



SERVICE & DISTRIBUTION
GmbH
INDUSTRIAL AUTOMATION



OUR ADDED VALUE FOR YOU

INDUSTRIAL CYBER SECURITY

TABLE OF CONTENTS

- OUR ADDED VALUE FOR YOU 3**

- CRITICAL INFRASTRUCTURES (KRITIS) 4**
- EUROPEAN UNION’S NIS-2 (NETWORK AND INFORMATION SECURITY) . 5**
- NETWORK STANDARDIZATION & SEGMENTATION 6**
- OT NETWORK ANALYSIS 7**
- RISK ANALYSIS ACCORDING TO IEC 62443 8**
- OT FIREWALL ANALYSIS 9**
- SWITCH CONFIGURATION ANALYSIS 10**

- NETWORK MONITORING. 11**
- INTRUSION DETECTION SYSTEM (IDS) 12**
- MANAGEMENT SECURITY DASHBOARD 13**
- IoT HONEYPOT 14**
- INDUSTRIAL FIREWALL. 15**
- NETWORK ACCESS CONTROL (NAC) 16**
- INDUSTRIAL REMOTE ACCESS 17**

- SERVICE LEVEL AGREEMENTS 18**

- CONTACT 19**

OUR ADDED VALUE FOR YOU

In recent years, the demands placed on IT and OT departments have grown exponentially. Tasks are increasingly overlapping across departments to an equal degree.

It is only when we look closer at the priorities established among these tasks that it becomes clear that, in some cases, these demands conflict with one another:

- Confidentiality vs. integrity vs availability vs safety?
- Which hardware meets the specific needs of a production environment?

- Which actions must be carried out automatically, and which ones may not be?
- Does it really make sense to centrally manage and be responsible for the enterprise and production networks?

We answer these and many other questions based on our many years of practical experience, and work with you to develop a secure and available OT network that meets your personal requirements and the requirements of IEC 62443, while helping to improve your KPIs.

NETWORK INFRASTRUCTURE

- Network design
- Network segmenting
- Defining zones and connections
- Securing devices and access points
- Network documentation

COLLECT & MANAGE DATA

- Collecting data (Syslog & sensors)
- Filter & manage log data
- Investigation, analysis & reporting

ASSESSMENTS ACCORDING TO INTERNATIONAL STANDARDS

- Analyze risks
- Assess security vulnerabilities
- Best practice & policy testing
- Independent evaluation

ENSURE INTEGRITY

- Detect changes in real time
- Resolve vulnerabilities
- Software-based monitoring & reporting
- Training and raising awareness among staff

CRITICAL INFRASTRUCTURES (KRITIS)

What is KRITIS?

Critical infrastructures (KRITIS) are the most important supply and security systems in our society that are essential for the functioning of the state and the economy. These sectors are particularly vulnerable to cyber-attacks as they process a large amount of sensitive data and ensure the continuity of daily life.

These include:

- Energy supply
- Water supply
- Healthcare
- Transportation and traffic
- Finance and insurance
- Food
- Waste disposal
- Information and communication technology (ICT)

Why is it important?

The KRITIS regulation requires companies in these sectors to implement resilient cybersecurity measures to protect their systems from threats. The security of OT (Operational Technology) networks plays a central role in this, as they control the physical processes responsible for the operation of these critical infrastructures. Given the increasing complexity and integration of these systems, the need to protect them from cyber attacks is becoming ever more urgent.

Why we are the right partner:

We understand the criticality of your systems and the serious consequences of failures. As an experienced partner, we offer individual solutions tailored to your specific requirements. With a step-by-step approach, we secure your OT environment, minimize risks and guarantee maximum security – without disrupting ongoing operations.

Why KRITIS compliance is critical for your business:

- **Increased security requirements:** Companies covered by the KRITIS regulation face the challenge of protecting their IT and OT networks against a wide range of threats. This requires a comprehensive security strategy that includes both preventive and reactive measures.
- **Legal and regulatory obligations:** Failure to comply with KRITIS requirements can lead to significant legal consequences, including heavy fines and claims for damages. In addition, public trust in your company could be damaged, which could have a long-term impact on your business.
- **Protecting society:** As a company operating a critical infrastructure, you have a special responsibility. Protecting your systems not only contributes to the security of your company, but also to the stability and security of society as a whole. A successful attack on your systems could have serious consequences for public safety and economic stability.

EUROPEAN UNION'S NIS-2 (NETWORK AND INFORMATION SECURITY)

What is the NIS-2 Directive?

The European Union's NIS-2 (Network and Information Security) Directive represents a significant tightening of the existing NIS Regulation and aims to strengthen cyber security in essential sectors. This directive is relevant for companies operating in the areas of:

- Energy
- Water and Wastewater
- Health
- Transportation and Traffic
- Government
- Finance and Insurance
- Space
- Food
- Waste Management
- Post/Courier
- Manufacturing
- Digital Services
- Research
- Information and Communication Technology (ICT)

It sets out stricter requirements for the cyber security measures that companies must take to protect their networks from attacks.

What does it mean for your company

Companies that operate OT networks face the challenge of meeting the new requirements of the NIS-2 directive. These ' networks', which are responsible for controlling and monitoring physical processes in critical infrastructures, are increasingly the target of cyber attacks. The NIS-2 directive requires not only the introduction of technical measures, but also the implementation of organizational and procedural security measures.

Why we are the right partner:

We know the high requirements of the NIS-2 directive and the importance of reliability. Our tailor-made solutions ensure that your OT systems remain secure and compliant. Step by step, we develop a stable security strategy that minimizes risks and avoids downtime.

Why NIS-2 compliance is crucial for your company:

- **Mandatory security measures:** The NIS-2 directive requires companies to comprehensively rethink and adapt their cybersecurity strategies. This includes implementing security measures such as intrusion detection systems, firewalls and network access control to detect and defend against threats at an early stage.
- **Increased liability and sanctions:** Failure to comply with NIS-2 requirements can lead to significant legal consequences, including financial penalties and loss of reputation. Companies must therefore ensure that their security measures meet the latest standards.
- **Protecting critical systems and data:** Ensuring the continuity of your operational processes and protecting sensitive data are key elements of the NIS-2 directive. A successful attack could not only cause financial damage, but also jeopardize public safety..

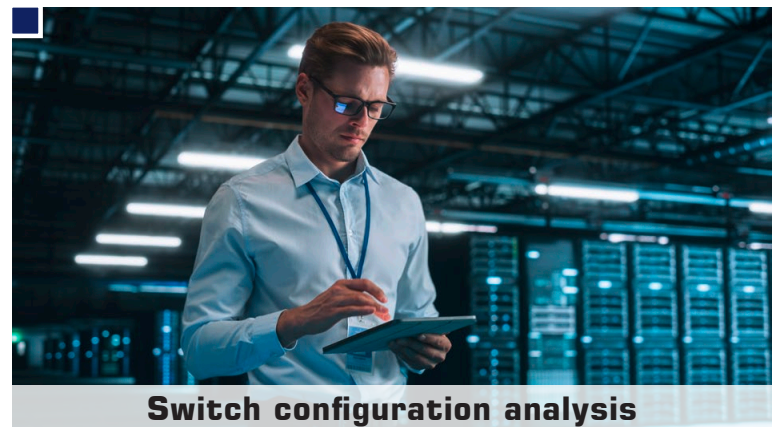
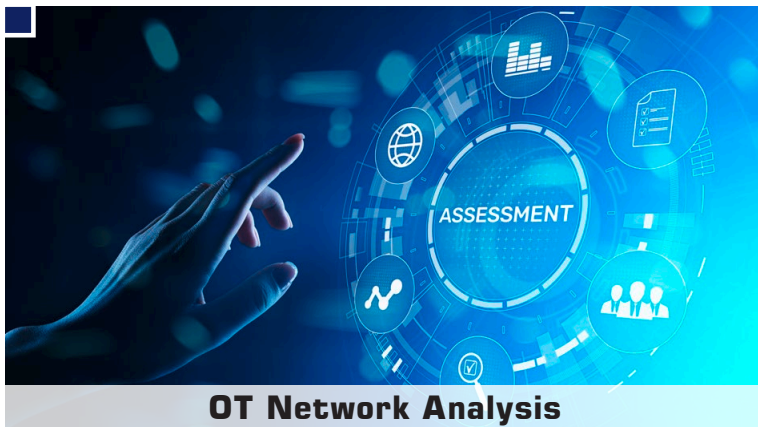
NETWORK STANDARDIZATION & SEGMENTATION

Maintain an overview of the hardware you use, ensure the shortest possible reaction times by stockpiling important spare parts and divide your production network into highly secure and autonomous zones.

Our network standardization and segmentation solutions provide the tools and techniques to efficiently manage and

protect your network infrastructure. Discover our specialized products and services to help you optimize your networks, minimize risk and keep your business running. Learn more about our innovative approaches and let us help you implement your custom network strategy.

OUR SERVICES



OT NETWORK ANALYSIS

Our OT Network Analysis evaluates your existing network infrastructure according to the current security standards. This helps you identify vulnerabilities and make targeted improvements to your network security.

WHY CONDUCT A OT NETWORK ANALYSIS?

INVENTORY OF THE OT NETWORK

We analyze your existing OT network to build a comprehensive view of your infrastructure.

VERIFICATION ACCORDING TO IEC 62443 STANDARDS

Our assessment follows the international safety standards of IEC 62443 to ensure that your OT network meets the highest safety requirements..

DOCUMENTATION AND CREATION OF A NETWORK TOPOLOGY

Based on our findings, we create detailed documentation and a network topology that serves as the basis for further security measures..

CUSTOMER LOYALTY

A proactive security strategy enables you to avoid disruptions and outages, which not only increases productivity, but also boosts your customers' confidence in your services..

OUR SERVICE

IN-DEPTH ANALYSIS

Our experts will conduct in-depth analysis of your network to identify potential security risks.

DOCUMENTATION AND NETWORK PLANNING

We create comprehensive documentation and network topologies to help you better understand and manage your infrastructure.

RECOMMENDATIONS FOR OPTIMIZING YOUR OT SECURITY

Based on our findings, we provide recommendations for optimizing your OT security to increase the security and reliability of your network.

INDEPENDENT ADVICE

We provide you with independent advice that focuses exclusively on your needs. We help you improve the security of your network, regardless of the specific vendors or solutions you use.

YOUR BENEFITS

SECURITY CONFORMITY

Our assessment helps you meet security requirements according to international standards such as IEC 62443.

RISK MITIGATION

We minimize potential threats to your network by identifying and remediating security risks.

IMPROVED NETWORK PERFORMANCE

Thorough analysis and documentation enables you to more efficiently manage and optimize your network.

REDUCED DOWNTIME AND SHUTDOWNS

By identifying and addressing potential vulnerabilities, we can minimize downtime and maximize the availability of your IT network.

RISK ANALYSIS ACCORDING TO IEC 62443

The risk analysis according to IEC 62443 supports you in identifying and evaluating potential security risks in your network. Based on this analysis, you can implement effective risk minimization and operational security measures.

WHY CONDUCT A RISK ANALYSIS?

IDENTIFY VULNERABILITIES

Our analysis identifies potential vulnerabilities in your OT network that could allow attackers to enter and/or inflict harm.

THREAT DETECTION

We identify and assess current and potential threats that could compromise your network, including malware, phishing attacks, and insider threats.

RISK ASSESSMENT

Based on our findings, we assess the risk to your OT network and help you prioritize and take appropriate security measures.

OUR SERVICES

VULNERABILITY ASSESSMENT

We conduct a comprehensive network analysis to identify and assess vulnerabilities in your infrastructure.

THREAT IDENTIFICATION

Our experts identify threats and attack patterns to understand and address potential attack vectors.

RISK ASSESSMENT

We assess the risks to your business and help you make informed decisions about security investments and actions.

INDEPENDENT ADVICE

We offer independent advice that focuses exclusively on your needs. Our goal is to help you minimize the risks to your OT network and optimize your security strategy.

YOUR BENEFITS

RISK MITIGATION

Minimize the risk of security incidents and data loss by identifying and assessing vulnerabilities and threats.

PROTECTION AGAINST FINANCIAL LOSSES

A well-founded risk analysis allows you to avoid potential financial losses due to security incidents and to ensure your business continuity.

IMPROVED COMPLIANCE

Comprehensive risk & threat analysis helps you ensure compliance with security standards and regulatory.

OT FIREWALL ANALYSIS

Our firewall analysis checks the configuration and effectiveness of your firewall systems. This ensures that your network security meets the highest standards and prevents unauthorized access.

WHY CONDUCT A FIREWALL ANALYSIS?

OPTIMIZE EFFECTIVENESS

Our review ensures your firewall rules are effective and potential security vulnerabilities are closed

SCOPE REVIEW

We assess the scope of your firewall rules to ensure they are properly configured and meet your security needs.

OUR SERVICES

FIREWALL RULES ASSESSMENT

We review and analyze your firewall rules to ensure they provide the best protection for your network.

OPTIMIZATION RECOMMENDATIONS

Based on our findings, we provide recommendations to optimize your firewall rules to close security gaps and increase efficiency.

COMPLIANCE AUDIT

We ensure that your firewall rules meet applicable security standards and compliance requirements.

INDEPENDENT CONSULTING

Our independent consulting services are focused on improving the security and effectiveness of your firewall rules, no matter the specific vendors or solutions you use.

YOUR BENEFITS

INCREASED NETWORK SECURITY

By optimizing your firewall rules, you minimize security risks and protect your network from potential attacks.

IMPROVED PERFORMANCE

Effective firewall configuration ensures optimal network performance without compromising security.

COMPLIANCE

We ensure that your firewall rules meet applicable security standards and compliance requirements to minimize legal risk.

SWITCH CONFIGURATION ANALYSIS

Switch configuration analysis ensures your network switches are configured optimally. We review and optimize settings to maximize the performance and security of your network infrastructure.

WHY CHOOSE A SWITCH CONFIGURATION ANALYSIS?

IDENTIFYING VULNERABILITIES

Our analysis identifies potential vulnerabilities in your switch configuration that may pose security risks to your network..

OPTIMIZING CONFIGURATION

We can help you optimize your switch configuration to improve security and maximize performance.

OUR SERVICES

ASSESSING VULNERABILITIES

We thoroughly evaluate your switch configuration to identify vulnerabilities and potential attack vectors.

RECOMMENDED REMEDIATION

Based on our findings, we provide specific recommendations to address vulnerabilities and improve the security of your switch configuration.

OPTIMIZING PERFORMANCE

We can help you optimize your switch configuration to improve network performance and eliminate bottlenecks.

INDEPENDENT CONSULTING

Our independent consulting services are focused on improving the security of your switch configuration, regardless of specific vendors or solutions.

YOUR BENEFITS

INCREASED NETWORK SECURITY

By identifying and fixing vulnerabilities, you minimize the risk of security incidents and protect your network from potential attacks.

IMPROVED NETWORK PERFORMANCE

Optimized switch configuration improves network performance and reduces bottlenecks, resulting in a better user experience.

COMPLIANCE

We ensure that your switch configuration meets applicable security standards and compliance requirements to minimize legal risk.

NETWORK MONITORING

Easily create an up-to-date asset overview, save a blueprint of your desired network structure and get intelligently prioritized and summarized recommendations for action from our tools to continuously improve your network.

Our comprehensive network monitoring solutions provide a real-time view of the health and performance of your entire IT and OT infrastructure. Through continuous

monitoring and analysis, you can identify potential problems early and take proactive measures to prevent outages and increase operational safety. Leverage our advanced monitoring tools and services to ensure a robust and efficient network environment that meets the highest security and performance standards.

OUR SERVICES



Intrusion Detection System (IDS)



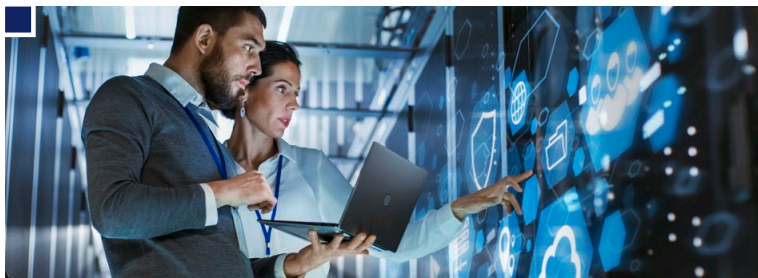
Management Security Dashboard



IoT Honeypot



Industrial Firewall



Network Access Control (NAC)



Industrial Remote Access

INTRUSION DETECTION SYSTEM (IDS)

Our Intrusion Detection System (IDS) continuously monitors your network for suspicious activity and potential security breaches. It alerts you in real time so you can take immediate action to neutralize threats.

WHY CHOOSE AN INTRUSION DETECTION SYSTEM (IDS)?

EARLY DETECTION OF ATTACKS

IDS allows suspicious behavior to be detected in real time and acted upon before damage occurs.

DATA LOSS PREVENTION

Network traffic monitoring helps protect sensitive data from unauthorized access.

COMPLIANCE WITH SECURITY STANDARDS

An IDS helps organizations meet industry-specific security standards and compliance requirements.

OUR SERVICES

ANALYZING CUSTOMER REQUIREMENTS

We understand the unique needs of each customer's IT environment and develop customized solutions.

CHOOSING THE RIGHT IDS SOLUTION

Based on a thorough analysis, we recommend the right IDS software to meet your needs.

IMPLEMENTATION AND CONFIGURATION

Our experts will help you seamlessly integrate IDS with your existing infrastructure and tailor it to your needs.

TRAINING AND SUPPORT

We provide training for your team and technical support to ensure you get the most out of your IDS.

INDEPENDENT ADVICE

We provide you with independent advice that focuses exclusively on your needs. We are not tied to specific vendors and instead choose the best solution for you.

YOUR BENEFITS

CHOOSE FROM A VARIETY OF VENDORS

We work with a variety of IDS vendors to ensure you get the best possible solution.

TAILORED SOLUTIONS

We develop solutions that are tailored to your needs and do not offer one-size-fits-all solutions.

OBJECTIVE RECOMMENDATIONS

Our advice is based on objective criteria and aims to ensure the long-term security and efficiency of your network.

MANAGEMENT SECURITY DASHBOARD

The Management Security Dashboard gives you a single overview of all security-related events and conditions in your network. It provides you with clear and understandable signals so you can make informed decisions to improve your network security.

WHY CHOOSE A MANAGEMENT SECURITY DASHBOARD?

CLEAR DISPLAY

Our dashboard solution provides a clear and intuitive display of all key figures relevant to production and cyber security.

REAL-TIME DATA

With real-time data, you can have an up-to-date view of the status of your production and the security of your network at any time.

INFORMATION BASIS FOR DECISION-MAKING

Our dashboard provides you with the information you need to make informed decisions about how to optimize your production and improve your cybersecurity.

OUR SERVICES

PRODUCTION KEY FIGURES

visualization of production data such as machine utilization, downtime, production progress, etc.

CYBERSECURITY KEY FIGURES

Illustration of Cybersecurity key figures such as attack frequency, security events, compliance status, etc.

CUSTOM DASHBOARDS

Customizable dashboards that allow you to track key features and KPIs that are relevant to you.

ALARM FUNCTIONS

Alerts and notifications regarding abnormal or critical events so you can react immediately.

YOUR BENEFITS

INCREASED EFFICIENCY

By clearly displaying all relevant key figures, you can optimize your production processes and identify bottlenecks.

ENHANCED SECURITY

Our dashboard allows you to identify security risks early on and take appropriate action to protect your network.

SUPPORT FOR DECISION-MAKING

Real-time data and meaningful visualizations help you make informed decisions to advance your.

IoT HONEYPOT

Our IoT Honeypot is a strategically placed trap for cybercriminals who try to enter your network without authorization. It helps you identify attackers and gather valuable information about their methods to strengthen your security measures.

WHY CHOOSE AN IoT HONEYPOT?

DECEIVING ATTACKERS

With a IoT Honeypot, you can mislead attackers by simulating an obvious vulnerability that does not contain productive data.

DETECT ATTACKS EARLY

Alerting you to unauthorized access provides early warning of potential attacks and enables you to react accordingly

PROTECT YOUR CORE NETWORK

By keeping attackers out of your core network, you can ensure the security of your productive systems.

OUR SERVICES

CONFIGURING AN OBVIOUS VULNERABILITY

We configure a honeypot with a targeted vulnerability to attract potential attackers.

REAL-TIME ALERTS

Access to the honeypot triggers alerts immediately to notify you of potential threats.

ATTACK PATTERN TRACKING

We analyze the attack data to identify attack patterns and take appropriate countermeasures.

INTEGRATION WITH EXISTING SECURITY INFRASTRUCTURE

Our IoT Honeypot solution integrates seamlessly with your existing security infrastructure and complements your existing protection mechanisms.

YOUR BENEFITS

EARLY DETECTION OF THREATS

Early detection of attacks allows you to react quickly and minimize potential damage.

ENHANCED SECURITY

A honeypot complements your existing security measures and increases your network's resilience against attacks.

REDUCED RISK

By keeping attackers out of your productive systems, you reduce the risk of data loss and business disruption.

INDUSTRIAL FIREWALL

The Industrial Firewall protects your operating technology from unauthorized access and attacks. By implementing specific rules and filters, it ensures that only authorized traffic flows are allowed, enhancing the security and integrity of your network.

WHY CHOOSE AN INDUSTRIAL FIREWALL?

PROTECTION AGAINST CYBER ATTACKS

An Industrial Firewall provides comprehensive protection against unauthorized access and targeted attacks on your operating technology. It filters network traffic and blocks harmful packets before they can reach your system.

SECURING OPERATING PROCESSES

By separating and monitoring network interfaces, an Industrial Firewall ensures that your critical operating processes run securely and without interference.

CHOOSING THE RIGHT OT FIREWALL

Based on a thorough analysis, we recommend the appropriate firewall technology that meets your security needs and protects your network infrastructure optimally.

OUR SERVICES

CUSTOMER NEEDS ANALYSIS

We understand the specific needs of your IT environment and develop custom firewall solutions that perfectly match your needs.

CHOOSING THE RIGHT OT FIREWALL

Based on a thorough analysis, we recommend the appropriate firewall technology that meets your security needs and protects your network infrastructure optimally.

IMPLEMENTATION AND CONFIGURATION

Our experts will help you seamlessly integrate the Industrial Firewall into your existing infrastructure and adapt the configuration to your individual needs.

TRAINING AND SUPPORT

We provide comprehensive training for your team and technical support to ensure that your Industrial Firewall is utilized optimally and meets your security requirements.

INDEPENDENT ADVICE

We provide you with independent advice that focuses exclusively on your needs. We are not tied to specific vendors and instead choose the best solution for you.

YOUR BENEFITS

CHOOSE FROM A VARIETY OF VENDORS

We work with a variety of Industrial Firewall vendors to ensure that you get the best possible solution that meets your specific needs.

TAILORED SOLUTIONS

We develop solutions that are tailored to your requirements, instead of offering only one-size-fits-all solutions. Each firewall solution is customized to meet your security needs.

OBJECTIVE RECOMMENDATIONS

Our advice is based on objective criteria and aims to ensure the long-term security and efficiency of your network. We recommend the best technologies and strategies to protect your OT infrastructure.

NETWORK ACCESS CONTROL (NAC)

With Network Access Control (NAC), we enable you to control and monitor all network access. This solution will help you strictly regulate access to your network and exclude unauthorized devices.

WHY CHOOSE A NETWORK ACCESS CONTROL (NAC) SOLUTION?

PROTECT AGAINST UNAUTHORIZED ACCESS

Our NAC solution prevents unauthorized access to endpoints and protects your network from potential threats.

STRICTER ACCESS CONTROL

By implementing strict access control, you can ensure that only authorized users and devices can access your network.

SECURING SENSITIVE DATA

By preventing unauthorized access to endpoints, you protect sensitive business data from unauthorized access and data loss.

FUNCTIONS

ENDPOINT IDENTIFICATION

Our NAC solution identifies and verifies all endpoints that are attempting to access your network.

GUIDELINE-BASED ACCESS CONTROL

We implement guideline-based access controls to ensure that only authorized users and devices can access your network.

GUEST ACCESS CONTROL

We enable you to securely provide guest access while ensuring the security of your network.

REAL-TIME MONITORING

Our NAC solution continuously monitors network access and responds immediately to unauthorized access attempts.

YOUR BENEFITS

INCREASED SECURITY

Our NAC solution enhances your network's security by preventing unauthorized access to endpoints and protecting sensitive data.

IMPROVED COMPLIANCE

By implementing strict access controls, you can ensure compliance with security standards and regulatory requirements.

REDUCE SECURITY RISKS

By controlling access to your network, you reduce the risk of security incidents and data loss.

INDUSTRIAL REMOTE ACCESS

Our Industrial Remote Access solutions offer safe and reliable ways to remotely monitor and maintain your operating technology. This ensures quick problem resolution and reduces downtimes in your production.

WHY CHOOSE INDUSTRIAL REMOTE ACCESS?

RAPID PROBLEM RESOLUTION

Industrial remote access allows technicians to access your systems and instantly diagnose and resolve problems without having to be on site. This significantly reduces downtime.

COST-EFFICIENCY

Remote access eliminates travel costs and time. This makes maintenance more efficient and cost-effective.

SECURE ACCESS

Our industrial remote access solutions provide encrypted connections and strict access controls to ensure that only authorized people can access your systems.

OUR SERVICES

NEEDS-BASED ANALYSIS

We understand the specific requirements of your OT environment and develop customized remote access solutions that exactly match your needs.

INDIVIDUAL SOLUTION SELECTION

Based on a detailed analysis, we recommend the appropriate remote access tools and technologies that best suit your infrastructure and requirements.

SEAMLESS INTEGRATION AND SETUP

Our experts will help you implement and configure the remote access solution into your existing infrastructure to ensure smooth operation.

TRAINING AND TECHNICAL SUPPORT

We provide comprehensive training for your team and ongoing technical support to ensure your remote access solution is used efficiently and meets your needs at all times.

INDEPENDENT CONSULTING

Our consulting focuses exclusively on your needs, independent of specific providers, in order to find the best solution for you.

YOUR BENEFITS

DIVERSITY OF PROVIDERS

We work with numerous OT Remote Access providers to ensure that you get the best solution for your specific needs.

CUSTOMIZED SOLUTIONS

Each remote access solution is tailored to your specific needs and not offered as a one-size-fits-all solution.

OBJECTIVE RECOMMENDATIONS

Our recommendations are based on objective criteria and aim to ensure the long-term efficiency and security of your IT infrastructure.

SERVICE LEVEL AGREEMENTS

Are your engineers having trouble guaranteeing continuous functionality and support for your production network? No problem, because we support you 24/7 by phone, by e-mail and personally on site. In addition, staff training courses “on the job,” combined with detailed documentation, allow for response times of just a few minutes if service is required.

Our Service Level Agreements (SLAs) ensure that you can count on top-notch support around the clock, especially in the event of a cyber security incident or unforeseen failure of your production network. We offer custom-made SLA packages that are tailored to your needs and requirements. Whether it's preventive maintenance, proactive monitoring, or rapid troubleshooting, our team is always on hand to help keep your network infrastructure running smoothly.

In the event of a cyber security incident or an unforeseen network failure, making sure you can resume production as soon as possible is our top priority, so that you do not suffer significant damage. Our SLAs give you guaranteed response and resolution times to resolve technical issues quickly and efficiently. Our experts ensure that your systems are quickly restored and backed up so that your production processes are not interrupted. Trust in our comprehensive services and enjoy the assurance that your network is in the best hands.

CONTACT

UMER BHATTI

Business Development Manager OT-Security
(TÜV cert. Information Security Officer)

📞 +49 151 27648814
✉ bhatti@sud-gmbh.de

PATRICK POBERITZ

Head of Business Development & Marketing

📞 +49 151 27648842
✉ poberitz@sud-gmbh.de



🌐 <https://sud-gmbh.de/en/industrial-cyber-security>



SERVICE & DISTRIBUTION
GmbH
INDUSTRIAL AUTOMATION

S&D Service & Distribution GmbH
Bischofstraße 113, 47809 Krefeld
Carl-Zeiss-Str. 8, 72124 Pliezhausen
Fuggerstraße 1b, 04158 Leipzig

☎ +49 2151 4576-600
☎ +49 2151 4576-777
✉ info@sud-gmbh.de
🌐 www.sud-gmbh.de



**Value-Add
Distributor**

A ROCKWELL AUTOMATION PARTNER