



Your Operational Technology. Protected.

Cybersecurity Risk Management in Rail and Transit Systems.

www.tuv.com/informationsecurity

 **TÜVRheinland**[®]
Precisely Right.

CYBERSECURITY RISK IN RAIL AND TRANSIT SYSTEMS

The number of cybersecurity related incidents in OT and control networks in rail and transit systems has risen across every region in recent years, and there have been well publicized reports of lines being halted and passenger sensitive information being stolen as a result of cyberattacks. This is impacting profitability as well as the ability of operators to comply with growing cybersecurity compliance requirements.

As digital transformations across rail and transit systems gather momentum associated cybersecurity risks increase as more equipment and systems on the digital railway are interconnected. Conventional IT security risk models often fail to understand the specialized nature of the digital railway as they can be markedly different to those used in an office or commercial environment. This could also impact rail safety. A transit system that meets a particular safety design requirement could be compromised by a cyber-attack. Embracing digital and modern transit 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 help you understand how mature your digital rail cybersecurity posture is. Engagements are adaptable using appropri-

ate industry standards depending on what is best for your situation. 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. We 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 CYBERSECURITY RISKS?

- There is a regulatory or legal requirement to understand this risk as you operate in a safety critical or hazardous industry.
- Business executives are concerned how cybersecurity issues can impact their business.
- Investors and shareholders need reassuring that systems are robust and capable of managing likely cybersecurity issues and that new investments will be protected.

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.

<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](#)

TÜV Rheinland
 ICT & Business Solutions
 otsecurity@tuv.com

www.tuv.com/en/industrial-sec

