Sandalwood
Engineering & Ergonomics
Work Smarter. Work Safer.

The Challenge of Industrial Control System (ICS) Security and Industry 4.0

IIoT enables unprecedented levels of real-time connectivity, dramatically increasing cybersecurity risks on the plant floor. ICS networks have different operational requirements that impact the ability to adapt and respond to new threats – and open new paths for cyber-attacks.

As ICS stakeholders connect operational technology (OT) to enterprise information technology (IT) systems to improve operational efficiency, they should be aware that their vulnerability will increase as they raise their level of digitalization. How Secure Are Your Industrial Control Systems?

- Do you know what devices you have in your ICS environment?
- Are you protected from the threat of removable media?
- Do you know what kind of network traffic and communication is coming across your private networks?
- Do you have a plan in place to protect your plant floor from malware attacks?
- Do you know what devices in your facilities present the most risk if affected by a cyber-attack?
- Do you have a process in place to ensure your critical systems are patched appropriately?

Where We Can Help!

Sandalwood clearly understands that cybersecurity priorities regarding factory floor systems differ from corporate. With our experience in setting up and implementing measures to thwart attempts to infiltrate ICS networks and equipment, we can help you secure your manufacturing environment from these threats.

Sandalwood is an engineering and ergonomics consulting firm. Since our founding in 1989, Sandalwood has successfully engaged in over 3,000 projects helping execute strategic solutions for our clients. By providing their knowledge, research, technology, and resources, Sandalwood supports its clients from the executive level to the factory floor so you can…

Work Smarter. Work Safer.

Sandalwood Engineering & Ergonomics 19500 Victor Pkwy, Livonia, MI 48152 www.sandalwood.com

P: (248)848-9500, F: (248)893-0266