GE
Grid Solutions

CyberSentry

Umspannwerk-Cybersicherheit

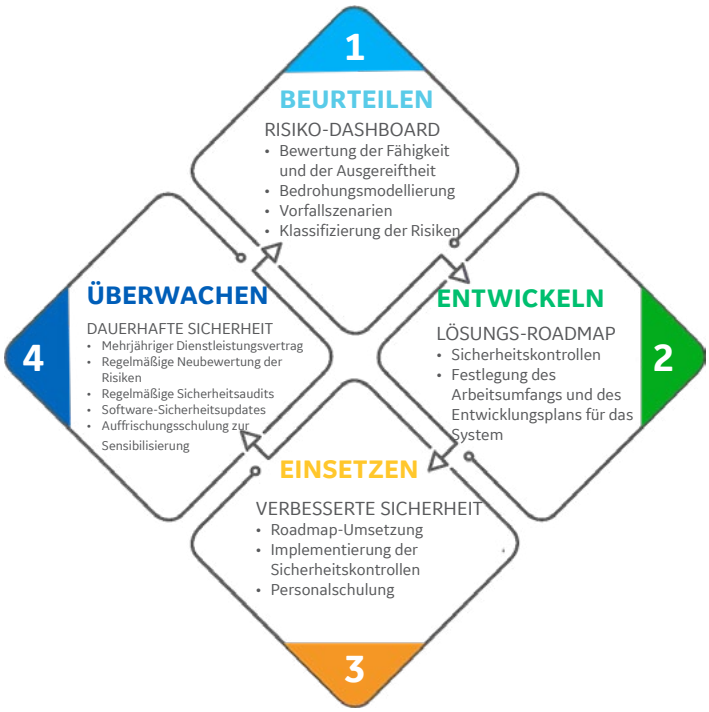
Mit der zunehmenden Digitalisierung von Umspannwerken müssen verschiedene Aspekte der Systeme und Netzwerke überdacht werden, darunter auch die Cybersicherheit. Die CyberSentry*-Lösung von GE wurde speziell entwickelt, um diesem neuen und immer wichtiger werdenden Bedarf gerecht zu werden, und zwar nicht nur, um das erforderliche Maß an Datenschutz zu gewährleisten, sondern auch, um die Einhaltung gesetzlicher Vorschriften zu gewährleisten.

In Übereinstimmung mit den neuesten NERC*-, NIS*-, IEC*- und IEEE*-Richtlinien zur Cybersicherheit setzt die CyberSentry-Lösung von GE auf eine mehrschichtige Strategie der tief gestaffelten Verteidigung (Defense-in-Depth) um die mit Cyberangriffen verbundenen Risiken zu mindern. Dadurch und indem sie als integrierter Bestandteil des gesicherten IT-Systems des Kunden funktionieren, können die IEDs und Umspannwerkleitsysteme von GE Cybersicherheit bieten.

Das CyberSentry-Angebot von GE Grid Solutions umfasst 3 sich ergänzende Aspekte:

- Produkte werden mit den installierten, konfigurierten und getesteten Möglichkeiten von CyberSentry Core Protection geliefert, die alle notwendigen Funktionen für ein eigenständiges gehärtetes System bieten.
- Darüber hinaus bietet CyberSentry Advanced Security die zentrale Verwaltung von Cybersicherheitskomponenten, entweder auf Umspannwerkebene oder integriert in ein größeres System, und ermöglicht einen sicheren Fernzugriff und die Netzwerküberwachung.
- CyberSentry Security Services stehen jederzeit zur Verfügung, um Kunden von der ersten Sicherheitsbeurteilung über die Festlegung der Sicherheits-Roadmap bis hin zur Bereitstellung und langfristigen Sicherheitswartung zu begleiten und zu unterstützen.

Außerdem sind wir stolz darauf, dass unsere Komplettlösung nach der internationalen Cybersicherheitsnorm IEC 62443 bewertet und zertifiziert wurde. Dies gibt unseren Kunden die Gewissheit, dass sie mit äußerster Sorgfalt entwickelt wurde.



Mehrschichtige Sicherheit

- Sicherheit durch Entwurf
- Netzwerksicherheit
- Host-Härtung
- Schutz vor Schadsoftware
- Authentifizierung
- Protokollierung von Sicherheitsereignissen

Sicherheitsdienste

- Risikobewertung, Audit
- Anwenderschulung
- System-Upgrades
- Beratung
- Sicherheitsupdates

Internationale Normen

- Zertifiziert nach IEC62443-2-4
- Zertifiziert nach IEC62443-3-3
- Zertifiziert nach IEC62443-4-1

Anwendungen

- Energieerzeugung
- Übertragung und Verteilung
- Öl und Gas, Petrochemie
- Industriekunden
- Datenzentren

CyberSentry™ Core Protection

GE-Produkte, insbesondere solche mit dem CyberSentry-Logo, verfügen über eine Reihe von Sicherheitsmerkmalen, die im Folgenden beschrieben werden.

Host-Sicherheit

Gerätehärtung

Ziel der Härtung ist die Verbesserung der Sicherheit. Dies geschieht durch die Reduzierung der Möglichkeiten, mit der eine Bedrohung das Betriebssystem, auf dem die Software der Lösung installiert ist, stören oder kontrollieren kann.

Netzwerkdienste, Kommunikationsanschlüsse und Benutzer, die nicht unbedingt notwendig sind, werden deaktiviert.

Richtlinien für Audits, Passwörter, Benutzerkontosperren und Sitzungszeitabschaltungen werden festgelegt.

Host-Firewalls sind so konfiguriert, dass sie nur die erforderlichen Kommunikationsflüsse zwischen autorisierten Geräten zulassen.

Schutz vor Schadsoftware

Die Ausführung von Schadsoftware (z. B. Viren, Ransomware und Spyware), die Daten und Systeme erheblich schädigen oder sich unbefugt Zugang zu einem Netzwerk verschaffen könnte, wird verhindert. Eine Positivliste von Anwendungen (Whitelisting) wird verwendet, um die Integrität und Glaubwürdigkeit von Binärdateien zu gewährleisten und die Ausführung unbekannter Schadsoftware wirksam zu blockieren.

Für Scans nach Bedarf ist ein Anti-Viren-Scanner installiert.

Sichere Kommunikation

Verschlüsselte Kommunikation verhindert das Abhören. Konfigurations- und Wartungsprotokolle werden entweder mit TLS oder SSH gesichert.

Sicherheit von Anwendungen

Authentifizierung und Autorisierung

Um mit einem IED interagieren zu können, müssen sich alle Benutzer authentifizieren. Jeder Benutzer hat sein individuelles Konto und Passwort (keine gemeinsamen Konten). Jedem Benutzerkonto werden eine oder mehrere Rollen zugewiesen (RBAC).

Es gibt keine Hintertüren oder fest kodierte Benutzerkonten. Sämtliche Passwörter werden sicher gespeichert, um zu gewährleisten, dass keine Klartextpasswörter aus dem System extrahiert werden können.

Integrität der Software

Die gesamte Soft- und Firmware von GE ist digital signiert, um die Authentizität und Integrität zum Zeitpunkt der Installation zu gewährleisten.

Protokollierung von Sicherheitsereignissen

Sämtliche grundlegenden Sicherheitsereignisse werden auf jedem Gerät protokolliert. Die Protokolle enthalten den Benutzernamen, die IP-Adresse des Absenders, den Zeitstempel und die Beschreibung der jeweiligen Handlung. Es werden keine sensiblen Informationen (z. B. Passwörter) protokolliert.

Zertifizierung nach IEC 62443-4-1 – Lebenszyklus für eine sichere Produktentwicklung (Secure Development Lifecycle (SDL)

Die IEC-Norm 62443-4-1 legt die Prozessanforderungen für die Entwicklung von sicheren Produkten fest, die in industriellen Automatisierungs- und Steuerungssystemen eingesetzt werden. Unsere Zertifizierung nach dieser Norm bedeutet, dass unsere Produkte nach einem zertifizierten Lebenszyklus für eine sichere Produktentwicklung entwickelt werden. Dadurch wird sichergestellt, dass die Produkte unter der Aufsicht eines Leiters für Produktsicherheit nach den höchsten Cybersicherheitsstandards entworfen, implementiert und getestet werden.

CyberSentry™ Advanced Security

Die Schutz-, Automatisierungs- und Steuerungslösungen von GE können vollständig in eine zentralisierte Sicherheitsinfrastruktur integriert werden. Eine hochmoderne Netztopologie mit geeigneter Zoneneinteilung und Fernzugriffssicherheit vervollständigt die Defence-in-Depth-Strategie.

Netzwerksicherheit

Netzwerktrennung

Der allgemeine Schutz wird durch eine Firewall gewährleistet, die standardmäßig die gesamte Kommunikation verweigert und nur vorgegebene Kommunikationsprotokolle zwischen bestimmten Zonen zulässt.

Netzwerk-Angrifferkennungssystem (Network Intrusion Detection System, NIDS)

Das Netzwerk-IDS ist für die Erkennung und Meldung von schädlichem Datenverkehr konfiguriert. So kann ein autorisierter Bediener bei Erkennung einer Bedrohung schnell reagieren, um die Bedrohung abzuwehren und ihre Auswirkungen zu minimieren.

Virtual Private Network

Die Kommunikation zwischen dem Umspannwerk und anderen entfernten Systemen (entfernte Leitstellen oder andere Umspannwerke) erfolgt innerhalb eines virtuellen privaten Netzwerks (VPN), d. h. in einem sicheren, verschlüsselten Punkt-zu-Punkt-Kommunikationskanal.

Fernzugriff über die Jump Box

Die Fernwartung erfolgt über eine Verbindung zu einer so genannten Jump Box (einem PC mit Ethernet-Zugang in der demilitarisierten Zone (DMZ)), von der aus auf eine begrenzte Liste von Geräten und Anwendungen in der privaten Zone zugegriffen wird. Dies ermöglicht die Steuerung des Datenverkehrs zu den IEDs des Umspannwerks.

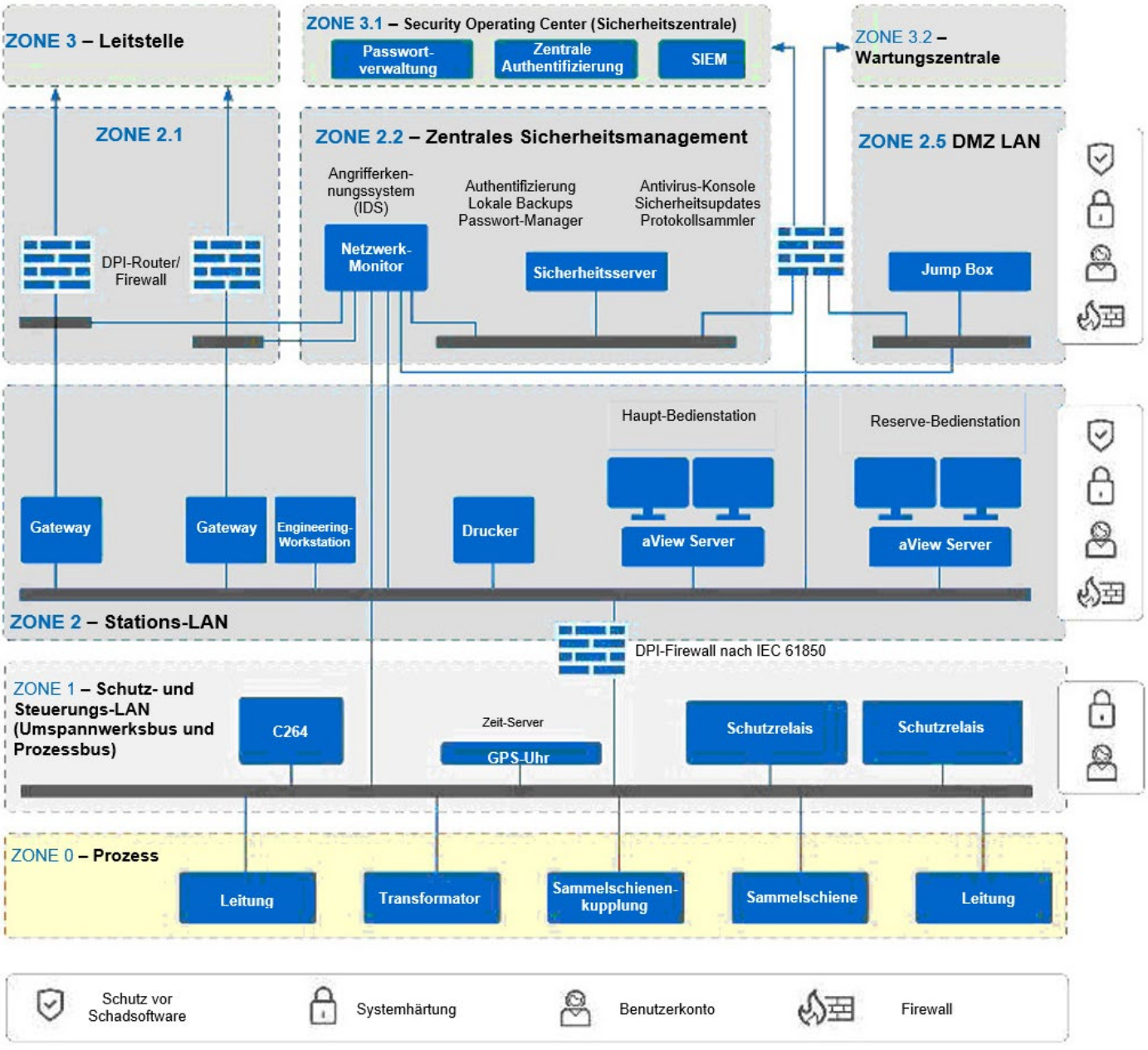
Fernzugriff – Authentifizierung

Für den Fernzugriff auf das LAN des Umspannwerks kann eine Authentifizierung gefordert werden, indem die Firewall als Proxy-Authentifizierung konfiguriert wird.

Switches

Netzwerk-Switches werden so konfiguriert, dass sie die Auswirkungen der Bedrohung durch die Verwaltung des Datenverkehrs reduzieren (Begrenzung von Broadcast-Stürmen, Dienstgüte (QoS) zur Priorisierung des IEC-61850-Datenverkehrs, VLANs zur Trennung des Datenverkehrs, MAC-Adressfilterung usw.).

Standard-Netzwerkarchitektur



Zentrales Sicherheitsmanagement

Benutzerverwaltung

Zentrale Verwaltung von Benutzerkonten, Passwörtern und Rollen über Microsoft Active Directory unter Verwendung von LDAP over TLS- und RADIUS-Protokollen

Sicherheitsprotokolle

Sammeln von Sicherheitsprotokollen an einer zentralen Stelle im Umspannwerk unter Verwendung des Syslog-Protokolls (über UDP, TCP oder TLS) und Weiterleitung der Protokolle an ein SIEM-System (Security Information Event Management).

Plan zur Sicherung und Wiederherstellung

Vorbereitung auf den Ernstfall mit einer umfassenden Strategie zur Datensicherung und Wiederherstellung sowie Lösungen zur Backup-Automatisierung unter Einbeziehung von Datensicherungsoptionen offline und online sowie am Standort und außerhalb des Standortes

Erweiterter Schutz vor Schadsoftware

Zentrale Verwaltung von Anti-Malware-Richtlinien und automatische Bereitstellung von Updates für Virendefinitionen (DAT-Dateien) (monatlich von GE getestet).

Zentrale Sicherheitsupdates

Automatische Bereitstellung von Sicherheitsupdates für Microsoft* Windows; Windows-Sicherheitsupdates werden monatlich von GE getestet

Zertifizierung nach IEC 62443-3-3 – zertifizierte Automatisierungslösung

Die IEC-Norm 62443-3-3 enthält detaillierte technische Anforderungen an Automatisierungssysteme im Zusammenhang mit den sieben in der Norm IEC 62443-1-1 beschriebenen grundlegenden Anforderungen, einschließlich der Definition der Anforderungen für erreichbare Security Levels der Automatisierungssysteme. Unsere Zertifizierung nach dieser Norm bedeutet, dass unsere Lösung über die erforderlichen Fähigkeiten für Cybersicherheit verfügt. Im Lieferumfang enthalten ist der Secure Deployment Guide, der die Installationsschritte des Systems und die bewährten Verfahren zur optimalen Nutzung seiner Sicherheit dokumentiert.

CyberSentry™ Sicherheitsdienste

GE bietet ein umfassendes Portfolio an Dienstleistungen, die unsere Kunden auf dem Weg zur Cybersicherheit unterstützen. Der Inhalt kann auf die spezifischen Kundenbedürfnisse zugeschnitten werden und einige der folgenden Punkte umfassen:

Beurteilung der Umspannwerksicherheit

- Schulungen zum Sicherheitsbewusstsein
- Beurteilung der Risiken für die Cybersicherheit von Systemen
- Verbesserung der Sicherheit ohne Prozessänderung und Minimierung der Notwendigkeit von Abschaltungen
- Upgrade-Dienste zur Nutzung der neuesten Sicherheitsfunktionen neuer Versionen
- Laufende Unterstützung zur Aufrechterhaltung der Sicherheit

Überwachung der Schwachstellen von Umspannwerken

- Monatliche Sicherheitsberichte über die Kompatibilität von Sicherheitsupdates für Microsoft Windows 10 mit der Lösung; Sicherheitsupdates werden zunächst in unserem FuE-Labor in einer repräsentativen Umgebung getestet, die das typische Leitsystem des Kunden simuliert
- Monatliche Sicherheitsmitteilungen über neu entdeckte Schwachstellen für jedes IED im Systembestand, einschließlich Schweregrad und möglicher Abhilfemaßnahmen
- Firmware-Sicherheitsupdates für GE-Produkte, mit Sicherheitsupdate-Bereitstellung vor Ort oder per Fernzugriff

Zertifizierung nach IEC 62443-3-4 – zertifizierter Integrator

Die IEC-Norm 62443-2-4 spezifiziert eine umfassende Reihe von Anforderungen an die Sicherheitsfähigkeiten von IACS-Anbietern (Industrial Automation and Control Service), die sie dem Anlagenbesitzer während der Integrations- und Wartungsaktivitäten für eine Automatisierungslösung anbieten können. Unsere Zertifizierung nach dieser Norm bedeutet, dass wir ein zertifizierter Integrator für unsere Schutz-, Automatisierungs- und Steuerungssysteme für Umspannwerke sind. Durch die Wahl von GE als Anbieter einer Komplettlösung können die Kunden Risiken während der Implementierung der Lösung vermeiden und bewältigen und so die Sicherheit ihrer Lieferkette verbessern.

CyberSentry™ Sicherheitsdienste

GE bietet ein umfassendes Portfolio an Dienstleistungen, die unsere Kunden auf dem Weg zur Cybersicherheit unterstützen. Der Inhalt kann auf die spezifischen Kundenbedürfnisse zugeschnitten werden und einige der folgenden Punkte umfassen:

Beurteilung der Umspannwerksicherheit

- Schulungen zum Sicherheitsbewusstsein
- Beurteilung der Risiken für die Cybersicherheit von Systemen
- Verbesserung der Sicherheit ohne Prozessänderung und Minimierung der Notwendigkeit von Abschaltungen
- Upgrade-Dienste zur Nutzung der neuesten Sicherheitsfunktionen neuer Versionen
- Laufende Unterstützung zur Aufrechterhaltung der Sicherheit

Überwachung der Schwachstellen von Umspannwerken

- Monatliche Sicherheitsberichte über die Kompatibilität von Sicherheitsupdates für Microsoft Windows 10 mit der Lösung; Sicherheitsupdates werden zunächst in unserem FuE-Labor in einer repräsentativen Umgebung getestet, die das typische Leitsystem des Kunden simuliert
- Monatliche Sicherheitsmitteilungen über neu entdeckte Schwachstellen für jedes IED im Systembestand, einschließlich Schweregrad und möglicher Abhilfemaßnahmen
- Firmware-Sicherheitsupdates für GE-Produkte, mit Sicherheitsupdate-Bereitstellung vor Ort oder per Fernzugriff

Zertifizierung nach IEC 62443-3-4 – zertifizierter Integrator

Die IEC-Norm 62443-2-4 spezifiziert eine umfassende Reihe von Anforderungen an die Sicherheitsfähigkeiten von IACS-Anbietern (Industrial Automation and Control Service), die sie dem Anlagenbesitzer während der Integrations- und Wartungsaktivitäten für eine Automatisierungslösung anbieten können. Unsere Zertifizierung nach dieser Norm bedeutet, dass wir ein zertifizierter Integrator für unsere Schutz-, Automatisierungs- und Steuerungssysteme für Umspannwerke sind. Durch die Wahl von GE als Anbieter einer Komplettlösung können die Kunden Risiken während der Implementierung der Lösung vermeiden und bewältigen und so die Sicherheit ihrer Lieferkette verbessern.

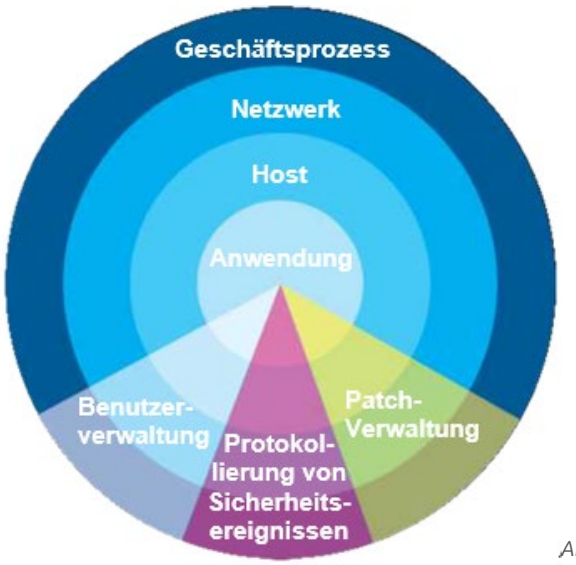


Abbildung 2: CyberSentry™ Defence-in-depth

Weitere Informationen erhalten Sie bei:
GE
Grid Solutions

Worldwide Contact Center

Web: www.GEGridSolutions.com/contact
Telefon: +44 (0) 1785 250 070

GEGridSolutions.com

GEA-33235-(GW)
German
220913