# SecurityST* für die Stromerzeugung

In einer komplexen Welt mit sich ständig ändernden Technologien erkennt GE an, dass sehr wichtig ist, einen erfahrenen Partner zu haben, der Sie erfolgreich durch die Umsetzung von Cyber-Sicherheit führt. Als ein weltweit führendes Unternehmen im Bereich industrielle Bedienelemente verfügt GE über die Fachkompetenz zur Verbesserung der Sicherheit seiner Kunden und zur Unterstützung bei der Einhaltung von Vorschriften. Wir haben bei unseren Lösungen den Schwerpunkt auf Sicherheit gelegt und sie lassen sich gut in umfassendere Systeme auf Anlagenebene und in IT-Architekturen integrieren.

SecurityST von GE ist eine zentrale Lösung für das Sicherheitsmanagement und ein wesentlicher Bestandteil von Systemen mit gestaffelten Sicherheitsebenen für Turbinen-, Anlagen- und Generatorsteuerungen. Das zentrale System verwendet modulare Abwehrdienste und -technologien und bietet einen einzelnen Ausgangspunkt, von dem aus Unternehmen ihre Vorrichtungen für die Cyber-Sicherheit betrachten können, proaktive Strategien und Regelungen zum Schutz von kritischen Steuersystemen und der dazugehörigen Netzwerke umsetzen und eine zentrale Berichtsfunktion für die Handhabung des Cyber-Risikos bieten können. Diese Lösung trägt dazu bei, Cyber-Anfälligkeiten auf Netzwerk-, Endpunkt- und Controller-Ebene zu reduzieren.

Die SecurityST Mark* VIe Solution and Commissioning Services ist nach Achilles® Practices – Bronze zertifiziert. Das bezeugt, dass die Lösung die optimalen Verfahren für eine hohe Cyber-Sicherheit einhält und zeigt dem Kunden damit auf, dass die Systeme sicher entwickelt und umgesetzt werden. Die Lösung Security ST und die dazugehörigen Serviceleistungen wurden entwickelt, um Unternehmen bei der Einhaltung der Normen und Richtlinien für die Cyber-Sicherheit wie NERC CIP, NEI 08-09 und ISA99/IEC 62443 durch die Anlagen zu unterstützen.

## Beispiele für Richtlinien für die Cyber-Sicherheit

- Das Steuersystem muss von internen und externen Bedrohungen geschützt werden
- Das Netzwerk des Steuersystems muss von anderen Netzwerken getrennt sein
- Die Zugangspunkte zum Netzwerk müssen geschützt und fortlaufend überwacht werden; potenzielle Bedrohungen protokolliert und an das zuständige Personal gemeldet werden
- Alle Anwender und Geräte müssen authentifiziert und nur mit den unbedingt erforderlichen Rechten ausgestattet werden
- Alle Geräte und Schnittstellen mit dem Steuersystem müssen nach den Normen und optimalen Verfahren der Branche verstärkt werden
- Das System ist fortlaufend auf ungewöhnliche Aktivitäten im System und bekannte Cyber-Angriff-Signaturen zu überwachen
- Validierte und genehmigte Sicherheits-Updates der Software müssen auf die Komponenten des Steuersystems angewendet werden, so bald sie verfügbar sind
- Es sind mehrere Abwehr- und Erkennungsmaßnahmen in die Lösung einzubauen
- Ausfallsicher – der Ausfall von Sicherheitsfunktionen wirkt sich nicht auf den Betrieb des Systems aus
- Umsetzung, Standort und Übertragung müssen gesichert sein
- Externe Zugangspunkte (EAPs) müssen gesichert sein

## Systeme für die Erkennung und Vermeidung von Angriffen auf Netzwerke

Diese individuelle anpassbare Option für die Netzwerksicherheit ermöglicht die Überwachung und das Blockieren von böswilligen Aktivitäten und Angriffen.

- Macht ungewöhnliche Aktivitäten und potenzielle Bedrohungen des Steuersystem-Netzwerks sichtbar
- Erfasst Datenverkehrsprotokolle und ermöglicht eine fortlaufende Netzwerkanalyse sowohl auf lokaler als auch auf Unternehmensebene
- Fortlaufend aktualisierter Schutz, der durch von GE bereitgestellten Updates der IDS/IPS-Signaturen verbessert wird, die zum Feststellen oder zum Schutz gegen bekannte Bedrohungen ausgelegt sind
- Fördert eine besser Kontrolle über OT-Anwendungsprotokolle, erzwingt Regeln für Erlauben/Verweigern im Netzwerk des Steuersystems

## Rollenbasierte Zugriffskontrolle

Diese Funktion bietet zentrale Steuerung und Warnung des Managements speziell für die Umgebung der Bedienelemente. Vereinfacht ausgedrückt: Wer hat Zugang zum industriellen Steuersystem und welche Zugangsberechtigung haben diese Personen?

**Vorteile:**

- Einfaches Einrichten mit Hilfe von vordefinierten Rollen für die Anlage, die mit den optimalen Verfahren der Branche erstellt wurden
- Reduzierung des Risikos durch Beschränkung des Zugang zur kritischen Infrastruktur
- Höhere Transparenz der Zugriffsebenen für die Anwender mit der Möglichkeit, den Zugriff sofort zu gewähren oder zu sperren, um die Anforderungen von Mitarbeitern und Dritten zu rationalisieren
- Controller mit gesichertem Zwei-Faktoren-Modus reduziert den Zugriff noch weiter und erhöht den Schutz

- Zwangsweise zentrale Passwortverwaltung ermöglicht dem Kunden die einfache Umsetzung und Verwaltung einer Passwortregelung mit einer Auswahl von voreingestellten oder vom Kunden definierten Möglichkeiten

## Management von Sicherheitsinformationen und Ereignissen

Wir bieten eine skalierbare Lösung mit der Anzeige von Cyber-Aktivitäten wie die Änderung von Switch-Konfigurationen, fehlgeschlagene Anmeldeversuche, unberechtigter Zugriff auf Ports und Nutzung von USB in Echtzeit oder historisch.

**Vorteile:**

- Eine zentrale Funktion mit einer Instrumententafel, auf der der visuelle Sicherheitsstatus und Ereignisse in Echtzeit angezeigt werden, sorgt für einen kompletten Überblick über Ihre Anlagen und warnt Sie vor potenziellen Bedrohungen
- Zeichnet Protokolle auf und speichert sie für alle Systemkomponenten, damit Sie vergangene Aktivitäten aufrufen und den Bezug zwischen einzelnen Ereignissen für Ereigniswarnungen und gesetzlich vorgeschriebene Berichte herstellen können. Die Protokolle können zur weiteren Unterstützung an das Unternehmensteam weitergeleitet werden.

## Sicherheit für den Fernzugriff

Wir wenden optimale Verfahren an, um die Sicherheit beim Fernzugriff den Anforderungen und Standards des Kunden entsprechend zu unterstützen. Unsere Lösung umfasst Optionen wie Authentifizierung mit mehreren Faktoren, Lockbox, Datendiode (in einer Richtung), VPN, Abwehr von Angriffen und schreibgeschützter Zugriff. Mit unserer Hilfe können Sie kontrollieren, wer Zugang zu Ihren kritischen Anlagen hat und zu welchen Informationen sie Zugang haben.

**Vorteile:**

- Segmentiert den Zugang mit eindeutigen Erzwingungsbereichen zwischen internen und externen Netzwerken, trägt zur Einhaltung von Vorschriften bei und verhindert den unbefugten Zugang zum Steuersystem
- Definiert und kapselt die autorisierten Benutzer und die Systeme ein, die sie an die Kundenumgebungen anbinden dürfen
- Überwacht und überprüft den Datenverkehr zwischen Unternehmen auf anomale Verhaltenweisen und erfasst die Aktivitäten des Geräts und der Anwender

## Backup und Wiederherstellen

- Automatischer, zentraler Backup und Wiederherstellung der Domain für die Prozesssteuerung spart Zeit und Geld durch Sicherstellen eines Plans zur schnellen Wiederherstellung im Notfall mit minimalen Stillstandszeiten
- Alle Backup-Aktivitäten werden protokolliert und sind für Berichte verfügbar, zur Unterstützung der Compliance-Berichterstattung

## Patch-Update-Service

Das Cyber Asset Protection-Abonnement liefert monatliche Updates für Ihre HMI, Historian-Funktionen, Switches, Firewalls, OSM und RSG. Software-Updates umfassen:

- Betriebssystem Windows®
- GE Cimplicity (ICS-CERT-spezifisch)
- Angriffserkennungs-Signaturen
- Antivirus-Signaturen
- Switch-Updates
- System 1*
- Microsoft® Excel und Microsoft® Word
- Adobe

**Vorteile:**

- Zentraler Einsatz des Aboservice von GE für Patch-Management spart 4 Stunden pro HMI, das kann bei einer typischen Anlage zu monatlichen Einsparungen von 10.000 - 20.000 US-$ führen
- Erhöht Ihre Sicherheit durch den Schutz Ihrer kritischen Anlagen vor bekannten Anfälligkeiten auf einer monatlichen Basis
- Einfach einzurichtende Updates sind kumulativ und können automatisch erfolgen oder entsprechend den Anforderungen der Anlage eingeplant werden
- Sie erhalten einen Anwendbarkeitsbericht, in dem die Kritikalität, die Zeit, die für das Update benötigt wird, ob ein Neustart erforderlich ist, definiert werden und Ihenn dadurch die Informationen liefern, die Sie für eine fundierte Entscheidung über Ihren Betrieb benötigen

## Endpunktschutz

Mit dem Endpunktschutz wird die Integrität Ihrer Daten und der Systeme, die Ihre Anlage betreiben, geschützt. Er überwacht auf böswillige Aktivitäten durch interne Zugangspunkte (USB, CD/DVD, Ethernet-Ports, etc.) und blockiert den unbefugten Zugang.

Mit der neuen Option Whitelisting von Anwendungen können auf Windows® basierende Geräte ihre Sicherheit verbessern, indem Sie die Gefahr und die Kosten durch Malware reduzieren, und die Stabilität und Zuverlässigkeit des Netzwerks verbessern. Diese Funktion identifiziert vertrauenswürdige Software, die für die Verwendung auf den HMIs des Steuersystems genehmigt ist, und verhindert die Verwendung von unbekannter oder unerwünschter Software.

## Sichere Umsetzung und Überwachungskette

Als Lieferant beginnt Sicherheit hier. Beim Aufbau und bei der Vorbereitung jedes SecurityST wird genau auf die physische und digitale Sicherheit geachtet durch de Einsatz von physischen Grenzbereichen, Zugangskontrolle mit Videoüberwachung und die sichere Übertragung der Überwachung. Unser Unternehmenssitz in Longmont, Colorado ist für die Anforderungen von Kunden aus den Bereichen Kernkraft, Öl + Gas und Stromerzeugung zertifiziert durch die genaue Einhaltung der Standards, die von NEI 08-09, NERC-CIP und IEC 62443 gefordert werden.

Für weitere Informationen wenden Sie sich bitte an:
GE Oil & Gas
Nordamerika: 1-888-943-2272; 1-540-387-8726
Lateinamerika (Brasilien): +55-11-3958-0098
Europa (Frankreich): +33-2-72-249901
Asien/China (Singapur): +65-6622 1623
Afrika/Indien/Naher Osten (VAE): +971-2-699 7119

E-Mail: ControlsConnect@ge.com
Kunden-Portal: ge-controlsconnect.com

1800 Nelson Road
Longmont, CO, USA 80501
https://www.gemeasurement.com/machinery-control



GEA31245C-DE (06/2016)