Your Operational Technology. Protected.
Cybersecurity Risk Management in OT.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

INDUSTRY 4.0 AND OPERATIONAL TECHNOLOGY RISK

Digital transformation across the industrial and OT sector represents a huge opportunity to better serve customers, fuel business growth and enhance operational efficiency; but it comes with a health warning. Current business models and existing technology platforms that support them aren't always designed for this increasingly digital world. The number of incidents in OT networks has risen across every sector in recent years. This is complicated by the need to consider the often disparate worlds of functional safety and cybersecurity when assessing industrial systems. No longer can a process or a piece of hardware be considered completely "safe" if it operates in an always-on, connected environment.

FUNCTIONAL SAFETY AND CYBERSECURITY

The worlds of functional safety and cybersecurity are now inextricably linked in modern plant and process control systems. Functional safety is the defense against random and systematic technical failure for the protection of life and environment. Cybersecurity, on the other hand, is the defense against negligent and willful actions protecting devices and facilities. A plant that is safe from technical failure due to its rigorous functional safety design and implementation may still be compromised by a cyber-attack. Embracing Industry 4.0 means embracing the challenge of both safety and cybersecurity risks.

A COLLABORATION WITH TÜV RHEINLAND.

TÜV Rheinland is a global independent specialist in operational technology cybersecurity consulting & solutions and combines its experience in functional safety and cybersecurity with its industrial expertise gained over the past 140 years.

BY WORKING WITH US YOU WILL:

- Have global access to leading experts across both OT cybersecurity and functional safety.
- Be connected to excellent technical expertise backed up by comprehensive industry know-how.
- Engage with cost effective services that provide a proportionate response to your risks.
- Have access to strategic guidance, proven processes and best-in-class technology to effectively manage risk, protect critical assets and thrive in the digital era.

TÜV RHEINLAND AND OT CYBERSECURITY

Your experienced Partner with expert capability and industry credentials:

Domains	Sectors	OT Capability Lens	Lifecycle
ICS	Traffic & Rail	Security Visibility & Response	Risk Assessment
DCS	Industrial	Security Control: Network Security	Cybersecurity Testing
SCADA	Energy & Env.	Security Control: Identity & Access	Consulting
Ctrl. Networks		Security Control: Endpoint Security	Managed Services
Industrial IoT		Governance: Risk Management Platform	
		Data Protection & Privacy	

UNDERSTANDING YOUR OT CYBERSECURITY RISK

A starting point for many organisations on their OT Cybersecurity journey is to understand their associated cybersecurity risks. TÜV Rheinland is able to offer a flexible, cost effective risk assessment for manufacturers, systems integrators and operators. This provides:

- An independent, vendor neutral perspective informed by broad industry experience from enterprise level corporations.
- A clear understanding of the current maturity of your OT cybersecurity program and prioritization of remediation recommendations.
- A management structure for your OT cyber business risk within your budget and with an actionable plan.
- A concise executive level summary that will help senior management and the board of directors understand current risks and prioritize investments – from an objective and independent perspective.

TÜV Rheinland
ICT Business Solutions
otsecurity@tuv.com

www.tuv.com/en/ot-security

TÜVRheinland®
Precisely Right.