KUHSE
POWER SOLUTIONS

CYBER SECURITY IN KRITISCHEN INFRASTRUKTUREN

KRAFTWERKE
REGELKONFORM SCHÜTZEN

MOTIVATION

Cyber-Angriffe stellen eine große Herausforderung für die Betriebssicherheit von dezentralen Energieerzeugungsanlagen in kritischen Infrastrukturen dar. Viele Kraftwerke und Industrieanlagen sind für den Umgang mit Schadsoftware, die industrielle Automatisierungs- und Steuerungssysteme (IACS) ins Visier nimmt, nicht gerüstet.

Insbesondere SPS-, HMI- und SCADA-Systeme sind empfindliche Angriffsziele, deren Beeinträchtigung durch einen Cyber-Angriff zu einer massiven Störung oder Ausfall des gesamten Kraftwerks führen können. Neben diesen direkten Auswirkungen auf die Energieversorgung kommen oftmals noch wirtschaftliche sowie Reputationsschäden und Vertrauensverluste hinzu.

Internationale Normen und Richtlinien bieten einen Leitfaden für eine hohe Cyber Security im Anlagenbetrieb und schaffen sichere, KRITIS-konforme Umgebungen für Hersteller, Betreiber und Integratoren.

Als Spezialist für Kraftwerkssteuerungen und -systeme ist Kuhse Ihr kompetenter Partner für „cyber secure“ und KRITIS-konforme Steuerungslösungen. Ob Consulting, Produktion, Inbetriebnahme oder Service - wir bieten alle Leistungen aus einer Hand.

HERAUSFORDERUNGEN

ZUNEHMENDE KOMPLEXITÄT IM BEREICH DER IT-SICHERHEIT DURCH

- Digitalisierung der Industrial Automation & Control Systems (IACS), zu denen auch die Steuerungssysteme der dezentralen Energieerzeugungsanlagen gehören
- schnell wachsende Technologie für Industrie 4.0
- zunehmende Vernetzung zwischen
  - Industriedatennetzen (OT) und
  - Unternehmensdatennetzen (IT)

VERNETZUNG

- Absicherung zuvor isolierter Gebiete / Schutzzonen gegen Cyber-Angriffsmöglichkeiten
- Zunehmende Anzahl von Schwachstellen in IACS Systemen, davon 20% den industriellen Energiesektor betreffend
- Umsetzung der IT-Sicherheitskonzepte auf die OT-Umgebung unter Berücksichtigung der unterschiedlichen Prioritäten:
  - IT: Daten- und Informationsschutz
  - OT: Zuverlässigkeit und Verfügbarkeit sowie langer Life Cycle

NORMEN UND ZERTIFIZIERUNG

Internationale Normen und Cyber Security Programme setzen auf weltweit bewährte Verfahren für die Entwicklung und Integration von sicheren und KRITIS-konformen Systemen.

EU CYBER SECURITY ACT:

Aufbau einer sicheren, Cyber Security-konformen Umgebung (Hersteller, Integratoren und Betreiber) für Produkte und Systeme der Industrie 4.0

IEC 62443:

Internationale Normenreihe für Cyber Security von industriellen Automatisierungs- und Steuerungssystemen (IACS), Regelwerk und Leitfaden für eine verbindliche Sicherheit in Industriedatennetzen (OT) - Umgebungen

IT-SICHERHEITSGESETZ 2.0:

Gesetz zur Erhöhung der Sicherheit von Unternehmensdatennetzen (IT)-Systemen zum Schutz der Bundesverwaltung, kritischer Infrastrukturen und Unternehmen öffentlichen Interesses

IEC 62443 ZERTIFIZIERUNG - VORTEILE

- Anwendungsbereich für Cyber Security von Steuerungssystemen für dezentrale Energieerzeugungsanlagen umfasst kritische Infrastrukturen, Anlagen öffentlichen Interesses und Industriesektoren
- Standardisierte Cyber Security von Steuerungen und Systemlösungen auf internationaler Ebene und auf Basis bewährter sowie neuer IT-Sicherheitskonzepte wie z.B. „Defense in Depth“ und „Zones & Conduits“
- Zertifizierung als Schlüsselargument für Kunden und als Antwort auf die Frage nach der Gewährleistung einer sicheren Einführung von Industrie 4.0
- Skalierbarkeit der Cyber Security hinsichtlich der Anforderungen und Prioritäten des Steuerungssystems

IEC 62443 - LEVEL

In der Norm erfolgt die Bewertung der Wirksamkeit und Güte der Maßnahmen differenziert durch Rollen und Level.

Für Kuhse als Integrator von Steuerungssystemen für dezentrale Energieerzeugungsanlagen gelten:

Sicherheitslevel (Security Level)

- „für Unternehmen, die in Hinblick auf Cyber Security klare Ziele und effektive, aber kostenbewusste Gegenmaßnahmen zu Cyber-Angriffen entwickeln und umsetzen“

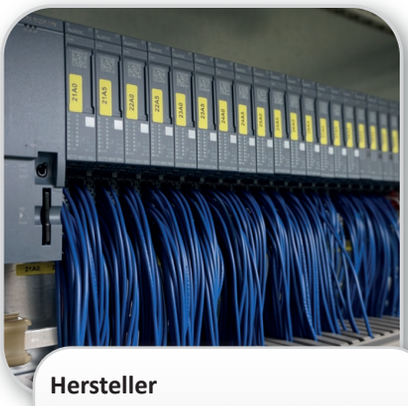
Reifegrad (Maturity Level)

- „für Unternehmen, die ihre Organisation und dokumentierten Prozesse entsprechend der Cyber Security Ziele entwickeln und implementieren“

IEC 62443

REGULATIVE ANFORDERUNGEN

Die Einteilung der Prozessbeteiligten erfolgt in drei wesentliche Rollen:



Hersteller
(Komponenten & Produkte)

- Hersteller von
- Steuerungskomponenten (SPS und HMI)
- Netzwerkkomponenten (Router und Switch)
  - Sicherheitskomponenten (Firewall)

Integratoren
(auf System-/Subsystemlevel)

- **Systemlevel**
  - Generalunternehmer (EPC = Engineering, Procurement and Construction)
  - Generator Set Packager
- **Subsystemlevel**
  - OEM-Maschinenhersteller
  - Ausrüster der funktionalen Kraftwerkssicherheit
  - Ausrüster der elektrischen Anlagen und Systeme

Betreiber

- Betreiber von „Kritischen Infrastrukturen“, Anlagen öffentlichen Interesses sowie von Industrieanlagen mit sensiblen Prozessen
  - unabhängige Stromversorger
  - EVUs und Kraftwerksbetreiber
  - Rechenzentren
  - Krankenhäuser
  - Kultur und Medien
  - Versorgung und Logistik
  - Mobilität
  - Kommunikation

Kuhse ist **Ihr Partner** bei der Auswahl der Cyber Security Komponenten für ihr regelkonformes Steuerungssystem für dezentrale Energieerzeugungsanlagen.

Kuhse ist **Ihr Integrator** auf Subsystemlevel für die elektrische Ausrüstung ihrer Energieerzeugungsanlage von der Projektierung bis zur Integration und Wartung (gemäß Technik nach IEC 62443-3-3)

Kuhse ist **Ihr Consultant** für den regelkonformen Anlagenbetrieb und Ihr Wartungspartner für die Steuerungssysteme (gemäß Prozesse und Regeln nach IEC 62443-2-4)

MAßNAHMENKATALOG

SPEKTRUM DER TECHNISCHEN MAßNAHMEN FÜR INTEGRATOREN

Architektur & Design

BESTIMMUNG DER GEEIGNETEN NETZWERK-ARCHITEKTUR UND BENÖTIGTEN NETZWERK-GERÄTE

- Netzwerk-Segmentierung
- GesicherteNetzwerk-Verbindungen
- Limitierung / Verschlüsselung des Datenverkehrs
- Konfiguration der Netzwerk- und Sicherheitsgeräte

LIMITIERUNG DER ZUGANGS-MÖGLICHKEITEN

- Unterstützung bei der Festlegung, Platzierung und Konfiguration benötigter Sicherheitsmechanismen zur Zugangskontrolle und Zugangserkennung von Gebäuden / Räumen
- Vorsehen von Schaltschrankschlössern und Schaltschrankzugangserfassung

HÄRTUNG VON SYSTEMEN (INKL. HARDWARE, SOFTWARE, DIENSTE)

- Deaktivieren bzw. Entfernen nicht benötigter Funktionen, Module und Services sowie nicht-autorisierter Netzwerkadressen
- Deaktivieren bzw. Verriegeln nicht benötigter physikalischer Ports

Access Management

ADMINISTRATION VON BENUTZERKONTEN

- Benutzerkonten- und Zugangsverwaltung inklusive
  - Benutzerverwaltung zur Authentifizierung
    - Passwort Management
    - Zwei-Faktor-Authentifzierung
  - Nutzungskontrolle zur Autorisierung von Benutzern, Geräten, Apps und Diensten

LIMITIERUNG DER ZUGRIFFSBERECHTIGUNGEN

- für definierte Benutzer (Authentifizierung)
- auf definierte Inhalte (Autorisierung)
  - Rechteverwaltung (Benutzer, Geräte, Dienste)
  - Whitelisting

  nach dem Prinzip der minimalen Rechtevergabe
- durch verschlüsselte Verbindungen

FERNZUGRIFFSMANAGEMENT (FÜR KUNDEN FERNWARTUNG UND KUHSE SERVICE) ÜBER

- Schutzmechanismen, d.h.
  - Netzwerkfunktionen (Gateway, Router, Switch)
  - Sicherheitsfunktionen (Firewall)
- gesicherte und verschlüsselte Verbindungen mit digitalen Zertifikaten für sichere Kommunikation

Event & Protection Management

EVENT MANAGEMENT

- Überwachen und Loggen von
  - Zugriffen bzw. Zugriffsversuchen
  - Cyber Attacken
  - Änderung der Netzwerk-Konfiguration
  - Änderung der Anlagenparameter
- Melden von versuchten Attacken und Verstößen

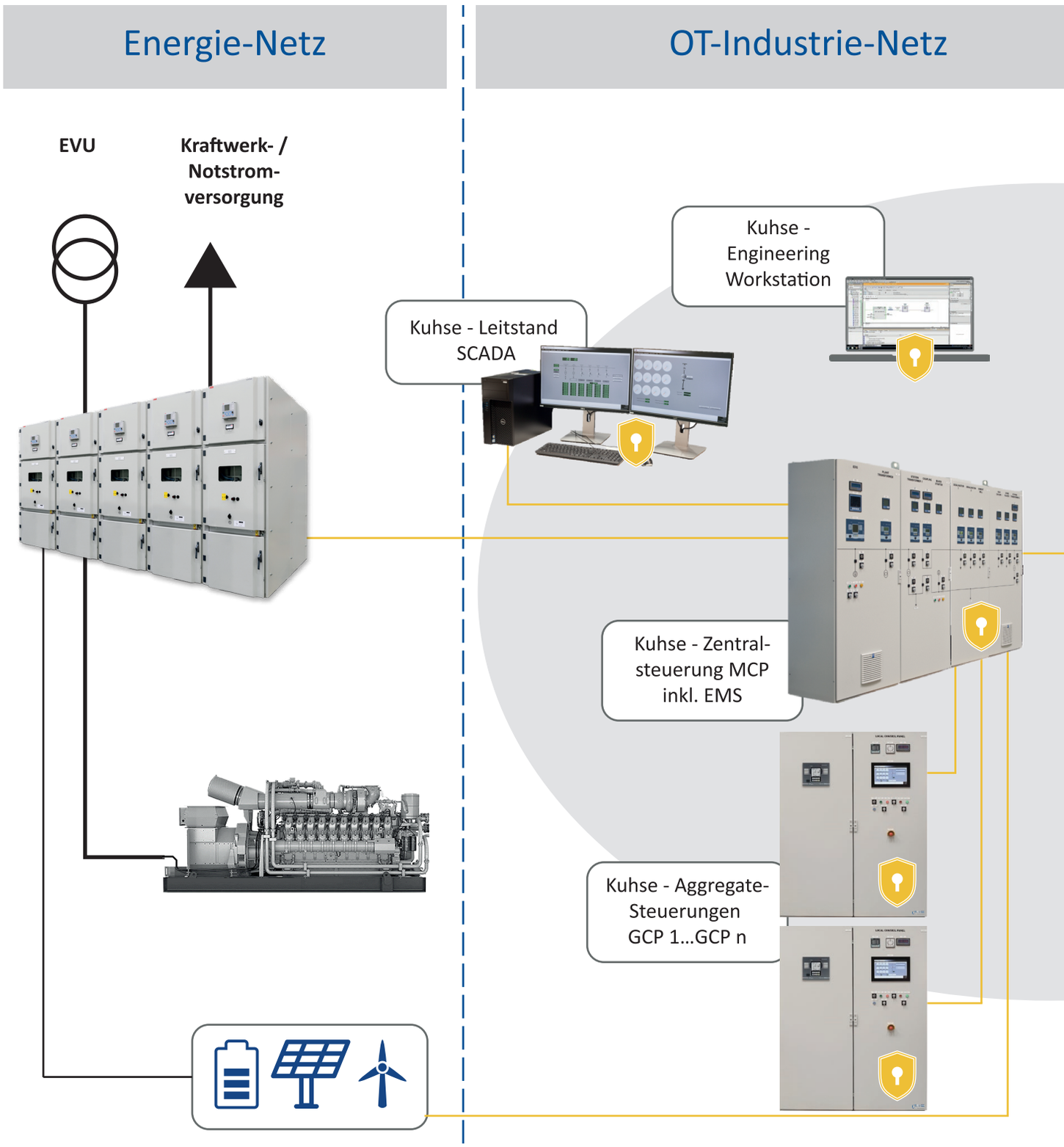
MANAGEMENT VON SICHERHEITS-TOOLS UND ANTI-SCHADPROGRAMMEN

- Patch Management
- Update der Anti-Malware-Programme und Definitionsdateien
- Whitelist - Aktualisierung

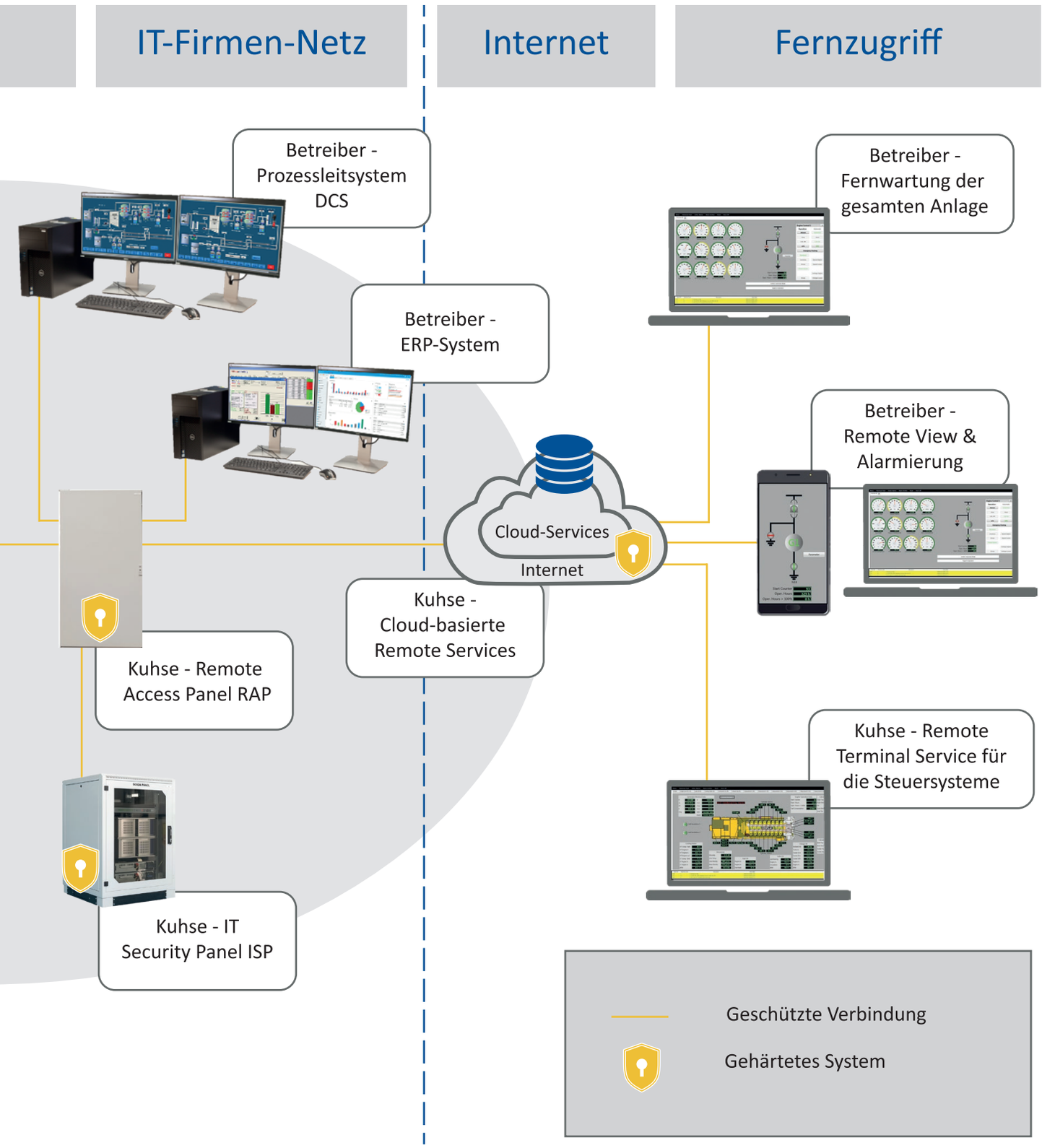
SCHUTZMECHANISMEN UND -PROZESSE FÜR

- Datensicherung und Datenwiederherstellung
- Notfallwiederherstellung

SYSTEMTOPOLOGIE FÜR KRAFTWERKE MIT CYBER



SECURITY MAßNAHMEN



KUHSE ALS SYSTEMINTEGRATOR

In der Cyber Security Norm IEC 62443 sind Aufgaben- und Leistungspakete für die unterschiedlichen Rollen vordefiniert.

Als **Systemlieferant und Systemintegrator** von „cyber securen“ industriellen Steuerungen für dezentrale Energieerzeugungsanlagen ist Kuhse verantwortlich für

- die fachgerechte Cyber Security - Auslegung des Steuerungssystems (gemäß Architektur und Design)
- die Integration des Steuerungssystems in die dezentrale Energieerzeugungsanlage gemäß Cyber Security - Gesichtspunkten.

AUFGABEN GEMÄß IEC 62443 & LEISTUNGEN SEITENS KUHSE

AUFGABEN GEMÄß IEC 62443	LEISTUNGEN SEITENS KUHSE
■ Einhaltung von Mindeststandards für KRITIS-Kernkompetenzen (Anforderung an Technik sowie Organisation und Prozesse)	■ Information über technische und organisatorische Anforderungen der Cyber Security Normen in Bezug auf die Auslegung und Integration des industriellen Steuerungssystems ■ Unterstützung bei Cyber Security Systemanforderungs- und Abstimmungsgesprächen mit den Projektbeteiligten
■ Umsetzung sicherheitsrelevanter Anforderungen ■ Spezifizierung und Auswahl geeigneter Komponenten-Hersteller und Komponenten für industrielle Steuerungssysteme ■ Einbindung geeigneter Komponenten und Lösungen in das industrielle Steuerungssystem ■ Einrichtung von Systemen zur Angriffserkennung	■ Durchführung einer Schwachstellenanalyse und Risikobewertung für das industrielle Steuerungssystem; Unterstützung bei der Implementierung dieser Ergebnisse in die übergeordnete Cyber Security Studie des Betreibers in enger Zusammenarbeit mit den jeweils benötigten Parteien (z.B. IT-Experte des Betreibers, Integrator der gesamten dezentralen Energieerzeugungsanlage) ■ Bestimmung, Auswahl und Spezifizierung geeigneter technischer Maßnahmen nach IEC 62443-3-3 sowie notwendiger Anpassungen von Maßnahmen bezüglich der Organisation und der Prozesse nach IEC 62443-2-4

■ Projektierung und Inbetriebnahme des sicheren industriellen Steuerungssystems unter Berücksichtigung der Anforderungen des Betreibers bzw. des Generalunternehmers / Integrators der dezentralen Energieerzeugungsanlage	■ Umsetzung der notwendigen Cyber Security Maßnahmen von der Projektierung bis zur Inbetriebnahme des Steuerungssystems,
	  ■ nach IEC 62443-3-3 bezüglich Technik
	  ■ nach IEC 62443-2-4 bezüglich Organisation und Prozesse sowie
	■ Bei der Übergabe des Steuerungssystems werden zusätzlich überreicht:
	  ■ Prozesshandbuch für Betrieb und Wartung
	  ■ Statusdokumentation
	  ■ „Cyber-Secure“ - Zertifikat

KUHSE ALS SERVICEPARTNER

In der Rolle als **Service-Partner** für Integratoren und Betreiber von dezentralen Energieerzeugungsanlagen kümmert sich Kuhse um

- die fachgerechte erweiterte Wartung des industriellen Steuerungssystems zur Aufrechterhaltung des Schutzes gemäß Cyber Security - Gesichtspunkten
- die Unterstützung des Service-Personals des Betreibers bei Cyber-Angriffen und Verstößen.

AUFGABEN GEMÄß IEC 62443 & LEISTUNGEN SEITENS KUHSE

AUFGABEN GEMÄß IEC 62443	LEISTUNGEN SEITENS KUHSE
▪ Einhaltung von Mindeststandards für KRITIS-Kernkompetenzen (Anforderung an Technik sowie Organisation und Prozesse)	▪ Information über technische und organisatorische Anforderungen der Cyber Security Normen in Bezug auf die Wartung von industriellen Steuerungssystemen ▪ Unterstützung bei Cyber Security Wartungsanforderungs- und Abstimmungsgesprächen für die Steuerung der dezentralen Energieerzeugung mit den Projektbeteiligten
▪ Wartung der sicherheitsrelevanten Maßnahmen ▪ Wartung von Systemen zur Angriffserkennung und Angriffsvermeidung inklusive Patching ▪ Wartung von Back-Up / Wiederherstellungsmaßnahmen	▪ Überprüfung der umgesetzten sicherheitsrelevanten Maßnahmen ▪ Überprüfung der Wirksamkeit und Aktualität von Systemen zur Angriffserkennung ▪ Überprüfung von Back-Up- und Wiederherstellungsprozeduren
▪ Wartung des sicheren Steuerungssystems unter Berücksichtigung der Anforderungen des Betreibers bzw. des Integrators der gesamten dezentralen Energieerzeugungsanlage ▪ Support zur Aufrechterhaltung des sicheren Betriebs des Steuerungssystems	▪ Im Zuge eines Wartungsvertrages gewährleisten wir turnusmäßig die „Cyber Secure“ - Überprüfung des Steuerungssystems auf Basis von IEC 62443-3-3 und IEC 62443-2-4 (Nachweispflicht für KRITIS-Betreiber nach §8A BSIG alle 2 Jahre) ▪ Übergabe der Statusdokumentation, des aktualisierten Wartungshandbuchs und des „Cyber-Secure-Update“ Zertifikats über die erfolgreich durchgeführte Wartung ▪ Schulung des kundenseitigen Bedien- und Servicepersonals ▪ Sicherstellung des Remote Supports bei erfolgten Angriffen, Verstößen und Warnungen des Sicherheitssystems

KUHSE ALS CONSULTANT

Als **Consultant** für Integratoren und Betreiber von dezentralen Energieerzeugungsanlagen begleitet Kuhse

- die Einführung von technischen und organisatorischen Cyber Security Standards und
- die Bestimmung und Umsetzung notwendiger technischer und organisatorischer Maßnahmen

AUFGABEN INTEGRATOREN / BETREIBER & LEISTUNGEN SEITENS KUHSE

▪ Einhaltung von Mindeststandards für KRITIS-Kernkompetenzen (Anforderung an Technik sowie Organisation und Prozesse)	▪ Schulung über die technischen und organisatorischen Anforderungen der Cyber Security Normen ▪ Unterstützung bei Cyber Security Anforderungs- und Abstimmungsgesprächen mit den Projektbeteiligten
▪ Bestimmung sicherheitsrelevanter Anforderungen ▪ Spezifizierung geeigneter Komponenten und sicherer industrieller Steuerungssysteme ▪ Auswahl geeigneter Hersteller und Integratoren ▪ Einsatz geeigneter Komponenten und sicherer industrieller Steuerungssysteme ▪ Einrichtung und Wartung von Systemen zur Angriffserkennung	▪ Unterstützung bei der Schwachstellenanalyse und Risikobewertung in enger Zusammenarbeit mit der IT-Abteilung des Betreibers bzw. des Integrators der dezentralen Energieerzeugungsanlage ▪ Bestimmung, Auswahl und Spezifizierung geeigneter technischer Maßnahmen nach IEC 62443-3-3 und Maßnahmen bezüglich Organisation und Prozesse des Betreibers bzw. Integrators nach IEC 62443-2-4 ▪ Unterstützung bei der Umsetzung eines Cyber Security Managementsystems auf Basis von IEC 62443-2-1/2-2
▪ für Integratoren: Anforderungen an die entsprechende Planung, Integration und Wartung sicherer dezentraler Energieerzeugungsanlagen ▪ für Betreiber: Anforderungen an die entsprechende Nutzung und den Betrieb der industriellen Steuerungssysteme	▪ Bestimmung der notwendigen Cyber Security Maßnahmen für die Integration bzw. den Betrieb und Wartung des Steuerungssystems der dezentralen Energieerzeugungsanlage inkl. der Erstellung des Prozesshandbuches und der Statusdokumentation ▪ Optional: Unterstützung bei der Zertifizierungsvorbereitung bezüglich Organisation und Prozesse nach IEC 62443-2-4 und des Steuerungssystems nach IEC 62443-3-3

KUHSE CYBER SECURITY LÖSUNGEN

KUHSE CYBER SECURITY PREMIUM PAKET

für Kraftwerke mit **erhöhten** Cyber Security Anforderungen

TECHNISCHE MAßNAHMEN

- Netzwerk-Architektur und erhöhte Netzwerk-Sicherheit mittels geeigneter Segmentierung
- Zentrales Management von Benutzer-Konten, Zugriffs- und Nutzungsrechten
- Benutzerauthentifizierung mittels Zwei-Faktor-Authentifizierung
- Minimierung der Zugangs- und Zugriffsmöglichkeiten und somit der potentiellen Angriffsstellen
- Härtung des Systems (Hardware, Software, Dienste)
- Loggen von Anmelde-, Angriffsversuchen und Verstößen
- Datensicherung/-wiederherstellung, Notfallplan

SERVICE MAßNAHMEN

- Prozesshandbuch für Betrieb und Wartung sowie den Umgang mit Cyber-Angriffen
- Schulung des kundenseitigen Bedien- und Servicepersonals
- Wiederholungsprüfungen zur Sicherstellung der Wirksamkeit der technischen Maßnahmen und umgesetzten Prozesse
- Aktualisierung von Netzwerk- und Sicherheitsgeräten, relevanten Anlagenkomponenten sowie der eingesetzten Sicherheitstools (Patching, Anti-Malware, Application Whitelisting, digitale Zertifikate)

KUHSE CYBER SECURITY BASIS PAKET

für Kraftwerke mit **elementaren** Cyber Security Anforderungen

TECHNISCHE MAßNAHMEN

- Netzwerk-Architektur und Basis-Netzwerk-Sicherheit mittels entsprechender Netzwerkgeräte
- Management von Benutzer-Gruppenkonten, Zugriffs- und Nutzungsrechten
- Benutzerauthentifizierung mittels Zwei-Faktor-Authentifizierung
- Begrenzung der Zugangs- und Zugriffsmöglichkeiten und somit der potentiellen Angriffsstellen
- Härtung der Netzwerk- und Sicherheitsgeräte sowie relevanten Steuerungskomponenten
- Loggen von Anmeldungen und Anmeldeversuchen
- System-Datensicherung nach Auslieferung und Inbetriebnahme

SERVICE MAßNAHMEN

- Prozesshandbuch für Betrieb und Wartung
- Regelmäßige manuelle Aktualisierung der Sicherheitsmechanismen (optional)
- Regelmäßige Überprüfung der Wirksamkeit der Sicherheitsmaßnahmen (optional)
- Schulung des kundenseitigen Bedien- und Servicepersonals (optional)

KUHSE CYBER SECURITY LEISTUNGEN

SYSTEME (CYBER SECURE BASIEREND AUF IEC 62443)

- Steuerungen / Schaltanlagen für Prime Power Anlagen
- Steuerungen / Schaltanlagen für Netzersatzanlagen (NEA)
- Steuerungen / Schaltanlagen für Hybrid Power Anlagen

SERVICE

- Gesicherte Inbetriebsetzung und Wartung des Systems
- Schulung des Bedien- und Wartungspersonals
- Überprüfung der Wirksamkeit und Aktualität der Cyber Security Maßnahmen
- Durchführung von Sicherheitsupdates
- Remote Support bei Cyber-Attacken

CONSULTING

- Schulung Cyber Security Normen
- Evaluierung notwendiger technischer Maßnahmen und Prozesse
- Festlegung geeigneter technischer Maßnahmen und Prozesse
- Prozesshandbuch für Integration, Betrieb, Wartung, Backup/Restore, Notfallwiederherstellung des Systems und für den Umgang mit Cyber-Attacken

WARUM SIE SICH FÜR KUHSE ENTSCHEIDEN

- langjährige Erfahrung mit Steuerungssystemen in Kraftwerken zur dezentralen Energieerzeugung als Partner von renommierten Motorenherstellern
- umfangreiches Know-How über komplexe Steuerungsprozesse im Gesamtanlagenzusammenhang
- Unterstützung von Anlagenbetreibern und Integratoren in allen Phasen des Anlagen-Lebenszyklus
- alle Leistungen - von der Beratung bis zur Inbetriebnahme und Wartung - aus einer Hand

KONTAKT

Kuhse Power Solutions GmbH
Jörg Delbos
Ohepark 2
21224 Rosengarten
Tel. +49 4171 798-162
j.delbos@kuhse.de
www.kuhse-energy.com