Gesamtübersicht

Version 3.4

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, Anlagenbetreiber, Solarteure 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 (AWC) mit den diversen Secure Automation Komponenten für die Anbindung von verteilten Liegenschaften sowie den Fernwartungszugriff:

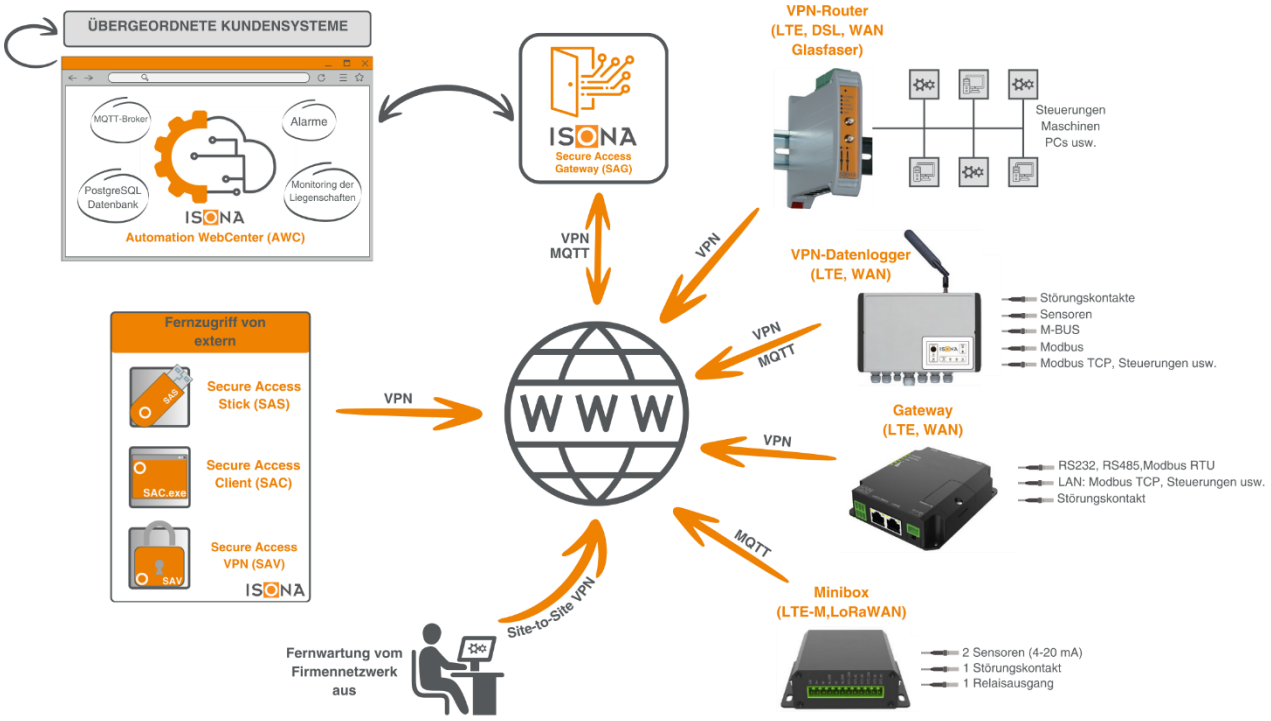

Abb. 1: Übersicht – ISONA Automation WebCenter (AWC) in Verbindung mit den Secure Automation Komponenten.

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
- ⇨ Inventarsystem mit allen Informationen über die in den Liegenschaften verbauten Geräte (Manuals, Pläne)
- ⇨ 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
- ⇨ Automatische Zertifikatserneuerung nach Ablaufzeit der Zertifikate (üblicherweise 1-3 Jahre Maximallaufzeit)
- ⇨ Div. Schnittstellen zu übergeordneten Energiemanagementsystemen, GLT-Servern, Abrechnungssystemen, ERP, Leitwarten etc.

Gesamtübersicht

Version 3.4

Die ISONA Secure Automation Komponenten stellen eine optimale Ergänzung zum ISONA Automation WebCenter dar. Nachfolgend werden die einzelnen Secure Automation Komponenten vorgestellt:

Secure Access Gateway (SAG)

Das Secure Access 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 die Secure Access Komponenten. Das Secure Access 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 Access Gateway und einem Firmennetzwerk lässt sich zusätzlich ein sicheres und herstellerunabhängiges Fernwartungssystem realisieren.

Secure Access Stick (SAS)

Der Secure Access 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 erfolgen zentral über das SAG.

Secure Access Client (SAC)

Der Secure Access Client (SAC) ist die USB-sticklose Variante des *Secure Access 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 Access 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-Hardware-Token oder eine OTP-App auf dem Smartphone (z.B. Google Authenticator) verwendet werden.

Secure Access VPN (SAV)

Das Secure Access VPN (SAV) 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 als Profil für den dort installierten OpenVPN-Client (Download unter https://openvpn.net/vpn-client) abgespeichert werden.

Ein weiterer Einsatzbereich des Secure Access VPN (SAV) sind Tablets (IOS, Android) oder MACs, um damit auf Server/Maschinen zuzugreifen. Für eine sichere Authentifizierung des Benutzers wird der Secure Access VPN ergänzt um eine 2-Faktor-Authentifizierung (2FA) mit einem Einmalkennwort. Für das Einmalkennwort stehen die gleichen Varianten wie beim Secure Access Client (siehe oben) zur Verfügung.

Geräte für die verteilten Liegenschaften

Für die Vernetzung der verteilten 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

Automation Terminalserver (ATS)

Dieser optionale Terminalserver auf Windowsbasis kommt zum Einsatz, wenn Tablet-Benutzer und auch MAC-Benutzer einen Fernzugriff auf Anlagen, Steuerungen usw. benötigen. Dazu wird der Secure Access VPN (SAV) (siehe oben) auf dem Endgerät eingesetzt, darüber verbindet sich das Endgerät via RDP auf den Automation Terminalserver, der für die Benutzer ähnlich einem Jumpserver fungiert. Auf diesem Automation Terminalserver werden dann alle benötigten Windows-Applikationen für den Fernzugriff auf die Server/Maschinen/Steuerungen installiert.