STAR GROUP

CYBERSECURITY
FOR YOUR PRODUCTION FACILITIES

Secure. Compliant with the law. Future-proof.

SUSTAINABLE SAFETY FOR PRODUCTION AND OPERATIONAL PROCESSES STARTS WITH SAR

The ongoing digitalization of industrial plants, production environments, and infrastructure is creating significant efficiency and competitive advantages. Connected machines, automated processes, and the continuous exchange of data between IT and OT systems are now an integral part of modern industrial environments.

At the same time, however, the attack surface for cyberattacks is growing significantly. In particular, OT (Operational Technology) environments, which were not designed for networked use, are increasingly becoming targets of ransomware, malware, and sabotage. The consequences range from production downtime and quality losses to security breaches and reputational damage.

This white paper explains why traditional security approaches are no longer sufficient and how a comprehensive cybersecurity strategy can provide long-term protection for production facilities.

CYBER THREATS IN INDUSTRIAL OT ENVIRONMENTS

Operational Technology (OT) encompasses systems and networks used to control, monitor, and automate physical processes, including, but not limited to:

- PLCs for controlling robotic arms and assembly lines
- SCADA systems for monitoring production lines
- HMIs (human-machine interfaces) for machine operation
- Energy, water, and utility systems
- Transportation and logistics (e.g., traffic control systems, train and fleet monitoring)
- Critical infrastructure (water supply, wastewater treatment, process control systems)

Unlike traditional IT, the focus in OT environments is not on data, but on the **availability, integrity, and security of processes**. Disruptions or tampering have a direct impact on production, delivery capabilities, and supply security.

Cyberattacks are increasingly targeting industrial processes directly. Tampered control systems, altered parameters, or targeted shutdowns can have an immediate and lasting impact on physical production.

As connectivity increases, the risks grow significantly:

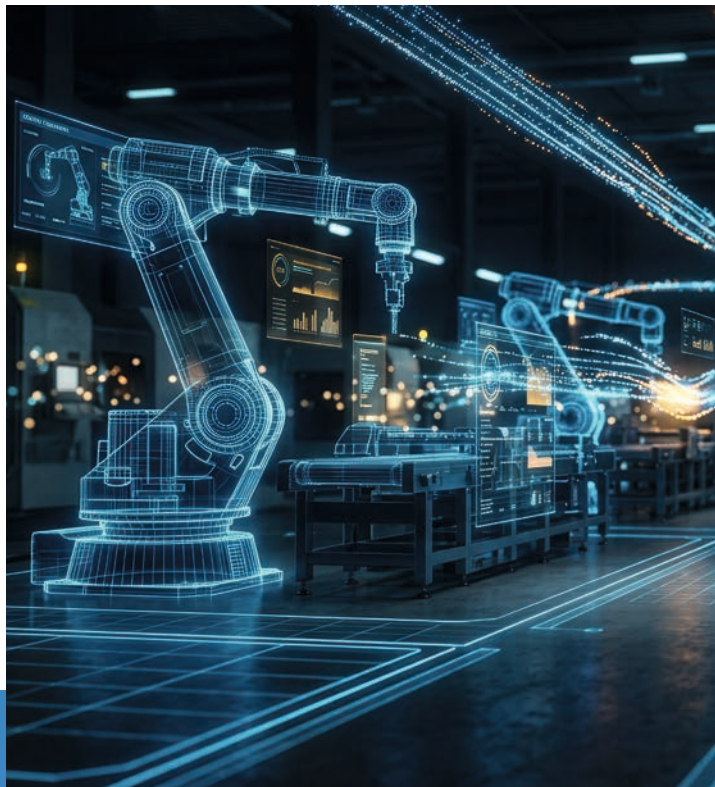
- **Expanded attack** surfaces due to remote access, cloud connections, and external service providers
- **Lack of transparency** regarding assets and communication links
- **Outdated systems** with limited update capabilities
- **Significant impact** even during brief outages

THE UNIQUE THREAT LANDSCAPE IN OT ENVIRONMENTS

For a long time, OT systems were operated in isolation and were therefore considered relatively secure. This assumption is no longer valid today. The main reasons for this are:

- Increasing integration of OT and IT systems
- Remote maintenance access and external service providers
- Use of mobile devices and removable media
- Outdated systems that cannot be patched

Modern cyberattacks are increasingly aimed at **sabotage, extortion, and production outages**. Traditional IT security measures, such as antivirus scanners and firewalls, quickly reach their technological and operational limits in OT environments.



COMMON CHALLENGES FOR BUSINESSES

Many businesses face similar challenges when it comes to OT cybersecurity:

- Lack of transparency regarding systems and communication links
- High demands on availability and real-time performance
- Long lifecycles of plants and control systems
- Limited maintenance windows
- Increasing regulatory requirements (e.g., NIS2, IEC 62443)

In particular, operators of critical infrastructure (KRITIS) are subject to expanded legal requirements, including heightened security, documentation, and reporting obligations. Security incidents in OT environments must be reported within defined timeframes. A lack of transparency or inadequate monitoring not only jeopardizes operations but can also result in legal and financial consequences.

REQUIREMENTS FOR MODERN INDUSTRIAL CYBERSECURITY

To effectively address these risks, companies need specialized security solutions that meet the specific requirements of industrial environments. Simply applying traditional IT security approaches is not enough. What is needed are concepts specifically tailored to OT, which are organized around five key pillars:

Transparency and Inventory Management
Complete visibility of all systems, devices, and data connections—without disrupting ongoing operations.

Continuous Monitoring
Constant monitoring of network traffic to detect deviations from normal operation at an early stage.

Anomaly and intrusion detection
Identification of unusual communication patterns, manipulation, and potential attacks.

Intelligent Alerts
Prioritized and clear presentation of relevant security events to enable quick, targeted action.

Integration into existing processes
Seamless integration of OT cybersecurity into existing operational, maintenance, and security processes.

The comprehensive implementation of these action areas creates a robust security foundation for industrial IT and OT environments. Cybersecurity thus evolves from a purely technical protective mechanism into a strategic factor for stable processes and regulatory compliance.

SAR AS A PARTNER FOR OT CYBERSECURITY

With **IRMA® (Industrial Risk Management Automation)**, SAR offers a cybersecurity solution specifically designed for OT environments.

IRMA® protects production facilities through passive, continuous network monitoring without disrupting ongoing operations. Cyber threats are detected early, and risks are minimized in a targeted manner. This holistic security approach is based on four key steps:

Analyze

Automatic identification of all networked assets in IT and OT environments.

Manage

Structured classification and grouping of systems for high transparency.

Rate

Real-time detection of threats, anomalies, and vulnerabilities, including risk assessment.

Visualization

Clear dashboards and intelligent alerts for quick responses.

BENEFITS FOR INDUSTRIAL PLANT OPERATORS

The use of IRMA® offers companies numerous operational and strategic benefits:

- ✓ **Real-time threat detection:** Immediate detection of attacks and security incidents before production outages occur.
- ✓ **Automated asset visibility:** A complete overview of all connected systems—even in complex OT environments.
- ✓ **Minimization of production downtime:** Early alerts enable timely countermeasures.
- ✓ **Support for regulatory requirements:** Assistance with the implementation of NIS2, KRITIS, DORA, or IT SiG 2.0.
- ✓ **Protection even for systems that cannot be patched:** Effective protection of older control systems and operating systems through passive monitoring.
- ✓ **Support for compliance and audits:** Transparency, documentation, and reporting make it easier to maintain records.
- ✓ **Sustainable risk reduction:** Continuous risk transparency as the basis for well-informed security decisions.
- ✓ **Easy implementation:** Rapid integration without costly modifications or production interruptions.
- ✓ **Future-proof:** Scalable security architecture for growing digitalization requirements.

SAR IT-SERVICES

Cybersecurity in industrial IT and OT environments is a key success factor for stable, secure, and future-proof production and operational processes. SAR combines in-depth IT security expertise with a deep understanding of industrial processes to develop comprehensive security concepts that can be seamlessly integrated without disrupting operations. Companies benefit from practical solutions for sustainable risk reduction, compliance with regulatory requirements, and long-term planning security. With many years of experience in the field of IT services, SAR GmbH is a reliable partner for an effective and future-oriented cybersecurity strategy.

Schedule your consultation now at **www.sar.biz**

SAR Elektronic GmbH
Gobener Weg 31
84130 Dingolfing

its@sar.biz
www.sar.biz