Your Operational Technology. Protected.

Ensuring your policies and procedures meet regulatory requirements.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

THE CHALLENGE OF OPERATIONAL TECHNOLOGY (OT) AND INDUSTRIAL CYBERSECURITY

As your organisation embraces new connected systems, equipment and facilities it is vital that cybersecurity related policies, processes and procedures are created or refrehed to reflect emerging threats and risks that such systems can introduce. Applying default IT policies, processes and procedures to an industrial technology environment can lead to under provision in important areas, failure to address key risks and a reduced ability to respond to an incident.

For example:

- Are mobile devices such as smartphones used in your plant? Could a user take photographs of your plant or control room? Are control systems accessible from smartphones?
- Are accounts shared between users impacting your ability to track who has been accessing which systems?
- What is the impact of new data protection regulations on your operational environment?

HOW ARE YOUR POLICIES AND PROCEDURES ASSESSED?

We will engage with you to help you understand how your existing policies, processes and procedures address OT cybersecurity issues in your business. These will be compared against best practices developed at TÜV Rheinland as well as appropriate industry standards. This is a collaborative process enabling you to gain proactive insight from our team of industrial security experts.

The team is then able to work with you to update your OT cybersecurity policies, processes and procedures to ensure they are suitable for your business going forward and help you meet regulatory and customer requirements.

WHY ASSESS YOUR POLICIES, PROCESSES AND PROCEDURES?

- There has been an incident or event that has challenged an existing policy, process or procedure.
- Audits or reviews have identified issues and you need help in implementing new policies.
- Systems have been breached but those responsible cannot be held to account as there is no suitable policy in place.
- You are concerned how upcoming industrial security regulations may impact plant operations or personal information.

WORKING WITH TÜV RHEINLAND

The TÜV Rheinland 145+ year heritage gives us a deep understanding of the markets we serve, with unmatched depth of experience solving complex safety, security, data privacy, and infrastructure challenges.

INDUSTRIAL SECURITY RISK ASSESSMENTS Do you understand your operational technology and industrial security risk?	**OT ARCHITECTURE REVIEW** Is your industrial technology design and architecture secure and compliant with cybersecurity standards and regulations?	**OT SYSTEMS PENETRATION TESTING** Do you need to undertake operational technology vulnerability assessments and penetration tests?	**OT SERVICES FOR THE NUCLEAR INDUSTRY** Do you understand your nuclear facility operational technology and industrial security risk?
OT POLICY, PROCESS AND PROCEDURE REVIEW Are your policies, processes and procedures keeping up with the unique cybersecurity and regulatory requirements of industrial and operational technology systems?	**OT SYSTEMS INCIDENT RESPONSE AND RECOVERY** Do you have existing operational technology incident response and recovery plans in place?	**OT SYSTEMS SECURITY MONITORING** Do you know what is happening on your OT network and systems?	**OT SERVICES FOR THE RAIL AND TRANSIT INDUSTRY** Do you understand your overall rail and transit systems operational technology and industrial security risk?

Overview industrial security service portfolio

TÜV Rheinland
Digital Transformation & Cybersecurity
otsecurity@tuv.com

www.tuv.com/en/industrial-sec

TÜVRheinland®
Precisely Right.