Gesamtübersicht

V. 2.1

ISONA Automation WebCenter und Secure Automation System

ISONA bietet seinen Kunden mit dem Automation WebCenter (Webportal) in Verbindung mit dem Secure Automation System eine innovative Systemlösung. Die hohen Sicherheitsstandards und die vielfältigen Einsatzszenarien lassen keine Wünsche offen. Die ISONA-Lösung adressiert sowohl Energiecontracting-Unternehmen, MSR-Firmen als auch Hersteller von Steuerungen, Maschinen und GLT-Anlagen und lässt sich durch sein flexibles Konzept bei Bedarf kundenspezifisch anpassen.

Auch für bestehende Fernwartungslösungen ist dies eine zukunftssichere Ergänzung mit neuen Funktionalitäten und ermöglicht darüber hinaus auch die schrittweise Migration von modembasierten Anbindungen auf IP-basierte VPN-Verbindungen über das Internet.

Die folgende Grafik veranschaulicht das Zusammenspiel des Automation WebCenters mit dem Secure Automation System und die Anbindung der Liegenschaften sowie den Fernwartungszugriff:

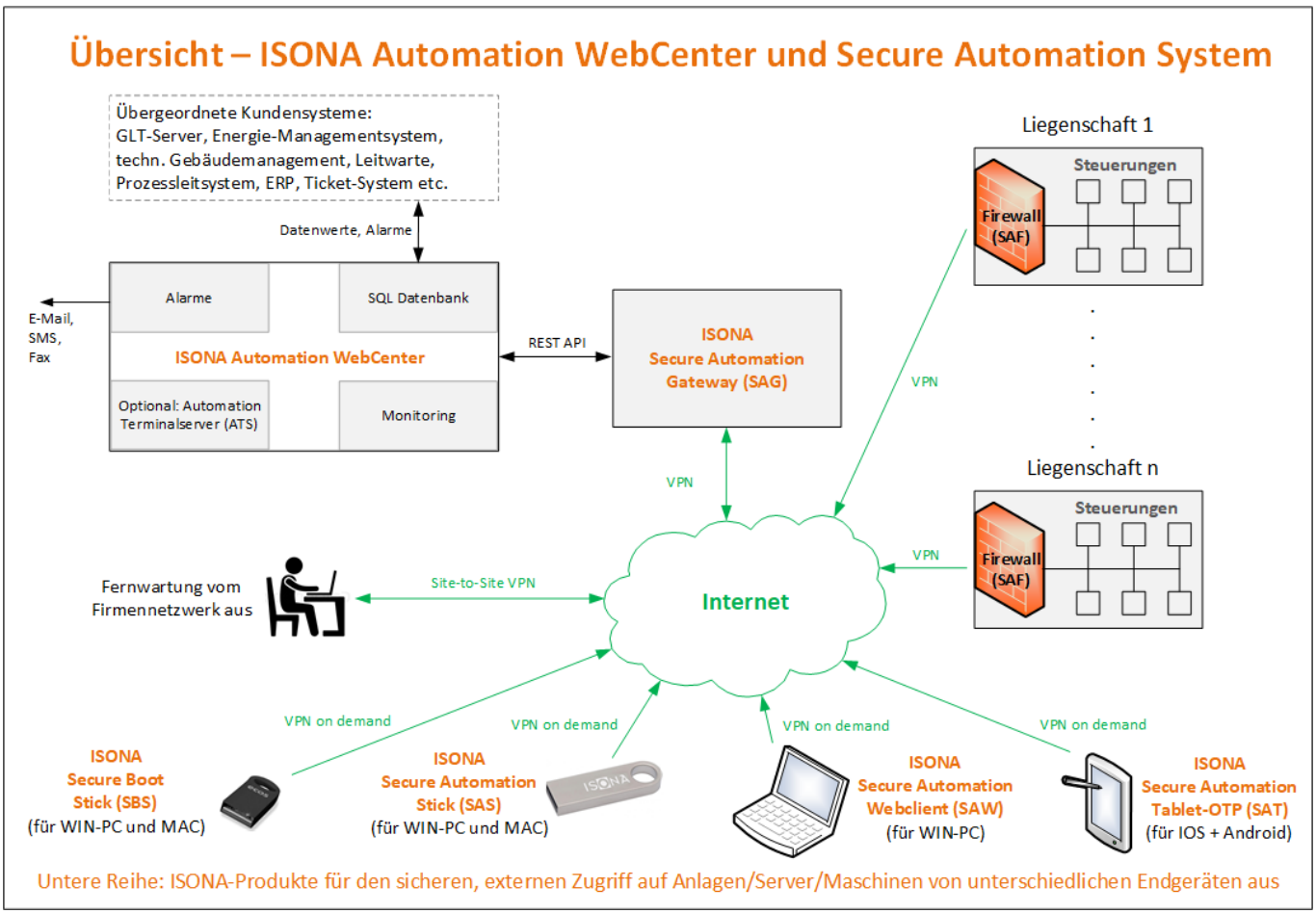

Abb. 1: Übersicht - Automation WebCenter in Verbindung mit den Komponenten des Secure Automation Systems

Das ISONA Automation WebCenter umfasst folgende Komponenten und Funktionen:

⇨ Monitoring der Firewalls und Steuerungen in den einzelnen Liegenschaften, ob diese online sind

⇨ Alarmierung via E-Mail, SMS oder Fax, wenn eine Anlage eine Störung meldet

⇨ Standortübergreifende Erfassung von Zählerständen und Messwerten in einer zentralen SQL-Datenbank

⇨ Inventarsystem, in dem alle Informationen über Geräte und Anlagen in den Liegenschaften erfasst sind

⇨ Adressverwaltung mit den Kontaktdaten von Herstellern, MSR-Firmen, Kunden, Projektpartnern usw.

⇨ Einfache VPN-Erstkonfiguration von Tablets durch den Endbenutzer über das Automation WebCenter

⇨ Download von Konfigdateien zur schnellen Offline-Konfiguration von VPN-Firewallroutern über einen USB-Stick

⇨ Diagnose-Tools für eine schnelle Fehlersuche in der Inbetriebnahmephase

⇨ Schnittstellen zu Energiemanagementsystemen, GLT-Servern, Abrechnungssystemen, ERP, Leitwarten etc.

Gesamtübersicht

V. 2.1

Das ISONA Secure Automation System stellt eine optimale Ergänzung zum ISONA Automation WebCenter dar. Nachfolgend werden kurz die einzelnen Komponenten des Secure Automation Systems beschrieben (siehe hierzu auch Abb. 1):

Komponente 1: Secure Automation Gateway (SAG)

Das Secure Automation Gateway (SAG) stellt die zentrale Komponente des *Secure Automation Systems* dar. Es dient als VPN-Gateway, Fernwartungsserver, Authentisierungsserver, PKI-Server, Berechtigungssystem, Routingserver sowie als zentraler Managementserver für alle Komponenten des *Secure Automation Systems*. Das Secure Automation Gateway ist als virtuelle Appliance (lauffähig auf VMware®, Hyper-V®, XenServer®, Oracle VirtualBox®) oder als Hardware-Appliance im 1HE Rack-Gehäuse erhältlich. Die virtuelle Appliance wird entweder beim Kunden oder in unserem Rechenzentrum gehostet, je nach Anforderung. Über einen ständigen VPN-Tunnel zwischen dem Secure Automation Gateway und einem Firmennetzwerk lässt sich ein sicheres und herstellerunabhängiges Fernwartungssystem realisieren.

Komponente 2: Secure Automation Stick (SAS)

Der Secure Automation Stick (SAS) erlaubt es, von extern sicher auf beliebige Anlagenvisualisierungen oder Steuerungen zuzugreifen. Dieser spezielle USB-Stick benötigt keinerlei Installation oder Adminrechte und hinterlässt auf dem Windows®-Gastsystem keine Spuren, da er in einer abgeschirmten Umgebung läuft. Sämtliche Software, die der Anwender benötigt um eine sichere VPN-Verbindung aufzubauen und auf die vorhandene Automationsinfrastruktur zuzugreifen, ist bereits auf dem Stick integriert. Dieser ermöglicht zusammen mit dem Passwort eine hochsichere 2-Faktor-Authentifizierung des Benutzers und ist somit immun gegenüber Angriffen mit Keyloggern oder Viren, die bei den üblicherweise verwendeten VPN-Clients die Passwörter abfangen und damit Cyber-Kriminellen einen unbefugten Zugriff auf Automationsanlagen ermöglichen.
Der Stick kann auch zur Fernwartung für mobile Servicetechniker genutzt werden, da er die Möglichkeit bietet einen transparenten VPN-Tunnel aufzubauen. Hierzu muss, im Gegensatz zu konventionellen VPN-Clients, keine Client-Software auf dem PC installiert werden. Die Konfiguration des Sticks erfolgt zentral über das SAG.

Komponente 3: Secure Automation Webclient (SAW)

Der Secure Automation Webclient (SAW) ist die USB-sticklose Variante des *Secure Automation Sticks (SAS)* mit identischen Features. Dadurch wird auch ein Zugang von Windows®-PCs aus ermöglicht, bei denen eine Nutzung von USB-Sticks gesperrt ist oder wenn explizit ein browserbasierter Zugang gewünscht ist.
Sämtliche Software, die der Anwender benötigt um eine sichere VPN-Verbindung aufzubauen und auf die vorhandene Automationsinfrastruktur zuzugreifen, wird ad-hoc via Browser von dem *Secure Automation Gateway (SAG)* auf den Gast-PC geladen und in einer abgeschotteten Sandbox ausgeführt. Für die sichere 2-Faktor-Authentisierung des Benutzers kann je nach Wunsch entweder ein OTP-Token (**O**ne**T**ime**P**assword = Einmalkennwort), ein Soft-Token (auf Smartphone) oder eine SMS-TAN (Einmalkennwort via SMS) verwendet werden. Die Verwaltung der unterschiedlichen OTP-Varianten erfolgt zentral im SAG

Komponente 4: Secure Boot Stick (SBS)

Der Secure Boot Stick (SBS) kommt zum Einsatz, wenn beim externen Zugriff auf Anlagen höchste IT-Sicherheitsanforderungen vorgegeben sind, z.B. bei kritischen Infrastrukturen. Oder wenn Telearbeiter von privaten PCs aus hochsicher auf Anlagen zugreifen sollen. Dabei wird der PC mit dem Bootstick gestartet und baut über einen vertraulichen VPN-Tunnel die Verbindung zur Anlage auf um dann über RDP, VNC oder den onstick Firefox Browser auf die Geräte in den dezentralen Liegenschaften zuzugreifen. Da das potentiell unsichere Windows des PCs nicht gestartet wird sondern ein sicheres Betriebssystem auf dem Stick, werden mit dem Secure Boot Stick höchste IT-Sicherheitslevels gewährleistet. Wenn für den Zugriff auf Anlagen von div. Herstellern spezielle Windowsclients benötigt werden, dann kann als Ergänzung der Automation Terminalserver (ATS) eingesetzt werden, auf den der Secure Boot Stick dann per RDP zugreift. Auf diesem Automation Terminalserver können dann beliebige Windowsclients für den Zugriff auf die Anlagen installiert werden, um einen hochsicheren Zugriff zu realisieren.

Komponente 5: Secure Automation Tablet-OTP (SAT)

Mit dem Secure Automation Tablet-OTP (SAT) ist ein hochsicherer Zugriff auf Automationsanlagen von Tablets oder Smartphones aus möglich. Beim iPad®/iPhone® wird dazu der im iOS® integrierte VPN-Client verwendet, erweitert um eine zweistufige Authentisierung mit einem OTP-Token. Bei Android®-Tablets/-Smartphones wird die Original OpenVPN-App unterstützt, ergänzt um eine Zwei-Faktor-Authentisierung mit OTP-Token.
Beim Einsatz des optionalen ISONA Automation Terminalservers ATS (siehe hierzu auch Abb. 1) kann der Tablet-/Smartphone Benutzer sehr einfach auf Steuerungen diverser Hersteller zugreifen, ohne die herstellerspezifischen Apps (kostenpflichtig) benutzen zu müssen. Teilweise sind die Apps auch nur für iOS oder nur für Android erhältlich, dieses Problem lässt sich mit dem ISONA Automation Terminalservers ATS umgehen.

Gesamtübersicht

V. 2.1

Komponente 6: Secure Automation Firewalls (SAF)

Für die VPN-Vernetzung der Anlagenstandorte liefert ISONA sog. Secure Automation Firewalls (SAF). Die Firewallrouter (für Hutschiene und Desktop) werden so konfiguriert, dass nach dem Einschalten ein ausgehender VPN-Tunnel zum zentralen *Secure Automation Gateway (SAG)* aufgebaut wird und somit ein verschlüsseltes VPN-Netzwerk (**V**irtual **P**rivate **N**etwork) entsteht, bei Bedarf erfolgt die VPN-Aktivierung über einen Schlüsselschalter oder zeitgesteuert.
Wenn ein ISONA Automation WebCenter vorhanden ist, kann man die VPN-Router zentral verwalten und die Konfigurationsdatei direkt vom Webportal herunterladen und per USB-Stick offline in die Secure Automation Firewalls (SAF) einspielen.
Zusätzlich stehen weitere, spezielle Secure Automation Firewalls zur Verfügung, bei denen z.B. im Gehäuse ein Datenlogger integriert ist oder eine SPS mit integriertem VPN-Router.

Kontaktdaten

ISONA GmbH
Sant-Ambrogio-Ring 13a
D-55276 Oppenheim

Telefon +49 6133 / 509098-0
E-Mail vertrieb@isona.de
Internet www.isona.de