Your Operational Technology. Protected.

Ensuring your operational technology addresses cybersecurity regulations and best practices.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

INDUSTRIAL AND OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY OVERVIEW

The number of cybersecurity related incidents in industrial security and industrial control networks has risen in every region in recent years, and there have been well publicized reports of sophisticated malware and threat actors disrupting safety critical industrial operations.
This has raised concerns about cybersecurity vulnerabilities across all types of industries.

The trend to digitization and system inter-connectivity means that operational technology engineering and operating personnel may not realize the full extent of cybersecurity vulnerabilities they face and are thus inadequately prepared to deal with potential attacks.

No longer can industrial systems rely on an 'air gap' to provide security as it has been demonstrated time and again that such measures can be overcome easily. More conventional IT security risk models fail to understand the specialized nature of operational technology and industrial control systems as they can be markedly different to those used in an office or commercial environment.

Embracing modern digital industrial systems means embracing the challenge of both safety and cybersecurity risks. You can no longer have a safe plant if it is not secure.

WHY IMPROVE YOUR CYBERSECURITY POSTURE FOR INDUSTRIAL AND OT SYSTEMS?

- There is a regulatory or legal requirement to understand and manage cybersecurity risk as you operate in a safety critical or hazardous industry.
- Government agencies are concerned how cybersecurity issues can impact your part in a critical national infrastructure.
- Customers are demanding that their intellectual property and process information is protected on your industrial network.

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.

We have a comprehensive portfolio of consulting, testing, system integration services and certification services which are aligned to NIST CSF, IEC 62443 and other leading international standards to accelerate your cybersecurity program.

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.