

Hier ist die
Lösung!

Fernwirktechnik-Lösung von SEGNO mit modernen Kommunikationsmethoden und aktuellen IT-Sicherheitsanforderungen

SEGNO@smartFWT

SEGNO smartes Fernwirktechnik System

Die Lösung

Die smarte Fernwirktechnik-Lösung von SEGNO ist branchenübergreifend einsetzbar, fokussiert jedoch auf kritische Infrastrukturen wie Wasser, Abwasser und Energie. Dabei werden Ansätze zur IT-Sicherheit basierend auf B3S und NIS2 berücksichtigt. Gerade mit der Abkündigung des 2G Netzes (GPRS) stellt die SEGNO Lösung eine weitere Alternative zu den marktüblichen Fernwirk-Systemen dar, die klassische Fernwirkprotokolle nutzen.

Wussten Sie schon ?

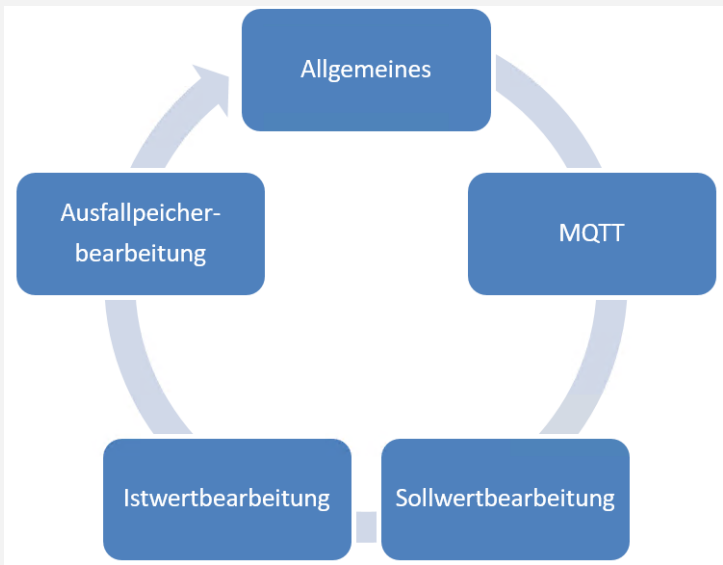
Bis zum Sommer 2028 will die Deutsche Telekom das veraltete Mobilfunknetz GSM (2G) außer Dienst stellen.

Traditionell wurde für die Kommunikation zwischen Außenbauwerke und Leitstellen das 2G-Netz (GPRS) genutzt. Dieses Netzwerk hat sich über viele Jahre als stabil erwiesen und war für viele Anwendungen ausreichend schnell. Mit der Ankündigung der Deutschen Telekom, das 2G-Netz abzuschalten, müssen Betreiber jedoch umdenken. Die Abkündigung bedeutet nicht nur das Ende einer bewährten Technologie, sondern auch eine Aufforderung zur Modernisierung.

Netzwerkprotokoll MQTT

Das MQTT-Netzwerkprotokoll basiert auf dem Prinzip der publish-/subscribe-Architektur. Dadurch verläuft die Kommunikation zwischen den einzelnen Fernwirk-Teilnehmern über einen zentralen Broker, der die ankommenden Nachrichten weiter verteilt. Der SEGNO@smartFWT verwendet den standardisierten Mosquitto MQTT-Broker. Über den Broker werden Istwert und Sollwert Telegramme gesendet bzw. empfangen.

Für die Datenübertragung wird die höchste Stufe des Qualitätslevels QoS2 im SEGNO@FWT verwendet. Damit wird sichergestellt, dass es eine Garan-



SEGNO smartes Fernwirktechnik System

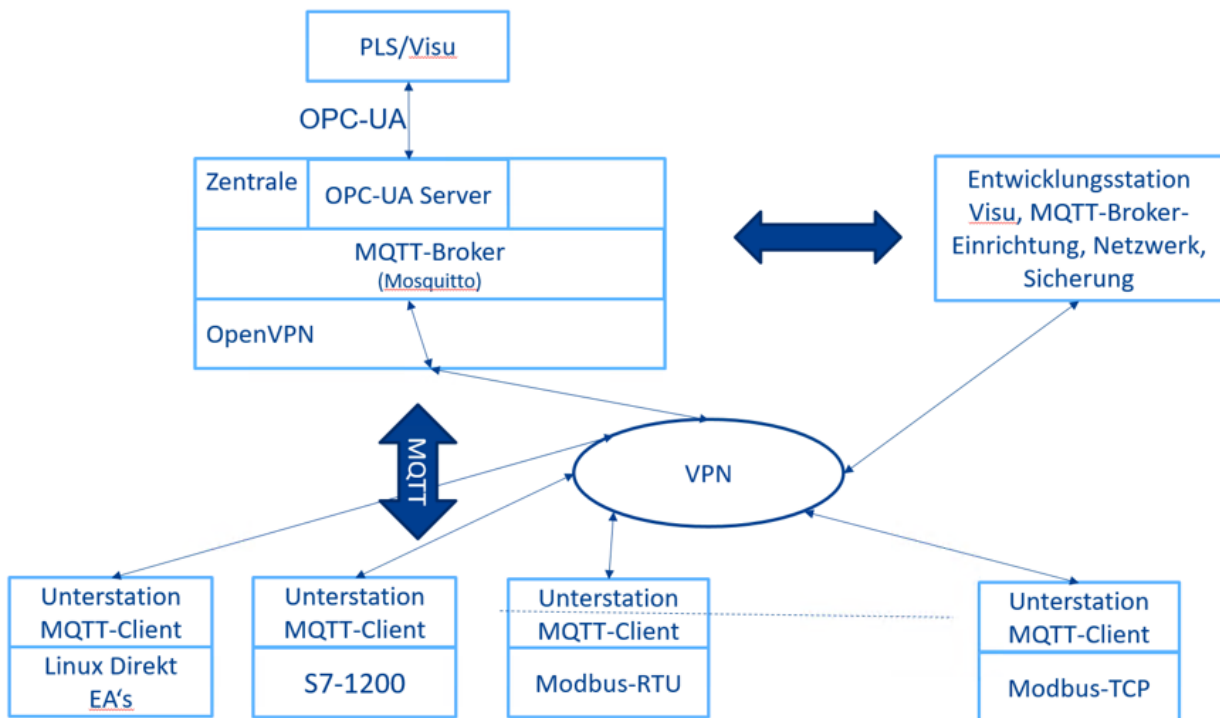


Abbildung: Prinzip SEGNO@smartFWT

Fernwirknetzwerk - IT-Sicherheit

Für das smarte Fernwirk-Netzwerk wird ein virtuelles Server-MultiClient-Netzwerk aufgebaut. Die OpenVPN Community Version lässt sich in verschiedene Modi betrieben. Dabei dient der auf dem Fernwirkrechner installierte OpenVPN als OpenVPN-Server, welcher gleichzeitig Mittelpunkt des virtuellen Netzwerks ist.

Für das Aufsetzen eines virtuellen Server-MultiClient-Netzwerks mit OpenVPN werden passende Zertifikate und Schlüssel für den Server und die Clients angelegt. Mittels eigener PKI (Public Key Infrastructure) und eigener CA (Certificate Authority / Zertifizierungsstelle) erstellen wir für die Authentifizierung sogenannte selbstsignierte

SmartFWT

Stationen / HBG

HBG

Status: Offline

IP: _____

Signalstärke (ASU): 29

Mobile Daten: 18979 MB

Stand: 18.02.2025 12:05:00

[Echtzeit Daten](#)

Ist-Werte		Soll-Werte	
dt_LOCAL	18.02.2025 13:05:00	dt_LOCAL	03.02.2025 08:07:51
dt_UTC	18.02.2025 12:05:00	dt_UTC	03.02.2025 07:07:51
udj_UNIX	21.01.1970 03:18:00	udj_UNIX	21.01.1970 02:56:06
i_0	0	b_active	1
i_1	0	i_0	5
i_2	0	i_1	45
r_0	0	i_2	15
r_1	0	r_0	55.54999923706055
s_0			
udj_0	0	r_1	100
udj_1	0	s_0	15170846644
w_0	4096	udj_0	0
w_000	0	udj_1	0
w_001	0	w_0	0
w_002	0	w_000	0
w_003	0	w_001	0
w_004	0	w_002	0

SEGNO SmartFWT v1.00

Admin

Remote Fernparametrierung

Mit SEGNO@smartFWT steuern und überwachen Sie Ihre Fernwirkstationen bequem über den Webbrowser.

- Einfache Konfiguration ohne zusätzliche Software
- Sichere Fernprogrammierung über VPN-Tunnel
- Benutzerverwaltung für individuelle Zugriffsrechte
- Zertifikatsverwaltung mit intuitiver Menüführung
- Online-Statusanzeige und Stationsdetails auf einen Blick
- Flexible Konfiguration einzelner Datenpunkte

SEGNO@smartFWT Lösung

- Voll in bestehende und neu zu projektierende Leitsysteme integrierbar, wie z.B.: Siemens WinCC, GE iFIX, AVEVA Wonderware InTouch, FlowChief, atvise, Videc ACRON, etc...
- OPC-UA und MQTT Kommunikation dient als Schnittstelle zwischen den Unterstationen und der Leittechnik
- Besondere Maßnahmen für IT-Sicherheit und Datenschutz nach B3S und NIS2 sind umgesetzt
- Standard Fernwirkfunktionalitäten enthalten : Datenzwischenpufferung, automatisches Aktualisieren nach Beseitigung von Verbindungsstörungen , Zeitstempel bei der Datenübertragung, remote Fernparametrierung, umfangreiches Datenlogging u.v.m.
- Konzipiert für herstellernerneutrale und in der Industrie verbreitete Automatisierungs-, IT-Sicherheits- und Leittechnik-Komponenten
- Einfache, praxisnahe Umsetzung und Anpassung für große und kleine Anlagen
- Konfigurierbar über Webbrowser und Konfigurationsoberfläche
- Kombinierbar mit anderen SEGNO-Lösungen, wie Z.B.: SEGNO@Alarm, SEGNO@NetMon, etc..
- Lokaler autarker SMS Versand aus der Unterstation möglich
- Werterhaltung durch die Verwendung von standardisierten Industrie-Komponenten
- Volle Unterstützung für Fernwartung und Fernservice

Einsatzgebiete



- KRITIS Anlagen (Kritische Infrastrukturen nach BSI IT-Sicherheitsgesetz)
- Industrie-Anlagen mit hohen IT-Sicherheitsanforderungen B3S / NIS2
- Industrie-Anlagen mit hoher Produktions-Verfügbarkeit
- Wasser-, Abwasser- und Energieanlagen
- Unabhängigkeit durch Integration herstellernerutraler Leittechnik
- Unabhängigkeit durch Integration herstellernerutraler Automatisierungskomponenten
- Unabhängigkeit durch Integration herstellernerutraler IT-Sicherheits-Komponenten

Eckdaten und Alleinstellungsmerkmale

- Konzipiert für herstellerunabhängige Hardware
- Lokale Installation oder auch als System in der Cloud betreibbar
- Remote Fernprogrammierung
- Stand der Technik zur IT-Sicherheit nach B3S/NIS2
- Sichere Kommunikation über Netzwerkprotokoll MQTT mit QoS2
- niedrige Bandbreite und hohe Zuverlässigkeit
- Industrieprotokoll OPC UA
- geschützte Datentransfer über Zertifikate
- robuste dezentrale Datenzwischenspeicherung
- Unterstützung VPN Tunnel
- lokaler autarker SMS Versand aus der Unterstation möglich

Kontakt

Für weitere Informationen wenden Sie sich bitte an die

SEGNO Industrie Automation GmbH
Admiralstraße 54
28215 Bremen

Telefon: +49 421 792 88-0
email: kontakt@segno.de
www.segno.de

