

# 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](http://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](mailto:supporto@seneca.it)

**ORIGINAL INSTRUCTIONS**

Product information

[commerciale@seneca.it](mailto:commerciale@seneca.it)

This document is the property of SENECA srl.  
Copies and reproduction are prohibited unless authorised

## 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

**TABLE OF CONTENTS**

<b>1. INTRODUCTION</b> .....	<b>9</b>
1.1. FIRMWARE WITH OPEN SOURCE LPG .....	9
<b>2. MODELS</b> .....	<b>9</b>
2.1. MODEL DESCRIPTION.....	10
2.1.1. SSD .....	10
2.1.2. R-PASS .....	11
2.1.3. Z-PASS1-RT / Z-TWS4-RT .....	11
2.1.4. Z-PASS2-RT .....	11
2.2. HARDWARE AND SOFTWARE OPTIONS .....	12
2.2.1. SSD .....	12
<b>3. THE DISPLAY / REMOTE DISPLAY (ONLY SMART DISPLAY, R-PASS, Z-PASS1-RT, Z-PASS2-RT)</b> .....	<b>13</b>
3.1. INFORMATION BAR .....	14
3.2. MENU.....	14
3.2.1. SETUP .....	15
3.2.1.1. NETWORK .....	15
3.2.1.2. PAGES .....	15
3.2.1.3. TAGS.....	17
3.2.1.4. DISPLAY .....	17
3.2.1.5. USERS .....	19
3.2.1.6. SERIAL.....	20
3.2.1.7. SNIFFER.....	20
3.2.1.7.1. SNIFFER MODE CONFIGURATION STEPS.....	21
3.2.2. ALARMS.....	22
3.2.3. BUS .....	23
3.2.4. MAINTENANCE .....	24
3.2.5. CHART .....	25
3.3. TYPE OF WIDGETS .....	27
3.3.1. PAGE CHANGE .....	29
3.4. TYPE OF WIDGET PAGE .....	29
3.5. SYNOPTIC PAGE TYPE .....	30
3.5.1. "ADD WIDGET" TOOL .....	31
3.5.2. DATABASE OF SYMBOLS FOR THE SYNOPTIC PAGES .....	32
3.6. ALARMS.....	33
3.7. REMOTE DISPLAY .....	33
3.8. DOWNLOADING LOG FILES TO USB FLASH DRIVE.....	34
<b>4. FIRMWARE UPDATE</b> .....	<b>35</b>
4.1. FW UPDATE FROM USB FLASH DRIVE.....	35
<b>5. IP ADDRESSES</b> .....	<b>36</b>
5.1. FACTORY IP ADDRESSES .....	36

5.2.	IP ADDRESS SEARCH .....	36
<b>6.</b>	<b>GATEWAY MODBUS ETHERNET TO SERIAL (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY).....</b>	<b>37</b>
<b>7.</b>	<b>GATEWAY ETHERNET TO TRANSPARENT SERIAL (R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY).....</b>	<b>38</b>
7.1.	VIRTUAL COM PORT WITH RFC 2217 .....	38
7.2.	SENECA ETHERNET TO SERIAL CONNECT .....	39
7.2.1.	INSTALLING THE SENECA SERIAL TO ETHERNET DRIVER.....	40
7.2.2.	COM PORT SELECTION FOR SENECA ETHERNET TO SERIAL TO CONNECT .....	43
7.2.3.	SENECA SERIAL TO ETHERNET CONFIGURATION .....	44
7.2.4.	DEBUGGING THE CONNECTION .....	45
7.2.5.	CHANGING THE PORT NUMBER .....	45
7.3.	SERIAL TUNNEL POINT ON TCP .....	49
7.4.	POINT-TO-POINT SERIAL TUNNEL ON UDP .....	50
7.5.	SERIAL TUNNEL FROM POINT TO MULTIPOINT .....	50
<b>8.</b>	<b>MODBUS GATEWAY WITH SHARED MEMORY (R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY).....</b>	<b>51</b>
<b>9.</b>	<b>DATALOGGER (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY) .....</b>	<b>54</b>
<b>10.</b>	<b>LOGIC REGULATIONS (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY).....</b>	<b>56</b>
<b>11.</b>	<b>ALARMS (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY) .....</b>	<b>56</b>
<b>12.</b>	<b>VPN .....</b>	<b>56</b>
12.1.	VPN "SINGLE LAN" ALWAYS ON.....	58
12.2.	VPN "POINT TO POINT" ON DEMAND .....	59
<b>13.</b>	<b>ROUTER.....</b>	<b>59</b>
<b>14.</b>	<b>NETWORK REDUNDANCY .....</b>	<b>60</b>
<b>15.</b>	<b>DISABLING THE REMOTE CONNECTION.....</b>	<b>60</b>
<b>16.</b>	<b>AUTO APN .....</b>	<b>61</b>
<b>17.</b>	<b>HTTP REST CLIENT PROTOCOL (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY) .....</b>	<b>61</b>

<b>18.</b>	<b>OPC UNIFIED ARCHITECTURE SERVER PROTOCOL (OPC-UA)</b> .....	<b>62</b>
<b>19.</b>	<b>MQTT CLIENT PROTOCOL</b> .....	<b>62</b>
19.1.	MQTT CHARACTERISTICS (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY).....	63
<b>20.</b>	<b>STRATON PLC (R-PASS-S, Z-TWS4-RT-S, Z-PASS2-RT-S MODELS ONLY)</b> ....	<b>63</b>
20.1.	WRITE, DOWNLOAD AND RUN YOUR FIRST PROGRAM.....	63
20.1.1.	MANUAL INSTALLATION OF LIBRARIES AND TEMPLATES IN STRATON .....	64
20.2.	ENERGY MANAGEMENT PROTOCOLS .....	68
20.3.	SNMP V2C PROTOCOL .....	69
<b>21.</b>	<b>R-COMM OPTION (R-PASS MODEL ONLY)</b> .....	<b>69</b>
<b>22.</b>	<b>CONFIGURATION VUA WEB SERVER (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>69</b>
22.1.	SUMMARY.....	69
22.2.	NETWORK AND SERVICES.....	69
22.3.	PLC (R-PASS-S, Z-TWS4-RT-S, Z-PASS2-RT-S MODELS ONLY) .....	70
22.4.	WI-FI CONFIGURATION (R-PASS MODEL ONLY).....	70
22.5.	SERIAL PORTS (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY).....	71
22.6.	I/O CONFIGURATION .....	71
22.7.	REAL TIME CLOCK SETUP .....	73
22.8.	GATEWAY CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY) .....	73
22.8.1.	GATEWAY ETHERNET TO SERIAL .....	73
22.8.2.	TRANSPARENT GATEWAY .....	74
22.8.2.1.	VIRTUAL COM .....	74
22.8.2.2.	POINT-TO-POINT SERIAL TUNNEL ON TCP/UDP (MASTER) .....	74
22.8.2.3.	POINT-TO-MULTIPOINT SERIAL TUNNEL (MASTER) .....	74
22.8.2.1.	POINT-TO-MULTIPOINT SERIAL TUNNEL (SLAVE) .....	74
22.8.3.	MODBUS GATEWAY WITH SHARED MEMORY (TO BE USED FOR DATALOGGERS AND LOGICS) .....	75
22.9.	VPN CONFIGURATION .....	76
22.9.1.	OPEN VPN .....	76
22.9.1.1.	CONFIGURATION FILE.....	76
22.9.1.2.	CA CERTIFICATE .....	77
22.9.1.3.	CLIENT CERTIFICATE .....	77
22.9.1.4.	CLIENT KEY.....	77
22.9.1.5.	ADDITIONAL FILE .....	77
22.9.1.6.	CONFIGURATION FILE FOR USE AS OPENVPN SERVER.....	78
22.9.1.7.	CONFIGURATION FILE FOR USE AS OPENVPN CLIENT .....	78
22.9.2.	VPN BOX.....	79
22.10.	OPC-UA SERVER CONFIGURATION .....	81
22.10.1.	UA EXPERT CLIENT CONFIGURATION .....	82
22.11.	OPC-UA CLIENT CONFIGURATION (SSD, R-PASS-S, Z-PASS2-S-RT, Z-TWS4-RT MODELS ONLY) .....	87
22.12.	SNMP CONFIGURATION (R-PASS-S, Z-PASS2-RT-S, Z-TWS4-RT-S MODELS ONLY).....	88
22.13.	USERS CONFIGURATIONS .....	89
22.14.	ROUTER CONFIGURATION.....	89
22.15.	NAT 1:1 RULES .....	91
22.16.	STATIC ROUTES .....	92

<b>22.17.</b>	<b>TCP SERVER (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>93</b>
<b>22.18.</b>	<b>TAG SETUP (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>94</b>
<b>22.19.</b>	<b>TAG VIEW (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>97</b>
<b>22.20.</b>	<b>DB DEVICE (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>97</b>
<b>22.21.</b>	<b>ALARM CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>97</b>
<b>22.22.</b>	<b>ALARM SUMMARY (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>99</b>
<b>22.23.</b>	<b>ALARM HISTORY (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>99</b>
<b>22.24.</b>	<b>USB TRANSFER CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>99</b>
<b>22.25.</b>	<b>FTP CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>100</b>
<b>22.26.</b>	<b>EMAIL CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>101</b>
<b>22.27.</b>	<b>HTTP CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>102</b>
<b>22.28.</b>	<b>MQTT CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>102</b>
<b>22.29.</b>	<b>PHONEBOOK (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>106</b>
<b>22.30.</b>	<b>MESSAGE CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>107</b>
<b>22.31.</b>	<b>TIMER CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>107</b>
<b>22.32.</b>	<b>RULE MANAGEMENT (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>108</b>
22.32.1.	"ALARM STATE" PARAMETERS .....	113
22.32.2.	"ALARM ACTIVE" PARAMETERS .....	113
22.32.3.	"DIGITAL TAG" PARAMETERS .....	113
22.32.4.	"ANALOG TAG" PARAMETERS .....	114
22.32.5.	"TIMER" PARAMETERS .....	114
22.32.6.	"SCHEDULER" PARAMETERS .....	116
22.32.7.	"RULE STATUS" PARAMETERS.....	116
22.32.8.	"BIT MASK" PARAMETERS.....	116
22.32.9.	"DIGITAL TAG" PARAMETERS .....	117
22.32.10.	"ANALOG TAG" PARAMETERS .....	117
22.32.11.	EXAMPLE OF THE IMPLEMENTATION OF A PROGRAM WITH LOGICAL RULES .....	121
<b>22.33.</b>	<b>DATALOGGER: GENERAL SETTINGS (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>130</b>
<b>22.34.</b>	<b>GROUP CONFIGURATION (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>131</b>
<b>22.35.</b>	<b>USB FILE MANAGER (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>131</b>
<b>22.36.</b>	<b>DATA LOGGER (R-PASS-S, Z-PASS2-RT-S, Z-TWS4-RT-S ONLY)</b> .....	<b>131</b>
<b>22.37.</b>	<b>ETHERNET INTERFACES</b> .....	<b>131</b>
<b>22.38.</b>	<b>MODBUS SERIAL TRACE (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)</b> .....	<b>131</b>
<b>22.39.</b>	<b>METER-BUS PROTOCOL (M-BUS) (R-PASS-S, Z-PASS2-RT-S, Z-TWS4-RT-S ONLY)</b> .....	<b>132</b>
22.39.1.	M-BUS SCAN .....	132
22.39.2.	"CREATE CONFIGURATION" BUTTON.....	134
22.39.3.	M-Bus Configuration .....	134
22.39.4.	IMPORTING THE CONFIGURATION INTO STRATON .....	135
22.39.5.	DELETING UNUSED MBUS VARIABLES .....	142
22.39.6.	REPLACING AN M-BUS DEVICE .....	143
22.39.7.	ADDING AN M-BUS DEVICE.....	143
22.39.8.	DELETING AN MBUS DEVICE .....	143
22.39.9.	"TAG ERROR REPORT" SPECIAL TAG .....	144
<b>22.40.</b>	<b>FIRMWARE VERSION</b> .....	<b>144</b>
<b>22.41.</b>	<b>FIRMWARE UPGRADE</b> .....	<b>144</b>
<b>22.42.</b>	<b>MANAGEMENT CONF</b> .....	<b>144</b>
<b>22.43.</b>	<b>LICENCE MANAGEMENT (SSD ONLY)</b> .....	<b>144</b>
<b>22.44.</b>	<b>WEBSERVER WITH "GUEST" ACCOUNT</b> .....	<b>144</b>
<b>22.45.</b>	<b>WEBSERVER WITH "USER" ACCOUNT</b> .....	<b>145</b>
<b>22.46.</b>	<b>FTP / SFTP ACCESS</b> .....	<b>145</b>

<b>23.</b>	<b>MQTT CLIENT PROTOCOL (R-PASS-S, Z-PASS2-RT-S, Z-TWS4-RT-S ONLY)</b>	<b>147</b>
23.1.	PARAMETERS OF THE MQTT PROTOCOL FROM THE PLC PROGRAM.....	147
23.1.1.	MANAGING MULTIPLE MQTT CONNECTIONS.....	148
23.2.	MQTT CONFIGURATION OF SSL/TLS RETRYs.....	149
23.3.	STATIC AND DYNAMIC CLIENT CERTIFICATES.....	149
23.4.	CHANGING MQTT PARAMETERS IN RUNTIME VIA FILE.....	150
<b>24.</b>	<b>FACTORY RESET.....</b>	<b>151</b>
24.1.	FACTORY RESET FOR SSD.....	151
24.2.	FACTORY RESET FOR R-PASS AND R-PASS-S.....	152
24.3.	FACTORY RESET FOR Z-PASS1-RT, Z-PASS2-RT, Z-TWS4-RT-S, Z-PASS2-RT-S.....	152
<b>25.</b>	<b>MAINTENANCE MODE (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT ONLY).....</b>	<b>152</b>
<b>26.</b>	<b>MODBUS EMBEDDED I/O REGISTERS (SSD, R-PASS, Z-PASS1-RT, Z-PASS2-RT ONLY).....</b>	<b>153</b>
26.1.	SSD.....	153
26.2.	R-PASS.....	154
26.3.	Z-PASS1-RT, Z-PASS2-RT.....	154
<b>27.</b>	<b>Z-NET4 (R-PASS-S, Z-TWS4-RT-S, Z-PASS2-RT-S ONLY).....</b>	<b>155</b>

## 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](mailto: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:



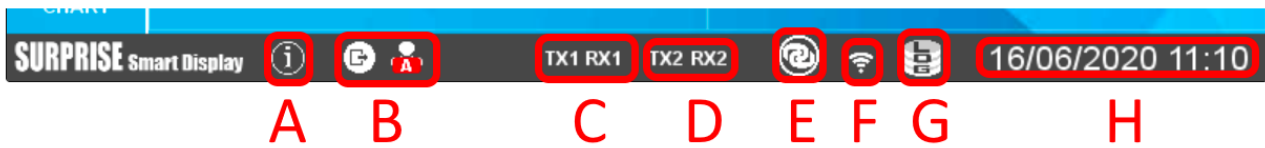
"A" Represents the bar with the device information

"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 : 

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:



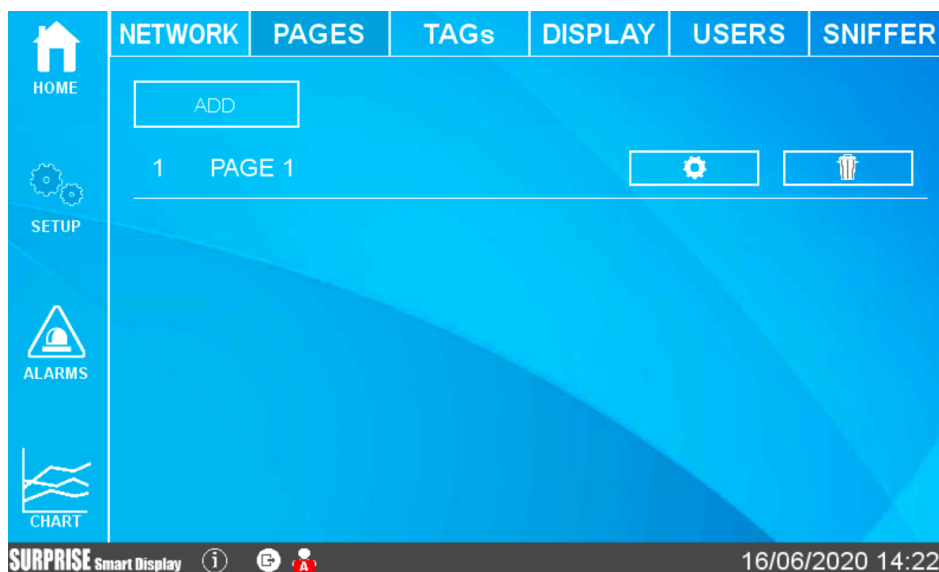
### 3.2.1.SETUP

#### 3.2.1.1. NETWORK



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



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.



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.

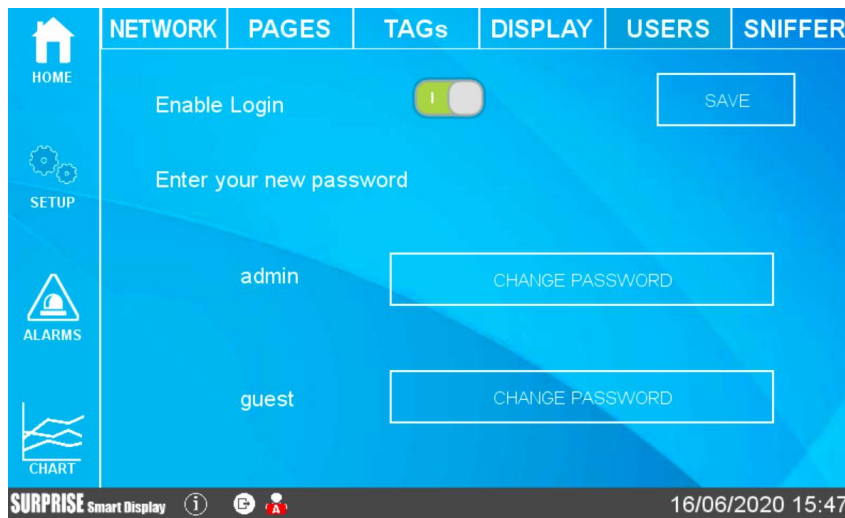


In order to safeguard the consumption and the duration of the screen, it is possible to activate the screensaver (the backlighting of the screen is lowered after the set idle time).

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

<b>ACCOUNT TYPE</b>	<b>CHANGING THE VALUE OF A TAG</b>	<b>SETUP MENU DISPLAY</b>	<b>SETUP MODIFICATION</b>
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.



### 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

ALARMS			HISTORICAL 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	

CONFIRM

**SURPRISE** Smart Display 16/06/2020 16:56

This section shows the active alarms and alarm history.

If the alarm requires manual acknowledgement, it is possible to use the appropriate button:

ALARMS			HISTORICAL ALARMS		
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	

CONFIRM

**SURPRISE** Smart Display 16/06/2020 17:01

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

HOME	ALARMS			HISTORICAL ALARMS		
	NAME	TAG	VALUE	LEVEL	STATUS	TIME
SETUP	ALR_DO_1	SMART_D ISP_DO_1	1	Alarm	Acknowledge	16/5/2020 17:0:16
	ALR_DO_1	SMART_D ISP_DO_1	1	Alarm	Acknowledge	16/5/2020 16:58:51
	ALR_DO_2	SMART_D ISP_DO_2	1	Alarm	Alarm	16/5/2020 16:53:27
	ALR_DO_1	SMART_D ISP_DO_1	1	Alarm	Alarm	16/5/2020 16:53:21
ALARMS	<input type="button" value="CLEAN"/>					
CHART						
						16/06/2020 17:04

**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:

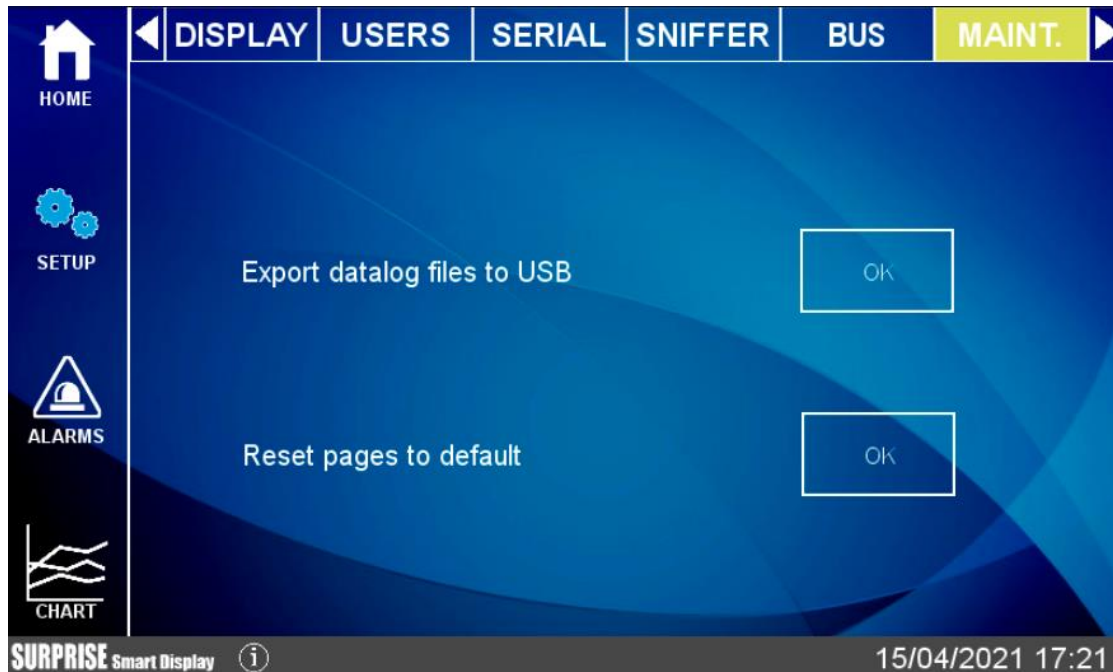


The device uses a database that includes records of all Seneca devices.

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

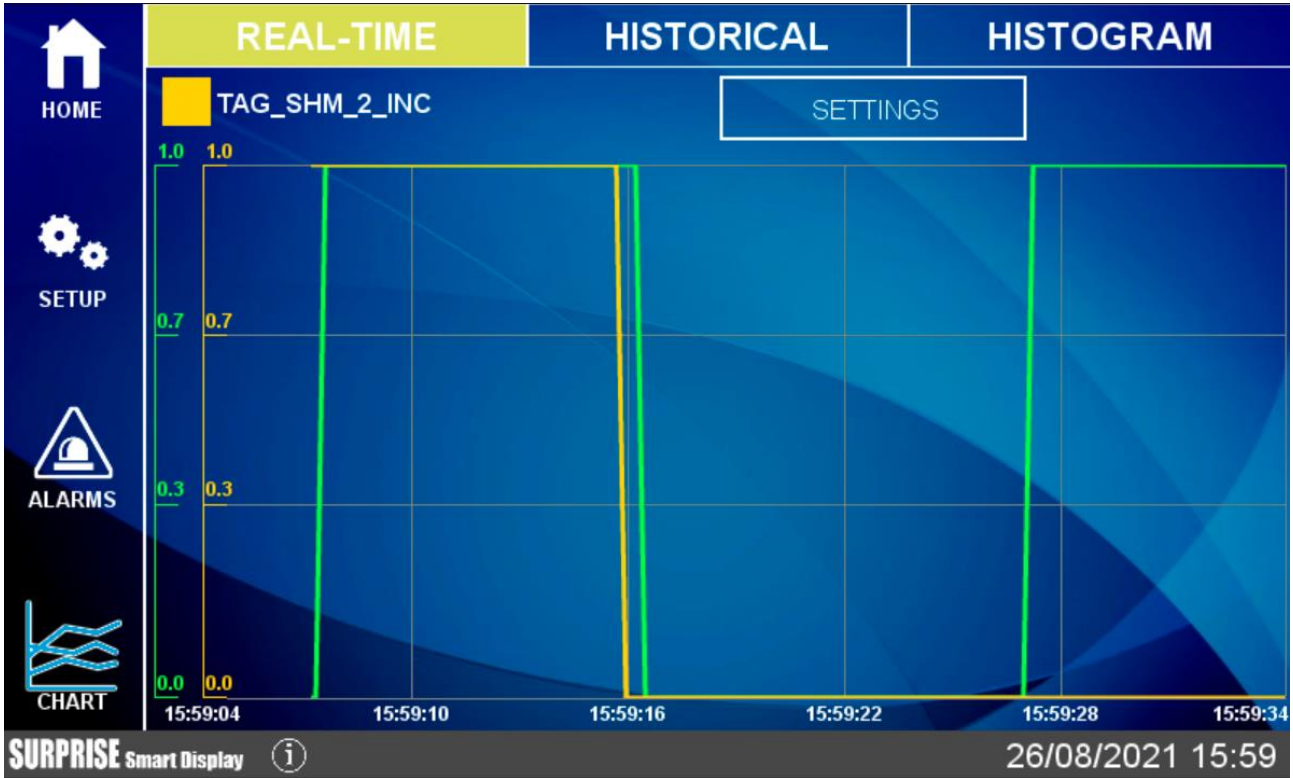
The Maintenance menu allows maintenance operations to be carried out on the device:



3.2.5. **CHART**

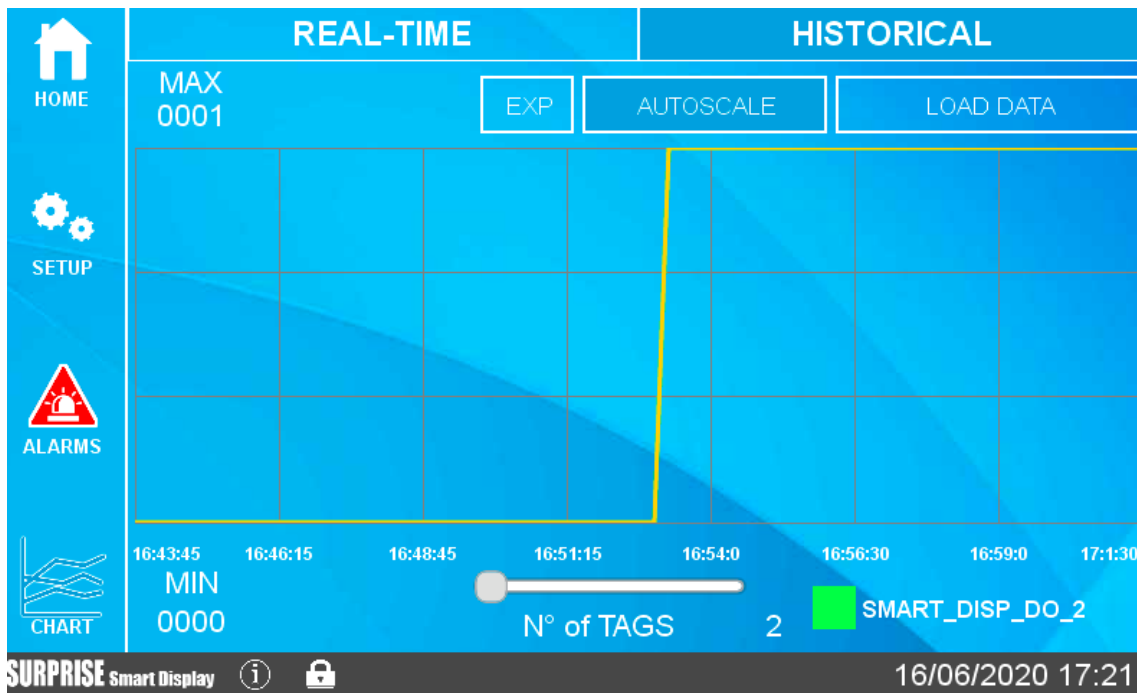
There are 3 types of graph available: Real Time, Historical and Histogram.

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 Histogram 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:

	<p><b>Text widget</b></p> <p>The TAG value will be displayed as text</p>
	<p><b>Gauge widget</b></p> <p>The TAG value will be displayed with a gauge indicator</p>
	<p><b>LED widget</b></p> <p>OFF/ON statuses will be displayed with colors</p>
	<p><b>LED BIT widget</b></p> <p>OFF/ON bit-mask statuses will be displayed with colors</p>

	<p><b>Button command widget</b></p> <p>When the button is pressed, the TAG will be set to the preset value</p>
	<p><b>Graphic Widget</b></p> <p>The TAG value will be displayed on a dynamic graph</p>
	<p><b>Vertical Bar widget</b></p> <p>The TAG value will be displayed on a dynamic vertical bar</p>
	<p><b>Horizontal Bar widget</b></p> <p>The TAG value will be displayed on a dynamic horizontal bar</p>

	<p><b>IMAGE widget</b></p> <p>Static image</p>
	<p><b>MULTI IMAGE widget</b></p> <p>Tag values will be displayed with different images</p>
	<p><b>Label widget</b></p> <p>Static label</p>
	<p><b>Multi Label widget</b></p> <p>Tag values will be displayed with different labels</p>

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.

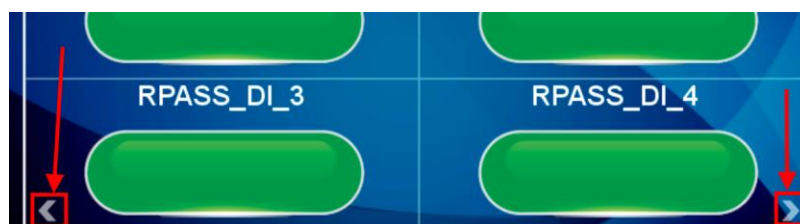
It is possible to place up to 2 virtual displays for each widget page.

### 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.

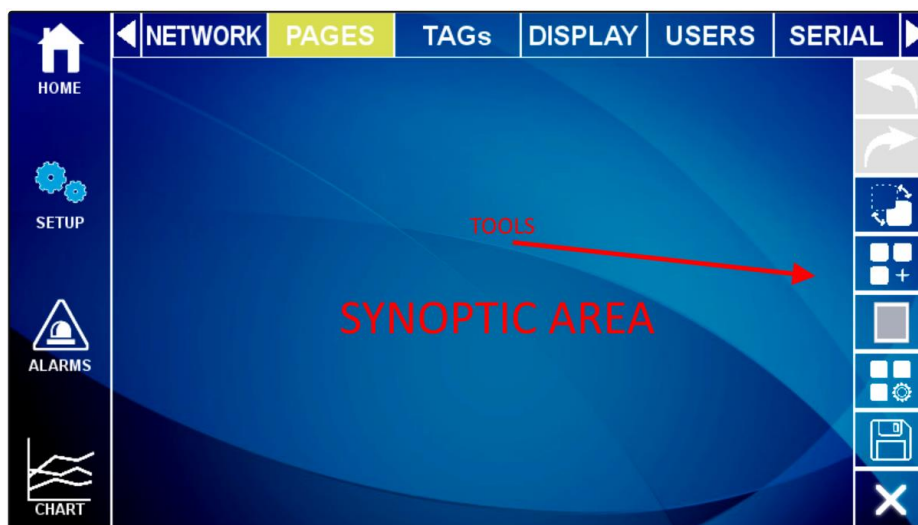
Each widget graphically represents the value of one or more TAGs.

### 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



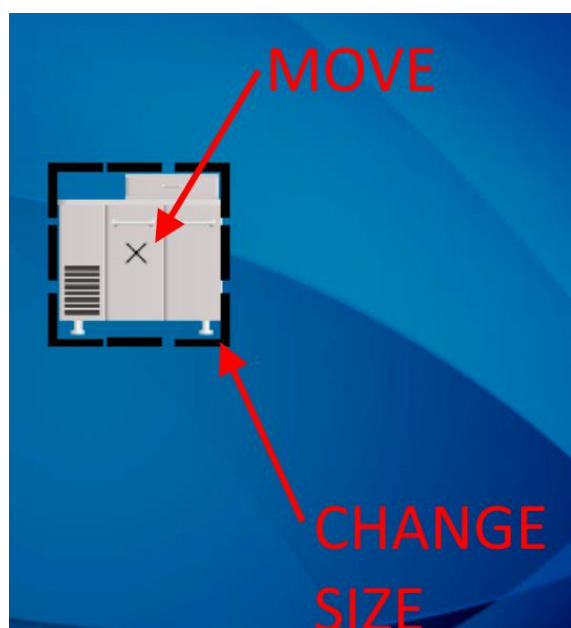
EXIT

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:



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



The widget is aligned



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



The Widget is removed from the page

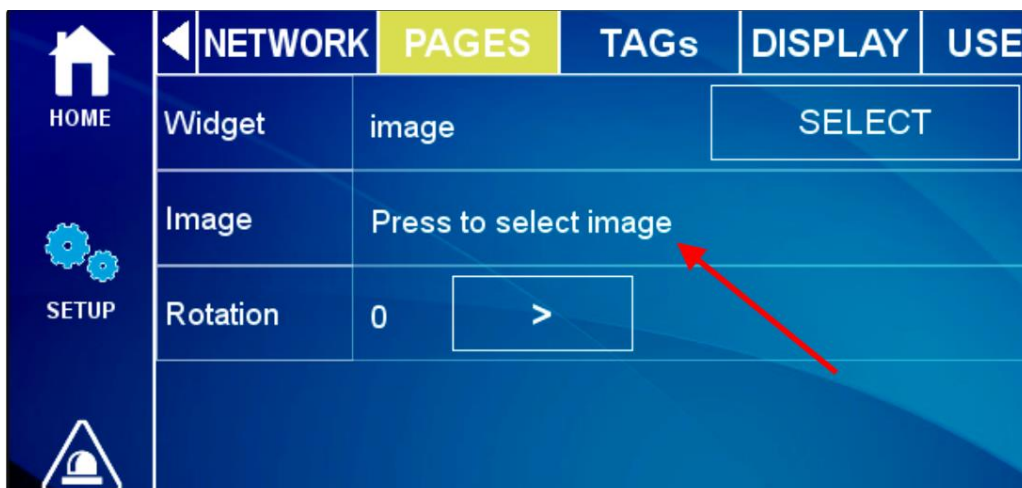


You return to the initial page of the synoptic

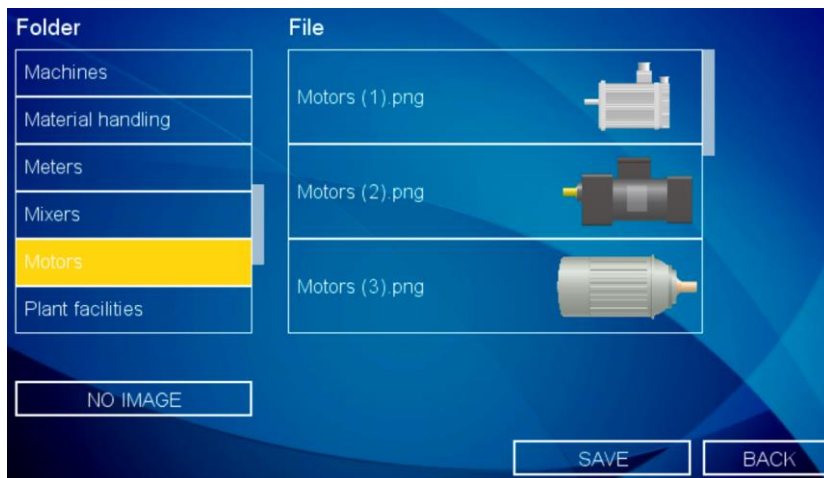
### 3.5.2. DATABASE OF SYMBOLS FOR THE SYNOPTIC PAGES

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:



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



### 3.6. ALARMS

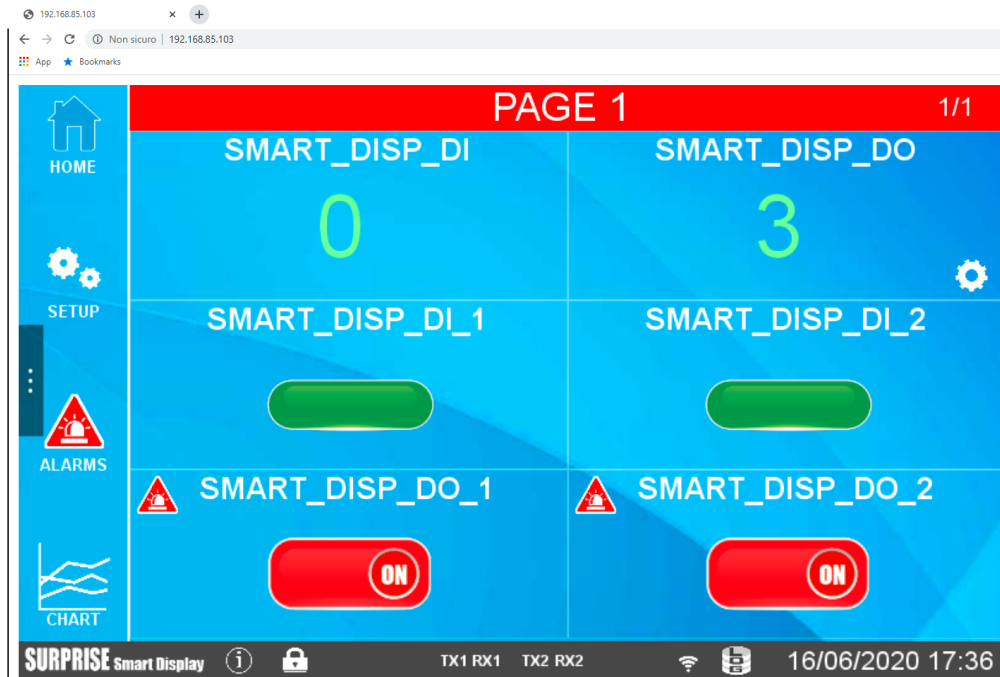
When an alarm occurs on at least one TAG, the title of the page is outlined in red and the faulty tags display the alarm icon, see the figure:



### 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).

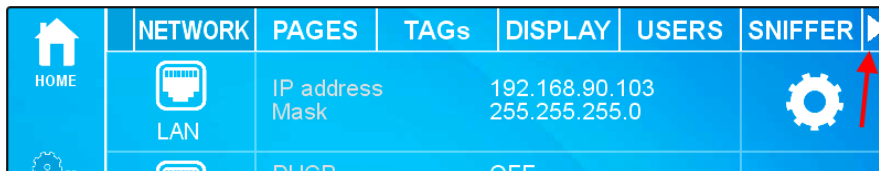
To connect to the remote display, enter the device's IP address into a browser on a PC or smart device:



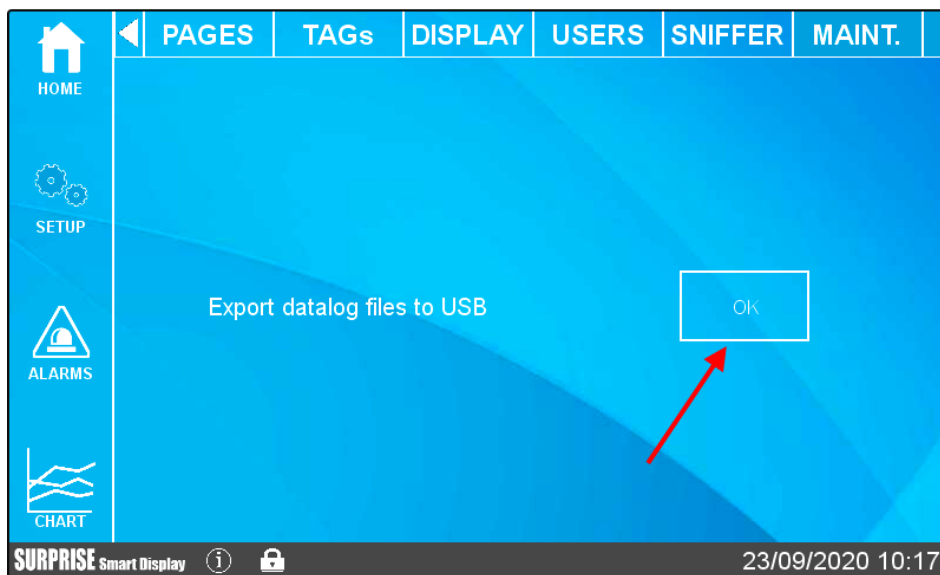
### 3.8. DOWNLOADING LOG FILES TO USB FLASH DRIVE

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:



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



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

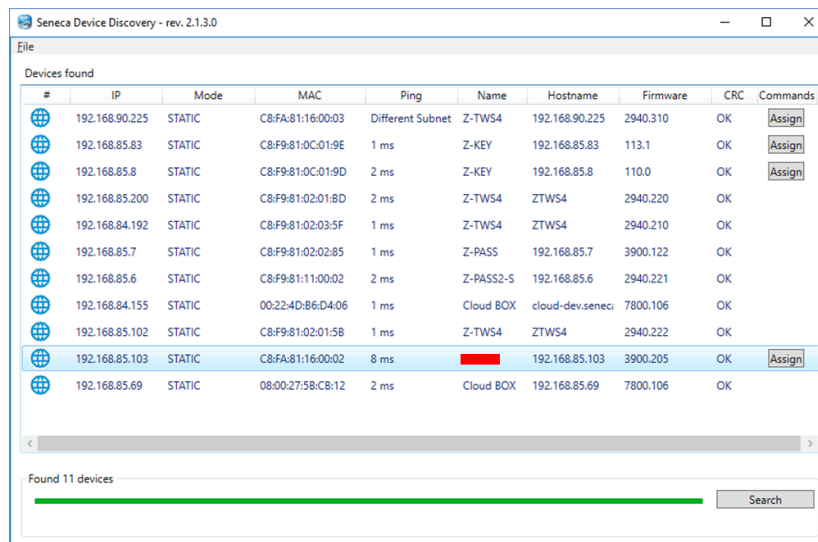
#### 5.1. FACTORY IP ADDRESSES

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

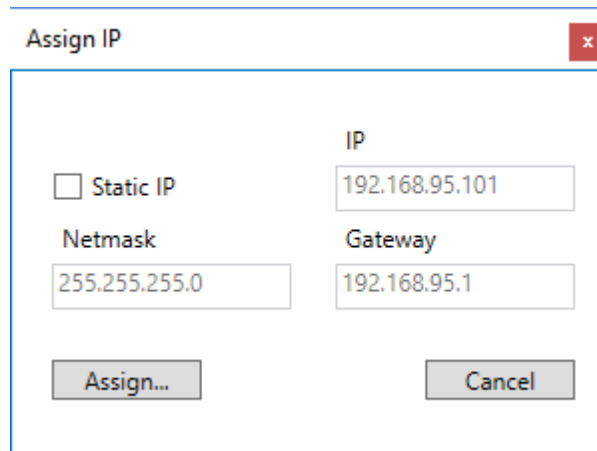
#### 5.2. IP ADDRESS SEARCH

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.

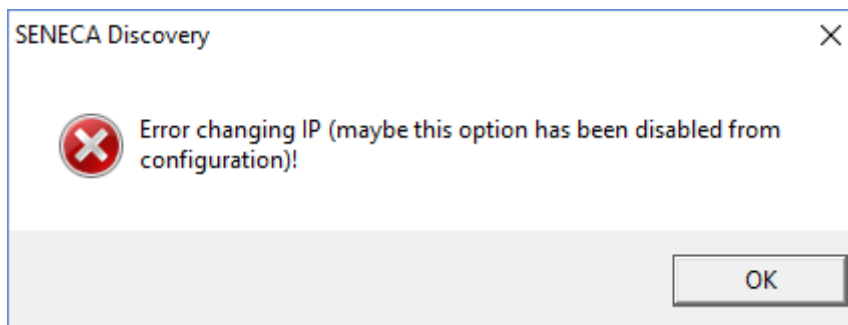


This application shows the IP address, MAC address, FW version and some other useful information, for each SENECA device connected to PC.

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



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



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 Ethernet 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.

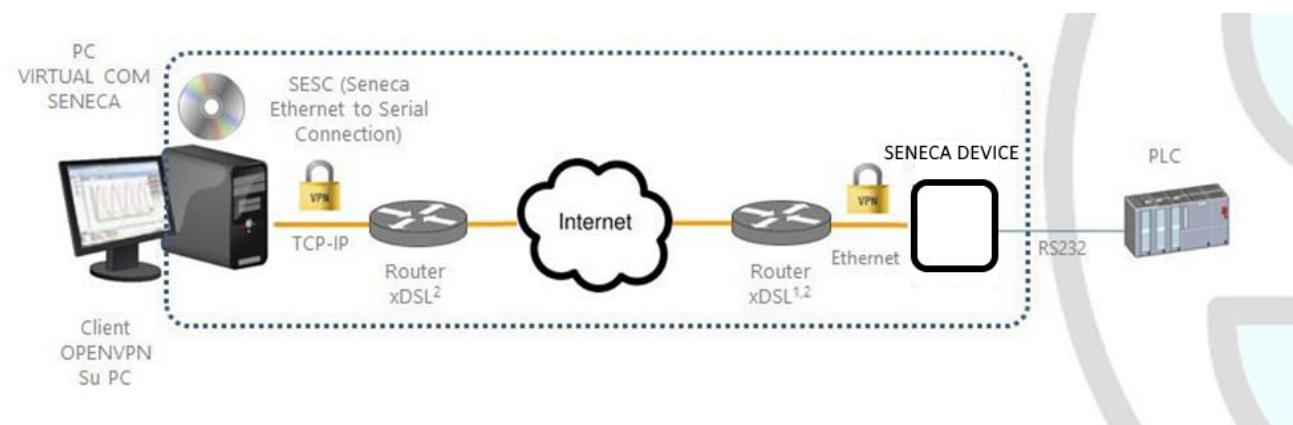
## 7. GATEWAY ETHERNET TO TRANSPARENT SERIAL (R-PASS, Z-PASS1-RT, Z-PASS2-RT MODELS ONLY)

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***

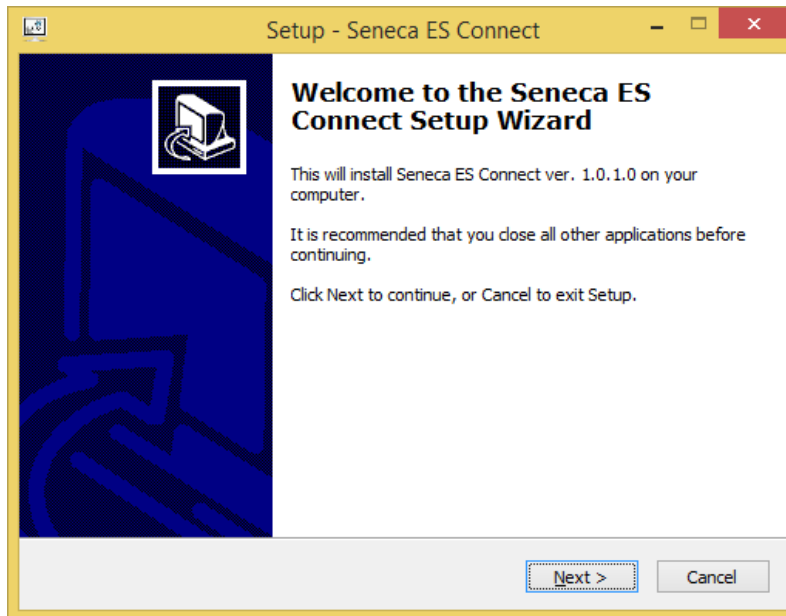
## **7.2. SENECA ETHERNET TO SERIAL CONNECT**

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

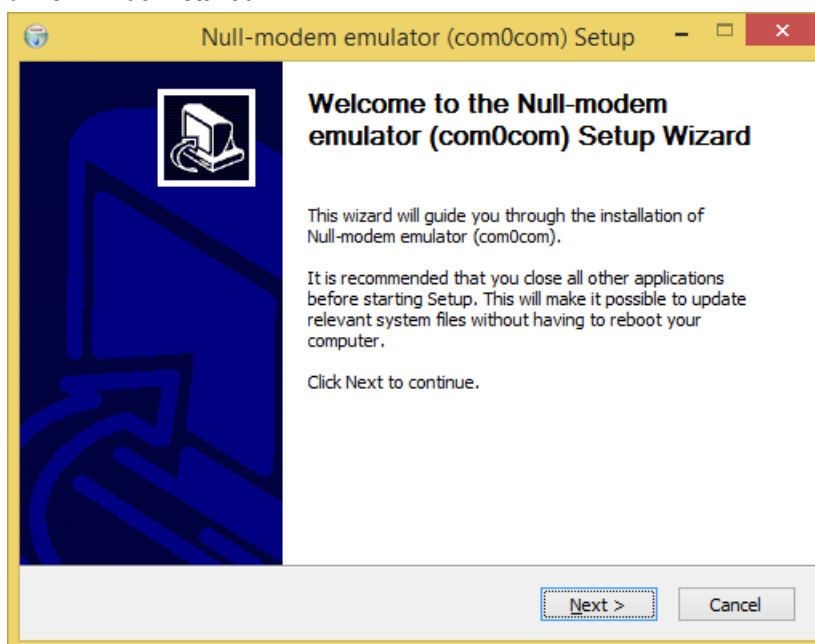
### 7.2.1. INSTALLING THE SENECA SERIAL TO ETHERNET DRIVER

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

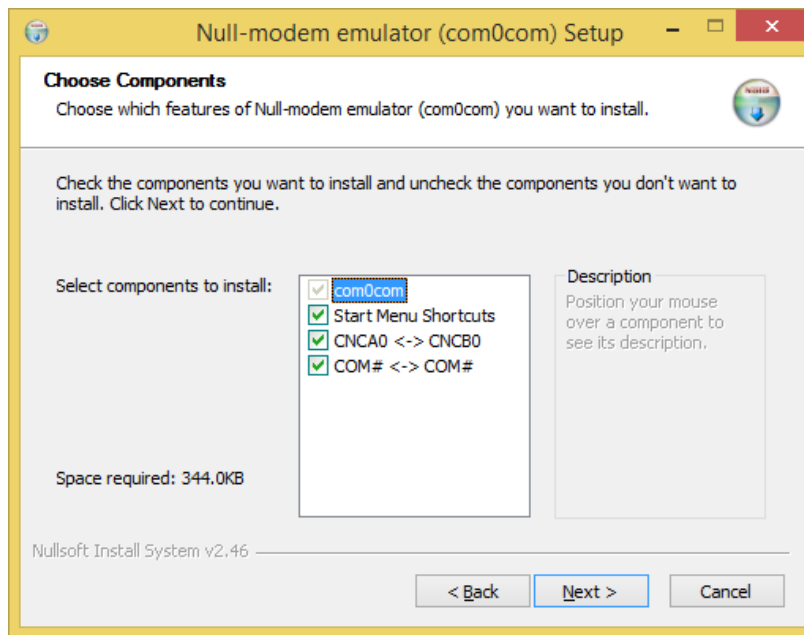
Double-click on the installer



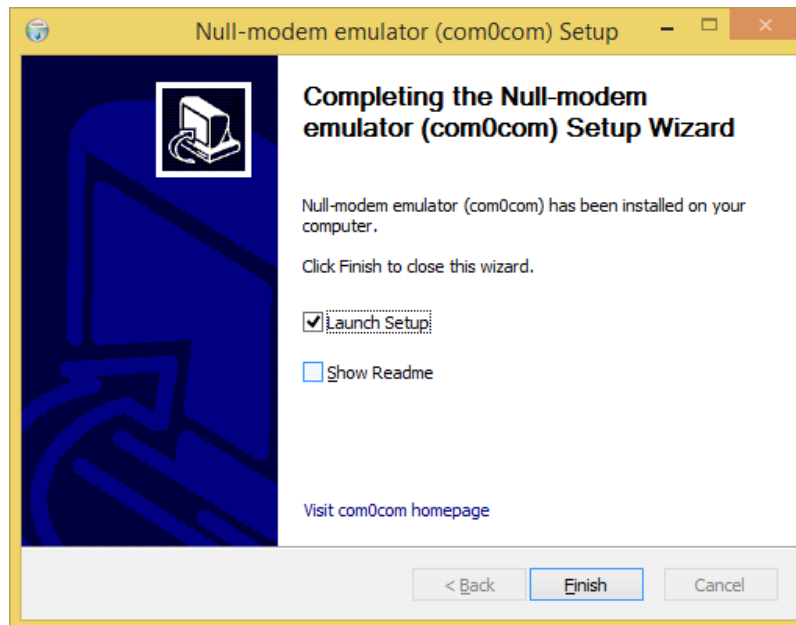
Then the com0com driver will be installed:



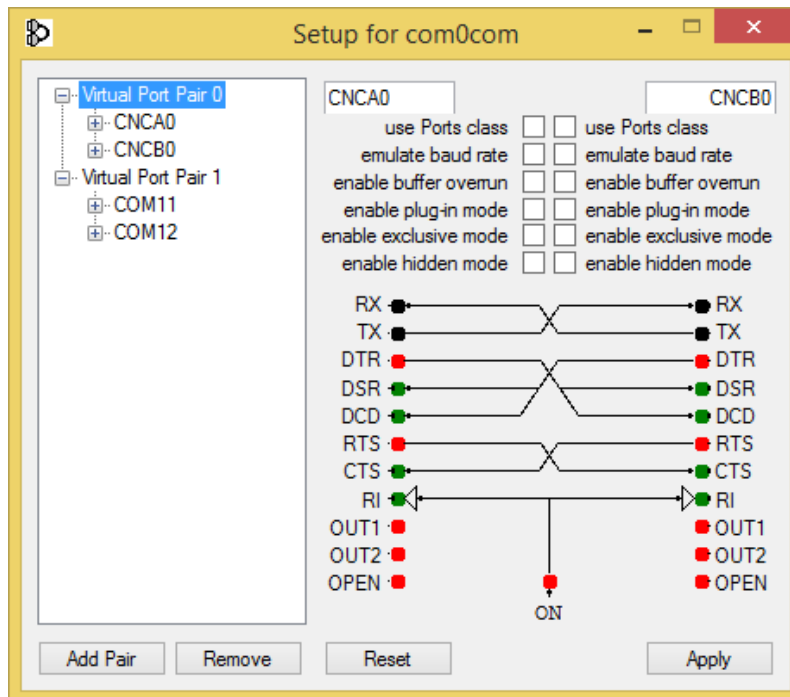
Select the virtual port names CNCA0<->CNCB0 and COM#<->COM#:



Now click on "Start Setup":



Press Finish, the com0com setup will open:



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

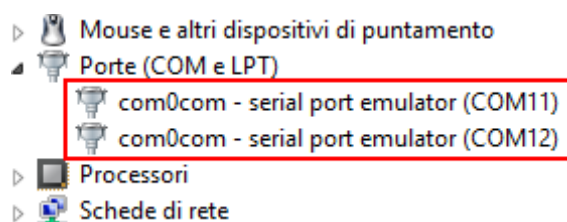
COM11, COM12 (note that com# may be different in your system).

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.

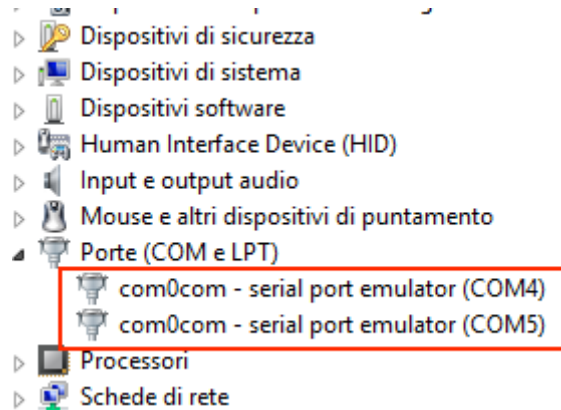
Confirm the driver installation with "Apply".

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



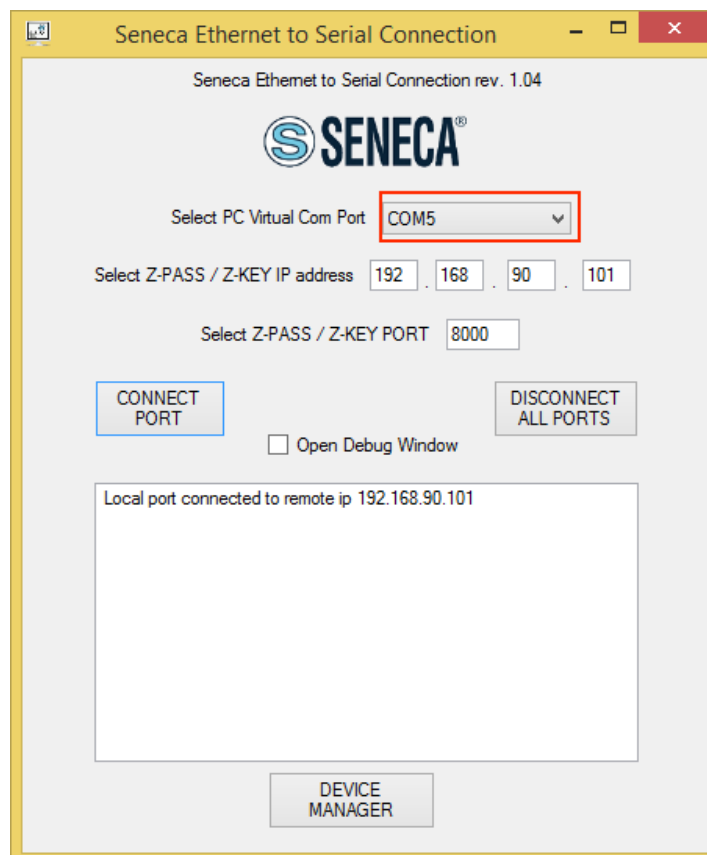
### 7.2.2.COM PORT SELECTION FOR SENECA ETHERNET TO SERIAL TO CONNECT

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):

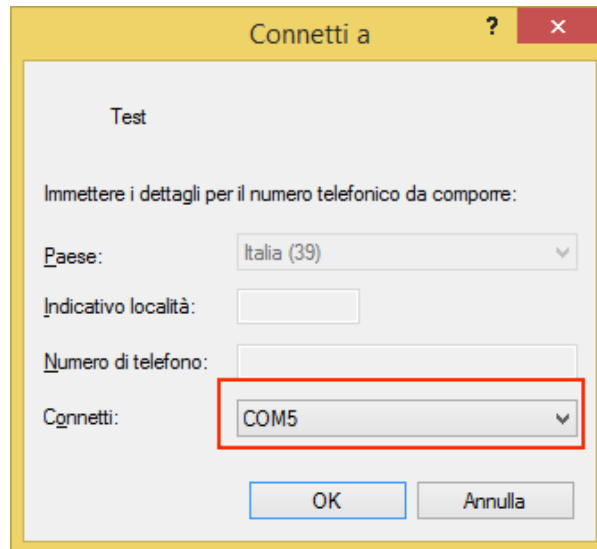


The SESC interface visualizes only com0com ports and it will only use one port

Select COM5 in the Seneca ES connector:

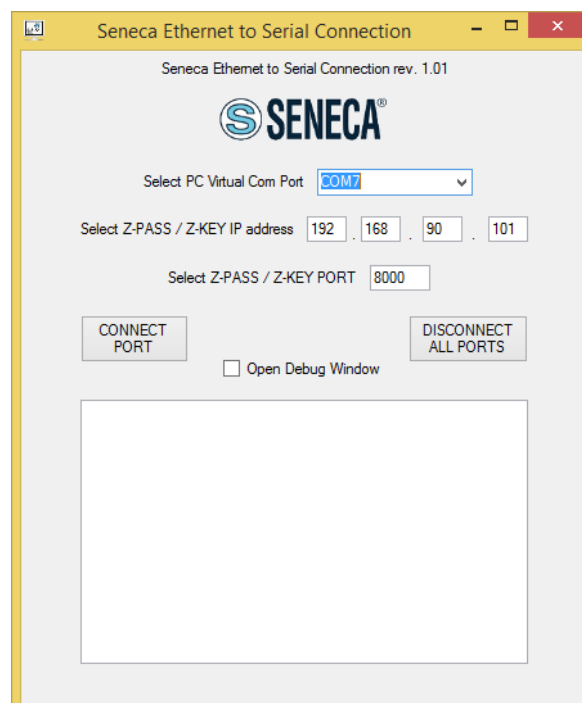


Now use the same COM port on application to use (e.g. in the terminal software)



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

### 7.2.3. SENECA SERIAL TO ETHERNET CONFIGURATION



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

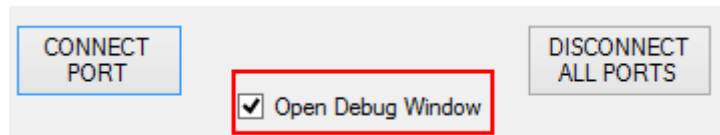
Click on "CONNECT PORT".

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".

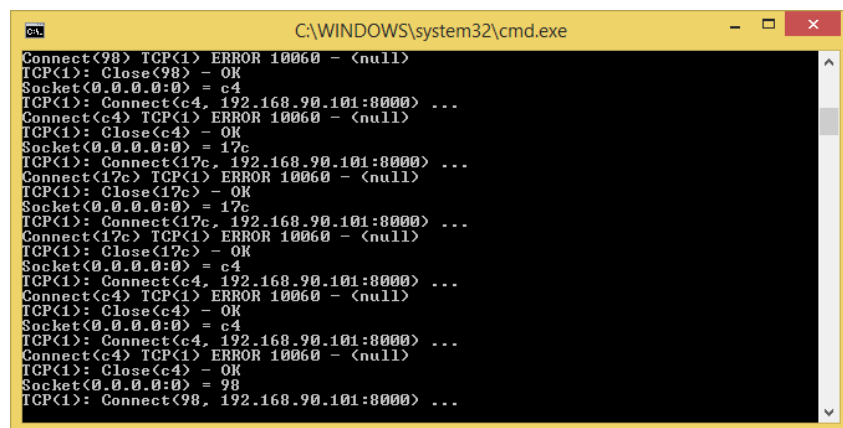
### 7.2.4. DEBUGGING THE CONNECTION

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:

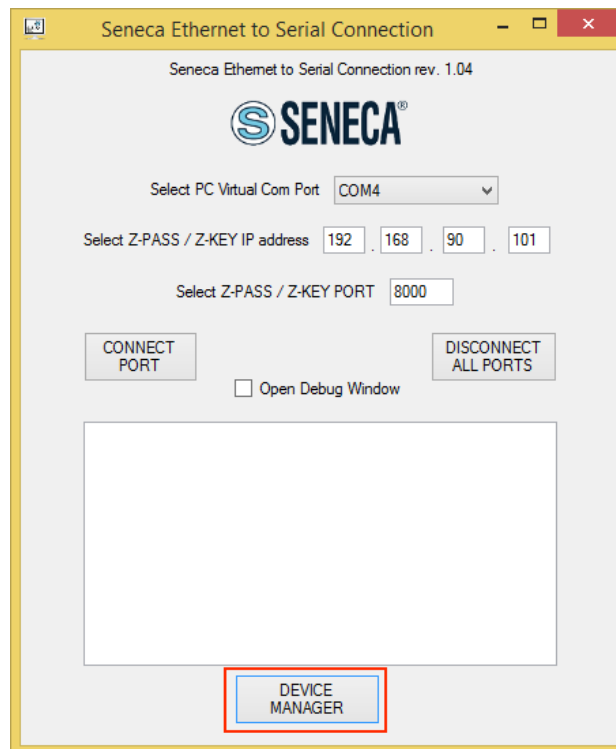


check the configuration (IP address and TCP port).

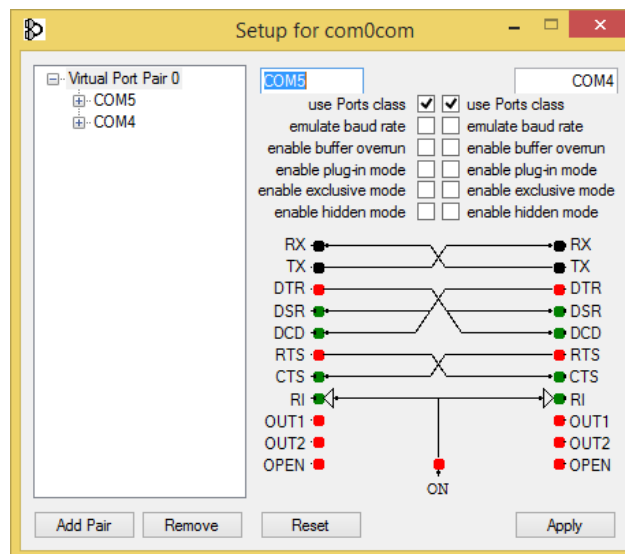
### 7.2.5. CHANGING THE PORT NUMBER

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

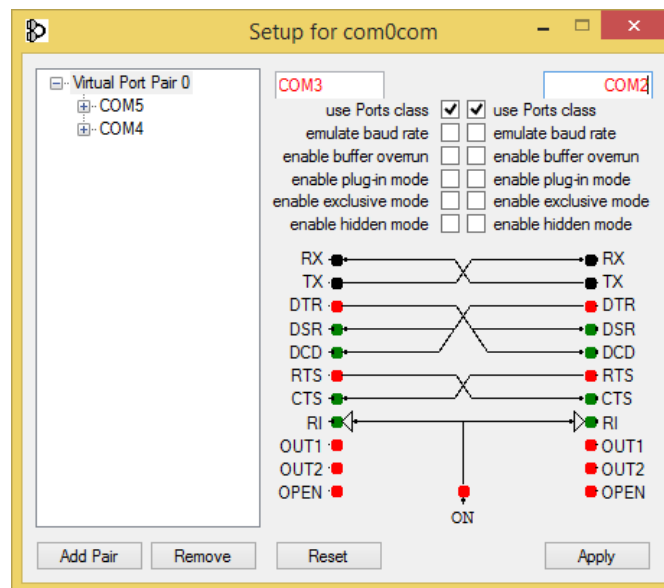
In our case the COM pair created is COM4/COM5, let's see the procedure to change it to COM2/COM3  
Click on the "DEVICE MANAGER" button:



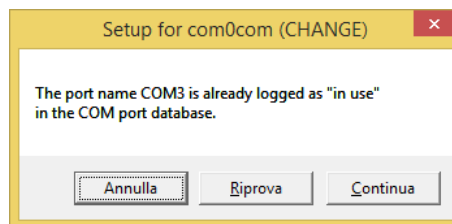
The com0com configuration window appears:



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

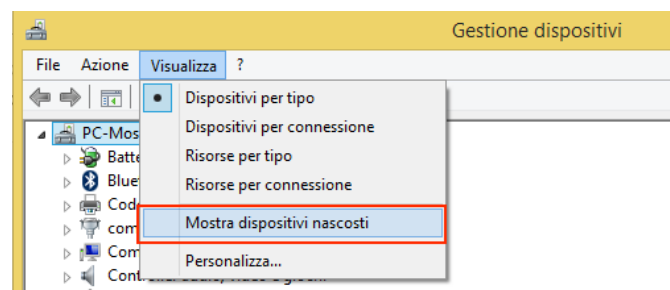


Sometimes the COM may be marked "in use":

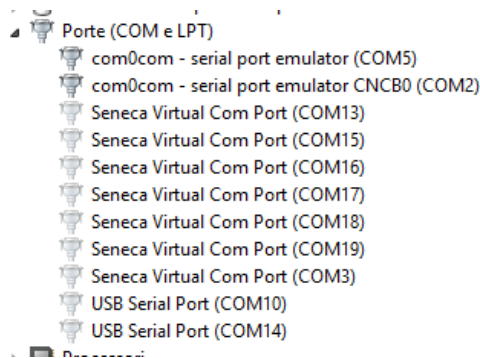


If you need to use this COM number, click "Continue", then go to device configuration.

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



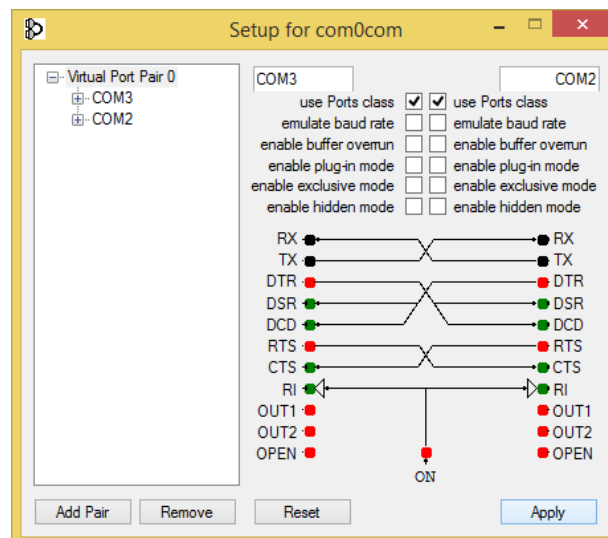
Now all unused ports are displayed in transparency (even our COM3):



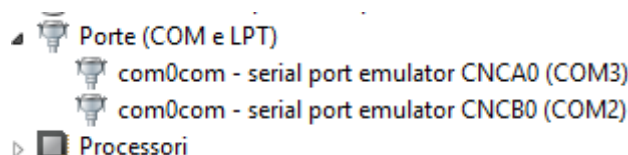
Now select the COM3 port and click on "Uninstall":



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

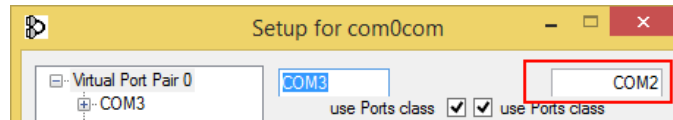


Finally click on "Apply", now the pair COM3/COM2 is created:

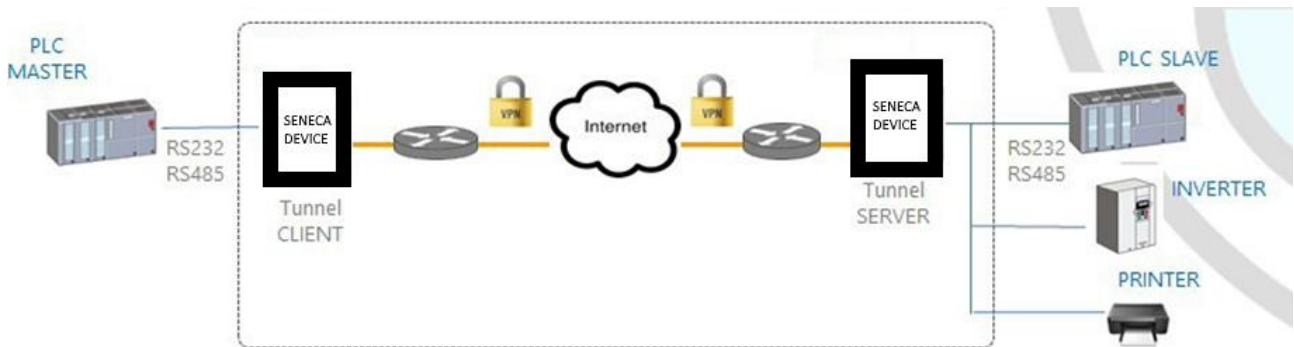


**ATTENTION!**

*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.

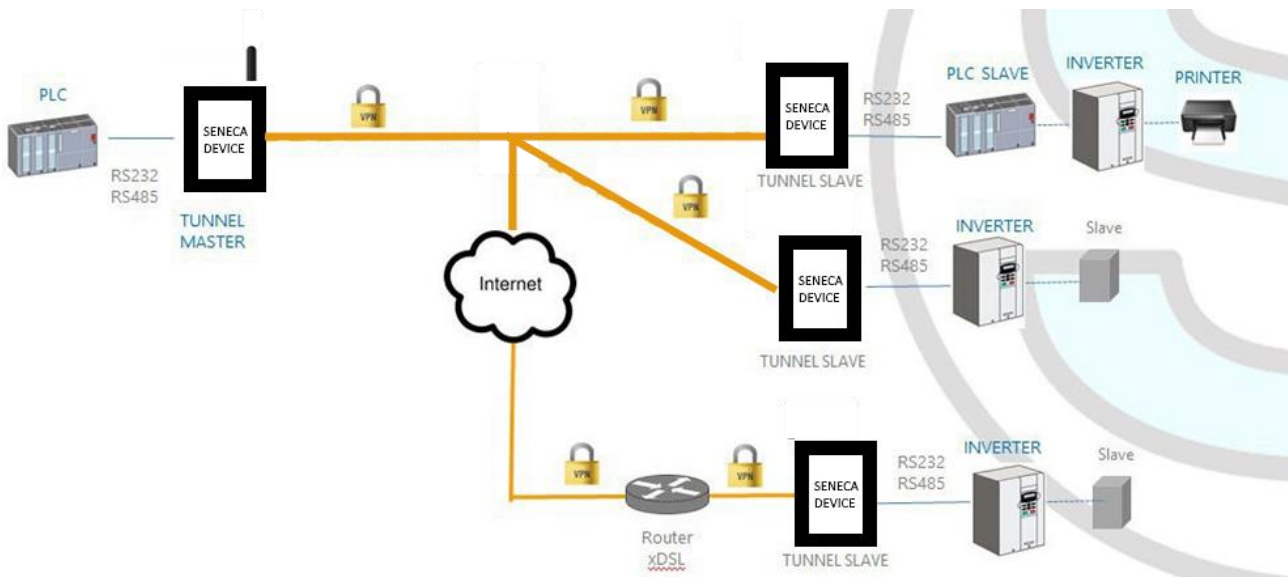
The only difference is that none TCP connection is established and the serial data is carried by a UDP packet. The configuration parameters are the same as for the serial tunnel over TCP.

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.

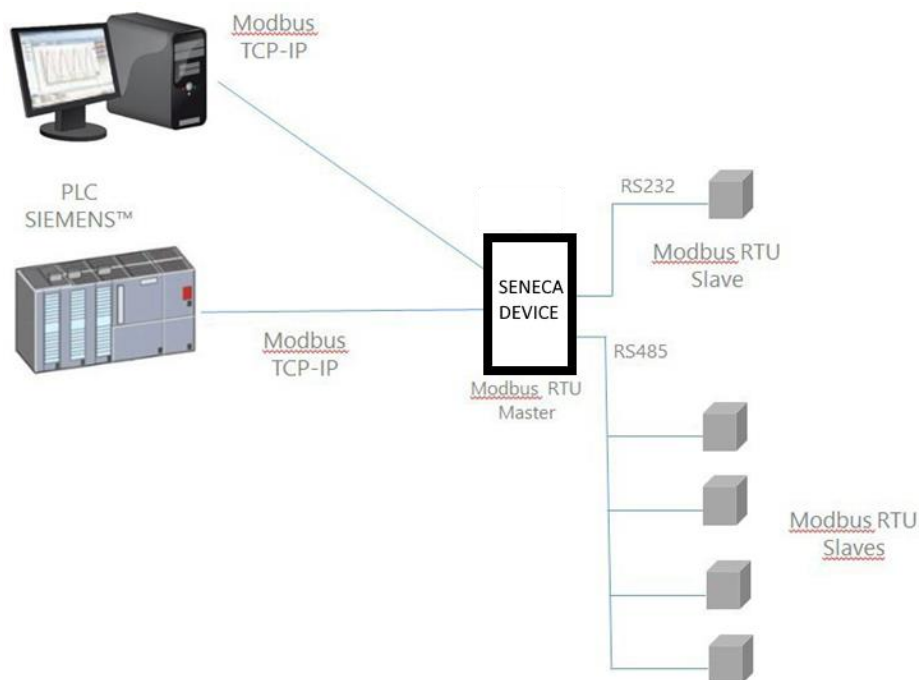
For each of the available serial ports you can define the type of "Task": a serial port can be configured as Modbus RTU Master or Modbus RTU Slave or disabled.

In this way different combinations are possible.

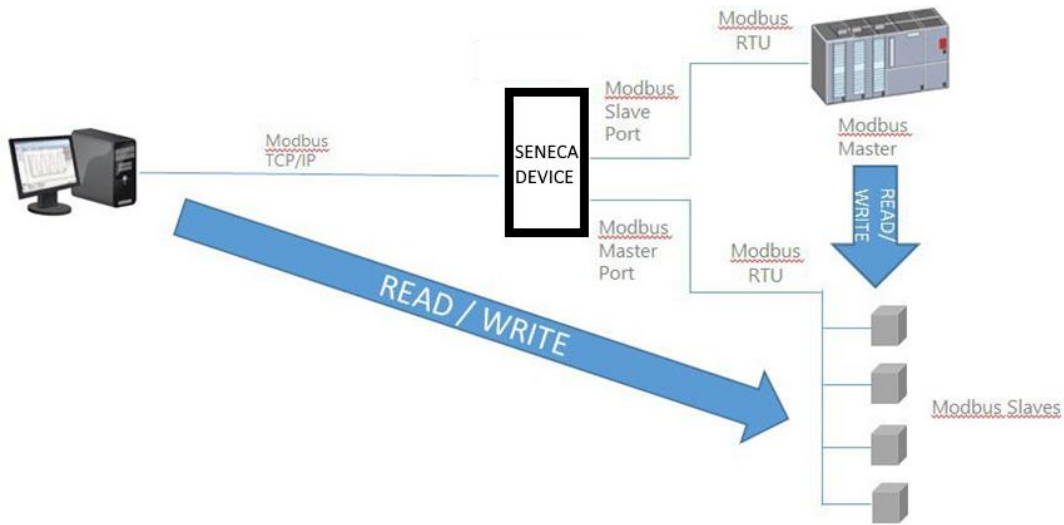
In addition, tags can be read to/from up to 25 Modbus TCP Server.

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.

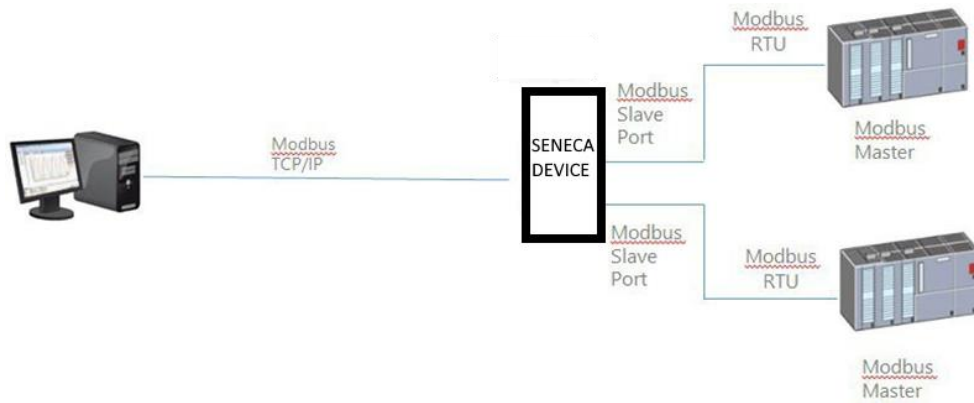


In the figure above, two serial ports are configured as Modbus RTU Master.



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;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;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;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;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:

#### Layer 2

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

#### Layer 3

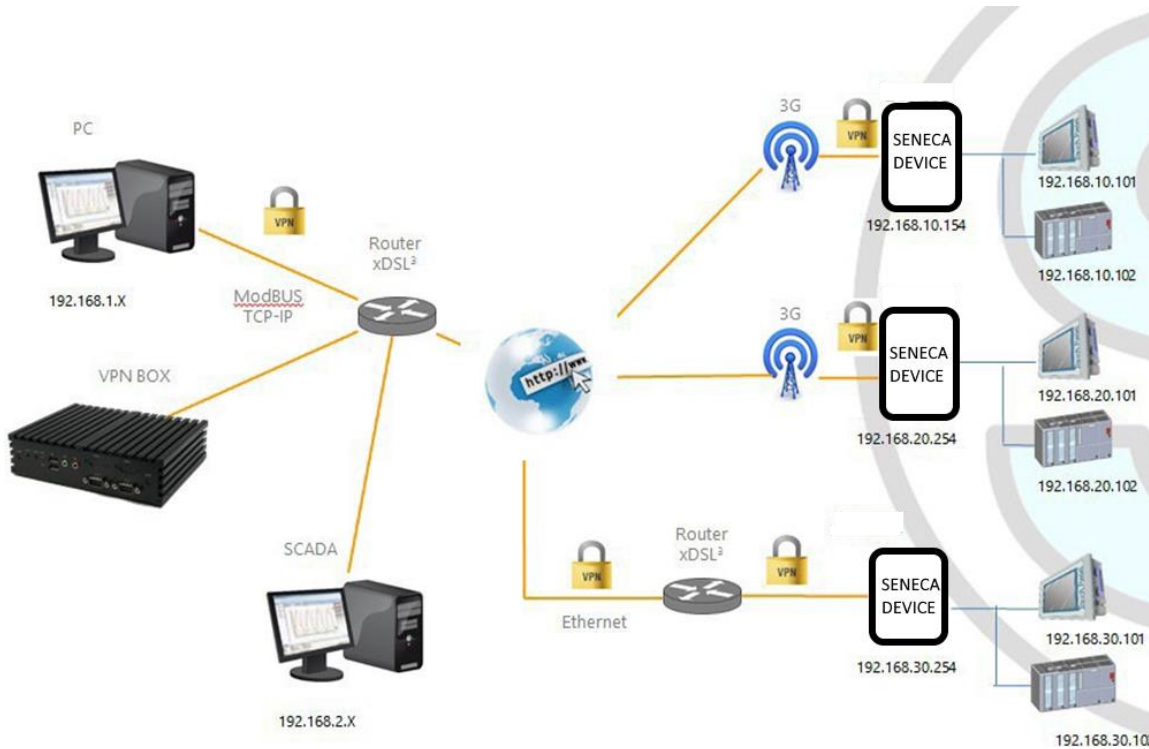
- can carry only IP traffic
- layer2 traffic (e.g.: DHCP) is not transported
- reduces traffic management costs, transports only traffic destined for clients

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.

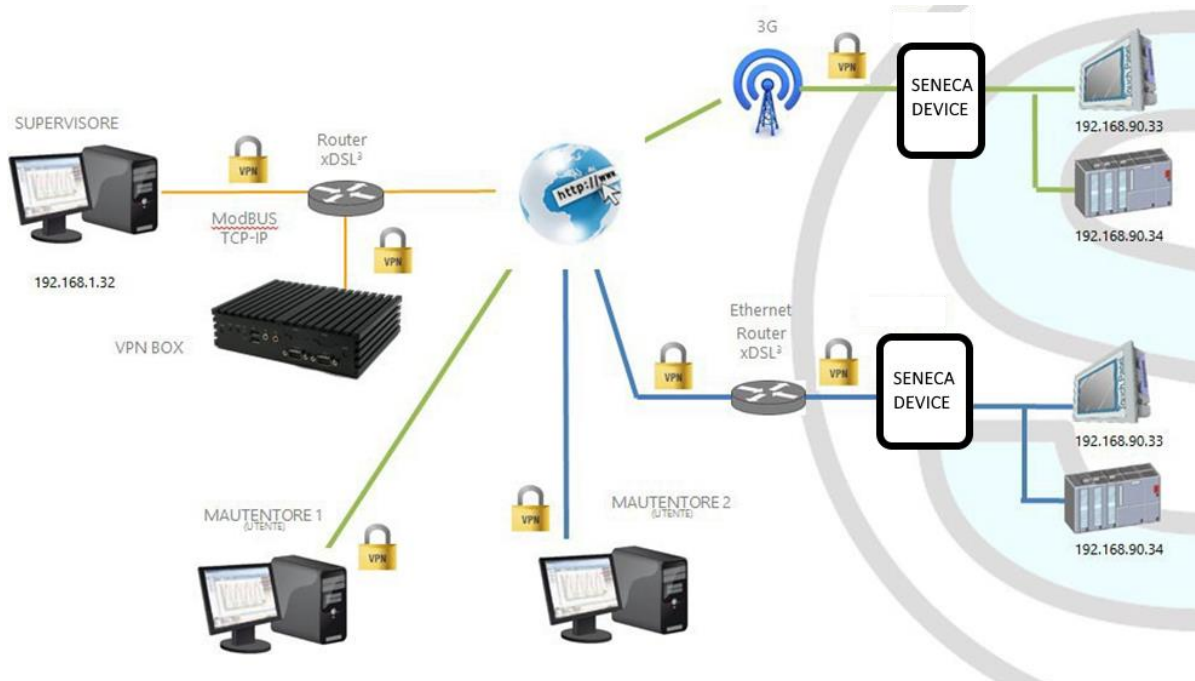
Also, two devices that are in two different LANs of the same VPN network (e.g.: 192.168.10.101 and 192.168.20.102) can connect to each other, again using their local IP addresses.

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
	4
SENECA DEVICE LAN	192.168.20.0/24
	4
SENECA DEVICE LAN	192.168.30.0/24
	4

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.

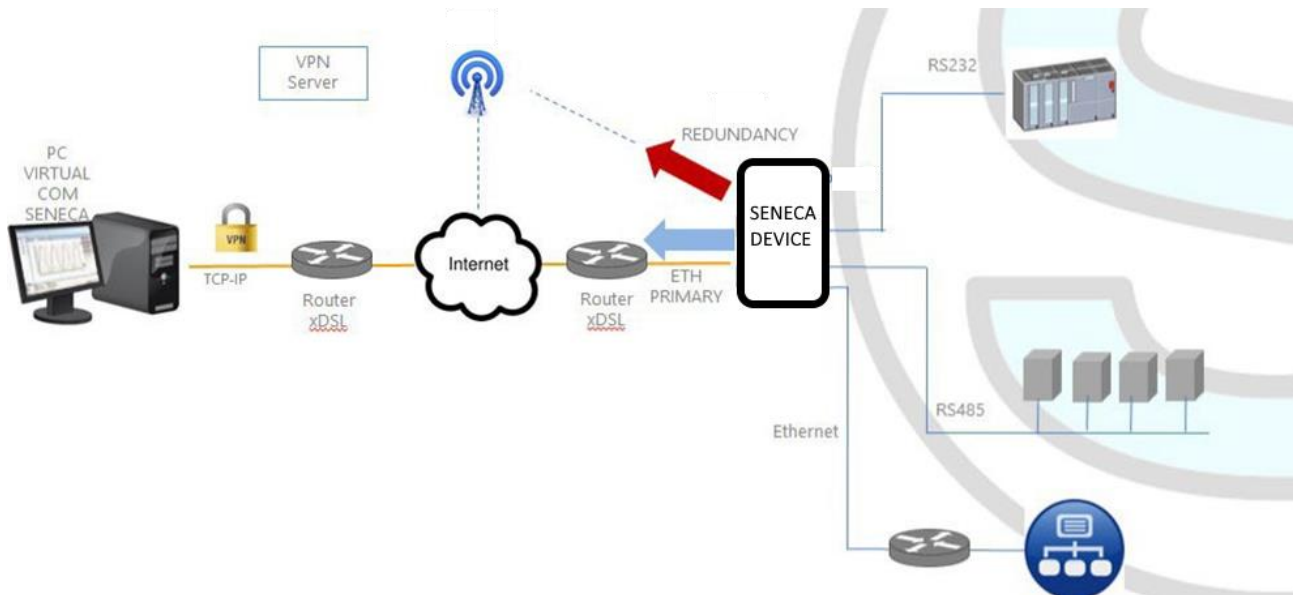
Another important feature is the availability of a DNS server/forwarder, which can resolve names with or without external DNS.

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. **HTTP 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](mailto: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](mailto: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:

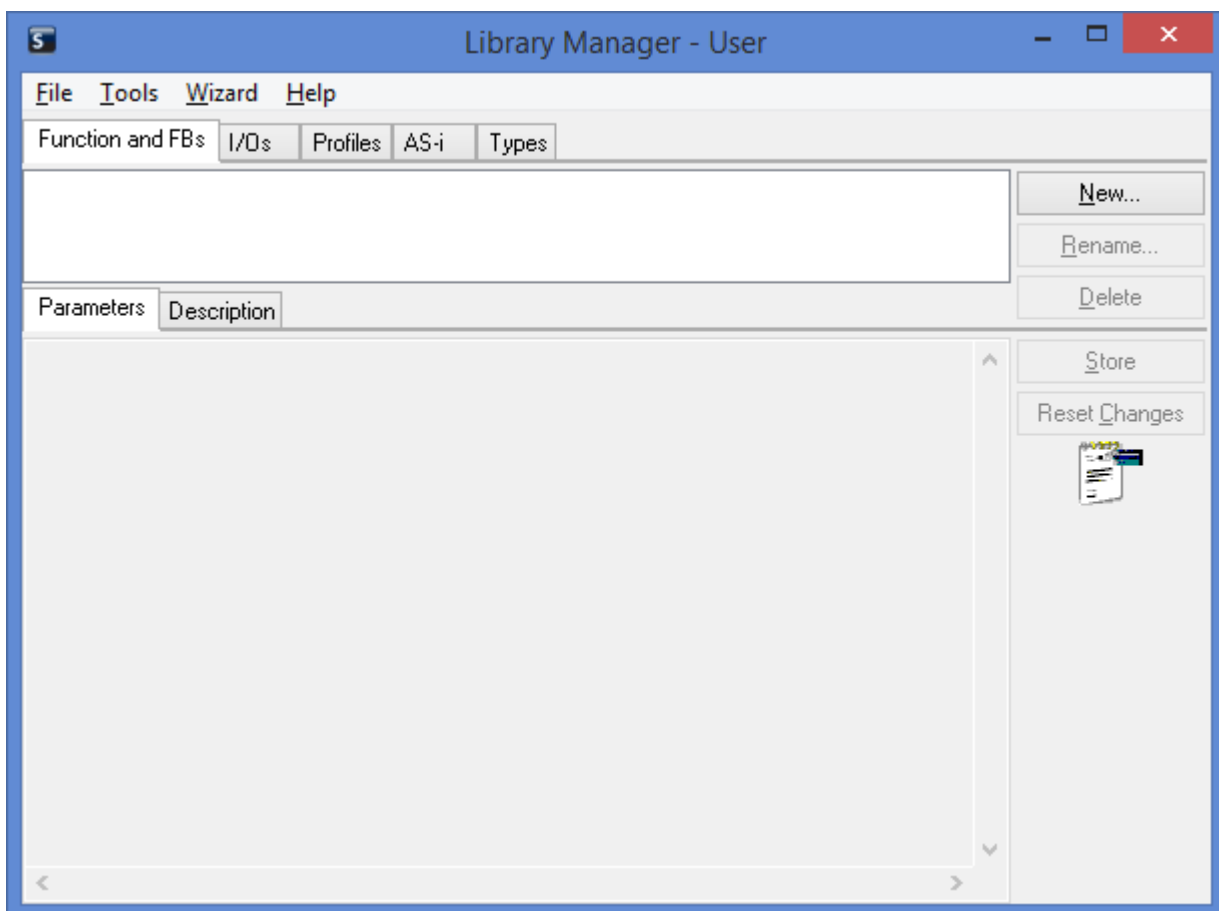
<http://www.seneca.it/products/seneca-straton-package>

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:

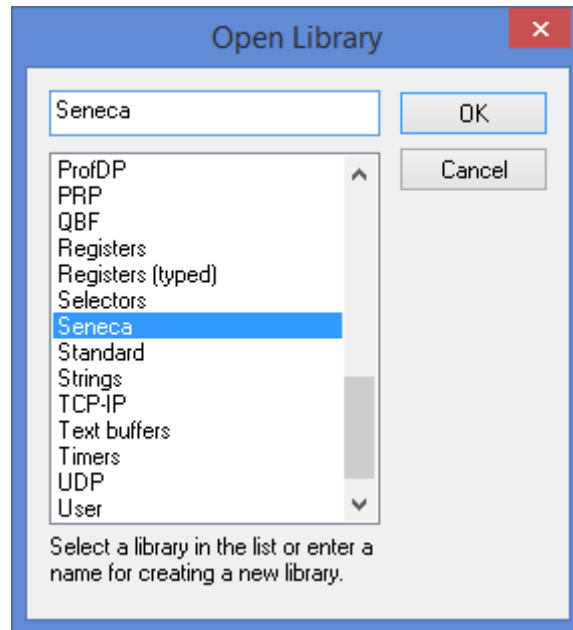
### 20.1.1. **MANUAL INSTALLATION OF LIBRARIES AND TEMPLATES IN STRATON**

The following steps are required to integrate Seneca libraries and profiles into the Straton IDE.

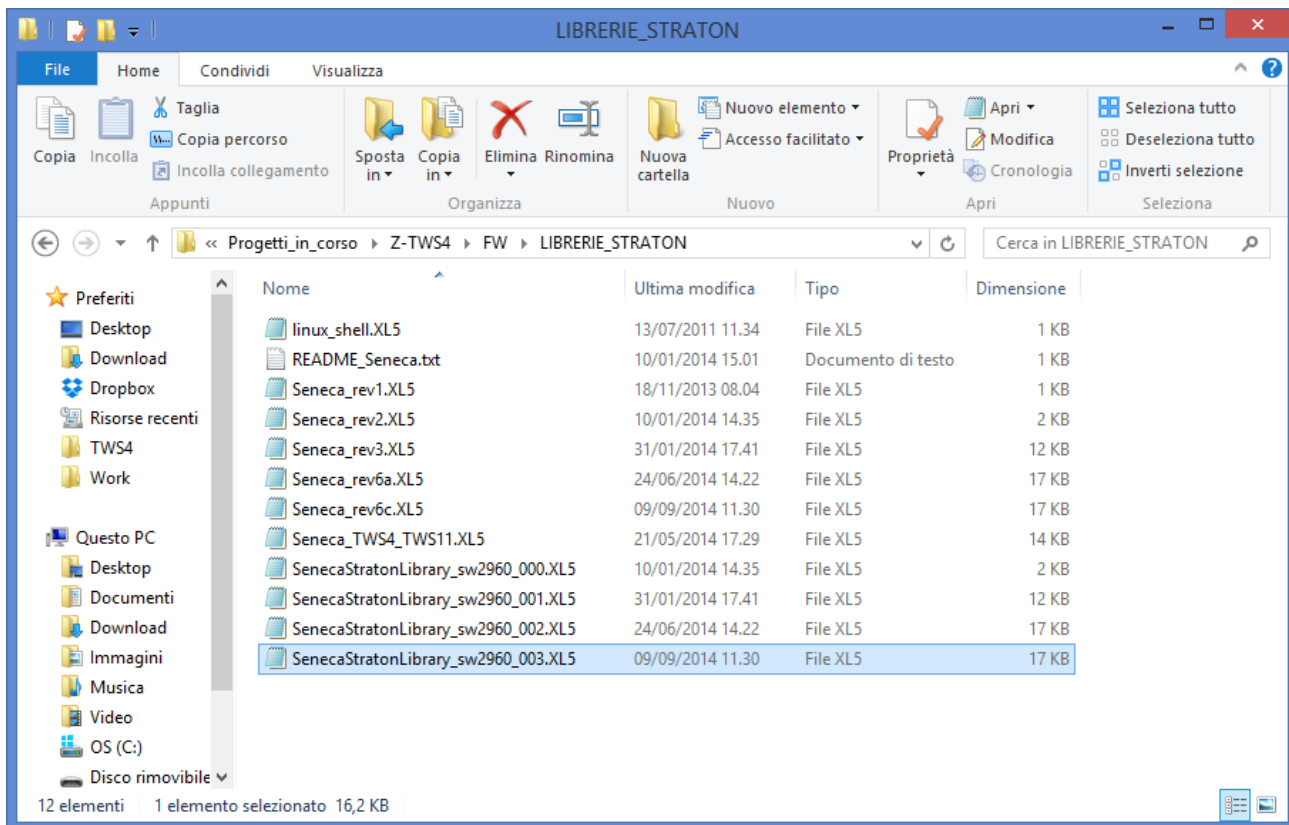
First, we need to add the Seneca FB library (SenecaStratonLibrary.XL5 file) to the IDE, using the "Library Manager" tool:

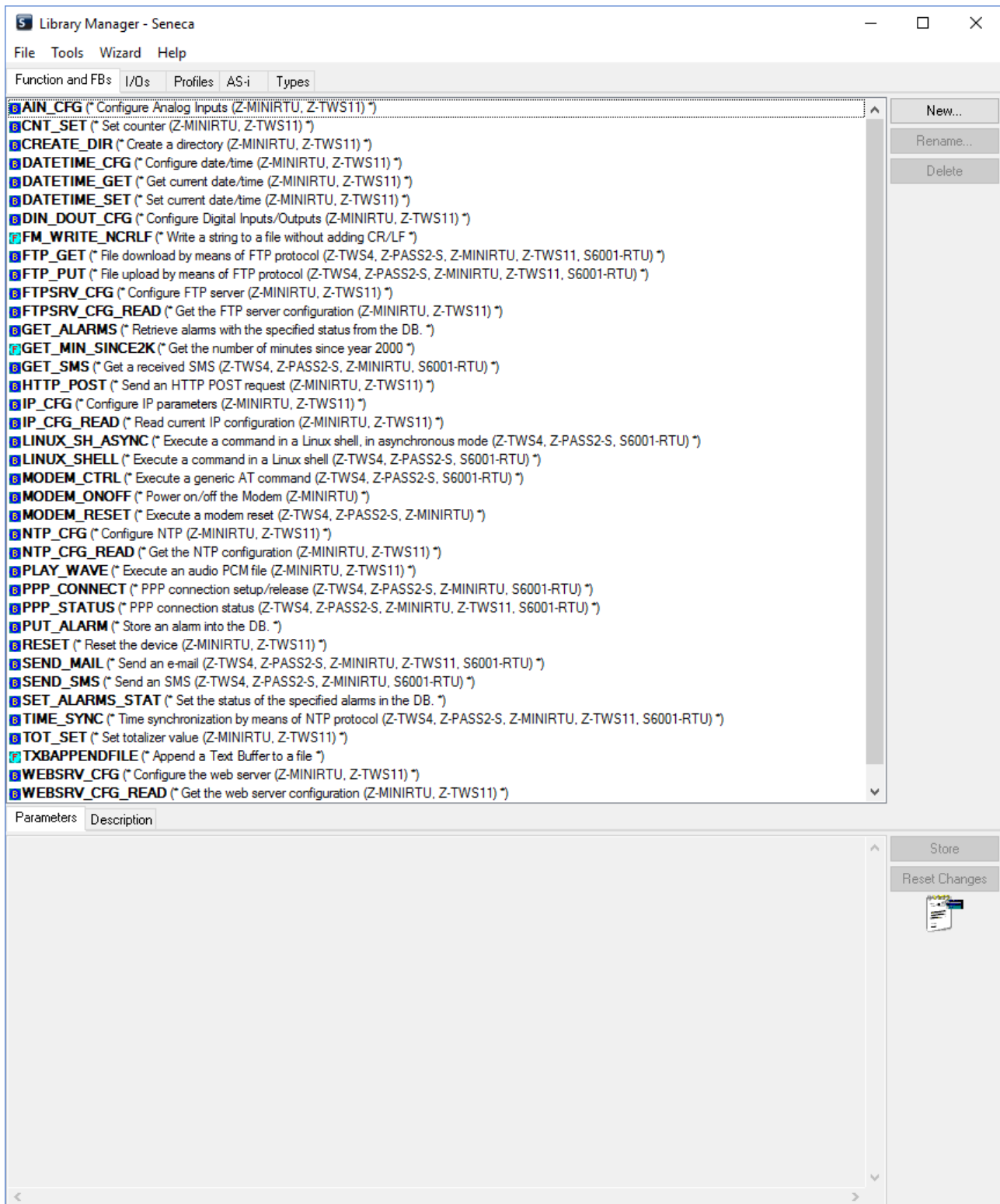


Select the "File / Open Library" option and enter the name "Seneca" to create the new Seneca library.



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



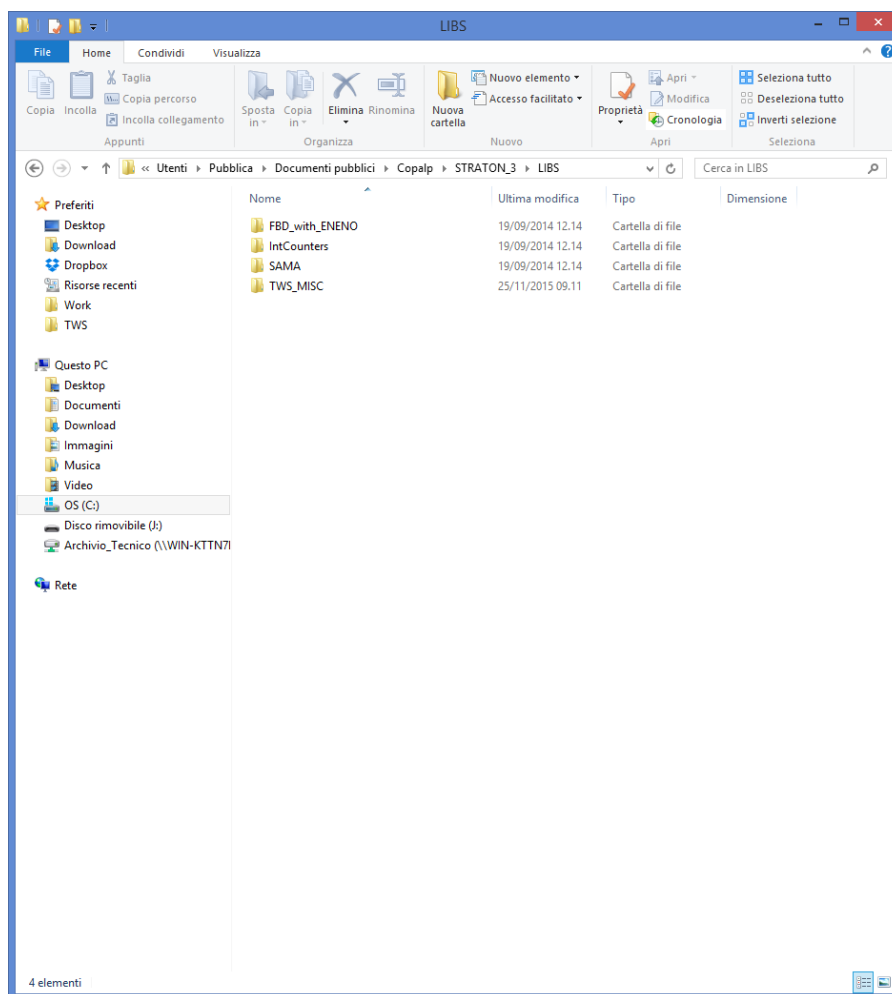


Save the library (“File / Save Library” menu).

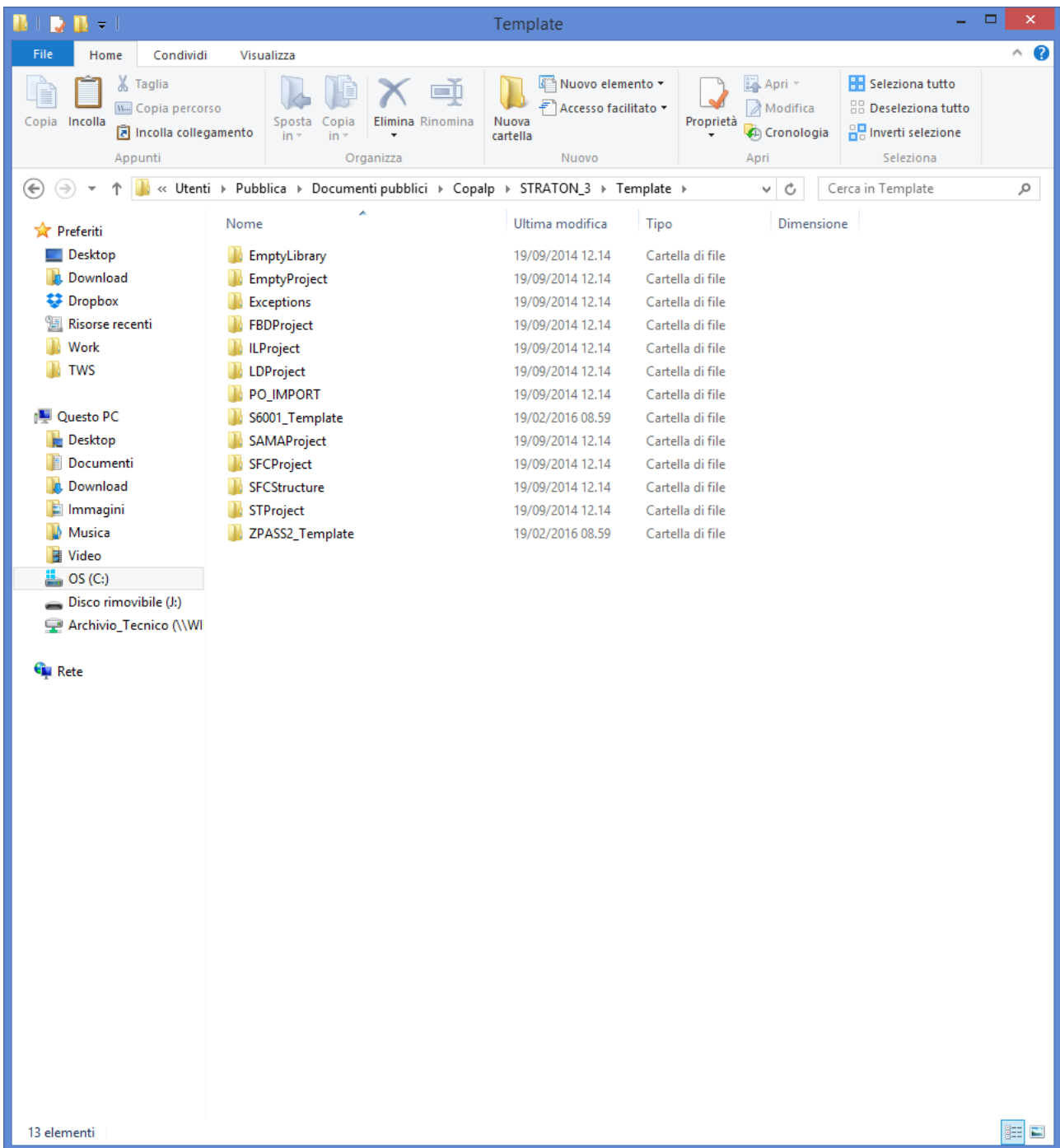
The procedure for adding the Profiles library to the IDE is identical to the one just explained; the only difference is that the SenecaStratonProfiles.XL5 file must be selected (instead of the SenecaStratonLibrary.XL5 file).

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:*



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



## 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 the V2C 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 VIA 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.

<b>Field</b>	<b>Meaning</b>
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-COMM 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
<b>IO CONFIGURATION</b>	
INPUT/OUTPUT1 MODE	<p>Remote connection disable Allows you to use the pin as input. If high blocks remote VPN access</p> <p>General Input Allows you to use the pin as a digital input</p> <p>General Output Allows you to use the pin as Digital Output</p>
INPUT/OUTPUT2 MODE	<p>Remote connection active Allows you to use the pin as an output, if active it indicates the presence of remote VPN access.</p> <p>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.</p> <p>Remote Toggle is an output controllable from the Seneca VPN box status interface.</p> <p>General Input Allows you to use the pin as a digital input</p> <p>General Output Allows you to use the pin as Digital Output</p>
<b>SECURITY LEVEL</b>	

Service Disable	<p>This parameter defines which access services are disabled when the "Remote Connection Disable" digital input is HIGH.</p> <p>The possible values are:</p> <ul style="list-style-type: none"><li>Blocking VPN Connection (VPN Service and Internet active)</li><li>VPN Service blocking (Internet active)</li><li>Blocking of internet access (both internet and VPN are blocked in the device)</li></ul>
-----------------	---

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 register 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 OpenVPN 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	<p>“None”                      “Basic128Rsa15”                      “Basic256Sha256”</p> <p>Note:                      a predefined pair of certificates is already included in the product.</p>

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

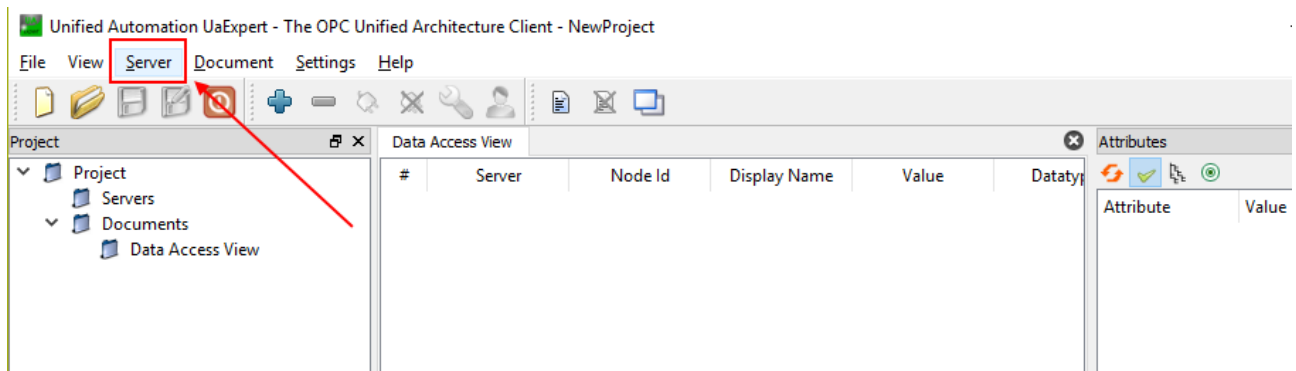
The device's OPC-UA server "exports" the Modbus Shared Memory Gateway tags; therefore, using an OPC-UA client software, it is possible to read / write tags using the OPC-UA protocol.

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

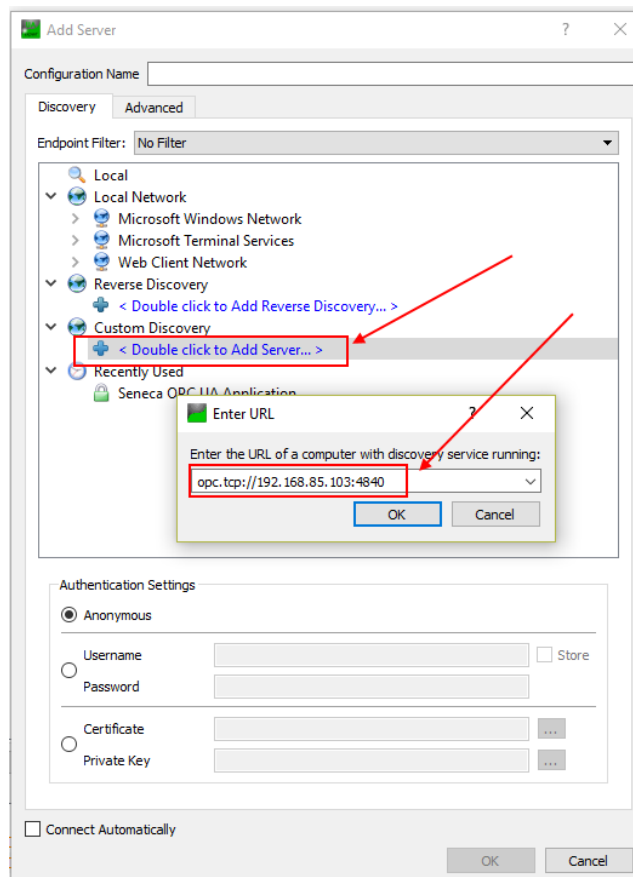
### 22.10.1.UA EXPERT CLIENT CONFIGURATION

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

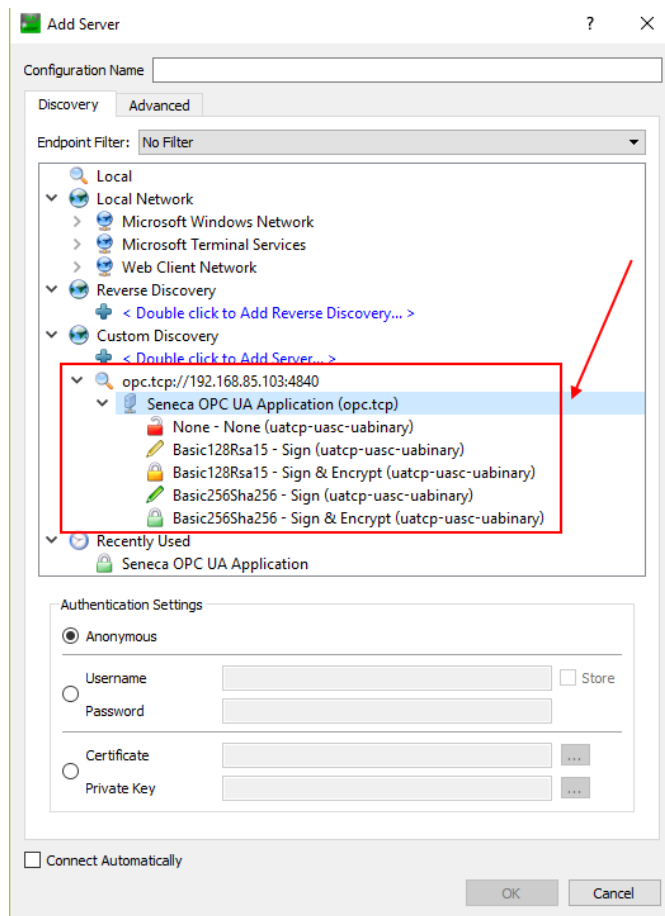


In "Custom Discovery" enter the url for the OPC-UA server:

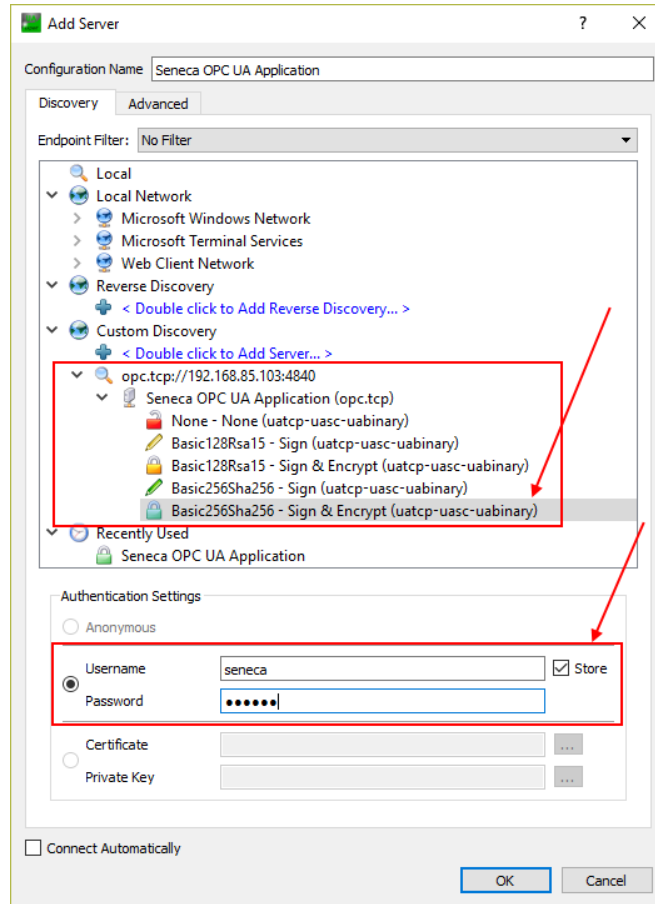


Press OK.

Supported security policies are now displayed:

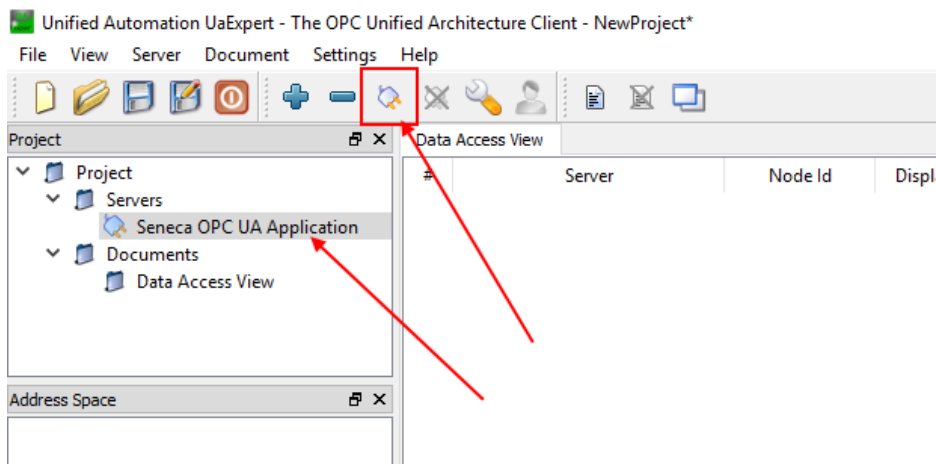


Select the one to use. Then go to Authentication settings and enter the user name and password configured in the OPC-UA server:

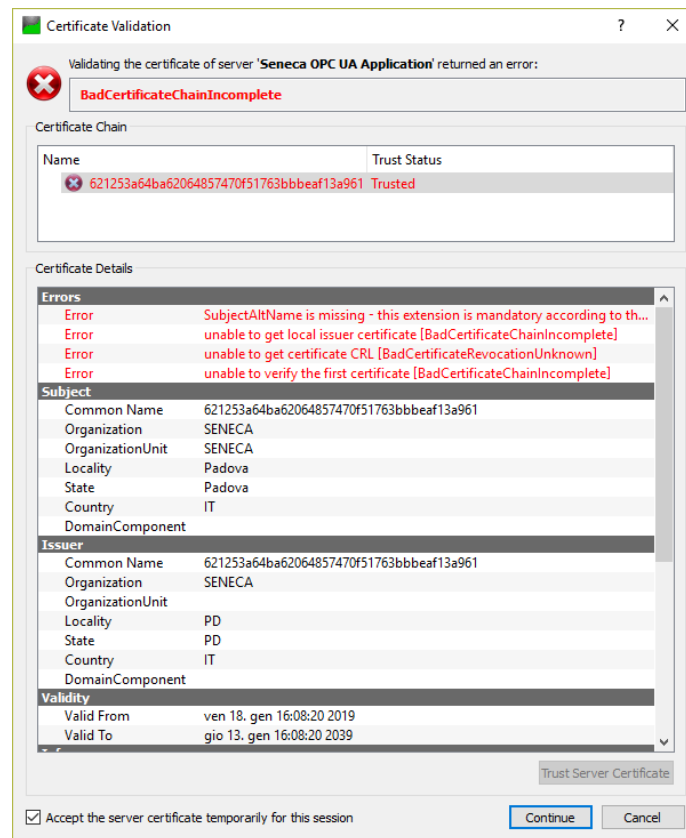


Press OK:

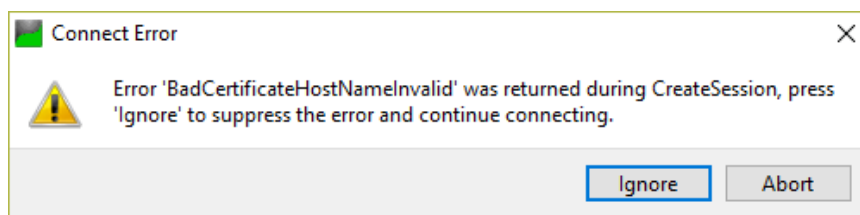
Now it is possible to connect to the server using the appropriate icon:



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.

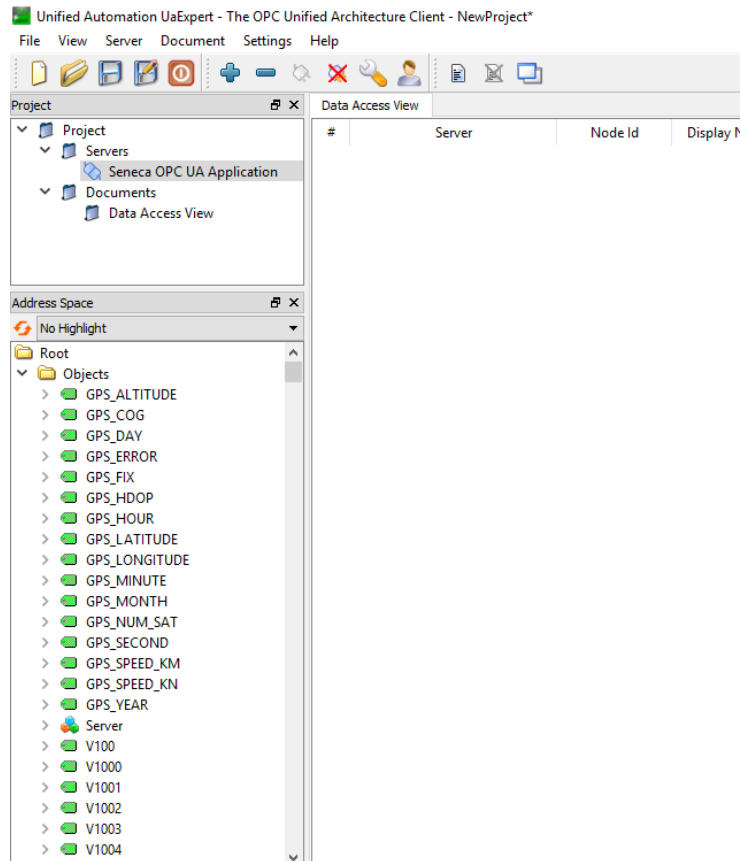


The Certificate Error window will now appear:

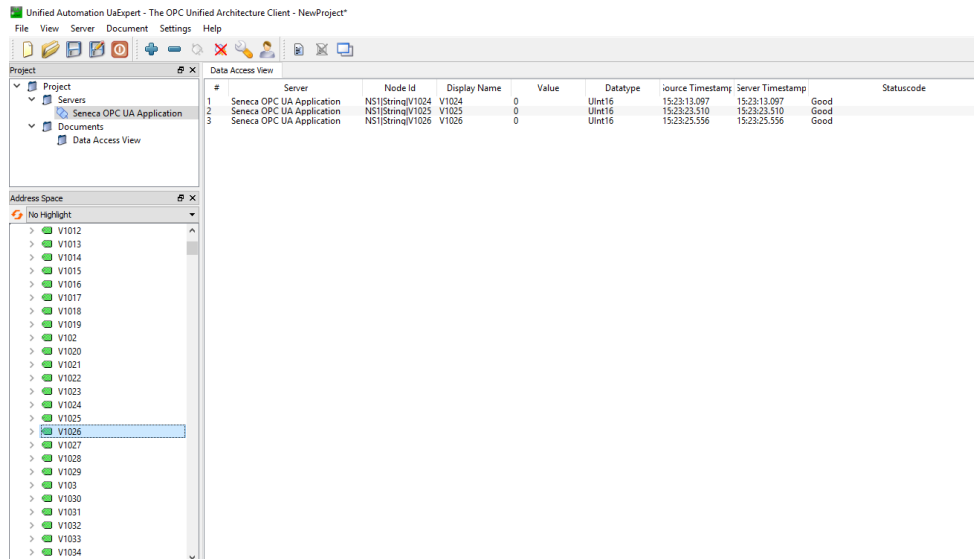


Click on "Ignore" to continue.

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.



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	ON	ON ▾		
<i>When this parameter is OFF, access will be allowed only for hosts below with "Access" checked.</i>				
Communities				
	Name	Read	Write	
Community 1	public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community 2	private	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Community 3		<input type="checkbox"/>	<input type="checkbox"/>	
Community 4		<input type="checkbox"/>	<input type="checkbox"/>	
Community 5		<input type="checkbox"/>	<input type="checkbox"/>	
Hosts				
	IP Address	Community	Access	Trap
Host 1		public ▾	<input type="checkbox"/>	<input type="checkbox"/>
Host 2		public ▾	<input type="checkbox"/>	<input type="checkbox"/>
Host 3		public ▾	<input type="checkbox"/>	<input type="checkbox"/>
Host 4		public ▾	<input type="checkbox"/>	<input type="checkbox"/>
Host 5		public ▾	<input type="checkbox"/>	<input type="checkbox"/>

APPLY

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

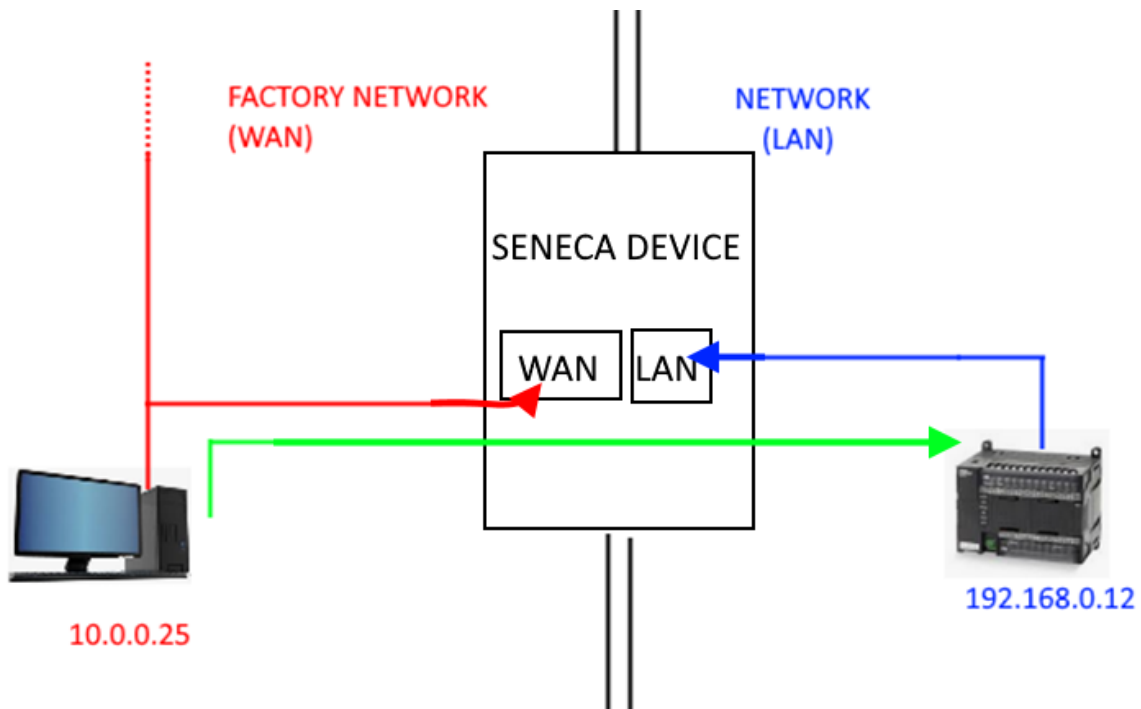
In this example 2 rules have been set:

Enable	ON	ON ▼
<i>Port Mapping / Virtual Server 1</i>		
Protocol	TCP	TCP ▼
External Port	80	80
Server IP Address		
Internal Port	8080	8080
<i>Port Mapping / Virtual Server 2</i>		
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
<b>NAT 1:1 Configuration</b>		
Interface	WAN	
Device IP Address	192.168.0.12	
Mapped IP Address	10.0.0.26	
Description	WAN to LAN ACCESS1	
<input type="button" value="APPLY"/>		

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
<b>Static Route Configuration</b>		
Destination Address	192.168.85.23	
Subnet Mask	255.255.255.255	
Gateway	192.168.80.1	
Interface	LAN	
Description	Go to 85	
<input type="button" value="APPLY"/>		

And also:

	CURRENT	UPDATED
<b>Static Route Configuration</b>		
Destination Address	192.168.82.56	
Subnet Mask	255.255.255.255	
Gateway	192.168.80.100	
Interface	LAN	
Description	Go to 82	
<input type="button" value="APPLY"/>		

### 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:

		<input type="button" value="ADD"/>	<input type="button" value="MODIFY"/>	<input type="button" value="DELETE"/>					
#	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		<input type="text" value="TAG"/>	
GATEWAY MODBUS START REGISTER ADDRESS		<input type="text" value="1"/>	Equivalent to the address in the Seneca documentation : 10001
TARGET DEVICE		<input type="text" value="Z-10-D-IN"/>	
TARGET RESOURCE		<input type="text" value="INPUT 1"/>	
TARGET CONNECTED TO		<input type="text" value="COM2"/>	
TARGET MODBUS STATION ADDRESS		<input type="text" value="1"/>	
TARGET MODBUS START REGISTER ADDRESS		<input type="text" value="1"/>	Equivalent to the address in the Seneca documentation : 10001
TARGET MODBUS REQUEST TYPE		<input type="text" value="DISCRETE INPUT"/>	
TARGET REGISTER DATA TYPE		<input type="text" value="BOOL"/>	
GATEWAY TAG MODE		<input type="text" value="GATEWAY"/>	
GAIN		<input type="text" value="1"/>	
OFFSET		<input type="text" value="0"/>	
ERROR MODE		<input type="text" value="LAST VALUE"/>	
HTTP POST VID		<input type="text" value="26"/>	Corresponding to HTTP POST variable : V26
READ ONLY		<input type="text" value="OFF"/>	If ON, tag value cannot be changed by means of Modbus protocol
EXPORT TO DISPLAY		<input type="text" value="ON"/>	If ON, this tag will be shown in SMART-DISPLAY GUI
ALARM ENABLED		<input type="text" value="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.

	<p>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.</p> <p>EMBEDDED for integrated digital I/Os on board the device</p>
Gain	<p>This field corresponds to the value of the coefficient <math>m</math> in the formula <math>m * val + q</math> applied to the value "val" read by the device</p>
Offset	<p>This field corresponds to the value of the coefficient <math>q</math> in the formula <math>m * val + q</math> applied to the value "val" read by the device</p>
Initial Value	Start value of the tag
Error Mode	<p>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.</p> <p>The possible ways are:</p> <p>LAST VALUE: the last available value is given.</p> <p>ERROR VALUE: the value specified in the field " ERROR VALUE " is provided.</p>
Error Value	<p>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 ".</p>
HTTP POST VID	<p>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).</p> <p>The VID string is given by the "V" character plus the number contained in the field</p>
Read Only	<p>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.</p>
Retain	<p>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.</p> <p>This option is only available for SHARED MEMORY tags.</p>
Calculated Function	<p>Only active if Tag mode is "Shared Memory". Can be used to calculate the MIN / MAX / AVG value of a tag.</p> <p>Note that the calculation is only enabled if the datalogger is enabled. The averaging calculation time is given by the acquisition time.</p>
Export to Display	<p>If active it allows you to display the tag on the display or virtual display (depending on the device)</p>
Alarm Enabled	<p>This field is a read-only flag that indicates whether an alarm has been defined for the tag.</p>

### 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* (yyy=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: <ul style="list-style-type: none"> <li>- None</li> <li>- TLS/SSL Implicit</li> <li>- TLS/SSL Explicit</li> </ul>
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

Broker Host	Defines the host name of the MQTT broker																		
Broker Port	Defines the MQTT broker port																		
Use WebSockets	Allows you to activate MQTT communication via Websockets																		
Keep Alive Interval (seconds)	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.																		
Clean Session	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.																		
Message Retain	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.																		
Quality of service	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)																		
Authentication	This parameter defines whether user/password authentication should be used to access the broker																		
Username	Broker Username																		
Password	Broker password																		
SSL/TLS	Defines if the crypto is SSL/TLS																		
Log on Change	This parameter defines whether topics should only be sent in case of change (based on minimum time) or not.																		
Publish with multiple tags	This parameter defines whether the publish contains multiple tags or whether the device should send a publish for each tag																		
Publish Topic for Logs	Select the topic name for the logs using the following table: <table border="1" data-bbox="486 1541 1428 2016"> <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>	%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")
%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")																		

	<table border="1"> <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>	%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																		
%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																										
Publish Payload for Logs	<p>Select the format to be used for the payload in Json format using the following table:</p> <table border="1"> <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>	%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
%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																										
Publish Bulk Format	<p>Select the format for "bulk mode" according to the following table:</p> <table border="1"> <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>	%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")						
%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")																										

	<table border="1"> <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>	%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																				
%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	<p>Select the format for topic names in alarms according to the following table:</p> <table border="1"> <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>	%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
%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	<p>Select the Topic Subscribe according to the following table:</p> <table border="1"> <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>	%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
%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																										

LWT Topic	Select the "Last Weel and Testament" topic according to the following table: <table border="1"> <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>	%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
%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																										
LWT Payload	Select the Payload text of "Last Weel and Testament"																										
Save Configuration URL	This is the URL for the "Save Configuration" command received from mqtt																										
Load Configuration URL	This is the URL for the "Load Configuration" command received from mqtt																										
FW Update URL	This is the URL for the "FW Update" command received from mqtt																										
Sleep Timeout	MQTT task wake-up time, the shorter it is, the more responsive MQTT is (at the expense of higher CPU load).																										
MQTT Certificates	It is used to manage the certificates necessary for the TLS connection.																										

## 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.

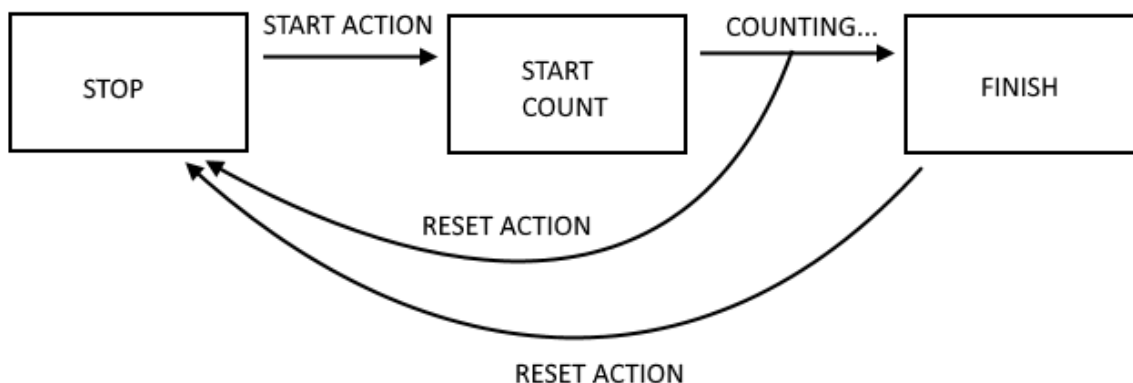
The ID represents the mnemonic of the timer that must be used in the rules.

"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)

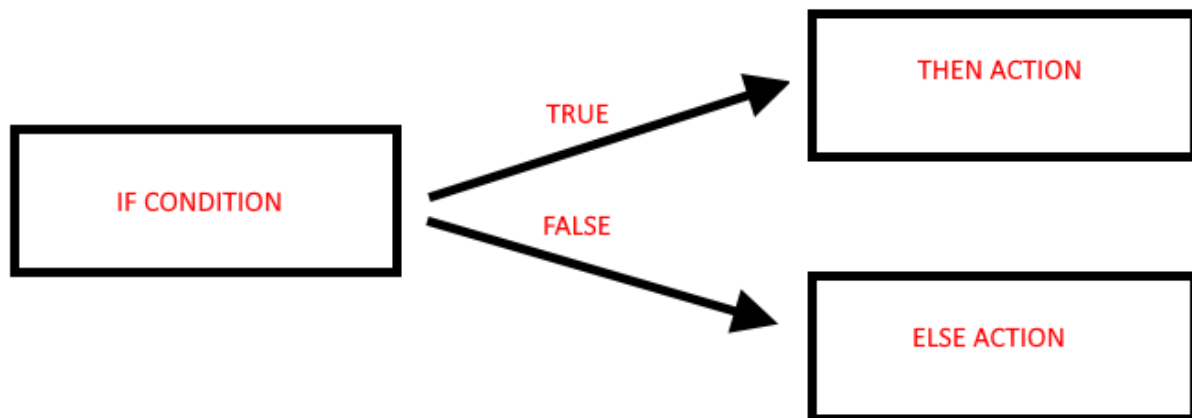
In this section you can define a set of logical rules that will implement a program.

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:



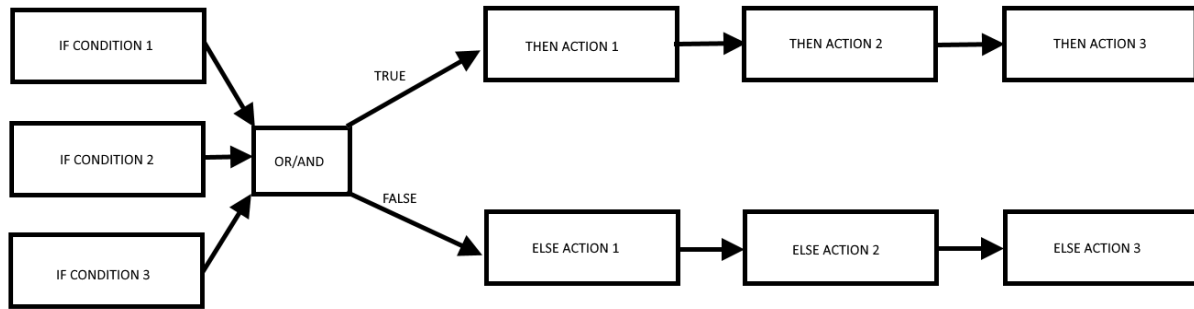
If the "IF" condition is true, the "THEN" action is executed, otherwise the "ELSE" action is executed.

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

		CURRENT	UPDATED												
<b>RULE GENERAL CONFIGURATION</b>															
Writing Mode		After execution	After execution												
APPLY															
<b>RULE STATUS</b>															
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	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	2
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	OR	---	AREA = RADIUS1 * 3.14	AREA =	---	AREA = RADIUS2 * 3.14	AREA =	---	FALSE	4

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]	<p>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).</p> <p>If the value is different from 0 ms the actions are performed trying to respect the inserted timing.</p> <p>Do not use small period values for sending EMAIL / SMS / HTTP / MQTT actions!</p> <p>NOTE: If Period is &gt; 0 the actions are always performed in "repeat" mode</p>
If Condition X Type Where X=[1..3]	<p>This parameter defines the type of condition, for each of the three "if conditions" available (1..3)</p> <p>The possible types are:</p> <p><b>None</b> No conditions to be assessed</p> <p><b>Alarm State</b> See 22.32.1</p> <p><b>Alarm Active</b> See 22.32.2</p> <p><b>Always</b> 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 &gt; 0ms.</p> <p><b>Digital Tag</b> See 22.32.3</p> <p><b>Analog Tag</b> See 22.32.4</p> <p><b>Timer</b></p>

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

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

**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	<p>Alarm status.</p> <p>Possible states are:</p> <ul style="list-style-type: none"> <li>- <b>None</b></li> <li>- <b>Alarm (digital only)</b></li> <li>- <b>Alarm Low Low (analog only)</b></li> <li>- <b>Alarm Low (analog only)</b></li> <li>- <b>Alarm High (analog only)</b></li> <li>- <b>Alarm High High (analog only)</b></li> <li>- <b>Acknowledge</b></li> <li>- <b>Return</b></li> <li>- <b>End</b></li> </ul> <p>Depending on the type (digital or analog) of the selected alarm, some states are disabled</p>
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	<p>Indicates whether or not the alarm should be active.</p> <p>The alarm is active if it is in one of these states:</p> <ul style="list-style-type: none"> <li>- <b>Alarm (only for digital tags)</b></li> <li>- <b>Alarm Low Low (only for analog tags)</b></li> <li>- <b>Alarm Low (only for analog tags)</b></li> <li>- <b>Alarm High (only for analog tags)</b></li> <li>- <b>Alarm High High (only for analog tags)</b></li> <li>- <b>Acknowledge</b></li> </ul> <p>The alarm is not active if it is in one of the following states:</p> <ul style="list-style-type: none"> <li>- <b>None</b></li> <li>- <b>Return</b></li> <li>- <b>End</b></li> </ul>
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

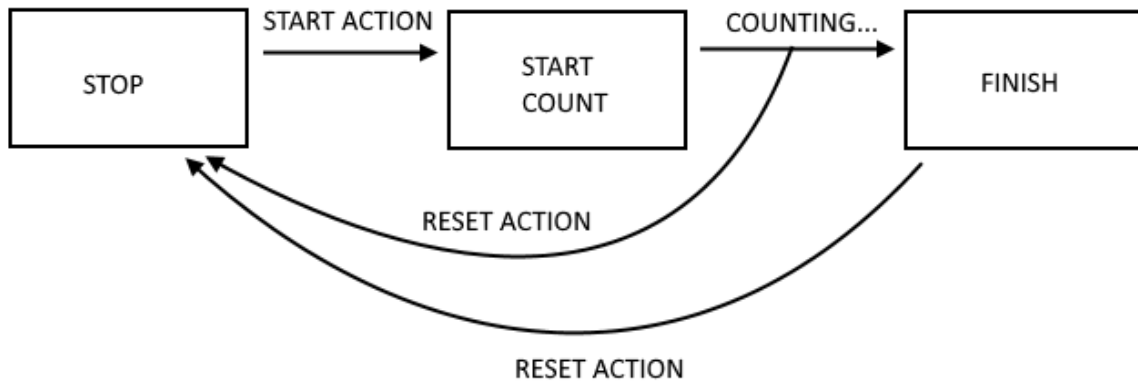
#### 22.32.4. "ANALOG TAG" PARAMETERS

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

	<p>Example: Destination tag = Destination tag + Origin tag 1</p> <p>"- =" 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</p> <p>"* =" 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</p> <p>"/ =" 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</p> <p>"% =" 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)</p> <p>Example: Destination tag = Destination tag% Source tag1</p> <p>"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)</p> <p>Example: Target tag = abs (Source tag 1)</p> <p>"Sqrt"</p>
--	--

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

	<p>Example: Target tag = Source tag 1+ Source tag 2</p> <p>"_" 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</p> <p>"*" 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</p> <p>"/" 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</p> <p>"%" 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</p> <p>"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 = <math>[(\text{Source Tag1}) ^ (\text{Source Tag2})]</math></p>
--	--

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:

- VPN Configuration
- Router Configuration
- Users Configuration
- Mobile Configuration
- Mobile Network
- DDNS Configuration
- Shared Memory Tag Conf.
- TCP Servers
- Tag Setup
- Tag View
- Alarms
- Alarm Configuration
- Alarm Summary
- Alarm History
- Logic Configuration
- Phonebook
- SMS Configuration
- Email Configuration
- HTTP Configuration
- Message Configuration

**TAG 27**

	CURRENT	UPDATED	
GATEWAY TAG NAME	RADIUS1	<input type="text" value="RADIUS1"/>	
GATEWAY MODBUS START REGISTER ADDRESS	100	<input type="text" value="100"/>	Equivalent to the address in the Seneca documentation : 40100
TARGET CONNECTED TO	INTERNAL	<input type="text" value="INTERNAL"/>	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	<input type="text" value="HOLDING REGISTER"/>	
TARGET REGISTER DATA TYPE	16BIT SIGNED	<input type="text" value="16BIT SIGNED"/>	
GATEWAY TAG MODE	SHARED MEMORY	<input type="text" value="SHARED MEMORY"/>	
INITIAL VALUE	0	<input type="text" value="0"/>	
HTTP POST VID	26	<input type="text" value="26"/>	Corresponding to HTTP POST variable : V26 If READ ONLY = ON, tag value cannot be changed by means of Modbus protocol
READ ONLY	OFF	<input type="text" value="OFF"/>	
CALCULATED FUNCTION	NONE	<input type="text" value="NONE"/>	
ALARM ENABLED	OFF	<input type="text" value="OFF"/>	This parameter can be changed in "Alarm Configuration" page

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

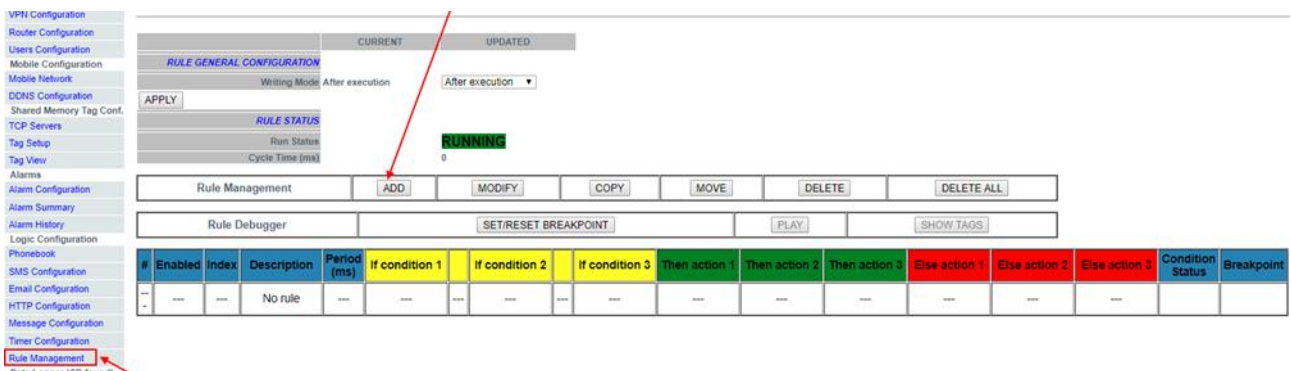
### TAG 29

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

### TAG 30

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

Now click on "Rules Management" and then on ADD to add a new 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
<b>RULE CONFIGURATION</b>		
<p><i>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&gt;0 are always executed. In all other cases, actions are executed only when there is a change in the condition result.</i></p>		
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):

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

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

<b>Then Action 1</b>		
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
<b>Then Action 2</b>		
Type	None	None ▼
<b>Then Action 3</b>		
Type	None	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

Action Mode One time

Destination Tag CIRCUMFERENCE

Operator \*

Source Tag 1 RADIUS2

Source Tag 2 constant value

Constant Value 2 6.28

**Else Action 2**

Type

**Else Action 3**

Type

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	---	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

Index 2

Description Calculate Biggest Area

Period (ms) 1000

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

**if Condition 1**

Type Analog Tag

Tag RADIUS1

Operator >

Tag RADIUS2

**if Condition 2**

Type None

**if Condition 3**

Type None

**if Condition Operator**

Operator OR

Now we have to calculate the AREA using the following calculation:

$$\text{AREA} = ([\text{RADIUS}] ^ 2) * 3.14$$

We have to break the formula in two phases:

In the first phase we calculate:

$$\text{AREA} = (\text{RADIUS1}) ^ 2$$

And in the second:

$$\text{AREA} = \text{AREA} * 3.14$$

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

$$\text{AREA} = \text{sqr} (\text{RADIUS1})$$

And then

$$\text{AREA} = \text{AREA} * 3.14$$

Then Action 1		Type	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
Action Mode	One time	One time	
Destination Tag	AREA	AREA	
Operator	*	*	
Source Tag 1	AREA	AREA	
Source constant value	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:

**EIse Action 1**

Type Analog Tag

Action Mode One time

Destination Tag AREA

Operator eqr

Source Tag 1 RADIUS2

---

**EIse Action 2**

Type Analog Tag

Action Mode One time

Destination Tag AREA

Operator \*

Source Tag 1 AREA

Source Tag 2 constant value

Constant Value 2 3.14

---

**EIse Action 3**

Type

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	EIse action 1	EIse action 2	EIse action 3	Condition Status	Breakpoint
1	ON	1	Calculate Biggest Circumference	1000	RADIUS1 > RADIUS2	OR	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	---
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	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):

Writing Mode After execution

**RULE STATUS**

Run Status **RUNNING**

Cycle Time (ms) 0

Rule Management

Rule Debugger

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

Router Configuration

Users Configuration

Mobile Configuration

Mobile Network

DDNS Configuration

Shared Memory Tag Conf.

TCP Servers

Tag Setup

**Tag View**

Alarms

Alarm Configuration

Alarm Summary

Alarm History

Logic Configuration

Phonebook

SMS Configuration

Email Configuration

HTTP Configuration

Message Configuration

Timer Configuration

Rule Management

Data Logger (SD found)

General Settings

SD Transfer Conf.

FTP Transfer Conf.

Group Configuration

SD File Manager

Maintenance

Ethernet Interfaces

Data Logger:

Page : 1/20

			REGISTER	UNSIGNED						
17	GPS_YEAR	16	HOLDING REGISTER	16BIT REGISTER	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	<input type="button" value="CHANGE"/>
28	RADIUS2	101	HOLDING REGISTER	16BIT SIGNED	0	-	07/03/2019 10:07:25.651519	NONE	NONE	<input type="button" value="CHANGE"/>
29	CIRCUMFERENCE	103	HOLDING REGISTER	32BIT REAL MSW	0	-	07/03/2019 11:11:16.130379	NONE	NONE	<input type="button" value="CHANGE"/>
30	AREA	105	HOLDING REGISTER	32BIT REAL MSW	0	-	07/03/2019 11:11:16.130488	NONE	NONE	<input type="button" value="CHANGE"/>

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

192.168.85.103:8080 dice

RADIUS1

192.168.85.103:8080 dice

RADIUS2

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	<input type="button" value="CHANGE"/>
28	RADIUS2	101	HOLDING REGISTER	16BIT SIGNED	50	-	07/03/2019 11:34:12.465220	NONE	NONE	<input type="button" value="CHANGE"/>
29	CIRCUMFERENCE	103	HOLDING REGISTER	32BIT REAL MSW	628	-	07/03/2019 11:34:39.634836	NONE	NONE	<input type="button" value="CHANGE"/>
30	AREA	105	HOLDING REGISTER	32BIT REAL MSW	31400	-	07/03/2019 11:34:39.634973	NONE	NONE	<input type="button" value="CHANGE"/>

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

CURRENT
UPDATED

**RULE GENERAL CONFIGURATION**

Writing Mode: After execution After execution ▾

**RULE STATUS**

Run Status: RUNNING

Cycle Time (ms): 0

Rule Management

Rule Debugger

#	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	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	TRUE	---
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	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 ▾

**RULE STATUS**

Run Status: RUNNING

Cycle Time (ms): 0

Rule Management

Rule Debugger

#	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	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	---
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	OR	---	AREA sqr RADIUS1	AREA = AREA * 3.14	---	AREA sqr RADIUS2	AREA = AREA * 3.14	---	FALSE	---

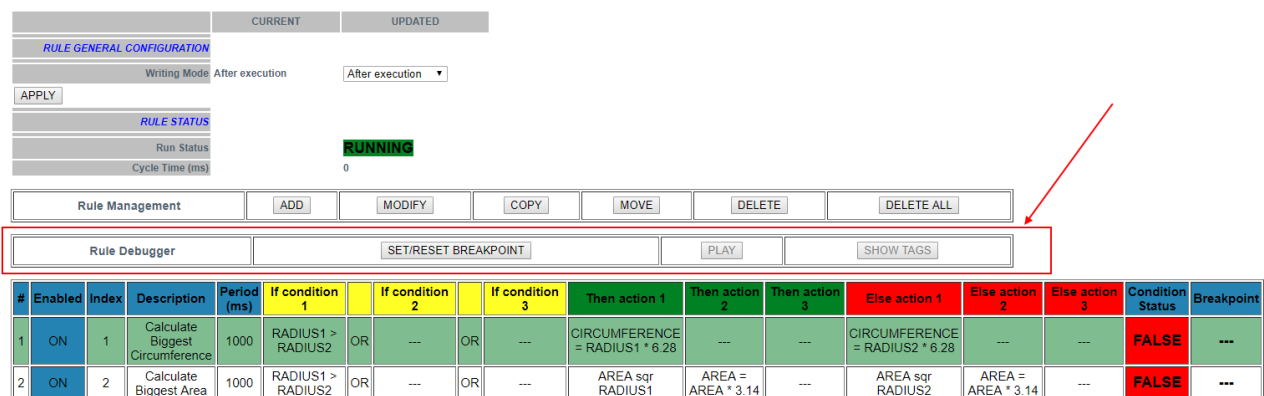
Now the condition status of the 2 rules is false because  $RADIUS1 < RADIUS2$ , so the "Else Actions" are executed

It is also possible to debug the program using the internal rule debugger.

With the internal debugger it is possible:

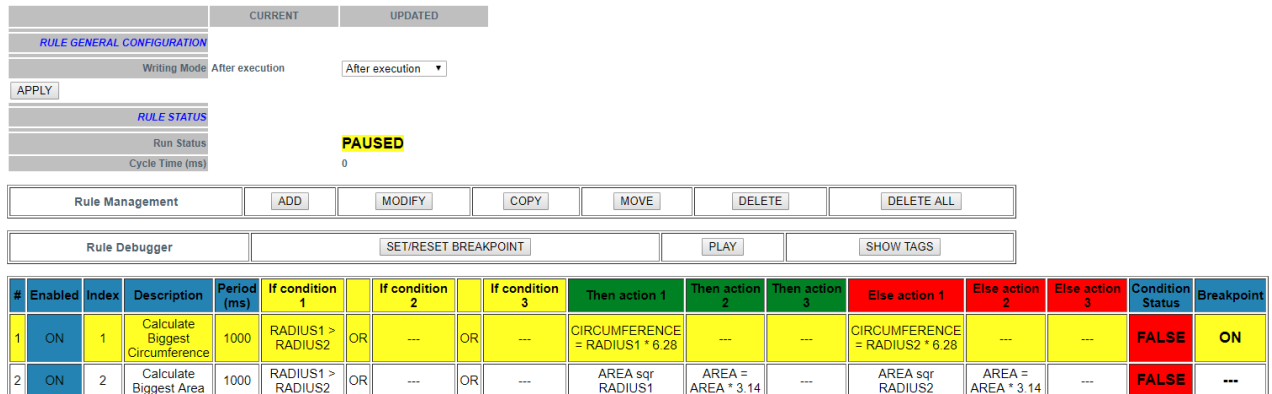
- Insert a breakpoint before the execution of a rule
- View the tag values before / after the execution of a rule

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



The screenshot shows the 'Rule Management' interface with the 'Run Status' set to 'RUNNING'. The 'Rule Debugger' section is highlighted with a red box, and a red arrow points to the 'SET/RESET BREAKPOINT' button. Below the interface is a table showing the status of two rules.

#	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	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	---
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	OR	---	AREA sqr RADIUS1	AREA = AREA * 3.14	---	AREA sqr RADIUS2	AREA = AREA * 3.14	---	FALSE	---



The screenshot shows the 'Rule Management' interface with the 'Run Status' set to 'PAUSED'. The 'Rule Debugger' section is highlighted, and the 'SET/RESET BREAKPOINT' button is visible. Below the interface is a table showing the status of two rules.

#	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	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	ON
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	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	
<b>RULE GENERAL CONFIGURATION</b>			
Writing Mode	After execution	After execution	▼
APPLY			
<b>RULE STATUS</b>			
Run Status	<b>PAUSED</b>		
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	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	ON
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	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	
<b>RULE GENERAL CONFIGURATION</b>			
Writing Mode	After execution	After execution	▼
APPLY			
<b>RULE STATUS</b>			
Run Status	<b>PAUSED</b>		
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	---	CIRCUMFERENCE = RADIUS1 * 6.28	---	---	CIRCUMFERENCE = RADIUS2 * 6.28	---	---	FALSE	---
2	ON	2	Calculate Biggest Area	1000	RADIUS1 > RADIUS2	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 the 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. It is possible to set a group "disabled".

It is possible to activate the following datalogger modes for each of the 4 groups:

<b>Field</b>	<b>Meaning</b>
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<sup>1</sup>; 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)

STOP SCAN

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

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)

NOTE: "All" means all baud rates except for 38400

All ▾

Address Mask  
(for secondary scan)

FFFFFFFFFFFFFFF

PRIMARY SCAN
SECONDARY SCAN
CREATE CONFIGURATION

READ DATA

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

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) FFFFFFFFFFFFFF

#	Baud Rate (2400)	Address (Mask=FFFFFFFFFFFFFF)
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:

ADD      DELETE      CREATE TAGS

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

Tag Prefix	Baud Rate	Address	Scan Rate (s)
MBUS1	2400	00008431614C0402	60
MBUS2	2400	00008432614C0402	60
MBUS3	2400	00008434614C0402	60
MBUS4	2400	00008435614C0402	60
MBUS5	2400	00008436614C0402	60
MBUS6	2400	00008441614C0402	60
MBUS7	2400	00008444614C0402	60
MBUS8	2400	00008446614C0402	60
MBUS9	2400	00008449614C0402	60
MBUS10	2400	00008453614C0402	60
MBUS11	2400	00008454614C0402	60
MBUS12	2400	00008458614C0402	60
MBUS13	2400	00008461614C0402	60
MBUS14	2400	00008464614C0402	60
MBUS15	2400	00008466614C0402	60
MBUS16	2400	00008470614C0402	60
MBUS17	2400	00008471614C0402	60
MBUS18	2400	20884031C514010D	60
MBUS19	2400	20884034C514010D	60
MBUS20	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.

Energy Protocols: none  
 PLC Status: running (app: mbus\_vars)  
 Router: disabled

---

ADD      DELETE      CREATE TAGS

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

Tag Prefix	Baud Rate	Address	Scan Rate (s)
MBUS1	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)*

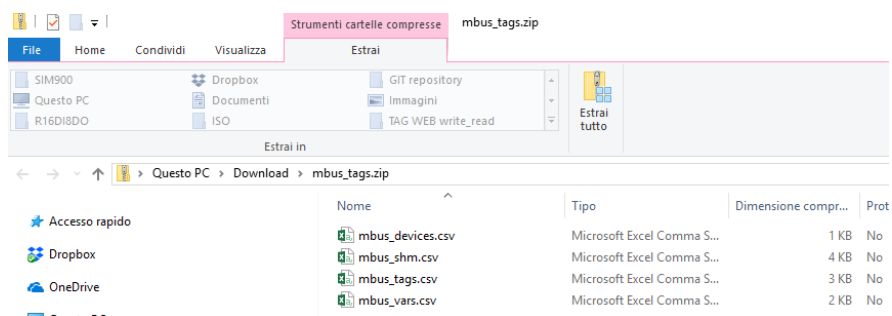
*(10 seconds elapsed)*

STOP TAGS CREATION

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



The .zip file contains 4 files:



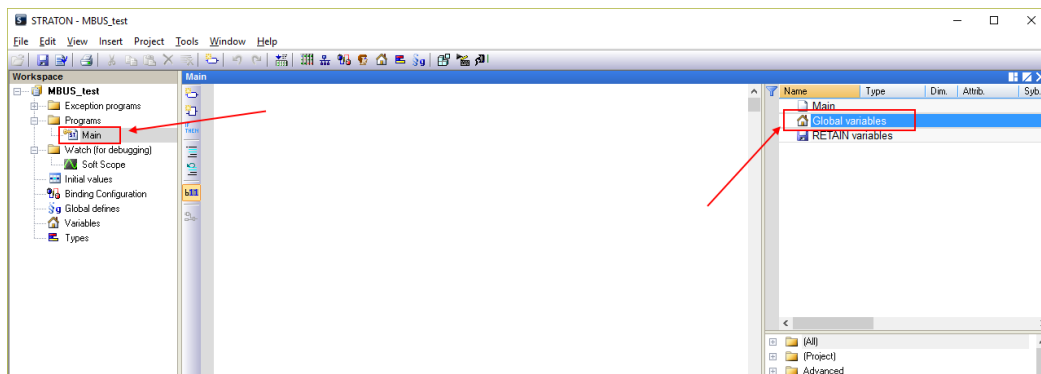
Two of these files are to be used in Straton:

mbus\_shm.csv (the shared memory configuration)

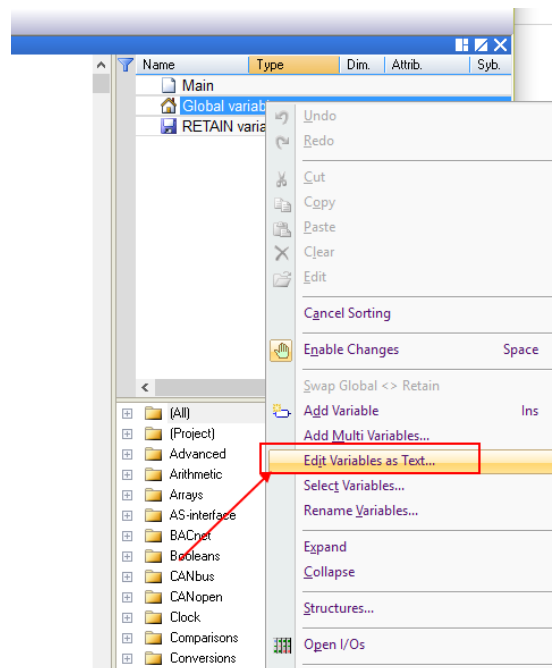
mbus\_vars.csv (the M-Bus vars)

At this point, perform the following steps:

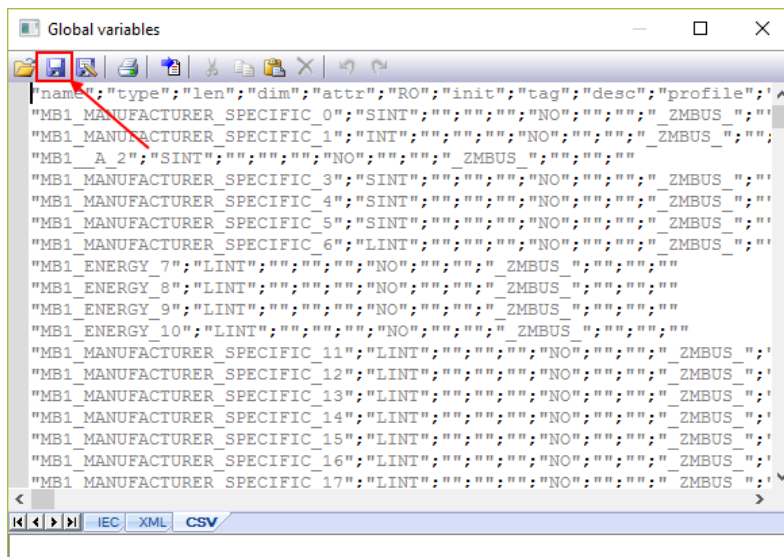
- 1) Extract the zip file to a directory.
- 2) Start Straton workbench
- 3) Select main and then Global variables:



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

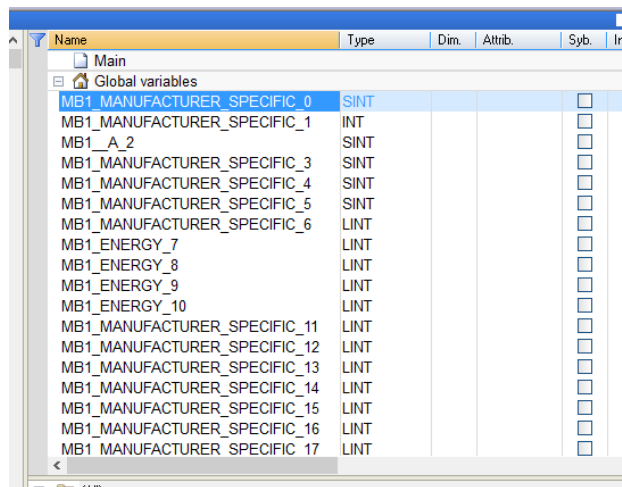


Open the “mbus\_vars.csv” file with a text editor, copy and paste the list of variables into the "Global variables" module in Straton then save the configuration with the "disk" icon:

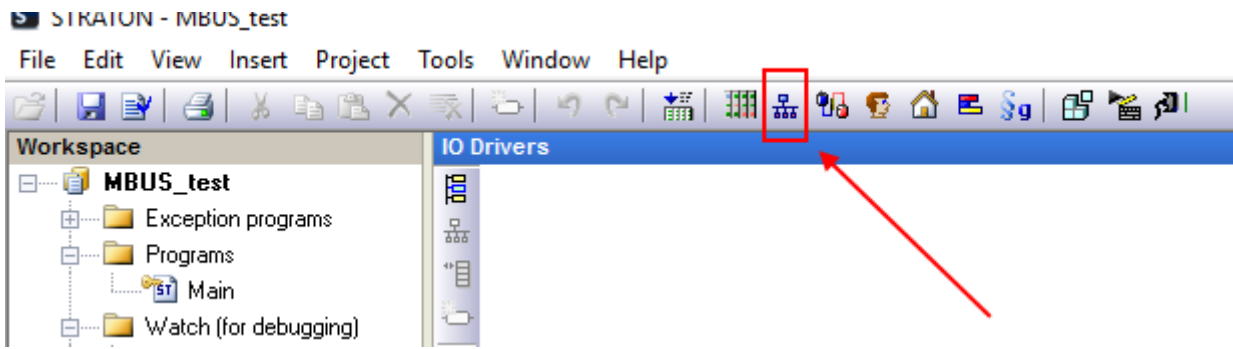


**NOTE: The first line  
 “name”;”type”;”len”;...  
 must occur only once and only on the first line.**

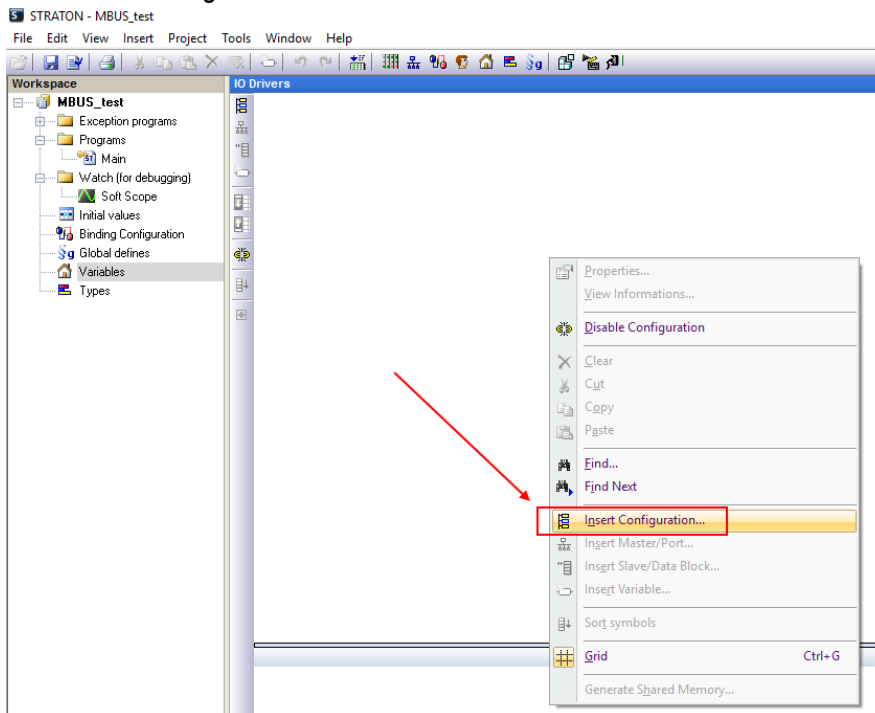
Now the variables are imported:



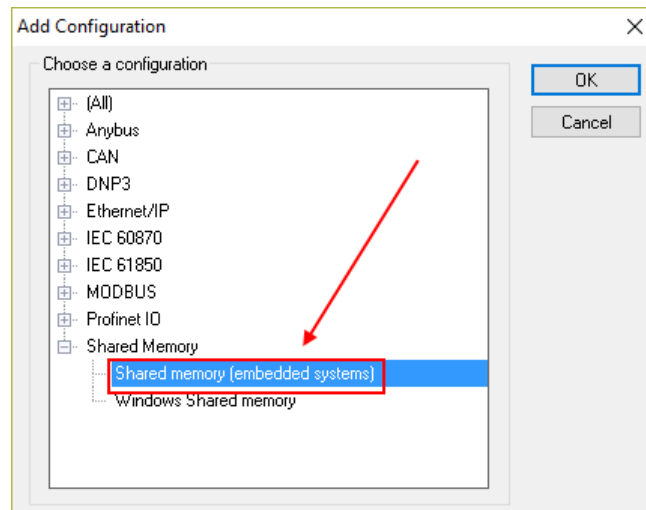
Now we need to create the shared memory used to share data from M-BUS:  
 Click on the fieldbus icon:



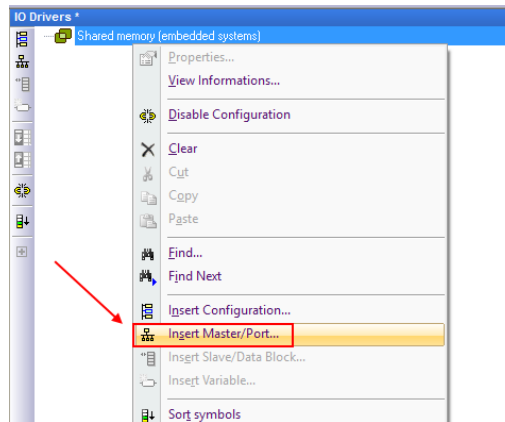
Right-click and select “Insert Configuration”:



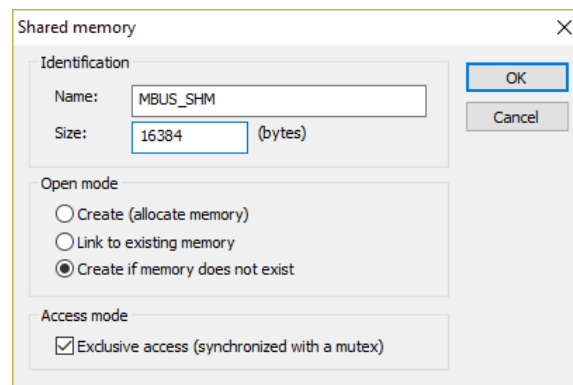
Now create the Shared Memory:



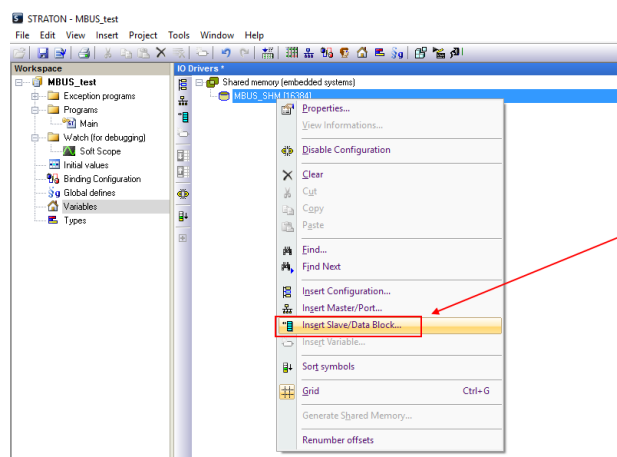
Enter a Master port:



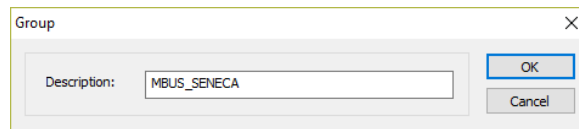
The shared memory configuration must be as shown in the figure (do not change the setting):



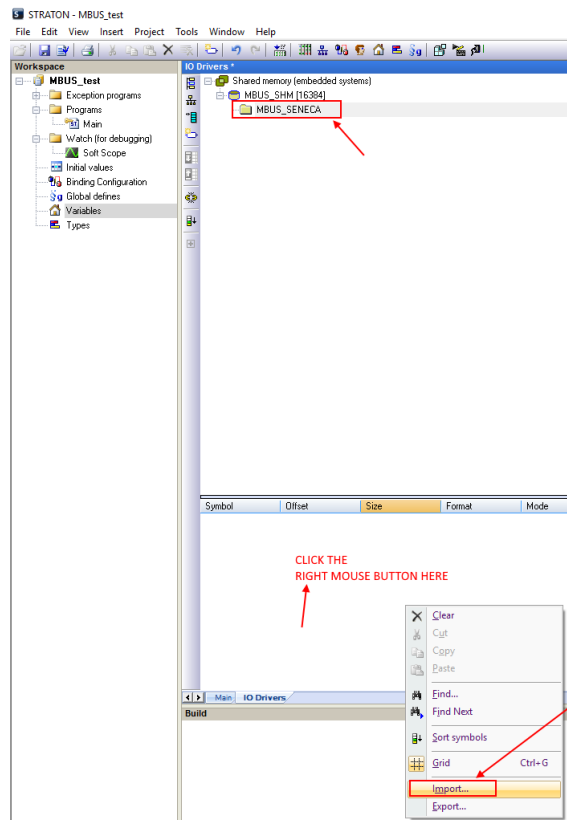
Now insert the data block:



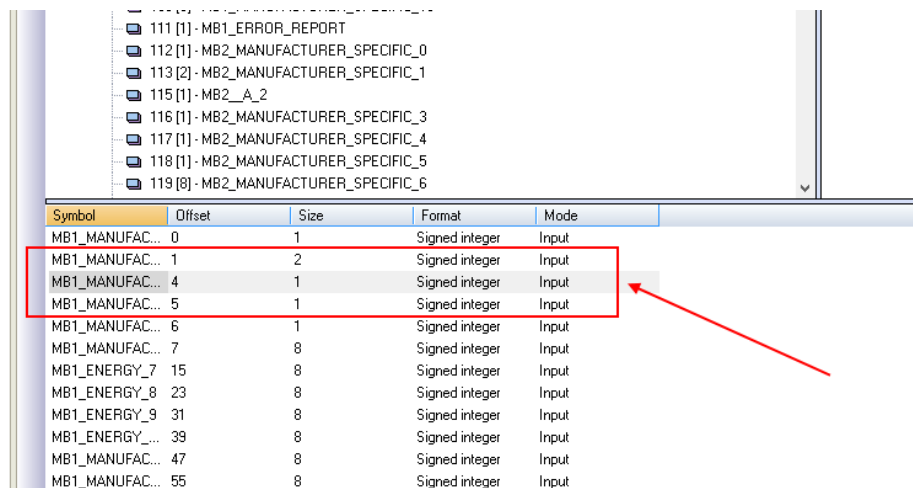
Create a Group and enter a name:



Now import the shared memory file:







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:

<b>VALUE OF THE "ERORR REPORT" TAG</b>	<b>MEANING</b>
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 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

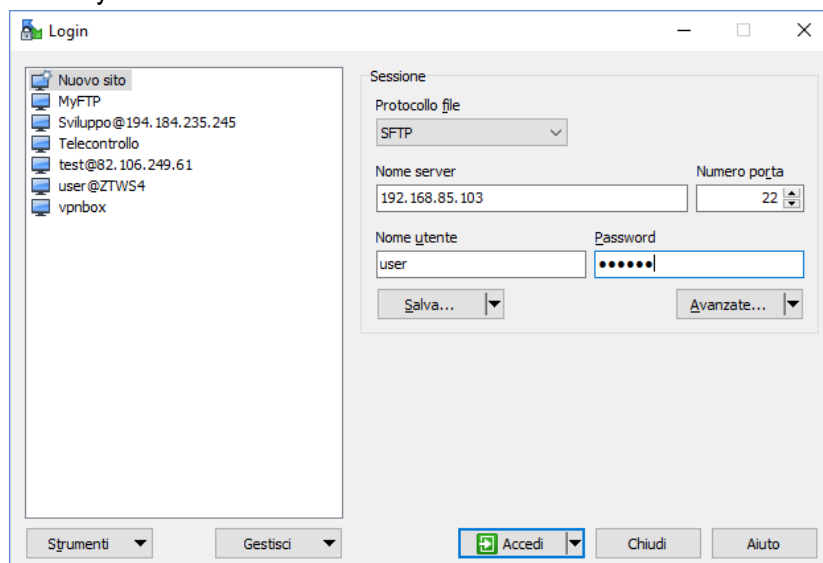
To easily access the device via FTP / SFTP, you can for example use the WINSCP program; you can download WINSCP for free from:

<http://winscp.net/eng/download.php>

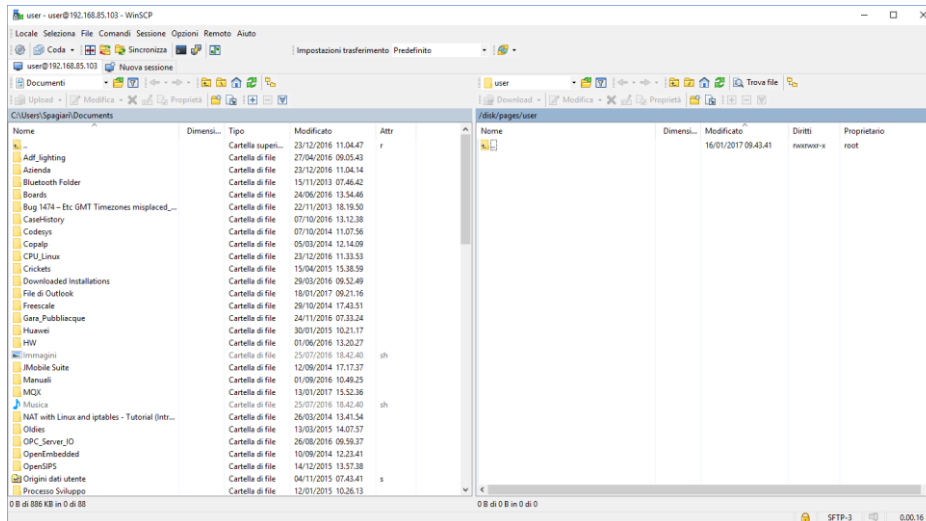
Set the connection as in the following figure (the screen shows a connection to IP address 192.168.85.103):

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.



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.

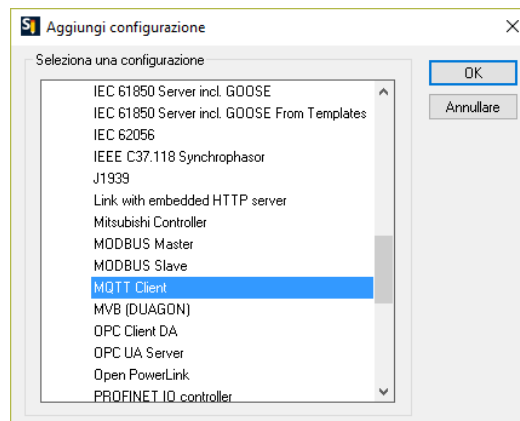


## 23. MQTT CLIENT PROTOCOL (R-PASS-S, Z-PASS2-RT-S, Z-TWS4-RT-S ONLY)

The MQTT version supported is 3.1.1

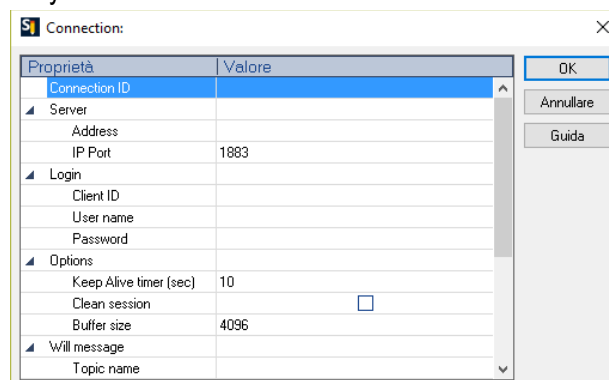
To use the MQTT protocol it is necessary to use Straton workbench 9.3 or later.

To use the MQTT client select it from the Straton Workbench Fieldbus section:



### 23.1. PARAMETERS OF THE MQTT PROTOCOL FROM THE PLC PROGRAM

MQTT setup can be done directly from the workbench:



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/eseui/mqtt_par_password`

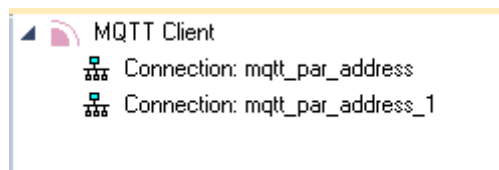
**Warning!**

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:



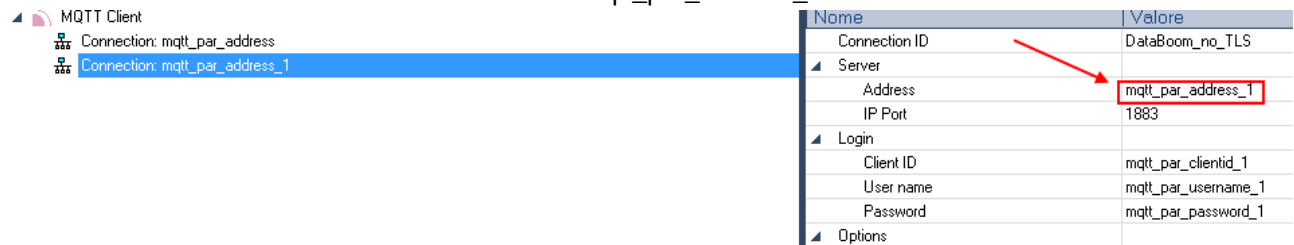
The first connection uses the Field address "mqtt\_par\_address"



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"



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
```

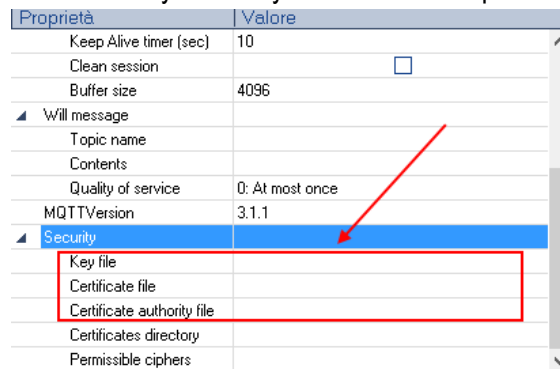
It means CONN\_TRY\_MAX = 50 and CONN\_TRY\_WAIT = 200 ms.

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:



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

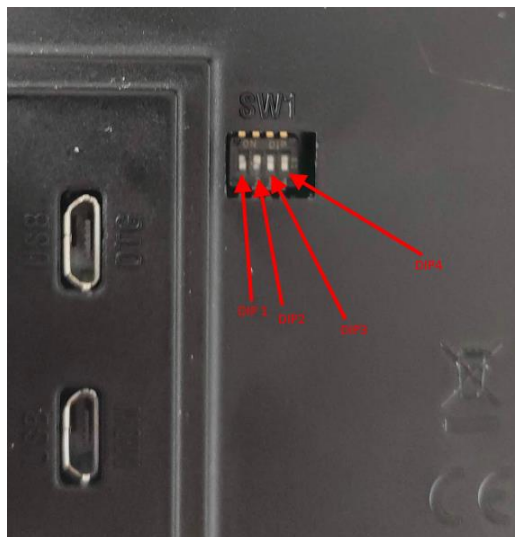
With this procedure it is possible to obtain

- 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:

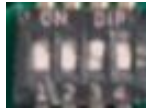


- 3) Bring the dip switches in: DIP1 = OFF, DIP2 = ON, DIP3 = ON, DIP4 = ON
- 4) Switch the device on and wait until it has completed charging
- 5) With the device switched on, bring the dips in: DIP1 = OFF, DIP2 = ON, DIP3 = OFF, DIP4 = OFF

## 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:

<b>Data Type</b>	<b>Digital I/Os</b>	<b>Indirizzo di default</b>
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:

<b>Data Type</b>	<b>Digital I/Os</b>	<b>Indirizzo di default</b>
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 (UIN16)	3 (40004)
Holding Registers	Analog Input 2 (UIN16)	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. 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.