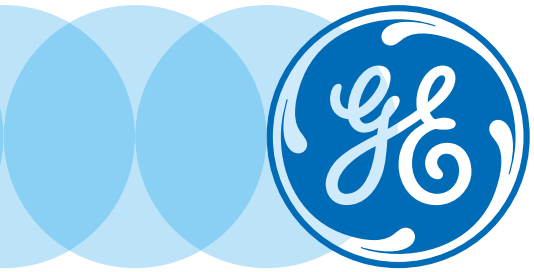
GE Oil & Gas

GEA32435A
März 2016

IEC 62443-2-4 Programm für die Cyber-Sicherheit gemäß



Cyber-Sicherheit gemäß IEC 62443-2-4

Normative Grundlage

IEC 62443-2-4 ist eine veröffentlichte internationale Norm, in der Programme zur Cyber-Sicherheit beschrieben werden, die Anbieter von industriellen Automatisierungssystemen (Industrial Automation and Control System - IACS) realisieren und anbieten können. Die Norm kann den Eigentümern von Anlagen bei der Beschaffung und beim Management von Fachkompetenz im Bereich Sicherheit für Steuersysteme behilflich sein. IEC 62443-2-4 wurde vom Technischen Komitee 65 der IEC in Zusammenarbeit mit International Instrumentation Users Association (vormals WIB) und den Mitgliedern des ISA 99 Komitees erarbeitet.

Unterstützung für IEC 62443-2-4 durch GE Oil & Gas

GE verstärkt die Systeme seiner Kunden mit einer Kombination aus technischen und verfahrenstechnischen Maßnahmen, die nach der Sicherheitsnorm IEC 62443-2-4 zertifiziert sind. Diese Normen enthalten umfassende Vorgaben von Sicherheitsanforderungen für die Installation und Wartung von industriellen Automatisierungssystemen (IACS). Dieses Whitepaper gibt einen Überblick über die Verstärkungssysteme von GE, die die Norm IEC 62443-2-4 erfüllen.

Unterstützung für ISO 27002 durch GE Oil & Gas

GE unterstützt seine Kunden dabei ISO 27002 Comliance zu erreichen. Wir verfügen über dokumentierte Prozesse und Best Practices um Unternehmen dabei zu unterstützen ihre eigenen Richtlinien zu entwickeln. Aufgrund unserer Technologien und Prozesse sind wir in der Lage ein verlässlicher Partner für 27002 Compliance zu sein.

Serviceleistungen und Lösungen für die Sicherheit

GE bietet eine Sicherheitsberatung für die Eigentümer und Betreiber von Anlagen im Öl- und Gassektor an. Wir bieten auch technische Lösungen an, die für den Bereich industrielle Bedienelemente entworfen und getestet wurden. 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. Zusammen mit Wurldtech Security Technologies bietet GE zertifizierte Sicherheitsdienste für die Integration und Wartung dieser Lösungen an.

Die Lösungen von GE, die für IEC 62443-2-4 relevant sind, umfassen folgendes:

SecurityST* Mark* VIe Lösung und Serviceleistungen für die Inbetriebnahme

Diese Lösungen sind Achilles® Practices – Bronze zertifiziert. Das bezeugt, dass GE die optimalen Verfahren für eine hohe Cyber-Sicherheit einhält, darunter auch die Konfiguration und Wartung der Lösung für einen sicheren Betrieb. Die Lösung ist für die Unterstützung von optimalen Verfahren bei der Sicherheit ausgelegt, und um eine effizientere Einhaltung von IEC 62443-2-4 zu ermöglichen.

Cyber Asset Protection (CAP) Abonnement für Software-Updates und SecurityST Appliance

Diese Reihe von Lösungen bietet mehrere Programme zur Unterstützung von optimalen Verfahren im Bereich Cyber-Sicherheit. Die Funktionen umfassen zentrales Patch-Management, Updates für Antivirus/Host Intrusion Detection, zentrale Kontoverwaltung, Protokollierung und Ereignisverwaltung, Angriffserkennung, Whitelisting und automatischer Backup.

Wurldtech OpShield Technologie

Diese Lösung ist für den Schutz von kritischer Infrastruktur, Steuersystemen und Betriebstechnik ausgelegt. Sie überwacht und blockiert böswillige Aktivitäten und Fehlkonfiguration, bietet einfach anzuwendende Steuerungen für die Segmentierung von Netzwerken und eine verbesserte Visualisierung des elektronischen Sicherheitsbereichs (Electronic Security Perimeter). Sie trägt dazu bei, die Gefahr durch Exploits zu vermindern, d.h., bekannte Sicherheitslücken, während der Betreiber auf Patches des Lieferanten oder das Wartungsfenster für Patches wartet.

Diese Lösungen bieten eine umfassende Liste von Funktionen und Vorteilen, die in diesem Whitepaper zu Normen nicht vollständig dokumentiert sind.

Ausführliche Informationen zur Funktionalität der Lösungen finden Sie in den Datenblättern für unsere Lösungen auf unseren Websites: www.gemeasurement.com und www.wurldtech.com.

Die Lösungen von GE, die für IEC 62443-2-4 relevant sind, werden im folgenden Abschnitt genauer erläutert.

Programme von GE zur Unterstützung von IEC 62443-2-4

Die folgende Tabelle enthält einen Überblick über die Programme von GE, die IEC 62443-2-4 unterstützen und zugehörige Funktionen.

Lösungen	GE Fähigkeiten im Bereich Cyber-Security	
Lösung Bereitstellung von Personal	Dabei handelt es sich um die Bereitstellung von Personal für Automatisierungslösungen von Serviceanbietern. Alle Zertifizierungsanwendungen müssen diesen Konformitätsblock enthalten.	• GE Oil & Gas stellt ein Produktsicherheits-Team bereit, um Verbesserungen bei der Sicherheit unserer Lösungen und unserer Prozesse voranzutreiben.
		• Wir verfügen über Experten für verschiedene Aspekte des Bereichs Sicherheit zur Unterstützung der jeweiligen Sicherheitslösungen und -serviceleistungen.
		• Unser Team verfügt über einen Schulungsplan, um Andere am Wissen der Mitarbeiter im Bereich Sicherheit teilhaben zu lassen.
		– Im Schulungsplan sind die Rollen, die Schulungen für diese Rollen sowie die Mitarbeiter, die für Schulungen bestimmt wurden, festgelegt.
		– Die Schulungen werden in regelmäßigen Abständen durchgeführt.
Lösung Verstärkung	Zu den Programmen gehören die Reduzierung der Angriffsfläche bei Automatisierungslösungen, einschließlich Risikoanalysen, die Feststellung von Bedrohungen und Anfälligkeiten sowie die Handhabung von USB-Ports.	• Die Lösungen von GE beginnen mit einer für die Sicherheit segmentierten Referenzarchitektur und verstärkenden Maßnahmen, die für die Verringerung der Sicherheitsgefahr ausgelegt sind.
		– Durchführung von Bewertungen zur Verstärkung des Systems für die individuelle Sicherheitsumgebung und Unternehmenspolitik des jeweiligen Kunden.
		– Platzierung von Firewall und IDS und deren Regeln werden im Rahmen der Architektur vorgegeben.
		– Switches können gesperrt werden.
		– Unnötige Ports, Services und Programme werden von Arbeitsplätzen, Servern und Controllern entfernt oder deaktiviert, um sie als Angriffspunkte auszuschalten.
		– Arbeitsplätze werden zum Schutz gesperrt, wenn sie nicht besetzt sind.
		– Identifizierung von fehlenden Sicherheits-Patches ist automatisiert.
		– An Arbeitsplätzen und bei Servern werden Antivirus-Software und Programme für die Validierung und Installation der neuesten Dateien zur Definition von Viren verwendet.
		– Durch Verfahrensweisen wird sichergestellt, dass die mobilen Medien, die bei der Integration und Wartung verwendet werden, genehmigt und frei von Viren sind und nicht für andere Zwecke verwendet werden.
		– Es werden Tests zur Überprüfung der Sicherheit und Robustheit von Netzwerken bei den Produkten durchgeführt, die für die Lösungen verwendet werden, um die Zuverlässigkeit und Integrität zu gewährleisten.

Lösungen	GE Fähigkeiten im Bereich Cyber-Security	
Sicherheit von Netzwerken	Die Programme beziehen sich auf die Unterstützung der Segmentierung und Verwaltung von Netzwerken.	• GE verfügt über eine dokumentierte Netzwerksicherheits-Architektur, die genau auf die individuellen Bedürfnisse des Kunden zugeschnitten werden kann.
		• Eine sichere Konnektivität für den Fernzugriff wird auf Anfrage individuell angepasst, normalerweise durch eine Kombination aus RDP-Firewalls und Zugangskontrollen. SecurityST unterstützt die Verwaltung der Geräte im Netzwerk und erzwingt die Authentifizierung und Verschlüsselung des Datenverkehrs für die Netzwerkadministration in beide Richtungen.
		• Unsere Netzwerksicherheits-Architektur trennt das Anlagennetzwerk über eine Firewall und ein „Angrifferkennungssystem“ (Intrusion Detection System - IDS), das mit empfohlenen Regeln konfiguriert wurde..
		• Im Aboservice Cyber Asset Protection (CAP) und SecurityST sind Host Intrusion Detection (HIDs) und Virenschutz enthalten. In SecurityST ist auch Network Intrusion Detection (NIDs) enthalten.
		• Unsere Netzwerksicherheits-Architektur schützt interne Schnittstellen mit „Managed“ Switches, die gesperrt werden können.
		• Der drahtlose Zugriff ist im Netzwerk des Steuersystems verboten.
		• Unsere Steuersysteme werden so ausgelegt und installiert, dass die Interaktion zwischen den Netzwerken, vor allem zwischen dem Überwachungs-/HMI-Netzwerk, dem Steuernetzwerk und den E/A-Netzwerken reduziert wird. Das E-/A-Netzwerk, in dem sich das Steuersystem E/A befindet, ist physisch von allen anderen Netzwerken getrennt.

Lösungen	GE Fähigkeiten im Bereich Cyber-Security	
Sicherheit von Benutzern	Dieses Programm umfasst die Unterstützung der Verwaltung der Sicherheit des Betriebssystems und der Benutzerkonten.	• SecurityST bietet eine zentrale, rollenbasierte Zugangskontrolle für Windows Arbeitsplätze/Server über Active Directory Server, die auf redundanten Domain-Controllern laufen. Mit Active Directory wird die Verwaltung von Benutzerkonten und Maschinen zentralisiert und es bietet zusätzliche Sicherheitsauflagen für die Handhabung der funktionalen Trennung.
		• RADIUS Server werden in Active Directory integriert, um den Zugang zu Elementen zu steuern, die nicht auf Domains basieren (wie etwa Netzwerk-Switches, Firewalls und NIDs).
		• SecurityST wird vorkonfiguriert ausgeliefert mit Standardeinstellungen für Geräte, Benutzer/Passwörter sowie Gruppen, denen neue und voreingestellte Benutzer/Geräte zugeordnet werden. Die Gruppen stellen die Rollen von Benutzern und Geräten dar und definieren angemessene Rechte und Beschränkungen für sie.
		• Standardeinstellungen für Passwörter sind so konfiguriert, dass sie bei erstmaliger Benutzung geändert werden müssen, um sicherzustellen, dass sie in das in Betrieb befindliche System mit aufgenommen werden. Dazu empfehlen wir, dass Passwörter für lokale Benutzer und Benutzer der Domain so konfiguriert werden, dass sie nach einem voreingestellten Zeitraum automatisch ungültig werden. Mit Active Directory werden die Benutzer dazu aufgefordert, ihr Passwort zu ändern, bevor es ungültig wird.
		• GE entfernt alle provisorischen Konten, die zum Einrichten oder zur Wartung des Systems verwendet wurden, wenn sie nicht mehr benötigt werden und empfiehlt dazu, alle unnötigen Konten wie „Backdoor“, „Superuser“ und „Gast“ vor der Inbetriebnahme des Systems zu entfernen oder zu deaktivieren.
Anwendungssicherheit	Dabei handelt es sich um spezifische Steuer- und Überwachungsfunktionen der Automatisierungslösung.	• Die Konfiguration der gelieferten Lösung, einschließlich der Zeichnungen zur Architektur und den Versionennummern der Komponenten wird während des gesamten Lebenszyklus der Lösung mit einer Kombination aus automatischen und manuellen Verfahren gewartet.
		• Authentifizierung und Verschlüsselung in beide Richtungen für den HMI-Zugriff auf die Mark Vie Controller erfolgt über den SecurityST Certificate Authority Server.
		• Die Konfiguration der Parameter des Steuersystems erfolgt über Downloads zum Mark* VIe Controller. Die Software ControlST* und Cimplicity* erzwingt Regeln für die Erarbeitung dieser Downloads. SecurityST User Security beschränkt das Erstellen und Durchführen von Downloads zu autorisierten Benutzern an den HMI-Arbeitsplätzen.
		• Beim Herunterladen der Konfigurationen werden Wertebereiche für Laufzeitparameter wie Sollwerte festgelegt, um sicherzustellen, dass die Benutzer keine die Sicherheit gefährdenden oder unerwünschten Werte festlegen können.
		• Zum Sammeln von Laufzeitdaten und Ereignissen zur Unterstützung von Prozessanalysen und Sicherheitsforensik können Historian-Funktionen konfiguriert werden. Die gesammelten Daten können mit früheren Werten verglichen werden, um zu ermitteln, welche Änderungen im System aufgetreten sind. Die Änderungen können analysiert und Korrekturmaßnahmen ergriffen oder eine Genehmigung erteilt werden.

Lösungen	GE Fähigkeiten im Bereich Cyber-Security	
Security Information and Event Management (SIEM)	Dabei handelt es sich um die Unterstützung der Verwaltung von die Sicherheit betreffenden Informationen und Ereignissen, im Allgemeinen für die Handhabung von Sicherheitsvorfällen und und die Forensik.	• GE verfügt über ein Team für Notfälle bei Produkten. Es befolgt einen formellen Prozess, um den Kunden über Anfälligkeiten, die in seinen Produkten festgestellt werden, zu informieren.
		• Das SIEM-System bietet individuell anpassbare, umfassende Funktionen für die Protokollierung und die Erstellung von Berichten.
		• Das SIEM-System unterstützt die logische Gruppierung von verwalteten Anlagen, und es können damit individuell anpassbare Berichte erstellt werden, die auf Ereignistypen basieren.
		• Das SIEM-System umfasst HMI-Sicherheitsprotokolle des ICS von GE und Protokolle von sicherheitsrelevanten Ereignissen für Netzwerkgeräte wie An- und Abmelden und Änderungen bei der Konfiguration. So werden zum Beispiel nicht erfolgreiche Anmeldeversuche an HMI und Netzwerkgeräten (NIDs, Firewall, Switches, etc.) protokolliert.
		• Das SIEM-System protokolliert die Überwachungsaktivitäten von NIDs, HIDs und Antivirus. Diese Protokolle erfassen Ereignisse, die mit Informationsströmen zusammenhängen, um den Benutzern mit Erfassung und Meldung von böswilligen Aktivitäten in Echtzeit zu unterstützen.
		• Die Lösung Mark VIe und SecurityST protokolliert auch Zustandsänderungen und verfügt über Berichtsfunktionen für Standardereignisse, die eine sichere Ereignismeldung gewährleisten.
		• Individuell gestaltete SIEM-Berichte können ganz einfach erstellt werden, um den Zusammenhang zwischen Ereignissen festzustellen und zu überprüfen und dadurch eine schnelle Reaktion auf Vorfälle zu ermöglichen.
		• Wir erstellen die SIEM-Anmelderegelung zusammen mit dem Kunden und führen eine Feinabstimmung des Zusammenhangs zwischen Ereignissen durch, die auf vordefinierten Arten von Ereignissen basiert, für Benutzerrollen, Origin-Host, Impacted Host, Anwendung, Warnungen oder unbefugte oder verdächtige Aktivitäten sowie andere Messgrößen zur Reduzierung von Auditprotokollen.

Lösungen	GE Fähigkeiten im Bereich Cyber-Security	
Patch-Management	Damit wird die Validierung und Installation von Sicherheits-Patches unterstützt.	• SecurityST bietet einen zentralen Service für die Überprüfung und den Einsatz von Sicherheits-Patches.
		• Im Patching-Servicelabor von SecurityST werden alle Patches vor der Freigabe überprüft, um sicherzustellen, dass sie mit der Mark VIe und SecurityST Lösung kompatibel sind.
		• GE bietet eine Dokumentation zum SecurityST Patch-Service an, darunter auch empfohlene und dokumentierte Einführungsverfahren, den Prozess des Patch-Verfahrens, Abhilfe für nicht genehmigte Patches sowie Strategien zur Risikominderung.
		• Die Patches werden monatlich auf einer DVD zur Verfügung gestellt, um das unnötige Öffnen von Netzwerk-Ports und Services, die für eine Online-Verteilung erforderlich sind, zu vermeiden. Die DVDs werden mit manipulationssicheren Siegeln verteilt und bei der Ankunft am Kundenstandort gescannt.
		• Im Bericht CAP Patch Applicability (Patch-Anwendbarkeit) werden die Informationen zur Kritikalität, zur Zeit, die für das Update erforderlich ist und ob ein Neustart erforderlich ist, festgelegt.
Backup/ Wiederherstellen	Damit werden die Funktionen Backup und Wiederherstellen der Automatisierungslösung und ihrer Komponenten unterstützt.	• SecurityST bietet eine Dokumentation für Backup/Wiederherstellen von Computern, Netzwerkgeräten und anderen Komponenten, einschließlich des Einplanens von Backups.
		• GE stellt ein Dokument zur Backup-Architektur zur Verfügung, in dem die Speicherung von Backups beim Kunden beschrieben wird und Empfehlungen für die Speicherung außerhalb des Firmengeländes gegeben werden. Verschlüsselung von Backups und deren Archive wird unterstützt.
		• SecurityST stellt Skripts für die Konfiguration und individuelle Anpassung der Backup-Konfigurationen bereit. Es wird eine Anleitung für das Hinzufügen von neuen Komponenten und das Erstellen zusätzlicher Backup-Pläne bereitgestellt. Die Backup-Funktion von SecurityST ist für den Betrieb während des normalen Anlagenbetriebs ausgelegt. Die Bandbreite der Backups ist für die minimale Nutzung von Netzwerkressourcen ausgelegt.

Imagination at work

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

www.gemeasurement.com/machinery-control

GEA32435A (05/2016)