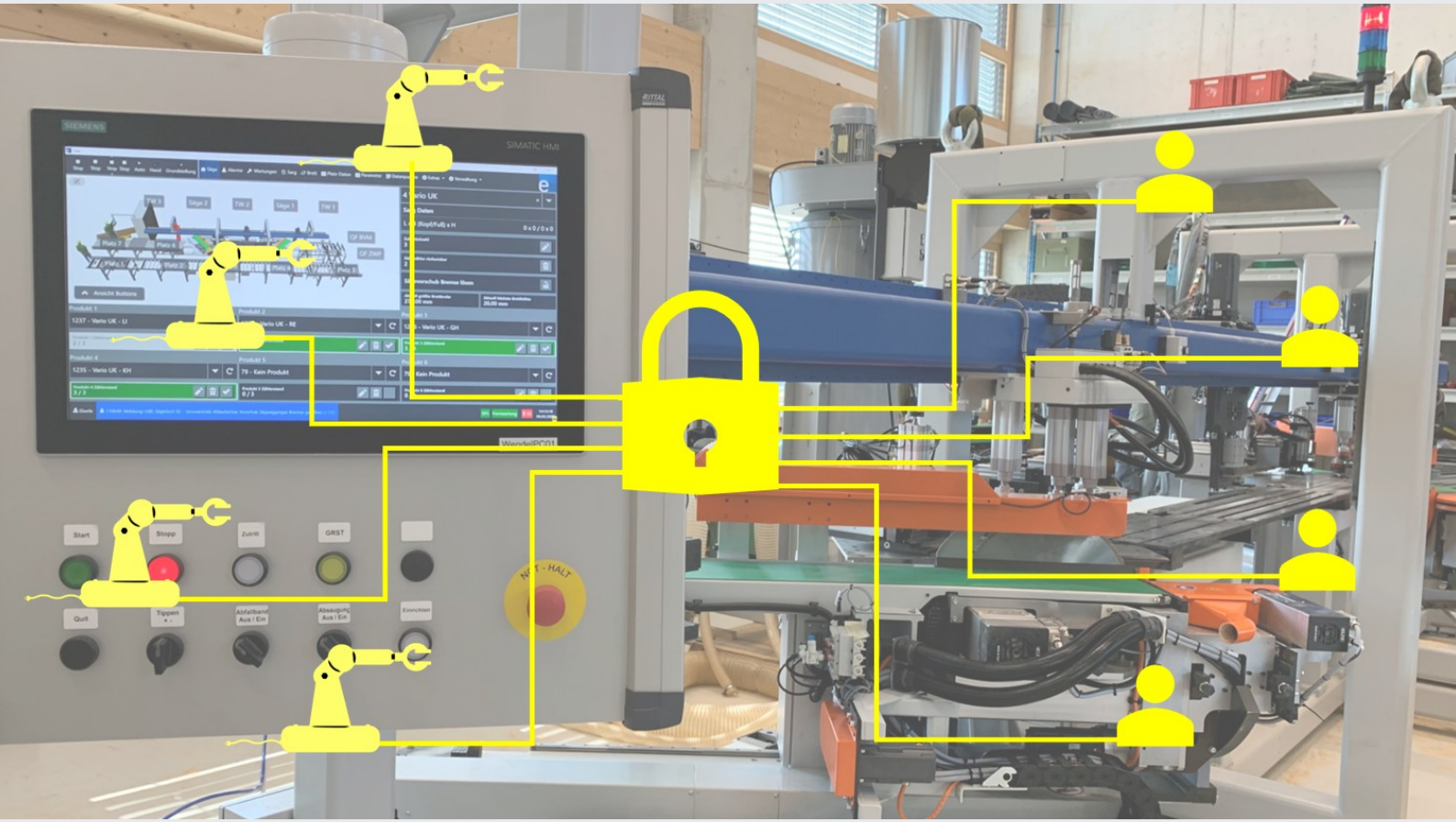
eberle
automatische
systeme



NIS2-Policy and OT-Security

Security is more than trust

NIS stands for “Network and Information Security”

Legal

NIS stands for ‘Network and Information Security’ in administration and production. The management level is responsible for compliance. The NIS applies in full to medium-sized and large companies. Minimum measures are recommended for small companies. The NIS applies to all sectors throughout Europe.

Terms

- NIS: Network and Information Security
- IT: Information Technology. Administrative area
- OT: Operational Technology. Production area
- Security: Security in networked systems.
- Safety: Security for people.
- MFA: Access via multifactor authentication.
- ICT: Information and communication technology
- HMI: Human Machine Interface
- GDPR: General Data Protection Regulation
- ERP: Enterprise Resource Planning
- OEE: Overall Equipment Effectiveness
- Backup: Backing up data
- Restore: Restoring data

OT Networks are increasingly becoming the target of cyber attacks!

Key points of the NIS policy

- Risk analysis and security concept for information systems to deal with security incidents.
- Business > continuity and crisis management.
- Security of the supply chain.
- Security measures for the acquisition, development and maintenance of ICT.
- Concepts and procedures for evaluating the effectiveness of risk management measures.
- Cyber hygiene and cyber security training.
- Cryptography and encryption of data where appropriate.
- Personnel security, access control concepts
- Multi-factor authentication.

NIS Baseline Security for all companies.

- Create a risk assessment, security policy and emergency plan.
- Define security responsibilities.
- Hold security training sessions.
- Create a list of all networked devices.
- Create a directory of access data using secure technology. Restrict access to files and programs.
- Restrict and protect internet presence and external access.
- Carry out security updates promptly. Replace discontinued devices, operating systems and applications.
- Install protection programs against malicious software. Attack protection, malware protection, virus protection. Create regular backups.

Our Expertise

Eberle Automatic Systems has many years of experience with networked automatic systems. Comprehensive networking is essential for efficient operation. Controllers communicate with robots and cameras. Master computers and HMIs communicate with the ERP level, edge devices are connected to the internet and send sensor values for monitoring. **The increasing threat of cybercrime is often not sufficiently taken into account in systems that have 'grown' over the years.**

Eberle employees are experts in the fields of Automation, Software and IT. We are able to comprehensively assess the existing situation, propose measures and implement them. In doing so, we attach great importance to cost-effectiveness. **In the course of a retrofit, a machine can become faster, more accurate, more stable, more energy-efficient and at the same time - without major additional costs - fit for NIS2.**

Our service portfolio

- Retrofitting of machines and systems (mechanical, electrical, software, OT) taking into account the requirements of NIS2 and the GDPR.
- Risk assessment and emergency plan. Consideration of recovery scenarios for energy supply and infrastructure of critical systems.
- Firewall for separation and segmentation of IT- and OT-networks.
- Access protection via MFA. Encrypted communication.
- Spare parts. Training and awareness.
- Backup & restore: machine parameters, product parameters, programs, historical measured values.
- Monitoring of devices and components such as overload, energy consumption, OEE, Preventive maintenance
- Recurring analyses and tests for security and safety.

"Information security is related to personal safety. Although the benefits are not obvious, both are needed to operate machines and systems safely and prevent damage. Eberle has over 30 years of experience in the secure networking and operation of automated systems."

Johannes Drexel, Automation and Robotics Engineer

"We have already created the prerequisites for our internal IT to comply with NIS2. Now we are looking forward to the tasks in OT security."

Nils Berger, IT/OT-Infrastructure

Our common path to NIS2 in OT

- Kickoff meeting to define goals and expectations.
- Review of the OT security architecture.
- Identify vulnerabilities and potential attack surfaces.
- Develop a robust, secure OT network architecture that incorporates industry best practices and standards.

Security recommendations and concrete measures that can be implemented.

Scan here and carry out the security check yourself

Information security increases the availability of machines and reduces damages.

Contact us for a non-binding on-site analysis.

Eberle Automatische Systeme GmbH & Co KG
6850 Dornbirn, Austria
info@eberle.at
+43 5572 55580

www.eberle.at

Partner