MANUALE UTENTE

SERIE GATEWAY 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

Introduzione

Il contenuto della presente documentazione si riferisce a prodotti e tecnologie descritti in esso.
Tutti i dati tecnici contenuti nel documento possono essere modificati senza preavviso.
Il contenuto di questa documentazione è soggetto a revisione periodica.
Per utilizzare il prodotto in modo sicuro ed efficace, leggere attentamente le seguenti istruzioni prima dell'uso.
Il prodotto deve essere utilizzato solo per l'uso per cui è stato progettato e realizzato: qualsiasi altro uso è sotto piena responsabilità dell'utente.
L'installazione, la programmazione e il set-up sono consentiti solo agli operatori autorizzati, fisicamente e intellettualmente adatti.
Il set-up deve essere eseguito solo dopo una corretta installazione e l'utente deve seguire tutte le operazioni descritte nel manuale di installazione con attenzione.
Seneca non è responsabile per guasti, rotture e incidenti causati dall'ignoranza o dalla mancata applicazione dei requisiti indicati.
Seneca non è considerata responsabile per eventuali modifiche non autorizzate.
Seneca si riserva il diritto di modificare il dispositivo, per qualsiasi esigenza commerciale o di costruzione, senza l'obbligo di aggiornare tempestivamente i manuali di riferimento.
Nessuna responsabilità per il contenuto di questo documento può essere accettata.
Utilizzare i concetti, gli esempi e altri contenuti a proprio rischio.
Potrebbero esserci errori e imprecisioni in questo documento che potrebbero danneggiare il tuo sistema, procedere quindi con cautela, l'autore(i) non se ne assumono la responsabilità.
Le caratteristiche tecniche sono soggette a modifiche senza preavviso.

CONTACT US	
Technical support	supporto@seneca.it

ORIGINAL INSTRUCTIONS

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 23 (MQTT client)	MM
21/12/2023	MI00557-13	Aggiunto il capitolo “Comandi SMS”	AZ

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.

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*
SSD	2 DIDO	NO	7" TOUCH	NO	NO	NO	2	2	NO	SI'
R-PASS	4DI 4DO	2	NO	NO	OPZIONALE	OPZIONALE	2	2 o 4	SI'	OPZIONALE
R-PASS-S	4DI 4DO	2	NO	SI'	OPZIONALE	OPZIONALE	2	2 o 4	SI'	OPZIONALE
Z-PASS1-RT	6 DIDO	2	NO	NO	NO	NO	3	2	SI'	NO
Z-PASS2-RT	6 DIDO	2	NO	NO	SI'	NO	3	2	SI'	NO
Z-TWS4-RT-S	6 DIDO	2	NO	SI'	NO	NO	3	2	SI'	NO
Z-PASS2-RT-S	6 DIDO	2	NO	SI'	SI'	NO	3	2	SI'	NO

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

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.

2.1.2.R-PASS

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 collegare l'opzione R-COMM che include un modem 4G e un UPS (opzionale).
È disponibile il modello con 2 e 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 –S-E oltre ad includere il PLC Straton dispone delle licenze per i protocolli di energy management.

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

Z-PASS1-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.

2.1.4.Z-PASS2-RT

Z-PASS2-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.
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.

2.2. OPZIONI HARDWARE E SOFTWARE

2.2.1. SSD

Smart Display dispone delle seguenti opzioni hardware:

OPZIONI HARDWARE	DESCRIZIONE
SMART DISPLAY	SMART DISPLAY NR 2 DIGITAL INPUT NR 2 DIGITAL OUTPUT NR 2 ETHERNET WI-FI / ROUTER WI-FI

E delle seguenti opzioni software (i pacchetti sono attivabili anche più di uno contemporaneamente).

OPZIONI SOFTWARE	DESCRIZIONE
PACCHETTO “BASE”	Display Grafico con widget Display remoto Scalature Datalogger max 2000tag Allarmi Gateway 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
PACCHETTO “LOGICHE”	Logiche programmabili tramite programmazione “IF THEN ELSE” Allarmistica Remota
PACCHETTO VPN “SENECA LET’S”	Connessione VPN semplificata tramite ambiente “Seneca LET’s VPN” Oppure Open VPN Standard

3. IL DISPLAY / DISPLAY REMOTO (SOLO SMART DISPLAY, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Nel prodotto Smart Display il display è integrato nel dispositivo, nel dispositivo R-PASS è possibile accedere al display tramite connessione con un browser web (ad esempio Chrome).

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

3.1. BARRA DELLE INFORMAZIONI

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

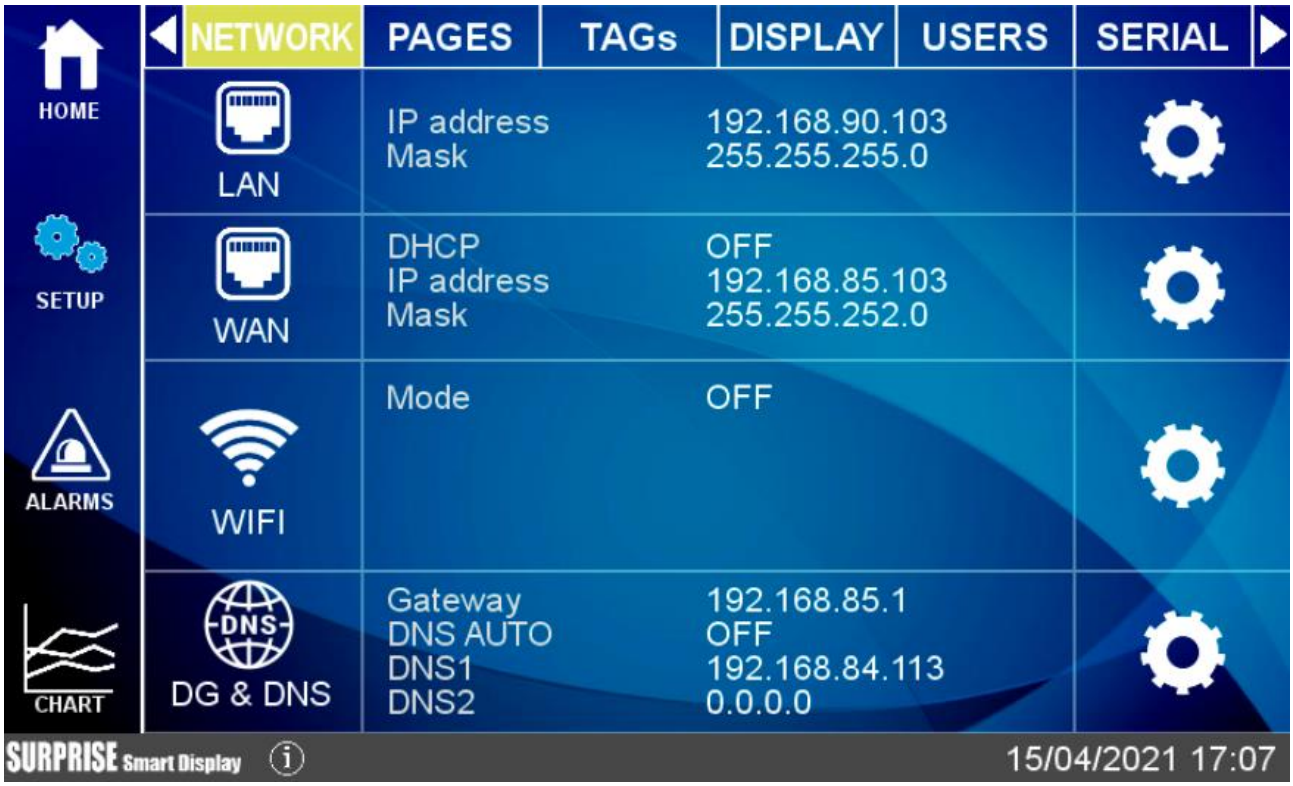
Icona “A” Fornisce informazioni sul dispositivo (come la revisione firmware) ed il produttore
Icona “B” Fornisce informazioni sull’account dell’utente, nel caso non si sia ancora loggati l’icona è sostituita da un lucchetto. L’icona di sinistra, se premuta, permette di effettuare il logout, quella di 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

3.2. 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:

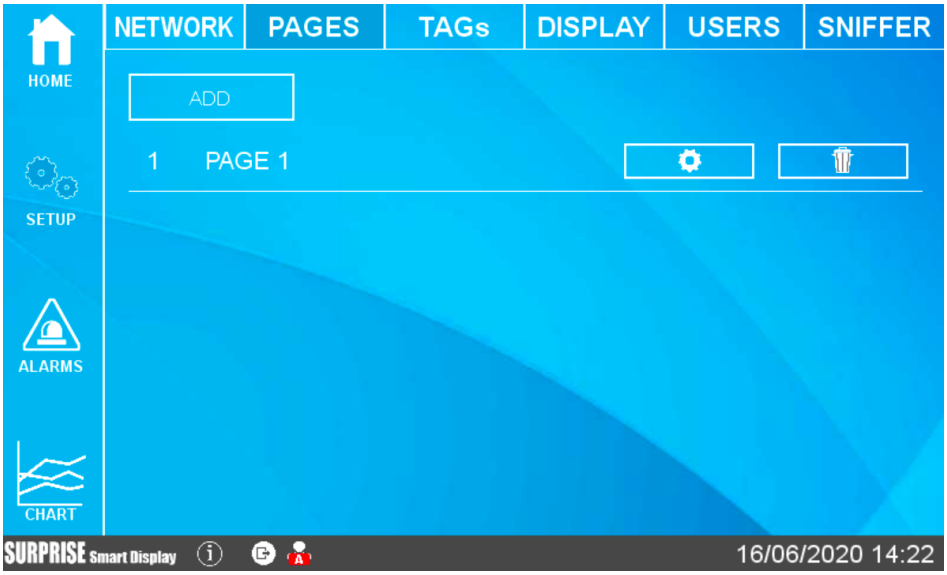
3.2.1. SETUP

3.2.1.1. NETWORK

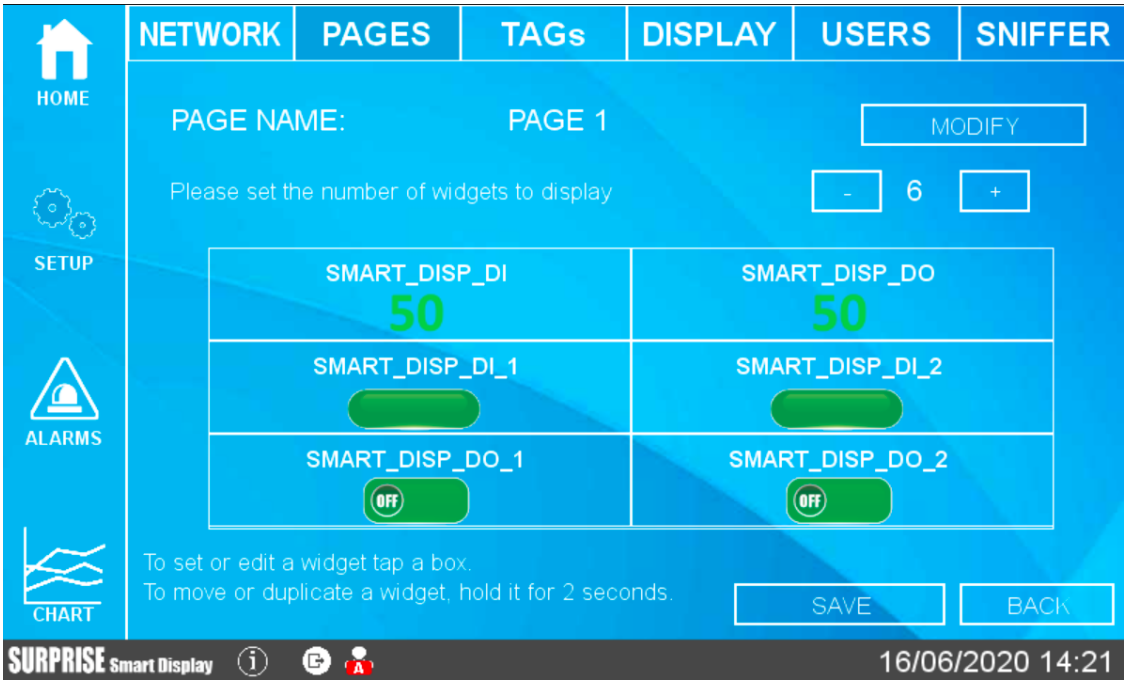


In questa sezione è possibile configurare le impostazioni delle due ethernet LAN e WAN e della porta WI-FI.
Nella sezione della porta WI-FI è possibile anche selezionare la modalità WI-FI Station o Access Point.
Nella modalità Station è il dispositivo che è connesso ad un access point Wi-Fi esistente,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

3.2.1.2. PAGES



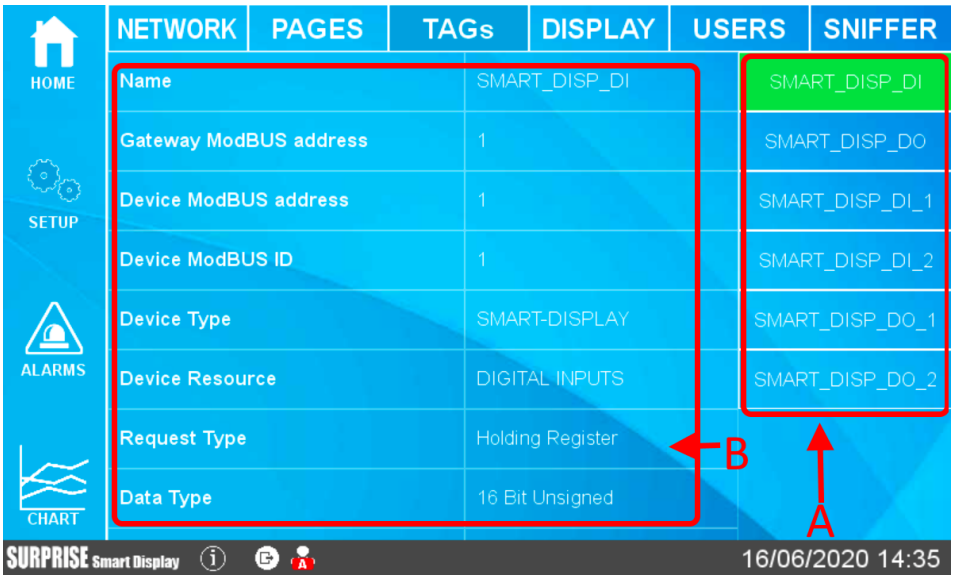
In questa prima schermata è possibile aggiungere il numero di pagine dei widget che si desidera, una volta impostato è possibile accedere alla configurazione di ciascuna pagina:



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…

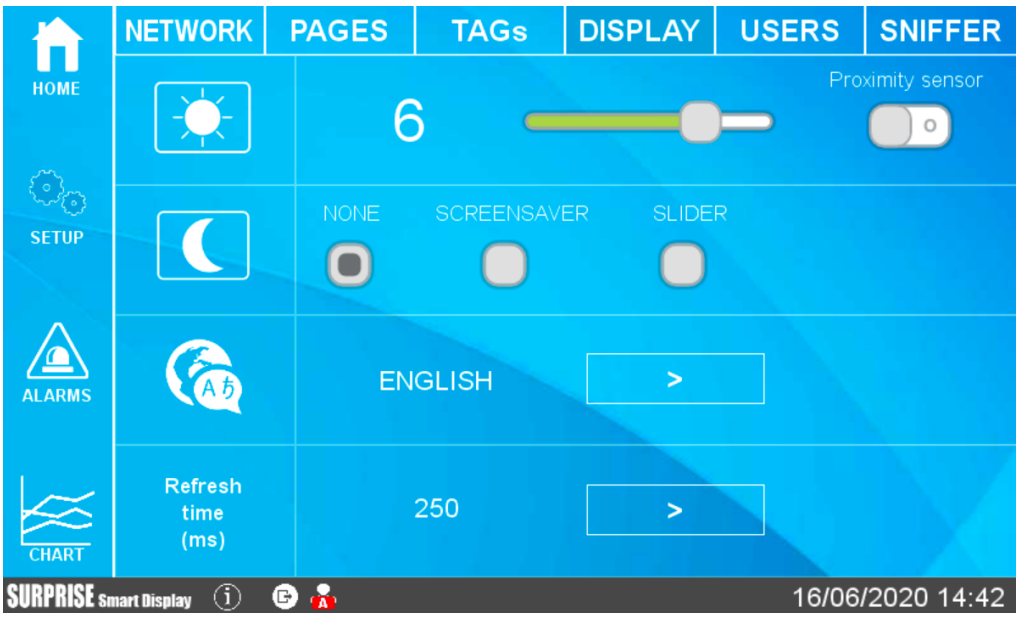
Oltre ad una pagina widget è possibile aggiungere una pagina Synoptic (sinottico). In una pagina sinottico è possibile posizionare liberamente i widget e caricare grafica da un PC o da una libreria grafica interna al dispositivo per creare dei sinottici senza l'ausilio di un software esterno.

3.2.1.3. 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.

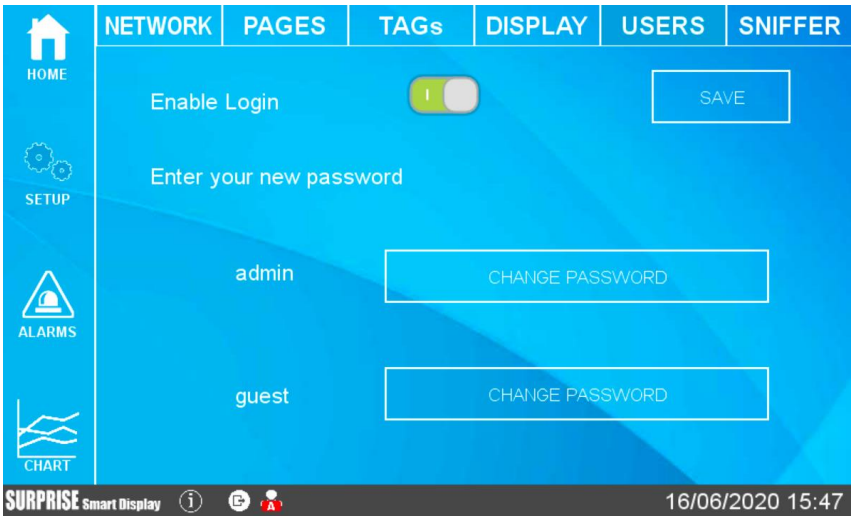
3.2.1.4. DISPLAY



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.

3.2.1.5. 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.

3.2.1.6. SERIAL

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

3.2.1.7. SNIFFER

La funzionalità di sniffer seriale permette di inserire uno o più Smart Display 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 smart display in modalità passiva (sniffer).
A questo punto Smart Display riceverà 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

3.2.1.7.1. 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 Smart Display 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 SMART DISPLAY 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.

3.2.2. 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

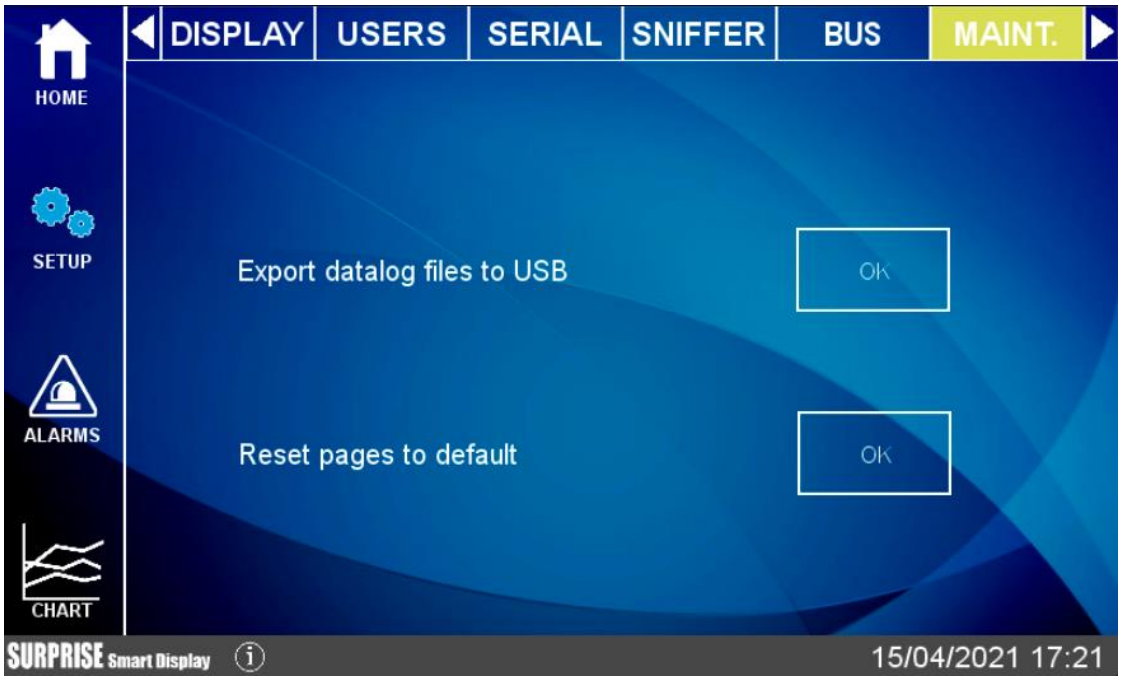
3.2.3. BUS

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.

3.2.4. MAINTENANCE

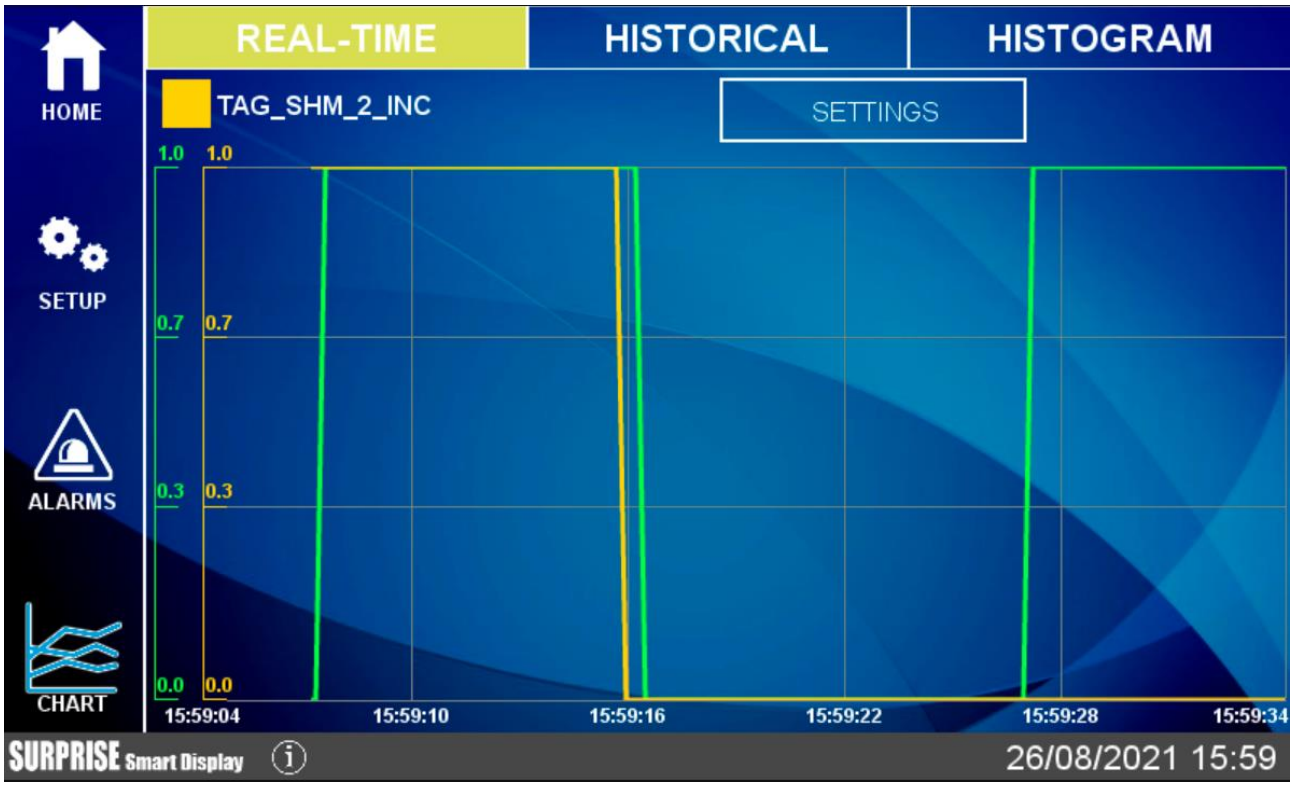
Tramite il menu Maintenance è possibile effettuare operazioni di manutenzione del dispositivo:



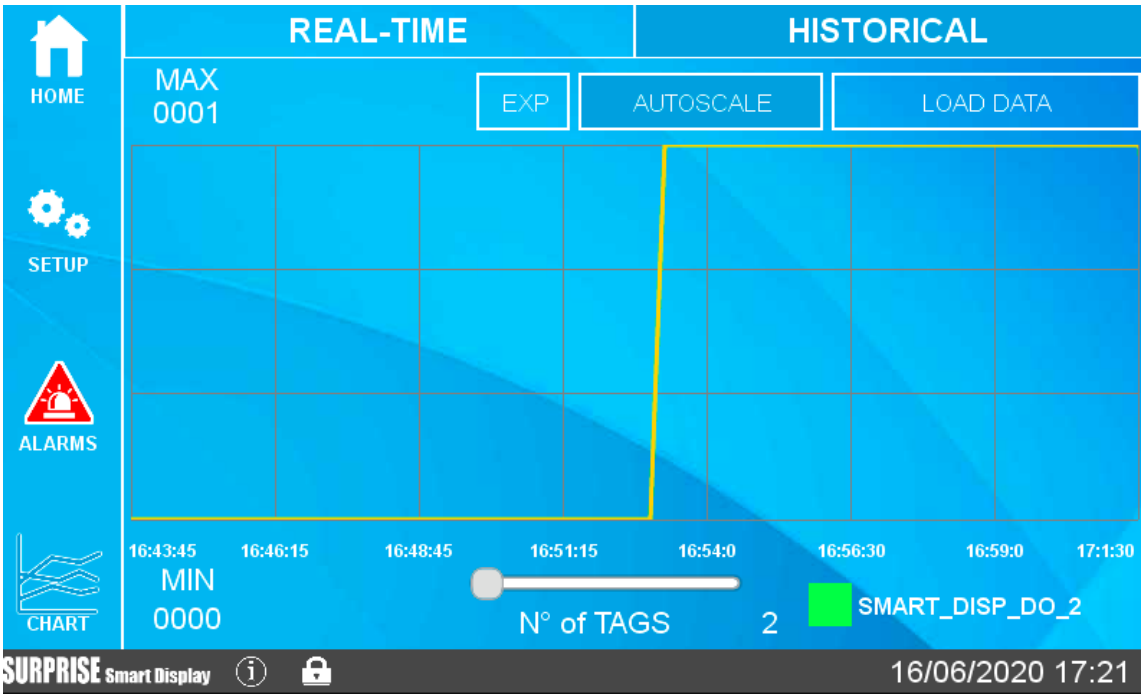
3.2.5. CHART

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.

3.3. 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:

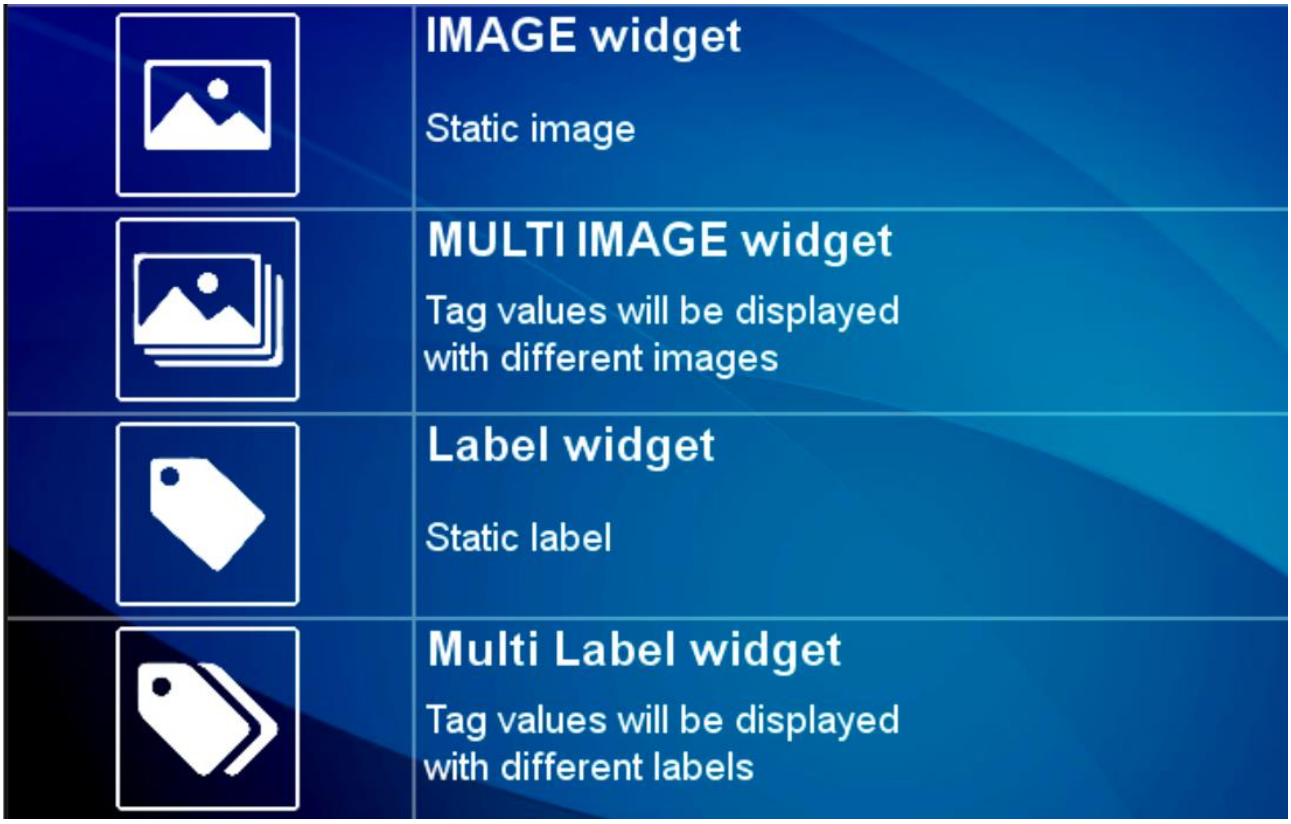
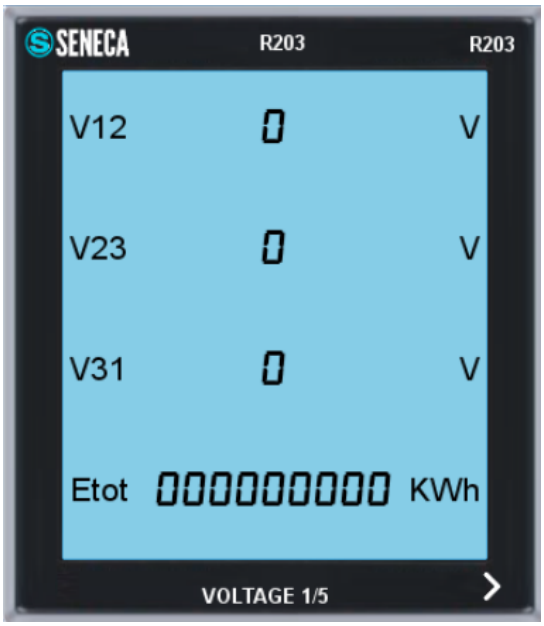


Grafico macro widget (virtual display):



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.

3.3.1. 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:

3.4. TIPO DI PAGINA WIDGET

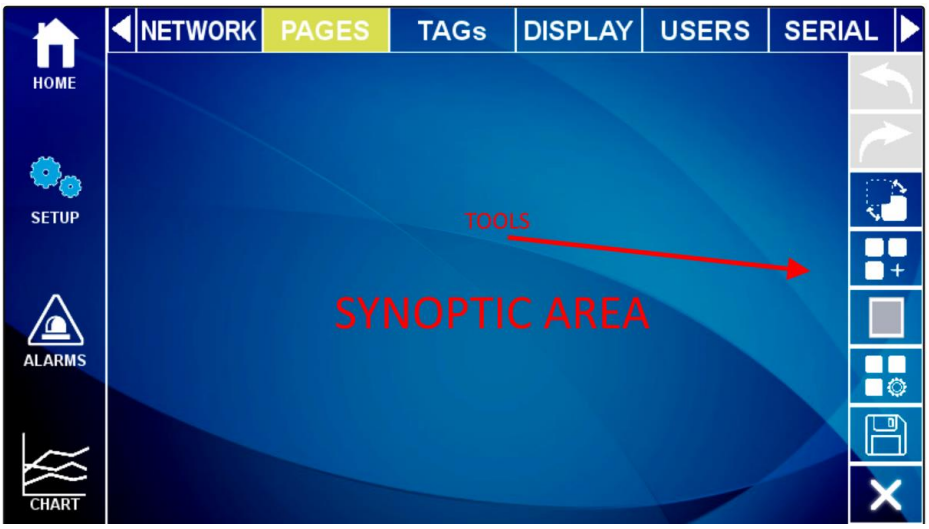
Rappresenta la pagina dei widget, in questa sezione compariranno i widget legati ai tag configurati. È possibile scegliere tra le varie griglie disponibili, i widget saranno posizionati automaticamente all’interno della griglia.
Ogni widget rappresenta in modo grafico il valore di uno o più TAG.

3.5. 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

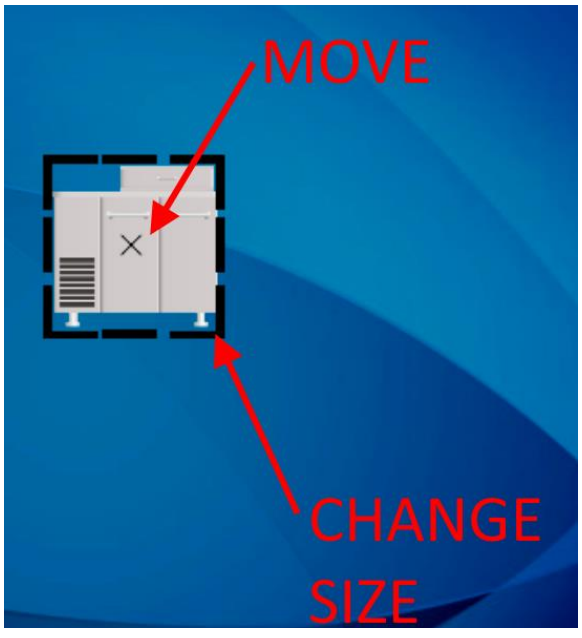
 WIDGET CONFIGURATOR
Permette la configurazione del widget

 SAVE PAGE
Salva le modifiche alla pagina

 EXIT
Esce dalla pagina

3.5.1. 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

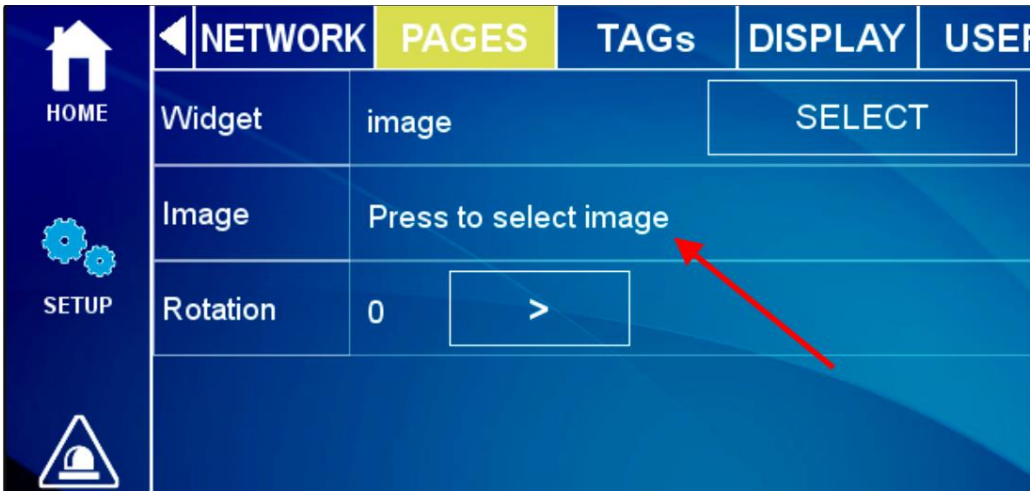
Elimina il Widget dalla pagina

 EXIT

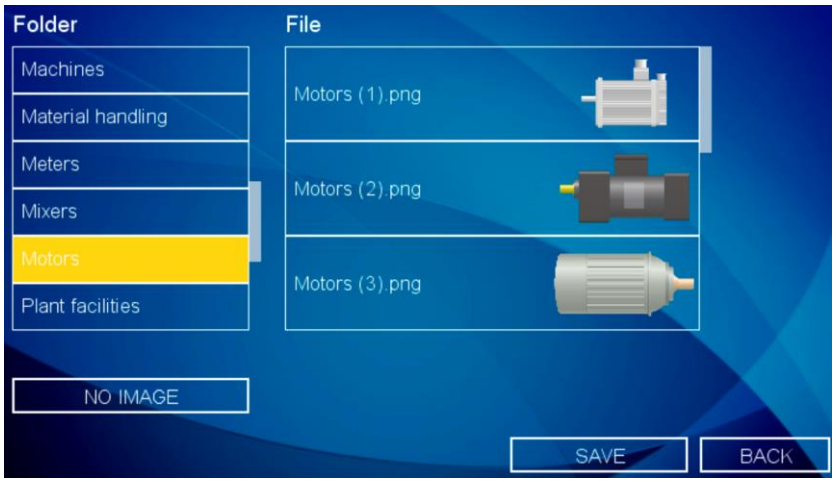
Torna alla pagina iniziale del sinottico

3.5.2. 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":

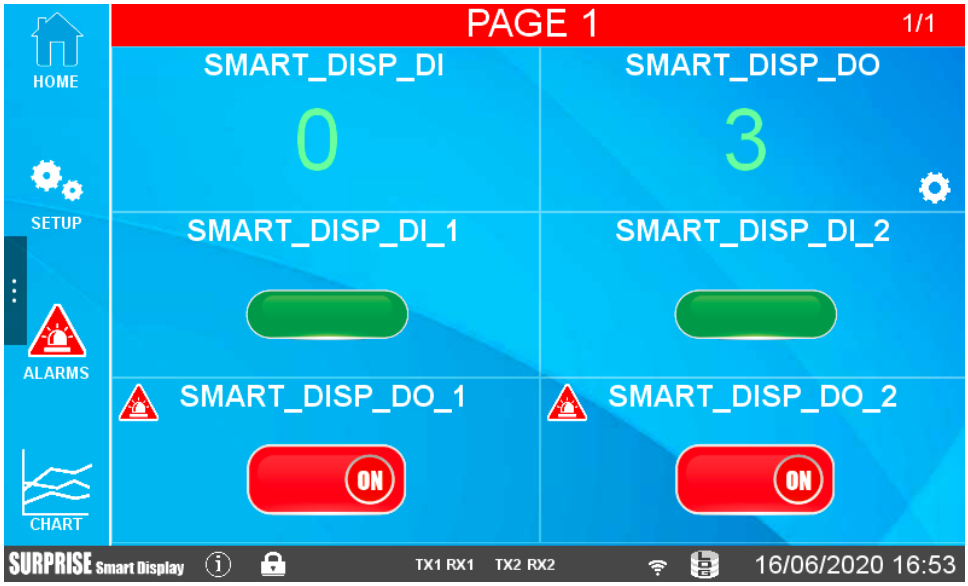


Ad esempio selezionando la categoria “Motors” vengono visualizzati i file grafici relativi a motori:



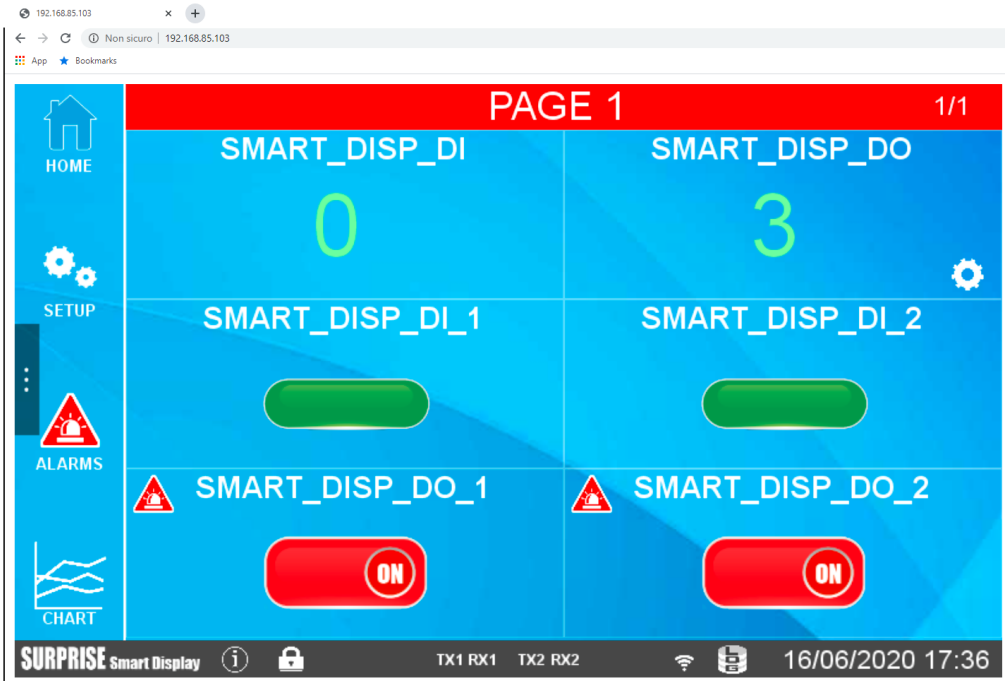
3.6. ALLARMI

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:



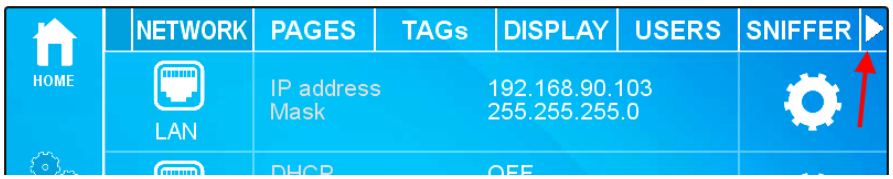
3.7. DISPLAY REMOTO

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

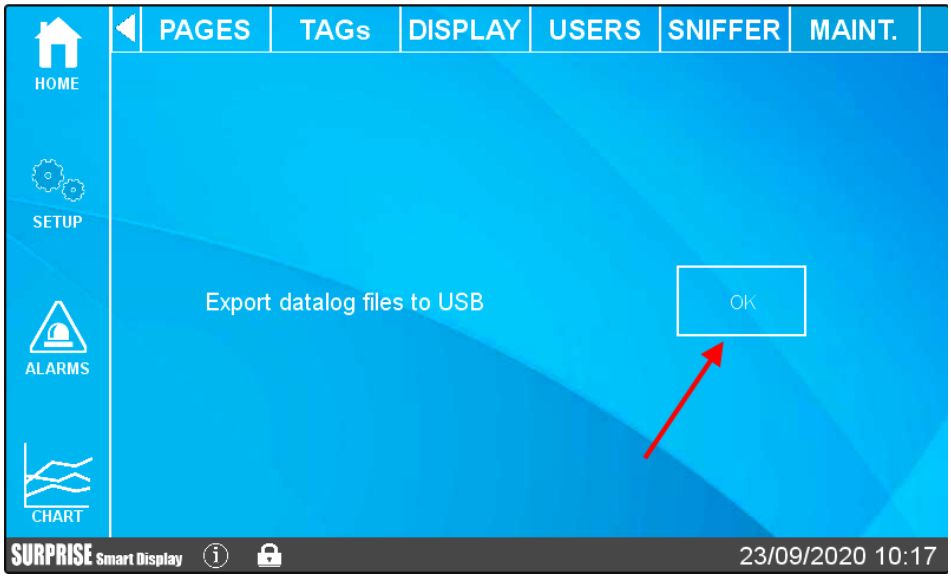


3.8. DOWNLOAD DEI FILE DI LOG SU CHIAVETTA USB

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".

4. AGGIORNAMENTO DEL FIRMWARE

Il firmware può essere aggiornato da pagina web (sezione FW UPDATE) oppure con una penna USB formattata con il filesystem FAT32.

4.1. AGGIORNAMENTO FW 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 e verrà riavviato più volte automaticamente.

5. INDIRIZZI IP

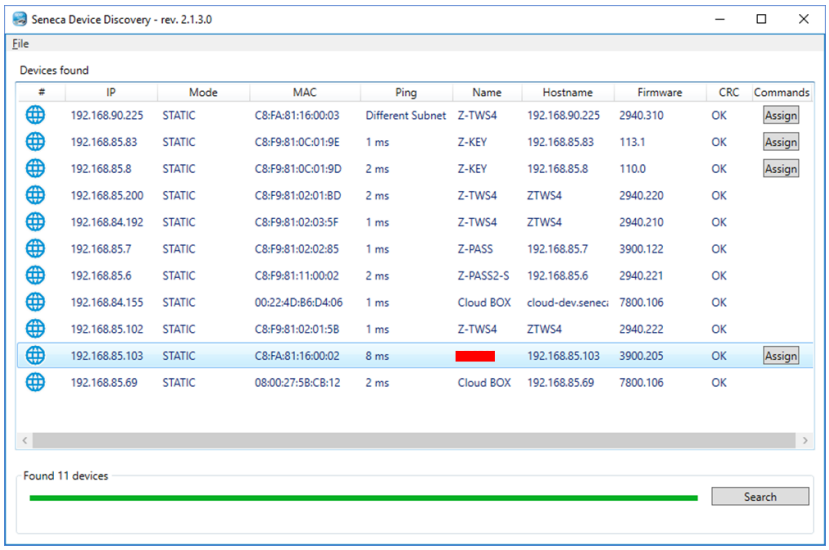
5.1. INDIRIZZI IP DI FABBRICA

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

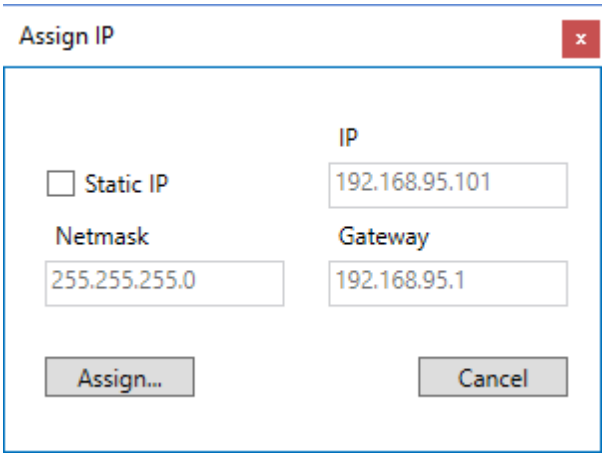
5.2. RICERCA DELL'INDIRIZZO IP

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".

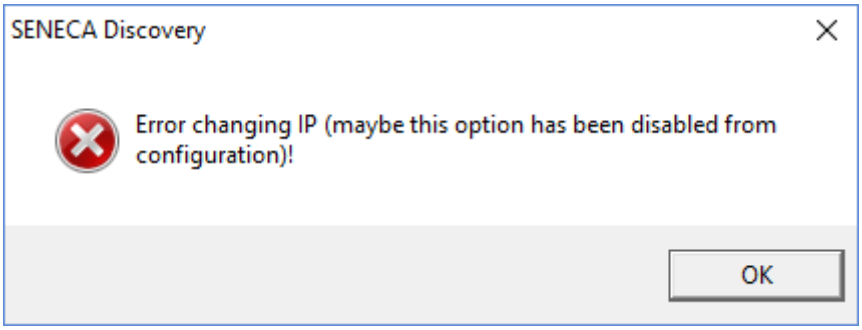


Questa applicazione mostra l'indirizzo IP, l'indirizzo MAC, la versione FW e alcune altre informazioni utili, per ogni dispositivo SENECA trovato nella LAN.

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 SDD 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'SDD è l'indirizzo IP della porta 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 porta.

6. GATEWAY MODBUS ETHERNET TO SERIAL (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Il dispositivo può essere configurato per funzionare come Gateway da Modbus Ethernet a 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 tre porte seriali disponibili: ognuna può ricevere le richieste Modbus TCP.

Un'altra possibile configurazione è quella di eseguire la conversione Gateway Modbus Ethernet to Serial su più seriali contemporaneamente.

Ogni istanza Gateway Modbus Ethernet to Serial può supportare fino a 32 connessioni TCP simultanee. La connessione TCP può essere stabilita anche attraverso un tunnel VPN

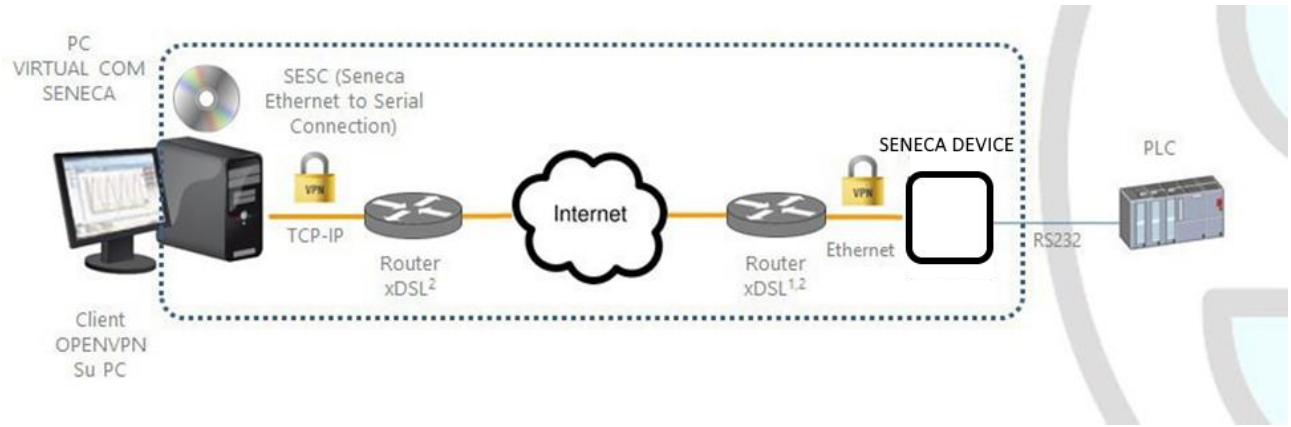
7. GATEWAY ETHERNET TO SERIAL TRASPARENTE (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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.

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

Ogni modalità sarà descritta in modo completo nei prossimi paragrafi.

7.1. VIRTUAL COM PORT CON RFC 2217



La funzionalità Virtual COM 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.

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!

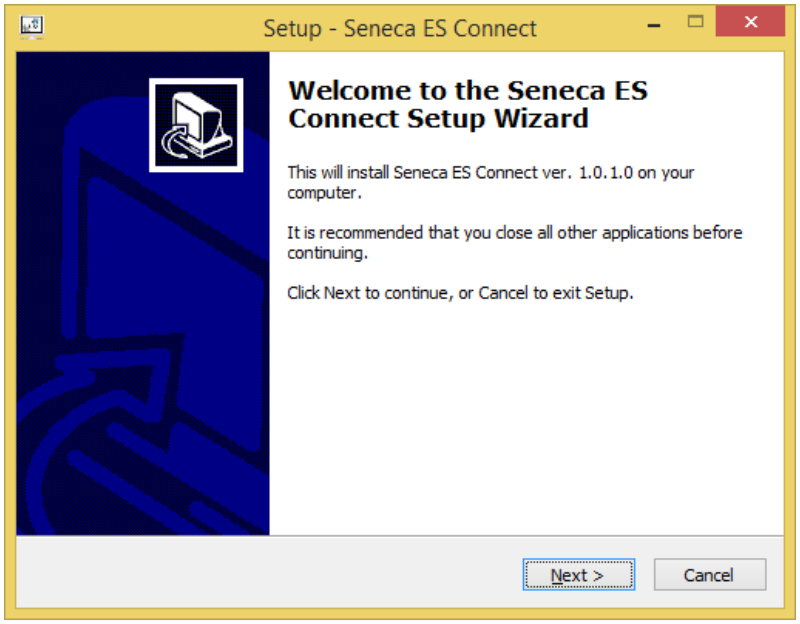
Nel modo operativo Virtual COM può essere utilizzata una sola porta seriale

7.2. SENECA ETHERNET TO SERIAL CONNECT

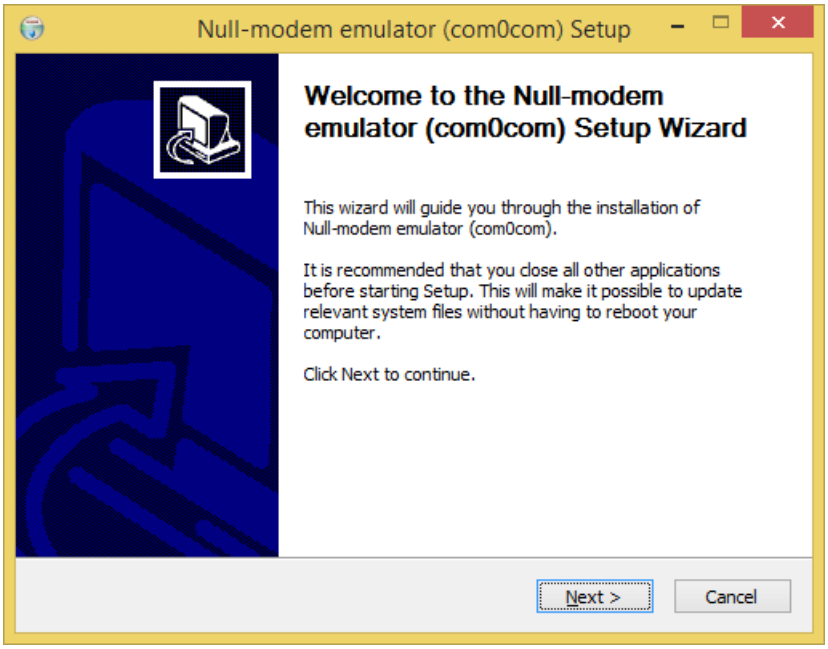
La seguente guida si riferisce alla versione 1 di Seneca Ethernet to Serial Connection, le versioni successive sono analoghe.

7.2.1. INSTALLAZIONE DEL DRIVER SENECA SERIAL TO ETHERNET

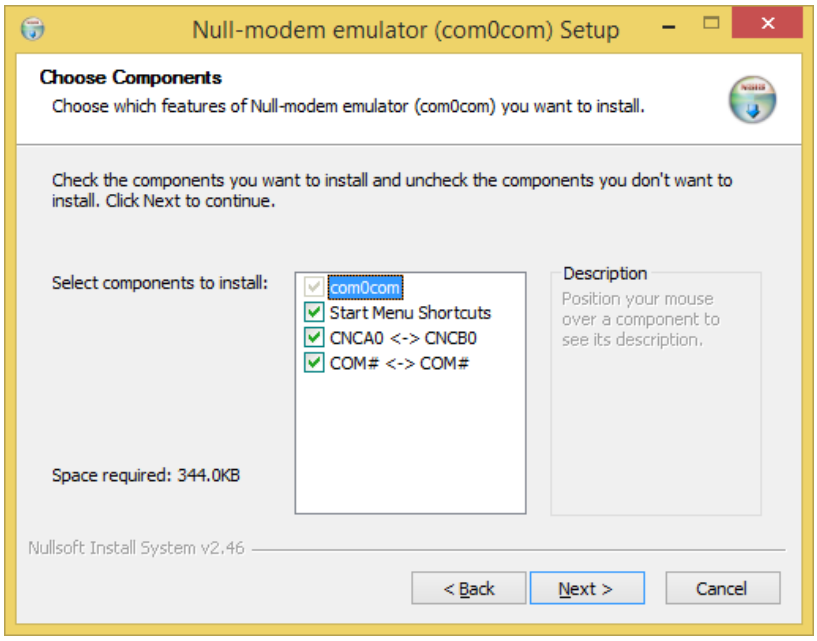
Seneca Ethernet to Serial Connect è compatibile con sistemi Windows a 32 e 64 bit.
Fare doppio clic sul programma di installazione



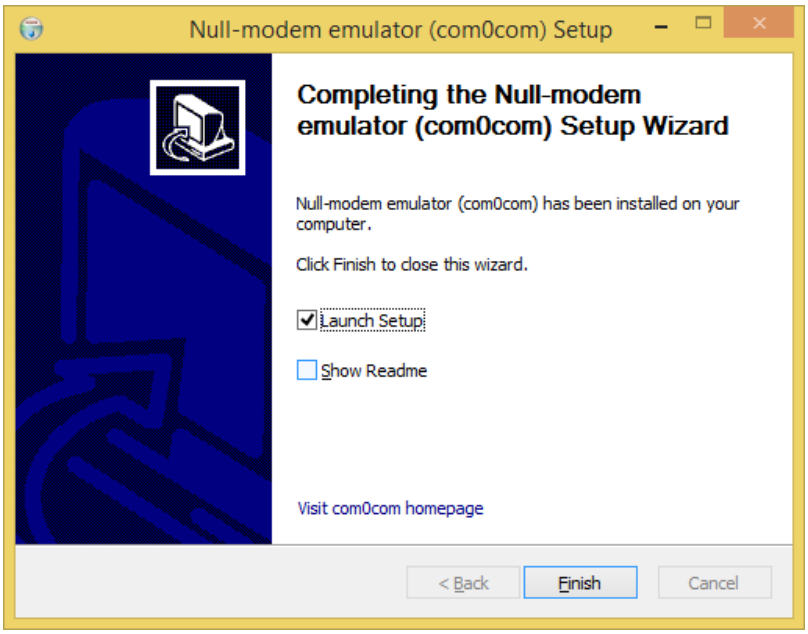
Dopodiché verrà installato il driver com0com:



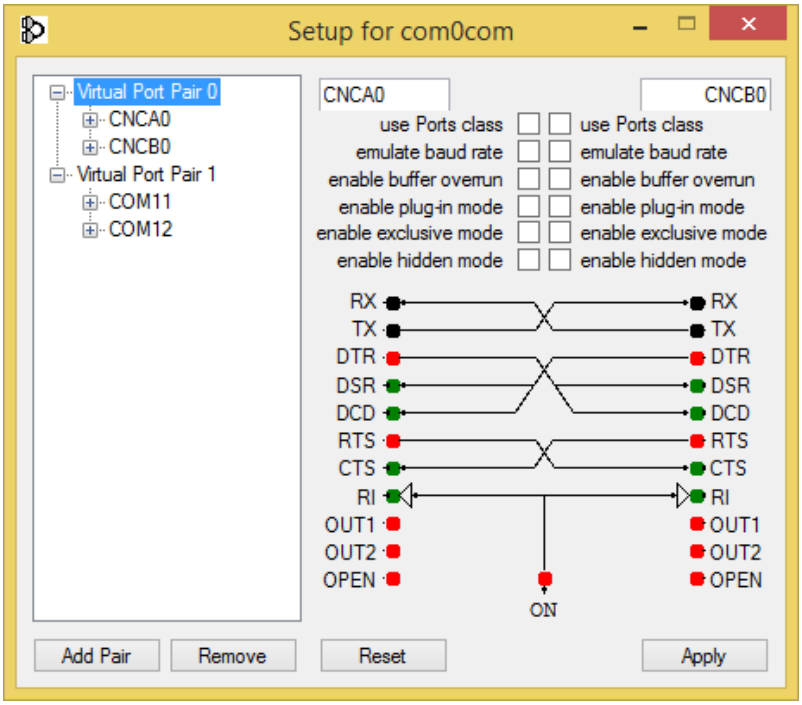
Selezionare i nomi delle porte virtuali CNCA0<->CNCB0 e COM#<->COM#:



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:

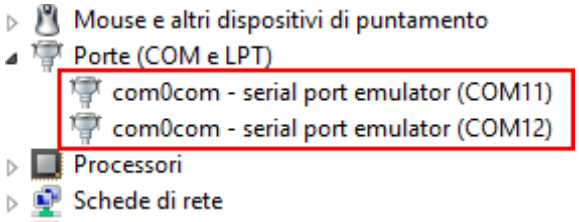
COM11, COM12 (si noti che nel vostro sistema il com# può essere differente).

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.

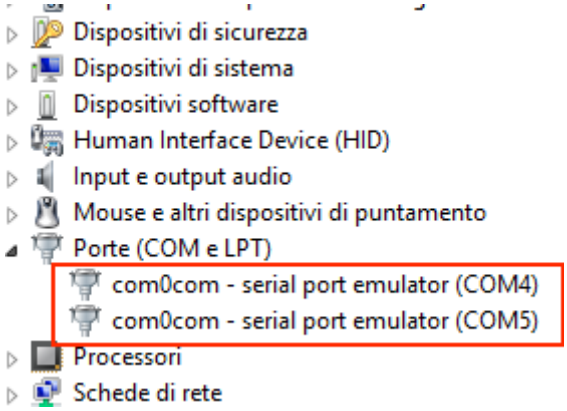
Confermare l'installazione del driver con “Apply”.

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



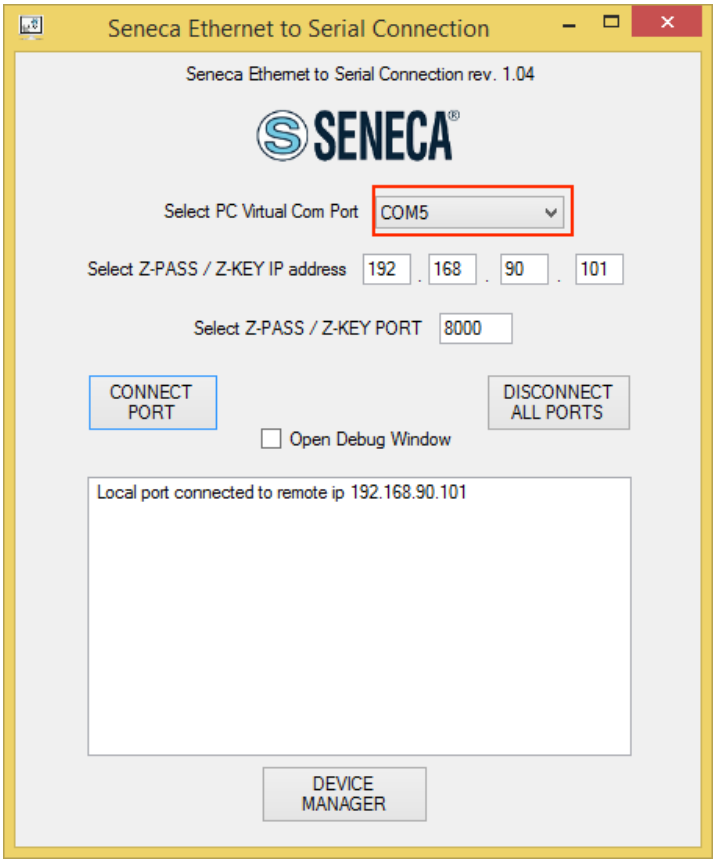
7.2.2. SELEZIONE DELLA PORTA COM PER SENECA ETHERNET TO SERIAL TO CONNECT

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):

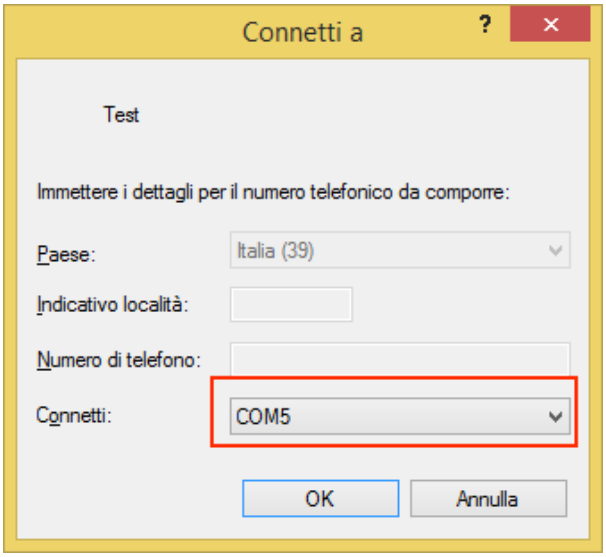


Il software utilizzerà una sola porta (la porta giusta nel setup di com0com), verranno visualizzate solo le porte com0com.

Selezioniamo la COM5 nel connettore Seneca ES:

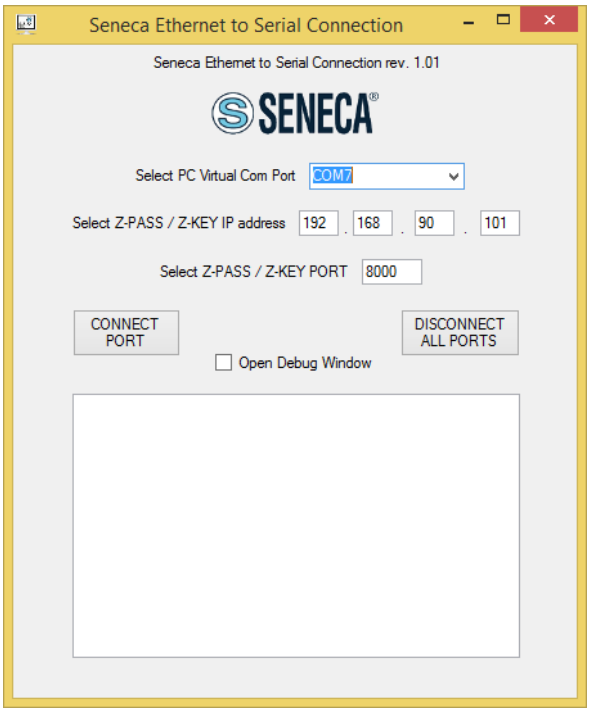


Ora utilizzate la stessa COM5 (ad esempio nel software terminale)



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

7.2.3. CONFIGURAZIONE DI SENECA SERIAL TO ETHERNET



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

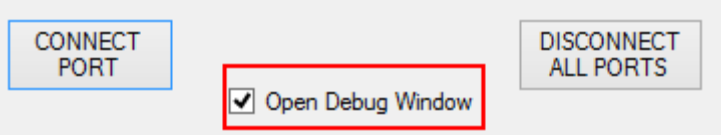
Cliccare su "CONNECT PORT"

Se è necessario collegare un'altra com seriale ad un altro dispositivo Seneca, configurare la nuova porta com e il nuovo indirizzo IP, dopodiché premere il pulsante “CONNECT PORT”.

Per scollegare tutte le porte, cliccare su "DISCONNECT ALL PORTS”

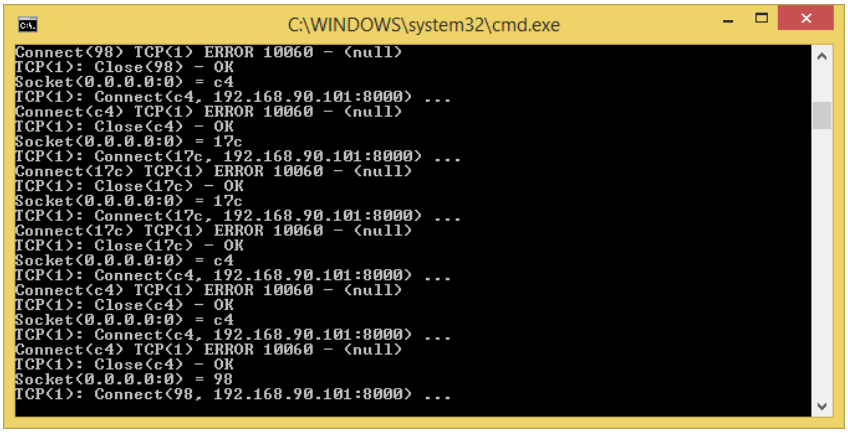
7.2.4. DEBUG DEL COLLEGAMENTO

Prima di cliccare su "CONNECT PORT", potete scegliere di aprire una finestra di debug per verificare la connessione



Poi cliccare su "CONNECT PORT”

Se vedete "Connect Error" come nell’immagine seguente:

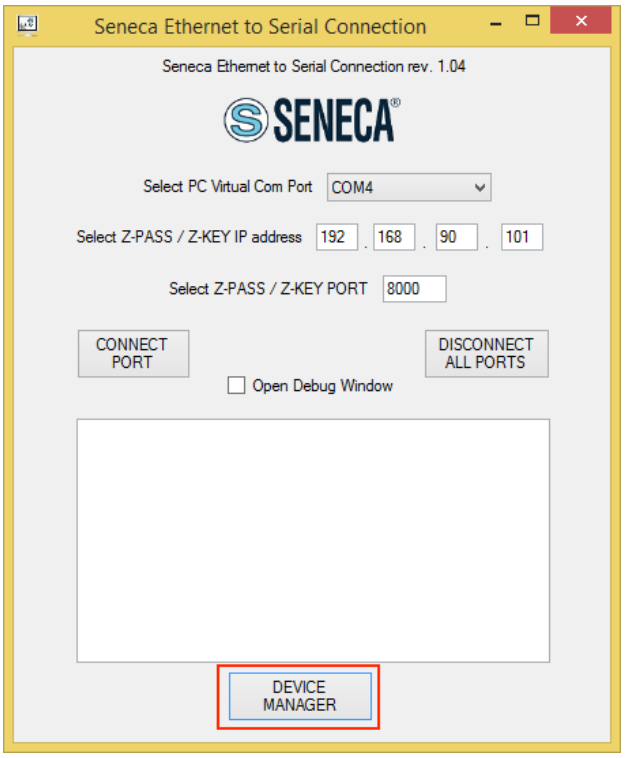


controllare la configurazione (indirizzo IP e porta TCP).

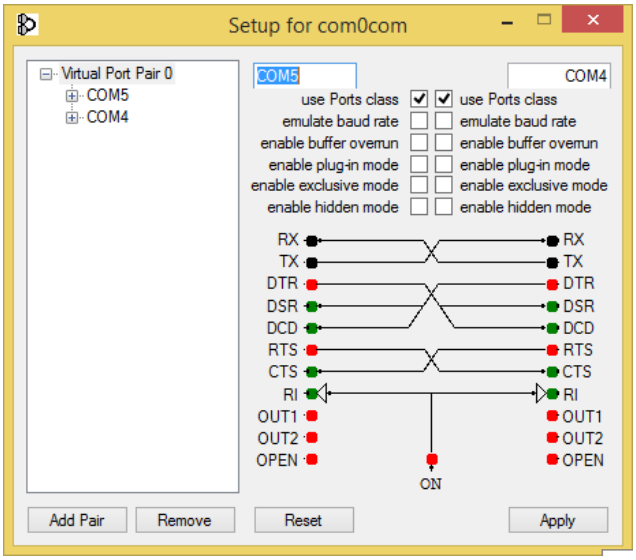
7.2.5. MODIFICA DEL NUMERO DI PORTA

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

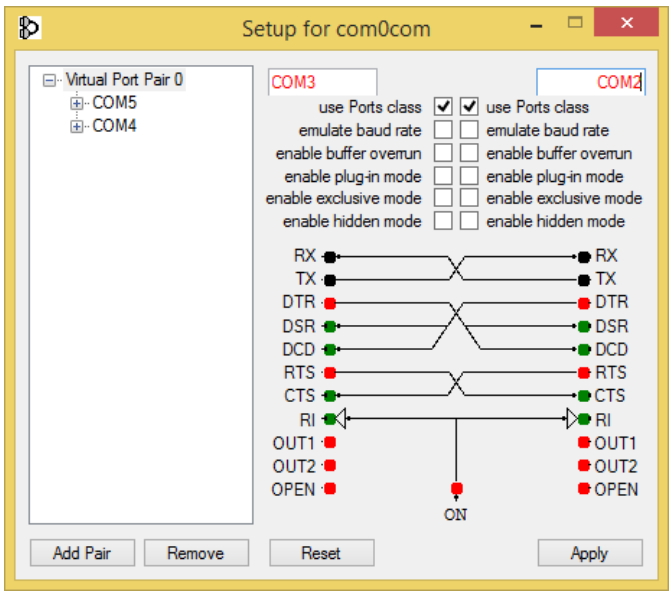
Nel nostro caso la coppia COM creata è COM4/COM5, vediamo la procedura per cambiarle in COM2/COM3
Cliccare sul pulsante "DEVICE MANAGER”:



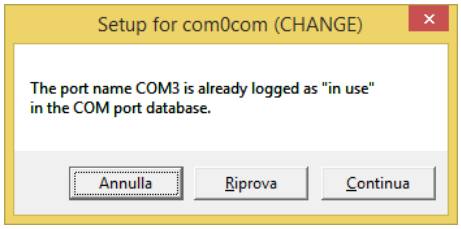
Si aprirà la finestra di configurazione di com0com:



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

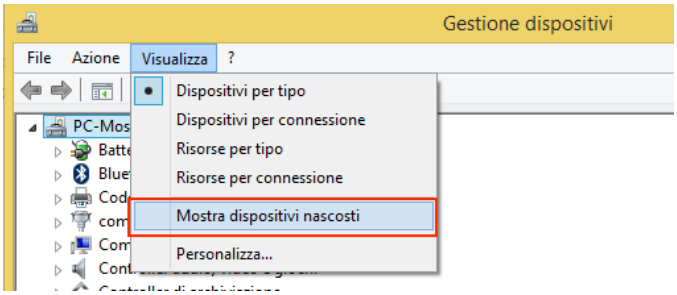


A volte la COM può essere contrassegnata “in uso”:

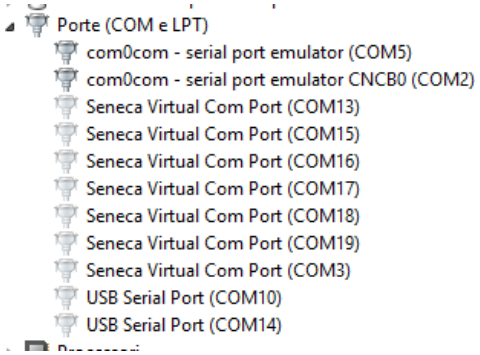


Se è necessario utilizzare questo numero COM, cliccare su "Continua", quindi andare su configurazione dispositivo.

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

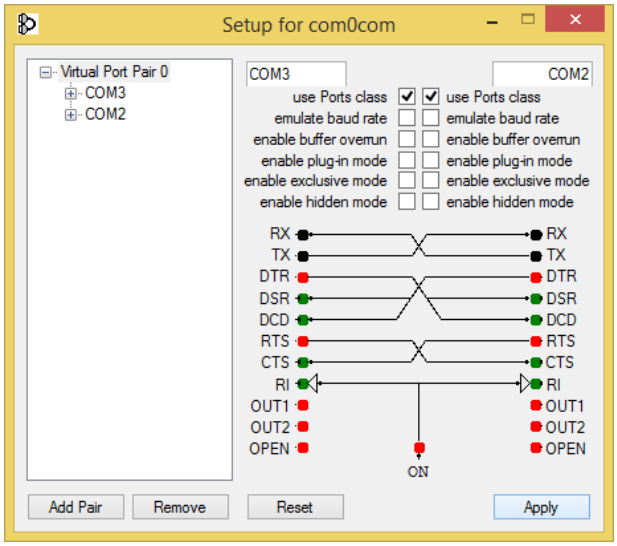


Ora tutte le porte non utilizzate sono visualizzate in trasparenza (anche la nostra COM3):

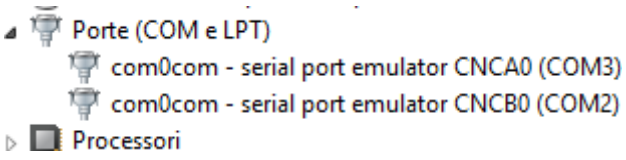


Ora selezionate la porta COM3 e cliccate su “Disinstalla”:

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

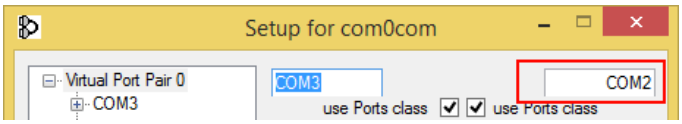


Infine cliccate su "Apply", ora viene creata la coppia COM3/COM2:

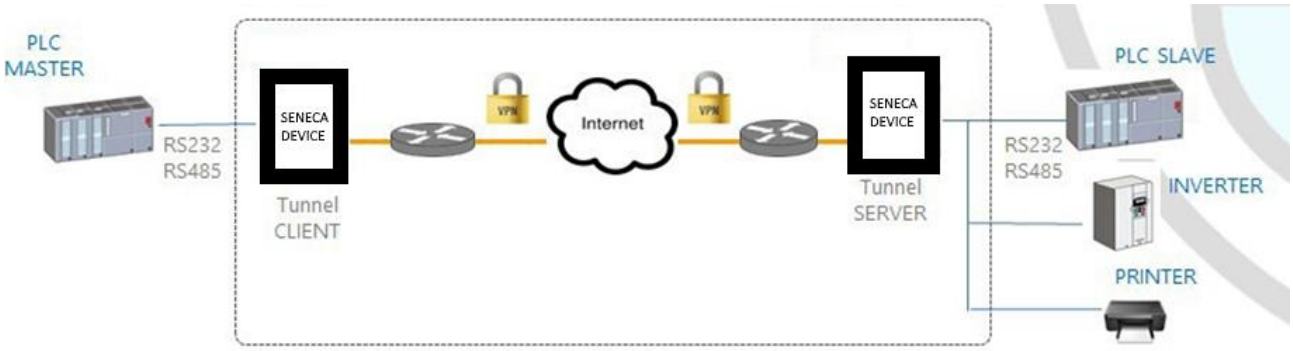


ATTENZIONE!

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



7.3. 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.

7.4. TUNNEL SERIALE PUNTO A PUNTO SU UDP

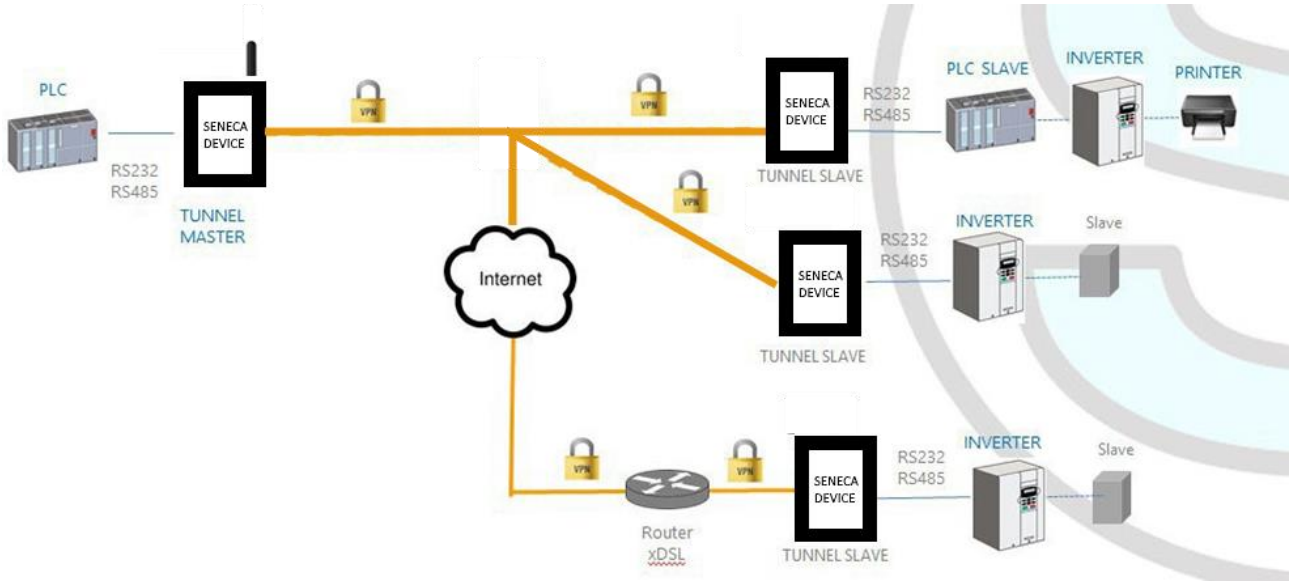
Il modo operativo Serial Tunnel Point-to-Point su UDP è molto simile a quello del TCP.

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.

7.5. TUNNEL SERIALE DA PUNTO A MULTIPUNTO



Il Serial Tunnel Point-to-Multipoint permette di creare un tunnel con un master e più di uno slave; su lato master, i dati ricevuti dalla linea seriale vengono inviati a tutti gli slave, tramite la modalità di trasmissione *multicast*, in pacchetti UDP.

Per far funzionare il multicast, il master e gli slave devono far parte dello stesso gruppo multicast, per cui esiste un parametro "Gruppo Multicast" che deve essere opportunamente impostato; inoltre, per la configurazione del master devono essere definiti i parametri "Destination Port" e "Multicast Interface", quest'ultimo deve essere impostato per selezionare l'interfaccia di rete che permette di inviare i pacchetti; per la configurazione dello slave sono richiesti "Listen Port" e "Multicast Interface"; quest'ultimo deve essere impostato per selezionare l'interfaccia di rete che permette di ricevere i pacchetti.

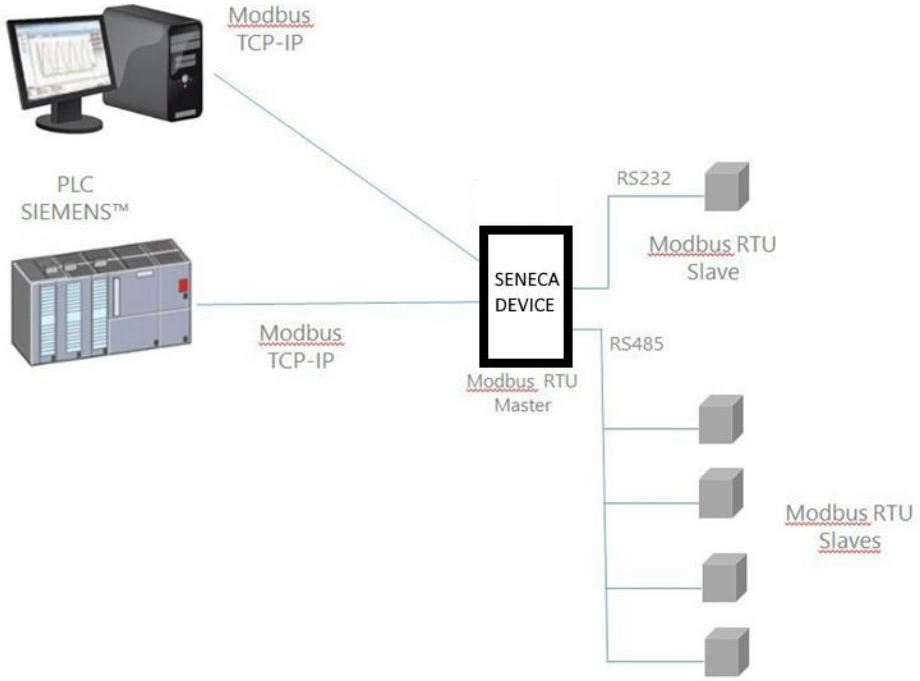
ATTENZIONE!

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

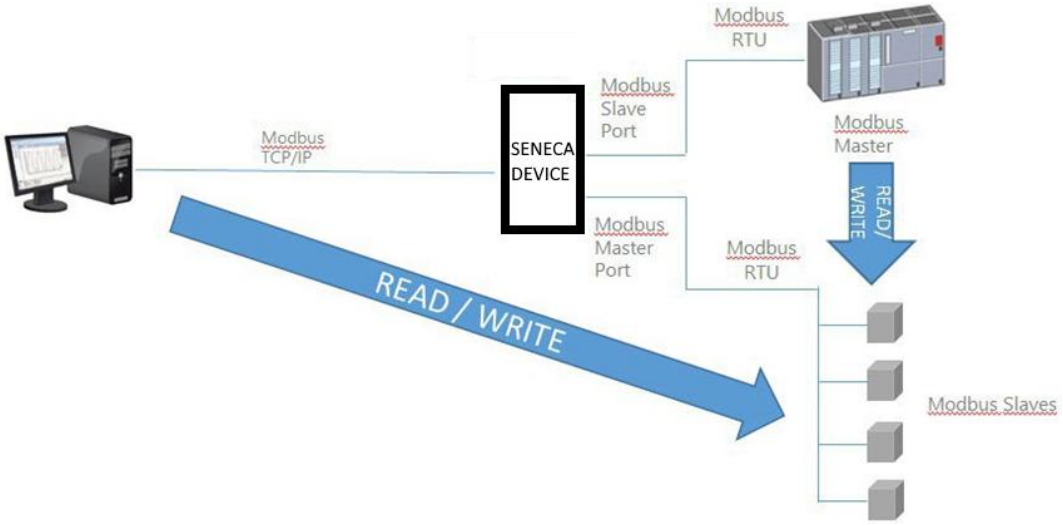
8. MODBUS GATEWAY CON MEMORIA SHARED (CONDIVISA) (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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 sempre disponibili in una memoria condivisa, leggibile tramite Modbus TCP/RTU.
La modalità supporta fino a 2000 tag e fino a 32 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.

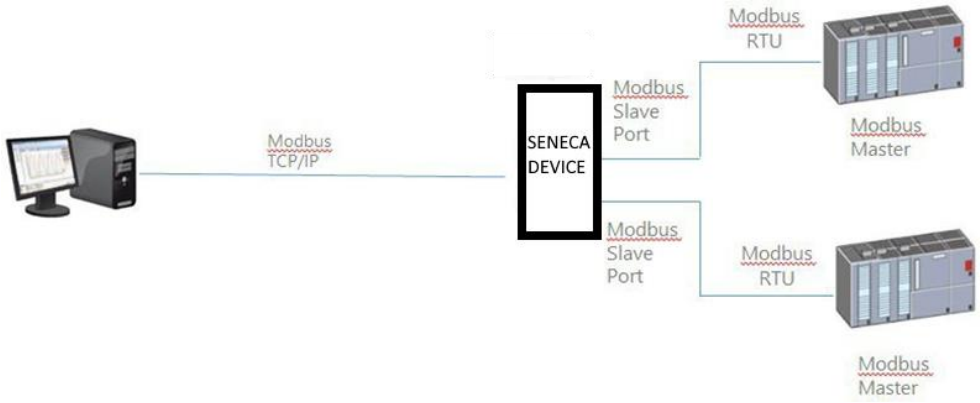


Nella figura sopra, due porte seriali sono configurate come Modbus RTU Master.



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 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.

9. IL DATALOGGER (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Quando la funzionalità Modbus Gateway con Shared Memory è abilitata 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
- 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" del file di log, cioè i file più vecchi vengono sovrascritti dal nuovo.

I 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:

```
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 interno viene cancellata

10. REGOLE LOGICHE (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Il dispositivo può essere configurato con un massimo di 2000 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

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

11. ALLARMI (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Per quanto riguarda gli allarmi Sono disponibili una serie completa di parametri per definire il comportamento degli allarmi, come indicato nella pagina "Configurazione degli allarmi"; l'intero stato degli allarmi può essere visualizzato nella pagina "Riepilogo degli allarmi” e lo storico degli allarmi può essere recuperato nella pagina "Cronologia degli allarmi".

Inoltre, nella pagina "Tag View", le colonne "ALARM" e "ANALOG DANGER ALARM" mostrano lo stato corrente degli allarmi per ogni tag.
Le azioni possono essere utilizzate per l'invio di un SMS, EMAIL o HTTP POST, MQTT …;

12. VPN

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 (o una macchina virtuale) che permette all'utente di configurare facilmente due tipi alternativi di VPN:
"VPN " Single LAN (Always on)
VPN "Point-to-Point" (On demand)

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 "punto a punto":
- 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:
Layer 2
- può trasportare qualsiasi protocollo di rete (ad esempio il protocollo profinet)
- causa più traffico sul tunnel VPN rispetto il layer3

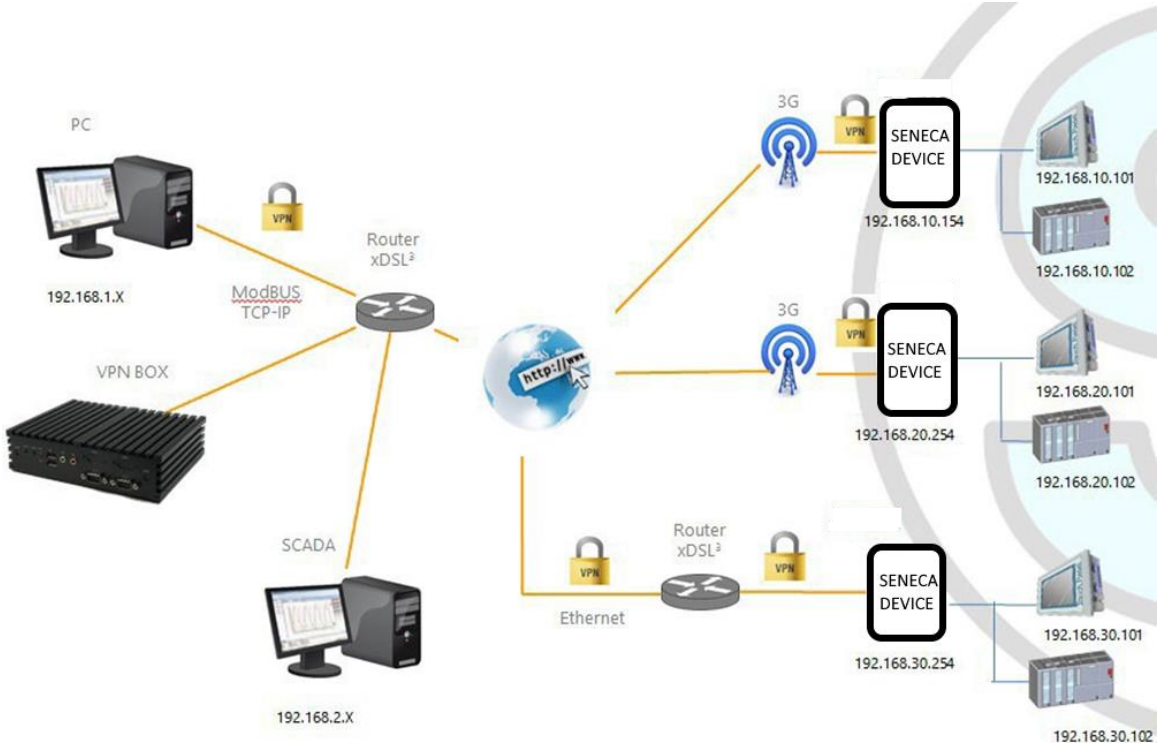
Layer 3
- può trasportare solo traffico IP
- il traffico layer2 (ad es.: DHCP) non viene trasportato
- riduce i costi di gestione del traffico, trasporta solo il traffico destinato ai client

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")

Una descrizione dettagliata del "VPN Box2" si trova nel Manuale d'uso di VPN BOX 2.

Una descrizione dettagliata dei parametri di configurazione di una VPN è riportata nei seguenti due sottoparagrafi.

12.1. 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.

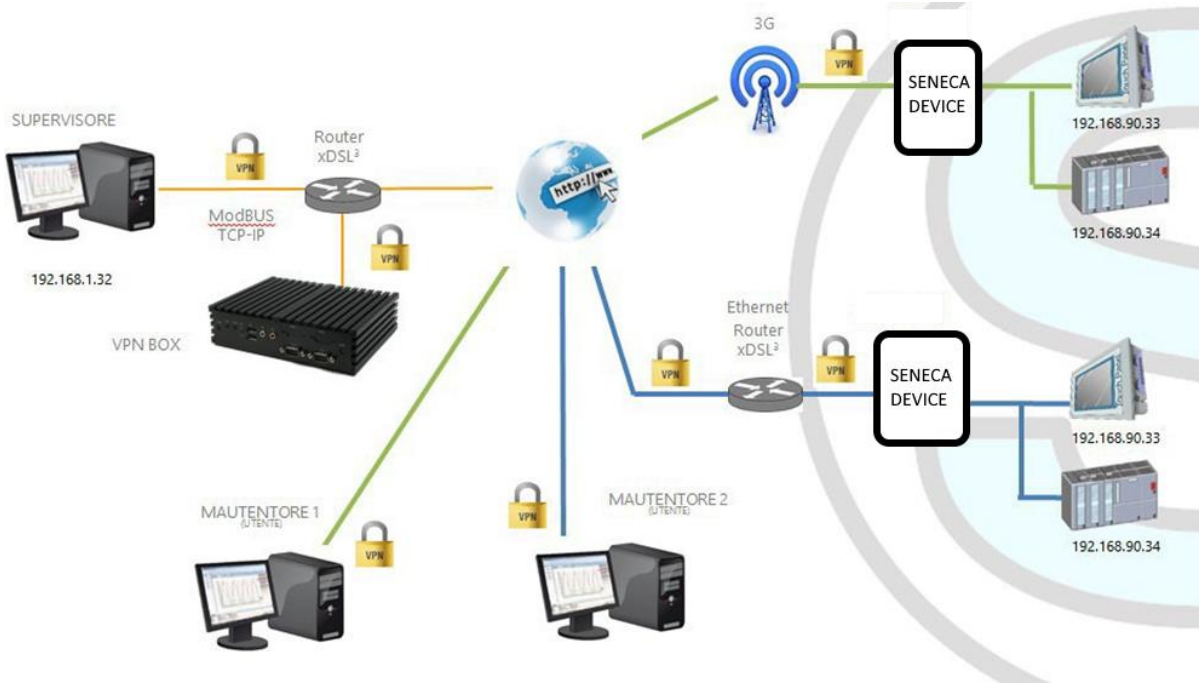
Inoltre, due dispositivi che si trovano in due diverse LAN della stessa rete VPN (ad es: 192.168.10.101 e 192.168.20.102) possono connettersi tra loro, sempre utilizzando i loro indirizzi IP locali.

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".

12.2. 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

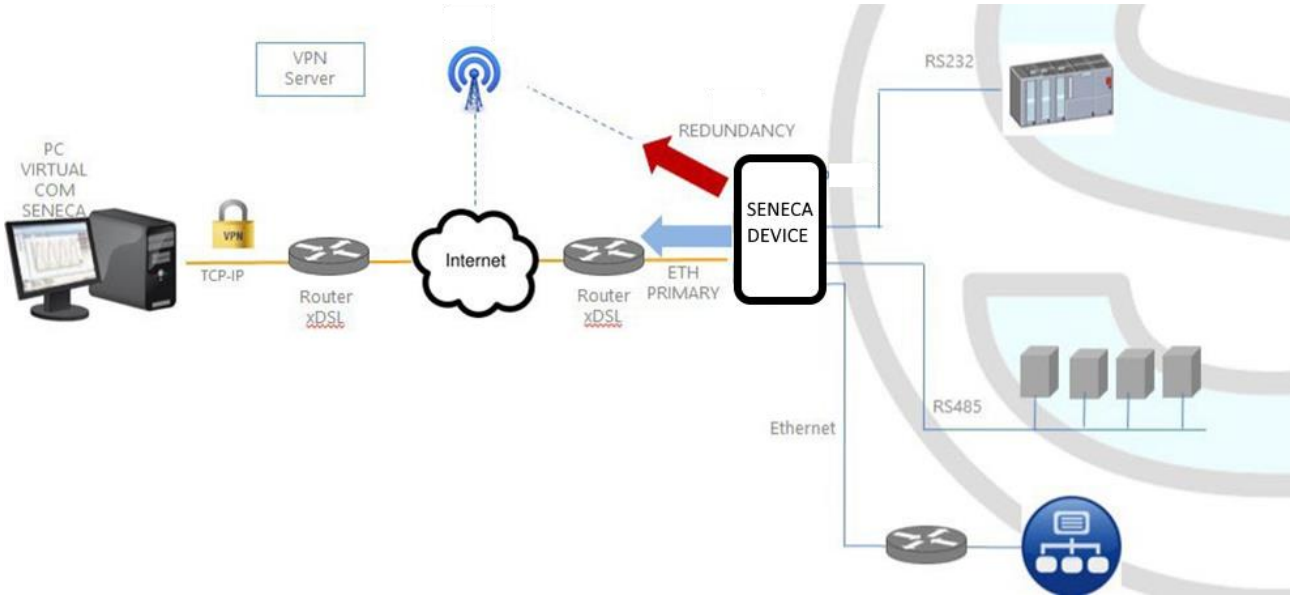
13. ROUTER

Come già detto in precedenza, la funzionalità "Router" instrada i pacchetti tra l'interfaccia LAN (Ethernet) e l'interfaccia interfaccia WAN (Mobile Network) / WI-FI oppure connessione mobile.

Più specificamente, una caratteristica importante del Router è il cosiddetto "IP forwarding"; ciò significa che quando il dispositivo riceve un pacchetto non destinato ad esso, non scarta il pacchetto ma lo inoltra alla sua effettiva destinazione; quando un pacchetto viene instradato dalla LAN alla WAN, il dispositivo esegue anche il cosiddetto "IP masquerading", ovvero la sostituzione dell'indirizzo IP di origine con l'indirizzo IP dell'interfaccia WAN.
Un'altra importante caratteristica è la disponibilità di un server/forwarder DNS, che può risolvere i nomi con un DNS esterno o senza.

Inoltre, è disponibile un server DHCP che assegna indirizzi IP ai client collegati sulla porta LAN (oppure sulla WI-FI quando impostata in modalità Access Point); qui, è possibile configurare la gamma di indirizzi utilizzati dal server e l'orario di locazione.
C'è anche la possibilità di definire delle regole di "Port Forwarding" o "Server Virtuali"; utilizzando questi è possibile, ad esempio, reindirizzare i pacchetti ricevuti da una porta TCP o UDP ad un'altra porta o indirizzo IP.
In alternativa all'utilizzo delle regole di "Port Forwarding", le funzionalità Router + VPN consentono l'utilizzo di indirizzi locali come mostrato nel capitolo precedente; nella configurazione del router è presente un flag per abilitare queste funzionalità.

14. RIDONDANZA DELLA RETE



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.

15. DISABILITAZIONE DELLA CONNESSIONE REMOTA

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

16. AUTO APN

La funzione Auto-APN consente al dispositivo dotato di modem cellulare di stabilire connessioni dati mobili senza che l'utente debba configurare i dati APN per la SIM in uso.

Questo si ottiene utilizzando il codice IMSI contenuto nella SIM e, possibilmente, alcuni altri dati disponibili sulla SIM. In alcuni casi particolari, tuttavia, quando si utilizza un "APN personalizzato", la funzione Auto-APN può essere disabilitata, impostando il parametro "APN Mode" su "Manual".

17. PROTOCOLLO CLIENT HTTP REST (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

La comunicazione tra RTU e Cloud può avvenire tramite protocollo HTTP con una chiamata di tipo POST.
La rappresentazione della chiamata è REST (REpresentational State Transfer) dove i dati sono configurati come quelli di un classico web FORM ma tramite JSON (JavaScript Object Notation). Per ulteriori informazioni sul protocollo di comunicazione HTTP POST si rimanda a "Seneca HTTP POST Communication Protocol" (è possibile richiedere il documento all'indirizzo supporto@seneca.it).
Il dispositivo è compatibile sia con il prodotto Seneca Cloud Box che con un server generico attraverso il protocollo di comunicazione HTTP POST.
Questo protocollo è dotato di un set di API HTTP POST (RESTFUL); la relativa documentazione può essere fornita da Seneca ai clienti che desiderano sviluppare il proprio software lato server; per informazioni, contattare Seneca Service & Support all'indirizzo supporto@seneca.it.

Il protocollo HTTP POST può essere abilitato insieme agli altri metodi di trasferimento (MEMORIA, FTP, EMAIL, …); tuttavia, quando il protocollo HTTP POST è abilitato, le seguenti modifiche si applicano al comportamento del Data Logger:

- può essere abilitato un solo gruppo di registrazione;
- il periodo di campionamento è un multiplo di 30 secondi;
- ogni campione viene inviato al server http in un messaggio *LOG*, trasportato da un HTTP POST

Il protocollo Seneca HTTP POST consente inoltre al server di eseguire le seguenti azioni sullo 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 HTTP POST, utilizzata per memorizzare i messaggi di log mentre non è possibile inviarli al server; questa cache può contenere fino a 3000 messaggi:

18. PROTOCOLLO SERVER OPC UNIFIED ARCHITECTURE (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.

In particolare, il server OPC-UA "esporta" i tag della Shared Memory; quindi, utilizzando un OPC-UA client sarà possibile leggere e scrivere direttamente a tutti i tag.

19. 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

19.1. CARATTERISTICHE DI MQTT (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Il protocollo MQTT può essere abilitato insieme agli altri metodi di trasferimento (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

20. STRATON PLC (SOLO MODELLI R-PASS-S, Z-TWS4-RT-S, Z-PASS2-RT-S)

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.

20.1. SCRIVERE, SCARICARE ED ESEGUIRE IL PRIMO PROGRAMMA

Per consentire allo sviluppatore PLC di creare facilmente applicazioni Straton per CPU 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"

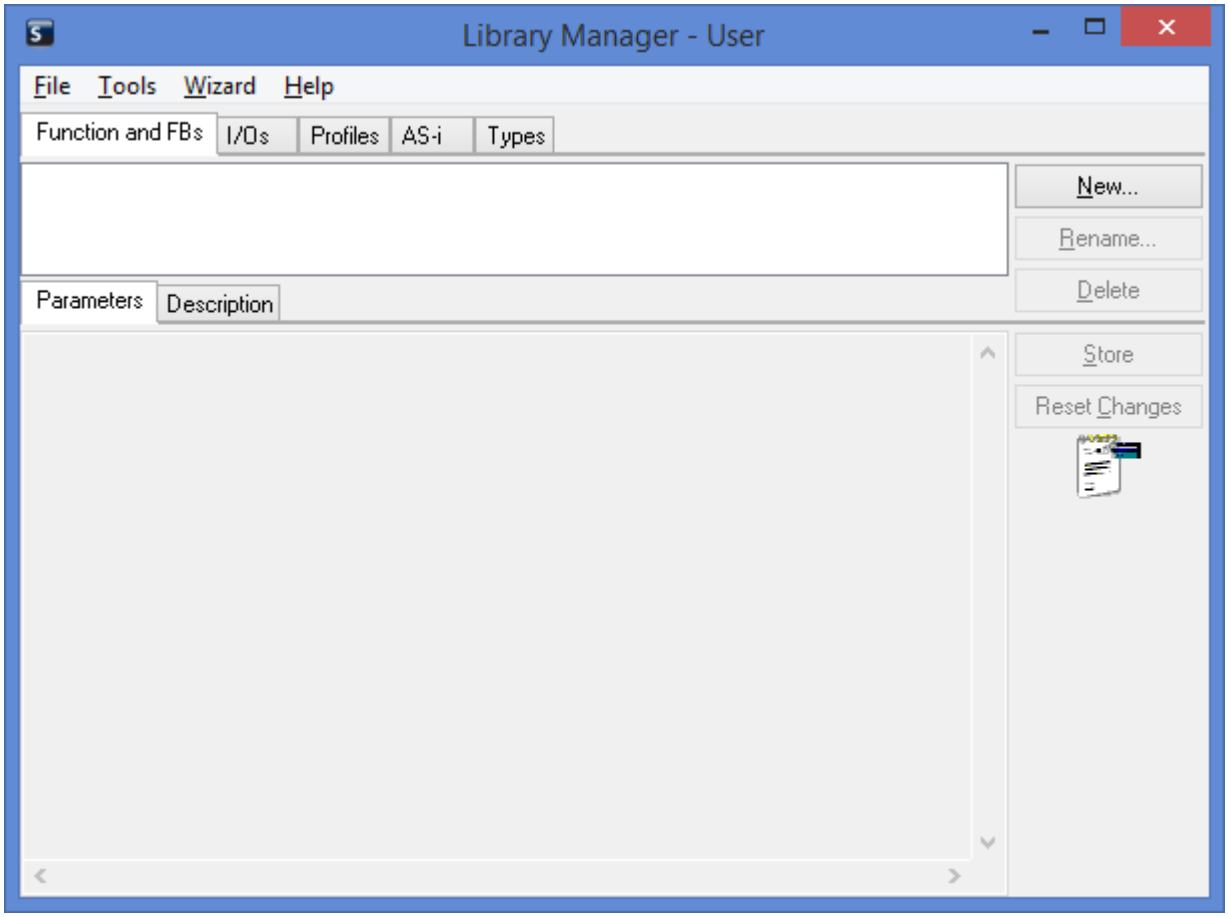
• una libreria “User Defined Function Block” (UDFB), in linguaggio ST, che semplifica l'utilizzo dei suddetti FB, fornendo un accesso più semplice e di “livello superiore” alle loro funzionalità.

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

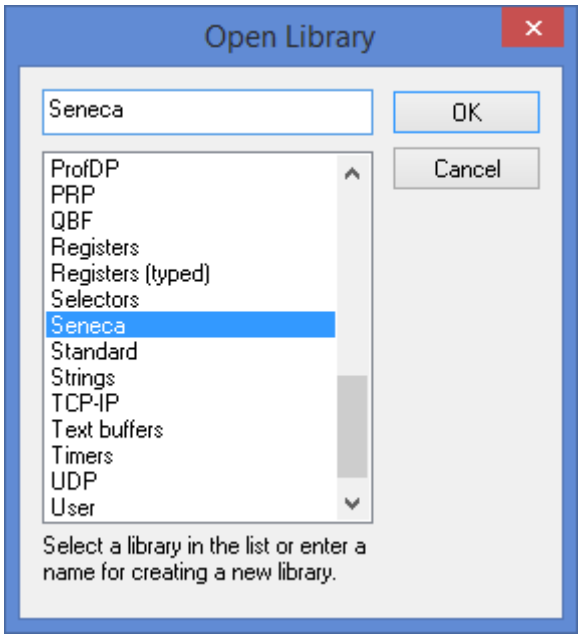
Se, per qualche motivo, non è possibile eseguire il programma di installazione, le librerie e i modelli di cui sopra possono essere installati manualmente come descritto nel successivo sottoparagrafo:

20.1.1. INSTALLAZIONE MANUALE DI LIBRERIE E TEMPLATE IN STRATON

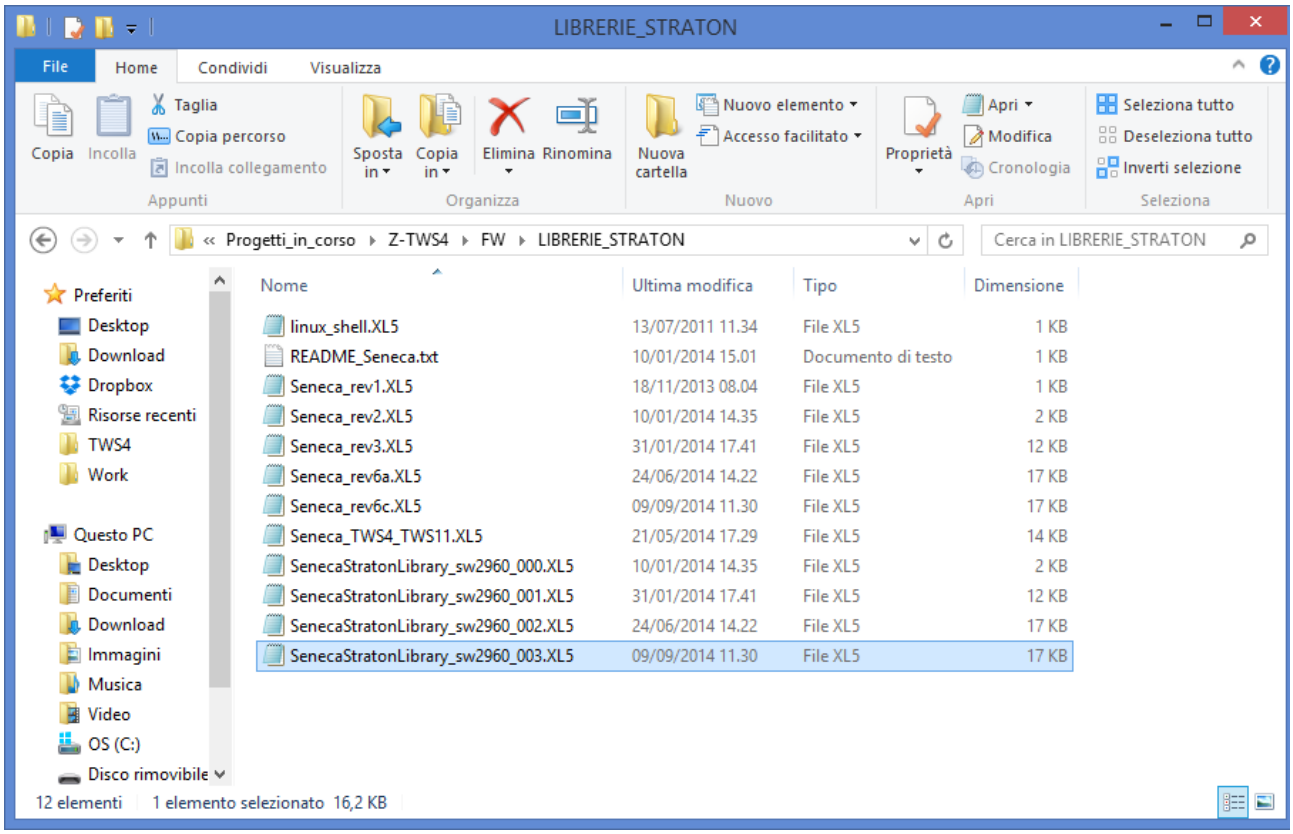
I seguenti passaggi sono necessari per integrare le librerie e i profili Seneca nell'IDE Straton.
Innanzitutto, dobbiamo aggiungere la libreria FB Seneca (file SenecaStratonLibrary.XL5) all'IDE, utilizzando lo strumento "Library Manager":

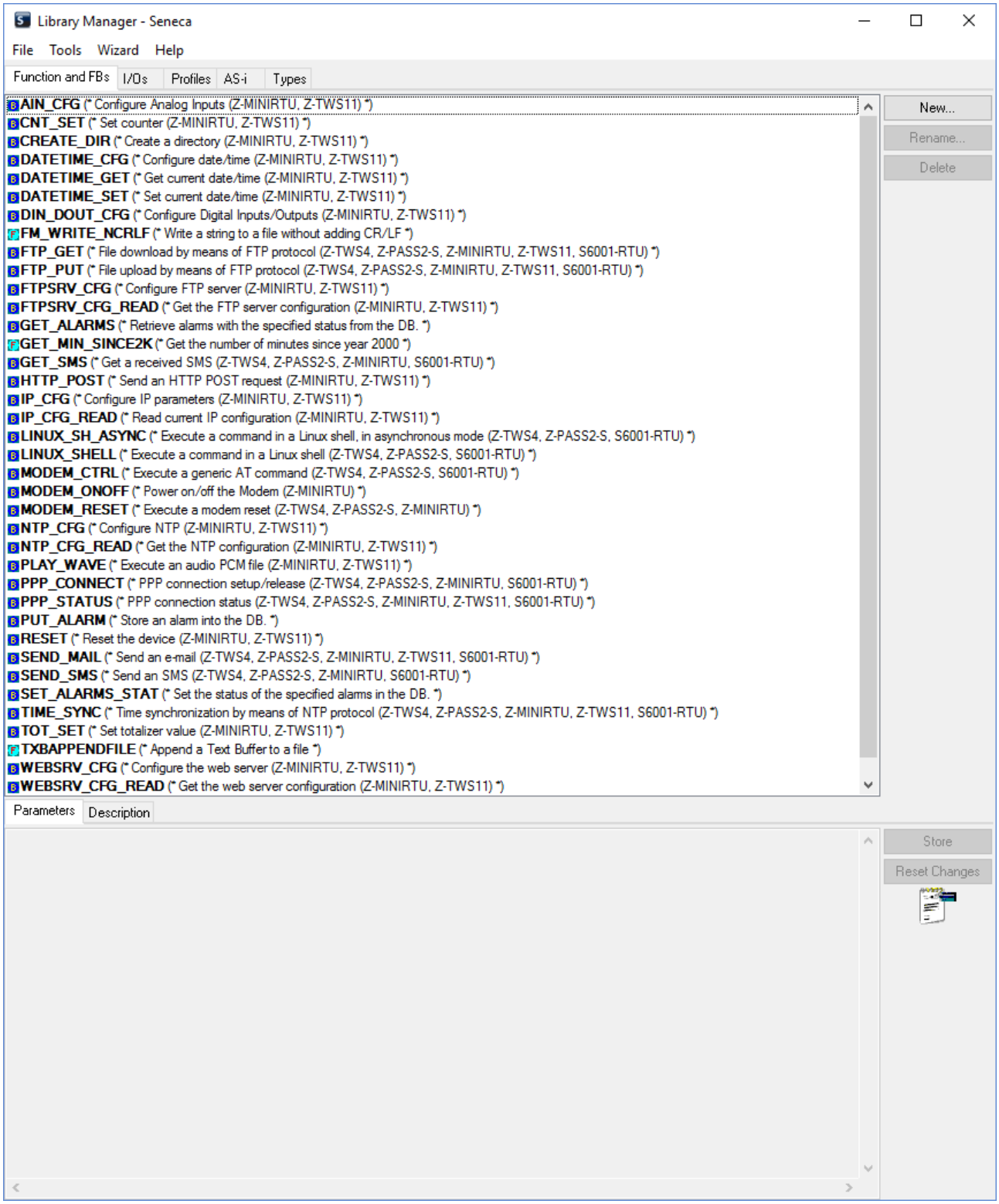


Selezionare l'opzione "File / Open Library " e inserire il nome "Seneca" per creare la nuova libreria Seneca.



Quindi, importare la Libreria (menu “Tools / Import”):



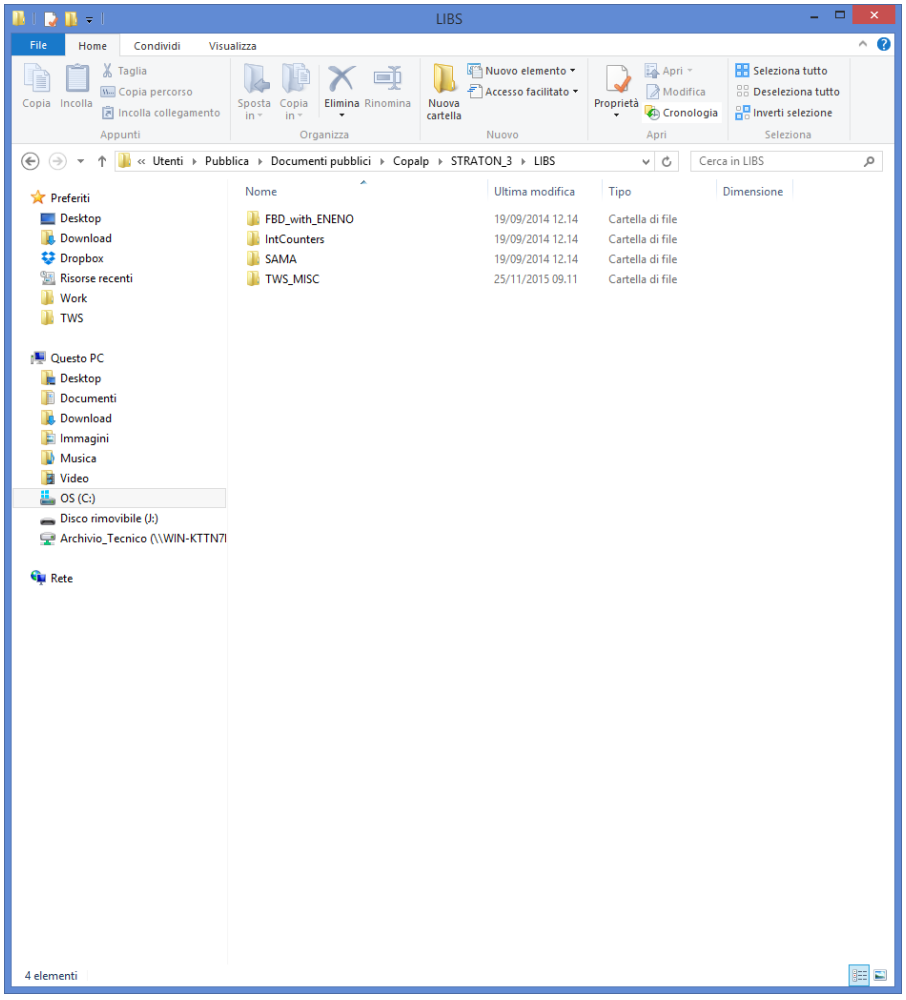


Salvare la libreria (menu “File / Save Library”).

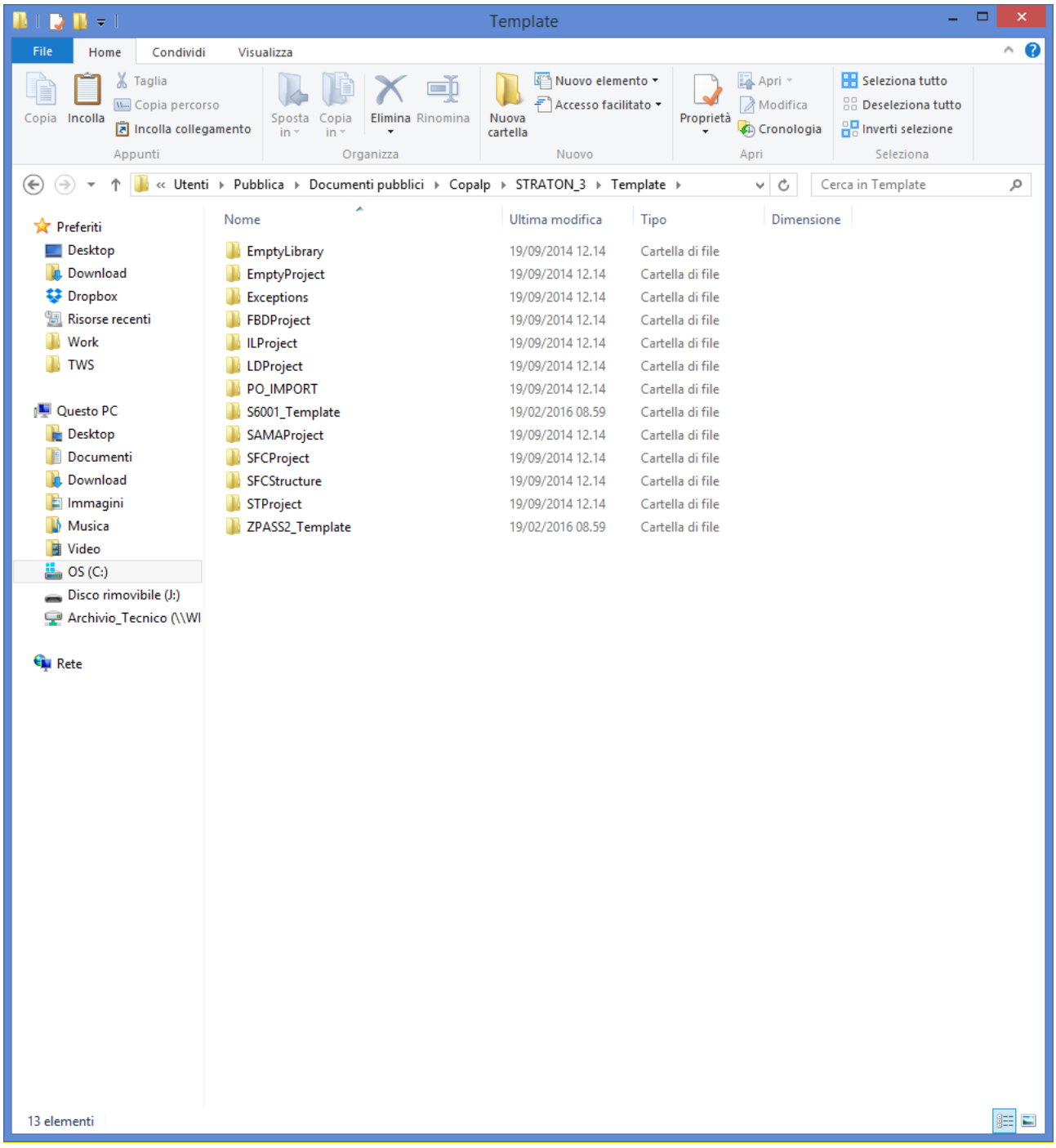
La procedura per aggiungere la libreria Profili all'IDE è identica a quella appena spiegata; l'unica differenza è che deve essere selezionato il file SenecaStratonProfiles.XL5 (invece del file SenecaStratonLibrary.XL5).

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\Copalp\STRATON\LIBS:



Le cartelle dei template devono essere copiate nella directory seguente:
C:\Users\Public\Documents\Copalp\STRATON\Template



20.2. PROTOCOLLI DI ENERGY MANAGEMENT

Il PLC Straton supporta i seguenti protocolli di “Energy Management” (opzionali):

- IEC 60870-5-101 (Master/Slave)
- IEC 60870-5-104 (Master/Slave)
- IEC 61850 (Master/Slave)

L'attivazione di questi protocolli è basata su licenza.

Si prega di contattare Seneca per avere maggiori informazioni sull'ottenimento della licenza per i protocolli di Energy Management.

20.3. PROTOCOLLO SNMP V2C

Il PLC Straton supporta il protocollo SNMP versione V2C. Per maggiori informazioni fare riferimento al manuale di Straton.

21. OPZIONE R-COMM (SOLO MODELLO R-PASS)

Per i modelli R-PASS è possibile acquistare l'hardware R-COMM che permette (a seconda del modello) di aggiungere un modem 4G con posizionamento GNSS e un UPS che permette il funzionamento di R-PASS fino ad 1 ora senza alimentazione esterna.
Per l'installazione di R-COMM fare riferimento al manuale installazione di R-COMM, per i modelli disponibili fare riferimento al sito seneca.

22. CONFIGURAZIONE TRAMITE WEB SERVER (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

I dispositivi possono essere completamente configurati tramite una serie di pagine di configurazione web.
Per accedere al sito di configurazione, è necessario connettere il browser all'indirizzo IP sulla porta 8080, ad es:
http://192.168.90.101:8080
e, quando richiesto, fornire le seguenti credenziali (valori predefiniti):
Nome utente: admin
Password: admin
Si arriva alla pagina "Summary", descritta nel paragrafo seguente.

22.1. SUMMARY

In questa pagina sono rappresentate le principali informazioni sullo stato del dispositivo e sull'utente attualmente loggato.

22.2. NETWORK AND SERVICES

Nella tabella seguente 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.

Campo	Significato
NETWORK	Sezione dedicata alla configurazione dei parametri di rete delle porte ethernet LAN/WAN.

WEB SERVER	Sezione dedicata alla configurazione del web server.
FILE TRANSFER	Sezione dedicata alla configurazione del protocollo FTP
NETWORK REDUNDANCY Enable	Permette di abilitare la ridondanza di rete impostando come rete primaria la porta WAN e come secondaria la porta WI-FI. Per SSD il Wi-Fi deve essere presente.
NETWORK REDUNDANCY Ping Address	Indirizzo che il sistema utilizza per verificare la presenza di connettività. Questo indirizzo deve essere diverso da quello impostato per il parametro "DNS Server", altrimenti viene visualizzato un errore.
WATCHDOG Enable	Abilita o no il Watchdog nel dispositivo
WATCHDOG Timeout (s)	Timeout del watchdog, in secondi; quando il watchdog è abilitato, se non viene aggiornato per questo intervallo di secondi, il sistema verrà riavviato. I valori possibili sono compresi nell'intervallo [30..3600 s].
R-COMMM Available	Configura se è attivo o no il funzionamento con l'opzione R-COMM
R-COMM UPS Mode	Configura il tipo di funzionamento dell'UPS. 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, Shutdown immediatly, Shutdown on low power. "OFF" non utilizza l'UPS di R-COMM per alimentare R-PASS "Shutdown immediatly" 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
DEBUG LOGS Enable	Flag per abilitare/disabilitare i log di debug

22.3. PLC CONFIGURATION (SOLO MODELLI R-PASS-S, Z-TWS4-RT-S, Z-PASS2-RT-S)

In questa pagina è possibile impostare i parametri di connessione con il workbench di Straton, attivare una licenza opzionale (ad esempio per i protocolli di energy management) e impostare il funzionamento della porta seriale COM1 tra Rs232/RS485/Z-MBUS.
Z-MBUS è un dispositivo opzionale che permette di connettere il dispositivo ad un bus METERBUS.

22.4. WI-FI CONFIGURATION (SOLO MODELLO R-PASS)

Permette di configurare i parametri della porta WI-FI.
Qui sotto un estratto dei parametri principali:

Campo	Significato

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

22.5. PORTE SERIALI (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Questa pagina permette di configurare le porte seriali (baud rate, bit di stop, configurazioni RS232/RS485 etc…).

22.6. CONFIGURAZIONE I/O

Campo	Significato
IO CONFIGURATION	
INPUT/OUTPUT1 MODE	Remote connection disable Permette di utilizzare il pin come ingresso. Se alto blocca l'accesso VPN remoto General Input Permette di utilizzare il pin come ingresso digitale General Output Permette di utilizzare il pin come Uscita digitale
INPUT/OUTPUT2 MODE	Remote connection active Permette di utilizzare il pin come uscita, se attiva indica la presenza di un accesso VPN remoto Local Alarm: è un ingresso che viene collegato ad un PLC di controllo, quando è alto indica un errore generale che è visibile da remoto tramite l'interfaccia di stato di Seneca VPN box. Remote Toggle è un'uscita comandabile dall'interfaccia di stato di Seneca VPN box. General Input Permette di utilizzare il pin come ingresso digitale General Output Permette di utilizzare il pin come Uscita digitale
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: Blocco della VPN Connection (VPN Service ed Internet attivi) Blocco della VPN Service (Internet attivo) Blocco dell'accesso ad internet (nel dispositivo è bloccato sia internet che la VPN)

22.7. REAL TIME CLOCK SETUP

Campo	Significato
NTP	
Enable	Flag per abilitare/disabilitare la sincronizzazione della data/ora con un server Network Time Protocol
Server primary	Indirizzo IP o FQDN20 del Server NTP primario
Server secondary	Indirizzo IP o FQDN del Server NTP secondario
Timezone	Fuso orario

22.8. GATEWAY CONFIGURATION (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Questa pagina permette di configurare la tipologia di Gateway Ethernet-Seriale che si vuole utilizzare.
È possibile scegliere tra:

Modbus Ethernet to Serial (Conversione di tipo real time)
Modbus with Memory
Transparent

22.8.1. GATEWAY ETHERNET TO SERIAL

Campo	Significato
Enable	Flag per abilitare / disabilitare la funzionalità gateway Modbus da Ethernet a seriale sulla porta
Port	Porta TCP per accedere a Modbus da Ethernet a Serial Gateway Se vengono impostati tre valori distinti, vengono eseguite più istanze del Gateway, ognuna delle quali gestisce una singola porta seriale. Se lo stesso valore di porta è impostato per più di una porta seriale, la stessa istanza di Gateway gestirà due o più porte seriali (a seconda del dispositivo), ovvero le richieste Modbus RTU verranno inviate simultaneamente alle porte seriali.
Response Wait Time	Timeout alla ricezione delle risposte Modbus RTU Il valore è in millisecondi; i valori possibili sono compresi nell'intervallo [10 - 10000] ms.
Slave ID for Embedded I/O	ID slave utilizzato per accedere ai registri Modbus corrispondenti agli I / O digitali del dispositivo (se presenti) questo ID può essere utilizzato anche per accedere ai registri Modbus contenenti informazioni del posizionamento GNSS. Valori possibili: [1..255] nei dispositivi che ne siano dotati. Valido solo per la modalità Serial to Ethernet.

22.8.2. GATEWAY TRASPARENTE

Per ciascuna porta seriale con “Modalità gateway” = “Transparent”, i parametri di configurazione disponibili dipendono dal valore del parametro “Operating Mode” selezionato per la porta.
I possibili valori per il parametro “Operating Mode” sono:

- **None (valore di default)**
- **Virtual COM**
- **Serial Tunnel Point-to-Point on TCP**
- **Serial Tunnel Point-to-Point on UDP**
- **Serial Tunnel Point-to-Multipoint**

Inoltre, per le modalità operative "Serial Tunnel", i parametri disponibili dipendono dal “Tunnel Role” (Master o Slave).
Le seguenti tabelle descrivono i parametri rilevanti per le varie modalità operative.

22.8.2.1. VIRTUAL COM

Campo	Significato
Listen Port	Porta TCP per accedere al gateway trasparente
Data Packing Interval	Intervallo di tempo utilizzato come criterio per impacchettare i byte di dati ricevuti dalla porta seriale, prima di inviarli alla rete; vale a dire, se per questo tempo non viene ricevuto alcun pacchetto, i byte disponibili vengono inviati alla rete. Il valore è in millisecondi; i valori possibili sono compresi nell'intervallo [0 - 1000].

22.8.2.2. SERIAL TUNNEL POINT-TO-POINT ON TCP/UDP (MASTER)

Campo	Significato
Indirizzo Destinazione	L'indirizzo IP a cui si connetterà il gateway trasparente
Porta Destinazione	La porta TCP / UDP a cui si connetterà il gateway trasparente

22.8.2.3. SERIAL TUNNEL POINT-TO-MULTIPOINT (MASTER)

Campo	Significato
Destination Port	La porta UDP a cui verranno inviati i pacchetti
Multicast Group	Indirizzo IP che identifica il gruppo Multicast
Multicast Interface	Interfaccia di rete a cui vengono inviati i pacchetti UDP; valori possibili: Ethernet | VPN; L'opzione "VPN" è disponibile solo quando la VPN è attiva

22.8.2.1. SERIAL TUNNEL POINT-TO-MULTIPOINT (SLAVE)

Campo	Significato
Listen Port	La porta UDP da cui verranno ricevuti i pacchetti
Multicast Group	Indirizzo IP che identifica il gruppo Multicast
Multicast Interface	Interfaccia di rete da cui vengono ricevuti i pacchetti UDP; valori possibili: Ethernet | VPN; L'opzione "VPN" è disponibile solo quando la VPN è attiva

22.8.3. GATEWAY MODBUS CON MEMORIA SHARED (DA UTILIZZARE PER DATALOGGER E LOGICHE)

Campo	Significato
Enable	Questo parametro abilita / disabilita il servizio Modbus Shared Memory Gateway. È importante notare che, quando questo parametro è impostato su OFF, il servizio non è in esecuzione anche se ad esso sono assegnate alcune porte seriali.
TCP Port	Porta di ascolto per il server Modbus TCP
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 ("Il dispositivo di destinazione del gateway non è riuscito a rispondere").
Diagnostic Area Type	Selezionare se è possibile accedere alla diagnostica tramite Holding o Input Modbus Registers.
Diagnostic Area Address	L'area diagnostica si riserva un bit per ogni tag (125 registri): 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 regsiter 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).

Quindi, per ciascuna porta seriale con “Gateway Mode” = “Modbus Shared Memory”, sono disponibili i parametri descritti nella tabella seguente.

Campo	Significato
Task	Questo parametro definisce quale tipo di task Modbus Shared Memory Gateway è in esecuzione sulla porta seriale; i valori possibili sono: Nessuno, Master, Slave
Slave Address	Intervallo tra le richieste Modbus RTU, in millisecondi (disponibile solo quando Task = Master)
Timeout (ms) [10 – 10000]	Timeout di risposta per richieste Modbus RTU, in millisecondi (disponibile solo quando Task = Master)
Delay between Polls (ms) [10 – 1000]	Intervallo tra richieste Modbus RTU, in millisecondi (disponibile solo quando Task = Master)
Read/Write Retries [0 – 10]	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 "Gateway Tag Mode" = "BRIDGE"
Multiple Read Max Number [1 – 32]	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, eseguendo così l'ottimizzazione
Multiple Write Max Number [1 – 32]	Numero massimo di registri Modbus che possono essere scritti in una singola richiesta Modbus RTU; viene utilizzato per ridurre il numero di richieste di scrittura inviate sul bus seriale, eseguendo così l'ottimizzazione

22.9. CONFIGURAZIONE VPN

La connessione VPN può essere configurata come VPN BOX SENECA oppure OPEN VPN.

22.9.1. OPEN VPN

22.9.1.1. CONFIGURATION FILE

Questo file deve contenere tutte le informazioni necessarie per configurare il comportamento 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 l'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)

22.9.1.2. 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".

22.9.1.3. 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".

22.9.1.4. 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".

22.9.1.5. 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.
Puoi sfogliare il tuo PC per selezionare i file sopra 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 fa clic sul 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".

22.9.1.6. FILE DI CONFIGURAZIONE PER UTILIZZO COME OPENVPN SERVER

Questo paragrafo fornisce un esempio di configurazione del 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
```

22.9.1.7. FILE DI CONFIGURAZIONE PER UTILIZZO COME OPENVPN CLIENT

Questo paragrafo fornisce un esempio di configurazione del server OpenVPN.

```
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
```

22.9.2. VPN BOX

Campo	Significato
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”)
VPN BOX/Server	Indirizzo IP o FQDN del server “VPN Box”
VPN BOX/Password	Password per accedere al server “VPN Box”
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)

22.10. OPC-UA SERVER CONFIGURATION

In questa pagina, è possibile impostare i parametri relativi al server OPC Unified Architecture (OPC-UA), come elencato nella seguente tabella:

Campo	Significato
Enable	Abilita/Disabilita il server OPC-UA
Port	Porta del server
Username	Username per accesso al server
Password	Password per accesso al server
Security Policy	"None" "Basic128Rsa15" "Basic256Sha256" Nota: una coppia predefinita di certificati è già inclusa nel prodotto.

È possibile aggiungere i propri certificati con gli appositi pulsanti
Si noti che, per accedere al server OPC-UA, un client deve utilizzare il seguente URL:
opc.tcp://IP_ADDR:PORT/
Dove
IP_ADDR è l'indirizzo IP del server OPC-UA (il dispositivo stesso)
PORT è la porta TCP configurata per l'OPC-UA server

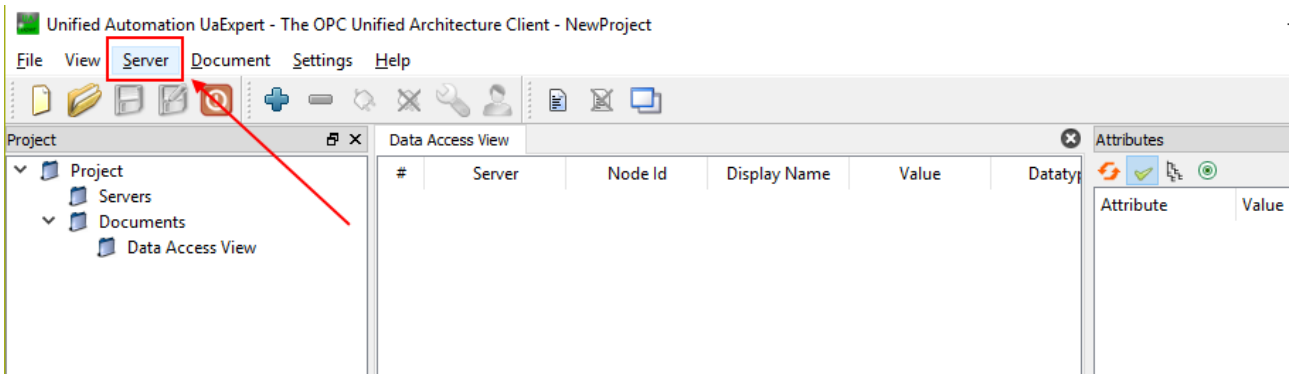
Il server OPC-UA del dispositivo "esporta" i tag Modbus Shared Memory Gateway; pertanto, utilizzando un software client OPC-UA, è possibile leggere / scrivere i tag mediante il protocollo OPC-UA.

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

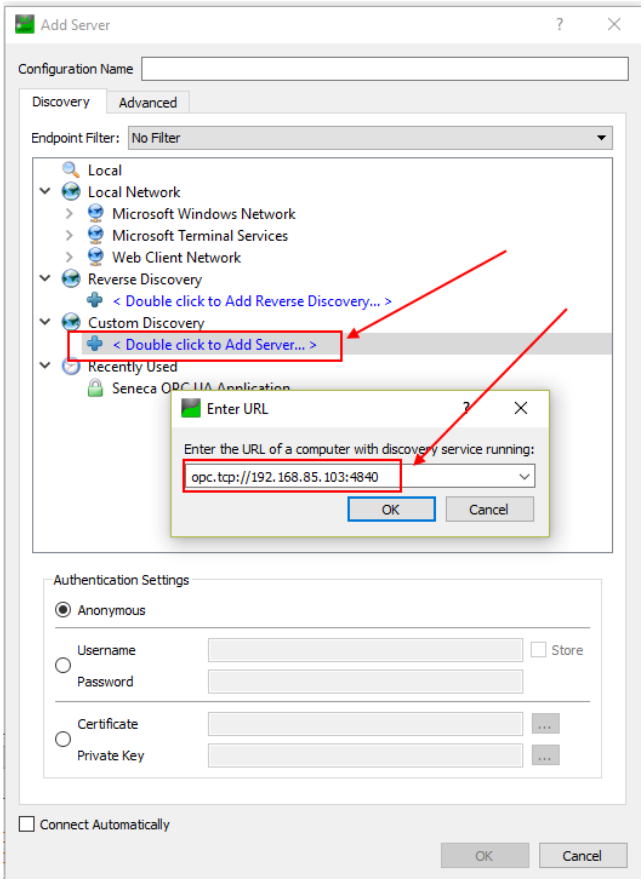
22.10.1.UA EXPERT CLIENT CONFIGURATION

Questo capitolo ti aiuterà a configurare la connessione e la corretta security policy con il software UA Expert Client

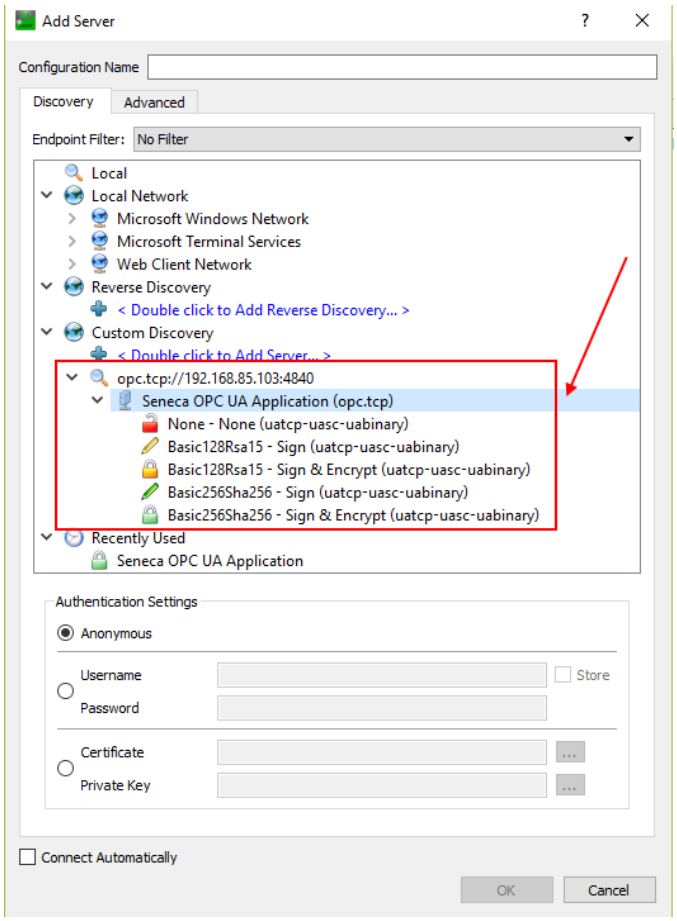
Fai clic su Seleziona server-> Add



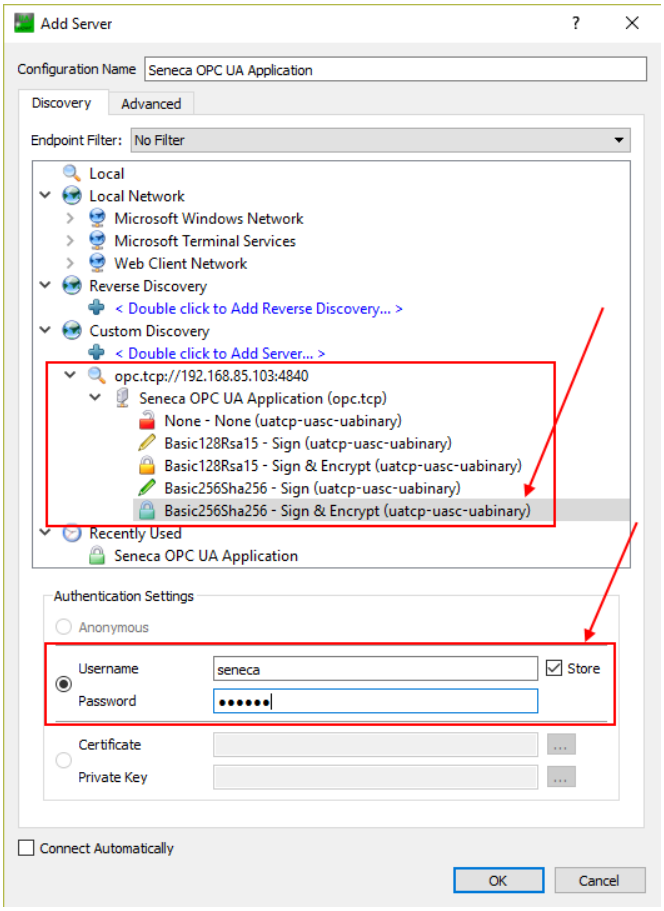
In “Custom Discovery” inserire l’url relativa al server OPC-UA:



Premere OK.
Ora le politiche di sicurezza supportate sono visualizzate:

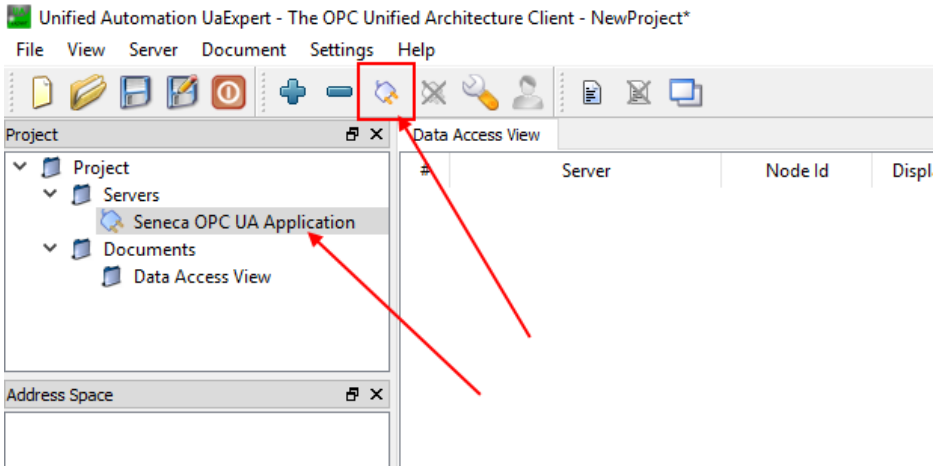


Selezionare quella che si desidera utilizzare. Passare poi all' Authentication settings ed inserire lo user name e la password configurati nel server OPC-UA:

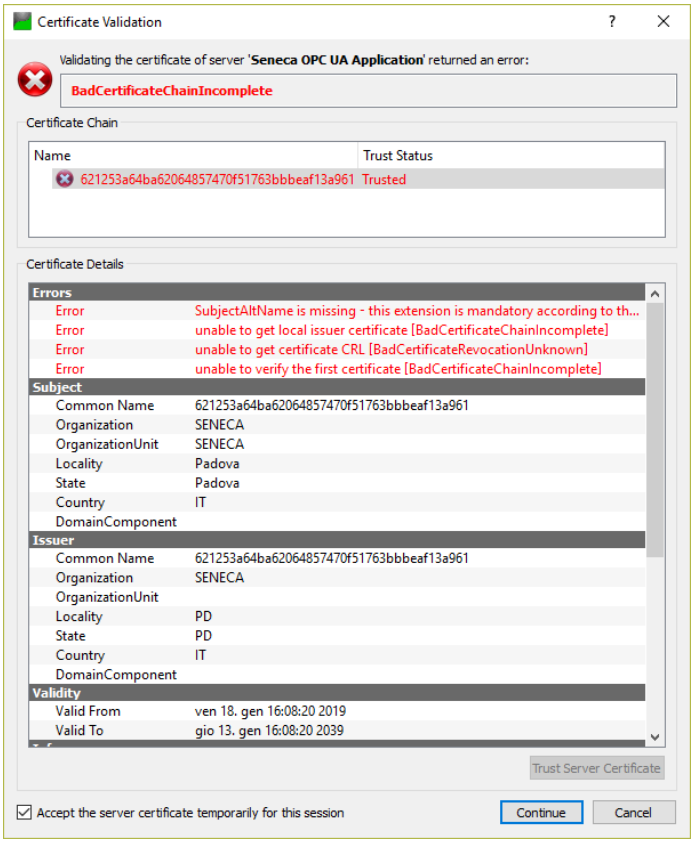


Premere OK:

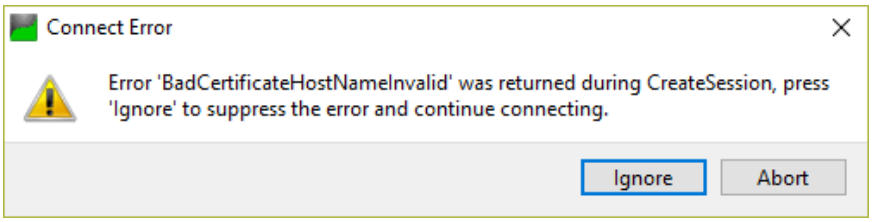
Ora possiamo collegarci al server usando l'icona opportuna:



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.

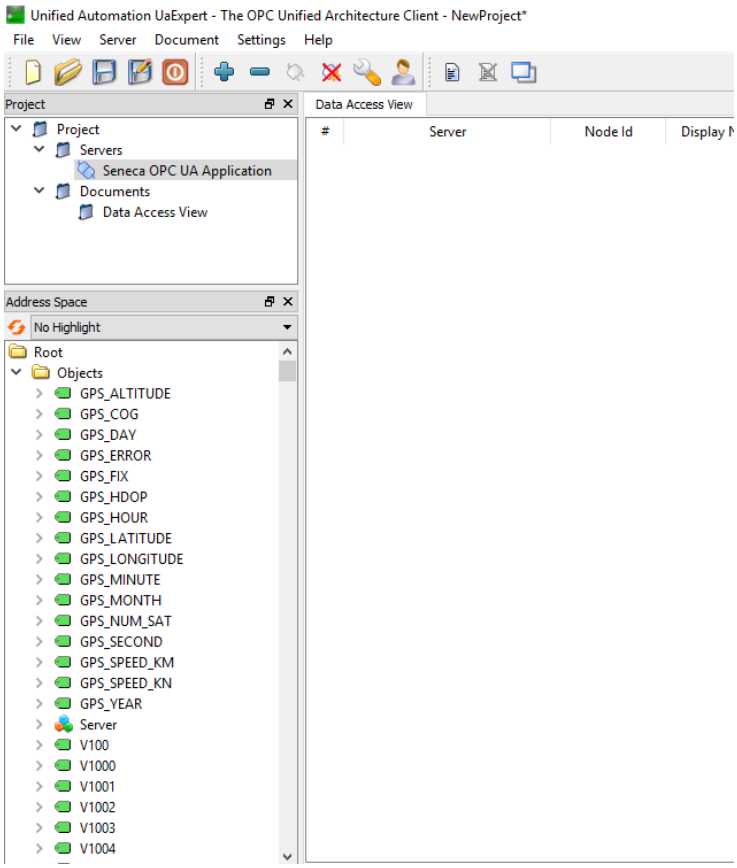


Ora verrà visualizzata la finestra Errore certificato:

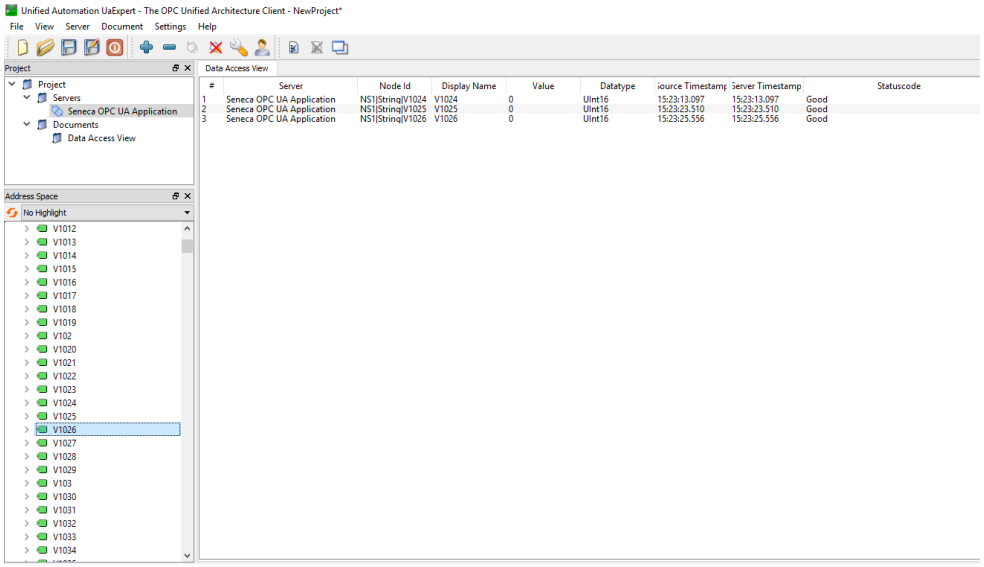


Cliccare su “Ignore” per continuare.

Ora la connessione è stabilita, è possibile leggere/scrivere il valore dei tag

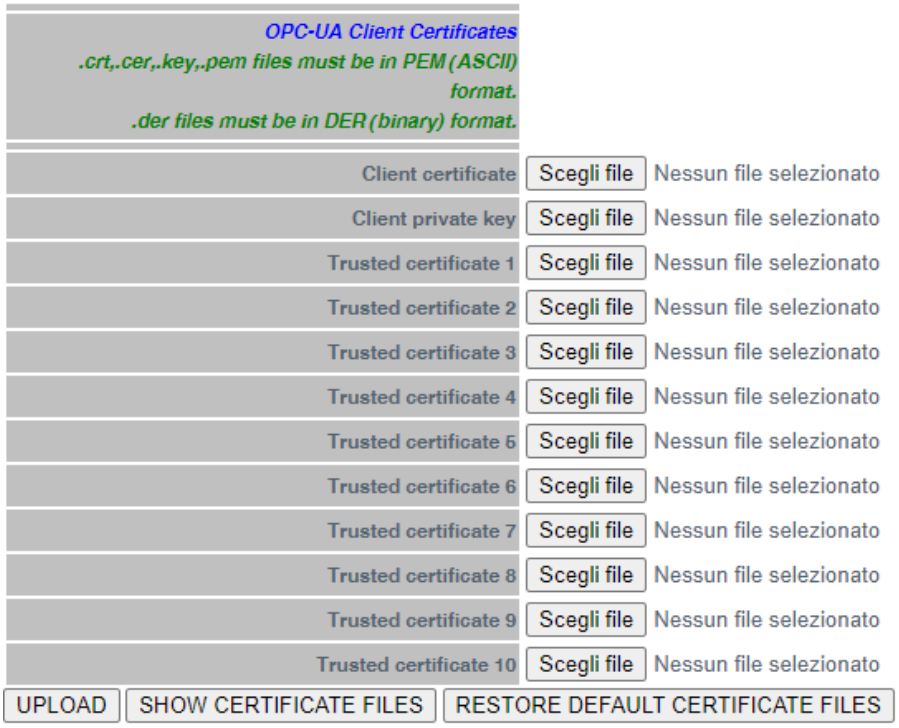


Per aggiornare in tempo reale I tag fare drag and drop con I tag che si desidera visualizzare.



22.11. OPC-UA CLIENT CONFIGURATION (SOLO MODELLI SSD, R-PASS-S, Z-PASS2-S-RT, Z-TWS4-RT)

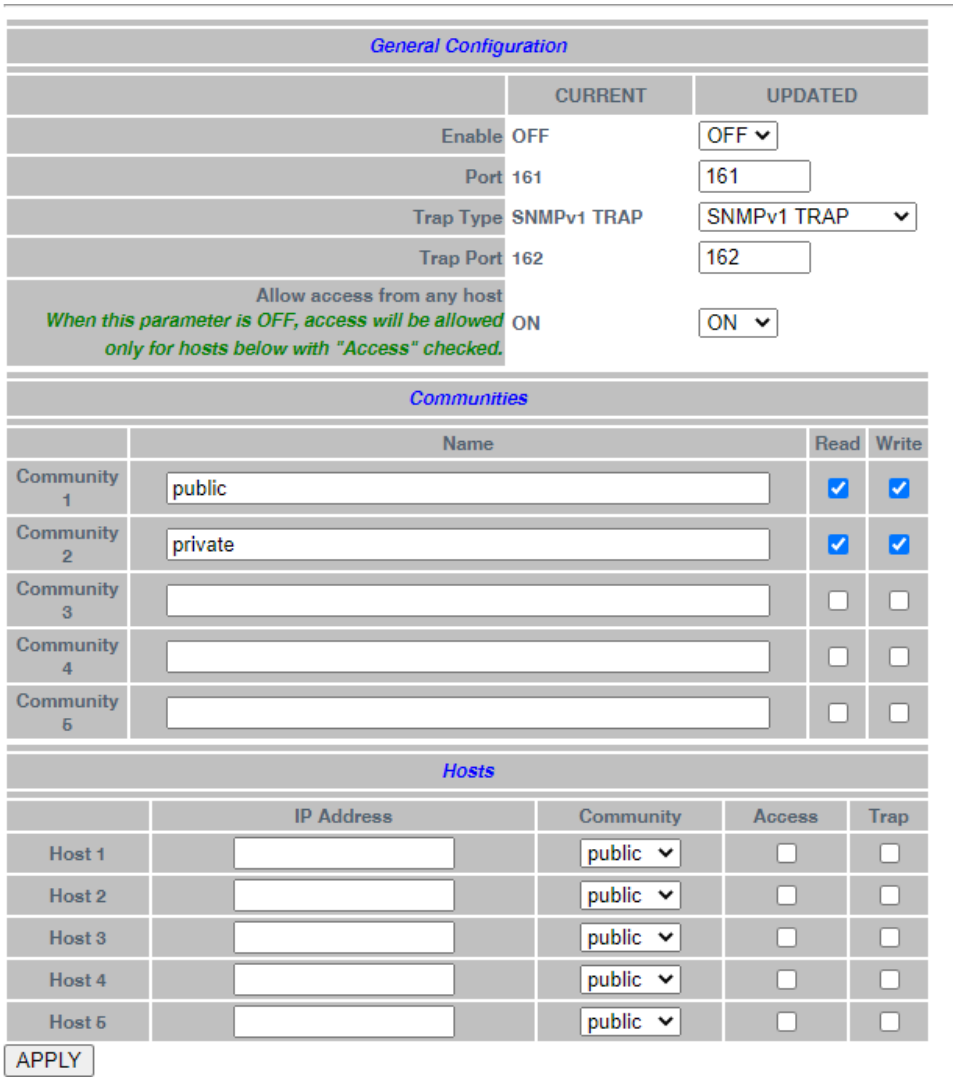
In questa sezione è possibile caricare i certificati di connessione ai server per l'OPC-UA client.



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.

22.12. SNMP CONFIGURATION (SOLO MODELLI R-PASS-S, Z-PASS2-RT-S, Z-TWS4-RT-S)

In questa sezione viene descritta la configurazione dell'Agent SNMP.
È supportata la versione SNMP V2C.



Campo	Significato
Enable	Abilita o no il protocollo
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	Permette a qualunque host di accedere

Communities: Name	Identificativo del Community
Communities: Read	Fornisce le proprietà di lettura al Community selezionato
Communities: Write	Fornisce le proprietà di Scrittura al Community selezionato
Hosts: IP Address	Permette di definire l'IP del Host
Hosts: Community	Permette di definire a quale community è associato l'Host
Hosts: Access	Se Flaggato permette all'host di accedere all' Agent SNMP
Hosts: Trap	Se Flaggato permette all'host di ricevere le Trap dall' Agent SNMP

22.13. USERS CONFIGURATIONS

In questa sezione è riportata la configurazione (user/password) di tutti gli account disponibili per l'accesso al Webserver e al Display:

ADMINISTRATOR
È l'account che permette ogni operazione

GUEST
È l'account che permette di accedere a tutte le pagine ad eccezione delle pagine "FW Upgrade", e "Configuration Management", visualizzando tutti i parametri di configurazione e le informazioni sullo stato, senza poter modificare alcun parametro; quindi, in tutte le pagine, i pulsanti "APPLICA" (e qualsiasi altro pulsante utilizzato per eseguire le modifiche) sono disabilitati.

USER
È l'account che permette di accedere solo alla pagina "Summary" e "tag view" pages (e solo delle pagine web, non ha accesso al display).

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

22.14. ROUTER CONFIGURATION

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

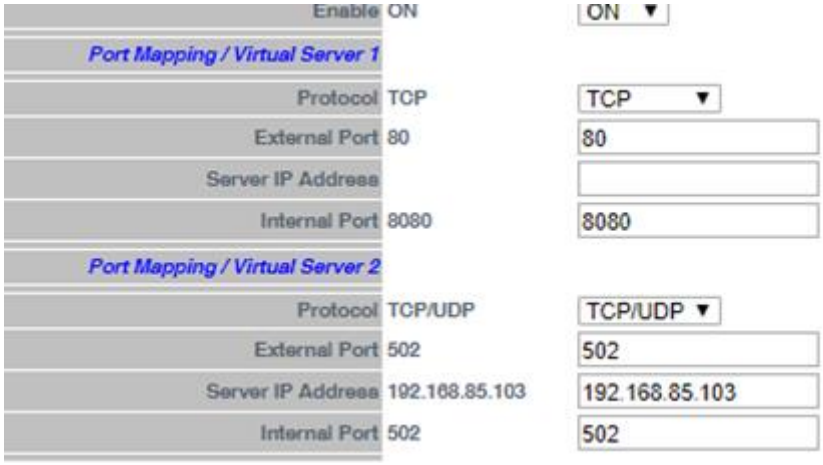
Campo	**Significato**
Router Enable	Abilita/Disabilita la funzionalità di router

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. I valori possibili sono compresi nell'intervallo [1..60].
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

Infine, ci sono le regole di port mapping (note anche come "server virtuali"), I parametri di ciascuna sono:

Campo	**Significato**
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

In questo esempio sono state impostate 2 regole:

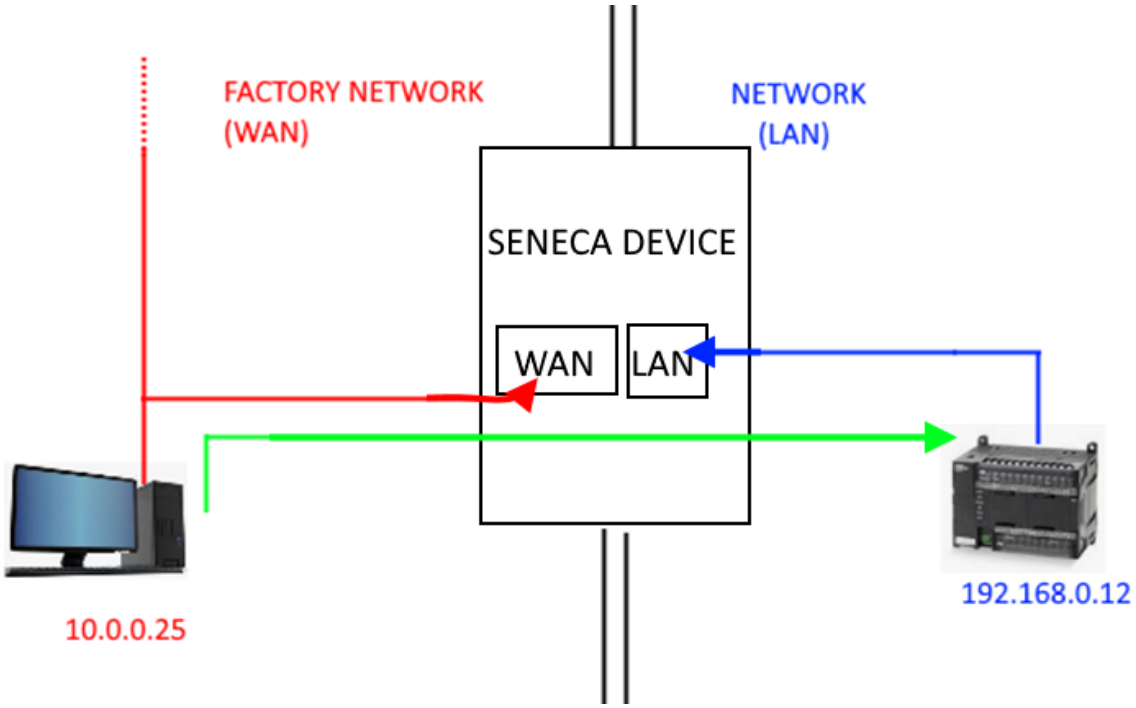


• la prima regola dice al dispositivo che qualsiasi pacchetto TCP ricevuto sulla porta 80 (HTTP) deve essere inoltrato alla porta 8080, lasciando invariato l'indirizzo IP di destinazione originale; quindi, questa regola consente di accedere al sito Web di configurazione sulla porta HTTP standard (80);

• la seconda regola dice al dispositivo che qualsiasi pacchetto TCP o UDP ricevuto 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) sullo stessa porta di destinazione (502).

22.15. NAT 1:1 RULES

È possibile utilizzare questa funzione per accedere a un dispositivo (ad esempio) dalla WAN alla LAN (un PC nella rete WAN che deve ottenere i dati da un PLC nella rete LAN):



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

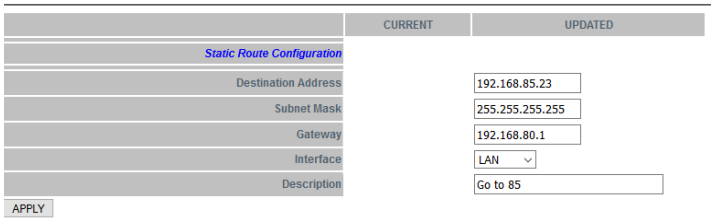
APPLY

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

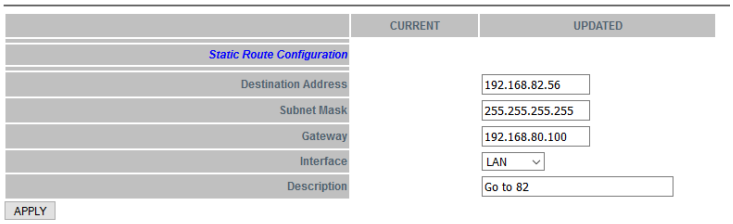
22.16. STATIC ROUTES

Utilizzare questa funzione per instradare un indirizzo o un intervallo di indirizzi a gateway diversi.
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.

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:

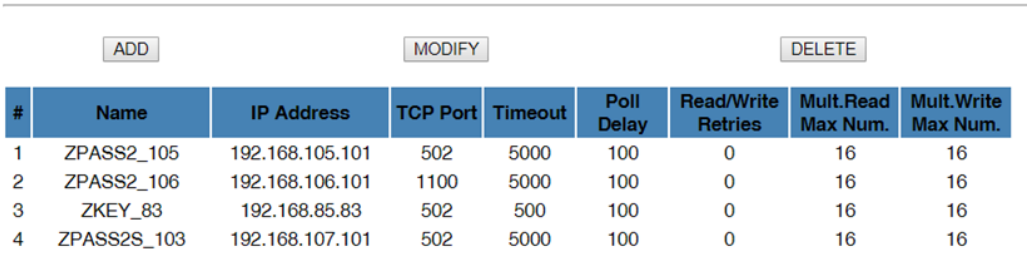


E anche:



22.17. TCP SERVER (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

In questa pagina viene mostrato l'elenco dei server TCP, utilizzati per la 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

La tabella seguente spiega il significato dei parametri relativi a un server TCP.

Campo	Meaning
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
TCP Port	Porta TCP del server
Timeout (ms) [10-10000]	Timeout di connessione / risposta per richieste TCP Modbus, in millisecondi

Delay between Polls (ms) [10-1000]	Intervallo tra richieste TCP Modbus, in millisecondi
Read/Write Retries [0-10]	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 [1-32]	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 [1-32]	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

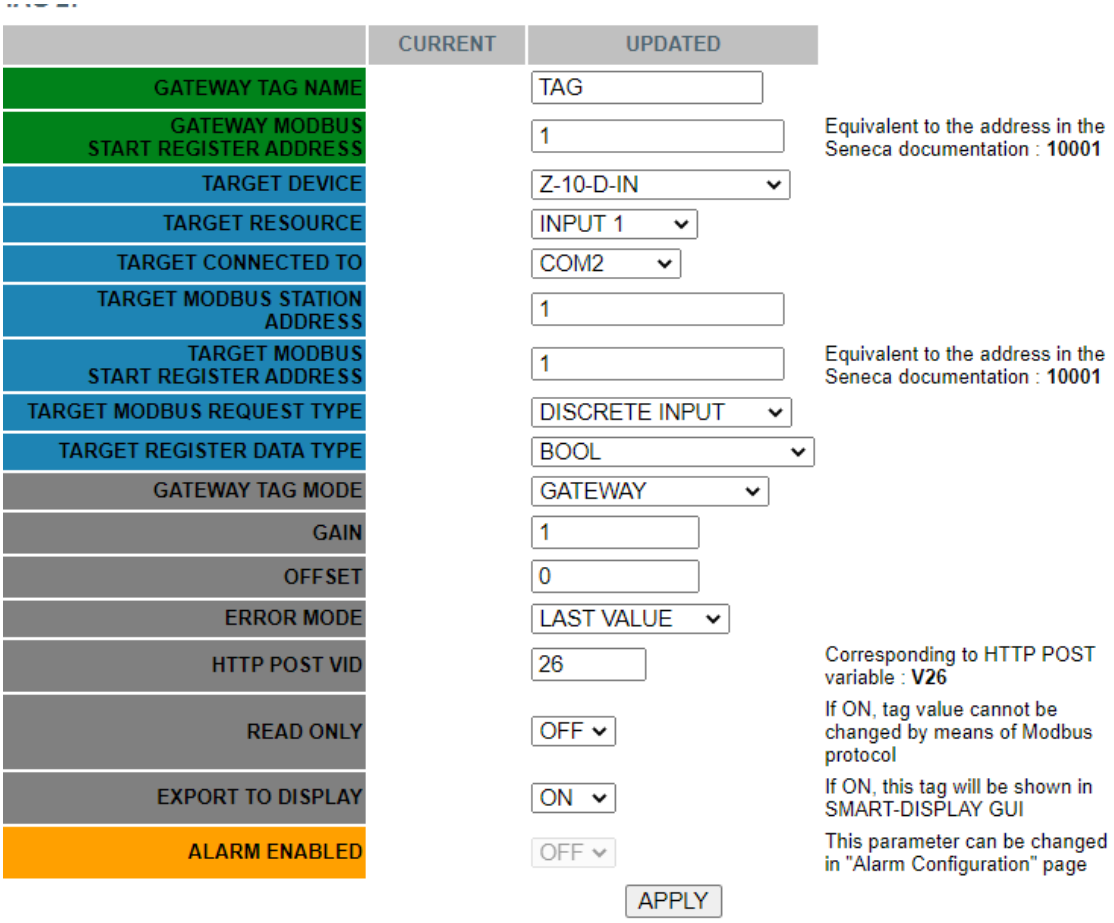
Il numero massimo di Server Modbus TCP-IP configurabili è 25.

22.18. TAG SETUP (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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 quella attuale.

È anche possibile inserire nuovi tag direttamente dalla pagina web, tutti i dispositivi Seneca sono disponibili tramite un database interno, è anche possibile definire un proprio database.

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



I principali parametri:

Campo	Significato
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 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	Se attivo permette di visualizzare il tag sul display o display virtuale (a seconda del dispositivo)
Alarm Enabled	Questo campo è un flag di sola lettura che indica se è stato definito un allarme per il tag.

22.19. TAG VIEW (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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.

Come mostrato nelle figure seguenti, la colonna “ALARM” riporta lo stato dell'allarme definito per il tag, se presente; la colonna DANGER ANALOG 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”.

22.20. DEVICE DB (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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

22.21. ALARM CONFIGURATION (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

In questa pagina viene visualizzato l'elenco degli allarmi configurati.
Facendo clic sul pulsante "ADD", è possibile configurare un nuovo allarme.
La tabella seguente spiega il significato di tutti i parametri disponibili per un allarme.

Campo	Significato
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 (s)	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 nella tabella precedente, 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

22.22. ALARM SUMMARY (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Questa pagina mostra gli allarmi attualmente attivi nel sistema.
La tabella seguente spiega il significato di tutte le informazioni fornite per un allarme.

Campo	Significato
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)

22.23. ALARM HISTORY (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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.

22.24. USB TRANSFER CONFIGURATION (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Questa pagina contiene i parametri che indicano se i file di log vengono copiati su una chiavetta USB collegata e per quanto tempo vengono conservati, come spiegato nella tabella seguente.

Campo	Significato	Valore di default
Enable	Abilita o no la copia dei log su USB	OFF
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)	10
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	15

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.	30

Nella USB 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 del prima riga di log esempio:

L9701690.csv

22.25. FTP CONFIGURATION (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Questa pagina contiene i parametri relativi al trasferimento di file di log tramite FTP, come spiegato nella tabella seguente.

Campo	**Significato**
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 (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 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

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`

22.26. EMAIL CONFIGURATION (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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".
Tutti i parametri sono spiegati nella tabella seguente.

Campo	Significato
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

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

22.27. HTTP CONFIGURATION (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Il protocollo http post può essere utilizzato per inviare campioni di log o allarmi (eventi).
Tutti i parametri sono spiegati nella tabella seguente.

Campo	Significato
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.
Crypto Mode	Questo parametro definisce il tipo di crittografia della connessione http. Le modalità possibili sono: OFF (HTTP) ON (HTTPS)
Host	Hostname (FQDN) o IP address del server HTTP
Port	Porta TCP del server HTTP
Password	Password del server HTTP

22.28. MQTT CONFIGURATION (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Il protocollo MQTT può essere utilizzato per inviare (e ricevere) dati o eventi a un cloud (chiamato broker).
Tutti i parametri sono spiegati nella tabella seguente:

Campo	Significato
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.

<table>
<tr><td>Publish with multiple tags</td><td>Questo parametro definisce se la publish contiene più tag o se il dispositivo deve inviare una publish per ciascun tag</td></tr>
<tr><td>Publish Topic for Logs</td><td>Seleziona il nome del topic per i log utilizzando la seguente tabella:<table>
<tr><td>%c</td><td>Device Client ID</td></tr>
<tr><td>%m</td><td>Device MAC Address</td></tr>
<tr><td>%e</td><td>Device IMEI</td></tr>
<tr><td>%d</td><td>Data/ora</td></tr>
<tr><td>%t</td><td>timestamp (numero di secondi dal 01/01/1970)</td></tr>
<tr><td>%x</td><td>testo (solo per "Publish Payload for Alarms")</td></tr>
<tr><td>%b</td><td>bulk (formato specificato in "Publish Bulk Format")</td></tr>
<tr><td>%n</td><td>Nome del tag (solo per "Publish Bulk Format")</td></tr>
<tr><td>%v</td><td>Valore del tag (solo in "Publish Bulk Format")</td></tr>
<tr><td>%i</td><td>Flag di validità del tag (solo in "Publish Bulk Format")</td></tr>
<tr><td>%j[field]</td><td>Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON</td></tr>
<tr><td>%tag_name</td><td>Valore del tag "tag_name"</td></tr>
<tr><td>%#tag_name#</td><td>Validità del tag "tag_name"</td></tr>
</table></td></tr>
<tr><td>Publish Payload for Logs</td><td>Seleziona il formato che deve essere utilizzato per il payload in formato Json utilizzando la seguente tabella:<table>
<tr><td>%c</td><td>Device Client ID</td></tr>
<tr><td>%m</td><td>Device MAC Address</td></tr>
<tr><td>%e</td><td>Device IMEI</td></tr>
<tr><td>%d</td><td>data-ora</td></tr>
<tr><td>%t</td><td>timestamp (numero di secondi dal 01/01/1970)</td></tr>
<tr><td>%x</td><td>testo (solo per "Publish Payload for Alarms")</td></tr>
<tr><td>%b</td><td>bulk (formato specificato in "Publish Bulk Format")</td></tr>
<tr><td>%n</td><td>Nome del tag (solo per "Publish Bulk Format")</td></tr>
<tr><td>%v</td><td>Valore del tag (solo in "Publish Bulk Format")</td></tr>
<tr><td>%i</td><td>Flag di validità del tag (solo in "Publish Bulk Format")</td></tr>
<tr><td>%j[field]</td><td>Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON</td></tr>
<tr><td>%tag_name</td><td>Valore del tag "tag_name"</td></tr>
<tr><td>%#tag_name#</td><td>Validità del tag "tag_name"</td></tr>
</table></td></tr>
<tr><td>Publish Bulk Format</td><td>Seleziona il formato per il “bulk mode” secondo la seguente tabella:</td></tr>
</table>

%c	Device Client ID
%m	Device MAC Address
%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")
%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"

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
%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")
%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"

Subscribe Topic

Seleziona il Subscribe Topic secondo la seguente tabella:

%c	Device Client ID
%m	Device MAC Address
%e	Device IMEI

<table>
<tr><td></td><td>
<table>
<tr><td>%d</td><td>Data/ora</td></tr>
<tr><td>%t</td><td>timestamp (numero di secondi dal 01/01/1970)</td></tr>
<tr><td>%x</td><td>testo (solo per "Publish Payload for Alarms")</td></tr>
<tr><td>%b</td><td>bulk (formato specificato in "Publish Bulk Format")</td></tr>
<tr><td>%n</td><td>Nome del tag (solo per "Publish Bulk Format")</td></tr>
<tr><td>%v</td><td>Valore del tag (solo in "Publish Bulk Format")</td></tr>
<tr><td>%i</td><td>Flag di validità del tag (solo in "Publish Bulk Format")</td></tr>
<tr><td>%j[field]</td><td>Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON</td></tr>
<tr><td>%tag_name</td><td>Valore del tag "tag_name"</td></tr>
<tr><td>%#tag_name#</td><td>Validità del tag "tag_name"</td></tr>
</table>
</td></tr>
<tr><td>LWT Topic</td><td>Seleziona il “Last Weel and Testament” topic secondo la seguente tabella:
<table>
<tr><td>%c</td><td>Device Client ID</td></tr>
<tr><td>%m</td><td>Device MAC Address</td></tr>
<tr><td>%e</td><td>Device IMEI</td></tr>
<tr><td>%d</td><td>Data/ora</td></tr>
<tr><td>%t</td><td>timestamp (numero di secondi dal 01/01/1970)</td></tr>
<tr><td>%x</td><td>testo (solo per "Publish Payload for Alarms")</td></tr>
<tr><td>%b</td><td>bulk (formato specificato in "Publish Bulk Format")</td></tr>
<tr><td>%n</td><td>Nome del tag (solo per "Publish Bulk Format")</td></tr>
<tr><td>%v</td><td>Valore del tag (solo in "Publish Bulk Format")</td></tr>
<tr><td>%i</td><td>Flag di validità del tag (solo in "Publish Bulk Format")</td></tr>
<tr><td>%j[field]</td><td>Aggiunge i doppi apici " a [field]. I doppi apici rappresentano una stringa in JSON</td></tr>
<tr><td>%tag_name</td><td>Valore del tag "tag_name"</td></tr>
<tr><td>%#tag_name#</td><td>Validità del tag "tag_name"</td></tr>
</table>
</td></tr>
<tr><td>LWT Payload</td><td>Seleziona il testo del Payload del “Last Weel and Testament”</td></tr>
<tr><td>Save Configuration URL</td><td>È la URL per il comando “Save Configuration” ricevuto da mqtt</td></tr>
<tr><td>Load Configuration URL</td><td>È la URL per il comando “Load Configuration” ricevuto da mqtt</td></tr>
<tr><td>FW Update URL</td><td>È la URL per il comando “FW Update” ricevuto da mqtt</td></tr>
<tr><td>Sleep Timeout</td><td>Tempo di risveglio del task MQTT, più è breve, più è reattivo MQTT (a scapito di un carico della CPU più elevato)</td></tr>
<tr><td>MQTT Certificates</td><td>È utilizzato per gestire i certificati necessari alla connessione TLS.</td></tr>
</table>

22.29. PHONEBOOK (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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.

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.
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.

22.30. MESSAGE CONFIGURATION (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

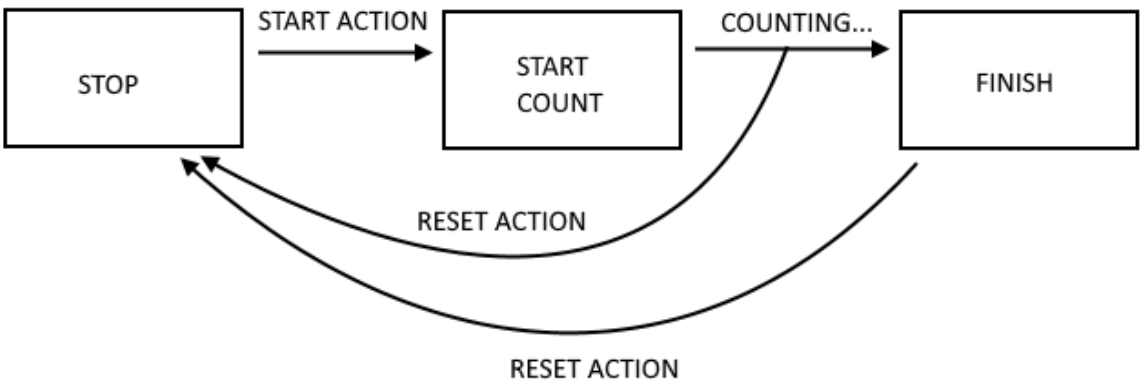
In questa sezione è possibile definire i messaggi di testo relativi agli allarmi che il dispositivo deve gestire.
Il testo del messaggio può contenere solo caratteri ASCII.
È anche possibile utilizzare la sintassi {NOME_TAG} per includere nel testo il valore attuale di un tag.
La sintassi permette di aggiungere il valore corrente del tag il cui nome è quello definito all'interno delle parentesi graffe. 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.

22.31. TIMER CONFIGURATION (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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:



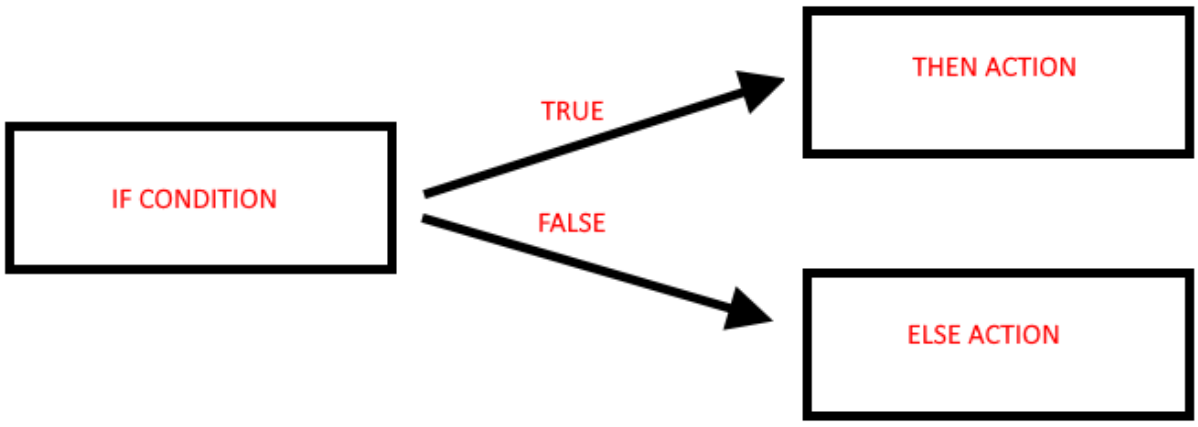
22.32. RULE MANAGEMENT (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

In questa sezione è possibile definire un insieme di regole logiche che realizzeranno un programma.
Ad esempio è possibile eseguire programmi che utilizzano dell'IO interno o esterno, inviano messaggi di testo e/o scritture 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).

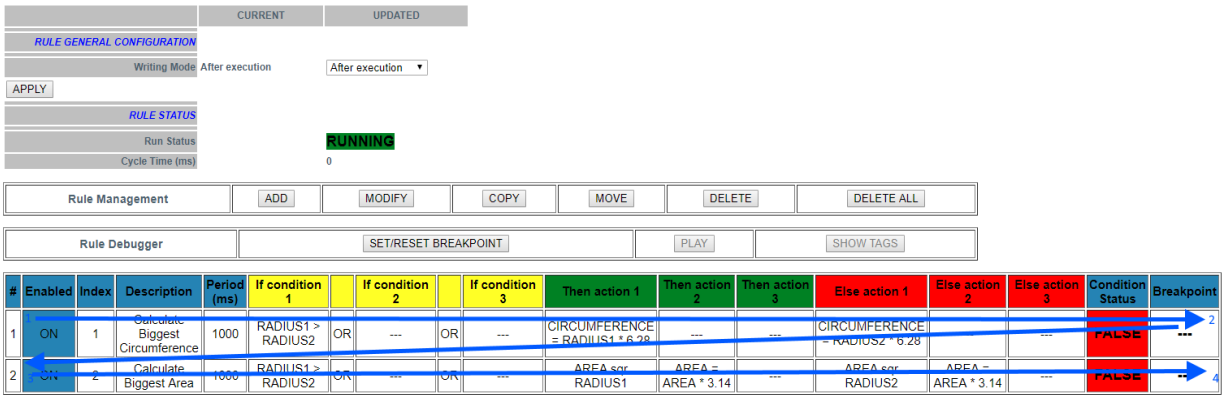
Una regola è composta da una o più "If Condition", una o più "Then Action" e una o più "Else Action".

Schematicamente una regola esegue il seguente flusso:

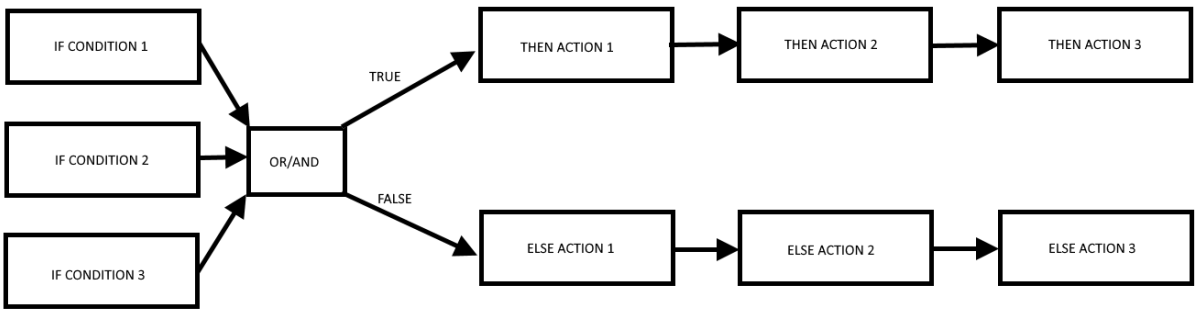


Se la condizione "IF" è vera viene eseguita l'azione "THEN", altrimenti viene eseguita l'azione "ELSE".

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.

Le "condizioni IF" possono essere combinate insieme in logica "OR" o "AND", in pratica:
Le “condizioni IF” legate assieme da “OR” vanno allo stato THEN se almeno una delle condizioni è vera.
Le “condizioni IF” legate assieme da “AND” vanno allo stato THEN solo se tutte sono vere.
Più in dettaglio seguono la seguente tabella:

IF CONDITION 1	*IF CONDITION 2*	*IF CONDITION 3*	*“OR” RESULT*	*“AND” RESULT*
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

È possibile creare fino a 2000 differenti regole.
È possibile configurare una regola per eseguire azioni:
-Solo quando c'è una modifica nel risultato "OR / AND"

-Ad ogni loop

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 state eseguite tutte le regole.
Con “During Execution”, si ottiene che i valori dei tag vengano scritti nella memoria shared alla fine di ogni 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):

Per configurare una regola, sono disponibili i parametri spiegati nella tabella seguente:

Campo	Significato
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. Non utilizzare piccoli valori di periodo per l'invio di azioni EMAIL / SMS / HTTP / MQTT! NOTA: Se Period è > 0 le azioni vengono sempre eseguite in modalità “repeat”
If Condition X Type Dove X=[1..3]	Questo parametro definisce il tipo di condizione, per ognuna delle tre "condizioni if" disponibili (1..3) I tipi possibili sono: **None** Nessuna condizione da valutare **Alarm State** Vedi 22.32.1

	Alarm Active Vedi 22.32.2 **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 ogni xx ms, è necessario impostare Period> 0ms. **Digital Tag** Vedi 22.32.3 **Analog Tag** Vedi 22.32.4 **Timer** Vedi 22.32.5 **Scheduler** Vedi 22.32.6 **Rule Status** Vedi 22.32.7 **Bitmask** Vedi 22.32.8
If Condition Operator	I tipi possibili sono: OR / AND Le condizioni IF possono essere combinate in operazioni booleane OR o AND.
Then/Else Action X dove X=[1..3]	Questo parametro definisce il tipo di azione, per ciascuna delle tre "azioni then / else" disponibili I possibili tipi di azione sono suddivisi per tipologia: **None** Nessuna azione **Send Alarm SMS** **Send Alarm EMAIL** **Send Alarm HTTP POST** **Send Alarm MQTT** Permettono di inviare un messaggio di testo (definito nella sezione messaggi) di allarme attraverso i protocolli disponibili

	Digital Tag Vedi 22.32.9 **Analog Tag** Vedi 22.32.10 Timer È possibile selezionare l'azione da eseguire nel timer tra "Start" avvierà un timer per contare "Reset" resetterà il timer allo stato di stop **Scheduler** Vedi 22.32.6 **Datalogger** Permette di Far partire o fermare il datalogger. **Network** Sono azioni che permettono di agire sullo stato della VPN (abilitarla oppure disabilitarla) o del modem. **Set Bits** Permette di portare al valore 1 o al valore 0 un numero configurabile di bit di un determinato tag.

22.32.1. PARAMETRI "ALARM STATE"

Campo	Significato
Alarm Name	Il nome dell'allarme può essere selezionato 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

22.32.2. PARAMETRI "ALARM ACTIVE"

Campo	Significato
Alarm Name	Il nome dell'allarme può essere selezionato 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.

22.32.3. PARAMETRI “DIGITAL TAG”

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 tag o un valore booleano costante

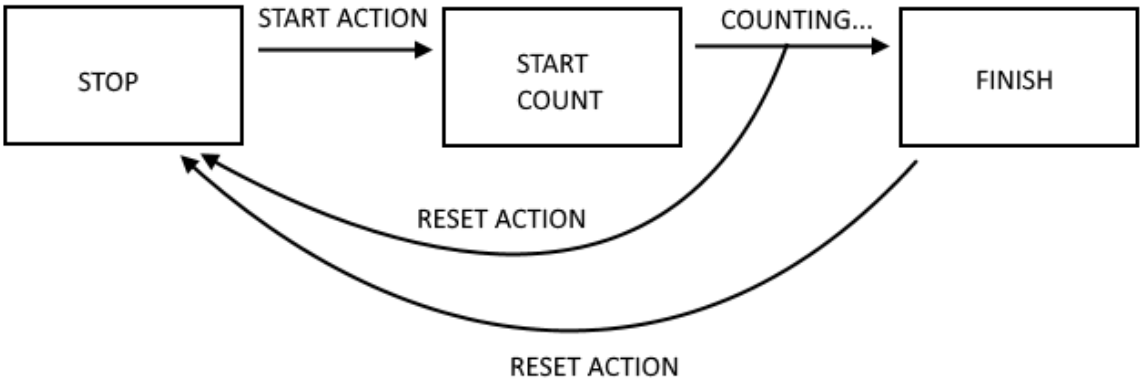
22.32.4. PARAMETRI “ANALOG TAG”

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 tag o un valore costante

22.32.5. PARAMETRI “TIMER”

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 STATE. Quando il timer è nello stato FINISH la condizione diventa falsa.

Il funzionamento del Timer è rappresentato nello schema seguente:



22.32.6.PARAMETRI “SCHEDULER”

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

22.32.7.PARAMETRI “RULE STATUS”

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.

22.32.8.PARAMETRI “BIT MASK”

Campo	Significato
Tag	Seleziona il tag a cui applicare la maschera di bit da un elenco contenente tutti i tag con tipo di dati "16Bit Unsigned" e indice di bit 0
Mask	La maschera di bit rappresentata come una stringa di 4 cifre esadecimali

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

22.32.9. PARAMETRI "DIGITAL TAG"

Campo	Significato
Action Mode	selezionare tra "One Time" o "Repeat". Con "One Time" le azioni vengono eseguite solo se c'è un cambiamento nel risultato delle condizioni OR / AND. Con "Repeat" le Azioni vengono 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 calcolato
Operator	È l'operatore booleano da utilizzare, selezionato tra =, NOT, OR ecc ...
Source Tag 1 / Constant value 1	Seleziona il 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 possibile anche usare una costante booleana

22.32.10. PARAMETRI "ANALOG TAG"

Campo	Significato
Action Mode	selezionare tra "One Time" o "Repeat". Con "One Time" le azioni vengono eseguite solo se c'è un cambiamento nel risultato delle condizioni OR / AND. Con "Repeat" le Azioni vengono 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 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 / Constant value 1 e copia il risultato nel Destination Tag (Notare che abs (-4) = 4) Esempio: Tag di destinazione = abs (Tag sorgente 1) "Sqrt"

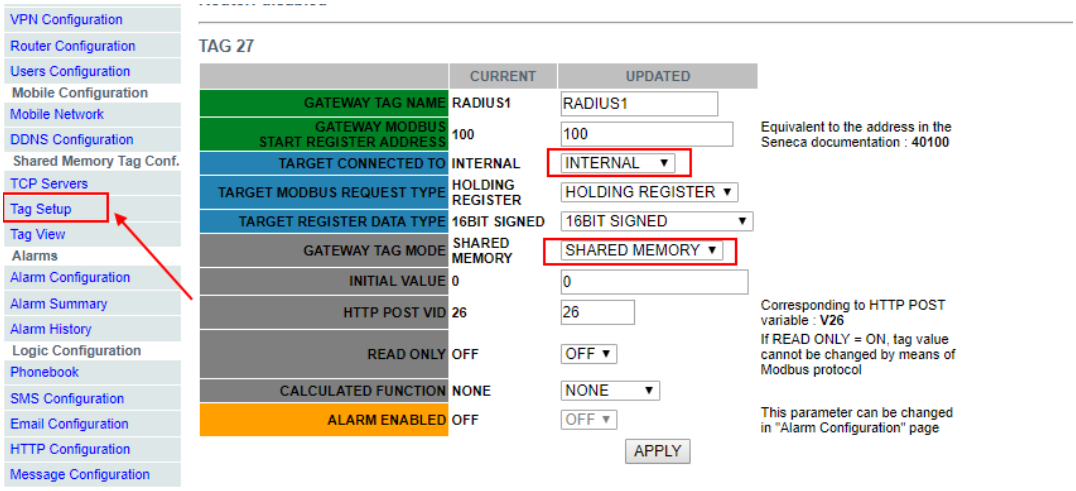
	Calcola il valore della radice quadrata del tag sorgente 1 / valore costante 1 e copia il risultato nel tag di destinazione. (Notare che sqrt (9) = √9 = 3) Esempio: Tag di destinazione = sqrt (tag di origine 1) "Sqr" Calcola il valore quadrato del tag di origine 1 / valore costante 1 e copia il risultato 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 / 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 / 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 / Constant value 1 e copia il risultato nel Destination Tag. (Nota che exp 〖(3) = e ^ 3 = 20,0855369232〗 ln (exp (3)) = 3 Esempio: Tag di destinazione = scadenza (tag di origine 1) "+" Sum to Source Tag 1 / Constant value 1 Con il valore di Source Tag 2 / Constant value 2 e copia il risultato nel Destination Tag.

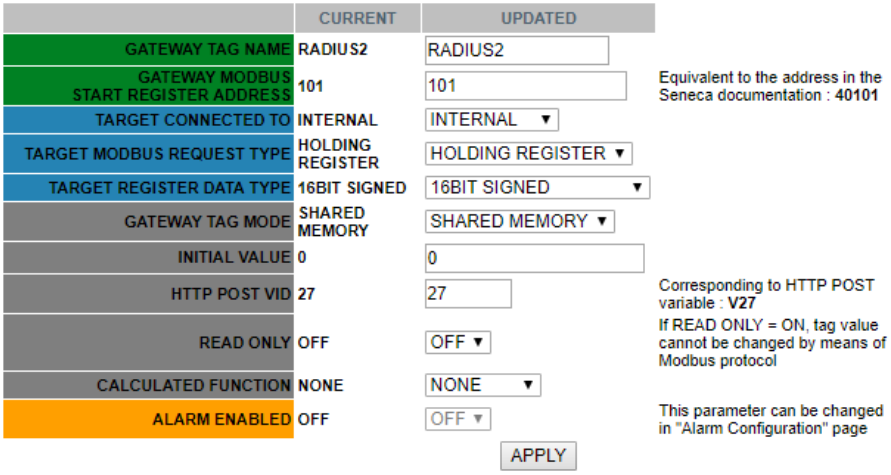
	Esempio: Tag di destinazione = Tag sorgente 1+ Tag sorgente 2 "-" Sottrai il tag sorgente 1 / valore costante 1 con il valore del tag sorgente 2 / valore costante 2 e copia il risultato nel tag di destinazione. Esempio: Tag di destinazione = Tag di origine 1- Tag di origine 2 "*" Moltiplicare il tag di origine 1 / valore costante 1 con il valore di tag di origine 2 / valore costante 2 e copiare il risultato nel tag di destinazione. Esempio: Tag di destinazione = Tag sorgente 1 * Tag sorgente 2 "/" Dividere il tag di origine 1 / valore costante 1 con il valore di tag di origine 2 / valore costante 2 e copiare 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 / valore costante 1 e il valore del tag sorgente 2 / 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 / Constant 1 elevato alla potenza del Sorce Tag2 / Constant value 2 e copia il risultato nel tag di destinazione. Esempio: DestinationTag = 〖Source Tag1〗 ^ (Source Tag2)

Source Tag 1 / Constant value 1	Selezionare il tag da utilizzare come ingresso 1 per l'operatore utilizzato. Puoi anche usare un valore costante.
Source Tag 2 / Constant value 2	Selezionare il Tag da utilizzare come input 2 nel calcolo se l'operatore necessita di 2 input. Puoi anche usare un valore costante.

22.32.11. ESEMPIO DI REALIZZAZIONE DI UN PROGRAMMA CON LE REGOLE LOGICHE

Creeremo un programma di esempio che calcoli la Circonferenza massima e l'Area massima dati 2 diversi raggi.
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) type:





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

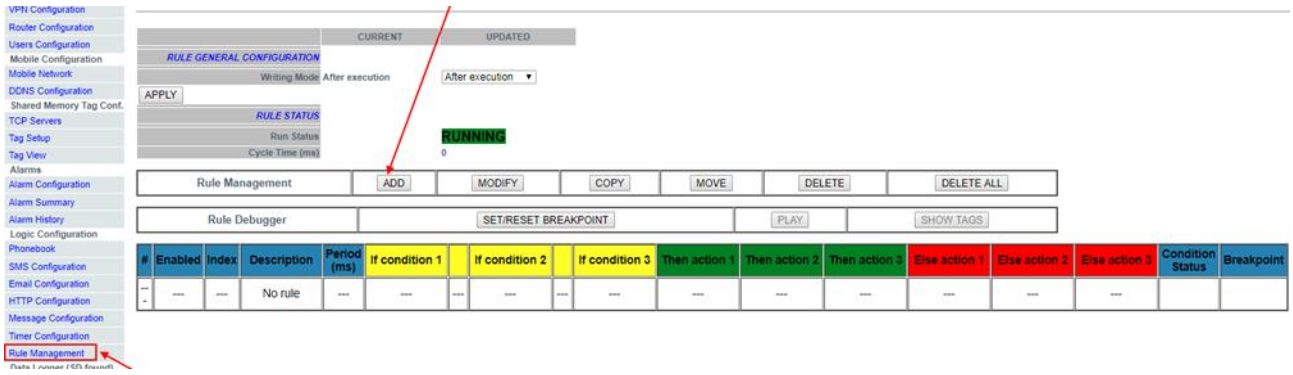
APPLY

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:

	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	1	1
Description	Calculate Biggest Circumference	Calculate Biggest Circumference
Period (ms)	1000	1000

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

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	

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:

Then Action 1			
Type	Analog Tag	Analog Tag	
Action Mode	One time	One time	
Destination Tag	CIRCUMFERENCE	CIRCUMFERENCE	
Operator	*	*	
Source Tag 1	RADIUS1	RADIUS1	
Source Tag 2	constant value	constant value	
Constant Value 2	6.28	6.28	
Then Action 2			
Type		None	
Then Action 3			
Type		None	

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

		Else Action 1	
		Type Analog Tag	Analog Tag ▼
Action Mode	One time	One time ▼	
Destination Tag	CIRCUMFERENCE	CIRCUMFERENCE ▼	
Operator	*	* ▼	
Source Tag 1	RADIUS2	RADIUS2 ▼	
Source Tag 2	constant value	constant value ▼	
Constant Value 2	6.28	6.28	
		Else Action 2	
		Type	None ▼
		Else Action 3	
		Type	None ▼

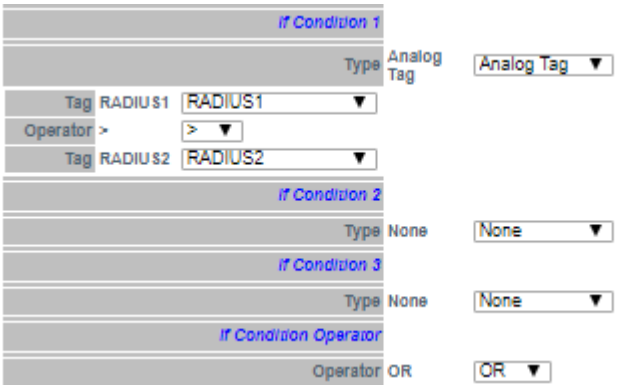
Ora fai clic su "APPLY" per salvare la prima regola:

#	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:

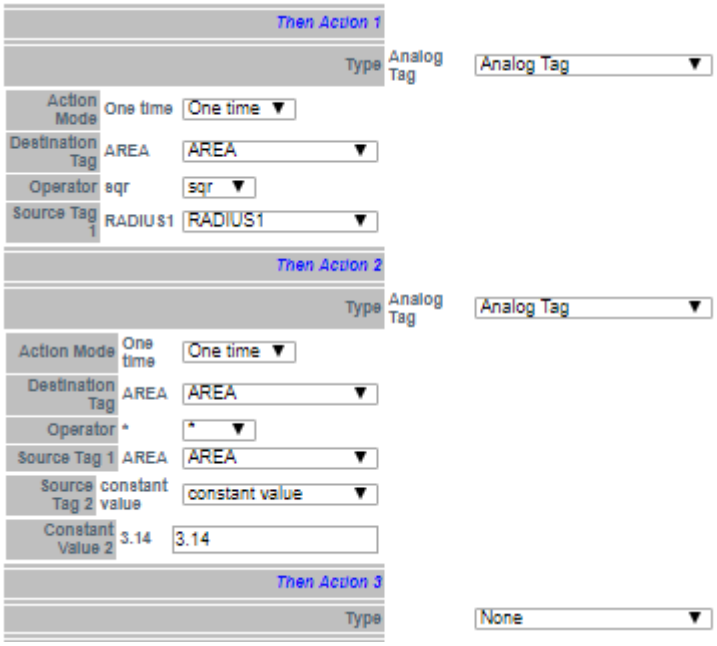
	CURRENT	UPDATED
RULE CONFIGURATION		
NOTE: "Then Actions" are executed when the condition result, as a whole, is TRUE; otherwise "Else Actions" are executed. *Actions with Mode=Repeat and actions in rules with Period>0 are always executed.* *In all other cases, actions are executed only when there is 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:

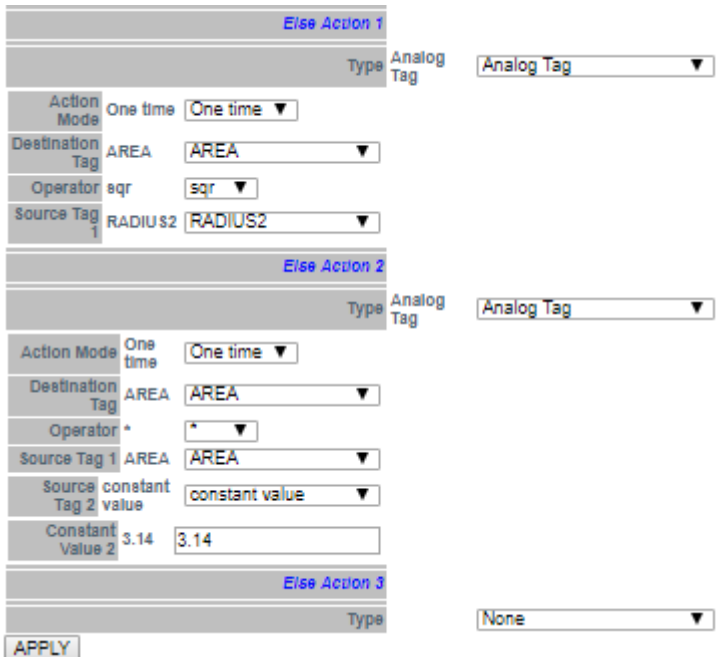


Ora dobbiamo calcolare l'AREA utilizzando il seguente calcolo:
AREA = ([RAGGIO] ^ 2) * 3.14
Dobbiamo spezzare la formula in due fasi:
Nella prima fase calcoliamo:
AREA = (RAGGIO1) ^ 2
E nel secondo:
AREA = AREA * 3.14

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:

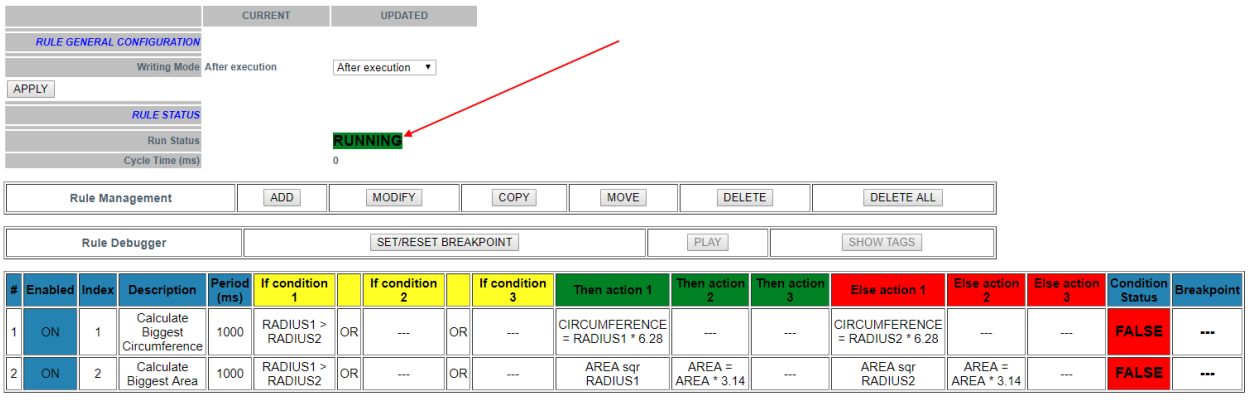


Ora facciamo clic su "APPLY" per salvare anche la seconda regola:

#	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:

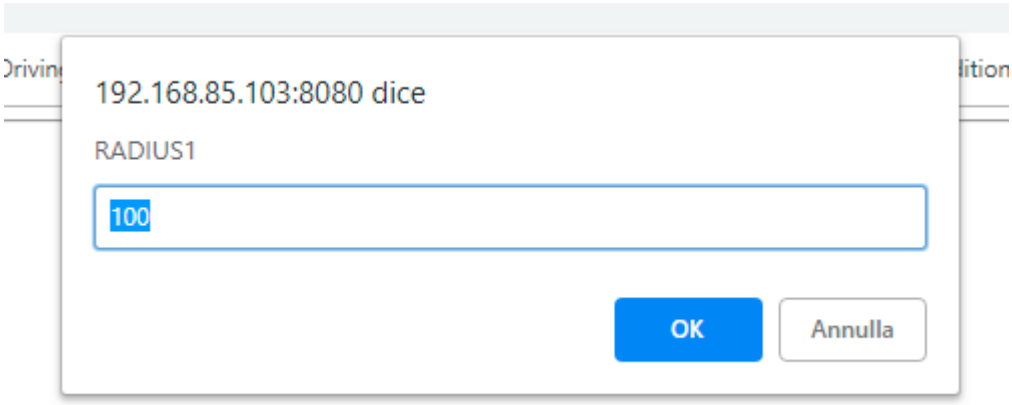
Quando viene aggiunta una regola, la regola si avvia automaticamente (RUNNING):

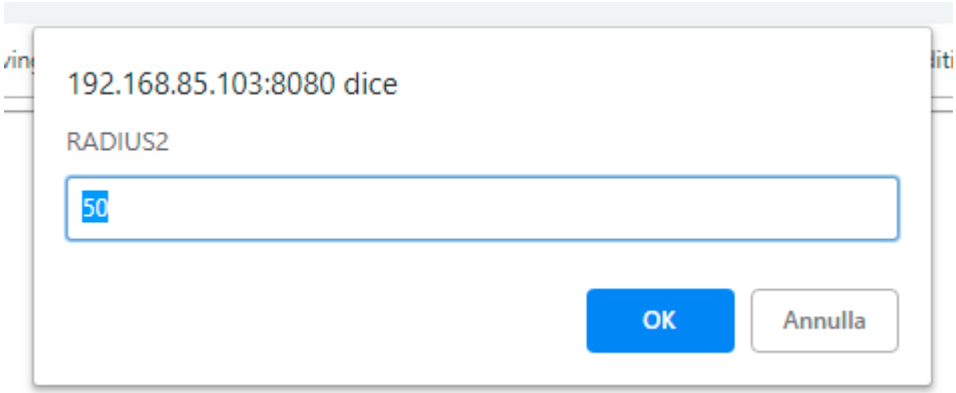


#	Enabled	Index	Description	Period (ms)	If condition 1		If condition 2		If condition 3	Then action 1	Then action 2	Then action 3	Else action 1	Else action 2	Else action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	OR	---	CIRCUMFERENCE = RADIUS1 *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

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

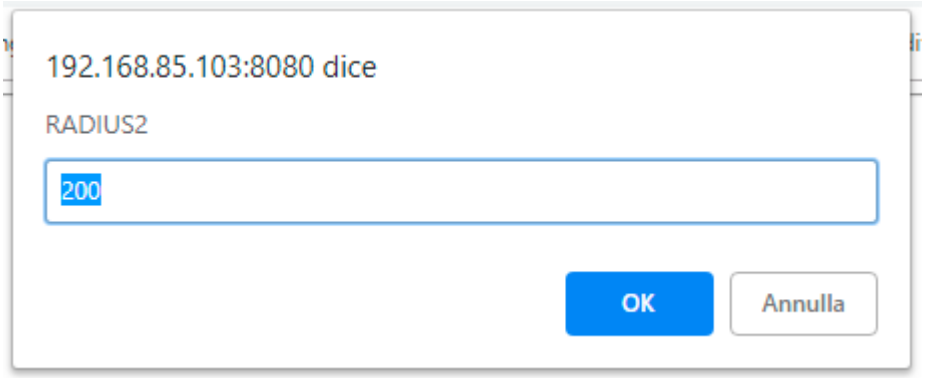
Rule Management	ADD	MODIFY	COPY	MOVE	DELETE	DELETE ALL

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

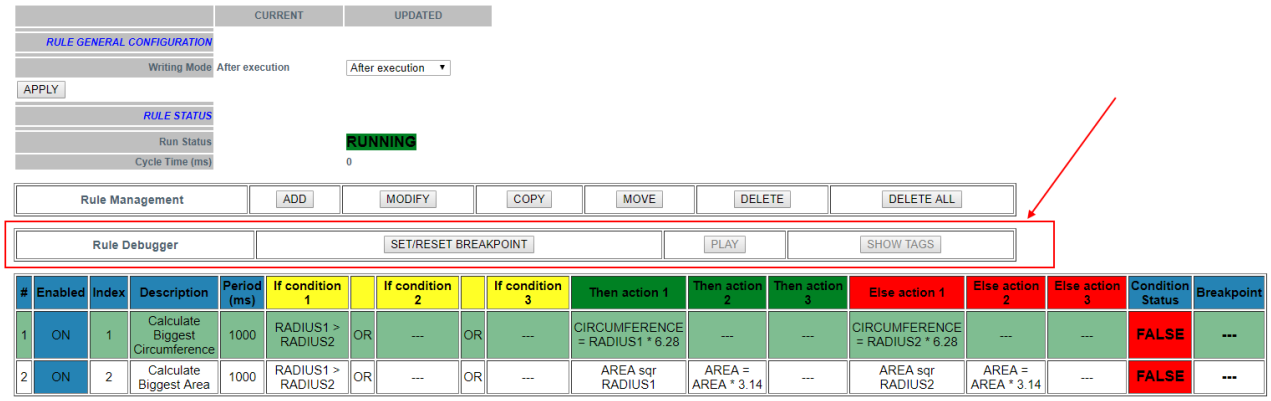
Rule Debugger	SET/RESET BREAKPOINT	PLAY	SHOW TAGS

#	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	---

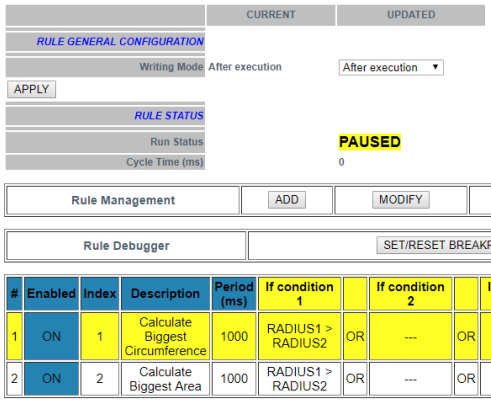
Ora lo stato della condizione delle 2 regole è falso perché RADIUS1 <RADIUS2, quindi vengono eseguite le "Else Actions"

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":

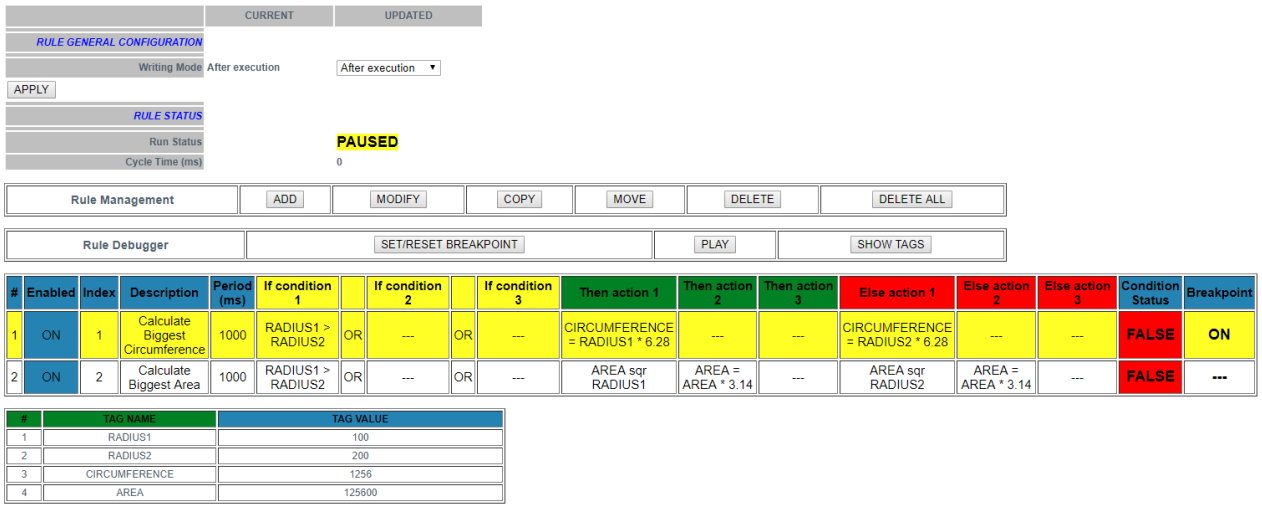


#	Enabled	Index	Description	Period (ms)	If condition 1		If condition 2		If condition 3	Then action 1	Then action 2	Then action 3	Else action 1	Else action 2	Else action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	OR	---	CIRCUMFERENCE = RADIUS1 *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

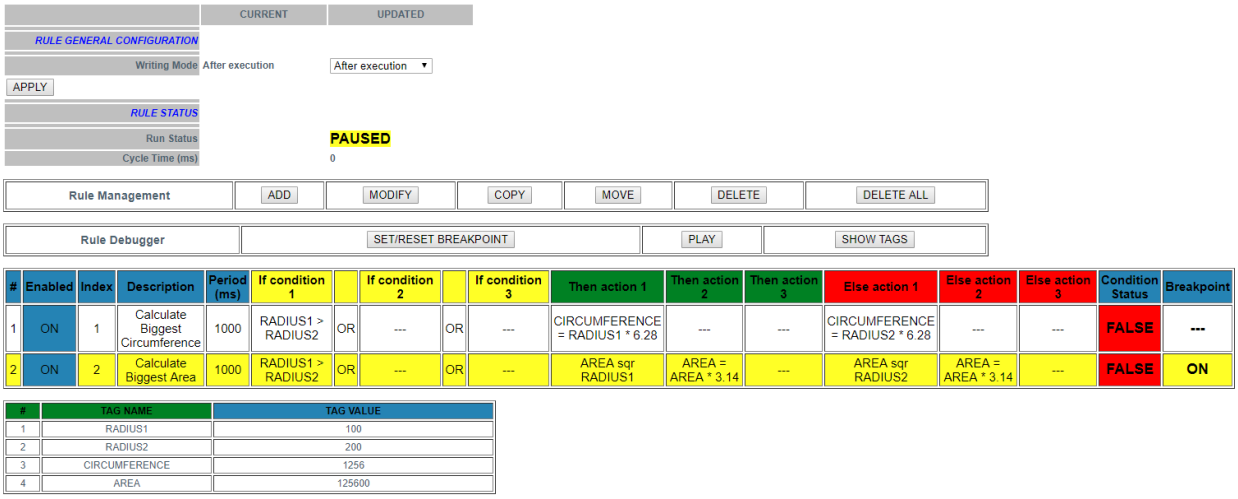


#	Enabled	Index	Description	Period (ms)	If condition 1		If condition 2		If condition 3	Then action 1	Then action 2	Then action 3	Else action 1	Else action 2	Else action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	OR	---	CIRCUMFERENCE = RADIUS1 *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

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:



22.33. DATALOGGER: GENERAL SETTINGS (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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,
-Invio EMAIL
-Invio FTP
-Invio http (se attivo è possibile solo il gruppo 1)
-Invio MQTT (invierà solo dal gruppo 1, gli altri gruppi sono disponibili anche per gli altri protocolli)

In questa sezione esiste un apposito enable per l'invio dei log su http poiché è possibile utilizzare il canale http anche solo per l'invio delle notifiche.
-L'odine di invio: Vengono inviati prima i file più recenti o quelli più vecchi (in caso di mancata comunicazione con il server il dispositivo bufferizza i dati e li invia appena ritorna disponibile il server secondo questa logica).
-È possibile configurare inoltre: il formato della data ora del campione, il tipo di separatore, il numero di cifre decimali, la presenza o no di ulteriori colonne etc…

22.34. GROUP CONFIGURATION (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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. L'azione di trigger è configurabile nella sezione delle logiche vedi 22.32 (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. Minimo: 1 s, Massimo: 7200 s
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. Minimo: 1 min, Massimo: 43200 min

22.35. USB FILE MANAGER (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Questa pagina permette di effettuare il download dei file di log sul proprio PC.
È anche possibile inviare dei file verso il dispositivo.

22.36. DATA LOGGER (SOLO R-PASS-S, Z-PASS2-RT-S E Z-TWS4-RT)

Permette di accedere ai file salvati sulla chiavetta USB collegata.

22.37. ETHERNET INTERFACES

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

22.38. MODBUS SERIAL TRACE (SOLO MODELLI SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

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

22.39. PROTOCOLLO METER-BUS (M-BUS) (SOLO R-PASS-S, Z-PASS2-RT-S, Z-TWS4-RT-S)

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.

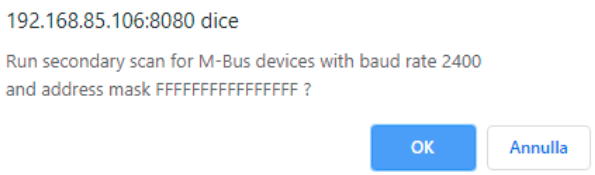
Per gestire i dispositivi M-Bus sono disponibili le seguenti risorse:
- le pagine web della sezione "M-Bus".
- la funzione MBUS_READ_CTL
- il blocco funzione MBUS_WRITE_RAW

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.

22.39.1. M-BUS SCAN

The "SECONDARY SCAN" button lets you scan the bus, detecting M-Bus secondary addresses; select the correct baud-rate for the COM1 serial port or select "All" to repeat the scan for any possible baud-rate[1]; then click on the button; a confirmation pop-up will be shown.

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.

M-Bus scan in progress with baud rate 2400, please wait...

(55 seconds elapsed)

STOP SCAN

#	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:

M-Bus Scan Parameters
NOTE: only on serial port COM1 with mode set to Z-MBUS

Baud Rate (bit/s) All
NOTE: "All" means all baud rates except for 38400

Address Mask (for secondary scan) FFFFFFFFFFFFFFF

PRIMARY SCAN SECONDARY SCAN CREATE CONFIGURATION

READ DATA

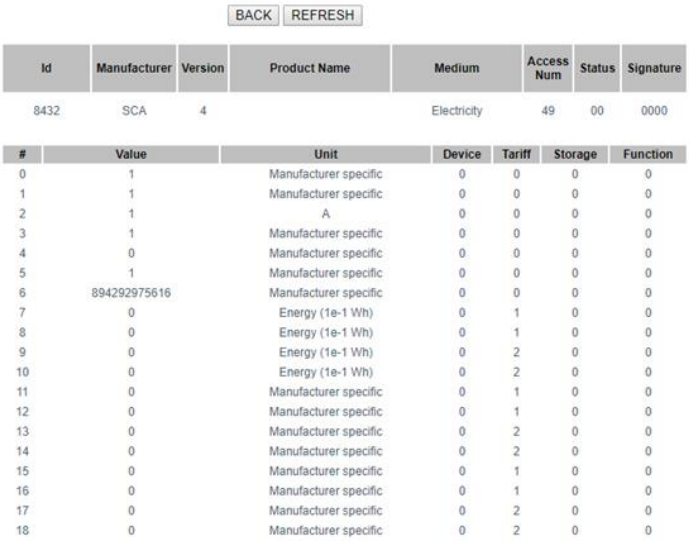
#	Baud Rate (2400)	Address (Mask=FFFFFFFFFFFFFFF)
1	2400	00008431614C0402
2	2400	00008432614C0402
3	2400	00008434614C0402
4	2400	00008435614C0402
5	2400	00008436614C0402
6	2400	00008441614C0402
7	2400	00008444614C0402
8	2400	00008446614C0402
9	2400	00008449614C0402
10	2400	00008453614C0402
11	2400	00008454614C0402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

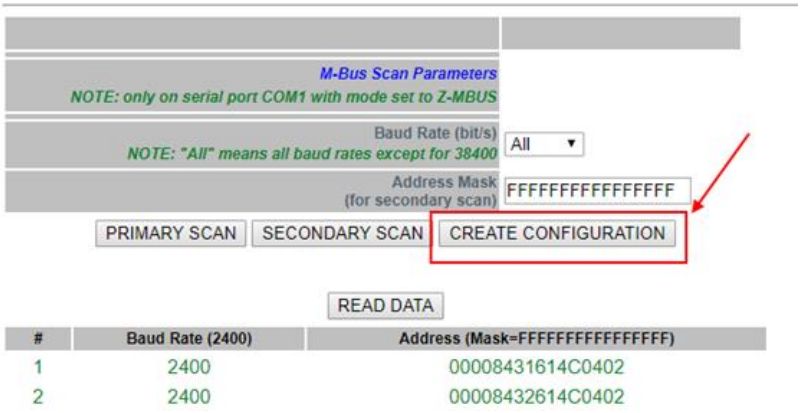
- la prima tabella contiene una sola riga, che fornisce le "informazioni slave";

- 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.

22.39.2. PULSANTE "CREATE CONFIGURATION"

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

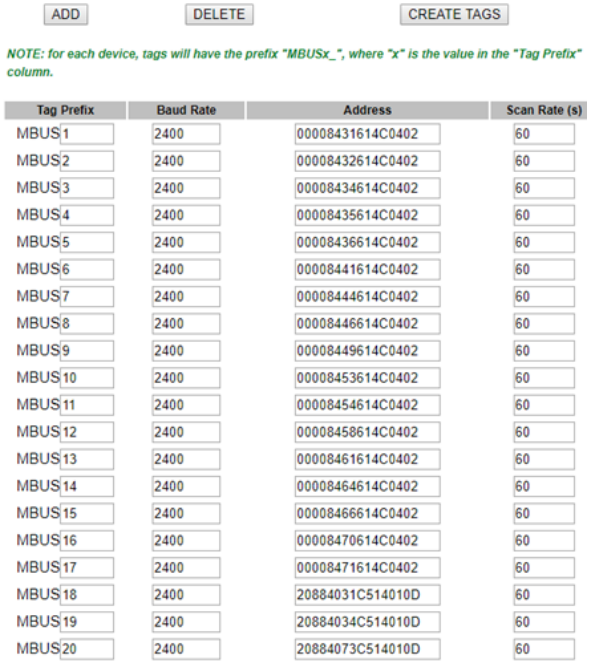


#	Baud Rate (2400)	Address (Mask=FFFFFFFFFFFFFFFF)
1	2400	00008431614C0402
2	2400	00008432614C0402

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".

22.39.3.M-Bus Configuration

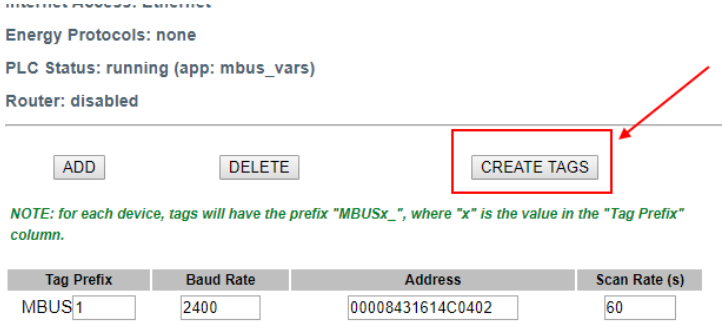
Dopo aver premuto il pulsante “Crea configurazione” nella pagina M-Bus Scan si ottiene la seguente pagina nella configurazione M-Bus:



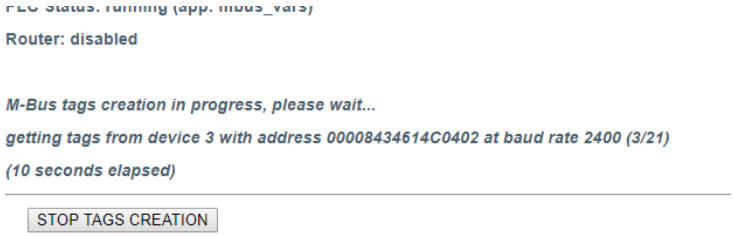
Il risultato della scansione può ora essere modificato.
La prima colonna rappresenta il nome Prefisso del Tag in Straton
La seconda colonna rappresenta il Baud Rate da utilizzare.
La terza colonna rappresenta l'indirizzo del dispositivo.
La quarta colonna rappresenta il tempo di scansione in secondi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

22.39.4.IMPORTAZIONE DELLA CONFIGURAZIONE IN STRATON

Prima di tutto dobbiamo esportare l’attuale configurazione.

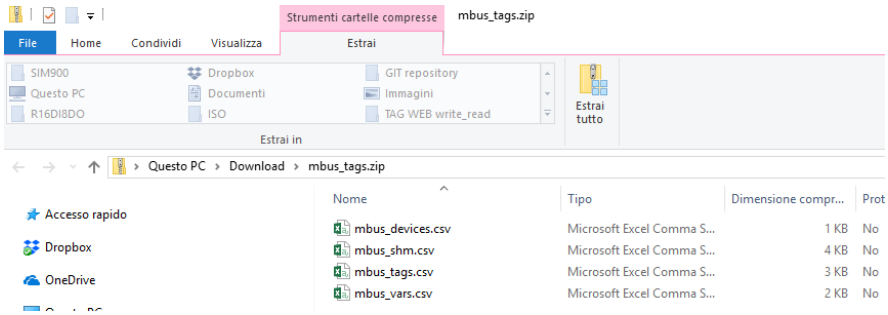


Ora l'acquisizione automatica dei tag inizia:



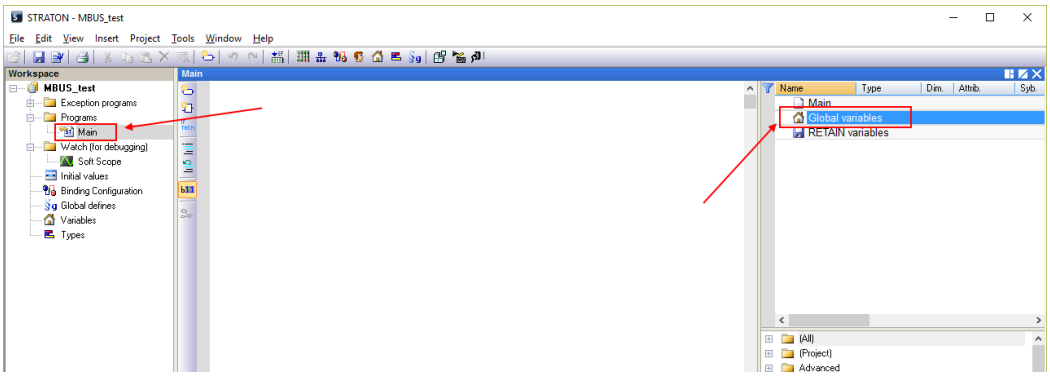
Alla fine del processo un file .zip (mbus_tags.zip) verrà scaricato dal browser:

Il file .zip contiene 4 file:

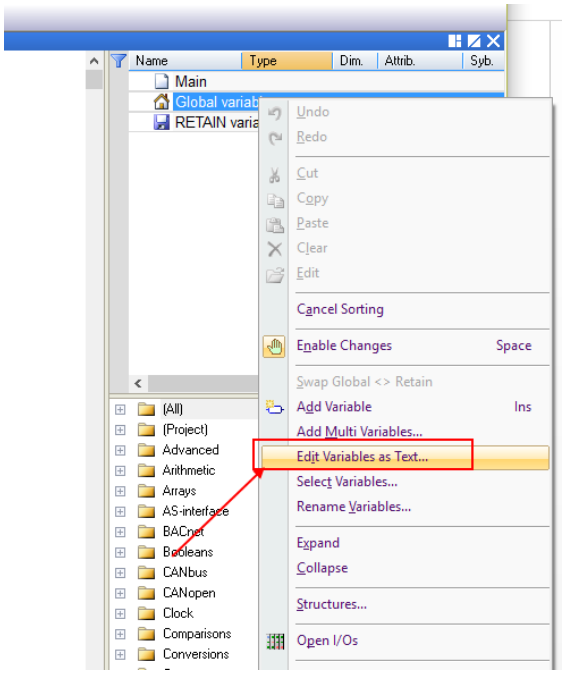


Due di questi file devono essere utilizzati in Straton:
mbus_shm.csv (la configurazione della memoria condivisa)
mbus_vars.csv (l'M-Bus vars)
A questo punto eseguire i seguenti punti:

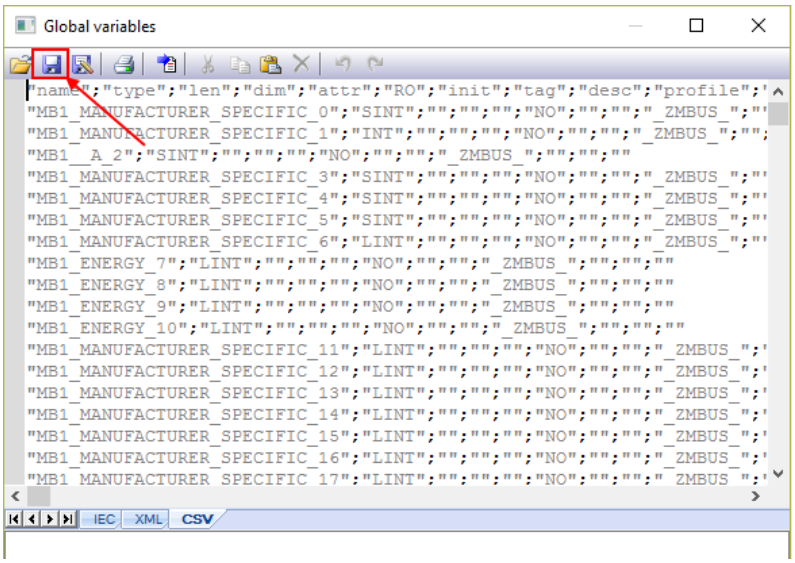
1) Estrarre il file zip in una directory.
2) Avviare Straton workbench
3) Selezionare main e poi Global variables:



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

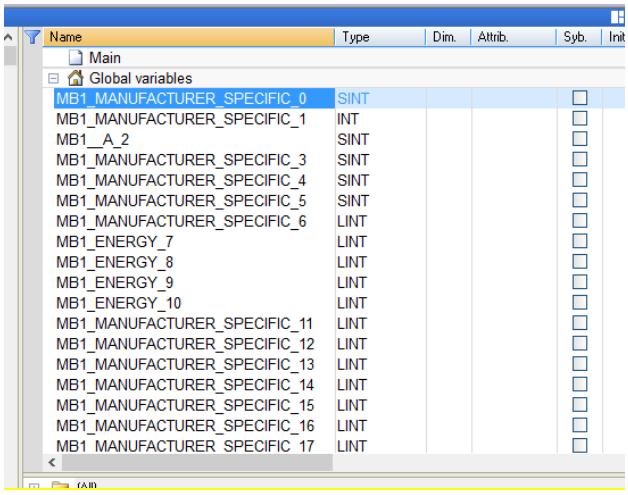


Aprire il file “mbus_vars.csv” con un editor di testo, copiare e incolla l'elenco delle variabili nel modulo "Global variables" in Straton quindi salva la configurazione con l'icona "disco":

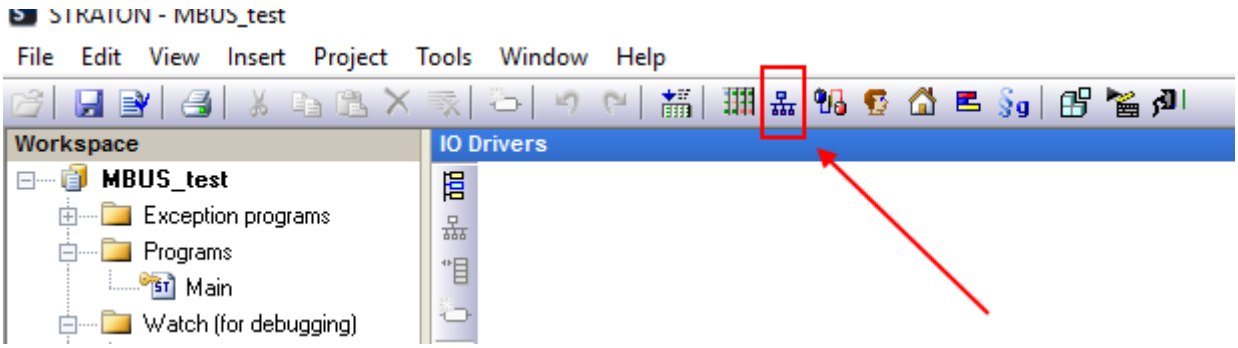


NOTA: La prima riga
"nome";"tipo";"len";...
deve essere presente una sola volta e solo nella prima riga.

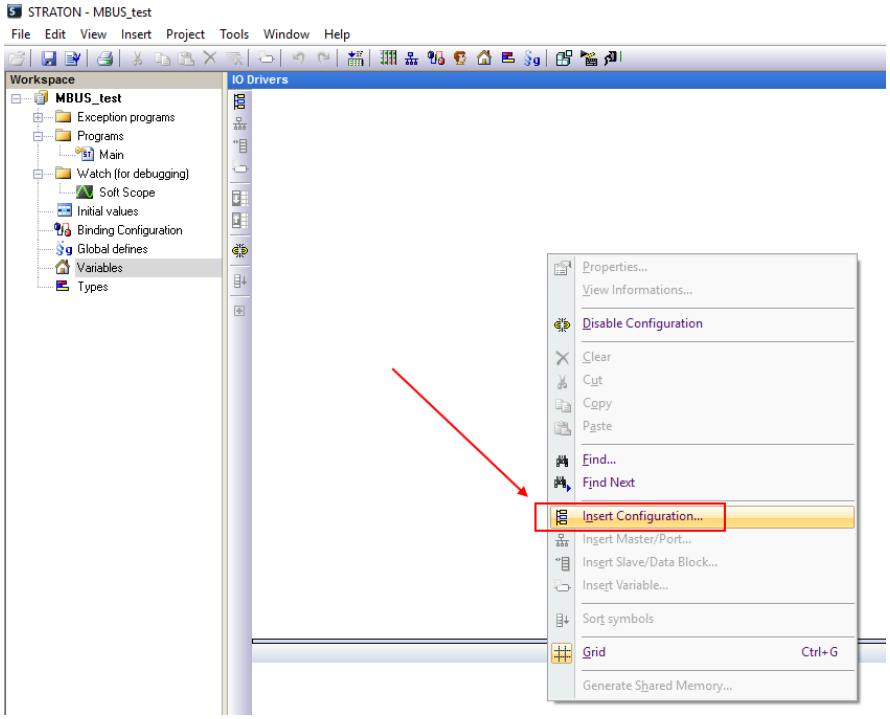
Ora le variabili sono importate:



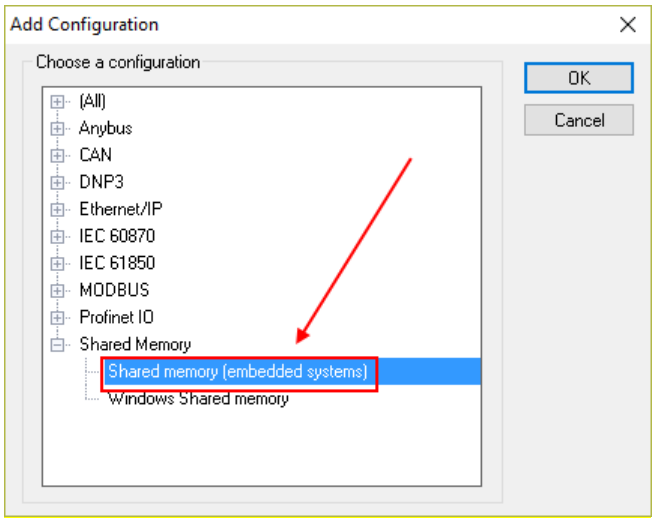
Ora dobbiamo creare la memoria condivisa utilizzata per condividere i dati da M-BUS:
Fare clic sull'icona del bus di campo:



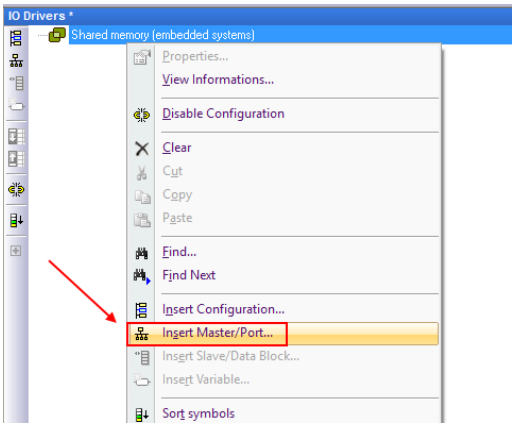
Fare clic con il tasto destro del mouse e selezionare “Insert Configuration”:



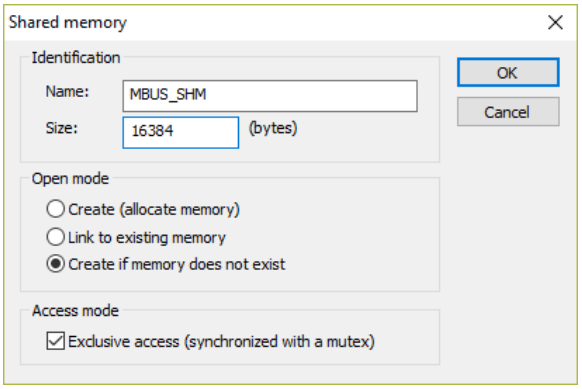
Ora creare la Shared Memory:



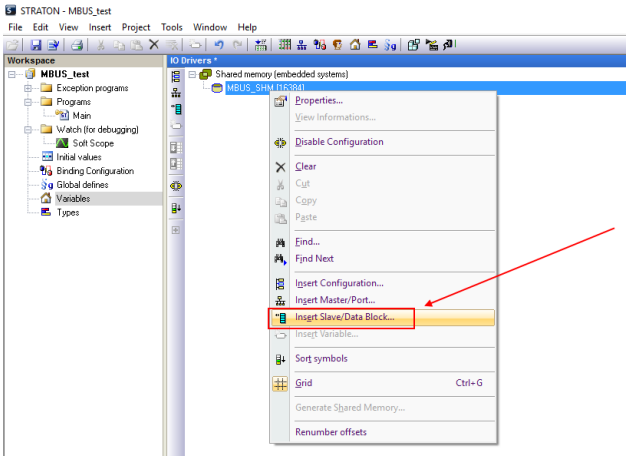
Inserire una porta Master:



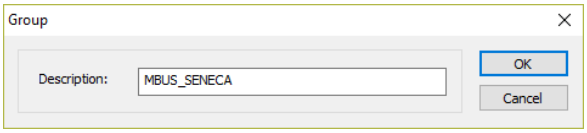
La configurazione della memoria shared deve essere come da figura (non cambiare il setting):



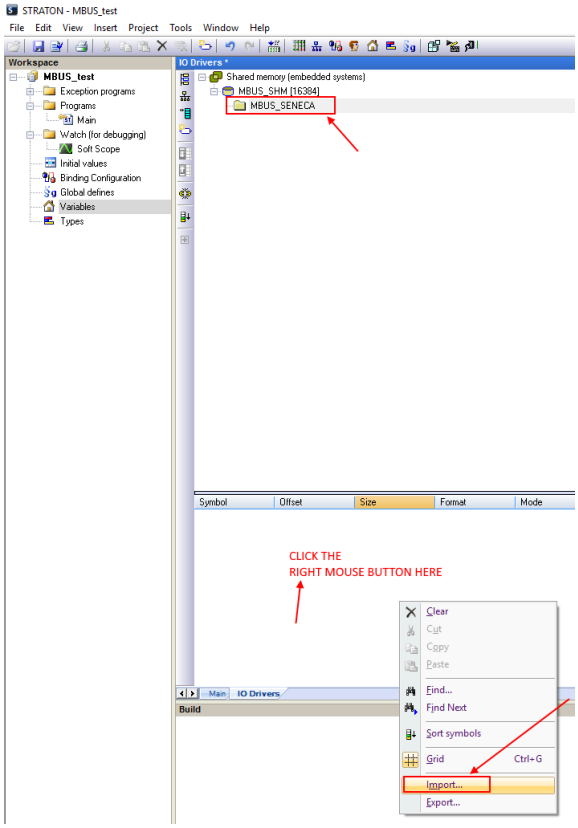
Ora inserire il data block:



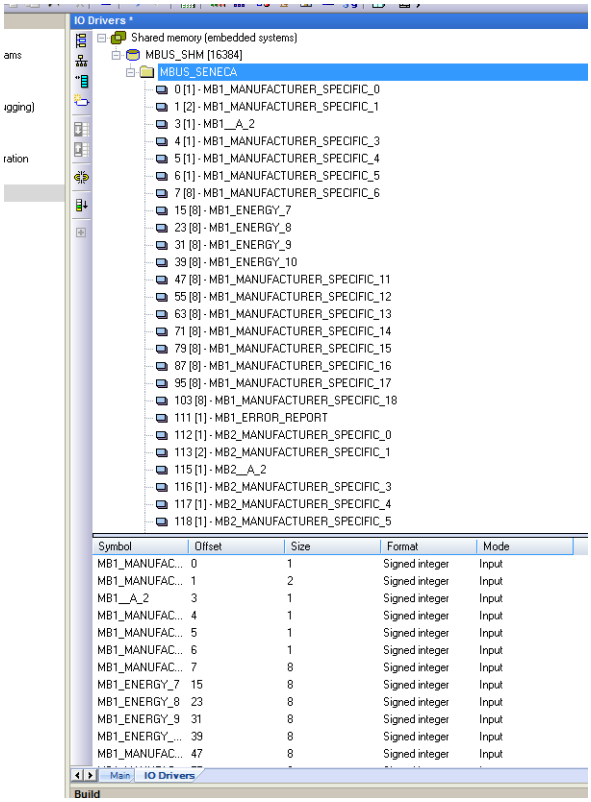
Creare un Gruppo ed inserire un nome:



Ora importare il file della shared memory:

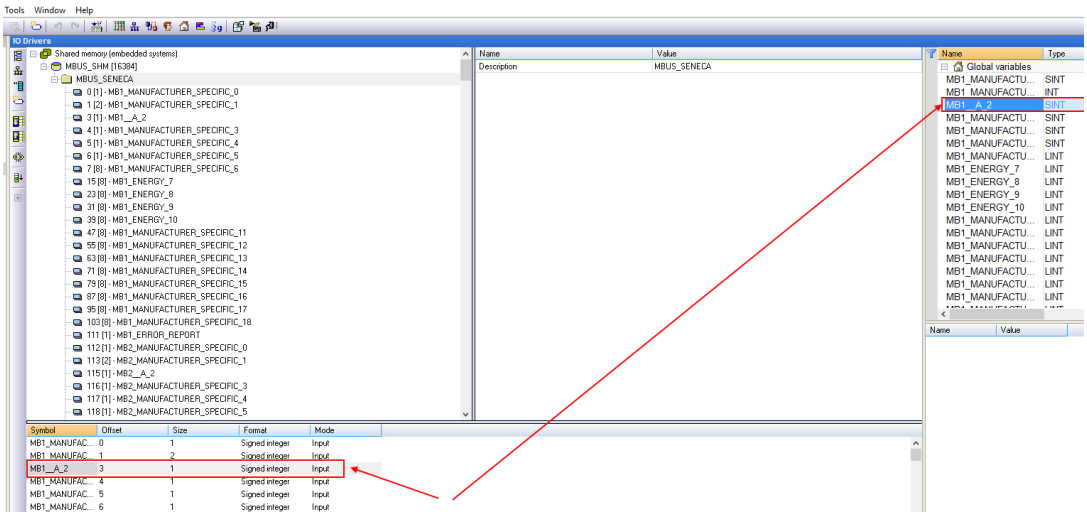


Selezionare il file “mbus_shm.csv”:

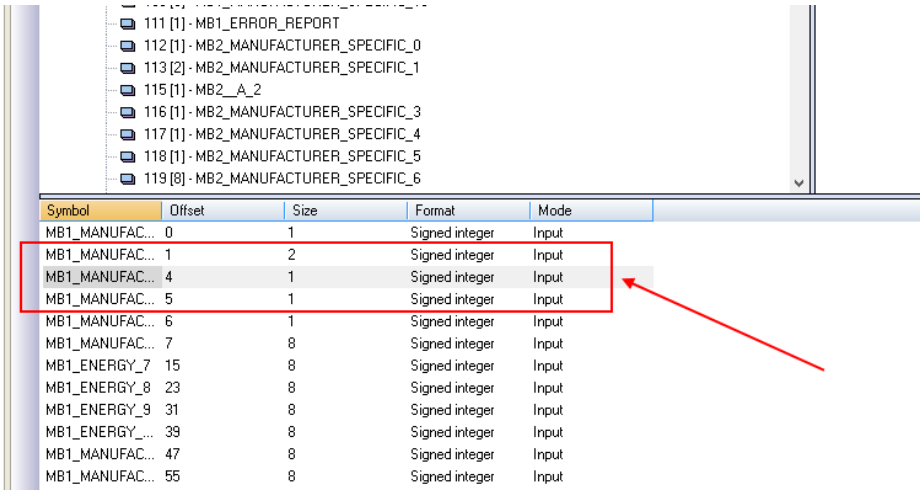


22.39.5.CANCELLARE LE VARIABILI MBUS NON UTILIZZATE

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:



22.39.6. 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

22.39.7.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)

22.39.8.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

22.39.9. 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

22.40. FIRMWARE VERSION

Riporta la revisione del firmware attuale e del firmware presente nella partizione di emergenza.

22.41. FIRMWARE UPGRADE

Permette di aggiornare il firmware del dispositivo.

22.42. CONF. MANAGEMENT

Permette di esportare o importare la configurazione del dispositivo (utile nel caso si debba copiare la configurazione su un altro dispositivo).
È anche possibile salvare i file di log di sistema (debug log) per essere inviati al supporto Seneca.

22.43. LICENCE MANAGEMENT (SOLO SSD)

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.
Per maggiori informazioni fare riferimento al supporto Seneca.

22.44. WEBSERVER CON ACCOUNT “GUEST”

È possibile accedere al sito di configurazione del dispositivo con account “guest”; a tale account è consentito accedere a tutte le pagine ad eccezione della “FW Upgrade”, “Configuration Management” e “USB File Manager”, visualizzando tutti i parametri di configurazione e le informazioni di stato, senza modificare alcun

parametro; 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

22.45. WEBSERVER CON ACCOUNT “USER”

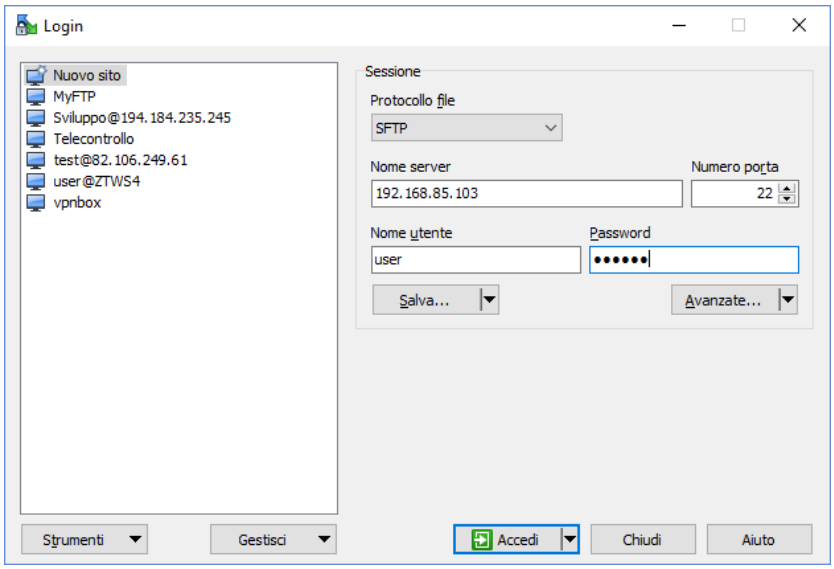
È possibile accedere al sito di configurazione del dispositivo con account “user”; questo account può accedere solo alle pagine "Summary" e "Tag View".
Per accedere con account "user", collegarsi al browser all'indirizzo IP del dispositivo sulla porta 8080, ad esempio:
http://192.168.90.101:8080
e, quando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

22.46. ACCESSO FTP / SFTP

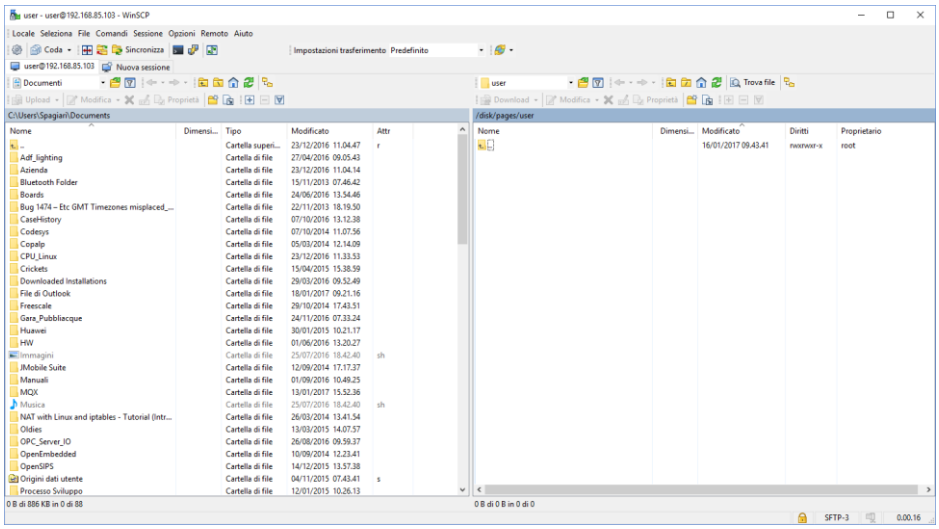
Per accedere facilmente al dispositivo tramite FTP / SFTP, è possibile utilizzare ad esempio il programma WINSCP; puoi scaricare gratuitamente WINSCP da:
http://winscp.net/eng/download.php

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.

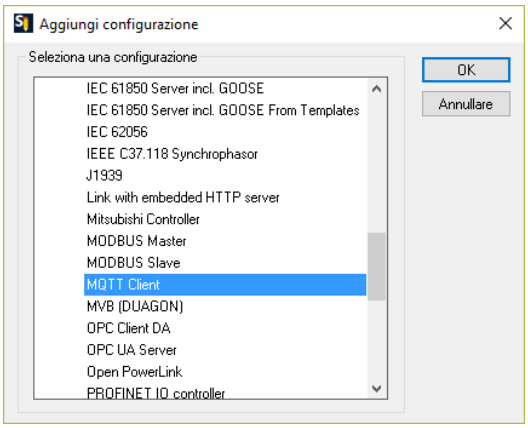


Il programma WinSCP può essere utilizzato sia come client FTP che SFTP per trasferire file da / al dispositivo; basta selezionare il protocollo "FTP" o "SFTP" nella finestra "Accesso WinSCP"; normalmente, è meglio utilizzare SFTP, poiché fornisce un servizio sicuro (cioè crittografato).



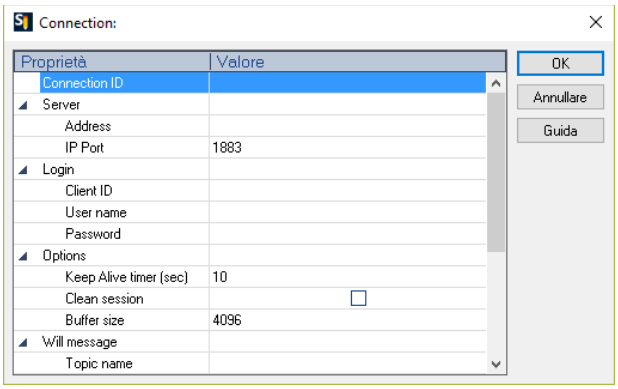
23. PROTOCOLLO MQTT CLIENT (SOLO R-PASS-S, Z-PASS2-RT-S, Z-TWS4-RT-S)

La versione MQTT supportata è la 3.1.1
Per utilizzare il protocollo MQTT è necessario utilizzare Straton workbench 9.3 o successivo.
Per utilizzare il client MQTT selezionalo dalla sezione Straton Workbench Fieldbus:



23.1. 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

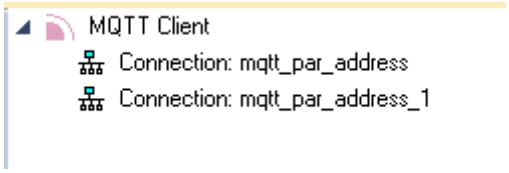
Nel campo “Password” digitare: mqtt_par_password in modo che il campo “Password” sia ottenuto dal file:
/var/esegui/mqtt_par_password

Attenzione!

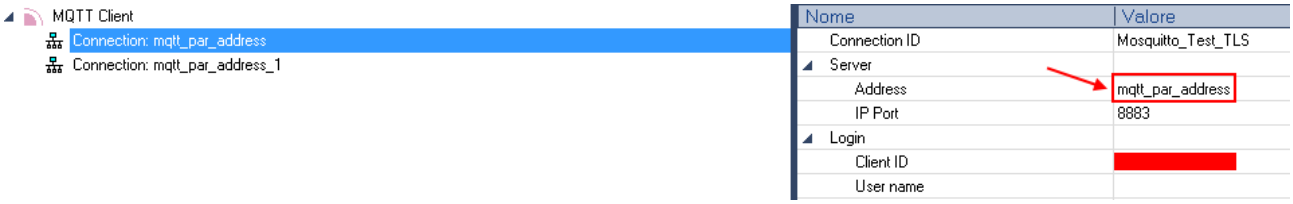
il parametro Address non deve contenere un FQDN, ma l’indirizzo IP, questo perché il FB MQTTCONNECT non esegue la risoluzione DNS.
In alternativa, può contenere il nome del file (es.: mqtt_par_address), creato nella directory /var/run dal FB DNS_RESOLVE e contenente il risultato della risoluzione DNS.

23.1.1. GESTIRE CONNESSIONI MQTT MULTIPLE

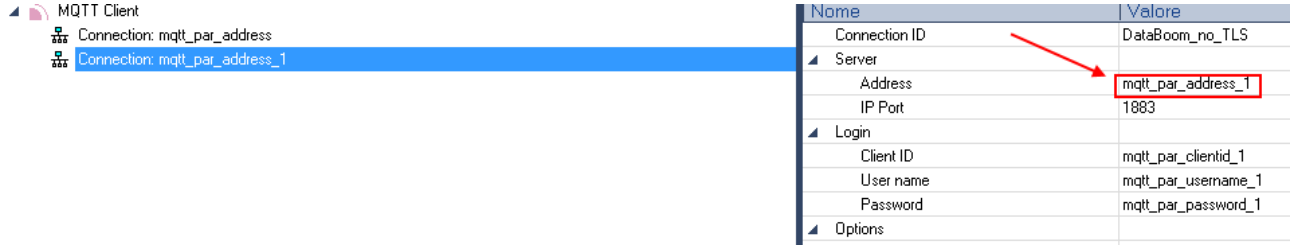
È possibile gestire più connessioni MQTT utilizzando parametri che iniziano con le parole speciali (mqtt_par_address123, mqtt_par_address_aaa, …), ad esempio per creare 2 connessioni mqtt:



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).

23.2. CONFIGURAZIONE MQTT DEI RETRY SSL/TLS

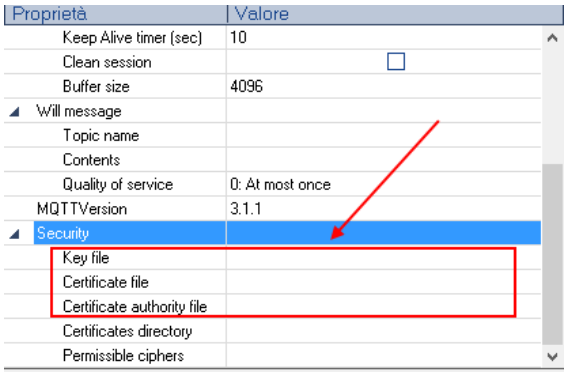
La configurazione predefinita per la connessione SSL/TLS MQTT è:
CONN _TRY_MAX = 10
CONN_TRY_WAIT = 1000 ms
In cui si:
CONN _TRY_MAX è il numero di tentativi per la connessione.
CONN_TRY_WAIT è il timeout di ogni tentativo di connessione.
Se è necessario modificare questa configurazione predefinita è 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.

23.3. 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...

23.4. 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.

24. RESET DI FABBRICA

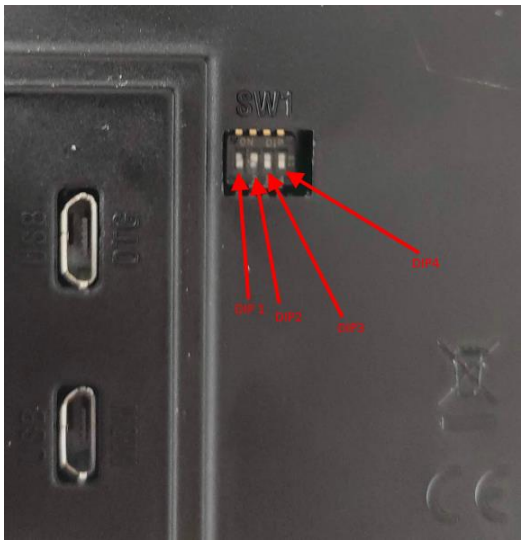
Con questa procedura è possibile ottenere:

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)

24.1. 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

24.2. 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

24.3. 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

25. MAINTENANCE MODE (SOLO SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

Tramite webserver o tramite modbus tcp-ip/RTU è possibile attivare la modalità manutenzione.
Nella modalità manutenzione i tag non sono scrivibili tramite il pannello ma solo tramite i protocolli (ethernet e seriali).
Per abilitare la “maintenance mode” portare ad 1 il valore del registro “Maintenance Mode”.

26. REGISTRI MODBUS I/O EMBEDDED (SOLO SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

26.1. SSD

I registri che rappresentano gli I / O sono accessibili tramite protocollo Modbus TCP-IP o RTU e sono riportati nella tabella seguente:

Data Type	Digital I/Os	Indirizzo di default
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, 3 = 4G)	50 (40051)
Discrete Inputs	DI1	0 (10001)
Discrete Inputs	DI2	1 (10002)
Coils	DO1	0
Coils	DO2	1

26.2. R-PASS

I registri che rappresentano gli I / O digitali sono accessibili tramite protocollo Modbus TCP-IP o RTU e sono riportati nella tabella seguente:

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 = 4G)	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)

26.3. Z-PASS1-RT, Z-PASS2-RT

I registri che rappresentano gli I / O digitali sono accessibili tramite protocollo Modbus TCP-IP o RTU e sono riportati nella tabella seguente:

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	1 (40002)

	Bit 5: DO6	
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 = 4G)	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

27. COMANDI SMS (SOLO MODELLI R-PASS E Z-PASS2-RT)

Sui dispositivi R-PASS+R-COMM e Z-PASS2-RT 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, 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.

27.1. 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)
```

27.2. 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
```

27.3. 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)
```

27.4. 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
```

27.5. 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]
```
[2]

"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
```

[2] Le parentesi quadre indicano che il parametro è facoltativo.

27.6. 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
```

27.7. 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
```

27.8. 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
```

27.9. 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
```

27.10. 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)[3], 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)

→    GET DIN2
←    GET DIN2 EXECUTING (0)
```

27.11. 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)[4], 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

[3] Questa condizione può essere vera per Z-PASS2-RT-4G.
[4] Questa condizione può essere vera per Z-PASS2-RT-4G.

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)
```

27.12. 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

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".

Esempio:

```
→    SET DOUT2.CLOSE
←    SET DOUT2.CLOSE EXECUTING
```

[5] Questa condizione può essere vera per Z-PASS2-RT-4G.

27.13. 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[6], 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";
- 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
```

27.14. 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.

[6] Questa condizione può essere vera per Z-PASS2-RT-4G.

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
```

27.15. 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.

27.16. 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
```

27.17. 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.

27.18. 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[7] ("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.

[7] Consultare il Capitolo "LED di segnalazione".

Esempio:

```
→     STATUS
←     STATUS EXECUTING (Z-PASS2-RT-4G 2018/03/09 08:01:31 RUNNING
OFF,OFF HI,LO,HI,LO,LO,LO)
```

27.19. 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)
```

27.20. RESET

Questo comando può essere utilizzato per riavviare ("reboot") il dispositivo.

Questo comando non viene mai rifiutato.

Esempio:

```
→    RESET
←    RESET EXECUTING
```

27.21. 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)
```

27.22. 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

27.23. 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

27.24. 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

27.25. CLEAN LOGS

Questo comando eliminerà tutti i registri di dati.

→ CLEAN LOGS

← CLEAN LOGS EXECUTING

28. Z-NET4 (SOLO R-PASS-S, Z-TWS4-RT-S, Z-PASS2-RT-S)

Quando si utilizzano i PLC Seneca con i moduli I/O Modbus RTU, uno strumento molto utile e potente è fornito dalla suite di programmi Z-NET4, in esecuzione su PC Windows.
Tra le altre cose, questi programmi ti consentono di:
• aggiungere automaticamente i moduli I/O disponibili sul bus;
• configurare il PLC e i moduli I/O;
• creare automaticamente un progetto Straton contenente le variabili I/O, con i task Modbus necessari per acquisirle/controllarle e le variabili corrispondenti agli I/O presenti nel dispositivo;
• generare automaticamente codice per il progetto Straton, eseguendo “Funzioni di Controllo Remoto”, quali:
Registrazione dati
SMS di comando e stato
Generazione allarmi
• creare facilmente pagine web personalizzate, con widget grafici, e caricarle nella CPU

Il software Z-NET4 è disponibile al seguente link:
http://www.seneca.it/products/z-net4
Si prega di contattare Seneca per avere maggiori informazioni sulla suite Z-NET4.