Choose certainty.
Add value.

Risk Analysis

Protect your Industrial Operations and Critical Infrastructures from IT Threats.

Your challenges

As industrial IT security is a new and evolving field, the risks for manufacturers, operators and system integrators are still emerging. Existing security measures and solutions from the office IT space cannot simply be adopted without changes. Industrial IT security must support the organisation's safety requirements. At the same time, security measures must address performance requirements without disrupting safety functions. With the increasing digital dependence of many organisations, web-based malware will continue to be the most prominent vector of attack. The wide range of consumer-owned smartphones and tablets connecting to corporate networks also poses significant challenges for industrial IT security.

What is industrial IT security risk analysis?

To account for the many threats to industrial and critical infrastructure IT environments, TÜV SÜD's risk analysis combines a generic methodology with different industry-specific threat scenarios, damage classes and probabilities of occurrence. This helps to identify customer-specific risks for the industrial environment/ production plant and results in an action plan with steps to reduce risks. Our experts make use of tools such as threat catalogues, assessment methodology for vulnerabilities, and differences for safety and operations control. The analysis can follow a customer-defined methodology upon request.

Why is risk analysis important for your business?

Our risk analysis provides a detailed overview of the risks to production in the form of a risk matrix. This enables you to evaluate risks, communicate them to management, define appropriate protective measures and know the residual risk. With risk analysis, you can protect against downtime, production losses, product piracy and financial damage caused by attacks and industrial espionage. The solution also examines devices, equipment and systems for unpredictable risks.

FOUR STEPS FOR BETTER INDUSTRIAL IT SECURITY

Determine the goal, scale and definition of the object of investigation and collect relevant documents.

Perform structure analysis, analysis of data protection requirements and derive protection requirements for all objects of investigation.

Develop definition and description of relevant threat scenarios and evaluate the potential damage and probabilities.

Provide description of risks, including a risk matrix, and make recommendations of countermeasures. Compile and review the report, including a management summary.

Our services

From the onset, our industrial IT security experts are able to provide comprehensive advice and guidance related to identifying the risks and potential damages of your industrial control systems. We support you with our knowledge of the risk methodologies that work most efficiently.

- **Proven generic methodology for the compilation of risks for different industrial environments**
  TÜV SÜD adopts a generic methodology (for example, based on ISO/IEC 27005) for general IT environments and customises it for industrial environments, keeping factors such as safety requirements in mind.
- **Use of industry-specific threat and/or danger catalogues**
  We recognise that threats differ considerably by industry. These differences are reflected in threat scenarios described in the threat catalogues.
- **Structure analysis**
  TÜV SÜD identifies all aspects of the current status of the system (logical network plan, all communication lines, all assets and their dependencies). Processes such as change management and incident handling are included in this structure analysis.
- **Proven methodology for the evaluation of probabilities**
  Our experts refer to methods described in standards to assess probabilities, ensuring they are efficient and traceable.
- **Representation in a risk matrix**
  We summarise the risk landscape in a risk matrix that is suitable for management presentations. Our experts also provide an action plan with a prioritised list of countermeasures.
- **Cost/benefit presentation**
  Whenever possible, our risk methodology includes calculation of costs in comparison to the reduction of risks, providing a clear basis for decision-making.

Your business benefits

- **Save money** – with a prioritised list of measures to mitigate risks in a cost-efficient manner.
- **Save time** – by using our effective, efficient and proven methodology.
- **Minimise risk** – with a comprehensive action plan that ensures the mitigation and traceability of risks.
- **Achieve transparency** – of risks analysed, which are all reproducible and understandable to management.
- **Resolve potential problems** – at an early stage with TÜV SÜD's countermeasures and solutions.

Why choose TÜV SÜD?

TÜV SÜD combines expertise in industrial IT security with process knowledge in a wide range of industries and critical infrastructures. Our highly trained experts have extensive experience of industrial environments and can draw upon their knowledge to determine which industry-specific risks are relevant to each customer. The methodology we utilise for risk analysis combines safety and security for our customers. It has also been tested and proven over the course of many projects.

Choose certainty. Add value.

TÜV SÜD is a premium quality, safety and sustainability solutions provider that specialises in testing, inspection, auditing, certification, training and knowledge services. Represented in over 800 locations worldwide, we hold accreditations in Europe, the Americas, the Middle East, Asia and Africa. By delivering objective solutions to our customers, we add tangible value to businesses, consumers and the environment.

Related services

TÜV SÜD provides the following related services:

- Security check
- Industrial IT Security – Penetration Testing
- ISO/IEM 27005

TÜV SÜD Rail GmbH Barthstraße 16, 80339 Munich, Germany
+49 89 5791-1473 **embedded@tuv-sud.com** **www.tuv-sud.com/embedded**