MANUALE UTENTE

DISPOSITIVI EDGE IIOT

SENECA S.r.l.
Via Austria 26 – 35127 – Z.I. - PADOVA (PD) - ITALY
Tel. +39.049.8705355 – 8705355 Fax +39 049.8706287
www.seneca.it

ORIGINAL INSTRUCTIONS

ATTENZIONE

SENECA non garantisce che tutte le specifiche e/o gli aspetti del prodotto e del firmware, ivi incluso, risponderanno alle esigenze dell'effettiva applicazione finale pur essendo, il prodotto di cui alla presente documentazione, rispondente a criteri costruttivi secondo le tecniche dello stato dell'arte.
L'utilizzatore si assume ogni responsabilità e/o rischio segnatamente alla configurazione del prodotto per il raggiungimento dei risultati previsti in relazione all'installazione e/o applicazione finale specifica.
SENECA, previ accordi al caso di specie, può fornire attività di consulenza per la buona riuscita dell'applicazione finale, ma in nessun caso può essere ritenuta responsabile per il buon funzionamento della stessa.
Il prodotto SENECA è un prodotto avanzato, il cui funzionamento è specificato nella documentazione tecnica fornita con il prodotto stesso e/o scaricabile, anche in un momento antecedente all'acquisto, dal sito internet www.seneca.it.
SENECA adotta una politica di continuo sviluppo riservandosi, pertanto, il diritto di effettuare e/o introdurre - senza necessità di preavviso alcuno – modifiche e/o miglioramenti su qualsiasi prodotto descritto nella presente documentazione.
Il prodotto quivi descritto può essere utilizzato solo ed esclusivamente da personale qualificato per la specifica attività ed in conformità con la relativa documentazione tecnica avendo riguardo, in particolare modo, alle avvertenze di sicurezza.
Il personale qualificato è colui che, sulla base della propria formazione, competenza ed esperienza, è in grado di identificare i rischi ed evitare potenziali pericoli che potrebbero verificarsi nell'utilizzo di questo prodotto.
I prodotti SENECA possono essere utilizzati esclusivamente per le applicazioni e nelle modalità descritte nella documentazione tecnica relativa ai prodotti stessi.
Al fine di garantire il buon funzionamento e prevenire l'insorgere di malfunzionamenti, il trasporto, lo stoccaggio, l'installazione, l'assemblaggio, la manutenzione dei prodotti SENECA devono essere eseguiti nel rispetto delle avvertenze di sicurezza e delle condizioni ambientali specificate nella presente documentazione.
La responsabilità di SENECA in relazione ai propri prodotti è regolata dalle condizioni generali di vendita scaricabili dal sito www.seneca.it.
SENECA e/o i suoi dipendenti, nei limiti della normativa applicabile, non saranno in ogni caso ritenuti responsabili di eventuali mancati guadagni e/o vendite, perdite di dati e/o informazioni, maggiori costi sostenuti per merci e/o servizi sostitutivi, danni a cose e/o persone, interruzioni di attività e/o erogazione di servizi, di eventuali danni diretti, indiretti, incidentali, patrimoniali e non patrimoniali, consequenziali in qualsiasi modalità causati e/o cagionati, dovuti a negligenza, imprudenza, imperizia e/o altre responsabilità derivanti dall'installazione, utilizzo e/o impossibilità di utilizzo del prodotto.

CONTACT US	
Technical support	supporto@seneca.it
Product information	commerciale@seneca.it

Document revisions

DATE	REVISION	NOTES	AUTHOR
31/08/2020	0	First revision	MM
23/09/2020	1	Aggiunta la nuova funzione “Serial Trace” Aggiunta la nuova funzione “Reset di fabbrica” Aggiunta la nuova funzione “Copia Log su USB” da display e da webserver Spostato capitolo REGISTRI MODBUS I/O EMBEDDED	MM
23/09/2020	2	Aggiunto nuovo parametro “Sleep Timeout” in MQTT CONFIGURATION Allineato alla revisione firmware 104	MM
26/11/2020	MI00557-3	Eliminato “opzionale” dalle caratteristiche Wi-Fi	A. Zambolin
15/04/2021	MI00557-4	Allineato alla revisione fw 108	MM
25/08/2021	MI00557-5	Allineato alla revisione fw 109 Aggiunto prodotto R-PASS Eliminato parametro Bandwidth Limitation nel capitolo 21.11	MM
02/05/2022	MI00557-6	Allineato alla revisione fw 109 Aggiunto prodotto R-PASS con 2 porte ethernet	MM
06/05/2022	MI00557-7	Aggiunto prodotto R-PASS-S allineato alla revisione fw 210	MM
15/12/2022	MI00557-8	Aggiunte info su Protocollo SNMP, OPC-UA. Aggiunta supporto a R-COMM Allineato con versione fw 223 Aggiunta lista function block per versioni -S	MM
20/06/2023	MI00557-9	Aggiunte inserite da Service Seneca	AS / MM
28/06/2023	MI00557-10	Aggiunti nuovi modelli Z-PASS1-RT, Z-PASS2-RT, Z-TWS4-RT, Z-PASS2-RT-S. Sostituito VPN BOX con VPNBOX2 Allineato alla revisione SSD/R-PASS fw 232 Allineato alla revisione -RT fw 1012	MM
03/07/2023	MI00557-11	Piccole correzioni	AZ
20/07/2023	MI00557-12	Riportate correzioni al capitolo 11.2 (MQTT client)	MM
21/12/2023	MI00557-13	Aggiunto il capitolo “Comandi SMS”	AZ
14/11/2024	MI00557-14	Riscritto il manuale per nuova versione di firmware rev 3xxx Aggiunto modello SSD-S Aggiunto modello SSD-E Aggiornato alla rev fw 3100	MM
26/11/2024	MI00557-15	Aggiornato alla rev fw 3120 Aggiunta azione script execution	MM
27/11/2024	MI00557-16	Aggiunto capitolo su creazione chiavi per accesso SSH al dispositivo	MM

INDICE

1. INTRODUZIONE

ATTENZIONE!

Questo manuale utente estende le informazioni dal manuale di installazione sulla configurazione del dispositivo. Utilizzare il manuale di installazione per maggiori informazioni.

ATTENZIONE!

In ogni caso, SENECA s.r.l. o i suoi fornitori non saranno responsabili per la perdita di dati / incassi o per danni consequenziali o incidentali dovuti a negligenza o cattiva/impropria gestione del dispositivo, anche se SENECA è ben consapevole di questi possibili danni.
SENECA, le sue consociate, affiliate, società del gruppo, i suoi fornitori e rivenditori non garantiscono che le funzioni soddisfino pienamente le aspettative del cliente o che il dispositivo, il firmware e il software non debbano avere errori o funzionare continuativamente.

I gateway SENECA IIoT EDGE sono componenti fondamentali dell'automazione industriale e offrono una serie di funzionalità che favoriscono l'efficienza e l'affidabilità. Questi gateway fungono da sentinelle digitali della fabbrica, combinando funzioni di supervisione, diagnostica, elaborazione e archiviazione dei dati in un'unica unità compatta.

La **supervisione** è la prima linea di difesa, in quanto i gateway IIoT EDGE monitorano continuamente la salute e le prestazioni dei dispositivi di campo connessi, raccolgono dati in tempo reale e forniscono informazioni che consentono la manutenzione predittiva, riducendo i tempi di inattività e i costi operativi.

Anche le **capacità diagnostiche** sono fondamentali. Questi gateway utilizzano analisi avanzate per rilevare anomalie e deviazioni dal comportamento previsto. In questo modo, consentono la risoluzione proattiva dei problemi, prevenendoli prima che si aggravino. Il risultato è un tempo di attività più elevato e una produzione più costante.

La **potenza di elaborazione** è un'altra caratteristica fondamentale. I gateway IIoT EDGE possiedono la potenza di calcolo necessaria per eseguire operazioni di elaborazione dei dati al volo. Possono pre-elaborare i dati alla fonte, filtrandoli, aggregandoli o trasformandoli prima di inviarli al cloud o ai sistemi centrali. Questo riduce al minimo l'utilizzo della larghezza di banda e la latenza, massimizzando il valore dei dati.

L'**archiviazione dei dati** è essenziale per il buffering e l'archiviazione dei dati a livello locale. In caso di interruzioni della rete, questi gateway assicurano che i dati critici non vadano persi e, inoltre, facilitano l'analisi storica e la creazione di report, consentendo di prendere decisioni informate.

La **gestione in tempo reale** dei dispositivi di campo è il tratto distintivo di questi gateway, sono in grado di configurare, aggiornare e controllare in remoto le apparecchiature industriali, consentendo agli operatori di rispondere prontamente a condizioni mutevoli o a situazioni di emergenza. Questa capacità semplifica le operazioni e migliora la resilienza complessiva del sistema.

La **sicurezza** è fondamentale e i gateway IIoT EDGE eccellono in questo aspetto. Stabiliscono connessioni VPN sicure ai sistemi di controllo centrali, criptando i dati in transito e, inoltre, applicano controlli di accesso, assicurando che solo il personale autorizzato possa interagire con essi, salvaguardandosi dalle minacce informatiche. Questi gateway sono conformi ai più severi standard di cybersecurity, a partire dalla conformità ai test di penetrazione condotti secondo OWASP, NIST 800 115 Risk Analysis e IEC 62443.

I gateway IIoT EDGE sono indispensabili nelle moderne realtà industriali. Essi fungono da intelligence in prima linea, offrendo funzionalità di supervisione, diagnostica, elaborazione e archiviazione dei dati. Le connessioni VPN sicure e la gestione dei dispositivi in tempo reale ne fanno il perno di operazioni industriali efficienti, reattive e sicure.

1.1. FIRMWARE CON GPL OPEN SOURCE

I firmware possono contenere anche software Open Source sotto contratto GPL. Secondo la Sezione 3b della GPL, è possibile ottenere il codice sorgente relativo a queste parti. Il codice sorgente con i termini di licenza del software Open Source può essere ottenuto su richiesta da Seneca s.r.l..
Inviate la vostra richiesta a supporto@seneca.it con oggetto "Open Source".

2. MODELLI

La serie di Gateway Edge IIOT è composta dai seguenti modelli:

MODELLO	*I/O DIGITALI*	*INGRESSI ANALOGICI*	*DISPLAY*	*PLC STRATON*	*MODEM 4G*	*UPS INTEGRATO*	*PORTE SERIALI*	*PORTE ETHERNET*	*PORTA CAN*	*WIFI*	*PROTOCOLLI IEC61850 IEC60870*
SSD	2 DIDO	NO	7" TOUCH + VIRTUALE	NO	NO	NO	2	2	NO	SI'	NO
SSD-S	2 DIDO	NO	7" TOUCH + VIRTUALE	SI'	NO	NO	2	2	NO	SI'	NO
SSD-E	2 DIDO	NO	7" TOUCH + VIRTUALE	SI'	NO	NO	2	2	NO	SI'	SI'
R-PASS	4DI 4DO	2	VIRTUALE	NO	OPZIONALE	OPZIONALE	2	4 (1+3 in switch)	SI'	OPZIONALE	NO
R-PASS-S	4DI 4DO	2	VIRTUALE	SI'	OPZIONALE	OPZIONALE	2	4 (1+3 in switch)	SI'	OPZIONALE	NO
R-PASS-E	4DI 4DO	2	VIRTUALE	SI'	OPZIONALE	OPZIONALE	2	4 (1+3 in switch)	SI'	OPZIONALE	SI'
Z-PASS1-RT	6 DIDO	2	VIRTUALE	NO	NO	NO	3	2	SI'	NO	NO
Z-TWS4-RT	6 DIDO	2	VIRTUALE	SI'	NO	NO	3	2	SI'	NO	NO
Z-TWS4-RT-E	6 DIDO	2	VIRTUALE	SI'	NO	NO	3	2	SI'	NO	SI'
Z-PASS2-RT-4G	6 DIDO	2	VIRTUALE	NO	SI'	NO	3	2	SI'	NO	NO
Z-PASS2-RT-4G-S	6 DIDO	2	VIRTUALE	SI'	SI'	NO	3	2	SI'	NO	NO
Z-PASS2-RT-4G-E	6 DIDO	2	VIRTUALE	SI'	SI'	NO	3	2	SI'	NO	SI'

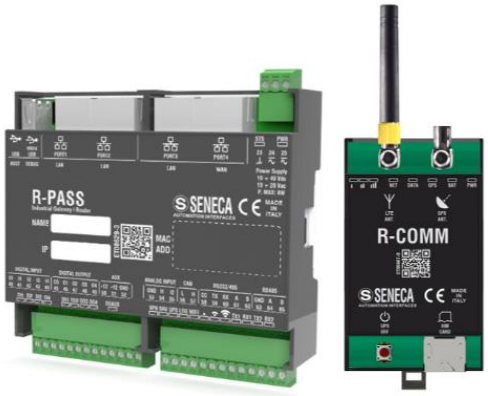
N.B. A seconda del modello, la porta CAN potrebbe essere disponibile ma non gestita dalla revisione firmware.

2.1. DESCRIZIONE DEI MODELLI

2.1.1.SSD / SSD-S / SSD-E

Surprise Smart Display è un display a colori sensibile al tocco (touch panel capacitivo) da 7 pollici HMI, con risoluzione
800 x 480 e retroilluminazione a LED.
È anche un terminale operatore progettato per il controllo e il monitoraggio del funzionamento di dispositivi, impianti o linee di produzione.
Smart Display offre inoltre una connettività estesa grazie alle le funzionalità di Industrial Gateway, Serial Device Server, Bridge e WI-FI, è inoltre dotato di un numero di protocolli industriali in continuo aumento.
Una novità introdotta nel mondo dell'automazione industriale è la possibilità di visualizzare variabili del protocollo Modbus RTU in modalità completamente passiva (sniffer seriale).
L'applicativo software precaricato consente la visualizzazione parametri, l'invio di comandi, la configurazione dei tag, della comunicazione, delle singole pagine video e la gestione allarmi.
Include il supporto all'ultima versione di LET'S VPN per la manutenzione e il monitoraggio di dispositivi remoti.
È disponibile anche la versione -S che include il PLC Straton IEC 61131.
La versione -E oltre ad includere il PLC Straton dispone delle licenze per i protocolli di energy management IEC61850 e IEC60870.

2.1.2.R-PASS / R-PASS-S / R-PASS-E



R-PASS è un dispositivo progettato per il controllo e il monitoraggio del funzionamento di dispositivi,
Impianti o linee di produzione, offre inoltre una connettività estesa grazie alle le funzionalità di Industrial Gateway, Serial Device Server, Bridge e WI-FI, è inoltre dotato di un numero di protocolli industriali in continuo aumento soprattutto nel settore IOT.
Una novità introdotta nel mondo dell'automazione industriale è la possibilità di visualizzare variabili del protocollo Modbus RTU in modalità completamente passiva (sniffer seriale).
È anche dotato di un display virtuale accessibile da qualunque dispositivo tramite un browser web.
Include il supporto all'ultima versione di LET'S VPN per la manutenzione e il monitoraggio di dispositivi remoti.
È disponibile anche la versione -S che include il PLC Straton IEC 61131.
È possibile agganciare al dispositivo l'opzione R-COMM che include un modem 4G e un UPS (opzionale).
È disponibile il modello con 4 porte ethernet, con e senza WIFI.
Per maggiori informazioni sul PLC Straton fare riferimento al sito internet: https://straton-plc.com/en/
La versione -E oltre ad includere il PLC Straton dispone delle licenze per i protocolli di energy management IEC61850 e IEC60870.

2.1.3.Z-PASS1-RT / Z-TWS4-RT / Z-TWS4-RT-E

Z-PASS1-RT/Z-TWS4-RT è un dispositivo progettato per il controllo e il monitoraggio del funzionamento di dispositivi,

Impianti o linee di produzione, offre inoltre una connettività estesa grazie alle le funzionalità di Industrial Gateway, Serial Device Server e Bridge, è inoltre dotato di un numero di protocolli industriali in continuo aumento soprattutto nel settore IOT.
Una novità introdotta nel mondo dell'automazione industriale è la possibilità di visualizzare variabili del protocollo Modbus RTU in modalità completamente passiva (sniffer seriale).
È anche dotato di un display virtuale accessibile da qualunque dispositivo tramite un browser web.
Include il supporto all'ultima versione di LET'S VPN per la manutenzione e il monitoraggio di dispositivi remoti.
È disponibile anche la versione Z-TWS4-RT che include il PLC Straton IEC 61131.
Per maggiori informazioni sul PLC Straton fare riferimento al sito internet: https://straton-plc.com/en/
La versione -E oltre ad includere il PLC Straton dispone delle licenze per i protocolli di energy management IEC61850 e IEC60870.

2.1.4.Z-PASS2-RT-4G / Z-PASS2-RT-4G-S / Z-PASS2-RT-4G-E

Z-PASS2-RT-4G è un dispositivo progettato per il controllo e il monitoraggio del funzionamento di dispositivi, Impianti o linee di produzione, offre inoltre una connettività estesa grazie alle le funzionalità di Industrial Gateway, Serial Device Server e Bridge, è inoltre dotato di un numero di protocolli industriali in continuo aumento soprattutto nel settore IOT.
Una novità introdotta nel mondo dell'automazione industriale è la possibilità di visualizzare variabili del protocollo Modbus RTU in modalità completamente passiva (sniffer seriale).
È anche dotato di un display virtuale accessibile da qualunque dispositivo tramite un browser web.
Include il supporto all'ultima versione di LET'S VPN per la manutenzione e il monitoraggio di dispositivi remoti.
Integra un modem 4G universale di ultima generazione.
È disponibile anche la versione -S che include il PLC Straton IEC 61131.
Per maggiori informazioni sul PLC Straton fare riferimento al sito internet: https://straton-plc.com/en/
La versione -E oltre ad includere il PLC Straton dispone delle licenze per i protocolli di energy management IEC61850 e IEC60870.

2.2. OPZIONI HARDWARE E SOFTWARE

I dispositivi sono disponibili in vari formati hardware e con caratteristiche software differenti.
Tutte le caratteristiche software possono essere acquistate al momento dell'ordine oppure acquistate in un secondo momento. Lo sblocco delle funzionalità software avviene tramite l'inserimento di una chiave nell'apposita pagina del webserver del dispositivo.

2.2.1.SSD

Smart Display dispone delle seguenti opzioni hardware:

OPZIONI HARDWARE	DESCRIZIONE
SMART DISPLAY	DISPLAY 7" CON TOUCH CAPACITIVO NR 2 DIGITAL INPUT

	NR 2 DIGITAL OUTPUT NR 2 ETHERNET INDIPENDENTI WI-FI / ROUTER WI-FI NR 1 PORTA USB HOST
Z-MBUS	CONVERTITORE PER PROTOCOLLO MBUS (METERBUS)

E delle seguenti opzioni software (i pacchetti sono attivabili anche più di uno contemporaneamente), è possibile acquistare le licenze contattando direttamente Seneca.

OPZIONI SOFTWARE	DESCRIZIONE
PACCHETTO INCLUSO	Display Grafico con widget e sinottici Display virtuale con widget e sinottici Datalogger max 2000 tag con scalature Allarmi Gateway/Router/Firewall Gateway ethernet-seriale Sniffer seriale Protocollo Modbus TCP Client/Server Protocollo Modbus RTU Master/Slave Protocollo OPC-UA server
PACCHETTO “IOT”	Protocollo http e MQTT per connessione ai cloud con tecnologia “Easy Cloud”
PACCHETTO “LOGICHE”	Logiche programmabili tramite “IF THEN ELSE” Allarmistica Remota
PACCHETTO VPN “SENECA LET’S”	Connessione VPN semplificata tramite ambiente “Seneca LET’s VPN” e supporto a VPNBOX2 Oppure Open VPN Standard

PACCHETTO PLC STRATON (-S)	Permette di attivare il PLC Straton IEC 61131 Protocolli aggiuntivi forniti: Modbus RTU, Modbus TCP-IP, MQTT, OPC-UA Client, MeterBus, S7 Client, SNMP
PACCHETTO PROTOCOLLI ENERGIA (-E)	Permette di attivare il PLC Straton e le licenze per i protocolli aggiuntivi IEC61850, IEC60870, Modbus RTU, Modbus TCP-IP, MQTT, OPC-UA Client, MeterBus, S7 Client, SNMP

2.2.2. R-PASS

R-PASS dispone delle seguenti opzioni hardware:

OPZIONI HARDWARE	DESCRIZIONE
R-PASS	NR 4 DIGITAL INPUT NR 4 DIGITAL OUTPUT NR 4 TOTALI: NR 1 ETHERNET INDIPENDENTE + NR 3 IN SWITCH TRA LORO NR 1 PORTA USB HOST
R-PASS-W	NR 4 DIGITAL INPUT NR 4 DIGITAL OUTPUT NR 4 TOTALI: NR 1 ETHERNET INDIPENDENTE + 3 IN SWITCH TRA LORO WIFI
R-COMM-0-4GWW	MODEM 4G GLOBAL
R-COMM-B-4GWW	MODEM 4G GLOBAL + UPS A BATTERIA
Z-MBUS	CONVERTITORE PER PROTOCOLLO MBUS (METERBUS)

E delle seguenti opzioni software (i pacchetti sono attivabili anche più di uno contemporaneamente), è possibile acquistare le licenze contattando direttamente Seneca.

OPZIONI SOFTWARE	DESCRIZIONE
PACCHETTO INCLUSO	Display virtuale con widget e sinottici

	Datalogger max 2000 tag con scalature Allarmi Gateway/Router/Firewall Gateway ethernet-seriale Sniffer seriale Protocollo Modbus TCP Client/Server Protocollo Modbus RTU Master/Slave Protocollo OPC-UA server Protocollo http e MQTT per connessione ai cloud con tecnologia “Easy Cloud” Logiche programmabili tramite “IF THEN ELSE” Connessione VPN semplificata tramite ambiente “Seneca LET’s VPN” e supporto a VPNBOX2 Oppure Open VPN Standard
PACCHETTO PLC STRATON (-S)	Permette di attivare il PLC Straton IEC 61131 Protocolli aggiuntivi forniti: Modbus RTU, Modbus TCP-IP, MQTT, OPC-UA Client, MeterBus, S7 Client, SNMP
PACCHETTO PROTOCOLLI ENERGIA (-E)	Permette di attivare il PLC Straton e le licenze per i protocolli aggiuntivi IEC61850, IEC60870, Modbus RTU, Modbus TCP-IP, MQTT, OPC-UA Client, MeterBus, S7 Client, SNMP

2.2.3.Z-PASS1-RT / Z-TWS4-RT

Z-PASS1-RT / Z-TWS4-RT dispone delle seguenti opzioni hardware:

OPZIONI HARDWARE	DESCRIZIONE
Z-PASS1-RT / Z-TWS4-RT	NR 6 DIGITAL INPUT/OUTPUT CONFIGURABILI NR 2 ANALOG INPUT 0-10V / 0-20 mA NR 2 ETHERNET INDIPENDENTI NR 1 PORTA USB HOST NR 1 SLOT SD CARD
Z-MBUS	CONVERTITORE PER PROTOCOLLO MBUS (METERBUS)

OPZIONI SOFTWARE	DESCRIZIONE
PACCHETTO INCLUSO	Display virtuale con widget e sinottici Datalogger max 2000 tag con scalature Allarmi Gateway/Router/Firewall Gateway ethernet-seriale Sniffer seriale Protocollo Modbus TCP Client/Server Protocollo Modbus RTU Master/Slave Protocollo OPC-UA server Protocollo http e MQTT per connessione ai cloud con tecnologia “Easy Cloud” Logiche programmabili tramite “IF THEN ELSE”

	Connessione VPN semplificata tramite ambiente “Seneca LET’s VPN” e supporto a VPNBOX2 Oppure Open VPN Standard
PACCHETTO PLC STRATON (-S) (GIA’ INCLUSO NEL SOLO MODELLO Z-TWS4-RT)	Permette di attivare il PLC Straton IEC 61131 Protocolli aggiuntivi forniti: Modbus RTU, Modbus TCP-IP, MQTT, OPC-UA Client, MeterBus, S7 Client, SNMP
PACCHETTO PROTOCOLLI ENERGIA (-E)	Permette di attivare il PLC Straton e le licenze per i protocolli aggiuntivi IEC61850, IEC60870, Modbus RTU, Modbus TCP-IP, MQTT, OPC-UA Client, MeterBus, S7 Client, SNMP

2.2.4.Z-PASS2-RT-4G

Z-PASS2-RT-4G dispone delle seguenti opzioni hardware:

OPZIONI HARDWARE	DESCRIZIONE
Z-PASS2-RT-4G	NR1 MODEM 4G GLOBAL + GNSS NR 6 DIGITAL INPUT/OUTPUT CONFIGURABILI NR 2 ANALOG INPUT 0-10V / 0-20 mA NR 2 ETHERNET INDIPENDENTI NR 1 PORTA USB HOST NR 1 SLOT SD CARD
Z-MBUS	CONVERTITORE PER PROTOCOLLO MBUS (METERBUS)

OPZIONI SOFTWARE	DESCRIZIONE
PACCHETTO INCLUSO	Display virtuale con widget e sinottici Datalogger max 2000 tag con scalature Allarmi

	Gateway/Router/Firewall Sniffer seriale Gateway ethernet-seriale Protocollo Modbus TCP Client/Server Protocollo Modbus RTU Master/Slave Protocollo OPC-UA server Protocollo http e MQTT per connessione ai cloud con tecnologia “Easy Cloud” Logiche programmabili tramite “IF THEN ELSE” Connessione VPN semplificata tramite ambiente “Seneca LET’s VPN” e supporto a VPNBOX2 Oppure Open VPN Standard
PACCHETTO PLC STRATON (-S)	Permette di attivare il PLC Straton IEC 61131 Protocolli aggiuntivi forniti: Modbus RTU, Modbus TCP-IP, MQTT, OPC-UA Client, MeterBus, S7 Client, SNMP
PACCHETTO PROTOCOLLI ENERGIA (-E)	Permette di attivare il PLC Straton e le licenze per i protocolli aggiuntivi IEC61850, IEC60870, Modbus RTU, Modbus TCP-IP, MQTT, OPC-UA Client, MeterBus, S7 Client, SNMP

3. INDIRIZZI IP

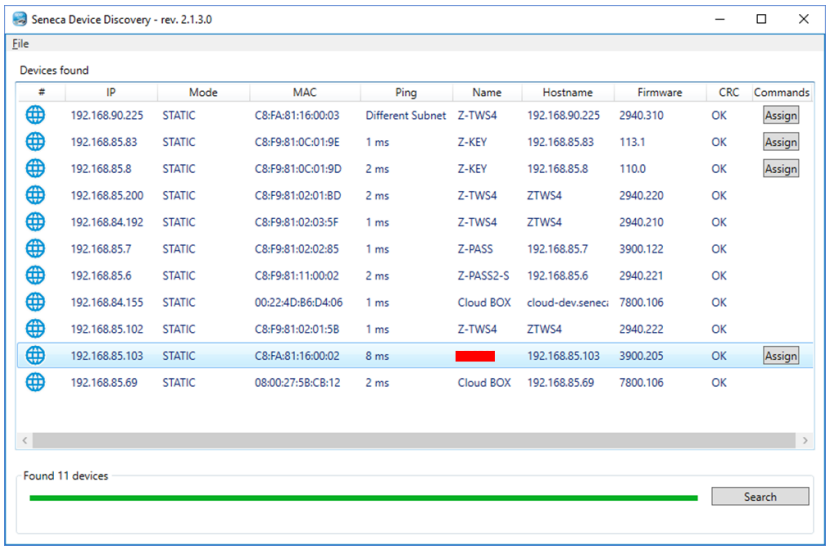
3.1. INDIRIZZI IP DI FABBRICA

I dispositivi escono di fabbrica con la seguente configurazione:

PORTA ETHERNET “LAN”	IP statico: 192.168.90.101
PORTA ETHERNET “WAN”	DHCP attivo
WI-FI	Non attiva (dove presente)

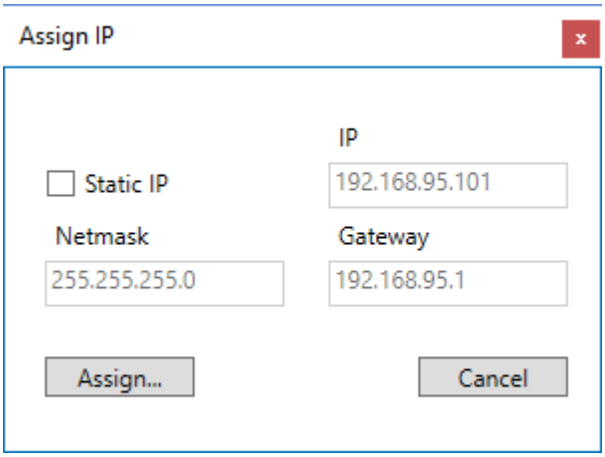
3.2. RICERCA DELL’INDIRIZZO IP

I dispositivi escono di fabbrica con l'indirizzo IP di default 192.168.90.101, su Ethernet (LAN),
Se questo indirizzo viene modificato o dimenticato, può essere recuperato utilizzando il software "Seneca Device Discovery".

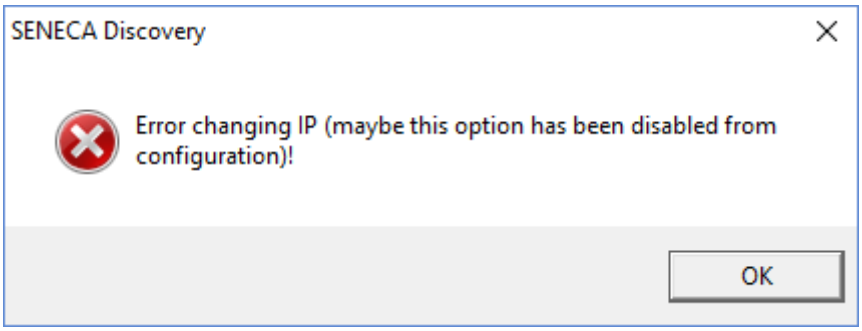


Questa applicazione mostra l'indirizzo IP, l'indirizzo MAC, la versione FW e alcune altre informazioni utili, per ogni dispositivo SENECA trovato nella LAN.

Inoltre, cliccando sul pulsante "Assegna", è possibile modificare i parametri di configurazione della rete di un dispositivo, come mostrato nella figura seguente:



Per motivi di sicurezza, questa funzione può essere disabilitata sul dispositivo, in questo caso, dopo aver cliccato sul pulsante "Assegna" viene visualizzato il seguente messaggio di errore".



Il software può essere facilmente installato eseguendo il programma di installazione disponibile al seguente link: http://www.seneca.it/products/sdd

NOTA:
L'indirizzo IP mostrato dall software Seneca Discovery Device è l'indirizzo IP della periferica LAN quando il PC è collegato alla porta LAN, l'indirizzo IP WAN quando il PC è collegato alla porta WAN e del WI-FI nel caso si sia collegati a quest'ultimo; inoltre, le modifiche dei parametri di configurazione della rete si applicano alla relativa periferica.

4. ACCESSO AI WEBSERVER DEI DISPOSITIVI

I dispositivi IIOT sono dotati di due webserver:

- Il webserver con il display virtuale
- Il webserver di configurazione

4.1. ACCOUNT DEL WEBSERVER DI CONFIGURAZIONE

Oltre all'account "ADMIN" sono presenti anche gli account "guest" e "operator":

4.1.1. WEBSERVER DI CONFIGURAZIONE CON ACCOUNT "GUEST"

È possibile accedere al sito di configurazione del dispositivo con account "guest"; a tale account non è consentito accedere a tutte le pagine ma è possibile visualizzare tutti i parametri di configurazione e le informazioni di stato, senza poterli modificare; quindi, in tutte le pagine, i pulsanti "APPLY" (e ogni altro pulsante utilizzato per effettuare modifiche) sono disabilitati.
Per accedere con account "guest", collegare il browser all'indirizzo IP del dispositivo sulla porta 8080, ad esempio:
http://192.168.90.101:8080
e, quando richiesto, fornire le seguenti credenziali (valori predefiniti):
Nome utente: guest
Password: guest

4.1.2. WEBSERVER DI CONFIGURAZIONE CON ACCOUNT "OPERATOR"

È possibile accedere al sito di configurazione del dispositivo con account "operator"; questo account può configurare solo gli indirizzi IP.
Per accedere con account "operator", collegarsi al browser all'indirizzo IP del dispositivo sulla porta 8080, ad esempio:
http://192.168.90.101:8080
e, quando richiesto, fornire le seguenti credenziali (valori predefiniti):
Nome utente: operator
Password: operator

4.2. PRIMO ACCESSO AI WEBSERVER

I dispositivi sono accessibili di fabbrica dalla porta ethernet "LAN" con l'indirizzo ip statico 192.168.90.101
I webserver sono disponibili via http e/o https (a seconda della configurazione). Di default sono attivi entrambi i protocolli.

Su protocollo http il webserver con il display virtuale si trova nella porta 80 (default per i browser), digitare quindi:

http://192.168.90.101

mentre quello https è:

https://192.168.90.101

Diversamente il webserver su protocollo http per la configurazione si trova nella porta 8080, quindi:

http://192.168.90.101:8080

mentre per l' https:

https://192.168.90.101/maintenance

Nome utente: admin
Password: admin

4.3. WEBSERVER CON IL DISPLAY VIRTUALE

Per maggiori informazioni su questo Webserver fare riferimento al relativo capitolo di questo manuale.

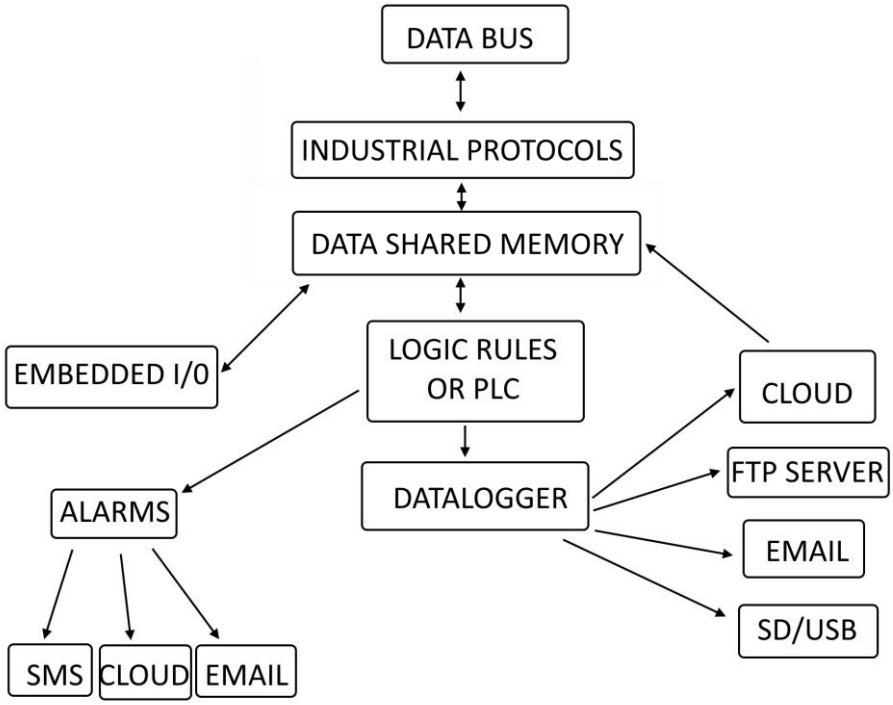
4.4. WEBSERVER DI CONFIGURAZIONE

Per maggiori informazioni su questo Webserver fare riferimento al relativo capitolo di questo manuale.

5. ACQUISIZIONE ED ELABORAZIONE DEI DATI, GENERAZIONE E INVIO DI ALLARMI, INVIO DI DATI

I dispositivi Edge IIOT permettono di acquisire dati dagli IO embedded dei dispositivi o dai bus (tramite i protocolli di comunicazione industriale), questi dati sono salvati in una memoria condivisa (shared) e possono essere elaborati tramite scalature oppure tramite le regole logiche oppure tramite il PLC straton. Una volta elaborati i dati è possibile salvarli in un dispositivo di storage esterno (USB o SD card) oppure inviarli verso i cloud o server FTP/Email etc…
Gli allarmi sono generati dalle regole logiche e possono essere inviati anch'essi ai cloud o via Email/SMS.

Si faccia riferimento al seguente al seguente schema a blocchi:



L'acquisizione dei dati (Tag) nei bus (Data Bus) avviene attraverso i protocolli industriali (Industrial Protocols) o tramite acquisizione diretta degli I/O integrati (Embedded I/O).
Questi dati confluiscono nella memoria condivisa (Data Shared Memory), in questa memoria le regole logiche o il PLC eseguono le elaborazioni dei dati (Logic Rules or PLC).
Il datalogger acquisisce i dati elaborati e li archivia tramite i protocolli client (su Cloud, FTP server, Email, SD card, Usb storage).
Le regole logiche o il PLC generano allarmi che possono essere inviati via EMAIL, Cloud o SMS.
Il Cloud può accedere e quindi scrivere i dati già elaborati nella memoria condivisa (Shared Memory).
Di seguito analizzeremo i principali componenti dello schema a blocchi.

5.1. IL DATA BUS E I PROTOCOLLI INDUSTRIALI

Tipicamente i dati risiedono in dispositivi esterni e devono essere connessi tramite protocolli industriali.
Il dispositivo include una serie di protocolli industriali in modo da potersi connettere con i più svariati produttori di terze parti.
Tra i più importanti protocolli citiamo i protocolli Modbus e il protocollo OPC-UA

5.1.1. PROTOCOLLI MODBUS

Modbus è nato come protocollo di comunicazione seriale da Modicon (azienda ora parte del gruppo Schneider Electric) per mettere in comunicazione i propri controllori logici programmabili (PLC). È diventato uno standard de facto nella comunicazione di tipo industriale, ed attualmente è uno dei protocolli di connessione più diffusi al mondo fra i dispositivi elettronici industriali. Oltre alla versione seriale i dispositivi Seneca supportano anche quella basata su Ethernet.
I protocolli Modbus supportati sono:

Protocollo Modbus RTU Master
Protocollo Modbus RTU Slave
Protocollo Modbus TCP-IP Client
Protocollo Modbus TCP-IP Server

Per maggiori informazioni si faccia riferimento al sito:

https://modbus.org/

Grazie a questi protocolli è possibile acquisire le variabili in memoria direttamente da dispositivi esterni Modbus RTU slave o Modbus TCP-IP server.

5.1.2. PROTOCOLLO OPC-UA

OPC Unified Architecture (OPC-UA) è un protocollo di comunicazione standardizzato da macchina a macchina per l'industria 4.0 sviluppato da OPC Fundation.
OPC-UA è un protocollo di comunicazione indipendente dal fornitore e si basa sul principio client-server.
I dispositivi Seneca supportano il protocollo server OPC-UA anche con security policy.

Per maggiori informazioni si faccia riferimento al sito:

https://opcfoundation.org/

In particolare, il server OPC-UA "esporta" i tag nella memoria interna e quindi, utilizzando un OPC-UA client o un altro protocollo client sarà possibile leggere e scrivere direttamente tutti i tag.

5.2. LA SHARED MEMORY (MEMORIA CONDIVISA) E I TAG

I dati acquisiti dai bus o dagli I/O integrati nei dispositivi confluiscono nella memoria condivisa, questa memoria è accessibile dall'esterno del dispositivo con vari protocolli (ad esempio OPC-UA o Modbus TCP-IP o RTU).
Ogni dato è individuato da un nome mnemonico e da un tipo (intero, a virgola mobile etc…), così caratterizzato prende il nome di "Tag".
Su questi Tag è possibile effettuare vari tipi di elaborazioni come vedremo più avanti nel manuale.

5.3. IL DATALOGGER

I Gateway IIOT Edge Seneca includono un potente datalogger che permette di gestire fino a 2000 variabili contemporaneamente (TAG). È anche possibile scalare ciascuna variabile ed effettuare ulteriori elaborazioni con il PLC o con le regole logiche. I dati acquisiti dal datalogger possono poi essere inviati ai diversi cloud/FTP/EMAIL o alle memorie USB/SD.

Per la funzionalità Quando la funzionalità gateway è impostata a "Modbus Gateway con Shared Memory" nel dispositivo è possibile attivare anche la modalità "Data Logger":

I valori dei tag vengono periodicamente memorizzati in file (chiamati "log files"), che possono poi essere trasferiti.

I tag possono essere associati ad un massimo di quattro gruppi di Data Logger, che possono avere diversi periodi di campionamento e periodi di trasferimento.

Attualmente sono supportati i seguenti metodi di "trasferimento":

- copiato su chiavetta USB / SD card
- trasferito su un server FTP
- inviato a uno o più indirizzi e-mail, come allegato
- Inviato ad un server via http post
- Inviato ad un broker MQTT

Possono essere abilitati anche più di uno dei metodi di cui sopra contemporaneamente.

I file di log sono memorizzati nella memoria flash, quindi, se uno dei metodi di trasferimento temporaneamente fallisce, questo può essere trasferito con successo in un secondo momento.

Per ogni gruppo di data logger, la "cache" si riempie se è raggiunto almeno uno dei seguenti casi:

- 1000 file di log
- 500000/(numero di gruppi abilitati) campioni (cioè numero di linee di un singolo file di log)

Quando viene raggiunto il limite, si verifica la "rotazione" della cache, cioè i file più vecchi vengono sovrascritti dal nuovo.

I protocolli a file (copia su USB/SD card, invio EMAIL o su FTP) utilizzano file di log del tipo "csv" standard, possono quindi essere elaborati da Excel™ o da software PC.

Ecco una porzione di un file di log di esempio:

```
INDEX;TYPE;TIMESTAMP;ZPASS_DI;ZPASS_DO;ZPASS_DI_1;ZPASS_DI_2;ZPASS_DI_3;ZPASS_DI_4;ZPASS_DO_1;ZPASS_
DO_2;ZPASS_DO_3;ZPASS_DO_4;GPS_ERROR;GPS_HOUR;GPS_MINUTE;GPS_SECOND;GPS_DAY;GPS_MONTH;GPS_YEAR;GPS_L
ATITUDE;GPS_LONGITUDE;GPS_HDOP;GPS_ALTITUDE;GPS_COG;GPS_SPEED_KM;GPS_SPEED_KN;GPS_FIX;GPS_NUM_SAT;SH
M_TAG1;ZPASS2_105_TAG1;ZPASS2_106_TAG1;ZPASS2_106_TAG2
1;LOG;29/05/2018 09:49:45;0;0;0;0;0;0;0;0;0;0;7;49;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;4;0;32767;14;11.5
2;LOG;29/05/2018 09:49:50;0;0;0;0;0;0;0;0;0;0;7;49;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;4;0;32767;14;11.5
3;LOG;29/05/2018 09:49:55;0;0;0;0;0;0;0;0;0;0;7;49;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;4;0;32767;14; 11.5
4;LOG;29/05/2018 09:50:00;0;0;0;0;0;0;0;0;0;0;7;49;31;29;5;18;45.37417;11.94554;1.5;12.7;249.56;0;0;2;4;0;32767;14;11.5
```

Se per un tag il valore effettivo non è disponibile (ad esempio, se il tag corrisponde ad un registro che non risponde alle richieste Modbus), il valore scritto nel campo corrispondente del file di log può essere impostato ad "`ERR!`"
Il parametro "ERROR MODE" può essere impostato anche su LAST VALUE oppure su un valore di FAIL definito dall'utente.

Si prega di notare che ogni volta che viene effettuata una modifica della configurazione che influisce sulla funzionalità del Data Logger (da una pagina della sezione "Datalogger") viene eseguita la seguente procedura:

- I processi del Data Logger vengono interrotti
- La cache dei file di log viene cancellata

5.4. ELABORAZIONE DEI TAG: LE REGOLE LOGICHE E IL PLC STRATON

Nel dispositivo è possibile utilizzare due principali forme di elaborazione dei Tag.
La prima è attraverso le regole logiche, la seconda è attraverso un PLC (opzionale).
Per maggiori informazioni fare riferimento ai rispettivi capitoli del presente manuale.

5.5. CONNESSIONE AI CLOUD TRAMITE TECNOLOGIA "EASY CLOUD"

La tecnologia "Easy Cloud" si basa sul protocollo MQTT e permette la connessione bidirezionale con i principali cloud disponibili.

Alcuni dei cloud a cui i dispositivi possono connettersi sono:

Cumulocity IoT ADM4.0 ANALISI DATI MACCHINA onsystem

5.6. ALLARMI

Per l'allarmistica dei TAG sono disponibili una serie completa di parametri, come indicato nella pagina "Alarm Configuration" del webserver.
L'intero stato degli allarmi può essere visualizzato nella pagina "Alarm Summary" e lo storico degli allarmi può essere recuperato nella pagina "Alarm History".
Inoltre, nella pagina "Tag View", le colonne "ALARM" e "ANALOG DANGER ALARM" mostrano lo stato corrente degli allarmi per ogni tag.
La generazione di allarmi è gestita attraverso le regole logiche oppure direttamente dal PLC Straton (opzionale).

6. VISUALIZZAZIONE GRAFICA DEI DATI SUL DISPLAY / DISPLAY VIRTUALE

I Gateway IIOT Edge Seneca includono una potente interfaccia grafica, a seconda dei modelli è presente un display fisico da 7" touch e/o un display virtuale accessibile tramite un browser web. Tutto ciò che è possibile fare nel display reale è disponibile anche in quello virtuale, il tocco delle dita è sostituito dal puntatore e il pulsante del mouse.

Il display è composto da 3 sezioni:

"A" Rappresenta la barra con le informazioni del dispositivo
"B" Rappresenta il menù
"C" Rappresenta la pagina dei widget

6.1. BARRA DELLE INFORMAZIONI

Rappresenta le informazioni relative allo stato del dispositivo, in particolare:

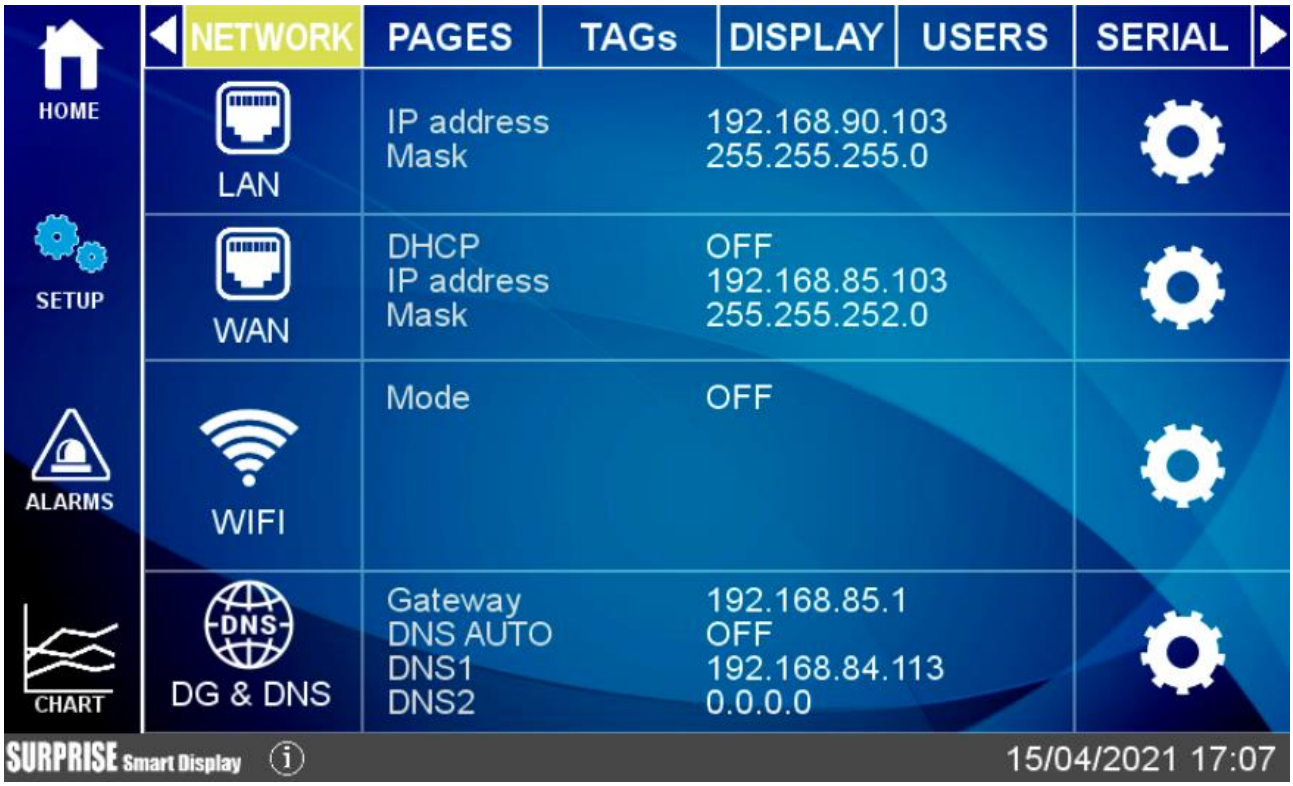
Icona “A” Fornisce informazioni sul dispositivo (come la revisione firmware) ed il produttore
Icona “B” Fornisce informazioni sull’account dell’utente, nel caso non si sia ancora loggati l’icona è sostituita da un lucchetto. L’icona di sinistra, se premuta, permette di effettuare il logout, quella di destra indica il tipo di account utente (la A sta per amministratore). Nel caso di account guest l’icona è la seguente: 
Icona “C” Fornisce lo stato della porta seriale COM1
Icona “D” Fornisce lo stato della porta seriale COM2
Icona “E” Fornisce lo stato della connessione VPN “Seneca Let’s VPN” o “OpenVPN standard”
Icona “F” Fornisce la potenza del segnale Wi-Fi (se presente, a seconda del modello)
Icona “G” Fornisce lo stato del datalogger
“H” Rappresenta la data / ora del dispositivo

6.2. MENU

Rappresenta il menù:
HOME porta alla pagina principale
SETUP porta alla configurazione del dispositivo
ALARMS porta alla sezione relativa agli allarmi
CHART porta alla sezione relativa all’analisi grafica dei dati del datalogger
È anche possibile far scomparire il menù premendo la barra laterale:

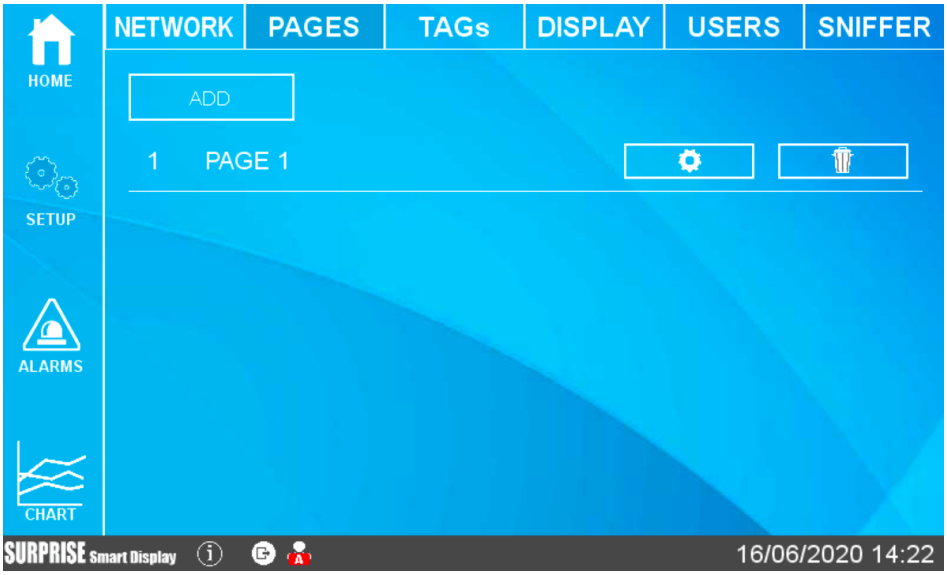
6.2.1.SETUP

6.2.1.1. NETWORK

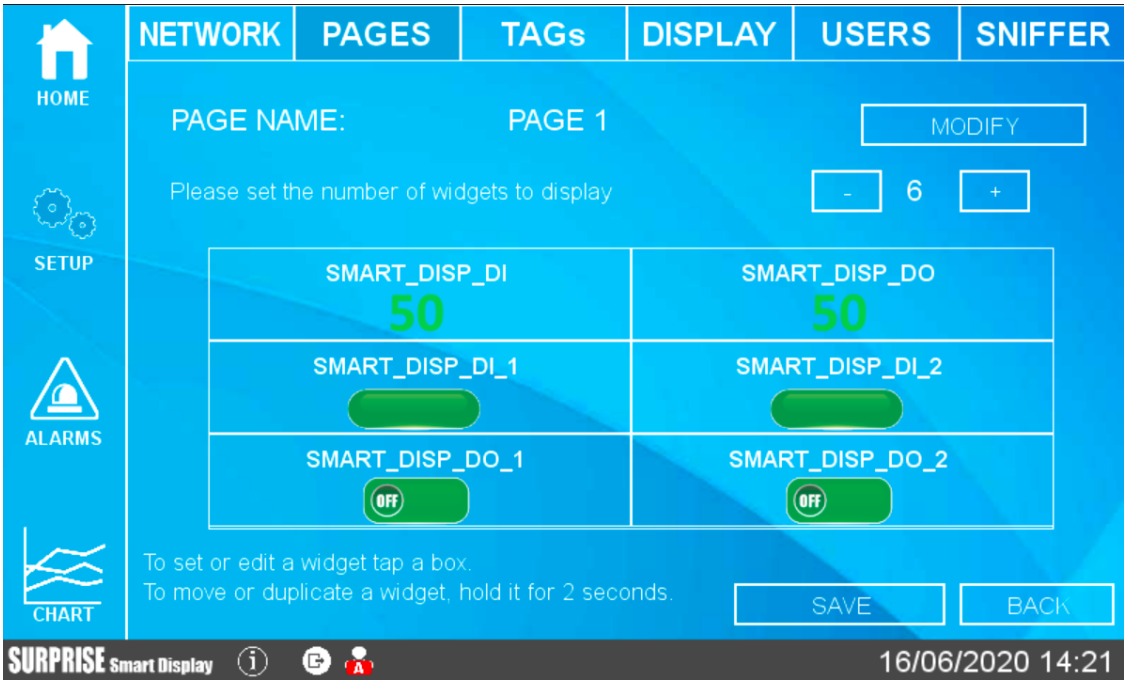


In questa sezione è possibile configurare le impostazioni delle due ethernet LAN e WAN e della porta WI-FI.
Nella sezione della porta WI-FI è possibile anche selezionare la modalità WI-FI Station o Access Point.
Nella modalità Station è il dispositivo che è connesso ad un access point Wi-Fi esistente, nella modalità Access Point il dispositivo Seneca creerà una nuova rete Wi-Fi a cui potranno collegarsi altri dispositivi.

6.2.1.2. PAGES



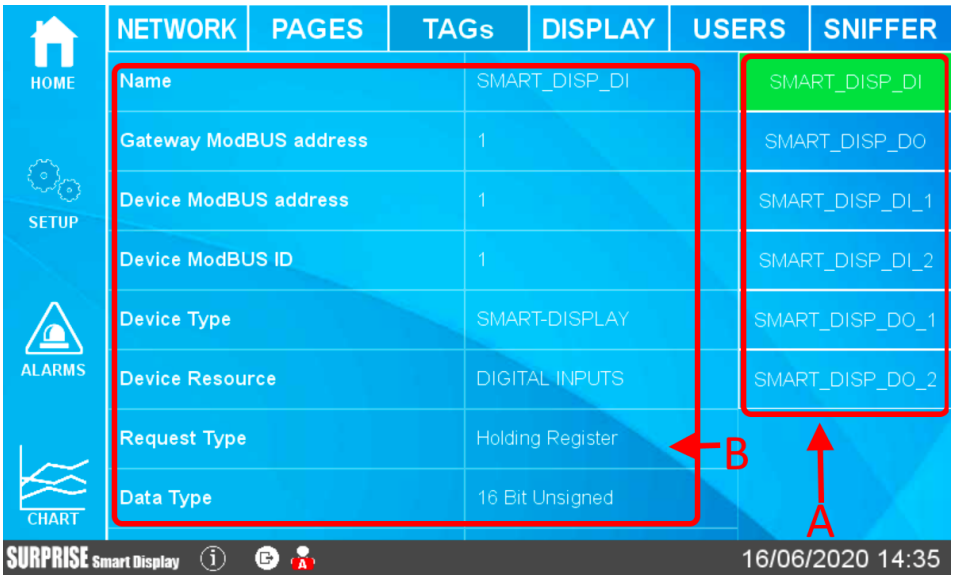
In questa prima schermata è possibile aggiungere il numero di pagine dei widget che si desidera, una volta impostato è possibile accedere alla configurazione di ciascuna pagina:



È possibile modificare sia il nome della pagina sia il numero di widget che devono essere visualizzati.
Nella parte centrale è riportata una anteprima della visualizzazione della pagina.
Ora facendo una pressione su un widget qualsiasi è possibile modificare il tipo di widget, il colore, etc…

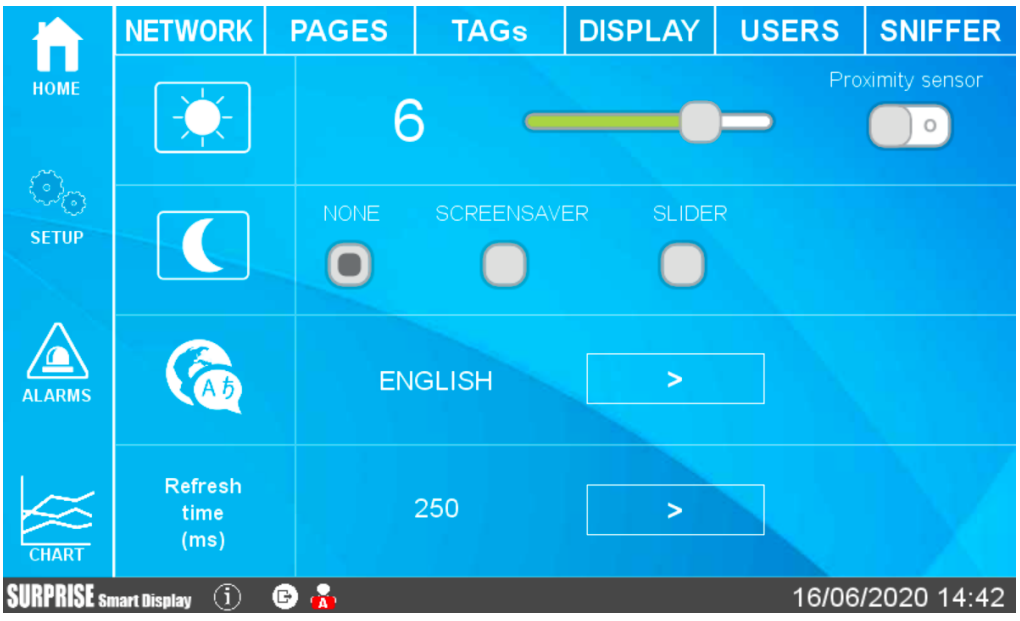
Oltre ad una pagina widget è possibile aggiungere una pagina Synoptic (sinottico). In una pagina sinottico è possibile posizionare liberamente i widget e caricare grafica da un PC o da una libreria grafica interna al dispositivo per creare dei sinottici senza l'ausilio di un software esterno.

6.2.1.3. TAGS



In questa sezione è possibile visualizzare i tag configurati.
I tag presenti nel dispositivo si trovano nella parte destra (A), è anche possibile scorrerne la lista.
I parametri di ciascun tag compaiono nella parte centrale (B), è anche possibile scorrerne la lista.
Dalla versione firmware 109 è possibile aggiungere, modificare e cancellare i tag anche da display.

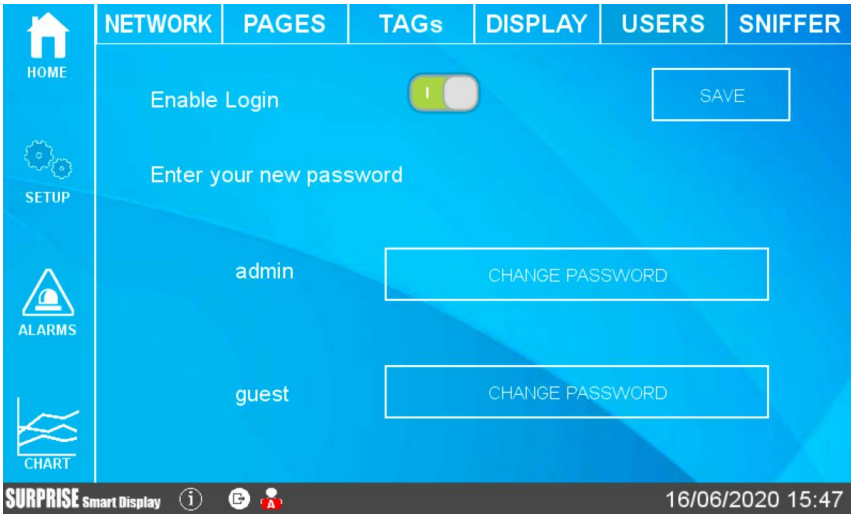
6.2.1.4. DISPLAY



In questa sezione è possibile configurare la luminosità dello schermo, la lingua ed il tempo di aggiornamento dello schermo.

Per salvaguardare i consumi e la durata dello schermo è anche possibile attivare lo screensaver (viene abbassata la retroilluminazione dello schermo dopo il tempo impostato di inattività).
Se si è nella modalità screensaver è possibile uscirne premendo un punto qualsiasi dello schermo (oppure effettuando un movimento davanti lo schermo se il sensore di prossimità è attivato).
La modalità Slider, invece, permette di far ciclare autonomamente le pagine dei widget dopo un tempo prestabilito.

6.2.1.5. USERS



In questa sezione è possibile configurare gli utenti che possono accedere al display.
È possibile eliminare la necessità di inserire una login per accedere al display (accesso libero) oppure attivare un account amministratore e/o un account ospite.

Secondo la seguente tabella

TIPO ACCOUNT	***CAMBIO VALORE DI UN TAG***	***VISUALIZZAZIONE MENU SETUP***	***MODIFICA SETUP***
ADMIN	Sì	COMPLETO	Sì
GUEST	Sì	SOLO “NETWORK” E “TAGS”	NO
NESSUN ACCOUNT	No	NO	NO

Se lo screen saver è disinserito e non si tocca lo schermo per 2 minuti il sistema effettua un logout automatico.
Se lo screen saver è attivato e non si tocca lo schermo per il tempo di screen saver il sistema effettua un logout automatico.

6.2.1.6. SERIAL

Permette di configurare i parametri delle seriali e definire se il protocollo Modbus deve essere Master o slave.

6.2.1.7. SNIFFER

La funzionalità di sniffer seriale permette di inserire uno o più dispositivi sniffer in un impianto esistente con protocollo Modbus RTU in un bus RS485.
Nel protocollo Modbus RTU è sempre presente un unico master ed una serie di dispositivo slave. Il master richiede dei registri a ciascuno slave il quale li invia al master stesso.
Per poter inserire un dispositivo che visualizzi dei dati senza modificare la configurazione esistente è necessario inserire uno o più dispositivi in modalità passiva (sniffer).
A questo punto i dispositivi riceveranno tutti i pacchetti seriali trasmessi tra il master e gli slave, è necessario associare a questi pacchetti dei tag che verranno poi valorizzati.

ATTENZIONE!
Poiché la modalità SNIFFER è puramente passiva tutti i tag definiti saranno di sola lettura

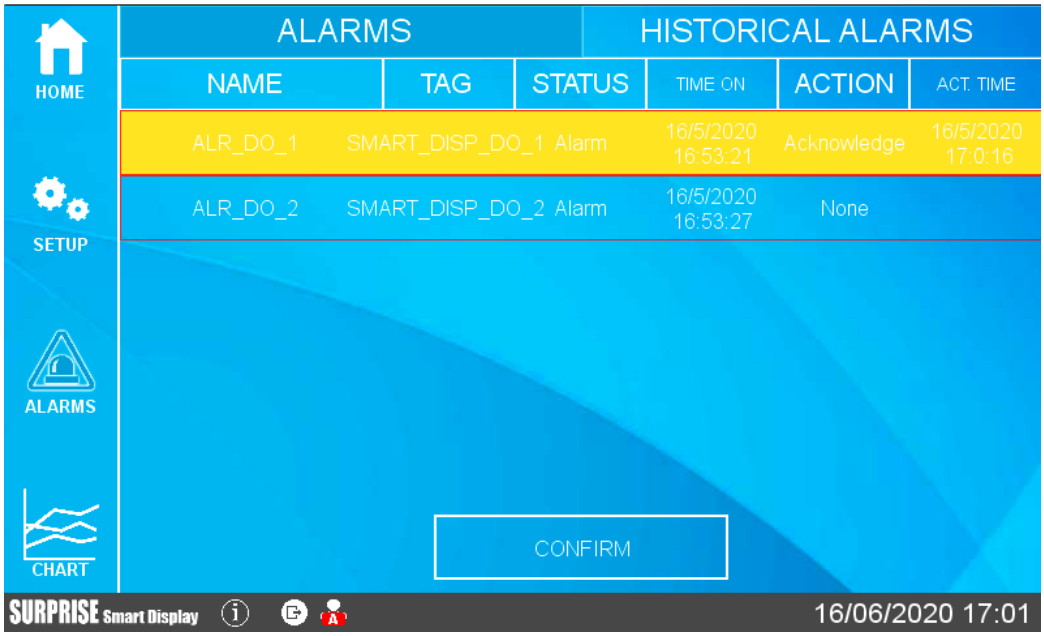
6.2.1.8. FASI DI CONFIGURAZIONE DELLA MODALITA' SNIFFER

La modalità sniffer viene configurata attraverso le seguenti fasi (i tre pulsanti posti in alto nella pagina):

1) SCAN DELLA COMUNICAZIONE NEL BUS
In questa modalità di apprendimento il dispositivo inizierà ad analizzare il flusso di informazioni che transita nel bus. Tipicamente un Master interroga a ciclo continuo tutti i dispositivi, quindi quando si è certi che il ciclo è terminato è possibile fermare lo scan. Attenzione: l'operazione di stop dello scan è sempre manuale.
2) CREAZIONE DEI TAG
In questa fase il dispositivo ha individuato i registri che i dispositivi si stanno scambiando, ora è necessario associare il nome del tag e il tipo di dato contenuto. Nel caso si tratti di un sistema con prodotti Seneca sarà necessario introdurre il tipo di dispositivo Seneca ed il sistema automaticamente assocerà i tag corretti, nel caso di dispositivi di terze parti verranno richieste le informazioni relative ad ogni registro individuato.

6.2.2. ALARMS

In questa sezione sono riportati gli allarmi attivi e lo storico degli allarmi.
Nel caso in cui l'allarme necessiti di una conferma manuale è possibile farlo tramite l'apposito pulsante:



Nella sezione Storico sono, invece, rappresentati tutti gli allarmi che sono avvenuti fino a questo momento:

ATTENZIONE!
LA CONFIGURAZIONE DEGLI ALLARMI AVVIENE NELL'APPOSITA SEZIONE DEL WEBSERVER

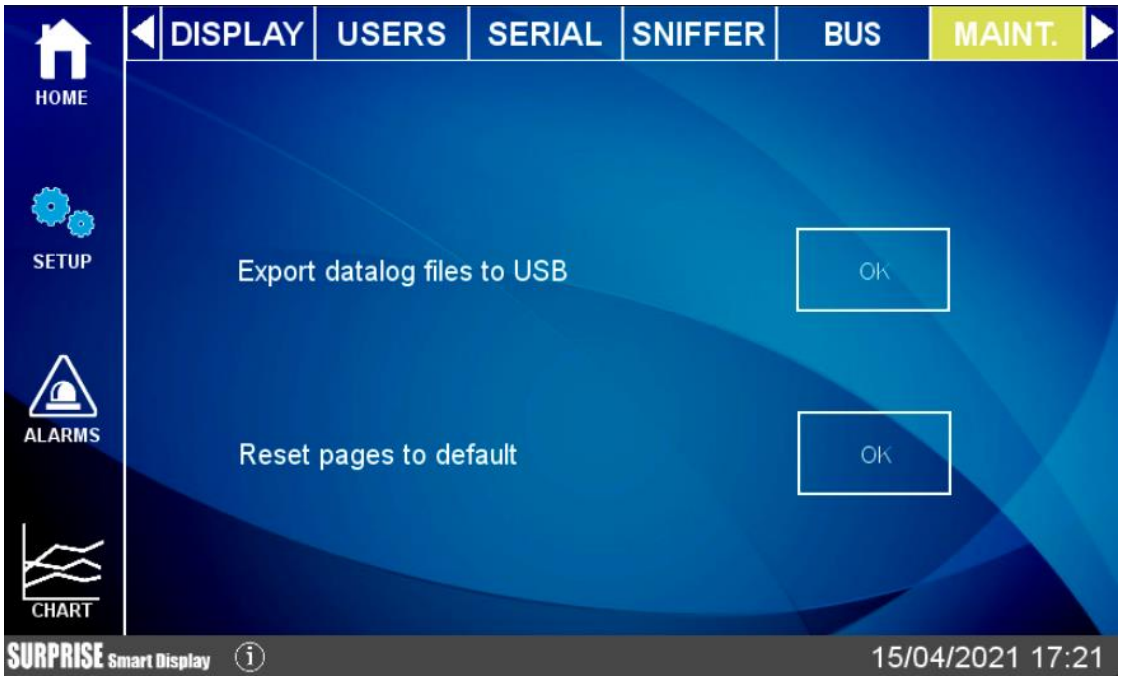
6.2.3. BUS

Questa sezione permette di aggiungere dei dispositivi esterni tramite seriale e/o ethernet e di inserire i relativi tag:

Il device utilizza un database che include i registri di tutti i dispositivi Seneca.
L'aggiunta di un dispositivo può avvenire in modalità manuale (inserendo il dispositivo tra quelli nel database o di un produttore diverso da Seneca) oppure cercando automaticamente il dispositivo su seriale o ethernet.
La ricerca automatica crea automaticamente anche i tag ma funziona solo con dispositivi Seneca.

6.2.4. MAINTENANCE

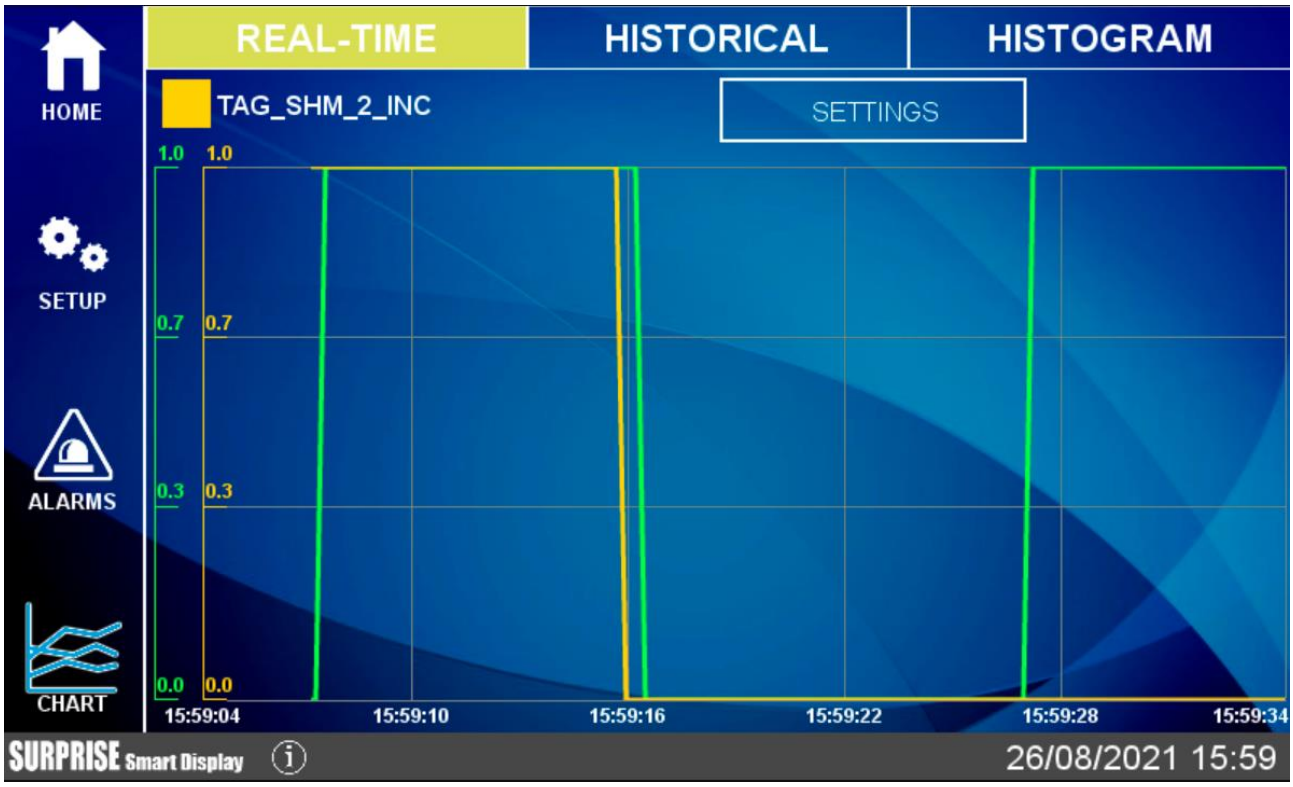
Tramite il menu Maintenance è possibile effettuare operazioni di manutenzione del dispositivo:



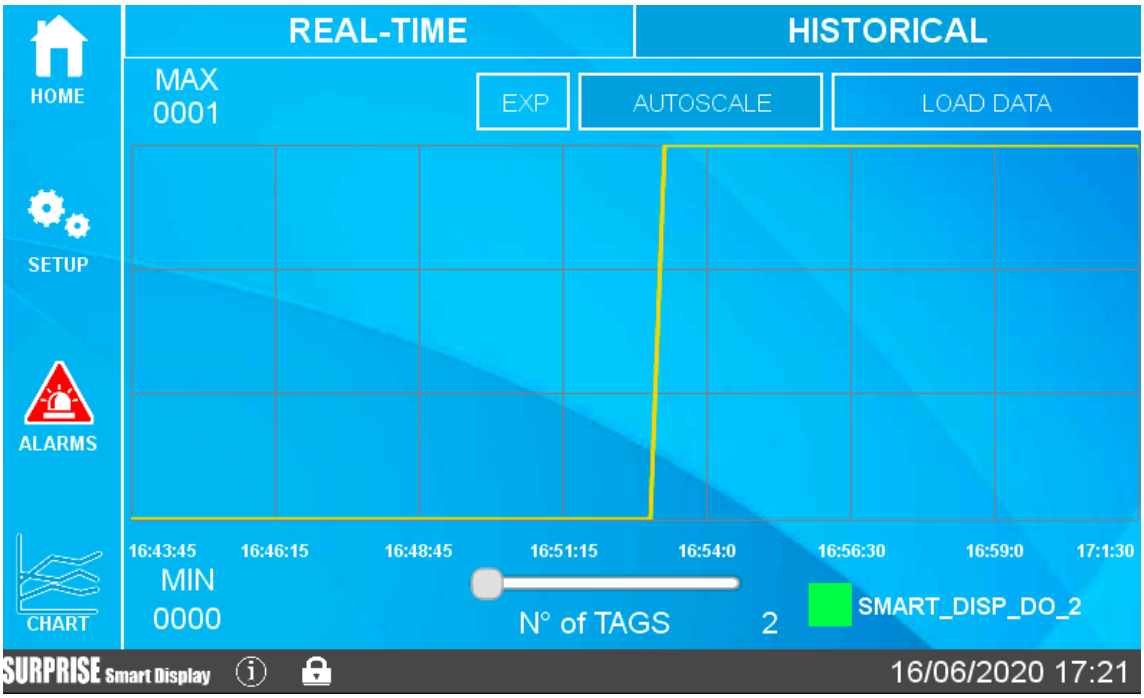
6.2.5. CHART

Vi sono 3 tipologie di grafico a disposizione: Real Time, Historical e Histogram.

Nella sezione Chart Real Time è possibile visualizzare i valori dei tag in tempo reale (massimo 10 tag):



La configurazione del grafico real time sarà richiamabile anche dal relativo widget.
Nella sezione Historical, invece, è possibile caricare i dati nell'intervallo desiderato e spostarsi avanti e indietro nel grafico usando il touch.



È anche possibile esportare i valori del grafico che si stanno visualizzando tramite la pressione del pulsante "EXP" nel caso sia inserita una chiavetta USB il file sarà salvato.
Se ci si sta connettendo tramite web al display remoto, premendo il pulsante "EXP" il browser scaricherà il file direttamente sul pc in uso.

Il grafico Histogram è sostanzialmente lo stesso grafico Historical ma con una rappresentazione ad istogramma.

6.3. TIPO DI WIDGET

I widget sono elementi grafici che possono essere collegati ad uno o più TAG.
Questi possono essere utilizzati sia nelle pagine dei widget sia nelle pagine sinottico.
Vi sono vari widget disponibili, qui sotto alcuni esempi:

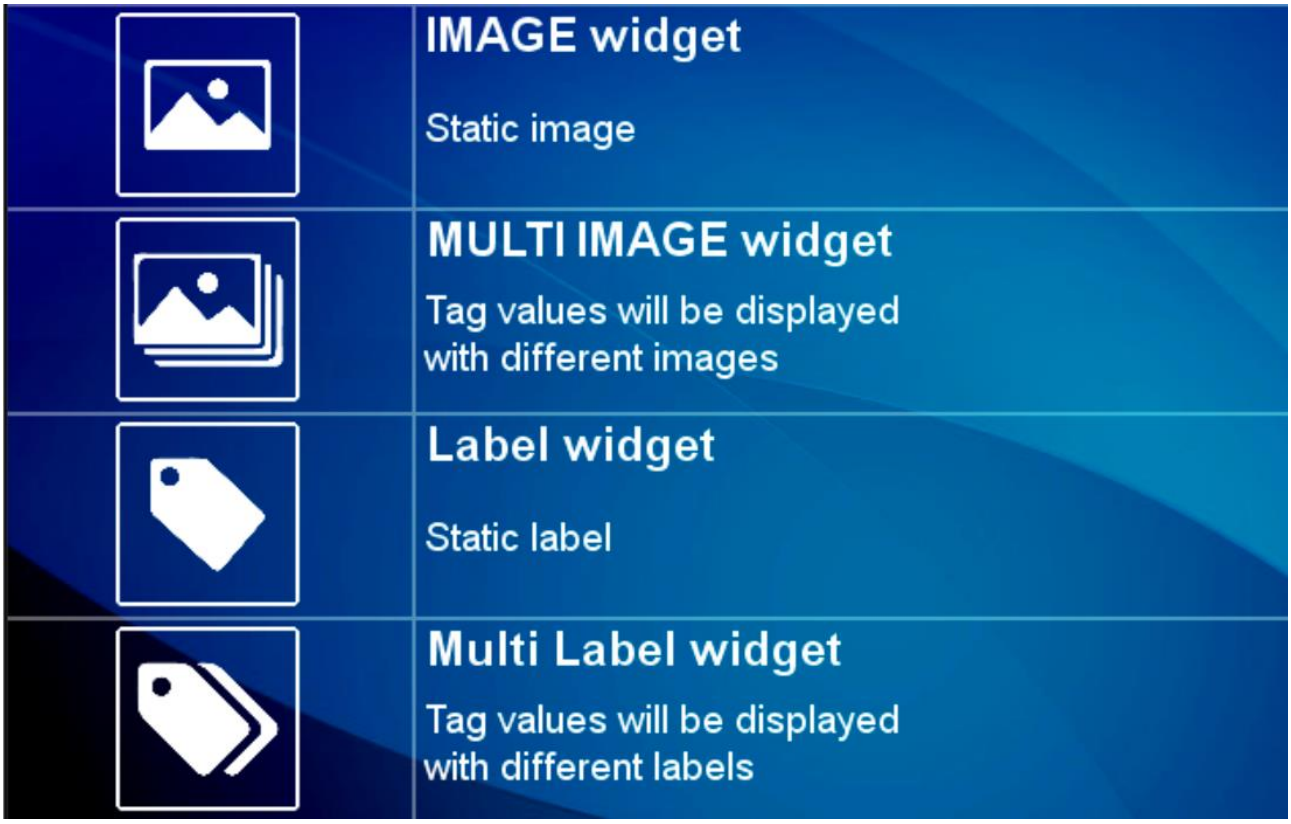
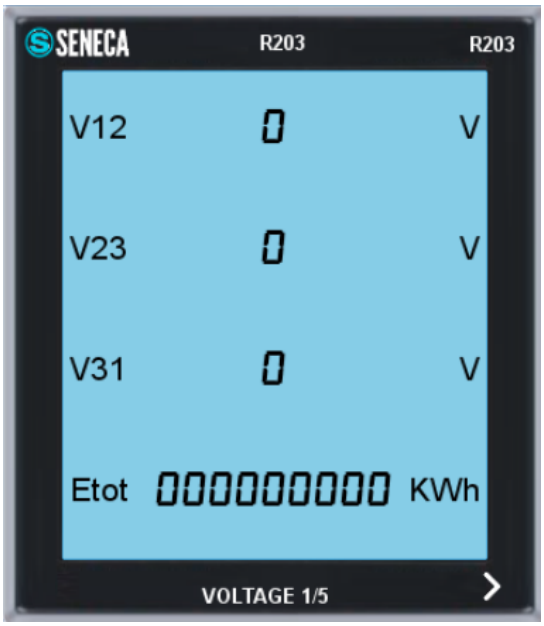


Grafico macro widget (virtual display):



Si tratta di un display virtuale, scorrere le pagine del display virtuale premendo la freccia “>” in basso a destra.
È possibile posizionare fino a 2 display virtuali per ogni pagina dei widget.

6.3.1. CAMBIO PAGINA

Per passare da una pagina alla successiva è sufficiente far scorrere il dito verso sinistra (in gergo l’operazione prende il nome di “swipe”) come si stesse sfogliando un libro.
Analogamente per passare alla pagina precedente è sufficiente far scorrere il dito verso destra.
È anche possibile premere una freccia di “avanti” e un freccia di “indietro” per cambiare pagina:

6.4. TIPO DI PAGINA WIDGET

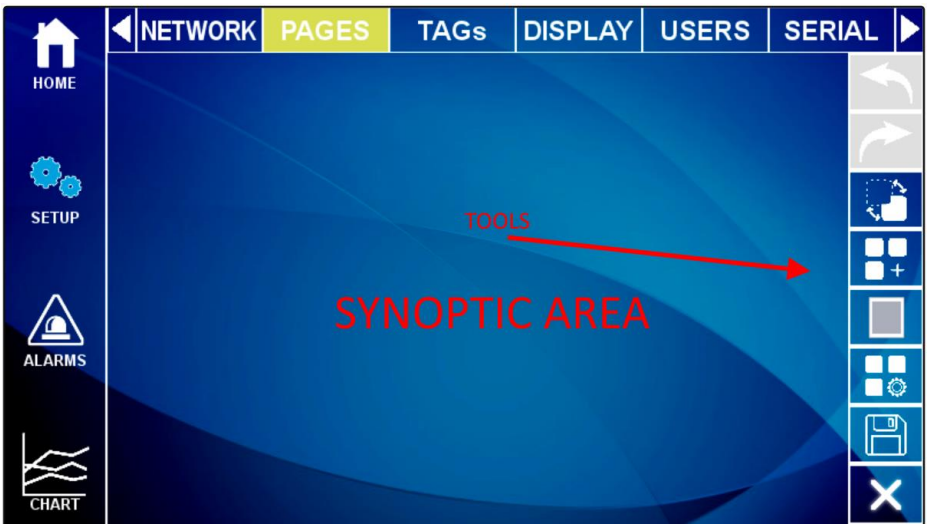
Rappresenta la pagina dei widget, in questa sezione compariranno i widget legati ai tag configurati.È possibile scegliere tra le varie griglie disponibili, i widget saranno posizionati automaticamente all’interno della griglia.
Ogni widget rappresenta in modo grafico il valore di uno o più TAG.

6.5. TIPO DI PAGINA SINOTTICO

In una pagina di tipo sinottico è possibile spostare liberamente i widget aggiungendo grafica e creare anche dei sinottici animati.

Le pagine di tipo sinottico possono essere mescolate liberamente con pagine di tipo widget.

Per creare una pagina sinottico Selezionare Pages e premere il pulsante “Add Synoptic Page”.
A questo punto si aprirà una nuova pagina con dei tool sulla sinistra:



Ecco il significato delle icone dei tool:

 UNDO
Annulla l’ultima operazione eseguita

 REDO
Esegue nuovamente l’ultima operazione annullata dall’ UNDO

 BACKGROUND
Permette di scegliere un file grafico da usare come sfondo della pagina

 ADD WIDGET
Aggiunge un widget alla pagina

 ADD VIRTUAL DISPLAY WIDGET
Aggiunge un widget di tipo virtual display

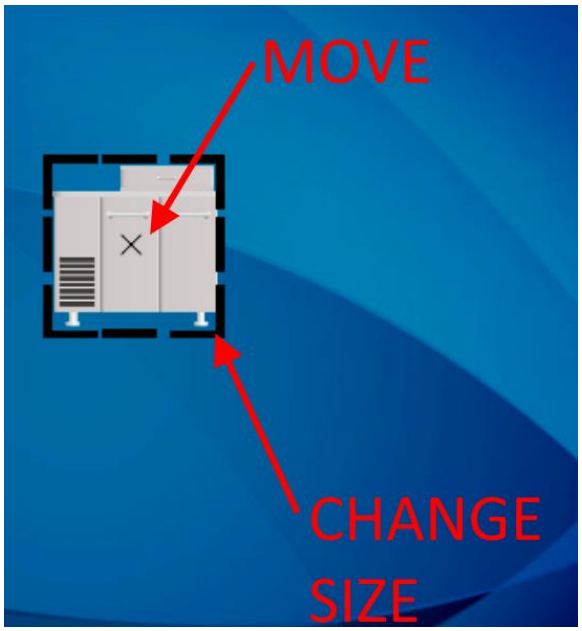
 WIDGET CONFIGURATOR
Permette la configurazione del widget

 SAVE PAGE
Salva le modifiche alla pagina

 EXIT
Esce dalla pagina

6.5.1. TOOL "ADD WIDGET"

Il pulsante "ADD WIDGET"  permette l'aggiunta di un widget sulla pagina, una volta inserito il widget è possibile spostarlo toccando il widget nella croce centrale. Per cambiare le dimensioni del widget spostare i lati del rettangolo che contiene il widget:



Quando si seleziona un widget compaiono sulla destra una nuova serie di tool il cui significato è il seguente:

 GRID

Attiva una griglia, spostando i widget questi seguiranno la griglia impostata.

 ALIGN

Allinea il widget

 CONFIG

Visualizza e permette la modifica dei parametri di configurazione del widget selezionato

 DELETE

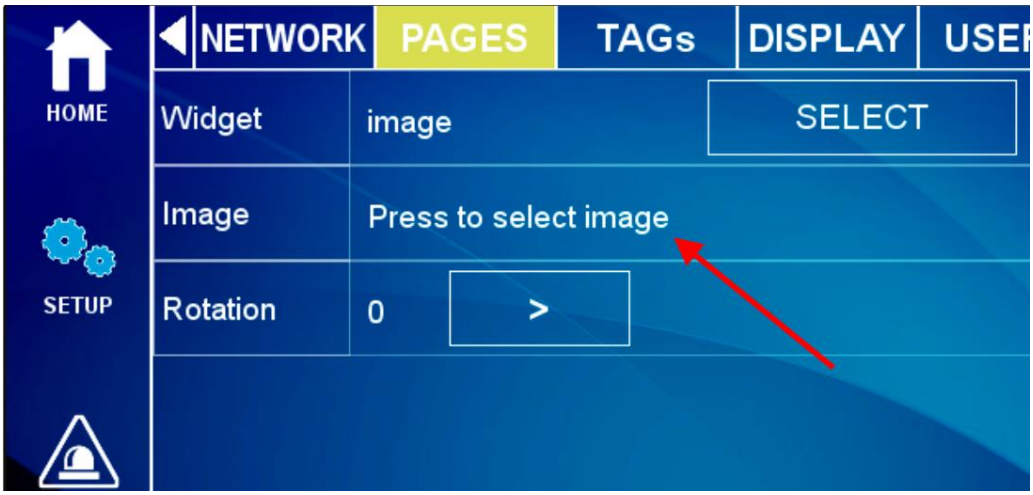
Elimina il Widget dalla pagina

 EXIT

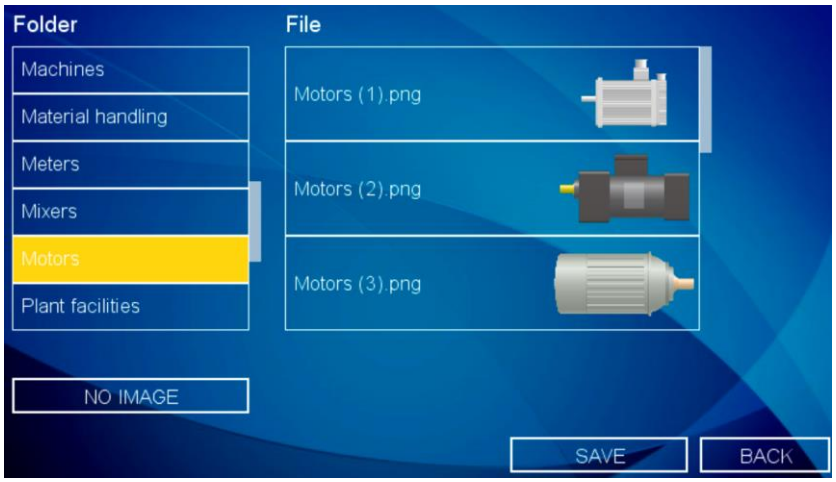
Torna alla pagina iniziale del sinottico

6.5.2. DATABASE DEI SIMBOLI PER LE PAGINE SINOTTICO

All'interno del dispositivo si trova un database di simboli grafici che può essere utilizzato nei widget.
I simboli sono suddivisi in categorie. Per accedere ai simboli si selezioni, ad esempio il widget "Image":

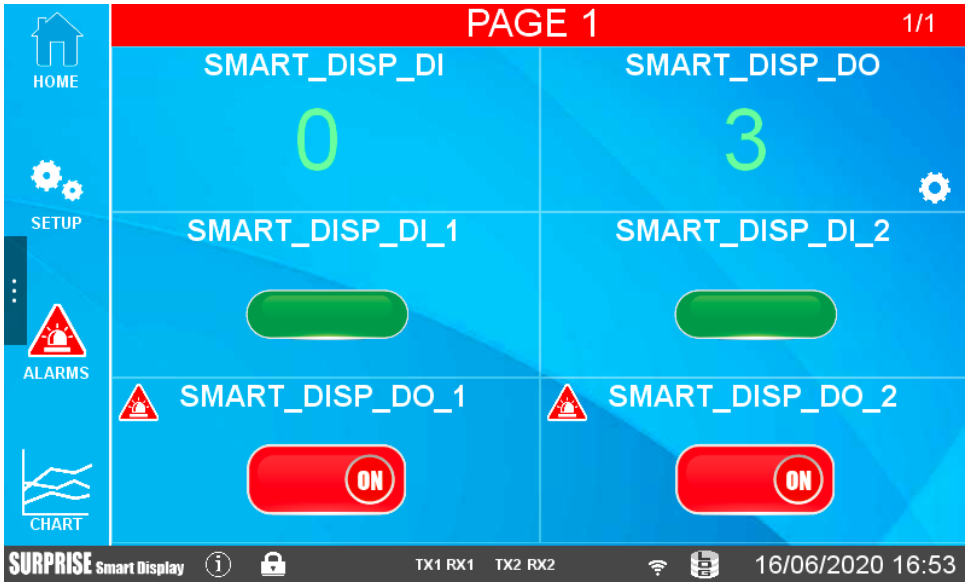


Ad esempio selezionando la categoria “Motors” vengono visualizzati i file grafici relativi a motori:



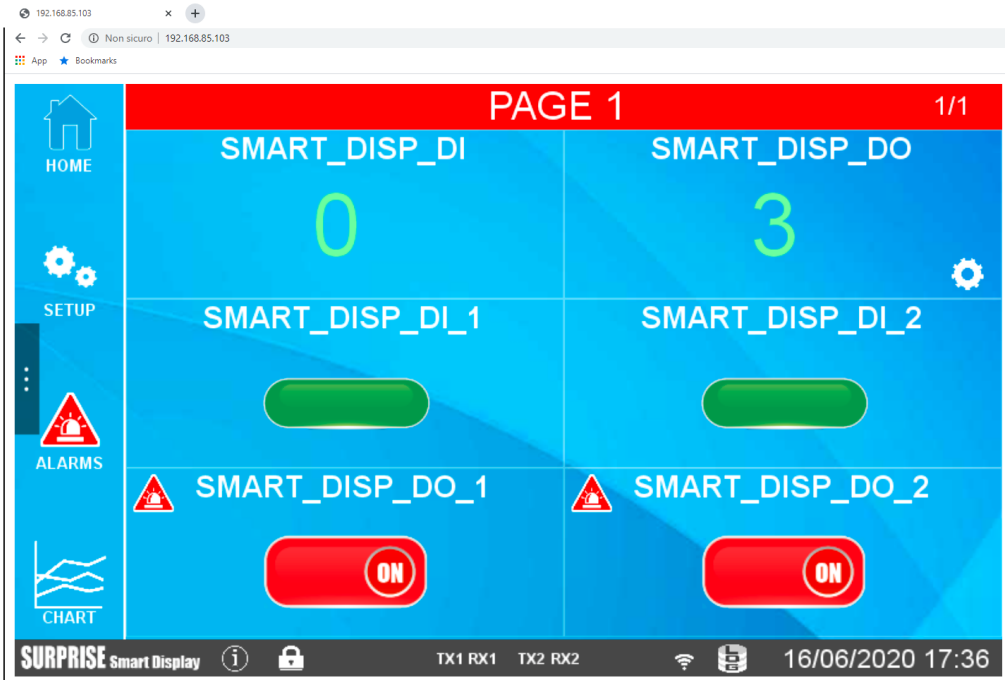
6.6. ALLARMI

Quando avviene un allarme su almeno un TAG il titolo della pagina viene contornato di rosso e i tag in errore visualizzano l’icona di allarme, si veda la figura:



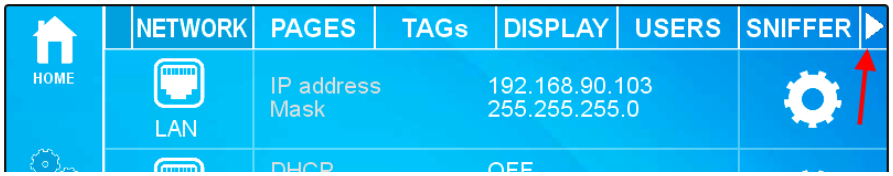
6.7. DISPLAY VIRTUALE

Tutte le operazioni che possono essere fatte sul display fisico possono anche essere effettuate collegandosi alla pagina web del dispositivo tramite un browser web tramite la porta 80 (default).
Per collegarsi al display virtuale inserire l'indirizzo IP del dispositivo in un browser su un PC o dispositivo smart:

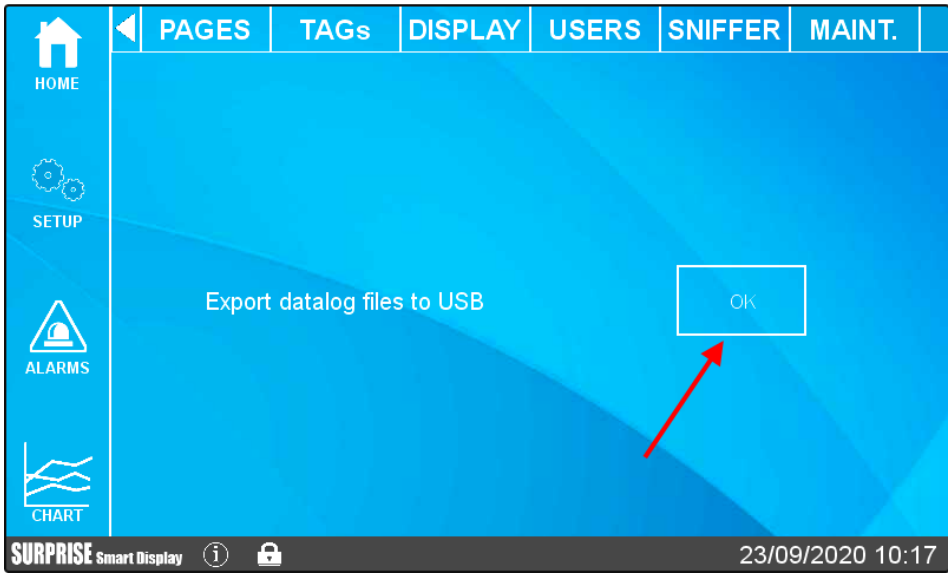


6.8. DOWNLOAD DEI FILE DI LOG SU CHIAVETTA USB

Inserendo una chiavetta USB nella porta HOST è possibile effettuare il download completo dei file acquisiti dal datalogger.
Per effettuare questa operazione è necessario raggiungere il menù "Maintenance" toccando "SETUP" e poi la freccia che estende il menù:



Ora selezionare “MAINT.” e successivamente premere il relativo pulsante per effettuare l’operazione:



A questo punto il sistema effettuerà il download di tutti i file acquisiti dal datalogger.
Nel root della chiavetta USB saranno quindi presenti tante cartelle (una per giorno di registrazione) con all’interno i file relativi a quella giornata (suddivisi a loro volta in cartelle che rappresentano i gruppi di log attivi). Questa funzionalità è attiva anche via Webserver nella sezione “TAG VIEW”.

7. GATEWAY INDUSTRIALE / ROUTER / FIREWALL

I dispositivi permettono di impostare il firewall, il port mapping e altre funzionalità avanzate come il NAT 1:1. Oltre a queste funzionalità è possibile anche attivare la funzionalità di gateway industriale.

7.1. GATEWAY ETHERNET SERIALE

È possibile attivare i protocolli disponibili per creare dei gateway per i protocolli industriali (ad esempio da/a Modbus RTU a/da Modbus TCP-IP). Oppure è possibile attivare la modalità trasparente.

7.2. GATEWAY MODBUS ETHERNET TO SERIAL

Il dispositivo può essere configurato per funzionare come Gateway da Modbus Ethernet a Modbus Seriale.
Le Richieste Modbus TCP ricevute dalle interfacce IP vengono convertite in richieste Modbus RTU e inviate all'interfaccia seriale; allo stesso modo, le risposte Modbus RTU ricevute dall'interfaccia seriale vengono convertite in risposte Modbus TCP e rinviate all'interfaccia di rete sorgente.

Un'istanza Modbus Ethernet to Serial Gateway può essere attivata per ognuna delle porte seriali disponibili.
Ogni istanza Gateway Modbus Ethernet to Serial può supportare fino a 50 connessioni TCP simultanee. La connessione TCP può essere stabilita anche attraverso un tunnel VPN

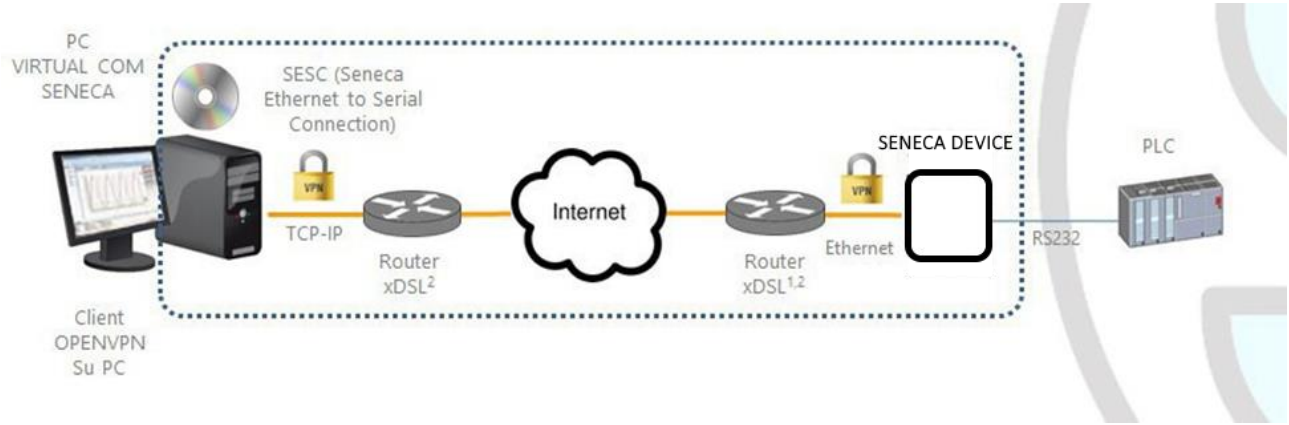
7.3. GATEWAY ETHERNET TO SERIAL TRASPARENTE

In alternativa al Modbus Ethernet to Serial Gateway, il dispositivo può essere configurato per funzionare come "Transparent Gateway". La grande differenza tra queste due modalità è che, mentre la prima funziona solo con il protocollo Modbus, la seconda può essere virtualmente applicata a qualsiasi protocollo seriale che può essere trasportato attraverso lo stack TCP/IP.
È possibile scegliere le seguenti modalità di gateway trasparente:

- COM virtuale (con supporto RFC 2217)
- Tunnel seriale punto-punto su TCP
- Tunnel seriale punto-punto su UDP

Ogni modalità sarà descritta in modo completo nei prossimi paragrafi.

7.3.1. COM VIRTUALE CON SUPPORTO RFC 2217



La funzionalità Virtual COM con supporto RFC 2217 permette ad un'applicazione PC, che trasmette i dati solo su una linea seriale, di comunicare con un dispositivo seriale remoto, utilizzando Ethernet/Internet; in altre parole, attraverso il dispositivo Seneca, un PC e un dispositivo seriale, collocati in siti distanti tra loro, possono comunicare in quanto direttamente collegati.

In questa modalità, i dati inviati attraverso la rete LAN o WAN, vengono ricevuti del dispositivo Seneca e inviati alla porta seriale; i pacchetti di risposta seguono il percorso inverso.

Il supporto a RFC 2217 definisce alcune caratteristiche che permettono al PC di impostare da remoto le proprietà (baud rate, bit di dati, bit di stop e parità) della porta seriale del dispositivo Seneca; così, quando si seleziona la modalità operativa Virtual COM per una porta, la porta viene riconfigurata indipendentemente dalle impostazioni precedenti e i valori configurati nel dispositivo Seneca vengono sovrascritti.

Per far funzionare la Virtual COM, sul PC deve essere installata una utility chiamata "Seneca Ethernet to Serial Connection".

La connessione TCP può essere stabilita attraverso un tunnel VPN, come mostrato sopra in figura.

Una volta stabilita la connessione, un programma che utilizza la porta COM virtuale trasmetterà i dati alla porta seriale del dispositivo; ad esempio, le richieste Modbus RTU inviate da un programma Modbus Master raggiungeranno i dispositivi Modbus slave collegati al bus RS485 della COM2.

Attenzione particolare deve essere data al parametro "Data Packing Interval", che può essere impostato quando è selezionata la modalità operativa Virtual COM: questo parametro permette di definire l'intervallo di tempo, in millisecondi, utilizzato dal dispositivo Seneca come criterio per impacchettare i byte di dati ricevuti dalla porta seriale prima di inviarli alla rete; in altre parole, quando il dispositivo Seneca non riceve più byte dalla porta seriale per il dato intervallo di tempo, impacchetta i byte ricevuti e li invia sulla connessione TCP stabilita; il valore ottimale da impostare per questo parametro dipende dal protocollo che viene instradato in modo trasparente dalla rete TCP/IP alla linea seriale e viceversa.

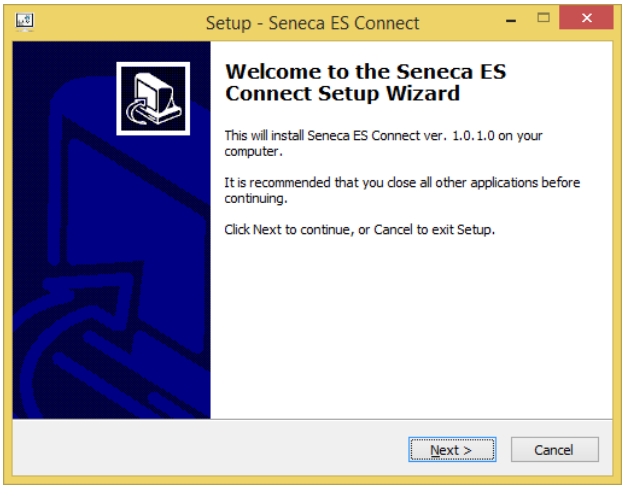
ATTENZIONE!

Nel modo operativo Virtual COM può essere utilizzata una sola porta seriale

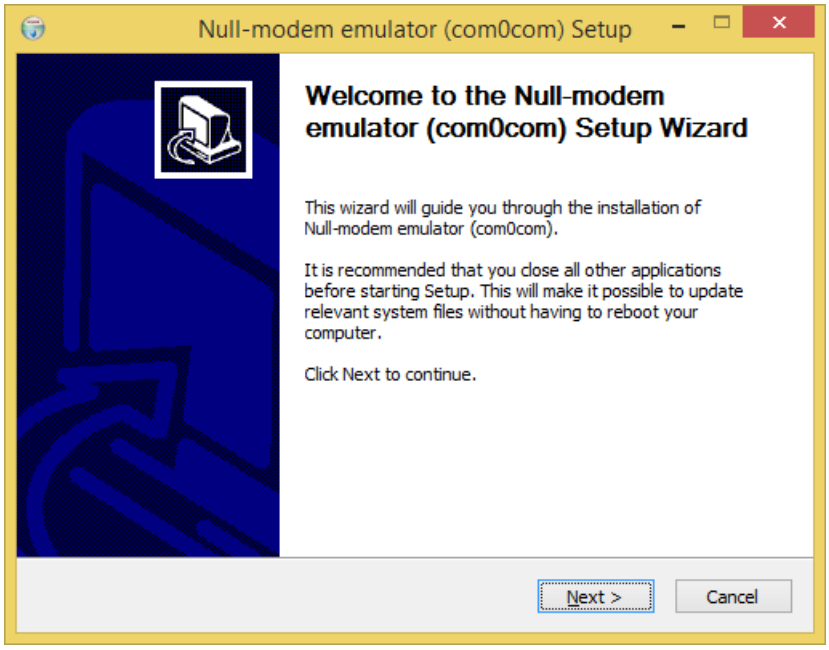
7.3.1.1. SENECA ETHERNET TO SERIAL CONNECT

7.3.1.1.1. INSTALLAZIONE DEL DRIVER SENECA SERIAL TO ETHERNET

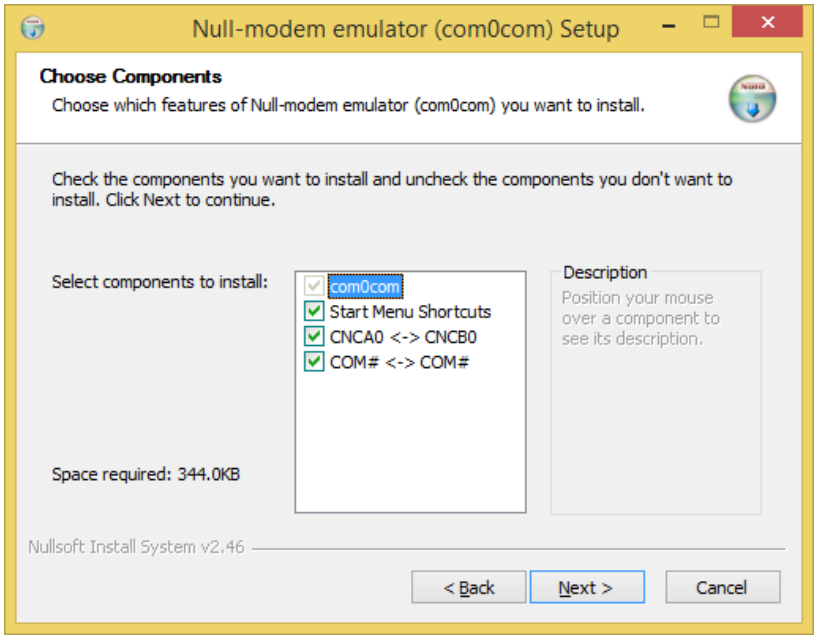
Seneca Ethernet to Serial Connect è compatibile con sistemi Windows a 64 bit.
Fare doppio clic sul programma di installazione



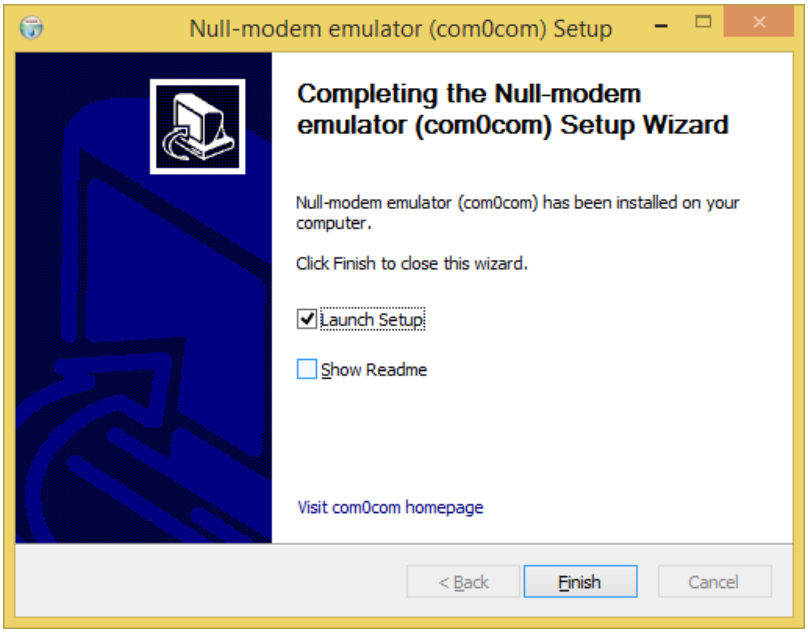
Dopodiché verrà installato il driver com0com:



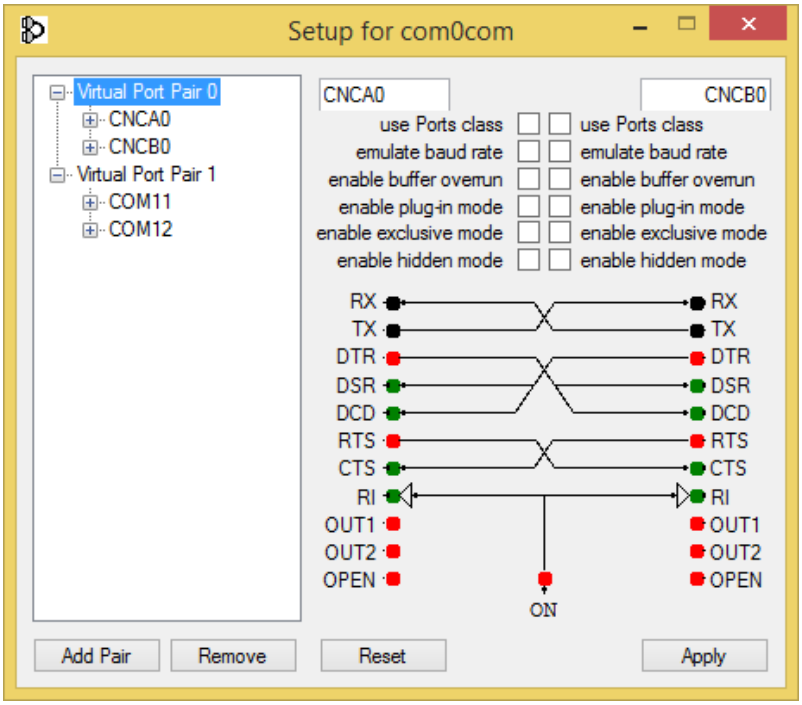
Selezionare i nomi delle porte virtuali CNCA0<->CNCB0 e COM#<->COM#:



Ora cliccate su "Avviare il Setup":



Premere Finish, si aprirà il setup di com0com:



Abbiamo installato due coppie di porte virtuali:
CNCA0, CNCB0
e anche:

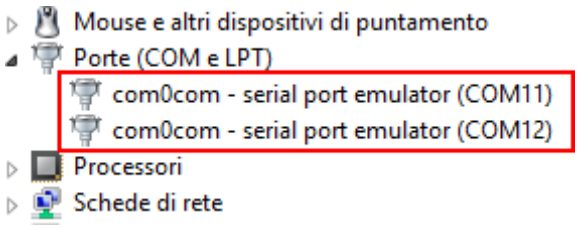
COM11, COM12 (si noti che nel vostro sistema il com# può essere differente).

La prima coppia può essere utilizzata nei software che supportano i nomi CNCA, l'altra nei software che supportano solo le Port Class.

Se è necessario aggiungere altre porte virtuali, premere il pulsante "Add Pair", quindi selezionare se è necessaria o meno una porta Class.

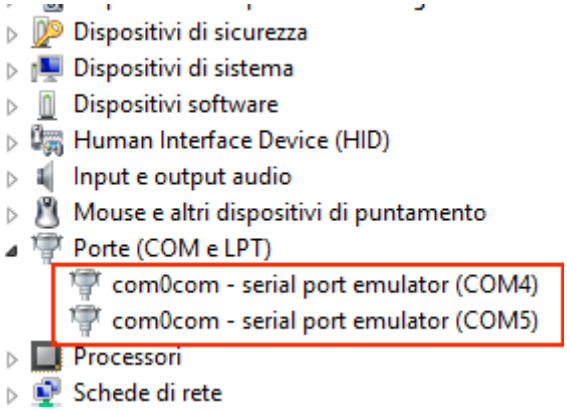
Confermare l'installazione del driver con “Apply”.

Sarà disponibile la coppia di emulatori di porte seriali COM11-COM12



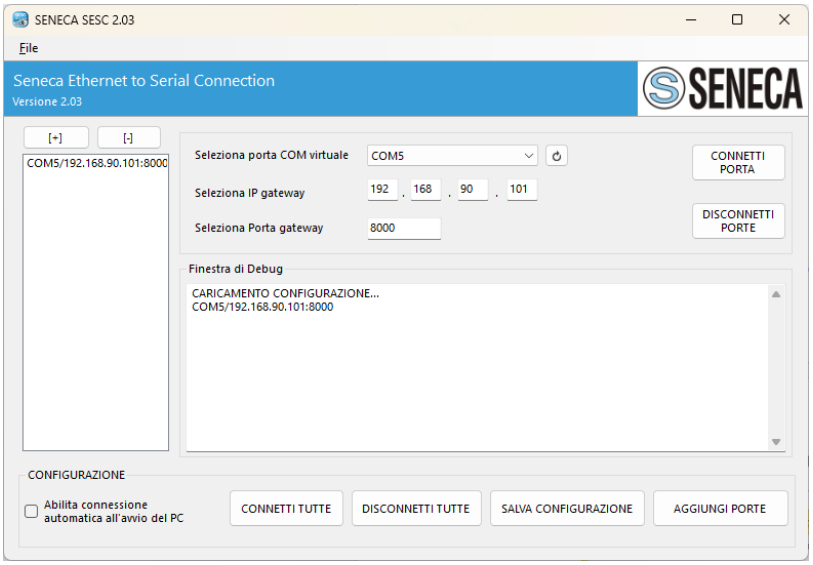
7.3.1.1.2. SELEZIONE DELLA PORTA COM PER SENECA ETHERNET TO SERIAL TO CONNECT

L'installazione del driver utilizzerà le prime 2 porte seriali che sono libere (nel nostro caso il driver ha creato la coppia COM4 e COM5):

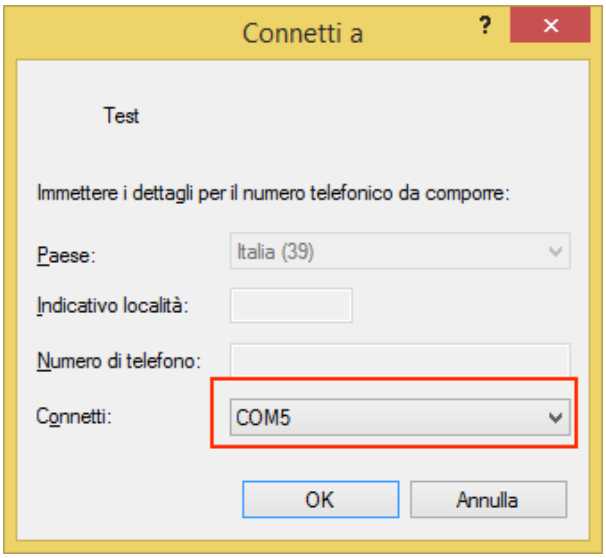


Il software utilizzerà una sola porta (la porta corretta nel setup di com0com), verranno visualizzate solo le porte com0com.

Selezioniamo la COM5 nel connettore Seneca ES:

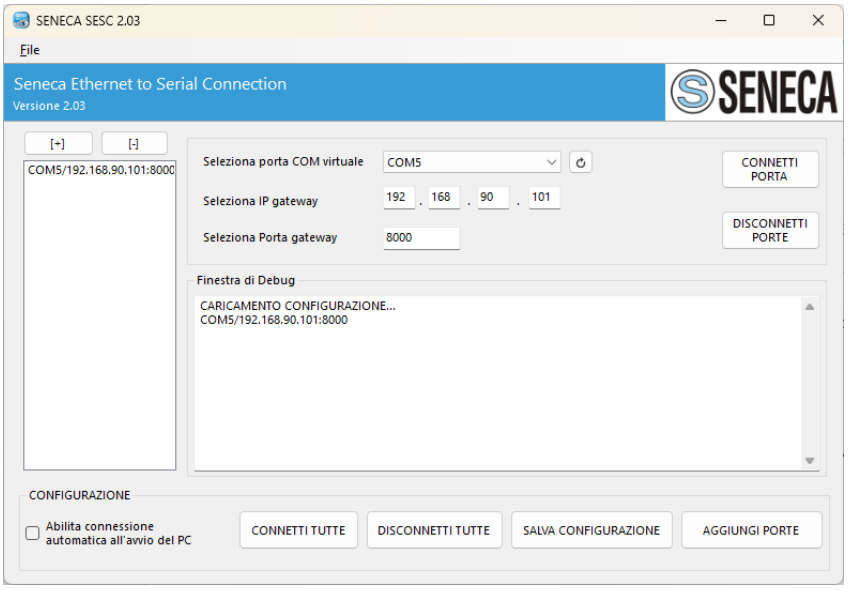


Ora utilizzate la stessa COM5 (ad esempio nel software terminale)



La COM5 è ora collegata al dispositivo Seneca, sulla porta TCP 8000.

7.3.1.1.3. CONFIGURAZIONE DI SENECA SERIAL TO ETHERNET



- Selezionare la porta COM virtuale
- Selezionare l'indirizzo IP del dispositivo Seneca
- Selezionare la porta TCP-IP

Cliccare su "CONNETTI PORTA”

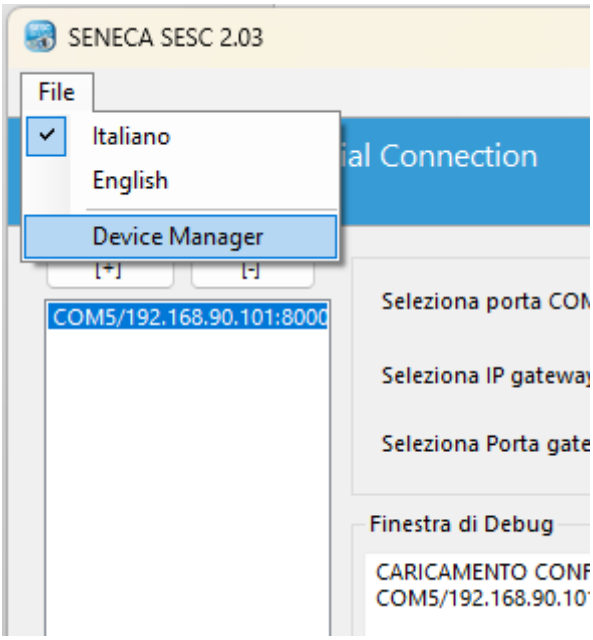
Se è necessario collegare un'altra com seriale ad un altro dispositivo Seneca basta premere il pulsante “AGGIUNGI PORTA” e poi il pulsante [+] per configurare la nuova porta com e, selezionandolo, inserire il nuovo indirizzo IP, dopodiché premere sempre il pulsante “CONNETTI PORTA”.

Per scollegare tutte le porte, cliccare su "DISCONNETTI PORTE”

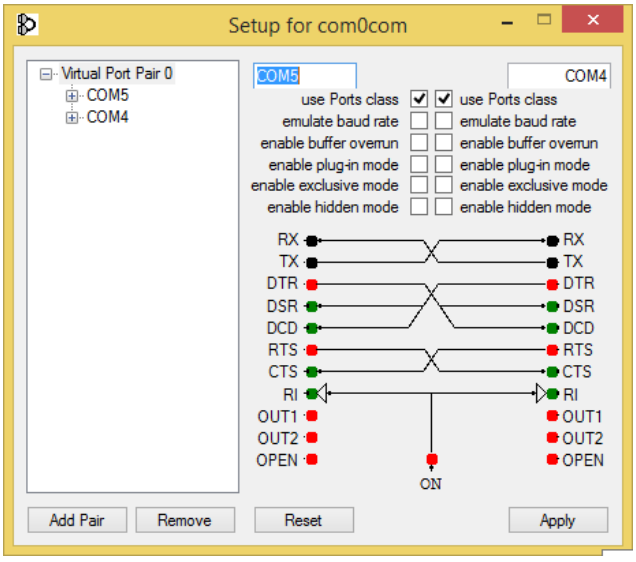
7.3.1.1.4. MODIFICA DEL NUMERO DI PORTA

Le vecchie applicazioni software possono utilizzare solo una piccola gamma di porte COM, quindi potrebbe essere necessario cambiare il numero della porta virtuale COM.

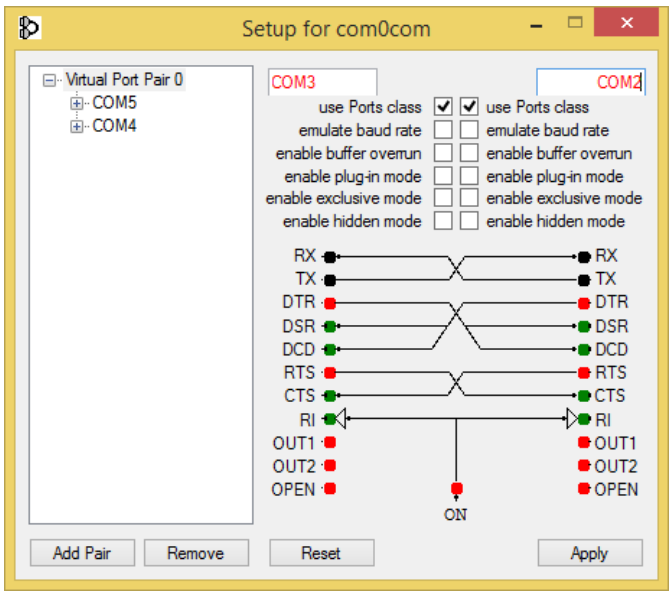
Nel nostro caso la coppia COM creata è COM4/COM5, vediamo la procedura per cambiarle in COM2/COM3
Cliccare sul menu File- DEVICE MANAGER:



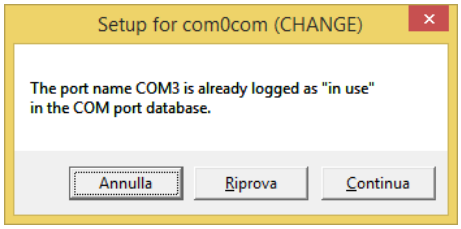
Si aprirà la finestra di configurazione di com0com:



Ora cambiate COM5 in COM3 e COM4 in COM2, quindi cliccate su “Apply”:

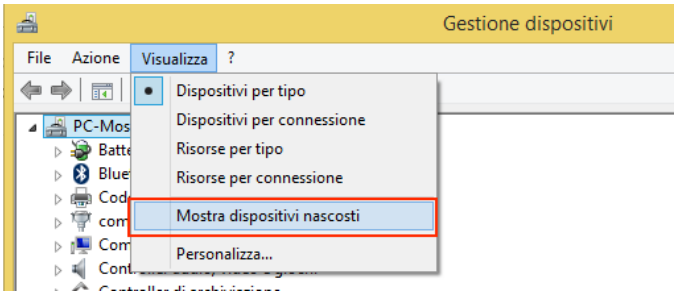


A volte la COM può essere contrassegnata “in uso”:

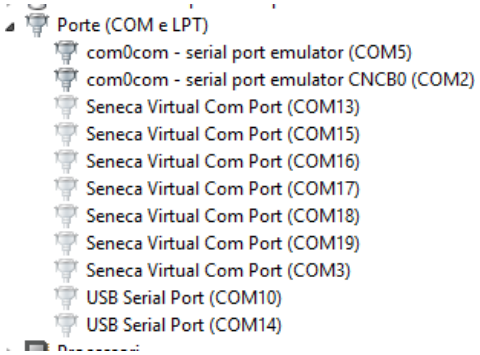


Se è necessario utilizzare questo numero COM, cliccare su "Continua", quindi andare su configurazione dispositivo.

Poiché la porta non è collegata, cliccate su "Mostra dispositivi nascosti”:

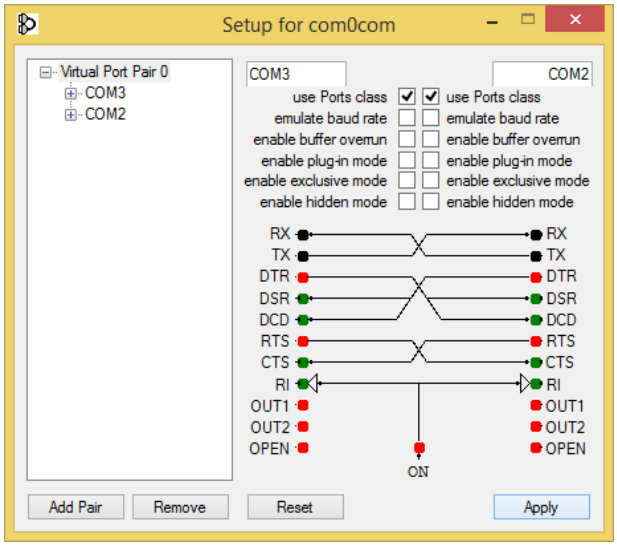


Ora tutte le porte non utilizzate sono visualizzate in trasparenza (anche la nostra COM3):

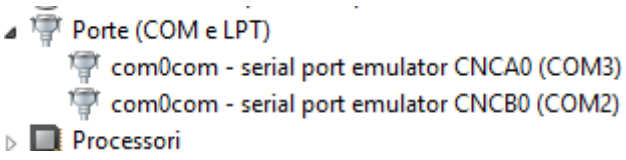


Ora selezionate la porta COM3 e cliccate su “Disinstalla”:

Ora la COM3 è libera e possiamo utilizzarla sul setup di com0com:

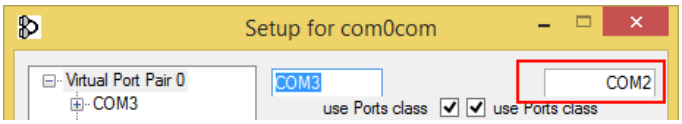


Infine cliccate su "Apply", ora viene creata la coppia COM3/COM2:



ATTENZIONE!

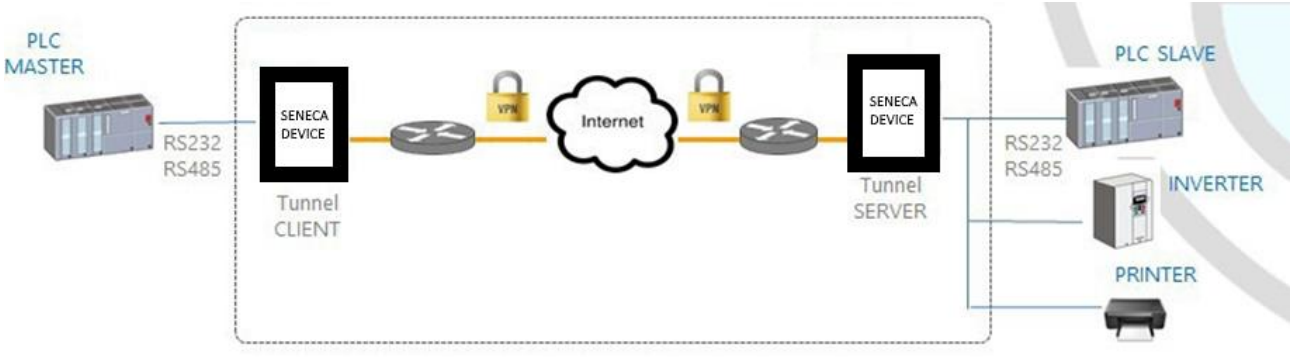
Il Software Seneca Ethernet to Serial Connect utilizza sempre la porta corretta della coppia creata nella configurazione com0com (nel nostro caso COM2)



7.3.1.1.5. CONNESSIONE AUTOMATICA ALL'AVVIO DEL PC

Una volta configurate le porte necessario è possibile far partire in automatico il software all'avvio del pc in modo da avere le connessioni sempre attive.
Per far questo salvare la configurazione con l'apposito pulsante e spuntare l'abilitazione della connessione automatica all'avvio del PC:

7.3.2. TUNNEL SERIALE PUNTO PUNTO SU TCP



Il tunnel seriale punto punto consente di estendere una connessione seriale tra due dispositivi seriali che supportano lo stesso protocollo tramite una connessione TCP/UDP.

Nel modo operativo TCP, uno dei due dispositivi Seneca è definito come "Master" e un altro è lo "Slave": il primo è un Tunnel Client, che riceve i dati dalla linea seriale e li invia ad una connessione TCP in uscita, mentre il

secondo è un Tunnel Server, che riceve i dati da una connessione TCP in entrata e li invia alla linea seriale; in questa modalità si stabilisce un "tunnel" tra le due porte seriali.

In fase di configurazione, sul Master è necessario impostare l'indirizzo IP di destinazione e la Porta di destinazione che definisce la connessione TCP in uscita; sullo Slave, si deve impostare la Porta di Ascolto sulla quale viene accettata la connessione TCP in entrata.
Il tunnel può anche sfruttare la connettività VPN.

ATTENZIONE!

Nel modo operativo Serial Tunnel Point-to-Point su TCP, viene accettata una sola connessione per una data porta seriale.

7.3.3. TUNNEL SERIALE PUNTO PUNTO SU UDP

Il modo operativo Serial Tunnel Point-to-Point su UDP è molto simile a quello del TCP.

L'unica differenza è che non viene stabilita alcuna connessione TCP e i dati seriali sono trasportati da un pacchetto UDP.
I parametri di configurazione sono gli stessi del tunnel seriale su TCP.
Anche in questo caso, il tunnel può anche sfruttare la connettività VPN.

ATTENZIONE

Nel modo operativo Serial Tunnel Point-to-Point su UDP, è accettata una sola connessione per una data porta seriale.

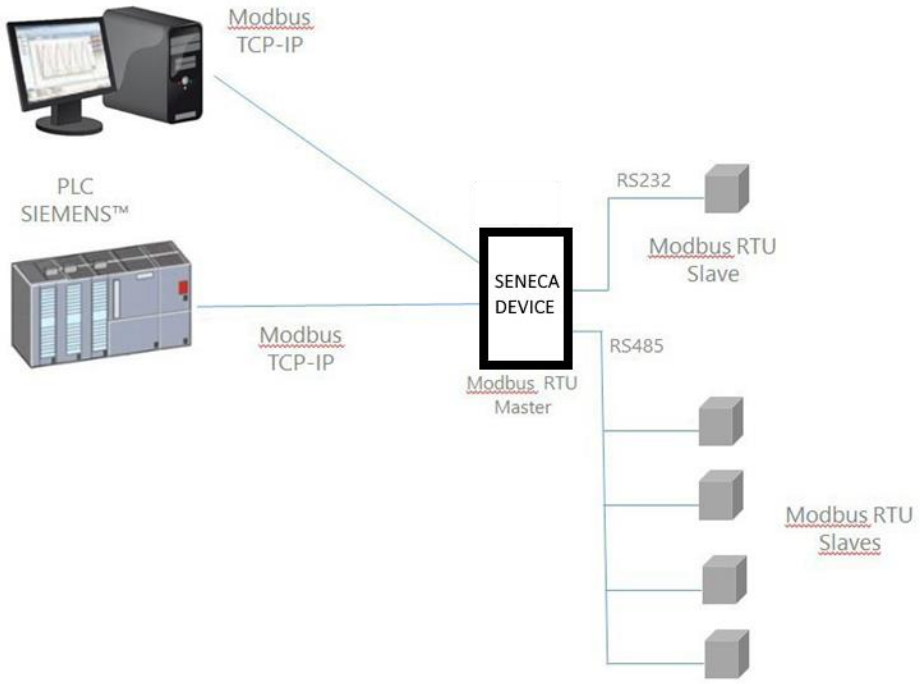
7.4. MODBUS GATEWAY CON MEMORIA SHARED

Il dispositivo può essere configurato per funzionare come Modbus Gateway con Shared Memory: in questa modalità, una serie di tag configurati vengono periodicamente e continuamente letti da dei dispositivi Modbus RTU Slave o Modbus TCP Server; questi valori sono copiati e resi disponibili in una memoria condivisa (shared).

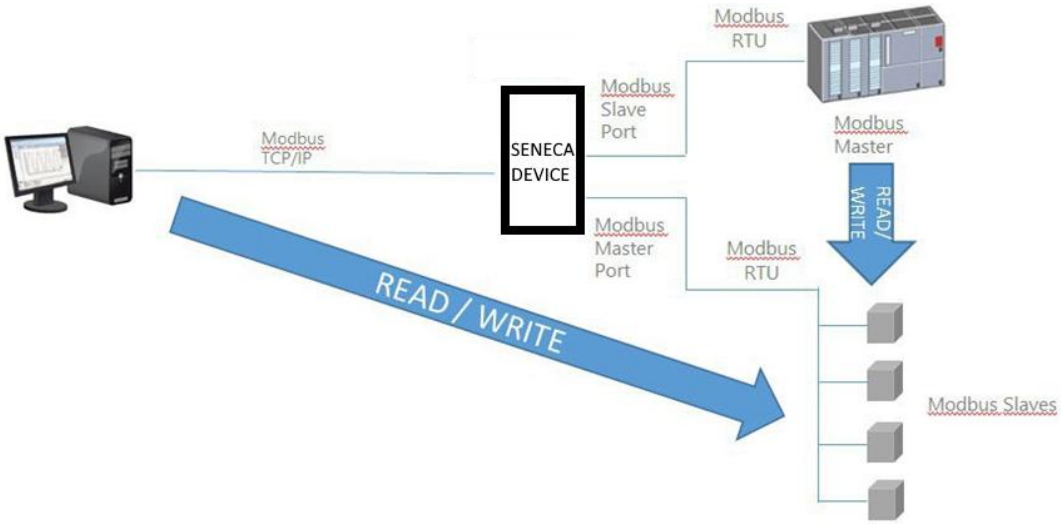
La modalità supporta fino a 2000 tag e accetta fino a 50 Modbus TCP Client contemporaneamente, un Modbus TCP/IP Server (o slave) è sempre in esecuzione su una porta TCP configurata.

Per ognuna delle porte seriali disponibili si può definire il tipo di "Task": una porta seriale può essere configurata come Modbus RTU Master o Modbus RTU Slave oppure disabilitata.
In questo modo sono disponibili diverse combinazioni possibili.

Inoltre, i tag possono essere letti da/scritti fino a 25 Modbus TCP Server.
Infine, si possono definire alcuni tag che sono relativi agli I/O digitali "embedded" presenti nel dispositivo.
Nelle immagini seguenti sono mostrati alcuni scenari tipici.

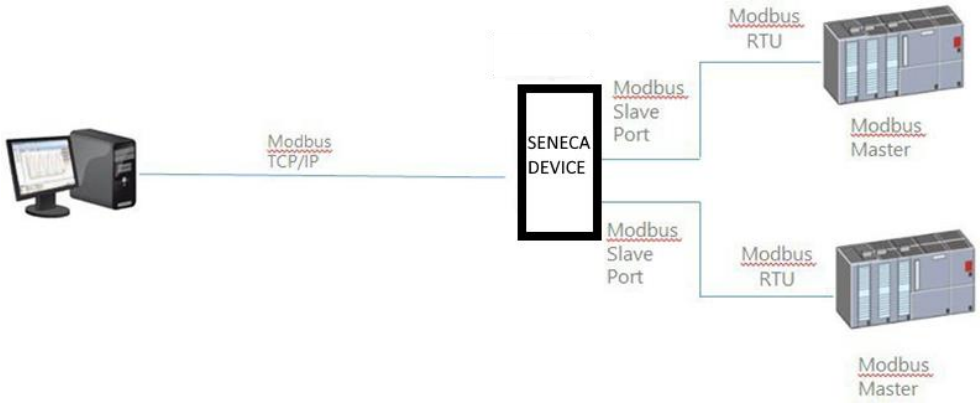


Nella figura sopra, due porte seriali sono configurate come Modbus RTU Master.



In questo caso, una porta seriale è configurata come Modbus Slave e un'altra è configurato come Modbus Master.

Quando alcuni registri acquisiti dagli Slave Modbus devono essere disponibili per un PLC, che supporta solo il protocollo Modbus Master, il dispositivo può essere configurato con una porta seriale definita come Modbus Slave (collegata al PLC) e un'altra in Modbus Master (collegata al bus Modbus Slaves). Il PLC Modbus RTU Master Modbus e il/i client TCP Modbus TCP scriveranno/leggeranno i registri della memoria condivisa del dispositivo Seneca, mentre lo la modalità Modbus gateway con Shared Memory mantiene la memoria condivisa allineata con i registri Modbus Slaves.



Nella figura sopra, due porte seriali sono configurate come Modbus Slave e collegate ad una porta PLC Modbus Master; in questo modo, i due PLC e il Modbus TCP Client possono scrivere/leggere la memoria condivisa per condividere i dati tra loro.

La modalità Modbus Gateway Shared Memory fornisce alcune interessanti caratteristiche, come spiegato di seguito.

Oltre al comportamento "classico" del gateway, i tag possono essere configurati per funzionare in modalità "Bridge"; questa modalità permette di “rinfrescare” i valori dei tag dal lato seriale solo quando il gateway riceve le richieste Modbus TCP/RTU per quei tag; questo può essere molto utile quando si utilizzano dispositivi RTU con uscite "Fail safe", dove è necessario effettuare ciclicamente le scritture delle uscite altrimenti si otterrebbe un fail.
Modbus Gateway Shared Memory esegue anche l'ottimizzazione delle richieste, inserendo il maggior numero possibile di registri in una singola richiesta di lettura/scrittura; è possibile impostare il numero massimo di registri in una richiesta indipendentemente per ogni porta seriale/TCP Server e per operazioni di lettura e scrittura; questa opzione può essere utile per collegare dispositivi RTU che supportano un numero massimo di registri diversi su diverse porte seriali.
La configurazione dei tag può anche essere creata utilizzando un Template Microsoft Excel™ fornito da Seneca, questo può ridurre notevolmente i tempi di configurazione, in particolare quando deve essere configurato un gran numero di tag.

8. CONFIGURAZIONE DEI DISPOSITIVI TRAMITE WEBSERVER DI CONFIGURAZIONE

I dispositivi possono essere completamente configurati tramite una serie di pagine web.

8.1. PAGINA "SUMMARY"

In questa pagina sono rappresentate le principali informazioni sullo stato del dispositivo e sull'utente attualmente loggato.
È anche possibile visualizzare la versione di firmware installata e le opzioni attivate.

8.2. PAGINA NETWORK AND SERVICES

Di seguito sono elencati tutti i parametri di configurazione disponibili in questa pagina, con una breve spiegazione e il valore predefinito del parametro per ciascuno di essi.

8.2.1. SEZIONE NETWORK

DHCP ON WAN
Permette di attivare o no il DHCP nella porta ethernet "WAN"

LAN IP Address
Permette di impostare l'indirizzo IP della porta ethernet "LAN"

LAN Network Mask
Permette di impostare la maschera della porta ethernet "LAN"

WAN IP Address
Permette di impostare l'indirizzo IP della porta ethernet "WAN"

WAN Network Mask
Permette di impostare la maschera della porta ethernet "WAN"

Default Gateway
Permette di impostare il default gateway della porta ethernet "WAN"

DNS Mode
Permette di impostare se il DNS deve essere definite statico o preso dal DHCP

DNS Server
Permette di impostare l'indirizzo IP del server DNS

IP Configuration from Discovery
Permette di selezionare se è possibile o meno cambiare la configurazione IP dal software Seneca Discovery Device (Attenzione: dal Seneca Discovery Device è possibile cambiare le impostazioni della sola porta ethernet a cui si è connessi). Attenzione che per la porta LAN non è possibile attivare il DHCP.

8.2.2. SEZIONE WEB SERVER

Protocol
Permette di selezionare il protocollo per il webserver, è possibile scegliere tra http, https o entrambi.

Se si seleziona http è possibile accedere ai due webserver con gli indirizzi di default:

http://192.168.90.101:8080 e http://192.168.90.101

Se si seleziona https è possibile accedere ai due webserver con gli indirizzi di default:

https://192.168.90.101/maintenance e https://192.168.90.101

HTTP Conf Port
Permette di impostare la porta del webserver di configurazione

HTTP Remote Display Port
Permette di impostare la porta del webserver del display virtuale

8.2.3. SEZIONE FILE TRANSFER

Protocol
Permette di configurare se attivare o no il protocollo SFTP server per l'accesso al filesystem del dispositivo.

SFTP Port
Permette di configurare la porta del server SFTP.

8.2.4. SEZIONE DATA FOLDER SHARING

Enable
Permette di abilitare o no la condivisione della cartella /data da dispositivi windows tramite protocollo Samba.

8.2.5. SEZIONE NETWORK REDUNDANCY

Enable
Permette di abilitare e di selezionare la strategia di ridondanza della comunicazione.
È possibile scegliere tra le seguenti configurazioni:

OFF -> La ridondanza è disabilitata
WAN/MOBILE -> Se la comunicazione verso il server impostato tramite la porta ethernet WAN è interrotta, abilita la comunicazione tramite modem Mobile (se disponibile).
MOBILE/WAN-> Se la comunicazione verso il server impostato tramite il modem Mobile è interrotta, abilita la comunicazione tramite la porta ethernet WAN.
WAN/WIFI-> Se la comunicazione verso il server impostato tramite la porta ethernet WAN è interrotta, abilita la comunicazione tramite la WIFI.
WIFI/WAN-> Se la comunicazione verso il server impostato tramite la WIFI è interrotta, abilita la comunicazione tramite la porta ethernet WAN.

Ping Address
Permette di impostare l'indirizzo del server da raggiungere da utilizzare come test per la ridondanza (attenzione: perchè funzioni la ridondanza il server deve rispondere alla richiesta di ping)

8.2.6. SEZIONE R-COMM (solo per modello R-PASS)

R-COMMM Available
Se abilitato attiva il controllo del modulo opzionale R-COMM

R-COMM UPS Mode
Configura il tipo di funzionamento dell'UPS presente nel modulo R-COMM.
Attenzione: Verificare che il modello di R-COMM acquistato abbia la funzione "UPS" prima di configurare questi parametri.
Nel caso l'R-COMM acquistato non preveda l'UPS questo parametro va impostato su "OFF".
OFF-> non utilizza l'UPS di R-COMM per alimentare R-PASS
Shutdown immediately-> in caso di mancanza di alimentazione di rete chiude i file di log ed esegue un shutdown pulito di R-PASS
Shutdown on low power-> in caso di mancanza di alimentazione di rete R-PASS continua a funzionare finché la batteria è carica, quando si sta scaricando chiude i file di log ed esegue un shutdown pulito di R-PASS

8.2.7. SEZIONE WATCHDOG

Enable
Se abilitato permette di eseguire un reboot se il dispositivo rimane bloccato per un tempo pari al watchdog timeout.

Timeout
Rappresenta il tempo in secondi che può rimanere bloccato il dispositivo prima di eseguire un reboot.

8.2.8. SEZIONE DEBUG LOGS

Enable
Se abilitato crea dei file di log per essere analizzati dai tecnici Seneca.

I file di log possono essere scaricati dalla pagina “Conf. Management“ del webserver

8.3. PAGINA PLC CONFIGURATION

8.3.1. SEZIONE STRATON PLC

Enable
Permette di attivare o no il PLC Straton

TCP Port
Permette di impostare la porta per la connessione con l’ambiente (IDE) di Straton

Redundancy Enable
Permette di abilitare o meno la ridondanza del PLC Straton, vengono creati 2 dispositivi uguali di cui uno è automaticamente impostato come master ed uno come slave. I dispositivi si scambiano continuamente le informazioni tra loro. Nel caso uno divenisse non disponibile, l’altro è attivato virtualmente senza perdita di continuità.
Per maggiori informazioni fare riferiemento al manuale del PLC Starton.

Redundancy IP Address
Permette di impostare l’indirizzo IP del secondo PLC che fa parte della ridondanza.

License Key
Permette di attivare i protocolli Energia (IEC61850, IEC60870-5-104 o IEC60870-5-101).
La chiave da inserire viene inviata dal supporto Seneca in caso di acquisto delle rispettive licenze.

Retain Variables Enable
Permette di configurare come devono essere gestiti i TAG di tipo retain (solo se il PLC Straton è impostato nella modalità “shared”).
Un Tag di tipo Retain viene salvato ciclicamente in una memoria non volatile così che, in caso di spegnimento del dispositivo, non perda il valore acquisito.
Un classico caso è il valore di un contatore di energia.

Se impostato ad OFF: le variabili retain sono gestite dal firmware, se impostato ad ON la gestione delle variabili retain è fatta dal PLC.

8.3.2. SEZIONE Real-Time Behaviour

ENABLE
Abilita la modalità Real Time nel PLC
Abilitando questa funzione lo scheduler del sistema operativo passa in modalità Real Time e permette di gestire il PLC riducendo il Jitter dei cycle time del PLC.
Nel caso si utilizzi un protocollo real time nel PLC è consigliato abilitare questa funzione.

8.4. PAGINA PLC MODBUS CONF.

8.4.1. SEZIONE Modbus TCP Client

Questi parametri permettono di impostare l'indirizzo ip e la porta del modbus TCP-IP server a cui il Modbus TCP-IP client del PLC Straton deve connettersi senza inserirli staticamente nella configurazione dell'IDE.
Questo è molto utile nel caso si debbano creare più PLC che puntano a Modbus TCP-IP server differenti senza ricompilare ogni volta il progetto Straton.
Affinchè straton utilizzi questi parametri è necessario usare il seguente testo al posto del valore dell'IP e della Porta del server Modbus TCP-IP:

mbtcpcli_param

a questo punto l'indirizzo IP e la porta saranno sostituiti con i valori qui impostati.

IP Address
Permette di impostare l'indirizzo IP del server Modbus TCP-IP a cui connettersi tramite il Modbus TCP-IP client di Straton.
Attenzione: nell'IDE di Straton va inserito il testo:

mbtcpcli_param

l posto dell'IP.

TCP Port
Permette di impostare la porta del server Modbus TCP-IP a cui connettersi tramite il Modbus TCP-IP client di Straton.
Attenzione: nell'IDE di Straton va inserito il testo:

mbtcpcli_param

al posto della TCP Port.

8.4.2. SEZIONE Modbus Pass-through

Questa funzione è disponibile solo se è attivo il PLC Straton

Enable

Se abilitato permette di attivare il modbus passthrough quando sta funzionando il PLC Straton. Qualunque richiesta modbus TCP-IP che arriva alla porta impostata verrà girata alla seriale COM2.
Solo nel caso si utilizzi il software Z-NET per la configurazione del dispositivo è possibile cambiare la porta COM2 con un'altra.

TCP Port

È la porta utilizzata per il Modbus passthrough.

8.5. PAGINA SERIAL PORTS

Il parametro Mode ha effetto sia sul Gateway del firmware sia sul PLC Straton, mentre le altre proprietà delle porte seriali si riferiscono alle funzionalità Gateway del firmware dei dispositivi, nel caso il PLC Straton utilizzasse la stessa seriale, i parametri qui configurati (baud, nr bit etc..) saranno sovrascritti e quindi non avranno alcun effetto (hanno priorità quelli definiti nel PLC Straton).

8.5.1. SEZIONE COM1 (RS485/RS232/MBUS)

Mode

Seleziona il tipo di seriale da utilizzare per la COM1 (sia per il PLC che per il firmware):
RS232, RS485 o RS232-MeterBus (attraverso dispositivo opzionale Z-MBUS).

Baud Rate

È il baud rate a cui deve funzionare la porta seriale.

Data Bits

È il numero di bit con cui deve funzionare la porta seriale.

Parity

Definisce se deve utilizzare la parità e che tipo.

Stop Bits

Definisce se usare o no I bit di stop.

8.5.2. SEZIONE COM2 (RS485)

Mode

Seleziona il tipo di seriale da utilizzare per la COM2 (sia per il PLC che per il firmware): per la COM2 è possibile scegliere solo RS485.

Baud Rate
È il baud rate a cui deve funzionare la porta seriale.

Data Bits
È il numero di bit con cui deve funzionare la porta seriale.

Parity
Definisce se deve utilizzare la parità e che tipo.

Stop Bits
Definisce se usare o no I bit di stop.

8.5.3. SEZIONE COM4 (RS485)

Questa porta è disponibile solo nei modelli Z-PASS1/2-RT, Z-TWS4-RT.

Mode
Seleziona il tipo di seriale da utilizzare per la COM2 (sia per il PLC che per il firmware): per la COM4 è possibile scegliere solo RS485.

Baud Rate
È il baud rate a cui deve funzionare la porta seriale.

Data Bits
È il numero di bit con cui deve funzionare la porta seriale.

Parity
Definisce se deve utilizzare la parità e che tipo.

Stop Bits
Definisce se usare o no I bit di stop.

8.6. PAGINA WI-FI CONFIGURATION

Questa pagina è disponibile solo nei modelli dotati di porta Wifi.

Mode

È possibile selezionare tra:
OFF: La porta WI-FI è spenta
Station: La Wi-Fi è connessa ad una rete esistente

Access Point: Il dispositivo crea una nuova rete Wi-Fi a cui i dispositivi potranno connettersi

SSID
Nel caso Mode valga “Access Point” è possibile definire il nome della nuova rete Wi-Fi che creerà il dispositivo
Nel caso Mode valga “Station” visualizza l’SSID della rete a cui si è connessi.

KEY MODE
Rappresenta il protocollo di crittografia da utilizzare.

SCAN/APPLY
Permette, in modalità Station, di selezionare la rete Wi-Fi a cui connettersi

8.7. PAGINA I/O CONFIGURATION

In questa pagina è possibile configurare gli IO a bordo del dispositivo.

8.7.1. SEZIONE Digital I/O Configuration

Questa sezione permette di configurare gli IO digitali.
Ogni modello di dispositivo ha una diversa configurazione di IO digitali:

MODELLO SSD

Input/Output 1 Mode
È possibile scegliere tra:

Remote Connection Disable
Il canale è impostato come INPUT e se portato BASSO abilita la possibilità di aprire una connessione VPN remota con il dispositivo, se ALTO ogni connessione VPN è bloccata.

General Input
Il canale è impostato come Ingresso digitale generico

General Output
Il canale è impostato come Uscita digitale generica

Input/Output 2 Mode
È possibile scegliere tra:

Remote Connection Active

Il canale è impostato come OUTPUT, se APERTO significa che non è attiva alcuna connessione VPN. Se CHIUSO significa che una connessione VPN è in corso.

Local alarm

Il canale è impostato come ingresso che viene tipicamente viene collegato ad un PLC di controllo esterno, quando è ALTO indica un errore generale che è visibile da remoto tramite l'interfaccia di stato di Seneca VPN BOX1, attualmente questo parametro non è utilizzato da VPN BOX2.

Remote toggle

Attualmente non usato

General Input

Il canale è impostato come Ingresso digitale generico

General Output

Il canale è impostato come Uscita digitale generica

MODELLO R-PASS

Input 1 Mode

È possibile scegliere tra:

Remote Connection Disable

Il canale è impostato come INPUT e se portato BASSO abilita la possibilità di aprire una connessione VPN remota con il dispositivo, se ALTO ogni connessione VPN è bloccata

General Input

Il canale è impostato come Ingresso digitale generico

Input 2 Mode

È possibile scegliere tra:

Local alarm

L' ingresso viene tipicamente vcollegato ad un PLC di controllo esterno, quando è ALTO indica un errore generale che è visibile da remoto tramite l'interfaccia di stato di Seneca VPN BOX1, attualmente questo parametro non è utilizzato da VPN BOX2.

General Input

Il canale è impostato come Ingresso digitale generico

Input 3 Mode

General Input

Il canale è impostato come Ingresso digitale generico

Input 4 Mode

General Input

Il canale è impostato come Ingresso digitale generico

Output 1 Mode

È possibile scegliere tra:

Remote Connection Active

Se APERTO significa che non è attiva alcuna connessione VPN. Se CHIUSO significa che una connessione VPN è in corso.

Remote toggle

Attualmente non usato

General Output

Il canale è impostato come Uscita digitale generica

Output 2 Mode

General Output

Il canale è impostato come Uscita digitale generica

Output 3 Mode

General Output

Il canale è impostato come Uscita digitale generica

Output 4 Mode

General Output

Il canale è impostato come Uscita digitale generica

MODELLO Z-PASS1/2

Input/Output 1 Mode

È possibile scegliere tra:

Remote Connection Disable

Il canale è impostato come INPUT e se portato BASSO abilita la possibilità di aprire una connessione VPN remota con il dispositivo, se ALTO ogni connessione VPN è bloccata.

General Input

Il canale è impostato come Ingresso digitale generico

General Output

Il canale è impostato come Uscita digitale generica

Input/Output 2 Mode

È possibile scegliere tra:

Remote Connection Active

Il canale è impostato come OUTPUT, se APERTO significa che non è attiva alcuna connessione VPN. Se CHIUSO significa che una connessione VPN è in corso.

General Input

Il canale è impostato come Ingresso digitale generico

General Output

Il canale è impostato come Uscita digitale generica

Input/Output 3 Mode

General Input

Il canale è impostato come Ingresso digitale generico

General Output

Il canale è impostato come Uscita digitale generica

Local alarm

Il canale è impostato come ingresso che viene tipicamente viene collegato ad un PLC di controllo esterno, quando è ALTO indica un errore generale che è visibile da remoto tramite l'interfaccia di stato di Seneca VPN BOX1, attualmente questo parametro non è utilizzato da VPN BOX2.

Input/Output 4 Mode

General Input

Il canale è impostato come Ingresso digitale generico

General Output

Il canale è impostato come Uscita digitale generica

Remote toggle

Attualmente non usato

Input/Output 5 Mode

General Input

Il canale è impostato come Ingresso digitale generico

General Output

Il canale è impostato come Uscita digitale generica

Input/Output 6 Mode

General Input

Il canale è impostato come Ingresso digitale generico

General Output

Il canale è impostato come Uscita digitale generica

8.7.2. SEZIONE Analog I/O Configuration

Permette di configurare gli ingressi analogici (non presenti nel prodotto SSD)

Analog Input 1 Mode

È possibile scegliere se impostare l'ingresso come ingresso Tensione (0-10V) o Corrente (0-20mA).

Analog Input 2 Mode

È possibile scegliere se impostare l'ingresso come ingresso Tensione (0-10V) o Corrente (0-20mA).

8.7.3. SEZIONE Security Level

Service Disable

Questo parametro determina quali servizi di accesso sono disabilitati quando l'ingresso digitale "Remote Connection Disable" è ALTO.

I valori possibili sono:

VPN Connection: Blocco della connessione VPN (Canale VPN di servizio ed Internet attivi)

VPN Service: Blocco del canale VPN di servizio (Internet attivo)

Internet Connection: Blocco dell'accesso ad internet (nel dispositivo è bloccato sia internet che la VPN)

SMS Service: Il modem viene spento e quindi non è possibile neanche la ricezione di SMS.

8.8. PAGINA REAL TIME CLOCK SETUP

Questa pagina permette di impostare i parametri della data/ora del dispositivo.
La data/ora è mantenuta per qualche giorno anche senza fornire alimentazione.

8.8.1. SEZIONE NTP

Il Network Time Protocol, in sigla NTP, è un protocollo per sincronizzare gli orologi dei dispositivi connessi all'interno di una rete. L'NTP è un protocollo client-server appartenente al livello applicativo ed è in ascolto sulla porta UDP 123.

Enable
Abilita o no l'acquisizione dell'ora dai server NTP impostati. La sincronizzazione avviene ogni 5 minuti.

Server primary
Indirizzo IP o FQDN del Server NTP primario

Server secondary
Indirizzo IP o FQDN del Server NTP secondario

Timezone
Impostazione del fuso orario

8.8.2. SEZIONE RTC

Nel caso di NTP server disabilitato è possibile impostare manualmente la data/ora o acquisirla direttamente dal PL collegato.

8.9. PAGINA GATEWAY CONFIGURATION

Questa pagina permette di attivare e di configurare il Gateway Ethernet-Seriale che si vuole utilizzare.
Per ogni seriale (a seconda del modello di dispositivo il numero di seriali è differente) è possibile scegliere tra:

Modbus Ethernet to Serial
Si tratta di una conversione di tipo real time da porta ethernet a porta seriale dal protocollo Modbus TCP-IP a Modbus RTU seriale.

Transparent

Si tratta di una conversione di tipo real time da porta ethernet a porta seriale indipendente dal protocollo.

Modbus Shared Memory
In questa modalità le acquisizioni vengono fatte da seriale (verso slave modbus RTU) o da ethernet (verso modbus TCP-IP server) e importati in una memoria interna. Questa modalità è indispensabile per l'utilizzo del datalogger, dei protocolli client e del cloud.

> ***⚠ ATTENZIONE!***
>
> ***Per poter utilizzare il datalogger, i protocolli client (ad esempio MQTT) e le regole logiche, è necessario impostare la modalità di funzionamento del gateway su Modbus Shared Memory.***

None
La porta seriale è libera o utilizzabile dai protocolli del PLC Straton (come ad esempio il MeterBUS).

Per maggiori informazioni sulle modalità di funzionamento del Gateway fare riferimento al rispettivo capitolo di questo manuale.

8.9.1. SEZIONE Modbus Shared Memory

In questa sezione sono riportate le configurazioni relative all'accesso alla memoria condivisa (shared) della modalità Modbus Shared Memory.

TCP Enable
Questo parametro abilita / disabilita il servizio Modbus Shared Memory Gateway.
È importante notare che, quando questo parametro è impostato su OFF, il servizio Modbus TCP-IP server non è in esecuzione anche se ad esso sono assegnate alcune porte seriali.

TCP Port
Imposta la porta di ascolto per il server Modbus TCP della Shared Memory

TCP Connections Max Number [1-50]
Numero massimo di connessioni TCP che possono essere accettate dal server Modbus TCP

Response Mode when Resource in Fail
Questo parametro definisce come viene costruita la risposta a una richiesta Modbus (lettura) per un tag corrispondente a una stazione Modbus che non risponde; quando mode è "Tag error value", il valore nella risposta Modbus è dato secondo i parametri "Error Mode" / "Error Value" nella definizione del tag; quando la modalità è "Exception", la risposta contiene un'eccezione con il valore 11 ("Gateway target device failed to respond").

Diagnostic Area Type

Selezionare se è possibile accedere alla diagnostica tramite registri Modbus Holding o registri Modbus Input Registers.

Diagnostic Area Address
Definisce il registro di partenza dell'area di diagnostica dei TAG.
L'area diagnostica riserva un bit per ogni tag configurato (125 registri) e ne fornisce lo stato FAIL/OK:

Il valore del bit su 0 -> significa Errore di lettura tag (o tag non configurato)
Il valore del bit su 1 -> significa Lettura tag OK

Pertanto, se è necessario controllare lo stato di errore dei primi 10 tag utilizzando l'area predefinita (9001 Holding Registers), è necessario leggere il registro 49001.
Ad esempio se il valore del register è:

0x3DB = 987 = 0000 0011 1101 1011
Tag 1 = OK
Tag 2 = OK
Tag 3 = FAIL
Tag 4 = OK
Tag 5 = OK
Tag 6 = FAIL
...
Si noti che un registro prima e un registro dopo l'area diagnostica saranno riservati (per impostazione predefinita i registri 49000 e 49126 o 39000 e 39126).

Internal Write Functions
Permette di scegliere come vanno scritti i TAG nei registri Modbus dei dispositivi slave o server.
Questo include le scritture con il pulsante "SET" della pagina del webserver dei TAG o le scritture delle regole logiche.

8.9.2. SEZIONE Modbus Ethernet to Serial e Modbus Shared Memory

Questa sezione permette di configurare l'indirizzo Slave ID (station modbus address) a cui il dispositivo risponde con i propri IO embedded.
I registri che rappresentano gli I / O sono accessibili tramite protocollo Modbus TCP-IP o RTU.
Gli indirizzi dei registri modbus variano a seconda del modello e sono definiti nel rispettivo capitolo di questo manuale.

8.9.3. SEZIONE COM0, COM1, COM2, COM4 (A SECONDA DEL MODELLO)

Qui è possibile impostare i parametri relativi alla modalità gateway che è stata scelta per ciascuna porta seriale.
La porta COM0 è disponibile quando viene connesso un convertitore USB-seriale

8.9.3.1. COM0 (USB)

A seconda della modalità scelta per la porta (in questo caso è disponibile solo la modalità Transparent) è possibile impostare i parametri:

Operating Mode
Per la porta COM0 è possibile scegliere solo la modalità “Virtual COM”.

Listen Port
È la porta su cui funziona il server della modalità Virtual port.

Data Packet Interval (ms)
È l’intervallo di tempo che sancisce la fine di un pacchetto, questo parametro deve essere impostato in base al tipo di protocollo che sta transitando.

8.9.3.1. COM1 (RS232/RS485) COM2 (RS485) COM4 (RS485)

A seconda della modalità scelta per la porta sono disponibili i seguenti parametri.

8.9.3.1.1. COM1/COM2/COM4 Modbus Ethernet to Serial

Permette di impostare i parametri della modalità Gateway Ethernet to Serial

Enable
Abilita o no la modalità Ethernet to Serial sulla porta seriale

Port
Imposta la porta TCP su cui funzionerà il gateway Ethernet to Serial

Response wait time [ms]
Imposta il tempo di attesa della seriale per decretare un timeout

8.9.3.1.2. COM1/COM2/COM4 Transparent

Permette di impostare il funzionamento della modalità trasparente.

Operating Mode
Per le porte COM1/COM4 è possibile scegliere tra:

VIRTUAL COM

SERIAL TUNNEL POINT TO POINT ON TCP

SERIAL TUNNEL POINT TO POINT ON UDP

8.9.3.1.2.1. COM1/COM2/COM4 VIRTUAL COM

Permette di impostare i parametri della modalità Gateway Ethernet to Serial

Enable
Abilita o no la modalità Ethernet to Serial sulla porta seriale

Port
Imposta la porta TCP su cui funzionerà il gateway Ethernet to Serial

Response wait time [ms]
Imposta il tempo di attesa della seriale per decretare un timeout

8.9.3.1.2.2. COM1/COM2/COM4 SERIAL TUNNEL POINT TO POINT ON TCP/UDP

Tunnel Role
Imposta il tunnel come master o slave

Destination Address
Se il Tunnel Role è master è l'indirizzo ip del Tunnel Role Slave remoto

Destination Port
Se il Tunnel Role è master è la Listen Port del Tunnel Role slave

Listen Port
Se il Tunnel Role è impostato su slave è la porta in ascolto del tunnel master remote

8.9.3.1.2.1. COM1/COM2/COM4 MODBUS SHARED GATEWAY

Task
Permette di selezionare il tipo di task Modbus Shared Gateway deve essere eseguito nella porta seriale selezionata tra:
None, Master, Slave o Sniffer

None
Nessun task attivo

Master
È attivo il modbus RTU master del gateway per acquisire dati da dispositivi modbus RTU slave

Slave
È attivo il modbus RTU slave del gateway per accettare connessioni da un modbus RTU master

Sniffer
È attivo lo sniffer seriale, ovvero acquisisce il protocollo modbus RTU dalla porta seriale in modo passivo. Viene utilizzato in impianti esistenti quando (ovvero quando esiste già un modbus master ed uno o più modbus slave) e si vuole acquisire dei dati in modo passivo.

Slave Address
Nella modalità Task = Slave è il valore dello slave address (station address) che deve assumere la seriale

Timeout (ms)
Nella modalità Task = Master è il Timeout di risposta per richieste Modbus RTU, in millisecondi

Delay between Polls (ms)
Nella modalità Task = Master è l'intervallo tra richieste Modbus RTU, in millisecondi

Read/Write Retries
Nella modalità Task = Master è il numero massimo di tentativi per richieste Modbus RTU; questo vale sempre per le richieste di scrittura; per le richieste di lettura, si applica solo ai tag con "Tag mode" = "BRIDGE"

Multiple Read Max Number
Nella modalità Task = Master è il numero massimo di registri Modbus che possono essere letti in una singola richiesta Modbus RTU; viene utilizzato per ridurre il numero di richieste di lettura inviate sul bus seriale (grazie a questo parametro il firmware esegue autonomamente una ottimizzazione)

Multiple Write Max Number
Nella modalità Task = Master è il numero massimo di registri Modbus che possono essere scritti in una singola richiesta Modbus RTU; viene utilizzato per ridurre il numero di richieste di scritture inviate sul bus seriale (grazie a questo parametro il firmware esegue autonomamente una ottimizzazione)

Validity Timeout
Nella modalità Task = sniffer se un determinato tag non lo si vede rinfrescato nella comunicazione per il tempo impostato allora viene impostato a FAIL.

8.10. PAGINA VPN CONFIGURATION

Questa pagina permette la configurazione di una VPN, i dispositivi Seneca supportano due tipi di VPN: VPN BOX oppure OPEN VPN.
Per maggiori informazioni sul server VPN BOX fare riferimento al capitolo VPN su questo manuale.

VPN MODE
Permette di scegliere il tipo di server VPN a cui connettersi, è possibile scegliere tra OPEN VPN o VPN BOX.

La versione di OPEN VPN installata è la 2.4.7

8.10.1.SEZIONE VPN FILES

Nel caso di connessione VPN con un server OPEN VPN questa sezione permette di caricare il file di configurazione e gli eventuali certificati.
Il file di configurazione deve contenere tutte le informazioni necessarie per configurare il comportamento di Open VPN.

Le principali opzioni di configurazione sono:
• se il dispositivo funzionerà da client o da server (in genere, sarà un client)
• il protocollo di trasporto (UDP o TCP)
• l'indirizzo IP del server / nome host e porta
• i file necessari per eseguire le procedure di autenticazione
• etc…

Questo file ha estensione ".ovpn" (nei sistemi Windows) o l'estensione ".conf" (nei sistemi Linux).
Indipendentemente dal nome originale, verrà rinominato come "ovpn.conf" sul dispositivo.
Questo è l'unico file obbligatorio, ovvero se questo file non è stato caricato sul dispositivo la VPN non può essere abilitata.
Come ricordato nella pagina Web, nelle opzioni che richiedono un argomento del file, deve essere fornito solo il nome del file, senza percorso, come nell'esempio seguente:

```
ca ca.crt                    OK

ca /home/config/vpn/ca.crt   FAIL
```

Altre due importanti regole che devono essere seguite sono:
• l'opzione "dev" deve essere: "dev tun0" o "dev tap0"
• l'opzione "log" deve essere omessa (in modo che i log vengano scritti su syslog)

Per maggiori informazioni sul file di configurazione OPEN VPN, fare riferimento alla documentazione di OPEN VPN 2.4 al link:

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/

CA CERTIFICATE

Questo file deve contenere il certificato dell'autorità di certificazione (CA) e ha l'estensione .crt.
È necessario quando il file di configurazione contiene l'opzione "ca".

CLIENT CERTIFICATE

Questo file deve contenere il certificato client e ha l'estensione .crt.
È necessario quando il file di configurazione contiene l'opzione "cert".

CLIENT KEY

Questo file deve contenere la chiave client e ha l'estensione .key.
È necessario quando il file di configurazione contiene l'opzione "key".

ADDITIONAL FILE

Questo file può essere di qualsiasi tipo e può essere necessario per opzioni di configurazione diverse da "ca", "cert" e "chiave".
Si noti che è possibile caricare più di un file aggiuntivo.

È possibile scegliere file dal proprio PC per selezionare i file e inviarli al dispositivo premendo il pulsante “UPLOAD”.
Al termine del caricamento, viene visualizzata una pagina dei risultati
È possibile controllare quali file VPN sono memorizzati sul dispositivo facendo clic sul pulsante "MOSTRA STATO VPN",

Come ricorda la pagina web, i file VPN possono essere scaricati dal dispositivo, se necessario, tramite FTP / SFTP; possono essere trovati nella directory /home/config/vpn.

È possibile cancellare tutti i file VPN, facendo clic sul pulsante “RESET”; apparirà un pop-up, che richiede una conferma.

Quando si preme il pulsante "SHOW VPN STATUS", viene visualizzata una terza sezione, denominata "VPN Status", che mostra:

• Il "Connection Status" della VPN (ovvero “Stopped” o “Running”)

• l'indirizzo IP assegnato all'interfaccia VPN quando “Connected”, l'indirizzo IP “fittizio” “0.0.0.0” quando “Disconnected”
• l'"OpenVPN Status" (ovvero: “Stopped” o “Running”)
• il numero di pacchetti / byte ricevuti dall'interfaccia VPN, quando connessi; "0/0" quando disconnesso
• il numero di pacchetti / byte inviati all'interfaccia VPN, quando connessi; "0/0" quando disconnesso
• i file VPN memorizzati sul dispositivo

Un'importante informazione sullo stato è data dal campo "OpenVPN Status"; se la VPN è abilitata ("ON"), ma questo stato è "Stopped", ciò significa che il processo Open VPN non può essere avviato correttamente: probabilmente, il file di configurazione contiene alcuni errori o, forse, alcune opzioni non supportate dall'implementazione OpenVpn del dispositivo.
È possibile aggiornare lo stato della VPN facendo clic sul pulsante "REFRESH".
Infine, è possibile nascondere la sezione "VPN Status", facendo clic sul pulsante "HIDE VPN STATUS".

8.10.2.SEZIONE OPEN VPN

Enable
Flag per abilitare / disabilitare la funzionalità “Open VPN”

Allowed Interface
Permette di forzare la connessione VPN tramite l'interfaccia specificata.

Reply on WAN to packets coming from WAN
Se abilitato permette che le risposte ai pacchetti provenienti dall'interfaccia WAN vengano inviate alla stessa interfaccia e non (ad esempio) tramite la VPN.

8.10.3.SEZIONE VPN BOX

Enable
Flag per abilitare / disabilitare la funzionalità “VPN Box”, ovvero la procedura / protocollo che consente al dispositivo di configurare la VPN, interagendo con il server “VPN Box” (consultare il “Manuale dell'utente di VPN Box”)

Server
Indirizzo IP o FQDN del server “VPN Box” o “VPN Box 2”

Password
Password per accedere al server “VPN Box”

Tag Name
Nome mnemonico utilizzato per identificare in modo univoco il dispositivo

Quando si fa clic sul pulsante "SHOW VPN STATUS", viene visualizzata una nuova sezione, denominata "VPN Status", che mostra:

• lo Stato connessione della VPN
• l'indirizzo IP VPN assegnato al dispositivo questa riga non viene visualizzata per la casella VPN "Point-to-Point (L2)", poiché nessun indirizzo IP è assegnato all'interfaccia VPN
• lo Stato di OpenVPN
• il numero di pacchetti / byte ricevuti dall'interfaccia VPN
• il numero di pacchetti / byte inviati all'interfaccia VPN
• il Tipo di VPN BOX, che può essere "Point-to-Point", "Point-to-Point (L2)" o "Single LAN"
• lo stato del VPN BOX, se la casella VPN è abilitata
• il nome utente dell'utente collegato, se presente

La tabella seguente fornisce una breve spiegazione delle possibili stringhe "Result" e "Status":

Result	Status	Significato
Error (Unexpected response)		È stato ricevuto un codice di risposta che non è gestito dal dispositivo (non dovrebbe mai verificarsi)
Error (No response from VPN Box)		Nessuna risposta ricevuta da VPN Box (timeout di risposta)
Error (Invalid response from VPN Box)		È stata ricevuta una risposta il cui contenuto non è valido per il dipositivo (non dovrebbe mai verificarsi)
Error (Wrong password)		La password impostata sul dispositivo è errata
Error (License Limit Reached)		Il numero massimo di dispositivi consentiti dalla licenza è già registrato su VPN Box
Error (VPN Box not configured)		La VPN Box non è stata ancora configurata
Error (Generic error)		Si è verificato un errore generico su VPN Box
OK		Il dispositivo è appena stato registrato su VPN Box
OK	New	Il dispositivo è registrato su VPN Box, ma non è ancora configurato (solo "LAN singola")
OK	Configuration updated	La configurazione del dispositivo è appena stata aggiornata
OK	Configured	Il dispositivo è correttamente configurato e disponibile per la connessione VPN
OK	Ban	Il dispositivo è stato “bannato”
OK	Not found	Il dispositivo non è noto a VPN Box; questo accade quando la registrazione del dispositivo viene cancellata su VPN Box
OK	Unknown	Il dispositivo ha uno stato sconosciuto in VPN Box (non dovrebbe mai verificarsi)

OK	Not bound	Il "tunnel" tra dispositivo e VPN Box non è attivo; ciò può verificarsi quando la porta del tunnel è bloccata (non aperta) nel router ADSL sul lato VPN Box (solo "Point-to-Point")
OK	Unexpected status	È stato ricevuto un codice di stato che non è gestito dal dispositivo (non dovrebbe mai verificarsi)

8.11. PAGINA OPC-UA SERVER CONFIGURATION

In questa pagina, è possibile impostare i parametri relativi al server OPC Unified Architecture (OPC-UA) integrato nel gateway.

Il server OPC-UA del dispositivo "esporta" i tag Modbus Shared Memory Gateway; pertanto, utilizzando un software client OPC-UA, è possibile leggere / scrivere i tag mediante il protocollo OPC-UA.

NOTA: per tutte le variabili sul server OPC-UA il namespace-id è fissato su "1".

8.11.1.SEZIONE OPC-UA Server Conf.

Enable
Abilita/Disabilita il server OPC-UA, una volta attivato il server è disponibile all' URL:

opc.tcp://IP_Address:Port/

Port
Imposta la porta del server OPC-UA

Username
Username per accesso al server

Password
Password per accesso al server

Security Policy
È possibile scegliere tra:

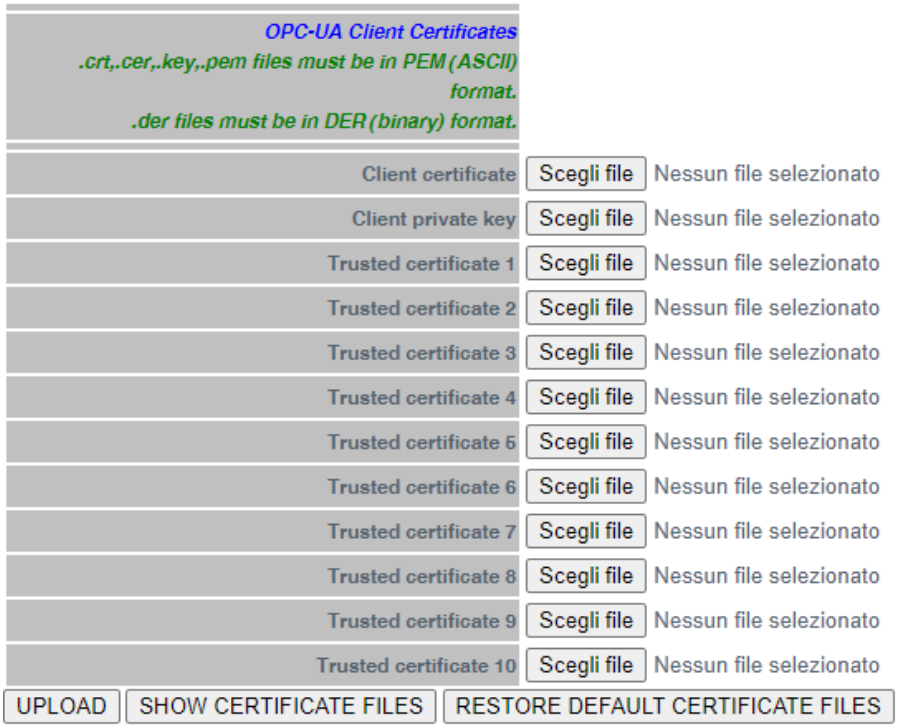
“None”
“Basic128Rsa15”
“Basic256Sha256”

8.11.1.1.SEZIONE OPC-UA SERVER CERTIFICATES

Una coppia predefinita di certificati è già inclusa nel prodotto, è anche possibile aggiungere i propri certificati con gli appositi pulsanti.

8.12. PAGINA OPC-UA CLIENT CONFIGURATION

In questa pagina è possibile caricare i certificati di connessione ai server per l'OPC-UA client.



Il pulsante "Scegli File" seleziona il certificato. Questi vengono caricati sul dispositivo solo dopo aver premuto il pulsante "Upload".
Il pulsante "Show Certificate Files" permette di visualizzare i file dei certificati caricati.
Il pulsante "Restore Default Certificate Files" permette di ripristinare i file dei certificati di default.

8.13. PAGINA SNMP CONFIGURATION

In questa pagina viene descritta la configurazione dell'Agent SNMP.
È supportata la versione SNMP V2C.
Il protocollo è utilizzabile solo se è abilitato il PLC Straton.

8.13.1.SEZIONE GENERAL CONFIGURATION

Enable
Abilita o no il protocollo SNMP

Port
Porta utilizzata dal protocollo SNMP

Trap Type
Seleziona il tipo di Trap da utilizzare

Trap Port
Porta utilizzata dalle Trap

Allow access from any host
Quando questo parametro è disattivato, l'accesso sarà consentito solo agli host indicati di seguito con "Access" selezionato.

8.13.2.SEZIONE COMMUNITIES

Name
Identificativo del Community

Read
Fornisce le proprietà di lettura al Community selezionato

Write
Fornisce le proprietà di Scrittura al Community selezionato

8.13.3.SEZIONE HOSTS

IP Address
Permette di definire l'IP dell'Host

Community
Permette di definire a quale community è associato l'Host

Access
Se Flaggato permette all'host di accedere all'Agent SNMP

Trap
Se Flaggato permette all'host di ricevere le Trap dall' Agent SNMP

8.14. PAGINA USERS CONFIGURATIONS

In questa pagina è riportata la configurazione (user/password) di tutti gli account disponibili per l'accesso al Webserver e al Display.
È possibile inserire solo un solo utente per tipo.

WEB / DISPLAY ADMINISTRATOR
È l'account che permette ogni operazione sia sul webserver di configurazione sia su quello relativo al display (e al display sui modelli che ne sono dotati).

WEB / DISPLAY OPERATOR
È l'account che permette di accedere solo ad alcune pagine del webserver di configurazione, mentre nel webserver del display e nel display fisico permette di bloccare l'accesso al menu setup.

WEB / DISPLAY GUEST
È l'account che permette di accedere a quasi tutte le pagine ad eccezione di quelle di manutenzione avanzata (ad esempio non permette l'accesso alle pagine "FW Upgrade", e "Configuration Management"). Può visualizzare tutti i parametri di configurazione e le informazioni sullo stato, senza poter modificare alcun parametro.
Di conseguenza, in tutte le pagine, i pulsanti "APPLICA" (e qualsiasi altro pulsante utilizzato per eseguire le modifiche) sono disabilitati.

FTP USER
È l'account per l'accesso all'FTP server del dispositivo.

8.15. PAGINA ROUTER CONFIGURATION

In questa pagina è possibile modificare i parametri relativi alla funzionalità del router.

Router Enable
Abilita/Disabilita la funzionalità di router

DNS Enable
Flag per abilitare / disabilitare il servizio di inoltro DNS

DHCP Server Enable

Flag per abilitare / disabilitare il servizio DHCP (server DHCP)

DHCP First Address
DHCP Last Address
Questi parametri definiscono l'intervallo di indirizzi IP assegnati dal server DHCP ai client richiedenti

DHCP Lease Time (min)
Intervallo di tempo di validità per l'assegnazione dell'indirizzo IP, in minuti.

Use Local Addresses Through VPN/Enable
Flag per abilitare / disabilitare l'accesso al dispositivo e ad altri che si trovano collegati alla LAN, usando i loro indirizzi IP (LAN) locali

Mobile network firewall
Permette di abilitare o no il firewall sulla rete mobile (se disponibile).

8.16. PAGINA PORT MAPPING RULES

In questa pagina è possibile impostare le regole di port mapping (note anche come "server virtuali).

Protocol
Questo parametro definisce il protocollo di trasporto (o tipo di porta) interessato dalla regola: TCP, UDP o entrambi

External Port
Porta TCP o UDP a cui è stato originariamente inviato un pacchetto

Server IP Address
Indirizzo IP al quale viene inoltrato il pacchetto ricevuto

Internal Port
Porta TCP o UDP a cui viene inoltrato il pacchetto ricevuto

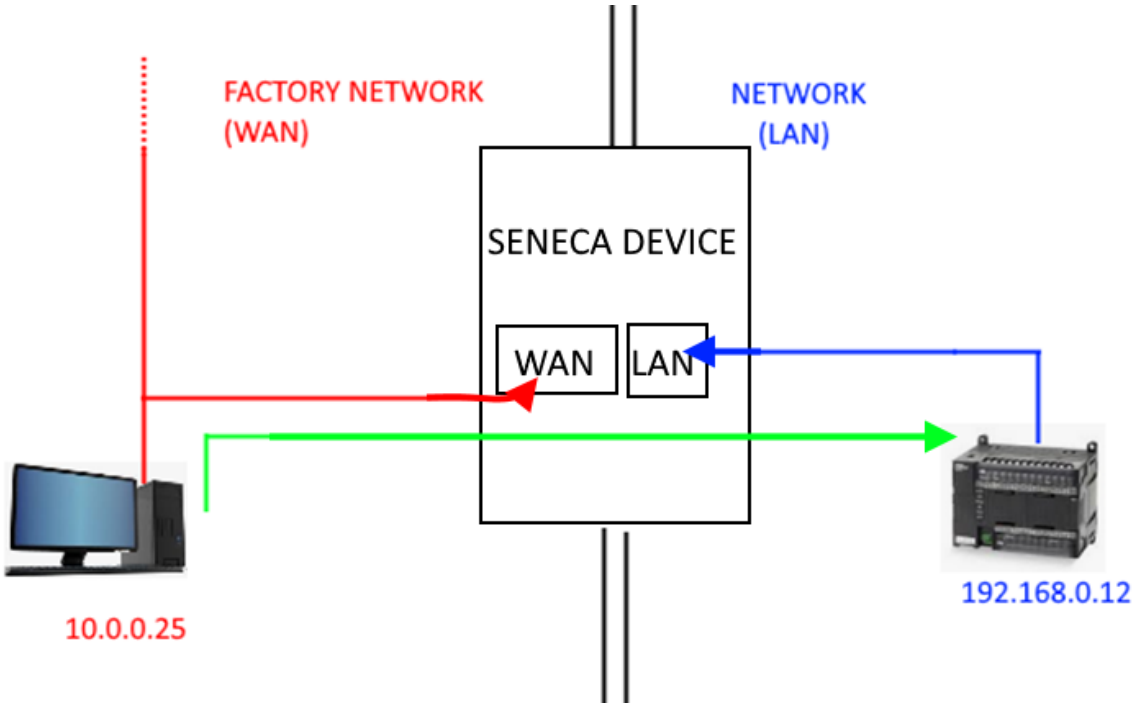
Ad esempio, se si impostano i valori:

Protocol = TCP-IP
External Port = 502
Server IP Address = 192.168.85.103
Internal Port = 503

La regola dice al dispositivo che qualsiasi pacchetto TCP o UDP ricevuto dal gateway sulla porta 502 (che viene spesso utilizzato per il protocollo Modbus TCP) deve essere inoltrato all'indirizzo IP 192.168.85.103 (che corrisponde a un altro dispositivo) sulla stessa porta di destinazione 503.

8.17. PAGINA NAT 1:1 RULES

È possibile utilizzare questa pagina per far accedere un dispositivo (ad esempio un PC) dalla WAN alla LAN. Si voglia quindi far accedere un PC connesso nella rete WAN ad un PLC connesso nella rete LAN come da figura:



Per fare ciò è necessario creare un nuovo indirizzo (10.0.0.26) che si trova in una rete compatibile con il PC (10.0.0.25).

	CURRENT	UPDATED
NAT 1:1 Configuration		
Interface		WAN
Device IP Address		192.168.0.12
Mapped IP Address		10.0.0.26
Description		WAN to LAN ACCESS1

APPLY

Ora il PLC 192.168.0.12 è accessibile dalla WAN utilizzando l'indirizzo 10.0.0.26.

Interface
Permette di scegliere l'interfaccia tra quelle disponibili

Device IP Address
È l'indirizzo del dispositivo che deve essere raggiunto

Mapped IP Address
È il nuovo indirizzo IP virtuale che deve essere compatibile con la rete (interfaccia) selezionata

Description
È la descrizione mnemonica della regola

8.18. PAGINA STATIC ROUTES

Questa pagina permette di impostare le static routes, questa funzione permette di instradare un indirizzo o un intervallo di indirizzi a gateway differenti.
Ad esempio, se di deve raggiungere 2 indirizzi diversi: 192.168.85.23 e 192.168.82.56 ma è necessario passare attraverso 2 gateway diversi.

Destination Address
È l'indirizzo di destinazione da raggiungere

Subnet Mask
È la subnet mask

Gateway
È l'indirizzo del gateway su cui deve passare

Interface
È l'interfaccia usata

Description
È il testo mnemonico della regola

Ad esempio si abbia:

1) Per accedere a 192.168.85.23 è necessario passare dal gateway 192.168.80.1
2) Per accedere a 192.168.82.56 è necessario passare dal gateway 192.168.80.100
Si dovrà utilizzare la configurazione:

Regola #1:
Destination Address = 192.168.85.23

Subnet Mask = 255.255.255.255

Gateway = 192.168.80.1

Interface = LAN

Description = Go to 85

Regola #2:
Destination Address = 192.168.82.56

Subnet Mask = 255.255.255.255

Gateway = 192.168.80.100

Interface = LAN

Description = Go to 82

8.19. PAGINA MOBILE NETWORK (Mobile Configuration)

Questa pagina permette la configurazione della connessione mobile (se presente).

8.19.1.SEZIONE SIM

PIN
È il numero del PIN per accedere alla SIM (se configurato)

8.19.2.SEZIONE OPERATOR SELECTOR

Mode
È possibile scegliere la strategia con cui selezionare l'operatore mobile:

Automatic: l'operatore è scelto in automatico
Manual: l'operatore è imposto manualmente, nel caso l'operatore non fosse disponibile, la connessione non potrà avvenire
Manual/Automatic: permette di impostare l'operatore in modalità manuale ma nel caso l'operatore non fosse disponibile il sistema passarà in modalità "automatic".

Operator
Consente di selezionare l'operatore manualmente, per far apparire una lista degli operatori disponibili nella zona è necessario premere il pulsante "Get Operator List"

8.19.3.SEZIONE DATA CONNECTION

Enable
Abilita o no l'utilizzo dei dati su rete mobile.

APN Mode
Permette di impostare manualmente l'APN o di utilizzare l'auto APN (l'APN viene recuperato da un database interno).
Attenzione, nel database non sono presenti tutti i possibili APN mondiali ma solo quelli principali.

APN
È l'APN (punto d'accesso che consente ai dispositivi mobili di di usufruire di una connessione a Internet) attualmente utilizzato o da utilizzare.

Authentication Type
È il tipo di autenticazione da utilizzare per l'APN

Username
È lo username per l'APN

Password
È la password per l'APN

Host for connection check (ping)
È l'url o l'IP che il dispositivo utilizza per la diagnosi della connessione mobile

Set Default Gateway
Permette di non impostare un default gateway per la rete mobile (e quindi di mantenere il default gateway della WAN o della rete WIFI).

8.20. PAGINA DDNS CONFIGURATION (Mobile Configuration)

Questa pagina permette la configurazione dei servizi di DDNS. DNS dinamico (dynamic DNS, DDNS) è una tecnologia che permette ad un nome DNS in Internet di essere sempre associato all'indirizzo IP di uno stesso host, anche se l'indirizzo cambia nel tempo.

TYPE
Permette di scegliere il servizio DDNS da utilizzare tra quelli elencati.

Hostname
È l'hostname del DDNS

Username

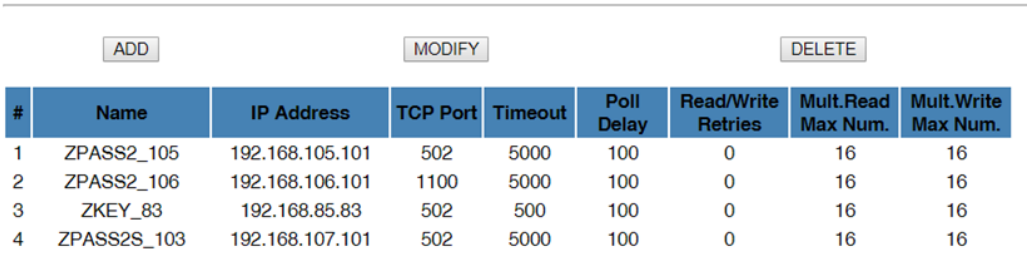
È lo username per il servizio

Password
È la password per il servizio

8.21. PAGINA TCP SERVERS (Shared Memory Tag Conf.)

In questa pagina viene mostrato l'elenco dei server Modbus TCP remoti, utilizzati per acquisire dati nella funzionalità Modbus Shared Memory Gateway.

Facendo clic sul pulsante "ADD" è possibile configurare un nuovo server TCP, come nella figura seguente:



#	Name	IP Address	TCP Port	Timeout	Poll Delay	Read/Write Retries	Mult.Read Max Num.	Mult.Write Max Num.
1	ZPASS2_105	192.168.105.101	502	5000	100	0	16	16
2	ZPASS2_106	192.168.106.101	1100	5000	100	0	16	16
3	ZKEY_83	192.168.85.83	502	500	100	0	16	16
4	ZPASS2S_103	192.168.107.101	502	5000	100	0	16	16

Name
Nome mnemonico del server TCP, questo nome viene utilizzato per identificare il server TCP nelle pagine “Tag Setup” e “Tag View”.

IP Address
Indirizzo IP del server modbus TCP-IP remoto

TCP Port
Porta TCP del server

Timeout (ms)
Timeout di connessione / risposta per richieste TCP Modbus, in millisecondi

Delay between Polls (ms)
Intervallo tra richieste TCP Modbus, in millisecondi

Read/Write Retries
Numero massimo di tentativi per richieste TCP Modbus; questo vale sempre per le richieste di scrittura; per le richieste di lettura, si applica solo ai tag con "Gateway Tag Mode" = "BRIDGE"

Multiple Read Max Number

Numero massimo di registri Modbus che possono essere letti in una singola richiesta Modbus TCP; viene utilizzato per ridurre il numero di richieste di lettura inviate tramite la connessione TCP eseguendo così una ottimizzazione delle prestazioni

Multiple Write Max Number
Numero massimo di registri Modbus che possono essere scritti in una singola richiesta Modbus TCP; viene utilizzato per ridurre il numero di richieste di scrittura inviate tramite la connessione TCP eseguendo così una ottimizzazione delle prestazioni

Il numero massimo di Server Modbus TCP-IP configurabili è 25.

8.22. PAGINA TAG SETUP (Shared Memory Tag Conf.)

Questa pagina viene utilizzata per configurare i tag nella modalità Modbus Shared Memory Gateway.
È possibile importare i tag inseriti tramite un template Excel (scaricabile dal sito Seneca) oppure esportare quelli attuali.
È anche possibile inserire nuovi tag direttamente dalla pagina web, tutti i dispositivi Seneca sono disponibili tramite un database interno.

L'aggiunta di un tag ha i seguenti campi (la maggior parte pre compilati poiché definiti nel database incluso nel prodotto)

Gateway Tag Name
Nome mnemonico del tag

Gateway Modbus Start Register Address
Indirizzo di partenza del tag sulla Gateway Shared Memory

Target Modbus Device
Dispositivo da cui leggere (o su cui scrivere) il tag (nel caso sia presente nel database) oppure custom.

Target Resource
Rappresenta la risorsa del dispositivo a cui associare il TAG (esempio Input1, Output2 etc…) solo nel caso diverso da Dispositivo Custom non presente in database.

Target Connected To
La porta seriale o la risorsa ethernet a cui è connesso il dispositivo esterno.

Gateway Tag Mode
Questo campo definisce come il tag verrà gestito dai processi del gateway; i valori possibili sono: GATEWAY, BRIDGE, SHARED MEMORY o EMBEDDED.

La differenza tra Gateway e Bridge è che i tag Bridge vengono aggiornati solo quando richiesto, nella modalità Gateway i tag sono aggiornati ciclicamente anche se non vengono richiesti.

SHARED MEMORY sono tag che possono essere scritti da Modbus RTU / Modbus TCP-IP o dalle Regole logiche e sono TAG che rappresentano variabili locali. Questo tipo di tag può essere utilizzato anche per i tag calcolati.

EMBEDDED
per I / O digitali integrati presenti a bordo nel dispositivo

Gain
Questo campo corrisponde al valore del coefficiente m nella formula
m * val + q
applicata al valore “val” letto dal dispositivo

Offset
Questo campo corrisponde al valore del coefficiente q nella formula
m * val + q
applicata al valore “val” letto dal dispositivo

Initial Value
Valore di partenza del tag

Error Mode
Questo campo definisce quale valore viene fornito nella risposta a una richiesta Modbus (lettura), quando il valore dal dispositivo di destinazione non è disponibile.
Le modalità possibili sono:

LAST VALUE: viene dato l'ultimo valore disponibile

ERROR VALUE: viene fornito il valore specificato nel campo " ERROR VALUE "

Error Value
Questo campo definisce quale valore viene dato nella risposta a una richiesta Modbus (lettura), quando il valore dal dispositivo di destinazione non è disponibile e il campo " ERROR MODE " è impostato su " ERROR VALUE"

HTTP POST VID
Questo campo viene utilizzato per creare il “Variable ID” (VID) che identifica il tag nelle richieste POST HTTP (utile solo quando il protocollo HTTP POST è abilitato).
La stringa VID è data dal carattere "V" più il numero contenuto nel campo

Read Only

Se selezionato, il tag può essere scritto solo da un protocollo esterno (ad esempio Modbus RTU o TCP-IP) e non da una regola logica.

Retain
Se selezionato, il tag viene salvato in una memoria ritentiva scrivibile infinite volte (feRAM), quando si riavvia il dispositivo l'ultimo valore viene caricato dalla memoria.
Questa opzione è disponibile solo per i tag SHARED MEMORY.

Calculated Function
Attivo solo se la modalità Tag è "Shared Memory". Può essere utilizzato per calcolare il valore MIN / MAX / AVG di un tag.
Si noti che il calcolo è abilitato solo se il datalogger è abilitato. Il tempo di calcolo delle medie è dato dal tempo di acquisizione.

Export to Display/PLC
Se attivo permette di visualizzare il tag sul display o display virtuale (a seconda se il dispositivo è provvisto o meno di display) e sul PLC Straton.

Alarm Enabled
Questo campo è un flag di sola lettura che indica se è stato definito un allarme per il tag.

8.23. PAGINA TAG VIEW (Shared Memory Tag Conf.)

In questa pagina sono visualizzati i valori in tempo reale dei tag configurati.

I pulsanti “Data Logger” possono essere usati per:
- avviare la funzionalità Data Logger, se è stata arrestato (START);
- interrompere la funzionalità Data Logger, se in esecuzione (STOP);
- pulire la cache interna del Data Logger (anche questo fermerà il Data Logger) (CLEAN CACHE).

La visualizzazione viene aggiornata automaticamente.

La colonna “ALARM” riporta lo stato dell'allarme definito per il tag, se presente; la colonna ANALOG DANGER ALARM” ha un comportamento simile, ma è significativa solo per i tag analogici quando, nella configurazione dell'allarme, vengono definite le soglie “Alarm Low Low Value” e “Alarm High High Value”.
È anche possibile esportare i file del datalogger su una chiavetta USB attraverso la pressione del pulsante “COPY TO USB”.
Se il TAG è scrivibile l’ultima colonna include anche un pulsante che può essere usato per scrivere un valore sul tag selezionato.

8.24. PAGINA CUSTOM DEVICE DB (Shared Memory Tag Conf.)

In questa pagina è possibile gestire il database dei registri dei dispositivi esterni a cui connettersi.

8.25. PAGINA ALARM CONFIGURATION (Alarms)

In questa pagina viene visualizzato l'elenco degli allarmi configurati.
Facendo clic sul pulsante "ADD", è possibile configurare un nuovo allarme.

Enabled
Flag per abilitare / disabilitare un allarme

Type
Questo parametro indica se si tratta di un allarme digitale o analogico; quando si modifica il tipo, alcuni parametri vengono abilitati o disabilitati

Name
Il nome dell'allarme; poiché questo parametro viene utilizzato come chiave per identificare l'allarme, non è possibile configurare due allarmi con lo stesso nome

Tag
Il tag a cui è collegato l'allarme.
L'elenco dei tag cambia in base al tipo di allarme (digitale o analogico).
È possibile associare un solo allarme a un tag

Activation Delays
Questo parametro definisce l'intervallo di tempo, in secondi, durante il quale la condizione di allarme deve essere mantenuta vera per generare l'allarme

Ignore on Boot
Questo è un flag utilizzato per evitare di generare l'allarme, se la condizione di allarme viene rilevata durante l'avvio del sistema

Auto Acknowledge
Questo è un flag utilizzato per evitare la necessità di un riconoscimento (ACK) da parte dell'utente per consentire la cancellazione dell'allarme quando questo cessa.

Boolean Alarm Value
Per un allarme digitale, questo parametro indica quale è il valore del tag (LOW o HIGH) che corrisponde alla condizione di allarme

Alarm Low Value
Per un allarme analogico, questo parametro definisce la soglia di allarme bassa cioè se il valore del tag scende al di sotto di questa soglia, viene attivata la condizione di allarme

Alarm High Value
Per un allarme analogico, questo parametro definisce la soglia di allarme alta cioè se il valore del tag supera questa soglia, viene attivata la condizione di allarme

Alarm Low Low Value
Per un allarme analogico, questo parametro definisce la soglia di allarme pericoloso basso cioè se il valore del tag scende al di sotto di questa soglia, viene attivata la condizione di allarme

Alarm High High Value
Per un allarme analogico, questo parametro definisce la soglia di allarme pericoloso alto cioè se il valore del tag supera questa soglia, viene attivata la condizione di allarme

Deadband Value
Questo parametro definisce una fascia entro la quale l'allarme non rientra (isteresi).

I possibili stati di allarme sono spiegati nella seguente tabella:

Stato	Livello	Significato
None	-	Il tag non è mai entrato nella condizione di allarme
Alarm	Alarm	Il valore del digitale ha raggiunto il valore definito dal parametro "Boolean Alarm Level"
Alarm Low	Alarm	Il tag analogico è sceso sotto il valore definito dal parametro "Alarm Low Value"
Alarm High	Alarm	Il tag analogico ha superato il valore definito dal parametro "Alarm High Value"
Alarm Low Low	Analog Danger Alarm	Il tag analogico è sceso sotto il valore definito dal parametro "Alarm Low Low Value"
Alarm High High	Analog Danger Alarm	Il tag analogico ha superato il valore definito dal parametro "Alarm High High Value"
Acknowledge	-	L'allarme ha ricevuto l'ACK da parte dell'utente (o era configurato con Auto Acknowledge)
Return	-	Il tag è uscito dalla condizione di allarme, ma l'allarme non è stato riconosciuto e l'allarme ha il parametro "Auto Acknowledge" impostato su OFF
End	-	Il tag è uscito dalla condizione di allarme e l'allarme è stato riconosciuto oppure l'allarme ha il parametro "Auto Acknowledge" impostato su ON

Come già menzionato, quando si esce dalla condizione di allarme gli stati di allarme possono seguire due percorsi diversi, a seconda del valore del parametro " Auto Acknowledge":

- Alarm* → Return → <ACK> → End se "Auto Acknowledge"=OFF
- Alarm* → End se "Auto Acknowledge"=ON

8.26. PAGINA ALARM SUMMARY (Alarms)

Questa pagina mostra gli allarmi attualmente attivi nel sistema.

Name
Nome dell'allarme

Tag Name
Tag collegato all'allarme

Level
Livello di "pericolosità" dell'allarme:
Vale "Alarm" per gli allarmi digitali
Può valere "Alarm" o "Analog Danger Alarm" per allarmi analogici

Status On
Stato dell'allarme quando è scattato

Timestamp On
Data Ora di quando è scattato l'allarme

Status Action
"None" quando l'allarme scatta
Può evolvere in:
"Acknowledged", Se l'allarme è stato confermato
"Return",se l'allarme è rientrato ma l'impostazione di "Auto Acknowledge" è OFF

Timestamp Action
Data Ora dell'azione (campo precedente)

8.27. PAGINA ALARM HISTORY (Alarms)

Questa pagina mostra tutte le transizioni di stato degli allarmi avvenute nel sistema, fino ad un massimo di 1000; le transizioni dello stato degli allarmi sono indicate dalla più recente alla più vecchia.

8.28. PAGINA SD/USB TRANSFER CONFIGURATION (CLIENT PROTOCOLS)

Questa pagina contiene i parametri che indicano se i file di log vengono copiati su una chiavetta USB (nei modelli sprovvisti di slot per micro SD card) o su micro SD card e per quanto tempo vengono conservati.

Enable
Abilita o no la copia dei log su USB

Max Failure Counter

Questo parametro definisce il numero massimo di tentativi di copia non riusciti prima di entrare nello stato “Wait after failure” (vedi campo successivo)

Wait After Failure (minutes)
Questo parametro definisce la durata, in minuti, dello stato " Wait after failure".
In questo stato, non viene eseguito alcun ulteriore tentativo di copiare un file di log sulla USB

Clean Period (days)
Questo parametro definisce per quanti giorni i file di log devono essere conservati sulla USB; ovvero, dopo il numero di giorni specificato, i file di log vengono eliminati.

I file sono salvati in cartelle secondo la seguente convenzione:

yyyymmdd (yyyy=anno, mm=mese, dd=giorno)

esempio:

20180612

Ciascuna di queste cartelle includono una sottocartella:

logX X=[1..4], numero del gruppo

Il nome del file di log ha la seguente convenzione:

Lmmmmmmm.csv

dove *mmmmmmm* è il numero di minuti dal [1/1/2000 00:00], corrisponde alla data della prima riga di log
esempio:

L9701690.csv

Le SD card e le chiavette USB devono essere formattate con il filesystem FAT32.

ATTENZIONE!

LE CHIAVETTE USB O LE SD CARD SONO SPESSO FORMATTATE CON IL FILESYSTEM “EXFAT” (IN BASE ALLA DIMENSIONE) E VANNO QUINDI RIFORMATTATE CON IL FILESYSTEM “FAT32”

8.29. PAGINA FTP CONFIGURATION (CLIENT PROTOCOLS)

Questa pagina contiene i parametri relativi al trasferimento di file di log verso un FTP server remoto.

Enable
Abilita o no il trasferimento dei log via FTP

Max Failure Counter
Questo parametro definisce il numero massimo di tentativi di copia non riusciti prima di entrare nello stato “Wait after failure” (vedi campo successivo)

Wait After Failure
Questo parametro definisce la durata, in minuti, dello stato " Wait after failure".
In questo stato, non viene eseguito alcun ulteriore tentativo di copiare un file di registro sulla USB

Crypto Mode
Definisce che crittografia utilizzare per la connessione FTP tra:
- None
- TLS/SSL Implicit
- TLS/SSL Explicit

Host
Hostname (FQDN) o indirizzo IP del server FTP

Port
Porta TCP del server FTP

Username
Username del server

Password
Password del server

Path
Percorso della directory, sul server FTP, dove verranno salvati i file di log. Deve iniziare con il carattere “/”.

I file di log trasferiti via FTP avranno il seguente formato:
<*RTU_Name*>_X_log<*date_time*>.csv
Dove:
- <*RTU_Name*> è il valore del campo “RTU Name” nella pagina “General Settings”
- *X=[1..4]* è il numero del gruppo
- <*date_time*> ha il formato *yyyymmdd* (yyyy=anno, mm=mese, dd=giorno); corrisponde alla data del prima riga di log

Esempio:

SENECA_1_log20180507101507.csv

8.30. PAGINA EMAIL CONFIGURATION (CLIENT PROTOCOLS)

Le e-mail possono essere utilizzate per trasferire file di log o per inviare allarmi; alcuni parametri in questa pagina vengono utilizzati solo durante il trasferimento di file di log, non durante l'invio di allarmi;
questi parametri sono contrassegnati con la didascalia "Data Logger Only".

Enable
Flag che indica se i file di log vengono trasferiti tramite EMAIL o meno
Si noti che è possibile inviare allarmi via EMAIL anche se questo parametro è impostato su OFF

Max Failure Counter
Questo parametro definisce il numero massimo di fallimenti prima di entrare nello stato “Wait after failure” (vedi campo successivo)

Wait After Failure (minutes)
Questo parametro definisce la durata, in minuti, dello stato di “Wait after failure”.
In questo stato, non viene eseguito alcun ulteriore tentativo di inviare un file di log o un allarme tramite EMAIL

Crypto Mode
Questo parametro definisce il tipo di crittografia della connessione EMAIL.
Le modalità possibili sono:
None
TLS/SSL
STARTTLS

Host
Hostname (FQDN) o IP address del MAIL server

Port
Porta dell’EMAIL server (TCP)

Username
Username dell’ EMAIL server

Password
Password dell’ EMAIL server

From
Indirizzo Email del mittente

To
Elenco di uno o più indirizzi di destinatari e-mail, separati da virgole.

Questo parametro viene utilizzato solo per il trasferimento dei file di log

Subject
Oggetto della mail.
Questo parametro viene utilizzato solo per il trasferimento dei file di log

Text
Testo della Email: Se lasciato vuoto viene aggiunto un testo standard.
Questo parametro viene utilizzato solo per il trasferimento dei file di log

Line Terminator
Tipo di terminatore della riga da utilizzare

I file di log inviati come allegati EMAIL hanno nomi con il seguente formato:
<RTU_Name> _X_log <date_time> .csv
dove:
- <RTU_Name> è il valore del parametro "RTU Name" nella pagina "General Settings"
- X = [1..4] è il numero del gruppo
- <date_time> ha il formato aaaammgg (aaaa = anno, mm = mese, gg = giorno); questo è il timestamp del primo campione (riga) nel file di log

per esempio.:
SENECA_1_log20180507101507.csv

Le email che contengono allarmi hanno il seguente formato di testo:
MESSAGGIO: <timestamp>
<nome rtu> <testo messaggio>

con il seguente oggetto:
<nome rtu>: ALARM

L'invio dei messaggi di allarme è gestito dalla sezione "Rule Management".

8.31. HTTP CONFIGURATION (CLIENT PROTOCOLS)

Il protocollo http post può essere utilizzato per inviare campioni di log o allarmi (eventi) verso un server HTTP.

Enable
Abilita o no l'invio dei log via http

Max Failure Counter

Questo parametro definisce il numero massimo di fallimenti prima di entrare nello stato “Wait after failure” (vedi campo successivo)

Wait After Failure (minutes)
Questo parametro definisce la durata, in minuti, dello stato di “Wait after failure”.
In questo stato, non viene eseguito alcun ulteriore tentativo di inviare un file di log o un allarme tramite http POST.

SSL/TLS
Questo parametro definisce se attivare o no la crittografia della connessione http.

Host
Hostname (FQDN) o IP address del server HTTP

Port
Porta TCP del server HTTP

Seneca Protocol
Se abilitato permette l'invio HTTP con i parametri tipici del protocollo Seneca (utilizzato su Cloud Box)

Authentication
Permette di abilitare o no l'autenticazione con user/password

Username
Username del server HTTP

Password
Password del server HTTP

Path
Aggiunge una stringa APTH

Url
Permette di visualizzare la stringa di pubblicazione

È anche possibile fare riferimento al documento specifico del protocollo http utilizzato.

8.32. MQTT CONFIGURATION (CLIENT PROTOCOLS)

Il protocollo MQTT può essere utilizzato per inviare (e ricevere) dati o eventi ad un server cloud (chiamato broker).

Enable
Abilita o no il protocollo MQTT.

Max Failure Counter
Questo parametro definisce il numero massimo di fallimenti prima di entrare nello stato “Wait after failure” (vedi campo successivo).

Wait After Failure (minutes)
Questo parametro definisce la durata, in minuti, dello stato di “Wait after failure”.
In questo stato, non viene eseguito alcun ulteriore tentativo di inviare o ricevere dati tramite MQTT.

Client ID
Definisce il Client ID usato nel protocollo MQTT

Broker Host
Definisce l’host name del broker MQTT

Broker Port
Definisce la porta del broker MQTT

Use WebSockets
Permette di attivare la comunicazione MQTT tramite Websockets

Keep Alive Interval (seconds)
Questo parametro definisce il Keep alive il quale assicura che la connessione tra il broker e il client sia ancora aperta e che il broker e il client siano consapevoli di essere connessi. Quando il client stabilisce una connessione al broker, comunica al broker un intervallo di tempo in secondi. Questo intervallo definisce il periodo di tempo massimo durante il quale il broker e il client possono non comunicare tra loro

Clean Session
Questo parametro definisce la “clean session”.
Quando il flag di clean session è impostato su true, il client non desidera una sessione persistente. Se il client si disconnette per qualsiasi motivo, tutte le informazioni e i messaggi accodati da una precedente sessione vengono persi.

Message Retain
Normalmente se un publisher pubblica un messaggio su un topic a cui nessuno è sottoscritto, il messaggio viene semplicemente scartato dal broker. Tuttavia il publisher può dire al broker di conservare l'ultimo messaggio di quel topic

Quality of service
Questo parametro definisce il QOS del protocollo MQTT.
Può essere selezionato tra
QOS 0 (solo una volta, senza ack)
QOS 1 (almeno una volta, con ack)

QOS 2 (solo una volta, con ack e rinvio)

Authentication
Questo parametro definisce se deve essere utilizzata l'autenticazione con utente / password per l'accesso al broker

Username
Username del broker

Password
Password del broker

SSL/TLS
Definisce se il crypto è SSL/TLS

Log on Change
Questo parametro definisce se i topic devono essere inviati solo in caso di modifica (in base al tempo minimo) o meno.

Publish with multiple tags
Questo parametro definisce se la publish contiene più tag o se il dispositivo deve inviare una publish per ciascun tag

Publish Topic for Logs
Seleziona il nome del topic per i log utilizzando la seguente tabella:

%c	Device Client ID
%m	Device MAC Address
%M	Device MAC Address (without ':')
%e	Device IMEI
%d	Data/ora
%t	timestamp (numero di secondi dal 01/01/1970)
%x	testo (solo per "Publish Payload for Alarms")
%b	bulk (formato specificato in "Publish Bulk Format")
%n	Nome del tag (solo per "Publish Bulk Format")
%v	Valore del tag (solo in "Publish Bulk Format")
%i	Flag di validità del tag (solo in "Publish Bulk Format")
%f	Tag id con numero progressivo (solo in "Publish Bulk Format")
%j[field]	Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON
%tag_name	Valore del tag "tag_name"
%#tag_name#	Validità del tag "tag_name"

%u	Timestamp in [ms] (solo in "Publish Fast Log Sample" e "Publish Bulk Format")
%p	Periodo di campionamento (solo in "Publish Fast Log Sample")
%w	Formato (solo in “Publish Fast Log Sample”)

Publish Payload for Logs

Seleziona il formato che deve essere utilizzato per il payload in formato Json utilizzando la seguente tabella:

%c	Device Client ID
%m	Device MAC Address
%M	Device MAC Address (without ':')
%e	Device IMEI
%d	Data/ora
%t	timestamp (numero di secondi dal 01/01/1970)
%x	testo (solo per "Publish Payload for Alarms")
%b	bulk (formato specificato in "Publish Bulk Format")
%n	Nome del tag (solo per "Publish Bulk Format")
%v	Valore del tag (solo in "Publish Bulk Format")
%i	Flag di validità del tag (solo in "Publish Bulk Format")
%f	Tag id con numero progressivo (solo in "Publish Bulk Format")
%j[field]	Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON
%tag_name	Valore del tag "tag_name"
%#tag_name#	Validità del tag "tag_name"
%u	Timestamp in [ms] (solo in "Publish Fast Log Sample" e "Publish Bulk Format")
%p	Periodo di campionamento (solo in "Publish Fast Log Sample")
%w	Formato (solo in “Publish Fast Log Sample”)

Publish Bulk Format

Seleziona il formato per il “bulk mode” secondo la seguente tabella:

%c	Device Client ID
%m	Device MAC Address
%M	Device MAC Address (without ':')
%e	Device IMEI

%d	Data/ora
%t	timestamp (numero di secondi dal 01/01/1970)
%x	testo (solo per "Publish Payload for Alarms")
%b	bulk (formato specificato in "Publish Bulk Format")
%n	Nome del tag (solo per "Publish Bulk Format")
%v	Valore del tag (solo in "Publish Bulk Format")
%i	Flag di validità del tag (solo in "Publish Bulk Format")
%f	Tag id con numero progressivo (solo in "Publish Bulk Format")
%j[field]	Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON
%tag_name	Valore del tag "tag_name"
%#tag_name#	Validità del tag "tag_name"
%u	Timestamp in [ms] (solo in "Publish Fast Log Sample" e "Publish Bulk Format")
%p	Periodo di campionamento (solo in "Publish Fast Log Sample")
%w	Formato (solo in “Publish Fast Log Sample”)

Publish Bulk Format for Fast Logging

Seleziona il formato per il “bulk mode” relativo ai dati del fast logging secondo la seguente tabella:

%c	Device Client ID
%m	Device MAC Address
%M	Device MAC Address (without ':')
%e	Device IMEI
%d	Data/ora
%t	timestamp (numero di secondi dal 01/01/1970)
%x	testo (solo per "Publish Payload for Alarms")
%b	bulk (formato specificato in "Publish Bulk Format")
%n	Nome del tag (solo per "Publish Bulk Format")
%v	Valore del tag (solo in "Publish Bulk Format")
%i	Flag di validità del tag (solo in "Publish Bulk Format")
%f	Tag id con numero progressivo (solo in "Publish Bulk Format")
%j[field]	Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON
%tag_name	Valore del tag "tag_name"

%#tag_name#	Validità del tag "tag_name"
%u	Timestamp in [ms] (solo in "Publish Fast Log Sample" e "Publish Bulk Format")
%p	Periodo di campionamento (solo in "Publish Fast Log Sample")
%w	Formato (solo in “Publish Fast Log Sample”)

Publish Topic for Alarms

Seleziona il formato per i nomi dei topic negli allarmi secondo la seguente tabella:

%c	Device Client ID
%m	Device MAC Address
%M	Device MAC Address (without ':')
%e	Device IMEI
%d	Data/ora
%t	timestamp (numero di secondi dal 01/01/1970)
%x	testo (solo per "Publish Payload for Alarms")
%b	bulk (formato specificato in "Publish Bulk Format")
%n	Nome del tag (solo per "Publish Bulk Format")
%v	Valore del tag (solo in "Publish Bulk Format")
%i	Flag di validità del tag (solo in "Publish Bulk Format")
%f	Tag id con numero progressivo (solo in "Publish Bulk Format")
%j[field]	Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON
%tag_name	Valore del tag "tag_name"
%#tag_name#	Validità del tag "tag_name"
%u	Timestamp in [ms] (solo in "Publish Fast Log Sample" e "Publish Bulk Format")
%p	Periodo di campionamento (solo in "Publish Fast Log Sample")
%w	Formato (solo in “Publish Fast Log Sample”)

Subscribe Topic

Seleziona il Subscribe Topic secondo la seguente tabella:

%c	Device Client ID
%m	Device MAC Address
%M	Device MAC Address (without ':')

%e	Device IMEI
%d	Data/ora
%t	timestamp (numero di secondi dal 01/01/1970)
%x	testo (solo per "Publish Payload for Alarms")
%b	bulk (formato specificato in "Publish Bulk Format")
%n	Nome del tag (solo per "Publish Bulk Format")
%v	Valore del tag (solo in "Publish Bulk Format")
%i	Flag di validità del tag (solo in "Publish Bulk Format")
%f	Tag id con numero progressivo (solo in "Publish Bulk Format")
%j[field]	Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON
%tag_name	Valore del tag "tag_name"
%#tag_name#	Validità del tag "tag_name"
%u	Timestamp in [ms] (solo in "Publish Fast Log Sample" e "Publish Bulk Format")
%p	Periodo di campionamento (solo in "Publish Fast Log Sample")
%w	Formato (solo in “Publish Fast Log Sample”)

LWT Topic

Seleziona il “Last Weel and Testament” topic secondo la seguente tabella:

%c	Device Client ID
%m	Device MAC Address
%M	Device MAC Address (without ':')
%e	Device IMEI
%d	Data/ora
%t	timestamp (numero di secondi dal 01/01/1970)
%x	testo (solo per "Publish Payload for Alarms")
%b	bulk (formato specificato in "Publish Bulk Format")
%n	Nome del tag (solo per "Publish Bulk Format")
%v	Valore del tag (solo in "Publish Bulk Format")
%i	Flag di validità del tag (solo in "Publish Bulk Format")
%f	Tag id con numero progressivo (solo in "Publish Bulk Format")
%j[field]	Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON

%tag_name	Valore del tag "tag_name"
%#tag_name#	Validità del tag "tag_name"
%u	Timestamp in [ms] (solo in "Publish Fast Log Sample" e "Publish Bulk Format")
%p	Periodo di campionamento (solo in "Publish Fast Log Sample")
%w	Formato (solo in “Publish Fast Log Sample”)

LWT Payload
Seleziona il testo del Payload del “Last Weel and Testament”

Save Configuration URL
È la URL per il comando “Save Configuration” ricevuto da mqtt (vedi capitolo di invio dei comandi dal cloud di questo manuale)

Load Configuration URL
È la URL per il comando “Load Configuration” ricevuto da mqtt (vedi capitolo di invio dei comandi dal cloud di questo manuale)

FW Update URL
È la URL per il comando “FW Update” ricevuto da mqtt (vedi capitolo di invio dei comandi dal cloud di questo manuale)

Sleep Timeout
Tempo di risveglio del task MQTT, più è breve, più è reattivo MQTT (a scapito di un carico della CPU più elevato)

MQTT Certificates
È utilizzato per gestire i certificati necessari alla connessione TLS.

8.33. PAGINA PHONEBOOK (LOGIC CONFIGURATION)

Questa pagina è utilizzata per configurare la rubrica per l’invio da parte del dispositivo di messaggi di testo tramite email e/o (nei modelli dotati di modem) di SMS.

User Type
È possibile definire tre diversi profili di account:

Admin
Questo account riceve gli allarmi via SMS o EMAIL da qualunque gruppo.

Questo account può inviare comandi SMS al dispositivo e, inoltre, riceve tutti i comandi SMS rifiutati o non riconosciuti (se il parametro “SMS Relay to Admin” è impostato su ON e tutti i messaggi “Startup SMS” se il parametro “Startup SMS” è impostato su ON).

Manager
Questo account riceve gli allarmi via SMS o EMAIL dal gruppo a cui appartiene.
Questo account può inviare comandi SMS al dispositivo.

User
Questo account riceve gli allarmi via SMS o EMAIL dal gruppo a cui appartiene.

Al momento della compilazione è richiesto il gruppo (o i gruppi) di appartenenza dell’account in questo modo è possibile suddividere gli allarmi di testo tra i vari account.
Si noti come gli account “Admin” ricevano gli allarmi di qualsiasi gruppo.

8.34. PAGINA MESSAGE CONFIGURATION (LOGIC CONFIGURATION)

In questa sezione è possibile definire i messaggi di testo relativi agli allarmi che il dispositivo deve gestire.
Il testo del messaggio può contenere solo caratteri ASCII.
È possibile utilizzare la sintassi {NOME_TAG} per includere nel testo il valore attuale di un tag.

Ad esempio il testo del messaggio:

“LIVELLO ACQUA ={LEVEL} m”

Fornirà un testo con il valore del tag riportato come testo, se il tag “LEVEL” vale 1.232 si avrà:

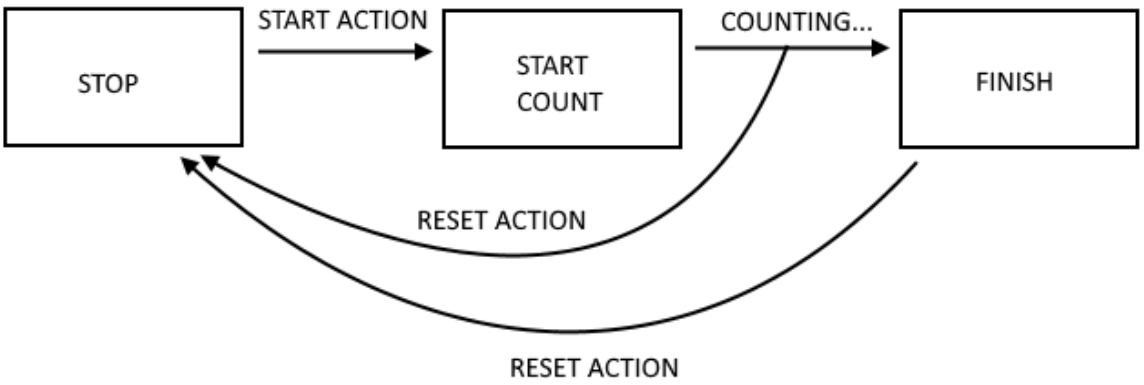
LIVELLO ACQUA = 1.232 m

Questa sintassi può essere utilizzata più di una volta nel testo di un messaggio.
Ogni messaggio ha un campo ID che è usato per associare il messaggio all’allarme nelle regole logiche.

8.35. PAGINA TIMER CONFIGURATION (LOGIC CONFIGURATION)

Questa sezione consente di definire fino a 100 timer da utilizzare nelle regole logiche.
L'ID rappresenta il mnemonico del timer che deve essere utilizzato nelle regole.
“Enable” seleziona se il timer è attivo o meno.
“Duration” è il valore di attivazione in [ms].

Nota
I timer per impostazione predefinita sono in modalità di stop, necessitano di un'azione per l'avvio e di un'azione per il ripristino, secondo lo schema seguente:



8.36. PAGINA RULE SCRIPTS (LOGIC CONFIGURATION)

In questa pagina è possibile caricare i file relativi agli script da eseguire come azioni delle regole logiche.
Deve essere rispettata l'estensione per il tipo di script da utilizzare:

Tipo di script	*Estensione*
Linux Shell	".sh"
PHP	".php"
Python	".py"
Binary	".bin"

E' possibile caricare al massimo un file da 100 Kbyte.

8.37. PAGINA RULE MANAGEMENT (LOGIC CONFIGURATION)

In questa sezione è possibile definire un insieme di regole logiche che realizzeranno un programma.
Per configurare una regola, sono disponibili i seguenti parametri:

8.37.1. RULE CONFIGURATION

Enabled
Indica se la regola è abilitato oppure se deve essere esclusa dall'esecuzione

Index
Ordine di esecuzione della regola (1 = Prima regola ad essere eseguita)

Description
Descrizione testuale mnemonica della regola

Period [ms]
Se il valore è = 0, le azioni vengono eseguite solo se c'è una modifica nel risultato dell' "OR / AND" (cioè su cambio di stato).

Se il valore è diverso da 0 ms le azioni vengono eseguite cercando di rispettare la tempistica inserita.

ATTENZIONE!

Utilizzare valori di periodo adeguati per le azioni di invio di EMAIL / SMS / http / MQTT !

NOTA:
Se Period è > 0 le azioni vengono sempre eseguite in modalità “repeat”

8.37.2.IF CONDITION: TYPE

Questa sezione definisce il tipo di condizione, sono possibili i seguenti tipi:

None
Nessuna condizione da valutare

Alarm State
La condizione fa riferimento allo stato di un allarme, sono possibili i seguenti parametri:

Campo	***Significato***
Alarm Name	Seleziona l'allarme dall'elenco di tutti gli allarmi configurati
Alarm State	Stato dell’allarme. Possibili stati sono: None Alarm (digital only) Alarm Low Low (analog only) Alarm Low (analog only) Alarm High (analog only) Alarm High High (analog only) Acknowledge Return End A seconda del tipo (digitale o analogico) dell'allarme selezionato, alcuni stati sono disabilitati
Analog Danger Alarm	Flag che indica se il livello di allarme deve essere “Analog Danger” o meno, vale solo per gli allarmi su tag analogici

Alarm Active

La condizione di allarme fa riferimento allo stato Attivo o No di un allarme, sono possibili i seguenti parametri:

Campo	*Significato*
Alarm Name	Seleziona l'allarme dall'elenco di tutti gli allarmi configurati
Alarm Active	Indica se l'allarme deve o no essere attivo. L'allarme è attivo se si trova in uno di questi stati: Alarm (solo per tag digitali) Alarm Low Low (solo per tag analogici) Alarm Low (solo per tag analogici) Alarm High (solo per tag analogici) Alarm High High (solo per tag analogici) Acknowledge L'allarme non è attivo se è in uno dei seguenti stati: None Return End
Analog Danger Alarm	Flag che indica se il livello di allarme deve essere "Analog Danger" o meno, significativo solo per gli allarmi analogici.

Always

La condizione If è sempre vera.

Nota che la regola viene eseguita solo una volta se Period è = 0 ms o se le azioni sono in modalità "one time mode".

Se è necessario eseguire una regola ad ogni ciclo, è necessario mettere le azioni in "repeat mode".

Se è necessario eseguire una regola a tempo (ogni x ms), è necessario impostare Period > 0ms.

Digital Tag

La condizione dipende dallo stato di un tag digitale:

Campo	*Significato*
Tag	Seleziona il tag che deve essere utilizzato per la condizione
Operator	Può valere solo "="
Tag / Constant value	Seleziona se il confronto è tra un altro tag digitale o un valore booleano costante (TRUE o FALSE)

Analog Tag

La condizione dipende da un confronto con un TAG analogico

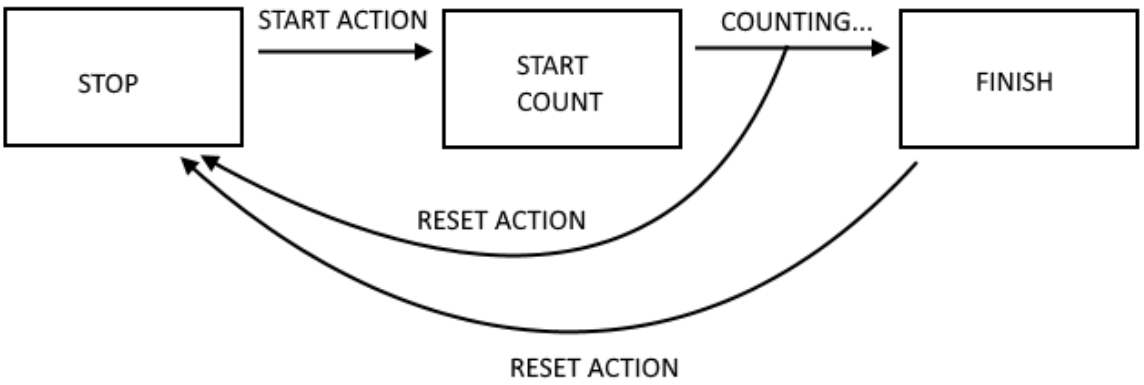
Campo	*Significato*
Tag	Seleziona il tag che deve essere utilizzato per la condizione
Operator	Può valere: “=” “>” “<” “>=” “<=”
Tag / Constant value	Seleziona se il confronto è tra un altro tag analogico o un valore costante

Timer

La condizione dipende dallo stato del timer selezionato

Campo	*Significato*
ID	Selezionare l'ID del timer da utilizzare
Expired	Può essere: "OFF" o "ON" Con “ON” la condizione è vera solo allo scadere del timer (stato FINISH). Con “OFF” la condizione è vera fino a quando il timer non è in STOP o COUNTING. Quando il timer è nello stato FINISH la condizione diventa falsa.

Il funzionamento del Timer è rappresentato nello schema seguente:



Scheduler

La condizione dipende dallo scheduler (calendario) impostato:

Campo	***Significato***
Type	Può valere: Daily, Weekly Monthly Daily: la condizione è vera ogni giorno all'ora e minuti configurati Weekly: la condizione è vera il giorno della settimana selezionato alle ore e minuti selezionati Monthly: la condizione è vera il giorno del mese selezionato alle ore e minuti selezionati
Day	Se il tipo è Weekly stabilisce il giorno della settimana: 0 = Domenica 1 = Lunedì 2 = Martedì 3 = Mercoledì 4 = Giovedì 5 = Venerdì 6 = Sabato Se il tipo è Monthly: Seleziona il giorno del mese da 1 a 31
Hour	Ore
Minute	Minuti

Rule Status

La condizione dipende dall'abilitazione o no di una regola:

Campo	*Significato*
ID	Selezina l'ID della regola
Enabled	Seleziona tra "enabled" o "disabled" Se "Enabled" la condizione è VERA se la regola selezionata è abilitata. Se "Disabilitato" la condizione è VERA se la regola selezionata è disabilitata.

Bitmask

La condizione dipende dalla mascheratura di un tag con una costante esadecimale:

Campo	*Significato*
Tag	Seleziona il tag a cui applicare la maschera di bit da un elenco contenente tutti i tag con tipo di dato "16Bit Unsigned"
Mask	La maschera di bit rappresentata come una stringa di 4 cifre esadecimali

La condizione di mascheratura "Bitmask" è VERA se l'operazione AND bit per bit tra il Tag e la Maschera dati è diversa da 0; FALSO altrimenti.

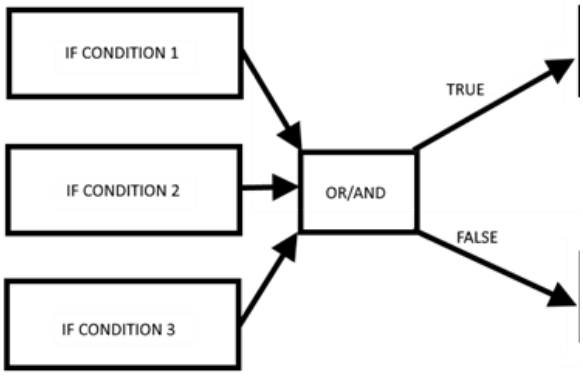
Esempio:
Tag=0x1233 (esadecimale) = 0b 0001 0010 0011 0011 (binario)
Mask=0x8001 (esadecimale) = 0b 1000 0000 0000 0001 (binario)
Significa che la maschera analizza il bit0 (meno significativo)e il bit 15 (più significativo) del Tag.
L' AND bit a bit fornisce:

0001 0010 0011 0011
1000 0000 0000 0001

0000 0000 0000 0001
Per cui la condizione è VERA.

8.37.3.IF CONDITION OPERATOR

Le "condizioni IF" possono essere combinate insieme in logica "OR" o "AND", in pratica:



Le “condizioni IF” legate assieme da “OR” assumono lo stato TRUE se almeno una delle condizioni è vera.
Le “condizioni IF” legate assieme da “AND” assumono lo stato TRUE solo se tutte sono vere.

Più in dettaglio seguono la seguente tabella:

IF CONDITION 1	*IF CONDITION 2*	*IF CONDITION 3*	*“OR”*	*“AND”*
FALSE	FALSE	FALSE	FALSE	FALSE
FALSE	FALSE	TRUE	TRUE	FALSE
FALSE	TRUE	FALSE	TRUE	FALSE
FALSE	TRUE	TRUE	TRUE	FALSE
TRUE	FALSE	FALSE	TRUE	FALSE
TRUE	FALSE	TRUE	TRUE	FALSE
TRUE	TRUE	FALSE	TRUE	FALSE
TRUE	TRUE	TRUE	TRUE	TRUE

8.37.4.THEN/ELSE ACTION

In questa sezione è possibile definire l'azione che deve essere eseguita nel caso le condizioni diano come risultato TRUE (azione THEN) o FALSE (azione ELSE).

NONE
Nessuna azione da eseguire

Send Alarm SMS
Send Alarm EMAIL
Send Alarm HTTP POST
Send Alarm MQTT
Permettono di inviare un messaggio di testo (definito nella sezione messaggi) attraverso i protocolli client disponibili

Campo	***Significato***
Message	Seleziona il messaggio di testo da inviare tra quelli configurati
Group	Seleziona il gruppo di invio (solo per SMS ed EMAIL)

Digital Tag
Esegue una scrittura su un Tag di tipo digitale.

Campo	***Significato***
Action Mode	Permette di selezionare tra "One Time" o "Repeat". Con "One Time" l'azione viene eseguita solo se c'è un cambiamento nel risultato delle condizioni OR / AND. Con "Repeat" l'azione viene eseguite ad ogni loop (se la regola è abilitata e se non c'è un periodo configurato).
Destination Tag	È il tag in cui viene copiato il risultato TRUE/FALSE calcolato
Operator	È l'operatore booleano da utilizzare, selezionato tra =, NOT, OR ecc ...
Source Tag 1 / Constant value 1	Seleziona il primo tag da utilizzare nel calcolo boolano. È possibile anche usare una costante booleana
Source Tag 2 / Constant value 2	Selezionare il secondo Tag se l'operatore necessita di 2 input (Ad esempio operatore "OR"). È anche possibile utilizzare una costante booleana

Analog Tag
Esegue una scrittura su un Tag di tipo analogico.

Campo	***Significato***

Action Mode	Selezionare tra “One Time” o “Repeat”. Con “One Time” l’azione viene eseguita solo se c'è un cambiamento nel risultato delle condizioni OR / AND. Con “Repeat” l’azione viene eseguita ad ogni loop (se la regola è abilitata e se non c'è un periodo configurato).
Destination Tag	È il tag in cui viene copiato il risultato calcolato
Operator	È l'operatore matematico da utilizzare, è possibile selezionare tra: "=" copia il tag di origine 1 oppure il valore costante 1 nel tag di destinazione Esempio: Tag di destinazione = Tag di origine 1 Oppure Tag di destinazione = valore costante 1 "+ =" Somma al tag di destinazione il valore del tag di origine1 oppure il valore costante 1 e copia il risultato nel tag di destinazione. Esempio: Tag di destinazione = Tag di destinazione + Tag di origine 1 "- =" Sottrae al tag di destinazione il valore del tag di origine1 e copia il risultato nel tag di destinazione. Esempio: Tag di destinazione = Tag di destinazione - Tag di origine 1 "* =" Moltiplica il tag di destinazione per il valore di tag di origine 1 e copia il risultato nel tag di destinazione. Esempio: Tag di destinazione = Tag di destinazione * Tag di origine 1 "/ =" Divide il tag di destinazione con il valore di tag di origine 1 e copia il risultato nel tag di destinazione. Esempio: Tag di destinazione = Tag di destinazione / Tag di origine 1

	"% =" Calcola il resto della divisione dal tag di destinazione e il valore del tag di origine1 e copia il risultato nel tag di destinazione. (Notare che 53% 7 = 4) Esempio: Tag di destinazione = Tag di destinazione% Tag di origine1 "abs" Calcola il valore assoluto di Source Tag 1 o Constant value 1 e copia il risultato nel Destination Tag (Notare che abs (-4) = 4) Esempio: Tag di destinazione = abs (Tag sorgente 1) "Sqrt" Calcola il valore della radice quadrata del tag sorgente 1 o valore costante 1 e copia il risultato nel tag di destinazione. (Notare che sqrt (9) = √9 = 3) Esempio: Tag di destinazione = sqrt (tag di origine 1) "Sqr" Calcola il valore quadrato del tag di origine 1 o valore costante 1 e copia il risultato nel tag di destinazione. (Notare che sqr (3) = 3^2 = 9) Esempio: Tag di destinazione = sqr (tag di origine 1) "Log" Calcola il logaritmo decimale del tag sorgente 1 o valore costante 1 e copia il risultato nel tag di destinazione. (Notare che log (3) = 0,4771212) Esempio: Tag di destinazione = log (tag di origine 1) "Ln" Calcola il logaritmo naturale del tag di origine 1 o valore costante 1 e copia il risultato nel tag di destinazione. (Notare che ln (3) = 1.09861228867) Esempio:

	Tag di destinazione = ln (Tag sorgente 1) "Exp" Calcola il numero di Eulero elevato a Source Tag 1 o Constant value 1 e copia il risultato nel Destination Tag. Si noti che: ln (exp 3) = 3 Esempio: Tag di destinazione = scadenza (tag di origine 1) "+" Somma il Source Tag 1 o Constant value 1 Con il valore di Source Tag 2 o Constant value 2 e copia il risultato nel Destination Tag. Esempio: Tag di destinazione = Tag sorgente 1+ Tag sorgente 2 "-" Sottrae il tag sorgente 1 o valore costante 1 con il valore del tag sorgente 2 o valore costante 2 e copia il risultato nel tag di destinazione. Esempio: Tag di destinazione = Tag di origine 1- Tag di origine 2 "*" Moltiplicare il tag di origine 1 o valore costante 1 con il valore di tag di origine 2 o valore costante 2 e copia il risultato nel tag di destinazione. Esempio: Tag di destinazione = Tag sorgente 1 * Tag sorgente 2 "/" Divide il tag di origine 1 o valore costante 1 con il valore di tag di origine 2 o valore costante 2 e copia il risultato nel tag di destinazione. Esempio: Tag di destinazione = Tag sorgente 1 / Tag sorgente 2 "%" Calcola il resto della divisione tra il tag sorgente 1 o valore costante 1 e il valore del tag sorgente 2 o valore costante 2 e copia il risultato nel tag di destinazione. (Notare che 53% 7 = 4) Esempio:

	Tag di destinazione = Tag sorgente 1% Tag sorgente 2 "Pow" Calcola il valore Source Tag1 o Constant 1 elevato alla potenza del Sorce Tag2 / Constant value 2 e copia il risultato nel tag di destinazione. Esempio: Tag di destinazione = (Source Tag1) ^ (Source Tag2)
Source Tag 1 / Constant value 1	Seleziona il tag da utilizzare come ingresso 1 per l'operatore utilizzato. È possibile utilizzare anche usare un valore costante.
Source Tag 2 / Constant value 2	Seleziona il tag da utilizzare come ingresso 2 nel calcolo se l'operatore necessita di 2 ingressi. Puè anche essere utilizzato un valore costante.

Timer

È possibile selezionare l'azione da eseguire nel timer selezionato.

Campo	***Significato***
Id	Seleziona il timer tra quelli configurati
Action	Seleziona il tipo di azione da eseguire nel timer selezionato. "Start" esegue l'azione di avvio del timer selezionato "Reset" esegue l'azione di reset del timer allo stato di stop

Rule Status

L'azione abilita o disabilita una regola.

Campo	***Significato***
Id	Seleziona la regola
Enable	Seleziona se l'azione deve o no abilitare la regola selezionata: "OFF" disabilita la regola selezionata "ON" abilita la regola selezionata

Datalogger

L'azione permette di Far partire o fermare il datalogger, è anche possibile selezionare il gruppo del log da controllare.

Campo	*Significato*
Group	Seleziona il gruppo di datalogger da controllare
Enable	Seleziona se l'azione deve o no abilitare il datalogger "OFF" disabilita il datalogger per il gruppo selezionato "ON" abilita il datalogger per il gruppo selezionato

Network

Sono azioni che permettono di agire sullo stato della VPN (abilitarla oppure disabilitarla) o del modem.

Campo	*Significato*
Feature	Permette di scegliere su quale elemento eseguire l'azione di ON/OFF È possibile scegliere tra: PPP si riferisce alla connessione dati del modem mobile (se presente) VPN si riferisce alla connessione VPN Firewall si riferisce al firewall di sistema OpenVPN si riferisce alla connessione OpenVPN standard
Start	È possibile scegliere l'azione da eseguire tra "ON" e "OFF".

Set Bits

Questa azione permette di portare al valore 1 o al valore 0 un numero configurabile di bit di un determinato tag.

Campo	*Significato*
Action Mode	Seleziona tra "One Time" o "Repeat". Con "One Time" l'azione viene eseguita solo se c'è un cambiamento nel risultato delle condizioni OR / AND. Con "Repeat" l'azione viene eseguite ad ogni loop (se la regola è abilitata e se non c'è un periodo configurato).
Destination Tag	È il tag in cui viene copiato il risultato dell'azione, il tag deve essere di tipo "16 bit unsigned"
Source Tag	Seleziona il tag da utilizzare nel calcolo. È possibile anche inserire il source tag ed il destination tag uguali in modo da eseguire l'azione sullo stesso TAG. Il tag deve essere di tipo "16 bit unsigned"
Mask	È la maschera in formato esadecimale che permette la mascheratura dei bit da controllare.
Action	È possibile scegliere tra "Set" ovvero porta ad 1 i bit, oppure "Reset" ovvero porta a 0 i bit.

Data Logger Trigger

Permette l'acquisizione di un singolo campione nei gruppi configurati come Trigger o Periodic and Trigger. Nel caso di gruppo configurato con fast logging avvia l'acquisizione dei max 1000 campioni.

Campo	*Significato*
Group	Permette di selezionare su quale gruppo di log eseguire l'azione
Source	Si tratta di una etichetta che viene salvata sul datalogger in modo da discriminare la sorgente del trigger. il campo "Source" può assumere i valori da "A" ad "H". Se l'azione "Data Logger Trigger" viene eseguita in più regole, al verificarsi di condizioni differenti, impostando dei valori distinti di "Source" si può discriminare quale condizione ha generato il trigger.

Data Logger Send

L'azione permette la chiusura del file di log predisponendolo per l'invio tramite i protocolli client configurati (vale per i protocolli che funzionano con i file: FTP, EMAIL e SD/USB). È da utilizzare sui gruppi configurati con sample mode "trigger".

Campo	*Significato*
Group	Seleziona su quale/i gruppo eseguire l'azione

Data Logger Trigger Stop (fast logging)

L'azione permette di fermare l'acquisizione impostata con il fast logging prima che l'acquisizione si fermi automaticamente una volta raggiunti i 1000 campioni.
Lo start dell'acquisizione fast logging è dato dall'azione di data logger trigger, nel caso non venga fermato da questa azione il fast logging campiona 1000 valori e poi si ferma automaticamente.

Campo	*Significato*
Group	Seleziona su quale/i gruppo eseguire l'azione

Script Execution

L'azione permette di eseguire uno script definito dall'utente. Per caricare i file degli script nel dispositivo è messa a disposizione la pagina "Rules Scripts".

Campo	*Significato*
Type	Seleziona il tipo di script tra: Linux Shell Permette di eseguire uno script bash. Estensione richiesta al file ".sh" Php

	Permette di eseguire uno script php. Estensione richiesta al file ".php". Il file deve essere conforme alla revisione PHP 7.3.9 Python Permette di eseguire uno script Python. Estensione richiesta al file ".py". Il file deve essere conforme alla revisione Python rev 3.7 Binary program Permette di eseguire un programma eseguibile. Estensione richiesta al file ".bin". Il file deve essere conforme alla versione arm v7 a 32 bit. Negli script è possibile accedere ai Tag tramite una sintassi spiegata nel relativo capitolo del seguente manuale.
File	Permette di selezionare il file relativo allo script tra quelli caricati nel dispositivo.
Asynchronous	Permette di selezionare tra: OFF Lo script viene eseguito in modalità sincrona cioè l'esecuzione delle successive regole è bloccata fino alla fine dell'esecuzione dello script. ON Lo script viene eseguito in modalità asincrona cioè l'esecuzione delle successive regole non viene bloccata dall'esecuzione dello script.

8.38. PAGINA GENERAL SETTINGS (DATALOGGER)

In questa sezione sono presenti i parametri generali del datalogger, in particolare è possibile editare come si presenterà il contenuto dei log.
Il datalogger funziona con i seguenti protocolli:

-Tramite copia su USB/SD card
-Invio EMAIL
-Invio FTP
-Invio http (se attivo è possibile solo il gruppo 1)
-Invio MQTT

RTU Name
È il nome della RTU, compare nel nome del file nei protocolli che inviano file (Mail e FTP).

Transfer Priority
Permette di selezionare se debbano essere inviati prima i log più recedenti o quelli più vecchi.

CSV Separator
Permette di impostare il separatore nel file tipo csv tra ";" "," " ". Viene utilizzato solo nei protocolli che inviano file (Mail e FTP).

Decimal Separator
Permette di selezionare il separatore decimale nei valori tra "," o "."

Floating Point Precision
Permette di selezionare la precisione con cui sono inviati i TAG di tipo floating point tra:
Automatico, Nessuna cifra decimale oppure da 1 a 10 cifre.

Index Column
Permette di aggiungere una colonna INDEX al file con il numero di riga, viene utilizzato solo nei protocolli che inviano file (Mail e FTP).

Type Column
Permette di aggiungere una colonna al file con il campo TYPE. Se il log è di tipo periodic allora comparirà sempre la scritta "LOG", se il log è di tipo periodic and trigger compare la scritta SYNC (nel caso riga dovuta al tempo di campionamento) ASYNC (nel caso di riga di campionamento dovuta ad un trigger). Viene utilizzato solo nei protocolli che inviano file (Mail e FTP).

Trigger Column
Permette di aggiungere una colonna al file con il campo TRIGGER. Se il log è di tipo periodic and trigger viene indicata la fonte che ha generato il trigger A, B, .. (vedi regole logiche). Viene utilizzato solo nei protocolli che inviano file (Mail e FTP).

Timestamp Format
Permette di impostare il formato della data ora nel log. Viene utilizzato solo nei protocolli che inviano file (Mail e FTP). Nel protocollo MQTT è possibile scegliere il formato del timestamp tramite i placeholder %.

Send Data logs via http Post
Se impostato su "ON" attiva automaticamente l'abilitazione sulla pagina http configuration e disabilita tutti i gruppi di log consentendo una eventuale abilitazione manuale solo del primo gruppo.

http Post Tag limitations
Limita ai primi 150 TAG l'invio del post http per non appesantire il server http.

8.39. PAGINA GROUP CONFIGURATION

Qui è possibile selezionare quali dei 4 gruppi di log vanno attivati e il tipo di log da effettuare.
Nel caso non si desideri attivare il datalogger è sufficiente impostare a "disabled" ciascun gruppo.

È possibile attivare le seguenti modalità di datalogger per ciascuno dei 4 gruppi:

Campo	Significato
Sampling Mode	"Disabled" il gruppo è disabilitato. "Periodic" Tutti i tag configurati sono acquisiti con il tempo impostato "Periodic and trigger" Tutti i tag configurati sono acquisiti con il tempo impostato e su azione di trigger. "Trigger" Tutti i tag configurati sono acquisiti su azione di trigger. L'azione di trigger è configurabile nelle regole logiche (quando si avvera una certa serie di condizioni viene eseguita l'azione di trigger e quindi si forza l'acquisizione dei tag).
Sampling Period (s)	Questo parametro definisce il periodo di campionamento, in secondi.
Transfer Period (min)	Questo parametro definisce il periodo di trasferimento, in minuti; cioè ogni intervallo di tempo definito da questo parametro il file di log viene chiuso e trasferito.

Time before overflow fornisce un'indicazione di quanto tempo passerà prima che i dati non inviati saranno sovrascritti.

8.40. PAGINA CLOUD CONFIGURATION

Questa pagina permette di impostare la configurazione MQTT in modo automatico per i vari cloud gestiti dal dispositivo.

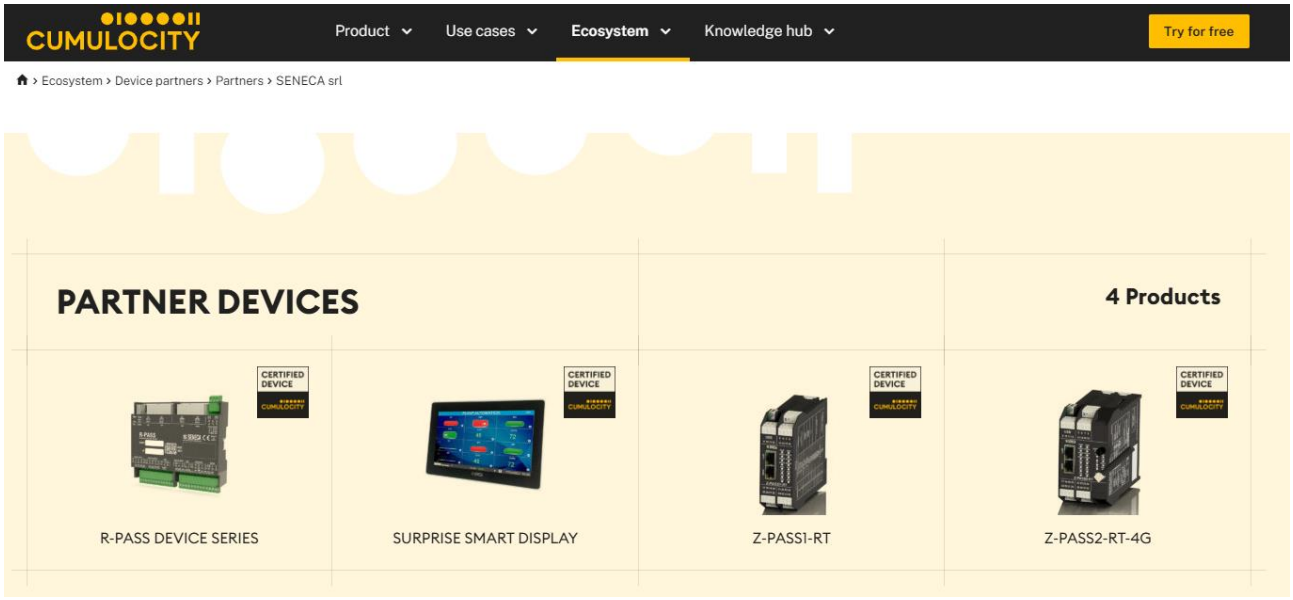
Attualmente è possibile configurare:
Generic: Tramite la configurabilità di MQTT del dispositivo è possibile virtualmente connettersi ad ogni cloud
Cumulocity: Imposta il dispositivo per la connessione con il cloud Cumulocity
Direl ADM: Imposta il dispositivo per la connessione con il cloud Direl ADM
On-Board: Imposta il dispositivo per la connessione con il cloud On-Board

Per aggiungere alla lista altri cloud è possibile formulare una richiesta a Seneca.

8.40.1. CUMULOCITY

Il coud Cumulocity è disponibile all'indirizzo:
https://cumulocity.com/

I dispositivi Seneca hanno superato i test di certificazione cumulocity:



I parametri da configurare sono:

Campo	Significato
Enable	Abilita o no la connessione con il cloud cumulocity
URL	È l'url su cui viene fatta la registrazione al cloud
Tenant ID	È un ID formito dal cloud cumulocity
Username	È la username per l'accesso al cloud
Password	È la password per l'accesso al cloud

8.40.2.DIREL ADM4.0

I parametri per il cloud di Direl (https://www.direl.it/) sono i seguenti:

Campo	Significato
Enable	Abilita o no la connessione con il cloud Direl ADM4.0
Username for Commands	È la username per l'accesso in scrittura dal cloud verso il dispositivo
Password for Commands	È la password per l'accesso in scrittura dal cloud verso il dispositivo

8.40.3.ONBOARD

Onboard è il cloud di innovation system s.r.l., per maggiori informazioni fare riferimento al sito:

https://www.onsystem-iot.com/onboard

I parametri per la connessione sono:

Campo	Significato
Enable	Abilita o no la connessione con il cloud Onboard
Username	È la username per l'accesso al cloud
Password	È la password per l'accesso al cloud

8.41. PROTOCOLLO METER-BUS (M-BUS)

Il protocollo MBUS è disponibile solo se è attivo PLC Straton.

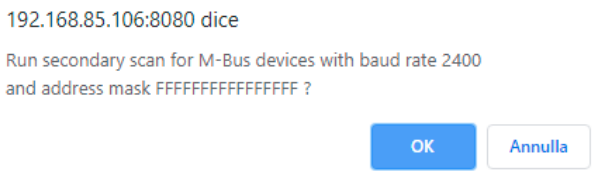
Per collegarsi ad un bus di campo M-Bus è necessario eseguire i seguenti step:
1) collegare l'adattatore opzionale RS232-MBUS Seneca "Z-MBUS" alla porta seriale COM1;
2) impostando la modalità COM1 su M-BUS.

Per gestire i dispositivi M-Bus sono disponibili le seguenti risorse:
- le pagine web della sezione "M-Bus".
- la funzione MBUS_READ_CTL
- il blocco funzione MBUS_WRITE_RAW

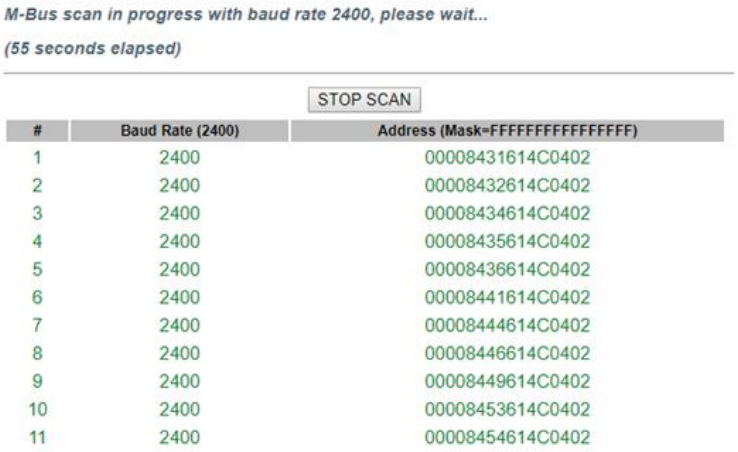
Le pagine web M-BUS consentono di scansionare il bus, ricercare i dispositivi, rilevarne gli indirizzi primari o gli indirizzi secondari; consente inoltre di leggere i record di dati e le informazioni sulle slave da un dispositivo e creare i file di configurazione da importare nel PLC Straton.
L'FB MBUS_READ_CTL permette di avviare/arrestare l'acquisizione M-BUS;
l'FB MBUS_WRITE_RAW consente di costruire e inviare un frame M-Bus generico, fornendo così un modo flessibile per inviare comandi di configurazione ai dispositivi M-Bus.

8.41.1. M-BUS SCAN

Il pulsante “SECONDARY SCAN” permette di scansionare il bus, rilevando gli indirizzi secondari M-Bus; selezionare il baud-rate corretto per la porta seriale COM1 oppure selezionare “ALL” per ripetere la scansione per ogni possibile baud-rate; quindi fare clic sul pulsante; verrà visualizzato un pop-up di conferma.

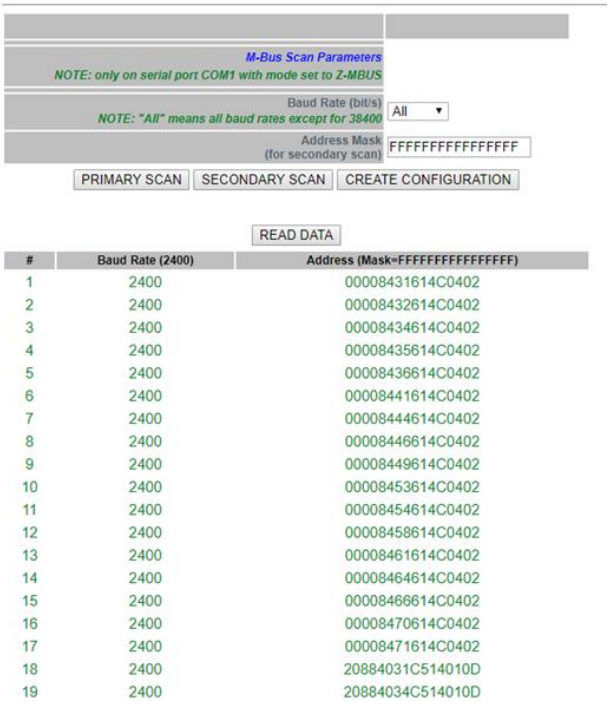


Il completamento della procedura di scansione potrebbe richiedere diversi minuti, quindi la pagina mostra il numero di secondi trascorsi; i dispositivi vengono visualizzati in termini di indirizzo secondario e baud rate non appena vengono rilevati.



#	Baud Rate (2400)	Address (Mask=FFFFFFFFFFFFFFF)
1	2400	00008431614C0402
2	2400	00008432614C0402
3	2400	00008434614C0402
4	2400	00008435614C0402
5	2400	00008436614C0402
6	2400	00008441614C0402
7	2400	00008444614C0402
8	2400	00008446614C0402
9	2400	00008449614C0402
10	2400	00008453614C0402
11	2400	00008454614C0402

Il pulsante “STOP SCAN” consente di annullare la procedura; comunque i risultati parziali vengono mantenuti. Al termine della procedura il webserver indica la fine della scansione e quindi viene visualizzata la seguente pagina:



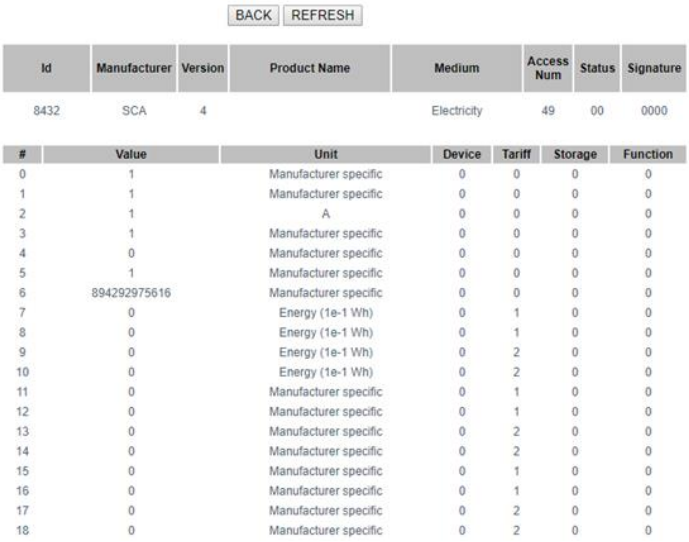
#	Baud Rate (2400)	Address (Mask=FFFFFFFFFFFFFFFF)
1	2400	00008431614C0402
2	2400	00008432614C0402
3	2400	00008434614C0402
4	2400	00008435614C0402
5	2400	00008436614C0402
6	2400	00008441614C0402
7	2400	00008444614C0402
8	2400	00008446614C0402
9	2400	00008449614C0402
10	2400	00008453614C0402
11	2400	00008454614C0402
12	2400	00008458614C0402
13	2400	00008461614C0402
14	2400	00008464614C0402
15	2400	00008466614C0402
16	2400	00008470614C0402
17	2400	00008471614C0402
18	2400	20884031C514010D
19	2400	20884034C514010D

Il valore del baud rate mostrato nell'intestazione della tabella ricorda la scelta del parametro per l'ultima procedura di scansione.

La tabella con i dispositivi M-Bus rilevati viene memorizzata in modo permanente, quindi dopo aver spento e riacceso il dispositivo sono ancora disponibili i risultati dell'ultima scansione; verranno sovrascritti dalla scansione successiva o eliminati da un ripristino delle impostazioni di fabbrica.

Allo stesso modo il pulsante “PRIMARY SCAN” permette di scansionare il bus, rilevando gli indirizzi primari M-Bus; selezionare il baud-rate corretto per la porta seriale COM1 oppure selezionare “All” per ripetere la scansione per ogni possibile baud-rate.

È possibile leggere i dati da uno dei dispositivi, selezionando la riga corrispondente e cliccando sul pulsante “READ DATA”, ad esempio:



Id	Manufacturer	Version	Product Name	Medium	Access Num	Status	Signature
8432	SCA	4		Electricity	49	00	0000

#	Value	Unit	Device	Tariff	Storage	Function
0	1	Manufacturer specific	0	0	0	0
1	1	Manufacturer specific	0	0	0	0
2	1	A	0	0	0	0
3	1	Manufacturer specific	0	0	0	0
4	0	Manufacturer specific	0	0	0	0
5	1	Manufacturer specific	0	0	0	0
6	894292975616	Manufacturer specific	0	0	0	0
7	0	Energy (1e-1 Wh)	0	1	0	0
8	0	Energy (1e-1 Wh)	0	1	0	0
9	0	Energy (1e-1 Wh)	0	2	0	0
10	0	Energy (1e-1 Wh)	0	2	0	0
11	0	Manufacturer specific	0	1	0	0
12	0	Manufacturer specific	0	1	0	0
13	0	Manufacturer specific	0	2	0	0
14	0	Manufacturer specific	0	2	0	0
15	0	Manufacturer specific	0	1	0	0
16	0	Manufacturer specific	0	1	0	0
17	0	Manufacturer specific	0	2	0	0
18	0	Manufacturer specific	0	2	0	0

In questa pagina:

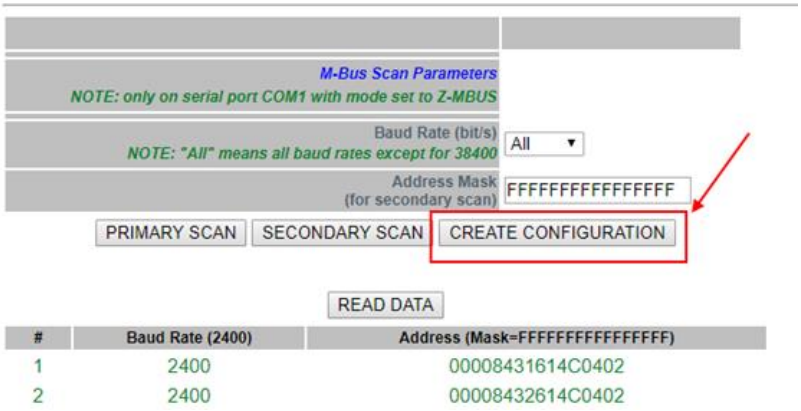
- la prima tabella contiene una sola riga, che fornisce le “informazioni slave”;

- la seconda tabella contiene un numero variabile di righe, ciascuna delle quali fornisce un “data record”.

Cliccando sul pulsante “REFRESH” è possibile aggiornare i dati; cliccando sul pulsante “BACK” si torna alla pagina con la tabella dei dispositivi.

8.41.2. PULSANTE “CREATE CONFIGURATION”

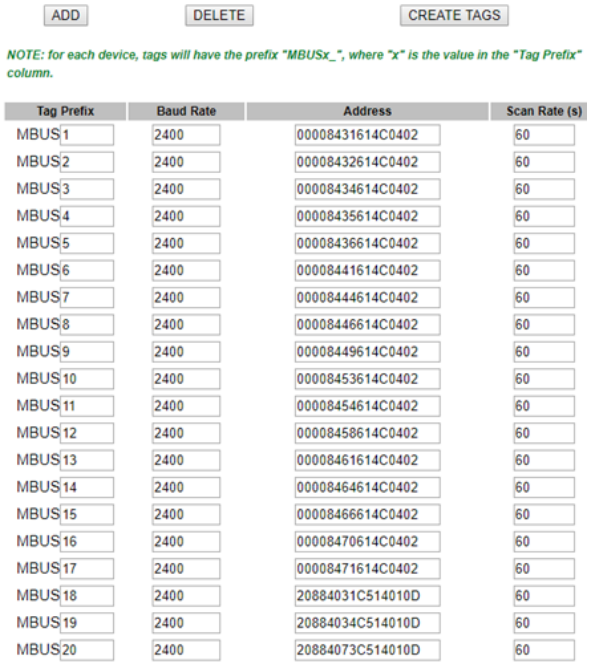
Ora è possibile tornare alle pagine precedenti e premere il pulsante “CREA CONFIGURAZIONE”.



In questo modo è stata salvata la configurazione attuale dell'M-BUS. Il web server si sposta automaticamente alla pagina successiva di “M-Bus Configuration”.

8.41.3. M-Bus Configuration

Dopo aver premuto il pulsante “Crea configurazione” nella pagina M-Bus Scan si ottiene la seguente pagina nella configurazione M-Bus:



ADD DELETE CREATE TAGS

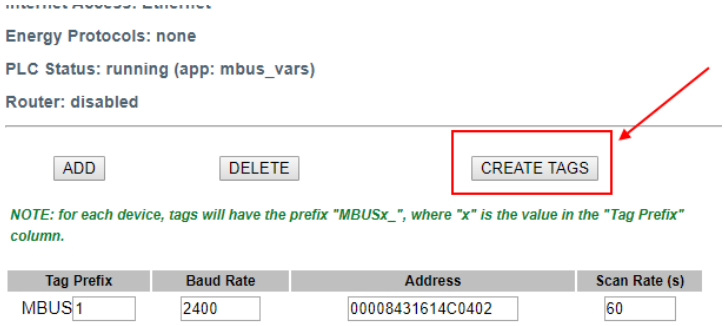
NOTE: for each device, tags will have the prefix "MBUSx_", where "x" is the value in the "Tag Prefix" column.

Tag Prefix	Baud Rate	Address	Scan Rate (s)
MBUS 1	2400	00008431614C0402	60
MBUS 2	2400	00008432614C0402	60
MBUS 3	2400	00008434614C0402	60
MBUS 4	2400	00008435614C0402	60
MBUS 5	2400	00008436614C0402	60
MBUS 6	2400	00008441614C0402	60
MBUS 7	2400	00008444614C0402	60
MBUS 8	2400	00008446614C0402	60
MBUS 9	2400	00008449614C0402	60
MBUS 10	2400	00008453614C0402	60
MBUS 11	2400	00008454614C0402	60
MBUS 12	2400	00008458614C0402	60
MBUS 13	2400	00008461614C0402	60
MBUS 14	2400	00008464614C0402	60
MBUS 15	2400	00008466614C0402	60
MBUS 16	2400	00008470614C0402	60
MBUS 17	2400	00008471614C0402	60
MBUS 18	2400	20884031C514010D	60
MBUS 19	2400	20884034C514010D	60
MBUS 20	2400	20884073C514010D	60

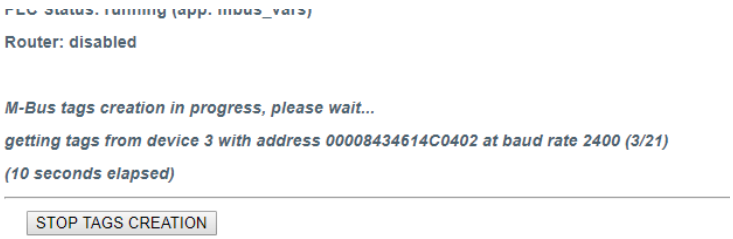
Il risultato della scansione può ora essere modificato.
La prima colonna rappresenta il nome Prefisso del Tag in Straton
La seconda colonna rappresenta il Baud Rate da utilizzare.
La terza colonna rappresenta l'indirizzo del dispositivo.
La quarta colonna rappresenta il tempo di scansione in secondi per questo dispositivo.

8.41.4. IMPORTAZIONE DELLA CONFIGURAZIONE IN STRATON

Prima di tutto dobbiamo esportare l'attuale configurazione.

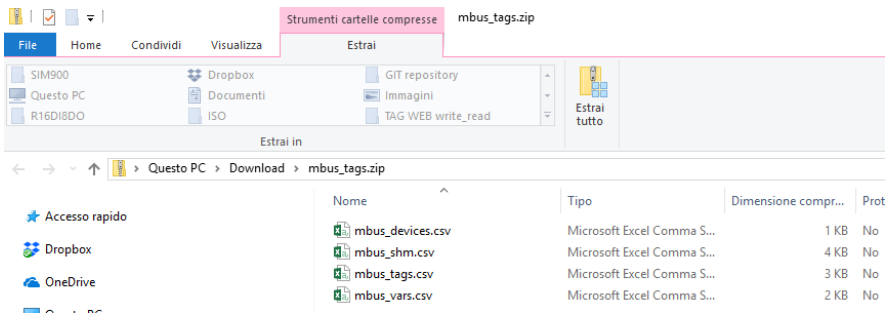


Ora l'acquisizione automatica dei tag inizia:



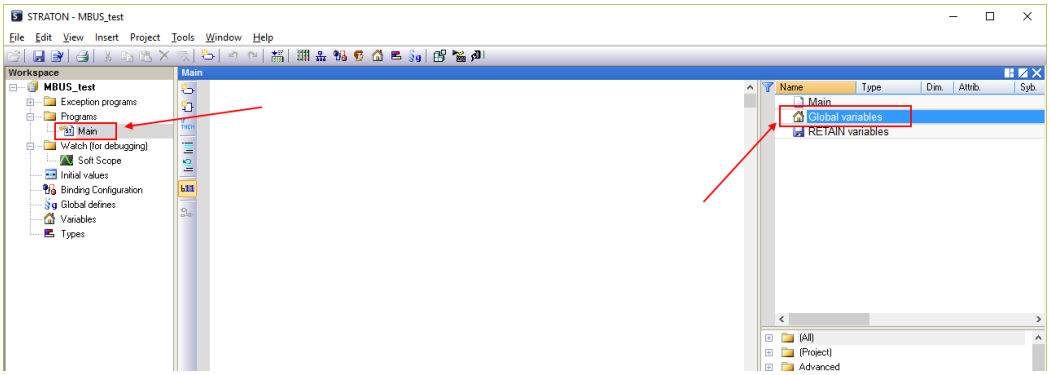
Alla fine del processo un file .zip (mbus_tags.zip) verrà scaricato dal browser:

Il file .zip contiene 4 file:

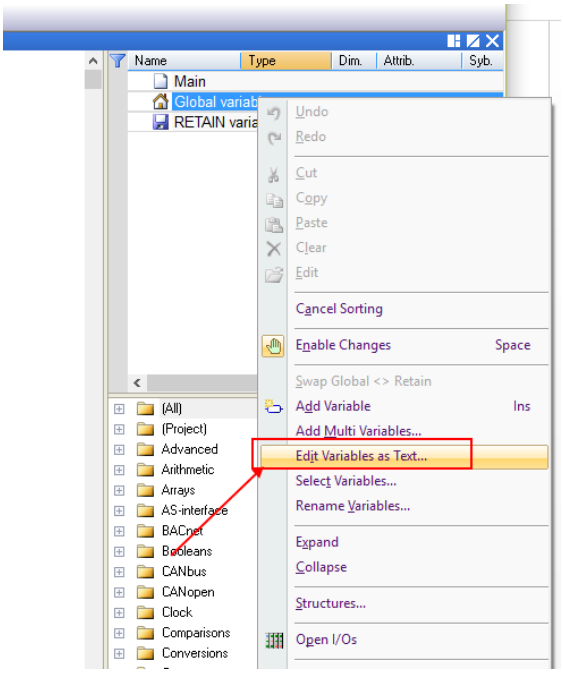


Due di questi file devono essere utilizzati in Straton:
mbus_shm.csv (la configurazione della memoria condivisa)
mbus_vars.csv (l'M-Bus vars)
A questo punto eseguire i seguenti punti:

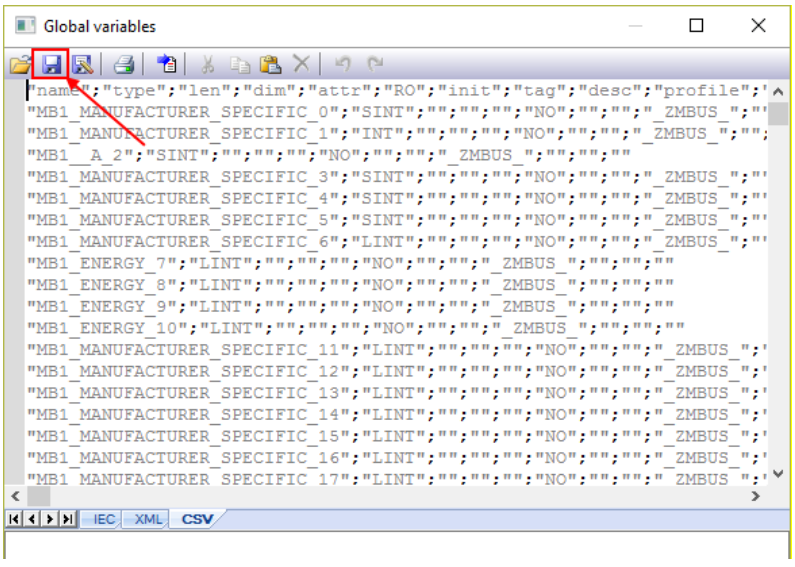
1) Estrarre il file zip in una directory.
2) Avviare Straton workbench
3) Selezionare main e poi Global variables:



Fare click con il pulsante destro del mouse e selezionare “Edit Variables as Text”:

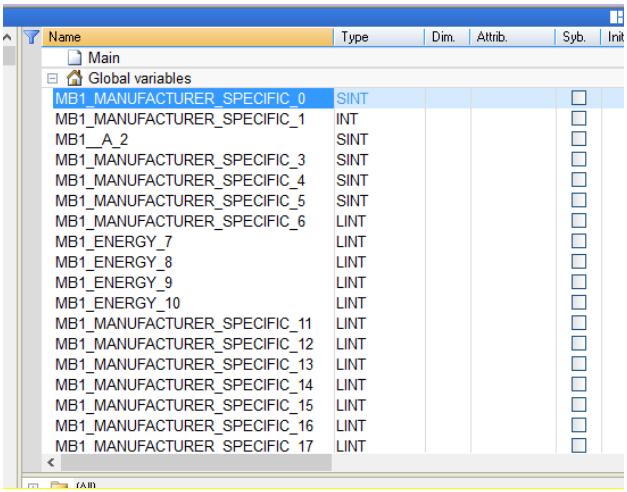


Aprire il file “mbus_vars.csv” con un editor di testo, copiare e incolla l'elenco delle variabili nel modulo "Global variables" in Straton quindi salva la configurazione con l'icona "disco":

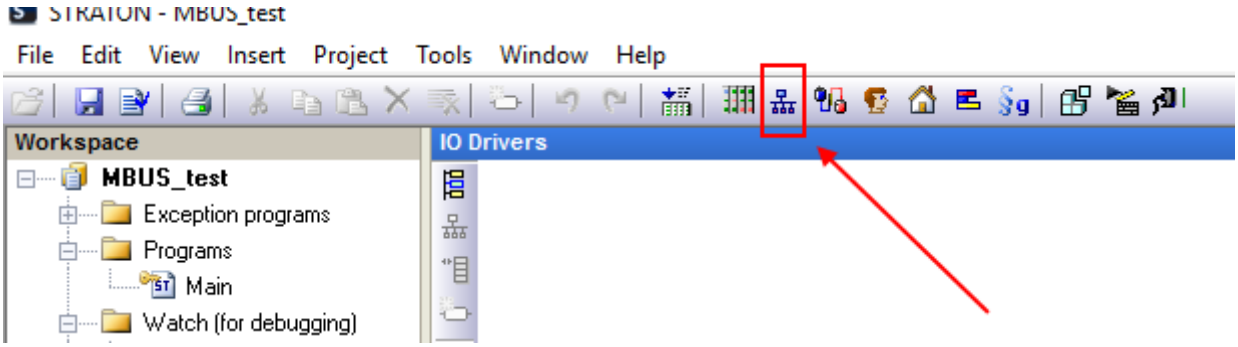


NOTA: La prima riga
“nome”;”tipo”;”len”;…
deve essere presente una sola volta e solo nella prima riga.

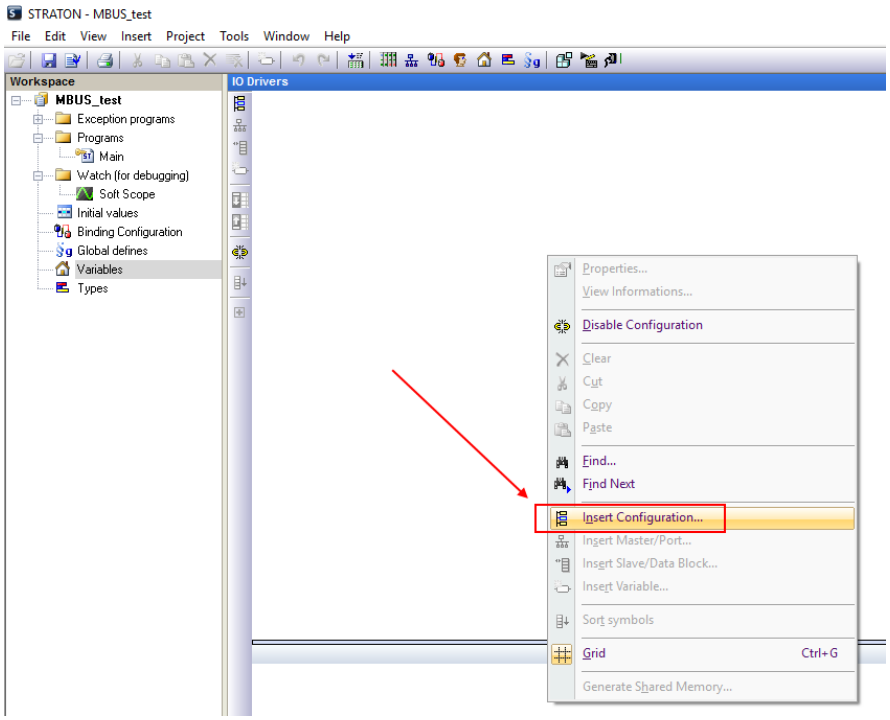
Ora le variabili sono importate:



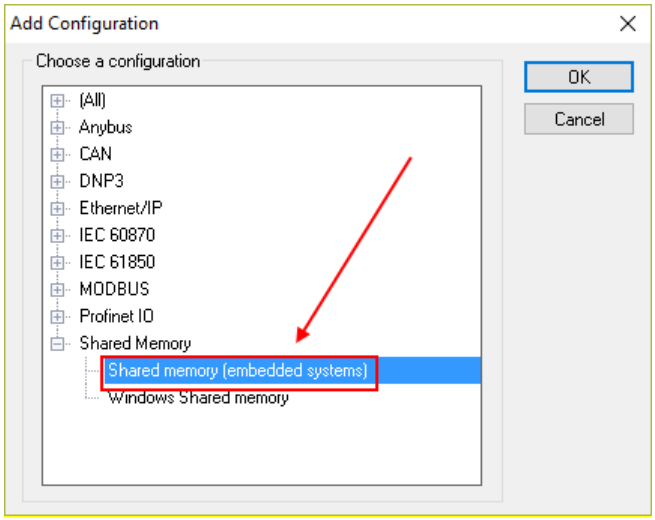
Ora dobbiamo creare la memoria condivisa utilizzata per condividere i dati da M-BUS:
Fare clic sull'icona del bus di campo:



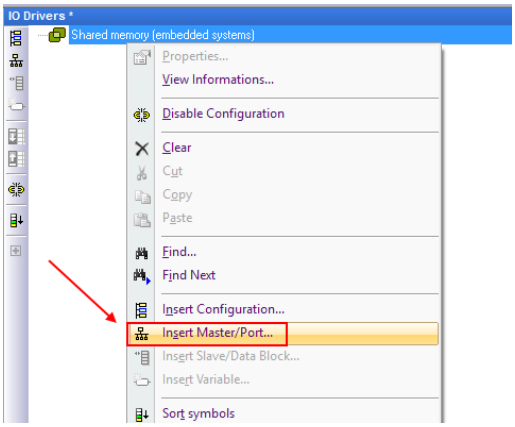
Fare clic con il tasto destro del mouse e selezionare “Insert Configuration”:



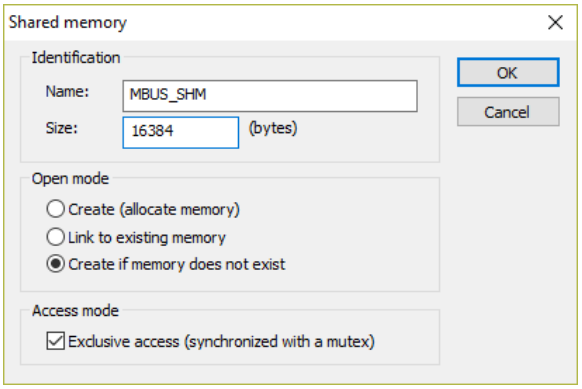
Ora creare la Shared Memory:



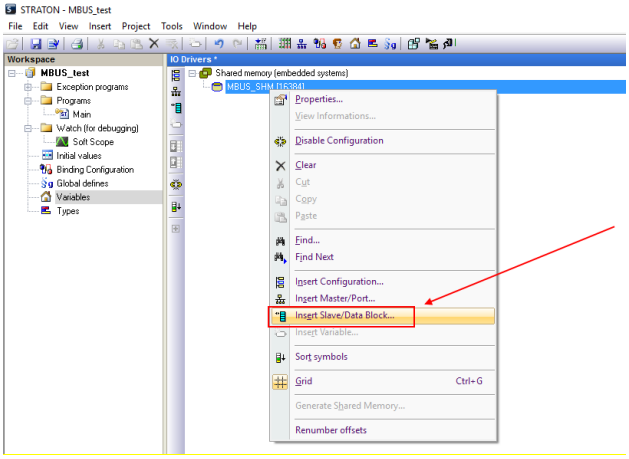
Inserire una porta Master:



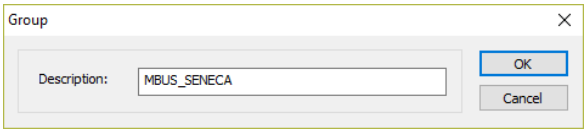
La configurazione della memoria shared deve essere come da figura (non cambiare il setting):



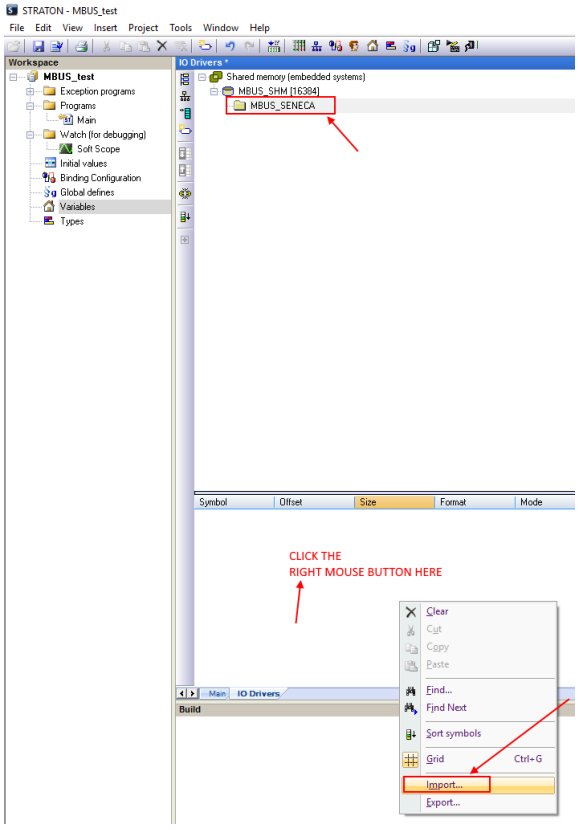
Ora inserire il data block:



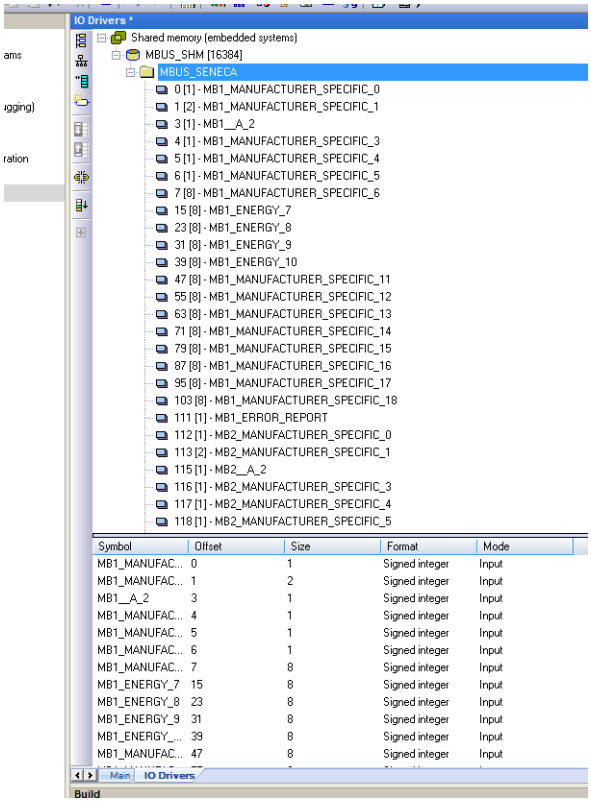
Creare un Gruppo ed inserire un nome:



Ora importare il file della shared memory:

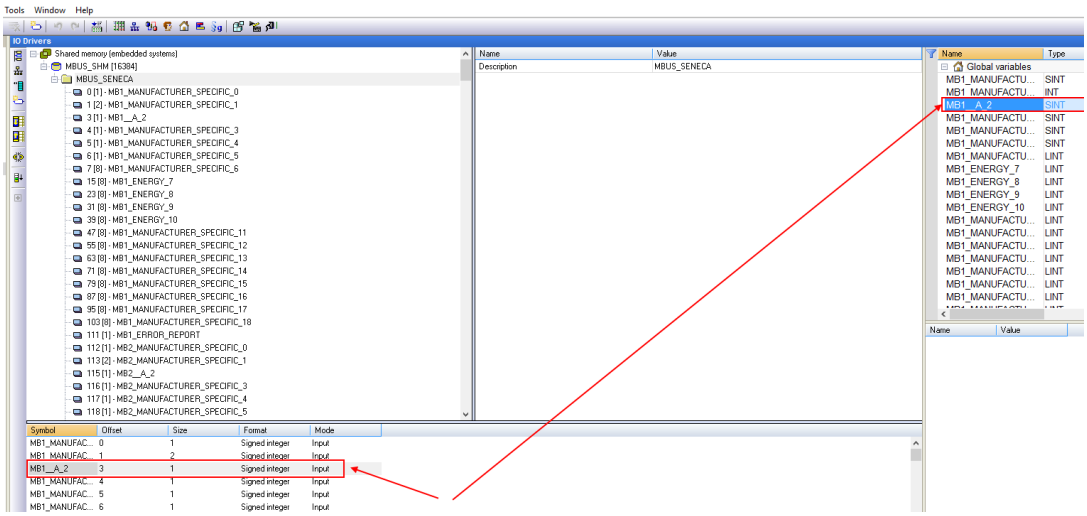


Selezionare il file “mbus_shm.csv”:

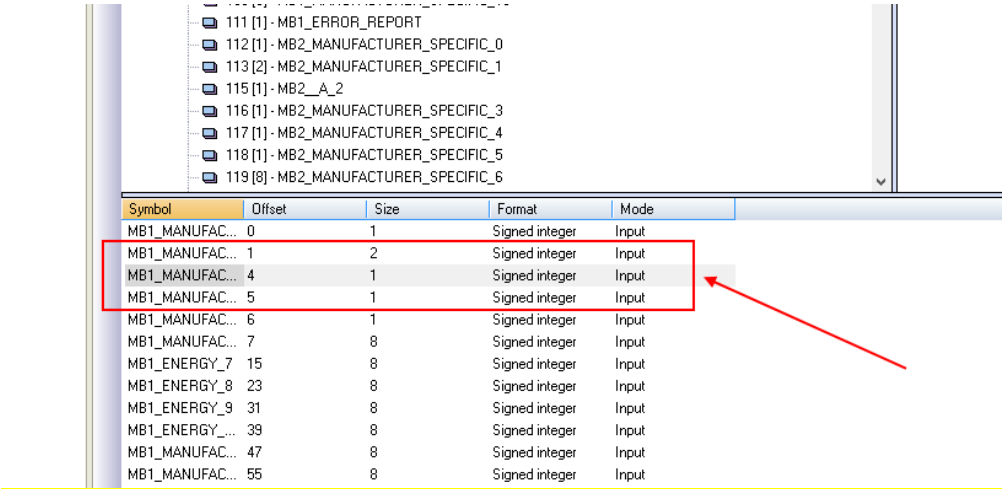


8.41.5. CANCELLARE LE VARIABILI MBUS NON UTILIZZATE

Per eliminare una o più variabili cancellare le variabili e la corrispondente voce di memoria condivisa:



Si noti che nella memoria condivisa gli offset delle altre variabili non vengono modificati:



8.41.6. SOSTITUIRE UN DISPOSITIVO M-BUS

Per Sostituire un dispositivo M-BUS esistente (ad esempio in caso di sostituzione per guasto)

1. Andare su M-BUS Scan ed effettuare una Scansione Secondaria o Primaria

2. Prendere nota del nuovo indirizzo

3. Andare su Configurazione M-BUS e modificare manualmente l'indirizzo dal vecchio al nuovo dispositivo

4. Premi il pulsante " Create Tag".

5. Non è necessario apportare modifiche a Straton

8.41.7. AGGIUNGERE UN DISPOSITIVO M-BUS

1. Andare su “M-BUS Scan” ed eseguire una scansione secondaria o primaria
2. Prendere nota del nuovo indirizzo e baudrate
3. Andare in “M-BUS Configuration” e aggiungere manualmente l'indirizzo e il baudrate del nuovo dispositivo con il pulsante “ADD”
4. Premere il pulsante "Create Tag".
5. Importare il file della shared memory
6. Importare il file delle variabili senza cancellare la tua variabile locale (usare il copia-incolla)

8.41.8. CANCELLARE UN DISPOSITIVO MBUS

1. Andare su M-BUS Scan ed effettuare una Scansione Secondaria o Primaria

2. Prendere nota dell'indirizzo del dispositivo da eliminare

3. Andare su “M-BUS Configuration” ed eliminare manualmente il dispositivo con il pulsante “Delete”.

4. Premi il pulsante "Create Tag".

5. Importare il file della memoria condivisa

6. Eliminare le variabili dal dispositivo eliminato

8.41.9. TAG SPECIALE “TAG ERROR REPORT”

Quando i tag delle variabili vengono importati in Straton, viene creato un tag speciale "Tag error report". Utilizzare questo tag per monitorare gli errori di comunicazione del dispositivo:

VALORE DEL TAG “ERORR REPORT”	***SIGNIFICATO***
0	LETTURA OK
-2	LETTURA IN TIMEOUT, NESSUNA RISPOSTA DAL DISPOSITIVO

8.42. PAGINA CUSTOM IMAGES (GUI CONFIGURATION)

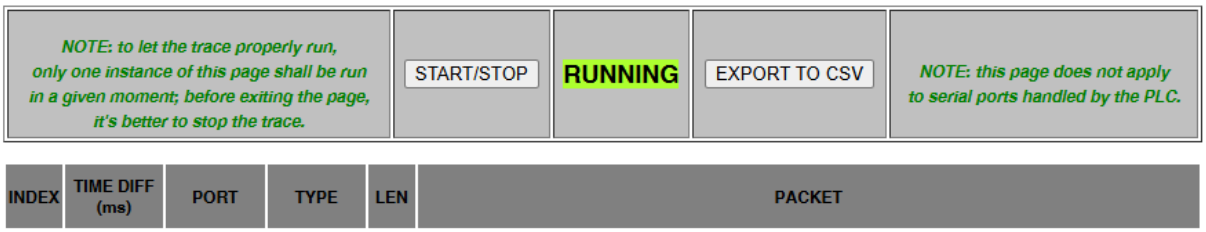
Nei dispositivi è già integrata una libreria di centinaia simboli per essere utilizzati nelle proprie dashboard o sinottici dell’interfaccia grafica fisica (nel modelli dotati di display) o virtuale.
Questa pagina permette di caricare immagini realizzate dall’utente (ad esempio per personalizzare i sinottici con loghi di aziende etc…).
È possibile caricare immagini .png e .jpg con profondità di colore di 8 bit. È consigliato di caricare immagini con una risoluzione massima di 800x 480 pixel.
Una volta caricate le immagini in questa pagina saranno aggiunte alla libreria di simboli.
Nel caso si salvi ed esporti la configurazione anche le immagini custom saranno salvate.

8.43. PAGINA ETHERNET INTERFACES (MAINTENANCE)

Qui sono rappresentati gli indirizzi e le statistiche delle porte ethernet del dispositivo.

8.44. PAGINA MODBUS SERIAL TRACE (MAINTENANCE)

Si tratta di uno sniffer seriale utile per analizzare il traffico seriale. È anche possibile esportare il traffico in formato csv per analizzarlo in un secondo momento.



8.45. PAGINA FW VERSION (MAINTENANCE)

In questa pagina sono riportate le revisioni della versione firmware in uso e della precedente versione installata. Il dispositivo include sempre anche la precedente installazione.

8.46. PAGINA FIRMWARE UPGRADE (MAINTENANCE)

Permette di aggiornare il firmware del dispositivo.

8.47. PAGINA CONF. MANAGEMENT (MAINTENANCE)

Permette di esportare o importare la configurazione del dispositivo (utile nel caso si debba copiare la configurazione su un altro dispositivo).
Sempre nella stessa pagina è possibile salvare i file di log di sistema (debug log) per essere inviati al supporto Seneca e caricare la chiave dell'algoritmo RSA per l'accesso al servizio ssh.

8.48. LICENCE MANAGEMENT (MAINTENANCE)

Qui è possibile verificare quale funzionalità opzionali sono abilitate sotto la voce "Optional Features".
È anche possibile inserire le chiavi di attivazione fornite da Seneca per aggiungere funzionalità opzionali al dispositivo.
Ad esempio è possibile aggiungere la funzionalità PLC Straton ad un dispositivo che non ne sia dotato.
Per maggiori informazioni fare riferimento al supporto Seneca.

8.49. MODBUS MODULES (MAINTENANCE)

Nel caso si utilizzi il PLC in modalità legacy e si utilizzi il software di configurazione legacy Z-NET4 in questa pagina compare l'elenco dei dispositivi Modbus collegati.

8.50. PLC MODE CONFIGURATION (MAINTENANCE)

In Questa pagina è possibile scegliere la modalità di funzionamento del PLC Straton.

Campo	Significato
PLC Mode	"None" il PLC è disabilitato "Legacy" il PLC è in modalità compatibilità per l'uso con configurazioni precedenti alla revisione firmware 3.x.x.x. Per utilizzare il software di configurazione Z-NET4 è indispensabile impostare il PLC in questa modalità. È la modalità di default per i dispositivi "-S" o "-E". In questa modalità il display virtuale, il datalogger, gli allarmi etc… non sono disponibili "Shared" il PLC è in modalità condivisa ovvero può condividere i TAG tra il PLC e il firmware e sfruttare quindi tutte le nuove funzionalità dei firmware versioni 3.x.x.x. Non è più possibile la configurazione con Z-NET4

9. VPN

Una VPN (Virtual Private Network) è una rete privata virtuale che garantisce privacy, anonimato e sicurezza attraverso un canale di comunicazione (tunnel VPN) creato sopra un'infrastruttura di rete pubblica.
I dispositivi possono creare delle VPN utilizzando la tecnologia Seneca LET'S che si basa su un server VPN BOX 2.
È anche possibile connettersi a server standard OpenVPN.

Per maggiori informazioni sulla tecnologia Let's visitare il sito:

https://www.seneca.it/linee-di-prodotto/comunicazione-industriale-e-telecontrollo/lets-connectivity-solutions/

Per maggiori informazioni su OpenVpn visitare il sito:

https://openvpn.net/

Per maggiori informazioni su VPN BOX 2 fare riferimento a:

https://www.seneca.it/linee-di-prodotto/comunicazione-industriale-e-telecontrollo/lets-connectivity-solutions/modulo-server-di-connettivita/

Il dispositivo può creare delle VPN utilizzando come server sia il prodotto Seneca VPN BOX2 sia un server standard OpenVPN.

I principali vantaggi che derivano dall'utilizzo di una VPN sono:

- connessioni sicure, poiché i dati trasportati sono criptati;
- la capacità di stabilire connessioni senza interferire con la LAN aziendale;
- nessuna necessità di avere un indirizzo IP statico/pubblico
- sul lato WAN; configurabilità remota tramite un Web Server

Sono disponibili due "modalità VPN", denominate rispettivamente "OpenVPN" e "VPN BOX".

La modalità "OpenVPN" può essere utilizzata quando il dispositivo deve essere installato in una VPN esistente. In questo caso, deve essere disponibile un server OpenVPN e i file di configurazione, certificato e chiave per il client Seneca devono essere forniti dall'amministratore della VPN.
I file possono essere caricati nel dispositivo utilizzando la pagina web dedicata.

Se l'infrastruttura VPN non esiste ancora, la scelta consigliabile è quella di adottare la soluzione "VPN Box2", sviluppato da Seneca.
"VPN Box2" è un'apparecchiatura hardware (disponibile anche in versione macchina virtuale) che permette all'utente di configurare facilmente due tipi alternativi di VPN:

- "VPN "Single LAN" (Always on per sistemi SCADA)
- VPN "Point-to-Point" (On demand per manutenzione remota di macchine)

Nella VPN "Single LAN", tutti i dispositivi e i PC (e le sottoreti locali associate) configurati in VPN sono sempre collegati nella stessa rete. In questo scenario qualsiasi PC Client può connettersi a qualsiasi dispositivo Seneca e ad altre macchine che si trovano nella stessa LAN, ma anche qualsiasi dispositivo/macchina può connettersi a qualsiasi altro dispositivo/macchina remota che appartiene alla stessa rete VPN.

Nella VPN "Point-to-Point", un PC client, in un determinato momento, può eseguire una singola connessione, su richiesta ad un solo dispositivo alla volta (e alle macchine che si trovano collegate alla porta LAN del dispositivo Seneca).
Inoltre, i dispositivi non possono comunicare tra loro anche se appartengono alla stessa VPN.
Il vantaggio di questa architettura è che la stessa sottorete può essere utilizzata in tutti i siti. La modalità punto-punto è la più usata nel caso di manutenzione remota degli impianti.

Ci sono due tipi di VPN "Point to point":
- Layer 3 VPN
- Layer 2 VPN

In " Layer 3 VPN", solo i pacchetti IP (Layer 3) vengono trasportati attraverso il tunnel VPN.
Al contrario, in "Bridging Layer 2 VPN", tutti i frame Ethernet vengono trasportati attraverso il tunnel VPN

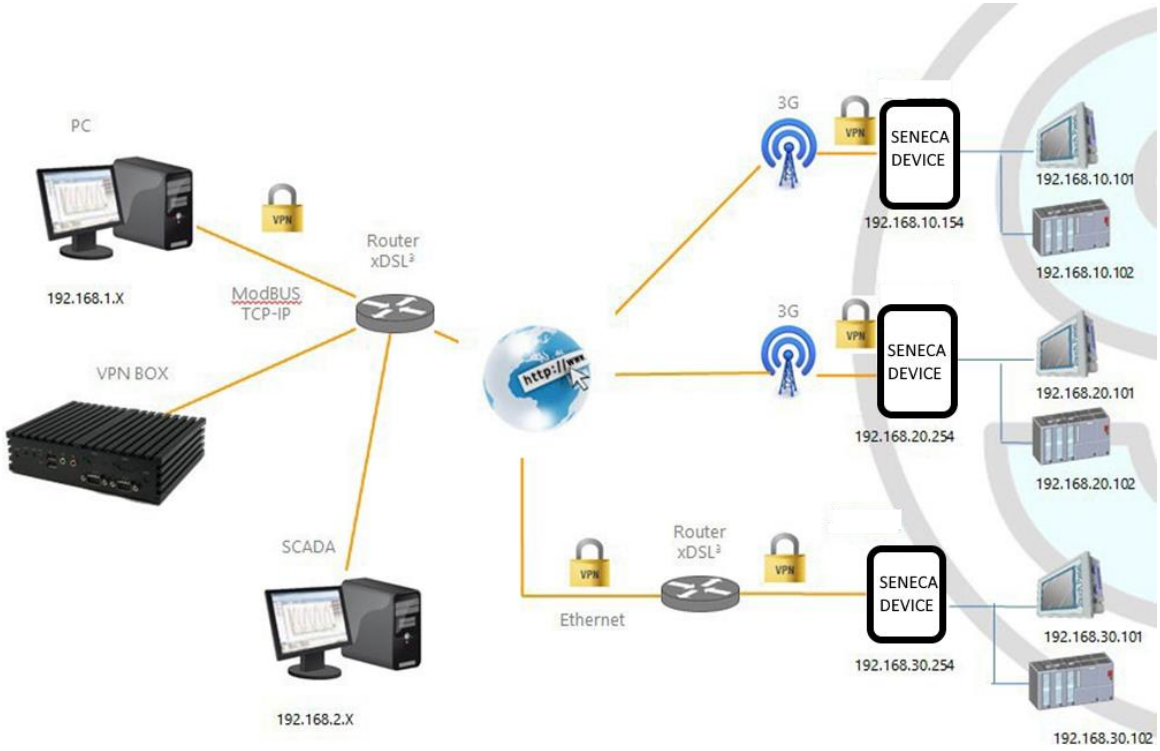
Ognuno dei due tipi ha vantaggi e svantaggi:

<u>Layer 2</u>
- può trasportare qualsiasi protocollo di rete (ad esempio la scansione del protocollo Siemens™ Profinet)
- causa più traffico sul tunnel VPN rispetto il layer3

<u>Layer 3</u>
- può trasportare solo traffico IP
- il traffico layer2 (ad es.: DHCP) non viene trasportato
- riduce i costi di gestione del traffico, trasporta solo il traffico destinato ai client

Il "VPN Box2" viene fornito con una applicazione Windows: "VPN Client Communicator" che permette all'utente di collegare il PC alla rete (nel caso "Single LAN") o ad un dispositivo specifico (nel caso "Point-to-Point")

9.1. VPN "SINGLE LAN" ALWAYS ON



La figura sopra riportata fornisce un esempio di VPN

Il PC client (con indirizzo IP 192.168.1.X) può collegarsi, a titolo di esempio, al primo dispositivo Seneca utilizzando il suo indirizzo IP locale.

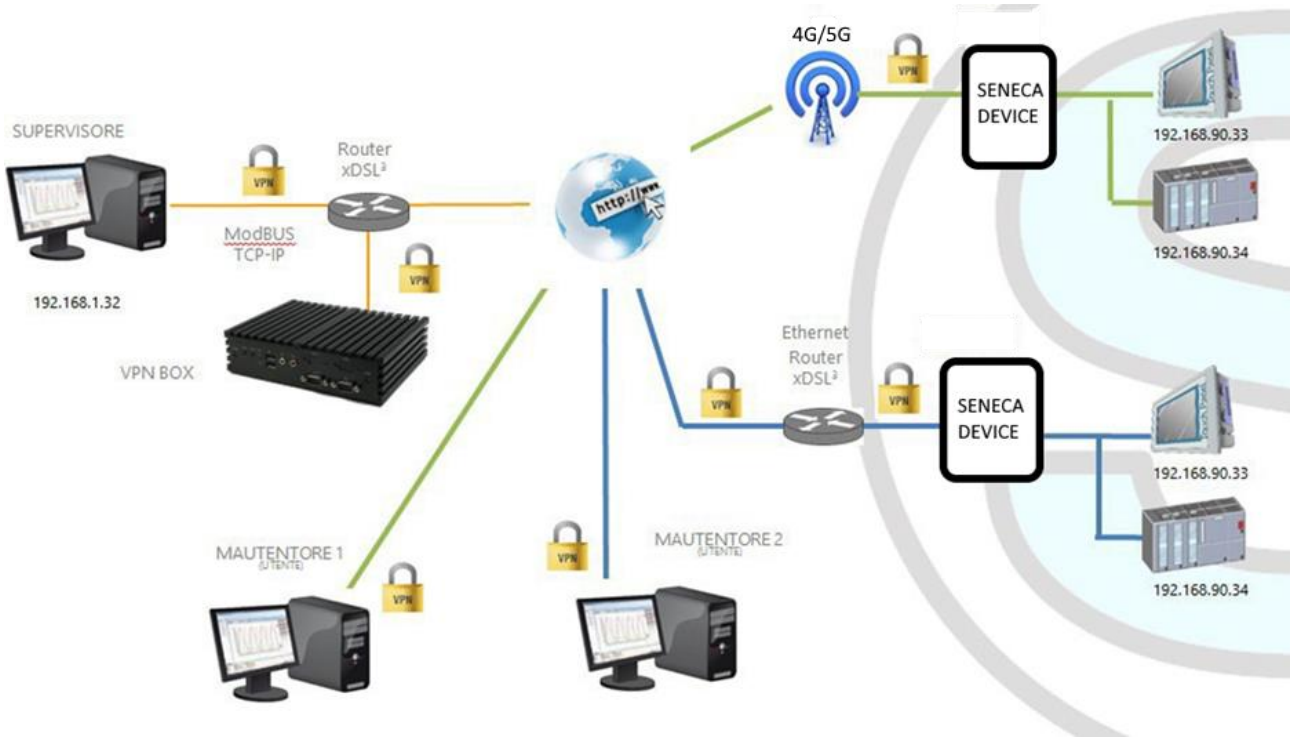
Inoltre, due dispositivi che si trovano in due diverse LAN della stessa rete VPN (ad es: 192.168.10.101 e 192.168.20.102) possono connettersi tra loro, sempre utilizzando i loro indirizzi IP locali.

Affinché questo scenario funzioni correttamente, occorre sempre seguire una regola essenziale: le LAN del dispositivo Seneca e la LAN del PC devono avere sottoreti diverse e non in collisione; pertanto, nella figura precedente, è stata raffigurata

PC LAN	192.168.1.0/24
SCADA LAN	192.168.2.0/24
SENECA DEVICE LAN	192.168.10.0/24
SENECA DEVICE LAN	192.168.20.0/24
SENECA DEVICE LAN	192.168.30.0/24

Se non è possibile evitare conflitti, è ancora possibile utilizzare una VPN "Single LAN" poiché i dispositivi possono essere raggiunti tramite i loro indirizzi IP VPN e le macchine al di là di essi possono essere raggiunte configurando regole di "port forwarding".

9.2. VPN "POINT TO POINT" ON DEMAND



La figura sopra riportata fornisce un esempio di VPN "Point-to Point".

In questo scenario un PC (che agisce come client VPN) può connettersi, su richiesta, ad un dispositivo Seneca e alla sua sottorete, utilizzando gli indirizzi IP locali tramite l'applicazione "VPN Client Communicator". Il software garantisce la gestione a gruppi delle utenze per permettere solo a chi appartiene ad un gruppo di accedere agli impianti che ne fanno parte

9.3. DISABILITAZIONE DELLA CONNESSIONE VPN

I prodotti forniscono un ingresso digitale e un'uscita digitale dedicati a controllare e monitorare la connessione remota al dispositivo.
In questo modo è possibile bloccare l'accesso (tramite ingresso digitale) da remoto ad una particolare macchina/impianto (per esempio se si stanno facendo delle operazioni di manutenzione locale) ed essere informati di un accesso remoto in corso (tramite l'uscita digitale).

Quando l'ingresso digitale "Remote Connection Disable" è impostato sullo stato HIGH, la connessione remota al dispositivo è disabilitata; al contrario, quando l'ingresso digitale "Remote Connection Disable" è impostato sullo stato LOW, la connessione remota al dispositivo è abilitata.

L'uscita digitale "Remote Connection Active" è impostata allo stato ALTO quando il dispositivo è remoto è connesso.

Quattro livelli di sicurezza possono essere configurati per disabilitare la connessione VPN remota:

Livello 1: Le connessioni VPN sono disabilitate in qualsiasi modalità VPN ma il servizio “VPN Box Service” è ancora in funzione, quindi il dispositivo può ancora essere monitorato su VPN Box Manager;
Livello 2: Il servizio “VPN Box Service” è disabilitato, ma il dispositivo può comunque accedere a Internet e inviare/ricevere SMS su un’eventuale interfaccia cellulare;
Livello 3: qualsiasi accesso ad Internet è disabilitato, ma il dispositivo può comunque inviare/ricevere SMS su un’eventuale interfaccia cellulare;
Livello 4: Come livello 3 ma anche l’interfaccia cellulare è spenta

9.4. FILE DI CONFIGURAZIONE PER L’UTILIZZO CON OPEN VPN

Questo paragrafo fornisce un esempio di configurazione per il server OpenVPN.

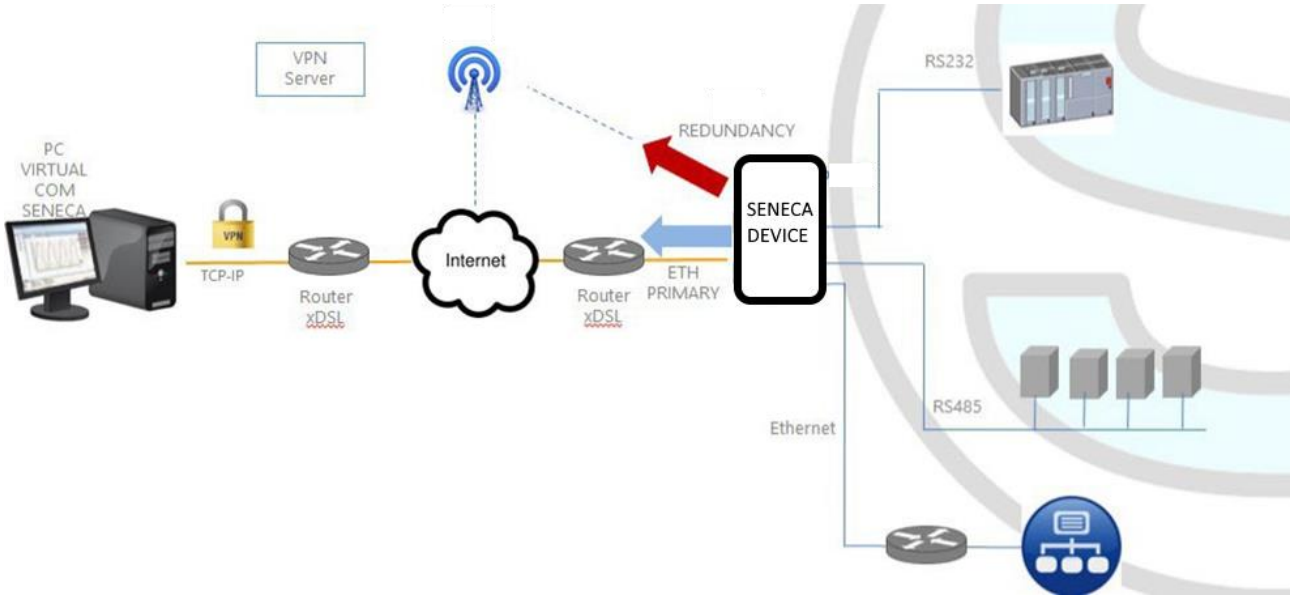
```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 10.9.7.0 255.255.255.0
ifconfig-pool-persist ipp.txt
client-config-dir ccd
client-to-client
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Questo paragrafo fornisce un esempio di configurazione del client Open VPN del dispositivo.

```
client
dev tun
port 1194
proto udp
remote 2.192.5.105 1194
nobind
ca ca.crt
cert tws4.crt
key tws4.key
comp-lzo
```

```
persist-key
persist-tun
script-security 3 system
verb 3
```

10. RIDONDANZA DELLA RETE DI COMUNICAZIONE



La "Ridondanza di rete" (network redundancy) è una funzionalità che può essere abilitata sui dispositivi dove è disponibile un modem mobile oppure il WI-FI.

Questa funzionalità ha lo scopo di commutare l'interfaccia di rete utilizzata per accedere a Internet da Ethernet (interfaccia "primary") all'interfaccia secondaria (modem Cellulare oppure WI-FI), quando l'accesso a Internet attraverso l'interfaccia primaria diventa non disponibile il sistema attinge ad internet tramite il canale secondario configurato. Quando il servizio internet ritorna disponibile dall'interfaccia primaria l'accesso torna nuovamente su quest'ultima.

11. PROTOCOLLO MQTT CLIENT

L'MQTT è il protocollo più utilizzato per le applicazioni IOT.

"MQTT" sta per MQ Telemetry Transport. Si tratta di un protocollo di messaggistica di pubblicazione/sottoscrizione, estremamente semplice e leggero, progettato per dispositivi con reti a bassa larghezza di banda, ad alta latenza o inaffidabili. I principi di progettazione sono quelli di ridurre al minimo i requisiti di larghezza di banda di rete e di risorse dei dispositivi, cercando al contempo di garantire l'affidabilità e un certo grado di garanzia della consegna. Questi principi si rivelano ideali per l'emergente mondo "machine-to-machine" (M2M) o "Internet delle cose.

Per maggiori informazioni sul protocollo MQTT vedi

La versione MQTT supportata è la 3.1.1

11.1. CARATTERISTICHE DELL'IMPLEMENTAZIONE DEL PROTOCOLLO MQTT

Il protocollo MQTT può essere abilitato insieme agli altri protocolli client (USB, FTP, EMAIL, …); tuttavia, quando il protocollo MQTT è abilitato, le seguenti modifiche si applicano al comportamento del Data Logger

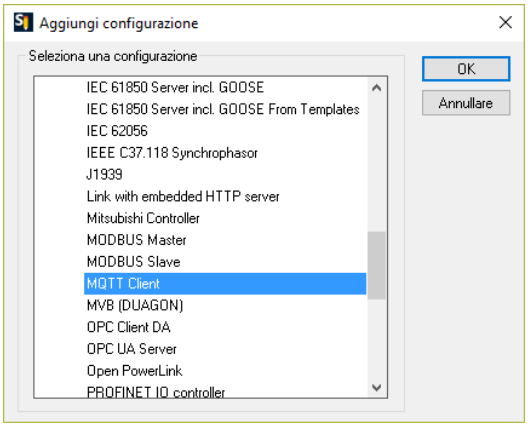
Il protocollo MQTT consente inoltre di eseguire le seguenti azioni sul dispositivo:

- impostazione dei valori di uno o più tag
- riavvio del dispositivo
- salvare la configurazione del dispositivo sul sito FTP del server
- caricare la configurazione del dispositivo dal sito FTP del server
- avvio dell'aggiornamento FW;

C'è una cache interna anche per i messaggi LOG inviati tramite richieste MQTT, utilizzata per memorizzare i messaggi di log mentre non è possibile inviarli al broker; questa cache può contenere fino a 3000 messaggi

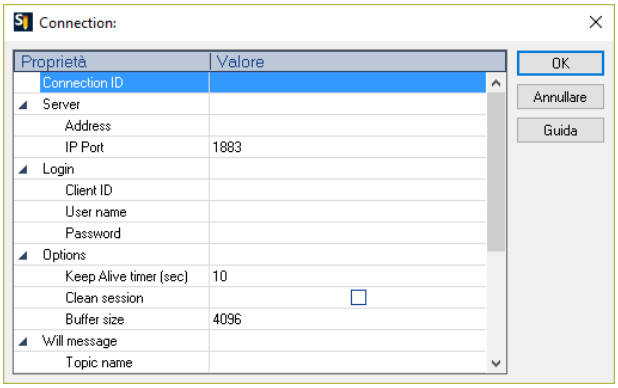
11.2. CARATTERISTICHE DELL'IMPLEMENTAZIONE DEL PROTOCOLLO MQTT DEL PLC STRATON

La versione MQTT supportata è la 3.1.1
Per utilizzare il client MQTT selezionalo dalla sezione Straton Workbench Fieldbus:



11.2.1. PARAMETRI DEL PROTOCOLLO MQTT DAL PROGRAMMA PLC

Il setup di MQTT può essere effettuato direttamente dal workbench:



Se fosse necessario configurare questi parametri dal programma Straton PLC, è possibile utilizzare una serie di parole speciali che caricheranno la configurazione da un file.
Le parole speciali sono:

Nel campo “Address” digitare: mqtt_par_address in modo che il campo “Address” sia ottenuto dal file:

/var/run/mqtt_par_address

Nel campo “Client ID” digitare: mqtt_par_clientid in modo che il campo “Client ID” sia ottenuto dal file:
/var/run/mqtt_par_clientid
Nel campo “Nome Utente” digitare: mqtt_par_username in modo che il campo “Nome Utente” sia ottenuto dal file:
/var/run/mqtt_par_username

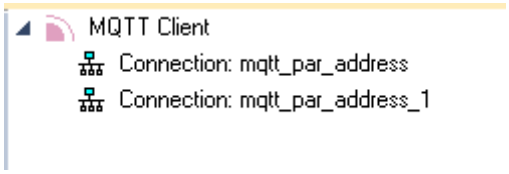
Nel campo “Password” digitare: mqtt_par_password in modo che il campo “Password” sia ottenuto dal file:
/var/esegui/mqtt_par_password

ATTENZIONE!

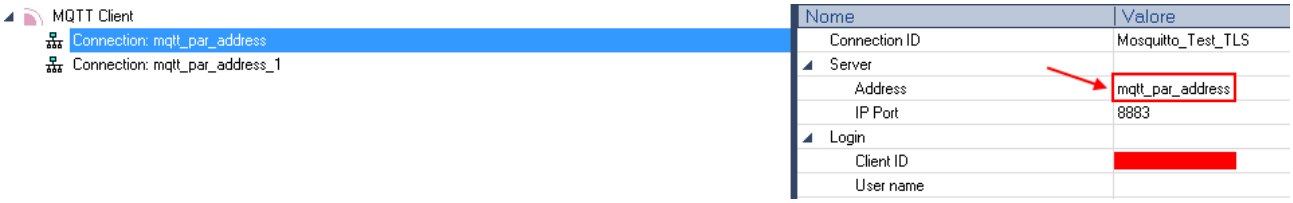
Il parametro Address non deve contenere un FQDN, ma l’indirizzo IP, questo perché il FB MQTTCONNECT non esegue la risoluzione DNS.
In alternativa, può contenere il nome del file (es.: mqtt_par_address), creato nella directory /var/run dal FB DNS_RESOLVE e contenente il risultato della risoluzione DNS.

11.2.2. GESTIRE CONNESSIONI MQTT MULTIPLE

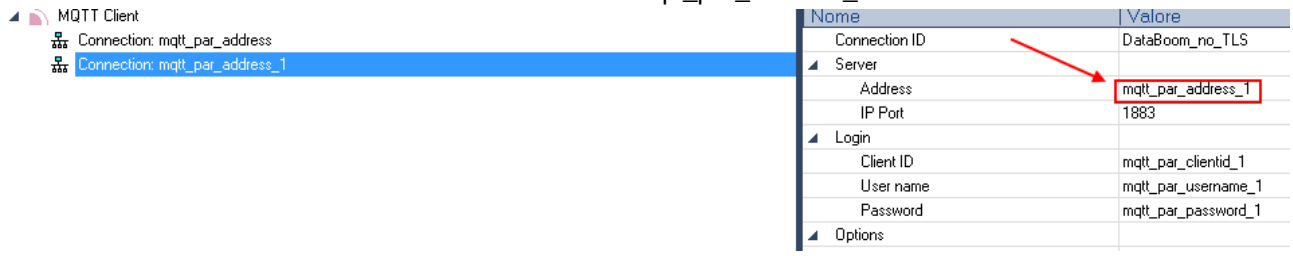
È possibile gestire più connessioni MQTT utilizzando parametri che iniziano con le parole speciali (mqtt_par_address123, mqtt_par_address_aaa, …), ad esempio per creare 2 connessioni mqtt:



The first connection use the Field address “mqtt_par_address”



Quindi caricherà l'indirizzo dal file:
/var/run/mqtt_par_address
La seconda connessione utilizza l'indirizzo archiviato “mqtt_par_address_1”



questo caricherà l'indirizzo dal file:
/var/run/mqtt_par_address_1
(la tecnica può essere utilizzata anche per gli altri parametri client id, username e password).

11.2.3. CONFIGURAZIONE MQTT DEI RETRY SSL/TLS

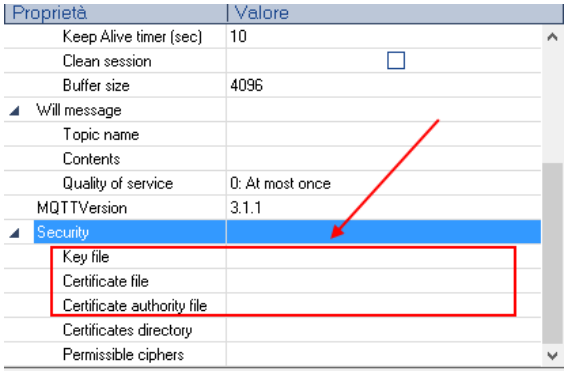
La configurazione predefinita per la connessione SSL/TLS MQTT è:
CONN _TRY_MAX = 10
CONN_TRY_WAIT = 1000 ms
In cui si:
CONN _TRY_MAX è il numero di tentativi per la connessione.
CONN_TRY_WAIT è il timeout di ogni tentativo di connessione.
Se è necessario modificare questa configurazione predefinita è necessario creare il file:
“ssl_con_try_params”
In questo percorso:
“/var/esegui/”
Con i valori dei parametri, ad esempio:

root@Z-PASS2-S:~# cat /var/run/ssl_conn_try_params
50,200

Significa CONN _TRY_MAX = 50 e CONN_TRY_WAIT = 200 ms.
NOTA1: Alla fine del file è necessario aggiungere un \n (carattere di nuova riga)
NOTA2: Il file viene caricato in un filesystem RAM, quindi è necessario crearlo ad ogni avvio.

11.2.4. CERTIFICATI CLIENT STATICI E DINAMICI

Nella configurazione MQTT sotto la sezione Sicurezza puoi inserire il percorso e il nome del file per i certificati:



Seneca suggerisce di utilizzare la directory /config per i certificati.
Il certificato del client MQTT può essere caricato solo dal server FTP.
Il file della chiave è il file della chiave privata del client.
Il file del certificato è il certificato del client.
Il file dell'autorità di certificazione è il certificato dell'Autorità di certificazione.

ATTENZIONE!

Il campo "Certificate directory" non è utilizzato quindi il nome dei file deve riportare il path assoluto esempio:
"/config/mqtt/client.key"
"/config/mqtt/client.crt"
"/config/mqtt/ca.crt"
Se si deve modificare dinamicamente questi file ed altri parametri senza ricompilare il progetto è possibile caricare nella directory /var/run un file con nome file che deve iniziare rispettivamente con: "mqtt_par_clientkey", "mqtt_par_clientcert", "mqtt_par_cacert"
Il contenuto dei file deve essere un testo con il nome del file senza il percorso.
Si noti che in un programma è possibile utilizzare più di un file di certificato, ad esempio "mqtt_par_clientcert00", "mqtt_par_clientcert01" ecc...

11.2.5. CAMBIARE I PARAMETRI MQTT IN RUNTIME TRAMITE FILE

È possibile modificare la porta e la configurazione keepalive sovrascrivendo in runtime la configurazione attuale con i seguenti file:
"mqtt_par_port" e "mqtt_par_keepalive".

Il contenuto dei file deve essere un testo con il nuovo valore del parametro.

12. LE REGOLE LOGICHE

Una regola logica si basa sul seguente concetto di

“IF -> THEN -> ELSE”

Ovvero:

SE LA CONDIZIONE SI È VERIFICATA -> ALLORA ESEGUI QUESTE AZIONI -> ALTRIMENTI ESEGUI QUESTE ALTRE AZIONI

È possibile definirne fino ad un massimo di 2000 regole.

In ogni regola possono essere configurate anche:

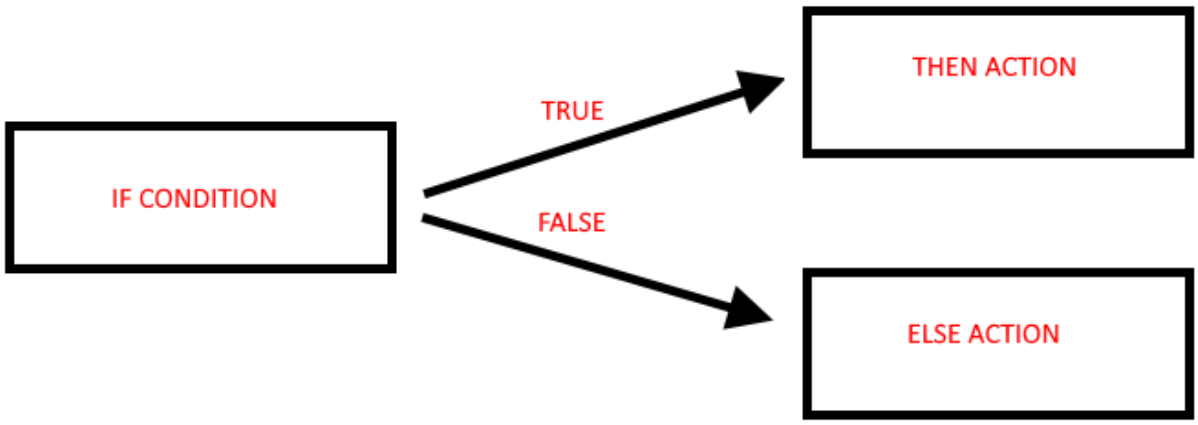
- Combinazioni di fino a tre condizioni logiche (basate sugli stati di allarme) in un'espressione logica OR;
- Possono essere eseguite fino a tre azioni

Tramite le regole logiche è quindi possibile eseguire programmi che utilizzano l’I/O interno o esterno, inviano messaggi di testo e/o scrivono TAG via MODBUS / EMAIL / SMS / http / MQTT etc… anche utilizzando complesse operazioni matematiche.

Le regole possono anche essere debuggate tramite l’esecuzione step by step e l’utilizzo di breakpoint che bloccano l’esecuzione del programma su una specifica riga (regola).

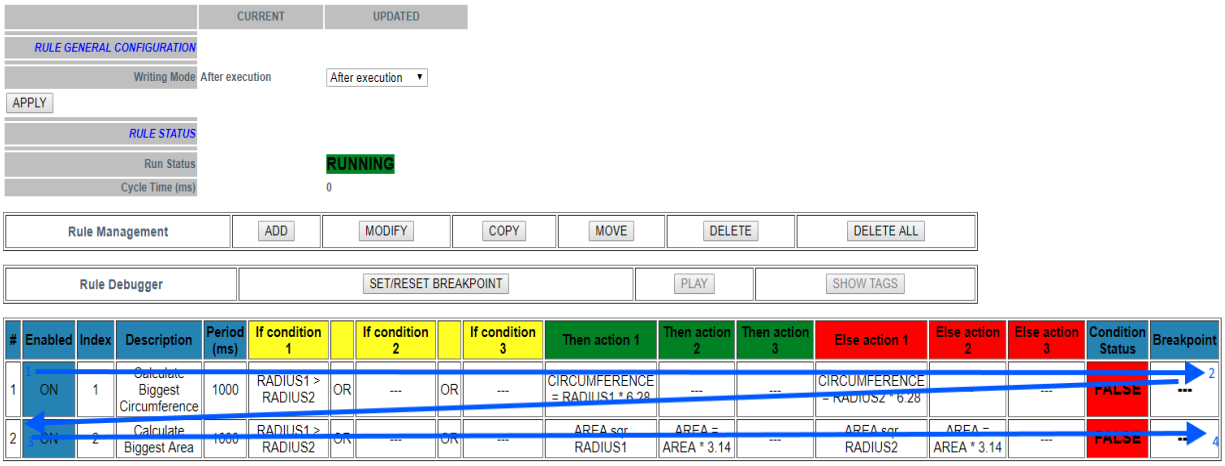
Una regola è composta da una o più “If Condition”, una o più “Then Action” e una o più “Else Action”.

Schematicamente una regola esegue il seguente flusso:

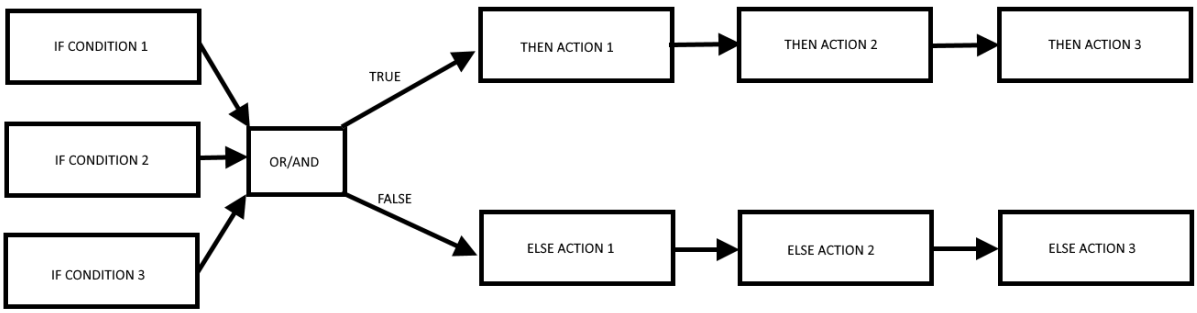


Se la condizione “IF” è vera viene eseguita l’azione “THEN”, altrimenti viene eseguita l’azione “ELSE”.

Le regole vengono eseguite dall'alto verso il basso e da sinistra a destra (in figura 1-> 2-> 3-> 4):



Quando tutte le regole sono eseguite, l'esecuzione riparte dalla prima.
Più in dettaglio il diagramma corretto è:



È infatti possibile definire fino a 3 condizioni if e fino a 3 azioni sia per lo stato THEN che ELSE.

È possibile creare fino a 2000 differenti regole.

Nella “Rule General Configuration” possiamo scegliere quando i Tag vengono scritti nella shared memory, è possibile scegliere tra “After Execution” o “During Execution”.

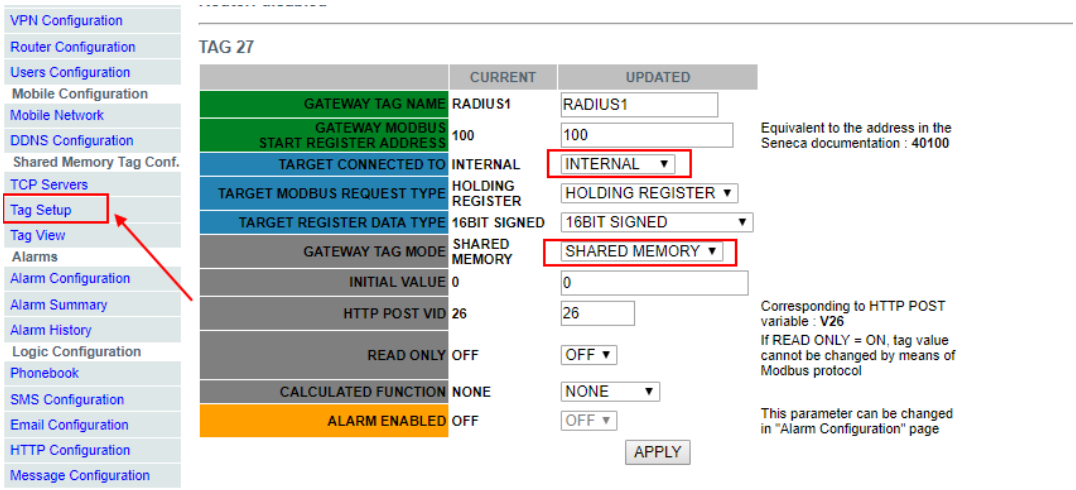
Con "After Execution", si ottiene che i valori dei tag vengono scritti nella memoria shared solo quando SONO state eseguite tutte le regole.
Con “During Execution”, si ottiene che i valori dei tag vengano scritti nella memoria shared alla fine di ogni singola regola.

Quindi, utilizzando la modalità "After Execution", i nuovi valori dei tag verranno aggiornati solo alla fine di tutte le regole (anche i tag che devono essere scritti su ModBUS RTU / TCP-IP).
Lo stato della regola mostrerà lo stato di esecuzione (se le regole sono in modalità di esecuzione o pausa) e il tempo di loop che rappresenta il tempo impiegato per eseguire tutte le regole (si noti che se è necessario scrivere tag con protocollo modbus, il tempo di ciclo includerà anche il tempo impiegato per questa operazione).

12.1. CREAZIONE DI UN PROGRAMMA CON LE REGOLE LOGICHE

Creeremo un programma di esempio che dati 2 diversi raggi di una circonferenza ne calcoli la Circonferenza massima e l'Area massima.

Prima di tutto aggiungiamo i Tag di cui abbiamo bisogno per il programma:
Definiamo i tag Radius1 e Radius2 di tipo intero
Circumference e Area in Real 32 bits (floating point single precision):



	CURRENT	UPDATED	
GATEWAY TAG NAME	RADIUS2	RADIUS2	
GATEWAY MODBUS START REGISTER ADDRESS	101	101	Equivalent to the address in the Seneca documentation : **40101**
TARGET CONNECTED TO	INTERNAL	INTERNAL ▼	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	HOLDING REGISTER ▼	
TARGET REGISTER DATA TYPE	16BIT SIGNED	16BIT SIGNED ▼	
GATEWAY TAG MODE	SHARED MEMORY	SHARED MEMORY ▼	
INITIAL VALUE	0	0	
HTTP POST VID	27	27	Corresponding to HTTP POST variable : **V27**
READ ONLY	OFF	OFF ▼	If READ ONLY = ON, tag value cannot be changed by means of Modbus protocol
CALCULATED FUNCTION	NONE	NONE ▼	
ALARM ENABLED	OFF	OFF ▼	This parameter can be changed in "Alarm Configuration" page
		APPLY	

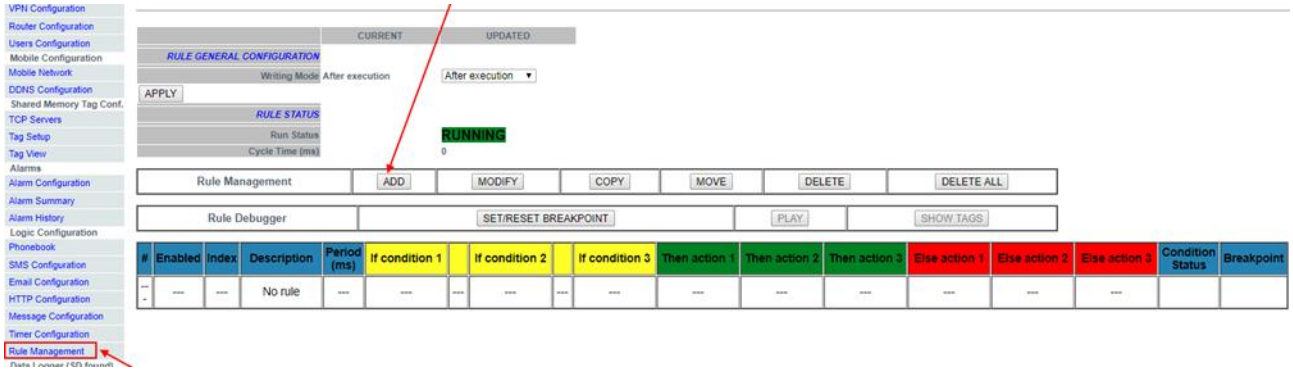
TAG 29

	CURRENT	UPDATED	
GATEWAY TAG NAME	CIRCUMFERENCE	CIRCUMFERENCE	
GATEWAY MODBUS START REGISTER ADDRESS	103	103	Equivalent to the address in the Seneca documentation : **40103**
TARGET CONNECTED TO	INTERNAL	INTERNAL ▼	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	HOLDING REGISTER ▼	
TARGET REGISTER DATA TYPE	32BIT REAL MSW	32BIT REAL MSW ▼	
GATEWAY TAG MODE	SHARED MEMORY	SHARED MEMORY ▼	
INITIAL VALUE	0	0	
HTTP POST VID	28	28	Corresponding to HTTP POST variable : **V28**
READ ONLY	OFF	OFF ▼	If READ ONLY = ON, tag value cannot be changed by means of Modbus protocol
CALCULATED FUNCTION	NONE	NONE ▼	
ALARM ENABLED	OFF	OFF ▼	This parameter can be changed in "Alarm Configuration" page
		APPLY	

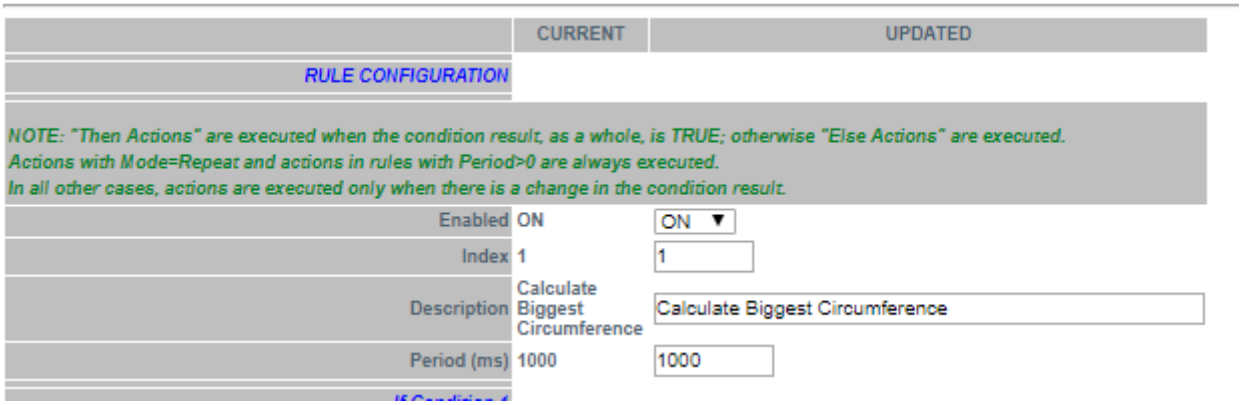
TAG 30

	CURRENT	UPDATED	
GATEWAY TAG NAME	AREA	AREA	
GATEWAY MODBUS START REGISTER ADDRESS	105	105	Equivalent to the address in the Seneca documentation : **40105**
TARGET CONNECTED TO	INTERNAL	INTERNAL ▼	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	HOLDING REGISTER ▼	
TARGET REGISTER DATA TYPE	32BIT REAL MSW	32BIT REAL MSW ▼	
GATEWAY TAG MODE	SHARED MEMORY	SHARED MEMORY ▼	
INITIAL VALUE	0	0	
HTTP POST VID	29	29	Corresponding to HTTP POST variable : **V29**
READ ONLY	OFF	OFF ▼	If READ ONLY = ON, tag value cannot be changed by means of Modbus protocol
CALCULATED FUNCTION	NONE	NONE ▼	
ALARM ENABLED	OFF	OFF ▼	This parameter can be changed in "Alarm Configuration" page
		APPLY	

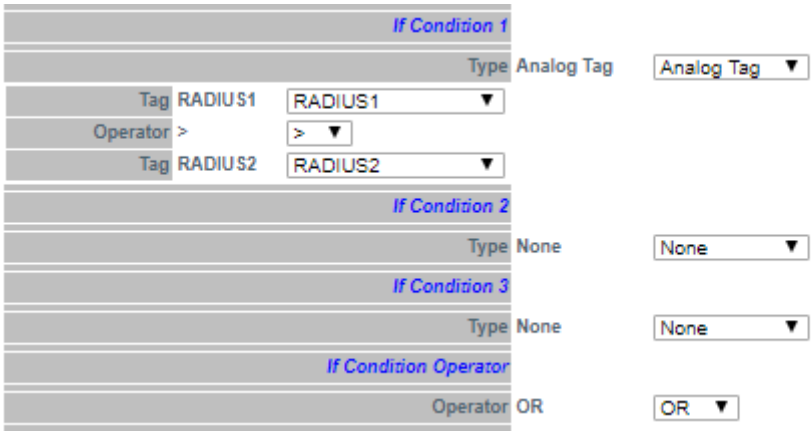
Ora fare clic su "Rules Management" e quindi su ADD per aggiungere una nuova regola:



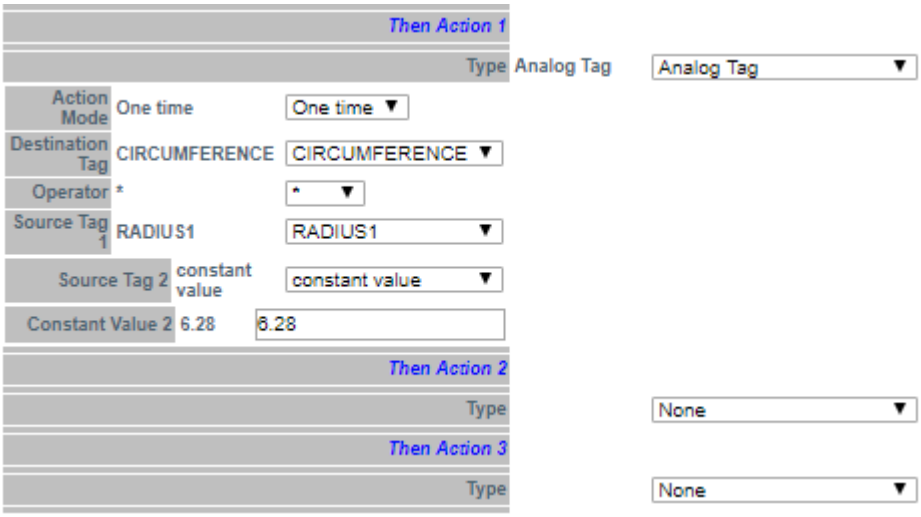
Creiamo ora la prima regola per calcolare la circonferenza utilizzando il raggio più grande tra Raggio1 e Raggio2:
Abbiamo bisogno che la regola venga eseguita ogni 1000 ms:



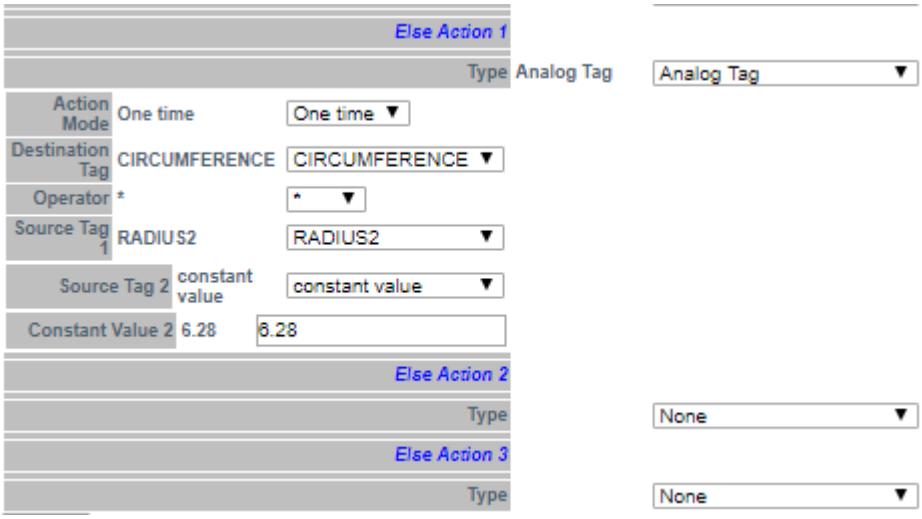
Quindi aggiungiamo la "condizione if" per stabilire quale sia il raggio più grande tra i due forniti (abbiamo bisogno solo di 1 condizione if):



Quindi, se la condizione è vera allora Raggio1> Raggio2 dobbiamo quindi calcolare la circonferenza con Raggio1, il calcolo della circonferenza sarà quindi: Circonferenza = Raggio1 * 6.28:



Altrimenti il Raggio 1 < Raggio 2 quindi dobbiamo calcolare la circonferenza con Raggio2 (Circonferenza = Raggio2 * 6.28):



Ora facciamo clic su "APPLY" per salvare la prima regola:

#	Enabled	Index	Description	Period (ms)	If condition 1		If condition 2		If condition 3	Then action 1	Then action 2	Then action 3	Else action 1	Else action 2	Else action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	OR	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	---

Allo stesso modo creiamo la Seconda Regola per calcolare l'Area con il raggio più grande:
Anche questa regola deve essere eseguita ogni 1000ms:

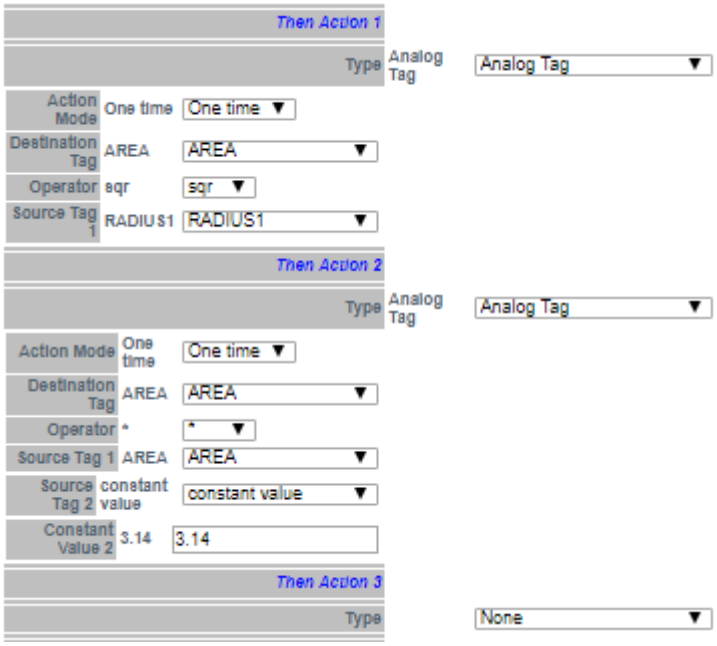
	CURRENT	UPDATED
RULE CONFIGURATION		
NOTE: "Then Actions" are executed when the condition result, as a whole, is TRUE; otherwise "Else Actions" are executed. *Actions with Mode=Repeat and actions in rules with Period>0 are always executed.* *In all other cases, actions are executed only when there is a change in the condition result.*		
Enabled	ON	ON ▼
Index	2	2
Description	Calculate Biggest Area	Calculate Biggest Area
Period (ms)	1000	1000

La "condizione if" è la stessa della prima regola:

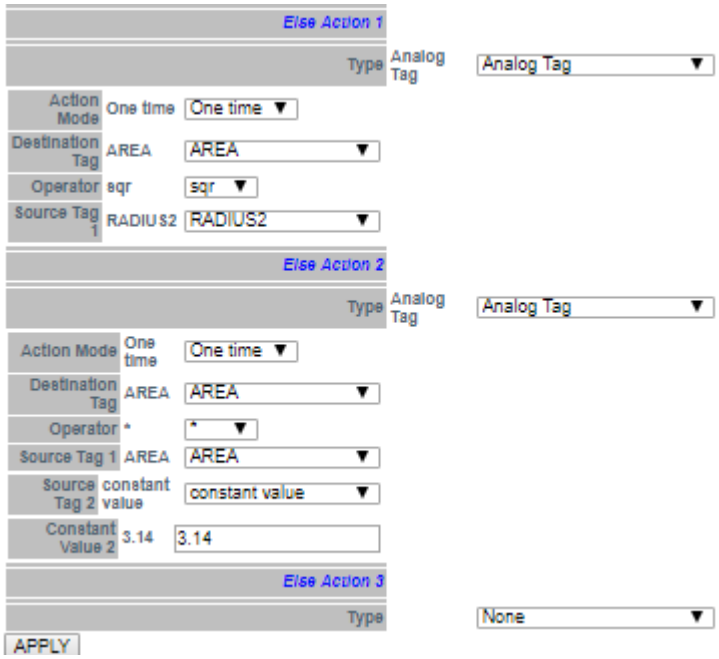
If Condition 1			
Type	Analog Tag	Analog Tag ▼	
Tag	RADIUS1	RADIUS1 ▼	
Operator	>	> ▼	
Tag	RADIUS2	RADIUS2 ▼	
If Condition 2			
Type	None	None ▼	
If Condition 3			
Type	None	None ▼	
If Condition Operator			
Operator	OR	OR ▼	

Ora dobbiamo calcolare l'AREA utilizzando il seguente calcolo:
AREA = ([RAGGIO] ^ 2) * 3.14
Dobbiamo spezzare la formula in due fasi:
Nella prima fase calcoliamo:
AREA = (RAGGIO1) ^ 2
E nel secondo:
AREA = AREA * 3.14

Quindi, nella nostra regola se RADIUS1> RADIUS2 calcoliamo AREA con RADIUS1 utilizzando la funzione quadrato (sqr):
AREA = sqr (RADIUS1)
E poi
AREA = AREA * 3.14



Quindi se RADIUS1 <RADIUS2 calcoliamo AREA con RADIUS2:

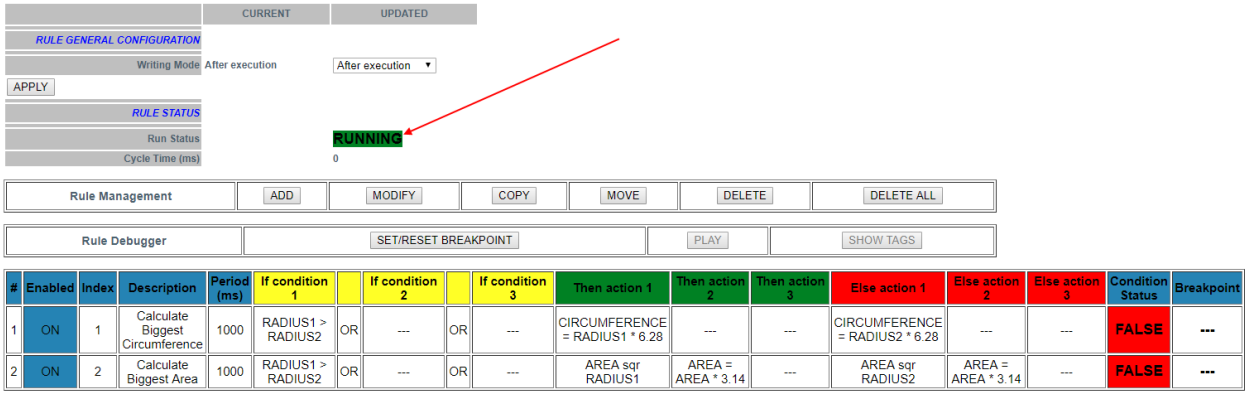


Ora facciamo clic su "APPLY" per salvare anche la seconda regola:

#	Enabled	Index	Description	Period (ms)	If condition 1		If condition 2		If condition 3	Then action 1	Then action 2	Then action 3	Else action 1	Else action 2	Else action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	OR	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	---
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	OR	---	OR	---	AREA sqr RADIUS1	AREA = AREA * 3.14	---	AREA sqr RADIUS2	AREA = AREA * 3.14	---	FALSE	---

Ora possiamo testare il funzionamento del nostro programma:

Quando viene aggiunta una regola, la regola si avvia automaticamente (RUNNING):



	CURRENT	UPDATED
RULE GENERAL CONFIGURATION		
Writing Mode	After execution	After execution
APPLY		
RULE STATUS		
Run Status		RUNNING
Cycle Time (ms)		0

Rule Management	ADD	MODIFY	COPY	MOVE	DELETE	DELETE ALL

Rule Debugger	SET/RESET BREAKPOINT	PLAY	SHOW TAGS

#	Enabled	Index	Description	Period (ms)	If condition 1		If condition 2		If condition 3	Then action 1	Then action 2	Then action 3	Else action 1	Else action 2	Else action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	OR	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	---
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	OR	---	OR	---	AREA sqr RADIUS1	AREA = AREA * 3.14	---	AREA sqr RADIUS2	AREA = AREA * 3.14	---	FALSE	---

Per testare il programma possiamo scrivere i tag RADIUS1 e RADIUS2 da Modbus RTU / MODBUS TCP-IP (registri 40100-40101 nel nostro esempio) oppure utilizzando la pagina “Tag View”:

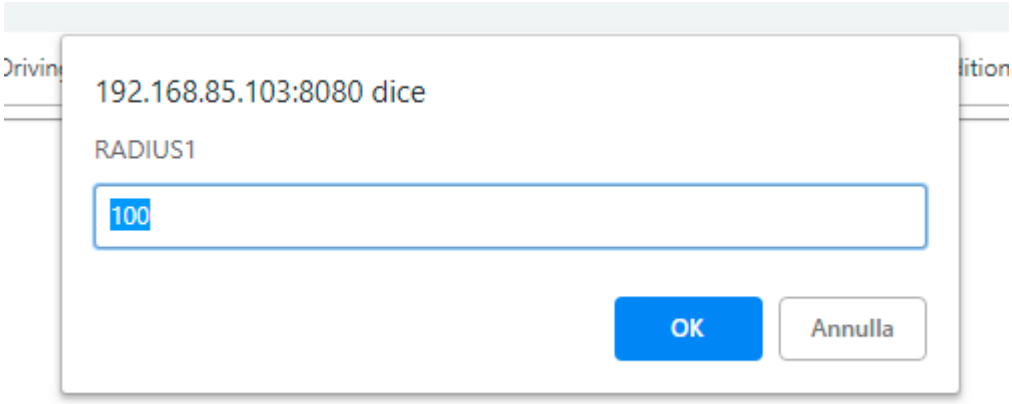
Router Configuration
Users Configuration
Mobile Configuration
Mobile Network
DDNS Configuration
Shared Memory Tag Conf.
TCP Servers
Tag Setup
Tag View
Alarms
Alarm Configuration
Alarm Summary
Alarm History
Logic Configuration
Phonebook
SMS Configuration
Email Configuration
HTTP Configuration
Message Configuration
Timer Configuration
Rule Management
Data Logger (SD found)
General Settings
SD Transfer Conf.
FTP Transfer Conf.
Group Configuration
SD File Manager
Maintenance
Ethernet Interfaces

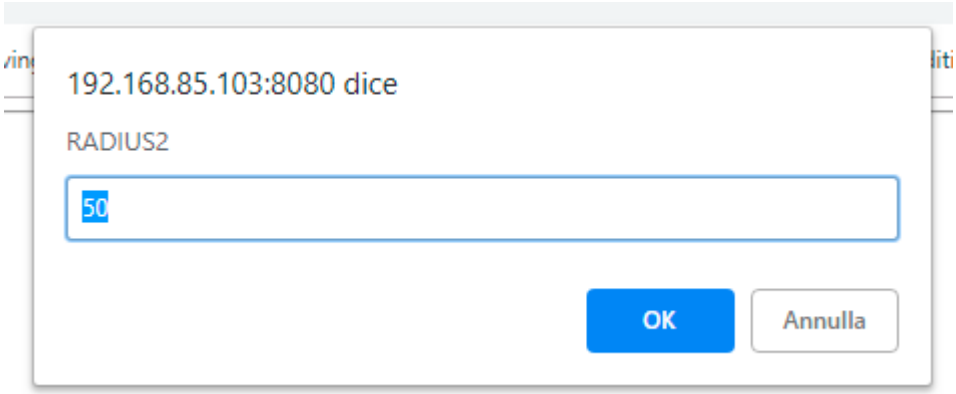
Data Logger: START STOP CLEAN CACHE

Page : 1/20 PREVIOUS PAGE NEXT PAGE

17	GPS_YEAR	16	HOLDING REGISTER	16BIT UNSIGNED	0	-	---	NONE	NONE	
18	GPS_LATITUDE	17	HOLDING REGISTER	64BIT REAL	0	-	---	NONE	NONE	
19	GPS_LONGITUDE	21	HOLDING REGISTER	64BIT REAL	0	-	---	NONE	NONE	
20	GPS_HDOP	25	HOLDING REGISTER	64BIT REAL	0	-	---	NONE	NONE	
21	GPS_ALTITUDE	29	HOLDING REGISTER	64BIT REAL	0	-	---	NONE	NONE	
22	GPS_COG	33	HOLDING REGISTER	64BIT REAL	0	-	---	NONE	NONE	
23	GPS_SPEED_KM	37	HOLDING REGISTER	64BIT REAL	0	-	---	NONE	NONE	
24	GPS_SPEED_KN	41	HOLDING REGISTER	64BIT REAL	0	-	---	NONE	NONE	
25	GPS_FIX	45	HOLDING REGISTER	16BIT UNSIGNED	0	-	---	NONE	NONE	
26	GPS_NUM_SAT	46	HOLDING REGISTER	16BIT UNSIGNED	0	-	---	NONE	NONE	
27	RADIUS1	100	HOLDING REGISTER	16BIT SIGNED	0	-	07/03/2019 10:07:25.651279	NONE	NONE	CHANGE
28	RADIUS2	101	HOLDING REGISTER	16BIT SIGNED	0	-	07/03/2019 10:07:25.651519	NONE	NONE	CHANGE
29	CIRCUMFERENCE	103	HOLDING REGISTER	32BIT REAL MSW	0	-	07/03/2019 11:11:16.130379	NONE	NONE	CHANGE
30	AREA	105	HOLDING REGISTER	32BIT REAL MSW	0	-	07/03/2019 11:11:16.130488	NONE	NONE	CHANGE

Ora cambiamo RADIUS1 = 100 e RADIUS2 = 50 facendo clic sul pulsante "CHANGE":





Nella visualizzazione Tag vengono aggiornati i calcoli di CIRCONFERENZA e AREA:

27	RADIUS1	100	HOLDING REGISTER	16BIT SIGNED	100	-	07/03/2019 11:15:56.934313	NONE	NONE	CHANGE
28	RADIUS2	101	HOLDING REGISTER	16BIT SIGNED	50	-	07/03/2019 11:34:12.465220	NONE	NONE	CHANGE
29	CIRCUMFERENCE	103	HOLDING REGISTER	32BIT REAL MSW	628	-	07/03/2019 11:34:39.634836	NONE	NONE	CHANGE
30	AREA	105	HOLDING REGISTER	32BIT REAL MSW	31400	-	07/03/2019 11:34:39.634973	NONE	NONE	CHANGE

Ora possiamo passare alla pagina "Rules Mamagement" per visualizzare il risultato:

	CURRENT	UPDATED
RULE GENERAL CONFIGURATION		
Writing Mode	After execution	After execution
APPLY		
RULE STATUS		
Run Status		RUNNING
Cycle Time (ms)		0

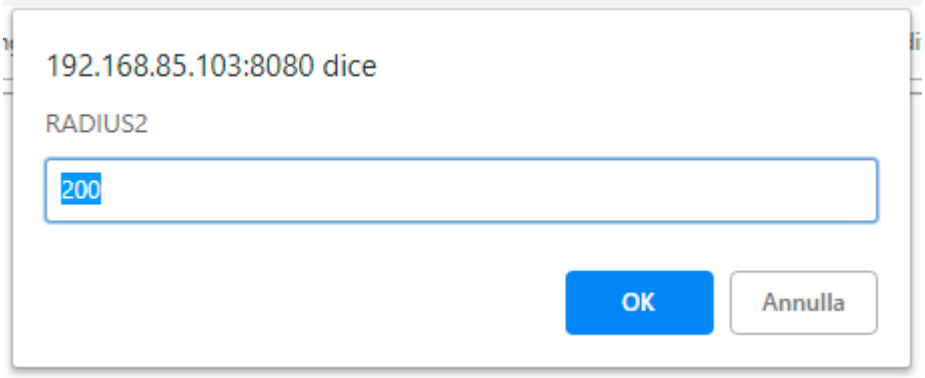
Rule Management	ADD	MODIFY	COPY	MOVE	DELETE	DELETE ALL

Rule Debugger	SET/RESET BREAKPOINT	PLAY	SHOW TAGS

#	Enabled	Index	Description	Period (ms)	If condition 1		If condition 2		If condition 3	Then action 1	Then action 2	Then action 3	Else action 1	Else action 2	Else action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	OR	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	TRUE	---
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	OR	---	OR	---	AREA sqr RADIUS1	AREA = AREA * 3.14	---	AREA sqr RADIUS2	AREA = AREA * 3.14	---	TRUE	---

Quindi entrambe le condizioni if sono TRUE (penultima colonna) e quindi vengono eseguite le “Then actions”.

Ora cambiamo a 200 il valore RADIUS2 nelle pagine di visualizzazione dei tag:



E quindi:

	CURRENT	UPDATED
RULE GENERAL CONFIGURATION		
Writing Mode	After execution	After execution
APPLY		
RULE STATUS		
Run Status		RUNNING
Cycle Time (ms)		0

Rule Management	ADD	MODIFY	COPY	MOVE	DELETE	DELETE ALL

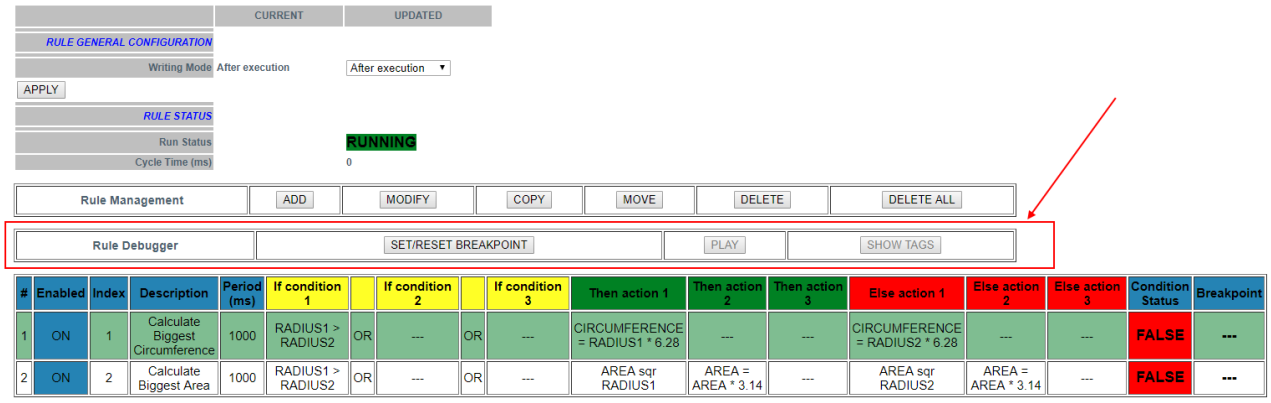
Rule Debugger	SET/RESET BREAKPOINT	PLAY	SHOW TAGS

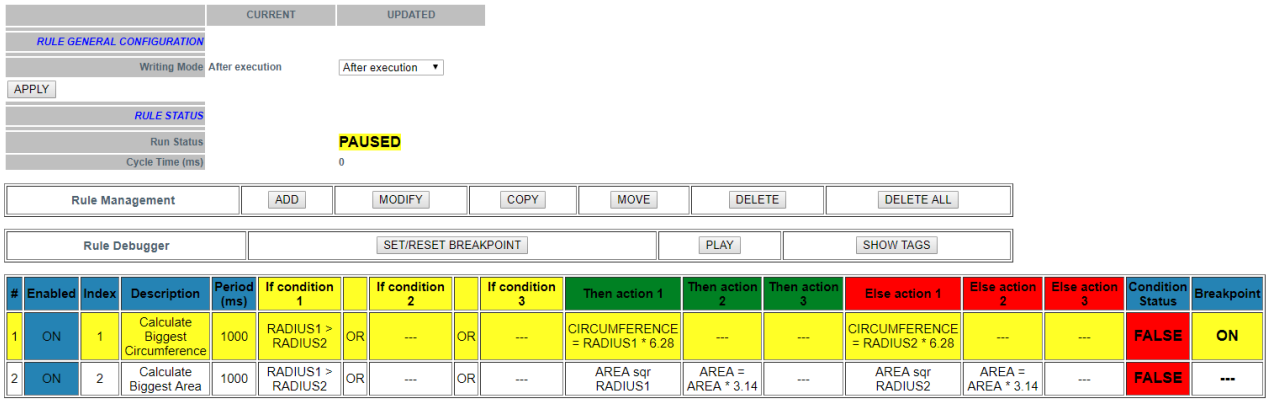
#	Enabled	Index	Description	Period (ms)	If condition 1		If condition 2		If condition 3	Then action 1	Then action 2	Then action 3	Else action 1	Else action 2	Else action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	OR	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	---
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	OR	---	OR	---	AREA sqr RADIUS1	AREA = AREA * 3.14	---	AREA sqr RADIUS2	AREA = AREA * 3.14	---	FALSE	---

Ora lo stato della condizione delle 2 regole è falso perché RADIUS1 <RADIUS2, quindi vengono eseguite le "Else Actions"

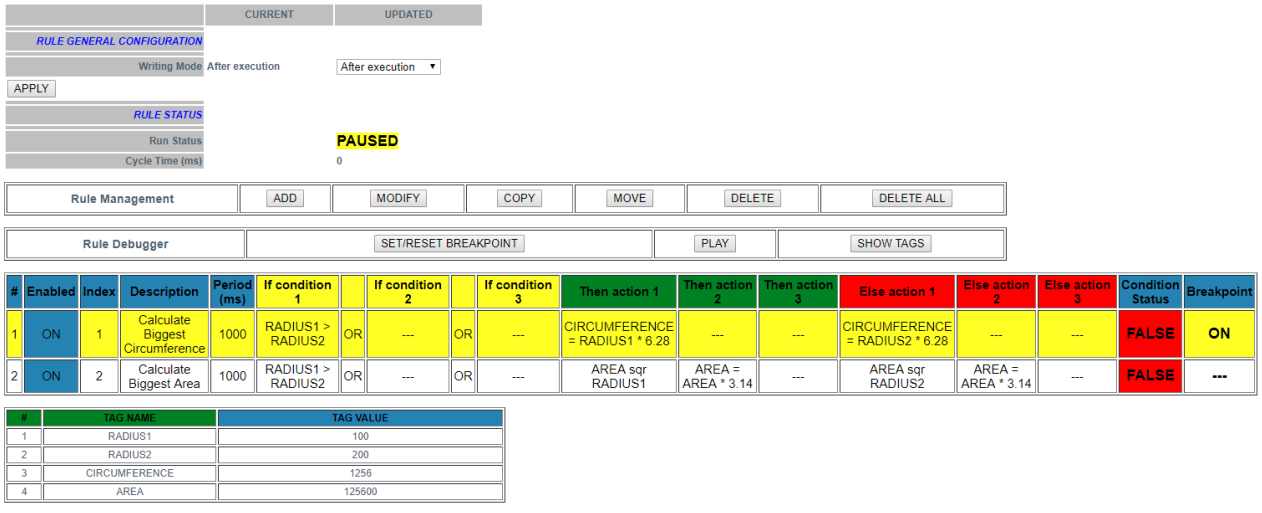
È anche possibile eseguire il debug del programma utilizzando il debugger interno delle regole.
Con il debugger interno è possibile:
-Inserire un breakpoint prima dell'esecuzione di una regola
-Visualizzare i valori dei tag prima / dopo l'esecuzione di una regola

Per aggiungere un breakpoint ed interrompere il flusso del programma selezionare la regola e quindi premere "SET / RESET BREAKPOINT":





La regola diventa gialla e lo stato della regola cambia in in “Paused". Notare che il breakpoint è prima dell'esecuzione della regola.
Facendo clic su "Show tag" vengono visualizzati i valori dei tag prima dell’esecuzione della regola selezionata.



Ora è possibile spostare il breakpoint sulla regola seguente, selezionare quindi la regola successiva e premere il pulsante "SET / RESET BREAKPOINT":
Premendo il pulsante “PLAY” l’esecuzione si fermerà prima dell’esecuzione della successiva regola:

	CURRENT	UPDATED
RULE GENERAL CONFIGURATION		
Writing Mode	After execution	After execution
APPLY		
RULE STATUS		
Run Status		PAUSED
Cycle Time (ms)		0

Rule Management	ADD	MODIFY	COPY	MOVE	DELETE	DELETE ALL

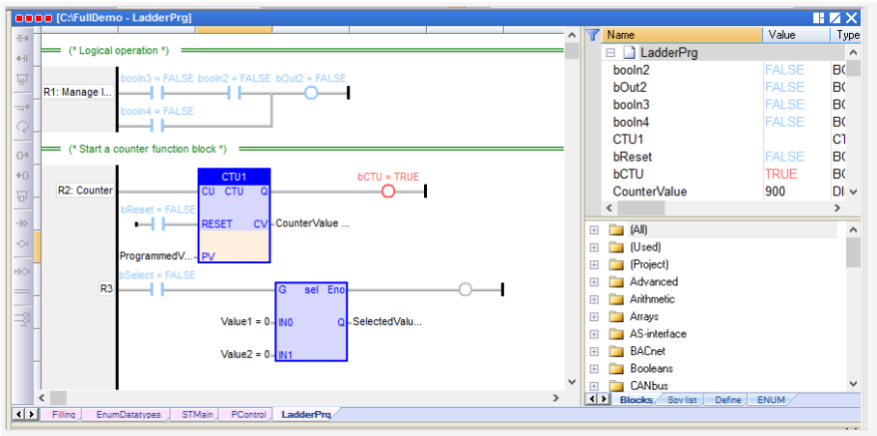
Rule Debugger	SET/RESET BREAKPOINT	PLAY	SHOW TAGS

#	Enabled	Index	Description	Period (ms)	If condition 1		If condition 2		If condition 3	Then action 1	Then action 2	Then action 3	Else action 1	Else action 2	Else action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	OR	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	---
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	OR	---	OR	---	AREA sqr RADIUS1	AREA = AREA * 3.14	---	AREA sqr RADIUS2	AREA = AREA * 3.14	---	FALSE	ON

#	TAG NAME	TAG VALUE
1	RADIUS1	100
2	RADIUS2	200
3	CIRCUMFERENCE	1256
4	AREA	125600

13. IL PLC STRATON

Il PLC Straton fornisce il supporto completo per lo standard PLC IEC 61131-3, un ambiente di sviluppo integrato (IDE) è disponibile per PC Windows™.
Lo Straton IDE include diversi strumenti come: uno strumento di configurazione del bus di campo, un editor di segnali analogici e editor di programma conformi ai cinque linguaggi della norma IEC 61131-3: Sequential Function Chart (SFC), Function Block Diagram (FBD), Ladder Diagram (LD), Testo strutturato (ST), Elenco istruzioni (IL).
Con Straton IDE, è semplice scrivere, scaricare ed eseguire il debug del codice IEC 61131-3.



A seconda del modello il dispositivo può avere o no attivato di default il PLC. Contattando Seneca è sempre possibile attivare il PLC inserendo un codice di attivazione.
Il PLC gestisce direttamente i seguenti protocolli: Modbus RTU, Modbus TCP-IP, MQTT, OPC-UA Client, MeterBus (MBUS), S7 Client, SNMP.

Per l'utilizzo del protocollo MeterBus è necessario acquistare il dispositivo opzionale Z-MBUS

Per maggiori informazioni fare riferimento al manuale del PLC STRATON.

https://straton-plc.com/en/downloads/

Per consentire allo sviluppatore PLC di creare facilmente applicazioni Straton per i gateway Seneca, sono disponibili le seguenti librerie:

• una libreria Function Block (FB) e Functions, che fornisce alcune funzionalità di uso frequente, in particolare relative alle attività di comunicazione e trasferimento dati, compilate nel firmware della CPU; l'uso diretto di questi FB e funzioni è rivolto a sviluppatori PLC esperti (una descrizione dettagliata degli FB e delle funzioni è data nell'apposito capitolo del seguente manuale);
• una libreria "Profiles", che consente l'accesso agli I/O della CPU tramite variabili "profilate"
• una libreria "User Defined Function Block" (UDFB), in linguaggio ST, che semplifica l'utilizzo dei suddetti FB, fornendo un accesso più semplice e di "livello superiore" alle loro funzionalità.

È disponibile un programma di installazione, chiamato "Seneca Straton Package", che installa automaticamente le librerie e i template Seneca. Il programma di installazione include anche Straton IDE e altri tool.
Il programma di installazione è disponibile al seguente link:

http://www.seneca.it/products/seneca-straton-package

Se, per qualche motivo, non è possibile eseguire il programma di installazione, le librerie e i modelli di cui sopra possono essere installati anche manualmente.

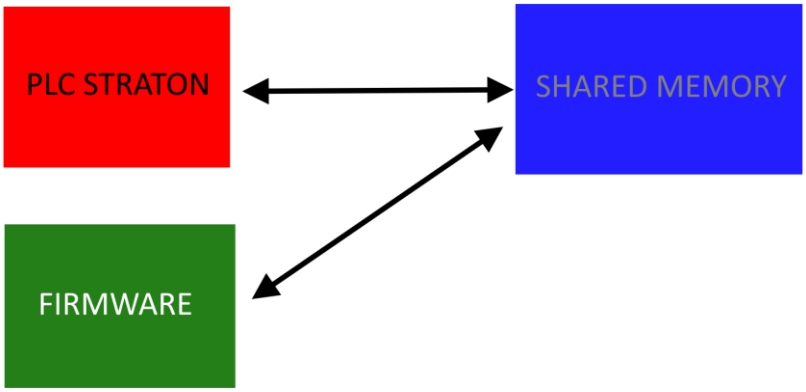
Il PLC Straton nei gateway Seneca può funzionare nelle seguenti modalità:

MODALITA' "NONE"
Il PLC Straton è disabilitato (modalità di default per i modelli SSD, Z-PASS1-RT, Z-PASS2-RT-4G, R-PASS)

MODALITA' "LEGACY (STAND-ALONE)"
Il PLC Straton funziona in modalità compatibile con le versioni di firmware precedenti alla 3000, ovvero i protocolli di comunicazione sono gestiti solo dal PLC (modalità di default per i modelli SSD-S, Z-TWS4-RT-S, Z-PASS2-RT-4G-S, R-PASS-S).

MODALITA' "SHARED"

Il PLC Straton funziona in modalità shared, ovvero il PLC Straton e il firmware comunicano tra loro tramite una memoria condivisa su protocollo OPC-UA.



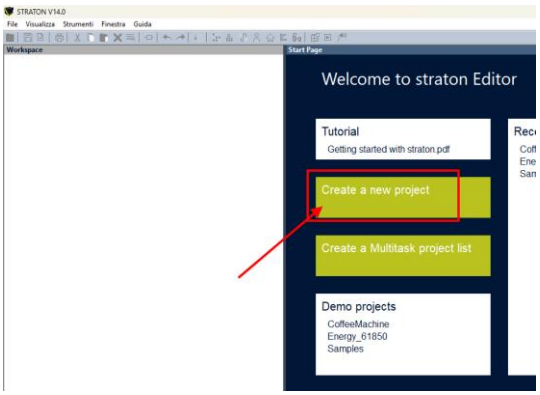
In questa modalità è possibile attivare il datalogger gli allarmi, il display / display virtuale e i protocolli di comunicazione già presenti nel firmware e di leggere e scrivere i TAG direttamente dal PLC.

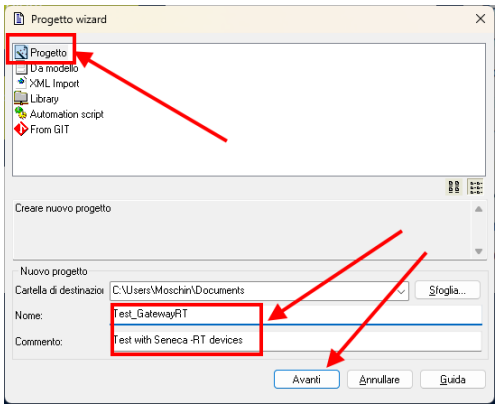
13.1. IMPORTARE I TAG NEL PLC (PLC MODE = SHARED)

In questo capitolo vedremo come:

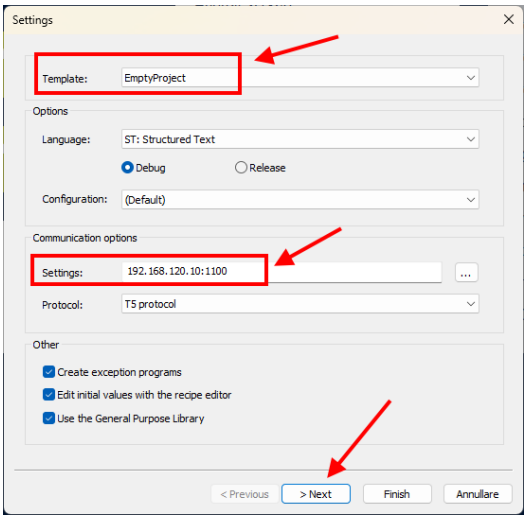
- Creare un nuovo progetto PLC Straton
- Importare Tag scritti dal firmware del Gateway sul PLC per poterli leggere
- Creare Tag scritti da Straton e poterli leggere nel firmware del gateway (ad esempio per essere visualizzati su sinottici del display / display virtuale).

Eseguire l'IDE Straton e creare un nuovo progetto:

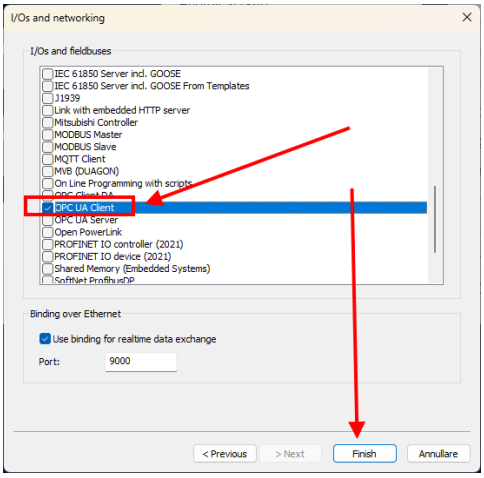




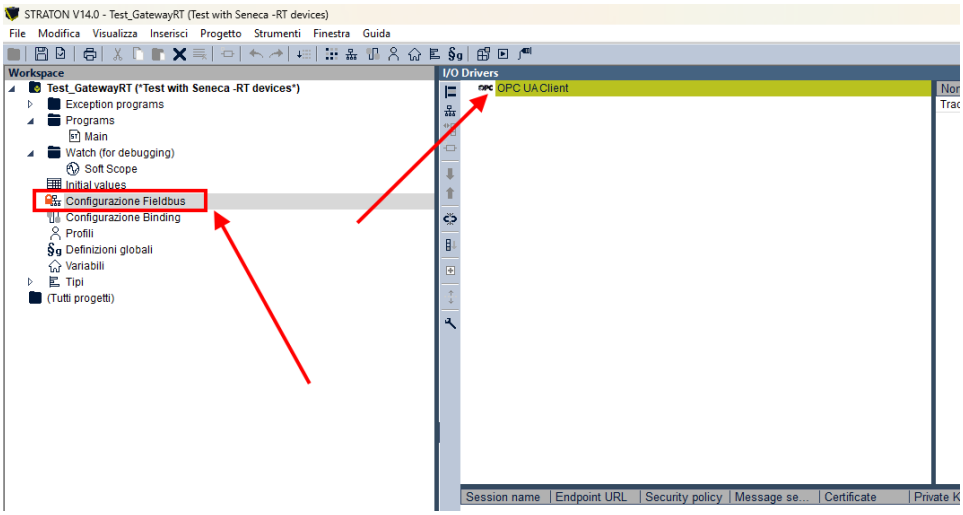
Partiamo da un progetto vuoto e inseriamo l'indirizzo IP del gateway (nell'esempio 192.168.120.10):



Come fildbus interno per lo scambio dei tag viene utilizzato OPC-UA quindi lo andiamo a selezionare e premiamo su finish:

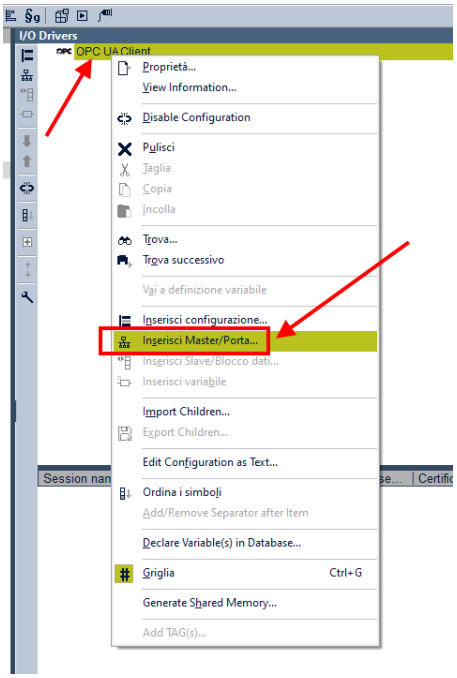


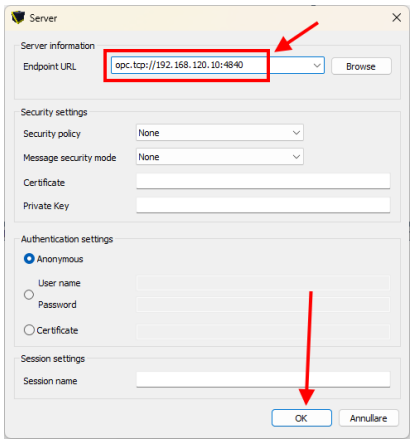
A questo punto nella configurazione fieldbus avremo nell' IDE l'OPC-UA client:



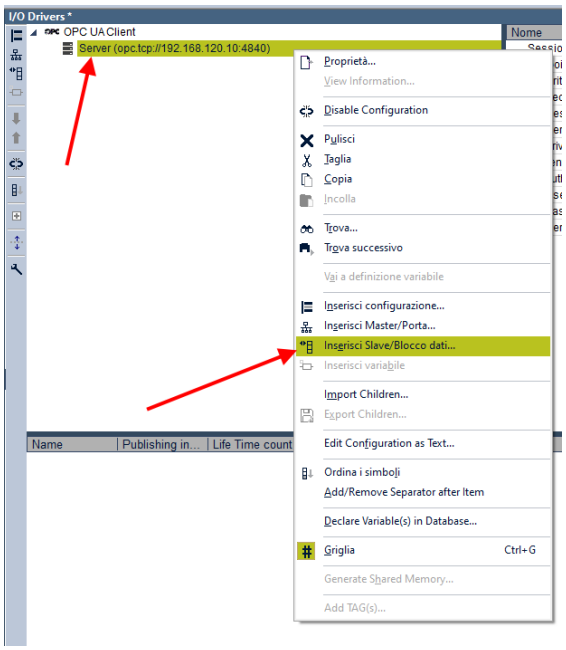
Ora importeremo i TAG definiti nel gateway per essere importati in Straton.
L'importazione avviene semplicemente eseguendo uno scan dei TAG.

Per prima cosa inseriamo il master OPC-UA e come indirizzo del server l'indirizzo del Gateway (nel nostro caso 192.168.120.10):

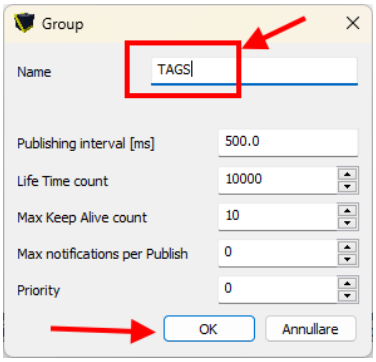




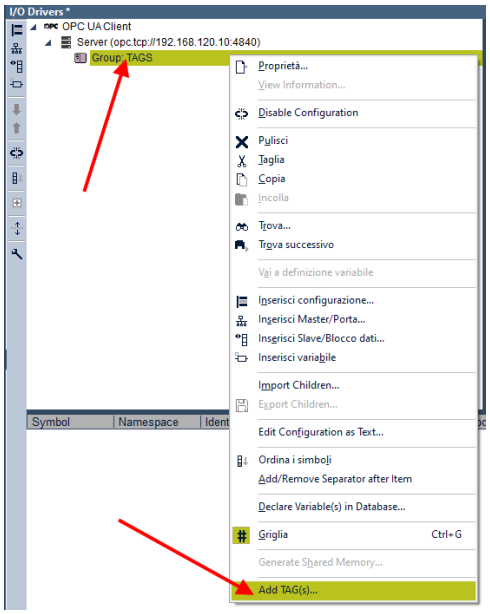
A questo punto prepariamo il blocco dati dove saranno inseriti i TAG:



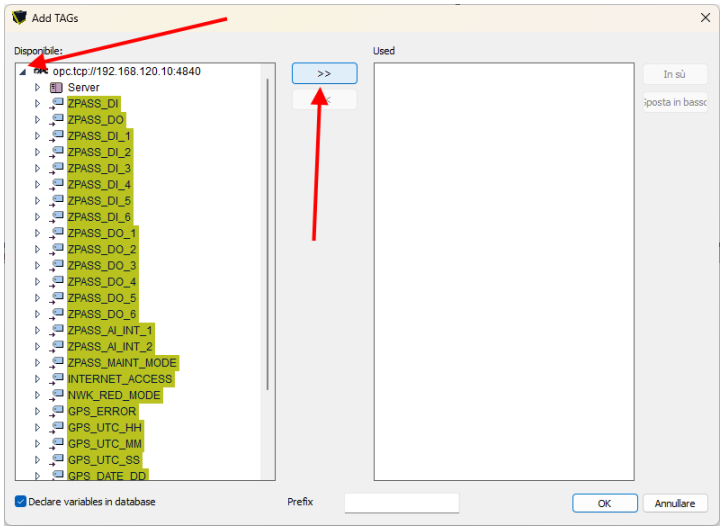
E chiamiamo il gruppo di dati con un nome a piacere, nel nostro caso TAGS:

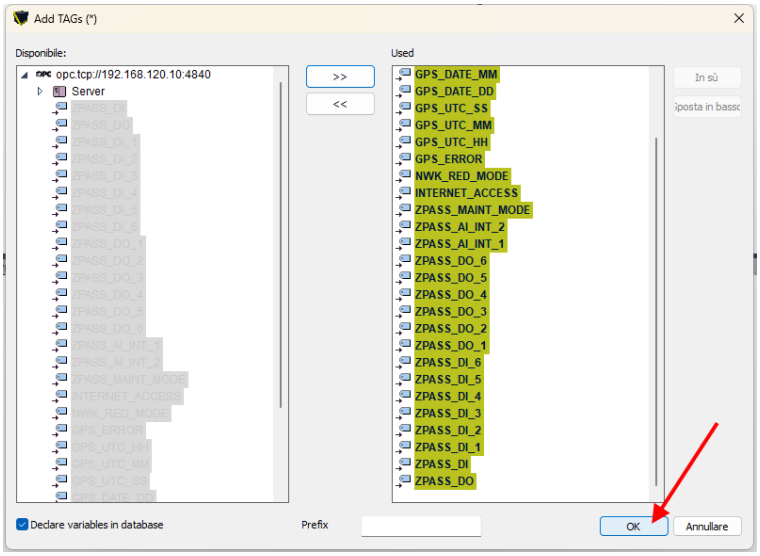


Ora siamo pronti ad importare i TAG facendo click su Add TAGS:

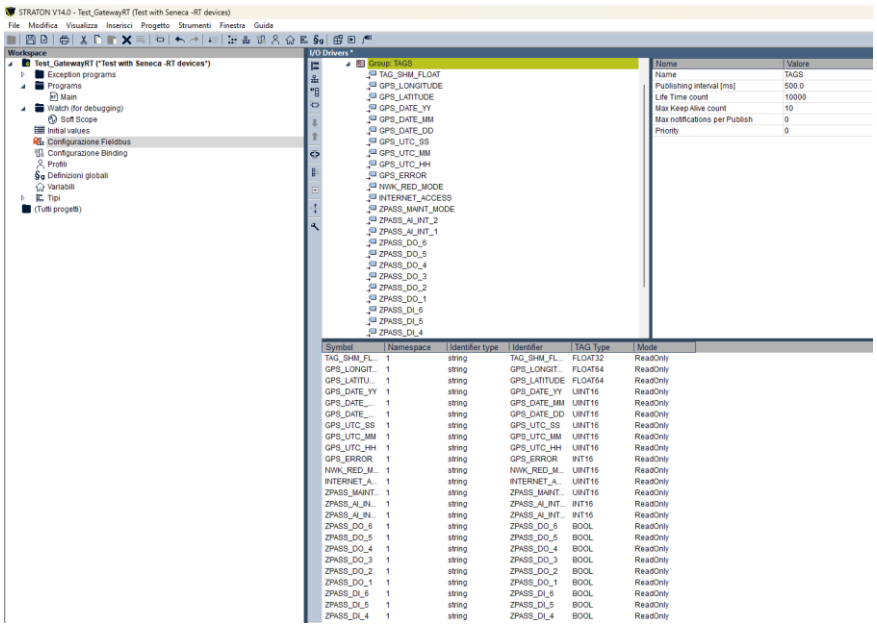


L'operazione elenca tutti i tag definiti dal gateway (compresi i Tag di tipo embedded).
Per importarli in Straton premere l'icona >>:

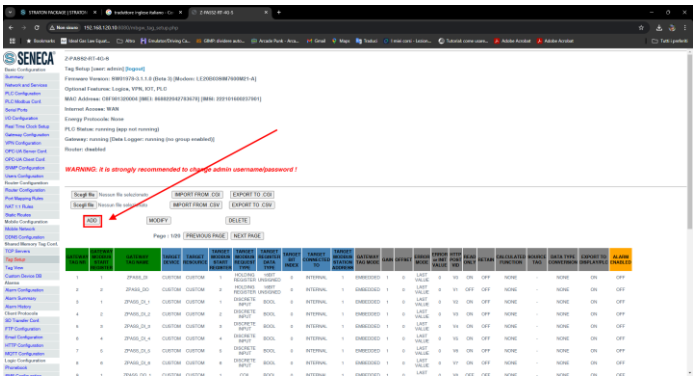


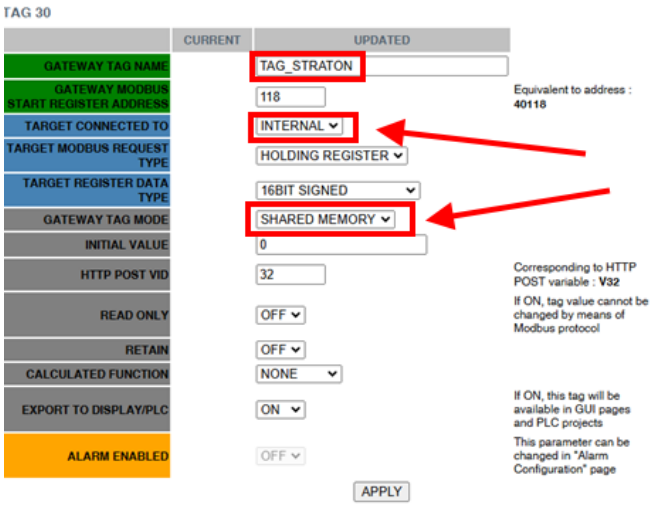


A questo punto i TAG sono importati nel PLC, si noti come tutti siano impostati di default come ReadOnly:



Se vogliamo creare un tag scrivibile da Straton e visualizzabile ad esempio sul display fisico o virtuale dobbiamo prima creare un TAG di tipo “internal” in “shared memory” e abilitare l’export su Display/PLC:

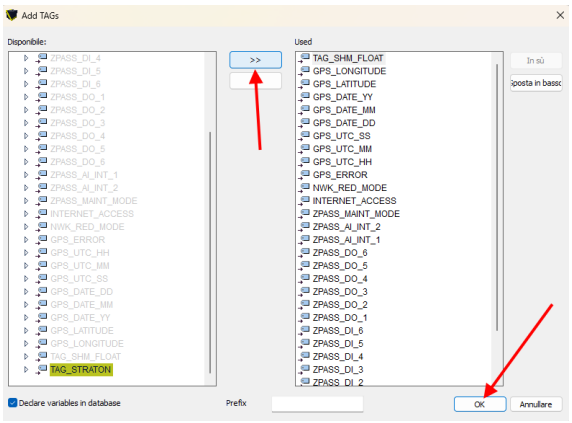




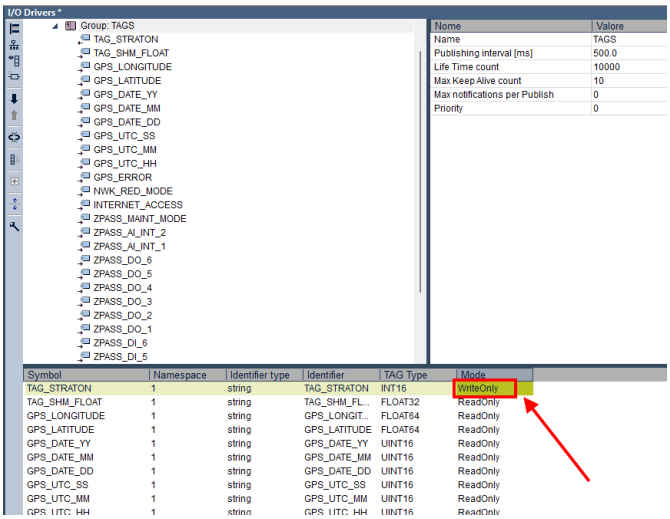
Nella pagina di Tag view compare il nuovo tag.

30	118	TAG_STRATON	-	-	-	HOLDING REGISTER	16BIT SIGNED	0	INTERNAL	-	SHARED-MEMORY	1	0	ERROR VALUE	0	V32	OFF	OFF	NONE	-	NONE	ON	OFF

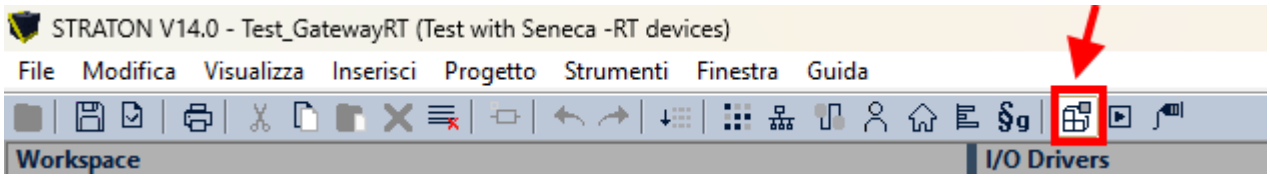
Ora torniamo in Straton e importiamo il nuovo tag con l'opzione "Add Tags":



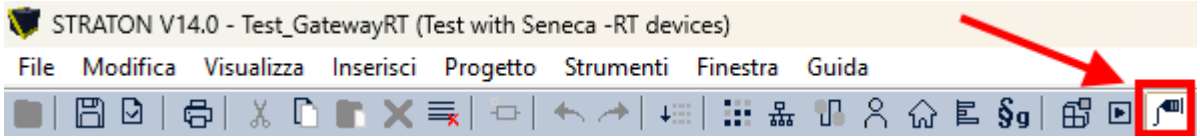
Poiché vogliamo scrivere il Tag da Straton lo impostiamo in scrittura:



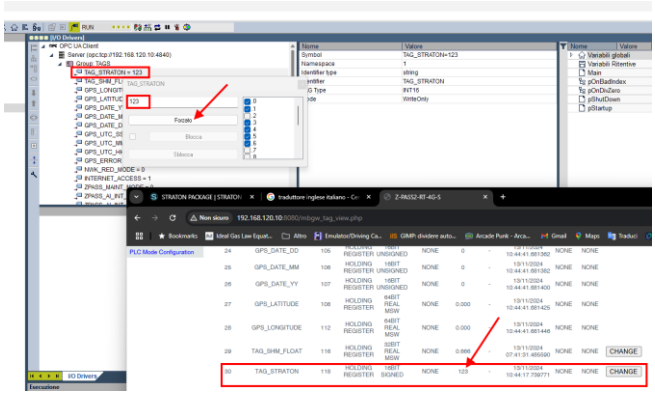
Compiliamo:



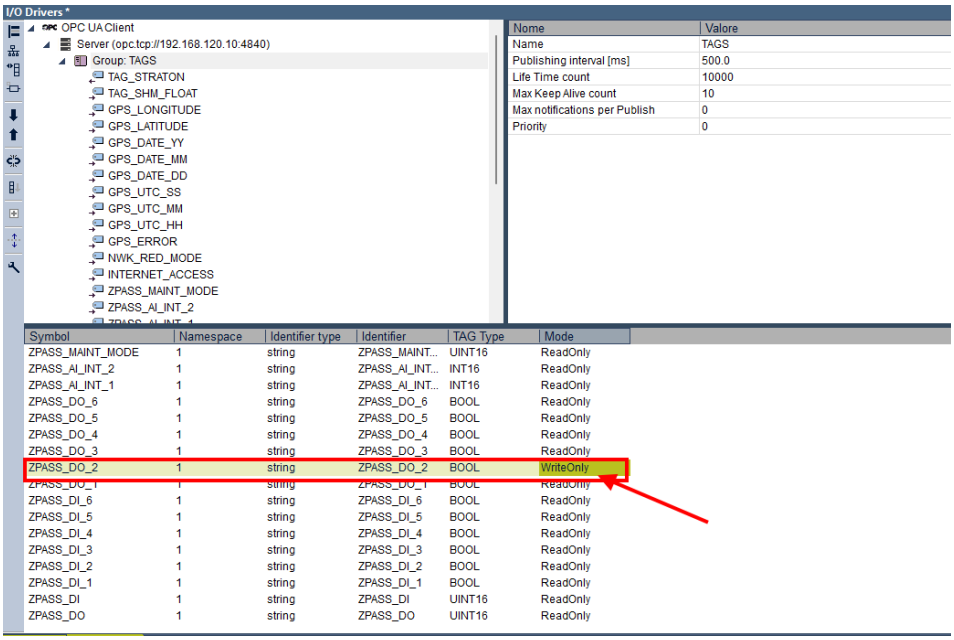
E inviamo il Progetto al target:



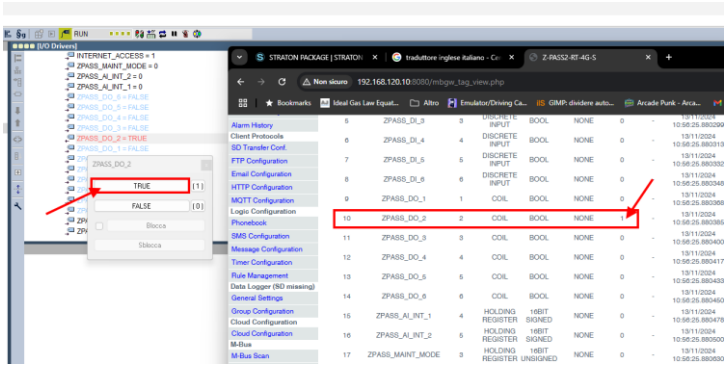
Ora se il TAG viene scritto da Straton vediamo l'effetto sul tag view del webserver:



Ora scriviamo un I/O embedded da Straton, modifichiamo il TAG ad esempio del DO2 in WriteOnly:



Compiliamo e inviamo il progetto.
Se forziamo il TAG da Straton vediamo l'effetto sulla pagina web (e sul led del dispositivo):



Attenzione che questo TAG è in sola scrittura su Straton quindi non è possibile scriverlo ad esempio da regole logiche.

14. ESECUZIONE DI SCIPT NELLE REGOLE LOGICHE

I dispositivi permettono di eseguire degli script come azione Then/Else nelle regole logiche.

ATTENZIONE!

Gli script sono uno strumento molto potente e come tale possono modificare il buon funzionamento del dispositivo. E' responsabilità dell'utente verificare che ciò non accada. È necessario verificare,

inoltre, che lo script non permetta di modificare la cybersicurezza del dispositivo ad esempio aprendo socket non prevesti.

14.1. Leggere e scrivere un Tag da script

La lettura e la scrittura di un tag da uno script sono eseguite tramite i comandi:
“tag_read” e “tag_write”.

14.1.1. Tag_read

Tramite il comando tag_read è possibile accedere in lettura al valore di un tag.
La sintassi è la seguente:

tag_read <tag_name>

ritorna:

<res>;<tag_value>;<is_valid>

Dove:
<res>
Può valere:

0: success
-1: invalid argument
-2: operation failed

<tag_value>
È il valore del tag in formato stringa

<is_valid>
0: il valore del tag è in fail
1: il valore del tag è valido

esempio:

tag_read TAG_SHM_CNT

ritorna:

0;172;1

Significa che il tag esiste, il valore del tag è 172 ed il tag non è in fail

14.1.2.Tag_write

Tramite il comando tag_write è possibile scrivere un tag.
La sintassi è la seguente:

tag_write <tag_name> <tag_value>

ritorna:

<res>
0: success
-1: invalid arguments
-2: operation failed

Esempio:

tag_write TAG_SHM_CNT 173

ritorna
0

Significa che il tag esiste, l'operazione di scrittura è stata eseguita con successo.

14.2. ESEMPIO DI UNO SCRIPT IN PYTHON

Il Seguente script legge il valore del tag "TAG_SHM_CNT" lo incrementa di 1 e riscrive nello stesso tag il nuovo valore. Per maggiori informazioni fare riferimento al link:
https://www.w3schools.com/python/python_intro.asp

```
from subprocess import run

tag_read_prog  = "/disk/bin/tag_read"
tag_write_prog = "/disk/bin/tag_write"

tag_name="TAG_SHM_CNT"

read_cmd = tag_read_prog + " " + tag_name
data = run(read_cmd, capture_output=True, shell=True, text=True) #read the tag
out_str = data.stdout
res_str = out_str.rstrip() # strip strailing newline character
```

```
res = res_str.split(";")
if res[0] == "0":
        print("tag_read success !")
        print("tag_value: " + res[1])
        print("tag_valid: " + res[2])
        val = int(res[1])
        read_ok = True
else:
        print("tag_read failure !")
        read_ok = False

if read_ok == True:
        new_val = val + 1 # increment by 1
        write_cmd = tag_write_prog + " " + tag_name + " " + str(new_val)
        data = run(write_cmd, capture_output=True, shell=True, text=True) #write the tag
        out_str = data.stdout
        res = out_str.strip() # strip strailing newline character
        if res == "0":
                print("tag_write success !")
        else:
                print("tag_write failure !")
```

14.3. MODULI PYTHON INSTALLATI

```
__future__          _threading_local    grp             secrets
_abc                _tracemalloc        gzip            select
_ast                _uuid               hashlib         selectors
_asyncio            _warnings           heapq           shelve
_bisect             _weakref            hmac            shlex
_blake2             _weakrefset         html            shutil
_bootlocale         _xxtestfuzz         http            signal
_bz2                abc                 idlelib         site
_codecs             aifc                imaplib         smtpd
_codecs_cn          antigravity         imghdr          smtplib
_codecs_hk          argparse            imp             sndhdr
_codecs_iso2022     array               importlib       socket
_codecs_jp          ast                 inspect         socketserver
_codecs_kr          asynchat            io              spwd
_codecs_tw          asyncio             ipaddress       sqlite3
_collections        asyncore            itertools       sre_compile
```

_collections_abc atexit json sre_constants
_compat_pickle audioop keyword sre_parse
_compression base64 ldb ssl
_contextvars bdb lib2to3 stat
_crypt binascii linecache statistics
_csv binhex locale string
_ctypes bisect logging stringprep
_ctypes_test builtins lzma struct
_curses bz2 macpath subprocess
_curses_panel cProfile mailbox sunau
_datetime calendar mailcap symbol
_dbm cgi marshal symtable
_decimal cgitb math sys
_dummy_thread chunk mimetypes sysconfig
_elementtree cmath mmap syslog
_functools cmd modulefinder tabnanny
_hashlib code multiprocessing talloc
_heapq codecs netrc tarfile
_imp codeop nis tdb
_io collections nntplib telnetlib
_json colorsys ntpath tempfile
_ldb_text compileall nturl2path termios
_locale concurrent numbers textwrap
_lsprof configparser opcode this
_lzma contextlib operator threading
_markupbase contextvars optparse time
_md5 copy os timeit
_multibytecodec copyreg ossaudiodev tkinter
_multiprocessing crypt parser token
_opcode csv pathlib tokenize
_operator ctypes pdb trace
_osx_support curses pickle traceback
_pickle dataclasses pickletools tracemalloc
_posixsubprocess datetime pipes tty
_py_abc dbm pkgutil turtle
_pydecimal decimal platform turtledemo
_pyio difflib plistlib types
_queue dis poplib typing
_random distutils posix unicodedata
_sha1 doctest posixpath unittest
_sha256 dummy_threading pprint urllib
_sha3 email profile uu

_sha512 encodings pstats uuid
_signal ensurepip pty venv
_sitebuiltins enum pwd warnings
_socket errno py_compile wave
_sqlite3 faulthandler pyclbr weakref
_sre fcntl pydoc webbrowser
_ssl filecmp pydoc_data wsgiref
_stat fileinput pyexpat xdrlib
_string fnmatch queue xml
_strptime formatter quopri xmlrpc
_struct fractions random xxlimited
_symtable ftplib re xxsubtype
_sysconfigdata_m_linux_arm-linux-gnueabi functools readline
zipapp
_tdb_text gc reprlib zipfile
_testbuffer genericpath resource zipimport
_testcapi getopt rlcompleter zlib
_testimportmultiple getpass runpy
_testmultiphase gettext samba
_thread glob sched

15. PROTOCOLLI ENERGIA PER IL PLC STRATON

Nei dispositivi è possibile attivare (assieme al PLC Straton) altri protocolli aggiuntivi relativi alla gestione dell'energia, è possibile attivare:

IEC61850 Server
IEC61850 Client
IEC60870-5-104 Server
IEC60870-5-104 Client
IEC60870-5-101 Master
IEC60850-5-101 Slave

IEC 61850 è uno standard per la progettazione dei sistemi di automazioni per le sottostazioni elettriche. Fa parte della Commissione Elettrotecnica Internazionale.

IEC 60870 parte 5 è uno degli standard IEC 60870 che definiscono i sistemi utilizzati per il telecontrollo (controllo di supervisione e acquisizione dati) in applicazioni di ingegneria elettrica e automazione dei sistemi di alimentazione. La parte 5 fornisce un profilo di comunicazione per l'invio di messaggi di telecontrollo di base tra due sistemi, che utilizza circuiti dati permanenti collegati direttamente tra i sistemi.
Il protocollo IEC 60870-5-104 (alias IEC 104 o protocollo 104) ha una modalità di trasmissione dei dati basato su TCP/IP, Il protocollo IEC 60870-5-101 (alias IEC 101 o protocollo 101) ha una modalità di trasmissione dei dati basato su seriale.

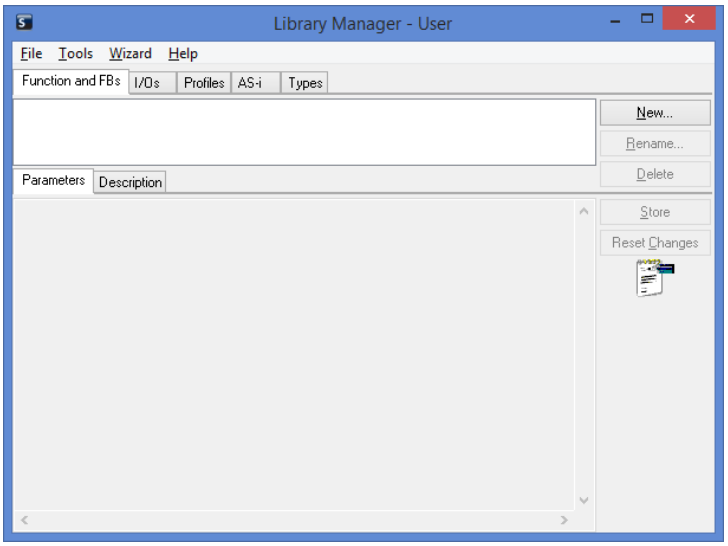
Per maggiori informazioni fare riferimento al manuale del PLC STRATON.

https://straton-plc.com/en/downloads/

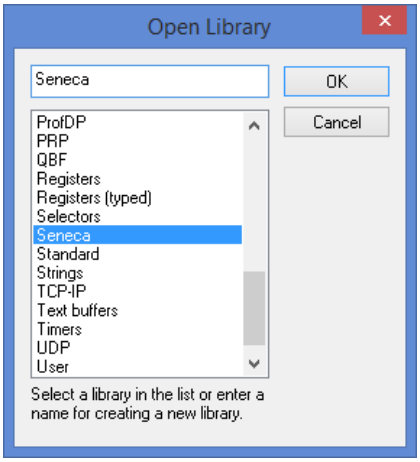
16. INSTALLAZIONE MANUALE DELLE LIBRERIE IN STRATON

I seguenti passaggi sono necessari per integrare le librerie nell'IDE Straton nel caso non si voglia utilizzare il software straton package.

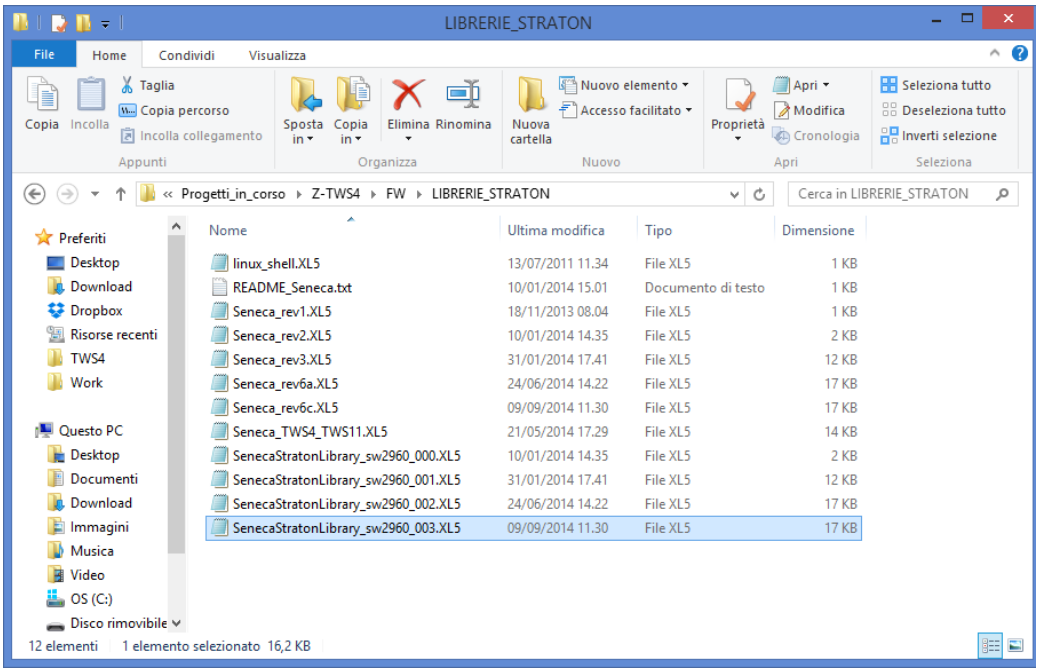
Innanzitutto, dobbiamo aggiungere la libreria FB Seneca (file SenecaStratonLibrary.XL5) all'IDE, utilizzando lo strumento "Library Manager":

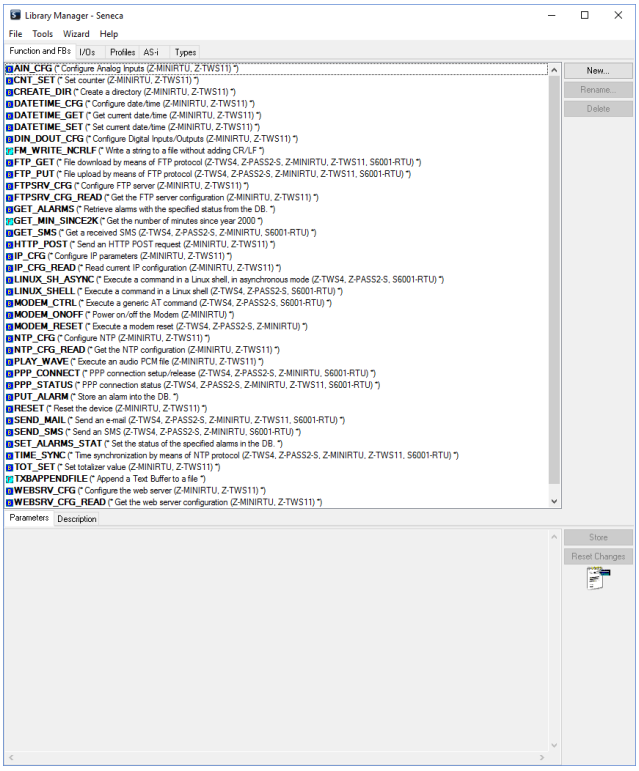


Selezionare l'opzione "File / Open Library " e inserire il nome "Seneca" per creare la nuova libreria Seneca.



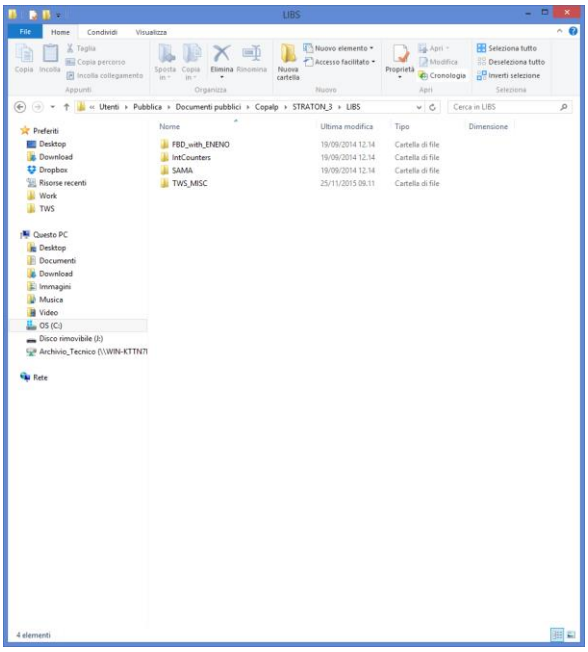
Quindi, importare la Libreria (menu “Tools / Import”):



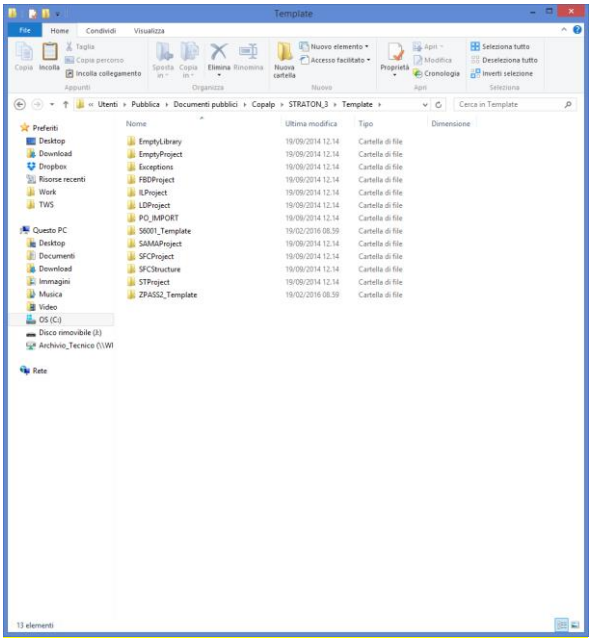


Salvare la libreria (menu “File / Save Library”).
Ora che gli FB di "basso livello" sono disponibili, dobbiamo installare la libreria UDFB.
La libreria UDFB viene fornita come file zip.

La cartella TWS_MISC, contenuta nel file zip, deve essere copiata nella seguente directory:
C:\Users\Public\Documents\CopaIp\STRATON\LIBS:



Le cartelle dei template devono essere copiate nella directory seguente:
C:\Users\Public\Documents\CopaIp\STRATON\Template



17. CYBERSECURITY

I dispositivi Gateway IIOT Seneca sono sottoposti regolarmente a severi test, da parte di aziende terze, al fine di verificare l'efficacia dei sistemi di protezione dei dati e dall'accesso non autorizzato da parte di un attaccante esterno.
Il continuo monitoraggio permette un maggiore controllo su tutti i firmware che vengono via via rilasciati.

18. SCRITTURE DA CLOUD VERSO IL DISPOSITIVO

18.1. SCRIVERE TAG DAL CLOUD AL DISPOSITIVO VIA MQTT

Tramite MQTT è possibile scrivere i TAG in due modalità fondamentali.
Nella prima nel payload non compare il nome del tag, nella seconda il nome del tag è esplicitato nel payload.

Per scrivere un tag senza esplicitare il suo nome nel payload bisogna eseguire una sottoscrizione al topic:

seneca/Z-PASS MQTT Client/info/#

Verrà poi ricevuta dal dispositivo una publish con topic:

seneca/Z-PASS MQTT Client/info/<nome tag>

e payload:

{"val": <valore tag>}

oppure

{"value": <valore tag>}

Ad esempio:

facendo la publish al topic:

seneca/Z-PASS MQTT Client/info/Pippo

con payload:

{“val”: 1234}

Si scrive il valore decimale 1234 nel Tag di nome “Pippo” (attenzione al case sensitive).

Per scrivere un tag esplicitando il nome nel payload bisogna eseguire una sottoscrizione al topic:

seneca/Z-PASS MQTT Client/info

Verrà poi ricevuta dal dispositivo una publish con topic:

seneca/Z-PASS MQTT Client/info

e payload:

{"tags": [{"<nome tag>": <valore tag>}]}

Ad esempio:

{“tags”: [{"Pippo_fp": 123.46}]}

Scrive nel tag “Pippo_fp” il valore floating point 123,46

Oppure è possibile invece che definire il nome del tag utilizzare l’ID (numero che compare nella colonna Vid dei Tag (vedi pagina web di configurazione Tag setup):

{"tags_id": [{"<(vid+1)>": <valore tag>}]}

Ad esempio:

{"tags_id": [{"25": 789}]}

Scrive nel tag con vid = 24 il valore intero decimale 789

È anche possibile scrivere più di un tag contemporaneamente con le sintassi:

{"tags": [{"<nome tag1>": <valore tag1>}, {"<nome tag2>": <valore tag2>},….] }

Oppure:

{"tags_id": [{"<(vid tag1)+1>": <valore tag1>}, {"< (vid tag2)+1>": <valore tag2>},….] }

Ad esempio:

{"tags": [{"Pippo": 1234}, {"Pippo_fp": 123.46}]}
{"tags_id": [{"25": 1234}, {"26": 123.46}]}

Scrivono entrambi i tag contemporaneamente.

18.2. INVIARE COMANDI DI AZIONE DAL CLOUD AL DISPOSITIVO VIA MQTT

Per inviare comandi al dispositivo tramite MQTT, il dispositivo deve ricevere una PUBLISH, del tipo:

seneca/Z-PASS MQTT Client/info
{"act": 1}

dove:
seneca/Z-PASS MQTT Client/info
è il valore del parametro “Subscribe Topic” della pagina del webserver di configurazione “MQTT Configuration”.

Le “azioni” possibili sono:

ACT	***COMANDO***
1	Effettua il riavvio del dispositivo
2	Fa in modo che il dispositivo vada a salvare la configurazione nell’ URL definito dal parametro “Save Configuration URL” Definito nella pagina del webserver di configurazione “MQTT Configuration”.
3	Legge la configurazione dall’ URL definito nel parametro “Load Configuration URL” Definito nella pagina del webserver di configurazione “MQTT Configuration”.
4	Scarica il firmware contenuto nell’URL definito dal parametro “FW Update URL” Definito nella pagina del webserver di configurazione “MQTT

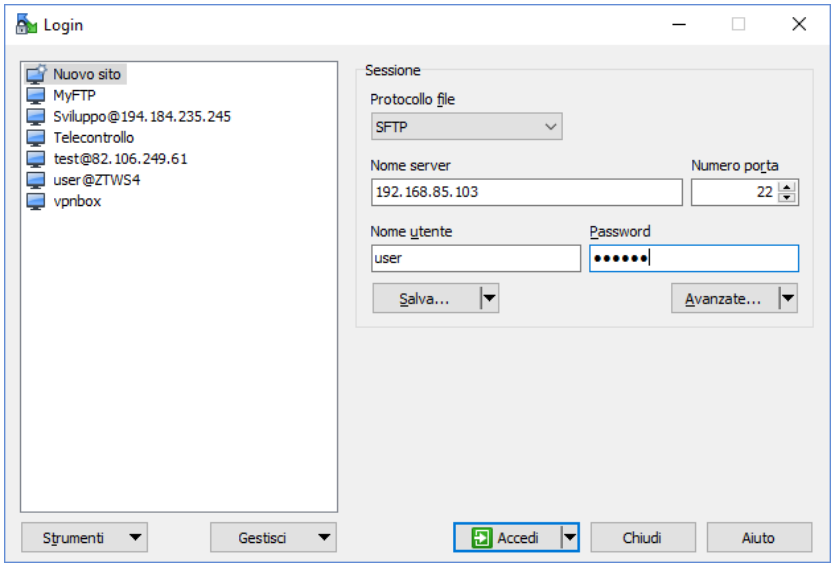
	Configuration” ed esegue l’aggiornamento.
5	Abilita la funzionalità VPN BOX 2 e attiva anche la connessione dati della rete mobile cellulare.
6	Abilita la funzionalità VPN BOX 2
7	Disabilita la funzionalità VPN BOX 2
8	Abilita la funzionalità OPEN VPN
9	Disabilita la funzionalità OPEN VPN
10	Cancella i file del Datalogger (equivale alla pressione del pulsante “Clean Cache” della pagina del webserver di configurazione “tag view”.

19. ACCESSO SFTP

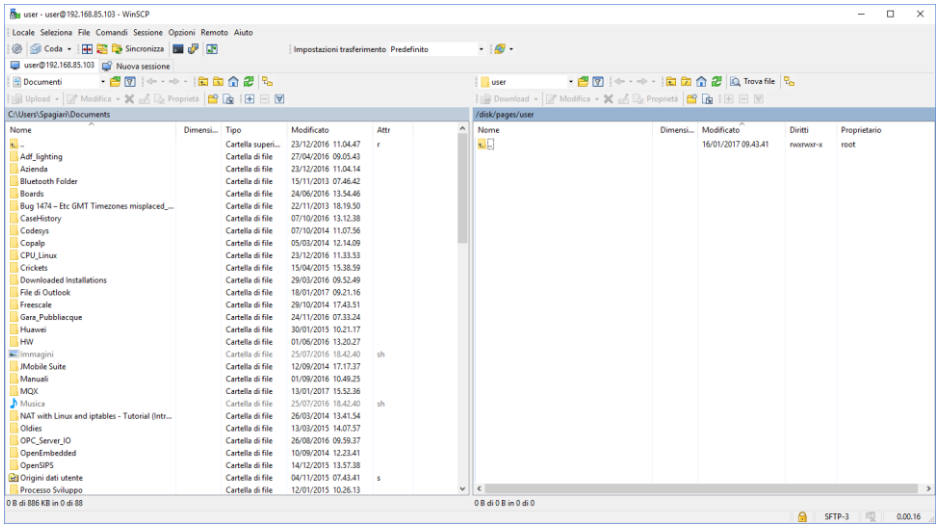
Per accedere facilmente al dispositivo tramite SFTP, è possibile utilizzare ad esempio il programma WINSCP; puoi scaricare gratuitamente WINSCP da:
http://winscp.net/eng/download.php

È necessario impostare la connessione come nella figura seguente (la schermata mostra una connessione all'indirizzo IP 192.168.85.103):

Le credenziali (username e password) sono quelle ("user", "123456") impostate per "FTP USER".
Dopo aver cliccato sul pulsante "Accedi", apparirà una nuova finestra, come nella seguente schermata; a destra è possibile copiare ed eliminare file direttamente sul / dal dispositivo.



Il programma WinSCP è utilizzato per trasferire file da / al dispositivo.



20. MAINTENANCE MODE

Tramite webserver o tramite modbus tcp-ip/RTU è possibile attivare la modalità manutenzione.
Nella modalità manutenzione i tag non sono scrivibili tramite il display fisico o virtuale ma solo tramite i protocolli (ethernet e seriali).
Per abilitare la “maintenance mode” portare ad 1 il valore del registro “Maintenance Mode”.

21. COMANDI SMS

Sui dispositivi dotati di modem mobile è possibile eseguire il controllo su una serie di funzionalità tramite gli “SMS commands”; tali funzioni includono la configurazione di una connessione dati mobili (PPP), l’attivazione della funzionalità VPN Box 2, l’impostazione di un’uscita digitale ecc.

I comandi SMS possono essere inviati attraverso i numeri di telefono presenti nella Rubrica del dispositivo come utenti “admin” o “manager”; quale alternativa, qualsiasi numero di telefono può inviare un comando SMS, a condizione che il comando contenga una “password”; la password è costituita dalle ultime quattro cifre dell’IMEI del modem; di conseguenza, il comando presenterà il seguente formato (deve esserci uno spazio vuoto tra la “password” e il testo del comando):

```
<last four IMEI digits> <command text>
```

Esempio:

```
6172 PPP ON
```

Tener presente che il testo del comando può essere scritto tutto in maiuscolo, tutto in minuscolo o con una combinazione di questi tipi di carattere.

Qualsiasi comando SMS ricevuto da un numero non riconosciuto come utente “admin” o “manager” e che non contiene la password verrà ignorato; come opzione, questi messaggi e tutti i messaggi non riconosciuti come comandi validi possono essere “relayed” all’utente “admin”.

Esempio:

```
PPP ON RELAYED
```

I comandi SMS rientrano sostanzialmente in due categorie:
i comandi “set” che eseguono un’azione
i comandi “get” che richiedono alcune informazioni
Mentre i comandi “get” hanno sempre una risposta, ai comandi “set commands” può essere fornita una risposta (“acknowledge”) o meno, a seconda del parametro di configurazione.
Qualsiasi risposta a un comando, sia esso “set” o “get”, conterrà il testo del messaggio originale oltre a una stringa di risultati, ad esempio:
“EXECUTING”

a indicare che il comando è stato elaborato correttamente; la forma “ING” viene utilizzata per indicare che la procedura avviata con il comando potrebbe non essere ancora stata completata
“FAILED”
a indicare che non è stato possibile elaborare il comando o che qualcosa non è riuscito; in questo caso è presente una stringa di errore che fornisce la ragione dell’errore

Esempi:

```
PPP ON EXECUTING (100.70.179.88)
PPP ON FAILED (System PPP ON)
```

Ovviamente, la risposta a un comando “get” contiene anche le informazioni richieste, se il comando è stato elaborato correttamente.

Esempio:

```
GET DIN EXECUTING (1,0,0,0)
```

Infine, è possibile disattivare l’intera funzionalità dei comandi SMS, se non necessaria, tramite un parametro di configurazione.
Nei paragrafi che seguono, viene fornito l'elenco completo dei comandi supportati insieme alle risposte corrispondenti.

21.1. PPP ON

Questo comando può essere utilizzato per configurare la connessione dei dati mobili (PPP); la connessione viene configurata con i parametri di configurazione del sistema (APN Mode, APN, Auth Type ecc.).
Se il comando viene elaborato correttamente, la risposta contiene l’indirizzo IP assegnato all’interfaccia di rete PPP.
Questo comando viene rifiutato nel seguente caso:

- se l’ingresso digitale “Remote Connection Disable” (RCD) è ALTO e il parametro “Security Level/Service Disable” è impostato su “Internet Connection”, il comando non verrà eseguito generando l’errore "Security Level error”.

Inoltre, se la procedura di configurazione della connessione non viene completata dopo il tempo di timeout (al momento fissato a 30 secondi), il comando non verrà eseguito generando l’errore “Timeout error”.

Tener presente che la mancata attivazione della connessione dati mobili con questo comando è di tipo permanente; di conseguenza se il dispositivo viene riavviato, la connessione dati mobili (PPP) non viene ristabilita.

Esempio:

```
→     PPP ON
```

```
←    PPP ON EXECUTING (100.70.179.88)
```

21.2. PPP OFF

Questo comando può essere utilizzato per disabilitare la connessione dei dati mobili (PPP) impostata con un precedente comando “PPP ON”.

Tener presente che questo comando non disabilita la connessione dei dati mobili in modo permanente; di conseguenza, se il dispositivo viene riavviato, la connessione di dati mobili (PPP) non viene ristabilita.

Questo comando non viene mai rifiutato.

Esempio:

```
→    PPP OFF
←    PPP OFF EXECUTING
```

21.3. PPP IP

Questo comando può essere utilizzato per ottenere l’indirizzo IP assegnato alla connessione di dati mobili (PPP); se la connessione PPP non è attiva, verrà indicato l’indirizzo IP “dummy” (0.0.0.0).

Questo comando non viene mai rifiutato.

Esempio:

```
→    PPP IP
←    PPP IP EXECUTING (100.70.179.88)
```

21.4. PPP CNF

Questo comando può essere utilizzato per modificare il valore dei parametri di configurazione del sistema relativamente alla connessione dei dati mobili (PPP); le modifiche sono permanenti.

Il comando avrà il seguente formato e i valori del parametro dovranno essere separati da uno spazio vuoto:

```
PPP CNF <APN mode> <APN> <Authentication Type> <Username> <Password> <PPP Connection Testing IP Address>
```

Tutti i parametri dovranno essere presenti nel suddetto ordine; nessun parametro può essere lasciato vuoto.

Per quanto riguarda il significato di questi parametri: <APN> e <Authentication Type> sono campi numerici con i seguenti valori:

```
APN Mode
0:    Automatic
1:    Manual

Authentication Type
0:    None
1:    CHAP/PAP
2:    CHAP only
3:    PAP only
```

Questo comando viene rifiutato nel seguente caso:

se uno dei parametri del comando manca o non è valido, il comando non verrà eseguito generando l'errore "Command parameter error".

Esempio:

```
→    PPP CNF 0 mobile.vodafone.it 0 user pass www.google.com
←    PPP CNF EXECUTING
```

21.5. VPN ON

Questo comando può essere utilizzato per attivare la funzionalità VPN Box; la funzionalità viene attivata con i parametri di configurazione del sistema (Server, Password, Nome tag).
Il comando presenta due parametri facoltativi, di conseguenza il suo formato è il seguente:
`VPN ON [PPP] [NOFWL]`[1]
"PPP"
In presenza di questo parametro, viene configurata la connessione dati mobili (PPP) (se non è già attiva), prima di attivare la funzionalità VPN Box
"NOFWL"
In presenza di questo parametro, "Mobile Network Firewall" viene disabilitato nella configurazione del sistema
Questo comando viene rifiutato nei seguenti casi:

- se la funzionalità VPN "custom" viene abilitata nella configurazione di sistema (parametro "VPN/Enable" = ON, "VPN Mode" = "OpenVPN"), il comando non verrà eseguito generando l'errore "System VPN ON";
- se l'ingresso digitale "Remote Connection Disable" (RCD) è ALTO e il parametro "Security Level/Service Disable" è impostato su VPN Connection", "VPN Service" o "Internet Connection", il comando non verrà eseguito generando l'errore "Security Level error".

Tener presente che questo comando non attiva la funzionalità VPN Box in modo permanente; di conseguenza se il dispositivo viene riavviato, la funzionalità non viene riattivata.

Esempi:

```
→    VPN ON
←    VPN ON EXECUTING

→    VPN ON PPP
←    VPN ON PPP EXECUTING

→    VPN ON NOFWL
←    VPN ON NOFWL EXECUTING

→    VPN ON PPP NOFWL
←    VPN ON PPP NOFWL EXECUTING
```

[1] Le parentesi quadre indicano che il parametro è facoltativo.

21.6. VPN OFF

Questo comando può essere utilizzato per disattivare la funzionalità VPN Box attivata con un precedente comando “VPN ON”; inoltre, disabilita la connessione dati mobili (PPP) configurata con un precedente comando “VPN ON PPP” o con il comando “PPP ON”.

Questo comando non viene mai rifiutato.

Tener presente che questo comando non disattiva la funzionalità VPN Box in modo permanente; di conseguenza se il dispositivo viene riavviato, la funzionalità viene riattivata.

Esempio:

```
→     VPN OFF
←     VPN OFF EXECUTING
```

21.7. VPN CNF

Questo comando può essere utilizzato per modificare il valore dei parametri di configurazione del sistema relativamente alla funzionalità VPN Box; le modifiche sono permanenti.

Il comando avrà il seguente formato e i valori del parametro dovranno essere separati da uno spazio vuoto:

```
VPN CNF <Server> <Password> <Tag Name>
```

Tutti i parametri dovranno essere presenti nel suddetto ordine; nessun parametro può essere lasciato vuoto.

Per quanto riguarda il significato di questi parametri.

Questo comando viene rifiutato nel seguente caso:

se uno dei parametri del comando manca o non è valido, il comando non verrà eseguito generando l'errore “Command parameter error”.

Esempio:

```
→     VPN CNF myvpnbox.seneca.it myvpnbox zpass2-GSP
←     VPN CNF EXECUTING
```

21.8. FWL ON

Questo comando può essere utilizzato per abilitare “Mobile Network Firewall” nella configurazione del sistema (parametro “Mobile Network Firewall/Enable” = ON).
Questo comando non viene mai rifiutato.

Esempio:

```
→     FWL ON
←     FWL ON EXECUTING
```

21.9. FWL OFF

Questo comando può essere utilizzato per disabilitare “Mobile Network Firewall” nella configurazione del sistema (parametro “Mobile Network Firewall/Enable” = OFF).
Questo comando non viene mai rifiutato.

Esempio:

```
→     FWL OFF
←     FWL OFF EXECUTING
```

21.10. GET DIN

Questo comando può essere utilizzato per ottenere lo stato di uno o di tutti gli ingressi digitali del dispositivo; se un ingresso digitale non è disponibile (poiché è utilizzato come uscita)[2], viene fornito il valore “0”.

Il comando può avere due formati:

`GET DIN<n>` con <n>=1..N ottiene lo stato di un singolo ingresso digitale

dove:
N=4 per R-PASS+R-COMM
N=6 per Z-PASS2-RT-4G

`GET DIN` ottiene lo stato di tutti gli ingressi digitali

Questo comando viene rifiutato nei seguenti casi:

- se il numero I/O digitale non è compreso nell’intervallo (ad esempio: 0 oppure N+1), il comando non verrà eseguito generando l’errore “Command parameter error”.

Esempi:

```
→     GET DIN
←     GET DIN EXECUTING (1,0,0,0)

→     GET DIN1
←     GET DIN1 EXECUTING (1)
```

[2] Questa condizione può essere vera per Z-PASS2-RT-4G.

```
→    GET DIN2
←    GET DIN2 EXECUTING (0)
```

21.11. GET DOUT

Questo comando può essere utilizzato per ottenere lo stato di una o di tutte le uscite digitali del dispositivo; se un'uscita digitale non è disponibile (poiché è utilizzata come ingresso)[3], viene fornito il valore "0".

Il comando può avere due formati:

`GET DOUT<n>` con <n>=1..N ottiene lo stato di una singola uscita digitale

dove:
N=4 per R-PASS+R-COMM
N=6 per Z-PASS2-RT-4G

`GET DOUT` ottiene lo stato di tutte le uscite digitali

Questo comando viene rifiutato nei seguenti casi:

- se il numero I/O digitale nel comando non è compreso nell'intervallo (ad esempio: 0 oppure N+1), il comando non verrà eseguito generando l'errore "Command parameter error".

Esempi:

```
→    GET DOUT
←    GET DOUT EXECUTING (0,1,0,0)

→    GET DOUT1
←    GET DOUT1 EXECUTING (0)

→    GET DOUT2
←    GET DOUT2 EXECUTING (1)
```

21.12. SET DOUT

Questo comando può essere utilizzato per impostare lo stato di una delle uscite digitali del dispositivo.

Il comando può avere due formati:

`SET DOUT<n>.CLOSE` with <n>=1..N imposta l'uscita digitale sullo stato ALTO

`SET DOUT<n>.OPEN` with <n>=1..N imposta l'uscita digitale sullo stato BASSO

dove:
N=4 per R-PASS+R-COMM
N=6 per Z-PASS2-RT-4G

[3] Questa condizione può essere vera per Z-PASS2-RT-4G.

Questo comando viene rifiutato nei seguenti casi:

- se l'uscita digitale non viene configurata come "General output" o l'I/O digitale viene utilizzato come ingresso[4], il comando non verrà eseguito generando l'errore "Digital I/O mode error";
- se il numero I/O digitale nel comando non è compreso nell'intervallo (ad esempio: 0 oppure N+1), il comando non verrà eseguito generando l'errore "Command parameter error";
- se lo stato richiesto non è né ".CLOSE" né ".OPEN", il comando non verrà eseguito generando l'errore "Command parameter error".

Esempio:

```
→     SET DOUT2.CLOSE
←     SET DOUT2.CLOSE EXECUTING
```

21.13. SET PULSE

Questo comando può essere utilizzato per generare un impulso su una delle uscite digitali del dispositivo.

Il comando può avere due formati:

`SET PULSE<n>.CLOSE <duration>` con <n>=1..N
dove:
N=4 per R-PASS+R-COMM
N=6 per Z-PASS2-RT-4G
per generare un impulso BASSO-ALTO-BASSO, con lo stato ALTO impostato per il numero di secondi indicato dal parametro <duration>

`SET PULSE<n>.OPEN <duration>` with <n>=1..N
dove:
N=4 per R-PASS+R-COMM
N=6 per Z-PASS2-RT-4G
per generare un impulso ALTO-BASSO-ALTO, con lo stato BASSO impostato per il numero di secondi indicato dal parametro <duration>

Questo comando viene rifiutato nei seguenti casi:

- se l'uscita digitale non viene configurata come "General output" o l'I/O digitale viene utilizzato come ingresso[5], il comando non verrà eseguito generando l'errore "Digital I/O mode error";
- se il numero I/O digitale nel comando non è compreso nell'intervallo (ad esempio: 0 oppure N+1), il comando non verrà eseguito generando l'errore "Command parameter error";
- se lo stato richiesto non è né ".CLOSE" né ".OPEN", il comando non verrà eseguito generando l'errore "Command parameter error";
- se il parametro < duration> manca o non è valido, il comando non verrà eseguito generando l'errore "Command parameter error";

[4] Questa condizione può essere vera per Z-PASS2-RT-4G.
[5] Questa condizione può essere vera per Z-PASS2-RT-4G.

- se viene indicato il parametro ".CLOSE" e l'uscita digitale è già nello stato ALTO, il comando non verrà eseguito generando l'errore "No pulse generated";
- se viene indicato il parametro ".OPEN" e l'uscita digitale è già nello stato BASSO, il comando non verrà eseguito generando l'errore "No pulse generated".

Esempio:

```
→    SET PULSE2.CLOSE 10
←    SET PULSE2.CLOSE 10 EXECUTING
```

21.14. SET USER.PHONE

Questo comando può essere utilizzato per inserire un utente con numero di telefono, tipo ed elenco gruppo specificati nella Rubrica; è possibile utilizzarlo anche per modificare il tipo e/o l'elenco del gruppo di un utente già esistente.

Il comando ha il seguente formato:

`SET USER.PHONE +<number> <type> <group list>,` with <type>=ADM|MGR|USR

Tener presente che il numero di telefono dovrà essere sempre indicato con "international format", di conseguenza il carattere iniziale '+' dovrà essere sempre presente.

"group list" è un elenco di numeri interi non negativi, separati dal carattere "-", che definisce i gruppi ai quali l'utente appartiene. Un esempio di elenchi di gruppi validi è il seguente:

"1-2-3"
"1-4"
"1"
"0"

Il valore "0" sta a indicare che l'utente non appartiene ad alcun gruppo.

Questo comando viene rifiutato nei seguenti casi:

- se il parametro <number> già esiste nella Rubrica, con <type> e <group list> specificati, il comando non verrà eseguito generando l'errore "Item already exists";
- se il parametro <number> manca o non è valido (incluso il caso in cui manchi il carattere '+'), il comando non verrà eseguito generando l'errore "Command parameter error";
- se il parametro <type> manca o non è valido, il comando non verrà eseguito generando l'errore "Command parameter error";
- se il parametro <group list> manca o non è valido, il comando non verrà eseguito generando l'errore "Command parameter error".

Esempio:

```
→    SET USER.PHONE +390123456789 ADM 1-2-3
←    SET USER.PHONE +390123456789 ADM 1-2-3 EXECUTING
```

21.15. RESET PHONE

Questo comando può essere utilizzato per eliminare dalla Rubrica un utente con il numero di telefono specificato.

Il comando ha il seguente formato:

`RESET PHONE +<number>`

Tener presente che il numero di telefono dovrà essere sempre indicato con "international format", di conseguenza il carattere iniziale '+' dovrà essere sempre presente.

Questo comando viene rifiutato nei seguenti casi:

- se il parametro <number> specificato non esiste nella Rubrica, il comando non verrà eseguito generando l'errore "Item does not exist";
- se il parametro <number> manca o non è valido (incluso il caso in cui manchi il carattere '+'), il comando non verrà eseguito generando l'errore "Command parameter error".

Esempio:

```
→    RESET PHONE +390123456789
←    RESET PHONE +390123456789 EXECUTING
```

Tener presente che se l'utente in Rubrica con il numero di telefono specificato ha anche un indirizzo e-mail anche quest'ultimo verrà eliminato tramite questo comando.

21.16. SET USER.EMAIL

Questo comando può essere utilizzato per inserire un utente con indirizzo e-mail, tipo ed elenco gruppo specificati nella Rubrica; è possibile utilizzarlo anche per modificare il tipo e/o l'elenco del gruppo di un utente già esistente.

Il comando ha il seguente formato:

`SET USER.EMAIL <email address> <type> <group list>`, with <type>=`ADM|MGR|USR`

"group list" è un elenco di numeri interi non negativi, separati dal carattere "-", che definisce i gruppi ai quali l'utente appartiene. Un esempio di elenchi di gruppi validi è il seguente:

"1-2-3"
"1-4"
"1"
"0"

Il valore "0" sta a indicare che l'utente non appartiene ad alcun gruppo.

Questo comando viene rifiutato nei seguenti casi:

- se il parametro <email address> già esiste in Rubrica, con <type> e <group list> specificati, il comando non verrà eseguito generando l'errore "Item already exists";
- se il parametro <email address> manca o non è valido, il comando non verrà eseguito generando l'errore "Command parameter error";
- se il parametro <type> manca o non è valido, il comando non verrà eseguito generando l'errore "Command parameter error";
- se il parametro <group list> manca o non è valido, il comando non verrà eseguito generando l'errore "Command parameter error".

Esempio:

```
→    SET USER.EMAIL admin@zpass.it ADM 1-2-3
←    SET USER.EMAIL admin@zpass.it ADM 1-2-3 EXECUTING
```

21.17. RESET EMAIL

Questo comando può essere utilizzato per eliminare dalla Rubrica un utente con un indirizzo e-mail specificato.

Il comando ha il seguente formato:

```
RESET EMAIL <email address>
```

Questo comando viene rifiutato nei seguenti casi:

- se il parametro <email address> specificato non esiste in Rubrica, il comando non verrà eseguito generando l'errore "Item does not exist";
- se il parametro <email address> manca o non è valido, il comando non verrà eseguito generando l'errore "Command parameter error".

Esempio:

```
→    RESET EMAIL admin@zpass.it
←    RESET EMAIL admin@zpass.it EXECUTING
```

Tener presente che se l'utente in Rubrica con l'indirizzo e-mail specificato ha anche numero di telefono anche quest'ultimo verrà eliminato tramite questo comando.

21.18. STATUS

Questo comando può essere utilizzato per ottenere dal dispositivo le informazioni sullo stato.

Le informazioni sullo stato fornite nella risposta hanno il seguente formato:

R-PASS+R-COMM:

```
R-PASS<hwrev>  <date>  <time>  RUNNING  <service status>,<vpn status>
<DI1>,<DI2>,<DI3>,<DI4>,<DO1>,<DO2>,<DO3>,<D04>
```

Z-PASS2-RT-4G:

```
Z-PASS2-RT-4G<hwrev> <date> <time> RUNNING <service status>,<vpn status> <DIDO1>,<DIDO
2>,<DIDO3>,<DIDO4>,<DIDO5>,<DIDO6>
```

dove:

<hwrev>: “”
<date> è nel formato “yyyy/mm/dd”
<hour> è nel formato “hh:mm:ss”
<service status> indica lo stato di “SRV” LED[6] (“OFF”|“ON”|”FAIL”)
<vpn status> reports the status of the “VPN” LED (“OFF”|“ON”|”FAIL”)
<DI1>,<DI2>,..., <DIDO5>,<DIDO6>, status (“LO”|”HI”) of the digital I/Os

Questo comando non viene mai rifiutato.

Esempio:

```
→    STATUS
←    STATUS EXECUTING (Z-PASS2-RT-4G 2018/03/09 08:01:31 RUNNING
OFF,OFF HI,LO,HI,LO,LO,LO)
```

21.19. GET GPS

Questo comando può essere utilizzato per ottenere dal dispositivo le informazioni sulla posizione GPS.

La risposta viene fornita come URL su Google Maps™:
https://www.google.com/maps/?q=<latitude>,<longitude>

Questo comando viene rifiutato nei seguenti casi:

- se il segnale GPS non è disponibile, il comando non verrà eseguito generando l’errore “GPS not fixed”.

Esempio:

```
→    GET GPS
←    GET                          GPS                          EXECUTING
(https://www.google.com/maps/?q=45.3742,11.94557)
```

21.20. RESET

Questo comando può essere utilizzato per riavviare (“reboot”) il dispositivo.

Questo comando non viene mai rifiutato.

Esempio:

```
→    RESET
←    RESET EXECUTING
```

[6] Consultare il Capitolo “LED di segnalazione”.

21.21. GET TAG

Questo comando può essere utilizzato per ottenere il valore di un tag (vedere la funzionalità “Modbus Shared Memory Gateway”).
Il comando ha il seguente formato:

```
GET TAG <tag name>
```

Tener presente che “tag name” distingue tra maiuscole e minuscole; inoltre, questo comando presume che ogni tag abbia un nome distinto; se sono presenti più tag con lo stesso nome, questo comando restituisce il valore del primo tag rilevato con il nome specificato.
Il valore viene indicato nella risposta con il seguente formato:

```
<tag value>,VALID
```

o:

```
<tag value>,INVALID
```

Lo stato “INVALID” potrebbe presentarsi per tag con “GATEWAY MODE”=”GATEWAY”, quando l’ultima richiesta di lettura Modbus non è riuscita.

Questo comando viene rifiutato nei seguenti casi:

- se nessuna porta seriale ha “Gateway Mode”=”Modbus Shared Memory”, il comando non verrà eseguito generando l’errore “Modbus Gateway not active”;
- se non vengono individuati tag con il nome specificato, il comando non verrà eseguito generando l’errore “Tag does not exist”;
- se il tag richiesto ha “GATEWAY MODE”=”BRIDGE” e la richiesta di lettura Modbus non riesce, il comando non verrà eseguito generando l’errore “Tag operation failed”.

Esempio:

```
→    GET TAG GPS_LONGITUDE
←    GET TAG GPS_LONGITUDE EXECUTING (11.94528,VALID)
```

21.22. SET TAG

Questo comando può essere utilizzato per impostare il valore di un tag (vedere la funzionalità “Modbus Shared Memory Gateway”).
Il comando ha il seguente formato:

```
SET TAG <tag name> <tag value>
```

Tener presente che “tag name” distingue tra maiuscole e minuscole; inoltre, questo comando presume che ogni tag abbia un nome distinto; se sono presenti più tag con lo stesso nome, questo comando tenta di impostare il valore del primo tag rilevato con il nome specificato.
Per i valori tag non interi, verrà utilizzato il carattere del punto decimale ‘.’.

Questo comando viene rifiutato nei seguenti casi:

- se nessuna porta seriale ha “Gateway Mode”=”Modbus Shared Memory”, il comando non verrà eseguito generando l’errore “Modbus Gateway not active”;
- se non vengono individuati tag con il nome specificato, il comando non verrà eseguito generando l’errore “Tag does not exist”;
- se il valore specificato non corrisponde a “Data Type” del tag target (ad esempio, il valore “2” per un tag “BOOLEANO”), il comando non verrà eseguito generando un errore “Invalid value for tag”;
- se, per una qualsiasi ragione, l’operazione di scrittura non riesce, il comando non verrà eseguito generando l’errore “Tag operation failed”; questo include i seguenti casi:
    - la richiesta di scrittura Modbus non riesce per i tag “GATEWAY” o “BRIDGE”;
    - il valore del tag non può essere modificato poiché non si tratta di “General output”, per tag I/O digitali (“EMBEDDED”);
    - il valore del tag non può essere modificato poiché si tratta di un tag “GPS info” (“EMBEDDED”).

Esempio:

→ `SET TAG ZPASS_DO 10`

← `SET TAG ZPASS_DO 10 EXECUTING`

21.23. OVPN ON

Questo comando può essere utilizzato per attivare la funzionalità OPEN VPN standard; la funzionalità viene attivata con i parametri di configurazione del sistema (Server, Password, Nome tag).
Tener presente che questo comando non attiva la funzionalità OPEN VPN in modo permanente; di conseguenza se il dispositivo viene riavviato, la funzionalità non viene riattivata.

Esempi:

→ `OVPN ON`

← `OVPN ON EXECUTING`

21.24. OVPN OFF

Questo comando può essere utilizzato per disattivare la funzionalità OPEN VPN attivata con un precedente comando “OVPN ON”.

Tener presente che questo comando non disattiva la funzionalità OPEN VPN in modo permanente; di conseguenza se Z-PASS viene riavviato, la funzionalità viene riattivata.

Esempio:

→ `OVPN OFF`

← `OVPN OFF EXECUTING`

21.25. CLEAN LOGS

Questo comando eliminerà tutti i registri di dati.

→ `CLEAN LOGS`

← `CLEAN LOGS EXECUTING`

22. AGGIORNAMENTO DEL FIRMWARE DEL DISPOSITIVO

Il firmware può essere aggiornato da pagina web (sezione FW UPDATE) oppure con una penna USB formattata con il filesystem FAT32.

22.1. AGGIORNAMENTO FIRMWARE DA CHIAVETTA USB

Per l'aggiornamento fw da chiavetta USB La procedura è la seguente:

Scaricare il file FW dal sito Seneca

il file scaricato è un file .zip; estrarre il file .bin; il file FW deve essere del tipo:

SW00xxxx_xxx.bin

1) Copiare il file nella directory principale (root) della penna USB
2) Spegnere il dispositivo
3) Inserire la penna USB nella porta USB
4) Accendere il dispositivo

la procedura di aggiornamento richiederà alcuni minuti per essere completata; durante questo tempo, il dispositivo NON DEVE essere spento.

23. RESET DI FABBRICA

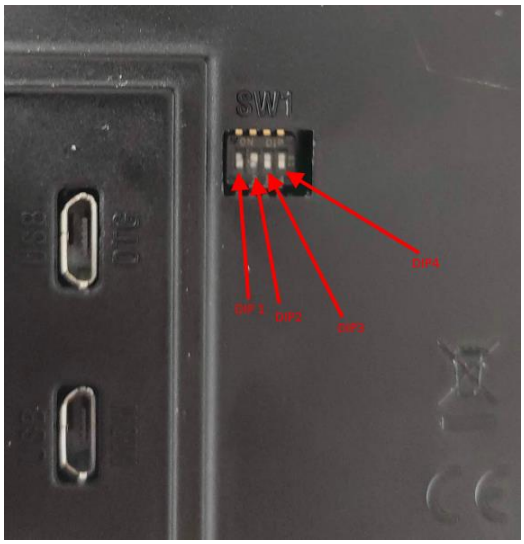
Con questa procedura è possibile ottenere:

1) Tutti i parametri a quelli di fabbrica
2) Vengono ripulite tutte le cartelle (e quindi eliminati tutti i file di log dati e di debug)

23.1. RESET DI FABBRICA PER SSD

Per ottenere un ripristino di fabbrica seguire la seguente procedura:

1) Spegnere il dispositivo
2) Raggiungere la parte posteriore del dispositivo ed individuare i dip switch come da figura:



3) Portare i dip switch in: DIP1 = OFF, DIP2 = ON, DIP3 = ON, DIP4 = ON
4) Accendere il dispositivo e attendere che abbia completato il caricamento
5) A dispositivo acceso portare i dip in: DIP1 = OFF, DIP2 = ON, DIP3 = OFF, DIP4 = OFF

23.2. RESET DI FABBRICA PER R-PASS E R-PASS-S

Per ottenere un ripristino di fabbrica seguire la seguente procedura:

1) Spegnere il dispositivo
2) Raggiungere la parte posteriore del dispositivo ed individuare i dip switch come da figura:

3) Portare i dip switch in: DIP1 = OFF, DIP2 = ON, DIP3 = ON, DIP4 = ON
4) Accendere il dispositivo e attendere che abbia completato il caricamento
5) A dispositivo acceso portare i dip in: DIP1 = OFF, DIP2 = ON, DIP3 = OFF, DIP4 = OFF

23.3. RESET DI FABBRICA PER Z-PASS1-RT, Z-PASS2-RT, Z-TWS4-RT-S, Z-PASS2-RT-S

Per ottenere un ripristino di fabbrica seguire la seguente procedura:

1) Spegnere il dispositivo
2) Raggiungere la parte posteriore del dispositivo togliendo il coperchio sul fondo del dispositivo e individuare la serie di DIP SW1
3) Portare i dip switch in: DIP1 = ON, DIP2 = ON, DIP3 = ON, DIP4 = OFF, DIP5=ON, DIP6 =ON
4) Accendere il dispositivo e attendere che abbia completato il caricamento
5) Riportare i portare i dip in: DIP1 = ON, DIP2 = ON, DIP3 = ON, DIP4 = OFF, DIP5=OFF, DIP6 =OFF

24. INDIRIZZI MODBUS DEGLI I/O EMBEDDED DEI DISPOSITIVI

Gli I/O embedded dei dispositivi sono accessibili anche esternamente tramite il protocollo Modbus TCP-IP o RTU attraverso gli indirizzi qui riportati:

24.1. INDIRIZZI MODBUS DEGLI I/O DI SSD

Data Type	***Digital I/Os***	***Default address offset***
Holding Registers	Bit 0: DI1 (LSB) Bit 1: DI2	0 (40001)
Holding Registers	Bit 0: DO1 (LSB) Bit 1: DO2	1 (40002)
Holding Registers	Bit 0: Maintenance Mode	2 (40003)
Holding Registers	Analog Input 1 (UINT16)	3 (40004)
Holding Registers	Analog Input 2 (UINT16)	4 (40005)

Holding Registers	Internet Access (0 = None, 1 = ETH, 2 = WIFI)	50 (40051)
Discrete Inputs	DI1	0 (10001)
Discrete Inputs	DI2	1 (10002)
Coils	DO1	0
Coils	DO2	1

24.2. INDIRIZZI MODBUS DEGLI I/O DI R-PASS

Data Type	***Digital I/Os***	***Indirizzo di default***
Holding Registers	Bit 0: DI1 (LSB) Bit 1: DI2 Bit 2: DI3 Bit 3: DI4	0 (40001)
Holding Registers	Bit 0: DO1 (LSB) Bit 1: DO2 Bit 2: DO3 Bit 3: DO4	1 (40002)
Holding Registers	Bit 0: Maintenance Mode	2 (40003)
Holding Registers	Internet Access (0 = None, 1 = ETH, 2 = WIFI, 3 = Mobile)	50 (40051)
Discrete Inputs	DI1	0 (10001)
Discrete Inputs	DI2	1 (10002)
Discrete Inputs	DI3	2 (10003)
Discrete Inputs	DI4	3 (10004)
Coils	DO1	0
Coils	DO2	1
Coils	DO3	2
Coils	DO4	3
Holding Registers	Analog Input 1 (UINT16)	3 (40004)
Holding Registers	Analog Input 2 (UINT16)	4 (40005)

24.3. INDIRIZZI MODBUS DEGLI I/O DI Z-PASS1-RT, Z-PASS2-RT

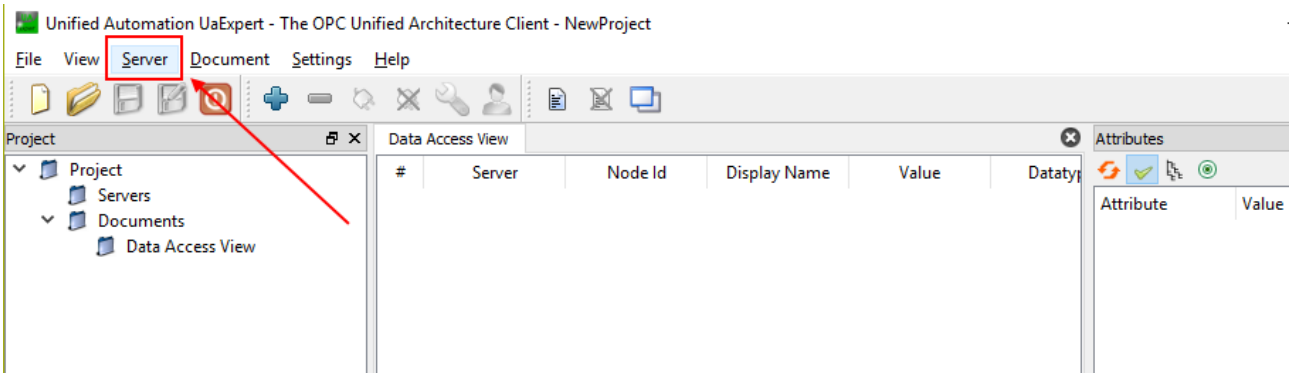
Data Type	***Digital I/Os***	***Indirizzo di default***
Holding Registers	Bit 0: DI1 (LSB) Bit 1: DI2 Bit 2: DI3 Bit 3: DI4 Bit 4: DI5 Bit 5: DI6	0 (40001)

Holding Registers	Bit 0: DO1 (LSB) Bit 1: DO2 Bit 2: DO3 Bit 3: DO4 Bit 4: DO5 Bit 5: DO6	1 (40002)
Holding Registers	Bit 0: Maintenance Mode	2 (40003)
Holding Registers	Analog Input 1 (UINT16)	3 (40004)
Holding Registers	Analog Input 2 (UINT16)	4 (40005)
Holding Registers	Internet Access (0 = None, 1 = ETH, 2 = WIFI, 3 = Mobile)	50 (40051)
Discrete Inputs	DI1	0 (10001)
Discrete Inputs	DI2	1 (10002)
Discrete Inputs	DI3	2 (10003)
Discrete Inputs	DI4	3 (10004)
Discrete Inputs	DI5	4 (10005)
Discrete Inputs	DI6	5 (10006)
Coils	DO1	0
Coils	DO2	1
Coils	DO3	2
Coils	DO4	3
Coils	DO5	4
Coils	DO6	5

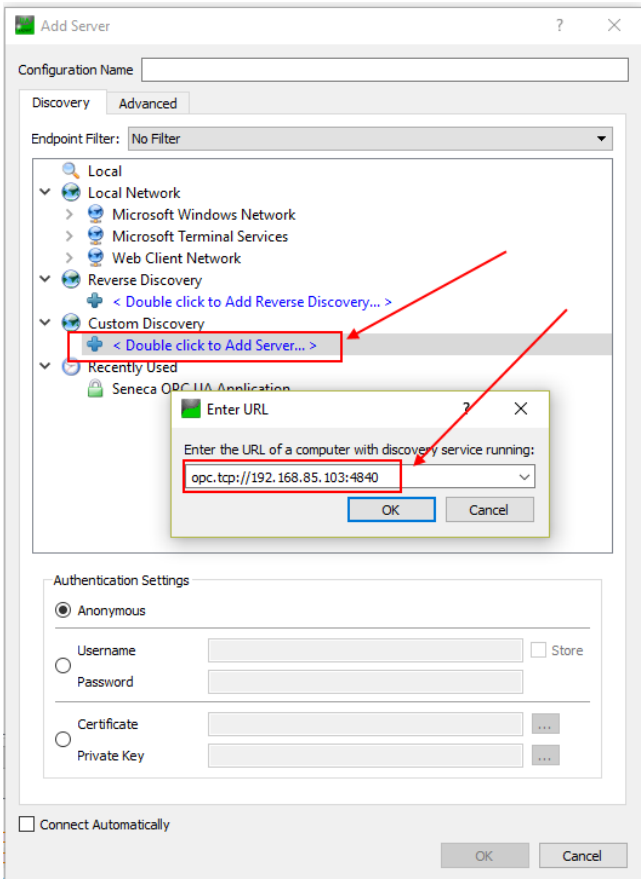
25. CONFIGURAZIONE DEL CLIENT "UA EXPERT"

Questo capitolo fornirà i passi per configurare la connessione e la corretta security policy con il software client "UA Expert"

Fare clic su Server-> Add

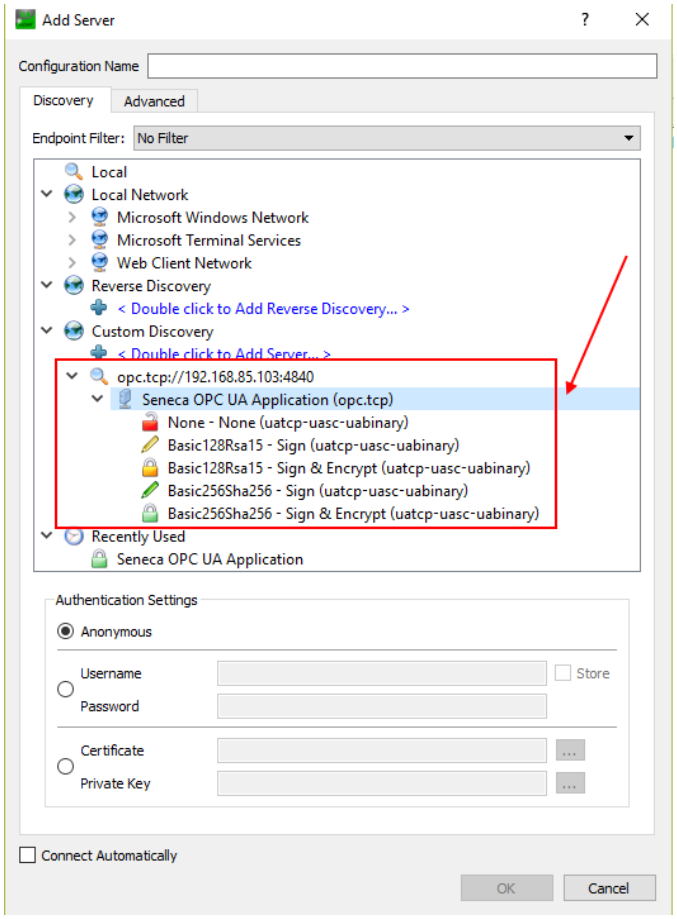


In “Custom Discovery” inserire l’url relativo al server OPC-UA:

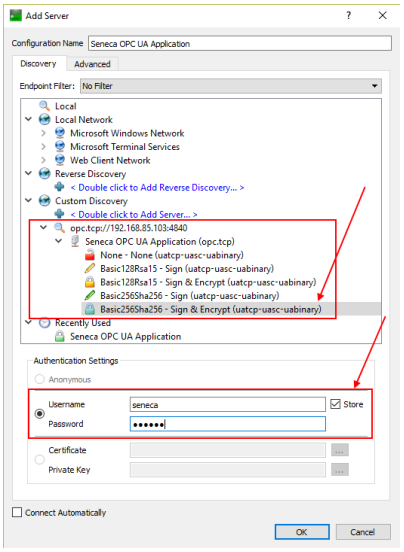


Premere OK.

Ora le politiche di sicurezza supportate sono visualizzate:

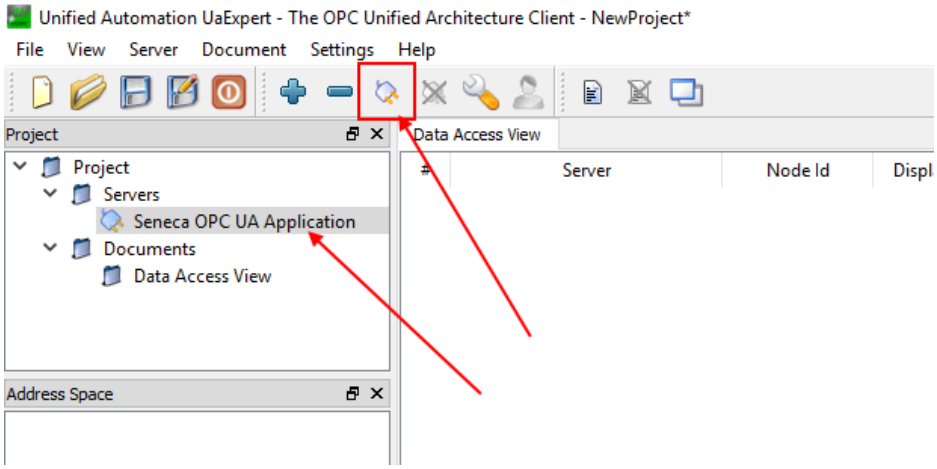


Selezionare quella che si desidera utilizzare.
Passare poi all' Authentication settings ed inserire lo user name e la password configurati nel server OPC-UA:

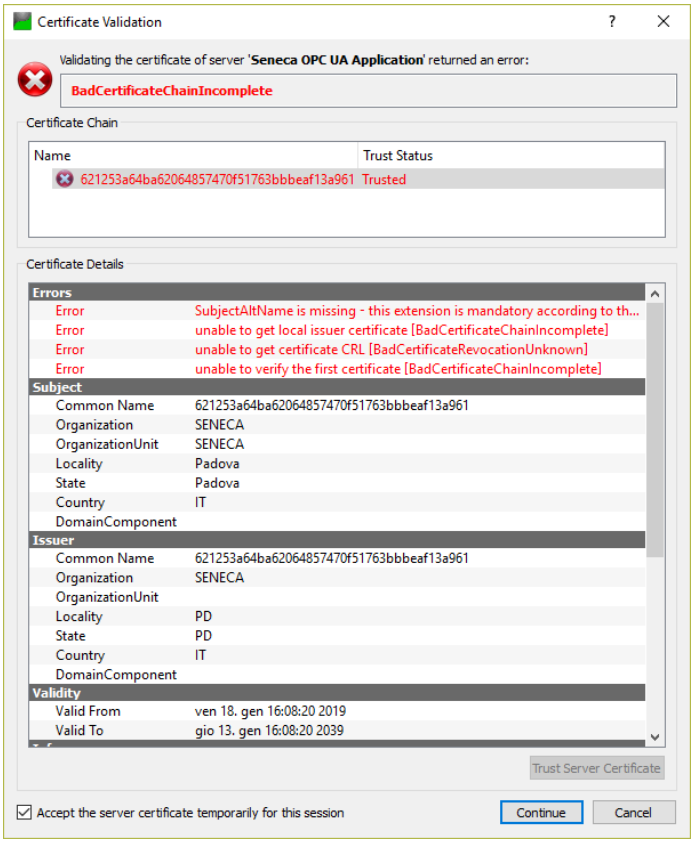


Premere OK:

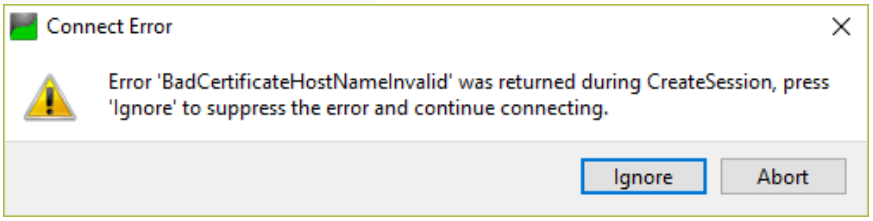
Ora possiamo collegarci al server usando l'icona opportuna:



Si aprirà una nuova finestra di dialogo per la convalida del certificato del server. Dopo aver esaminato il certificato, selezionare Trust Server Certificate per aggiungere permanentemente il certificato all'elenco di fiducia di UaExpert. È anche possibile selezionare la casella opportuna per accettare temporaneamente il certificato del server per questa sessione e scegliere Continua per non salvare il certificato nella trusted list oppure selezionare Cancel per rifiutare il certificato.

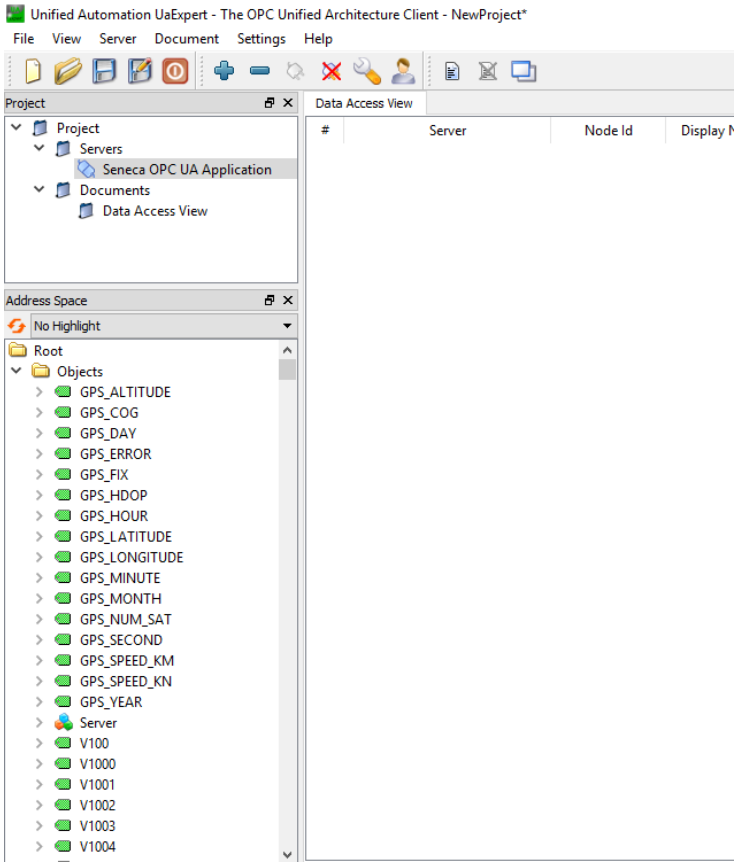


Ora verrà visualizzata la finestra Errore certificato:

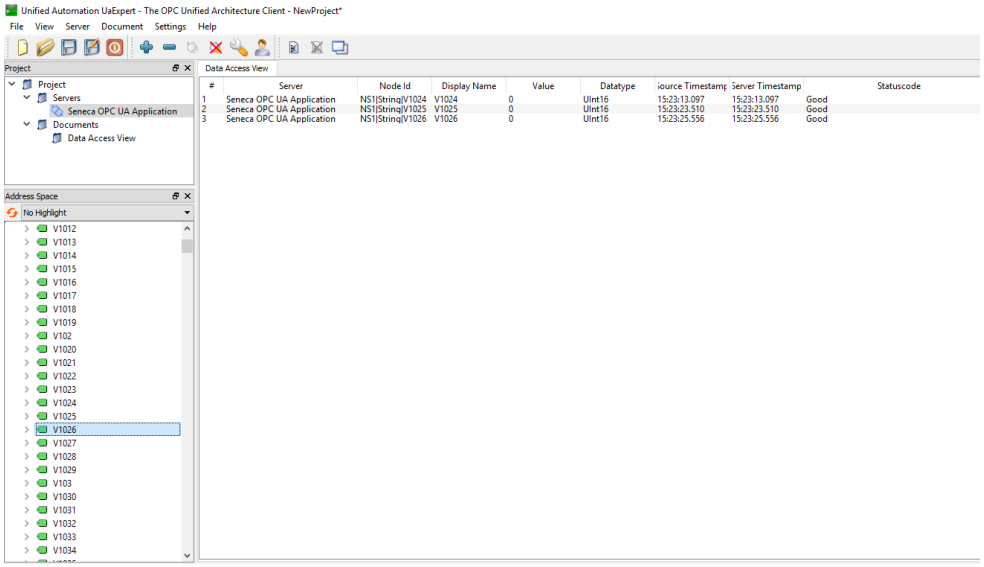


Cliccare su “Ignore” per continuare.

Ora la connessione è stabilita, è possibile leggere/scrivere il valore dei tag



Per aggiornare in tempo reale i tag fare drag and drop con ciò che si desidera visualizzare:



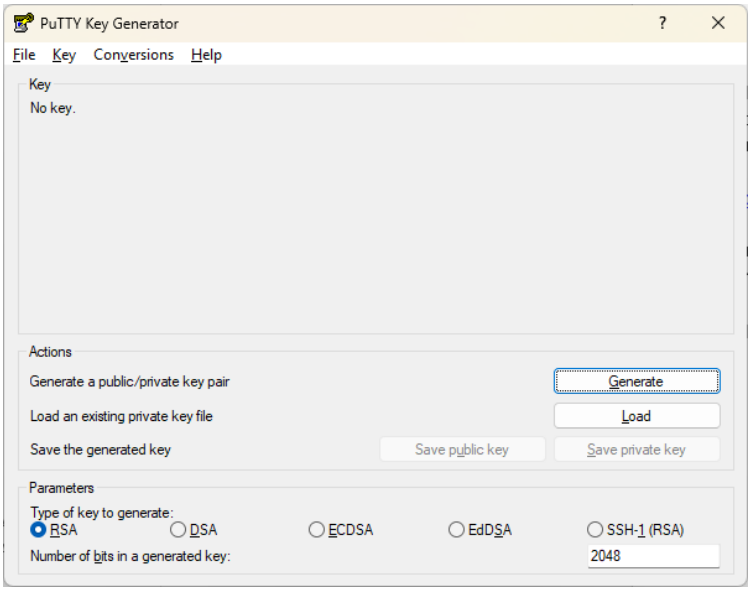
26. CREAZIONE CHIAVI PER CONNESSIONE SSH

Nel seguente capitolo verrà descritta la procedura per la creazione delle chiavi pubblica e privata per l'accesso al dispositivo tramite ssh.
Per la creazione delle chiavi si utilizzerà il software putty scaricabile da:

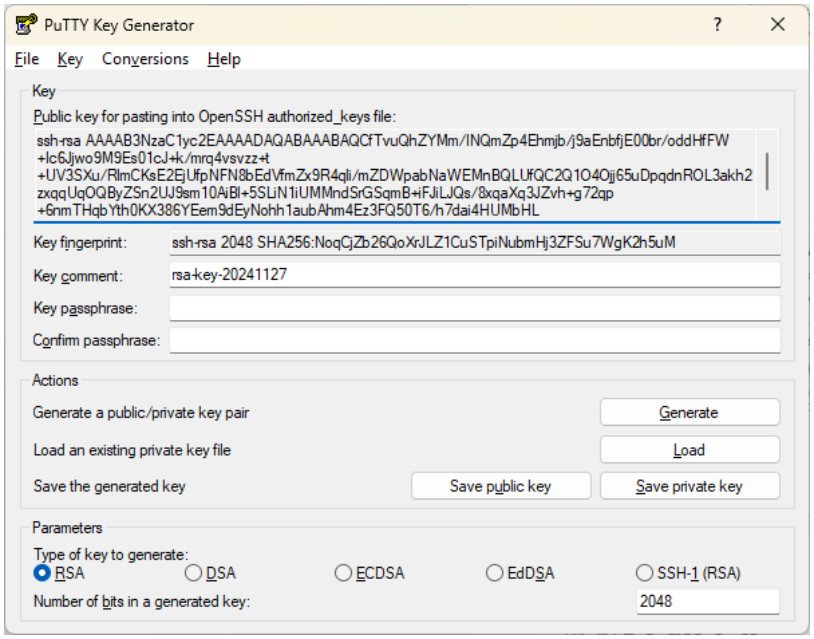
https://www.putty.org/

Per creare e utilizzare chiavi SSH su Windows, è necessario installare sia PuTTY, questo software installa anche altri tool indispensabili al nostro scopo.

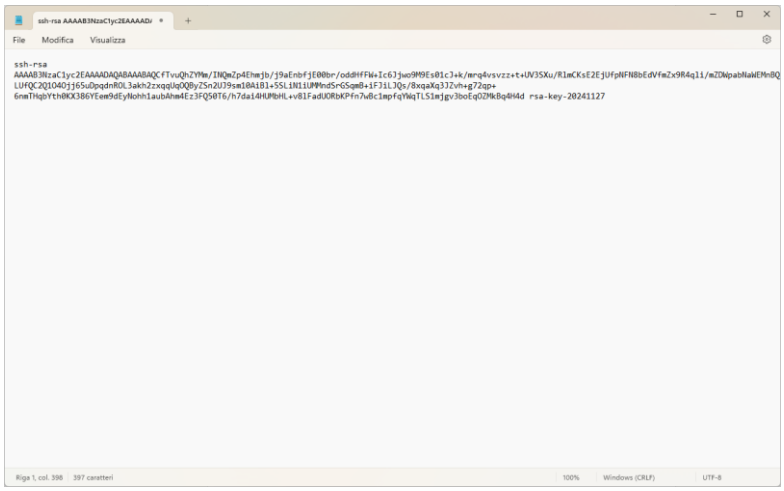
Dopo aver installato putty, avvia il programma PuTTYgen:



Ora è possibile premere il pulsante “Generate”:



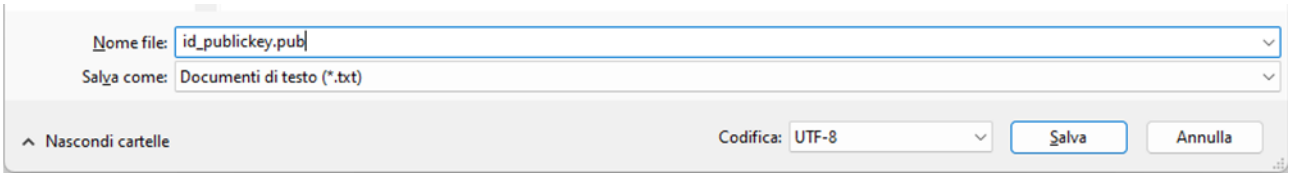
Ora nel textbox compare la chiave pubblica che dovremo copiare nel dispositivo, non salvare la chiave tramite la pressione del pulsante ma eseguire un copia/incolla in un nuovo file, avendo cura di selezionare TUTTA la chiave:



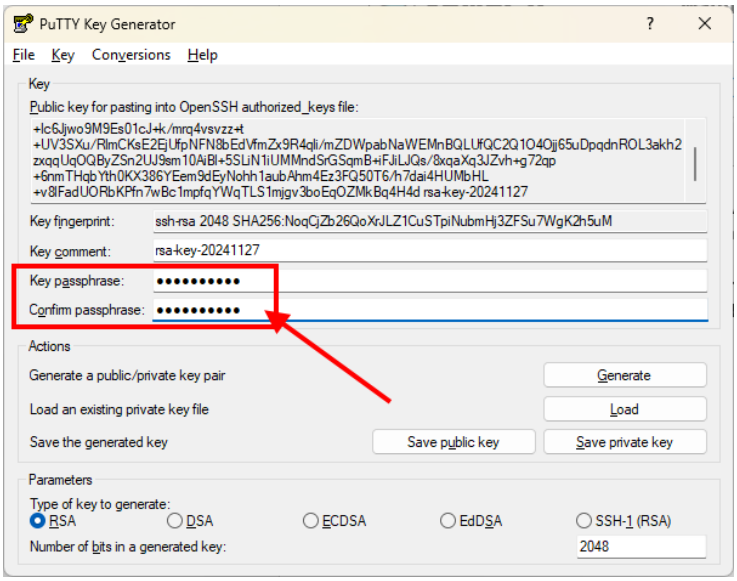
Per poter essere caricata nel dispositivo il file deve essere del tipo:
“id_*.pub “

Ad esempio rinominiamo il file come:

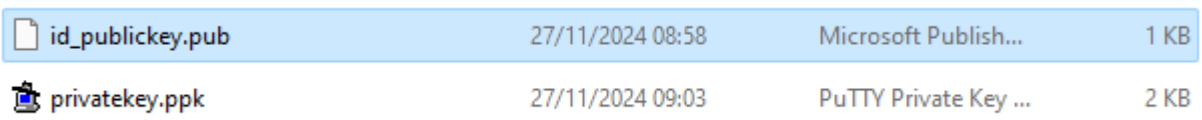
“id_publickey.pub”:



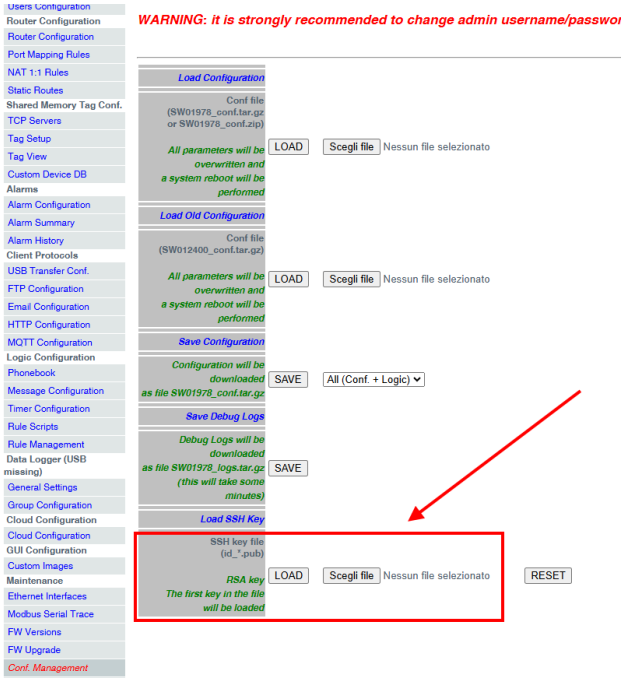
Ora salviamo la chiave privata, per far questo inseriamo una password:



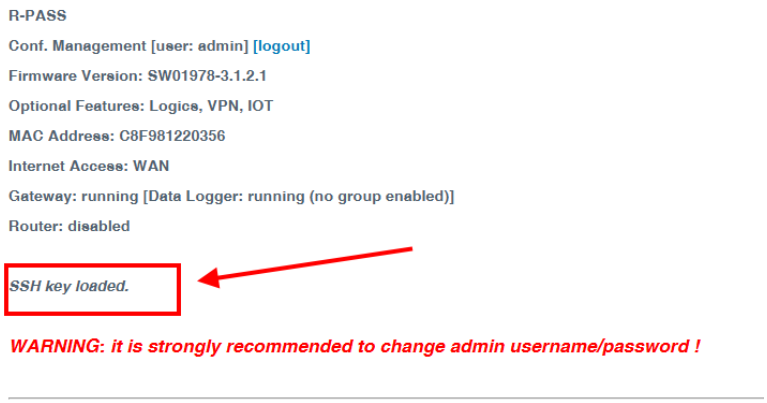
Una volta terminato, fai clic sul pulsante Salva chiave privata e seleziona un luogo sicuro in cui conservarla. Puoi nominare la tua chiave come preferisci, l'estensione ".ppk" verrà aggiunta automaticamente.
A questo punto abbiamo i 2 file di chiave pubblica e privata:



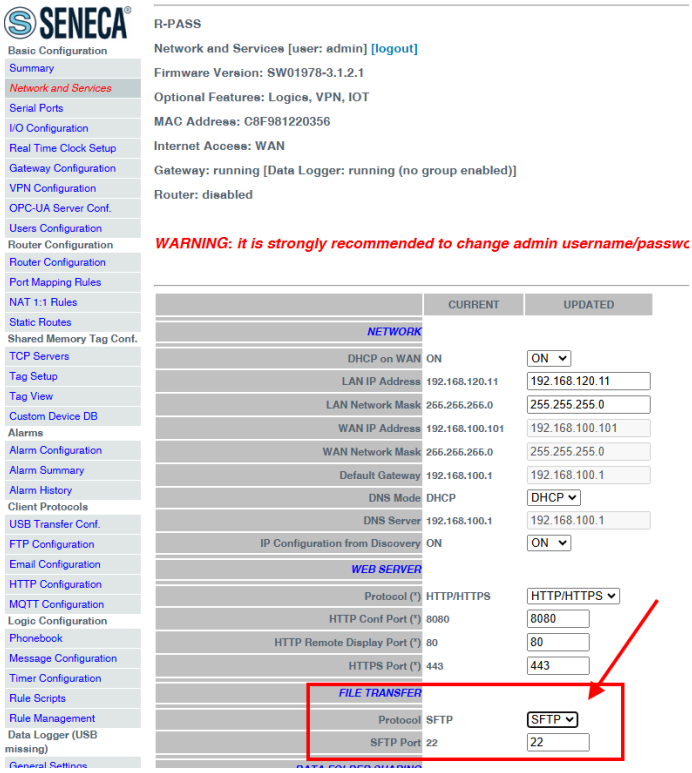
Carichiamo ora la chiave pubblica “id_publickey.pub” nel dispositivo edge dalla pagina “conf_management”:



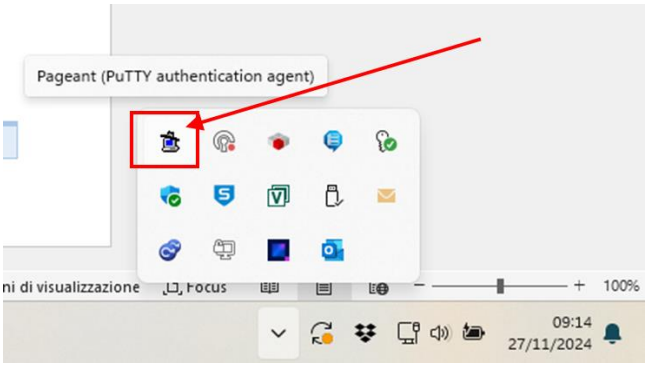
Premere il pulsante “LOAD” per caricare il file selezionato, otterremo la seguente schermata:



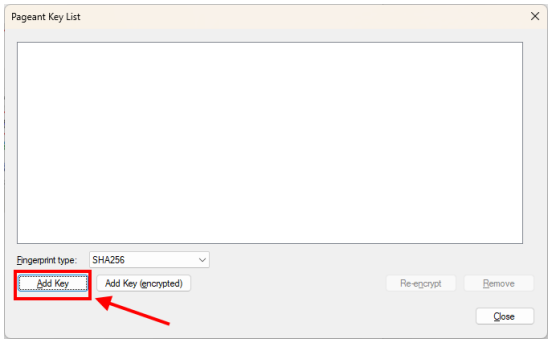
A questo punto attiviamo il servizio sftp/ssh nel dispositivo edge:



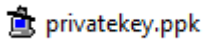
Ora eseguiamo il software su pc windows pageant (fa sempre parte dell'installazione di Putty), una volta eseguito lo troviamo qui:



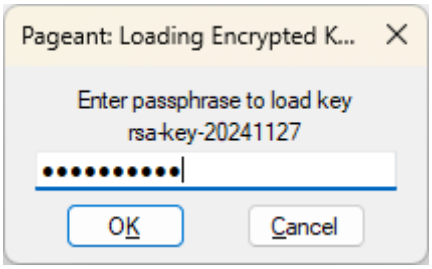
Facendo doppio click sull'icona selezioniamo poi "Add Key":



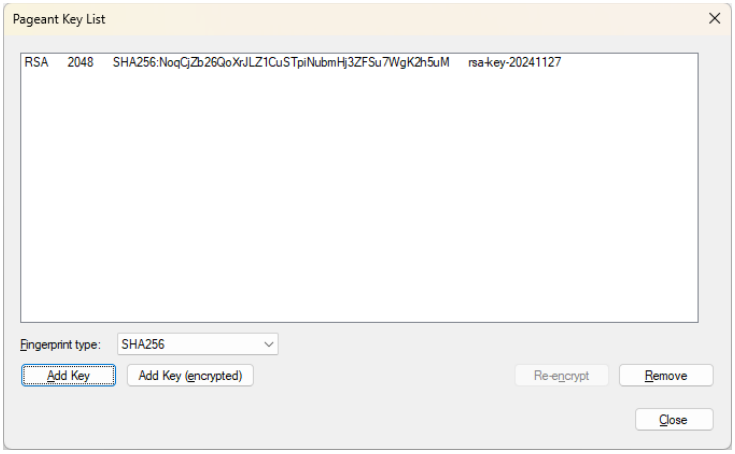
E selezioniamo la chiave privata appena generata:



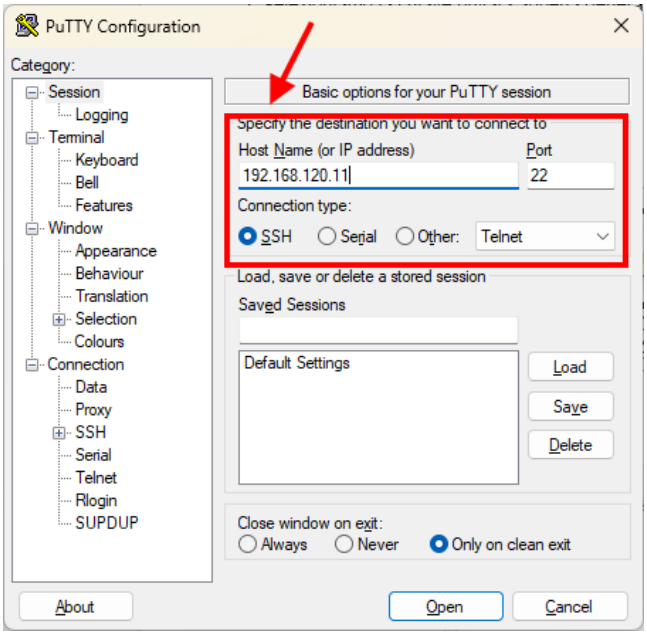
Verrà richiesto di inserire la password impostata in precedenza:



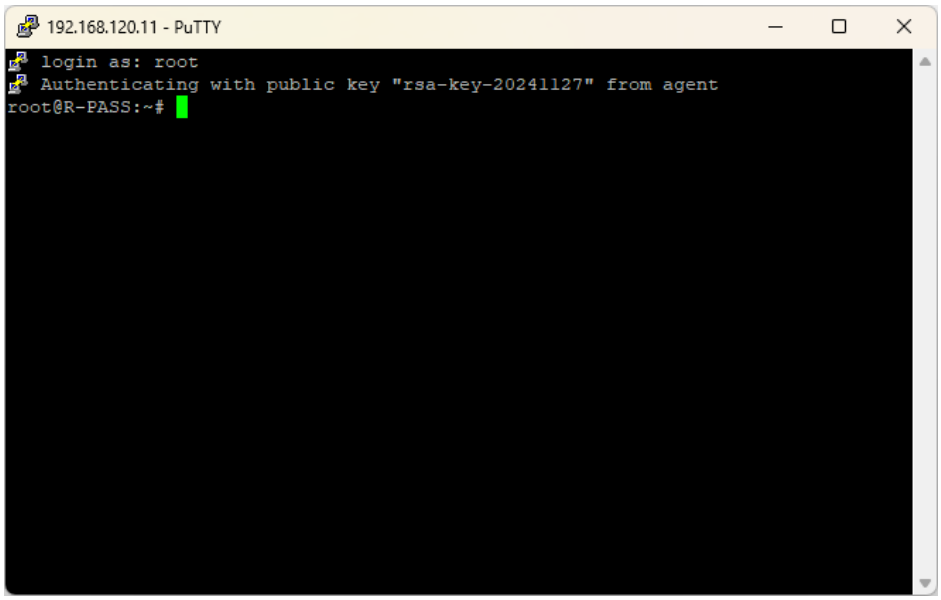
E confermare con OK:



A questo punto la chiave privata è installata in Putty, possiamo premere “Close” ed eseguire la connessione con Putty:



Ora possiamo accedere come root:



ATTENZIONE!

Ad ogni riavvio del PC sarà necessario ricaricare la chiave privata con il software pageant

ATTENZIONE!

L'attivazione del servizio sFTP/SSH può comportare una diminuzione delle difese del dispositivo edge da attacchi esterni (potenziali problemi di cybersecurity). Una volta terminate le operazioni di manutenzione tramite ssh Seneca suggerisce di disabilitare il servizio.