Gesamtübersicht

Vers. 3.0

ISONA Automation WebCenter und die Secure Automation Komponenten

ISONA bietet seinen Kunden mit dem Automation WebCenter (Webportal) in Verbindung mit den Secure Automation Komponenten eine innovative Gesamtlösung. Die hohen IT-Sicherheitsstandards und die vielfältigen Einsatzszenarien sind wegweisend und decken alle erdenklichen Kundenanforderungen ab. Die ISONA-Lösung adressiert alle Branchen u.a. Energie-Contracting Firmen, Stadtwerke, MSR-Firmen als auch Hersteller von Steuerungen, Energieerzeugungsanlagen, Maschinen usw. und lässt sich durch sein flexibles Konzept jederzeit kundenspezifisch anpassen.
Die folgende Grafik veranschaulicht das Zusammenspiel des Automation WebCenters mit den diversen Secure Automation Komponenten für die Anbindung von dezentralen Liegenschaften sowie den Fernwartungszugriff:

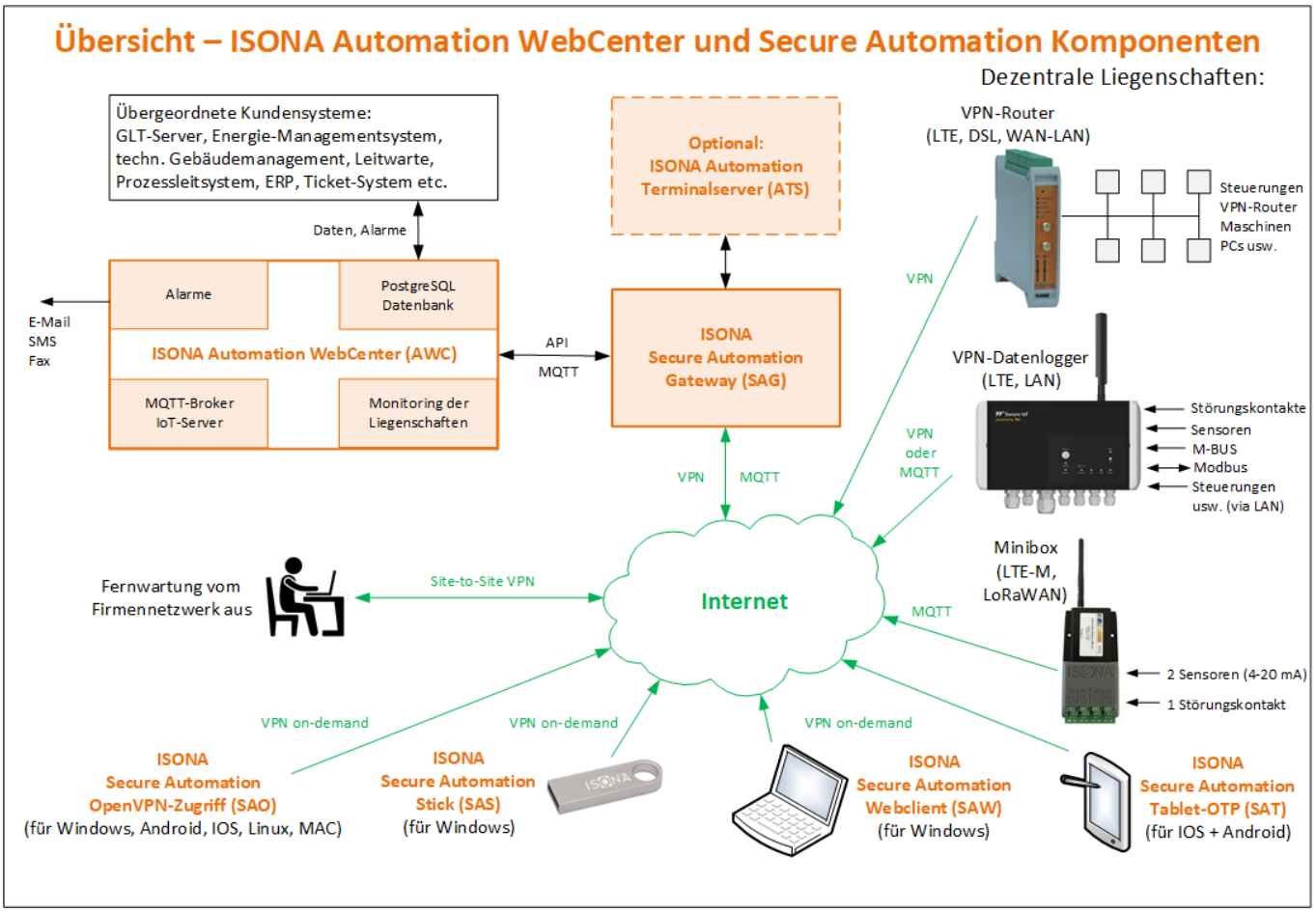

Abb. 1: Übersicht - Automation WebCenter in Verbindung mit den Secure Automation Komponenten. Die zentralen Komponenten des ISONA Gesamtsystems sind orange markiert.

Das ISONA Automation WebCenter umfasst folgende Funktionen und Module:

- ⇨ Im Störungsfall Alarmierung via E-Mail, SMS oder Fax
- ⇨ Standortübergreifende Erfassung von Zählerständen und Messwerten in einer zentralen PostgreSQL-Datenbank
- ⇨ MQTT-Broker für die Kommunikation mit IoT-Devices
- ⇨ Monitoring der Verfügbarkeit von Firewalls und Steuerungen in den einzelnen Liegenschaften
- ⇨ Geräte-Management für diverse VPN-Router, VPN-Datenlogger, Miniboxen: Offline-Erstkonfiguration, Remote-Konfiguration, Remote-Firmware-Update, Online-/Offline-Monitoring
- ⇨ Schnittstellen zu Energiemanagementsystemen, GLT-Servern, Abrechnungssystemen, ERP, Leitwarten etc.
- ⇨ Inventarsystem mit allen Informationen über die in den Liegenschaften verbauten Geräte
- ⇨ Adressverwaltung mit den Kontaktdaten von Herstellern, Dienstleistern, Kunden, Projektpartnern usw.
- ⇨ Diagnose-Tools für eine schnelle Inbetriebnahme neuer Liegenschaften
- ⇨ Einfache VPN-Konfiguration von Tablets durch den Endbenutzer

Gesamtübersicht

Vers. 3.0

Die ISONA Secure Automation Komponenten stellen eine optimale Ergänzung zum ISONA Automation WebCenter dar. Nachfolgend werden die einzelnen Secure Automation Komponenten vorgestellt (siehe hierzu auch Abb. 1):

Geräte für die Liegenschaften

Für die Vernetzung der dezentralen Anlagenstandorte liefert ISONA eine Reihe von Geräten (siehe Abb. 1, weitergehende Details zu den Geräten auf unserer Website https://www.isona.de/):

- Diverse VPN-Router (LTE, DSL oder WAN) für die Vernetzung unterschiedlichster LAN-fähiger Geräte in den Liegenschaften
- Diverse VPN-Datenlogger (LTE oder WAN) für den Anschluss von Störungskontakten, Sensoren, M-Bus Zählern, Modbus-Geräten, Steuerungen, Fremdroutern usw.
- ISONA Minibox (LTE-M oder LoRaWAN) für den Anschluss von bis zu 2 Sensoren (4-20 mA) sowie einem Störungskontakt. Geeignet für die Überwachung von Kleinst-Liegenschaften z.B. mit lediglich einem Brenner und einem Warmwasser-/Pufferspeicher und für die Drucküberwachung des Heizkreises

Secure Automation Gateway (SAG)

Das Secure Automation Gateway (SAG) ist die zentrale IT-Sicherheitskomponente des Gesamtsystems. Es fungiert als VPN-Gateway, Fernwartungsserver, Authentisierungsserver, Zertifikatsserver (PKI), Berechtigungssystem, Routingserver sowie als zentraler Managementserver für einige Secure Automation Komponenten. Das Secure Automation Gateway ist eine virtuelle Appliance, lauffähig auf den unterschiedlichsten Virtualisierungsservern. Die virtuelle Appliance wird entweder beim Kunden oder auf ISONA-Servern im Rechenzentrum gehostet, je nach Randbedingungen und Kundenwunsch. Über einen ständigen VPN-Tunnel zwischen dem Secure Automation Gateway und einem Firmennetzwerk lässt sich zusätzlich ein sicheres und herstellerunabhängiges Fernwartungssystem realisieren.

Secure Automation Stick (SAS)

Der Secure Automation Stick (SAS) erlaubt es, sicher von extern 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 (Sandbox) läuft. Sämtliche Software, die der Anwender benötigt um einen sicheren Application-Layer-VPN 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.
Die Konfiguration und das Management der Sticks erfolgt zentral über das SAG.

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 die Nutzung von USB-Sticks gesperrt ist.
Sämtliche Software, die der Anwender benötigt um einen sicheren Application-Layer-VPN aufzubauen und auf die vorhandene Automationsinfrastruktur zuzugreifen, wird nach der Authentisierung 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 oder eine OTP-App (z.B. Google Authenticator) verwendet werden.

Secure Automation OpenVPN-Zugriff (SAO)

Das Secure Automation OpenVPN-Zugriffsbundle kommt zum Einsatz, wenn der Benutzer einen transparenten VPN-Tunnel von seinem PC / Tablet zu einem Gerät in der Liegenschaft benötigt, um z. B. mit einem Programmiertool auf eine Steuerung zuzugreifen. Die komplette OpenVPN-Konfigurationsdatei (.ovpn-Datei) kann aus dem ISONA Automation WebCenter heruntergeladen und auf dem jeweiligen Endgerät abgespeichert werden, als Profil für den dort installierten offiziellen OpenVPN-Client (Download unter https://openvpn.net/vpn-client).

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® kann dazu der im iOS® integrierte IPsec VPN-Client oder die OpenVPN-App verwendet werden, erweitert um eine zweistufige Authentisierung mit einem OTP-Token oder einer OTP-App (z.B. Google Authenticator). Bei Android®-Tablets/-Smartphones wird die Original OpenVPN-App unterstützt, ergänzt um eine Zwei-Faktor-Authentisierung mit OTP-Token oder einer OTP-App (z.B. Google Authenticator).
Ergänzend empfehlen wir den Einsatz des ISONA Automation Terminalservers ATS (siehe hierzu auch Abb. 1). Damit kann der Tablet-/Smartphone Benutzer sehr einfach auf Steuerungen unterschiedlichster Hersteller zugreifen, ohne die teils kostenpflichtigen Hersteller-Apps benutzen zu müssen.