KUHSE

POWER SOLUTIONS

CYBER SECURITY IN **POWER GENERATION PLANTS**

COMPLIANT SECURITY OF CONTROL SYSTEMS

www.kuhse-energy.com

MOTIVATION

Cyber attacks pose a major challenge for the operational reliability of decentralized power plants in critical infrastructures. Many power plants and industrial plants are not armed for dealing with malware targeted on industrial automation and control systems (IACS).

Especially PLC, HMI and SCADA systems are vulnerable targets as cyber attacks on such systems could lead to a massive disruption in operation or even outage of the entire power plant. These direct impacts on the power supply often come along with economic losses as well as loss of reputation and trust.

International standards and regulations provide guidelines for effective cyber security in plant operation and create secure, CRITIS-compliant environments for manufacturers, integrators and operators.

As a specialist for power plant control systems, Kuhse is your competent partner for “cyber secure“ and CRITIS-compliant control solutions. Whether consulting, production, commissioning or service - we offer all services from a single source.

CHALLENGES

INCREASING COMPLEXITY IN THE FIELD OF IT SECURITY DUE TO

- digitization of Industrial Automation & Control Systems (IACS), including control systems for decentralized power generation systems
- rapidly growing technologies for Industry 4.0
- increasing interconnectivity between
  - industrial data networks (OT) and
  - enterprise data networks (IT)

INTERCONNECTIVITY

- Protection of previously isolated areas and network zones against possibilities of cyber attacks
- Increasing number of vulnerabilities in industrial control systems (IACS), of which 20% is related to the energy sector
- Application of IT security concepts on the OT environment under consideration of disparate priorities:
  - IT: data and information protection
  - OT: reliability and availability as well as a long life span

STANDARDS AND CERTIFICATIONS

International standards and Cyber Security programs are based on global best IT practices and technologies for the development and integration of secure and CRITIS-compliant systems.

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

IEC 62443 CERTIFICATION - ADVANTAGES

- Wide range of applications for cyber security of industrial control systems in decentralized power generation systems covering critical infrastructures, facilities of public interest and many industrial areas
- Standardized cyber security of control systems and system solutions on an international level based on proven and new IT security concepts such as “Defense in Depth“ and “Zones & Conduits“
- Certification as a key argument for customers and as an answer to the question of how to ensure the secure introduction of Industry 4.0
- Scalability of cyber security with regards to the respectve requirements and priorities of the control system

IEC 62443 - LEVEL

In the standard, the evaluation of the effectiveness and quality of measures is differentiated by roles and levels. The following applies to Kuhse as an integrator of control systems for decentralized power generation plants:

Security Level

- “for companies that develop and implement clear cyber security objectives and effective, but cost-conscious technical countermeasures to cyber attacks“

Maturity Level

- “for companies that develop and implement their organization and documented processes according to the cyber security objectives“

IEC 62443

REGULATORY REQUIREMENTS

The process participants are classified into three essential roles:

Manufacturers (Components & Products)

- Manufacturers of
  - Control components (PLC and HMI)
  - Network components (routers and switches)
  - Security components (firewalls)

Kuhse is **your partner** for the selection of cyber security components for your compliant control system for decentralized power generation plants.

Integrators (at system-/ subsystem level)

- **System level**
  - General contractors (EPC)
  - Genset packagers
- **Subsystem level**
  - OEM engine manufacturers
  - Suppliers of the functional safety system for the power plant
  - Supplier of the electrical system for the power plant

Kuhse is **your integrator** on subsystem level for the electrical equipment of your power station from project planning to integration and maintenance (based on IEC 62443-3-3 for technical measures).

Asset Owners / Operators

- Owners of “critical infrastructures“, facilities of public interest and industrial plants for sensitive processes
  - Independent power producers
  - Utilities and power plant owners
  - Data centers
  - Hospitals
  - Culture and media
  - Supply and Logistics
  - Mobility
  - Communication

Kuhse is **your consultant** for compliant plant operation and your maintenance partner for the control systems (based on IEC 62443-2-4 for organizational and process measures).

CATALOG OF MEASURES

SPECTRUM OF TECHNICAL MEASURES FOR INTEGRATORS

Architecture & Design

DETERMINATION OF A SUITABLE NETWORK ARCHITECTURE & NEEDED NETWORK DEVICES

- Network segmentation (zones)
- Protected network interconnections (conduits)
- Limitation and encryption of data traffic
- Configuration of network and security devices

LIMITATION OF PHYSICAL ACCESS

- Support in determination, positioning and configuration of necessary security mechanisms for physical access control of buildings & rooms
- Consideration of hardware access lockings
- Implementation of door locks and access detection for control panels and switchboards

HARDENING OF SOFTWARE AND SERVICES; STRENGTHENING OF HARDWARE

- Deactivation or removal of unneeded features, modules, programs, services, unauthorized network addresses
- Deactivation or locking of unneeded physical ports

Access Management

ADMINISTRATION OF USER ACCOUNTS

- Account and access management incl.:
  - user administration for authentication using
    - password management
    - two-factor-authentication
  - use control for authorization of users, devices, apps and services

LIMITATION OF ACCESS PERMISSIONS

- for defined users (authentication)
- to defined contents (authorization)
- permission management (for users, devices, services)
  - application whitelisting

  acc. to the principle of “least privilege“
- by means of encrypted connections

REMOTE ACCESS MANAGEMENT BY

- using appropriate security mechanisms, i.e.
  - network functions (gateway, router, switch)
  - security functions (firewall)
- using secure and encrypted connections
- (digital certificates for a secure communication)

Event & Protection Management

EVENT MANAGEMENT

- Monitoring and logging of
  - accesses and access attempts
  - cyber attacks
  - network configuration changes
  - parameter changes of the control system
- Alarming of security threads and attack attempts

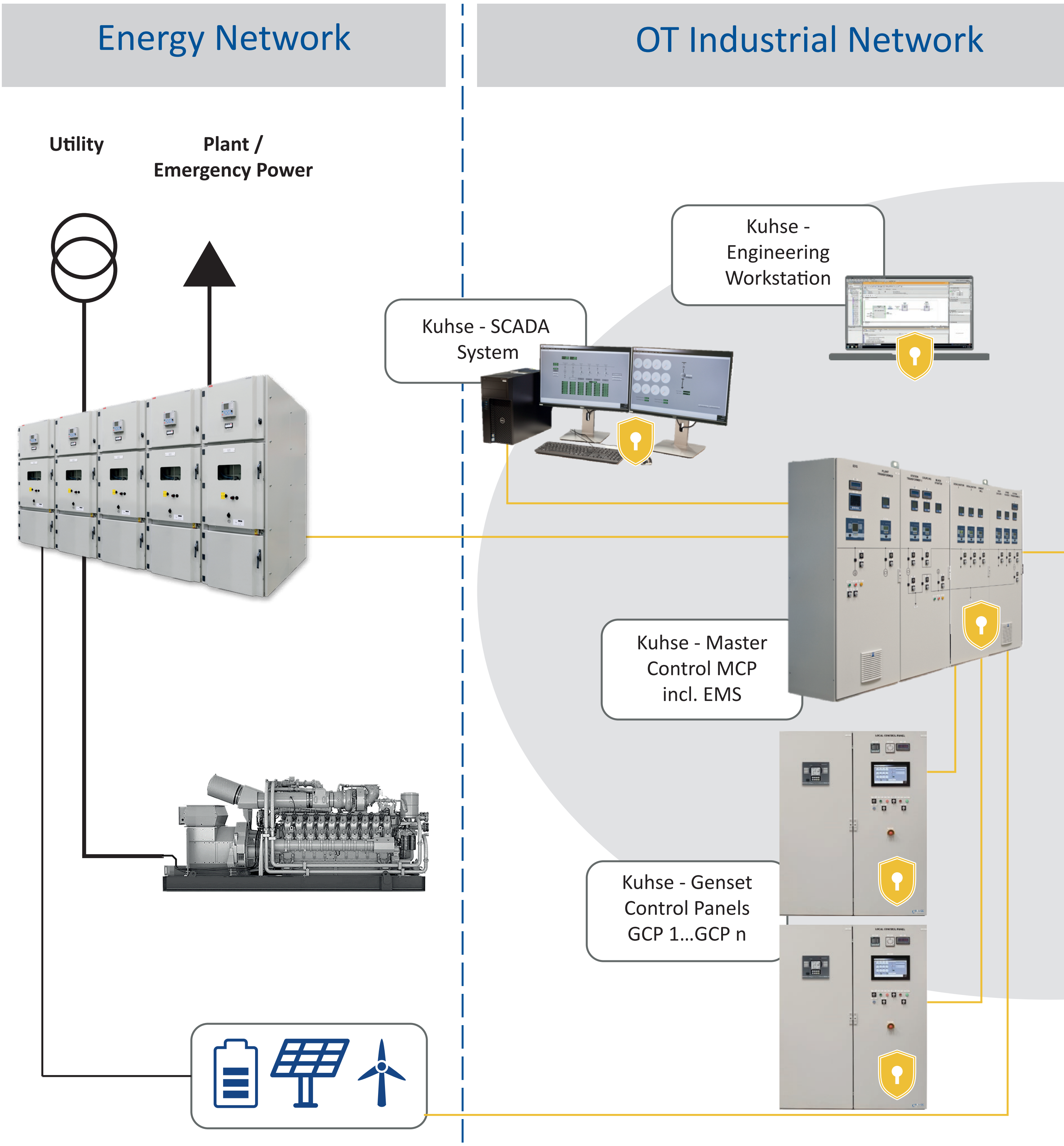
MANAGEMENT OF SECURITY TOOLS AND ANTI-MALWARE SOLUTIONS

- Patch Management
- Update of antivirus software and definition files
- Deliberate update of used whitelists

PROTECTION MECHANISMS & PROCEDURES FOR

- backup / restore
- disaster recovery

COMMUNICATION TOPOLOGY FOR POWER PLANT



Energy Network

OT Industrial Network

Utility

Plant / Emergency Power

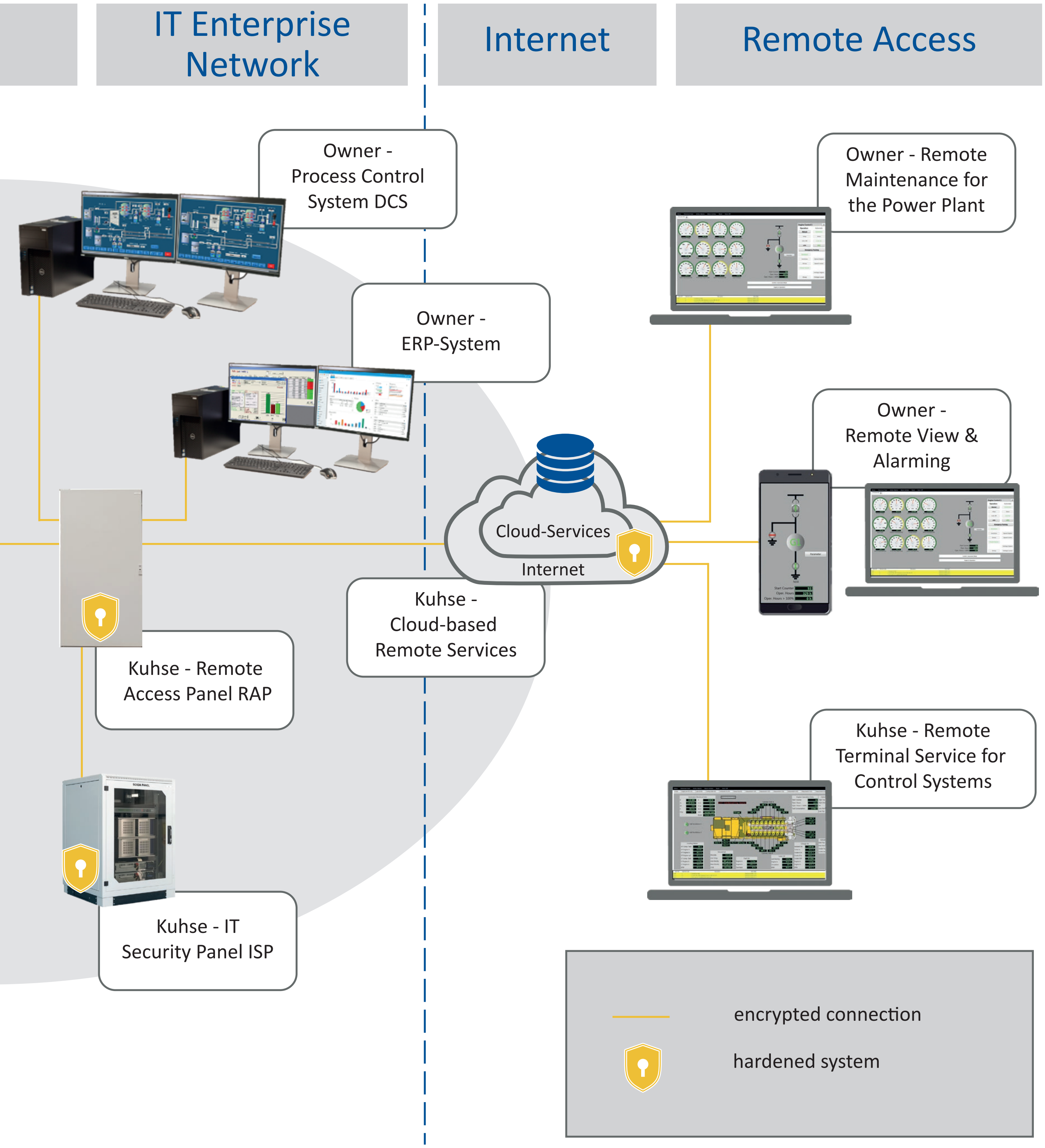
Kuhse - Engineering Workstation

Kuhse - SCADA System

Kuhse - Master Control MCP incl. EMS

Kuhse - Genset Control Panels GCP 1...GCP n

WITH INDICATED CYBER SECURITY MEASURES



IT Enterprise Network

Internet

Remote Access

Owner - Process Control System DCS

Owner - ERP-System

Kuhse - Remote Access Panel RAP

Kuhse - IT Security Panel ISP

Cloud-Services

Internet

Kuhse - Cloud-based Remote Services

Owner - Remote Maintenance for the Power Plant

Owner - Remote View & Alarming

Kuhse - Remote Terminal Service for Control Systems

encrypted connection

hardened system

KUHSE AS A SYSTEM INTEGRATOR

In the cyber security standard IEC 62443, tasks and services for the different roles are predefined.

Kuhse as a **System Provider and Integrator** of “cyber secure“ industrial control systems for decentralized power generation applications is responsible for

- the professional cyber security engineering of the control system (according to architecture and design)
- the integration of the control system into the decentralized power generation plant regarding cyber security aspects.

DUTIES ACC. TO IEC 62443 & RANGE OF SERVICES BY KUHSE

- Compliance with standards for CRITIS- related core competencies (demands on technology and organization & processes)

- Information about technical, organizational and process-related requirements based on cyber security standards regarding design & integration of the industrial control system
- Support in the context of cyber security project definition and coordination meetings with all relevant parties

- Implementation of security-related requirements
- Specification and selection of suitable component manufacturers and components for industrial control systems
- Integration of suitable components and solutions into the industrial control system
- Intrusion detection systems to be established

- Performing a vulnerability analysis and a risk assessment for the industrial control system; assistance in implementing these findings into the cyber security study of the entire power plant in close collaboration with other needed parties (e.g. IT experts of the enterprise network and the integrator of the overall power plant) in order to consider the entire network structure
- Determination, selection and specification of
  - suitable technical measures based on IEC 62443-3-3 and
  - necessary measures regarding organization and processes based on IEC 62443-2-4

- Engineering and commissioning of the cyber-secure industrial control system under consideration of additional requirements from the asset owner resp. operator or integrator of the total decentralized power generation plant

- Implementation of relevant cyber security measures from project planning to commissioning of the industrial control system
  - based on IEC 62443-3-3 for technical affairs and
  - based on IEC 62443-2-4 for organizational and process-related affairs.
- Taking-over of the industrial control system includes:
  - process manual for operation, maintenance, incident response guideline
  - status documentation
  - “Cyber-Secure“ - certificate

KUHSE AS A SERVICE PARTNER

In the role of a **Service Partner** for integrators and asset owners resp. operators of decentralized power generation applications Kuhse takes care of

- professional extended maintenance of our industrial control systems to ensure continuously cyber- secure operation
- supporting the owner‘s service personnel in case of cyber attacks and other according violations.

DUTIES ACC. TO IEC 62443 & RANGE OF SERVICES BY KUHSE

- Compliance with standards for CRITIS- related core competencies (demands on technology and organization & processes)

- Information about technical, organizational and process-related requirements based on cyber security standards regarding maintenance of industrial control systems
- Support in the context of cyber security maintenance requirements and in coordination meetings with all relevant parties

- Maintenance of security-related requirements
- Maintenance of intrusion detection and protection systems including patching
- Maintenance of backup / restore and recovery measures

- Review of implemented security-related measures
- Review of effectiveness and up-to-dateness of intrusion detection & protection systems
- Review of backup and recovery procedures

- Maintenance of the cyber-secure industrial control system under consideration of additional requirements from the asset owner resp. operator or integrator of the total decentralized power generation plant
- Support for maintaining the cyber-secure operation of the industrial control system

- In the course of a maintenance contract we ensure a regular “Cyber Secure“ review based on IEC 62443-3-3 and IEC 62443-2-4 (national requirements to be considered; e.g.: bi-yearly burden of proof for “CRITIS“ enterprises in Germany acc. to §8A BSIG)
- Take-over of status documentation, updated maintenance manual (if applicable) and “Cyber-Secure-Update“ certificate for successfully performed maintenance services
- Training of the owner‘s operators and service personnel
- Providing remote support in case of cyber attacks, violations and alarms from the intrusion detection system

KUHSE AS A CONSULTANT

As a **Consultant** for integrators and asset owners resp. operators of decentralized power generation applications Kuhse supports through

- the introduction of the technical and organizational cyber security standards
- the determination and implementation of necessary technical and organizational measures

DUTIES OF INTEGRATORS / OWNERS &

RANGE OF SERVICES BY KUHSE

- Compliance with standards for CRITIS- related core competencies (demands on technology and organization & processes)

- Information about technical, organizational and process-related requirements based on cyber security standards
- Support in the context of cyber security requirements specification and in coordination meetings with all relevant parties

- Determination of security-relevant requirements
- Specification of suitable components and cyber-secure industrial control systems
- Selection of appropriate manufacturers and integrators
- Integration of suitable components and solutions into the industrial control system
- Intrusion detection systems to be established

- Support with vulnerability analyses and a risk assessments for industrial control systems; collaboration with the IT department of the operator or the integrator of the decentralized power generation system
- Determination, selection and specification of suitable technical measures based on IEC 62443-3-3 as well as needed adaptations of the operator‘s or integrator‘s organization and processes based on IEC 62443-2-4
- Assist with the implementation of an information security management system (ISMS) based on IEC 62443-2-1/2-2

- for integrators:
  Planning, Integration and Maintenance requirement for secure decentralized power generation plants
- for operators:
  Use and Operation requirements for industrial control systems

- Determination of necessary cyber security measures for the maintenance, operation and integration of the industrial control system into the decentralized power generation plant incl. preparation of the process manual and status documentation
- Option: support with certification preparation regarding organization and processes based on IEC 62443-2-4 and the industrial control system based on IEC 62443-3-3

KUHSE CYBER SECURITY SOLUTIONS

KUHSE CYBER SECURITY PREMIUM PACKAGE

for Power Generation Plants with **extended** cyber security requirements

TECHNICAL MEASURES

- Network architecture & enhanced network security by means of suitable segmentation
- 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)
- 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 security devices, relevant control system components and implemented security tools (after verification) (patching, anti-malware, application whitelisting, digital certificates)

KUHSE CYBER SECURITY BASIC PACKAGE

for Power Generation Plants with **basic** cyber security requirements

TECHNICAL MEASURES

- Network architecture & basic network security by means of suitable segmentation
- 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 network & security devices, relevant control system & maintenance devices
- Logging of logins and login attempts
- System backup after delivery and commissioning

SERVICE MEASURES

- Process manual for operation and maintenance
- Regular manual updates of security mechanisms (as an option)
- Regular check of effectiveness of the security measures (as an option)
- Training of the owner's operators and service personnel (as an option)

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 in power plants for decentralized energy generation as a partner of renowned engine manufacturers
- 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
Jörg Delbos
Ohepark 2
21224 Rosengarten
Tel. +49 4171 798-162
j.delbos@kuhse.de
www.kuhse-energy.com