KUHSE
POWER SOLUTIONS

CYBER SECURITY IN **EMERGENCY POWER SYSTEMS**

COMPLIANT SECURITY OF CONTROL SYSTEMS

IS YOUR SYSTEM CYBER SECURE?

ARE YOU AN OWNER OR INTEGRATOR OF SYSTEMS FOR CRITICAL INFRASTRUCTURES?

Critical infrastructures (CRITIS) are organizations and facilities of major importance to the state community and security of supply, such as large hospitals, data centers, utilities and independent power producers.

According to the BSI (German federal office for information security), effective cyber security measures must be implemented and periodically verified not only for critical infrastructures, but also for facilities of public interest. Due to the rapidly increasing number of attacks even on companies and facilities, that do not directly belong to these categories, such as smaller hospitals, the self-interest of those companies and facilities in cyber security increased significantly.

NEED OF TECHNICAL & ORGANIZATIONAL MEASURES

Emergency power systems are an essential part of reliable power supply and exposed to an increased risk of cyber attacks through

- cyber attacks on control systems with remote access resp. remote monitoring
- malware infection caused by infected devices accessing the system locally or remotely
- faulty operation by unauthorized persons or persons with restricted authorization through local and remote access
- acts of sabotage

DO YOUR SYSTEMS COMPLY WITH THE CURRENT CYBER SECURITY STANDARDS?

EU CYBER SECURITY ACT:

Establishment of a secure, cyber security-compliant environment (for manufacturers, integrators and asset owners / operators) concerning Industry 4.0 products and systems

IEC 62443:

Rules and guidelines for mandatory security in OT environments (for manufacturers, integrators and asset owners / operators)

IT-SECURITY ACT 2.0:

The 2nd German Security Act to increase the security of IT systems for the protection of the federal administration, critical infrastructures and companies of public interest

WE MAKE YOUR EMERGENCY POWER SYSTEM CYBER SECURE!

As a specialist for emergency power systems in critical infrastructures we offer you **Cyber Security Kits** for new systems as well as a **Cyber Security Check** for your existing emergency power systems.

We analyze weak points and determine optimization potential to protect your applications against cyber attacks and to ensure maximum availability.

We would be happy to support you in an advisory capacity with the certification of your organization and processes according to the guidelines of the Cyber Security Standard IEC 62443-2-4.

KUHSE CYBER SECURITY PRODUCTS

KUHSE CYBER SECURITY PREMIUM KIT

for Emergency Power Systems with **extended** cyber security requirements

TECHNICAL MEASURES

- Network architecture & enhanced network security by means of suitable network devices
- Cloud-based central management of user accounts, access and permissions
- User authentication via two-factor-authentication
- Minimizing the physical and logical accessibility and thus points for potential attacks
- Hardening and strengthening of the control system (hardware, software, services, cloud)
- Logging of logins, login attempts and respective violations
- Backup/restore and disaster recovery tools and procedures

SERVICE MEASURES

- Process manual for operation, maintenance and dealing with cyber attacks
- Training of the owner‘s operators and service personnel
- Repeating tests for ensuring the effectiveness of technical measures and implemented procedures
- Updates for network and security devices, relevant control system components and implemented security tools (patching, anti-malware, application whitelisting, digital certificates)

KUHSE CYBER SECURITY BASIC KIT

for Emergency Power Systems with **basic** cyber security requirements

TECHNICAL MEASURES

- Network architecture & basic network security by means of suitable network devices
- Cloud-based central management of user group accounts, accesses and permissions
- User authentication via two-factor-authentication
- Limitation of physical and logical accessibility and thus points of potential attacks
- Hardening of the Kuhse Gateway and the Cloud environment
- Logging of logins and login attempts
- System backup after delivery and commissioning

SERVICE MEASURES

- Process manual for operation and maintenance
- Regular updates of security mechanisms of the Cloud environment

KUHSE CYBER SECURITY SERVICES

SYSTEMS (CYBER SECURE BASED ON IEC 62443)

- Control Systems / switchboards for prime power applications
- Control Systems / switchboards for emergency power systems
- Control Systems / switchboards for hybrid power applications

SERVICE

- Secure commissioning & maintenance of the system
- Training of the operator and maintenance personnel
- Review of effectiveness and up-to-dateness of cyber security measures
- Performing of security updates
- Remote support at cyber attacks

CONSULTING

- Cyber security awareness training considering relevant standards
- Evaluation of needed technical measures and processes
- Determination of suitable technical measures and processes
- Process manual for integration, operation, maintenance, backup/restore, disaster recovery and for dealing with cyber attacks

WHY YOU CHOOSE KUHSE

- Many years of experience with control systems for emergency power systems for decentralized power generation
- extensive know-how of complex control processes in the overall plant context
- support of plant operators and integrators in all phases of the plant life cycle
- all services - from consulting to commissioning and maintenance - from a single source

CONTACT

Kuhse Power Solutions GmbH
Norbert Reichert
Ohepark 2
21224 Rosengarten
Tel. +49 4171 798-176
n.reichert@kuhse.de
www.kuhse-energy.com