



Your Operational Technology. Protected.

Ensuring your operational technology addresses cybersecurity regulations and best practices.

www.tuvopensky.com

 **OPENSky**
A TÜV Rheinland Company

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 TUV RHEINLAND OPENSKY

TUV Rheinland OpenSky offers an integrated portfolio of security solutions and services for connected devices, platforms and IoT. We provide advisory, consulting, systems integration, testing, certification and managed security services for connected platforms in three core disciplines: Advanced Cyber Defense; Mastering Risk and Compliance and Secure Cloud Enablement.

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

[Overview industrial security service portfolio](#)

TUV Rheinland OpenSky
Digital Transformation & Cybersecurity
info@tuvopensky.com

www.tuvopensky.com

