the design of these control systems, an attacker with little training and few resources can add malicious messages to the network—confusing the HMI and shutting down its connection to the PLC.

Making matters worse, control systems are rarely updated, and vulnerabilities published years ago still work on systems in use today.

Once the attack is run we are no longer able to interact with our control system.

So, what can we do differently?

To find out more on how we can detect and respond to attacks like this, contact us.