Your Operational Technology. Protected.

Cybersecurity Risk Management in Nuclear Facilities.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

CYBERSECURITY RISK IN THE NUCLEAR INDUSTRY

The number of cybersecurity related incidents in industrial security and control networks in nuclear facilities has risen across every region in recent years, and there have been well publicized reports of sophisticated malware disrupting nuclear operations. This has raised concerns about cybersecurity vulnerabilities of nuclear facilities amongst operators and regulators.

Cybersecurity risk is growing as nuclear facilities become increasingly reliant on digital systems and make use of commercial IT and OT systems. These offer cost savings and quick deployment but may in turn increase the overall cybersecurity risk to the plant.

The world of safety and cybersecurity are now inextricably linked in any nuclear facility with control systems. A nuclear facility that meets a particular functional safety design requirement could be compromised by a cyberattack, impacting its safety integrity level. Embracing modern digital operational systems means embracing the challenge of both safety and cybersecurity risks.

HOW ARE CYBERSECURITY RISKS ASSESSED?

Our experts will engage with you in an effective way to whelp you understand how mature your industrial security posture is.
An assessment can be undertaken in a relatively short period of time to give quick feedback to the business so that any remedial steps can be started as soon as possible. TÜV Rheinland take a collaborative workshop approach enabling findings to be discussed in a friendly, informed way with internal teams to maximize the learning opportunity and ensure that key parts of the business and operations are engaged in the process.

WHY ASSESS YOUR NUCLEAR FACILITY AND INDUSTRIAL CYBERSECURITY RISK?

- There is a regulatory or legal requirement to understand this risk as you operate in a safety critical or hazardous industry.
- Government agencies and business executives are concerned how cybersecurity issues can impact their facility.

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.