USER MANUAL

EDGE IIOT GATEWAY SERIES

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

Introduction

The content of this documentation refers to products and technologies described in it.

All technical data contained in the document may be changed without notice.

The content of this documentation is subject to periodic review.

To use the product safely and effectively, read the following instructions carefully before use.

The product must be used only for the use for which it was designed and manufactured: any other use is under the full responsibility of the user.

Installation, programming and set-up are allowed only to authorized, physically and intellectually suitable operators.

Set-up must be performed only after correct installation and the user must follow all the operations described in the installation manual carefully.

Seneca is not responsible for failures, breakages and accidents caused by ignorance or failure to apply the stated requirements.

Seneca is not responsible for any unauthorized modifications.

Seneca reserves the right to modify the device, for any commercial or construction requirement, without the obligation to promptly update the reference manuals.

No liability for the contents of this document can be accepted.

Use the concepts, examples and other content at your own risk.

There may be errors and inaccuracies in this document that could damage your system, so proceed with caution, the author(s) will not take responsibility for it.

Technical specifications are subject to change without notice.

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 Aligned with firmware 104 revision	MM
26/11/2020	MI00557-3	Eliminated “optional” in the WI-FI characteristics	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 Added R-PASS product with 2 Ethernet ports	MM
06/05/2022	MI00557-7	Added R-PASS-S product aligned with fw 210 revision	MM
15/12/2022	MI00557-8	Added info on SNMP, OPC-UA protocol. Added R-COMM support Aligned with fw 223 version Added function block list for -S versions	MM
20/06/2023	MI00557-9	Additions by Seneca Service	AS / MM
28/06/2023	MI00557-10	Added new models Z-PASS1-RT, Z-PASS2-RT, Z-TWS4-RT, Z-PASS2-RT-S. Replaced VPN BOX with VPNBOX2 Aligned with SSD/R-PASS fw 232 revision Aligned with -RT fw 1012 revision	MM
03/07/2023	MI00557-11	Small corrections	AZ
20/07/2023	MI00557-12	Corrections in Chapter 23 (MQTT client)	MM
21/12/2023	MI00557-13	Chapter 'SMS Commands' added	AZ

TABLE OF CONTENTS

1. INTRODUCTION

⚠ **ATTENTION!**

This user manual extends the information from the installation manual to the configuration of the device. Use the installation manual for more information.

⚠ **ATTENTION!**

In any case, SENECA s.r.l. or its suppliers will not be responsible for the loss of data/revenue or consequential or incidental damages due to negligence or bad/improper management of the device, even if SENECA is well aware of these possible damages.
SENECA, its subsidiaries, affiliates, group companies, suppliers and distributors do not guarantee that the functions fully meet the customer's expectations or that the device, firmware and software should have no errors or operate continuously.

1.1. FIRMWARE WITH OPEN SOURCE LPG

Firmwares can contain Open Source software under GPL contract. According to Section 3b of the GPL, it is possible to have the source code for these parts. The source code with the Open Source software license terms can be obtained upon request from Seneca.
Send your request to supporto@seneca.it with the subject "Open Source".

2. MODELS

The Edge IIOT Gateway series consists of the following models:

MODEL	*DIGITAL I/O*	*ANALOG INPUTS*	*DISPLAY*	*PLC STRATON*	*MODEM 4G*	*INTEGRATED UPS*	*SERIAL PORTS*	*ETHERNET PORTS*	*CAN PORT*	*WIFI*
SSD	2 DIDO	NO	7" TOUCH	NO	NO	NO	2	2	NO	YES
R-PASS	4DI 4DO	2	NO	NO	OPTIONAL	OPTIONAL	2	2 or 4	YES	OPTIONAL
R-PASS-S	4DI 4DO	2	NO	YES	OPTIONAL	OPTIONAL	2	2 or 4	YES	OPTIONAL
Z-PASS1-RT	6 DIDO	2	NO	NO	NO	NO	3	2	YES	NO
Z-PASS2-RT	6 DIDO	2	NO	NO	YES	NO	3	2	YES	NO
Z-TWS4-RT-S	6 DIDO	2	NO	YES	NO	NO	3	2	YES	NO
Z-PASS2-RT-S	6 DIDO	2	NO	YES	YES	NO	3	2	YES	NO

N.B. Depending on the model, the CAN port may be available but not managed by the firmware revision.

2.1. MODEL DESCRIPTION

2.1.1.SSD

Surprise Smart Display is a 7-inch HMI touch-sensitive colour display (capacitive touch panel), with 800 x 480 resolution and LED backlight.
It is also an operator panel designed to control and monitor the device operation,
systems or production lines.
Smart Display also offers extended connectivity thanks to the functionalities of Industrial Gateway, Serial Device Server, Bridge and WI-FI, it is also equipped with an ever increasing number of industrial protocols.
A novelty introduced in the industrial automation world is the possibility to display variables of the Modbus RTU protocol in a completely passive mode (serial sniffer).
The preloaded software application allows you to view parameters, send commands and configure
tags, communication, individual video pages and alarm management.
Includes support for the latest version of LET'S VPN for the maintenance and monitoring of remote devices.

2.1.2.R-PASS

R-PASS is a device designed for the control and monitoring of the operation of devices, systems or production lines, it also offers extensive connectivity thanks to the Industrial Gateway, Serial Device Server, Bridge and WI-FI functions, it is also equipped with a continuously increasing number of industrial protocols especially in the IOT sector.

A novelty introduced in the industrial automation world is the possibility to display variables of the Modbus RTU protocol in a completely passive mode (serial sniffer).

It is also equipped with a virtual display accessible from any device via a web browser.

Includes support for the latest version of LET'S VPN for the maintenance and monitoring of remote devices.

The –S version is also available which includes the PLC Straton IEC 61131.

It is possible to connect the R-COMM option which includes a 4G modem and a UPS (optional).

The model with 2 and 4 Ethernet ports is available, with and without WIFI.

For more information on the Straton PLC refer to the website: https://straton-plc.com/en/

In addition to including the Straton PLC, the –S-E version has licenses for energy management protocols.

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

Z-PASS1-RT is a device designed for the control and monitoring of the operation of devices, systems or production lines, it also offers extensive connectivity thanks to the Industrial Gateway, Serial Device Server and Bridge functions, it is also equipped with a number of continuously increasing industrial protocols especially in the IOT sector.

A novelty introduced in the industrial automation world is the possibility to display variables of the Modbus RTU protocol in a completely passive mode (serial sniffer).

It is also equipped with a virtual display accessible from any device via a web browser.

Includes support for the latest version of LET'S VPN for the maintenance and monitoring of remote devices.

The Z-TWS4-RT version is also available which includes the PLC Straton IEC 61131.

For more information on the Straton PLC refer to the website: https://straton-plc.com/en/

In addition to including the Straton PLC, the-E version has licenses for energy management protocols.

2.1.4.Z-PASS2-RT

Z- PASS2-RT is a device designed for the control and monitoring of the operation of devices, systems or production lines, it also offers extensive connectivity thanks to the Industrial Gateway, Serial Device Server and Bridge functions, it is also equipped with a number of continuously increasing industrial protocols especially in the IOT sector.

A novelty introduced in the industrial automation world is the possibility to display variables of the Modbus RTU protocol in a completely passive mode (serial sniffer).

It is also equipped with a virtual display accessible from any device via a web browser.

Includes support for the latest version of LET'S VPN for the maintenance and monitoring of remote devices.

It integrates a latest generation universal 4G modem.

The –S version is also available which includes the PLC Straton IEC 61131.

For more information on the Straton PLC refer to the website: https://straton-plc.com/en/

In addition to including the Straton PLC, the -E version has licenses for energy management protocols.

2.2. HARDWARE AND SOFTWARE OPTIONS

2.2.1.SSD

Smart Display has the following hardware options:

HARDWARE OPTIONS	DESCRIPTION
SMART DISPLAY	SMART DISPLAY NR 2 INGRESSO DIGITALE NR 2 USCITE DIGITALI NR 2 ETHERNET WI-FI / ROUTER WI-FI

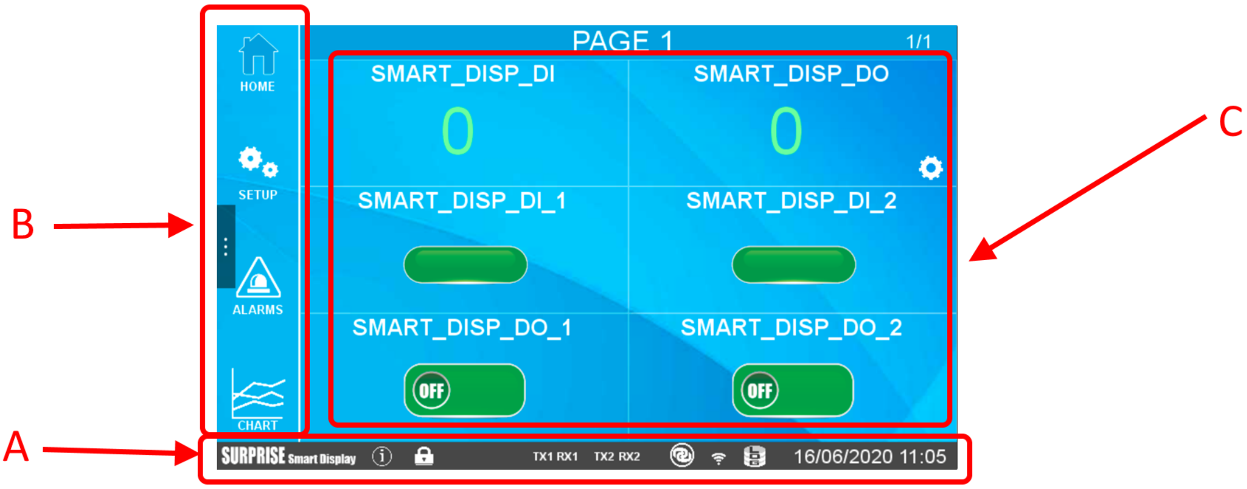
And the following software options (you can also activate more than one package at the same time).

SOFTWARE OPTIONS	DESCRIPTION
BASIC" PACKAGE	Graphic Display with widgets Remote display Climbing Datalogger max 2000tag Alarms Gateway Serial Sniffer Modbus TCP Client/Server protocol Modbus RTU master/Slave protocol OPC-UA server protocol
IOT" PACKAGE	HTTP and MQTT protocol for cloud connection
LOGIC" PACKAGE	Programmable logics through programming "IF THEN ELSE" Remote Alarming
SENECA LET'S" VPN PACKAGE	Simplified VPN connection via "Seneca LET's VPN" environment Or Open VPN Standard

3. THE DISPLAY / REMOTE DISPLAY (ONLY SMART DISPLAY, R-PASS, Z-PASS1-RT, Z-PASS2-RT)

In the Smart Display product the display is integrated into the device, in the R-PASS device the display can be accessed via a web browser connection (e.g. Chrome).

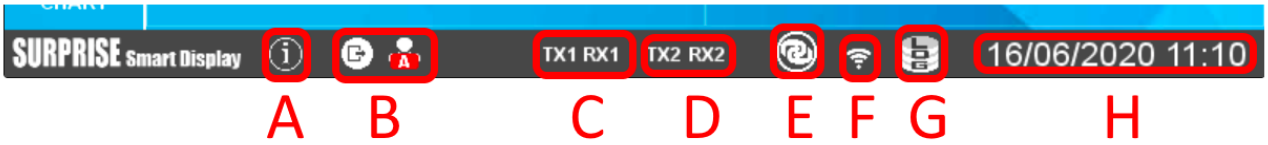
The display consists of 3 sections:



"A" Represents the bar with the device information
"B" Represents the Smart Display menu
"C" Represents the Widget page

3.1. INFORMATION BAR

Represents the information related to the device status , in particular:



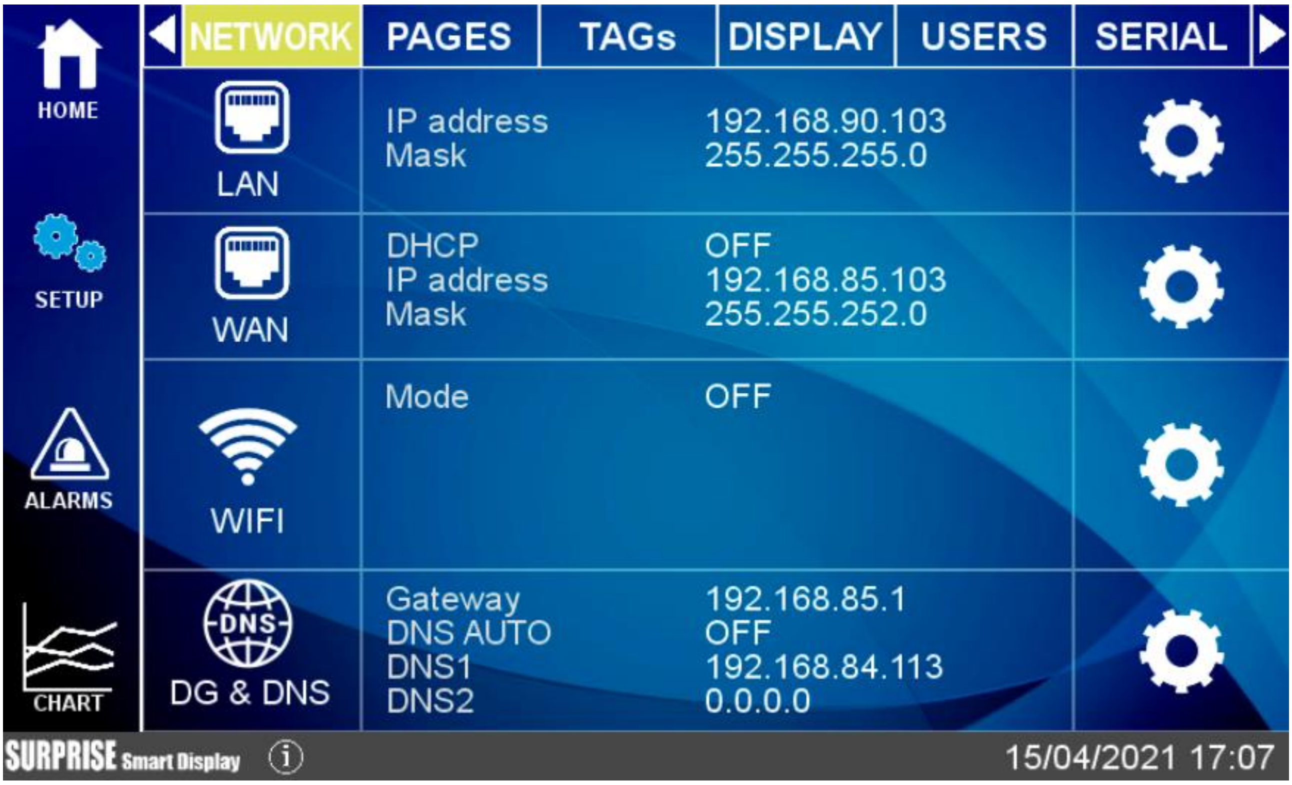
Icon "A" provides information about the device (such as firmware revision) and manufacturer
Icon "B" provides user account information; in case you are not logged in, the icon is replaced by a padlock. The icon on the left, if pressed, allows to logout, the icon on the right indicates the type of user account (A stands for administrator). In the case of guest accounts the icon is shown as follows :G
C" icon shows the status of the serial port COM1
Icon "D" shows the status of the serial port COM2
Icon "E" shows the status of the VPN connection: "Seneca Let's VPN" or "OpenVPN standard".
Icon “F” Provides the strength of the WI-FI signal (if present, depending on the model)
“G" icon shows the status of the datalogger
"H" shows the date/time of the device

3.2. MENU

Shows the menu:
HOME leads to the main page
SETUP leads to device configuration of the device
ALARMS leads to the alarms section
CHART leads to the section related to the graphic analysis of the datalogger data
It is also possible to hide the menu pressing the side bar:

3.2.1.SETUP

3.2.1.1. NETWORK



LAN
IP address 192.168.90.103
Mask 255.255.255.0

WAN
DHCP OFF
IP address 192.168.85.103
Mask 255.255.252.0

WIFI
Mode OFF

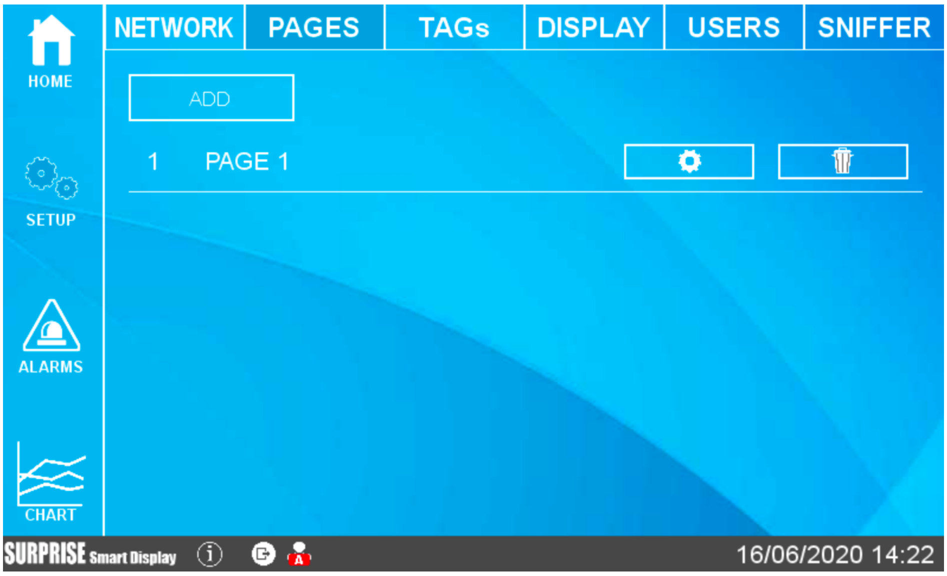
DG & DNS
Gateway 192.168.85.1
DNS AUTO OFF
DNS1 192.168.84.113
DNS2 0.0.0.0

15/04/2021 17:07

In this section it is possible to configure the settings for the LAN and WAN Ethernet ports and WI- FI network port. The WI- WIFI port section allows to you choose WI-FI Station or Access Point mode.

The Station mode allows the device to connect to an existing Wi-Fi network, instead, the Access Point mode allows the device to create a new Wi-Fi network to which other devices can connect.

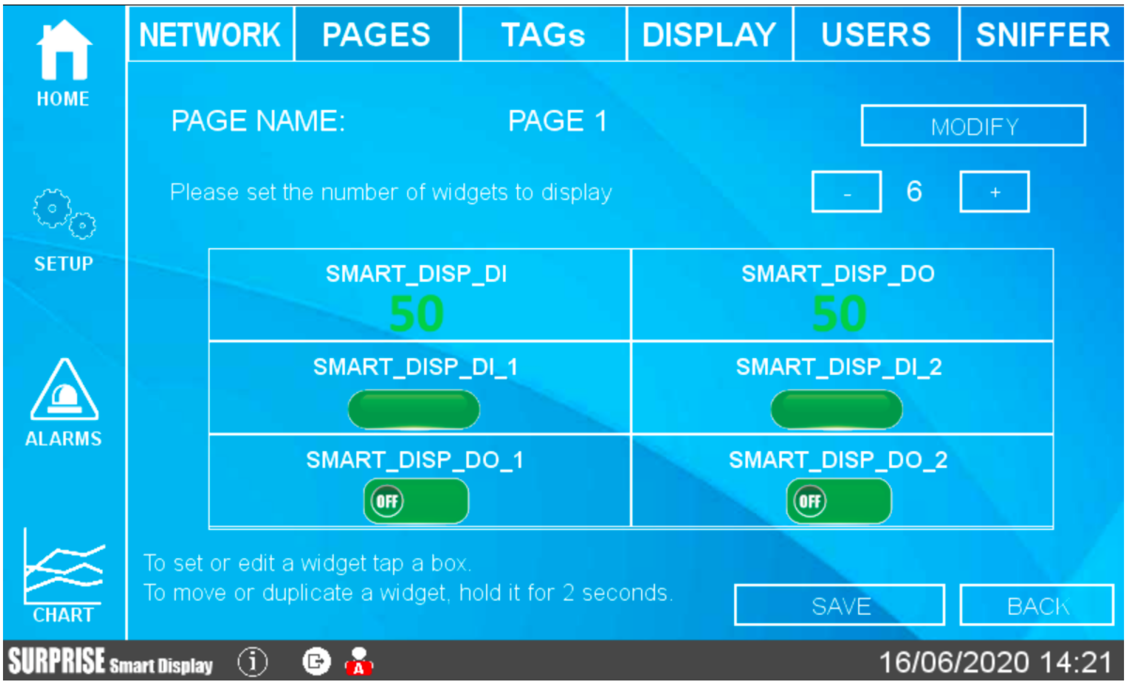
3.2.1.2. PAGES



1 PAGE 1

16/06/2020 14:22

On the first screen it is possible to add as many pages as user desires and once pages are created, he is able to edit configuration of each one.



PAGE NAME: PAGE 1

Please set the number of widgets to display 6

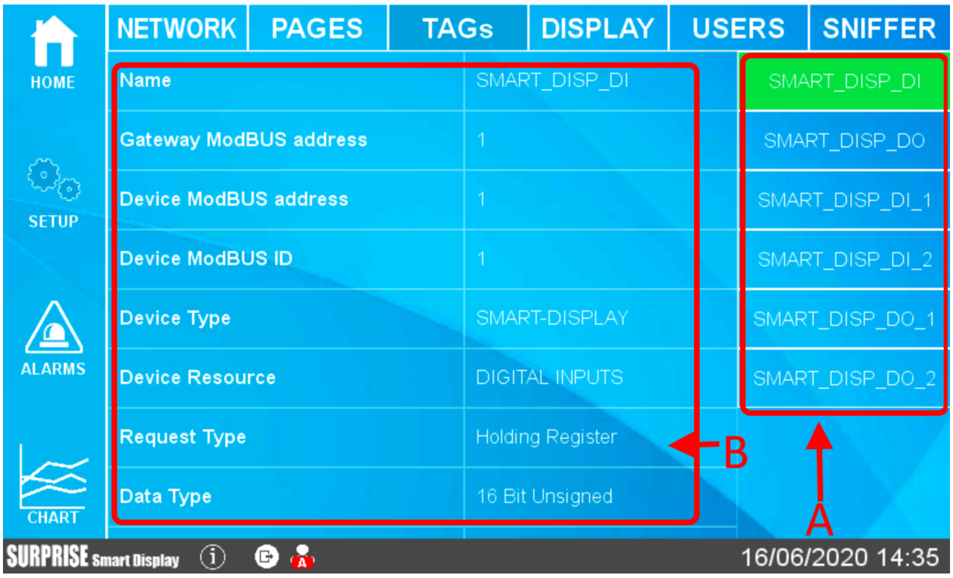
To set or edit a widget tap a box.
To move or duplicate a widget, hold it for 2 seconds.

16/06/2020 14:21

It is possible to change the page name and the number of widgets to show.
In the central part there is a preview of the page visualization.
Pressing on a widget icon it is possible to modify the widget parameters: type, colour, etc...

In addition to a widget page it is possible to add a Synoptic page. In a synoptic page it is possible to freely position the widgets and upload graphics from a PC or from a graphics library inside the device to create synoptic pages without the aid of external software.

3.2.1.3. TAGS

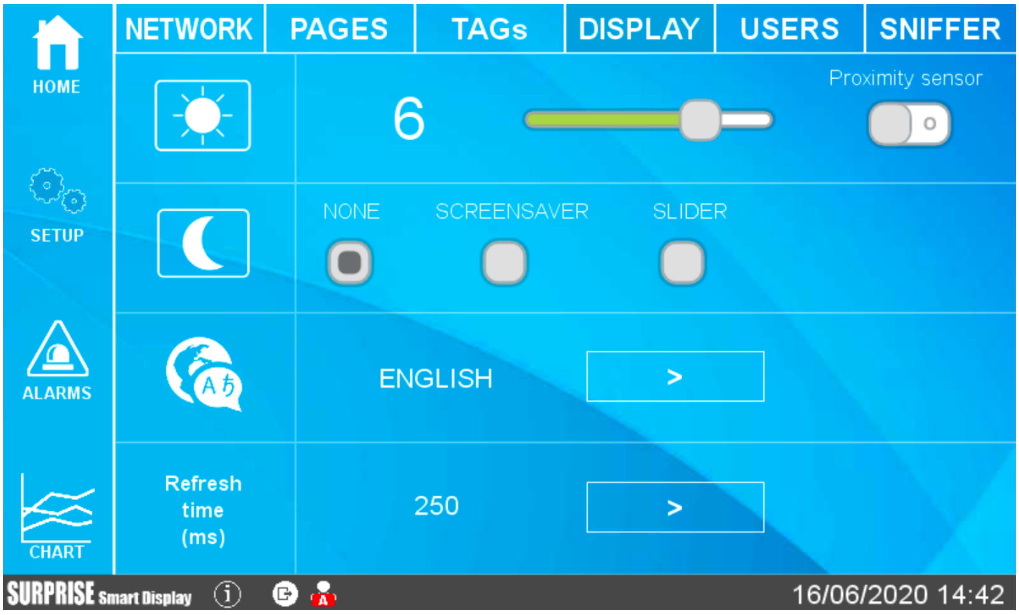


Name	SMART_DISP_DI
Gateway ModBUS address	1
Device ModBUS address	1
Device ModBUS ID	1
Device Type	SMART-DISPLAY
Device Resource	DIGITAL INPUTS
Request Type	Holding Register
Data Type	16 Bit Unsigned

SMART_DISP_DI
SMART_DISP_DO
SMART_DISP_DI_1
SMART_DISP_DI_2
SMART_DISP_DO_1
SMART_DISP_DO_2

In this section the configured tags are visualized.
The device tags are located on the right side (A), it is possible browse the list.
The parameters of each tag appear in the central part (B), you can also scroll through the list.
From firmware version 109 it is possible to add, edit and delete tags also from the display.

3.2.1.4. DISPLAY



6 Proximity sensor

NONE SCREENSAVER SLIDER

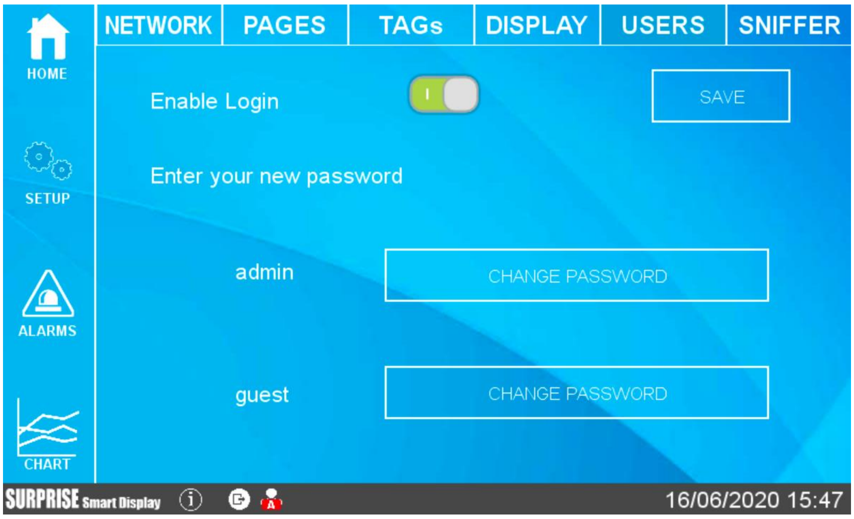
ENGLISH

Refresh time (ms) 250

This section allows to configure the screen brightness, language and screen refresh time.

In order to safeguard the consumption and the duration of the screen, it is possible to activate the screensaver (the backlighting of the screen is lowered after the set idle time).
If the screensaver mode is enabled it is possible to exit by pressing anywhere on the screen (or making a movement in front of the screen if the proximity sensor is activated).
Slider mode, instead, allows to cycle the widget pages automatically after a preset time.

3.2.1.5. USERS



This section allows to configure the users who can access to the display.
It is possible to disable the login to access the display (free access) or activate an administrator account and/or guest account.

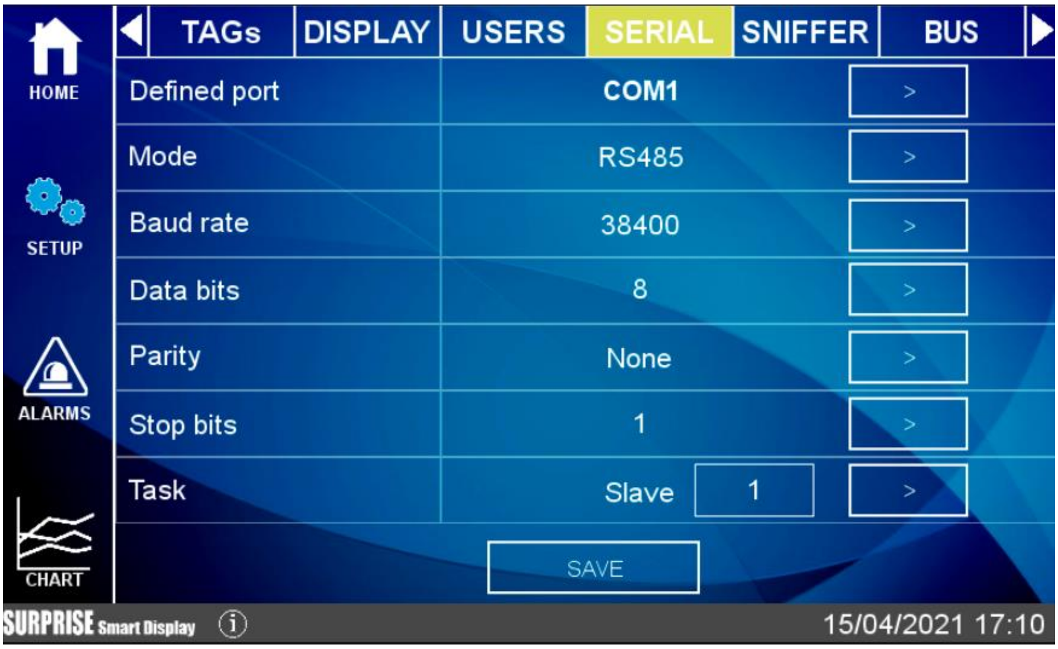
According to the following table

ACCOUNT TYPE	***CHANGING THE VALUE OF A TAG***	***SETUP MENU DISPLAY***	***SETUP MODIFICATION***
ADMIN	Yes	FULL	Yes
GUEST	Yes	ONLY "NETWORK" AND "TAGS"	NO
NO ACCOUNT	No	NO	NO

If the screen saver is switched off and none touch the screen for 2 minutes the system will automatically logout.
If the screen saver is activated and none touch the screen for a time equal to the screen saver time, the system will automatically logout.

3.2.1.6. SERIAL

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



Defined port	COM1	>
Mode	RS485	>
Baud rate	38400	>
Data bits	8	>
Parity	None	>
Stop bits	1	>
Task	Slave 1	>

3.2.1.7. SNIFFER

The serial sniffer function allows to insert one or more Smart Displays in an existing RS485 line with Modbus RTU protocol .

For Modbus RTU protocol there is always a single master and a series of slave devices. The master requires registers to read/write to each slave, who answers sending requested data.

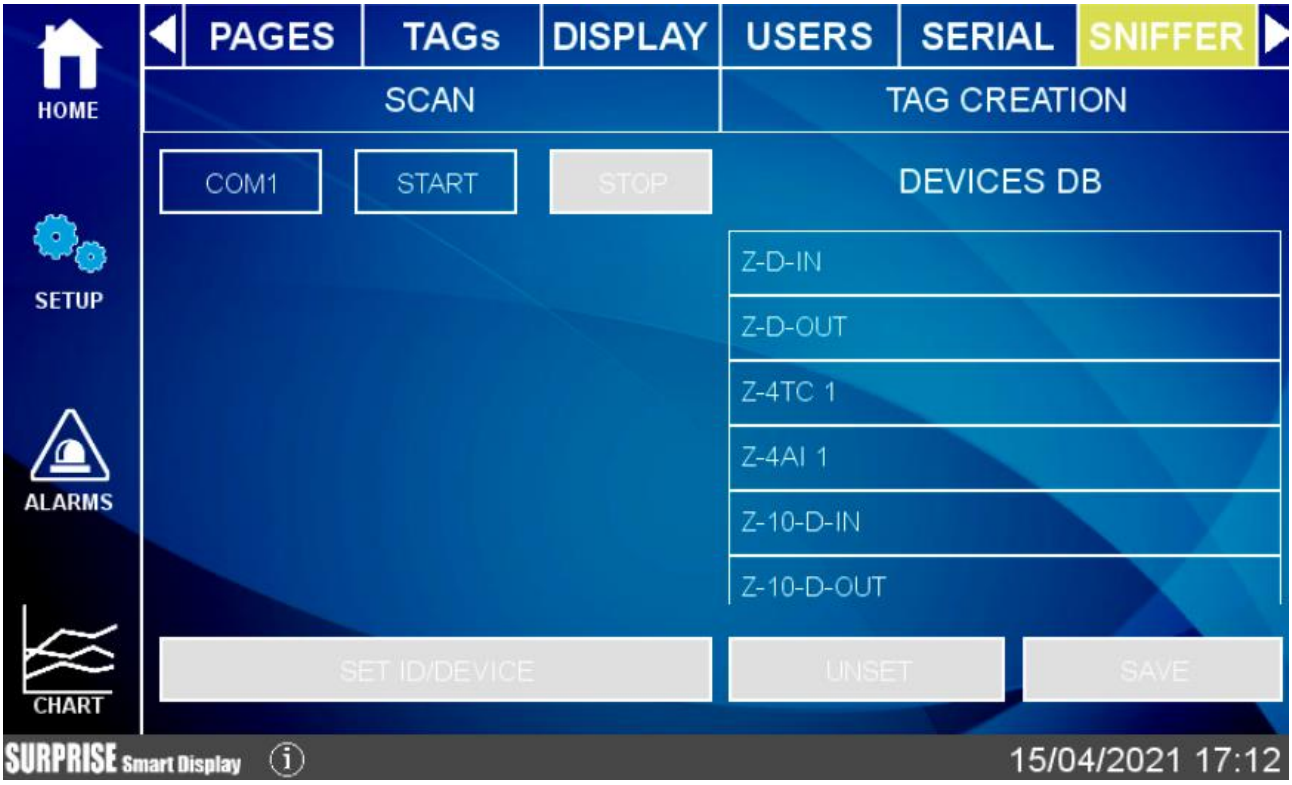
In order to insert a device that displays data without changing the existing configuration, it is necessary to insert one or more smart displays in passive mode (sniffer).

At this point Smart Display will receive all the serial packets transmitted between the master and the slaves and it is necessary associate these packets to tags that will be valued.

ATTENTION!

As the SNIFFER mode is purely passive all defined tags will be read-only

3.2.1.7.1. SNIFFER MODE CONFIGURATION STEPS



The sniffer mode is configured through the following steps (the three buttons at the top of the page):

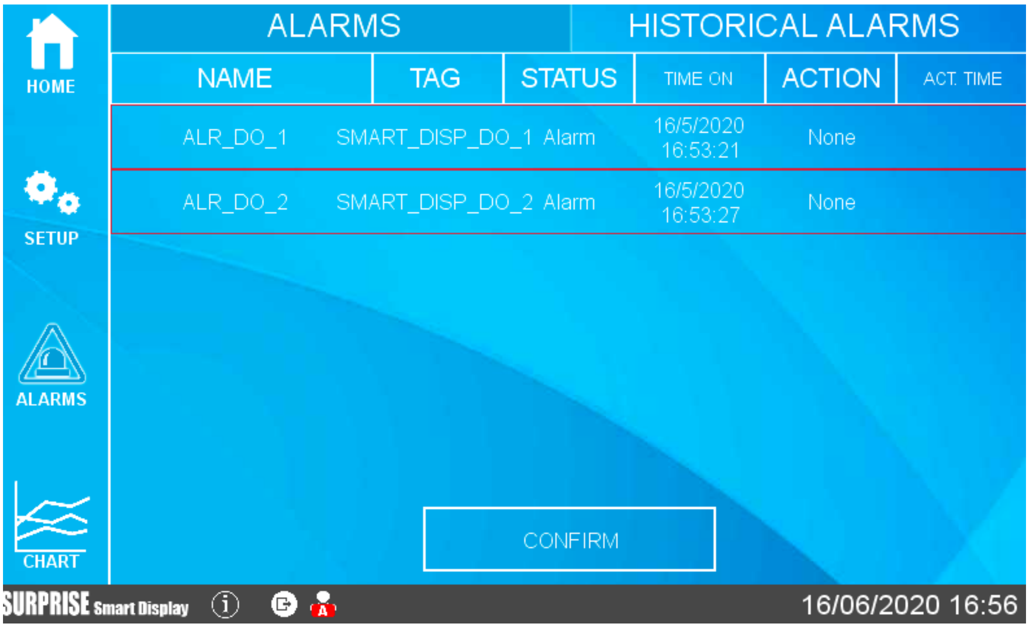
1) BUS COMMUNICATION SCAN

In this learning mode Smart Display will start to scan the flow of information passing through the bus. Typically, a Master interrogates all the devices in a continuous cycle, so when you are sure that the cycle has ended you can stop the scan. Attention: the operation to stop the scan is always manual.BUS COMMUNICATION SCAN

2) TAG CREATION

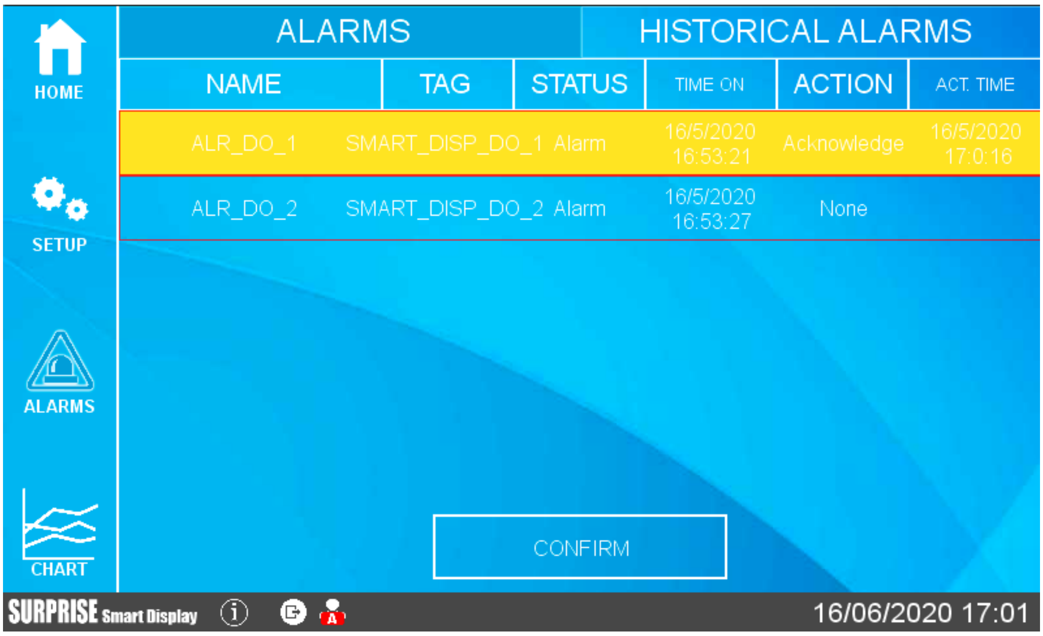
In this phase SMART DISPLAY has identified the registers that the devices are exchanging, now it is necessary to associate the name of the tag and the type of data it contains. In the case of a system with Seneca products, it will be necessary to introduce the type of Seneca device and the system will automatically associate the correct tags, in the case of third party devices, the information relating to each register identified will be requested.

3.2.2.ALARMS



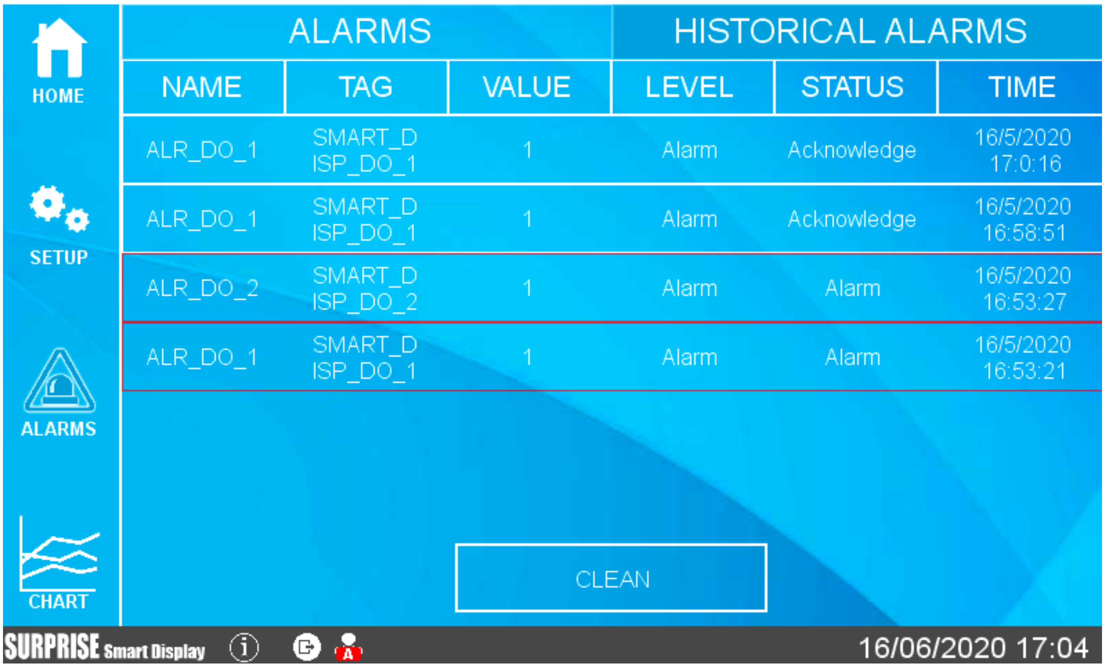
NAME	TAG	STATUS	TIME ON	ACTION	ACT. TIME
ALR_DO_1	SMART_DISP_DO_1	Alarm	16/5/2020 16:53:21	None	
ALR_DO_2	SMART_DISP_DO_2	Alarm	16/5/2020 16:53:27	None	

This section shows the active alarms and alarm history.
If the alarm requires manual acknowledgement, it is possible to use the appropriate button:



NAME	TAG	STATUS	TIME ON	ACTION	ACT. TIME
ALR_DO_1	SMART_DISP_DO_1	Alarm	16/5/2020 16:53:21	Acknowledge	16/5/2020 17:0:16
ALR_DO_2	SMART_DISP_DO_2	Alarm	16/5/2020 16:53:27	None	

In the Historical section are represented all the alarms that have occurred so far:

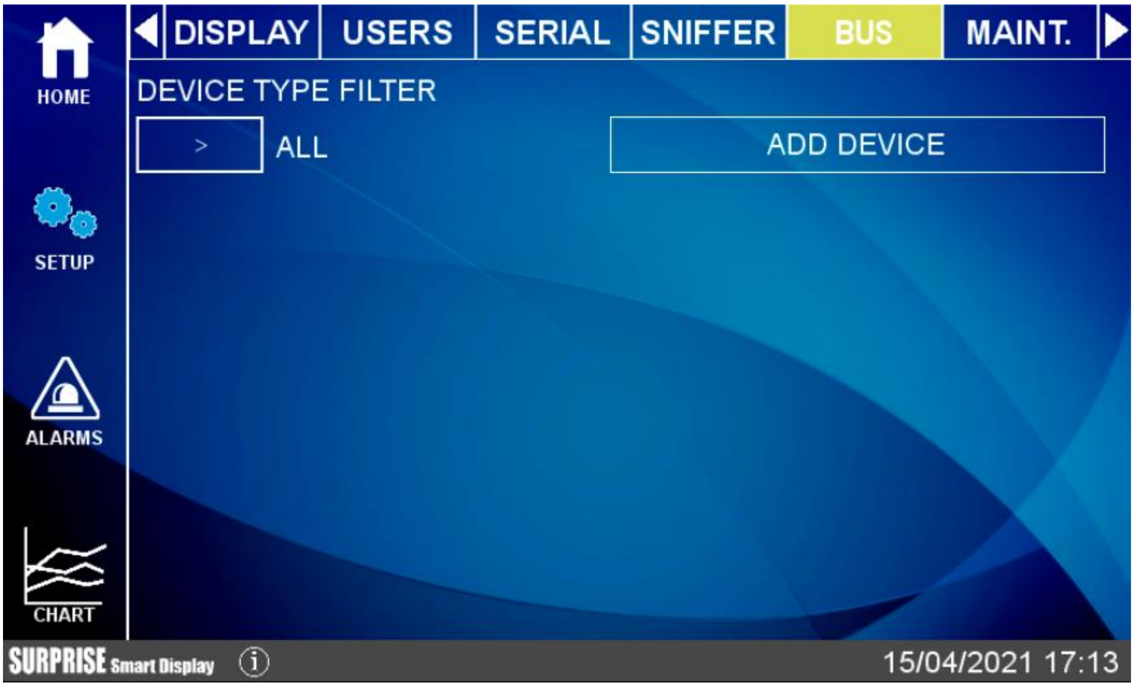


NAME	TAG	VALUE	LEVEL	STATUS	TIME
ALR_DO_1	SMART_DISP_DO_1	1	Alarm	Acknowledge	16/5/2020 17:0:16
ALR_DO_1	SMART_DISP_DO_1	1	Alarm	Acknowledge	16/5/2020 16:58:51
ALR_DO_2	SMART_DISP_DO_2	1	Alarm	Alarm	16/5/2020 16:53:27
ALR_DO_1	SMART_DISP_DO_1	1	Alarm	Alarm	16/5/2020 16:53:21

ATTENTION!
ALARMS ARE CONFIGURED IN THE APPROPRIATE SECTION OF THE WEBSERVER

3.2.3. BUS

This section allows external devices to be added via serial and/or Ethernet and their tags to be inserted:



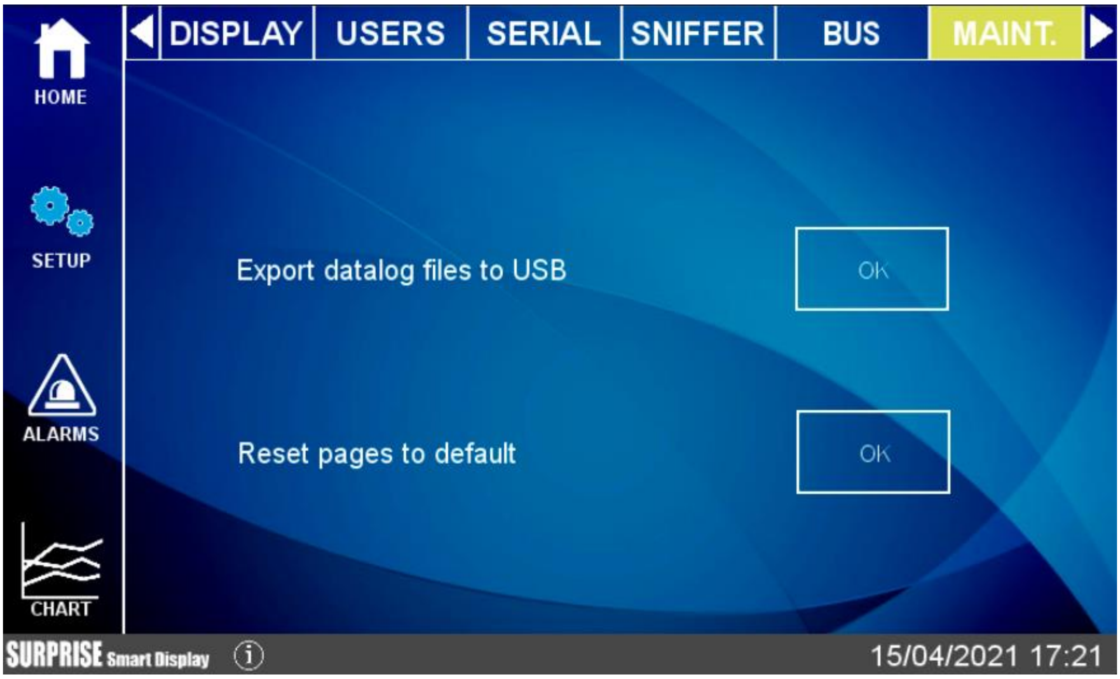
DEVICE TYPE FILTER
> ALL

The device uses a database that includes records of all Seneca devices.

Adding a device can be done in manual mode (by entering the device among those in the database or from a manufacturer other than Seneca) or by automatically searching for the device on serial or Ethernet.
The automatic search also automatically creates tags but only works with Seneca devices.

3.2.4.MAINTENANCE

The Maintenance menu allows maintenance operations to be carried out on the device:



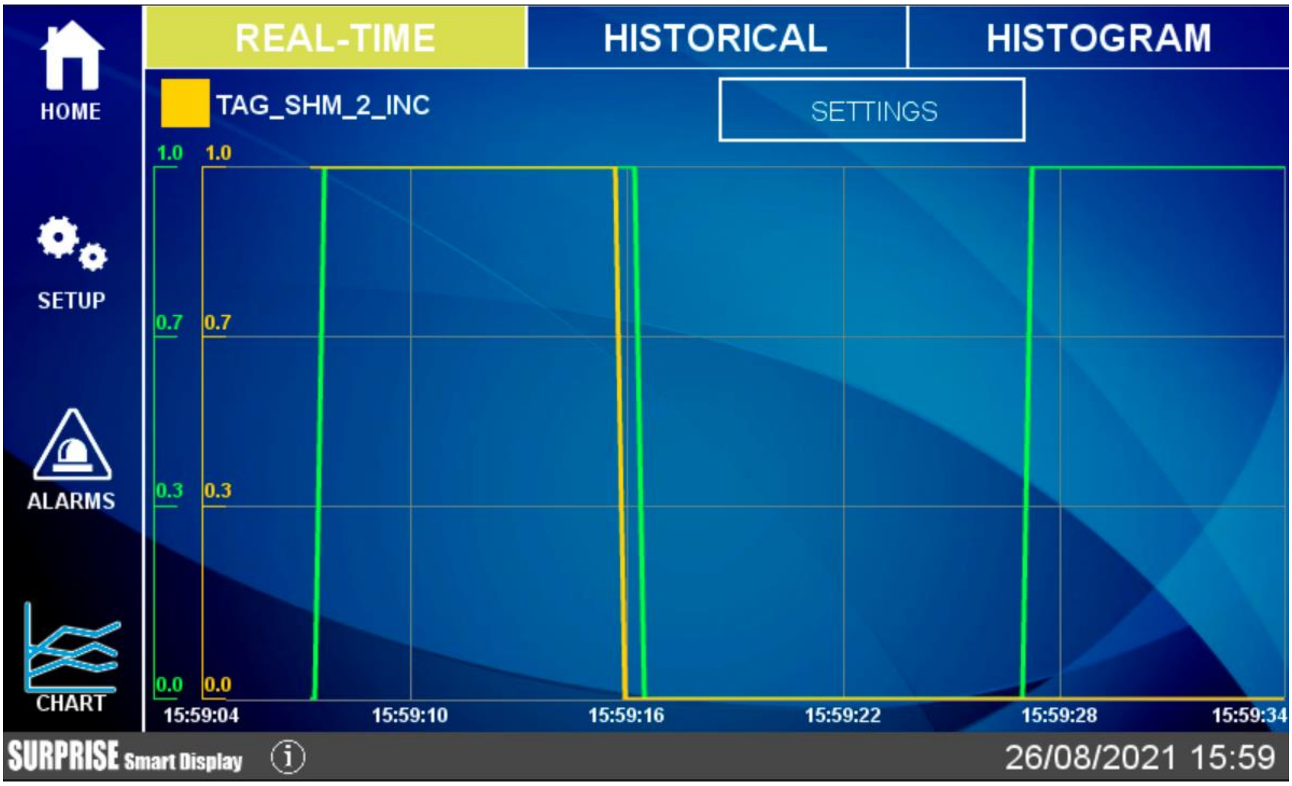
Export datalog files to USB OK

Reset pages to default OK

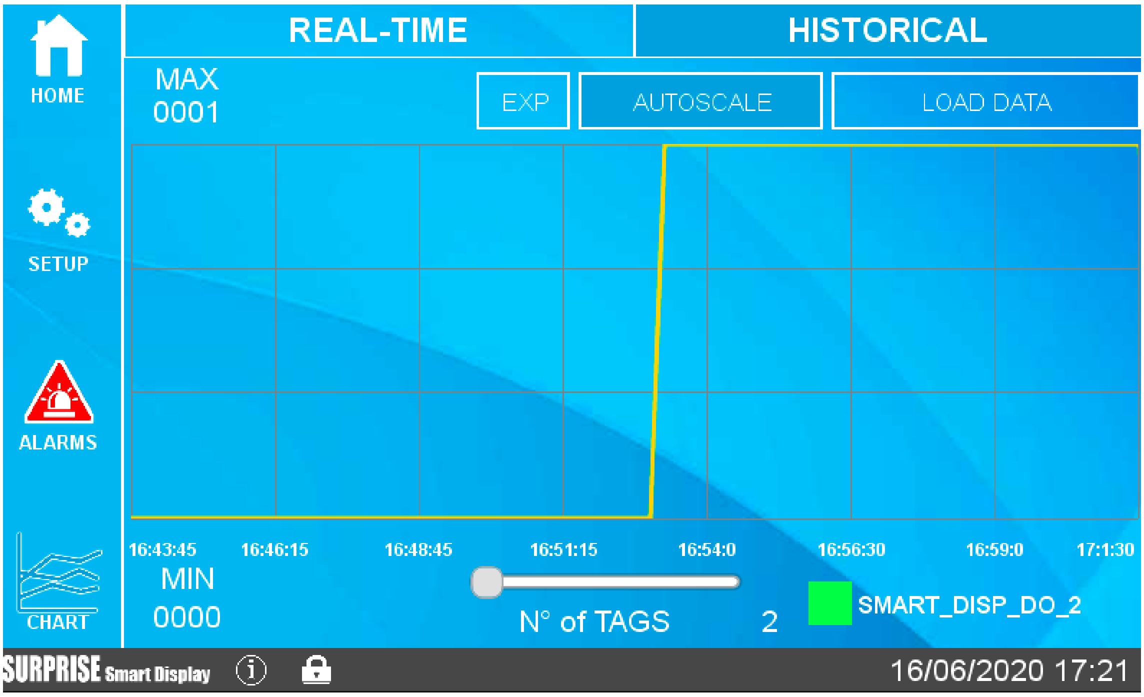
3.2.5.CHART

There are 3 types of graph available: Real Time, Historical and Histogram.

In the Chart Real Time section the tag values are displayed in real time (maximum 10 tags):



The configuration of the real time graph will be recalled also from the relative widget.
In the Historical section, on the other hand, you can load data in the desired range and move back and forth in the graph, using the touch screen.

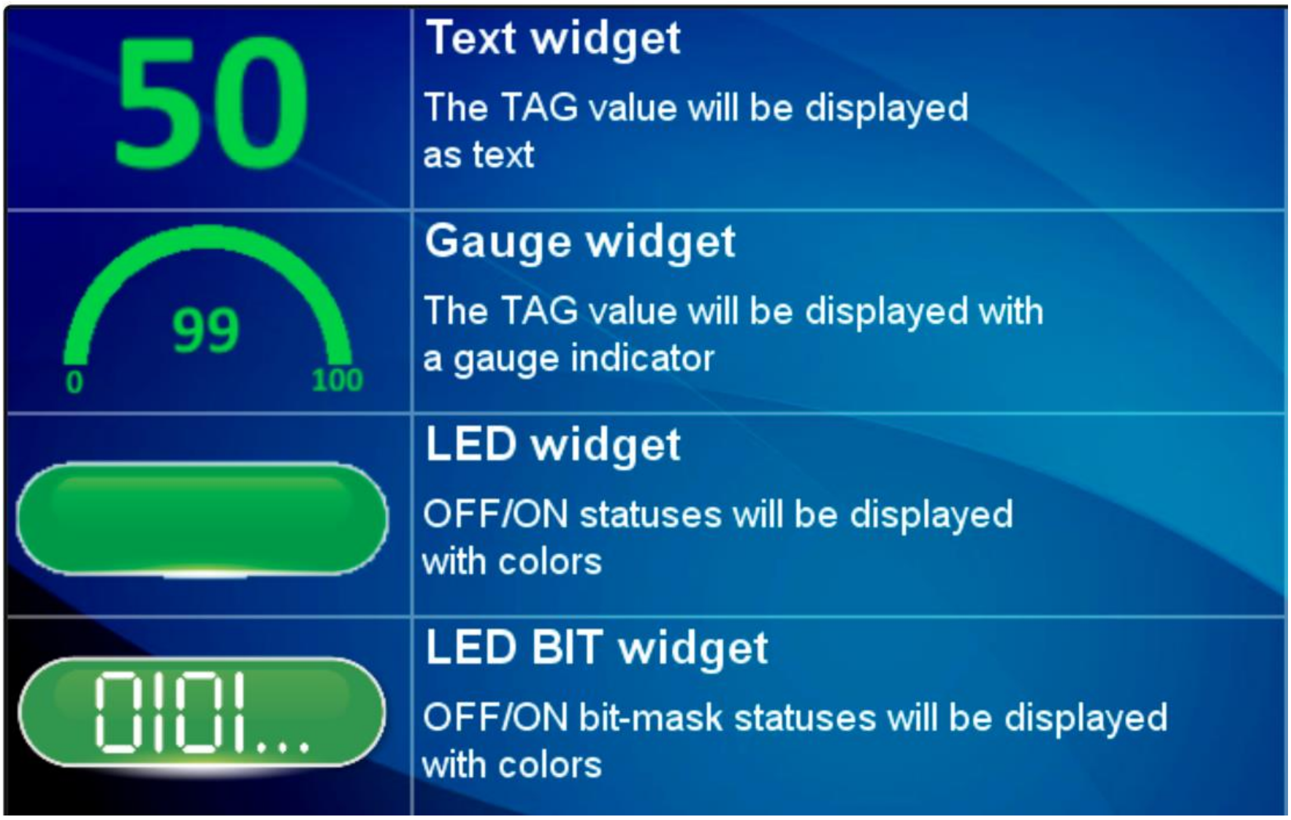


In case a USB disk is connected, it is possible to export to a file the chart values displayed, by pressing the "EXP" button.
If user is connected via web to the remote display, pressing the "EXP" button the browser will download the file directly to the PC.

The Hystogram chart is essentially the same as the Historical chart but with a histogram representation.

3.3. TYPE OF WIDGETS

Widgets are graphic elements that can be linked to one or more TAGs.
These can be used in both widget pages and synoptic pages.
There are various widgets available, here are some examples:



Text widget

The TAG value will be displayed as text

Gauge widget

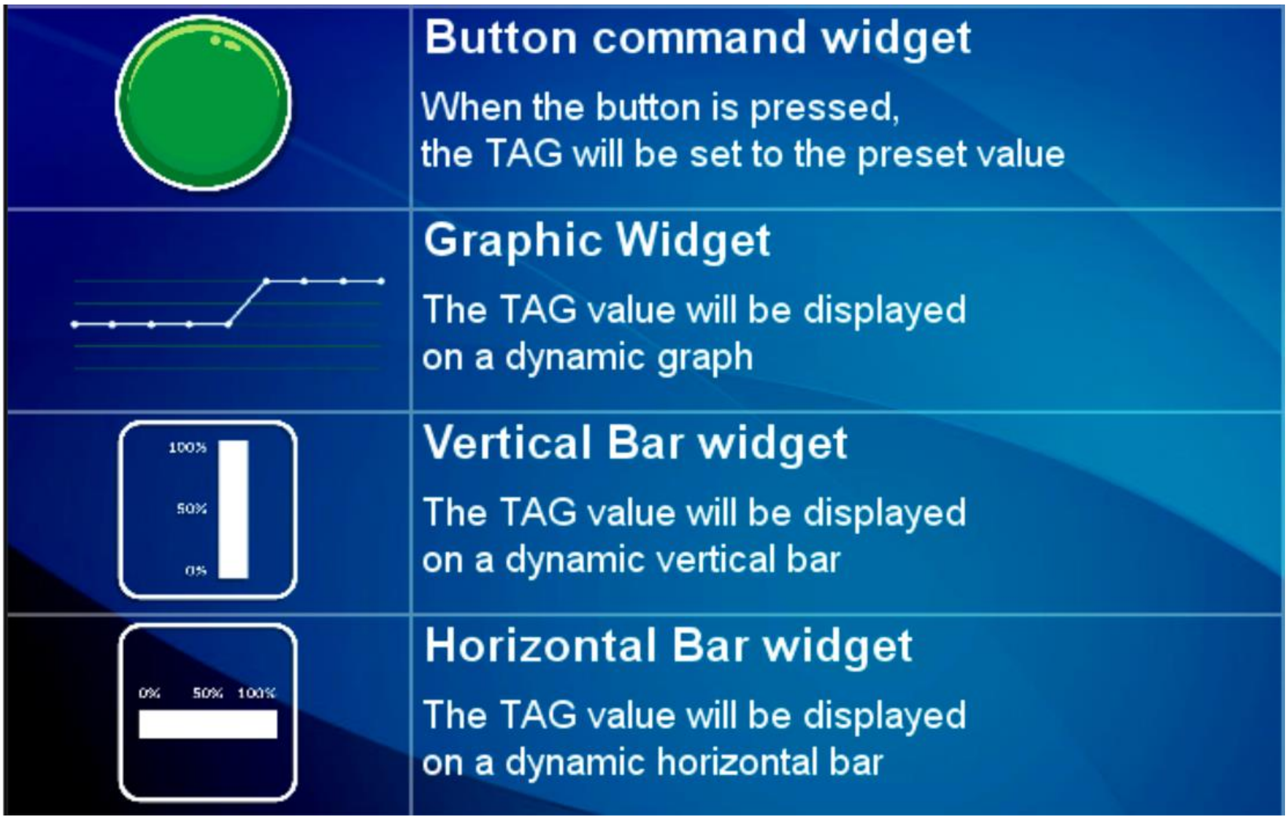
The TAG value will be displayed with a gauge indicator

LED widget

OFF/ON statuses will be displayed with colors

LED BIT widget

OFF/ON bit-mask statuses will be displayed with colors



Button command widget

When the button is pressed,
the TAG will be set to the preset value

Graphic Widget

The TAG value will be displayed
on a dynamic graph

Vertical Bar widget

The TAG value will be displayed
on a dynamic vertical bar

Horizontal Bar widget

The TAG value will be displayed
on a dynamic horizontal bar

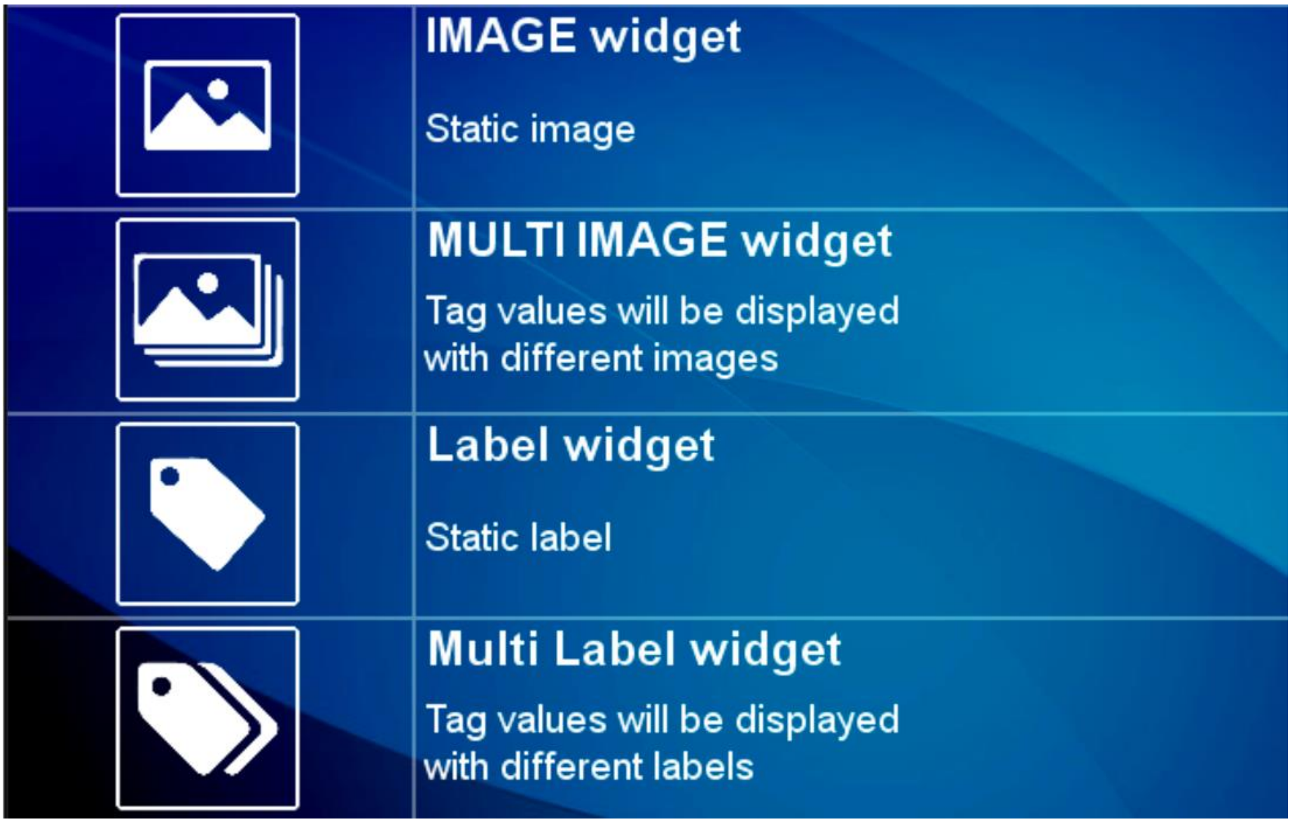


IMAGE widget

Static image

MULTI IMAGE widget

Tag values will be displayed
with different images

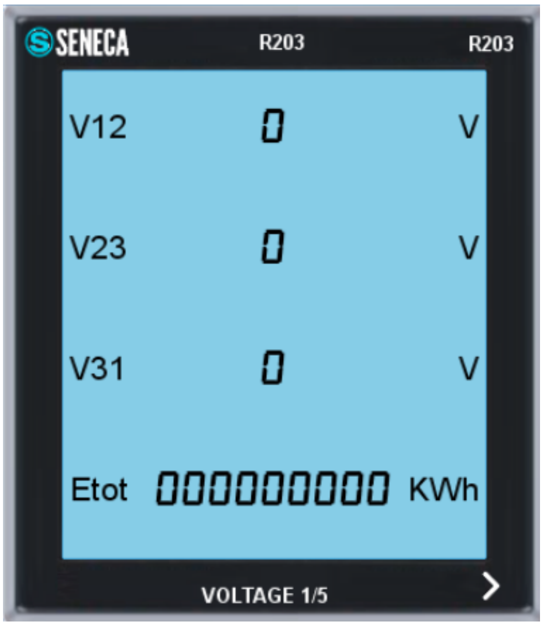
Label widget

Static label

Multi Label widget

Tag values will be displayed
with different labels

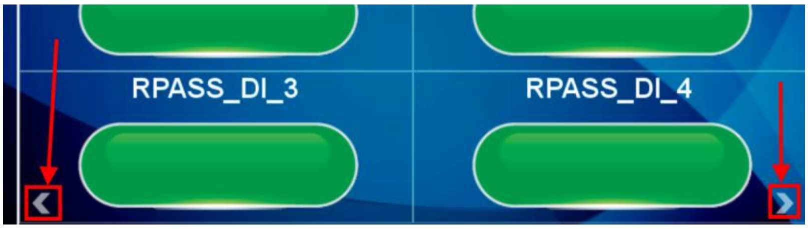
Grafico macro widget (display virtuale):



This is a virtual display, scroll through the pages of the virtual display by pressing the ">" arrow at the bottom right.
It is possible to place up to 2 virtual displays for each widget page.

3.3.1.PAGE CHANGE

To scroll from a page to the next, simply slide the finger to the left (this operation is called "swipe") as along the pages of a book;
similarly, to return to the previous page, simply slide the finger to the right.
To change the page it is also possible to press a "forward" arrow and a "back" arrow:



3.4. TYPE OF WIDGET PAGE

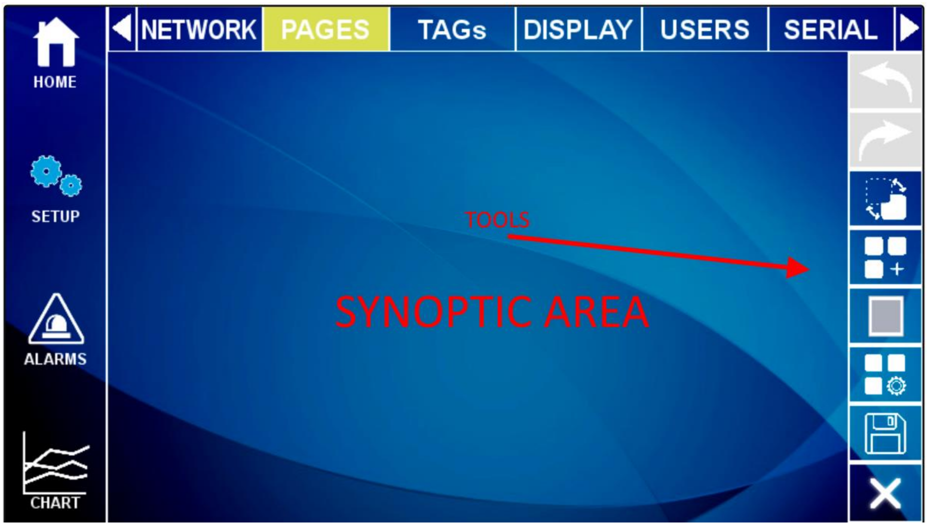
It represents the widgets page, in this section the widgets linked to the configured tags will appear. You can choose from the various grids available, the widgets will be automatically positioned within the grid.
Each widget graphically represents the value of one or more TAGs.

3.5. SYNOPTIC PAGE TYPE

In a synoptic type page it is possible to freely move the widgets by adding graphics and also create animated synoptic ones.

Synoptic type pages can be freely mixed with widget type pages.

To create a synoptic page Select Pages and press the "Add Synoptic Page" button.
At this point a new page will open with tools on the left:



Here is the meaning of the tool icons:

UNDO
Cancels the last operation performed

REDO
Repeats the last operation cancelled by the UNDO

BACKGROUND
Allows you to choose a graphic file to use as the background of the page

ADD WIDGET
Adds a widget to the page

ADD VIRTUAL DISPLAY WIDGET
Adds a virtual display widget

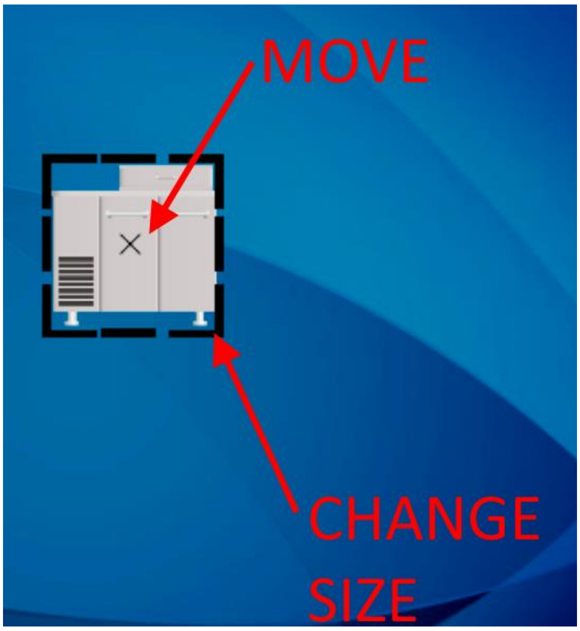
WIDGET CONFIGURATOR
Allows the widget configuration

SAVE PAGE
Saves the page changes

EXIT
Exits the page

3.5.1.“ADD WIDGET” TOOL

The "ADD WIDGET” button allows the addition of a widget on the page, once the widget has been inserted it is possible to move it by touching the widget in the central cross. To change the size of the widget, move the sides of the rectangle containing the widget:



When a widget is selected, a new series of tools appears on the right, the meaning of which is as follows:

GRID

A grid is activated, moving the widgets they will follow the set grid.

ALIGN

The widget is aligned

CONFIG

Modification of the configuration parameters of the selected widget is allowed and viewed

DELETE

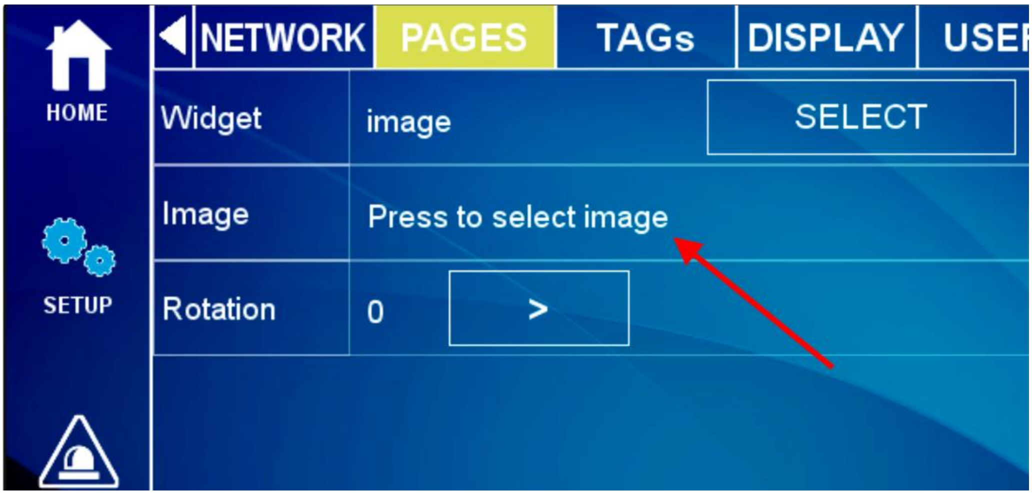
The Widget is removed from the page

EXIT

You return to the initial page of the synoptic

3.5.2. DATABASE OF SYMBOLS FOR THE SYNOPTIC PAGES

Inside the device is a database of graphic symbols that can be used in widgets.
The symbols are divided into categories. To access the symbols, select, for example, the "Image" widget:

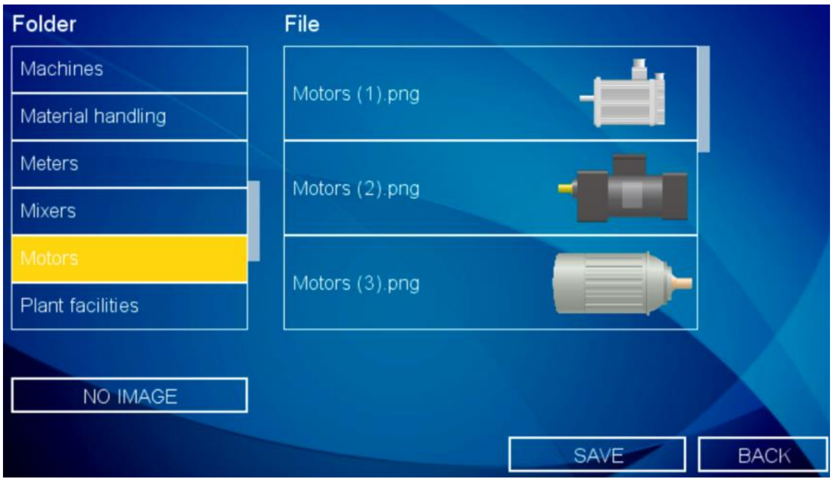


Widget image

Image Press to select image

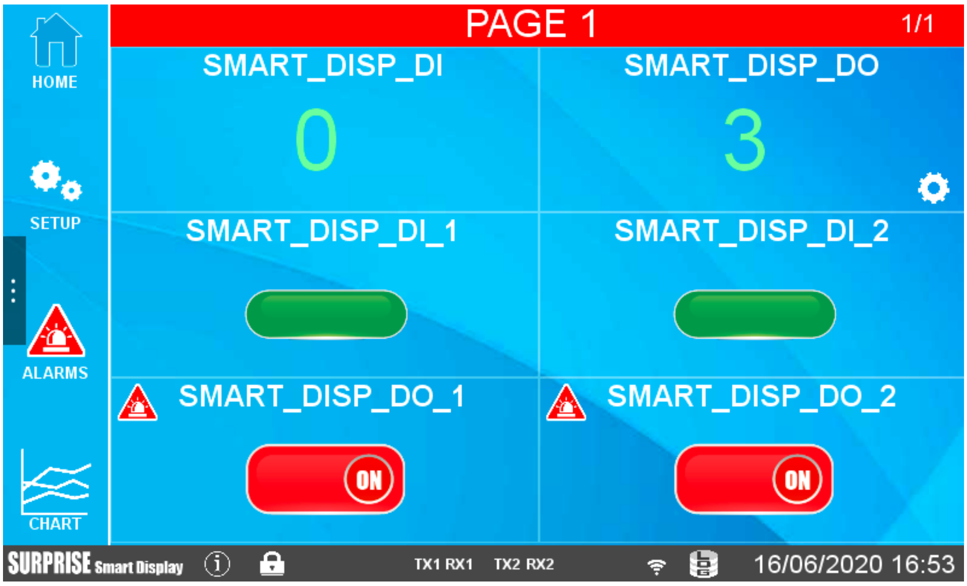
Rotation 0

For example, selecting the "Motors" category displays the graphic files relating to engines:



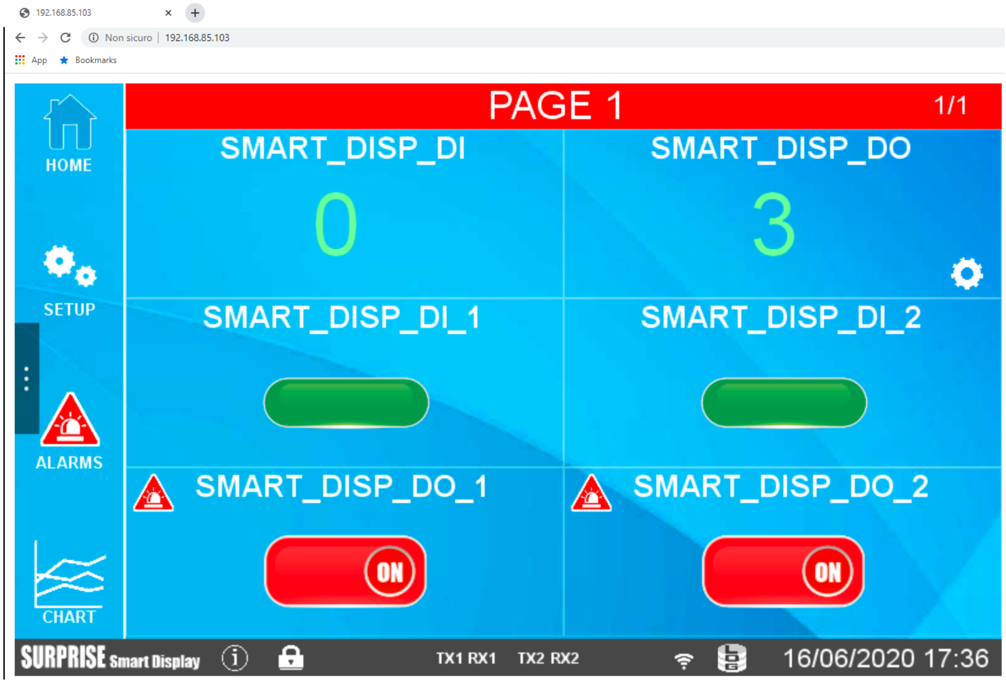
3.6. ALARMS

When an alarm occurs on at least one TAG, the title of the page is outlined in red and the faulty tags display the alarm icon, see the figure:



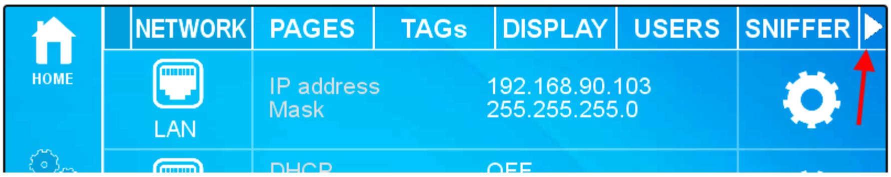
3.7. REMOTE DISPLAY

All the operations that can be done on the local display can also be done remotely by connecting to the device web page via a web browser via port 80 (default).
To connect to the remote display, enter the device's IP address into a browser on a PC or smart device:



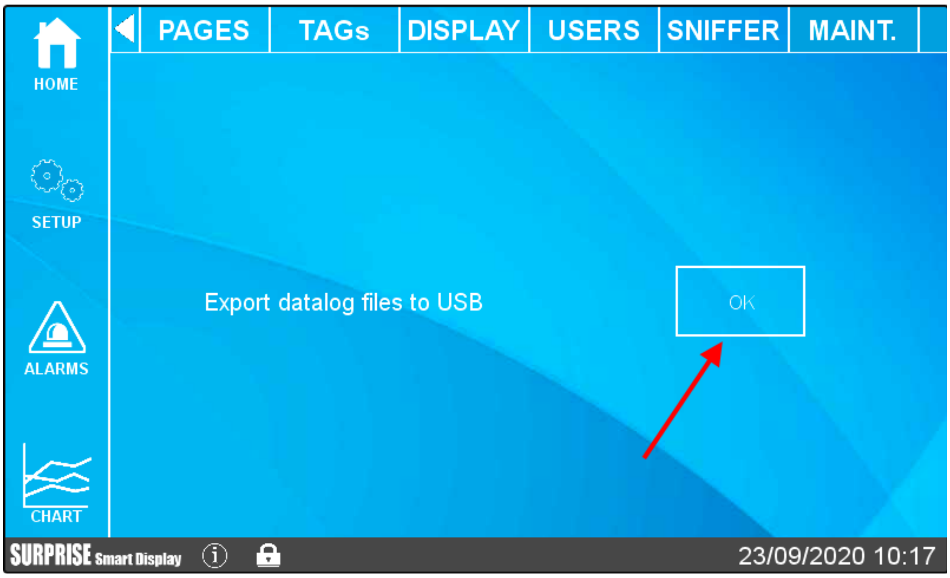
3.8. DOWNLOADING LOG FILES TO USB FLASH DRIVE

By inserting a USB stick in the HOST port it is possible to carry out a complete download of the files acquired by the datalogger.
To carry out this operation it is necessary to reach the "Maintenance" menu by tapping "SETUP" and then the arrow that extends the menu:



IP address 192.168.90.103
Mask 255.255.255.0
DHCP OFF

Now select "MAINT." and then press the relevant button to perform the operation:



Export datalog files to USB

At this point the system will download all the files acquired by the datalogger.
In the root of the USB stick there will then be many folders (one per day of recording) with the files related to that day (divided in turn into folders representing the active log groups). This functionality is also active via Webserver in the "TAG VIEW" section.

4. FIRMWARE UPDATE

The firmware can be updated from the web page (FW UPDATE section) or with a USB stick formatted with the FAT32 file system.

4.1. FW UPDATE FROM USB FLASH DRIVE

For updating fw from USB port, the procedure is as follows:

Download the FW file from the Seneca website

the downloaded file is a .zip file; extract the .bin file; the FW file must be of the following type:

SW00xxxx_xxx.bin

1) Copy this file to the root of the USB pen
2) Turn off the device
3) Insert the USB pen into the USB port
4) Turn on the device

the update procedure will take a few minutes to complete; during this time, the device MUST NOT be turned off and will be restarted several times automatically.

5. IP ADDRESSES

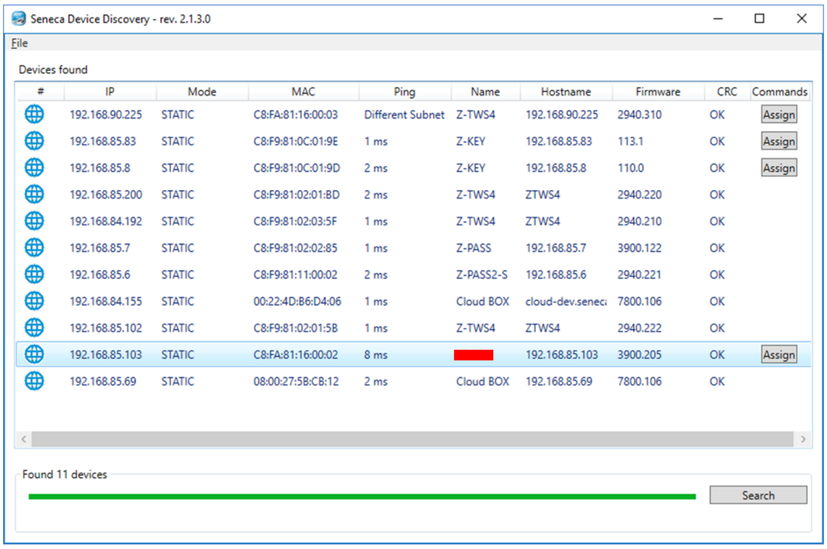
5.1. FACTORY IP ADDRESSES

The devices leave the factory with the following configuration:

ETHERNET LAN PORT	static IP: 192.168.90.101
ETHERNET WAN PORT	DHCP active
WI-FI	inactive

5.2. IP ADDRESS SEARCH

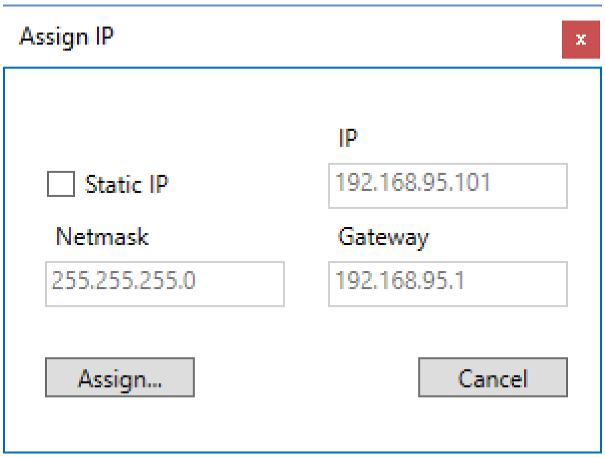
The devices leave the factory with the default IP address 192.168.90.101, on Ethernet (LAN).
If this address is changed or forgotten, it can be recovered using the "Seneca Device Discovery" software.



#	IP	Mode	MAC	Ping	Name	Hostname	Firmware	CRC	Commands
🌐	192.168.90.225	STATIC	C8:FA:81:16:00:03	Different Subnet	Z-TWS4	192.168.90.225	2940.310	OK	Assign
🌐	192.168.85.83	STATIC	C8:F9:81:0C:01:9E	1 ms	Z-KEY	192.168.85.83	113.1	OK	Assign
🌐	192.168.85.8	STATIC	C8:F9:81:0C:01:9D	2 ms	Z-KEY	192.168.85.8	110.0	OK	Assign
🌐	192.168.85.200	STATIC	C8:F9:81:02:01:BD	2 ms	Z-TWS4	ZTWS4	2940.220	OK	
🌐	192.168.84.192	STATIC	C8:F9:81:02:03:5F	1 ms	Z-TWS4	ZTWS4	2940.210	OK	
🌐	192.168.85.7	STATIC	C8:F9:81:02:02:85	1 ms	Z-PASS	192.168.85.7	3900.122	OK	
🌐	192.168.85.6	STATIC	C8:F9:81:11:00:02	2 ms	Z-PASS2-S	192.168.85.6	2940.221	OK	
🌐	192.168.84.155	STATIC	00:22:4D:B6:D4:06	1 ms	Cloud BOX	cloud-dev.seneca	7800.106	OK	
🌐	192.168.85.102	STATIC	C8:F9:81:02:01:5B	1 ms	Z-TWS4	ZTWS4	2940.222	OK	
🌐	192.168.85.103	STATIC	C8:FA:81:16:00:02	8 ms	[redacted]	192.168.85.103	3900.205	OK	Assign
🌐	192.168.85.69	STATIC	08:00:27:5B:CB:12	2 ms	Cloud BOX	192.168.85.69	7800.106	OK	

This application shows the IP address, MAC address, FW version and some other useful information, for each SENECA device connected to PC.

Moreover, by clicking on the "Assign" button, it is possible modify the device network parameters, as shown in the following figure:



Assign IP

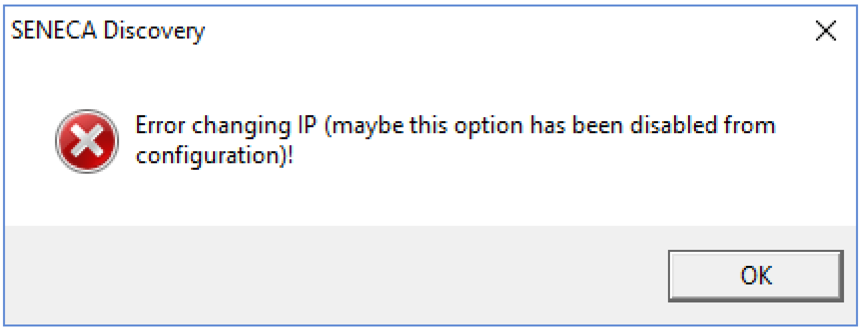
☐ Static IP

IP: 192.168.95.101

Netmask: 255.255.255.0

Gateway: 192.168.95.1

For security reasons, this function can be disabled, in this case, after clicking on the "Assign" button the following error message will be visualized



SENECA Discovery

Error changing IP (maybe this option has been disabled from configuration)!

The SDD software can be easily installed by running the installation program available at the following link: http://www.seneca.it/products/sdd

NOTE:

The IP address shown by the SDD is the IP address of the LAN port when the PC is connected to the LAN port, the WAN IP address when the PC is connected to the WAN port and the WI- FI if it is connected to the latter; moreover, all the changes of device network parameters are applied to the relative port.

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

The device can be configured to operate as a Gateway Modbus from Ethernet to Serial.

In this working mode, Modbus TCP Requests received from Ethermet interfaces are converted into Modbus RTU requests and sent to the serial interface; in the same way, Modbus RTU replies received from the serial interface are converted into Modbus TCP replies and sent back to the source network interface.

A Modbus Ethernet to Serial Gateway request can be activated for each of the three available serial ports: each can receive Modbus TCP requests.

Another possible configuration is to perform the Gateway Modbus Ethernet to Serial conversion on multiple serials at the same time.

In this mode Modbus Gateway can support up to 32 simultaneous Modbus TCP connections. These connections can also be established through a VPN tunnel.

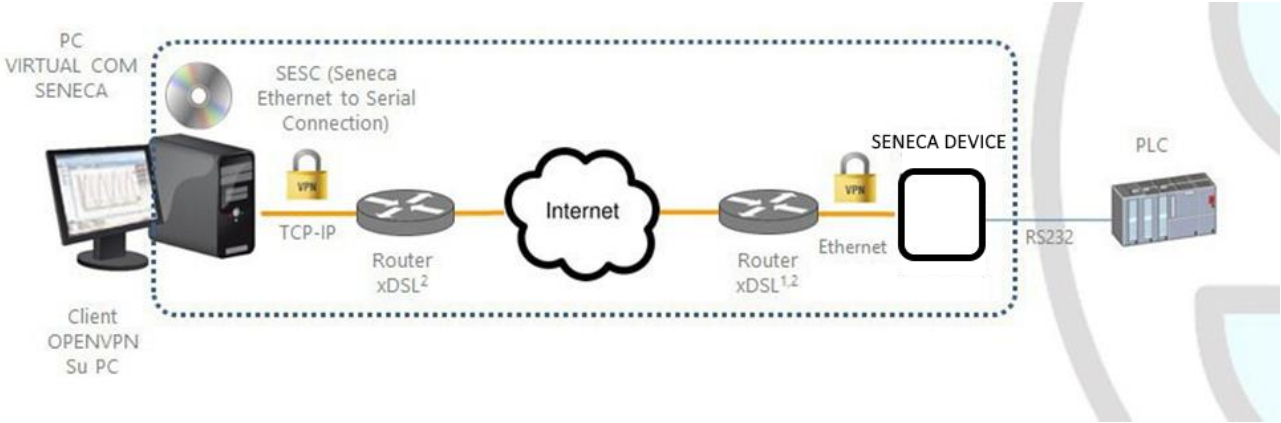
7. GATEWAY ETHERNET TO TRANSPARENT SERIAL (R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

As an alternative to Modbus Ethernet to Serial Gateway, the device can be configured to operate as a "Transparent Gateway". The big difference between these two working modes is that while Ethernet to Serial works only with the Modbus protocol, Transparent Gateway can be applied to extend (transport) any serial communication (regardless of RS232/RS85 protocol) through the TCP/IP stack.

- Virtual COM (with RFC 2217 support)
- Point-to-point serial tunnel on TCP
- Point-to-point serial tunnel on UDP
- Point-to-multipoint serial tunnel on UDP

Each mode will be fully described in the following paragraphs.

7.1. VIRTUAL COM PORT WITH RFC 2217



The Virtual COM functionality allows a PC application, which transmits data only on a serial line, to communicate with a remote serial device, using Ethernet/Internet; in other words, through the Seneca device, a PC and a serial device, located in distant sites, can communicate as they are directly connected.

In this mode, data sent over the LAN or WAN are received by the Seneca device and sent to the serial port; the response packets follow the reverse path.

RFC 2217 defines some features that allow to PC to set the properties (baud rate, data bits, stop bits and parity) of the serial port of the Seneca device remotely; so, when Virtual COM operating mode is selected for a port, the port is reconfigured independently from the previous settings and the values configured in the Seneca device are overwritten.

For the Virtual COM to work, a utility called "Seneca Ethernet to Serial Connection" must be installed on the PC. The TCP connection can be established through a VPN tunnel, as shown above.

Once the connection is established, a program using the virtual COM port will transmit the data to the serial port of the device; for example, Modbus RTU requests sent by a Modbus Master program will reach the Modbus slave devices connected to the RS485 bus of COM2.

Particular attention must be paid to the "Data Packing Interval" parameter, which can be set when the Virtual COM operating mode is selected: this parameter allows you to define the time interval, in milliseconds, used by the Seneca device as a criterion for packing the bytes of data received from the serial port before sending them to the network; in other words, when the Seneca device does not receive any more bytes from the serial port for the given time interval, it packs the received bytes and sends them over the established TCP connection; the optimal value to set for this parameter depends on the protocol that is transparently routed from the TCP/IP network to the serial line and vice versa.

ATTENTION!

In Virtual COM operating mode only one serial port can be used

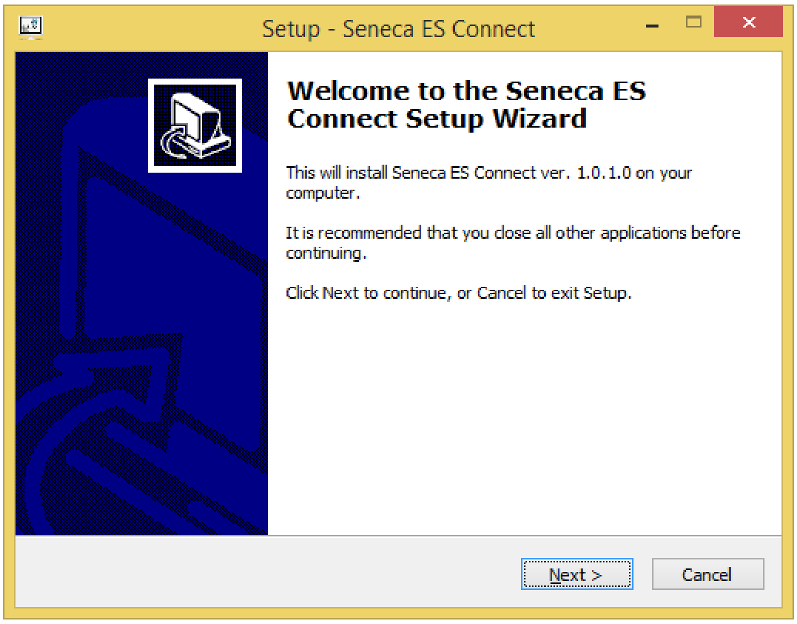
7.2. SENECA ETHERNET TO SERIAL CONNECT

The following guide refers to version 1 of Seneca Ethernet to Serial Connection, subsequent versions are similar.

7.2.1.INSTALLING THE SENECA SERIAL TO ETHERNET DRIVER

Seneca Ethernet to Serial Connect is compatible with 32 and 64 bit Windows systems.

Double-click on the installer



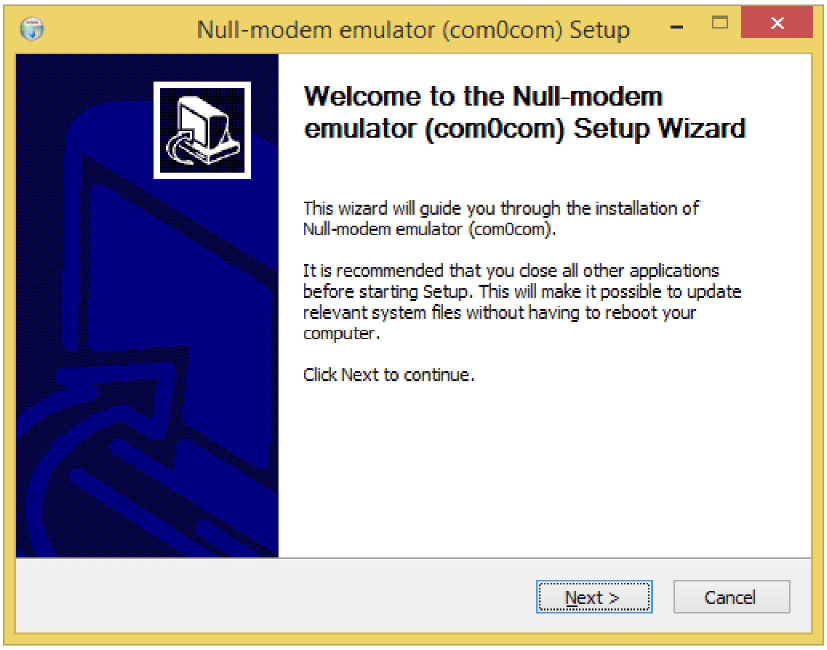
Welcome to the Seneca ES Connect Setup Wizard

This will install Seneca ES Connect ver. 1.0.1.0 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Then the com0com driver will be installed:



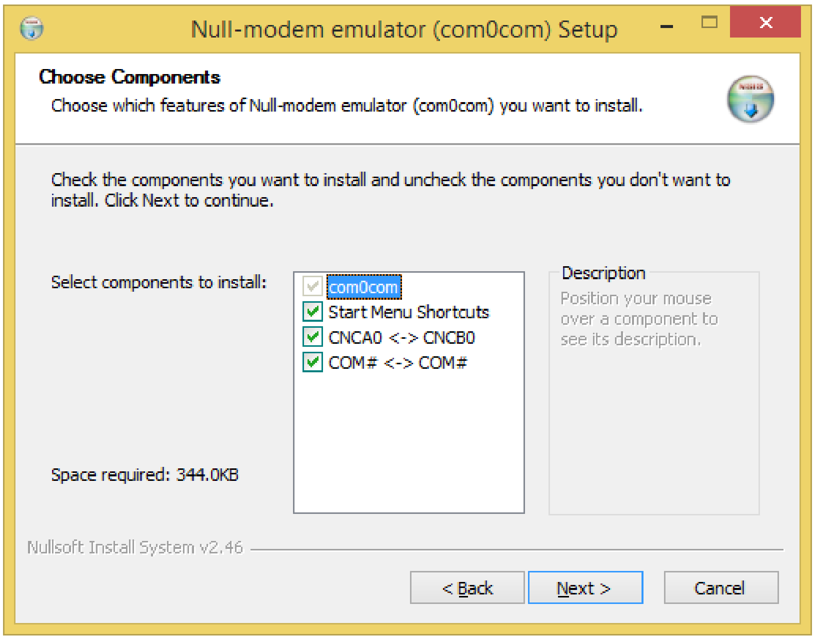
Welcome to the Null-modem emulator (com0com) Setup Wizard

This wizard will guide you through the installation of Null-modem emulator (com0com).

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Select the virtual port names CNCA0<->CNCB0 and COM#<->COM#:



Null-modem emulator (com0com) Setup

Choose Components

Choose which features of Null-modem emulator (com0com) you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ com0com
- ☑ Start Menu Shortcuts
- ☑ CNCA0 <-> CNCB0
- ☑ COM# <-> COM#

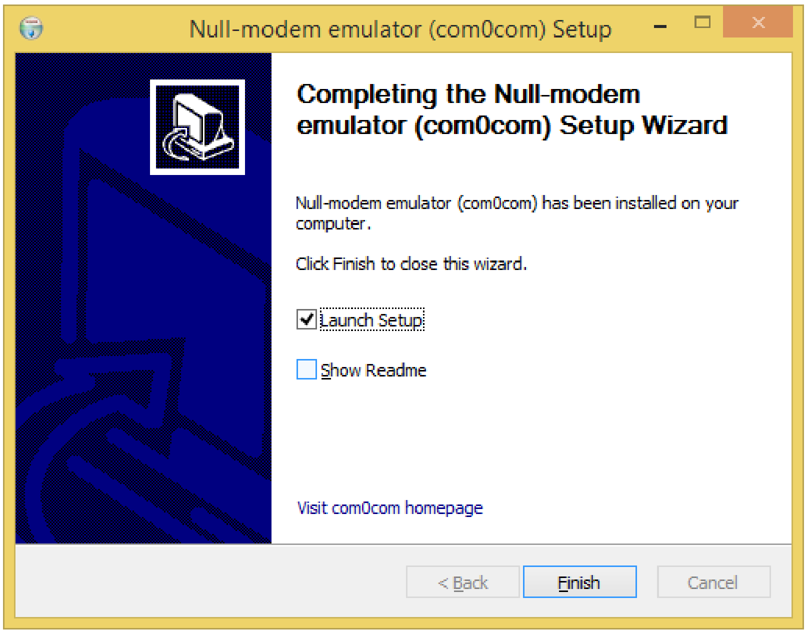
Description

Position your mouse over a component to see its description.

Space required: 344.0KB

Nullsoft Install System v2.46

Now click on "Start Setup":



Null-modem emulator (com0com) Setup

Completing the Null-modem emulator (com0com) Setup Wizard

Null-modem emulator (com0com) has been installed on your computer.

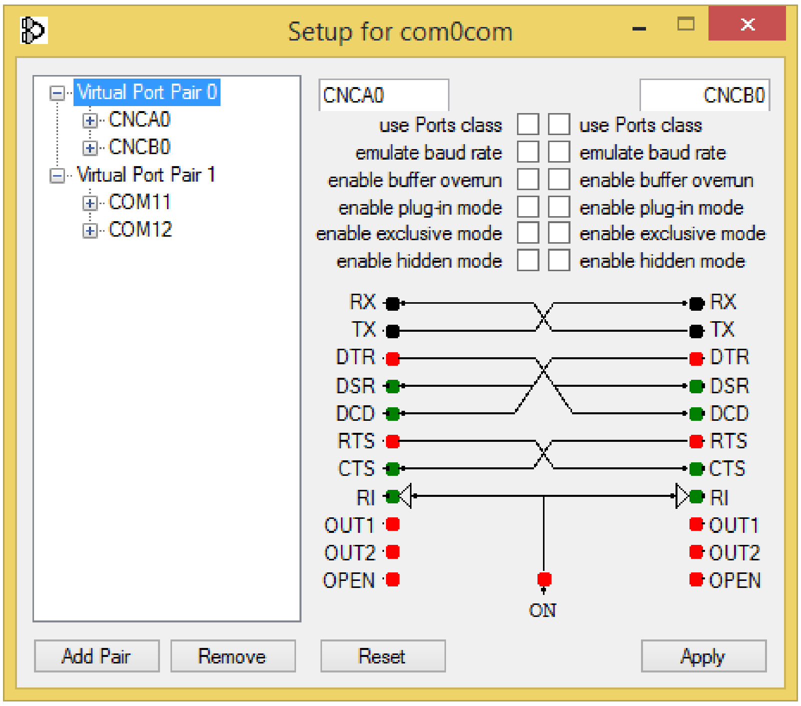
Click Finish to close this wizard.

☑ Launch Setup

□ Show Readme

Visit com0com homepage

Press Finish, the com0com setup will open:



Setup for com0com

- Virtual Port Pair 0
  - CNCA0
  - CNCB0
- Virtual Port Pair 1
  - COM11
  - COM12

CNCA0			CNCB0
use Ports class	□	□	use Ports class
emulate baud rate	□	□	emulate baud rate
enable buffer overrun	□	□	enable buffer overrun
enable plug-in mode	□	□	enable plug-in mode
enable exclusive mode	□	□	enable exclusive mode
enable hidden mode	□	□	enable hidden mode

During installation two pairs of virtual COM are created:
CNCA0, CNCB0
and also:

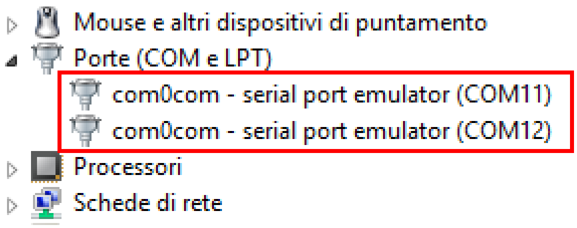
COM11, COM12 (note that com# may be different in your system).

The first pair can be used in software that supports CNCA names, the other in software that only supports Port Classes.

If you need to add more virtual ports, press the "Add Pair" button, then select whether or not you need a Class port.

Confirm the driver installation with "Apply".

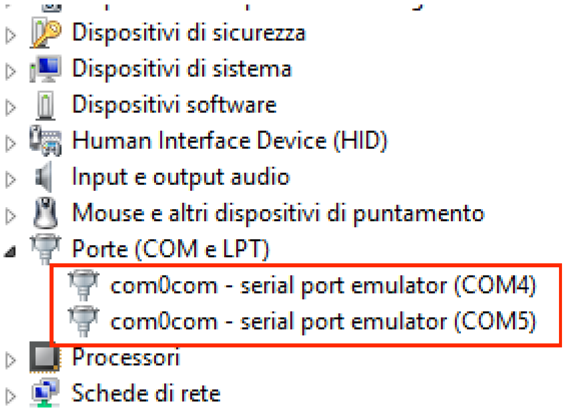
The pair of serial port emulators COM11-COM12 will be available in Device Manger



- Mouse e altri dispositivi di puntamento
- Porte (COM e LPT)
  - com0com - serial port emulator (COM11)
  - com0com - serial port emulator (COM12)
- Processori
- Schede di rete

7.2.2. COM PORT SELECTION FOR SENECA ETHERNET TO SERIAL TO CONNECT

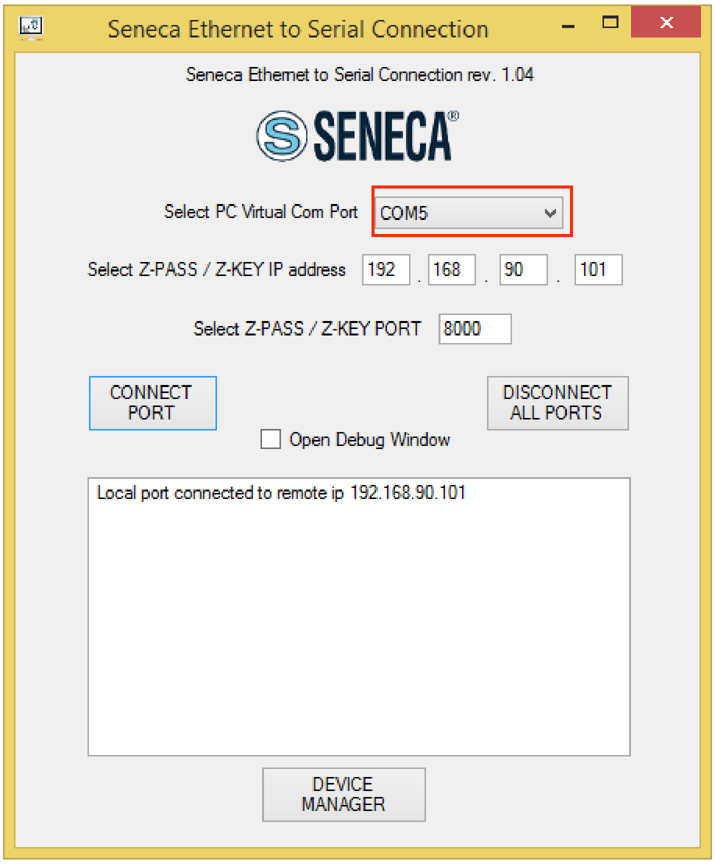
The driver installation will use the first 2 serial ports that are free (in our case the driver has created the pair COM4 and COM5):



- Dispositivi di sicurezza
- Dispositivi di sistema
- Dispositivi software
- Human Interface Device (HID)
- Input e output audio
- Mouse e altri dispositivi di puntamento
- Porte (COM e LPT)
  - com0com - serial port emulator (COM4)
  - com0com - serial port emulator (COM5)
- Processori
- Schede di rete

The SESC interface visualize only com0com ports and it will only use one port

Select COM5 in the Seneca ES connector:



Seneca Ethernet to Serial Connection

Seneca Ethernet to Serial Connection rev. 1.04

Select PC Virtual Com Port: COM5

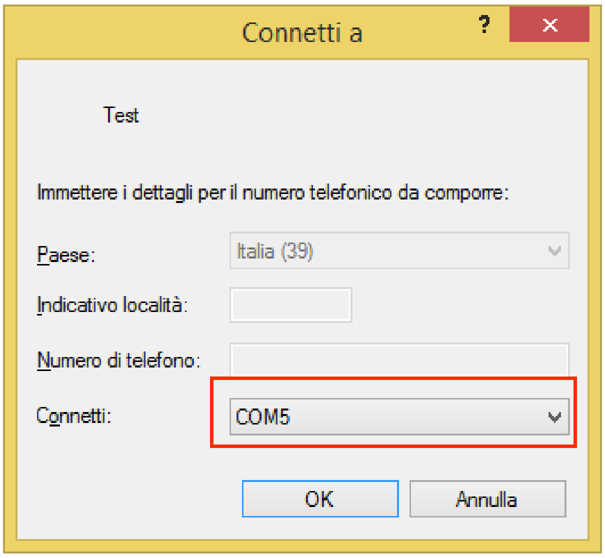
Select Z-PASS / Z-KEY IP address: 192 . 168 . 90 . 101

Select Z-PASS / Z-KEY PORT: 8000

□ Open Debug Window

Local port connected to remote ip 192.168.90.101

Now use the same COM port on application to use (e.g. in the terminal software)



Connetti a

Test

Immettere i dettagli per il numero telefonico da comporre:

Paese: Italia (39)

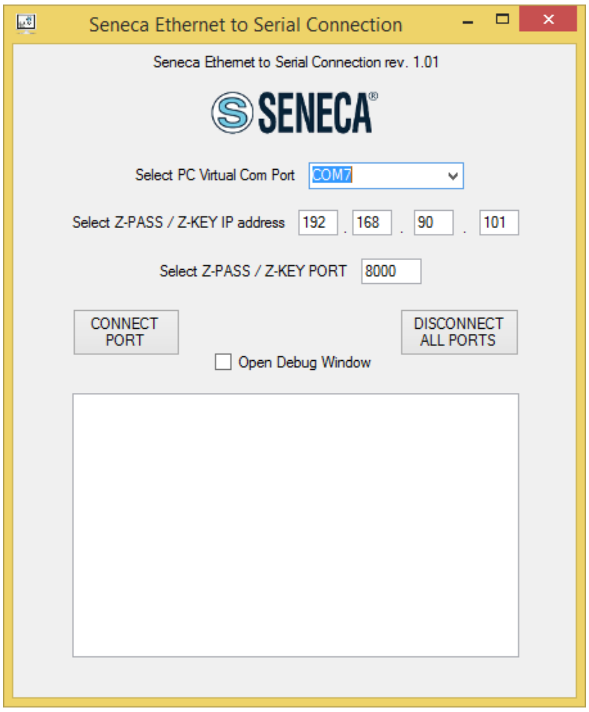
Indicativo località:

Numero di telefono:

Connetti: COM5

COM5 is now connected to the Seneca device by a TCP connection to port 8000.

7.2.3. SENECA SERIAL TO ETHERNET CONFIGURATION



Seneca Ethernet to Serial Connection

Seneca Ethernet to Serial Connection rev. 1.01

Select PC Virtual Com Port COM7

Select Z-PASS / Z-KEY IP address 192 . 168 . 90 . 101

Select Z-PASS / Z-KEY PORT 8000

- Select the virtual COM port
- Select the IP address of the Seneca device
- Select TCP-IP port

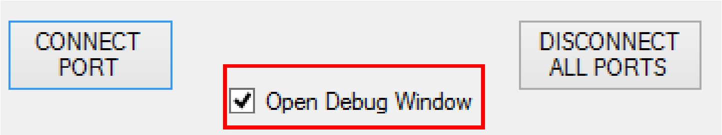
Click on "CONNECT PORT".

If it is necessary to connect another serial com to another Seneca device, configure the new com port and the new IP address, then press the "CONNECT PORT" button.

To disconnect all ports, click on "DISCONNECT ALL PORTS".

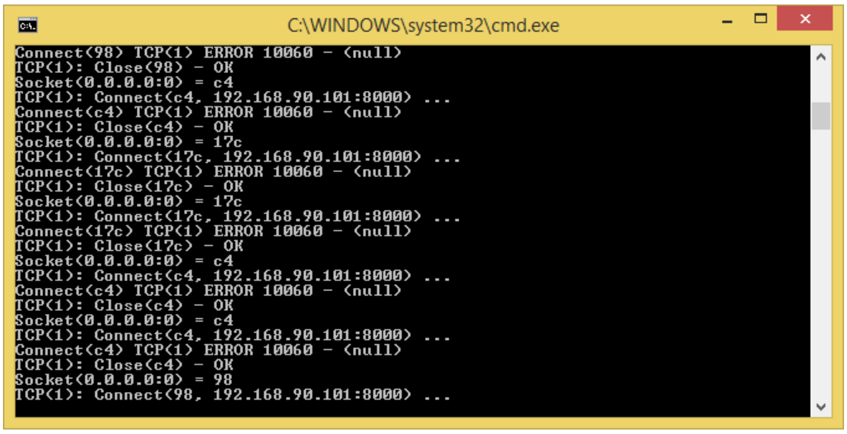
7.2.4. DEBUGGING THE CONNECTION

Before clicking on "CONNECT PORT", you can choose to open a debug window to check the connection



Then click on "CONNECT PORT".

If you see "Connect Error" as in the following image:



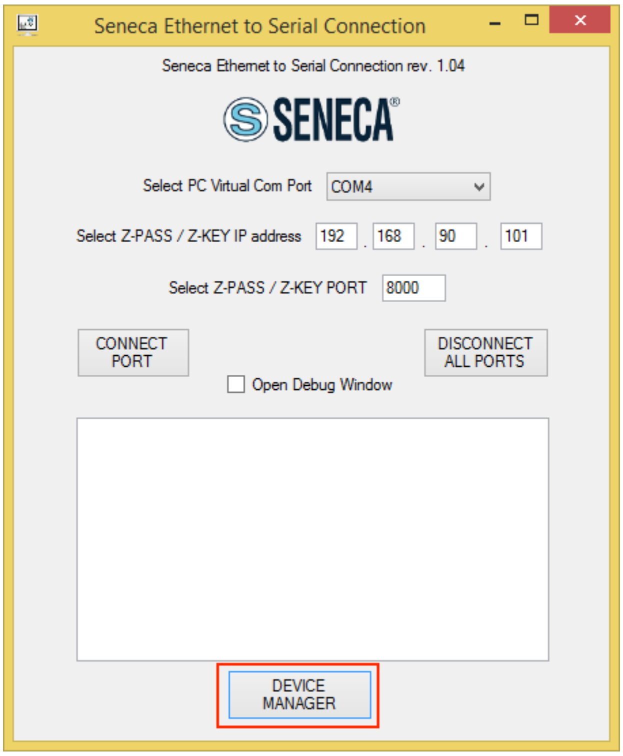
```
Connect(98) TCP(1) ERROR 10060 - (null)
TCP(1): Close(98) - OK
Socket(0.0.0.0:0) = c4
TCP(1): Connect(c4, 192.168.90.101:8000) ...
Connect(c4) TCP(1) ERROR 10060 - (null)
TCP(1): Close(c4) - OK
Socket(0.0.0.0:0) = 17c
TCP(1): Connect(17c, 192.168.90.101:8000) ...
Connect(17c) TCP(1) ERROR 10060 - (null)
TCP(1): Close(17c) - OK
Socket(0.0.0.0:0) = 17c
TCP(1): Connect(17c, 192.168.90.101:8000) ...
Connect(17c) TCP(1) ERROR 10060 - (null)
TCP(1): Close(17c) - OK
Socket(0.0.0.0:0) = c4
TCP(1): Connect(c4, 192.168.90.101:8000) ...
Connect(c4) TCP(1) ERROR 10060 - (null)
TCP(1): Close(c4) - OK
Socket(0.0.0.0:0) = c4
TCP(1): Connect(c4, 192.168.90.101:8000) ...
Connect(c4) TCP(1) ERROR 10060 - (null)
TCP(1): Close(c4) - OK
Socket(0.0.0.0:0) = 98
TCP(1): Connect(98, 192.168.90.101:8000) ...
```

check the configuration (IP address and TCP port).

7.2.5. CHANGING THE PORT NUMBER

Older software applications can only use a small range of COM ports, so you may need to change the virtual COM port number.

In our case the COM pair created is COM4/COM5, let's see the procedure to change it to COM2/COM3
Click on the "DEVICE MANAGER" button:



Seneca Ethernet to Serial Connection

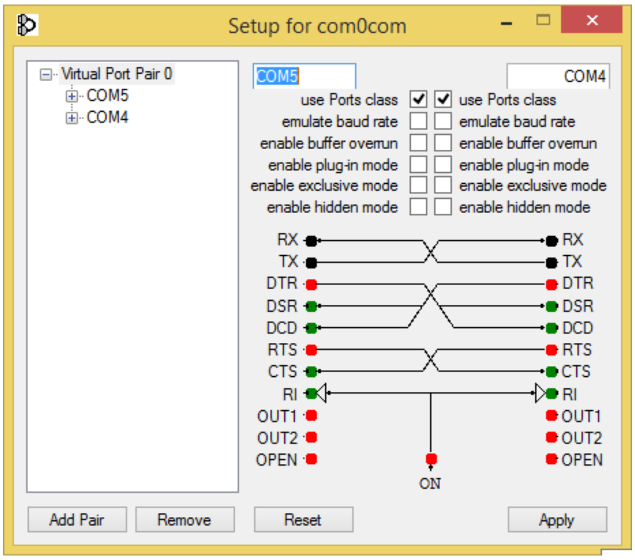
Seneca Ethernet to Serial Connection rev. 1.04

Select PC Virtual Com Port: COM4

Select Z-PASS / Z-KEY IP address: 192 . 168 . 90 . 101

Select Z-PASS / Z-KEY PORT: 8000

The com0com configuration window appears:

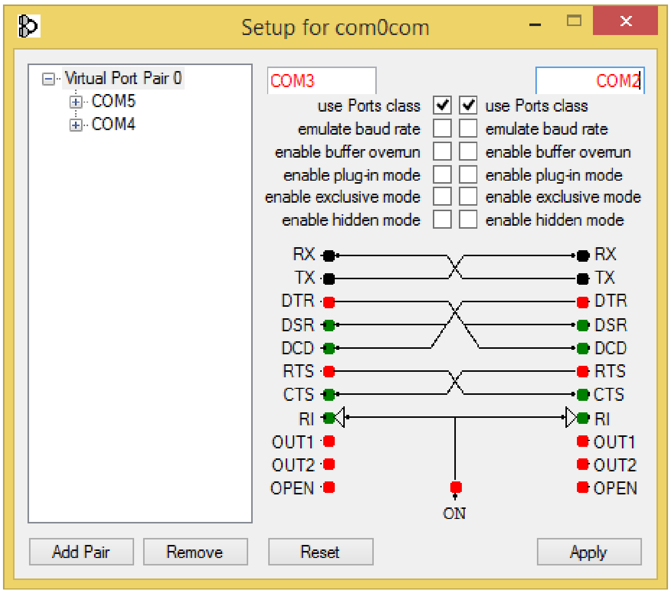


Setup for com0com

Virtual Port Pair 0
- COM5
- COM4

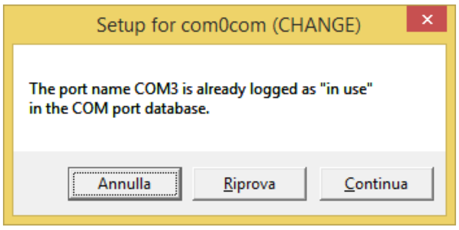
COM5			COM4
use Ports class	☑	☑	use Ports class
emulate baud rate	□	□	emulate baud rate
enable buffer overrun	□	□	enable buffer overrun
enable plug-in mode	□	□	enable plug-in mode
enable exclusive mode	□	□	enable exclusive mode
enable hidden mode	□	□	enable hidden mode

Now change COM5 to COM3 and COM4 to COM2, then click on "Apply":



COM3			COM2
use Ports class	☑	☑	use Ports class
emulate baud rate	□	□	emulate baud rate
enable buffer overrun	□	□	enable buffer overrun
enable plug-in mode	□	□	enable plug-in mode
enable exclusive mode	□	□	enable exclusive mode
enable hidden mode	□	□	enable hidden mode

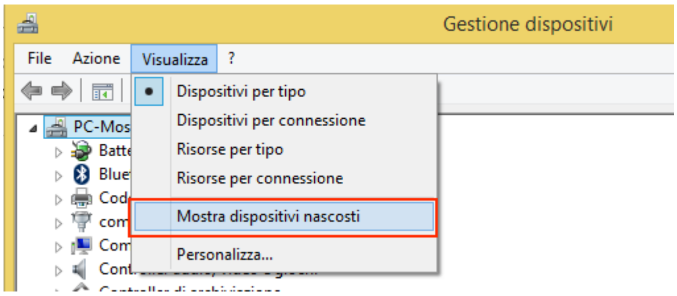
Sometimes the COM may be marked "in use":


Setup for com0com (CHANGE)

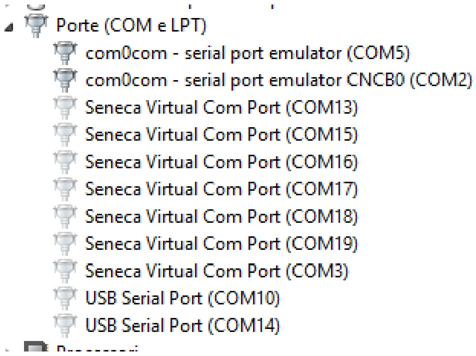
The port name COM3 is already logged as "in use"
in the COM port database.

If you need to use this COM number, click "Continue", then go to device configuration.

Since the port is not connected, click on "Show hidden devices":

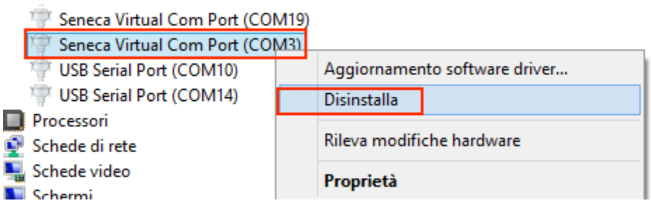


Now all unused ports are displayed in transparency (even our COM3):



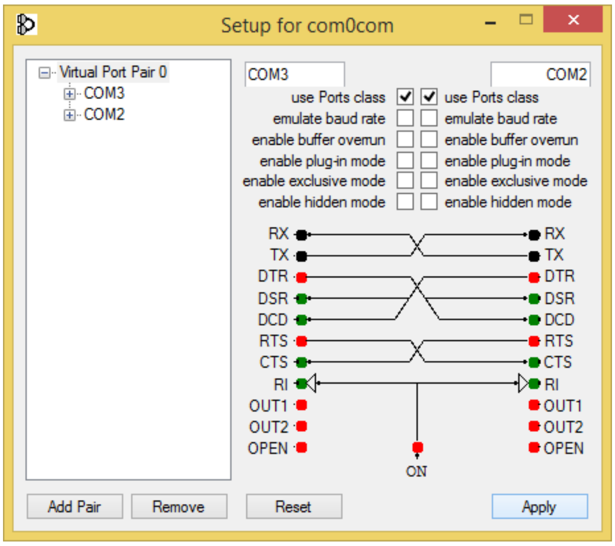
Porte (COM e LPT)
- com0com - serial port emulator (COM5)
- com0com - serial port emulator CNCB0 (COM2)
- Seneca Virtual Com Port (COM13)
- Seneca Virtual Com Port (COM15)
- Seneca Virtual Com Port (COM16)
- Seneca Virtual Com Port (COM17)
- Seneca Virtual Com Port (COM18)
- Seneca Virtual Com Port (COM19)
- Seneca Virtual Com Port (COM3)
- USB Serial Port (COM10)
- USB Serial Port (COM14)

Now select the COM3 port and click on "Uninstall":



Seneca Virtual Com Port (COM19)
Seneca Virtual Com Port (COM3)
USB Serial Port (COM10)
USB Serial Port (COM14)
Processori
Schede di rete
Schede video
Schermi
Aggiornamento software driver...
Disinstalla
Rileva modifiche hardware
Proprietà

Now COM3 is free, and we can use it on the com0com setup:

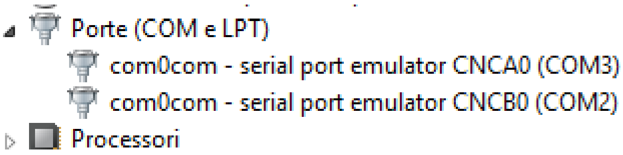


Setup for com0com

Virtual Port Pair 0
- COM3
- COM2

COM3		COM2
use Ports class ☑		☑ use Ports class
emulate baud rate □		□ emulate baud rate
enable buffer overrun □		□ enable buffer overrun
enable plug-in mode □		□ enable plug-in mode
enable exclusive mode □		□ enable exclusive mode
enable hidden mode □		□ enable hidden mode

Finally click on "Apply", now the pair COM3/COM2 is created:

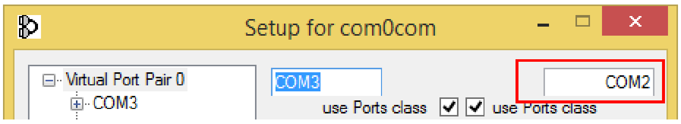


Porte (COM e LPT)
- com0com - serial port emulator CNCA0 (COM3)
- com0com - serial port emulator CNCB0 (COM2)

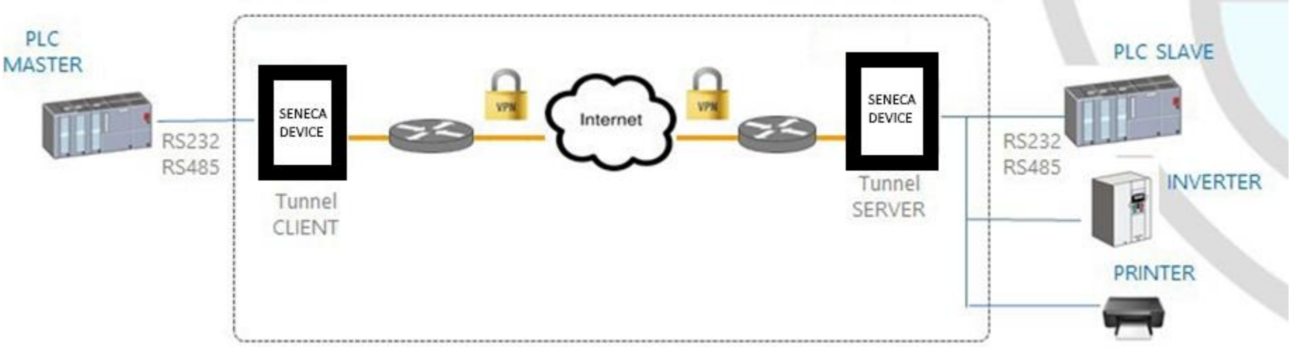
Processori

ATTENTION!

The Seneca Ethernet to Serial Connect Software always uses the correct port of the pair created in the com0com configuration (in our case COM2).



7.3. SERIAL TUNNEL POINT ON TCP



The point-to-point serial tunnel allows to extend a serial connection between two serial devices (that support the same protocol) via a TCP/UDP connection.

In TCP operating mode, one of the two Seneca devices is defined as "Master" and the other is the "Slave": the first is a Tunnel Client, which receives data from the serial line and sends them to an outgoing TCP connection, while the second is a Tunnel Server, which receives data from an incoming TCP connection and sends them to the serial line; in this mode a "tunnel" is established between the two serial ports.

During configuration, on the Master, you must set the destination IP address and the destination Port that defines the outgoing TCP connection; on the Slave, you must set the Listening Port on which the incoming TCP connection is accepted.
The tunnel can also be established through a VPN connection..

ATTENTION!

In Serial Tunnel Point-to-Point the operating mode on TCP, only one connection is accepted for a given serial port.

7.4. POINT-TO-POINT SERIAL TUNNEL ON UDP

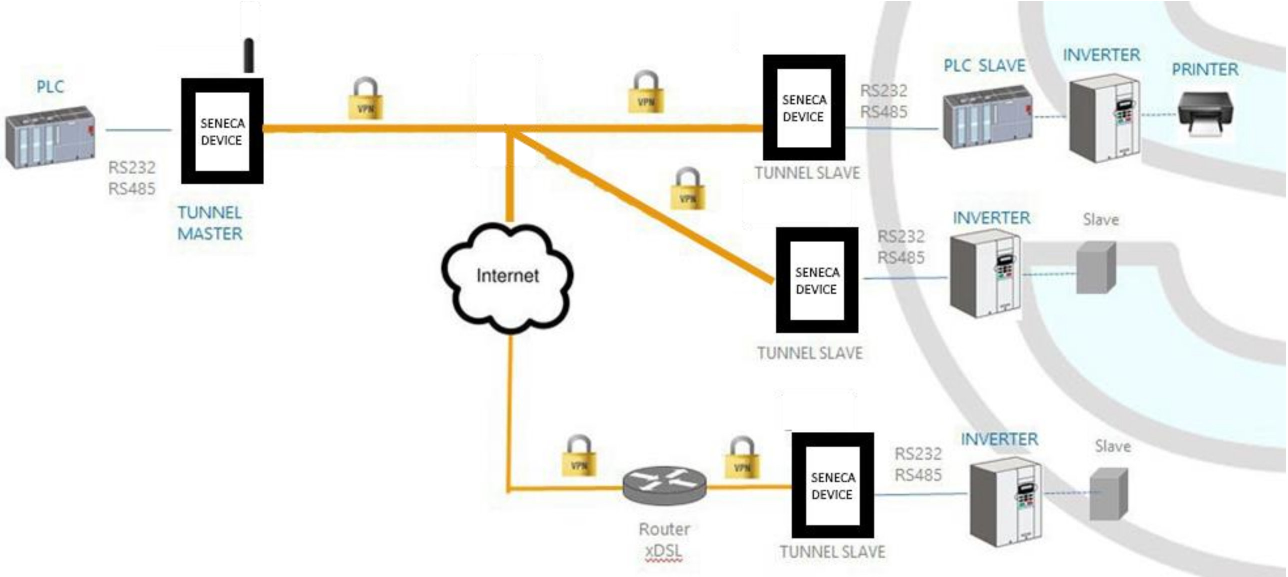
The Serial Tunnel Point-to-Point operating mode on UDP is very similar to that of TCP.

The only difference is that none TCP connection is established and the serial data is carried by a UDP packet.
The configuration parameters are the same as for the serial tunnel over TCP.
Again, The UDP packet can also passes through a VPN connection

CAUTION

In Serial Tunnel Point-to-Point operating mode on UDP, only one connection is accepted for a given serial port.

7.5. SERIAL TUNNEL FROM POINT TO MULTIPOINT



The Serial Tunnel Point-to-Multipoint allows you to create a tunnel with a master and more than one slave; on the master side, the data received from the serial line are sent to all the slaves, via the *multicast* transmission mode, in UDP packets.

For multicast to work, the master and slaves must be part of the same multicast group, so there is a "Multicast Group" parameter that must be set accordingly; moreover, for the configuration of the master the "Destination Port" and "Multicast Interface" parameters must be defined, the latter must be set to select the network interface which allows packets to be sent; "Listen Port" and "Multicast Interface" are required for slave configuration; the latter must be set to select the network interface that allows you to receive packets.

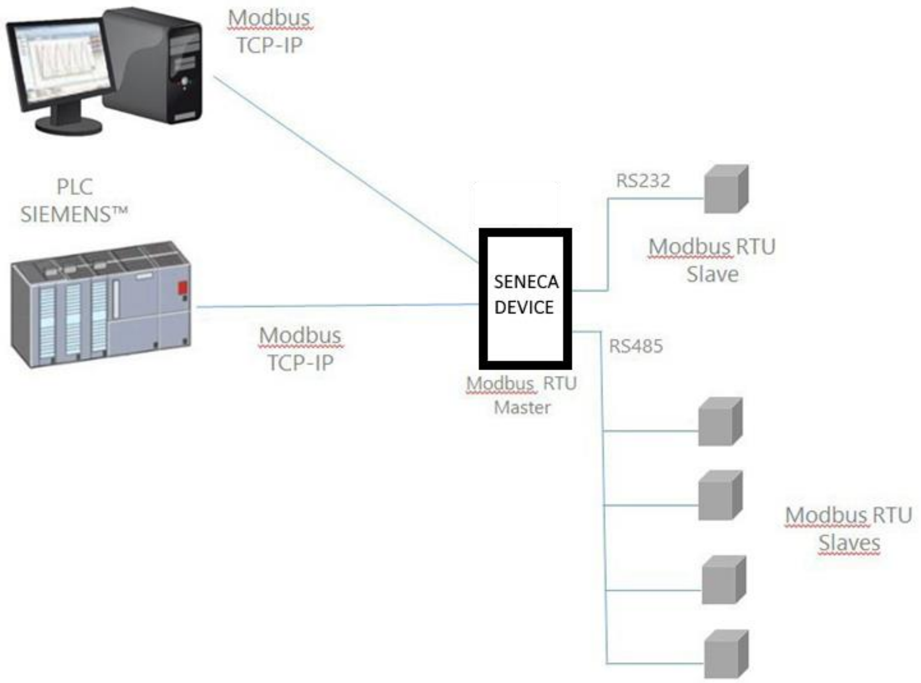
ATTENTION!

In Serial Tunnel Point-to-Multipoint operating mode, only one connection is accepted for a given serial port.

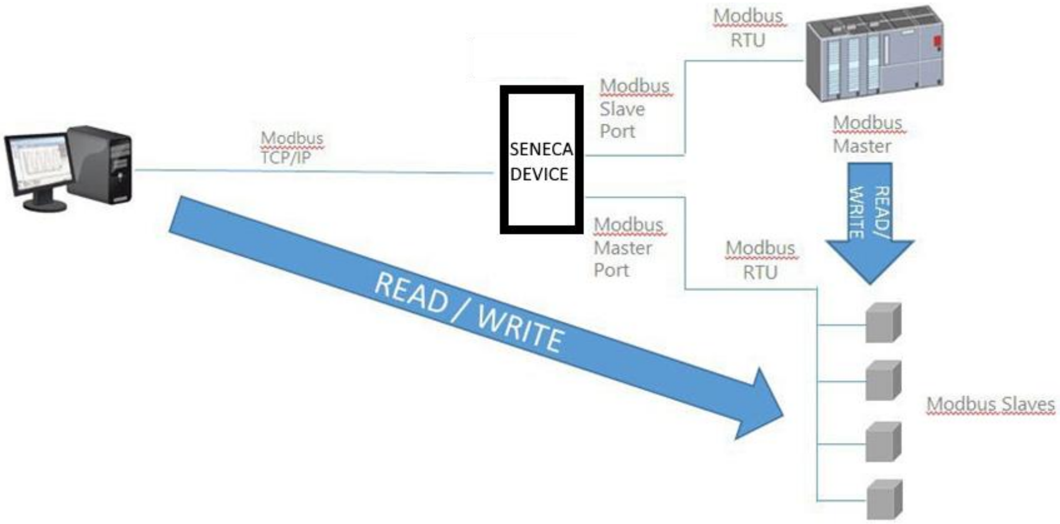
8. MODBUS GATEWAY WITH SHARED MEMORY (R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

The device can be configured to operate as a Modbus Gateway with Shared Memory: in this mode, a series of configured tags are periodically and continuously read by Modbus RTU Slave or Modbus TCP Server devices; these values are always available in a shared memory, readable via Modbus TCP/RTU.
This modality supports up to 2000 tags and up to 32 Modbus TCP Client simultaneously, one Modbus TCP/IP Server (or slave) is always running on a configured TCP port.
For each of the available serial ports you can define the type of "Task": a serial port can be configured as Modbus RTU Master or Modbus RTU Slave or disabled.
In this way different combinations are possible.

In addition, tags can be read to/from up to 25 Modbus TCP Server.
Finally, you can define some tags that are related to the "embedded" digital I/O present in the device.
The following pictures show some typical scenarios.

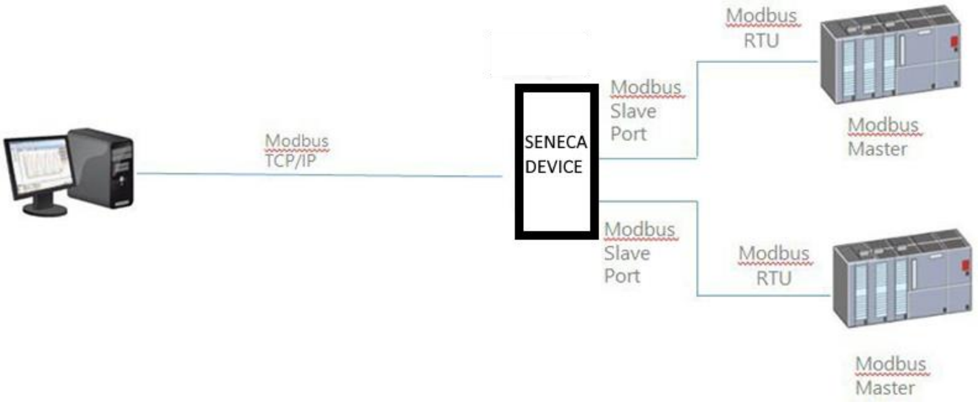


In the figure above, two serial ports are configured as Modbus RTU Master.



In this case, one serial port is configured as Modbus Slave and another is configured as Modbus Master.

When some registers acquired by the Modbus Slaves must be available for a PLC, which only supports the Modbus Master protocol, the device can be configured with one serial port defined as Modbus Slave (connected to the PLC) and another in Modbus Master (connected to the Modbus Slaves). The PLC Modbus RTU Master and the Modbus TCP client(s) will write/read the shared memory registers of the Seneca device, while the Modbus Gateway keeps the shared memory aligned with the Modbus Slaves registers.



In the figure above, two serial ports are configured as Modbus Slave and connected to a Modbus Master PLC port; in this way, the two PLCs and the Modbus TCP Client can write/read the shared memory to share data.

The Modbus Gateway Shared Memory mode provides some interesting features, as explained below.

In addition to the "classic" behaviour of the gateway, the tags can be configured to operate in "Bridge" mode; this mode allows you to "refresh" the tag values from the serial side only when the gateway receives Modbus TCP/RTU requests for those tags; this can be very useful when using RTU devices with "Fail safe" outputs, where it is necessary to cyclically write the outputs otherwise a fail would occur.
Modbus Gateway Shared Memory also performs request optimization, placing as many registers as possible in a single read/write request; it is possible to set the maximum number of registers in a request independently for

each serial port/TCP Server and for read and write operations; this option can be useful for connecting RTU devices that support a maximum number of different registers on different serial ports.

Tag configuration can be created using a Microsoft Excel™ Template provided by Seneca (see paragraph 24.3.2.4); this template can considerably reduce configuration time, particularly when a large number of tags need to be configured.

9. DATALOGGER (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

When the Modbus Gateway functionality with Shared Memory is enabled in the device you can also activate the "Data Logger" mode:
Tag values are periodically stored in files (called "log files"), which can then be transferred.

Tags can be associated with up to four groups of Data Loggers, which can have different sampling and transfer periods.

The following "transfer" methods are currently supported;

- copied to USB stick
- transferred to an FTP server;
- sent to one or more e-mail addresses, as an attachment.
- Sent to a server via http post
- Sent to an MQTT broker

More than one of the above methods can also be enabled at the same time.

Log files are stored in flash memory, so if one of the transfer methods temporarily fails, it can be successfully transferred later.

For each group of data loggers, the "cache" is filled if at least one of the following cases is reached:

- 1000 log files
- 500000/(number of groups enabled) samples (i.e. number of lines of a single log file)

When the limit is reached, the "rotation" of the log file occurs, i.e. the oldest files are overwritten by the new one.

Log files of the standard "csv" type can then be processed by Excel™ or PC software.

Here is a portion of a log file:

```
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;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;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;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;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
```

If for a tag the actual value is not available (for example, if the tag corresponds to a log that does not respond to Modbus requests), the value written in the corresponding field of the log file can be set to "ERR!
The "ERROR MODE" parameter can also be set to LAST VALUE or to a user-defined FAIL value.

Please note that each time a configuration change is made that affects the functionality of the Data Logger (from a page in the "Datalogger" section) the following procedure is performed:

- Data Logger processes are interrupted
- The internal log file cache is cleared

10. LOGIC REGULATIONS (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

The device can be configured with a maximum of 2000 logical rules
A logical rule is based on the following concept

“IF -> THEN -> ELSE”

It means:

IF THE CONDITION HAS OCCURRED -> THEN PERFORM THESE ACTIONS -> OTHERWISE PERFORM THESE OTHER ACTIONS

In each rule can also be configured:
- Combinations of up to three logical conditions (based on alarm states) in AND/OR logical expression;
- up to three actions can be performed

11. ALARMS (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

Regarding the alarms A complete set of parameters are available to define the behaviour of the alarms, as indicated in the "Alarm configuration" page; the entire alarm status can be viewed in the "Alarm Summary" page and the alarm log can be retrieved in the "Alarm Log" page.

Moreover, in the "Tag View" page, the columns "ALARM" and "ANALOG DANGER ALARM" show the current alarm status for each tag.
The actions can be used to send an SMS, EMAIL or HTTP POST, MQTT ...;

12. VPN

The device supports VPN connection using two different servers: Seneca VPN BOX2 and a standard OpenVPN Server.
The main advantages of using a VPN are:

- secure connections so the transmitted data are encrypted;
- the ability to establish connections without interfering with the corporate LAN;
- no need to have a static/public IP address
- on the WAN side; remote configurability via Web Server

Two "VPN modes" are available, respectively named "OpenVPN" and "VPN BOX".

The "OpenVPN" mode can be used when the device is to be installed in an existing VPN. In this case, an OpenVPN server must be available and configuration, certificates and key files for the Seneca Client must be provided by the VPN administrator.
Files can be uploaded to the device using the dedicated web page.

If the VPN infrastructure is not available, the recommended choice is to adopt the "VPN Box2" solution developed by Seneca.
"VPN Box2" is a hardware device (or virtual machine) that allows the user to easily configure two alternative types of VPN:
"VPN " Single LAN (Always on connection)
VPN "Point-to-Point" (On demand)

In "Single LAN" VPN, all devices and PCs (and associated local sub-networks) configured in VPN are always connected in the same network. In this scenario any VPN Client (PC or Seneca device) can communicate each other but also with the machines/devices connected to any Seneca device LAN, for this reason, all VPN Clients must have different network configuration.

In the "Point-to-Point" VPN, a client PC, at a given moment, can perform a single connection, upon request, to only one device at a time (and to the machines that are connected to the LAN port of the Seneca device).
Furthermore, the devices cannot communicate with each other even if they belong to the same VPN.
The advantage of this architecture is that the same subnetwork can be used at all sites. The point-to-point mode is the most used in case of remote maintenance of the systems.

There are two types of point-to-point VPN connection:

- Layer 3 VPN
- Layer 2 VPN

In "Layer 3 VPN", only IP packets (Layer 3) are transported through the VPN tunnel.
On the other side, in "Bridging Layer 2 VPN", all Ethernet frames are transported through the VPN tunnel

Each mode has advantages and disadvantages:
<u>Layer 2</u>

- can carry any network protocol (e.g. profinet protocol)
- causes more traffic on the VPN tunnel than layer3

<u>Layer 3</u>

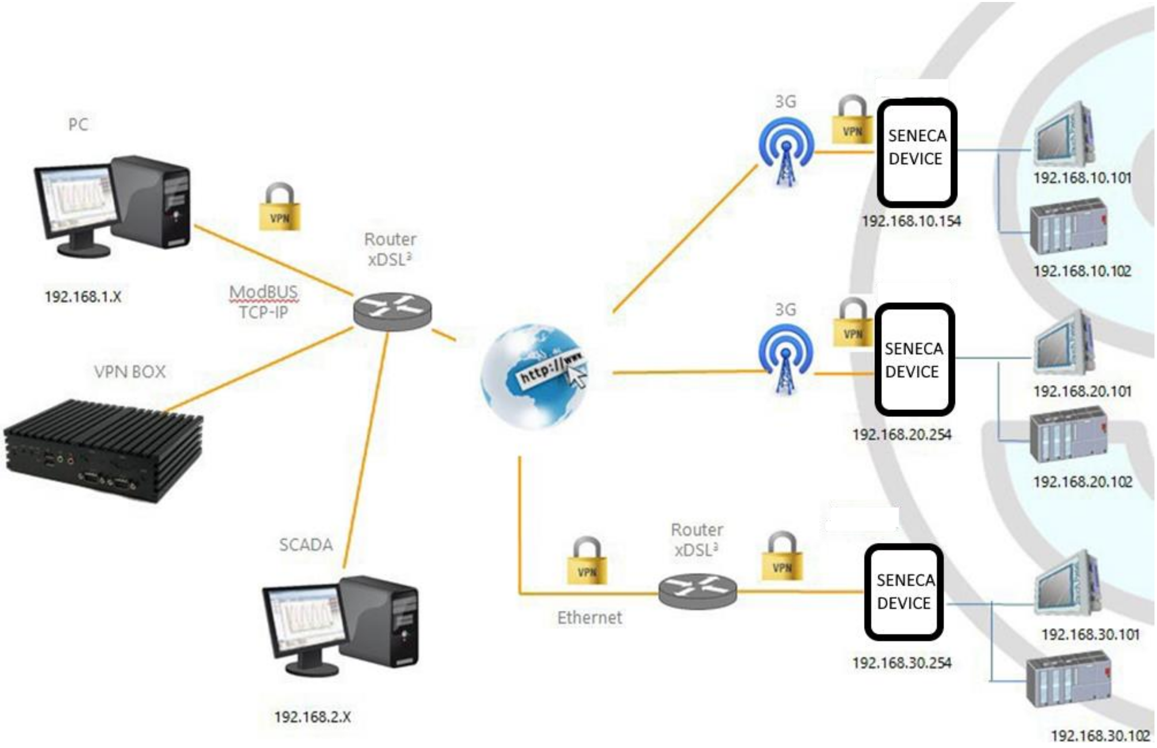
- can carry only IP traffic
- layer2 traffic (e.g.: DHCP) is not transported
- reduces traffic management costs, transports only traffic destined for clients

The "VPN Box2" comes with two Windows applications: "VPN Client Communicator" allows the user to connect the PC to the network (in the "Single LAN" case) or to a specific device (in the "Point-to-Point" case)

A detailed description of the "VPN Box2" can be found in the "VPN Box 2 User Manual.

A detailed description of the configuration parameters of a VPN is given in the following two sub-paragraphs.

12.1. VPN "SINGLE LAN" ALWAYS ON



The figure above provides an example of VPN

The client PC (with IP address 192.168.1.X) can connect, as an example, to the first Seneca device using its local IP address.

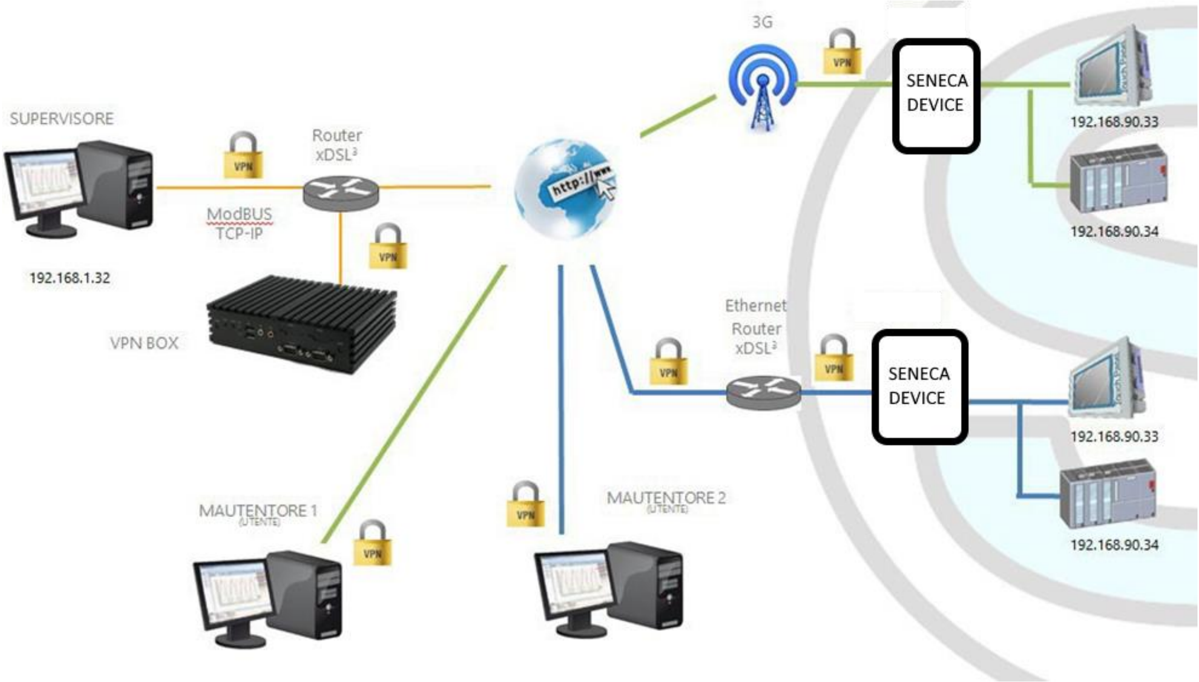
Also, two devices that are in two different LANs of the same VPN network (e.g.: 192.168.10.101 and 192.168.20.102) can connect to each other, again using their local IP addresses.

In order for this scenario to work properly, one essential rule must always be followed: the LANs of the Seneca device and the LAN of the PC must have different subnets and not in collision; therefore, in the figure above, the following is shown

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

If conflicts cannot be avoided, it is still possible to use a "Single LAN" VPN because devices can be reached via their VPN IP addresses and machines beyond them can be reached by configuring "port forwarding" rules.

12.2. VPN "POINT TO POINT" ON DEMAND



The figure above provides an example of "Point-to-Point” VPN.

In this scenario a PC (acting as a VPN client) can connect, on demand, to a Seneca device and its subnet using local IP addresses via the VPN Client Communicator application . The software guarantees group management of users to allow only those who belong to a group to access the systems that are part of it

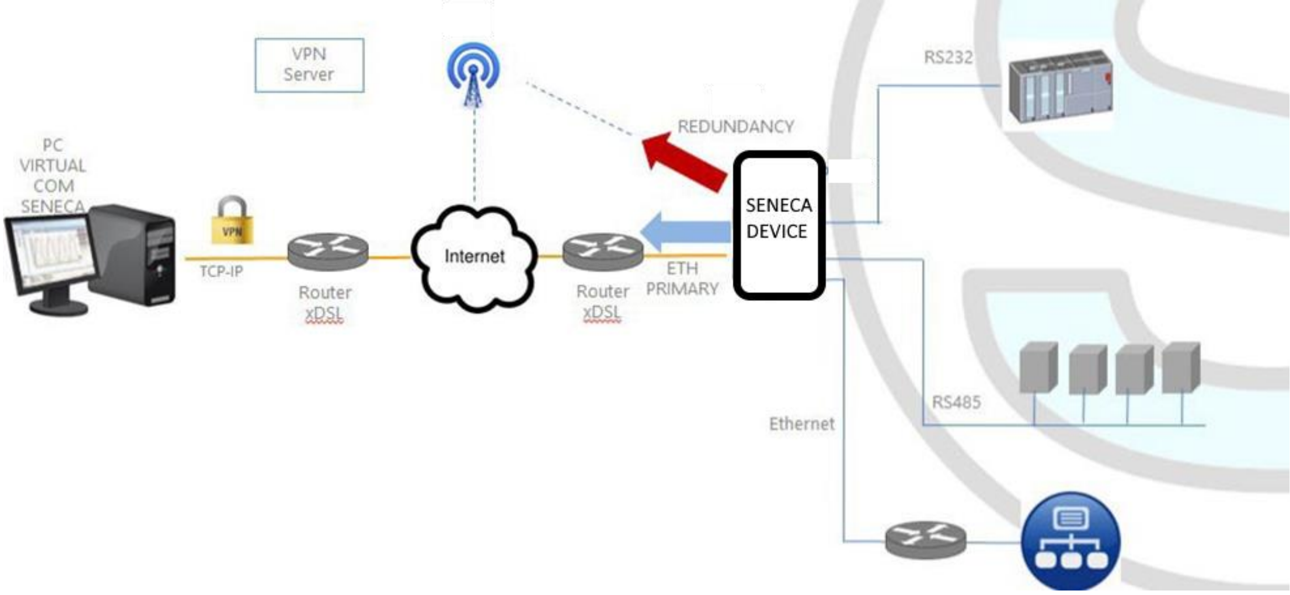
13. ROUTER

As mentioned above, the "Router" mode allows to route packets between the LAN (Ethernet) and the WAN (Mobile Network) / WI- WI interface or mobile connection.

More specifically, an important feature of the Router is the so-called "IP forwarding"; this means that when the device receives a packet not intended for it, it does not discard the packet but forwards it to its actual destination; when a packet is routed from the LAN to the WAN, the device also performs the so-called "IP masquerading", i.e. the replacement of the source IP address with the IP address of the WAN interface.
Another important feature is the availability of a DNS server/forwarder, which can resolve names with or without external DNS.
In addition, a DHCP server is available that assigns IP addresses to clients connected on the LAN port (or on the WI-FI when set in Access Point mode); here, the user can configure the range of addresses used by the server and the time of location.
There is also the possibility to define "Port Forwarding" or "Virtual Server" rules; using these
for example, packets received from a TCP or UDP port can be redirected to another port or IP address.

As an alternative to the use of "Port Forwarding" rules, the Router + VPN functions allow the use of local addresses as shown in the previous chapter; there is a flag in the router configuration to enable these features.

14. NETWORK REDUNDANCY



“Network redundancy” is a feature that can be enabled on devices where a mobile or WI-FI modem is available.

This feature is intended to switch the network interface used to access the Internet from Ethernet ("primary" interface) to the secondary interface (Cellular modem or WI-FI), when access to the Internet through the primary interface becomes unavailable, the system draws on the Internet through the configured secondary channel. When the Internet service becomes available again from the primary interface the access returns to the latter.

15. DISABLING THE REMOTE CONNECTION

The products provide an integrated digital input and digital output dedicated to control and monitor the remote connection to the device.
In this way it is possible to block access (via digital input) remotely to a particular machine/plant (e.g. if local maintenance operations are being carried out) and be informed of a remote access in progress (via digital output).

When the "Remote Connection Disable" digital input is set to HIGH, the remote connection to the device is disabled; conversely, when the "Remote Connection Disable" digital input is set to LOW, the remote connection to the device is enabled.

The "Remote Connection Active" digital output is set to the HIGH state when the device is connected.

Four security levels can be configured to disable the remote VPN connection:

Level 1: VPN connections are disabled in any VPN mode but the "VPN Box Service" service is still running, so the device can still be monitored on VPN Box Manager;
Level 2: The "VPN Box Service" is disabled, but the device can still access the Internet and send/receive SMS on a possible cellular interface;
Level 3: any Internet access is disabled, but the device can still send/receive SMS on a possible cellular interface;
Level 4: As level 3 but also the cellular interface is switched off

16. AUTO APN

The Auto-APN function allows the device with a cellular modem to establish mobile data connections without the user having to configure the APN data for the SIM in use.

This is obtained using the IMSI code contained in the SIM and, possibly, some other data available on the SIM. In some special cases, however, when using a "custom APN", the Auto-APN function can be disabled by setting the "APN Mode" parameter to "Manual".

17. HTPP REST CLIENT PROTOCOL (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

Communication between SSD and Cloud is possible via HTTP protocol with a POST call.
The architecture is REST (REpresentational State Transfer), where the data are configured as classic web FORM but through JSON (JavaScript Object Notation). For further information on the HTTP POST communication protocol, refer to "Seneca HTTP POST Communication Protocol" (the document can be requested at supporto@seneca.it).
The device is compatible with the Seneca Cloud Box product and also with a generic server that supports HTTP POST communication protocol.
This protocol is equipped with a set of HTTP POST APIs (RESTFUL); the relative documentation can be provided by Seneca to customers who wish to develop their own server-side software; for information, contact Seneca Service & Support at supporto@seneca.it.

The HTTP POST protocol can be enabled together with the other transfer methods (MEMORY, FTP, EMAIL, ...); however, when the HTTP POST protocol is enabled, the following changes apply to the behaviour of the Data Logger:

- only one recording group can be enabled;
- the sampling period is a multiple of 30 seconds;
- each sample is sent to the http server in a *LOG* message, carried by an HTTP POST

The Seneca HTTP POST protocol also allows the server to perform the following actions on the device:

- setting the values of one or more tags
- restarting the device
- save the device configuration on the FTP site of the server
- upload the device configuration from the FTP site of the server
- starting the FW update;

There is also an internal cache for LOG messages sent via HTTP POST requests, used to store log messages while unable to send them to the server; this cache can hold up to 3000 messages:

18. OPC UNIFIED ARCHITECTURE SERVER PROTOCOL (OPC-UA)

OPC Unified Architecture (OPC-UA) is a standardized machine-to-machine communication protocol for industry 4.0 developed by the OPC Foundation.

OPC-UA is a vendor-independent communication protocol and is based on the client-server principle.
Seneca devices support the OPC-UA server protocol also with security policy.

In particular, the OPC-UA server "exports" the Shared Memory tags, then, using an OPC-UA client it will be possible to read and write directly to all tags.

19. MQTT CLIENT PROTOCOL

MQTT is the most widely used protocol for IOT applications.

"MQTT" stands for MQ Telemetry Transport. It is an extremely simple and lightweight public/subscription messaging protocol designed for devices with low bandwidth, high latency or unreliable networks. The design principles are to minimize network bandwidth and device resource requirements while trying to ensure reliability and a certain degree of delivery guarantee. These principles prove ideal for the emerging machine-to-machine (M2M) or Internet of Things world.

For more information on the MQTT protocol see

The MQTT version supported is 3.1.1

19.1. MQTT CHARACTERISTICS (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

The MQTT protocol can be enabled together with the other transfer methods (USB, FTP, EMAIL, …); however, when the MQTT protocol is enabled, the following changes apply to the behaviour of the Data Logger

The MQTT protocol also allows you to perform the following actions on the device:

- setting the values of one or more tags
- restarting the device
- save the device configuration on the FTP site of the server
- upload the device configuration from the FTP site of the server
- starting the FW update;

There is also an internal cache for LOG messages sent via MQTT requests, used to store log messages while it is not possible to send them to the broker; this cache can hold up to 3000 messages

20. STRATON PLC (R-PASS-S, Z-TWS4-RT-S, Z-PASS2-RT-S MODELS ONLY)

The Straton PLC provides full support for the IEC 61131-3 PLC standard; an integrated development environment (IDE) is available for Windows™ PCs.
The Straton IDE includes several tools such as: a fieldbus configuration tool, an analog signal editor and program editors compliant with the five languages of the IEC 61131-3 standard: Sequential Function Chart (SFC), Function Block Diagram (FBD), Ladder Diagram (LD), Structured Text (ST), Instruction List (IL).
With Straton IDE, it's easy to write, download and debug the IEC 61131-3 code.

20.1. WRITE, DOWNLOAD AND RUN YOUR FIRST PROGRAM

To allow the PLC developer to easily create Straton applications for Seneca CPUs, the following libraries are available:
• a Function Block (FB) and Functions library, which provides some frequently used functions, in particular related to communication and data transfer activities, compiled in the CPU firmware; the direct use of these FBs and functions is aimed at expert PLC developers (a detailed description of the FBs and functions is given in the relevant chapter of this manual);
• a "Profile" library, which allows access to CPU I/OS via "profile" variables

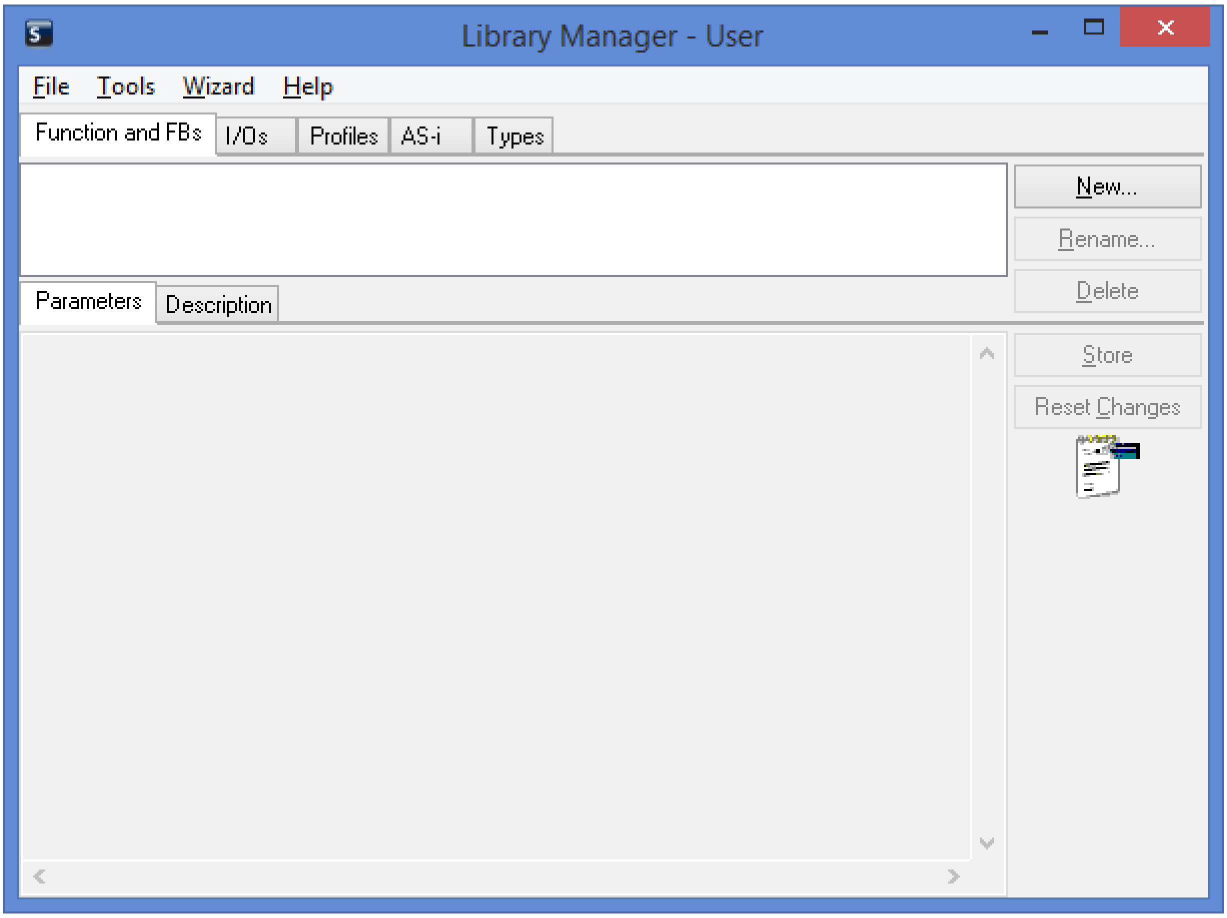
• a "User Defined Function Block" (UDFB) library, in ST language, which simplifies the use of the aforementioned FBs, providing simpler and "higher level" access to their functions.

An installation program called "Seneca Straton Package" is available which automatically installs the Seneca libraries and templates. The installation program also includes Straton IDE and other tools.
The installation program is available at the following link:
http://www.seneca.it/products/seneca-straton-package

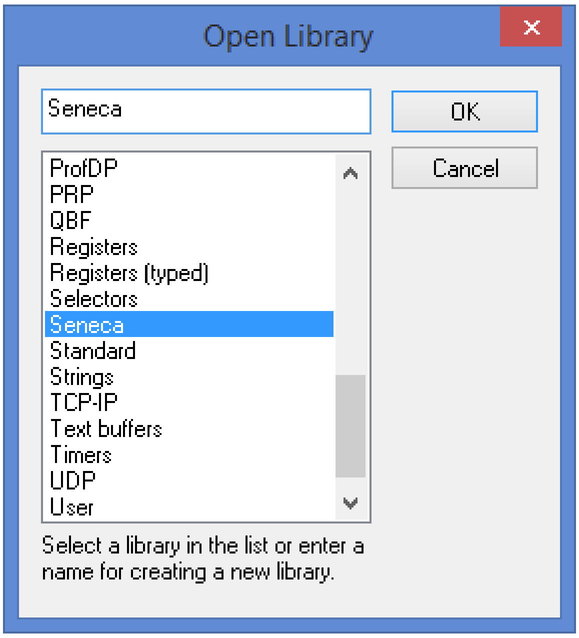
If, for some reason, you are unable to run the installation program, the above libraries and templates can be installed manually as described in the next subparagraph:

20.1.1. MANUAL INSTALLATION OF LIBRARIES AND TEMPLATES IN STRATON

The following steps are required to integrate Seneca libraries and profiles into the Straton IDE.
First, we need to add the Seneca FB library (SenecaStratonLibrary.XL5 file) to the IDE, using the "Library Manager" tool:



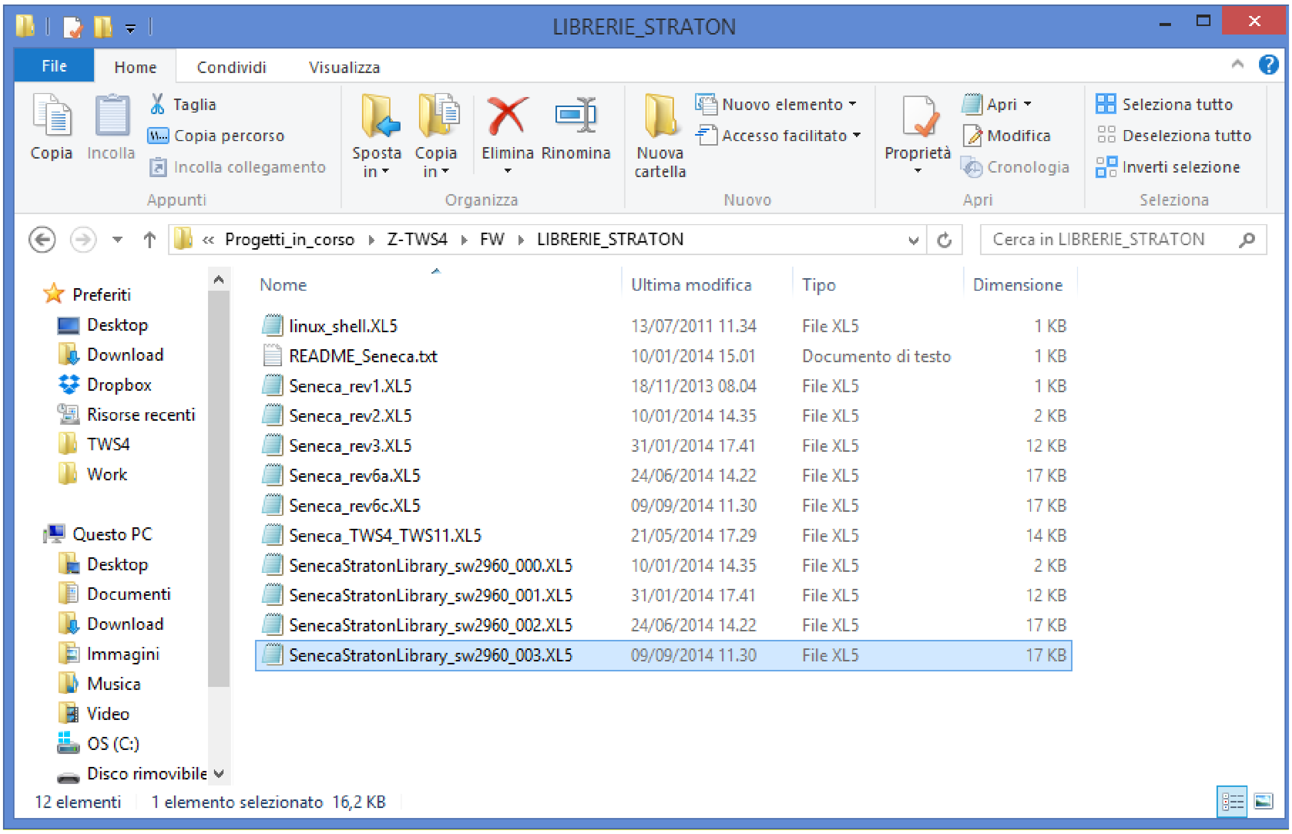
Select the "File / Open Library" option and enter the name "Seneca" to create the new Seneca library.



Seneca

Select a library in the list or enter a name for creating a new library.

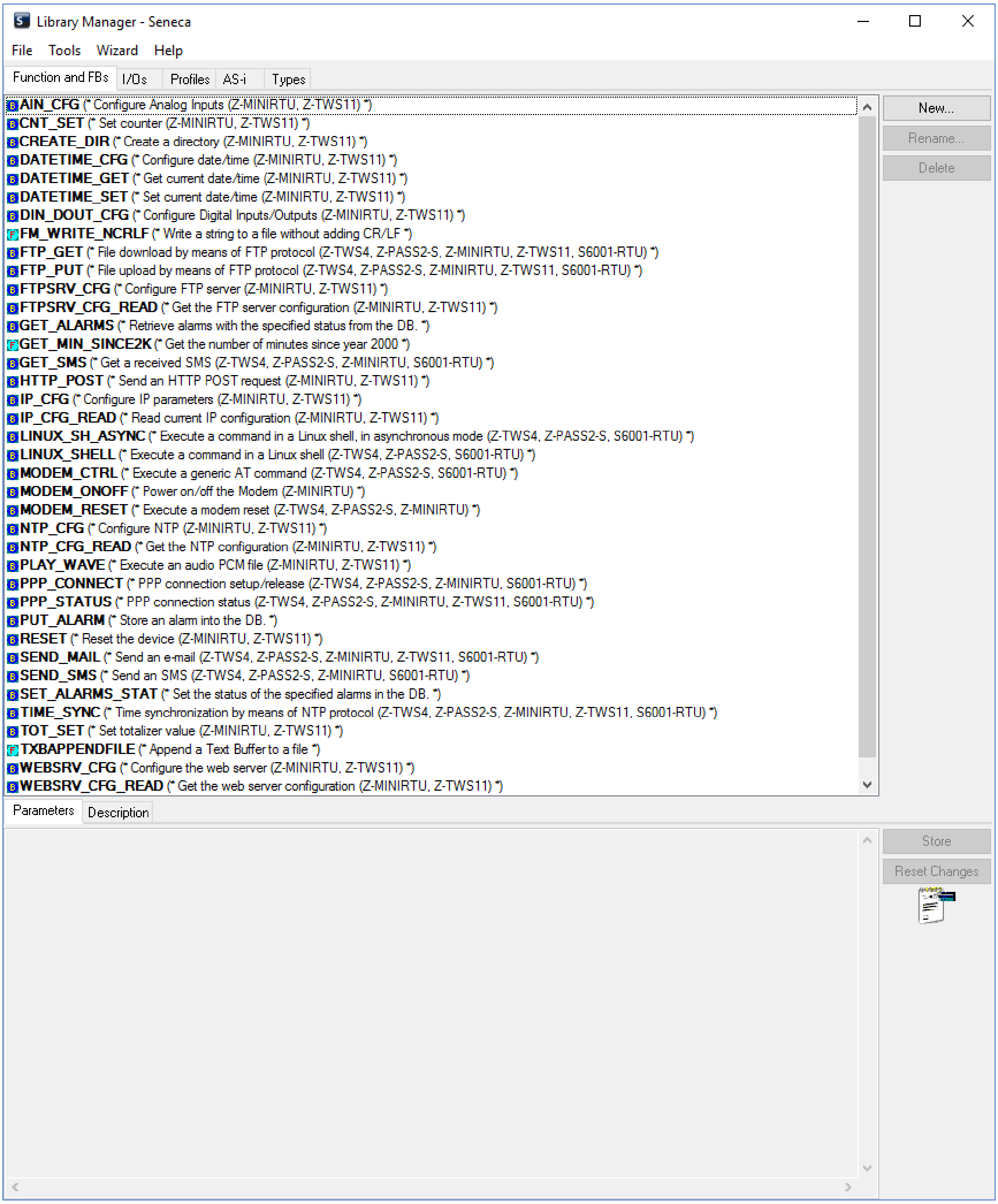
Then, import the Library (“Tools / Import” menu):



« Progetti_in_corso › Z-TWS4 › FW › LIBRERIE_STRATON

Nome	Ultima modifica	Tipo	Dimensione
linux_shell.XL5	13/07/2011 11.34	File XL5	1 KB
README_Seneca.txt	10/01/2014 15.01	Documento di testo	1 KB
Seneca_rev1.XL5	18/11/2013 08.04	File XL5	1 KB
Seneca_rev2.XL5	10/01/2014 14.35	File XL5	2 KB
Seneca_rev3.XL5	31/01/2014 17.41	File XL5	12 KB
Seneca_rev6a.XL5	24/06/2014 14.22	File XL5	17 KB
Seneca_rev6c.XL5	09/09/2014 11.30	File XL5	17 KB
Seneca_TWS4_TWS11.XL5	21/05/2014 17.29	File XL5	14 KB
SenecaStratonLibrary_sw2960_000.XL5	10/01/2014 14.35	File XL5	2 KB
SenecaStratonLibrary_sw2960_001.XL5	31/01/2014 17.41	File XL5	12 KB
SenecaStratonLibrary_sw2960_002.XL5	24/06/2014 14.22	File XL5	17 KB
SenecaStratonLibrary_sw2960_003.XL5	09/09/2014 11.30	File XL5	17 KB

12 elementi 1 elemento selezionato 16,2 KB



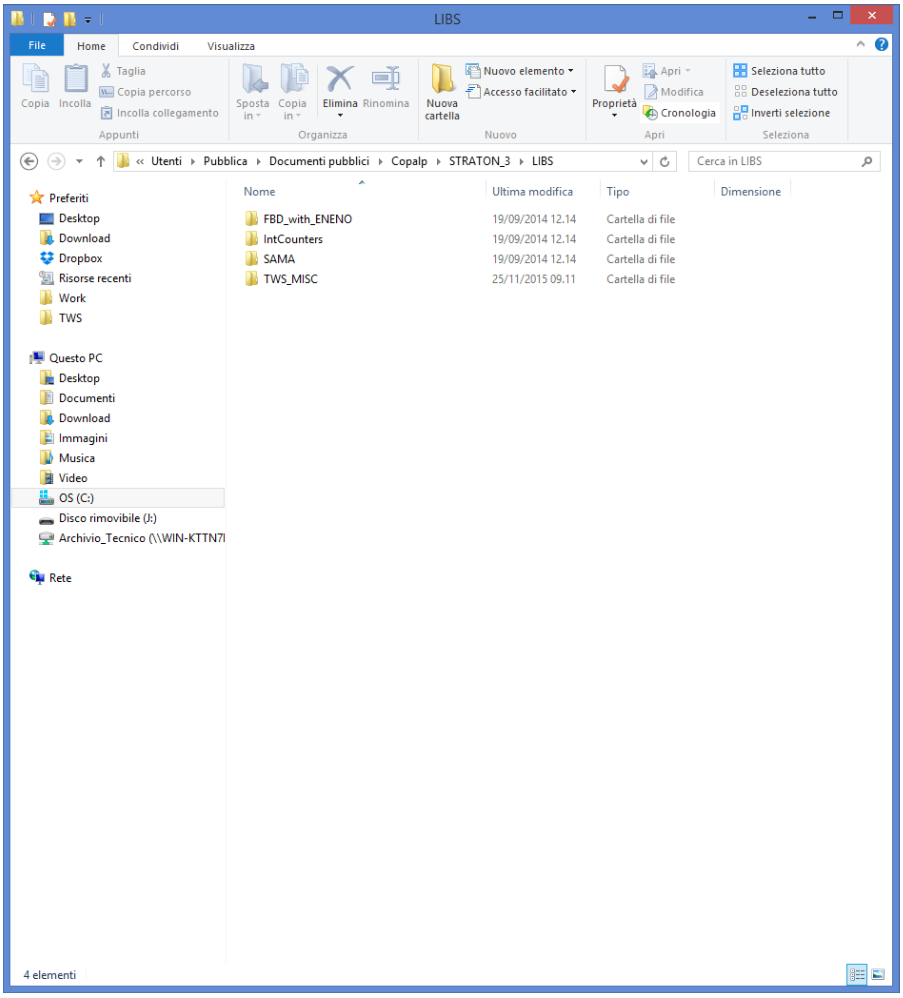
AIN_CFG (* Configure Analog Inputs (Z-MINIRTU, Z-TWS11) *)
CNT_SET (* Set counter (Z-MINIRTU, Z-TWS11) *)
CREATE_DIR (* Create a directory (Z-MINIRTU, Z-TWS11) *)
DATETIME_CFG (* Configure date/time (Z-MINIRTU, Z-TWS11) *)
DATETIME_GET (* Get current date/time (Z-MINIRTU, Z-TWS11) *)
DATETIME_SET (* Set current date/time (Z-MINIRTU, Z-TWS11) *)
DIN_DOUT_CFG (* Configure Digital Inputs/Outputs (Z-MINIRTU, Z-TWS11) *)
FM_WRITE_NCRLF (* Write a string to a file without adding CR/LF *)
FTP_GET (* File download by means of FTP protocol (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)
FTP_PUT (* File upload by means of FTP protocol (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)
FTPSRV_CFG (* Configure FTP server (Z-MINIRTU, Z-TWS11) *)
FTPSRV_CFG_READ (* Get the FTP server configuration (Z-MINIRTU, Z-TWS11) *)
GET_ALARMS (* Retrieve alarms with the specified status from the DB. *)
GET_MIN_SINCE2K (* Get the number of minutes since year 2000 *)
GET_SMS (* Get a received SMS (Z-TWS4, Z-PASS2-S, Z-MINIRTU, S6001-RTU) *)
HTTP_POST (* Send an HTTP POST request (Z-MINIRTU, Z-TWS11) *)
IP_CFG (* Configure IP parameters (Z-MINIRTU, Z-TWS11) *)
IP_CFG_READ (* Read current IP configuration (Z-MINIRTU, Z-TWS11) *)
LINUX_SH_ASYNC (* Execute a command in a Linux shell, in asynchronous mode (Z-TWS4, Z-PASS2-S, S6001-RTU) *)
LINUX_SHELL (* Execute a command in a Linux shell (Z-TWS4, Z-PASS2-S, S6001-RTU) *)
MODEM_CTRL (* Execute a generic AT command (Z-TWS4, Z-PASS2-S, S6001-RTU) *)
MODEM_ONOFF (* Power on/off the Modem (Z-MINIRTU) *)
MODEM_RESET (* Execute a modem reset (Z-TWS4, Z-PASS2-S, Z-MINIRTU) *)
NTP_CFG (* Configure NTP (Z-MINIRTU, Z-TWS11) *)
NTP_CFG_READ (* Get the NTP configuration (Z-MINIRTU, Z-TWS11) *)
PLAY_WAVE (* Execute an audio PCM file (Z-MINIRTU, Z-TWS11) *)
PPP_CONNECT (* PPP connection setup/release (Z-TWS4, Z-PASS2-S, Z-MINIRTU, S6001-RTU) *)
PPP_STATUS (* PPP connection status (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)
PUT_ALARM (* Store an alarm into the DB. *)
RESET (* Reset the device (Z-MINIRTU, Z-TWS11) *)
SEND_MAIL (* Send an e-mail (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)
SEND_SMS (* Send an SMS (Z-TWS4, Z-PASS2-S, Z-MINIRTU, S6001-RTU) *)
SET_ALARMS_STAT (* Set the status of the specified alarms in the DB. *)
TIME_SYNC (* Time synchronization by means of NTP protocol (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)
TOT_SET (* Set totalizer value (Z-MINIRTU, Z-TWS11) *)
TXBAPPENDFILE (* Append a Text Buffer to a file *)
WEBSRV_CFG (* Configure the web server (Z-MINIRTU, Z-TWS11) *)
WEBSRV_CFG_READ (* Get the web server configuration (Z-MINIRTU, Z-TWS11) *)

Save the library (“File / Save Library” menu).

The procedure for adding the Profiles library to the IDE is identical to the one just explained; the only difference is that the SenecaStratonProfiles.XL5 file must be selected (instead of the SenecaStratonLibrary.XL5 file).

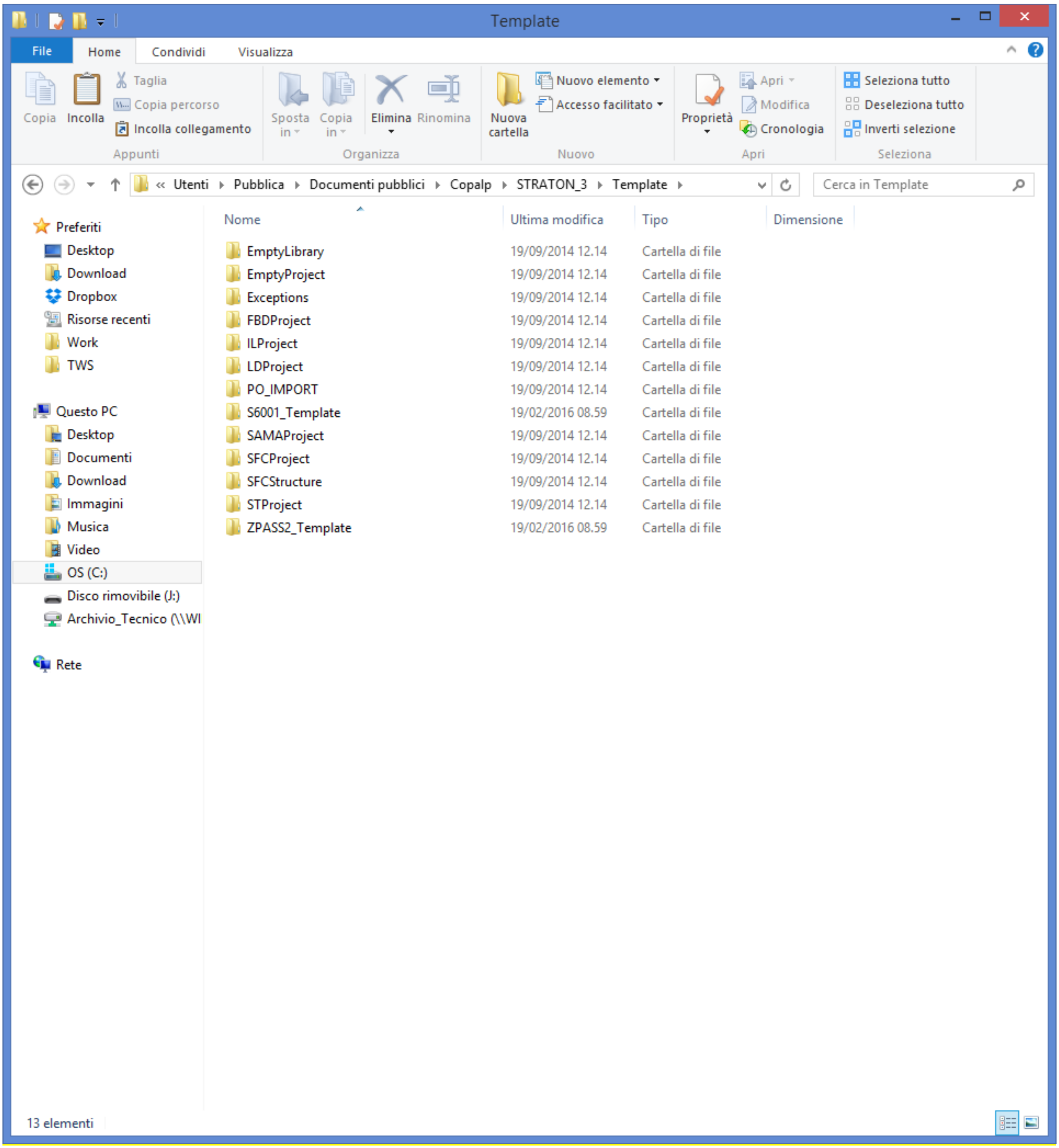
Now that the "low level" FBs are available, we need to install the UDFB library.
The UDFB library is provided as a zip file.

The TWS_MISC folder, contained in the zip file, must be copied to the following directory:
C:\Users\Public\Documents\Copalp\STRATON\LIBS:



Nome	Ultima modifica	Tipo	Dimensione
FBD_with_ENENO	19/09/2014 12.14	Cartella di file	
IntCounters	19/09/2014 12.14	Cartella di file	
SAMA	19/09/2014 12.14	Cartella di file	
TWS_MISC	25/11/2015 09.11	Cartella di file	

The template folders must be copied to the following directory:
C:\Users\Public\Documents\Copalp\STRATON\Template



Nome	Ultima modifica	Tipo	Dimensione
EmptyLibrary	19/09/2014 12.14	Cartella di file	
EmptyProject	19/09/2014 12.14	Cartella di file	
Exceptions	19/09/2014 12.14	Cartella di file	
FBDProject	19/09/2014 12.14	Cartella di file	
ILProject	19/09/2014 12.14	Cartella di file	
LDProject	19/09/2014 12.14	Cartella di file	
PO_IMPORT	19/09/2014 12.14	Cartella di file	
S6001_Template	19/02/2016 08.59	Cartella di file	
SAMAProject	19/09/2014 12.14	Cartella di file	
SFCProject	19/09/2014 12.14	Cartella di file	
SFCStructure	19/09/2014 12.14	Cartella di file	
STProject	19/09/2014 12.14	Cartella di file	
ZPASS2_Template	19/02/2016 08.59	Cartella di file	

20.2. ENERGY MANAGEMENT PROTOCOLS

The Straton PLC supports the following “Energy Management” protocols (optional):

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

The activation of these protocols is based on a license.

Please contact Seneca for more information on licensing Energy Management Protocols.

20.3. SNMP V2C PROTOCOL

Straton PLC supports theV2C version SNMP protocol. For more information, refer to the Straton manual.

21. R-COMM OPTION (R-PASS MODEL ONLY)

For the R-PASS models it is possible to purchase the R-COMM hardware which allows (depending on the model) to add a 4G modem with GNSS positioning and a UPS which allows the R-PASS to operate up to 1 hour without external power supply.

For the installation of R-COMM refer to the R-COMM installation manual, for the available models refer to the Seneca website.

22. CONFIGURATION VUA WEB SERVER (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

The devices can be fully configured via a series of web configuration pages.

To access the configuration site, you need to connect your browser to the IP address on port 8080, e.g.:

http://192.168.90.101:8080

and, when required, provide the following credentials (default values):

Username: admin

Password: admin

Once authentication is successfully checked, the "Summary" page is visualized, following all the configuration sections will be described.

22.1. SUMMARY

This page shows the main information about the status of the device and the user currently logged in.

22.2. NETWORK AND SERVICES

The following table lists all the configuration parameters available on this page, with a brief explanation and the default value of each parameter.

Field	Meaning
NETWORK	Section dedicated to the network parameters configuration of the Ethernet LAN/WAN ports.
WEB SERVER	Section dedicated to web server configuration.
FILE TRANSFER	Section dedicated to FTP protocol configuration

NETWORK REDUNDANCY Enable	Allows you to enable network redundancy by setting the WAN port as primary network and the WI-FI port as secondary. For SSD there must be a Wi-Fi.
NETWORK REDUNDANCY Ping Address	Address that the system uses to check connectivity. This address must be different from the one set for the "DNS Server" parameter, otherwise an error will be displayed.
WATCHDOG Enable	Enable or disable the Watchdog in the device
WATCHDOG Timeout (s)	Watchdog timeout, in seconds; when the watchdog is enabled, if it is not updated for this interval of seconds, the system will restart. Possible values are in the range [30..3600 s].
R-COMMM Available	Configure whether or not operation with the R-COMM option is active
R-COMM UPS Mode	Configures the UPS type of operation. Important: Check that the R-COMM model purchased has the "UPS" function before configuring these parameters. If the R-COMM purchased does not include the UPS, this parameter must be set to "OFF". OFF, Shutdown immediately, Shutdown on low power. “OFF” does not use R-COMM UPS to power R-PASS “Shutdown immediatly” in case of mains power failure closes the log files and performs a clean shutdown of R-PASS “Shutdown on low power” in case of a mains power failure R-PASS continues to work as long as the battery is charged, when it is discharging it closes the log files and performs a clean shutdown of R-PASS
DEBUG LOGS Enable	Flag to enable/disable the debug logs

22.3. PLC (R-PASS-S, Z-TWS4-RT-S, Z-PASS2-RT-S MODELS ONLY)

On this page it is possible to set the connection parameters with the Straton workbench, activate an optional license (for example for energy management protocols) and set the operation of the COM1 serial port between Rs232/RS485/Z-MBUS.
Z-MBUS is an optional device that allows you to connect the device to a METERBUS

22.4. WI-FI CONFIGURATION (R-PASS MODEL ONLY)

Allows you to configure the WI-FI port parameters.
Below is an extract of the main parameters:

Field	Meaning
Mode	You can select from: OFF: The WI-FI port is off Station: The WI-FI is connected to an existing network Access Point: The device creates a new WI-FI network to which devices can

	connect
SSID	If Mode is "Access Point" you can define the name of the new WI-FI network that the device will create. If Mode is valid "Station" displays the SSID of the network you are connected to.
KEY MODE	Represents the encryption protocol to be used.
SCAN/APPLY	Allows, in Station mode, to select the WI-FI to connect to

22.5. SERIAL PORTS (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This page allows you to configure the serial ports (baud rate, stop bits, RS232/RS485 configurations etc…).

22.6. I/O CONFIGURATION

Field	Meaning
IO CONFIGURATION	
INPUT/OUTPUT1 MODE	Remote connection disable Allows you to use the pin as input. If high blocks remote VPN access General Input Allows you to use the pin as a digital input General Output Allows you to use the pin as Digital Output
INPUT/OUTPUT2 MODE	Remote connection active Allows you to use the pin as an output, if active it indicates the presence of remote VPN access. Local Alarm: is an input that is connected to a control PLC, when it is high it indicates a general error that is visible remotely via the Seneca VPN box status interface. Remote Toggle is an output controllable from the Seneca VPN box status interface. General Input Allows you to use the pin as a digital input General Output Allows you to use the pin as Digital Output
SECURITY LEVEL	

Service Disable	This parameter defines which access services are disabled when the "Remote Connection Disable" digital input is HIGH. The possible values are: Blocking VPN Connection (VPN Service and Internet active) VPN Service blocking (Internet active) Blocking of internet access (both internet and VPN are blocked in the device)

22.7. REAL TIME CLOCK SETUP

Field	Meaning
NTP	
Enable	Flag to enable/disable date/time synchronization with a Network Time Protocol server
Server primary	IP address or FQDN20 of the NTP primary server
Secondary server	IP address or FQDN20 of the NTP secondary server
Timezone	Time zone

22.8. GATEWAY CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This page allows to configure the type of Ethernet-Serial Gateway you want to use.
It is possible to choose between:

Modbus Ethernet to Serial (Real time conversion)
Modbus with Memory
Transparent

22.8.1. GATEWAY ETHERNET TO SERIAL

Field	Meaning
Enable	Flag to enable / disable Modbus gateway functionality from Ethernet to serial on the port
Port	TCP port to access Modbus from Ethernet to Serial Gateway If three distinct values are set, several instances of the Gateway are executed, each of which manages a single serial port. If the same port value is set for more than one serial port, the same Gateway instance will manage two or more serial ports (depending on the device), i.e. Modbus RTU requests will be sent simultaneously to the serial ports.
Response Wait Time	Timeout when receiving Modbus RTU responses The value is in milliseconds; possible values are in the range [10 - 10000] ms.
Slave ID for Embedded I/O	Slave ID used to access the Modbus registers corresponding to the digital I/Os of the device (if any) this ID can also be used to access the Modbus registers containing GNSS positioning information. Possible values: [1..255] in devices that are equipped with them. Only valid for Serial to Ethernet mode.

22.8.2. TRANSPARENT GATEWAY

For each serial port with "Gateway Mode" = "Transparent", the available configuration parameters depend on the value of the "Operating Mode" parameter selected for the port.
The possible values for the "Operating Mode" parameter are:

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

Moreover, for the "Serial Tunnel" operating modes, the available parameters depend on the "Tunnel Role" (Master or Slave).
The following tables describe the relevant parameters for the various operating modes.

22.8.2.1. VIRTUAL COM

Field	Meaning
Listen Port	TCP port to access the transparent gateway
Data Packing Interval	Time interval used as a criterion for packing the data bytes received from the serial port, before sending them to the network; that is, if no packet is received for this time, the available bytes are sent to the network. The value is in milliseconds; possible values are in the range [0 - 1000].

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

Field	Meaning
Destination address	The IP address to which the transparent gateway will connect
Destination port	The TCP / UDP port to which the transparent gateway will connect

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

Field	Meaning
Destination Port	The UDP port to which the packets will be sent
Multicast Group	IP address that identifies the Multicast group
Multicast Interface	Network interface to which UDP packets are sent; possible values: Ethernet | VPN; The "VPN" option is only available when VPN is active

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

Field	Meaning
Listen Port	The UDP port from which the packets will be received
Multicast Group	IP address that identifies the Multicast group
Multicast Interface	Network interface from which UDP packets are received; possible values: Ethernet | VPN; The "VPN" option is only available when VPN is active

22.8.3. MODBUS GATEWAY WITH SHARED MEMORY (TO BE USED FOR DATALOGGERS AND LOGICS)

Field	Meaning
Enable	This parameter enables/disables the Modbus Shared Memory Gateway service. It is important to note that when this parameter is set to OFF, the service is not running even if some serial ports are assigned to it.
TCP Port	Listening port for the Modbus TCP server
TCP Connections Max Number [1-50]	Maximum number of TCP connections that can be accepted by the Modbus TCP server
Response Mode when Resource in Fail	This parameter defines how the response to a Modbus request (read) is constructed for a tag corresponding to an unresponsive Modbus station; when mode is “Tag error value”, the value in the Modbus response is given according to the "Error Mode" / "Error Value" parameters in the tag definition; when the mode is "Exception", the response contains an exception with value 11 ("The gateway target device failed to respond").
Diagnostic Area Type	Select whether diagnostics can be accessed via Holding or Input Modbus Registers.
Diagnostic Area Address	The diagnostic area reserves one bit for each tag (125 registers): Bit value on 0 -> means Tag reading error (or tag not configured) The bit value on 1 -> means Reading tag OK Therefore, if you need to check the error status of the first 10 tags using the default area (9001 Holding Registers), you must read the 49001 registry. For example if the value of the regsiter is: 0x3DB = 987 = 0000 0011 1101 1011 Tag 1 = OK Tag 2 = OK Tag 3 = FAIL Tag 4 = OK Tag 5 = OK Tag 6 = FAIL ... Note that one register before and one register after the diagnostic area will be reserved (by default registers 49000 and 49126).

Therefore, for each serial port with "Gateway Mode" = "Modbus Shared Memory", the parameters described in the following table are available.

Field	Meaning
Task	This parameter defines which type of Modbus Shared Memory Gateway task is running on the serial port; the possible values are: None, Master, Slave
Slave Address	Interval between Modbus RTU requests, in milliseconds (available only when Task = Master)
Timeout (ms) [10 – 10000]	Response timeout for Modbus RTU requests, in milliseconds (available only when Task = Master)
Delay between Polls (ms) [10 – 1000]	Interval between Modbus RTU requests, in milliseconds (available only when Task = Master)
Read/Write Retries [0 – 10]	Maximum number of retries for Modbus RTU requests; this always applies to write requests; for read requests, it only applies to tags with "Gateway Tag Mode" = "BRIDGE"
Multiple Read Max Number [1 – 32]	Maximum number of Modbus registers that can be read in a single Modbus RTU request; it is used to reduce the number of read requests sent on the serial bus, thus performing optimization
Multiple Write Max Number [1 – 32]	Maximum number of Modbus registers that can be written in a single Modbus RTU request; it is used to reduce the number of write requests sent on the serial bus, thus performing optimization

22.9. VPN CONFIGURATION

The VPN connection can be configured as SENECA VPN BOX or OPEN VPN.

22.9.1. OPEN VPN

22.9.1.1. CONFIGURATION FILE

This file must contain all the information needed to configure the Open VPN functioning, the main configuration options are:
- whether the device will function as a client or server (generally, it will be a client)
- the transport protocol (UDP or TCP)
- the IP address of the server / host name and port
- the files needed to perform authentication procedures
- etc...

This file has the extension ovpn (on Windows systems) or the extension .conf (on Linux systems); regardless of its original name, it will be renamed as ovpn.conf on the device.
This is the only mandatory file, i.e. if this file has not been uploaded to the device the VPN cannot be enabled.
As mentioned in the Web page, in the options that require a file argument, only the file name, without path, must be provided, as in the following example:

```
ca ca.crt                     OK

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

Two other important rules that must be followed are:
- the "dev" option must be: "dev tun0" or "dev tap0".
- the "log" option must be omitted (so that logs are written to syslog)

22.9.1.2. CA CERTIFICATE

This file must contain the certificate of the certification authority (CA) and has the extension .crt.
This is required when the configuration file contains the "ca" option.

22.9.1.3. CLIENT CERTIFICATE

This file must contain the client certificate and has the extension .crt.
This is required when the configuration file contains the "cert" option.

22.9.1.4. CLIENT KEY

This file must contain the client key and has the extension .key.
This is required when the configuration file contains the "key" option.

22.9.1.5. ADDITIONAL FILE

This file can be of any type and may be required for configuration options other than "ca", "cert" and "key".
Note that you can upload more than one additional file.
You can browse your PC to select the files above and send them to the device by pressing the "UPLOAD" button.
When loading is complete, a results page is displayed
You can check which VPN files are stored on your device by clicking the "SHOW VPN STATUS" button,

As the web page recalls, VPN files can be downloaded from the device, if necessary, via FTP / SFTP; they can be found in the /home/config/vpn directory.

You can clear all VPN files by clicking the “RESET” button; a pop-up will appear, asking for confirmation.

When you click the "SHOW VPN STATUS" button, a third section, called "VPN Status", is displayed:
- The "Connection Status" of the VPN (i.e. "Stopped" or "Running")
- the IP address assigned to the VPN interface when "Connected", the "dummy" IP address "0.0.0.0" when "Disconnected".
- the "OpenVPN Status" (i.e.: "Stopped" or "Running")

- the number of packets / bytes received by the VPN interface when connected; "0/0" when disconnected
- the number of packets / bytes sent to the VPN interface when connected; "0/0" when disconnected
- VPN files stored on the device

Important status information is given by the "OpenVPN Status" field; if the VPN is enabled ("ON"), but this status is "Stopped", this means that the Open VPN process cannot be started correctly: probably, the configuration file contains some errors or, perhaps, some options not supported by the OpenVpn implementation of the device.
You can update the VPN status by clicking the "REFRESH" button.
Finally, you can hide the "VPN Status" section by clicking the "HIDE VPN STATUS" button.

22.9.1.6. CONFIGURATION FILE FOR USE AS OPENVPN SERVER

This paragraph provides an example of OpenVPN server configuration.

```
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. CONFIGURATION FILE FOR USE AS OPENVPN CLIENT

This paragraph provides an example of OpenVPN server configuration.

```
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

Field	Meaning
VPN BOX/Enable	Flag to enable / disable the "VPN Box" feature, i.e. the procedure / protocol that allows the device to configure the VPN, interacting with the "VPN Box" server (see "VPN Box User Manual")
VPN BOX/Server	IP or FQDN address of the "VPN Box" server
VPN BOX/Password	Password to access the "VPN Box" server
VPN BOX/Tag Name	Mnemonic name used to uniquely identify the device

When you click the "SHOW VPN STATUS" button, a new section called "VPN Status" is displayed:
- VPN connection status
- the VPN IP address assigned to the device this line is not displayed for the VPN "Point-to-Point (L2)" box, as no IP address is assigned to the VPN interface
- the status of OpenVPN
- the number of packets / bytes received by the VPN interface
- the number of packets / bytes sent to the VPN interface
• the Type of VPN BOX, which can be "Point-to-Point", "Point-to-Point (L2)" or "Single LAN"
• the status of the VPN BOX, if the VPN box is enabled
- the user name of the connected user, if any
The following table gives a brief explanation of the possible "Result" and "Status" strings:

Result	Status	Meaning
Error (Unexpected response)		A response code has been received that is not managed by the device (should never occur)
Error (No response from VPN Box)		No response received from VPN Box (response timeout)
Error (Invalid response from VPN Box)		A response was received whose content is not valid for the device (should never occur)
Error (Wrong password)		The password set on the device is incorrect
Error (License Limit Reached)		The maximum number of devices allowed by the license is already registered on VPN Box
Error (VPN Box not configured)		The VPN Box has not yet been configured
Error (Generic error)		A generic error has occurred on VPN Box

OK		The device has just been registered on VPN Box
OK	New	The device is registered on VPN Box, but not yet configured (only "single LAN")
OK	Configuration updated	The device configuration has just been updated
OK	Configured	The device is correctly configured and available for VPN connection
OK	Ban	The device has been "banned
OK	Not found	The device is not known to VPN Box; this happens when the device registration is deleted on VPN Box
OK	Unknown	The device has an unknown status in VPN Box (should never occur)
OK	Not bound	The "tunnel" between device and VPN Box is not active; this may occur when the tunnel port is blocked (not open) in the ADSL router on the VPN Box side (only "Point-to-Point")
OK	Unexpected status	A status code has been received that is not managed by the device (should never occur)

22.10. OPC-UA SERVER CONFIGURATION

In this page, you can set the parameters related to the OPC Unified Architecture (OPC-UA) server, as listed in the following table:

Field	Meaning
Enable	Enable/Disable OPC-UA server
Port	Server port
Username	Username for server access
Password	Password for server access
Security Policy	"None" "Basic128Rsa15" "Basic256Sha256" Note: a predefined pair of certificates is already included in the product.

You can add your certificates with the appropriate buttons
Note that a client must use the following URL to access the OPC-UA server:
opc.tcp://IP_ADDR:PORT/
Where
IP_ADDR is the IP address of the OPC-UA server (the device itself).
PORT is the TCP port configured for the OPC-UA server

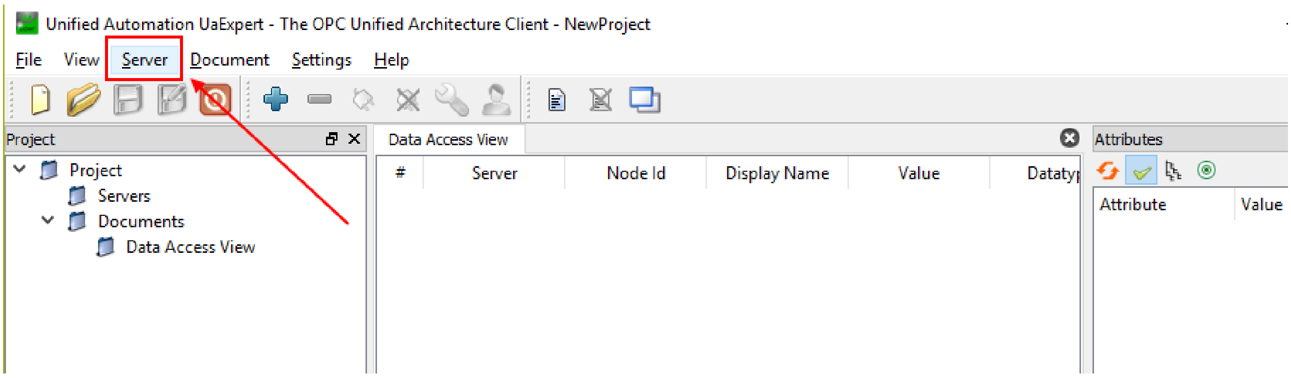
The device's OPC-UA server "exports" the Modbus Shared Memory Gateway tags; therefore, using an OPC-UA client software, it is possible to read / write tags using the OPC-UA protocol.

NOTE: for all variables on the OPC-UA server the namespace-id is set to "1".

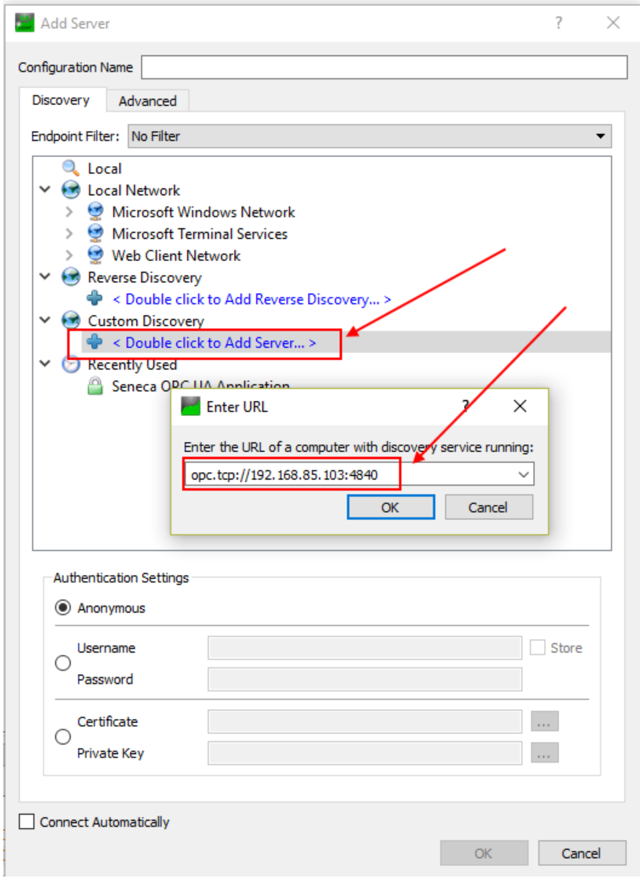
22.10.1. UA EXPERT CLIENT CONFIGURATION

This chapter will help you to configure the connection and the correct security policy with the UA Expert Client software

Click on Select server-> Add

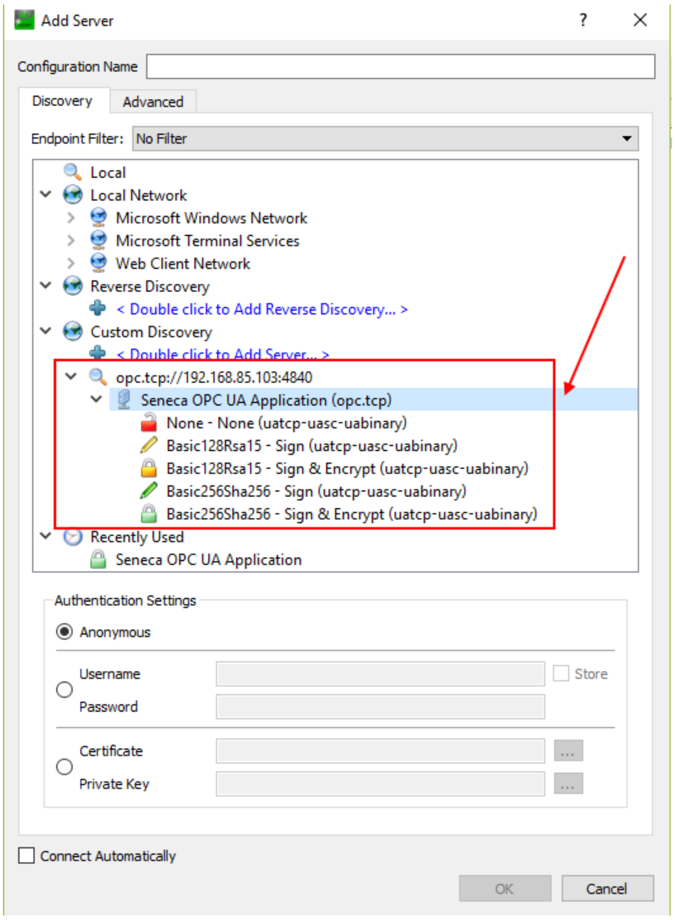


In "Custom Discovery" enter the url for the OPC-UA server:



opc.tcp://192.168.85.103:4840

Press OK.
Supported security policies are now displayed:



Add Server

Configuration Name

Discovery | Advanced

Endpoint Filter: No Filter

- Local
- Local Network
  - Microsoft Windows Network
  - Microsoft Terminal Services
  - Web Client Network
- Reverse Discovery
  - < Double click to Add Reverse Discovery... >
- Custom Discovery
  - < Double click to Add Server... >
  - opc.tcp://192.168.85.103:4840
    - Seneca OPC UA Application (opc.tcp)
      - None - None (uatcp-uasc-uabinary)
      - Basic128Rsa15 - Sign (uatcp-uasc-uabinary)
      - Basic128Rsa15 - Sign & Encrypt (uatcp-uasc-uabinary)
      - Basic256Sha256 - Sign (uatcp-uasc-uabinary)
      - Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary)
- Recently Used
  - Seneca OPC UA Application

Authentication Settings

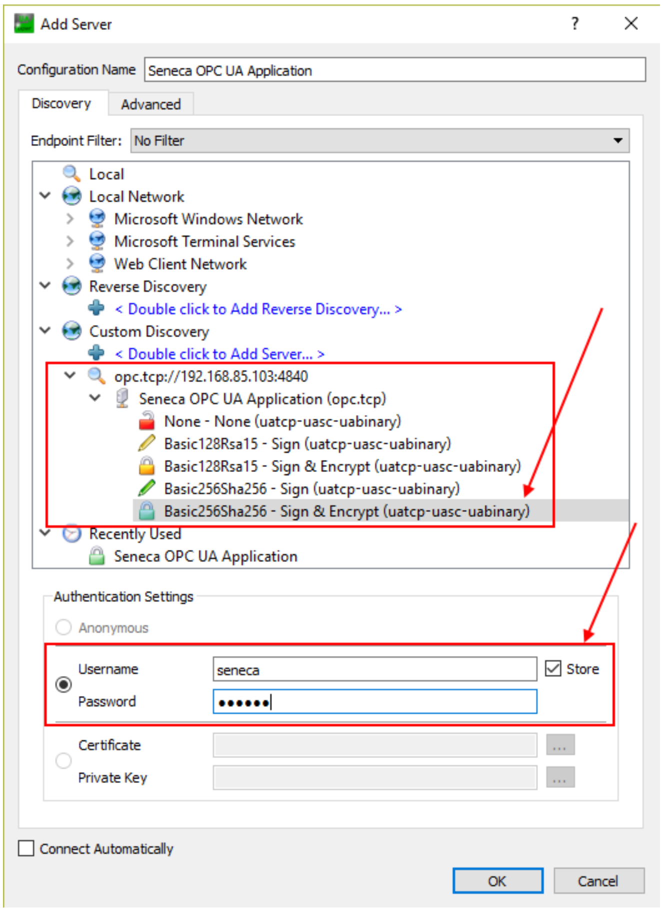
● Anonymous

○ Username / Password □ Store

○ Certificate / Private Key

□ Connect Automatically

Select the one to use. Then go to Authentication settings and enter the user name and password configured in the OPC-UA server:



Add Server

Configuration Name: Seneca OPC UA Application

Endpoint Filter: No Filter

- Local
- Local Network
  - Microsoft Windows Network
  - Microsoft Terminal Services
  - Web Client Network
- Reverse Discovery
  - < Double click to Add Reverse Discovery... >
- Custom Discovery
  - < Double click to Add Server... >
  - opc.tcp://192.168.85.103:4840
    - Seneca OPC UA Application (opc.tcp)
      - None - None (uatcp-uasc-uabinary)
      - Basic128Rsa15 - Sign (uatcp-uasc-uabinary)
      - Basic128Rsa15 - Sign & Encrypt (uatcp-uasc-uabinary)
      - Basic256Sha256 - Sign (uatcp-uasc-uabinary)
      - Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary)
- Recently Used
  - Seneca OPC UA Application

Authentication Settings

○ Anonymous

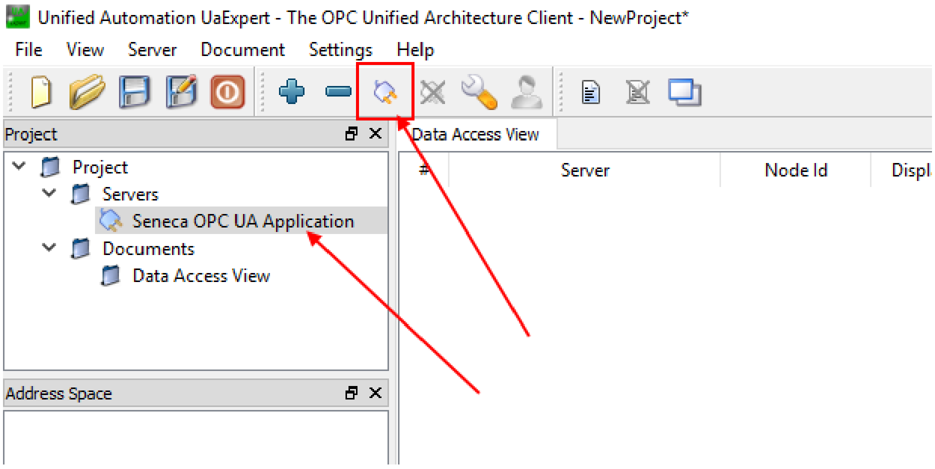
● Username: seneca ☑ Store
Password: ••••••

○ Certificate / Private Key

☐ Connect Automatically

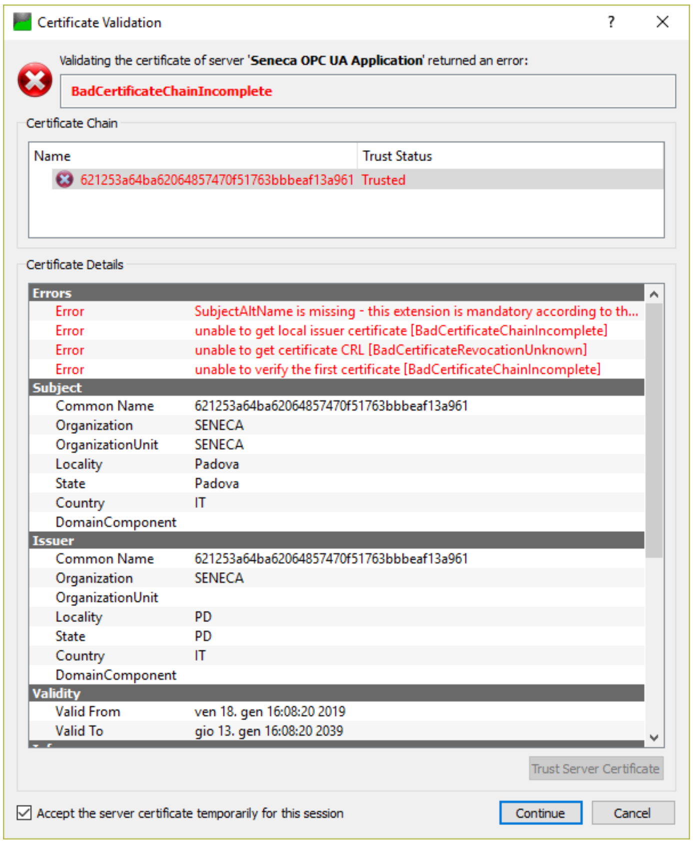
Press OK:

Now it is possible to connect to the server using the appropriate icon:



Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject*

A new server certificate validation dialog will open. After reviewing the certificate, select Trust Server Certificate to permanently add the certificate to UaExpert's trust list. It is also possible to check the appropriate box to temporarily accept the server certificate for this session and choose Continue to not save the certificate to the trusted list or select Cancel to reject the certificate.



Certificate Validation

Validating the certificate of server '**Seneca OPC UA Application**' returned an error:

BadCertificateChainIncomplete

Certificate Chain

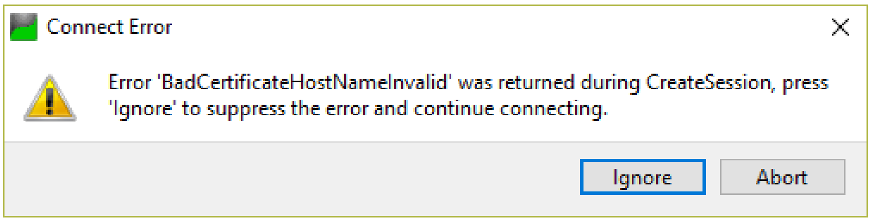
Name	Trust Status
621253a64ba62064857470f51763bbbeaf13a961	Trusted

Certificate Details

Errors	
Error	SubjectAltName is missing - this extension is mandatory according to th...
Error	unable to get local issuer certificate [BadCertificateChainIncomplete]
Error	unable to get certificate CRL [BadCertificateRevocationUnknown]
Error	unable to verify the first certificate [BadCertificateChainIncomplete]
Subject	
Common Name	621253a64ba62064857470f51763bbbeaf13a961
Organization	SENECA
OrganizationUnit	SENECA
Locality	Padova
State	Padova
Country	IT
DomainComponent	
Issuer	
Common Name	621253a64ba62064857470f51763bbbeaf13a961
Organization	SENECA
OrganizationUnit	
Locality	PD
State	PD
Country	IT
DomainComponent	
Validity	
Valid From	ven 18. gen 16:08:20 2019
Valid To	gio 13. gen 16:08:20 2039

☑ Accept the server certificate temporarily for this session

The Certificate Error window will now appear:

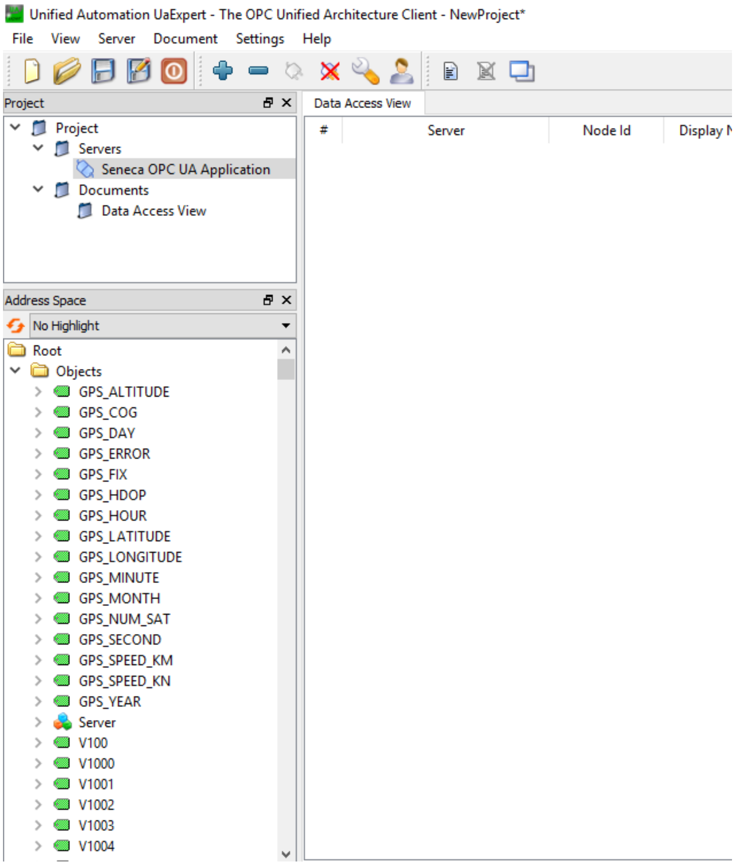


Connect Error

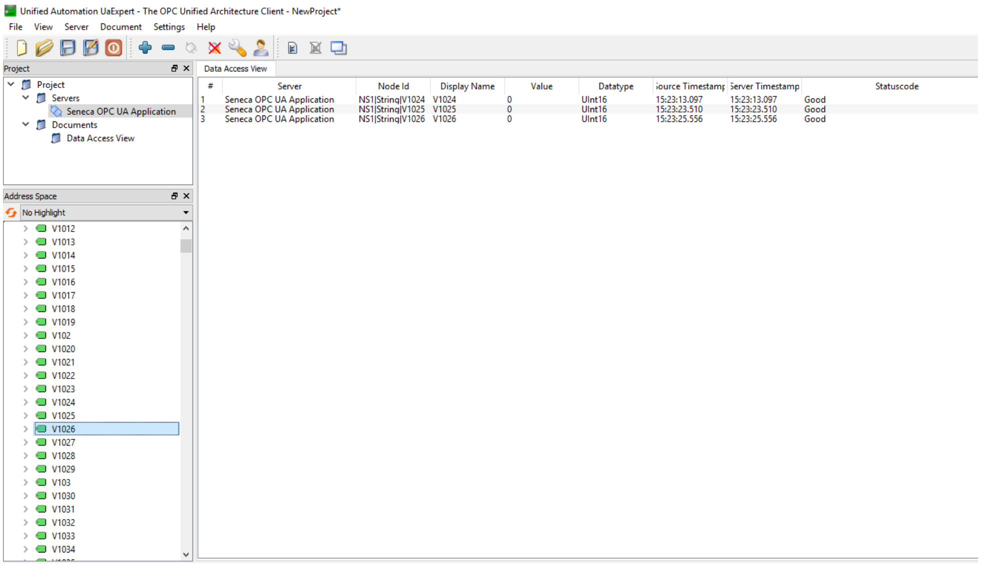
Error 'BadCertificateHostNameInvalid' was returned during CreateSession, press 'Ignore' to suppress the error and continue connecting.

Click on "Ignore" to continue.

Now the connection is established, you can read/write the value of the tags



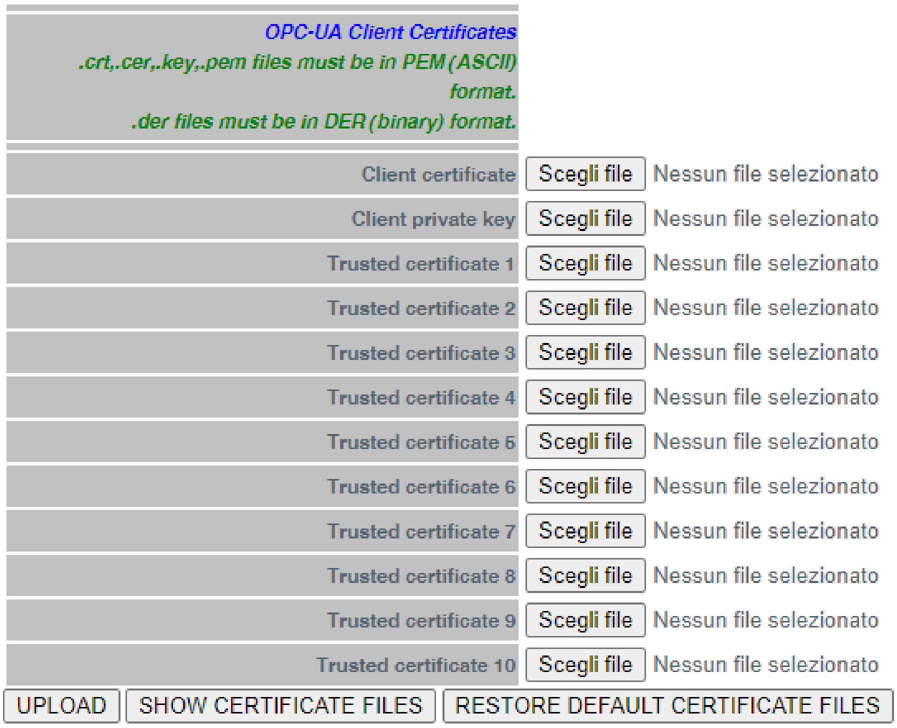
To update the tags in real time, drag and drop with the tags you want to display.



#	Server	Node Id	Display Name	Value	Datatype	;ource Timestamp	;erver Timestamp	Statuscode
1	Seneca OPC UA Application	NS1|String|V1024	V1024	0	UInt16	15:23:13.097	15:23:13.097	Good
2	Seneca OPC UA Application	NS1|String|V1025	V1025	0	UInt16	15:23:23.510	15:23:23.510	Good
3	Seneca OPC UA Application	NS1|String|V1026	V1026	0	UInt16	15:23:25.556	15:23:25.556	Good

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

In this section you can upload the server connection certificates for the OPC-UA client.



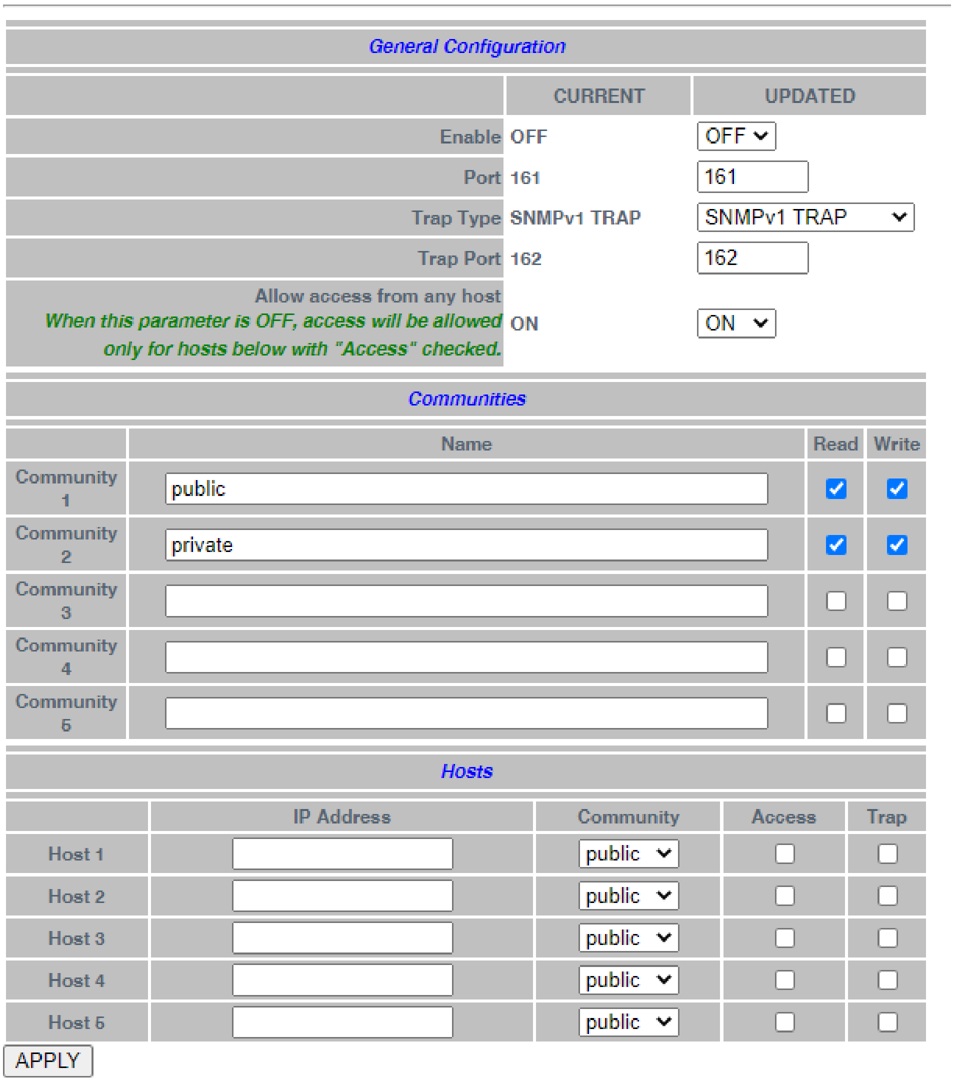
OPC-UA Client Certificates
.crt,.cer,.key,.pem files must be in PEM (ASCII) format.
.der files must be in DER (binary) format.

Client certificate	Scegli file	Nessun file selezionato
Client private key	Scegli file	Nessun file selezionato
Trusted certificate 1	Scegli file	Nessun file selezionato
Trusted certificate 2	Scegli file	Nessun file selezionato
Trusted certificate 3	Scegli file	Nessun file selezionato
Trusted certificate 4	Scegli file	Nessun file selezionato
Trusted certificate 5	Scegli file	Nessun file selezionato
Trusted certificate 6	Scegli file	Nessun file selezionato
Trusted certificate 7	Scegli file	Nessun file selezionato
Trusted certificate 8	Scegli file	Nessun file selezionato
Trusted certificate 9	Scegli file	Nessun file selezionato
Trusted certificate 10	Scegli file	Nessun file selezionato

The "Choose File" button selects the certificate. These are only uploaded to the device after pressing the "Upload" button.
The "Show Certificate Files" button allows you to view the uploaded certificate files.
The "Restore Default Certificate Files" button allows you to restore the default certificate files.

22.12. SNMP CONFIGURATION (R-PASS-S, Z-PASS2-RT-S, Z-TWS4-RT-S MODELS ONLY)

This section describes the configuration of the SNMP Agent.
The SNMP V2C version is supported.



General Configuration

	CURRENT	UPDATED
Enable	OFF	OFF
Port	161	161
Trap Type	SNMPv1 TRAP	SNMPv1 TRAP
Trap Port	162	162
Allow access from any host *When this parameter is OFF, access will be allowed only for hosts below with "Access" checked.*	ON	ON

Communities

	Name	Read	Write
Community 1	public	☑	☑
Community 2	private	☑	☑
Community 3		□	□
Community 4		□	□
Community 5		□	□

Hosts

	IP Address	Community	Access	Trap
Host 1		public	□	□
Host 2		public	□	□
Host 3		public	□	□
Host 4		public	□	□
Host 5		public	□	□

Field	Meaning
Enable	Enables or disables the protocol
Port	Port used by the SNMP protocol
Trap Type	Selects the type of Trap to use
Trap Port	Port used by Traps
Allow access from any host	Allows any host to access

Communities: Name	Community identifier
Communities: Read	Provides Read properties to the selected Community
Communities: Write	Provides Write properties to the selected Community
Hosts: IP Address	Allows you to define the Host IP
Hosts: Community	Allows you to define which community the Host is associated with
Hosts: Access	If Flagged, it allows the host to access the SNMP Agent
Hosts: Trap	If Flagged, it allows the host to receive Traps from the SNMP Agent

22.13. USERS CONFIGURATIONS

This section shows the configuration (user/password) of all the accounts available for access to the Webserver and the Display:

ADMINISTRATOR
It is the account that allows each operation

GUEST
It is the account that allows you to access all the pages except for the "FW Upgrade" and "Configuration Management" pages, displaying all the configuration parameters and status information, without being able to modify any parameter; therefore, in all pages, the "APPLY" buttons (and any other button used to make changes) are disabled.

USER
It is the account that allows access only to the "Summary" and "tag view" pages (and web pages only, it has no access to the display).

FTP USER
This is the account for accessing the FTP server of the device.

22.14. ROUTER CONFIGURATION

On this page you can change the parameters related to the functionality of the router.

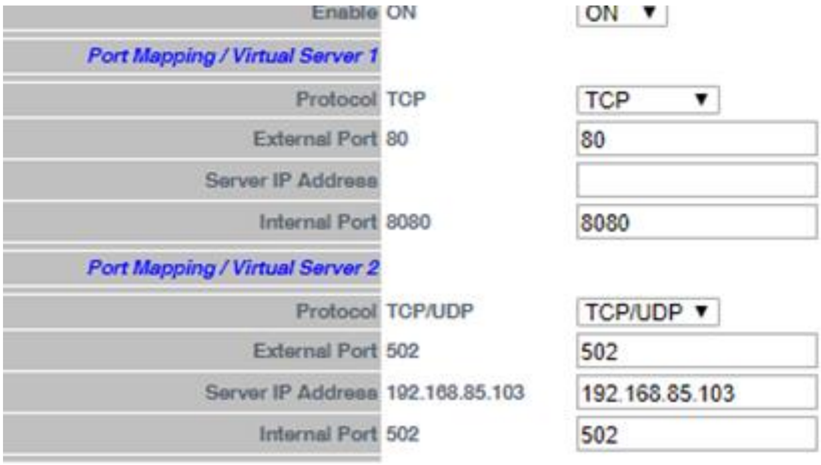
Field	Meaning
Router Enable	Enable/Disable router functionality
DNS Enable	Flag to enable/disable the DNS forwarding service

DHCP Server Enable	Flag to enable / disable DHCP service (DHCP server)
DHCP First Address DHCP Last Address	These parameters define the range of IP addresses assigned by the DHCP server to requesting clients
DHCP Lease Time (min)	Validity time interval for IP address assignment, in minutes. Possible values are in the range [1..60].
Use Local Addresses Through VPN/Enable	Flag to enable/disable access to the device and others that are connected to the LAN, using their local IP (LAN) addresses

Finally, there are the port mapping rules (also known as "virtual servers"), the parameters of each are:

Field	**Meaning**
Protocol	This parameter defines the transport protocol (or port type) affected by the rule: TCP, UDP or both
External Port	TCP or UDP port to which a packet was originally sent
Server IP Address	IP address to which the received packet is forwarded
Internal Port	TCP or UDP port to which the received packet is forwarded

In this example 2 rules have been set:



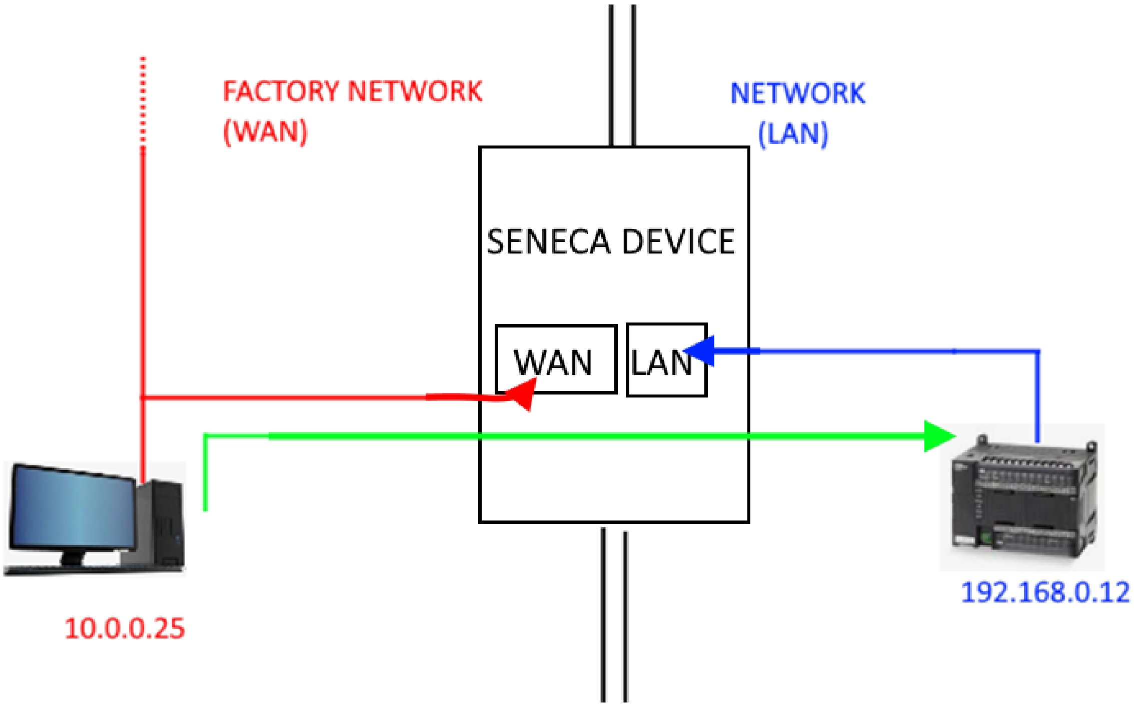
Enable	ON	ON ▼
Port Mapping / Virtual Server 1		
Protocol	TCP	TCP ▼
External Port	80	80
Server IP Address		
Internal Port	8080	8080
Port Mapping / Virtual Server 2		
Protocol	TCP/UDP	TCP/UDP ▼
External Port	502	502
Server IP Address	192.168.85.103	192.168.85.103
Internal Port	502	502

• the first rule tells the device that any TCP packet received on port 80 (HTTP) must be forwarded to port 8080, leaving the original destination IP address unchanged; therefore, this rule allows access to the configuration website on the standard HTTP port (80);

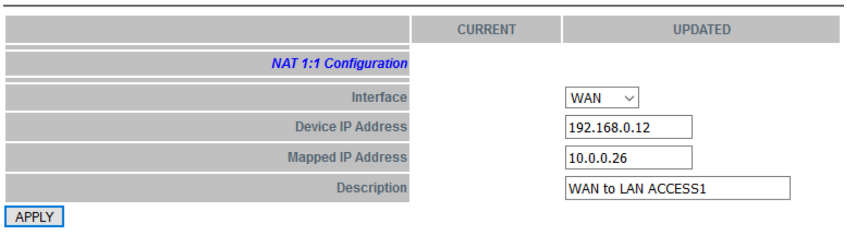
- The second rule means that any TCP or UDP packets received on port 502 (which is often used for Modbus TCP) must be forwarded to LAN IP address 192.168.85.103 (which corresponds to another device) on the same destination port (502).

22.15. NAT 1:1 RULES

This function allows to access to a device connected to the LAN Port (for example) from the WAN (a PC in the WAN that needs to obtain data from a PLC in the LAN):



It is necessary to create a new address (10.0.0.26) which is located on a PC-compatible network (10.0.0.25).



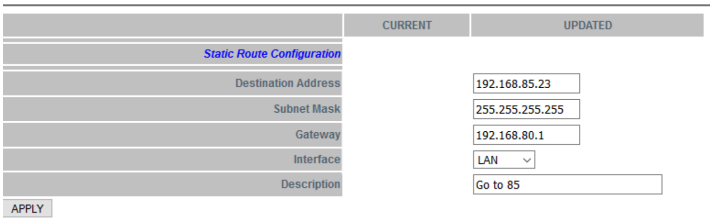
	CURRENT	UPDATED
NAT 1:1 Configuration		
Interface		WAN
Device IP Address		192.168.0.12
Mapped IP Address		10.0.0.26
Description		WAN to LAN ACCESS1

PLC 192.168.0.12 is now accessible from the WAN using address 10.0.0.26.

22.16. STATIC ROUTES

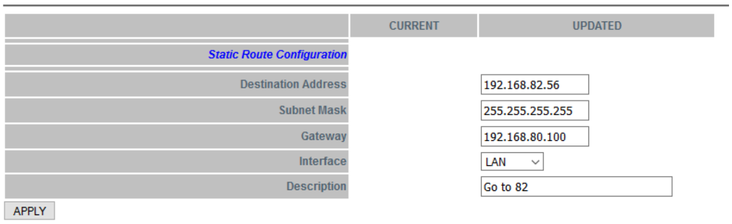
Use this function to route an address or range of addresses to different gateways.
For example, if you need to reach 2 different addresses: 192.168.85.23 and 192.168.82.56 but you need to go through 2 different gateways.

For example, you have:
1) To access 192.168.85.23 it is necessary to pass through gateway 192.168.80.1
2) To access 192.168.82.56 it is necessary to pass through gateway 192.168.80.100
You will have to use the configuration:



	CURRENT	UPDATED
Static Route Configuration		
Destination Address		192.168.85.23
Subnet Mask		255.255.255.255
Gateway		192.168.80.1
Interface		LAN
Description		Go to 85

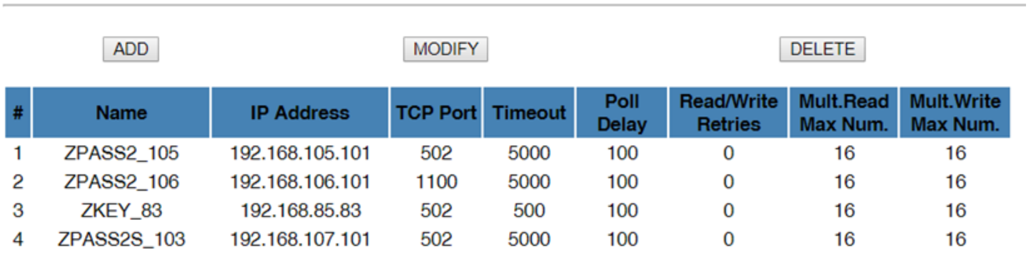
And also:



	CURRENT	UPDATED
Static Route Configuration		
Destination Address		192.168.82.56
Subnet Mask		255.255.255.255
Gateway		192.168.80.100
Interface		LAN
Description		Go to 82

22.17. TCP SERVER (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This page shows the list of TCP servers used for Modbus Shared Memory Gateway functionality. By clicking on the "ADD" button you can configure a new TCP server, as in the figure below:



#	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

The following table explains the meaning of the parameters related to a TCP server.

Field	Meaning
Name	Mnemonic name of the TCP server This name is used to identify the TCP server on the "Tag Setup" and "Tag View" pages.
IP Address	Server IP address
TCP Port	Server TCP port
Timeout (ms) [10-10000]	Connection timeout / response for Modbus TCP requests, in milliseconds

Delay between Polls (ms) [10-1000]	Interval between two consecutive Modbus TCP requests, in milliseconds
Read/Write Retries [0-10]	Maximum number of attempts for Modbus TCP requests; this always applies to write requests; for read requests, only applies to tags with "Gateway Tag Mode" = "BRIDGE".
Multiple Read Max Number [1-32]	Maximum number of Modbus registers that can be read in a single Modbus TCP request; it is used to reduce the number of read requests sent via the TCP connection, thus optimising performance
Multiple Write Max Number [1-32]	Maximum number of Modbus registers that can be written in a single Modbus TCP request; it is used to reduce the number of write requests sent via the TCP connection, thus optimising performance.

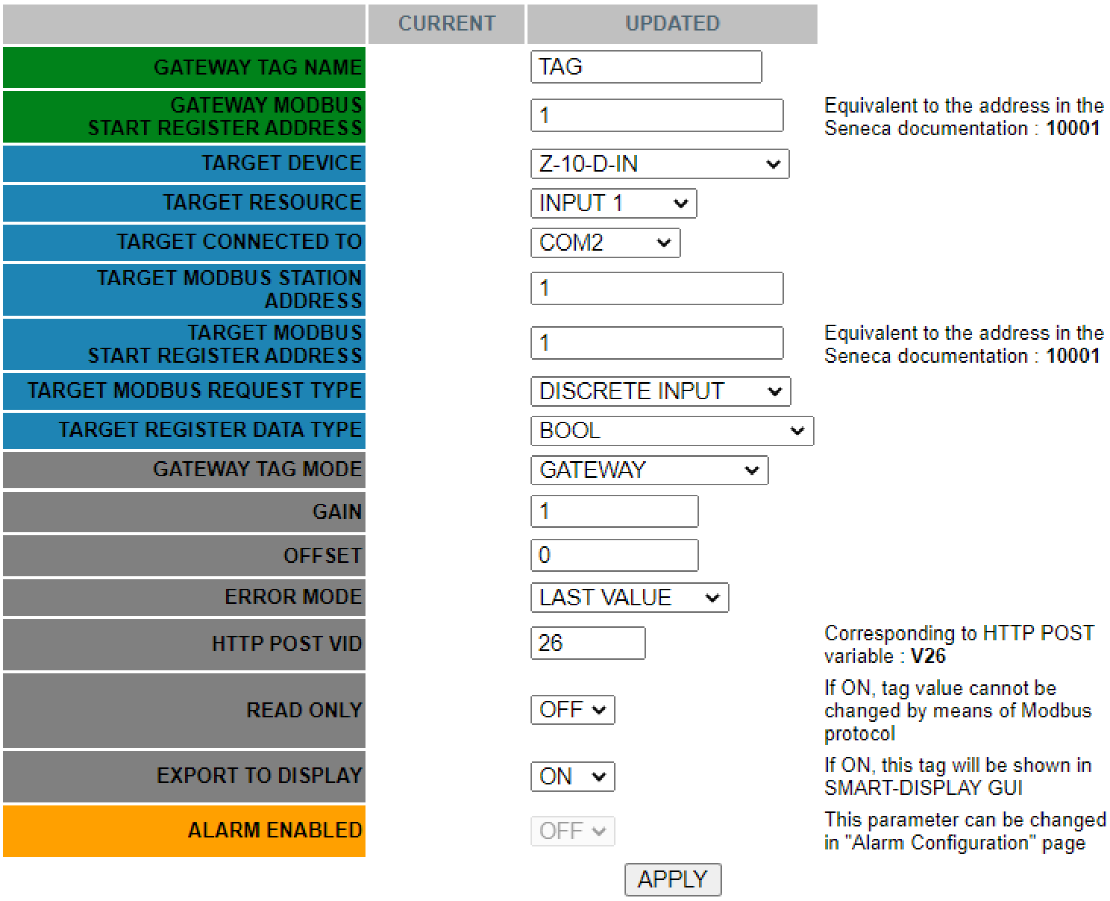
The maximum number of TCP-IP Modbus Servers that can be configured is 25.

22.18. TAG SETUP (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This page is used to configure tags in Modbus Shared Memory Gateway mode.
It is possible to import the inserted tags through an excel template (downloadable from the Seneca website) or export the current one.

It is also possible to insert new tags directly from the web page, all Seneca devices are available through an internal database, you can also define your own database.

The addition of a tag has the following fields (most of them pre-compiled as defined in the database included in the product)



	CURRENT	UPDATED	
GATEWAY TAG NAME		TAG	
GATEWAY MODBUS START REGISTER ADDRESS		1	Equivalent to the address in the Seneca documentation : **10001**
TARGET DEVICE		Z-10-D-IN	
TARGET RESOURCE		INPUT 1	
TARGET CONNECTED TO		COM2	
TARGET MODBUS STATION ADDRESS		1	
TARGET MODBUS START REGISTER ADDRESS		1	Equivalent to the address in the Seneca documentation : **10001**
TARGET MODBUS REQUEST TYPE		DISCRETE INPUT	
TARGET REGISTER DATA TYPE		BOOL	
GATEWAY TAG MODE		GATEWAY	
GAIN		1	
OFFSET		0	
ERROR MODE		LAST VALUE	
HTTP POST VID		26	Corresponding to HTTP POST variable : **V26**
READ ONLY		OFF	If ON, tag value cannot be changed by means of Modbus protocol
EXPORT TO DISPLAY		ON	If ON, this tag will be shown in SMART-DISPLAY GUI
ALARM ENABLED		OFF	This parameter can be changed in "Alarm Configuration" page

The main parameters:

Field	Meaning
Gateway Tag Name	Tag mnemonic name
Gateway Modbus Start Register Address	Start address of the tag on the Shared Memory Gateway
Target Modbus Device	Device from which to read the tag (if it is present in the database) or custom.
Target Resource	Represents the device resource to which the TAG is associated (e.g. Input1, Output2 etc...) only in the case other than Custom Device not present in the database.
Target Connected To	The serial port or Ethernet resource to which the external device is connected.
Gateway Tag Mode	This field defines how the tag will be handled by the gateway processes; possible values are: GATEWAY, BRIDGE, SHARED MEMORY or EMBEDDED. The difference between Gateway and Bridge is that Bridge tags are updated only when required, in Gateway mode the tags are updated cyclically even if they are not required.

	SHARED MEMORY are tags that can be written by Modbus RTU / Modbus TCP-IP or by Logical Rules and are TAGs representing local variables. This type of tag can also be used for calculated tags. EMBEDDED for integrated digital I/Os on board the device
Gain	This field corresponds to the value of the coefficient m in the formula m * val + q applied to the value "val" read by the device
Offset	This field corresponds to the value of the coefficient q in the formula m * val + q applied to the value "val" read by the device
Initial Value	Start value of the tag
Error Mode	This field defines which value is provided in the answer to a Modbus (read) request, when the value from the destination device is not available. The possible ways are: LAST VALUE: the last available value is given. ERROR VALUE: the value specified in the field " ERROR VALUE " is provided.
Error Value	This field defines which value is given in the reply to a Modbus request (reading), when the value from the destination device is not available and the " ERROR MODE " field is set to " ERROR VALUE".
HTTP POST VID	This field is used to create the "Variable ID" (VID) that identifies the tag in HTTP POST requests (useful only when HTTP POST protocol is enabled). The VID string is given by the "V" character plus the number contained in the field
Read Only	If selected, the tag can only be written by an external protocol (e.g. Modbus RTU or TCP-IP) and not by a logical rule.
Retain	If selected, the tag is saved in a writable retention memory (feRAM), when you restart the device the last value is loaded from the memory. This option is only available for SHARED MEMORY tags.
Calculated Function	Only active if Tag mode is "Shared Memory". Can be used to calculate the MIN / MAX / AVG value of a tag. Note that the calculation is only enabled if the datalogger is enabled. The averaging calculation time is given by the acquisition time.
Export to Display	If active it allows you to display the tag on the display or virtual display (depending on the device)
Alarm Enabled	This field is a read-only flag that indicates whether an alarm has been defined for the tag.

22.19. TAG VIEW (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This page displays the real time values of the configured tags.

The "Data Logger" buttons can be used for:
- start the Data Logger functionality, if it has been stopped (START);
- interrupt the Data Logger functionality, if running (STOP);
- clean the Data Logger's internal cache (this will also stop the Data Logger) (CLEAN CACHE).

The display is automatically updated.

As shown in the following figures, the "ALARM" column shows the status of the alarm defined for the tag, if present; the DANGER ANALOG ALARM" column has a similar behaviour, but is only meaningful for analog tags when the "Alarm Low Low Value" and "Alarm High High Value" thresholds are defined in the alarm configuration.
It is also possible to export the datalogger files to a USB stick by pressing the "COPY TO USB" button.

22.20. DB DEVICE (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

On this page you can manage the database of registers of external devices to connect to.

22.21. ALARM CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This page displays the list of configured alarms.
By clicking on the "ADD" button, you can configure a new alarm.
The following table explains the meaning of all the parameters available for an alarm.

Field	Meaning
Enabled	Flag to enable / disable an alarm
Type	This parameter indicates whether it is a digital or analog alarm; when changing the type, some parameters are enabled or disabled
Name	The name of the alarm; since this parameter is used as a key to identify the alarm, it is not possible to configure two alarms with the same name
Tag	The tag to which the alarm is connected. The list of tags changes according to the type of alarm (digital or analog). You can only associate one alarm to one tag
Activation Delays (s)	This parameter defines the time interval, in seconds, during which the alarm condition must be kept true to generate the alarm
Ignore on Boot	This is a flag used to avoid generating the alarm, if the alarm condition is detected during system startup
Auto Acknowledge	This is a flag used to avoid the need for an acknowledgement (ACK) by the user to allow the alarm to be cleared when it ceases.
Boolean Alarm Value	For a digital alarm, this parameter indicates the value of the tag (LOW or HIGH) that corresponds to the alarm condition.

Alarm Low Value	For an analog alarm, this parameter defines the low alarm threshold i.e. if the tag value falls below this threshold, the alarm condition is activated
Alarm High Value	For an analog alarm, this parameter defines the high alarm threshold i.e. if the tag value exceeds this threshold, the alarm condition is activated
Alarm Low Low Value	For an analog alarm, this parameter defines the low dangerous alarm threshold, i.e. if the tag value falls below this threshold, the alarm condition is activated
Alarm High High Value	For an analogical alarm, this parameter defines the high dangerous alarm threshold, i.e. if the tag value exceeds this threshold, the alarm condition is activated.
Deadband Value	This parameter defines a range within which the alarm does not fall (hysteresis).

The possible alarm states are explained in the following table:

Status	**Level**	**Meaning**
None	-	The tag has never entered the alarm condition
Alarm	Alarm	The value of the digital has reached the value defined by the parameter "Boolean Alarm Level".
Alarm Low	Alarm	The analog tag has fallen below the value defined by the "Alarm Low Value" parameter
Alarm High	Alarm	The analog tag has exceeded the value defined by the "Alarm High Value" parameter
Alarm Low Low	Analog Danger Alarm	The analog tag has fallen below the value defined by the "Alarm Low Value" parameter
Alarm High High	Analog Danger Alarm	The analog tag has exceeded the value defined by the "Alarm High Value" parameter
Acknowledge	-	The alarm received ACK from the user (or was configured with Auto Acknowledge)
Return	-	The tag has exited the alarm condition, but the alarm has not been acknowledged and the alarm has the "Auto Acknowledge" parameter set to OFF
End	-	The tag has exited the alarm condition and the alarm has been acknowledged or the alarm has the "Auto Acknowledge" parameter set to ON

As already mentioned in the previous table, when exiting the alarm condition the alarm states can follow two different paths, depending on the value of the " Auto Acknowledge" parameter:

- Alarm* → Return → <ACK> → End if “Auto Acknowledge”=OFF

- Alarm* → End if “Auto Acknowledge”=ON

22.22. ALARM SUMMARY (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This page shows the alarms currently active in the system.
The following table explains the meaning of all the information provided for an alarm.

Field	Meaning
Name	Alarm name
Tag Name	Tag connected to the alarm
Level	Hazard" level of the alarm: Alarm" value for digital alarms Alarm" or "Analog Danger Alarm" may apply for analog alarms
Status On	Alarm status when triggered
Timestamp On	Date Time of when the alarm was triggered
Status Action	"None" when the alarm goes off It can evolve into: "Acknowledged", If the alarm has been acknowledged "Return",if the alarm has returned but the "Auto Acknowledge" setting is OFF
Timestamp Action	Date Time of action (previous field)

22.23. ALARM HISTORY (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This page shows all alarm status transitions that have occurred in the system, up to a maximum of 1000; alarm status transitions are shown from the most recent to the oldest.

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

This page contains the parameters that indicate whether log files are copied to a connected USB stick and how long they are stored, as explained in the table below.

Field	Meaning	Default value
Enable	Enable or disable copying of logs to USB	OFF
Max Failure Counter	This parameter defines the maximum number of failed copy attempts before entering the "Wait after failure" state (see next field)	10
Wait After Failure (minutes)	This parameter defines the duration, in minutes, of the "Wait after failure" status. In this state, no further attempt is made to copy a log file to the USB	15
Clean Period (days)	This parameter defines for how many days the log files must be kept on the USB; that is, after the specified number of days, the log files are deleted.	30

In the USB the files are saved in folders according to the following convention:

yyyymmdd (yyyy=year, mm=month, dd=day)

example:

20180612

Each of these folders includes a subfolder:

logX X=[1..4], number of the group

The log file name has the following convention:

Lmmmmmmm.csv

where *mmmmmmm* is the number of minutes from [1/1/2000 00:00], corresponds to the date of the first log line example:

L9701690.csv

22.25. FTP CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This page contains the parameters related to the transfer of log files via FTP, as explained in the following table.

Field	**Meaning**
Enable	Enable or not the transfer of logs via FTP
Max Failure Counter	This parameter defines the maximum number of failed copy attempts before entering the "Wait after failure" state (see next field)
Wait After Failure (minutes)	This parameter defines the duration, in minutes, of the "Wait after failure" status. In this state, no further attempt is made to copy a log file to the USB
Crypto Mode	Defines which encryption to use for the FTP connection between: - None - TLS/SSL Implicit - TLS/SSL Explicit
Host	Hostname (FQDN) or FTP server IP address
Port	TCP port of the FTP server
Username	Server Username
Password	Server password
Path	Directory path, on the FTP server, where the log files will be saved

Log files transferred via FTP will have the following format:

<RTU_Name>_X_log<date_time>.csv

Where:
- <*RTU_Name*> is the value of the “RTU Name” field in the “General Settings” page
- *X=[1..4]* is the number of the group

- <*date_time*> has the format *yyyymmdd* (yyyy=year, mm=month, dd=day); corresponds to the log first line date

Example:

SENECA_1_log20180507101507.csv

22.26. EMAIL CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

E-mails can be used to transfer log files or to send alarms; some parameters on this page are used only when transferring log files, not when sending alarms; these parameters are marked with the caption "Data Logger Only".

All the parameters are explained in the following table.

Field	Meaning
Enable	Flag indicating whether log files are transferred via EMAIL or not Note that it is possible to send alarms via EMAIL even if this parameter is set to OFF.
Max Failure Counter	This parameter defines the maximum number of failures before entering the "Wait after failure" state (see next field).
Wait After Failure (minutes)	This parameter defines the duration, in minutes, of the "Wait after failure" status. In this state, no further attempt is made to send a log file or alarm via EMAIL
Crypto Mode	This parameter defines the encryption type of the EMAIL connection. The possible ways are: None TLS/SSL STARTTLS
Host	Hostname (FQDN) or IP address of the MAIL server
Port	EMAIL server port (TCP)
Username	EMAIL server username
Password	EMAIL server password
From	Sender's email address
To	List of one or more e-mail recipient addresses, separated by commas. This parameter is only used for the transfer of log files
Subject	Subject of the email. This parameter is only used for the transfer of log files
Text	Email text: If left blank a standard text is added. This parameter is only used for the transfer of log files

Log files sent as EMAIL attachments have names with the following format:

<RTU_Name> _X_log <date_time> .csv

where:

- <RTU_Name> is the value of the “RTU Name" parameter in the "General Settings" page
- X = [1..4] is the number of the group
- <date_time> has the format yyyymmdd (yyyy = year, mm = month, dd = day); this is the timestamp of the first sample (line) in the log file

for example..:
SENECA_1_log20180507101507.csv

Emails containing alerts have the following text format:
MESSAGE: <timestamp>
<nome rtu> <testo messaggio>

with the following object:
<nome rtu>: ALARM

22.27. HTTP CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

The http post protocol can be used to send log samples or alarms (events).
All the parameters are explained in the following table.

Field	Meaning
Enable	Enable or not the sending of logs via http
Max Failure Counter	This parameter defines the maximum number of failures before entering the "Wait after failure" state (see next field).
Wait After Failure (minutes)	This parameter defines the duration, in minutes, of the "Wait after failure" status. In this state, no further attempt is made to send a log file or alarm via http POST.
Crypto Mode	This parameter defines the encryption type of the http connection. The possible ways are: OFF (HTTP) ON (HTTPS)
Host	Hostname (FQDN) or HTTP server IP address
Port	TCP port of the HTTP server
Password	HTTP server password

22.28. MQTT CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

The MQTT protocol can be used to send (and receive) data or events to a cloud (called a broker).
All the parameters are explained in the following table:

Field	Meaning
Enable	Enable or not the MQTT protocol.
Max Failure Counter	This parameter defines the maximum number of failures before entering the "Wait after failure" state (see next field).
Wait After Failure (minutes)	This parameter defines the duration, in minutes, of the "Wait after failure" status. In this state, no further attempts are made to send or receive data via MQTT.
Client ID	Defines the Client ID used in the MQTT protocol

<table>
<tr><td>Broker Host</td><td>Defines the host name of the MQTT broker</td></tr>
<tr><td>Broker Port</td><td>Defines the MQTT broker port</td></tr>
<tr><td>Use WebSockets</td><td>Allows you to activate MQTT communication via Websockets</td></tr>
<tr><td>Keep Alive Interval (seconds)</td><td>This parameter defines Keep alive which ensures that the connection between the broker and client is still open and that the broker and client are aware that they are connected. When the client establishes a connection to the broker, it tells the broker a time interval in seconds. This interval defines the maximum period of time during which the broker and client may not communicate with each other.</td></tr>
<tr><td>Clean Session</td><td>This parameter defines the "clean session".
When the clean session flag is set to true, the client does not want a persistent session. If the client disconnects for any reason, all information and messages queued from a previous session are lost.</td></tr>
<tr><td>Message Retain</td><td>Usually if a publisher publishes a message on a topic to which no one is subscribed, the message is simply discarded by the broker. However, the publisher can tell the broker to keep the last message of that topic.</td></tr>
<tr><td>Quality of service</td><td>This parameter defines the QOS of the MQTT protocol.
Can be selected from
QOS 0 (once only, without ack)
QOS 1 (at least once, with ack)
QOS 2 (once only, with ack and resend)</td></tr>
<tr><td>Authentication</td><td>This parameter defines whether user/password authentication should be used to access the broker</td></tr>
<tr><td>Username</td><td>Broker Username</td></tr>
<tr><td>Password</td><td>Broker password</td></tr>
<tr><td>SSL/TLS</td><td>Defines if the crypto is SSL/TLS</td></tr>
<tr><td>Log on Change</td><td>This parameter defines whether topics should only be sent in case of change (based on minimum time) or not.</td></tr>
<tr><td>Publish with multiple tags</td><td>This parameter defines whether the publish contains multiple tags or whether the device should send a publish for each tag</td></tr>
<tr><td>Publish Topic for Logs</td><td>Select the topic name for the logs using the following table:
<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>Date/Time</td></tr>
<tr><td>%t</td><td>timestamp (number of seconds from 01/01/1970)</td></tr>
<tr><td>%x</td><td>text (only for "Publish Payload for Alarms")</td></tr>
<tr><td>%b</td><td>bulk (format specified in "Publish Bulk Format")</td></tr>
<tr><td>%n</td><td>Tag name (only for "Publish Bulk Format")</td></tr>
<tr><td>%v</td><td>Tag value (only in "Publish Bulk Format")</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>%i</td><td>Tag validity flag (only in "Publish Bulk Format")</td></tr>
<tr><td>%j[field]</td><td>Adds double quotes " to [field]. The double quotes represent a string in JSON</td></tr>
<tr><td>%tag_name</td><td>Value of the "tag_name" tag</td></tr>
<tr><td>%#tag_name#</td><td>Validity of the "tag_name" tag</td></tr>
</table>
</td></tr>
<tr><td>Publish Payload for Logs</td><td>Select the format to be used for the payload in Json format using the following table:
<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>date-time</td></tr>
<tr><td>%t</td><td>timestamp (number of seconds from 01/01/1970)</td></tr>
<tr><td>%x</td><td>text (only for "Publish Payload for Alarms")</td></tr>
<tr><td>%b</td><td>bulk (format specified in "Publish Bulk Format")</td></tr>
<tr><td>%n</td><td>Tag name (only for "Publish Bulk Format")</td></tr>
<tr><td>%v</td><td>Tag value (only in "Publish Bulk Format")</td></tr>
<tr><td>%i</td><td>Tag validity flag (only in "Publish Bulk Format")</td></tr>
<tr><td>%j[field]</td><td>Adds double quotes " to [field]. The double quotes represent a string in JSON</td></tr>
<tr><td>%tag_name</td><td>Value of the "tag_name" tag</td></tr>
<tr><td>%#tag_name#</td><td>Validity of the "tag_name" tag</td></tr>
</table>
</td></tr>
<tr><td>Publish Bulk Format</td><td>Select the format for "bulk mode" according to the following table:
<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>Date/Time</td></tr>
<tr><td>%t</td><td>timestamp (number of seconds from 01/01/1970)</td></tr>
<tr><td>%x</td><td>text (only for "Publish Payload for Alarms")</td></tr>
<tr><td>%b</td><td>bulk (format specified in "Publish Bulk Format")</td></tr>
<tr><td>%n</td><td>Tag name (only for "Publish Bulk Format")</td></tr>
<tr><td>%v</td><td>Tag value (only in "Publish Bulk Format")</td></tr>
<tr><td>%i</td><td>Tag validity flag (only in "Publish Bulk Format")</td></tr>
</table>
</td></tr>
</table>

	%j[field]	Adds double quotes " to [field]. The double quotes represent a string in JSON
	%tag_name	Value of the "tag_name" tag
	%#tag_name#	Validity of the "tag_name" tag
Publish Topic for Alarms	Select the format for topic names in alarms according to the following table:	
	%c	Device Client ID
	%m	Device MAC Address
	%e	Device IMEI
	%d	Date/Time
	%t	timestamp (number of seconds from 01/01/1970)
	%x	text (only for "Publish Payload for Alarms")
	%b	bulk (format specified in "Publish Bulk Format")
	%n	Tag name (only for "Publish Bulk Format")
	%v	Tag value (only in "Publish Bulk Format")
	%i	Tag validity flag (only in "Publish Bulk Format")
	%j[field]	Adds double quotes " to [field]. The double quotes represent a string in JSON
	%tag_name	Value of the "tag_name" tag
	%#tag_name#	Validity of the "tag_name" tag
Subscribe Topic	Select the Topic Subscribe according to the following table:	
	%c	Device Client ID
	%m	Device MAC Address
	%e	Device IMEI
	%d	Date/Time
	%t	timestamp (number of seconds from 01/01/1970)
	%x	text (only for "Publish Payload for Alarms")
	%b	bulk (format specified in "Publish Bulk Format")
	%n	Tag name (only for "Publish Bulk Format")
	%v	Tag value (only in "Publish Bulk Format")
	%i	Tag validity flag (only in "Publish Bulk Format")
	%j[field]	Adds double quotes " to [field]. The double quotes represent a string in JSON
	%tag_name	Value of the "tag_name" tag
	%#tag_name#	Validity of the "tag_name" tag

<table>
<tr><th></th><th></th></tr>
<tr><td>LWT Topic</td><td>Select the "Last Weel and Testament" topic according to the following table:
<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>Date/Time</td></tr>
<tr><td>%t</td><td>timestamp (number of seconds from 01/01/1970)</td></tr>
<tr><td>%x</td><td>text (only for "Publish Payload for Alarms")</td></tr>
<tr><td>%b</td><td>bulk (format specified in "Publish Bulk Format")</td></tr>
<tr><td>%n</td><td>Tag name (only for "Publish Bulk Format")</td></tr>
<tr><td>%v</td><td>Tag value (only in "Publish Bulk Format")</td></tr>
<tr><td>%i</td><td>Tag validity flag (only in "Publish Bulk Format")</td></tr>
<tr><td>%j[field]</td><td>Adds double quotes " to [field]. The double quotes represent a string in JSON</td></tr>
<tr><td>%tag_name</td><td>Value of the "tag_name" tag</td></tr>
<tr><td>%#tag_name#</td><td>Validity of the "tag_name" tag</td></tr>
</table></td></tr>
<tr><td>LWT Payload</td><td>Select the Payload text of "Last Weel and Testament"</td></tr>
<tr><td>Save Configuration URL</td><td>This is the URL for the "Save Configuration" command received from mqtt</td></tr>
<tr><td>Load Configuration URL</td><td>This is the URL for the "Load Configuration" command received from mqtt</td></tr>
<tr><td>FW Update URL</td><td>This is the URL for the "FW Update" command received from mqtt</td></tr>
<tr><td>Sleep Timeout</td><td>MQTT task wake-up time, the shorter it is, the more responsive MQTT is (at the expense of higher CPU load).</td></tr>
<tr><td>MQTT Certificates</td><td>It is used to manage the certificates necessary for the TLS connection.</td></tr>
</table>

22.29. PHONEBOOK (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This page is used to configure the address book for sending text messages by the device via email and/or (on models equipped with a modem) SMS.

It is possible to define three different account profiles:

Admin

This account receives alarms via SMS or EMAIL from any group.
This account can send SMS commands to the device.
It also receives all rejected or unrecognised SMS commands if the "SMS Relay to Admin" parameter is set to ON and all "Startup SMS" messages if the "Startup SMS" parameter is set to ON;

Manager

This account receives alarms via SMS or EMAIL from the group to which it belongs.

This account can send SMS commands to the device.

User

This account receives alarms via SMS or EMAIL from the group to which it belongs.

At the time of compilation, the group(s) to which the account belongs is required, so you can divide the text alerts between the various accounts.
Note how "Admin" accounts receive alarms from any group.

22.30. MESSAGE CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

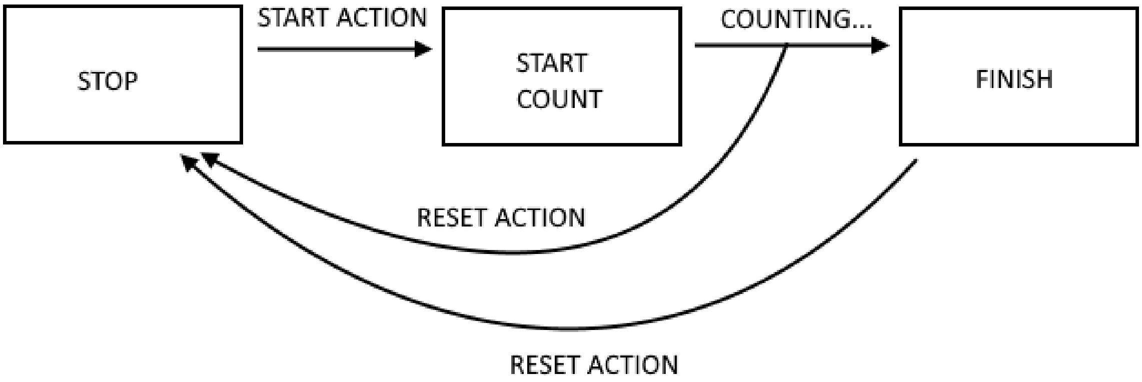
In this section it is possible define the text messages related to the alarms that the device must manage.
The message text can only contain ASCII characters.
It is possible to use the {TAG_NAME} syntax to include the current value of a tag in your text.
The syntax allows you to add the current value of the tag whose name is the one defined within the curly brackets.
This syntax can be used more than once in a message text.
Each message has an ID field which is used to associate the message to the alarm.

22.31. TIMER CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

This section allows you to define up to 100 timers to be used in logic rules.
The ID represents the mnemonic of the timer that must be used in the rules.
"Enable" selects whether the timer is active or not.
"Duration" is the activation value in [ms].

Note

The timers are in stop mode by default, they need an action to start and an action to restore, according to the following scheme:



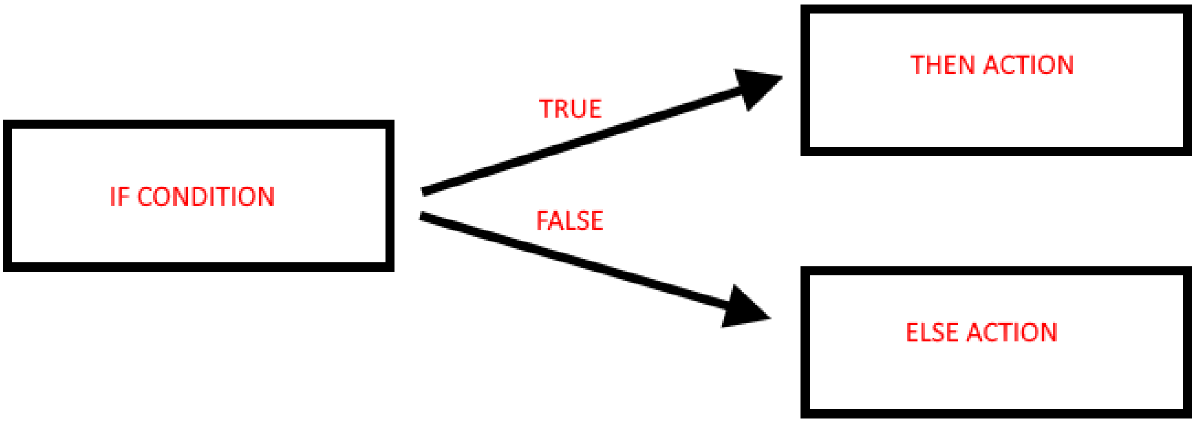
22.32. RULE MANAGEMENT (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

In this section you can define a set of logical rules that will implement a program.
For example it is possible to run programs that use internal or external IO, send text messages and/or writes via MODBUS / EMAIL / SMS / http / MQTT etc... even using complex mathematical operations.

Rules can also be debugged through step-by-step execution and the use of breakpoints that block program execution on a specific line (rule).

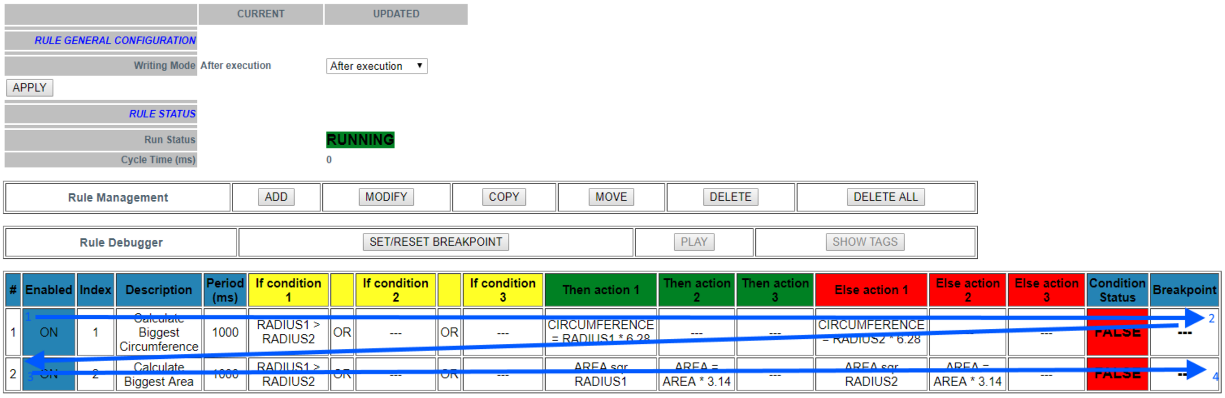
A rule consists of one or more "If Condition", one or more "Then Action" and one or more "Else Action".

Schematically a rule performs the following flow:



If the "IF" condition is true, the "THEN" action is executed, otherwise the "ELSE" action is executed.

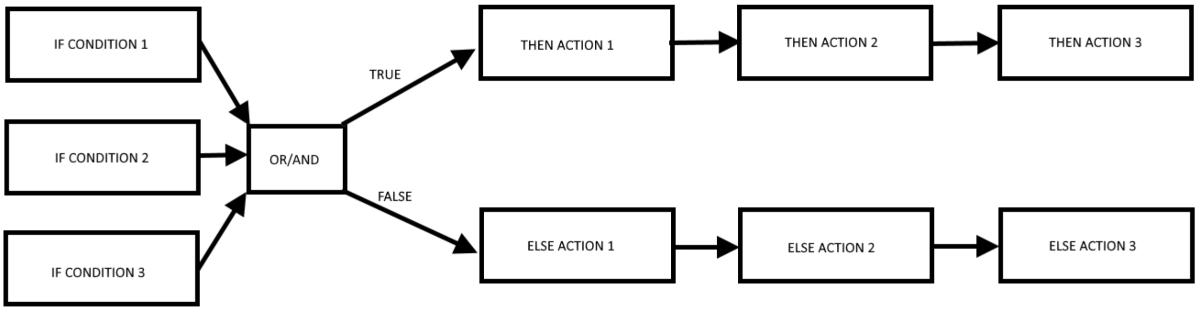
The rules are executed from top to bottom and from left to right (in figure 1-> 2-> 3-> 4):



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

#	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	---

When all the rules are executed, the execution starts again from the first one.
More in detail the correct diagram is:



It is in fact possible to define up to 3 if conditions and up to 3 actions for both the THEN and ELSE state.

The "IF conditions" can be combined together in "OR" or "AND" logic, in practice:
The "IF conditions" linked together by "OR" go to the THEN state if at least one of the conditions is true.
The "IF conditions" linked together by "AND" only go to the THEN state if all of them are true.
More details are given in the following table:

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

It is possible to create up to 2000 different rules.
You can configure a rule to perform actions:
-Only when there is a change in the "OR / AND" result
-At each loop

In the "Rule General Configuration" you can choose when Tags are written to shared memory, you can choose between "After Execution" or "During Execution".

With "After Execution", you get tag values written to shared memory only when you've executed all the rules.
With "During Execution", you get tag values written to shared memory at the end of each rule.

Therefore, using the "After Execution" mode, the new tag values will only be updated at the end of all rules (even tags that must be written on MODBUS RTU / TCP-IP).
The rule status will show the execution status (if the rules are in execution or pause mode) and the loop time which represents the time taken to execute all the rules (note that if you need to write tags with modbus protocol, the loop time will also include the time taken for this operation):

To configure a rule, the parameters explained in the following table are available:

Field	Meaning
Enabled	Indicates whether the rule is enabled or should be excluded from execution
Index	Rule execution order (1 = First rule to be executed)
Description	Mnemonic textual description of the rule
Period [ms]	If the value is = 0, actions are executed only if there is a change in the result of the "OR / AND" (i.e. on change of state). If the value is different from 0 ms the actions are performed trying to respect the inserted timing. Do not use small period values for sending EMAIL / SMS / HTTP / MQTT actions! NOTE: If Period is > 0 the actions are always performed in "repeat" mode
If Condition X Type Where X=[1..3]	This parameter defines the type of condition, for each of the three "if conditions" available (1..3) The possible types are: **None** No conditions to be assessed **Alarm State** See 22.32.1 **Alarm Active** See 22.32.2 **Always** The If condition is always true. Note that the rule is only executed once if Period is = 0 ms or if the actions are in one time mode. If you need to execute a rule at each cycle, you need to put the actions in "repeat mode". If you need to run a rule every xx ms, you must set Period> 0ms. **Digital Tag** See 22.32.3 **Analog Tag** See 22.32.4 **Timer**

	See 22.32.5 **Scheduler** See 22.32.6 **Rule Status** See 22.32.7 **Bitmask** See 22.32.8
If Condition Operator	The possible types are: OR / AND The IF conditions can be combined in Boolean OR or AND operations.
Then/Else Action X where X=[1..3]	This parameter defines the type of action, for each of the three "actions then/other" available The possible types of action are divided by type: **None** No action **Send Alarm SMS** **Send Alarm EMAIL** **Send Alarm HTTP POST** **Send Alarm MQTT** Allow to send a text message (defined in the messages section) of alarm through the available protocols **Digital Tag** See 22.32.9 **Analog Tag** See 22.32.10 Timer It is possible to select the action to be performed in the timer between "Start" will start a timer to count "Reset" will reset the timer to the stop state. **Scheduler** See 22.32.6 **Datalogger** Allows you to start or stop the datalogger. **Network**

	These are actions that allow you to act on the status of the VPN (enable or disable it) or the modem. **Set Bits** Allows you to bring a configurable number of bits of a given tag to the value 1 or 0.

22.32.1. "ALARM STATE" PARAMETERS

Field	Meaning
Alarm Name	The alarm name can be selected from the list of all configured alarms
Alarm State	Alarm status. Possible states are: - **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** Depending on the type (digital or analog) of the selected alarm, some states are disabled
Analog Danger Alarm	Flag indicating whether the alarm level must be "Analog Danger" or not, applies only to alarms on analog tags

22.32.2. "ALARM ACTIVE" PARAMETERS

Field	Meaning
Alarm Name	The alarm name can be selected from the list of all configured alarms
Alarm Active	Indicates whether or not the alarm should be active. The alarm is active if it is in one of these states: - **Alarm (only for digital tags)** - **Alarm Low Low (only for analog tags)** - **Alarm Low (only for analog tags)** - **Alarm High (only for analog tags)** - **Alarm High High (only for analog tags)** - **Acknowledge** The alarm is not active if it is in one of the following states: - **None** - **Return** - **End**
Analog Danger Alarm	Flag indicating whether the alarm level should be "Analog Danger" or not, significant only for analog alarms.

22.32.3. "DIGITAL TAG" PARAMETERS

Field	Meaning
Tag	Select the tag to be used for the condition
Operator	Only "=" may apply
Tag / Constant value	Select whether the comparison is between a tag or a constant Boolean value

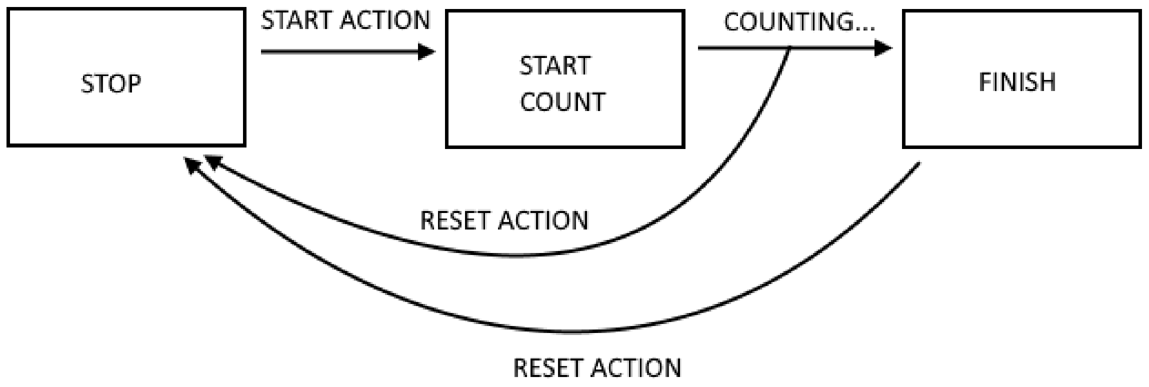
22.32.4.“ANALOG TAG" PARAMETERS

Field	Meaning
Tag	Select the tag to be used for the condition
Operator	It may apply : “=” “>” “<” “>=” “<=”
Tag / Constant value	Select whether the comparison is between a tag or a constant value

22.32.5.“TIMER" PARAMETERS

Field	Meaning
ID	Select the timer ID to use
Expired	It can be: "OFF" or "ON" With "ON" the condition is only true when the timer expires (FINISH status). With "OFF" the condition is true until the timer is in STOP or COUNTING STATE. When the timer is in FINISH state the condition becomes false.

The operation of the Timer is shown in the following diagram:



22.32.6.“SCHEDULER" PARAMETERS

Field	Meaning
Type	It may be: Daily, Weekly Monthly Daily: the condition is true every day at the configured hour and minute Weekly: the condition is true on the selected day of the week at the selected hour and minute Monthly: the condition is true on the selected day of the month at the selected hour and minute
Day	If the type is Weekly sets the day of the week: 0 = Sunday 1 = Monday 2 = Tuesday 3 = Wednesday 4 = Thursday 5 = Friday 6 = Saturday If the type is Monthly: Select the day of the month from 1 to 31
Hour	Hours
Minute	Minutes

22.32.7.“RULE STATUS" PARAMETERS

Field	Meaning
ID	Select the rule ID
Enabled	Select between "enabled" or "disabled If "Enabled" the condition is REAL if the selected rule is enabled. If "Disabled" the condition is REAL if the selected Rule is disabled.

22.32.8.“BIT MASK" PARAMETERS

Field	Meaning
Tag	Select the tag to apply the bit mask to from a list containing all tags with "16Bit Unsigned" data type and bit index 0
Mask	The bit mask represented as a string of 4 hexadecimal digits

The "Bit mask" condition is TRUE if the AND operation bit by bit between the Tag and the Data Mask is different from 0; FALSE otherwise.

22.32.9.“DIGITAL TAG" PARAMETERS

Field	Meaning
Action Mode	select from "One Time" or "Repeat". With "One Time" actions are only performed if there is a change in the result of the OR / AND conditions. With "Repeat" Actions are performed at each loop (if the rule is enabled and there is no configured period).
Destination Tag	This is the tag where the calculated result is copied to
Operator	This is the Boolean operator to use, selected from =, NOT, OR etc ...
Source Tag 1 / Constant value 1	Select the tag to use in the boolano calculation. It is also possible to use a boolean constant
Source Tag 2 / Constant value 2	Select the second Tag if the operator needs 2 inputs (For example operator "OR"). It is also possible to use a boolean constant

22.32.10. “ANALOG TAG" PARAMETERS

Field	Meaning
Action Mode	select from "One Time" or "Repeat". With "One Time" actions are only performed if there is a change in the result of the OR / AND conditions. With "Repeat" Actions are performed at each loop (if the rule is enabled and there is no configured period).
Destination Tag	This is the tag where the calculated result is copied to
Operator	It is the mathematical operator to use, you can select from: **"="** copies the source tag 1 or the constant value 1 to the destination tag Example: Destination tag = Origin tag 1 Or Target tag = constant value 1 **"+ ="** Add the value of the source tag1 or the constant value 1 to the target tag and copy the result to the target tag.

	Example: Destination tag = Destination tag + Origin tag 1 **"- ="** Subtracts the value of the source tag1 from the target tag and copies the result to the target tag. Example: Destination tag = Destination tag - Origin tag 1 **"* ="** Multiply the target tag by the value of source tag 1 and copy the result to the target tag. Example: Destination tag = Destination tag * Origin tag 1 **"/ ="** Splits the target tag with the source tag value 1 and copies the result to the target tag. Example: Destination tag = Destination tag / Origin tag 1 "% =" Calculates the rest of the division from the target tag and the value of the source tag1 and copies the result to the target tag. (Note that 53% 7 = 4) Example: Destination tag = Destination tag% Source tag1 "abs" Calculates the absolute value of Source Tag 1 / Constant value 1 and copies the result to the Destination Tag (Note that abs (-4) = 4) Example: Target tag = abs (Source tag 1) "Sqrt"

	Calculates the square root value of source tag 1 / constant value 1 and copies the result to the target tag. (Note that sqrt (9) = √9 = 3) Example: Destination tag = sqrt (origin tag 1) "Sqr" Calculates the square value of the source tag 1 / constant value 1 and copies the result to the target tag. (Note that sqr (3) = 3^2 = 9) Example: Destination tag = sqr (origin tag 1) "Log" Calculates the decimal logarithm of source tag 1 / constant value 1 and copies the result to the target tag. (Note that log (3) = 0.4771212) Example: Destination tag = log (origin tag 1) "Ln" Calculates the natural logarithm of the source tag 1 / constant value 1 and copies the result to the target tag. (Note that ln (3) = 1.09861228867) Example: Target tag = ln (Source tag 1) "Exp" Calculate the number of Euler elevated to Source Tag 1 / Constant value 1 and copy the result to the Destination Tag. (Note that exp⁡ 〖(3) = e ^ 3 = 20,0855369232〗 ln (exp (3)) = 3 Example: Destination tag = expiration (origin tag 1) "+" Sum to Source Tag 1 / Constant value 1 With the value of Source Tag 2 / Constant value 2 and copies the result to the Destination Tag.

	Example: Target tag = Source tag 1+ Source tag 2 "-" Subtract the source tag 1 / constant value 1 with the value of source tag 2 / constant value 2 and copy the result to the target tag. Example: Destination tag = Origin tag 1- Origin tag 2 "*" Multiply the source tag 1 / constant value 1 with the source tag 2 / constant value 2 and copy the result to the target tag. Example: Target tag = Source tag 1 * Source tag 2 "/" Split the source tag 1 / constant value 1 with the source tag 2 / constant value 2 and copy the result to the target tag. Example: Target Tag = Source Tag 1 / Source Tag 2 "%" Calculates the rest of the division between source tag 1 / constant value 1 and source tag 2 / constant value 2 and copies the result to the target tag. (Note that 53% 7 = 4) Example: Target tag = Source tag 1% Source tag 2 "Pow" Calculates the Source Tag1 / Constant value 1 elevated to the power of the Sorce Tag2 / Constant value 2 and copies the result to the destination tag. Example: DestinationTag = 〖Source Tag1〗 ^ (Source Tag2)

Source Tag 1 / Constant value 1	Select the tag to be used as input 1 for the operator used. You can also use a constant value.
Source Tag 2 / Constant value 2	Select the Tag to use as input 2 in the calculation if the operator needs 2 inputs. You can also use a constant value.

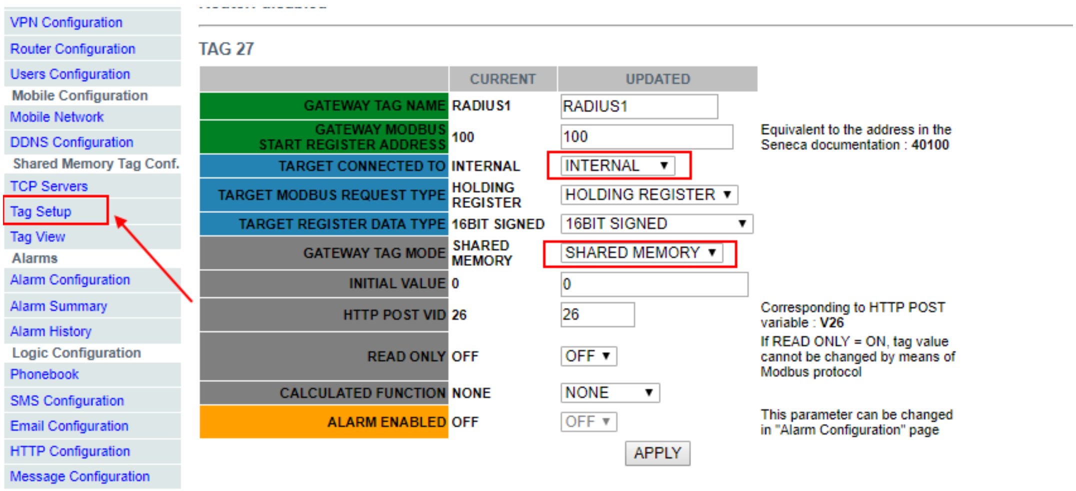
22.32.11. EXAMPLE OF THE IMPLEMENTATION OF A PROGRAM WITH LOGICAL RULES

We will create an example program that calculates the Maximum Circumference and Maximum Area from 2 different radii.

First of all we add the Tags we need for the program:

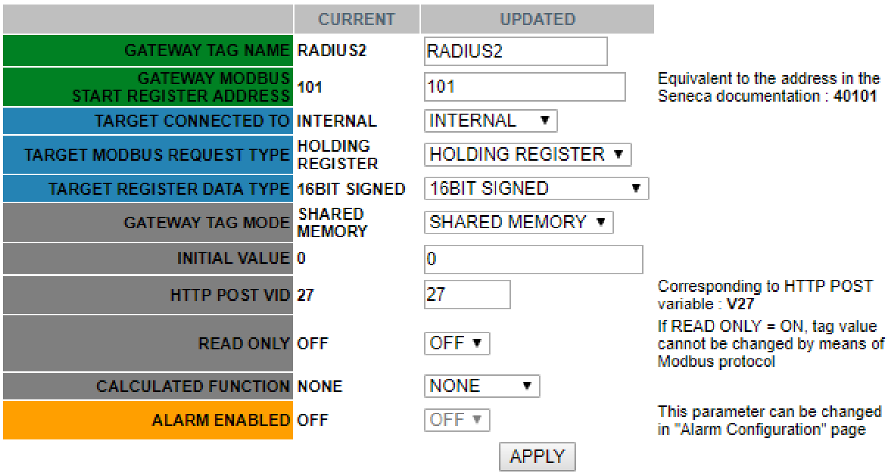
We define the Radius1 and Radius2 tags as integer type

Circumference e Area in Real 32 bits (floating point single precision) type:

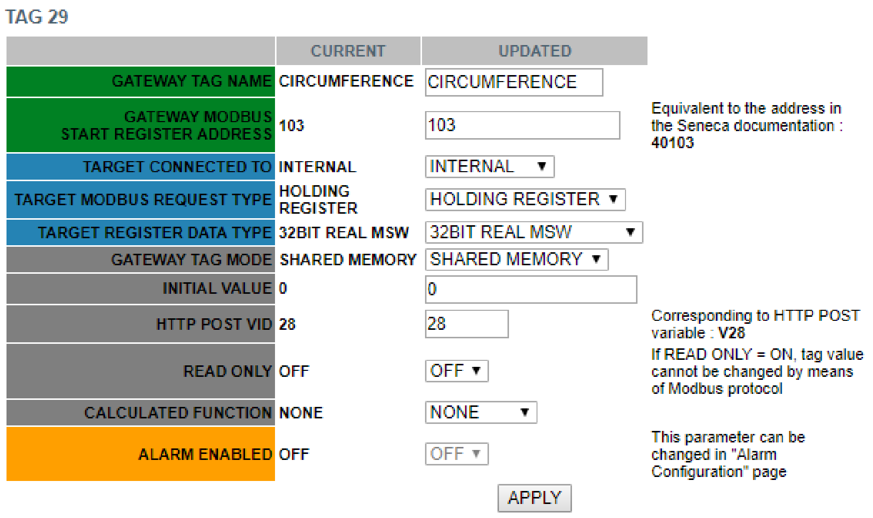


TAG 27

	CURRENT	UPDATED	
GATEWAY TAG NAME	RADIUS1	RADIUS1	
GATEWAY MODBUS START REGISTER ADDRESS	100	100	Equivalent to the address in the Seneca documentation : **40100**
TARGET CONNECTED TO	INTERNAL	INTERNAL ▼	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	HOLDING REGISTER ▼	
TARGET REGISTER DATA TYPE	16BIT SIGNED	16BIT SIGNED ▼	
GATEWAY TAG MODE	SHARED MEMORY	SHARED MEMORY ▼	
INITIAL VALUE	0	0	
HTTP POST VID	26	26	Corresponding to HTTP POST variable : **V26**
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

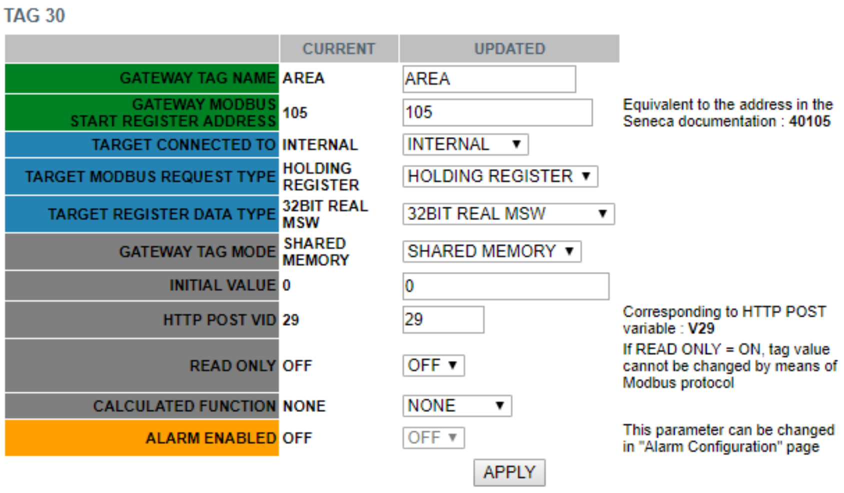


	CURRENT	UPDATED	
GATEWAY TAG NAME	RADIUS2	RADIUS2	
GATEWAY MODBUS START REGISTER ADDRESS	101	101	Equivalent to the address in the Seneca documentation : **40101**
TARGET CONNECTED TO	INTERNAL	INTERNAL ▼	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	HOLDING REGISTER ▼	
TARGET REGISTER DATA TYPE	16BIT SIGNED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



TAG 29

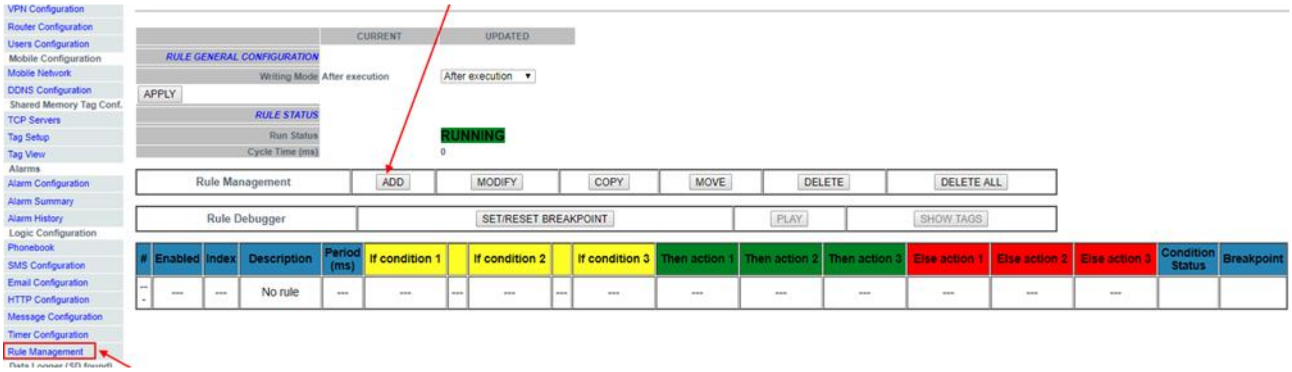
	CURRENT	UPDATED	
GATEWAY TAG NAME	CIRCUMFERENCE	CIRCUMFERENCE	
GATEWAY MODBUS START REGISTER ADDRESS	103	103	Equivalent to the address in the Seneca documentation : **40103**
TARGET CONNECTED TO	INTERNAL	INTERNAL ▾	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	HOLDING REGISTER ▾	
TARGET REGISTER DATA 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	

Now click on "Rules Management" and then on ADD to add a new rule:

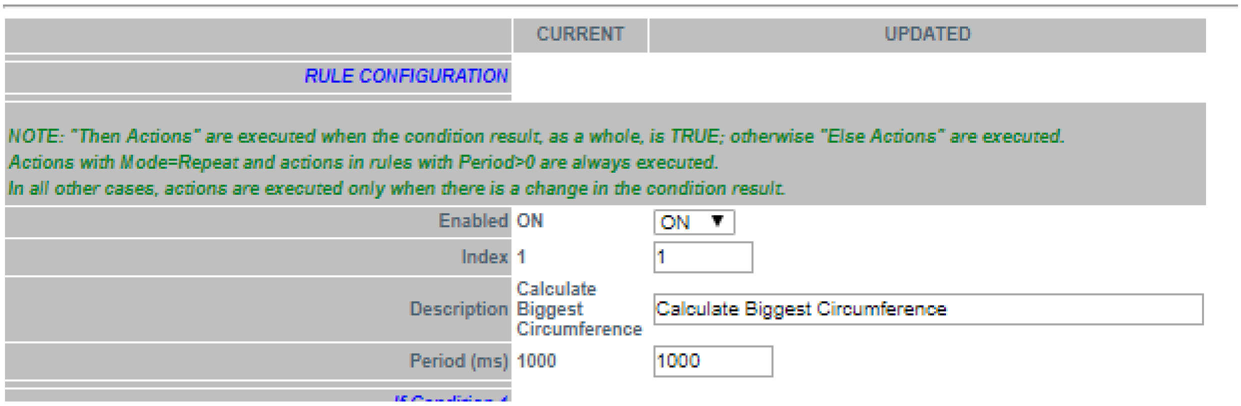


	CURRENT	UPDATED
RULE GENERAL CONFIGURATION		
Writing Mode	After execution	After execution ▾
RULE STATUS		
Run Status		RUNNING
Cycle Time (ms)		0

#	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
---	---	---	No rule	---	---	---	---	---	---	---	---	---	---	---	---		

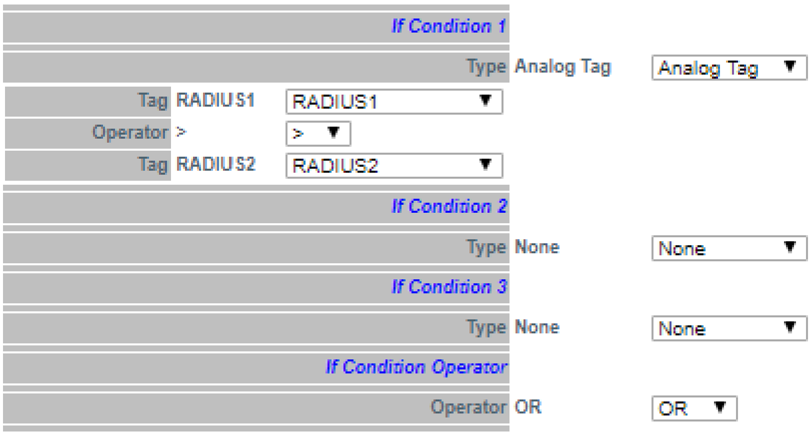
Let us now create the first rule to calculate the circumference using the largest radius between Radius1 and Radius2:

We need the rule to be performed every 1000 ms:



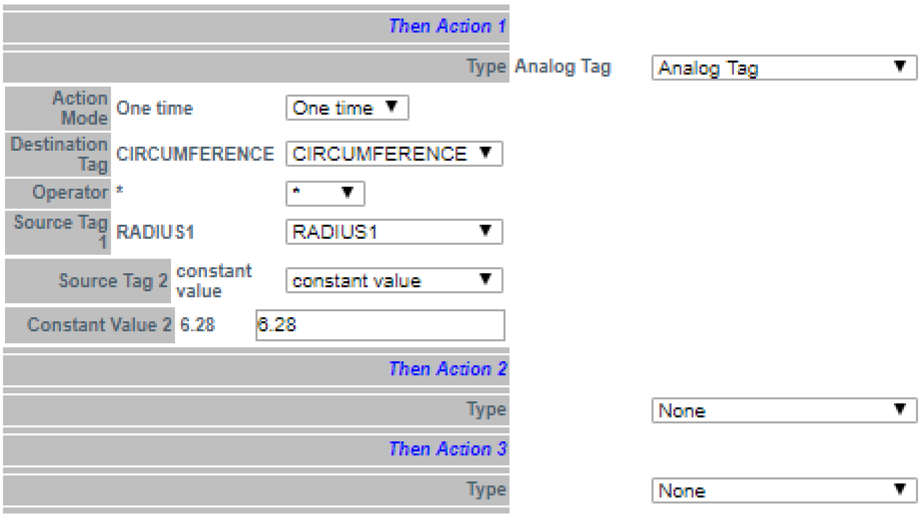
	CURRENT	UPDATED
RULE CONFIGURATION		
NOTE: "Then Actions" are executed when the condition result, as a whole, is TRUE; otherwise "Else Actions" are executed. Actions with Mode=Repeat and actions in rules with Period>0 are always executed. In all other cases, actions are executed only when there is a change in the condition result.		
Enabled	ON	ON ▼
Index	1	1
Description	Calculate Biggest Circumference	Calculate Biggest Circumference
Period (ms)	1000	1000

Then we add the "if condition" to determine which is the largest radius (we only need 1 if condition):



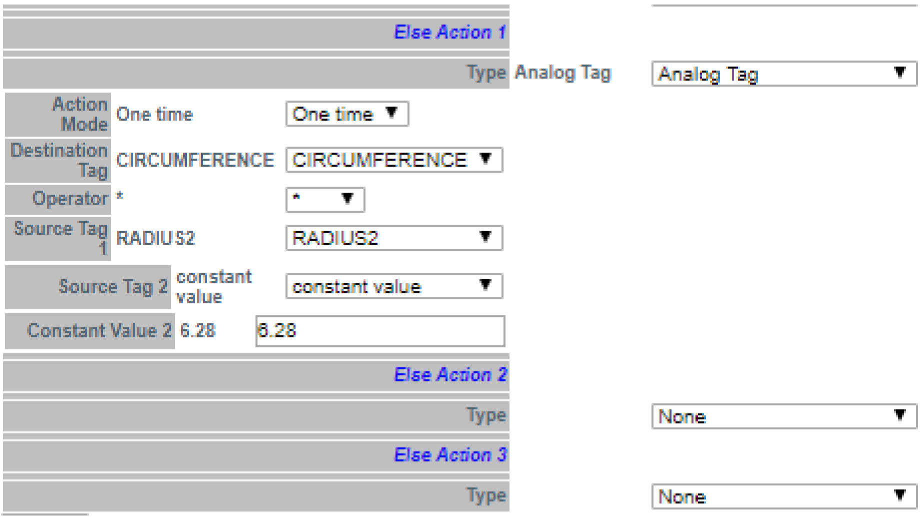
If Condition 1		
Type	Analog Tag	Analog Tag ▼
Tag	RADIUS1	RADIUS1 ▼
Operator	>	> ▼
Tag	RADIUS2	RADIUS2 ▼
If Condition 2		
Type	None	None ▼
If Condition 3		
Type	None	None ▼
If Condition Operator		
Operator	OR	OR ▼

So, if the condition is true then Radius1> Radius2 we must then calculate the circumference with Radius1: Circumference = Radius1 * 6.28:



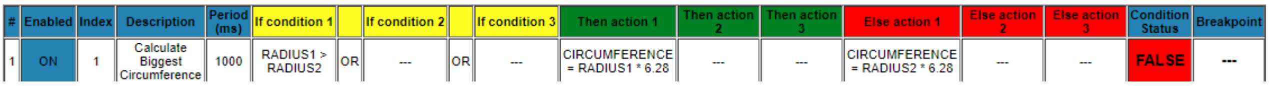
Then Action 1		
Type	Analog Tag	Analog Tag ▼
Action Mode	One time	One time ▼
Destination Tag	CIRCUMFERENCE	CIRCUMFERENCE ▼
Operator	*	* ▼
Source Tag 1	RADIUS1	RADIUS1 ▼
Source Tag 2	constant value	constant value ▼
Constant Value 2	6.28	6.28
Then Action 2		
Type		None ▼
Then Action 3		
Type		None ▼

Otherwise Radius 1 < Radius 2 then we must calculate the circumference with Radius 2 (Circumference = Radius2 * 6.28):



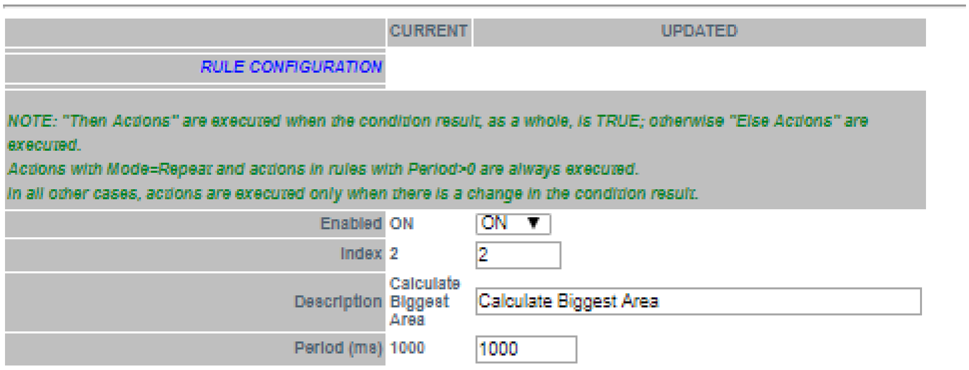
Else Action 1		
Type	Analog Tag	Analog Tag ▼
Action Mode	One time	One time ▼
Destination Tag	CIRCUMFERENCE	CIRCUMFERENCE ▼
Operator	*	* ▼
Source Tag 1	RADIUS2	RADIUS2 ▼
Source Tag 2	constant value	constant value ▼
Constant Value 2	6.28	6.28
Else Action 2		
Type		None ▼
Else Action 3		
Type		None ▼

Now click "APPLY" to save the first rule:



#	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	---

In the same way we create the Second Rule to calculate the Area with the largest radius:
This rule must also be performed every 1000ms:

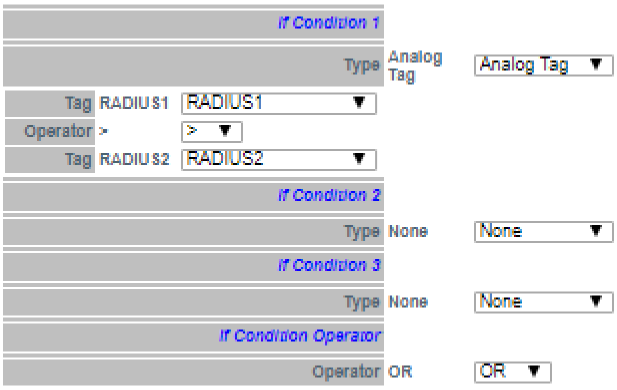


	CURRENT	UPDATED
RULE CONFIGURATION		

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

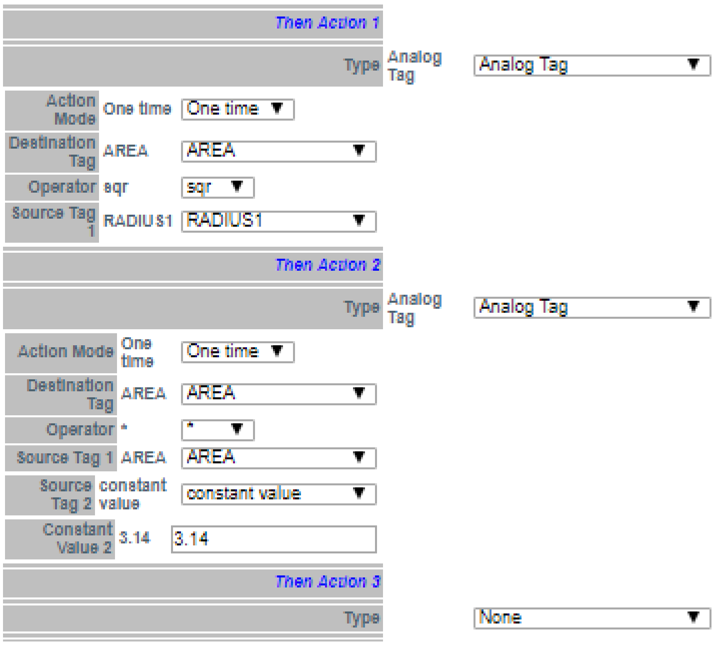
The "if condition" is the same as the first rule:



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 ▼

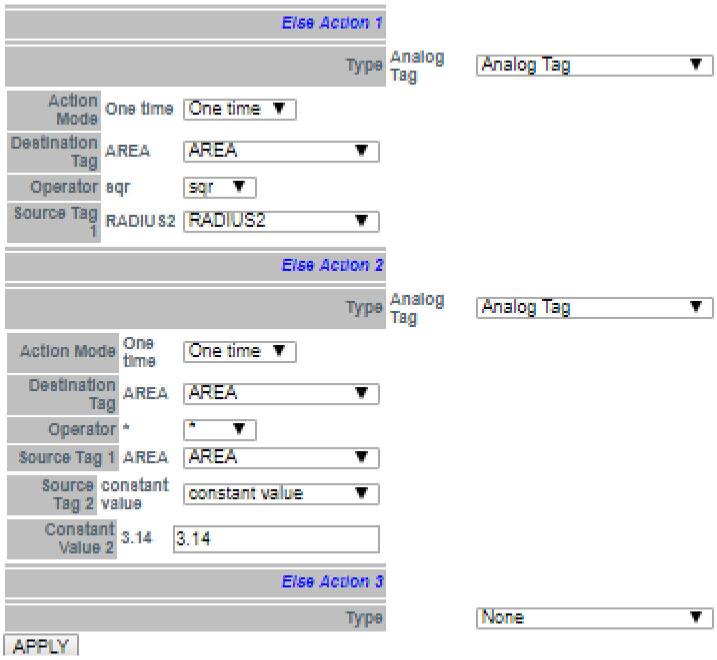
Now we have to calculate the AREA using the following calculation:
AREA = ([RADIUS] ^ 2) * 3.14
We have to break the formula in two phases:
In the first phase we calculate:
AREA = (RADIUS1) ^ 2
And in the second:
AREA = AREA * 3.14

So in our rule if RADIUS1> RADIUS2 we calculate AREA with RADIUS1 using the square function (sqr):
AREA = sqr (RADIUS1)
And then
AREA = AREA * 3.14



Then Action 1		
Type	Analog Tag	Analog Tag ▼
Action Mode	One time	One time ▼
Destination Tag	AREA	AREA ▼
Operator	sqr	sqr ▼
Source Tag 1	RADIUS1	RADIUS1 ▼
Then Action 2		
Type	Analog Tag	Analog Tag ▼
Action Mode	One time	One time ▼
Destination Tag	AREA	AREA ▼
Operator	*	* ▼
Source Tag 1	AREA	AREA ▼
Source Tag 2	constant value	constant value ▼
Constant Value 2	3.14	3.14
Then Action 3		
Type		None ▼

So if RADIUS1 <RADIUS2 we calculate AREA with RADIUS2:



Else Action 1

Type: Analog Tag — Analog Tag ▼

Action Mode: One time — One time ▼

Destination Tag: AREA — AREA ▼

Operator: sqr — sqr ▼

Source Tag 1: RADIUS2 — RADIUS2 ▼

Else Action 2

Type: Analog Tag — Analog Tag ▼

Action Mode: One time — One time ▼

Destination Tag: AREA — AREA ▼

Operator: * — * ▼

Source Tag 1: AREA — AREA ▼

Source Tag 2: constant value — constant value ▼

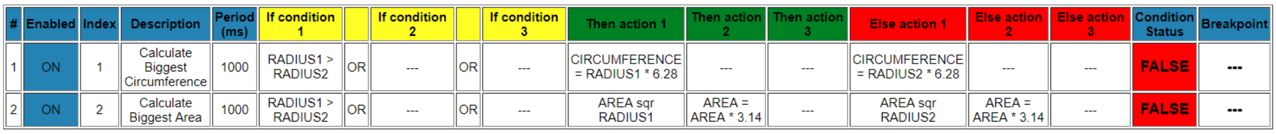
Constant Value 2: 3.14 — 3.14

Else Action 3

Type: None ▼

APPLY

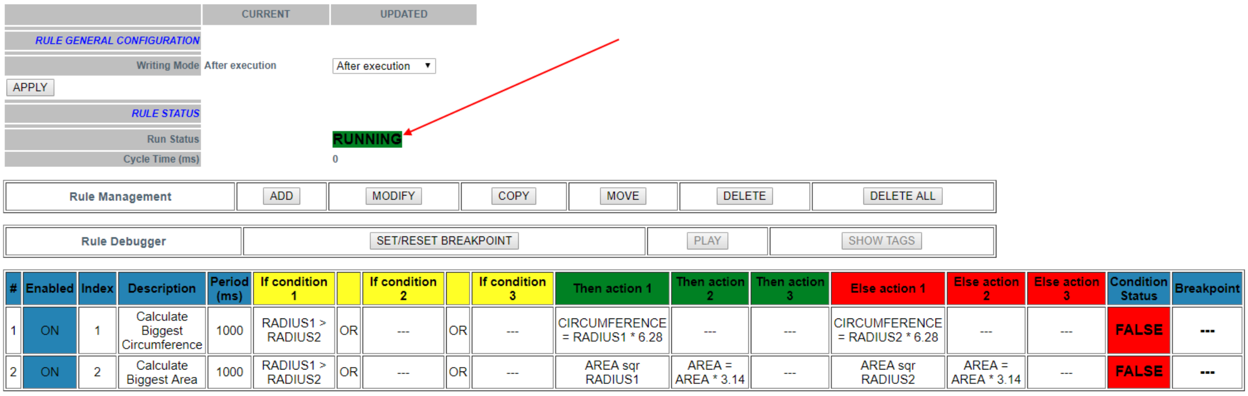
Now click on "APPLY" to save the second rule as well:



#	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	---

Now we can test how our programme works:

When a rule is added, the rule starts automatically (RUNNING):



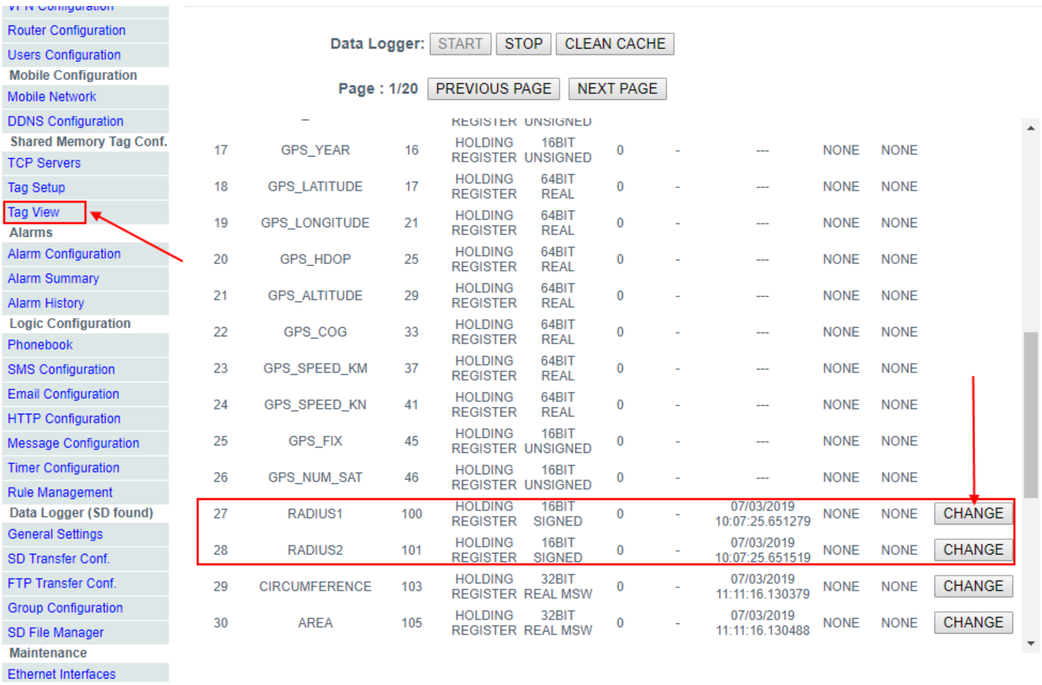
	CURRENT	UPDATED
RULE GENERAL CONFIGURATION		
Writing Mode	After execution	After execution ▾
APPLY		
RULE STATUS		
Run Status		RUNNING
Cycle Time (ms)		0

Rule Management: ADD | MODIFY | COPY | MOVE | DELETE | DELETE ALL

Rule Debugger: SET/RESET BREAKPOINT | PLAY | SHOW TAGS

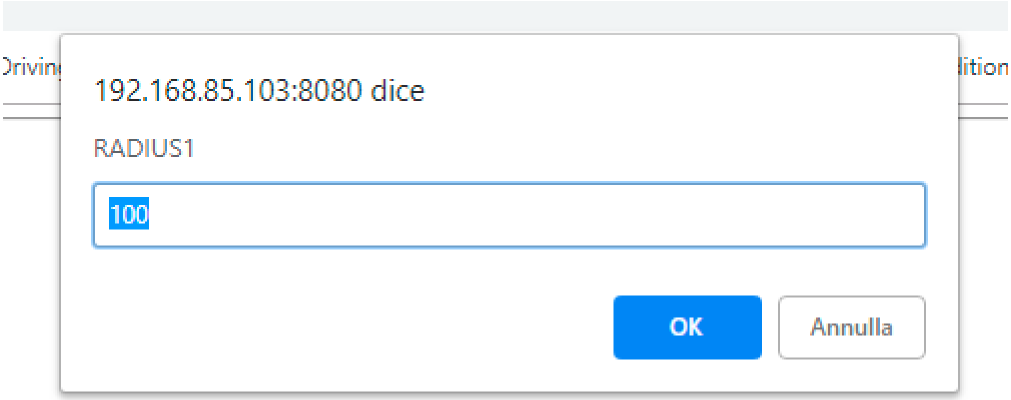
#	Enabled	Index	Description	Period (ms)	If condition 1		If condition 2		If condition 3	Then action 1	Then action 2	Then action 3	Else action 1	Else action 2	Else action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	OR	---	CIRCUMFERENCE = RADIUS1 *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

To test the program we can write the tags RADIUS1 and RADIUS2 from Modbus RTU / MODBUS TCP-IP (registers 40100-40101 in our example) or using the "Tag View" page:



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

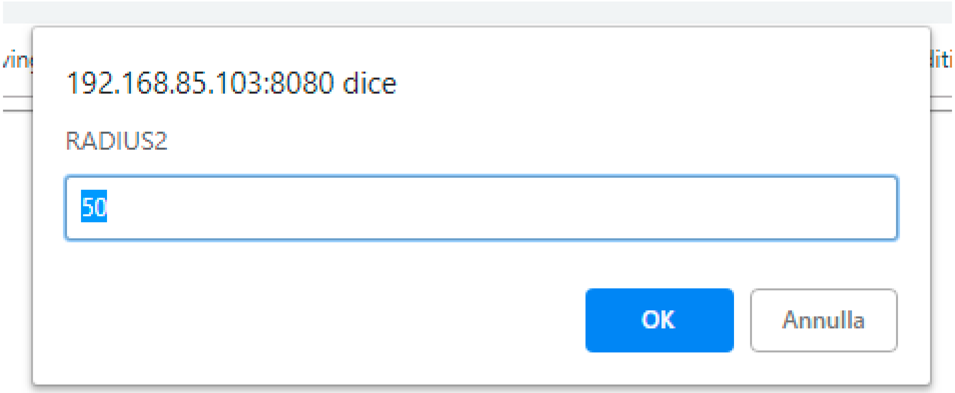
Now change RADIUS1 = 100 and RADIUS2 = 50 by clicking the "CHANGE" button:



192.168.85.103:8080 dice

RADIUS1

100

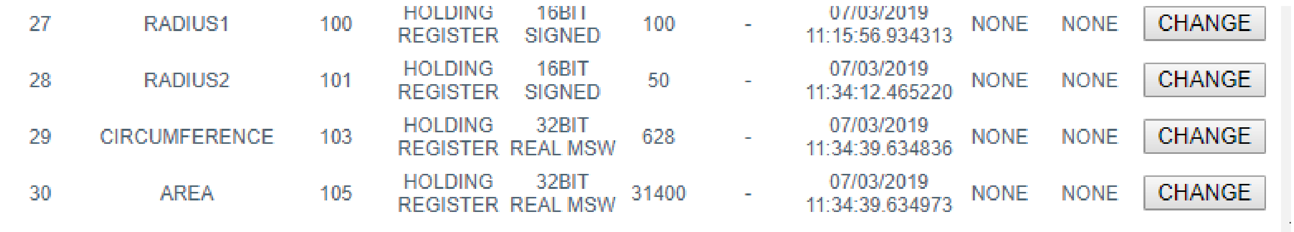


192.168.85.103:8080 dice

RADIUS2

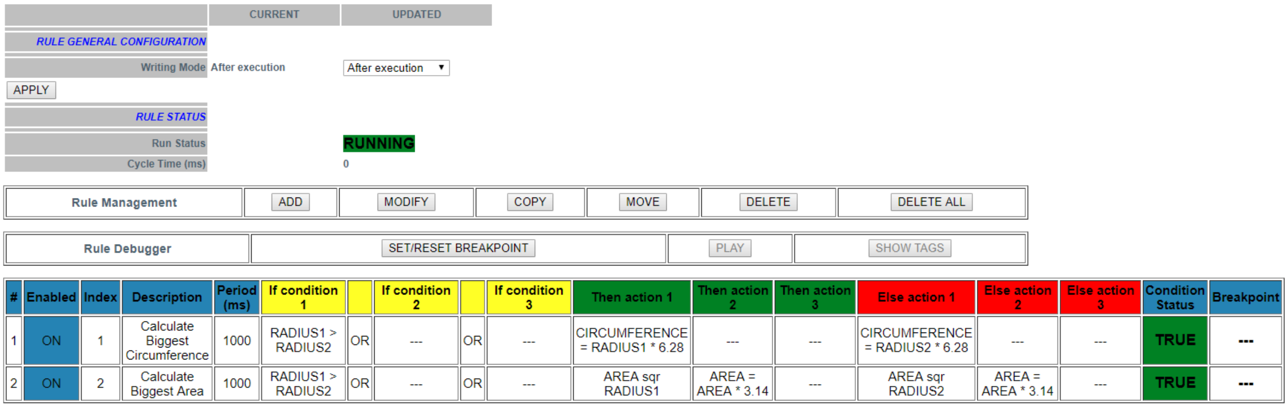
50

In the Tag view the CIRCONFERENCE and AREA calculations are updated:



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

Now we can go to the "Rules Mamagement" page to view the result:



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

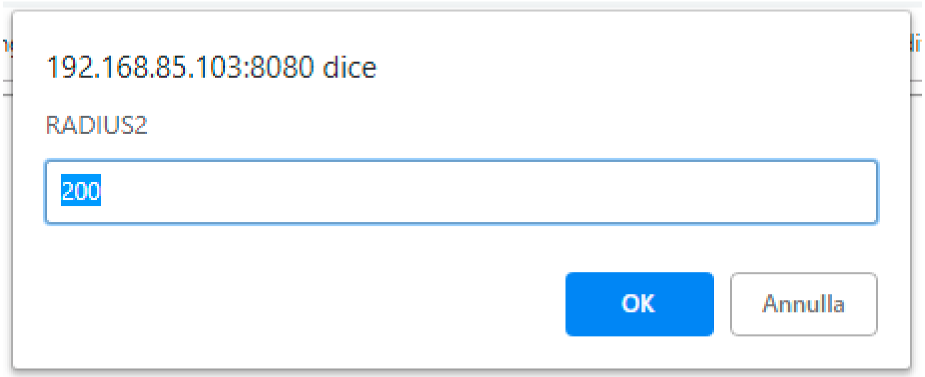
Rule Management | ADD | MODIFY | COPY | MOVE | DELETE | DELETE ALL

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	---

So both conditions if they are TRUE (penultimate column) and then "Then actions" are executed.

Now we change the RADIUS2 value in the tag display pages to 200:

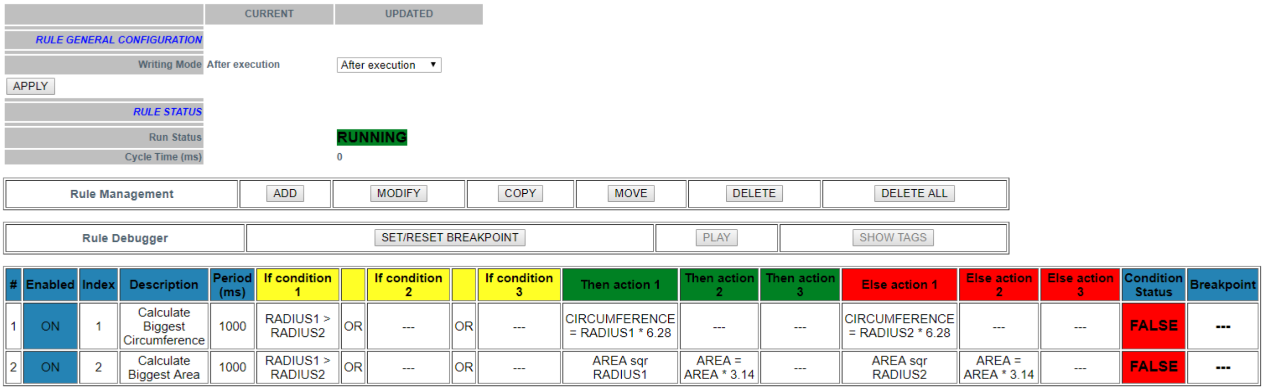


192.168.85.103:8080 dice

RADIUS2

200

So:



	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

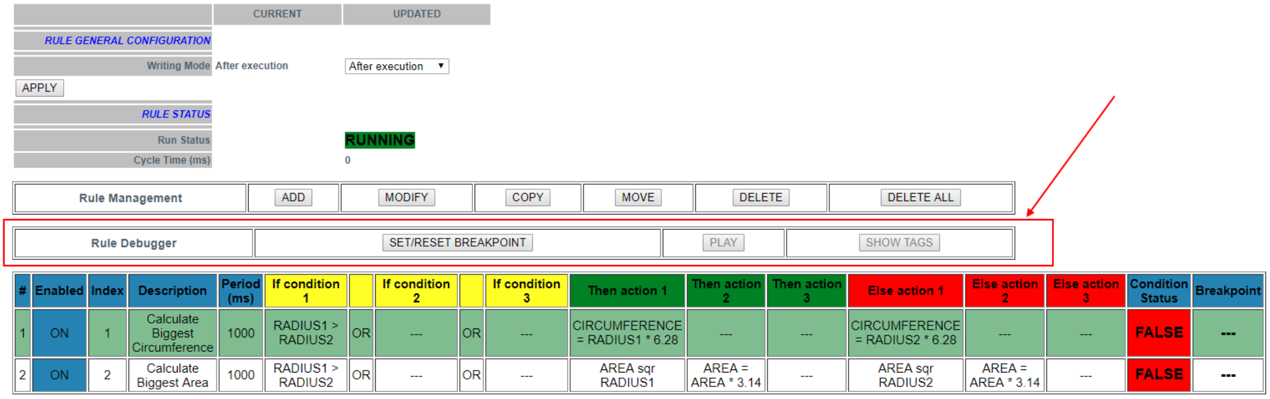
Rule Debugger | SET/RESET BREAKPOINT | PLAY | SHOW TAGS

#	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	---

Now the condition status of the 2 rules is false because RADIUS1 <RADIUS2, so the "Else Actions" are executed

It is also possible to debug the program using the internal rule debugger.
With the internal debugger it is possible:
-Insert a breakpoint before the execution of a rule
-View the tag values before / after the execution of a rule

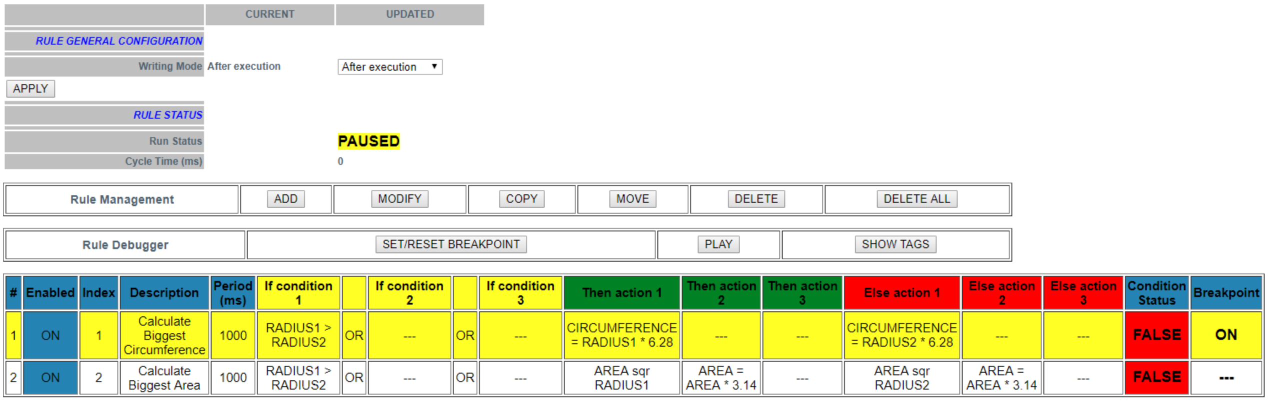
To add a breakpoint and stop the program flow select the rule and then press "SET / RESET BREAKPOINT":


	CURRENT	UPDATED
RULE GENERAL CONFIGURATION		
Writing Mode	After execution	After execution ▼

APPLY

RULE STATUS	
Run Status	RUNNING
Cycle Time (ms)	0

#	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	---

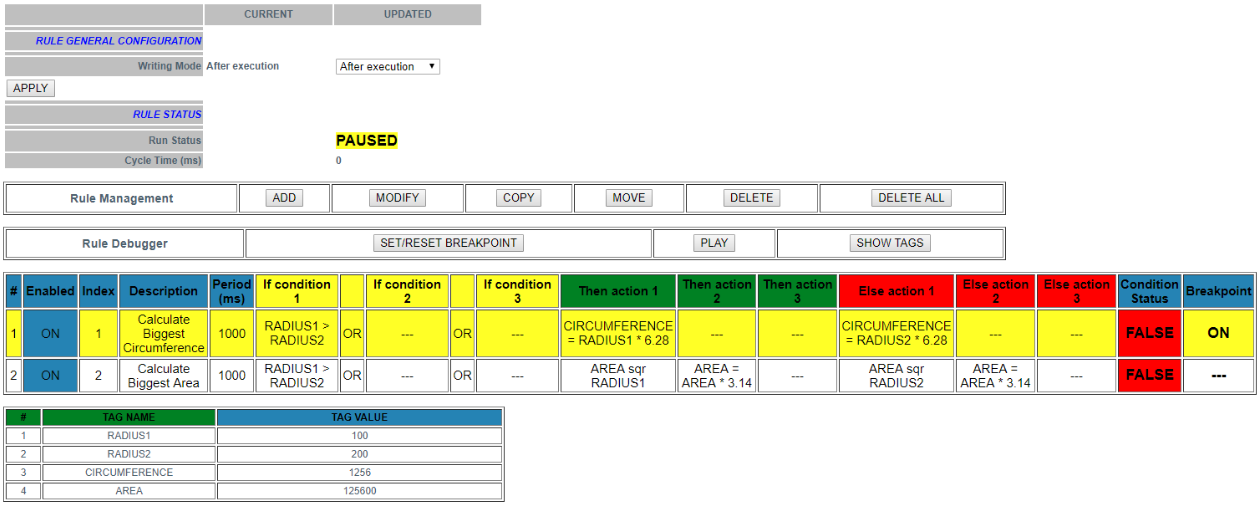

	CURRENT	UPDATED
RULE GENERAL CONFIGURATION		
Writing Mode	After execution	After execution ▼

APPLY

RULE STATUS	
Run Status	PAUSED
Cycle Time (ms)	0

#	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	---

The rule turns yellow and the rule status changes to "Paused". Note that the breakpoint is before the rule execution.
Clicking "Show tags" displays the tag values before the selected rule is executed.



	CURRENT	UPDATED
RULE GENERAL CONFIGURATION		
Writing Mode	After execution	After execution ▾

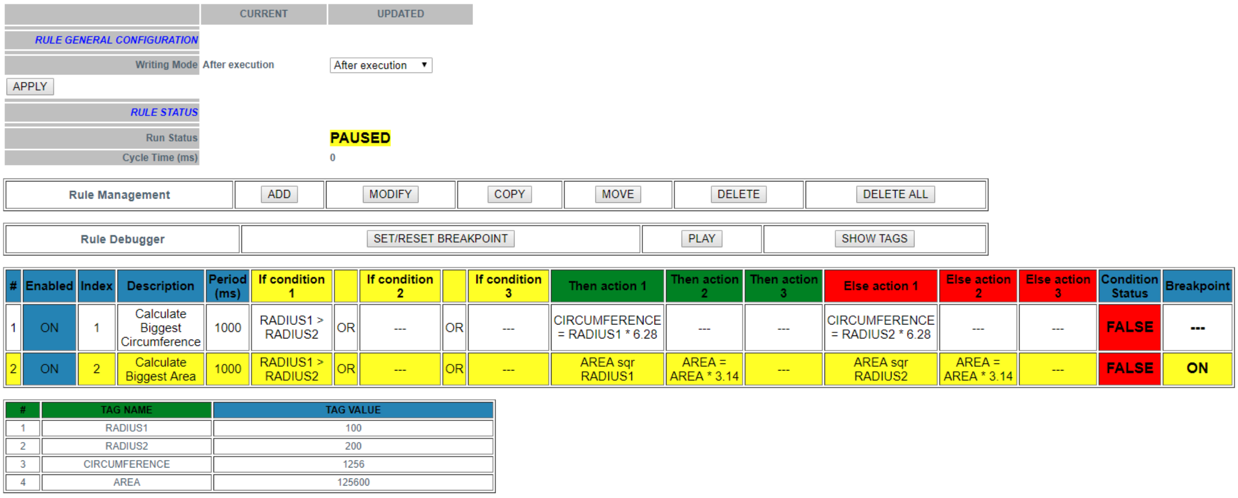
APPLY

RULE STATUS		
Run Status		PAUSED
Cycle Time (ms)		0

#	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	---

#	TAG NAME	TAG VALUE
1	RADIUS1	100
2	RADIUS2	200
3	CIRCUMFERENCE	1256
4	AREA	125600

Now you can move the breakpoint to the next rule, then select the next rule and press the "SET / RESET BREAKPOINT" button:
Pressing the "PLAY" button will stop the execution before the next rule is executed:



	CURRENT	UPDATED
RULE GENERAL CONFIGURATION		
Writing Mode	After execution	After execution ▾

APPLY

RULE STATUS		
Run Status		PAUSED
Cycle Time (ms)		0

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

#	TAG NAME	TAG VALUE
1	RADIUS1	100
2	RADIUS2	200
3	CIRCUMFERENCE	1256
4	AREA	125600

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

This section allows to define ithe general parameters of the datalogger, in particular to edit how the content of the logs will look like.
The datalogger works with the following protocols:
-Copy to USB,
-EMAIL sending
-FTP sending
-Post http (if active only for group 1)
-Send MQTT (will only send from group 1, the other groups are also available for the other protocols)

In this section there is a special enable for sending logs on http because it is possible to use the http channel even only for sending notifications.
-Sending order: The most recent or oldest files are sent first (in case of failure to communicate with the server, the device will buffer the data and send it as soon as the server becomes available according to this logic).
-And you can also configure: the format of the date and time of the sample, the type of separator, the number of decimal places, the presence or absence of further columns, etc.

22.34. GROUP CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

Here it is possible to select which of the 4 log groups should be activated and the type of log to be made.
I is possible to set a group "disabled".
It is possible to activate the following datalogger modes for each of the 4 groups:

Field	Meaning
Sampling Mode	Disabled: the group is disabled. -Periodic: All configured tags are acquired with the set time -Periodic and trigger: All configured tags are acquired with the set time and on trigger action. The trigger action can be configured in the logic section see 22.32 (when a certain series of conditions are fulfilled, the trigger action is executed and the tags are forced to be acquired).
Sampling Period (s)	This parameter defines the sampling period, in seconds. Minimum: 1 s, Maximum: 7200 s
Transfer Period (min)	This parameter defines the transfer period, in minutes; i.e. each time interval defined by this parameter the log file is closed and transferred. Minimum: 1 min, Maximum: 43200 min

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

This page allows you to download the log files to your PC.
It is also possible to send files to the device.

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

Allows you to access the files saved on the connected USB stick.

22.37. ETHERNET INTERFACES

The addresses and statistics of the device's Ethernet ports are shown here.

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

This is a serial sniffer useful for analyzing serial traffic. It is also possible to export the traffic for later analysis.

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

To connect to an M-Bus fieldbus it is necessary to carry out the following steps:
1) connect the optional RS232-MBUS Seneca “Z-MBUS” adapter to the COM1 serial port;
2) setting the COM1 mode to M-BUS.

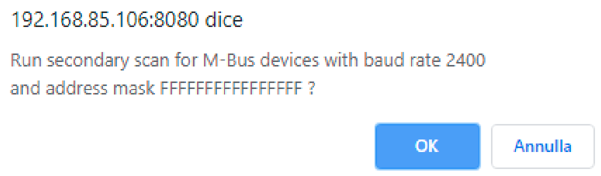
The following resources are available to manage M-Bus devices:
- the web pages of the "M-Bus" section.
- the MBUS_READ_CTL function
- the MBUS_WRITE_RAW function block

The M-BUS web pages allow you to scan the bus, search for devices, detect their primary or secondary addresses; it also allows you to read data records and slave information from a device and create configuration files for import into the Straton PLC.
The MBUS_READ_CTL FB allows you to start/stop the M-BUS acquisition;
the MBUS_WRITE_RAW FB allows you to build and send a generic M-Bus frame, thus providing a flexible way to send configuration commands to M-Bus devices.

22.39.1. M-BUS SCAN

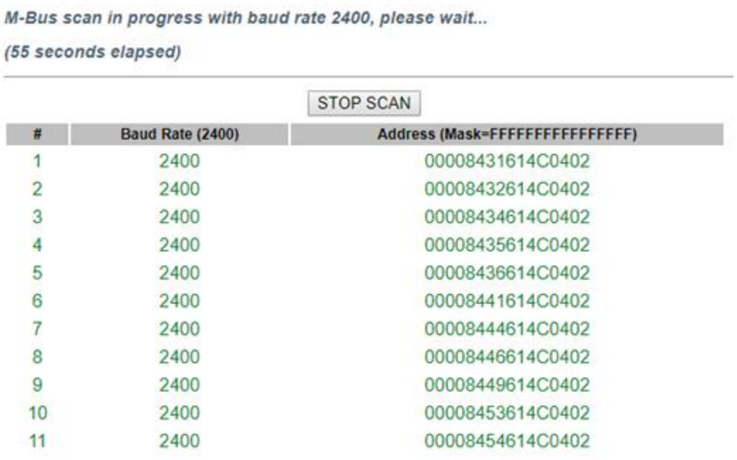
The “SECONDARY SCAN” button lets you scan the bus, detecting M-Bus secondary addresses; select the correct baud-rate for the COM1 serial port or select “All” to repeat the scan for any possible baud-rate[1]; then click on the button; a confirmation pop-up will be shown.

The "SECONDARY SCAN" button allows you to scan the bus, detecting the M-Bus secondary addresses; select the correct baud-rate for the COM1 serial port or select “ALL” to repeat the scan for each possible baud-rate; then click the button; a confirmation pop-up will appear.


192.168.85.106:8080 dice

Run secondary scan for M-Bus devices with baud rate 2400
and address mask FFFFFFFFFFFFFFFF ?

The scanning procedure may take several minutes to complete, so the page shows the number of seconds that have elapsed; devices are displayed in terms of secondary address and baud rate as soon as they are detected.

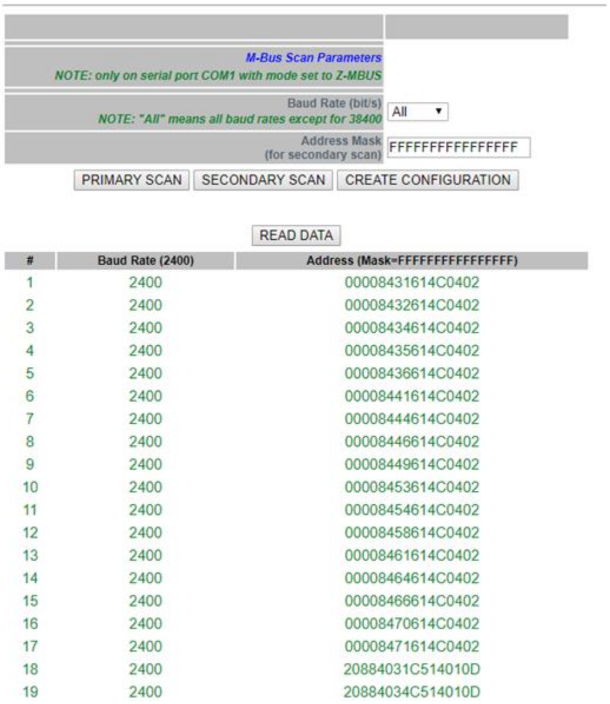


M-Bus scan in progress with baud rate 2400, please wait...

(55 seconds elapsed)

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

The "STOP SCAN" button allows you to cancel the procedure; however the partial results are kept. At the end of the procedure, the webserver indicates the end of the scan and then the following page is displayed:



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

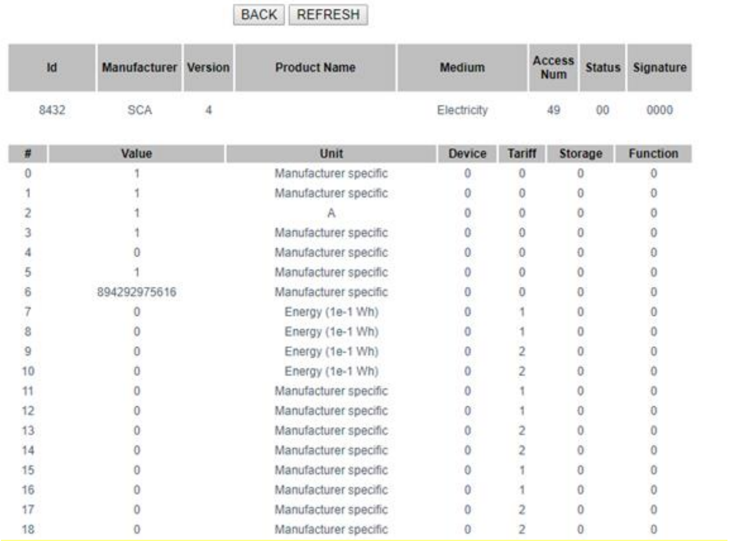
Address Mask (for secondary scan): FFFFFFFFFFFFFFFF

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

The baud rate value shown in the table header reminds you of the parameter choice for the last scan procedure. The table with the detected M-Bus devices is stored permanently, so after switching the CPU off and on again the results of the last scan are still available; they will be overwritten by the next scan or deleted by a factory reset.

Similarly, the "PRIMARY SCAN" button allows you to scan the bus, detecting the primary M-Bus addresses; select the correct baud-rate for the COM1 serial port or select “All” to repeat the scan for every possible baud-rate.

It is possible to read the data from one of the devices, selecting the corresponding row and clicking on the "READ DATA" button, for example:



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 this page:

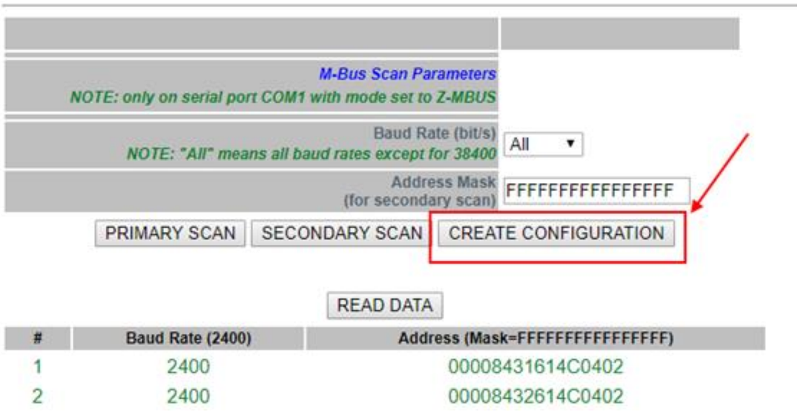
- the first table contains only one line, which provides the "slave information";

- the second table contains a variable number of rows, each of which supplies a "data record".

By clicking on the "REFRESH" button it is possible to update the data; by clicking on the "BACK" button you return to the page with the device table.

22.39.2.“CREATE CONFIGURATION” BUTTON

Now you can go back to the previous pages and press the "CREATE CONFIGURATION" button.



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

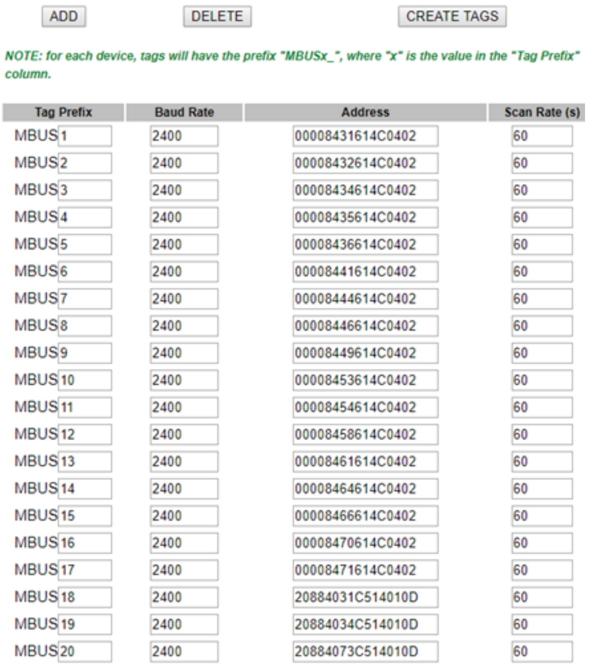
Address Mask (for secondary scan): FFFFFFFFFFFFFFFF

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

This saves the current M-BUS configuration. The web server automatically moves to the next page of "M-Bus Configuration".

22.39.3.M-Bus Configuration

After pressing the "Create configuration" button in the M-Bus Scan page you get the following page in the M-Bus configuration:



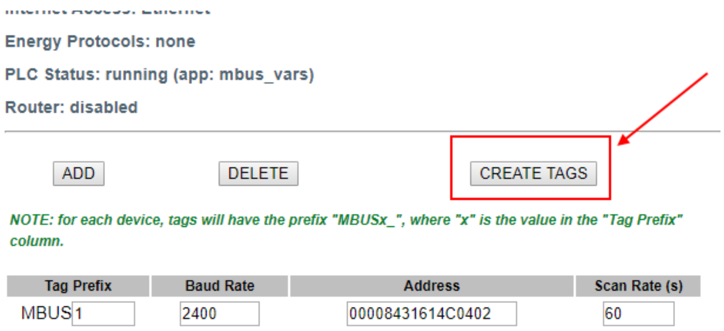
NOTE: for each device, tags will have the prefix "MBUSx_", where "x" is the value in the "Tag Prefix" column.

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

The scan result can now be edited.
The first column represents the Tag Prefix name in Straton
The second column represents the Baud Rate to use.
The third column represents the device address.
The fourth column represents the scan time in seconds for this device.

22.39.4. IMPORTING THE CONFIGURATION INTO STRATON

First of all we need to export the current configuration.


Internet Access: Ethernet

Energy Protocols: none

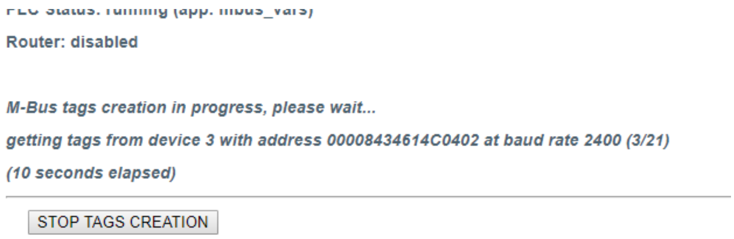
PLC Status: running (app: mbus_vars)

Router: disabled

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

Tag Prefix	Baud Rate	Address	Scan Rate (s)
MBUS 1	2400	00008431614C0402	60

Now the automatic acquisition of tags starts:



PLC status: running (app: mbus_vars)

Router: disabled

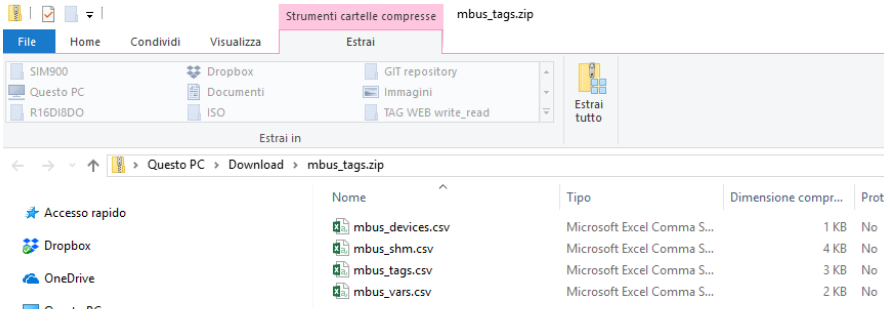
M-Bus tags creation in progress, please wait...

getting tags from device 3 with address 00008434614C0402 at baud rate 2400 (3/21)

(10 seconds elapsed)

At the end of the process a .zip file (mbus_tags.zip) will be downloaded by the browser:

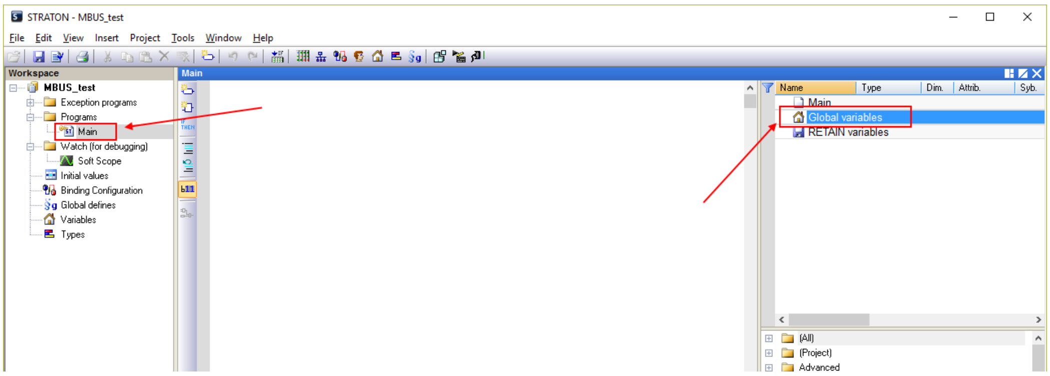
The .zip file contains 4 files:



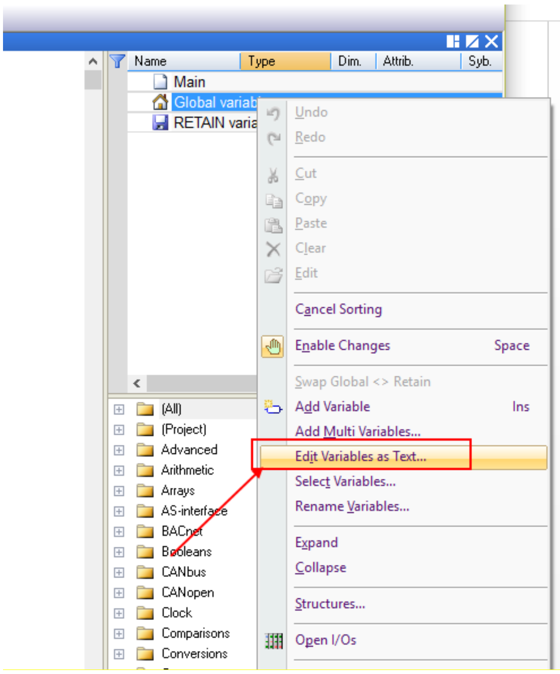
Nome	Tipo	Dimensione compr...	Prot
mbus_devices.csv	Microsoft Excel Comma S...	1 KB	No
mbus_shm.csv	Microsoft Excel Comma S...	4 KB	No
mbus_tags.csv	Microsoft Excel Comma S...	3 KB	No
mbus_vars.csv	Microsoft Excel Comma S...	2 KB	No

Two of these files are to be used in Straton:
mbus_shm.csv (the shared memory configuration)
mbus_vars.csv (the M-Bus vars)
At this point, perform the following steps:

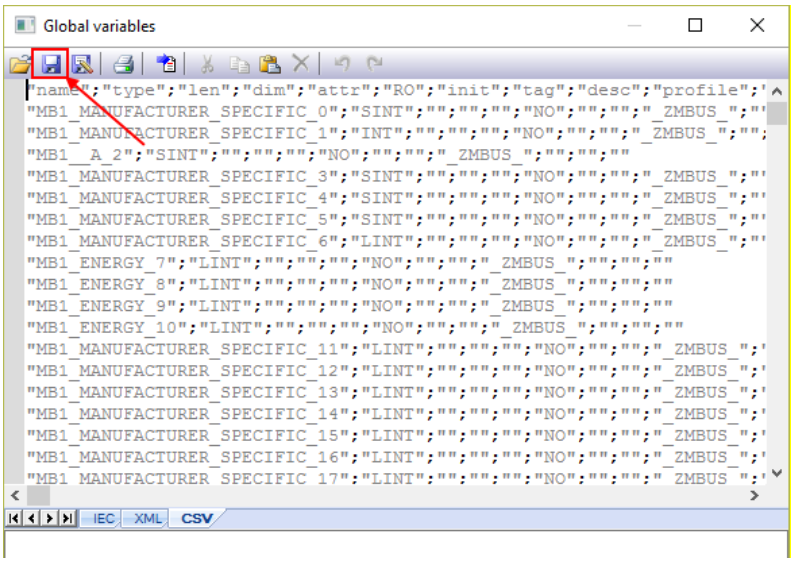
1) Extract the zip file to a directory.
2) Start Straton workbench
3) Select main and then Global variables:



Click the right mouse button and select “Edit Variables as Text”:



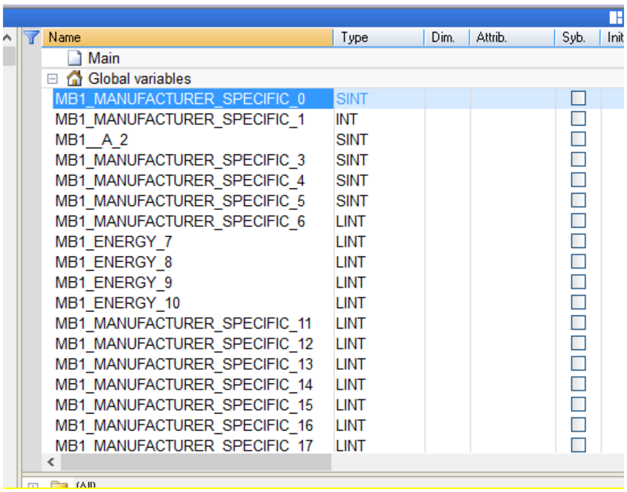
Open the “mbus_vars.csv” file with a text editor, copy and paste the list of variables into the "Global variables" module in Straton then save the configuration with the "disk" icon:



```
"name";"type";"len";"dim";"attr";"RO";"init";"tag";"desc";"profile";'
"MB1_MANUFACTURER_SPECIFIC_0";"SINT";"";"";"";"NO";"";"";"_ZMBUS_";"'
"MB1_MANUFACTURER_SPECIFIC_1";"INT";"";"";"";"NO";"";"";"_ZMBUS_";"";
"MB1__A_2";"SINT";"";"";"";"NO";"";"";"_ZMBUS_";"";"";""
"MB1_MANUFACTURER_SPECIFIC_3";"SINT";"";"";"";"NO";"";"";"_ZMBUS_";"'
"MB1_MANUFACTURER_SPECIFIC_4";"SINT";"";"";"";"NO";"";"";"_ZMBUS_";"'
"MB1_MANUFACTURER_SPECIFIC_5";"SINT";"";"";"";"NO";"";"";"_ZMBUS_";"'
"MB1_MANUFACTURER_SPECIFIC_6";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";"'
"MB1_ENERGY_7";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";"";"";""
"MB1_ENERGY_8";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";"";"";""
"MB1_ENERGY_9";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";"";"";""
"MB1_ENERGY_10";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";"";"";""
"MB1_MANUFACTURER_SPECIFIC_11";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";'
"MB1_MANUFACTURER_SPECIFIC_12";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";'
"MB1_MANUFACTURER_SPECIFIC_13";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";'
"MB1_MANUFACTURER_SPECIFIC_14";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";'
"MB1_MANUFACTURER_SPECIFIC_15";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";'
"MB1_MANUFACTURER_SPECIFIC_16";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";'
"MB1_MANUFACTURER_SPECIFIC_17";"LINT";"";"";"";"NO";"";"";"_ZMBUS_";'
```

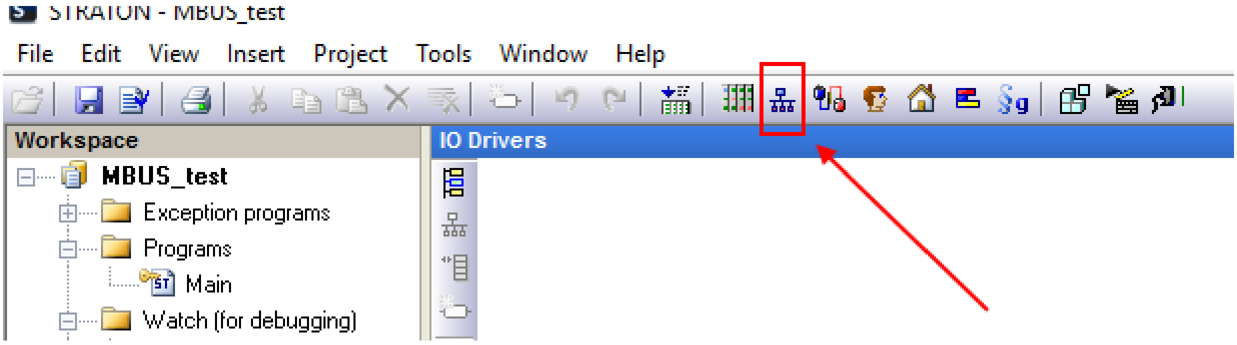
NOTE: The first line
"name";"type";"len";...
must occur only once and only on the first line.

Now the variables are imported:

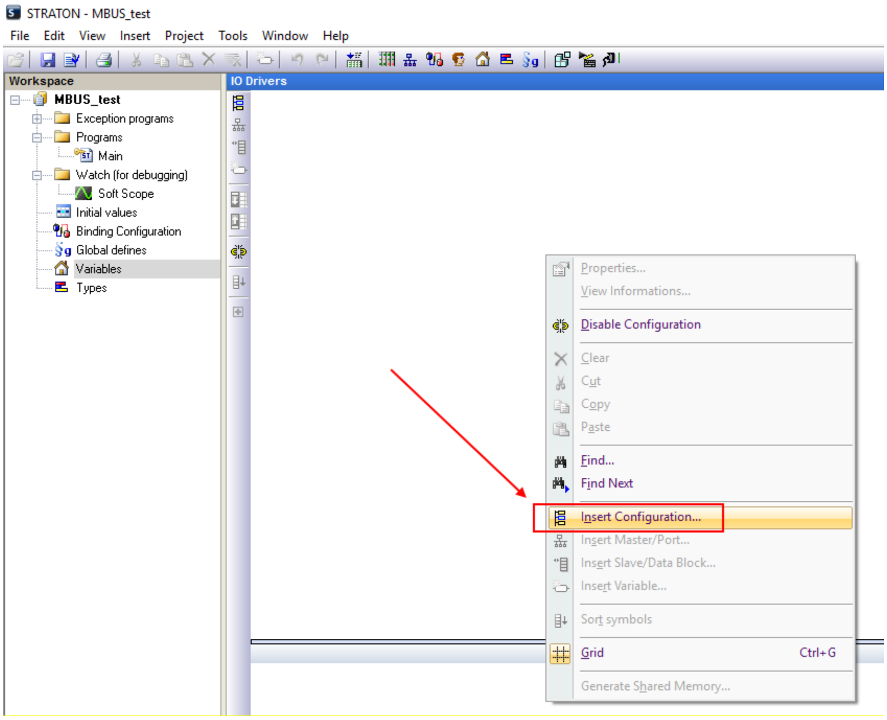


Name	Type	Dim.	Attrib.	Syb.	Init
Main					
Global variables					
MB1_MANUFACTURER_SPECIFIC_0	SINT			□	
MB1_MANUFACTURER_SPECIFIC_1	INT			□	
MB1__A_2	SINT			□	
MB1_MANUFACTURER_SPECIFIC_3	SINT			□	
MB1_MANUFACTURER_SPECIFIC_4	SINT			□	
MB1_MANUFACTURER_SPECIFIC_5	SINT			□	
MB1_MANUFACTURER_SPECIFIC_6	LINT			□	
MB1_ENERGY_7	LINT			□	
MB1_ENERGY_8	LINT			□	
MB1_ENERGY_9	LINT			□	
MB1_ENERGY_10	LINT			□	
MB1_MANUFACTURER_SPECIFIC_11	LINT			□	
MB1_MANUFACTURER_SPECIFIC_12	LINT			□	
MB1_MANUFACTURER_SPECIFIC_13	LINT			□	
MB1_MANUFACTURER_SPECIFIC_14	LINT			□	
MB1_MANUFACTURER_SPECIFIC_15	LINT			□	
MB1_MANUFACTURER_SPECIFIC_16	LINT			□	
MB1_MANUFACTURER_SPECIFIC_17	LINT			□	

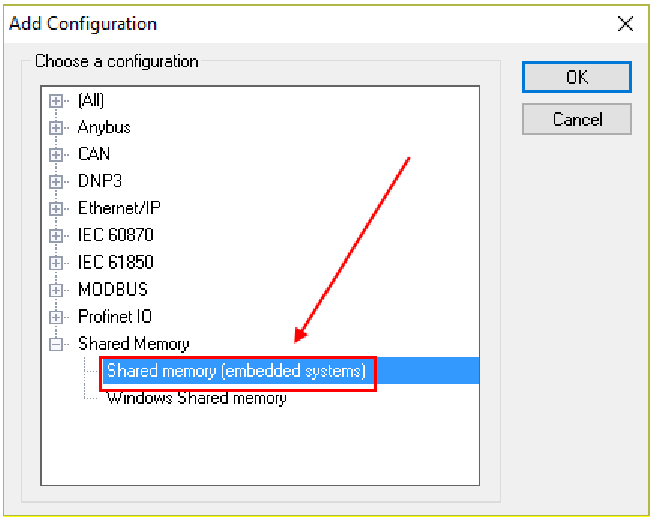
Now we need to create the shared memory used to share data from M-BUS:
Click on the fieldbus icon:



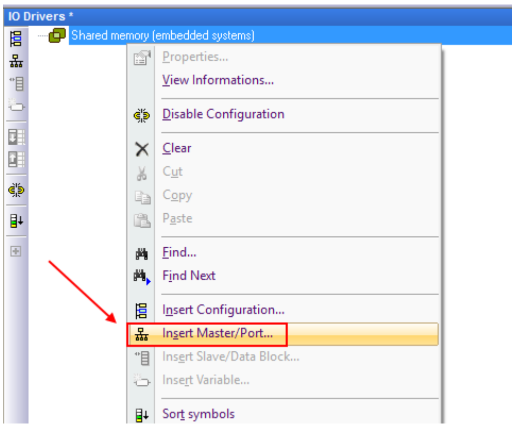
Right-click and select “Insert Configuration”:



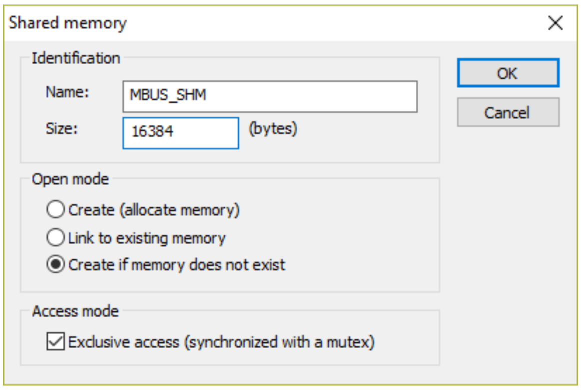
Now create the Shared Memory:



Enter a Master port:



The shared memory configuration must be as shown in the figure (do not change the setting):


Shared memory

Identification

Name: MBUS_SHM

Size: 16384 (bytes)

Open mode

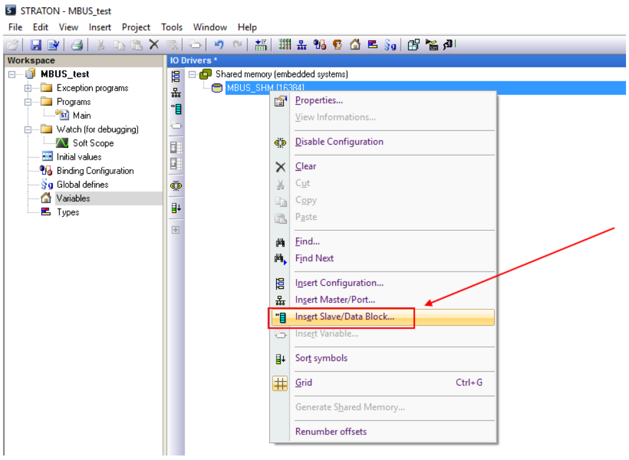
○ Create (allocate memory)
○ Link to existing memory
● Create if memory does not exist

Access mode

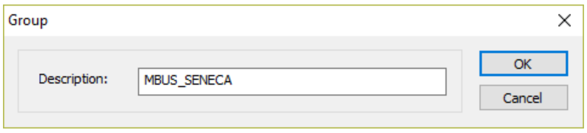
☑ Exclusive access (synchronized with a mutex)

OK
Cancel

Now insert the data block:



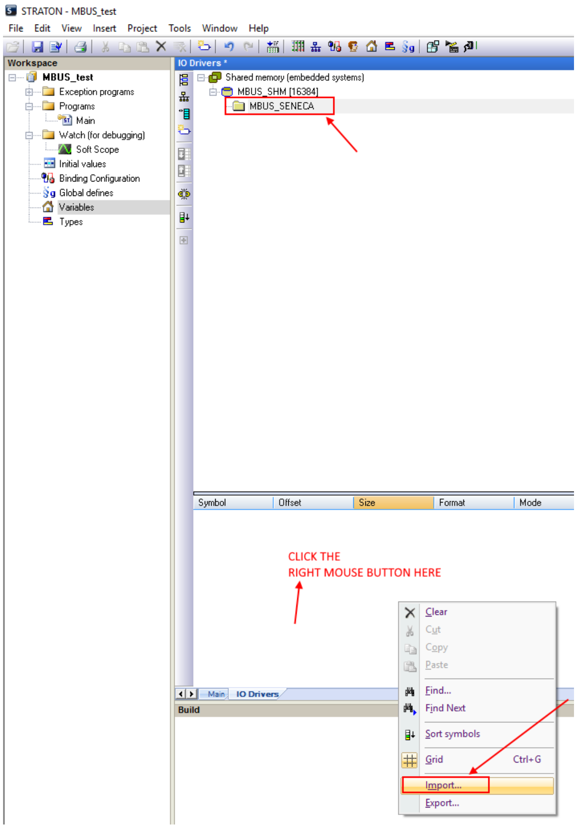
Create a Group and enter a name:



Group

Description: MBUS_SENECA

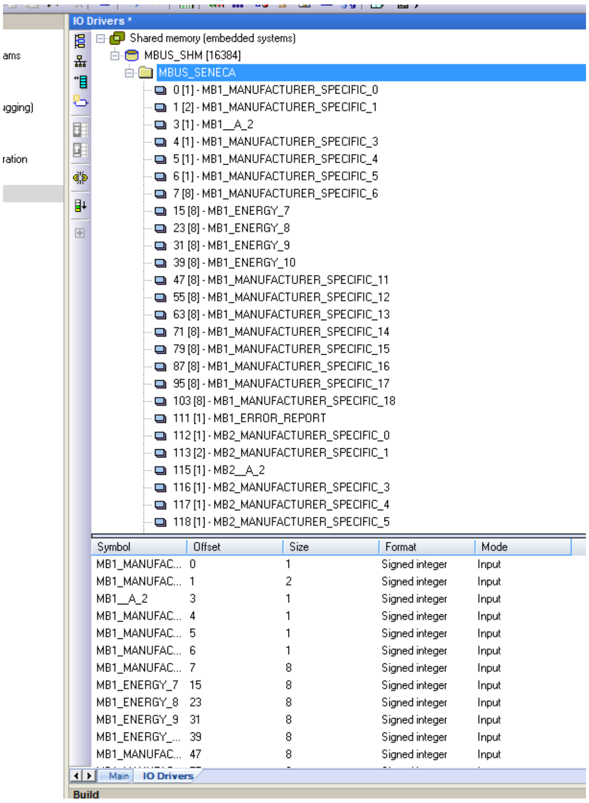
Now import the shared memory file:



STRATON - MBUS_test

CLICK THE RIGHT MOUSE BUTTON HERE

Select the “mbus_shm.csv” file:

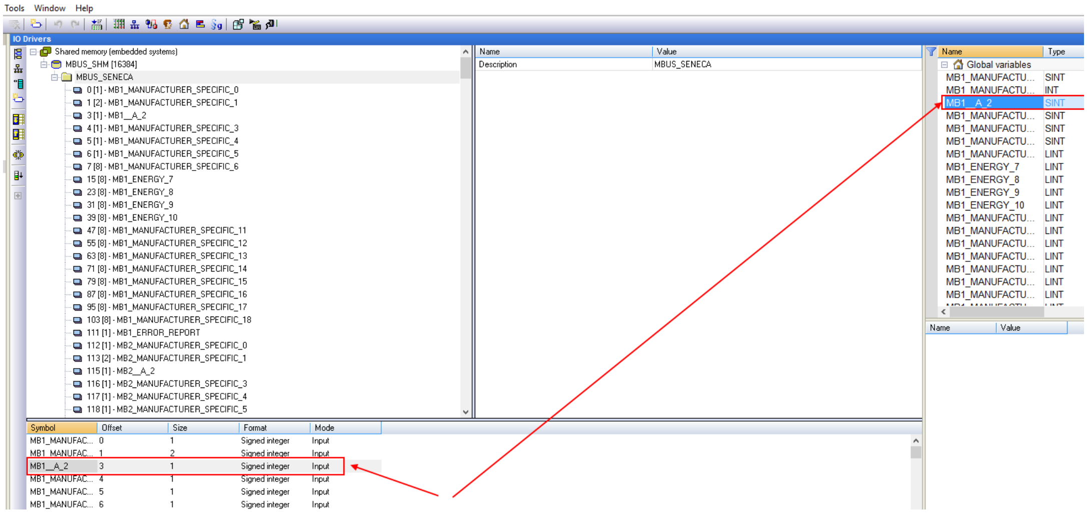


- Shared memory (embedded systems)
  - MBUS_SHM [16384]
    - MBUS_SENECA
      - 0 [1] - MB1_MANUFACTURER_SPECIFIC_0
      - 1 [2] - MB1_MANUFACTURER_SPECIFIC_1
      - 3 [1] - MB1__A_2
      - 4 [1] - MB1_MANUFACTURER_SPECIFIC_3
      - 5 [1] - MB1_MANUFACTURER_SPECIFIC_4
      - 6 [1] - MB1_MANUFACTURER_SPECIFIC_5
      - 7 [8] - MB1_MANUFACTURER_SPECIFIC_6
      - 15 [8] - MB1_ENERGY_7
      - 23 [8] - MB1_ENERGY_8
      - 31 [8] - MB1_ENERGY_9
      - 39 [8] - MB1_ENERGY_10
      - 47 [8] - MB1_MANUFACTURER_SPECIFIC_11
      - 55 [8] - MB1_MANUFACTURER_SPECIFIC_12
      - 63 [8] - MB1_MANUFACTURER_SPECIFIC_13
      - 71 [8] - MB1_MANUFACTURER_SPECIFIC_14
      - 79 [8] - MB1_MANUFACTURER_SPECIFIC_15
      - 87 [8] - MB1_MANUFACTURER_SPECIFIC_16
      - 95 [8] - MB1_MANUFACTURER_SPECIFIC_17
      - 103 [8] - MB1_MANUFACTURER_SPECIFIC_18
      - 111 [1] - MB1_ERROR_REPORT
      - 112 [1] - MB2_MANUFACTURER_SPECIFIC_0
      - 113 [2] - MB2_MANUFACTURER_SPECIFIC_1
      - 115 [1] - MB2__A_2
      - 116 [1] - MB2_MANUFACTURER_SPECIFIC_3
      - 117 [1] - MB2_MANUFACTURER_SPECIFIC_4
      - 118 [1] - MB2_MANUFACTURER_SPECIFIC_5

Symbol	Offset	Size	Format	Mode
MB1_MANUFAC...	0	1	Signed integer	Input
MB1_MANUFAC...	1	2	Signed integer	Input
MB1__A_2	3	1	Signed integer	Input
MB1_MANUFAC...	4	1	Signed integer	Input
MB1_MANUFAC...	5	1	Signed integer	Input
MB1_MANUFAC...	6	1	Signed integer	Input
MB1_MANUFAC...	7	8	Signed integer	Input
MB1_ENERGY_7	15	8	Signed integer	Input
MB1_ENERGY_8	23	8	Signed integer	Input
MB1_ENERGY_9	31	8	Signed integer	Input
MB1_ENERGY_...	39	8	Signed integer	Input
MB1_MANUFAC...	47	8	Signed integer	Input

22.39.5. DELETING UNUSED MBUS VARIABLES

To delete one or more variables delete the variables and the corresponding shared memory entry:



- Shared memory (embedded systems)
  - MBUS_SHM [16384]
    - MBUS_SENECA
      - 0 [1] - MB1_MANUFACTURER_SPECIFIC_0
      - 1 [2] - MB1_MANUFACTURER_SPECIFIC_1
      - 3 [1] - MB1__A_2
      - 4 [1] - MB1_MANUFACTURER_SPECIFIC_3
      - 5 [1] - MB1_MANUFACTURER_SPECIFIC_4
      - 6 [1] - MB1_MANUFACTURER_SPECIFIC_5
      - 7 [8] - MB1_MANUFACTURER_SPECIFIC_6
      - 15 [8] - MB1_ENERGY_7
      - 23 [8] - MB1_ENERGY_8
      - 31 [8] - MB1_ENERGY_9
      - 39 [8] - MB1_ENERGY_10
      - 47 [8] - MB1_MANUFACTURER_SPECIFIC_11
      - 55 [8] - MB1_MANUFACTURER_SPECIFIC_12
      - 63 [8] - MB1_MANUFACTURER_SPECIFIC_13
      - 71 [8] - MB1_MANUFACTURER_SPECIFIC_14
      - 79 [8] - MB1_MANUFACTURER_SPECIFIC_15
      - 87 [8] - MB1_MANUFACTURER_SPECIFIC_16
      - 95 [8] - MB1_MANUFACTURER_SPECIFIC_17
      - 103 [8] - MB1_MANUFACTURER_SPECIFIC_18
      - 111 [1] - MB1_ERROR_REPORT
      - 112 [1] - MB2_MANUFACTURER_SPECIFIC_0
      - 113 [2] - MB2_MANUFACTURER_SPECIFIC_1
      - 115 [1] - MB2__A_2
      - 116 [1] - MB2_MANUFACTURER_SPECIFIC_3
      - 117 [1] - MB2_MANUFACTURER_SPECIFIC_4
      - 118 [1] - MB2_MANUFACTURER_SPECIFIC_5

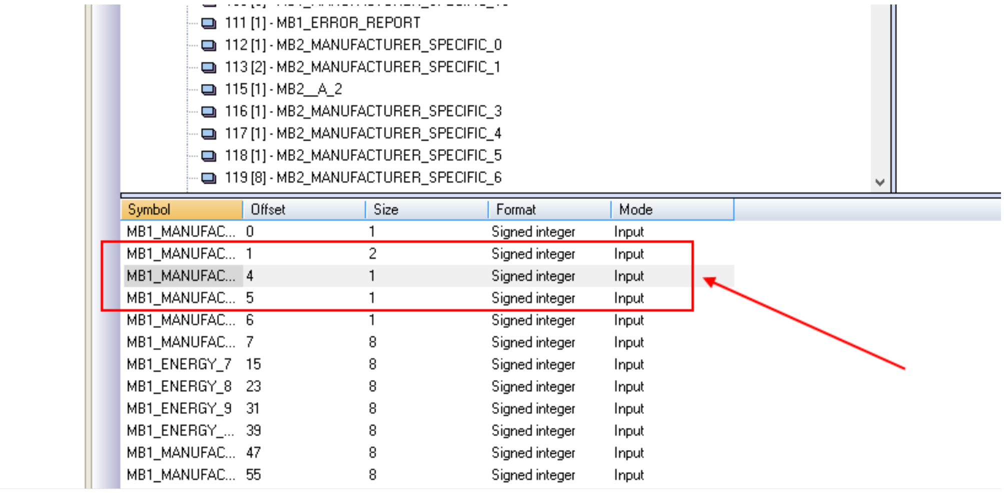
Name	Value
Description	MBUS_SENECA

Name	Type
Global variables	
MB1_MANUFACTU...	SINT
MB1_MANUFACTU...	INT
MB1__A_2	SINT
MB1_MANUFACTU...	SINT
MB1_MANUFACTU...	SINT
MB1_MANUFACTU...	SINT
MB1_MANUFACTU...	LINT
MB1_ENERGY_7	LINT
MB1_ENERGY_8	LINT
MB1_ENERGY_9	LINT
MB1_ENERGY_10	LINT
MB1_MANUFACTU...	LINT
MB1_MANUFACTU...	LINT
MB1_MANUFACTU...	LINT
MB1_MANUFACTU...	LINT
MB1_MANUFACTU...	LINT
MB1_MANUFACTU...	LINT
MB1_MANUFACTU...	LINT

Name	Value

Symbol	Offset	Size	Format	Mode
MB1_MANUFAC...	0	1	Signed integer	Input
MB1_MANUFAC...	1	2	Signed integer	Input
MB1__A_2	3	1	Signed integer	Input
MB1_MANUFAC...	4	1	Signed integer	Input
MB1_MANUFAC...	5	1	Signed integer	Input
MB1_MANUFAC...	6	1	Signed integer	Input

Note that in the shared memory the offsets of other variables are not changed:



111 [1] - MB1_ERROR_REPORT
112 [1] - MB2_MANUFACTURER_SPECIFIC_0
113 [2] - MB2_MANUFACTURER_SPECIFIC_1
115 [1] - MB2__A_2
116 [1] - MB2_MANUFACTURER_SPECIFIC_3
117 [1] - MB2_MANUFACTURER_SPECIFIC_4
118 [1] - MB2_MANUFACTURER_SPECIFIC_5
119 [8] - MB2_MANUFACTURER_SPECIFIC_6

Symbol	Offset	Size	Format	Mode
MB1_MANUFAC...	0	1	Signed integer	Input
MB1_MANUFAC...	1	2	Signed integer	Input
MB1_MANUFAC...	4	1	Signed integer	Input
MB1_MANUFAC...	5	1	Signed integer	Input
MB1_MANUFAC...	6	1	Signed integer	Input
MB1_MANUFAC...	7	8	Signed integer	Input
MB1_ENERGY_7	15	8	Signed integer	Input
MB1_ENERGY_8	23	8	Signed integer	Input
MB1_ENERGY_9	31	8	Signed integer	Input
MB1_ENERGY_...	39	8	Signed integer	Input
MB1_MANUFAC...	47	8	Signed integer	Input
MB1_MANUFAC...	55	8	Signed integer	Input

22.39.6. REPLACING AN M-BUS DEVICE

To replace an existing M-BUS device (e.g. in case of replacement due to failure)

1. Go to M-BUS Scan and do a Secondary or Primary Scan

2. Make a note of the new address

3. Go to M-BUS Configuration and manually change the address from the old to the new device

4. Press the "Create Tag" button.

5. There is no need to make any modifications to the Straton

22.39.7.ADDING AN M-BUS DEVICE

1. Go to “M-BUS Scan” and run a secondary or primary scan
2. Note the new address and baud rate
3. Go to "M-BUS Configuration" and manually add the address and baud rate of the new device with the "ADD" button
4. Press the "Create Tag" button.
5. Import the shared memory file
6. Import the variable file without deleting your local variable (use copy-paste)

22.39.8.DELETING AN MBUS DEVICE

1. Go to M-BUS Scan and do a Secondary or Primary Scan

2. Note the address of the device to be deleted

3. Go to "M-BUS Configuration" and manually delete the device with the "Delete" button.

4. Press the "Create Tag" button.

5. Import the shared memory file

6. Delete the variables from the deleted device

22.39.9.“TAG ERROR REPORT” SPECIAL TAG

When variable tags are imported into Straton, a special "Tag error report" tag is created.
Use this tag to monitor device communication errors:

VALUE OF THE “ERORR REPORT” TAG	***MEANING***
0	READING OK
-2	READING IN TIMEOUT, NO ANSWER FROM THE DEVICE

22.40. FIRMWARE VERSION

Returns the current firmware revision and the firmware on the emergency partition.

22.41. FIRMWARE UPGRADE

Allows you to update the firmware of the device.

22.42. MANAGEMENT CONF.

Allows you to export or import the configuration of the device (useful if you need to copy the configuration to another device).
It is also possible to save the system log files (debug log) to be sent to Seneca support.

22.43. LICENCE MANAGEMENT (SSD ONLY)

Here you can check which optional features are enabled under "Optional Features".
It is also possible to enter the activation keys provided by Seneca to add optional features to the device.
For more information please refer to Seneca support.

22.44. WEBSERVER WITH "GUEST" ACCOUNT

It is possible to access the device configuration site with a “guest” account; this account is allowed to access all pages except for the "FW Upgrade", "Configuration Management" and "USB File Manager", displaying all the configuration parameters and status information, without changing any parameters; therefore, in all pages, the "APPLY" buttons (and any other button used to make changes) are disabled.

To log in with a "guest" account, connect your browser to the IP address of the device on port 8080, for example:
http://192.168.90.101:8080
and, when required, provide the following credentials (default values):
Username: guest
Password: guest

22.45. WEBSERVER WITH "USER" ACCOUNT

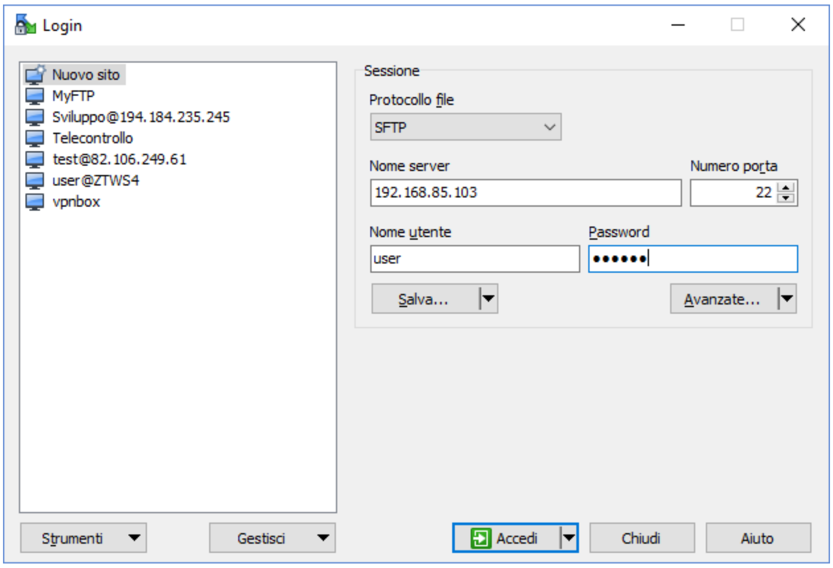
It is possible to access to the device configuration site with a "user" account; this account can only access the "Summary" and "Tag View" pages.
To log in with a "user" account, connect your browser to the IP address of the device on port 8080, for example:
http://192.168.90.101:8080
and, when required, provide the following credentials (default values):
Username: user
Password: user

22.46. FTP / SFTP ACCESS

To easily access the device via FTP / SFTP, you can for example use the WINSCP program; you can download WINSCP for free from:
http://winscp.net/eng/download.php

Set the connection as in the following figure (the screen shows a connection to IP address 192.168.85.103):

The credentials (username and password) are those ("user", "123456") set for "FTP USER".
After clicking on the "Login" button, a new window will appear, as in the following screen; on the right you can copy and delete files directly on / from the device.

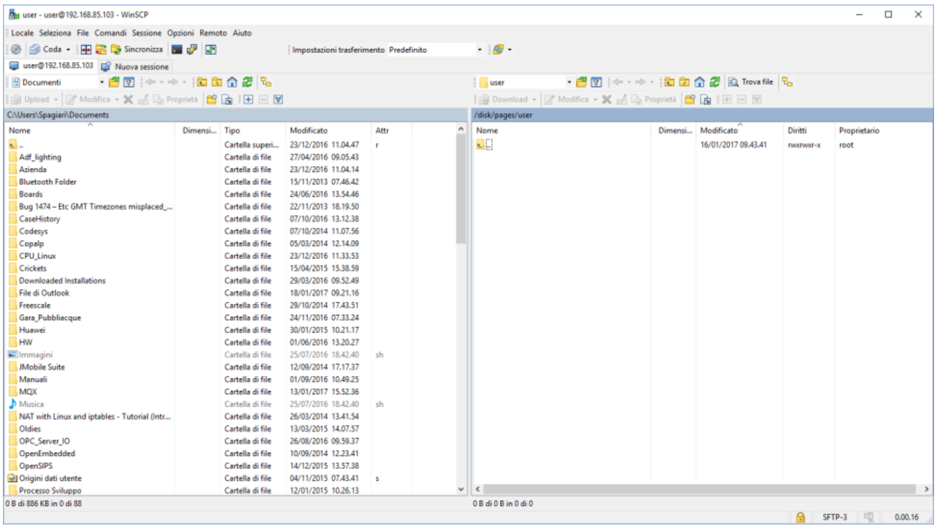


Login

- Nuovo sito
- MyFTP
- Sviluppo@194.184.235.245
- Telecontrollo
- test@82.106.249.61
- user@ZTWS4
- vpnbox

Sessione
Protocollo file: SFTP
Nome server: 192.168.85.103
Numero porta: 22
Nome utente: user
Password: ••••••

The WinSCP program can be used as both an FTP and SFTP client to transfer files from/to the device; just select the "FTP" or "SFTP" protocol in the "WinSCP Access" window; normally, it's best to use SFTP, as it provides a secure (i.e. encrypted) service.


user - user@192.168.85.103 - WinSCP
Locale Seleziona File Comandi Sessione Opzioni Remoto Aiuto
Coda
Sincronizza
Impostazioni trasferimento Predefinito
user@192.168.85.103
Nuova sessione
Documenti
Upload
Modifica
Proprietà
user
Trova file
Download
Modifica
Proprietà
SFTP-3
0.00.16

C:\Users\Spagiari\Documents

Nome	Dimensi...	Tipo	Modificato	Attr
..		Cartella superi...	23/12/2016 11.04.47	r
Adf_lighting		Cartella di file	27/04/2016 09.05.43	
Azienda		Cartella di file	23/12/2016 11.04.14	
Bluetooth Folder		Cartella di file	15/11/2013 07.46.42	
Boards		Cartella di file	24/06/2016 13.54.46	
Bug 1474 – Etc GMT Timezones misplaced_...		Cartella di file	22/11/2013 18.19.50	
CaseHistory		Cartella di file	07/10/2016 13.12.38	
Codesys		Cartella di file	07/10/2014 11.07.56	
Copalp		Cartella di file	05/03/2014 12.14.09	
CPU_Linux		Cartella di file	23/12/2016 11.33.53	
Crickets		Cartella di file	15/04/2015 15.38.59	
Downloaded Installations		Cartella di file	29/03/2016 09.52.49	
File di Outlook		Cartella di file	18/01/2017 09.21.16	
Freescale		Cartella di file	29/10/2014 17.43.51	
Gara_Pubbliacque		Cartella di file	24/11/2016 07.33.24	
Huawei		Cartella di file	30/01/2015 10.21.17	
HW		Cartella di file	01/06/2016 13.20.27	
Immagini		Cartella di file	25/07/2016 18.42.40	sh
JMobile Suite		Cartella di file	12/09/2014 17.17.37	
Manuali		Cartella di file	01/09/2016 10.49.25	
MQX		Cartella di file	13/01/2017 15.52.36	
Musica		Cartella di file	25/07/2016 18.42.40	sh
NAT with Linux and iptables - Tutorial (Intr...		Cartella di file	26/03/2014 13.41.54	
Oldies		Cartella di file	13/03/2015 14.07.57	
OPC_Server_IO		Cartella di file	26/08/2016 09.59.37	
OpenEmbedded		Cartella di file	10/09/2014 12.23.41	
OpenSIPS		Cartella di file	14/12/2015 13.57.38	
Origini dati utente		Cartella di file	04/11/2015 07.43.41	s
Processo Sviluppo		Cartella di file	12/01/2015 10.26.13	

0 B di 886 KB in 0 di 88

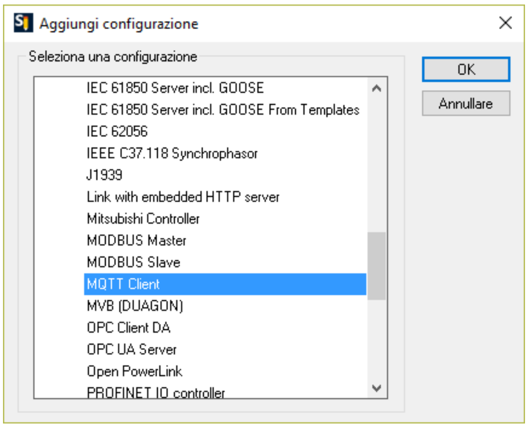
/disk/pages/user

Nome	Dimensi...	Modificato	Diritti	Proprietario
..		16/01/2017 09.43.41	rwxrwxr-x	root

0 B di 0 B in 0 di 0

23. MQTT CLIENT PROTOCOL (R-PASS-S, Z-PASS2-RT-S, Z-TWS4-RT-S ONLY)

The MQTT version supported is 3.1.1
To use the MQTT protocol it is necessary to use Straton workbench 9.3 or later.
To use the MQTT client select it from the Straton Workbench Fieldbus section:

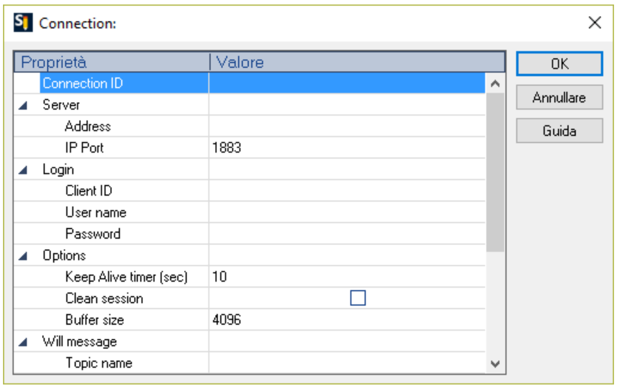


Seleziona una configurazione

- IEC 61850 Server incl. GOOSE
- IEC 61850 Server incl. GOOSE From Templates
- IEC 62056
- IEEE C37.118 Synchrophasor
- J1939
- Link with embedded HTTP server
- Mitsubishi Controller
- MODBUS Master
- MODBUS Slave
- MQTT Client
- MVB (DUAGON)
- OPC Client DA
- OPC UA Server
- Open PowerLink
- PROFINET IO controller

23.1. PARAMETERS OF THE MQTT PROTOCOL FROM THE PLC PROGRAM

MQTT setup can be done directly from the workbench:



Proprietà	Valore
Connection ID	
◢ Server	
Address	
IP Port	1883
◢ Login	
Client ID	
User name	
Password	
◢ Options	
Keep Alive timer (sec)	10
Clean session	□
Buffer size	4096
◢ Will message	
Topic name	

If it is necessary to configure these parameters from the Straton PLC program, a series of special words can be used which will load the configuration from a file.
The special words are:
In the "Address" field type: mqtt_par_address so that the "Address" field is obtained from the file:

/var/run/mqtt_par_address

In the “Client ID” field type: mqtt_par_clientid so that the “Client ID” field is obtained from the file: /var/run/mqtt_par_clientid
In the "Username" field type: mqtt_par_username so that the "Username" field is obtained from the file:

/var/run/mqtt_par_username

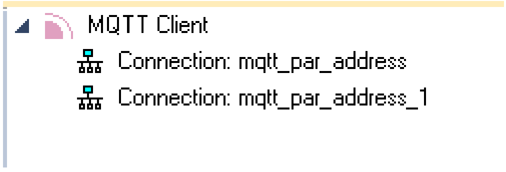
In the "Password" field type: mqtt_par_password so that the "Password" field is obtained from the file:
/var/esegui/mqtt_par_password

Warning!

the Address parameter must not contain an FQDN, but the IP address, this is because the FB MQTTCONNECT does not perform DNS resolution.
Alternatively, it may contain the name of the file (e.g.: mqtt_par_address), created in the /var/run directory by the FB DNS_RESOLVE and containing the result of DNS resolution.

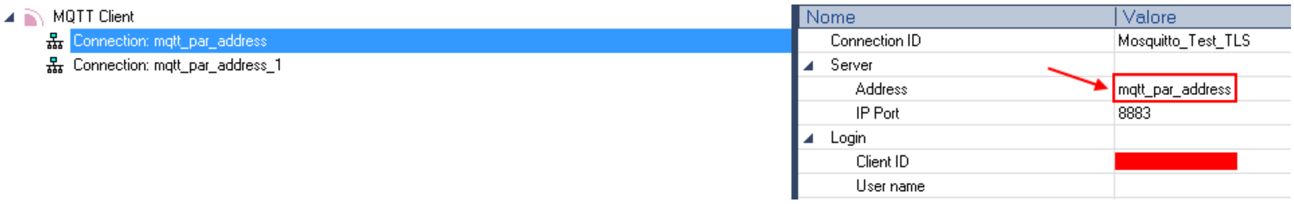
23.1.1. MANAGING MULTIPLE MQTT CONNECTIONS

It is possible to manage multiple MQTT connections using parameters starting with the special words (mqtt_par_address123, mqtt_par_address_aaa, …), for example to create 2 mqtt connections:



MQTT Client
- Connection: mqtt_par_address
- Connection: mqtt_par_address_1

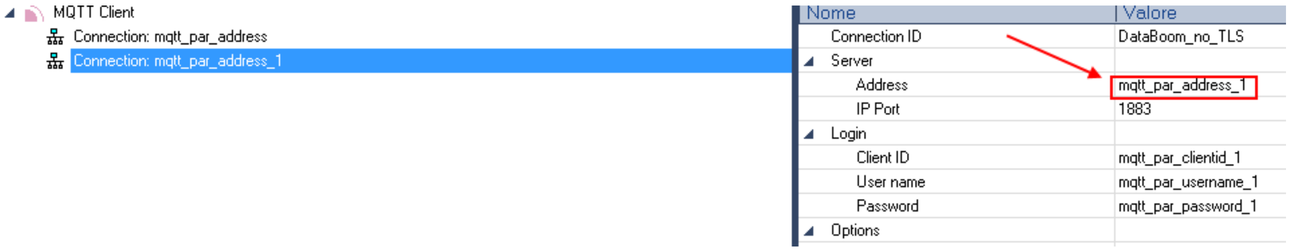
The first connection uses the Field address “mqtt_par_address”



MQTT Client
- Connection: mqtt_par_address
- Connection: mqtt_par_address_1

Nome	Valore
Connection ID	Mosquitto_Test_TLS
Server	
Address	mqtt_par_address
IP Port	8883
Login	
Client ID	[redacted]
User name	

Then it will load the address from the file:
/var/run/mqtt_par_address
The second connection uses the stored address “mqtt_par_address_1”



MQTT Client
- Connection: mqtt_par_address
- Connection: mqtt_par_address_1

Nome	Valore
Connection ID	DataBoom_no_TLS
Server	
Address	mqtt_par_address_1
IP Port	1883
Login	
Client ID	mqtt_par_clientid_1
User name	mqtt_par_username_1
Password	mqtt_par_password_1
Options	

this will load the address from the file:
/var/run/mqtt_par_address_1
(the technique can also be used for the other client id, username and password parameters).

23.2. MQTT CONFIGURATION OF SSL/TLS RETRYs

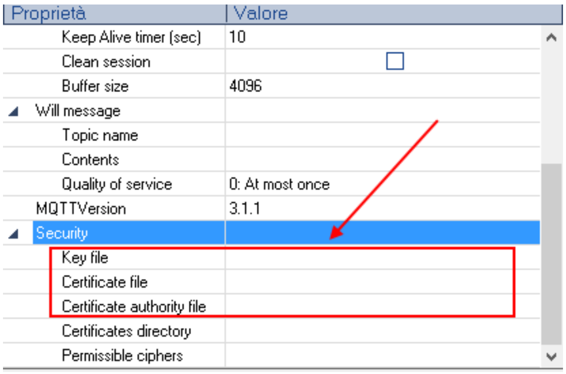
The default configuration for MQTT SSL/TLS connection is:
CONN _TRY_MAX = 10
CONN_TRY_WAIT = 1000 ms
Where:
CONN _TRY_MAX is the number of attempts to connect.
CONN_TRY_WAIT is the timeout of each connection attempt.
If you need to change this default configuration you need to create the file:
“ssl_con_try_params”
In this path:
“/var/esegui/”
With parameter values, for example:

```
root@Z-PASS2-S:~# cat /var/run/ssl_conn_try_params
50.200
```

It means CONN _TRY_MAX = 50 and CONN_TRY_WAIT = 200 ms.
NOTE1: At the end of the file you need to add an \n (new line character)
NOTE2: The file is loaded into a RAM filesystem, so you need to create it on every boot.

23.3. STATIC AND DYNAMIC CLIENT CERTIFICATES

In the MQTT configuration under the Security section you can enter the path and file name for the certificates:



Proprietà	Valore
Keep Alive timer (sec)	10
Clean session	□
Buffer size	4096
◢ Will message	
Topic name	
Contents	
Quality of service	0: At most once
MQTTVersion	3.1.1
◢ Security	
Key file	
Certificate file	
Certificate authority file	
Certificates directory	
Permissible ciphers	

Seneca suggests using the /config directory for certificates.
The MQTT client certificate can only be uploaded from the FTP server.
The key file is the client's private key file.
The certificate file is the client certificate.
The certification authority file is the certification authority certificate.

Warning!

The field "Certificate directory" is not used, so the file name must contain the absolute path e.g: "/config/mqtt/client.key".

If these files and other parameters need to be modified dynamically without recompiling the project, a file can be loaded into the /var/run directory with a file name that must start respectively with:
"mqtt_par_clientkey", "mqtt_par_clientcert", "mqtt_par_cacert"
The content of the files must be a text with the file name without the path.
Note that more than one certificate file can be used in a program, for example “mqtt_par_clientcert00”, “mqtt_par_clientcert01” etc...

23.4. CHANGING MQTT PARAMETERS IN RUNTIME VIA FILE

You can change the port and the keepalive configuration by overwriting the current configuration with the following files in runtime:
"mqtt_par_port" and "mqtt_par_keepalive".

The content of the files must be a text with the new parameter value.

24. FACTORY RESET

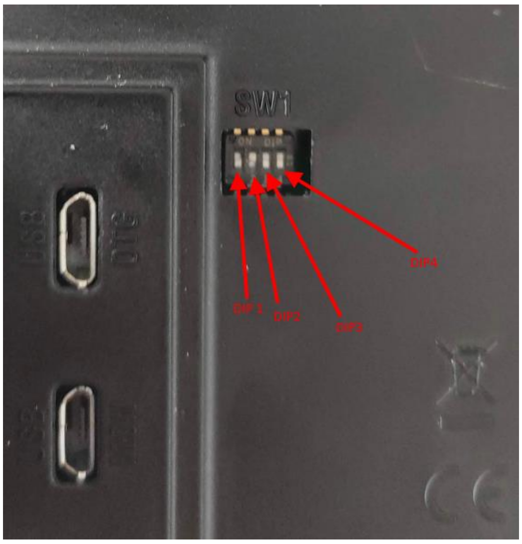
With this procedure it is possible to obtain

1) All the parameters at the factory
2) All folders are cleared (and therefore all data log files and debugging files are deleted).

24.1. FACTORY RESET FOR SSD

To obtain a factory reset follow the following procedure:

1) Turn off the device
2) Reach the back of the device and locate the dip switches as shown in the picture:



3) Bring the dip switches in: DIP1 = OFF, DIP2 = ON, DIP3 = ON, DIP4 = ON
4) Switch the device on and wait until it has completed charging
5) With the device switched on, bring the dips in: DIP1 = OFF, DIP2 = ON, DIP3 = OFF, DIP4 = OFF

24.2. FACTORY RESET FOR R-PASS AND R-PASS-S

To obtain a factory reset follow the following procedure:

1) Turn off the device
2) Reach the back of the device and locate the dip switches as shown in the picture:

3) Bring the dip switches in: DIP1 = OFF, DIP2 = ON, DIP3 = ON, DIP4 = ON
4) Switch the device on and wait until it has completed charging
5) With the device switched on, bring the dips in: DIP1 = OFF, DIP2 = ON, DIP3 = OFF, DIP4 = OFF

24.3. FACTORY RESET FOR Z-PASS1-RT, Z-PASS2-RT, Z-TWS4-RT-S, Z-PASS2-RT-S

To obtain a factory reset follow the following procedure:

1) Turn off the device
2) Reach the back of the device by removing the cover on the bottom of the device and locate the DIP SW1 set
3) Bring the dip switches in: DIP1 = ON, DIP2 = ON, DIP3 = ON, DIP4 = OFF, DIP5=ON, DIP6 =ON
4) Switch the device on and wait until it has completed charging
5) Bring the dips to: DIP1 = ON, DIP2 = ON, DIP3 = ON, DIP4 = OFF, DIP5=OFF, DIP6 =OFF

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

The maintenance mode can be activated via webserver or via modbus tcp-ip/RTU.
In the maintenance mode the tags cannot be written via the panel but only via the protocols (ethernet and serial).
To enable the "maintenance mode" set the value of the "Maintenance Mode" register to 1.

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

26.1. SSD

The registers representing I/Os are accessible via Modbus TCP-IP or RTU protocols and are shown in the table below:

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

The registers representing the digital I/Os are accessible via Modbus TCP-IP or RTU protocol and are shown in the table below:

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

The registers representing the digital I/Os are accessible via Modbus TCP-IP or RTU protocol and are shown in the table below:

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. SMS Commands (R-PASS and Z-PASS2-RT models only)

On R-PASS+R-COMM and Z-PASS2-RT-4G devices, a number of features can be controlled by means of “SMS commands”; such features include setting up a mobile data (PPP) connection, activating the VPN Box functionality, setting a digital output etc.

SMS Commands can be sent by phone numbers that are present in the device Phonebook as “admin” or “manager” users; as an alternative, any phone number can send an SMS command, provided that the command contains a “password”; the password is made by the last four digits of the modem IMEI; so the command will have the following format (there must be a blank character between the “password” and the command text):

```
<last four IMEI digits> <command text>
```

Example:

```
6172 PPP ON
```

Please note that the command text can be written in any letter case, all uppercase, all lowercase or a mix between the two.

Any SMS command received from a number that is not recognized as an “admin” or “manager” user and does not contain the password will be discarded; as an option, these messages and all messages that are not recognized as valid commands can be “relayed” to the “admin” user.

Example:

```
PPP ON RELAYED
```

SMS commands substantially fall into two categories:

- "set" commands which execute an action
- "get" commands which ask for some information

While "get" commands always have an answer, "set commands" can be given an answer ("acknowledge") or not, depending on a configuration parameter.
Any response to a command, both "set" or "get", will contain the original message text, plus a result string, which can be:

"EXECUTING"
meaning that the command has been correctly processed; the "ING" form is used to tell that the procedure started by the command might not be completed yet
"FAILED"
meaning that the command could not be processed or something failed; in this case, an error string is present giving the failure reason
Examples:

```
PPP ON EXECUTING (100.70.179.88)
```

```
PPP ON FAILED (System PPP ON)
```

Obviously, the response to a "get" command also contains the requested info, if the command has been successfully processed.
Example:

```
GET DIN EXECUTING (1,0,0,0)
```

Finally, the whole SMS commands functionality can be disabled, if not needed, by means of a configuration parameter.
In the following paragraphs, the full list of supported commands is given along with the corresponding responses.

27.1. PPP ON

This command can be used to set up the mobile data (PPP) connection; the connection is set up using system configuration parameters (APN Mode, APN, Auth Type etc.).
If the command is successfully processed, the response contains the IP address assigned to the PPP network interface.
This command is rejected in the following case:

- if "Remote Connection Disable" (RCD) digital input is HIGH and "Security Level/Service Disable" parameter is set to "Internet Connection", the command will fail with the "Security Level error" error.

Also, if the connection setup procedure is not completed after a timeout (currently fixed to 30 seconds), the command will fail with the "Timeout error" error.

Please note that this command that does not enable the mobile data connection in a persistent way, so if the device is restarted, the mobile data (PPP) connection is not re-established.

Example:

```
→     PPP ON
←     PPP ON EXECUTING (100.70.179.88)
```

27.2. PPP OFF

This command can be used to drop down the mobile data (PPP) connection set up by a previous "PPP ON" command.

Please note that this command does not disable the mobile data connection in a persistent way, so if the device is restarted, the mobile data (PPP) connection is re-established.

This command is never rejected.

Example:

```
→     PPP OFF
←     PPP OFF EXECUTING
```

27.3. PPP IP

This command can be used to get the IP address assigned to the mobile data (PPP) connection; if the PPP connection is not active, the "dummy" IP address (0.0.0.0) will be given.

This command is never rejected.

Example:

```
→     PPP IP
←     PPP IP EXECUTING (100.70.179.88)
```

27.4. PPP CNF

This command can be used to change the value of the system configuration parameters related to the mobile data (PPP) connection; the changes are persistent.

The command shall have the following format, where parameter values shall be separated by a blank character:

```
PPP CNF <APN mode> <APN> <Authentication Type> <Username> <Password> <PPP Connection Testing IP Address>
```

Please note that all the parameters shall be present, in the above order; no parameter can be left empty.

For the meaning of these parameters: <APN> and <Authentication Type> are numeric fields with the following values:

```
APN Mode
0:    Automatic
1:    Manual

Authentication Type
0:    None
1:    CHAP/PAP
2:    CHAP only
3:    PAP only
```

This command is rejected in the following case:

- if any of the command parameters is missing or invalid, the command will fail with the "Command parameter error".

Example:

```
→     PPP CNF 0 mobile.vodafone.it 0 user pass www.google.com
←     PPP CNF EXECUTING
```

27.5. VPN ON

This command can be used to activate the VPN Box functionality; the functionality is activated using system configuration parameters (Server, Password, Tag Name).

The command has two optional parameters, so its format is the following:

```
VPN ON [PPP] [NOFWL]
```
[2]

"PPP"

if this parameter is present, the mobile data (PPP) connection is set up (if it's not already active), before activating the VPN Box functionality

"NOFWL"

if this parameter is present, the "Mobile Network Firewall" is disabled in the system configuration

This command is rejected in the following cases:

- if the "custom" VPN functionality is enabled in the system configuration (parameter "VPN/Enable" = ON, "VPN Mode" = "OpenVPN"), the command will fail with the "System VPN ON" error;
- if "Remote Connection Disable" (RCD) digital input is HIGH and "Security Level/Service Disable" parameter is set to "VPN Connection" or "VPN Service" or "Internet Connection", the command will fail with the "Security Level error" error.

Please note that this command does not activate the VPN Box functionality in a persistent way, so if the device is restarted, the functionality is not re-activated.

Examples:

```
→     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] Square brackets tell that parameter is optional.

27.6. VPN OFF

This command can be used to deactivate the VPN Box functionality activated by a previous “VPN ON” command; it also drops down the mobile data (PPP) connection set up by a previous “VPN ON PPP” command or “PPP ON” command.

This command is never rejected.

Please note that this command does not de-activate the VPN Box functionality in a persistent way, so if the device is restarted, the functionality is re-activated.

Example:

```
→     VPN OFF
←     VPN OFF EXECUTING
```

27.7. VPN CNF

This command can be used to change the value of the system configuration parameters related to the VPN Box functionality; the changes are persistent.

The command shall have the following format, where parameter values shall be separated by a blank character:

```
VPN CNF <Server> <Password> <Tag Name>
```

Please note that all the parameters shall be present, in the above order; no parameter can be left empty.

For the meaning of these parameters.

This command is rejected in the following case:

- if any of the command parameters is missing or invalid, the command will fail with the “Command parameter error”.

Example:

```
→     VPN CNF myvpnbox.seneca.it myvpnbox zpass2-GSP
←     VPN CNF EXECUTING
```

27.8. FWL ON

This command can be used to enable the "Mobile Network Firewall" in the system configuration (parameter "Mobile Network Firewall/Enable" = ON).
This command is never rejected.

Example:

```
→     FWL ON
←     FWL ON EXECUTING
```

27.9. FWL OFF

This command can be used to disable the "Mobile Network Firewall" in the system configuration (parameter "Mobile Network Firewall/Enable" = OFF).
This command is never rejected.

Example:

```
→     FWL OFF
←     FWL OFF EXECUTING
```

27.10. GET DIN

This command can be used to get the status of one or all of the device digital inputs; if a digital input is not available (since it is used as an output)[3], the "0" value is given.

The command can have two formats:

`GET DIN<n>` with <n>=1..N gets the status of a single digital input

where:
N=4 for R-PASS+R-COMM
N=6 for Z-PASS2-RT-4G

`GET DIN` gets the status of all the digital inputs

This command is rejected in the following cases:

- if the digital I/O number in the command is out of range (e.g.: 0 or N+1), the command will fail with the "Command parameter error" error.

Examples:

```
→    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

This command can be used to get the status of one or all of the device digital outputs; if a digital output is not available (since it is used as an input)[4], the "0" value is given.

The command can have two formats:

`GET DOUT<n>` with <n>=1..N gets the status of a single digital output

where:
N=4 for R-PASS+R-COMM
N=6 for Z-PASS2-RT-4G

`GET DOUT` gets the status of all the digital outputs

This command is rejected in the following cases:

[3] This can be true for Z-PASS2-RT-4G.

[4] This can be true for Z-PASS2-RT-4G.

- if the digital I/O number in the command is out of range (e.g.: 0 or N+1), the command will fail with the "Command parameter error" error.

Examples:

```
→     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

This command can be used to set the status of one of the device digital outputs.

The command can have two formats:

`SET DOUT<n>.CLOSE` with <n>=1..N sets the digital output to the HIGH state

`SET DOUT<n>.OPEN` with <n>=1..N sets the digital output to the LOW state

where:
N=4 for R-PASS+R-COMM
N=6 for Z-PASS2-RT-4G

This command is rejected in the following cases:

- if the digital output is not configured as "General output" or the digital I/O is used as an input[5], the command will fail with the "Digital I/O mode error" error;
- if the digital I/O number in the command is out of range (e.g.: 0 or N+1), the command will fail with the "Command parameter error" error;
- if the requested state is neither ".CLOSE", nor ".OPEN", the command will fail with the "Command parameter error" error.

Example:

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

27.13. SET PULSE

This command can be used to generate a pulse on one of the device digital outputs.

The command can have two formats:

`SET PULSE<n>.CLOSE <duration>` with <n>=1..N

[5] This can be true for Z-PASS2-RT-4G.

where:
N=4 for R-PASS+R-COMM
N=6 for Z-PASS2-RT-4G
to generate a LOW-HIGH-LOW pulse, with the HIGH state set for the number of seconds given by the <duration> parameter

`SET PULSE<n>.OPEN <duration>` with <n>=1..N
where:
N=4 for R-PASS+R-COMM
N=6 for Z-PASS2-RT-4G
to generate a HIGH-LOW-HIGH pulse, with the LOW state set for the number of seconds given by the <duration> parameter

This command is rejected in the following cases:

- if the digital output is not configured as “General output” or the digital I/O is used as an input[6], the command will fail with the “Digital I/O mode error” error;
- if the digital I/O number in the command is out of range (e.g.: 0 or N+1), the command will fail with the “Command parameter error” error;
- if the requested state is neither “.CLOSE”, nor “.OPEN”, the command will fail with the “Command parameter error” error;
- if the <duration> parameter is missing or invalid, the command will fail with the “Command parameter error” error;
- if the “.CLOSE” parameter is given and the digital output is already in the HIGH state, the command will fail with the “No pulse generated” error;
- if the “.OPEN” parameter is given and the digital output is already in the LOW state, the command will fail with the “No pulse generated” error.

Example:

```
→     SET PULSE2.CLOSE 10
←     SET PULSE2.CLOSE 10 EXECUTING
```

27.14. SET USER.PHONE

This command can be used to enter a user with the specified telephone number, type and group list into the Phonebook; it can also be used to change the type and/or group list of an already existing user.

The command has the following format:

`SET USER.PHONE +<number> <type> <group list>,` with <type>=`ADM|MGR|USR`

Please note that the telephone number shall always be given in the “international format”, so the initial ‘+’ character shall always be present.

[6] This can be true for Z-PASS2-RT-4G.

The “group list” is a list of non-negative integer numbers, separated by the “-“ character, defining the groups which the user belongs to. Example of valid group lists are:

“1-2-3”
“1-4”
“1”
“0”

The “0” value means that the user is part of any group.

This command is rejected in the following cases:

- if the specified <number> already exists in the Phonebook, with the specified <type> and <group list>, the command will fail with the “Item already exists” error;
- if the <number> parameter is missing or invalid (including the case when the ‘+’ character is missing), the command will fail with the “Command parameter error” error;
- if the <type> parameter is missing or invalid, the command will fail with the “Command parameter error” error;
- if the <group list> parameter is missing or invalid, the command will fail with the “Command parameter error” error.

Example:

```
→    SET USER.PHONE +390123456789 ADM 1-2-3
←    SET USER.PHONE +390123456789 ADM 1-2-3 EXECUTING
```

27.15. RESET PHONE

This command can be used to delete a user with the specified telephone number from the Phonebook.

The command has the following format:

```
RESET PHONE +<number>
```

Please note that the telephone number shall always be given in the “international format”, so the initial ‘+’ character shall always be present.

This command is rejected in the following cases:

- if the specified <number> does not exist in the Phonebook, the command will fail with the “Item does not exist” error;
- if the <number> parameter is missing or invalid (including the case when the ‘+’ character is missing), the command will fail with the “Command parameter error” error.

Example:

```
→    RESET PHONE +390123456789
←    RESET PHONE +390123456789 EXECUTING
```

Please note that, if the Phonebook user with the specified telephone number also has an email address, this will be deleted by the command too.

27.16. SET USER.EMAIL

This command can be used to insert a user with the specified email address, type and group list into the Phonebook; it can also be used to change the type and/or group list of an already existing user.

The command has the following format:

`SET USER.EMAIL <email address> <type> <group list>`, with <type>=`ADM|MGR|USR`

The “group list” is a list of non-negative integer numbers, separated by the “-“ character, defining the groups which the user belongs to. Example of valid group lists are:

“1-2-3”
“1-4”
“1”
“0”

The “0” value means that the user is part of any group.

This command is rejected in the following cases:

- if the specified <email address> already exists in the Phonebook, with the specified <type> and <group list>, the command will fail with the “Item already exists” error;
- if the <email address> parameter is missing or invalid, the command will fail with the “Command parameter error” error;
- if the <type> parameter is missing or invalid, the command will fail with the “Command parameter error” error;
- if the <group list> parameter is missing or invalid, the command will fail with the “Command parameter error” error.

Example:

```
→     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

This command can be used to delete a user with the specified email address from the Phonebook.

The command has the following format:

```
RESET EMAIL <email address>
```

This command is rejected in the following cases:

- if the specified <email address> does not exist in the Phonebook, the command will fail with the “Item does not exist” error;

- if the < email address > parameter is missing or invalid, the command will fail with the "Command parameter error" error.

Example:

```
→    RESET EMAIL admin@zpass.it
←    RESET EMAIL admin@zpass.it EXECUTING
```

Please note that, if the Phonebook user with the specified email address also has a telephone number, this will be deleted by the command too.

27.18. STATUS

This command can be used to get some status information from the device.

The status info given in the response has the following format:

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>,<DIDO2>,<DIDO3>,<DIDO4>,<DIDO5>,<DIDO6>
```

where:

<hwrev>: ""
<date> is in the form "yyyy/mm/dd"
<hour> is in the form "hh:mm:ss"
<service status> reports the status of the "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

This command is never rejected.

Example:

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

[7] See Chapter "LEDs signaling".

27.19. GET GPS

This command can be used to get GPS location info from the device.

The response is given as an URL to Google Maps™:
https://www.google.com/maps/?q=<latitude>,<longitude>

This command is rejected in the following cases:

- If the GPS signal is not available, the command will fail with the “GPS not fixed” error.

Example:

```
→     GET GPS
←     GET                         GPS                         EXECUTING
(https://www.google.com/maps/?q=45.3742,11.94557)
```

27.20. RESET

This command can be used to restart (“reboot”) the device.

This command is never rejected.

Example:

```
→     RESET
←     RESET EXECUTING
```

27.21. GET TAG

This command can be used to get the value of a tag (see “Modbus Shared Memory Gateway” functionality). The command has the following format:

```
GET TAG <tag name>
```

Please note that the “tag name” is case-sensitive; also note that this command assumes that each tag has a distinct name; if more tags exist with the same name, this command returns the value of the first tag found with the given name.

The value is given in the response with the following format:

```
<tag value>,VALID
```

or:

```
<tag value>,INVALID
```

The “INVALID” status may occur for tags with “GATEWAY MODE”=”GATEWAY”, when the last Modbus read request has failed.

This command is rejected in the following cases:

- if no serial port has “Gateway Mode”=”Modbus Shared Memory”, the command will fail with the “Modbus Gateway not active” error;
- if no tag is found with the given name, the command will fail with the “Tag does not exist” error;
- if the requested tag has “GATEWAY MODE”=”BRIDGE” and the Modbus read request fails, the command will fail with the “Tag operation failed” error.

Example:

```
→    GET TAG GPS_LONGITUDE
←    GET TAG GPS_LONGITUDE EXECUTING (11.94528,VALID)
```

27.22. SET TAG

This command can be used to set the value of a tag (see “Modbus Shared Memory Gateway” functionality). The command has the following format:

```
SET TAG <tag name> <tag value>
```

Please note that the “tag name” is case-sensitive; also note that this command assumes that each tag has a distinct name; if more tags exist with the same name, this command tries to set the value of the first tag found with the given name.

For non-integer tag values, the decimal point character ‘.’ shall be used.

This command is rejected in the following cases:

- if no serial port has "Gateway Mode"="Modbus Shared Memory", the command will fail with the "Modbus Gateway not active" error;
- if no tag is found with the given name, the command will fail with the "Tag does not exist" error;
- if the given value does not fit the "Data Type" of the target tag (e.g. the "2" value for a "BOOL" tag), the command will fail with the "Invalid value for tag" error;
- if, for any reason, the write operation fails, the command will fail with the "Tag operation failed" error; this includes the following cases:
  - the Modbus write request fails, for "GATEWAY" or "BRIDGE" tags;
  - the tag value cannot be changed, since it is not a "General output", for Digital I/Os ("EMBEDDED") tags;
  - the tag value cannot be changed, since it is a "GPS info" ("EMBEDDED") tag.

Example:

```
→     SET TAG ZPASS_DO 10
←     SET TAG ZPASS_DO 10 EXECUTING
```

27.23. OVPN ON

This command can be used to activate the standard OPEN VPN functionality; the functionality is activated using system configuration parameters (Server, Password, Tag Name).
Please note that this command does not activate the OPEN VPN functionality in a persistent way, so if the device is restarted, the functionality is not re-activated.

Examples:

```
→     OVPN ON
←     OVPN ON EXECUTING
```

27.24. OVPN OFF

This command can be used to deactivate the OPEN VPN functionality activated by a previous "OVPN ON" command.

Please note that this command does not de-activate the OPEN VPN functionality in a persistent way, so if the Z-PASS is restarted, the functionality is re-activated.

Example:

```
→     OVPN OFF
←     OVPN OFF EXECUTING
```

27.25. CLEAN LOGS

This command will delete all data logs.

```
→     CLEAN LOGS

←     CLEAN LOGS EXECUTING
```

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

When using Seneca PLCs with Modbus RTU I/O modules, a very useful and powerful tool is provided by the Z-NET4 program suite, running on Windows PCs.
Among other things, these programs allow you to:
• automatically add the I/O modules available on the bus;
• configure the PLC and I/O modules;
• automatically create a Straton project containing the I/O variables, with the Modbus tasks needed to acquire/control them and the variables corresponding to the I/Os present in the device;
• automatically generate the code for the Straton project, performing "Remote Control Functions", such as:
Data logging
Command and status SMS
Alarm generation
• easily create custom web pages, with graphical widgets, and load them into the CPU

The Z-NET4 software is available at the following link:
http://www.seneca.it/products/z-net4
Please contact Seneca for further information on the Z-NET4 suite.