Deloitte.

If it isn't Secure, it isn't Safe. ®

Securing Operational Technology (OT)

OT Safety and Security

Cybersecurity is not just an Information Technology (IT) issue. Manufacturers, power and utility operators, energy companies, transportation and shipping operators, chemical companies, pipeline operators, and other critical infrastructure asset owners are frequent targets of cybersecurity attacks on their IT and OT systems.

Why is OT cybersecurity important?
Industrial control systems (ICS) have evolved from isolated, stand-alone, proprietary systems to highly integrated, open systems that integrate with and rely upon IT and OT. These technological advances have helped industrial manufacturing companies improve efficiency, productivity and meet the demands of doing more with less. Unfortunately, the technology and connectivity that enabled these advances has introduced cybersecurity vulnerabilities found in the general computing environment while exposing OT systems that were not designed to be secure.

What's particularly troubling about this is are the significant consequences that could result from an ICS compromise, including downtime, loss of production, health, safety, and environmental impacts. Does this mean that industry should revert to closed, isolated control systems? No, of course not. It means that, as we have done in the field of process and machine safety engineering, we need to evaluate consequences, understand the risks, and implement layers of protection to manage that risk.

The diverse technology, scale, and age of OT systems can be a challenge for companies when implementing an effective cybersecurity strategy. There is no one approach that will meet the operational requirements, business needs, and risk tolerance for every company. These complex environments have come under increased scrutiny from regulators and insurers who recognize the urgency of protecting them from cyber-attacks.

Value Drivers

- **Availability:** Secure OT systems are more resilient to both intentional and unintentional security incidents.
- **Integrity:** Secure OT systems are less likely to be corrupted or be vulnerable to data exfiltration.
- **Safety:** Securing OT systems and networks and following best practices reduces the likelihood of safety incidents.
- **Regulatory compliance:** Ensure OT systems comply with local, national, or industry specific regulations.

The relationship between industrial cybersecurity and safety

At Deloitte, we recognize the strong connection between industrial cybersecurity and functional safety. Functional safety systems enable safe shutdown of processes that have exceeded their normal operating limits. Cyber-attacks may compromise functional safety systems resulting in serious process or machine safety incidents. In today's world of open, integrated control systems you cannot achieve functional safety without addressing cybersecurity. We utilize our experience in both fields to help some of the world's leading companies integrate their industrial cybersecurity and safety programs.

How can we help?

We believe the solution to achieving and maintaining industrial cybersecurity, much like functional safety, involves adopting an engineering-driven lifecycle approach. Our goal is to help you in making sure that cybersecurity is properly engineered into your new or existing control systems and can be properly maintained. As such, we offer services throughout the phases of the industrial cybersecurity lifecycle.

Deloitte OT security services

- **OT security program design, development, implementation:** Design, develop and implement security programs that enable organizations to manage cyber risk associated with OT.
- **OT security assessments:** Assess the enterprise-level framework and associated processes that organizations use to secure their OT environments. This approach can follow a standards-based gap assessment methodology or a more technically based Cyber process hazards analysis (PHA) consequence-based assessment methodology.
- **Vulnerability rationalization:** Conduct an OT consequence-based vulnerability rationalization study, based on Cyber PHA and alarm rationalization methodologies, focused on defining when to treat, tolerate, terminate, or transfer vulnerabilities.
- **OT security design and implementation:** OT security design and implementation services for network design, system integration, and system hardening to improve the reliability and/or security of the OT environment.
- **Regulatory/certification readiness:** Conduct an OT assessment to evaluate against a selected industry standard or regulation with the goal to prepare for a regulatory review, attestation, or certification.
- **Security tool evaluation:** Assist in the generation of evaluation criteria, selection of vendors, technical evaluations, and recommendations for OT security tools.
- **OT detection tool architecture, deployment, and configuration:** Architecture design, development, and implementation for OT detection tooling to assist in the management and operation of an OT security and privacy program, including capabilities for security risk management and associated processes (e.g., asset inventorying, vulnerability monitoring, anomaly detection, vulnerability, and incident management).
- **Training:** Develop and conduct OT specific cybersecurity training courses (e.g., ISA IC32, Top 20 ICS practices, Maritime FSO) ranging from general awareness to customized technical training.
- **Operate/managed services:** Conduct outsourced managed services for OT security both in program-level governance through technical day-to-day operations.

Contact us:

For more information, please contact our OT security practice leadership below or visit www.deloitte.com

Wendy Frank
Cyber IoT Leader
Principal
Cyber Risk Services
Deloitte & Touche LLP
wfrank@deloitte.com

Ramsey Hajj
Principal
Cyber Risk Services
Deloitte & Touche LLP
rhajj@deloitte.com

Russell Jones
Partner
Cyber Risk Services
Deloitte & Touche LLP
rujones@deloitte.com

John Cusimano
Managing Director
Cyber Risk Services
Deloitte & Touche LLP
jcusimano@deloitte.com