





SENECA s.r.l.

Via Austria, 26 - 35127 - Z.I. CAMIN - PADOVA - ITALY

Tel. +39.049.8705359 - 8705408 Fax. +39.049.8706287

Web site: www.seneca.it



Sales: commerciale@seneca.it (IT), sales@seneca.it (Other)

This document is property of SENECA srl. Duplication and reprodution are forbidden, if not authorized. Contents of the present documentation refers to products and technologies described in it. All technical data contained in the document may be modified without prior notice Content of this documentation is subject to periodical revision.

To use the product safely and effectively, read carefully the following instructions before use. The product must be used only for the use for which it was designed and built. Any other use must be considered with full responsibility of the user. The installation, programmation and set-up is allowed only for authorized operators; these ones must be people physically and intellectually suitable. Set up must be performed only after a correct installation and the user must perform every operation described in the installation manual carefully. Seneca is not considered liable of failure, breakdown, accident caused for ignorance or failure to apply the indicated requirements. Seneca is not considered liable of any unauthorized changes. Seneca reserves the right to modify the device, for any commercial or construction requirements, without the obligation to promptly update the reference manuals.

MI003770_24

Date	Revision	Notes
06/09/2016	07	- Chapter "Features": new features forZ-PASS2-S-R01
		 Chapter "LEDs signalling": new par. " Z-PASS2-S-R01" New chapter "Ethernet Mode (Z-PASS2-S-R01)"
		- Chapter: "Discovering the IP address": network parameters setting
		- Chapter "Upgrading the firmware by a USB pen": revision
		- Par. "Web Configuration Pages/Administrator pages": changed
		paragraphs:
		- "Main View"
		- "Network and Services"
		- "Router Configuration"
		- "FW Upgrade"
		new paragraphs:
		- "VPN Configuration/OpenVPN Client/LED signalling (Z-PASS2-S-R01)"
		- VPN Configuration/OpenVPN Client/LED signalling (Z-PASS2-S-R01) - "VPN Configuration/VPN Box/LED signalling (Z-PASS2-S-R01)"
		- VPN Configuration/VPN Box/LED signaling (2-PASS2-3-K01) - Par. "Web Configuration Pages/User pages"
		changed paragraphs:
		- "Main View" - "Network and Services"
11/01/2017		
11/01/2017	08	- Renamed "Z-PASS2-S-1" \rightarrow ", "Z-PASS2-S-R01"
		- Chapter "Discovering the IP address": discovery working on both LAN
		and WAN interfaces
		- New chapter "Network Redundancy"
		- Paragraph "Main View" revision (also for "User Pages")
		- Paragraph "Network and Services": added "DNS Mode" parameter
		and Network Redundancy parameters; changed some default values
		(also for "User Pages")
		- Paragraph "Real Time Clock Setup": added "Central Europe" time
		zone value
		- Paragraph "VPN Configuration/OpenVPN Client": revision into "VPN
		Configuration/OpenVPN"; added packet/byte counters description
		- Paragraph "VPN Configuration/VPN Box": added packet/byte counters
		description
		- Paragraph "Mobile Network": added packet/byte counters
		description
		- Paragraph "Router Configuration": Port Mapping parameters no more
		disabled when "Use Local Addresses" is ON
		- Paragraph "Users Configuration": added "guest" user credentials
		- New paragraph "Ethernet Interfaces"
		- New paragraph "Modbus Modules"
		- New paragraph "Data Logs"
		- New paragraph "Guest Pages"
		- StratON FBs and Functions, new paragraphs: GET_ALARMS,
		PUT_ALARM, SET_ALARMS_STAT, FM_WRITE_NCRLF, TXBAPPENDFILE,
		GET_MIN_SINCE2K
o. /oo /		- Chapter Z-NET4: added note to "Remote Control Functions"
01/03/2017	09	- New paragraph "Configuration Management"
		- PLC application name shown in the web pages header
		- "Use Local Address through VPN" parameter: "ON" option always
		available
		- Paragraph "Network and Services" (Admin and User): changed default
		value for "Default Gateway" and "DNS Server" parameters; "Default
		Gateway" always in the WAN subnet, in LAN/WAN mode; "DHCP on
		LAN" disabled, in LAN/WAN mode

		 OpenVPN, Configuration File: added rules on "dev" and "log" options StratON FBs and Functions, new paragraphs: S7_DB_READ, S7_DB_WRITE
23/05/2017	10	 Chapter "Features": new features for Z-PASS2-S-IO New "LEDs signaling" sub-paragraph for IO HW revision New chapter "Remote Access Disable"
		- New chapter "Auto-APN"
		- Paragraph "Network and Services": added screen-shots for "IO"
		version; added "COM1/Mode" parameter
		- Paragraph "VPN Box": added "License Limit Reached" error reason
		- Paragraph "FW Upgrade": changed "Stop TWS Services" pop-up
		- Paragraph "Configuration Management": added "Save Debug Logs"
		feature
		- Paragraph "Mobile Network": added "APN Mode" parameter
		- New paragraph "Digital I/O Configuration"
		- Paragraph "PPP_CONNECT": changes for "Auto-APN"
		- StratON FBs and Functions, new paragraphs: PPP_CONNECT_R2,
		VPNBOX_STATUS, WDOG_KEEP_ALIVE, WDOG_SET_TMO
02/08/2017	11	- Chapter "Technical Specifications": added features for Z-PASS2-S-IO
		modem
		- Paragraph "LEDs signaling"/IO: added info about modem "STAT " LED
		- Chapter "VPN": added description of Layer 2 and Layer 3 VPN
		- Paragraph "VPN Configuration/VPN Box": changes related to L2 VPN
		and info about connected user; added L2 VPN figure
		- Deleted paragraph "Updating the StratON application by a USB pen"
		- Chapter "Upgrading the firmware": added notes about LEDs blinking
		- Paragraph "Main View" (admin): updated figure
		- Paragraph "Network and Services": added info about new Web Server
		and File Transfer parameters; updated figures
		- Paragraph "Real Time Clock Setup": updated figure
		- Paragraph "Router Configuration": changed default value for "Allow
		Access through Mobile Public IP Address" parameter
		- Paragraph "Configuration Management": added info about zip
		archive; updated figures
		- Paragraph "Mobile Network": updated figures
		- "Remote Access Disable" → "Remote Connection Disable"
06/10/2017	12	- Changed "-R02" → "-IO"
		- Chapters "Features", "Technical Specifications": note about GPS
		module and antenna
		- Chapter "Electrical Connections": added sub-paragraph for Z-PASS2-S-
		IO Digital I/Os
		- New sub-paragraph "Z-PASS2-S-IO profiles"
		- Paragraphs "Main View", "Network and Services": updated figures
		- Paragraph "Real Time Clock Setup": added figure with new time zones
		- Paragraph "VPN Box": updated first figure
		- Paragraph "Router Configuration": updated figures
		- Paragraph "Users Configuration": updated figure
		- Paragraph "FW Upgrade": updated figures
		- Paragraph "Configuration Management": added table about save
		option and archive contents; updated figure
		- New sub-paragraph "Factory reset by USB pen"
		- Paragraph "Mobile Network": added info and figure about "GPS
		Location"; updated some figures
		- Paragraph "Digital I/O Configuration": added info and figure about

		- New paragraph "FW Versions"
		- Deleted "DHCP on LAN" parameter
		- Paragraph "Network and Services" (user): updated figures
30/11/2017	13	 Paragraph "Router Configuration": parameter "Access through Mobile
50/11/201/	15	Public IP Address" changed to "Mobile Network Firewall"
		- Paragraph "Mobile Network": changes related to "Operator
		Selection" and PIN handling
		- New paragraph "DDNS Configuration"
		- Paragraphs "Main View" and "Guest pages": "RESET" button renamed
		to "RESTART"; updated figures
		- Chapter "Remote Connection Disable": added "Security Level 4 (SMS
		Service)"
		- Paragraph "Digital I/O Configuration": added "Security Level 4 (SMS
		Service)" ; updated figures
		- Paragraph "FW Versions": updated figure
		- StratON FBs, new paragraph: SERVICE_CTRL
40/04/2010		- Deleted references to Z-MODEM-3G
18/01/2018	14	- Chapter "Features": added Z-PASS2-S-IO-4G product
		- Chapter "Technical specifications": updated info about modem
		- Removed "None" value of "Security Level / Service Disable"
		parameter.
15/03/2018	15	- Removed CTS signal from COM1 port (Z-TWS4, Z-PASS2-S)
		- Added parts related to Z-TWS4-IO
30/07/2018	16	- Paragraph "Router Configuration": new "Ethernet Bandwidth
	(FW rel. SW002940_336)	Limitation" parameter; updated figures
28/09/2018	17	- New chapter "M-Bus"
	(FW rel. SW002940_340)	- New web page paragraph "Modbus TCP Client Configuration"
		- New web page paragraph "M-Bus Diagnostics"
		- New FB paragraphs MBUS_GET_DATA, MBUS_GET_INFO,
		MBUS_READ_DATA, MBUS_WRITE_RAW
10/10/2018	18	- Paragraph "M-Bus Diagnostics" reviewed
	(FW rel. SW002940_341)	
23/10/2018	19	- Paragraph "M-Bus Diagnostics" reviewed
	(FW rel. SW002940_342)	
20/03/2019	20	-Modified chapter "M-Bus Diagnostics" in "M-Bus Scan"
	(FW rel. SW002940_344)	-Added Chapter "M-Bus Configuration"
		- new function MBUS_READ_CTL
		- Deleted FB: MBUS_READ_DATA, MBUS_GET_DATA, MBUS_GET_INFO
05/04/2019	21	-Added Chapter "OPC-UA"
	(FW rel. SW00290_350)	-new FB
		UAC_CONNECT
		UAC_DISCONNECT
		UAC_READ
		UAC_WRITE
25/10/2019	22	-Added MQTT Client Protocol
	(FW rel. SW00290_360)	- OPC-UA Server:
		- added new "Security Policies":

		- Basic128Rsa15 / Sign
		- Basic128Rsa15 / Sign & Encrypt
		- Basic256Sha256 / Sign
		- Basic256Sha256 / Sign & Encrypt
		- Added certificate management in "OPC-UA Server Configuration"
		- OPC-UA Client:
		- added new "Security Policies":
		- Basic128Rsa15 / Sign
		- Basic128Rsa15 / Sign & Encrypt
		- Basic256 / Sign
		- Basic256 / Sign & Encrypt
		- Basic256Sha256 / Sign
		- Basic256Sha256 / Sign & Encrypt
		- Added new page "OPC-UA Client Configuration"
		- FB UAC_CONNECT: added new input parameters SEC_POLICY,
		SEC_MODE
		-Added new FB DSN_RESOLVE
		-Changed the "Modbus TCP-IP Client configuration" chapter with "Modbus Configuration"
		-Added The new Modbus Pass-Through mode
20/12/2019	23	-Added MQTT SSL/TLS connection retry file info
		-Fixed Chapter "Importing the M-BUS Configuration in Straton"
31/03/2020	24	-Added MOTT configuration from files (from firmware SW00204, 262)
31/03/2020	24	-Added MQTT configuration from files (from firmware SW00294_362

Table of contents

T	able	e of	conte	nts	. 6
1		Pre	limina	ry information / Informazioni preliminari	10
2		Fea	tures		11
3		Тес	hnica	specifications	12
4		Eleo	ctrical	Connections	17
	4.1	1	Z-TV	VS4, Z-TWS4-IO, Z-PASS2-S, Z-PASS2-S-R01, Z-PASS2-S-IO	17
		4.1.	.1	Z-TWS4-IO Digital I/Os	21
		4.1.	.2	Z-PASS2-S-IO Digital I/Os	21
	4.2	2	S600	D1-RTU	22
5		LED	s sign	aling	26
	5.1	1	Z-TV	VS4, Z-PASS2-S	26
	5.2	2	Z-PA	\SS2-S-R01	26
	5.3	3	Z-PA	\SS2-S-IO	28
	5.4	1	Z-TV	VS4-IO	29
	5.5	5	S600	D1-RTU	30
6		Disc	coveri	ng the IP address	31
7		FTP	/SFTP	access	33
8		Stra	atON I	PLC	34
	8.1	1	Writ	ing, downloading and running the first program	34
		8.1.	.1	Seneca libraries and templates installation	35
		8.1.	.2	Creating a project for Seneca CPUs	39
		8.1.	.3	Z-PASS2-S-IO profiles	44
		8.1.	.4	Z-TWS4-IO profile	45
	8.2	2	Enei	gy Management Protocols	46
	8.3	3	Stra	tON Redundancy	46
9		Eth	ernet	Mode (Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO)	47
1	0	v	′PN		49
	10	.1	"Sin	gle LAN" VPN	51
	10	.2	"Poi	nt-to-Point" VPN	52
1	1	Ν	letwo	rk Redundancy	53
1	2			·	

13	Re	Remote Connection Disable			
14	Αι	Auto-APN			
15	М	M-Bus (ONLY Z-TWS4-IO and Z-PASS2-S-IO)			
16	0	PC Ur	nified Architecture (OPC UA) protocol	56	
17	М	IQTT	client protocol	56	
17	7.1	MQ	IT protocol Parameters from PLC program	57	
	17.1	.1	Manage Multiple MQTT connections	58	
17	7.2	MQ	IT with SSL/TLS Connection retry configuration	58	
17	7.3	MQ	IT static and dynamic Client Certificates	59	
17	7.4	Char	nge MQTT parameters from a file	60	
18	U	pgrac	ling the firmware by USB pen	60	
19	W	eb C	onfiguration Pages	60	
19	9.1	Adm	inistrator pages	61	
	19.1	.1	Main View	62	
	19.1	.2	Network and Services	63	
	19.1	.3	Real Time Clock Setup	74	
	19.1	.4	VPN Configuration	78	
	19.1	.5	Router Configuration	95	
	19.1	.6	OPC UA Server Configuration	. 104	
	19.1	.7	Users Configuration	. 108	
	19.1	.8	FW Upgrade	. 109	
	19.1	.9	Configuration Management	. 118	
	19.1	.10	Modbus Configuration	. 121	
	19.1	.11	Mobile Network	. 122	
	19.1	.12	DDNS Configuration	. 136	
	19.1	.13	Digital I/O Configuration	. 140	
	19.1	.14	I/O View (S6001-RTU)	. 146	
	19.1	.15	FW Versions	. 149	
	19.1	.16	Ethernet Interfaces	. 151	
	19.1	.17	Modbus Modules	. 153	
	19.1	.18	M-Bus Scan	. 155	
	19.1	.19	M-Bus Configuration	. 160	
	19.1	.20	Data Logs	. 170	
19	9.2	User	pages	. 174	

	19.2	2.1	Main View	175
	19.2	2.2	Network and Services	176
	19.2	2.3	I/O View (S6001-RTU)	179
19	9.3	Gue	st pages	180
20	Se	eneca	a StratON Library	183
20	0.1	Fund	ction Blocks	184
	20.1	1	General FB behavior	184
	20.1	2	DNS_RESOLVE	184
	20.1	3	FTP_GET	185
	20.1	4	FTP_PUT	186
	20.1	5	GET_ALARMS	187
	20.1	6	GET_SMS	188
	20.1	7	LINUX_SHELL	189
	20.1	8	LINUX_SH_ASYNC	189
	20.1	.9	MBUS_WRITE_RAW	190
	20.1	10	MODEM_CTRL	191
	20.1	11	MODEM_ONOFF	192
	20.1	12	MODEM_RESET	192
	20.1	13	PPP_CONNECT	193
	20.1	14	PPP_CONNECT_R2	194
	20.1	15	PPP_STATUS	196
	20.1	16	PUT_ALARM	197
	20.1	17	S7_DB_READ	198
	20.1	18	S7_DB_WRITE	199
	20.1	19	SEND_MAIL	200
	20.1	20	SEND_SMS	201
	20.1	21	SERVICE_CTRL	202
	20.1	22	SET_ALARMS_STAT	203
	20.1	23	TIME_SYNC	204
	20.1	24	UAC_CONNECT	204
	20.1	25	UAC_DISCONNECT	205
	20.1	26	UAC_READ	206
	20.1	27	UAC_WRITE	206
	20.1	.28	VPNBOX_STATUS	207

20.2 Fu	nctions
20.2.1	FM_WRITE_NCRLF
20.2.2	TXBAPPENDFILE
20.2.3	GET_MIN_SINCE2K
20.2.4	MBUS_READ_CTL
20.2.5	WDOG_KEEP_ALIVE
20.2.6	WDOG_SET_TMO
21 Z-NE	T4
22 Acce	ss to Straton variables
22.1 Sh	ared Memory 212
22.2 C	program example
22.3 CG	il
22.3.1	CGI "readVariable" 216
22.3.2	CGI "writeVariable"
23 Gloss	ary

1 Preliminary information / Informazioni preliminari

WARNING!

IN NO EVENT WILL SENECA OR ITS SUPPLIERS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF CAUSE (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE Z-TWS4/Z-PASS2-S/S6001-RTU, EVEN IF SENECA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SENECA, ITS SUBSIDIARIES AND AFFILIATES COMPANY OR GROUP OF DISTRIBUTORS AND SENECA RETAILERS NOT WARRANT THAT THE FUNCTIONS WILL MEET YOUR EXPECTATIONS, AND THAT Z-TWS4/Z-PASS2-S/S6001-RTU, ITS FIRMWARE AND SOFTWARE WILL BE FREE FROM ERRORS OR IT OPERATES UNINTERRUPTED.

SENECA SRL CAN MODIFY THE CONTENTS OF THIS MANUAL IN ANY TIME WITHOUT NOTICE TO CORRECT, EXTEND OR INTEGRATING FUNCTION AND CHARACTERISTICS OF THE PRODUCT.

ATTENZIONE!

IN NESSUN CASO SENECA O I SUOI FORNITORI SARANNO RITENUTI RESPONSABILI PER EVENTUALI PERDITE DI DATI ENTRATE O PROFITTI, O PER CAUSE INDIRETTE, CONSEQUENZIALI O INCIDENTALI, PER CAUSE (COMPRESA LA NEGLIGENZA), DERIVANTI O COLLEGATE ALL' USO O ALL' INCAPACITÀ DI USARE Z-TWS4/Z-PASS2-S/S6001-RTU, ANCHE SE SENECA È STATA AVVISATA DELLA POSSIBILITÀ DI TALI DANNI.

SENECA, LE SUSSIDIARIE O AFFILIATE O SOCIETÀ DEL GRUPPO O DISTRIBUTORI E RIVENDITORI SENECA NON GARANTISCONO CHE LE FUNZIONI SODDISFERANNO FEDELMENTE LE ASPETTATIVE E CHE Z-TWS4/Z-PASS2-S/S6001-RTU, IL SUO FIRMWARE E SOFTWARE SIA ESENTE DA ERRORI O CHE FUNZIONI ININTERROTTAMENTE.

SENECA SRL PUO' MODIFICARE IL CONTENUTO DI QUESTO MANUALE IN QUALUNQUE MOMENTO E SENZA PREAVVISO AL FINE DI CORREGGERE, ESTENDERE O INTEGRARE FUNZIONALITA' E CARATTERISTICHE DEL PRODOTTO.

2 Features

Z-TWS4, Z-PASS2-S and S6001-RTU are programmable, communication oriented PLCs.

The Z-TWS4/Z-PASS2-S/S6001-RTU StratON[™] PLC is programmable according to the IEC 61131-3 standard, by means of the StratON development environment.

All three devices provide the following features:

- OpenVPN connectivity
- full configuration by means of an integrated web site
- FW upgrade, that can be performed locally, by means of a USB pen, or remotely, through the web site

Z-PASS2-S and S6001-RTU integrate a 3G HSPA modem.

S6001-RTU is equipped with a rich set of analog and digital inputs/outputs.

Z-PASS2-S, S6001-RTU and Z-TWS4 (when connected to an external modem) can be used as a Router, routing packets between the WAN (Mobile Network) and the LAN (Ethernet).

All three devices are based on a 32bits ARM9 processor, equipped with the Linux operating system (Linux kernel 2.6.28).

Z-PASS2-S-R01 is a new version of the Z-PASS2-S product, providing the following new features:

- the two available Ethernet ports can be configured as two fully separated network interfaces ("LAN" and "WAN"), whereas in the older versions they could only work as ports of an Ethernet switch; the user can choose if the two ports shall work in "LAN/WAN" mode or "Switch" mode, by means of a new configuration parameter ("Ethernet Mode");
- there are 4 more LEDs, providing information about the "Ethernet Mode" and the VPN functionalities.

Z-TWS4-IO is a new version of the Z-TWS4 product, providing the following new features:

- one digital input which can be used to disable remote connection to the device
- one digital output which goes HIGH when the device is remotely accessed
- one digital output which can also be used as a remote command
- one configurable digital input/output, which can also be used as a local alarm
- a new set of LEDs
- COM1 RS232/RS485 mode set by software (configuration parameter), instead of HW DIP switch

Z-PASS2-S-IO is a new version of the Z-PASS2-S product, providing the following new features:

- one digital input which can be used to disable remote connection to the device
- one digital output which goes HIGH when the device is remotely accessed
- one digital input which can also be used as a local alarm
- one digital output which can also be used as a remote command
- two configurable digital inputs/outputs
- a new set of LEDs
- COM1 RS232/RS485 mode set by software (configuration parameter), instead of HW DIP switch
- a new penta-band 3G+ modem, which also features a GPS module

Z-PASS2-S-IO-4G is a new version of the Z-PASS2-S-IO product, providing a new 4G LTE Cat.1 modem, instead of the 3G+ modem.

NOTE 1:

in the following chapters, the term "Device" will be used when describing features or characteristics that are available in all three products.

NOTE 2:

in the following chapters, any reference to 3G modem/connection applies also to 4G modem/connection.

3 Technical specifications

OMMUNICATION PORTS (Z-TWS4/Z-PASS2-S)
Baud rate: maximum 115 Kbps, minimum 110 bps
COM 4 (screw terminals 4-5-6)
COM 2 (screw terminals 1-2-3 or IDC10 connector)
COM 1 (removable 4 pin connector, as an alternative to RS232)
Baud rate: maximum 115 Kbps, minimum 110 bps
COM 1 (removable 4 pin connector, as an alternative to RS485)
CAN bus port 2.0A and 2.0B
Baud rate: maximum 500 Kbps, minimum 20 Kbps
(screw terminals 10-11-12 or IDC10 connector)
available only in Z-TWS4
Ethernet 10/100 Mbps
Two RJ45 connectors on front-panel
Maximum connection length 100 m
In Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO, the two ports can work either as
LAN/WAN ports (ETH1=LAN, ETH2=WAN) or ports of an Ethernet switch.
In Z-TWS4/Z-PASS2-S, the two ports can work only as ports of an Ethernet
<u>switch.</u>
Plug-in: USB type A
Plug-in: micro USB (available only in Z-TWS4)
COMMUNICATION PORTS (S6001-RTU)
Baud rate: maximum 115 Kbps, minimum 110 bps
COM 4 (screw terminals 54-55-56)
COM 2 (screw terminals 57-58-59)

RS 232	Baud rate: maximum 115 Kbps, minimum 110 bps
	COM 1 (DB9 male connector)
Optional Bus for future extensions	screw terminals 60-61-62
Ethernet	Ethernet 10/100 Mbps
	RJ45 connector
	Maximum connection length 100 m
USB #1 HOST	Plug-in: USB type A
	CPU AND MEMORY
Microprocessor	ARM 9, 32 bits, 400 MHz
Memories	64 Mbytes of RAM
	1 Gbyte of FLASH
	8 Kbytes of FeRAM, split in 2 partitions (4 Kbytes each) for redundancy
Slot for external memory	Micro SD card: max 32 Gbytes
	I/O CPU (S6001-RTU)
Microprocessor	8 bits, 24 MHz
	3G+ MODEM (Z-PASS2-S/S6001-RTU)
HSPA Modem	14.4 Mbps in downlink, 5.76 Mbps in uplink
Slot for SIM card	Mini SIM with push-push connector
	3G+ MODEM (Z-PASS2-S-IO)
Speed	HSPA+: max 14.4 Mbps DL, max 5.76 Mbps UL
	UMTS: max 384 Kbps (DL), max 384 Kbps (UL)
	EDGE: max 236.8 Kbps (DL), max 236.8 Kbps (UL)
	GPRS: max 85.6 Kbps (DL), max 85.6 Kbps (UL)
GNSS	GPS/GLONASS
	16 GPS channels
	14 GLONASS channels Accuracy <1.5m CEP-50 @ Open Sky
Approvals	RoHS Compliant, CE/GCF/Vodafone (Europe), DoC (Russia), FCC/PTCRB/AT&T
	(North America), RCM (Australia), ICASA (South Africa), SRRC/NAL/OFCA
	(China), JATE & TELEC (Japan), NCC (Taiwan), KC/SKT (Korea), IC/Rogers
	(Canada), Anatel (Brazil), NBTC (Thailand)
Slot for mini SIM	Mini SIM with push-push connector

	4G (LTE Cat. 1) MODEM (Z-PASS2-S-IO-4G)
Speed	LTE FDD: max 10 Mbps (DL), max 5Mbps (UL)
	LTE TDD: max 8.96 Mbps (DL), max 3.1 Mbps (UL)
	DC-HSPA+: max 42Mbps (DL), max 5.76 Mbps (UL)
	UMTS: max 384 Kbps (DL), max 384 Kbps (UL)
	EDGE: max 296 Kbps (DL), max 236.8 Kbps (UL)
	GPRS: max 107 Kbps (DL), max 85.6 Kbps (UL)
GNSS	GPS/GLONASS/BeiDou/Galileo/QZSS
Approvals	RoHS Compliant, CE/GCF/Vodafone (Europe), FCC/PTCRB/AT&T/Verizon*
	(North America), RCM/Telstra (Australia), JATE/TELEC/DOCOMO* (Japan), NCC
	(Taiwan), KC/SKT/KT*/LGU+* (Korea), IC/Rogers (Canada), Anatel (Brazil),
	CCC/SRRC/NAL (China)
	*= Under Development
Slot for mini SIM	Mini SIM with push-push connector
	POWER SUPPLY (Z-TWS4/Z-PASS2-S)
Power supply	1140 Vdc or 1928 Vac @ 5060 Hz
Consumption	Typical 4 W @ 24 Vdc; Max 6 W
	POWER SUPPLY (S6001-RTU)
Power supply	24 Vac/dc ± 15% @ 50/60Hz
Consumption	10 VA max , 6 VA typical
	ENVIRONMENTAL CONDITIONS (Z-TWS4/Z-PASS2-S)
Temperature	-20+55 °C
Humidity	3090 % @ 40 °C not condensing
Storage temperature	-20+85 °C
Protection degree	IP20
	ENVIRONMENTAL CONDITIONS (S6001-RTU)
Temperature	-10+65 °C
Humidity	1090 % not condensing
Storage temperature	-40+85 °C
Protection degree	IP20
	CONNECTIONS (Z-TWS4/Z-PASS2-S)
Connections	Removable 3 way screw terminals, 5.08 pitch

	Rear IDC10 connector for DIN 46277 rail
	Removable 4 pin connector
	Two RJ45 connectors
	Type A USB connector and micro USB connector (only in Z-TWS4)
	Plug in: micro SD card
	Two SMA antenna connectors: - for Main and Diversity antennas (only in Z-PASS2-S, Z-PASS2-S-R01) - for 3G and GPS antennas (only in Z-PASS2-S-IO)
	CONNECTIONS (S6001-RTU)
Connections	Removable screw terminals
	DB9 male connector
	RJ45 connector
	Type A USB connector
	Plug in: micro SD card
	Two SMA antenna connectors, for Main and Diversity antennas
	BOX / DIMENSIONS (Z-TWS4/Z-PASS2-S)
Dimensions	Z-TWS4: L: 100 mm; H: 112 mm; W: 35 mm
	Z-PASS2-S: L: 100 mm; H: 112 mm; W: 53 mm
Case	Nylon 6 with 30% fiberglass field, self-extinguishing class V0, black color
	WEIGHT / DIMENSIONS (S6001-RTU)
Dimensions	190 mm x 160 mm x 105 mm
Weight	600 g
	INPUTS / OUTPUTS (Z-TWS4-IO)
Digital Inputs	Max. number of channels: 2
	Voltage: OFF<4V ON>8V; Max. Current (Vout+): 20mA Current absorbed: 3mA at 12VC; 6mA at 24VC
Digital Outputs	Max. number of channels: 3
	Voltage (+Vext): 10 – 24VC Max. current delivered: 400mA
	INPUTS / OUTPUTS (Z-PASS2-S-IO)
Digital Inputs	Max. number of channels: 4
	Voltage: OFF<4V ON>8V; Max. Current (Vout+): 20mA Current absorbed: 3mA at 12VC; 6mA at 24VC

Digital Outputs	Max. number of channels: 4
	Voltage (+Vext): 10 – 24VC
	Max. current delivered: 400mA
	INPUTS / OUTPUTS (S6001-RTU) ¹
Analog inputs	4, current, 020 mA
	resolution: 12 bit
	accuracy: += 0.3% of full scale
	input impedance: 50 Ω
Analog outputs	1, current, 020 mA
	1, voltage, 010 Vdc
	resolution: 12 bit
	accuracy: += 0.3% of full scale
	output load: current: <= 500 Ω , voltage: >= 1 k Ω
Digital inputs	15, PNP, with optoisolation
	ON current > 4 mA, OFF current < 3 mA
Digital outputs	8, SPDT relays
	max peak current: 3 A
	operating current: 2 A
	operating voltage: 250 Vac
	minimum load: 0.5 W
	isolation: 3 kV
Liquid level control inputs	conductive liquid level switch, 2 channels
	adjustable sensitivity

The following table shows which frequency bands are supported by the modem available in Z-PASS2-S, Z-PASS2-S-R01, S6001-RTU, Z-PASS2-S-IO and Z-PASS2-S-IO-4G products.

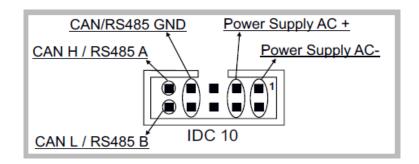
Standard	Frequency/Feature	Z-PASS2-S, Z-PASS2-S- R01, S001-RTU	Z-PASS2-S-IO	Z-PASS2-S-IO-4G
	GSM 850 MHz	ОК	ОК	
CCM	EGSM 900 MHz	ОК	ОК	OK
GSM	DCS 1800 MHz	ОК	ОК	OK
	PCS 1900 MHz	ОК	ОК	
	WCDMA 800 MHz		ОК	
	WCDMA 850 MHz		ОК	OK
WCDMA	WCDMA 900 MHz	ОК	ОК	OK
	WCDMA 1900 MHz		ОК	
	WCDMA 2100 MHz	ОК	ОК	OK
	LTE 800 DD			OK
	LTE 850			OK
LTE	LTE 900			ОК
LIE	LTE 1800			OK
	LTE 2100			OK
	LTE 2600			OK
	HSDPA	ОК	ОК	
HSPA	HSUPA	ОК	ОК	
пзра	HSPA+		ОК	
	DC-HSPA+			OK
DRX	Receiver Diversity	ОК		

¹ For more detailed information about S6001-RTU I/Os, see S6001-RTU Installation Manual.

4 Electrical Connections

4.1 Z-TWS4, Z-TWS4-IO, Z-PASS2-S, Z-PASS2-S-R01, Z-PASS2-S-IO

Power Supply and Modbus interface are available by using the bus for the Seneca DIN rail, by the rear IDC10 connector or by <u>Z-PC-DINAL1-35 accessory for Z-TWS4, Z-PC-DINAL2-52.5-17 for Z-PASS2-S</u>. The following picture shows the meaning of the IDC10 connector pins.



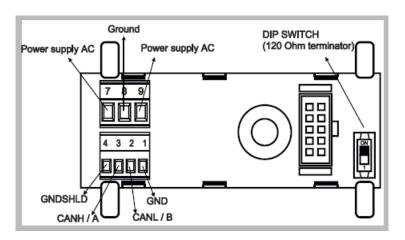
Power supply is available only from the rear connector for Z-TWS4, while:

Z-TWS4-IO can be powered also through 17-18 screw terminals;

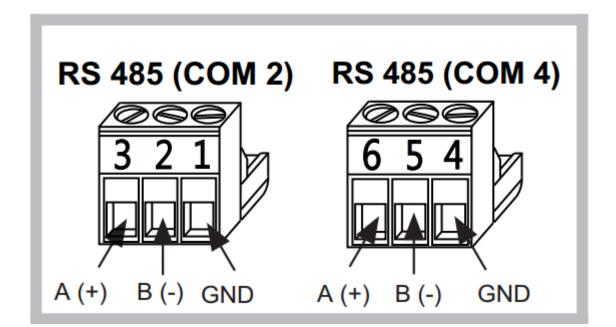
Z-PASS2-S/ZPASS2-S-R01/ZPASS2-S-IO can be powered also through 14-15 screw terminals.

If **Z-PC-DINAL1-35** or **Z-PC-DINAL2-52.5-17** accessory is used, the power supply signals and communication signals may be provided by the terminals block into the DIN rail support. In the following figure the meaning and the position of the terminal blocks are shown. The DIP-switch that sets the 120 Ω terminator is used only for CAN communication (<u>Z-TWS4 only</u>).

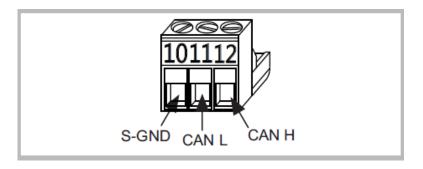
GNDSHLD: shield to protect the connection cables against interference (recommended).



The Device has two RS 485 serial ports for Modbus communication: COM 4 and COM 2. The RS485 connection for COM 2 can be set up by means of the corresponding screw terminals or by the IDC10 connector. On Z-TWS4, to select RS 485 on IDC10 connector, put the SW1 DIP-switch on OFF position; on Z-PASS2-S, no operation is needed.



The Z-TWS4 has a CAN port available on screw terminals 10-11-12. As an alternative, the connection can be set up on the IDC10 connector. To select CAN port on IDC10 connector, put the SW1 DIP-switch on ON position.

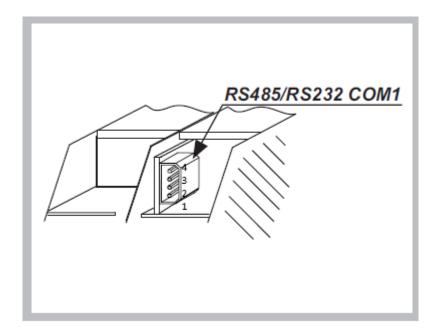


Through a removable 4 pin connector, the Device provides a serial RS232 port or, as an alternative, a third RS485 port. In order to select the RS232 port on the removable 4 pin connector, put the SW2 DIP-switch on ON position; to select the RS485 port on the removable 4 pin connector, put the SW2 DIP-switch on OFF position².

In Z-TWS4-IO/Z-PASS2-S-IO, the mode (RS485/RS232) of this port is set as a parameter in software configuration.

The cable length for the RS232 interface must be less than 3 meters.

² While in Z-TWS4 the SW2 DIP-switch position can be changed by the user, in Z-PASS2-S the DIP-switch is internal and its position is permanently set in the factory.

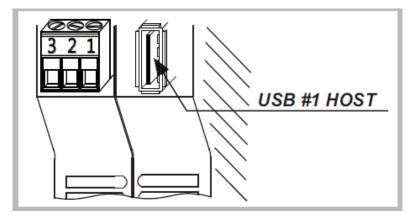


The connector pin-out is given in the following table:

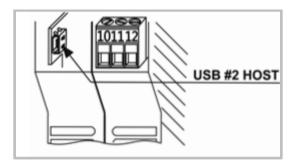
Pin	RS232	RS485
1 (bottom)	-	-
2	Тх	В
3	Rx	А
4 (top)	GND	GND

The Device has a USB HOST type A connector, that can be used as an additional serial port (using a Seneca S117P1, for example) or to connect an external USB memory; this is used for FW upgrade (see chapter 18).

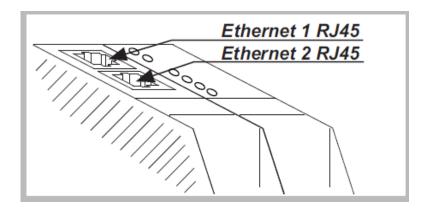
Please note that, on this USB port, the "hotplug" feature is not available; so, after plugging the USB device, it is necessary to power off/on the Z-TWS4/Z-PASS2-S to let it detect the USB device.



The Z-TWS4 also has a second USB HOST connector, with micro-USB plug-in, that can be used to connect a USB device by means of a "Micro USB to USB" adapter; this port is no more available in Z-TWS4-IO.

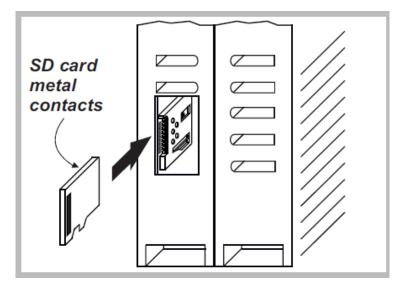


The Device has two Ethernet ports with RJ45 connectors on the front panel. <u>The two ports are internally connected in</u> <u>HUB/SWITCH mode. The two ports have the same MAC Address.</u>

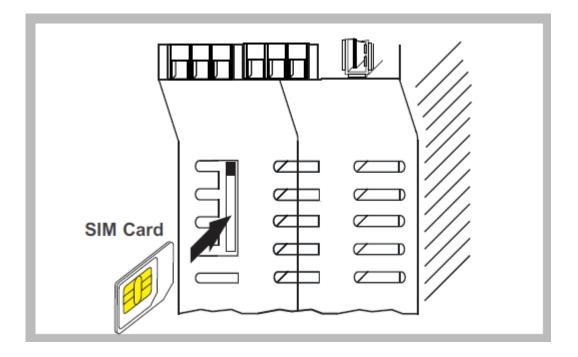


The Device has a plug-in connector for micro SD card placed in the side part of the case. To insert the SD card into the connector, be sure that the SD card is oriented with metal contacts facing towards left (with reference to the figure).

The SD card can be of any class.

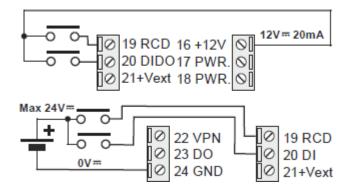


The Z-PASS2-S has a slot for SIM card, placed on the side of the case. Before pushing the SIM card into this slot, please be sure that the SIM card golden contacts are facing towards right (please see the figure below).

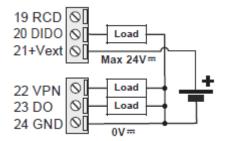


4.1.1 Z-TWS4-IO Digital I/Os

In Z-TWS4-IO, the electrical connections for the Digital Inputs shall be arranged as in the following figures.

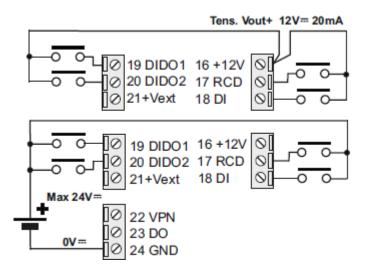


The electrical connections for the Digital Outputs shall be arranged as in the following figure.

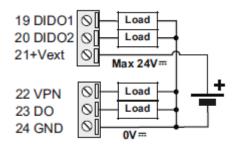


4.1.2 Z-PASS2-S-IO Digital I/Os

In Z-PASS2-S-IO, the electrical connections for the Digital Inputs shall be arranged as in the following figures.

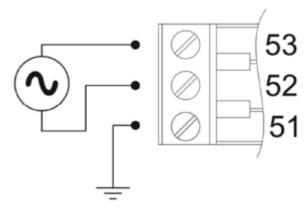


The electrical connections for the Digital Outputs shall be arranged as in the following figure.



4.2 S6001-RTU

Power supply must be connected to screw terminals 52 and 53. The supply voltage must be 24 \pm 15 % Vac/dc (any polarity).



<u>Upper limits must not be exceeded to avoid serious damage to the device</u>. It is necessary to protect the power supply source against any failure of the device by means of an appropriately sized fuse.

S6001-RTU has two RS485 serial ports (COM2 and COM4) available on removable screw terminals, as specified in the following table.

Signal	COM2	COM4
GND	57	54
В	58	55
А	59	56

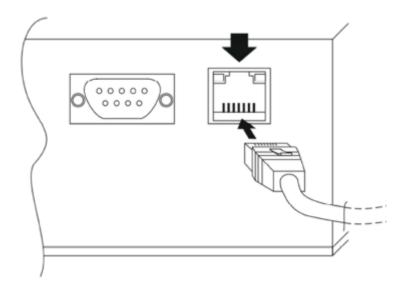
An RS232 serial port with full handshaking signals is available on DB9 male connector on the left side of S6001-RTU. Use the CS-DB9F-DB9F cable³ to connect RS232 devices. Signals on DB9 connector are listed in the table below.

Pin	Name	Description	IN/OUT
1	DCD	Data carrier detect	In
2	RXD	Receive data	In
3	TXD	Transmit data	Out
4	DTR	Data terminal ready	Out
5	SG	Signal ground	
6	DSR	Data set ready	In
7	RTS	Request to send	Out
8	CTS	Clear to send	In
9	RI	Ring indicator	In

An optional communication bus is available on removable screw terminals 60,61,62, for future extensions.

S6001-RTU has 1 USB port which is an USB HOST with connector type "A", suitable to connect, for example, a mass storage (e.g.: a USB pen) with maximum consumption of 300 mA @ 5 Vdc.

An Ethernet port is available on the left side of S6001-RTU on an RJ45 connector.



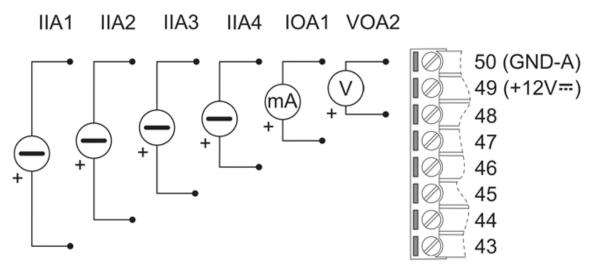
An SD card slot is available, near the optional bus screw terminals; SD cards with storage capacity up to 32 GB can be used.

A SIM card slot, with a push-push connector, is available; 3V mini SIM cards can be used.

Two SMA antenna connectors are available, for Main and Diversity antennas.

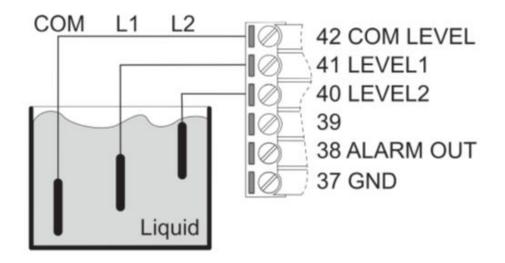
³ The CS-DB9F-DB9F cable is supplied on request.

Analog inputs and outputs are available on screw terminals 43-50, as shown in the following figure and table.



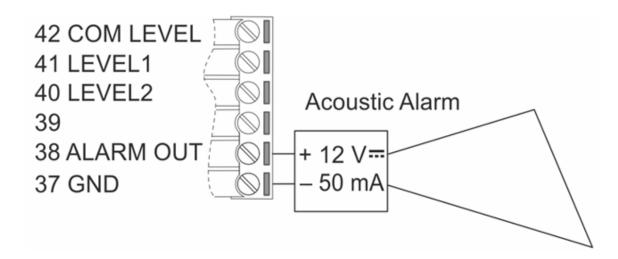
4 analog current inputs (0-20 mA)	Four active sensors are available from 43 to 46 screw terminals. Screw terminal 49 is a supply voltage (+12 Vdc) for passive current sensor.
1 analog current output (0-20 mA)	Available between 47 and 50 screw terminals.
1 analog voltage output (0-10 Vdc)	Available between 48 and 50 screw terminals.

The Liquid Level Inputs are available on screw terminals 40-42, as shown in the following figure.

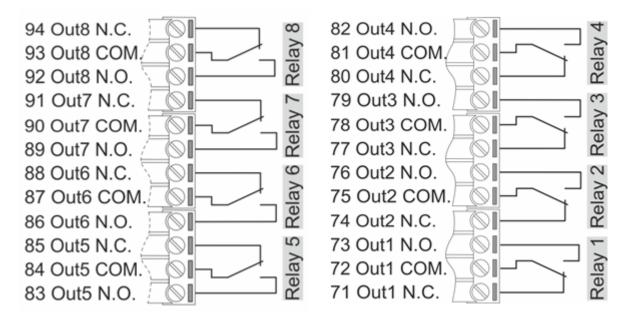


The analog level signals from screw terminals 40, 41, 42 can be used to control the level of liquid in a tank.

The supply voltage (12 Vdc @ 50mA) from screw terminals 38 and 37 can be used to connect, for example, an acoustic alarm. Screw terminal 39 must not be connected.

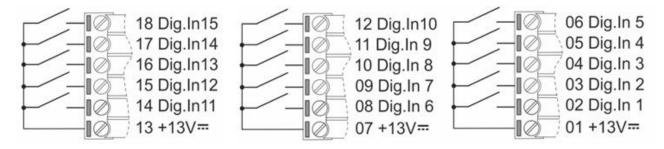


The 8 digital outputs (relays) are available on screw terminals 71-94, as shown in the following figure.



Eight SPDT relays are available to control, for example, external pumps. The operating voltage is 250 Vdc @ 2 A.

The 15 digital inputs are available on screw terminals 1-18, as shown in the following figure.



All digital inputs are PNP type with optoisolation.

5 LEDs signaling

5.1 Z-TWS4, Z-PASS2-S

LED	Status	Meaning
PWR Green	ON	The module is powered on
RUN Red	Blinking	The module is ready for use
LINK1 Yellow	ON	Ethernet 1 connection detected
	OFF	Ethernet 1 connection absent
ACT1 Green	Blinking	There is data activity (Ethernet 1)
	OFF	There is no data activity (Ethernet 1)
LINK2 Yellow	ON	Ethernet 2 connection detected
	OFF	Ethernet 2 connection absent
ACT2 Green	Blinking	There is data activity (Ethernet 2)
	OFF	There is no data activity (Ethernet 2)
RX1-2-4 Red	Blinking	Data reception (COM 1-2-4)
	ON	Check the connection (COM 1-2-4)
	OFF	No data reception (COM 1-2-4)
TX1-2-4 Red	Blinking	Data transmission (COM 1-2-4)
	ON	Check the connection (COM 1-2-4)
	OFF	No data transmission (COM 1-2-4)
3G PWR Green (Z-PASS2-S only)	ON	The 3G Modem is powered on
STAT Yellow	ON	Not registered on GSM network
(Z-PASS2-S only)	Slow Blinking	Registered on GSM network
	Fast Blinking	Mobile Network connection active

5.2 Z-PASS2-S-R01

LED	Status	Meaning
PWR Green	ON	The module is powered on
RUN Red	Blinking	The module is ready for use
LAN/WAN	ON	The Ethernet ports are working in "LAN/WAN" mode

witch" mode erly y is enabled but no client is connected or enabled but the Device is not configured
erly y is enabled but no client is connected or
erly y is enabled but no client is connected or
y is enabled but no client is connected or
-
-
enabled but the Device is not configured
orking properly
t working properly

Ethernet Connector LEDS

LED	Status	Meaning
ETH1-2 Green	ON	Ethernet 1-2 connection detected
	OFF	Ethernet 1-2 connection absent
ETH1-2 Yellow	Blinking	There is data activity (Ethernet 1-2)
	OFF	There is no data activity (Ethernet 1-2)

5.3 Z-PASS2-S-IO

LED	Status	Meaning
PWR Green	ON	The module is powered on
RUN Green	Blinking	The module is ready for use
DIDO1 Green	ON	Configurable Digital Input/Output 1 state is HIGH
	OFF	Configurable Digital Input/Output 1 state is LOW
DIDO2 Green	ON	Configurable Digital Input/Output 2 state is HIGH
	OFF	Configurable Digital Input/Output 2 state is LOW
DI Green	ON	Digital Input state is HIGH
	OFF	Digital Input state is LOW
DO Green	ON	Digital Output state is HIGH
	OFF	Digital Output state is LOW
RCD Green	ON	Remote Connection is disabled
	OFF	Remote Connection is enabled
VPN Green	ON	VPN connection is working properly
	Blinking	VPN connection is not working properly
	OFF	VPN functionality is disabled or VPN Box/Point-to-Point functionality is enabled but no client is connected or VPN Box/Single LAN functionality is enabled but the Device is not configured yet
LAN/WAN	ON	The Ethernet ports are working in "LAN/WAN" mode
Green	OFF	The Ethernet ports are working in "Switch" mode
SERV Green	ON	VPN Box "SERVICE" connection is working properly
	Blinking	VPN Box "SERVICE" connection is not working properly
	OFF	VPN Box functionality is disabled
RX2-4 Green	Blinking	Data reception (COM 2-4)
	ON	Check the connection (COM 2-4)
	OFF	No data reception (COM 2-4)
TX2-4 Green	Blinking	Data transmission (COM 2-4)
	ON	Check the connection (COM 2-4)

	OFF	No data transmission (COM 2-4)
3G PWR Green	ON	The 3G Modem is powered on
STAT Yellow	Slow blinking (200 ms OFF, 1800 ms ON) Slow blinking (1800 ms OFF, 200 ms ON) Fast blinking (125 ms OFF, 125 ms ON)	Searching for GSM network Registered on GSM network Data transfer is ongoing

Ethernet Connector LEDS

LED	Status	Meaning
ETH1-2 Green	ON	Ethernet 1-2 connection detected
	OFF	Ethernet 1-2 connection absent
ETH1-2 Yellow	Blinking	There is data activity (Ethernet 1-2)
	OFF	There is no data activity (Ethernet 1-2)

5.4 Z-TWS4-IO

LED	Status	Meaning
PWR Green	ON	The module is powered on
RUN Green	Blinking	The module is ready for use
DIDO Green	ON	Configurable Digital Input/Output state is HIGH
	OFF	Configurable Digital Input/Output state is LOW
DO Green	ON	Digital Output state is HIGH
	OFF	Digital Output state is LOW
RCD Green	ON	Remote Connection is disabled
	OFF	Remote Connection is enabled
VPN Green	ON	VPN connection is working properly
	Blinking	VPN connection is not working properly
	OFF	VPN functionality is disabled or
		VPN Box/Point-to-Point functionality is enabled but no client is connected or

		VPN Box/Single LAN functionality is enabled but the Device is not configured yet
LAN/WAN Green	ON	The Ethernet ports are working in "LAN/WAN" mode
Green	OFF	The Ethernet ports are working in "Switch" mode
SERV Green	ON	VPN Box "SERVICE" connection is working properly
	Blinking	VPN Box "SERVICE" connection is not working properly
	OFF	VPN Box functionality is disabled
RX2-4 Green	Blinking	Data reception (COM 2-4)
	ON	Check the connection (COM 2-4)
	OFF	No data reception (COM 2-4)
TX2-4 Green	Blinking	Data transmission (COM 2-4)
	ON	Check the connection (COM 2-4)
	OFF	No data transmission (COM 2-4)

Ethernet Connector LEDS

LED	Status	Meaning
ETH1-2 Green	ON	Ethernet 1-2 connection detected
	OFF	Ethernet 1-2 connection absent
ETH1-2 Yellow	Blinking	There is data activity (Ethernet 1-2)
	OFF	There is no data activity (Ethernet 1-2)

5.5 S6001-RTU

Frontal LEDS

Group	Number	Colour	S	Status		
Digital Inputs	1,2,3,4,5,6,7,8	Green	ON	High		
	9,10,11,12,13,14,15		OFF	Low		
Digital Outputs	1,2,3,4,5,6,7,8	Red	ON	Closed		
			OFF	Open		
3G Power Signal	2,3,4,5,6	Yellow	OFF	ON	6 ON = Max	
	1	renow	Blinking	ON	1 Blinking = Min	
Comm. Port COM2	RX, TX	Red	Blinking	·	RS485 activity	
		Red	Fixed ON		Verify connection	
Comm. Port COM4	RX, TX	Red	Blinking		RS485 activity	
		Red	Fixed ON		Verify connection	

Run	1	Red	Blinking	Run	
Level switch	L1, L2	Green	OFF, OFF (value ON, OFF (value ON, ON (value	e 1)	Under min level Between min and max levels Over max level

Following are some further notes about LED behavior:

- at power on, during the bootstrap phase, all LEDS, except for the COM PORT LEDs, are ON; when the system is fully operational, RUN LED is blinking
- when Straton application is not running, all LEDS, except for the COM PORT LEDs, are blinking
- 3G PWR SIG LED 1 is blinking, synchronously with RUN LED, in the following situations:
 - GSM/3G network is not available (or signal level is too low)
 - $\circ \quad \text{SIM is not inserted} \quad$

Modem LEDS

LED	Status	Meaning
3G PWR Green	ON	The 3G Modem is powered on
STAT Yellow	ON	Not registered on GSM network
	Slow Blinking	Registered on GSM network
	Fast Blinking	Mobile Network connection active

6 Discovering the IP address

Z-TWS4/Z-PASS2-S/S6001-RTU devices come out of the factory with the default 192.168.90.101 IP address on the Ethernet network interface.

If this address is changed, *and forgotten*, it can be retrieved by running the "Seneca Device Discovery" (SDD) application, as shown in the following figure:

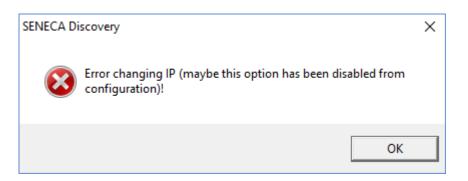
evices	found								
#	IP	Mode	MAC	Ping	Name	Hostname	Firmware	CRC	Comman
€	192.168.85.8	STATIC	C8:F9:81:0C:01:9D	2 ms	Z-KEY	192.168.85.8	110.0	OK	Assign
€	192.168.1.101	STATIC	C8:F9:81:0C:00:07	Different Subnet	Z-KEY	192.168.1.101	112.0	ОК	Assign
€	192.168.84.192	STATIC	C8:F9:81:02:03:5F	2 ms	Z-TWS4	ZTWS4	2940.210	ОК	
€	192.168.85.7	STATIC	C8:F9:81:02:02:85	2 ms	Z-PASS	192.168.85.7	3900.122	OK	
€	192.168.85.6	STATIC	C8:F9:81:11:00:02	2 ms	Z-PASS2-S	192.168.85.6	2940.221	ОК	
€	192.168.84.155	STATIC	00:22:4D:B6:D4:06	2 ms	Cloud BOX	cloud-dev.seneca	7800.106	ОК	
€	192.168.95.101	STATIC	C8:FA:81:16:00:02	Different Subnet	Z-PASS2-S	192.168.95.101	2940.310	ОК	Assign
€	192.168.85.102	STATIC	C8:F9:81:02:01:5B	2 ms	Z-TWS4	ZTWS4	2940.222	ОК	
€	192.168.85.106	STATIC	96:00:00:EA:18:F3	6 ms	S6001-RTU	S6001RTU	2940.310	ОК	Assign
€	192.168.85.200	STATIC	C8:F9:81:02:01:BD	2 ms	Z-TWS4	ZTWS4	2940.220	ОК	
€	192.168.85.69	STATIC	08:00:27:5B:CB:12	1 ms	Cloud BOX	192.168.85.69	7800.106	OK	
_									
	11 devices								

This application shows the IP address, MAC address, FW version and some other useful information, for every Z-TWS4/Z-PASS2-S/S6001-RTU device (and other Seneca products) found in the LAN.

Moreover, by clicking on the "Assign" button, it is possible to change the network configuration parameters of a device, as shown in the following figure:

Assign IP	x
	IP
Static IP	192.168.95.101
Netmask	Gateway
255.255.255.0	192.168.95.1
Assign	Cancel

For security reasons, this feature can be disabled on the Device (see paragraph 19.1.2); in this case, the following error message is shown, after clicking on the "Assign" button".



The SDD can be easily installed by running the installer program available at the following link:

http://www.seneca.it/products/sdd

NOTE:

- when the Device is working in "Switch" mode, the IP Address shown by the SDD is the same regardless of the Ethernet port which the PC running the SDD is connected to;

- when the Device is working in "LAN/WAN" mode, the IP Address shown by the SDD is the LAN IP Address when the PC is connected to the LAN port, the WAN IP Address when the PC is connected to the WAN port; moreover, the network configuration parameter changes apply to the relevant port.

7 FTP/SFTP access

To easily access the Device by means of FTP/SFTP, you can use the WINSCP[™] program; you can free download WINSCP[™] from:

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

You must set the connection as in the following figure (the screenshot shows a connection to the 192.168.85.106 IP address):

	WinSCP Login	? 🗙
Sessione Sessioni salvate Creazione log Ambiente	Sessione Nome server 192.168.85.106	Numero poţta
- Cartelle - SFTP - SCP Connessione - Proxy	Nome utente Passwo user •••••• File chiave privata	
- Tunnel SSH - Scambio chiave - Autenticazione	Protocollo Protocollo file SFTP V VC	onsenti SCP (allback
└─ Bug Preferenze ✔ Opzioni avanzate		Scegli cglore
Informazioni Lang	uages Accedi	Salva Chiudi

The credentials (username and password) are those ("user", "123456") set for the "FTP USER" (see "Users Configuration" web page in paragraph 19.1.7).

After clicking the "Access" button, you will get a new window, as in the following screenshot; on the right, you can copy and delete files directly to/from the Device.

			10g - dser@192.1	68.85.106 - WinSCP					- • ×
Locale Seleziona File Comandi Sessione O	•								
🏟 🗏 🗊 🔹 🔐 😵 🔛 🚱 😤 🕯		Predefinito -	🕶						
	- 🗈 🖾 🖓 🗞			🔒 log	• 🖮 🖕 • 🔿 • 🛅 加	🕼 🕼 😫			
C:\Users\Spagiari\Documents				/log					
Nome Estensione	Dimensi Tipo	Modificato	Attr	Nome Estensione	Dimensi	Modificato	Diritti	Proprietario	
±	Cartella superi	29/10/2014 17.43.39	r	🛓		01/01/1970 01	rwxr-xr-x	root	
Amministrazione	Cartella di file	05/11/2014 09.14.15		Conf		05/11/2014 15	INXENXENX	root	
Bluetooth Folder	Cartella di file	15/11/2013 07.46.42		a disk		05/11/2014 15	INXENXENX	root	
Boards	Cartella di file	27/06/2014 13.58.25		ash_history	672	05/11/2014 15	rw-rr	user	
Bug 1474 – Etc GMT Timezones misplaced	Cartella di file	22/11/2013 18.19.50		Cron.log	45	05/11/2014 15	rw	root	
🖟 Codesys	Cartella di file	07/10/2014 10.07.56		messages	4.014	05/11/2014 15	rw-rw-rw-	root	
📕 Copalp	Cartella di file	05/03/2014 12.14.09		mmc	16	05/11/2014 15	rwxrwxrwx	root	
📕 File di Outlook	Cartella di file	05/11/2014 14.28.18							
li Freescale	Cartella di file	29/10/2014 17.43.51							
🖹 Immagini	Cartella di file	03/12/2013 19.31.43	sh						
JMobile Suite	Cartella di file	12/09/2014 16.17.37							
🖥 Manuali	Cartella di file	17/06/2014 13.19.38							
Musica	Cartella di file	03/12/2013 19.31.43	sh						
NAT with Linux and iptables - Tutorial (Intr	Cartella di file	26/03/2014 13.41.54							
DpenEmbedded	Cartella di file	10/09/2014 11.23.41							
📙 Progetti ZNET3	Cartella di file	07/10/2014 08.27.09							
Progetti ZNET4	Cartella di file	28/08/2014 13.13.54							
Progetti_ZNET4	Cartella di file	29/08/2014 16.04.31							
Progetti_ZNET4_2	Cartella di file	02/10/2014 08.24.04							
Progetti_ZNET4_TWS5	Cartella di file	05/11/2014 12.06.19							
🔓 Seneca	Cartella di file	26/03/2014 10.09.45							
🖥 SIMCom	Cartella di file	17/10/2014 08.32.33							
b Standards	Cartella di file	21/03/2014 08.43.04							
📙 Straton	Cartella di file	26/09/2014 13.32.03							
📙 Tutorials	Cartella di file	22/04/2014 06.28.46							
📙 TWS3	Cartella di file	17/07/2014 14.20.45							
🐌 TWS5	Cartella di file	06/06/2014 07.37.59							
🖥 Video	Cartella di file	03/12/2013 19.31.43	sh						
🐌 Visual Studio 2008	Cartella di file	27/10/2014 14.57.02							
🐌 Visual Studio 2010	Cartella di file	27/10/2014 14.33.32	~						
) B di 93.891 B in 0 di 40				0 B di 4.747 B in 0 di 6					
🥒 F2 Rinomina 📝 F4 Modifica 📸 F5 Copia	📸 F6 Sposta 💣 F7 Crea carte	lla 🗙 F8 Elimina 😁 F	9 Proprietà 🧵 F10 Esci						
							A	SFTP-3	0.00.37
								5115	······································

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

8 StratON PLC

Z-TWS4/Z-PASS2-S/S6001-RTU StratON PLC provides the full support for 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 simple to write, download and debug IEC 61131-3 code.

8.1 Writing, downloading and running the first program

To let the PLC developer easily create StratON applications for Seneca CPUs, the following libraries are available:

- a Function Block (FB) and Functions library, which provides some frequently used functionalities, particularly related to communication and data transfer tasks, compiled in the CPU firmware; the direct use of these FBs and functions is targeted at skilled PLC developers (a detailed description of the FBs and Functions is given in chapter 20);
- a "Profiles" library, which provides access to the CPU I/Os by means of "profiled" variables; this is needed for S6001-RTU and Z-PASS2-S-IO CPUs;

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

Furthermore, two project templates are available for Z-PASS2-S and S6001-RTU CPUs, respectively.

An installer program, called *"Seneca StratON Package setup"*, is available which automatically installs the above Seneca libraries and templates. The installer can also be used to install the StratON IDE and Z-NET4 <u>SW</u> (see chapter 21).

The installer is available at the following link:

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

If, for some reasons, the installer can't be run, the above libraries and templates can be installed manually as described in the following sub-paragraph.

8.1.1 Seneca libraries and templates installation

The following steps are needed to integrate the Seneca libraries and templates in the StratON IDE.

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

S Library Manage	r - User	- 🗆 🗙
<u>F</u> ile <u>T</u> ools <u>W</u> izard <u>H</u> elp		
Function and FBs I/Os Profiles AS-i Types		
		<u>N</u> ew
		<u>R</u> ename
Parameters Description		<u>D</u> elete
	^	<u>S</u> tore
		Reset <u>C</u> hanges
<	>	

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

Open Libr	ary	×
Seneca		OK
ProfDP PRP QBF Registers Registers (typed) Selectors Selectors Standard Strings TCP-IP Text buffers Timers UDP User Select a library in the list or enter name for creating a new library.		Cancel

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

🏭 l 💽 👔 = l		LIE	BRERIE_STRATON				- 🗆	×
File Home Condi	vidi Visu	alizza						^ ?
Copia Incolla		Sposta Copia in v in v	mina Nuova cartella		Proprietà	Opri ▼ Modifica Cronologia	Seleziona tut Deseleziona	tutto
Appunti		Organizza	Nuovo			Apri	Seleziona	
🛞 🏵 🔻 🕇 <u>]</u> « Pr	ogetti_in_cors	so → Z-TWS4 → FW → LIBRE	RIE_STRATON		~ ¢	Cerca in LIE	BRERIE_STRATON	,c
☆ Preferiti	Nome	~	Ultima modifica	Тіро		Dimensione		
E Desktop	🥘 linux_s	hell.XL5	13/07/2011 11.34	File XL5		1 KB		
鷆 Download	READN	1E_Seneca.txt	10/01/2014 15.01	Documer	nto di testo	1 KB		
😻 Dropbox	🥘 Seneca	_rev1.XL5	18/11/2013 08.04	File XL5		1 KB		
💷 Risorse recenti	🥘 Seneca	_rev2.XL5	10/01/2014 14.35	File XL5		2 KB		
JWS4	🥘 Seneca	_rev3.XL5	31/01/2014 17.41	File XL5		12 KB		
퉬 Work	🧾 Seneca	_revбa.XL5	24/06/2014 14.22	File XL5		17 KB		
	🧾 Seneca	_revбc.XL5	09/09/2014 11.30	File XL5		17 KB		
🖳 Questo PC	🧾 Seneca	_TWS4_TWS11.XL5	21/05/2014 17.29	File XL5		14 KB		
膧 Desktop	🧾 Seneca	StratonLibrary_sw2960_000.XL5	10/01/2014 14.35	File XL5		2 KB		
📗 Documenti	🧾 Seneca	StratonLibrary_sw2960_001.XL5	31/01/2014 17.41	File XL5		12 KB		
📙 Download	🧾 Seneca	StratonLibrary_sw2960_002.XL5	24/06/2014 14.22	File XL5		17 KB		
📔 Immagini	Seneca	StratonLibrary_sw2960_003.XL5	09/09/2014 11.30	File XL5		17 KB		
🚺 Musica —								
📔 Video								
🚢 OS (C:)								
👝 Disco rimovibile 🗸								
12 elementi 1 elemento :	elezionato 1	6,2 KB						:

Si Library Manager - Seneca — File Tools Wizard Help — Function and FBs I/Os Profiles AS-i Types GAIN_CFG (* Configure Analog Inputs (Z-MINIRTU, Z-TWS11)*)	
Function and FBs I/Os Profiles AS-i Types AND CFG (* Configure Analog Inputs (Z-MINIRTU, Z-TWS11)*) CCNT_SET (* Set counter (Z-MINIRTU, Z-TWS11)*)	blau
CAIN_CFG (* Configure Analog Inputs (Z-MINIRTU, Z-TWS11) *) CNT_SET (* Set counter (Z-MINIRTU, Z-TWS11) *)	N
CNT_SET (* Set counter (Z-MINIRTU, Z-TWS11)*)	N.L.
	New
Chefte Dirt (Cleate a directory (2-minint to, 2-twort))	Rename
DATETIME CFG (* Configure date/time (Z-MINIRTU, Z-TWS11)*)	
DATETIME_GET (* Get current date/time (Z-MINIRTU, Z-TWS11) *)	Delete
DATETIME_SET (* Set current date/time (Z-MINIRTU, Z-TWS11) *)	
DIN_DOUT_CFG (* Configure Digital Inputs/Outputs (Z-MINIRTU, Z-TWS11) *)	
FM_WRITE_NCRLF (* Write a string to a file without adding CR/LF *)	
ETP_GET (* File download by means of FTP protocol (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *) FTP PUT (* File upload by means of FTP protocol (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)	
FTP_FOT (File upload by means of FTP protocol (2-11/34, 2-FX32-3, 2-MINIRTO, 2-11/311, 30001-FTO))	
BTPSRV_CFG_READ (* Get the FTP server configuration (Z-MINIRTU, Z-TWS11) *)	
GET_ALARMS (* Retrieve alarms with the specified status from the DB. *)	
GET_MIN_SINCE2K (* Get the number of minutes since year 2000 *)	
EGET_SMS (* Get a received SMS (Z-TWS4, Z-PASS2-S, Z-MINIRTU, S6001-RTU) *)	
BHTTP_POST (* Send an HTTP POST request (Z-MINIRTU, Z-TWS11) *)	
IP_CFG (* Configure IP parameters (Z-MINIRTU, Z-TWS11) *)	
IP_CFG_READ (* Read current IP configuration (Z-MINIRTU, Z-TWS11) *) INUX SH ASYNC (* Execute a command in a Linux shell, in asynchronous mode (Z-TWS4, Z-PASS2-S, S6001-RTU) *)	
ILINUX_SHELL (* Execute a command in a Linux shell (Z-TWS4, Z-PASS2-S, S6001-RTU) *)	
MODEM CTRL ("Execute a generic AT command (2:TWS4, ZPASS2-S, S6001-RTU)")	
MODEM_ONOFF (* Power on/off the Modem (Z-MINIRTU) *)	
MODEM_RESET (* Execute a modem reset (Z-TWS4, Z-PASS2-S, Z-MINIRTU) *)	
TP_CFG (* Configure NTP (Z-MINIRTU, Z-TWS11) *)	
INTP_CFG_READ (* Get the NTP configuration (2-MINIRTU, 2-TWS11) *)	
PLAY_WAVE (* Execute an audio PCM file (Z-MINIRTU, Z-TWS11) *) PPP CONNECT (* PPP connection setup/release (Z-TWS4, Z-PASS2-S, Z-MINIRTU, S6001-RTU) *)	
PPP_CONNECT (PPP connection setup/release (Z-TWS4, Z-PASSZ-S, Z-MINIRTU, Z-TWS11, S6001-RTU)) PPP_STATUS (* PPP connection status (Z-TWS4, Z-PASSZ-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)	
GPUT ALARM (Store an alam into the DB.)	
RESET (* Reset the device (Z-MINIRTU, Z-TWS11) *)	
SEND_MAIL (* Send an e-mail (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)	
SEND_SMS (* Send an SMS (Z-TWS4, Z-PASS2-S, Z-MINIRTU, S6001-RTU) *)	
SET_ALARMS_STAT (' Set the status of the specified alarms in the DB. ')	
TIME_SYNC (* Time synchronization by means of NTP protocol (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *) TOT SET (* Set totalizer value (Z-MINIRTU, Z-TWS11) *)	
TXBAPPENDFILE (* Append a Text Buffer to a file *)	
WEBSRV CFG (* Configure the web server (Z-MINIRTU, Z-TWS11) *)	
WEBSRV CFG READ (* Get the web server configuration (Z-MINIRTU, Z-TWS11) *)	
Parameters Description	
	Store
	D
	Reset Changes
	5
<	

Save the library (menu "File / Save Library").

The procedure to add the "Profiles library" to the IDE is identical to the one just explained; the only difference is that the *SenecaStratonProfiles.XL5* file shall be selected (instead of the *SenecaStratonLibrary.XL5* file).

Now that the "low-level" FBs are available, we have to install the UDFB library.

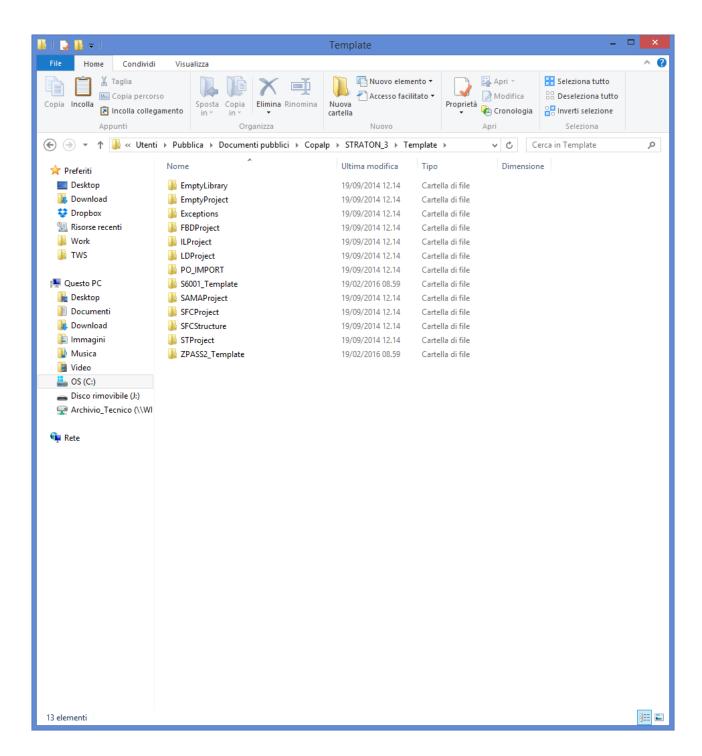
The UDFB library is provided as a zip file, containing the following folders:

- TWS_MISC
- ZPASS2_Template
- S6001_Template

The *TWS_MISC* folder shall be copied into the following directory: *C:\Users\Public\Documents\Copalp\STRATON\LIBS*

 Incolla collegamento Appunti 	za posta Copia in Copia Organizza a Documenti pubblici Copia Granizza a Documenti pubblici Copia Mome FBD_with_ENENO IntCounters SAMA TWS_MISC	Nuovo elemento ▼ Accesso facilitato ▼ Nuovo		Seleziona tutto Deseleziona tutto Inverti selezione Seleziona a in LIBS Dimensione	۸ (
Copia Incolla Copia percorso Copia Incolla Collegamento Appunti Copia Incolla Collegamento Appunti Copia Incolla Collegamento Appunti Copia Incolla Collegamento Appunti Copia Incolla Collegamento Appunti Copia Copia Collegamento Appunti Copia Copia Collegamento Appunti Copia Collegamento Appunti Copia Copia Collegamento Appunti Copia Collegamento Copia Copia Copia Collegamento Copia Copia Copia Collegamento Copia Copia Copia Copia Copia Collegamento Copia Copia Co	oosta Copia in Organizza a → Documenti pubblici → Copal Nome B FBD_with_ENENO IntCounters SAMA	Accesso facilitato ▼ Nuova cartella Nuovo P ▶ STRATON_3 ▶ LIBS Ultima modifica 19/09/2014 12.14 19/09/2014 12.14	Proprietà Apri Cconologia Apri Ccrco Tipo Cartella di file Cartella di file Cartella di file	Deseleziona tutto Inverti selezione Seleziona	م
 (→) ▼ ↑	a → Documenti pubblici → Copal Nome FBD_with_ENENO IntCounters SAMA	Ultima modifica 19/09/2014 12.14 19/09/2014 12.14 19/09/2014 12.14	 ✓ Cerc Tipo Cartella di file Cartella di file Cartella di file 		Q
 ✓ Preferiti ■ Desktop Download ♥ Dropbox ♥ Risorse recenti ● Work ● TWS 	Nome FBD_with_ENENO IntCounters SAMA	Ultima modifica 19/09/2014 12.14 19/09/2014 12.14 19/09/2014 12.14	Tipo Cartella di file Cartella di file Cartella di file		~
Desktop Documenti Domload Immagini Musica Video OS (C:)					
 Disco rimovibile (J:) Archivio_Tecnico (\\WIN-KTTN7I Rete 					

The *ZPASS2_Template* and *S6001_Template* folders shall be copied into the following directory: *C:\Users\Public\Documents\Copalp\STRATON\Template*



8.1.2 Creating a project for Seneca CPUs

Run the StratON IDE and create a new project based on a template, as in the following figure:

ß	Project wizard	×
Roject From template XML Import Library Automation script		
		8-8- 8-8- 8-8-
Creates a new projec	t using a template	~ ~
New project		
Destination folder :	C:\Users\Spagiari\Desktop\TWS4\StratonExamples V	
Name:	zpass2s	
Comment:	First project for Z-PASS2-S CPU	
	Next Cancel Hel	P

Select the "ZPASS2_Template" (or "S6001_Template") in the template list.

Template:	ZPASS2_Template			~
		Previous	Next	Help

Now, as you can see in the following figure, in the *Main* program a *ZMODEM_MNG* UDFB instance is already available, which lets you easily control the Z-PASS2-S/S6001-RTU modem.

5	STRATON - zpass2s	- đ 🗙
File Edit View Insert Project Tools Wi	ndow Help	
😂 🖬 🔮 🛃 👗 🗞 🖄 🕆 🛸 🏷	^ へ 語 調 圭 % 🤨 🛆 匹 🗊 😁 📷 🔎	
Workspace	Main	
🗄 – 🗿 zpass2s		 Type Dim. Attrib. Syb. Init value
Exception programs	Template utilize blocco gestione modern	B 🗋 Main
Programs	0	Inst_ZMODEM_MNG ZMODEM
	D Inst ZMODEM MVG	MDM_MNG_ON_OFF BOOL
 Watch (for debugging) 	Inst_ZMODEM_MNG	MDM_MNG_PPP_ON BOOL
Soft Scope	ZMODEM_MING	MDM_MNG_BUSY BOOL
Initial values		MDM_MNG_PPP_OK BOOL
Binding Configuration	T MDM_INNO_PPP_ON PPP_OK MDM_INNO_PPP_OK box bm X GPRS_APN BUSY MDM_INNO_BUSY	MDM_MNG_PWR_OK BOOL
	User User ALL ERAME ERA	MDM_MNG_ERR BOOL
Types	La pass PASSWORD RESULT MOM_MNG_RESULT	MDM_MNG_RESULT INT
in types	SIGLEV MOM_MNG_SIGLEV	MDM_MNG_SIGLEV INT
	->> REG NOM_MNG_REG	MDM_MNG_REG BOOL
	P MOM_MNG_OPID	MDM_MING_OFID STRING(50)
	- H MUM_MAS_IP	MORI, MING, QIL, QFF BOOL MORI, MING, PIPP ONI BOOL MORI, MING, PIPP ONI BOOL MORI, MING, PIPP, OK BOOL MORI, MING, PIPR, OK BOOL MORI, MING, PESULT NIT MOM, MING, RES BOOL MOM, MING, REG BOOL MOM, MING, POPO STRING(15) Het BOOL
		Global variables
	0	
		Variables, Proserves
	-	(A)
	0	🗄 🎦 (Used)
	SD.	🐵 🔚 (Project)
		🗄 📴 Advanced
	1	🗉 🛄 Aithmetic
	1st	Anays Asinterface
	5. S.	Ac-metrace Acnet
		Booleans
	12	B CANbus
		CANopen
		E Clock
		e Competitions
		III D Conversions
		Counters
		DNP3
	c	Finhedded HMI Blocks, Sovist Defre ENUM Gradies
	Build	Blocks, Sovist Units ENUM Grones /
	County -	
	Build, Cross references Runtime, Call stack, Breakpoints, Diotal sampling trace, Promot, HMI	
Ready		OffLine 192.168.90.101:502 💋 0,0 206 x 18 0,0 100% 🚲

Set the correct target IP address (for example 192.168.85.106); normally, the port shall be set to 502:

	Project settings		×
C:\Users\Sp	Communication Settings	×	
General Runtime Compiler Debugging Advanced (All)	T5 Runtime 192.168.85.106:502 192.168.85.103:1100 192.168.85.103:502 192.168.85.104:502 192.168.85.105:502 192.168.85.106:502 192.168.85.106:502 192.168.85.33:502 192.168.90.101:502	OK Cancel Browse Help	:502
			Cancel

Then press the icon:

ß

to compile the project.

Download the code by pressing the icon:

الكر

The project file will be placed into the */disk* directory of the Device.

If the Straton project is not based on "ZPASS2_Template"/"S6001_Template", the Seneca UDFB library can still be used, as described in the following.

In the Straton IDE, go to the "Project Settings" window, shown below (menu "Project/Settings"):

	Project settings	×
C:\Users\Spagiari\Docum	nents\Progetti_ZNET4_STEP3\s6001_default\s6001_defa	ult
General Runtime Compiler Debugging Advanced (All)	Name Communication parameters Cycle time Code Generation Complex variables in a separate segment On Line Change Version Libraries Use external objects	Value 192.168.85.104:502 2000 ms Release No Disabled V4 - 2016/01/22 12:32 Edit Edit
	Communication parameters for On Line connection to the Double click to edit	e runtime. OK Cancel

Click on "Libraries / Edit..."; the following window is shown:

Libraries	×
	Add Remove Close Help
Standard: FBD_WITH_ENENO INTCOUNTERS SAMA TWS_MISC	Add

Select the "TWS_MISC" library and click on "Add".

Libraries	×
C:\Users\Public\Documents\Copalp\STRATON_3\Libs\TWS_MISC	Add Remove Close Help
Standard: FBD_WITH_ENENO INTCOUNTERS SAMA	Add

Finally, click on "Close".

Now, the UDFB library is available in the project, as shown in the following figure:

S	STRATON - s6001_default								-	
File Edit View Insert Project Tools Win	dow Help									
C	◇ ◇ 話 珥 盂 物 ⑤ 凸 ■ 30 10 宮 和									
Workspace	main									12
💷 📴 s6001_default	5	^	Name	Type	Dim.	Attrib.	Syb.	Init value	User	Tag Di
Exception programs	8			*main program*)						
			🗉 🚮 Global							
P pOnDivZero				STRING(10)				Z-PAS		U
- II pShutDown			Z_MUTEX	BOOL						L
st pStartup	e		Z_MUTEX_	BOOL						U
📴 Graphic			Z_MODEM	BOOL						u
Programs	51		Z_MODEM							U.
🔤 1 main ("main program")	5. State 1.		Z_bPPPon							u
- Da Recipe			Z_bPoiRiac	c BOOL						u
Cal Signals			Z_bReqMO							u
- Soft Scope			Z_bReqMO							L L
Spy Distring Tables			M0_AI_CUF							-4
			M0_AI_CUF				H			-4
			M0_AI_CUF M0_AI_CUF							
			M0_A1_COF				H			-1
			M0_AO_CC				H			-4
1/0s			M0 AO EL				H			
- Sg Global defines			M0_AU_ELE							
Variables			<	DTTL		_	-			>
Types										,
,,=			🗉 🛄 Registers	(typed)						
			E Selectors							
			🗄 🛄 Seneca							
			 E Standard E Strings 							
			E is topings							
			🗄 🦲 Text buffe							
			🗄 🧾 Timers	15						
			E DDP							
			🗉 🧧 UML							
			TWS_MIS	c.						
			The age of the second s							
			8 ZFTP							
			👫 ZIP_U							
			35 ZMAI							
			2M00							
			8 ZM00							
			36 ZM00							
			35 ZSMS							
		~	S ZSMS	SEND						
			() Blooks St	vist Define El	IUM /					
	() IODrives main									
	Build									
	(1) Build, Cross references Runtime Cali stack Breakpoints Diptal sampling trace Promot HMI							_	_	_
Ready	Offline 192	. 168.85	. 104:502	/ 0,-540	517	x 18 0,0		100%	44	

If the Straton project has been built using the Seneca Z-NET4 SW (see chapter 21), the *TWS_MISC* is already included, so the above procedure is not needed.

In particular, when using S6001-RTU CPU, Z-NET4 SW provides a simple way to create the base Straton project; in fact, all the variables corresponding to the CPU I/Os will be inserted in the project, as shown in the following figure.

🝸 Name	Value	Туре	Dim.	Attrib.	Syb.	Init value	User	Tag	Descript
M0_AI_CUR1	5	INT							_ZNE 🔨
M0_AI_CUR2	8	INT							_ZNE
M0_AI_CUR3	2	INT							_ZNE
M0_AI_CUR4	14	INT							_ZNE
M0_AO_CUR	0	INT							_ZNE
M0_AO_VOLT	0	INT							_ZNE
M0_AO_ELEC_SENS	0	BYTE							_ZNE
M0_AI_ELEC_LEVEL	0	BYTE							_ZNE
M0_ADC_ERROR_STATUS	0	INT							_ZNE
M0_ADC_CRC_ERR_CNT	0	UINT							_ZNE
M0_DI_01	FALSE	BOOL							_ZNE
M0_DI_02	FALSE	BOOL							_ZNE
M0_DI_03	FALSE	BOOL							_ZNE
M0_DI_04	FALSE	BOOL							_ZNE
M0_DI_05	FALSE	BOOL							_ZNE
M0_DI_06	FALSE	BOOL							_ZNE
M0_DI_07	FALSE	BOOL							_ZNE
M0_DI_08	FALSE	BOOL							_ZNE
M0_DI_09	FALSE	BOOL							_ZNE
M0 DI 10	FAI SE	BOOL							
×									1

For more information about Straton IDE and related tools, please refer to StratON tutorials and on-line help.

8.1.3 Z-PASS2-S-IO profiles

Two Straton I/O profiles are available for Z-PASS2-S-IO CPU.

The first profile, named "ZPASS_DIO", provides variables corresponding to the available Digital I/Os, as shown in the following figure.

T	Name	🛆 Туре	Dim. Attrib.	Syb. Init va	ilue User Tag
	🕀 🗋 Main				
	🗉 🚮 Global vari	ables			
	DI1	BOOL			
	DI2	BOOL			
	DI3	BOOL			
	DI4	BOOL			
	DO1	BOOL			
	DO2	BOOL			
	DO3	BOOL			
	DO4	BOOL			
	🚽 RETAIN va	riables			

It should be noted that four "DIx" variables and four "DOx" variables are declared, corresponding to the maximum number of inputs and outputs possibly available; the Digital I/O configuration (see paragraph

19.1.13) determines which of these variables are actually handled by the PLC; for example, if DIDO1 is set as an input and DIDO2 as an output, DI3 and DO4 will be handled while DI4 and DO3 will not be used.

Moreover, while the variables corresponding to the inputs are updated by the PLC regardless of their function modes, only the variables corresponding to the outputs set as "General Output" will actually affect the digital outputs.

The second profile, named "ZPASS_GPS", provides variables corresponding to the information given by the GPS module, as shown in the following figure.

🝸 Name	Туре	Dim.	Attrib.	Syb.	Init value	User	Tag
🗆 📄 Main							
GPS_LAT	LREAL						
GPS_LONG	LREAL						
GPS_HDOP	LREAL						
GPS_ALT	LREAL						
GPS_FIX	BYTE						
GPS_COG	LREAL						
GPS_SPKM	LREAL						
GPS_SPKN	LREAL						
GPS_DATE	STRING(6)						
GPS_NSAT	BYTE						
GPS_ERROR	INT						
GPS_UTC	STRING(10)						
🗉 🚮 Global variables							
层 RETAIN variables							

In particular, the *GPS_ERROR* variable tells if the other variables contain valid and updated values or not, in the following way:

- GPS_ERROR = 0 GPS fixed; variables contain updated values
- GPS_ERROR = -1 GPS not fixed; variables contain not updated, possibly invalid, values
- GPS_ERROR = -2 some error has occurred; variables contain invalid values

8.1.4 Z-TWS4-IO profile

The "ZPASS_DIO" profile is available also for Z-TWS4-IO, providing variables corresponding to the available Digital I/Os, as shown in the following figure.

7	Name	Туре	Dim.	Attrib.	Syb.	Init value	User	Tag	Desc
	📄 main (*m	ain program*)							
	🗉 🚮 Global va	riables							
	DI3	BOOL							
	DI4	BOOL							
	DO1	BOOL							
	DO2	BOOL							
	DO3	BOOL							
	DO4	BOOL							
	🚽 RETAIN 🗤	variables							
	<								>

It should be noted that two "DIx" variables and four "DOx" variables are declared, corresponding to the maximum number of inputs and outputs possibly available; the Digital I/O configuration (see paragraph 19.1.13) determines which of these variables are actually handled by the PLC; for example, if DIDO1 is set as an input and DIDO2 as an output, DI3 and DO4 will be handled while DI4 and DO3 will not be used.

Moreover, while the variables corresponding to the inputs are updated by the PLC regardless of their function modes, only the variables corresponding to the outputs set as "General Output" will actually affect the digital outputs.

8.2 Energy Management Protocols

The StratON soft-PLC installed on Z-TWS4/Z-PASS2-S/S6001-RTU supports the following "Energy Management" protocols:

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

The activation of these protocols is license-based.

Please contact Seneca to get more information about getting the license for Energy Management protocols.

8.3 StratON Redundancy

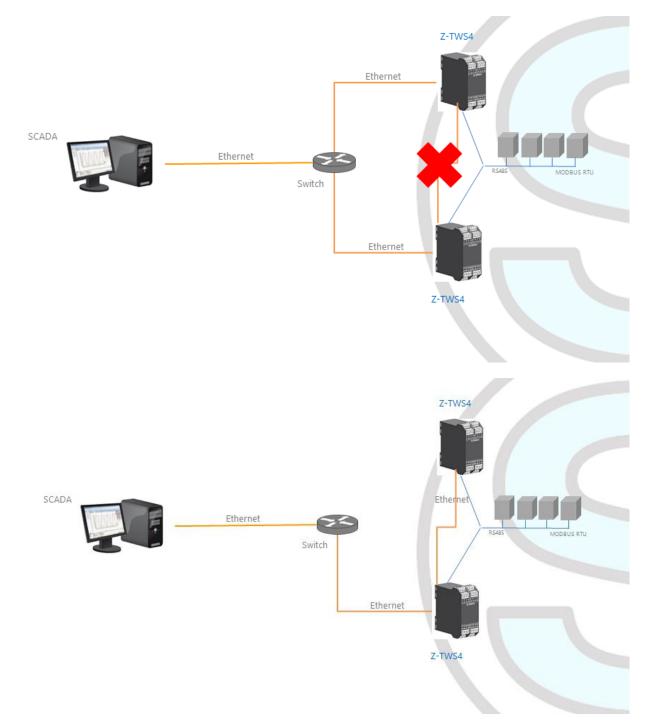
WARNING!

At the date of this manual, the "StratON Redundancy" functionality is still in a "Beta version"; this means that the proper operation of this functionality is not guaranteed for every kind of application; please contact Seneca for further information.

The StratON PLC provides a "Redundancy" functionality:

when this feature is enabled, two CPUs (Z-TWS4 or Z-PASS2-S or S6001-RTU) run the same StratON application; the two CPUs connect each other via the Ethernet, in order to keep variables, state-machines etc. synchronized between them; in each moment, only one of the two CPUs actually runs the application and drives the fieldbus; if, for any reason, that CPU stops running, the application execution is handed over to the second CPU.

When the redundancy is used, some care must be taken when connecting the devices, in order to avoid Ethernet loops; the Ethernet connections shall be set up as shown in the following figures.



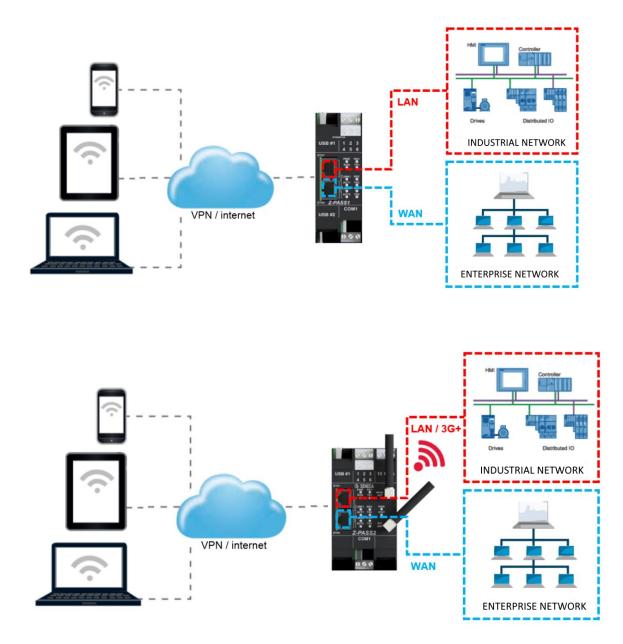
Please see paragraph 19.1.2 for a description of the configuration parameters related to StratON Redundancy.

9 Ethernet Mode (Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO)

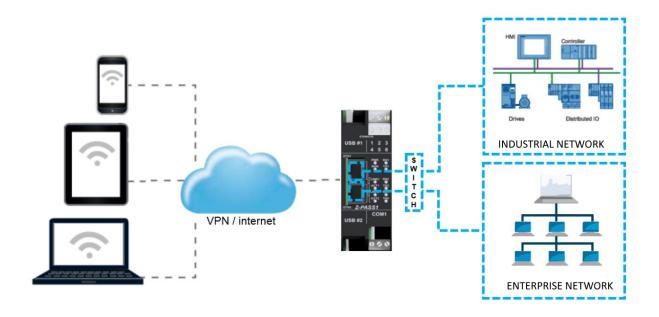
In Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO products, the two available Ethernet ports can be configured as two fully separated network interfaces ("LAN" and "WAN") or, as in the older versions, they can work as

ports of an Ethernet switch; the user can choose between the "LAN/WAN" mode and the "Switch" mode, by means of a configuration parameter ("Ethernet Mode") (see paragraph 19.1.2).

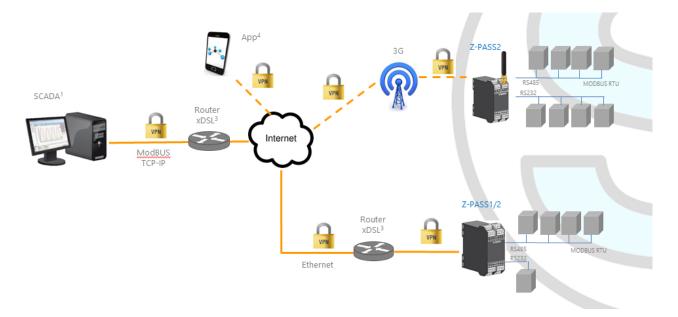
The "LAN/WAN" mode is needed when the "industrial" network connected to the LAN interface (comprising e.g. HMI and PLC devices) shall be separated from the "enterprise" network connected to the WAN interface (comprising enterprise PCs and servers); when the Device is remotely accessed through the WAN interface, only devices connected to the LAN interface can be reached, while access to machines lying in the enterprise network is forbidden; this is depicted in the following two figures.



When this separation is not needed or when the Internet access is achieved only through the mobile (3G+) interface, the "Switch" mode still lets the Device be used as an Ethernet switch, as shown in the following figure.



10 VPN



Z-TWS4/Z-PASS2-S/S6001-RTU support the standard OpenVPN protocol.

The main advantages that come from using a VPN are:

- secure connections, since transported 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 by a built-in Web Server.

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

The "OpenVPN" mode can be used when the Device shall be installed in an already existing VPN. In this case, an OpenVPN server shall be available and the certificate and key files for the Device client shall be provided by the VPN administrator; the files can be uploaded to the Device using the "VPN configuration" page of Device Web Server.

If the VPN infrastructure does not exist yet, the advisable choice is to adopt the "VPN Box" solution, developed by Seneca. The "VPN Box" is an hardware appliance (or a virtual machine) which lets the user easily setup two alternative kinds of VPN:

- "Single LAN" VPN
- "Point-to-Point" VPN

In the "Single LAN" VPN, all devices and PCs (and associated local subnets) configured into VPN are always connected in the same network. In this scenario any PC Client can connect to any Device and to other machines which lie in the Device LAN, but also any device/machine can connect to any other remote device/machine which belongs to the same VPN network. This VPN architecture puts some constraints on the device sub-networks definition, in fact all VPN clients must have a different IP address and different local LAN, to avoid conflicts. The software named "VPN BOX Manager" configures VPN BOX and will help you to avoid errors defining local subnets.

In the "Point-to-Point" VPN, a client PC, in a given moment, can perform a single connection, on demand, to only one Device (and to machines which lie in the Device LAN) at time. Furthermore, devices can't communicate each other. The advantage of this architecture is that the same sub-network can be used in all sites. Point to point mode makes it possible to define user groups and manage them. This VPN modality must be configured on "VPN Box".

There are two kinds of "Point-to-Point" VPN:

- routing Layer 3 VPN
- bridging Layer 2 VPN

In "Routing Layer 3 VPN", only IP (Layer 3) packets are transported over the VPN tunnel and a new virtual LAN is created with a network subnet which must be different from the LAN subnets of the server and clients.

Conversely, in "Bridging Layer 2 VPN", all Ethernet frames are transported over the VPN tunnel and the clients are inserted in the server LAN.

Each of the two kinds has benefits and drawbacks:

Layer 2 benefits/drawbacks:

- can transport any network protocol
- broadcast traffic (e.g.: DHCP) is transported
- > causes much more traffic overhead on the VPN tunnel

Layer 3 benefits/drawbacks:

- > can transport only IP traffic
- broadcast traffic (e.g.: DHCP) is not transported
- > lower traffic overhead, transports only traffic which is destined for the VPN clients

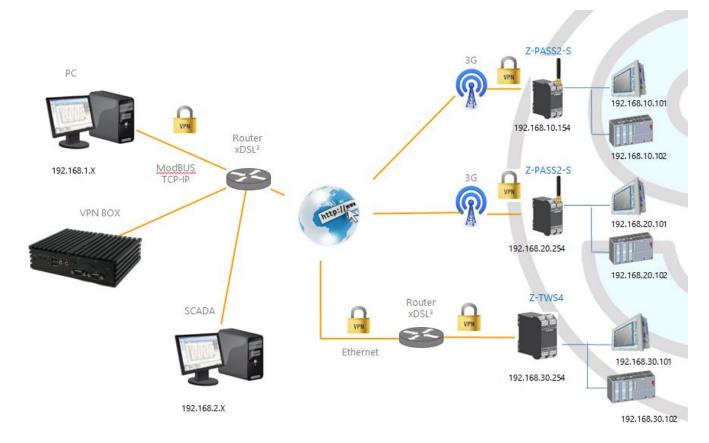
The "VPN Box" is supplied with two Windows applications:

- the "VPN Box Manager", which allows to configure the VPN⁴ mode on the VPN Box and manage the devices⁵
- the "VPN Client Communicator", which lets the user 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 "VPN Box" can be found in the "VPN Box User Manual".

A detailed description of Z-TWS4/Z-PASS2-S/S6001-RTU VPN configuration parameters is given in 19.1.4 paragraph.

The following two sub-paragraphs give some more info about the two kinds of VPN.



10.1 "Single LAN" VPN

The above figure gives an example of a "Single LAN" VPN.

The client PC (with IP address 192.168.1.X) can connect, just as an example, to the first Z-PASS2-S by using its 192.168.10.154 IP address and to the PLC in the Z-PASS2-S LAN by using its local IP address 192.168.10.102.

Also, two devices which lie 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.

⁴ Only one of the two kinds of VPN can be configured on a given VPN Box.

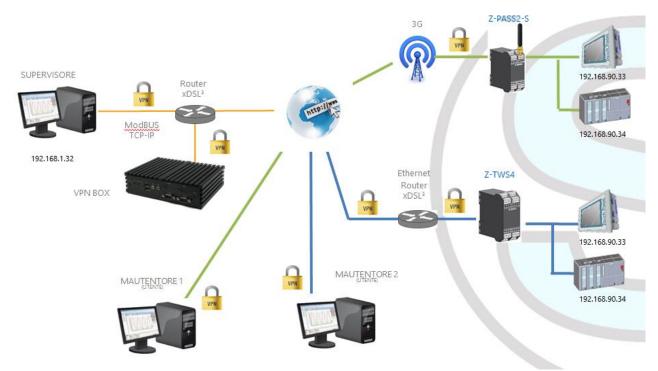
⁵ "VPN Box" functionality is available also on Seneca Z-PASS1 and Z-PASS2 products.

To let this scenario work correctly, an essential rule must always be followed: <u>the Device LANs and the PC</u> <u>LAN shall have different and not colliding subnets</u>; so, in the above figure, the following subnets allocation has been depicted:

PC LAN	192.168.1.0/24
SCADA LAN	192.168.2.0/24
Z-PASS2 LAN	192.168.10.0/24
Z-PASS2 LAN	192.168.20.0/24
Z-PASS1 LAN	192.168.30.0/24

The "VPN Box Manager" application guides you in the configuration task, checking that no subnet/IP address conflict is present in the network.

If subnet/conflicts cannot be avoided, using a "Single LAN" VPN is still possible if local IP addresses are not used; devices can be reached by means of their VPN IP addresses and machines beyond them can be reached by configuring some "port forwarding" rules on the Device Router (see 19.1.5 paragraph).



10.2 "Point-to-Point" VPN

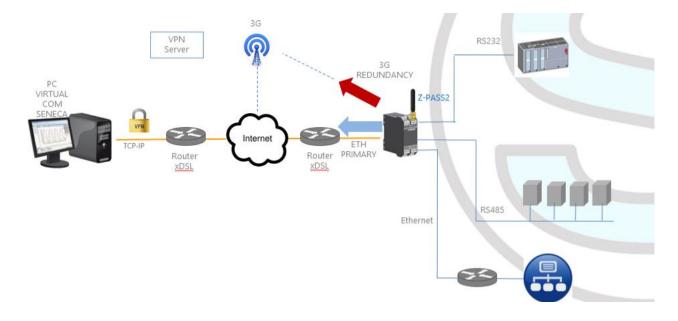
The above figure gives an example of a "Point-to-Point" VPN.

In this scenario a PC (acting as a VPN Client) can connect, on demand, to only one Device and its subnet, using local IP addresses. Since the client "sees" just one Z-TWS4/Z-PASS2-S/S6001-RTU (and attached devices) at time, the same subnet configuration can be assigned to different sites, without creating conflicts.

For this kind of VPN, the "VPN Box Manager" application lets define group of users that can connect only to assigned devices.

The "VPN Client Communicator" application retrieves the list of devices which are available for the logged user; then the user can select one device on the list and connect to it.

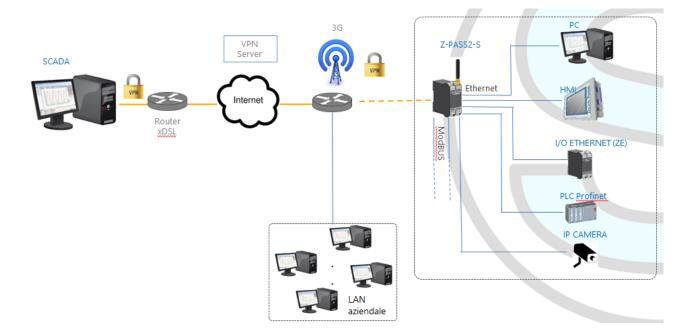
11 Network Redundancy



"Network Redundancy" is a functionality than can be enabled on the Device when a 3G modem is available (true for Z-PASS2-S and S6001-RTU).

This functionality switches the network interface used to access the Internet from the Ethernet ("primary" interface) to the Mobile/3G ("secondary" interface), when Internet access through the primary interface becomes unavailable; when access through the primary interface become available again, the network interface is switched back to Ethernet.

The parameters provided to configure Network Redundancy are explained in paragraph 19.1.2 "Network and Services".



12 Router

As already told before, "Router" functionality routes packets between the WAN (Mobile Network) interface and the LAN (Ethernet) interface and vice versa; so, this functionality especially makes sense when a 3G connection is active, which needs the availability of a 3G modem (true for Z-PASS2-S and S6001-RTU).

More specifically, an important feature of the Router is what is known as "IP forwarding"; this means that when the Device receives a packet not targeted 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 what is known as "IP masquerading", meaning that the original source IP address is replaced with the IP address of the WAN (Mobile Network) interface.

Another important feature is the availability of a DNS server/forwarder, which can resolve names either by itself or querying the external configured DNS server.

Also, a DHCP server is available which assigns IP addresses to clients connected on the Device LAN; here, you can configure the range of addresses used by the server and the lease time.

There is also the possibility to define up to five "Port Forwarding" rules or "Virtual Servers"; using these rules, you can, for example, redirect packets received on a TCP or UDP port to another Device port or to another machine, with a different IP address, on the same or another port.

As an alternative to using "Port Forwarding" rules, Router + VPN functionalities allow the use of local addresses, as shown in the previous chapter; in the router configuration, a flag is given to enable this feature.

A detailed description of the Router configuration can be found in paragraph 19.1.5.

13 Remote Connection Disable

Z-PASS2-S-IO and Z-TWS4-IO products provide a dedicated digital input and a dedicated digital output to control and monitor remote connection to the device.

In details:

- when "Remote Connection Disable" digital input is set to HIGH state, remote connection to the device is disabled; conversely, when "Remote Connection Disable" digital input is set to LOW state, remote connection to the device is enabled; "Remote Connection Disable" digital input state is reported by the "RCD" LED;
- "Remote Connection Active" digital output is set to HIGH state when the device is remotely accessed (VPN connection is active); it is set to LOW state when VPN connection is not active.

Four levels of security can be configured to disable remote connection:

- Level 1 ("VPN Connection"): VPN connections are disabled in any VPN mode (VPN Box Point-to-Point, VPN Box Single LAN, OpenVPN), but VPN Box Service is still running, so the device can still be monitored on VPN Box Manager;
- Level 2 ("VPN Service"): VPN Box Service is disabled, but the device can still access the Internet and send/receive SMSs;
- Level 3 ("Internet Connection"): any Internet access is disabled, but the device can still send/receive SMSs;
- Level 4 ("SMS Service"): modem is off, so SMSs can't be sent/received.

See "Digital I/O Configuration" paragraph to learn how to set the desired security level.

14 Auto-APN

The Auto-APN feature lets the Device establish mobile data connections without requiring the user to configure APN data⁶ for the SIM in use.

This is accomplished by using the SIM IMSI and, possibly, some other data available on the SIM, to select the proper APN record in an internal DB⁷, containing APN records for all mobile operators in the world.

In some particular cases, however, when a "custom APN" shall be used, the Auto-APN feature can be disabled, setting the "APN Mode" parameter to "Manual", in the "Mobile Network" page (see paragraph 19.1.10).

15 M-Bus (ONLY Z-TWS4-IO and Z-PASS2-S-IO)

Z-TWS4-IO and Z-PASS2-S-IO, can be connected to a M-Bus fieldbus in the following way:

- connecting the Seneca "Z-MBUS" RS232-MBUS adapter to the COM1 serial port;
- setting the COM1 mode to RS232 (see paragraph 19.1.2).

⁶ APN data are: APN, Username, Password and Authentication Type.

⁷ This DB is updated to the one used in the last Android O.S. version.

To handle M-Bus devices, the following resources are provided:

- the "M-Bus" section web pages
- the MBUS_READ_CTL function
- the MBUS_WRITE_RAW function block

The M-BUS web pages lets you scan the bus, searching for devices, detecting either their primary addresses or secondary addresses; it also lets you read the data records and slave information from a device and create the configuration files to be imported in Straton PLC.

The **MBUS_READ_CTL** FB lets you start/stop the M-BUS acquisition;

the MBUS_WRITE_RAW FB lets you build and send a generic M-Bus frame, thus providing a flexible way to send configuration commands to M-Bus devices.

16 OPC Unified Architecture (OPC UA) protocol

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

OPC UA is a vendor-independent communication protocol and it's based on the client-server principle with a robust security.

The devices support both OPC-UA server and OPC-UA client protocols.

17 MQTT client protocol

The MQTT is the most used protocol for IOT applications:

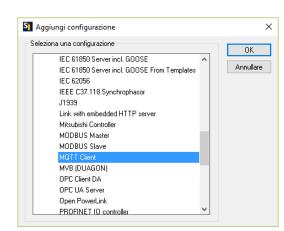
"MQTT stands for MQ Telemetry Transport. It is a publish/subscribe, extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, highlatency or unreliable networks. The design principles are to minimise network bandwidth and device resource requirements whilst also attempting to ensure reliability and some degree of assurance of delivery. These principles also turn out to make the protocol ideal of the emerging "machine-to-machine" (M2M) or "Internet of Things" world of connected devices, and for mobile applications where bandwidth and battery power are at a premium".

For more info on MQTT protocol see http://mqtt.org/



The MQTT version supported by the Z-PASS1/2 is the 3.1.1

For using the MQTT protocol *you must use Straton workbench 9.3 or later*.



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

17.1 MQTT protocol Parameters from PLC program

The MQTT setup can be made directly from the workbench:

Proprietà	Valore	OK
Connection ID		
▲ Server		Annulla
Address		Guida
IP Port	1883	
🖌 Login		
Client ID		
User name		
Password		
 Options 		
Keep Alive timer	(sec) 10	
Clean session		
Buffer size	4096	
 Will message 		
Topic name		~

But if you need to configure these parameters from the Straton PLC Program you can use a set of special words that will load the configuration from a file.

Special Words are:

In the filed "Address" type: mqtt_par_address so the filed "Address" is obtained from the file:

/var/run/mqtt_par_address

In the filed "Client ID" type: mqtt_par_clientid so the filed "Client ID" is obtained from the file:

/var/run/mqtt_par_clientid

In the filed "User Name" type: mqtt_par_username so the filed "User Name" is obtained from the file:

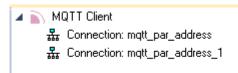
/var/run/mqtt_par_username

In the filed "Password" type: mqtt_par_password so the filed "Password" is obtained from the file:

/var/run/mqtt_par_password

17.1.1 Manage Multiple MQTT connections

You can manage multiple MQTT connections using parameters *that starts with the special words* (*mqtt_par_address123, mqtt_par_address_aaa, ...*), for example create 2 mqtt connections:



The first connection use the Field address "mqtt_par_address"



So will load the Address from the file:

/var/run/mqtt_par_address

The second connection use the Filed 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 others parameters client id, username and password).

17.2 MQTT with SSL/TLS Connection retry configuration

The default configuration for the MQTT SSL/TLS connection is:

CONN _TRY_MAX = 10

CONN_TRY_WAIT = 1000 ms

Where:

CONN _TRY_MAX is the number of retry for the connection.

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/run/"

Whith the values of parameters, for example:

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

50,200

Means that CONN_TRY_MAX = 50 and CONN_TRY_WAIT = 200 ms.

NOTE1: At the end of the file you need to add $a \ln (newline character)$

NOTE2: The file is loaded in a RAM filesystem so you need to create it at each boot.

17.3 MQTT static and dynamic Client Certificates

In the MQTT configuration Under Security section you can enter the path and the filename for the certificates:

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

Seneca suggests to use the /log directory for the certificates.

MQTT Client certificate can be upload only by the FTP server.

The Key file is the client private key file.

Certificate file is the client certificate.

Certificate Authority file is the Certification Athority certificate.

If you need to change dynamically these files and others parameters without recompiling the project you can load in /var/run directory a file with filename that must starts respectively with:

"mqtt_par_clientkey", "mqtt_par_clientcert", "mqtt_par_cacert"

The contents of the files must be a text with the file name without the path.

Note that in a program you can use more than one certificate file for example "mqtt_par_clientcert00", "mqtt_par_clientcert01" etc...

17.4 Change MQTT parameters from a file

You can change the port and the keepalive configuration overwriting in runtime the actual configuration with the following files:

"mqtt_par_port" and "mqtt_par_keepalive".

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

18 Upgrading the firmware by USB pen

The Device firmware can be upgraded by means of a USB pen; a pen drive formatted with FAT32 filesystem is needed.

The procedure is the following:

1) download the FW file from one of the following links:

http://www.seneca.it/products/z-tws4 http://www.seneca.it/products/z-pass2-s http://www.seneca.it/products/s6001-rtu

the downloaded file is a .zip file; extract the FW file from it; the FW file shall have a name like the following:

SW002940_xxx.bin

- 2) copy the file into the root of the USB pen
- 3) switch off the Device
- 4) insert the USB pen into the USB#1 port
- 5) switch on the Device; the upgrade procedure will take some minutes to be completed; during this time, the Device MUST NOT be switched off; during the procedure, the Device will be rebooted several times; also, during the procedure, several LEDS will blink simultaneously⁸
- 6) the upgrade procedure is ended when only the LED "RUN" is blinking⁹
- 7) remove the USB pen

19 Web Configuration Pages

NOTE: in this chapter, the web pages screen-shots are shown for only one of the products (Z-TWS4, Z-PASS2-S, Z-PASS2-S-R01, Z-PASS2-S-IO, S6001-RTU); the pages for the other products are identical, except

⁸ This applies only to products with HW revisions IO and R01; in details: for IO HW revision, all LEDs will blink simultaneously, except for Power, LAN/WAN, COM and modem LEDs; for R01 HW revision, RUN, VPN and SERV LEDs will blink.

⁹ Also SERV and VPN LEDs might blink, depending on the Device configuration and status.

for the product name shown in the top of the pages and for some details explained in the following paragraphs.

Furthermore, for S6001-RTU one more page ("I/O View") is available.

19.1 Administrator pages

The Device can be fully configured by means of a set of web configuration pages.

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

http://192.168.90.101:8080¹⁰

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

Username: admin Password: admin

You come to the "Main View" page, described in the following paragraph.

¹⁰ The default 80 HTTP port has been left available for customer pages.

19.1.1 Main View

🗋 Z-PASS2-S	×	😲 Giovanni	-		×
← → C 🛈 1	92.168.85.104:8080/index.php		Q	☆ 🔎	
SENFC A	Z-PASS2-S				
	Main View [user: admin] [logout]				
General Configuration					
Main View	Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G]				
Network and Services	MAC Address: C8F9811B0000 [IMEI: 861075026600976] [IMSI: 222101600237890]				
Real Time Clock Setup					
VPN Configuration	Internet Access: Mobile				
Router Configuration	Energy Protocols: none				
Users Configuration	DI C Statuar munning (annu 2002)				
FW Upgrade	PLC Status: running (app: s203)				
	Router: running				
Conf. Management Mobile Configuration					
Mobile Network	NETWORK				
	Ethernet Mede LANAVAN				
DDNS Configuration Digital I/O	Ethemet Mode LANWAN DHCP on WAN OFF				
Digital I/O Configuration	LAN IP Address 192.168.90.101				
Diagnostics	LAN Network Mask 255.255.255.0				
FW Versions	WAN IP Address 192.168.85.104				
	WAN Network Mask 255.255.252.0				
Ethernet Interfaces	Default Gateway 10.64.64.64				
Modbus Modules	DNS Mode Static				
Data Logger (SD found)	DNS Server 83.224.65.143 83.224.65.134				
Logs	IP Configuration from Discovery ON				
	WEB SERVER				
	Protocol HTTP/HTTPS				
	HTTP Conf Port 8080				
	HTTP User Port 80				
	HTTPS Port 443				
	FILE TRANSFER				
	Protocol FTP/SFTP				
	FTP Port 21				
	SFTP Port 22				
	PLC				
	Straton TCP Port 502				
	Straton Redundancy Enable OFF				
	Straton Redundancy IP Address 192.168.90.102				
	License Key 1122334455667788				
	NTP				
	Enable ON				
	Primary Server ntp1.inrim.it				
	Secondary Server ntp2.inrim.it				
	Time Zone Central Europe (CET/CEST)				
	VPN				
	Mode VPN Box				
	Enable OFF				
	Server 192.168.90.1				
	Password seneca				
	Tag Name zpass2s				
	MOBILE NETWORK				
	Enable ON APN Mode Manual				
	APN Mode Manual APN m2mbis.vodafone.it				
	Authentication Type None				
	Usemane user				
	Password pass				
	PIN 8342				
	Ping Connection Testing IP Address www.google.com				
	NETWORK REDUNDANCY				
	Enable OFF				

In this page, main Device configuration parameters are shown, with their current values.

On the left side of the page, like in all the other pages, a menu is shown which lets you access all the configuration pages; the menu is divided in several sections:

- General Configuration
- Mobile Configuration (not available on Z-TWS4 and Z-TWS4-IO)
- Digital I/O (on Z-PASS2-S-IO, Z-TWS4-IO products)
- Diagnostics
- Data Logger

In S6001-RTU, a "S6001-RTU" section is also present.

On top of the page, like in all the other pages, the following information are shown:

- the page name
- the FW version, along with the modem FW revision, for Z-PASS2-S/S6001-RTU; for S6001-RTU, the FW version of the I/O board is also shown
- the MAC address; the modem IMEI, for Z-PASS2-S/S6001-RTU; the SIM IMSI, for Z-PASS2-S/S6001-RTU, when a SIM is present
- the network interface used for Internet Access (i.e.: "Ethernet" or "Mobile")
- which energy protocols are enabled (on a license base)
- the Soft PLC status (i.e.: "running" or "stopped"); if the PLC application execution is stopped or no application is loaded on the Device, the status "app not running" is also shown; if the PLC application is running, the name of the application is also shown
- the Router status (i.e.: "running" or "disabled")

The currently logged user (e.g.: "admin") and the "Logout" link are also present, near the page name.

In this page, the following buttons are available:

- "RESTART", to perform the Device reboot
- "FACTORY DEFAULT", to reset the Device to its factory state
- "CLEAN INTERNAL DATA LOGS", to delete internal data log files (this does not affect the data log files stored on the SD card, see paragraph 19.1.18)

Probably, the first parameters you need to change when setting up a new Device are those related to its network configuration.

You can accomplish this in the "Network and Services" page, described in the following paragraph.

19.1.2 Network and Services

The parameters shown in this page slightly change, depending on the HW version of the product (Z-TWS4/Z-PASS2-S or Z-PASS2-S-R01 or Z-TWS4-IO/Z-PASS2-S-IO) and, for new HW versions, on the selected "Ethernet Mode"; this is shown in the following figures.

🗋 Z-PASS2-S	×			(!) Covend	_			×
\leftrightarrow \Rightarrow C ()	192.168.85.104:8080/setup.php				Q	☆	J.	:
SENECA General Configuration Vain View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade	Z-PAS82-8 Network and Services [user: admin] [logout Firmware Version: 8W002940_331 [Modem: MAC Address: C8F9811B0000 [IMEI: 861079 Internet Access: Mobile Energy Protocols: none PLC Status: running (app: zpass2s_io) Router: disabled	UC20GQBR03A1	-					
Conf. Management								_
Mobile Configuration		CURRENT	UPDATED					
Mobile Network Digital I/O	NETWORK							
Digital I/O Configuration	Ethernet Mode (*)	Switch	Switch T					
Diagnostics	DHCP		OFF V					
FW Versions	IP Address	192.168.95.104	192.168.95.104					
Ethernet Interfaces	Network Mask	255.255.255.0	255.255.255.0					
Modbus Modules	IP Address 2 Enable	ON	ON V					
Data Logger (SD missing)	IP Address 2	192.168.85.104	192.168.85.104					
	Network Mask 2	255.255.252.0	255.255.252.0					
	Default Gateway		192.168.85.1					
	DNS Mode		Static V					
		192.168.84.113	192.168.84.113					
	IP Configuration from Discovery		ON V					
			UN T					
	WEB SERVER							
	Protocol (*)		HTTP V					
	HTTP Conf Port (*)		8080					
	HTTP User Port (*)	8082	8082					
	HTTPS Port (*)	8043	8043					
	FILE TRANSFER							
	Protocol	FTP/SFTP	FTP/SFTP V					
	FTP Port		21					
	SFTP Port		22					
	LOG FOLDER SHARING							
	Enable	ON	ON V					
	PLC							
	Straton TCP Port	502	502					
	Straton Redundancy Enable	OFF	OFF V					
	Straton Redundancy IP Address		192.168.90.102					
	License Key	1122334455667788	1122334455667788					
	NETWORK REDUNDANCY							
	Enable		OFF V					
	Ping Address		8.8.4.4					
	WATCHDOG							
	Enable (*)	ON	ON V					
	Timeout (8)	60	60					
	DEBUG LOGS							
	Enable	UN	ON V					
	СОМ							
	Mode	RS232	RS232 ¥					
	NOTE: changing fields marked with * will cause a							

The previous figure shows the "Network and Services" page for a Z-PASS2-S-IO, when the "Ethernet Mode" parameter is set to "Switch"; it also applies to a Z-TWS4-IO in "Switch" mode.

🗋 Z-PASS2-S	×			() Ciovanni	- 0	×
\leftrightarrow \Rightarrow C ()	192.168.85.104:8080/setup.php				९ 🛧 🗵	:
SENECA General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration	Z-PA882-8 Network and Services [user: admin] [logout Firmware Version: 8W002940_331 [Modem: MAC Address: C8F9811B0000 [IMEI: 861075 Internet Access: Mobile	UC20GQBR03A1	-			
Router Configuration Users Configuration FW Upgrade	Energy Protocols: none PLC Status: running (app: zpass2s_io) Router: disabled					
Conf. Management						
Mobile Configuration Mobile Network		CURRENT	UPDATED			
Digital I/O	NETWORK	r				
Digital I/O Configuration	Ethernet Mode (*)	LAN/WAN	LAN/WAN V			
Diagnostics	DHCP on WAN	OFF	OFF V			
FW Versions	LAN IP Address	192.168.95.104	192.168.95.104			
Ethernet Interfaces	LAN Network Mask	255.255.255.0	255.255.255.0			
Vodbus Modules Data Logger (SD missing)	WAN IP Address	192.168.85.104	192.168.85.104			
oura cogger (oo moonig)	WAN Network Mask	255.255.252.0	255.255.252.0			
	Default Gateway	192.168.85.1	192.168.85.1			
	- DNS Mode	Static	Static V			
	DNS Server	192.168.84.113	192.168.84.113			
	IP Configuration from Discovery	ON	ON V			
	WEB SERVER					
			HTTP V			
	Protocol (*)		HTTP V 8080			
	HTTP Conf Port (*)					
	HTTP User Port (*)		8082			
	HTTPS Port (*)	8043	8043			
	FILE TRANSFER					
	Protocol	FTP/SFTP	FTP/SFTP V			
	FTP Port	21	21			
	SFTP Port	22	22			
	LOG FOLDER SHARING					
	Enable		ON Y			
			UN V			
	PLC					
	Straton TCP Port		502			
	Straton Redundancy Enable	OFF	OFF V			
	Straton Redundancy IP Address	192.168.90.102	192.168.90.102			
	License Key	1122334455667788	1122334455667788			
	NETWORK REDUNDANCY	•				
	Enable	OFF	OFF V			
	Ping Address	8.8.4.4	8.8.4.4			
	WATCHDOG					
	Enable (*)		ON V			
	Timeout (8)	60	80			
	DEBUG LOGS					
	Enable	ON	ON V			
	COM1					
		RS232	RS232 V			
	NOTE: changing fields marked with * will cause a					
	system restart.					
			ADDLY			

The previous figure shows the "Network and Services" page for a Z-PASS2-S-IO, when the "Ethernet Mode" parameter is set to "LAN/WAN" it also applies to a Z-TWS4-IO in "LAN/WAN" mode.

Th Z-PASS2-S	×			(!) Ciovanni	_		×
						•	
$\epsilon \rightarrow C$ (1) 19	2.168.85.106:8080/setup.php				Q	☆ 🗵	:
General Configuration Main View Network and Services	Z-PASS2-S Network and Services [user: admin] [logout] Firmware Version: SW002940_331 [Modem: 1		E]				-
Real Time Clock Setup	MAC Address: C8FA81160002 [IMEI: 8622640	20406716]					
VPN Configuration	Internet Access: Ethernet						
Router Configuration Users Configuration	Energy Protocols: none						
FW Upgrade	PLC Status: running (app: zpass2s_r01_8)						- 1
Conf. Management	Router: running						- 1
Mobile Configuration Mobile Network		CURRENT	UPDATED				
Diagnostics	NETWORK						
FW Versions	Ethernet Mode (*)	Switch	Switch V				
Ethernet Interfaces Modbus Modules	DHCP	OFF	OFF V				
Data Logger (SD missing)	IP Address	192.168.95.106	192.168.95.106				
	Network Mask		255.255.255.0				
	IP Address 2 Enable		ON V				
	IP Address 2 Network Mask 2	192.168.85.106	192.168.85.106				
	Default Gateway		255.255.252.0 192.168.85.1				
	Disadit Galeway DNS Mode		Static V				
		192.168.84.113	192.168.84.113				
	IP Configuration from Discovery	ON	ON V				
	WEB SERVER						
	Protocol (*)	нттр	HTTP V				
	HTTP Conf Port (*)	8080	8080				
	HTTP User Port (*)	80	80				
	HTTPS Port (*)	443	443				
	FILE TRANSFER						
	Protocol	FTP/SFTP	FTP/SFTP ▼				
	FTP Port	21	21				
	SFTP Port	22	22				
	LOG FOLDER SHARING						
	Enable	ON	ON V				
	PLC						
	Straton TCP Port		502				
	Straton Redundancy Enable		OFF V				
	Straton Redundancy IP Address		192.168.90.102				
			1122334455667788				
	NETWORK REDUNDANCY						
	Enable Ping Address		OFF V				
			8.8.4.4				
	WATCHDOG Enable (?)		01				
	Enable (*) Timeout (8)		ON V				
	DEBUG LOGS		~~				
	Enable		ON V				
	NOTE: changing fields marked with * will cause a						-

The previous figure shows the "Network and Services" page for a Z-PASS2-S-R01, when the "Ethernet Mode" parameter is set to "Switch".

🗋 Z-PASS2-S	×			(!) Ciovanni	-			×
\leftrightarrow \rightarrow C (i) 19	92.168.85.106:8080/setup.php				Q	☆	J.	
SENECA"	Z-PASS2-S							
General Configuration	Network and Services [user: admin] [logout]							
Aain View	Firmware Version: SW002940_331 [Modem: 1	231B02SIM5350	FI					
letwork and Services			-1					
Real Time Clock Setup	MAC Address: C8FA81160002 [IMEI: 8622640	20406716]						
PN Configuration	Internet Access: Ethernet							
Router Configuration	Energy Protocols: none							
Jsers Configuration	PLC Status: running (app: zpass2s_r01_8)							
FW Upgrade	Router: running							
Conf. Management								
Mobile Configuration Mobile Network		CURRENT	UPDATED					
Diagnostics	NETWORK							
W Versions	Ethernet Mode (*)	LAN/WAN	LAN/WAN V					
Ethernet Interfaces	DHCP on WAN		OFF V					
Modbus Modules	LAN IP Address		192.168.95.106					
Data Logger (SD missing)	LAN Network Mask		255.255.255.0					
	WAN IP Address							
			192.168.85.106					
	WAN Network Mask		255.255.252.0					
	Default Gateway		192.168.85.1					
	DNS Mode		Static V					
		192.168.84.113	192.168.84.113					
	IP Configuration from Discovery	ON	ON V					
	WEB SERVER							
	Protocol (*)	нттр	HTTP 🔻					
	HTTP Conf Port (*)	8080	8080					
	HTTP User Port (*)	80	80					
	HTTPS Port (*)	443	443					
	FILE TRANSFER							
		FTP/SFTP	FTP/SFTP V					
	FTP Port							
	SETP Port		21					
			22					
	LOG FOLDER SHARING							
	Enable	ON	ON V					
	PLC							
	Straton TCP Port	502	502					
	Straton Redundancy Enable		OFF T					
	Straton Redundancy IP Address		192.168.90.102					
		1122334455667788	1122334455667788					
	NETWORK REDUNDANCY							
			055 -					
	Enable		OFF V					
	Ping Address		8.8.4.4					
	WATCHDOG							
	Enable (*)	ON	ON V					
	Timeout (8)	60	60					
	DEBUG LOGS							
	Enable		ON T					
	NOTE: changing fields marked with * will cause a							
	system restart.							

The previous figure shows the "Network and Services" page for a Z-PASS2-S-R01, when the "Ethernet Mode" parameter is set to "LAN/WAN".

[] S6001-RTU	×			(!) Clovenni	_		×	
	2.168.85.106:8080/setup.php				Q	☆	<u>,</u>	
General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration	S6001-RTU Network and Services [user: admin] [logout] Firmware Version: SW002940_331 [I/O: SW00 MAC Address: C8F981000198 [IMEI: 8622640 Internet Access: Ethernet		231B02\$IM6360E]					•
Router Configuration Users Configuration FW Upgrade Conf. Management	Energy Protocols: none PLC Status: running (app: znet_s6001_2) Router: running							
Mobile Configuration Mobile Network		CURRENT	UPDATED					
S6001-RTU	NETWORK							
I/O View	DHCP		OFF T					
Diagnostics		192.168.85.106	192.168.85.106					
FW Versions								
Ethernet Interfaces	Network Mask IP Address 2 Enable		255.255.255.0					
Modbus Modules Data Logger (SD missing)			OFF ▼					
		192.168.100.101	192.168.100.101					
	Network Mask 2		255.255.255.0					
	Default Gateway		192.168.85.1					
	DNS Mode		Static V					
		192.168.84.113	192.168.84.113					
	IP Configuration from Discovery	ON	ON V					
	WEB SERVER							
	Protocol (*)	HTTP/HTTPS	HTTP/HTTPS ▼					
	HTTP Conf Port (*)	8080	8080					
	HTTP User Port (*)	80	80					
	HTTPS Port (*)	443	443					
	FILE TRANSFER							
	Protocol	FTP/SFTP	FTP/SFTP V					
	FTP Port		21					
	SFTP Port		22					
			22					
	LOG FOLDER SHARING							
	Enable	ON	ON V					
	PLC							
	Straton TCP Port	502	502					
	Straton Redundancy Enable	OFF	OFF V					
	Straton Redundancy IP Address	192.168.90.102	192.168.90.102					
	License Key	1122334455667788	1122334455667788					
	NETWORK REDUNDANCY							
	Enable		OFF T					
	Ping Address		8.8.4.4					
			0.0.7.7					
	WATCHDOG							
	Enable (*)		ON V					
	Timeout (s)	60	60					
	DEBUG LOGS							
	Enable	ON	ON V					
	NOTE: changing fields marked with * will cause a system restart.							Ŧ

The previous figure shows the "Network and Services" page for a S6001-RTU; it also applies to a Z-TWS4 and Z-PASS2-S (old version).

There is an important difference between the parameter values shown in this page and those shown in the "Main View" page: the former are <u>configured</u> values, whereas the latter are <u>actual</u> values.

To better explain this difference, let's consider the case when the DHCP parameter is set to ON; in the "Network and Services" page, you may see the 192.168.90.101 default value for the "IP Address" parameter, whereas the "Main View" page shows the actual IP Address, assigned by the DHCP server.

In the following table, all configuration parameters available in the page are listed, with a short explanation and the parameter default value for each of them.

Field	Meaning	Default value
NETWORK/Ethernet Mode	MeaningThis parameter determines if the two Ethernet ports work as two fully separated network interfaces ("LAN/WAN") or as the ports of an Ethernet switch ("Switch"); depending on the value of this parameter, some other network parameters are hidden/shown or renamed as described below.This parameter is available only for Z-PASS2-S-RO1, Z-PASS2-S-IO and Z-TWS4-IO products. For all other products, only "Switch" mode is available, hence the parameter is not shown.	LAN/WAN
Ethernet Mode = "Switch"		
NETWORK/DHCP NETWORK/IP Address	Flag to enable/disable the DHCP functionality on the Ethernet interface.IP address of the Ethernet interface	OFF 192.168.90.101
	(disabled when "DHCP" is set to "ON")	
NETWORK/Network Mask	Network mask of the Ethernet interface (disabled when "DHCP" is set to "ON")	255.255.255.0
NETWORK/IP Address 2 Enable	Flag to enable/disable the second IP address on the Ethernet interface. Note that the second IP address can be enabled also when the DHCP functionality is active.	OFF
NETWORK/IP Address 2	Second IP address of the Ethernet interface	192.168.100.101
NETWORK/Network Mask 2	Second network mask of the Ethernet interface	255.255.255.0
Ethernet Mode = "LAN/WAN"		
NETWORK/DHCP on WAN	Flag to enable/disable the DHCP	ON

[
	functionality on the WAN Ethernet interface	
NETWORK/LAN IP Address	IP address of the LAN Ethernet	192.168.90.101
	interface	
NETWORK/LAN Network Mask	Network mask of the LAN Ethernet	255.255.255.0
	interface	
NETWORK/WAN IP Address	IP address of the WAN Ethernet	192.168.100.101
	interface (disabled when "DHCP on	
	WAN" is set to "ON")	
NETWORK/WAN Network Mask	Network mask of the WAN	255.255.255.0
	Ethernet interface (disabled when	
	"DHCP on WAN" is set to "ON")	
NETWORK/Default Gateway	Default Gateway IP address	192.168.100.1 , for Z-TWS4-R0x
NETWORK/Default Galeway	Default Gateway IP address (disabled when DHCP functionality	and Z-PASS2-S-R0x (x=1,2)
	is enabled on any interface).	192.168.90.1, for all other
	When "Ethernet Mode" is set to	products
	"LAN/WAN", the Default Gateway	
	shall be in the WAN subnet.	
NETWORK/DNS Mode	Tells if the DNS Server shall be set	DHCP, for Z-TWS4-R0x and Z-
	statically (value: "Static") or	PASS2-S-R0x (x=1,2)
	dinamically assigned by the DHCP	Static, for all other products
	Server (value: "DHCP")	
NETWORK/DNS Server	DNS server IP address (disabled	192.168.100.1 , for Z-TWS4-R0x
	when DHCP functionality is enabled	and Z-PASS2-S-R0x (x=1,2)
	on any interface and DNS Mode =	192.168.90.1, for all other
	DHCP)	products
NETWORK/IP Configuration from	Flag to enable/disable the	ON
Discovery	possibility of changing some of the	
	network configuration parameters by means of the SDD application	
	(see chapter 6)	
WEB SERVER/Protocol	Protocol used to access the web	HTTP/HTTPS
	pages:	
	HTTP/HTTPS, HTTPS, HTTP	
WEB SERVER/HTTP Conf Port	TCP port to access the	8080
	configuration pages, using HTTP	Default URL for conf pages:
	protocol.	Errore. Riferimento a
	Please note that if this parameter is	collegamento ipertestuale non
	set to 80 (standard HTTP port), the	valido.
	web user site won't be available	
	anymore.	
WEB SERVER/HTTP User Port	TCP port to access the user pages,	80
	using HTTP protocol.	Default URL for user pages:
		Errore. Riferimento a

		collegamento ipertestuale non valido.>
WEB SERVER/HTTPS Port	TCP port to access the configuration and user pages, using HTTPS protocol.	443Default URL for conf pages:Errore.Riferimentoacollegamentoipertestualenonvalido.Default URL for user pages:Errore.Riferimentoacollegamentoipertestualenonvalido.
FILE TRANSFER/Protocol	Protocol used for File Transfer: FTP/SFTP, SFTP, FTP	FTP/SFTP
FTP Port	TCP Port for FTP protocol	21
SFTP Port	TCP Port for SFTP protocol	22
LOG FOLDER SHARING/Enable	Flag to enable/disable the sharing of the "/log" directory (by means of "Samba" service)	ON
PLC/Straton TCP Port	TCP port to connect to the Straton server	502
PLC/Straton Redundancy Enable	Flag to enable/disable the Straton Redundancy functionality	OFF
PLC/Straton Redundancy IP Address	IP address of the second Device used for Straton Redundancy	192.168.90.102
PLC/License Key	Key to enable/disable Energy Protocol functionalities in Straton (see paragraph 8.2)	1122334455667788 (dummy value) ¹¹
NETWORK REDUNDANCY/Enable	Flag to enable/disable the "Network Redundancy" functionality, that is using the Ethernet interface as the primary interface to access the Internet and the Mobile interface as the secondary interface, if the access through the primary interface becomes unavailable	OFF
NETWORK REDUNDANCY/Ping Address	IP Address used as ping destination to check if access to the Internet through the primary interface (Ethernet) is available. This address shall be different from the one set for "DNS Server"	8.8.4.4

¹¹ The correct License Key string is provided by Seneca.

parameter, otherwise an error is	
shown.	
Flag to enable/disable the	ON
watchdog functionality	
Watchdog timeout, in seconds;	60
when watchdog is enabled, if it's	
not refreshed for this amount of	
seconds, the system will be	
rebooted.	
Possible values are in the range	
[303600].	
Flag to enable/disable the debug	OFF
logs	
Operating mode of the COM1 serial	RS485
port; possible values: RS485,	
RS232, Z-MBUS (Meter Bus	
extension)	
RS232 and Z-MBUS parameters are	
available only for Z-TWS4-IO and Z-	
PASS2-S-IO products.	
	Flag to enable/disable the watchdog functionality Watchdog timeout, in seconds; when watchdog is enabled, if it's not refreshed for this amount of seconds, the system will be rebooted. Possible values are in the range [303600]. Flag to enable/disable the debug logs Operating mode of the COM1 serial port; possible values: RS485, RS232, Z-MBUS (Meter Bus extension) <u>RS232 and Z-MBUS parameters are available only for Z-TWS4-IO and Z-</u>

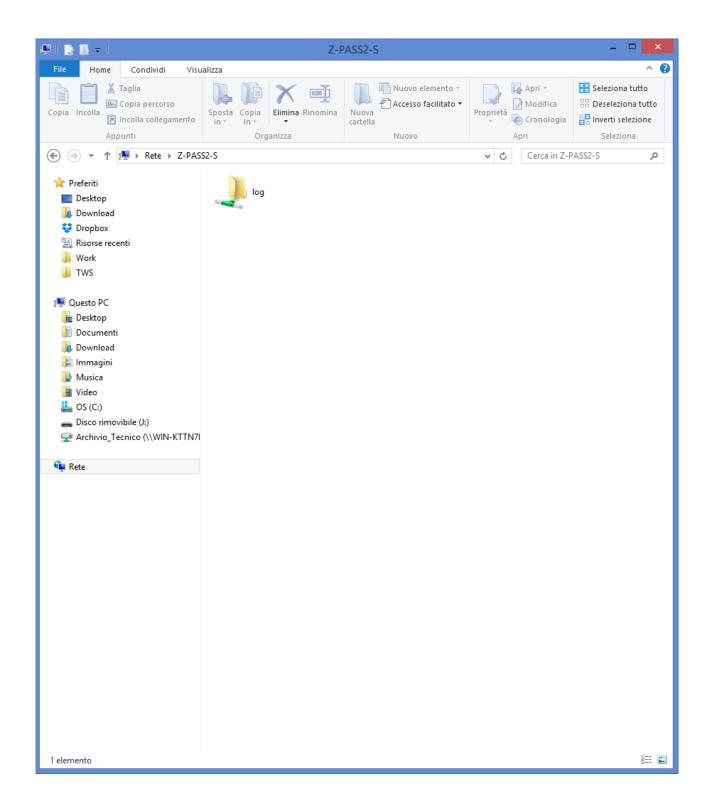
Some notes about the "DHCP" parameters:

- the "DHCP" parameter can be set to "ON" only if the "DHCP Server" parameter of the "Router Configuration" page is set to "OFF" (see paragraph 19.1.5);
- only the "DHCP on WAN" parameter can be set to "ON".

You can change any of the above parameters; to apply the changes, press the "APPLY" button; as warned by the note on the page, only for some parameters, the parameter change requires rebooting the Device; these parameters are:

- NETWORK/Ethernet Mode
- WEB SERVER/Port
- WATCHDOG/Enable, only when changing ON -> OFF
- DEBUG LOGS/Enable, only when changing ON -> OFF

If the "LOG FOLDER SHARING/Enable" parameter is ON, on a Windows PC, you can directly access the "/log" directory, as shown in the following pictures (the sharing name is equal to the product name, without '-' character, that is "ZPASS2S", "ZTWS4" or "S6001RTU"):



🖳 l 💫 🚹 = l		log		- 🗆 🗙
File Home Condividi Visu	alizza			<u>^</u>
Copia Incolla Copia Copia percorso	Sposta Copia in * Copia	Nuova elemento ▼ Nuova cartella	Proprietà	Seleziona tutto
Appunti	Organizza	Nuovo	Apri	Seleziona
🔄 🄄 🔻 ↑ 🖳 → Rete → Z-PAS	S2-S → log →		✓ 🖒 Cerca in log	م و
🛛 🔆 Preferiti	Nome	Ultima modifica	Тіро	Dimensione
E Desktop	퉬 conf	26/10/2015 13.56	Cartella di file	
🝺 Download	퉬 disk	27/10/2015 09.22	Cartella di file	
💱 Dropbox	퉬 tmp	27/10/2015 07.40	Cartella di file	
📃 Risorse recenti	🔠 .lmnt.log	27/10/2015 07.41	File LOG	5 KB
퉬 Work	🔝 .upgrade_firmware.log	27/10/2015 07.40	File LOG	2 KB
iii TWS	🔼 at_exec.log	27/10/2015 08.32	File LOG	115 KB
	at_exec.log.1	26/10/2015 17.12	File 1	293 KB
🛛 🖳 Questo PC	at_exec.log.2	26/10/2015 16.45	File 2	1.731 KB
🖻 膭 Desktop	at_exec.log.3	26/10/2015 16.30	File 3	1.690 KB
🖻 📗 Documenti	at_exec.log.4	26/10/2015 16.15	File 4	1.511 KB
> 🚺 Download	at_exec.log.5	26/10/2015 16.00	File 5	1.689 KB
> 崖 Immagini	<pre></pre> <pre></pre> <pre></pre>	27/10/2015 09.48	File LOG	121 KB
Musica	fb_exec_handler.log	27/10/2015 09.21	File LOG	2 KB
> 📑 Video	fb_exec_handler.log.1	27/10/2015 08.44	File 1	316 KB
> 📥 OS (C:)	fb_exec_handler.log.2	26/10/2015 16.45	File 2	1.362 KB
Disco rimovibile (J:)	fb_exec_handler.log.3	26/10/2015 16.30	File 3	1.158 KB
Archivio_Tecnico (\\WIN-KTTN7I	fb_exec_handler.log.4	26/10/2015 16.15	File 4	1.188 KB
	fb_exec_handler.log.5	26/10/2015 16.00	File 5	1,329 KB
🖓 📬 Rete	Mb_conf_handler.log	27/10/2015 09.21	File LOG	60 KB
A.	messages	27/10/2015 09.48	File	5 KB
	messages.0	27/10/2015 09.45	File 0	1.025 KB
	messages.1	26/10/2015 13.22	File 1	1.025 KB
	messages.2	26/10/2015 09.52	File 2	1.025 KB
	messages.3	26/10/2015 08.32	File 3	1.025 KB
	messages.4	23/10/2015 14.19	File 4	1.025 KB
	messages.5	22/10/2015 16.36	File 5	1.025 KB
	messages.6	21/10/2015 17.00	File 6	1.025 KB
	messages.7	20/10/2015 17.09	File 7	1.025 KB
	openvpn-status.log	27/10/2015 09.47	File LOG	1 KB
	E t5energy.log	27/10/2015 09.47	File LOG	122 KB
	t5energy.log.1	26/10/2015 16.45	File 1	405 KB
	t5energy.log.2	26/10/2015 16:30	File 2	356 KB
	t5energy.log.3	26/10/2015 16.15	File 3	355 KB
	t5energy.log.4	26/10/2015 16.00	File 4	395 KB
	t5energy.log.5	26/10/2015 15.45	File 5	394 KB
		20/10/2013 13:43	110.2	55 F KB
35 elementi				

Depending on the LAN configuration, a login may be needed to access the shared folder; if so, use the credentials shown in the following figure (username: "\guest", password: "" [empty]).

19.1.3 Real Time Clock Setup

By clicking on the "Real Time Clock Setup" link, in the "General Configuration" menu, you come to the following page:

Z-PASS2-S	×		(:) (Bovanni	-		×
← → C ① 192.168.8	5.106:8080/rtc.php				Ð	☆ 🛛	. :
SENECA General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration	Z-PASS2-S Real Time Clock Setup [user: admi Firmware Version: SW002940_331 MAC Address: C8FA81160002 [IME Internet Access: Ethernet	[Modem: 1231]		DE]			
Router Configuration	Energy Protocols: none						
Users Configuration	PLC Status: running (app: zpass2s	_r01_bis)					
FW Upgrade	Router: running						
Conf. Management							
Mobile Configuration Mobile Network		CURRENT		UPDA	TED		
Diagnostics	NTP						
FW Versions	Enable	ON	ON 🔻				
Ethernet Interfaces	Primary Server	ntp1.inrim.it	ntp1.inrim.i	t			
Modbus Modules	Secondary Server		ntp2.inrim.i	t			
Data Logger (SD missing)		Central Europe			TICE	CT) -	
	Time Zone	(CET/CEST)	Central Eu			51) •	
				APP	LY		
		RTC					
		YEAR 201	7	2017			
		MONTH Oct	ober	Octo	ber	Ŧ	
		DAY 05		05			
		HOUR 08		08			
		MINUTE 59		59			
		SECOND 05		05			
					SET (LOCK	
						2001	
•							

This page is made up of two sections: "NTP" and "RTC".

In the "NTP" section, you can change the parameters related to the Network Time Protocol and to the Time Zone, as listed in the following table:

Field	Meaning	Default value
NTP/Enable	Flag to enable/disable time	ON
	synchronization by means of NTP	
	protocol	
NTP/Primary Server	IP address or FQDN ¹² of the Primary	ntp1.inrim.it
	NTP Server	
NTP/Secondary Server	IP address or FQDN of the Secondary	ntp2.inrim.it
	NTP Server	
NTP/Time Zone	Time Zone	Central Europe (CET/CEST)

When the "Time Zone" parameter is set to "Central Europe (CET/CEST)" value, the Device automatically enables (CEST) / disables (CET) the "Daylight Saving Time" setting.

A large number of Time Zones are available, as partially shown in the following figure:

¹² FQDN: Fully Qualified Domain Name, e.g.: "pool.ntp.org".

 	🗋 Z-PASS2-S	×		(!) Ciovanni — 🗆	×
General Configuration General Configuration Real Time Clock Setup [Luser: admin] [logout] Firmware Version: SW002940_331 [Modem: 1231B02SIM5350E] MAC Address: C8FA81160002 [IMEI: 862264020406715] MAC Address: C8FA81160002 [IMEI: 862264020406715] Internet Access: Ethernet Energy Protocols: none PLC Status: running (app: zpass2s_r01_bis) Router: running Mobile Network Diagnostics FV Versions Ethernet Interfaces Modbus Modules Data Logger (8D missing) Real Time Zong Real Time	← → C ③ 192.168.8	5.106:8080/rtc.php		€ ☆	<u>الر</u>
Network and Services MAC Address: C8FA81160002 [IMEI: 862264020406715] Internet Access: Ethernet Energy Protocols: none PPL Configuration PLC Status: running (app: zpass2s_r01_bis) Router: running PLC Status: running (app: zpass2s_r01_bis) Router: running CURRENT UPDATED Mobile Configuration Abbie Network NP Secondary Server ntp1.inrim.it Internet Interfaces Primary Server Modules Secondary Server Data Logger (8D missing) Time Zon Central Europe (CET/CEST) UTC-10:00 Huawai UTC-09:00 Alaska UTC-09:00 Alaska UTC-07:00 Chinahua UTC-07:00 Chinahua UTC-07:00 Chinahua UTC-05:00 Bogota UTC-05:00 Haavaa UTC-05:00 Haavaa UTC-05:00 Rester Zone UTC-05:00 Rester Zone UTC-05:00 Rester Zone UTC-05:00 Haavaa UTC-05:00 Rester Zone UTC-05:00 Rester Zone UTC-05:00 Rester Zone UTC-05:00 Rester Zone UTC-04:00 Caitaba UTC-04:00 Caitaba UTC-04:00 Caitaba UTC-04:00 Caitaba UTC-04:00 Caitaba UTC-04:00 Caitaba <tr< td=""><td>-</td><td>Real Time Clock Setup [user: admin</td><td></td><td>02SIM5350E1</td><td></td></tr<>	-	Real Time Clock Setup [user: admin		02SIM5350E1	
VPN Configuration Energy Protocols: none PLC Status: running (app: zpass2s_r01_bis) FW Upgrade Conf. Management Mobile Configuration Wolgrade Conf. Management Mobile Network Diagnostics FW Versions Elternet Interfaces Modules Data Logger (SD missing) Secondary Server Time Zone Central Europe UTC-10:00 Huawai (CTC-10:00 Huawai UTC-00:00 Aleutian UTC-00:00 Central Zone UTC-00:00 Central Zone UTC-00:00 Eastern Zone UTC-05:00 Eastern Zone UTC-04:00 Cauada UTC-04:00 Cauada UTC-04:00 Aleutian UTC-04:00 Aleutian UTC-04:00 Aleutian UTC-04:00 Aleutian UTC-04:00 Cauada UTC-04:00 Cauada		MAC Address: C8FA81160002 [IME	-	-	
W Upgrade Router: running Mobile Configuration Mobile Configuration Mobile Configuration Mobile Network Diagnostics NTP W Versions Enable Stennet Interfaces Modules Modolus Modules Secondary Server Data Logger (SD missing) Time Zone Central Europe (CET/CEST) UTC-10:00 Huawai VECA 2017 ITIC - 09:30 Marquesas UTC-09:00 Alaska UTC-00:00 Alaska UTC-07:00 Alaska UTC-07:00 Anizona UTC-06:00 Havaai UTC-05:00 Bogota UTC-05:00 Bogota UTC-05:00 Bogota UTC-05:00 Havaai UTC-05:00 Havaai UTC-05:00 Havaai UTC-05:00 Bogota UTC-05:00 Havaai UTC-04:00 Asuncion UTC-04:00 Asuncion UTC-04:00 Caracas UTC-04:00 Caracas UTC-04:00 Caracas UTC-04:00 Alantic Coast					
Mobile Configuration Aobile Network CURRENT UPDATED Adobie Network NTP NTP Diagnostics NTP N W Versions Enable ON ON Ethernet Interfaces Primary Server ntp1.inrim.it ntp1.inrim.it Adobus Modules Secondary Server ntp2.inrim.it ntp2.inrim.it Data Logger (SD missing) Secondary Server ntp2.inrim.it UTC-10:00 Huawai Time Zone Central Europe (CET/CEST) UTC-10:00 Alaska UTC-09:00 Alaska UTC-09:00 Alaska UTC-09:00 Alaska UTC-09:00 Alaska UTC-07:00 Arizona UTC-05:00 Eastern Zone UTC-05:00 Bogota UTC-05:00 Bogota UTC-05:00 Indiana UTC-05:00 Indiana UTC-05:00 Havana UTC-05:00 Havana UTC-04:00 Caracas UTC-04:00 Cairacas UTC-04:00 Cairacas UTC-04:00 Cairacas UTC-04:00 Cairacas	-		_r01_bis)		
W Versiona Shernet Interfaces Aodbus Modules Data Logger (SD missing) Becondary Server Data Logger (SD missing) Becondary Server Time Zone Central Europe (CET/CEST) Brrc VEAR 2017 VIC-10:00 Huawai UTC-10:00 Huawai UTC-10:00 Aleutian UTC-09:00 Alaska UTC-09:00 Central Zone UTC-06:00 Central Zone UTC-06:00 Eastern Zone UTC-05:00 Indiana UTC-04:00 La Paz UTC-04:00 Alantic Coast	Mobile Configuration		CURRENT	UPDATED	
Aodbus Modules Data Logger (SD missing) Primary Server ntp1.inrim.it ntp2.inrim.it nt	0		ON	ON V	
Time Zone Central Europe (CET/CEST) UTC-10:00 Huawai RTC UTC-10:00 Huawai UTC-10:00 Aleutian UTC-09:30 Marquesas UTC-09:00 Alaska UTC-09:00 Alaska UTC-09:00 Alaska UTC-09:00 Alaska UTC-07:00 Chihuahua UTC-07:00 Arizona UTC-06:00 Central Zone UTC-06:00 Mexico City UTC-05:00 Bogota UTC-05:00 Bogota UTC-05:00 Indiana UTC-05:00 Havana UTC-05:00 Havana UTC-05:00 Havana UTC-05:00 Havana UTC-05:00 Havana UTC-05:00 Lastern Zone UTC-05:00 Havana UTC-04:00 Cuiaba UTC-04:00 Cuiaba UTC-04:00 La Paz UTC-04:00 Atlantic Coast				ntp1.inrim.it	
RTCUTC-10:00 HuawaiVTC-10:00 AleutianUTC-09:30 MarquesasUTC-09:00 AlaskaUTC-09:00 AlaskaUTC-08:00 Pacific CoastUTC-07:00 ArizonaOctorUTC-07:00 ChihuahuaUTC-06:00 Central ZoneUTC-06:00 Mexico CityMINUTE55UTC-05:00 BogotaSECOND15UTC-05:00 IndianaUTC-04:00 AsuncionUTC-04:00 AsuncionUTC-04:00 CaracasUTC-04:00 CaracasUTC-04:00 La PazUTC-04:00 Atlantic Coast)ata Logger (S D missing)		Central Europe	UTC-10:00 Huawai	
UTC-04:00 Santiago			YEAR 2017 MONTH Octo DAY 05 HOUR 08 MINUTE 55	UTC-10:00 Huawai UTC-10:00 Aleutian UTC-09:30 Marquesas UTC-09:00 Alaska UTC-08:00 Pacific Coast UTC-07:00 Arizona UTC-07:00 Chihuahua UTC-06:00 Central Zone UTC-06:00 Mexico City UTC-05:00 Bogota UTC-05:00 Eastern Zone UTC-05:00 Indiana UTC-05:00 Havana UTC-05:00 Havana UTC-04:00 Asuncion UTC-04:00 Caracas UTC-04:00 Cuiaba UTC-04:00 La Paz	

The "RTC" section of the page lets you manually change the Device date/time settings; since this makes sense only if NTP time synchronization is not enabled, when "NTP/Enable" parameter is "ON" the input fields and the "SET CLOCK" button are disabled and the parameters are only for viewing.

Instead, when "NTP/Enable" parameter is "OFF", the input fields in the "NTP" section are still enabled; this lets you change and save the parameter values, even if they are not actually used.

19.1.4 VPN Configuration

By clicking on the "VPN Configuration" link, in the "General Configuration" menu, you come to the following page:

The page has a different layout depending on the value of the "VPN Mode" parameter, which can be "OpenVPN" or "VPN Box" (for an explanation of these values, see chapter 10).

19.1.4.1 **OpenVPN**

The page is made up of two sections: "VPN Files" and "VPN Configuration".

The "VPN Files" section lets you load the files needed to configure Open VPN and establish a secure VPN connection; these files are described in the following.

19.1.4.1.1 Configuration File

This file shall contain all the information needed to configure the Open VPN behaviour; the main configuration options are¹³:

• if the Device shall act as a client or a server (typically, it will be a client)

¹³ For more information about Open VPN configuration options, please refer to the OpenVPN web page ("openvpn.net").

- the transport protocol (UDP or TCP)
- the server IP address/host name and port
- the files needed to perform authentication procedures
- etc.

This file has the *.ovpn* extension (in Windows systems) or *.conf* extension (in Linux systems); regardless of the original name, it will be renamed as *ovpn.conf* on the Device.

This is the only mandatory file, that is if this file has not been loaded on the Device, VPN can't be enabled.

As reminded in the web page, in options requiring a file argument, only the file name shall be given, with <u>no path</u>, as in the following example:

ca ca.crt OK

ca /home/config/vpn/ca.crt KO!

Other two important rules that shall be followed are:

- the "dev" option shall be: "dev tun0" or "dev tap0"
- the "log" option shall be omitted (so that, logs are written to syslog)

An example of a client configuration file is given in paragraph 19.1.4.1.7.

19.1.4.1.2 CA certificate

This file shall contain the Certification Authority (CA) certificate and has the .crt extension.

It is needed when the configuration file contains the "ca" option.

19.1.4.1.3 Client certificate

This file shall contain the client certificate and has the .crt extension.

It is needed when the configuration file contains the "cert" option.

19.1.4.1.4 Client key

This file shall contain the client key and has the .key extension.

It is needed when the configuration file contains the *"key"* option.

19.1.4.1.5 Additional file

This file can be of any type and may be needed for configuration options other than "ca", "cert" and "key".

More than one additional file can be loaded.

You can browse your PC to select the above files and send them to the Device by pressing the "UPLOAD" button.

Once the upload is done, a result page is shown like in the following figure.

WINDOW VPN Configuration [user: admin] [logout] Main View Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E] Network and Services MAC Address: C8FA81160002 Real Time Clock Setup Internet Access: Mobile
Router Configuration Energy Protocols: none Ugers Configuration PLC Status: running (app not running) Router: disabled Router: disabled Wobile Configuration Upload: CLIENT1a.ovpn Modbus Modules

You can check which VPN files are stored on the Device by clicking on the "SHOW VPN STATUS" button, as shown in the following figure (remember that the configuration file is renamed as "ovpn.conf"):

		🥵 Giovanni	- 0	Х
C Z-PASS2-S	×			
$\leftarrow \rightarrow \mathbf{C}$ \bigcirc 192	2.168.85.103:8080/vpn_files.php?showinfo=1		ର ☆	:
Seneral Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Mobile Configuration	Z-PASS2-S VPN Configuration [user: admin] [logout] Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E] MAC Address: C8FA81160002 Internet Access: Mobile Energy Protocols: none PLC Status: running (app not running) Router: disabled			
Mobile Network Diagnostics	CURRENT UPDATED	•		
Ethernet Interfaces				
Modbus Modules Data Logger (SD found)	VPN Mode OpenVPN OpenVPN			
Logs	VPN Files			
	Configuration File (.ovpn or .conf) NOTE 1: the file will be reader as ovpn.conf NOTE 2: in options requiring a file ("ca", "cert", "key" etc.), only filename must be specified (without path) CA certificate (.crt) Scegli file Nessun file selezionato Client certificate (.crt) Scegli file Nessun file selezionato Client key (.key) Scegli file Nessun file selezionato (.crt, .key, auth,) VPN Configuration			
	Enable OFF OFF •			
	APPLY HIDE VPN STATUS VPN Status Disconnected OpenVPN Status Stopped OPONVPN Status Stopped RX Packets / Bytes 0/0 TX Packets / Bytes 0/0 VPN Files (size in bytes) 0/0 NOTE: these files can be downloaded via FTP from 'home/config/vpn' directory. CLIENT1.crt (3600) CLIENT1.ret (3600) CLIENT1.key (912) ca.crt (1139) ovpn.conf (193) REFRESH			

As reminded by the web page, the VPN files can be downloaded from the Device, if needed, via FTP/SFTP; they can be found in the */home/config/vpn* directory, as shown in the following figure.

OpenVPN_Client - user@192.168.85.	.117 - WinSCP									-		>
ocale Seleziona File Comandi Sess	sione Opzioni Remo	oto Aiuto										
🐉 🎒 Coda 👻 拱 🚝 📚 Sincro	onizza 🗾 🧬 💽		Impostazioni trasferim	ento Prede	inito	- 🧬 -						
📮 user@192.168.85.117 📑 Nuova se	essione											
Desktop 🗾 🖻 🔽 🕴	🔶 - 🔶 - 🖹 🖻	a 🎧 🌮 😘				vpn 🔹 🚰 🖸	7 🔶 - 🔶 - 💼 🔁	🏫 🤔 🔝 Trova file	R.			
🖟 Upload 👻 📝 Modifica 👻 🚮	h 🕞 Proprietà 📑					Download 👻 📝 Modifica 👻	🗙 🚮 🕞 Proprietà 📑					
\Users\Spagiari\Desktop\OpenVPN_Cli						/home/config/vpn						
lome	Dimensi	Тіро	Modificato	Attr		Nome	Dimensi	Modificato	Diritti	Proprietario		
		Cartella superi	16/09/2016 15.56.06			t.,		20/09/2016 09.26.52	rwxr-xr-x	root		
a.crt	2 KB	Certificato di s	04/05/2015 09.30.28	а		a.crt	2 KB	20/09/2016 10.42.53	rw-rr	root		
CLIENT1.conf	1 KB	File CONF	06/09/2016 14.19.40	а		CLIENT1.crt	4 KB	20/09/2016 10.42.53	rw-rr	root		
CLIENT1.crt	4 KB	Certificato di s	04/05/2015 09.30.42	а		CLIENT1.key	1 KB	20/09/2016 10.42.53	rw	root		
CLIENT1.key	1 KB	File KEY	04/05/2015 09.30.40	а		vpn.conf	1 KB	20/09/2016 10.42.53	rw-rr	root		
CLIENT1a.conf	1 KB	File CONF	07/09/2016 08.26.05	а								
CLIENT1a.ovpn	1 KB	File OVPN	07/09/2016 08.26.05	а								
CLIENT2.crt	4 KB	Certificato di s	04/05/2015 09.30.44	а								
CLIENT2.key	1 KB	File KEY	04/05/2015 09.30.44	а								
CLIENT53.crt	4 KB	Certificato di s	04/05/2015 09.33.54	a								
CLIENT53.key	1 KB	File KEY	04/05/2015 09.33.52	a								
CLIENT54.ovpn	1 KB	File OVPN	06/05/2015 15.23.11	a								
						<						
3 di 15.504 B in 0 di 11						0 B di 5.844 B in 0 di 4						
									🔒 SF	тр-з 🗐	0.	.00.52

Is is possible to clear all the VPN files, by clicking on the "RESET" button; a pop-up will appear, requiring a confirmation:

	192.168.85.117:8080 dice:			×
¢	This will delete VPN files. Are you sure ?			
٤				
9		ОК	Annulla	
i,	,			

If VPN is enabled, the user is not allowed to delete VPN files, as warned by the following pop-up:

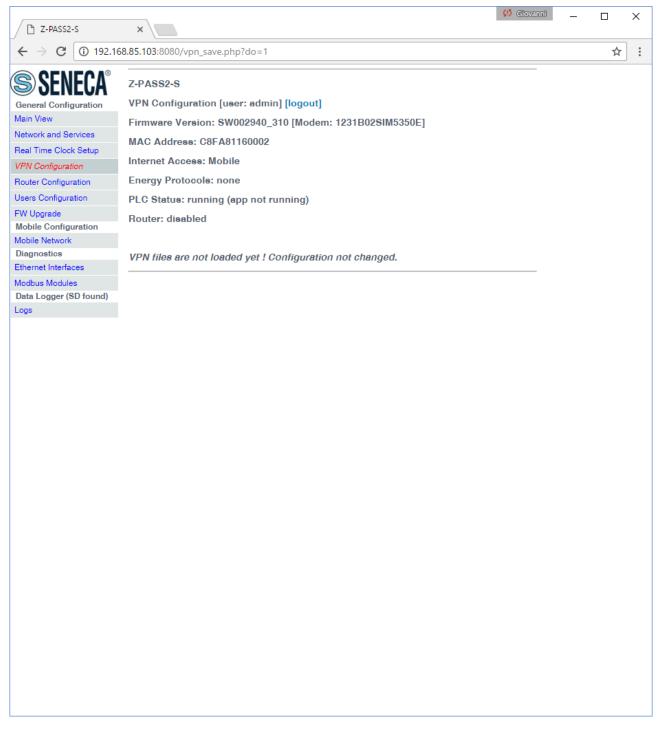
	192.168.85.117:8080 dice:	×	
	VPN is enabled: files can't be deleted.		
¢	ок		
\$	UK .		

In the "VPN Configuration" section, there is only one parameter, as described in the following table:

Field	Meaning	Default value
VPN Configuration/Enable	Flag to enable/disable the VPN	OFF
	connectivity; when enabled, the	

Device will run the Open VPN		
process with the loaded		
configuration		

As already told above, if you try to enable the VPN connectivity, but no configuration file has been uploaded to the Device yet, an error is given as shown in the following figure:



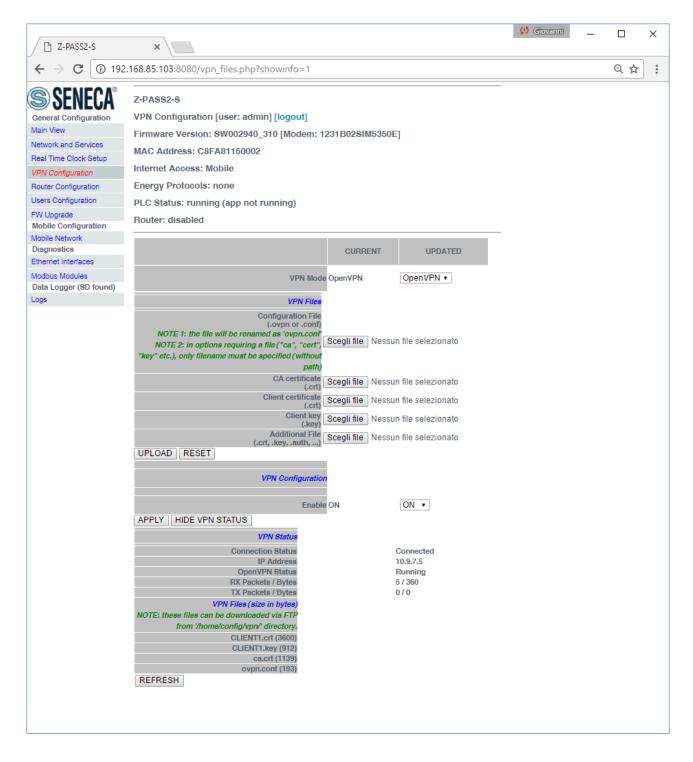
When you click on the "SHOW VPN STATUS" button, a third section appears, named "VPN Status", showing:

• the VPN "Connection Status" (i.e.: "Disconnected" or "Connected")

- 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 from 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
- the VPN files stored on the Device (see above)

as shown in the following couple of figures:

Pi Z-PASS2-S	×	😲 Giovanni	- 🗆 X
	2.168.85.103:8080/vpn_files.php?showinfo=1		९☆ :
S SENECA® General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Mobile Configuration	Z-PASS2-S VPN Configuration [user: admin] [logout] Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E] MAC Address: C8FA81160002 Internet Access: Mobile Energy Protocols: none PLC Status: running (app not running) Router: disabled		
Mobile Network Diagnostics Ethernet Interfaces	CURRENT UPDATED		
Modbus Modules Data Logger (SD found) Logs	VPN Mode OpenVPN OpenVPN • VPN Files Configuration File (.ovpn or .conf) Scegli file Nessun file selezionato NOTE 1: the file will be renamed as 'ovp.conf' Scegli file Nessun file selezionato NOTE 2: in options requiring a file ("ca", "cert", Scegli file Nessun file selezionato pdf) CA certificate (.crt) Scegli file Nessun file selezionato (.crt) Key Scegli file Nessun file selezionato (.crt) Scegli file Nessun file selezionato UPLOAD RESET VPN Configuration Scegli file Nessun file selezionato IPAddress OpenVPN status Stopped OpenVPN status NoTe: these files cane be downloaded via FTP trom 'home/config/vpn' directory. no file NOTE: these files cane be downloaded via FTP trom 'home/config/vpn' directory. no file <td></td> <td></td>		



An important status information is given by the "OpenVPN Status" field; <u>if VPN is enabled ("ON")</u>, <u>but this</u> <u>status is "Stopped"</u>, <u>Open VPN process could not be correctly started</u>: <u>probably</u>, <u>the configuration file</u> <u>contains some errors or</u>, <u>maybe</u>, <u>some options not supported by the Device Open VPN implementation</u>.

You can refresh the VPN status, by clicking on the "REFRESH" button.

Finally, you can hide the "VPN Status" section, by clicking on the "HIDE VPN STATUS" button.

19.1.4.1.6 OpenVPN Server configuration file

This paragraph gives an example of OpenVPN server configuration; this is the server configuration typically used with Z-TWS4/Z-PASS2-S/S6001-RTU devices.

```
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
```

19.1.4.1.7 OpenVPN Client configuration file

This paragraph gives an example of OpenVPN client configuration; this is the client configuration typically loaded on Z-TWS4/Z-PASS2-S/S6001-RTU devices.

```
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
```

19.1.4.1.8 LED signalling (Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO)

In Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO products, when VPN functionality is enabled in "OpenVPN" mode, the "SERV" and "VPN" LEDs give the following status information (see chapter 5):

LED	Status	Meaning
VPN Yellow	ON	VPN connection is working properly
	Blinking	VPN connection is not working properly

	OFF	VPN functionality is disabled
SERV Green	-	Not used

19.1.4.2 VPN Box

The page contains only ony section: "VPN Box", as shown in the following figure.

Z-PASS2-S	(!) Ciovanni —		×
← → C ① 192.16	3.85.106:8080/vpn_files.php	☆ 🗵	:
SERVECA® General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration	Z-PASS2-S VPN Configuration [user: admin] [logout] Firmware Version: SW002940_331 [Modem: 1231B02SIM5350E] MAC Address: C8FA81160002 [IMEI: 862264020406715] Internet Access: Ethernet Energy Protocols: none		
FW Upgrade	PLC Status: running (app: zpass2s_r01_qua)		
Conf. Management	Router: running		
Mobile Configuration Mobile Network Diagnostics	CURRENT UPDATED		
FW Versions Ethernet Interfaces	VPN Mode VPN Box VPN Box VPN Box VPN Box		
Ethernet Interfaces Modbus Modules	VPN Box		
Data Logger (SD missing)	Enable OFF OFF T		
	Server 194,184,235,246	7	
]	
	Tag Name zpass2s zpass2s		
	APPLY SHOW VPN STATUS		

The "VPN Box" section contains the following parameters:

Field	Meaning	Default value
VPN BOX/Enable	Flag to enable/disable the "VPN	OFF
	Box" functionality, that is the	
	procedure/protocol that lets the	

	Device setup the VPN, by interacting	
	with the "VPN Box" server (see "VPN	
	Box User Manual")	
VPN BOX/Server	IP address or FQDN of the "VPN Box"	192.168.90.1
	server	
VPN BOX/Password	Password to access the "VPN Box"	seneca
	server	
VPN BOX/Tag Name	Mnemonic name used to uniquely	zpass2s
	identify the Device; if the default	
	("zpass2s") value is left, the Device	
	will register as	
	"zpass2s_ <macaddress>" or</macaddress>	
	"ztws4_ <macaddress>" on the VPN</macaddress>	
	Вох	

When you click on the "SHOW VPN STATUS" button, a new section appears, named "VPN Status", showing:

- the VPN "Connection Status" (i.e.: "Disconnected" or "Connected")
- the IP address assigned to the VPN interface when "Connected", the "dummy" IP address "0.0.0.0" when "Disconnected"; this row is not shown for "Point-to-Point (L2)" VPN Box, since no IP address is assigned to the VPN interface
- 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 by the VPN interface, when connected; "0/0" when disconnected
- the "VPN Box Type", which can be "Point-to-Point", "Point-to-Point (L2)" or "Single LAN", if VPN Box is enabled
- the "VPN Box Status", if VPN Box is enabled
- the username of the connected user, if any

as shown in the following three figures:

🕒 Z-PASS2-S	() (etovanni)	- 🗆 ×
	58.85.103:8080/vpn_files.php?showinfo=1	☆ :
		μ.
SENELA	Z-PASS2-S	
General Configuration	VPN Configuration [user: admin] [logout]	
Main View	Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]	
Network and Services	MAC Address: C8FA81160002	
Real Time Clock Setup	Internet Access: Ethernet	
VPN Configuration		
Router Configuration	Energy Protocols: none	
Users Configuration	PLC Status: running (app not running)	
FW Upgrade Mobile Configuration	Router: disabled	
Mobile Network		
Diagnostics	CURRENT UPDATED	
Ethernet Interfaces		
Modbus Modules Data Logger (SD found)	VPN Mode VPN Box VPN Box V	
Logs	VPN Box	
	Enable OFF OFF T	
	Server 192.168.90.1 192.168.90.1	
	Password seneca seneca	
	Tag Name zpass2s zpass2s APPLY HIDE VPN STATUS	
	VPN Status	
	Connection Status Disconnected	
	IP Address 0.0.0.0	
	OpenVPN Status Stopped	
	RX Packets / Bytes 0 / 0	
	TX Packets / Bytes 0 / 0	
	REFRESH	

	💔 Giovanni	– 🗆 🗙
🗋 Z-PASS2-S	×	
$\boldsymbol{\leftarrow}$ \rightarrow C (i) 192.16	58.85.103:8080/vpn_files.php?showinfo=1	☆ :
SENECCA General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Mobile Configuration Mobile Network Diagnostics Ethernet Interfaces	Z-PASS2-S VPN Configuration [user: admin] [logout] Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E] MAC Address: C8FA81160002 Internet Access: Ethernet Energy Protocols: none PLC Status: running (app not running) Router: running UVPDATED	
Modbus Modules	VPN Mode VPN Box VPN Box VPN Box VPN Box	
Data Logger (SD found) Logs	VPN Box	
	EnableONONServer194.184.235.246PasswordlaboratoriolaboratoriolaboratorioTag Namezpass2sr01Zpass2sr01zpass2sr01APPLYHIDE VPN STATUSVPN StatusConnection StatusConnectedIP Address10.9.0.1OpenVPN StatusRunningRX Packets / Bytes26 / 3.3KTX Packets / Bytes31 / 26.1KVPN Box TypePoint-to-PointVPN Box StatusOK (Configured)REFRESH	

		🧭 Giovanni 💷 🗆 🗙
🗋 Z-PASS2-S	×	
$\epsilon \rightarrow c$ A Non side	curo bttps://192.168.85.104/maintenance/vpn_files	s.php?showinfo=1 ☆ 🗵 :
SERVECA® General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Conf. Management Mobile Configuration	Z-PASS2-S VPN Configuration [user: admin] [logout] Firmware Version: SW002940_330 [Modem: Ud MAC Address: C8F9811B0000 [IMEI: 86107502 Internet Access: Mobile Energy Protocols: none PLC Status: running (app: ppp_blocks) Router: running	-
Mobile Network		CURRENT UPDATED
Digital I/O Digital I/O Configuration Diagnostics	VPN Mode	VPN Box VPN Box V
Ethernet Interfaces	VPN Box	
Modbus Modules	Enable ON	ON V
Data Logger (SD found) Logs	Server 194.184.235.246	194.184.235.246
	Password seneca Tag Name zpass2s APPLY HIDE VPN STATUS VPN Status Connection Status OpenVPN Status RX Packets / Bytes TX Packets / Bytes TX Packets / Bytes VPN Box Type VPN Box Status Connected User REFRESH	seneca zpass2s Connected Running 349 / 73.8K 0 / 0 Point-to-Point (L2) OK (Configured) gspagiari

For an explanation of the differences between a "Single LAN" VPN and a "Point-to-Point" VPN, see chapter 10.

The "VPN Box Status" string has the following format:

Result (Status)

The following table gives a short explanation of the possible "Result" and "Status" strings:

Result	Status	Meaning
Error (Unexpected response)		A response code has been received that is not
		handled by the Device (it should never occur)
Error (No response from VPN		No response has been received from the VPN Box
Box)		(response timeout); this is normally due to
		connectivity problems
Error (Invalid response from		A response has been received whose content is
VPN Box)		not valid for the Device (it should never occur)
Error (Wrong password)		The password set on the Device is wrong
Error (License Limit Reached)		The maximum number of devices allowed by the
		license are already registered on VPN Box
Error (VPN Box not configured)		The VPN Box has not been configured yet
Error (Generic error)		A generic error has occurred on the VPN Box
ОК		The Device has just been registered on the VPN
		Box
ОК	New	The Device is registered on the VPN Box, but it is
		not configured yet ("Single LAN" only)
ОК	Configuration updated	The Device configuration has just been updated
ОК	Configured	The Device is properly configured and available
		for VPN connection
ОК	Ban	The Device has been banned
ОК	Not found	The Device is unknown for the VPN Box; this
		happens when Device registration is deleted on
		the VPN Box
ОК	Unknown	The Device has an "unknown" status in the VPN
		Box (it should never occur)
ОК	Not bound	The "tunnel" between the Device and the VPN
		Box is not up; this may occur when the tunnel
		port is blocked ("not open") in the ADSL router
		on the VPN Box side ("Point-to-Point" only)
ОК	Unexpected status	A status code has been received that is not
		handled by the Device (it should never occur)

You can refresh the VPN status, by clicking on the "REFRESH" button.

Finally, you can hide the "VPN Status" section, by clicking on the "HIDE VPN STATUS" button.

19.1.4.2.1 LED signalling (Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO)

In Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO products, when VPN functionality is enabled in "VPN Box/Single LAN" mode, the "SERV" and "VPN" LEDs give the following status information (see chapter 5):

LED	Status	Meaning
VPN Yellow	ON	VPN connection is working properly

	Blinking	VPN connection is not working properly
	OFF	The Device has not been configured by the VPN Box yet or VPN Box functionality is disabled
SERV Green	Green ON VPN Box "SERVICE" connection is working properly	
	Blinking	VPN Box "SERVICE" connection is not working properly
	OFF	VPN Box functionality is disabled

Similarly, when VPN functionality is enabled in "VPN Box/Point-to-Point" mode, the "SERV" and "VPN" LEDs give the following status information (see chapter 5):

LED	Status	Meaning	
VPN Yellow	ON	A VPN client is connected to the Device	
	OFF	No VPN client is connected to the Device or VPN Box functionality is disabled	
SERV Green	ON	VPN Box "SERVICE" connection is working properly	
	Blinking	VPN Box "SERVICE" connection is not working properly	
	OFF	VPN Box functionality is disabled	

19.1.5 Router Configuration

By clicking on the "Router Configuration" link, in the "General Configuration" menu, you come to the following page:

Z-PASS2-S	×				Ciovanni	-			×
← → C 🛈 1	92.168.85.104:8080/mobile_router.php					Q	☆	J.	:
SENECA® General Configuration Mair View Network and Services Real Time Clock Setup VPN Configuration Router Configuration	Z-PASS2-S Router Configuration [user: admin] [logout] Firmware Version: SW002940_336 [Modem: I MAC Address: C8F9811B0000 [IMEI: 8610760 Internet Access: Ethernet Energy Protocols: none		-						-
Users Configuration FW Upgrade Conf. Management	PLC Status: running (app: ftp_blocks) Router: disabled								I
Mobile Configuration									- 1
Mobile Network		CURRENT	UPDATED	1					
DDNS Configuration	Router Enable		OFF V						
Digital I/O Configuration	Ethernet Bandwidth Limitation	Unlimited	Unlimited V						
Digital I/O Configuration Diagnostics	DNS-DHCP								
FW Versions	DNS Enable	ON	ON V						
Ethernet Interfaces	DHCP Server Enable		OFF V	_					
Modbus Modules	DHCP First Address	192.168.90.201	192.168.90.201						
Data Logger (SD found)	DHCP Last Address	192.168.90.210	192.168.90.210]					
SD File Manager	DHCP Lease Time (min)	15	15						
	Use Local Addresses through VPN								
	Enable	OFF	OFF V						
	Mobile Network Firewall								
	Enable	ON	ON V						
	Port Mapping / Virtual Server 1								
		TCP/UDP	TCP/UDP V	1					
	External Port								
	Server IP Address								
	Internal Port								
	Port Mapping / Virtual Server 2								
	Protocol	TCP/UDP	TCP/UDP T						
	External Port]					
	Server IP Address]					
	Internal Port								
	Port Mapping / Virtual Server 3			-					
		TCP/UDP	TCP/UDP V						
	External Port]					
	Server IP Address]					
	Internal Port]					
]					
	Port Mapping / Virtual Server 4								
		TCP/UDP	TCP/UDP V	1					
	External Port								
	Server IP Address								
	Internal Port								
	Port Mapping / Virtual Server 5								
	Protocol	TCP/UDP	TCP/UDP V						
	External Port]					
	Server IP Address]					
	Indone of David								*

In this page, you can change the parameters related to the Router functionality.

First, you have a set of general parameters, as listed in the following table:

Field	Meaning	Default value
Router Enable	Flag to enable/disable the Router	OFF
	functionality	
Ethernet Bandwidth Limitation	This parameter can be used to limit	Unlimited
	the bandwidth on the ethernet	
	interfaces; this may be needed to	
	avoid overloading the CPU, when a	

	large amount of data is forwarded	
	from one interface to the other (LAN	
	\leftrightarrow WAN).	
	Since this does not occur when the	
	two ethernet interfaces work in	
	"switch" mode, the parameter is not	
	shown when "Ethernet Mode"	
	parameter is set to "Switch" (see	
	paragraph 19.1.2).	
	Possible values are:	
	Unlimited	
	20 Mbit/s	
	10 Mbit/s	
	1 Mbit/s	
DNS Enable	Flag to enable/disable the DNS	ON
	forwarding service	
DHCP Server Enable	Flag to enable/disable the DHCP	OFF
	service (DHCP server)	
	NOTE: this parameter can be set to	
	<u>"ON" only if the "DHCP" parameter</u>	
	of the "Network and Services" page	
	is set to "OFF".	
DHCP First Address	These parameters define the range	192.168.90.201
DHCP Last Address	of IP addresses assigned by the	192.168.90.210
	DHCP server to requesting clients	
DHCP Lease Time (min)	Validity period for the IP address	15
	assignment, in minutes.	
	Possible values are in the range	
	[160].	
	I	1

Then, you have the parameter shown in the following table.

Field	Meaning	Default value
Use Local Addresses Through VPN	Flag to enable/disable the access to	OFF
	the Device and other devices which	
	are in the Device LAN by using their	
	local (LAN) IP addresses	

Then, you have another important parameter, which is shown in the following table.

Field	Meaning	Default value
Mobile Network Firewall/Enable	Flag to enable/disable the "Mobile	ON
	Network Firewall", that is	
	disable/enable access to the Device	
	and other devices which are in the	
	Device LAN, by using the IP address	

assigned to the Mobile Network (3G)	
interface.	
To open a port in the firewall, a	
"Port Mapping / Virtual Server" rule	
shall be defined.	

The above parameter shall be set to ON, to protect the Device against undesired (maybe malicious) accesses.

This is the only parameter in the "Router Configuration" page that is working also when the Router functionality is disabled (Router Enable = OFF).

It is important to note that, when the VPN is activated (see 19.1.4 paragraph), the parameter is automatically set to ON, as warned by the message shown in the following figure.

Th Z-PASS2-S	×	(!) Giovanni	- 🗆 X
	58.85.103:8080/vpn_save.php?do=2		☆ ↗ :
	58.85.103:8080/vpn_save.php?do=2 Z-PASS2-S VPN Configuration [user: admin] [logout] Firmware Version: SW002940_334 [Modem: EC21EFAR02A03M4G] MAC Address: C8F9811B0001 [IMEI: 861108030033046] Internet Access: Ethernet Energy Protocols: none PLC Status: running (app not running) Router: running VPN Box configuration changed. Mobile Network Firewall has been enabled.		☆ 🗾 :
FW Versions Ethernet Interfaces Modbus Modules Data Logger (SD missing)			

Finally, there are 5 sections which let you define up to 5 "Port Mapping" rules (also known as "Virtual Servers"); in each section, the available parameters are the following:

Field	Meaning	Default value
Protocol	This parameter defines the transport	TCP/UDP
	protocol (or kind of port) which is	
	affected by the rule: TCP, UDP or	
	both	
External Port	TCP or UDP port which a packet was	Empty

	originally sent to	
Server IP Address	IP address which the received packet	Empty
	is forwarded to	
Internal Port	TCP or UDP port which the received	Empty
	packet is forwarded to	

If Router is left disabled (Router Enabled = OFF), you can still change parameters; changes will be saved without actually applying them (except for the "Mobile Network Firewall" parameter, as told before); the following message will be given, after clicking the "APPLY" button:

If you try to enable the DHCP server functionality (DHCP Server Enable = ON), but the "DHCP First Address" and "DHCP Last Address" parameters define an address range that is not congruent with the Ethernet configuration (IP address and network mask), an error is given, as shown in the following figure:

Z-PASS2-S	(!) Giovanni	-			X
	3.85.104:8080/mobile_router_save.php?do=1		☆	J.,	:
			_		•
SENECA SENECA	Z-PASS2-S				
General Configuration	Router Configuration [user: admin] [logout]				
Main View	Firmware Version: SW002940_331 [Modem: UC20GQBR03A14E1G]				
Network and Services	MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 22210160023789	3]			
Real Time Clock Setup	Internet Access: Mobile				
VPN Configuration	Energy Protocols: none				
Router Configuration					
Users Configuration	PLC Status: running (app: zpass2s_io)				
FW Upgrade	Router: running				
Conf. Management Mobile Configuration					
Mobile Network	Invalid DHCP parameters ! Configuration not changed.				
Digital I/O					
Digital I/O Configuration					
Diagnostics					
FW Versions					
Ethernet Interfaces					
Modbus Modules					
Data Logger (SD missing)					

As already told before, the Router configuration page lets you define up to 5 "Port Forwarding" rules or "Virtual Servers".

An example is given in the following figure:

🗅 Z-PASS2-S	×				Clovenni	-		×
÷ → C 🛈 1	92.168.85.104:8080/mobile_router.php					Q	☆ 🔎	
SENECA Bineral Configuration	Z-PASS2-S Router Configuration [user: admin] [logout]							
in View	Firmware Version: SW002940_336 [Modem: 1		45401					
twork and Services								
al Time Clock Setup	MAC Address: C8F9811B0000 [IMEI: 8610750	26666172][IMS	: 222101600237893]					
N Configuration	Internet Access: Ethernet							
uter Configuration	Energy Protocols: none							
ers Configuration	PLC Status: running (app: ftp_blocks)							
V Upgrade	Router: running							
nf. Management obile Configuration				-				
bile Network		CURRENT	UPDATED					
NS Configuration	Router Enable		ON V					
ital I/O Configuration	Ethernet Bandwidth Limitation	20 Mbit/s	20 Mbit/s V					
ital I/O Configuration gnostics	DNS-DHCF							
Versions	DNS Enable	ON	ON V					
ernet Interfaces	DHCP Server Enable	OFF	OFF V					
dbus Modules	DHCP First Address	192.168.90.201	192.168.90.201					
a Logger (SD found)	DHCP Last Address	192.168.90.210	192.168.90.210					
File Manager	DHCP Lease Time (min)	15	15					
	Use Local Addresses through VPN							
	Enable	OFF	OFF V					
	Mobile Network Firewall							
	Enable	ON	ON V					
	Port Mapping / Virtual Server 1							
		TOP	TOD					
	Protocol External Port		TCP V					
		80	80					
	Server IP Address							
	Internal Port	8080	8080					
	Port Mapping / Virtual Server 2							
	Protocol	TCP/UDP	TCP/UDP V					
	External Port	502	502					
	Server IP Address	192.168.85.103	192.168.85.103					
	Internal Port	502	502					
	Port Mapping / Virtual Server 3							
	Protocol	TCP/UDP	TCP/UDP V					
	External Port							
	Server IP Address							
	Internal Port							
	Port Mapping / Virtual Server 4							
		TCP/UDP	TCP/UDP V					
	External Port							
	Server IP Address							
	Internal Port							
	Port Mapping / Virtual Server 5							
		TCP/UDP	TCP/UDP ▼					
	External Port							
	Server IP Address							

In this example, 2 rules have been set:

- the first rule tells the Device that any TCP packet received on the 80 (HTTP) port has to be forwarded to the 8080 port, leaving the original destination IP address unchanged; so, this rule lets you access the Device configuration web site on the standard HTTP port; <u>however</u>, by doing this, <u>the access to the custom user's pages won't be possible anymore !</u>
- the second rule tells the Device that any TCP or UDP packet received on the 502 port (which is often used for Modbus TCP protocol) shall be forwarded to the 192.168.85.103 IP address (which corresponds to another device) on the same (502) destination port.

Another important aspect of "Port Mapping / Virtual Server" rules is that they let define <u>which ports are</u> <u>open in the "Mobile Network Firewall"</u>; for example, if you want to connect to the web configuration site

and to the SSH console, through the public IP address assigned to the 3G interface, the 8080 and 22 TCP ports shall be open; this can be done as shown in the following figure.

Z-PASS2-S	×		Covant	- 🗆 X
	92.168.85.104:8080/mobile_router.php			Q ☆ ∠ :
	Z-PASS2-S			
INEUA 🥯				
General Configuration	Router Configuration [user: admin] [logout]			
Main View Network and Services	Firmware Version: SW002940_336 [Modem: UC20G(QBR03A14E1G]		
Real Time Clock Setup	MAC Address: C8F9811B0000 [IMEI: 8610750266661	172] [IMSI: 222101600237893]		
VPN Configuration	Internet Access: Ethernet			
Router Configuration	Energy Protocols: none			
Users Configuration	PLC Status: running (app: ftp_blocks)			
FW Upgrade				
Conf. Management	Router: running			
Mobile Configuration	cu	RRENT UPDATED		
Mobile Network	Router Enable ON	ON V	•	
DDNS Configuration Digital I/O Configuration	Ethernet Bandwidth Limitation 20 Mbit			
Digital I/O Configuration	DNS-DHCP			
Diagnostics	DNS Enable ON	ON V		
FW Versions	DHCP Server Enable OFF	OFF V		
Ethernet Interfaces Modbus Modules	DHCP First Address 192.168			
Data Logger (SD found)	DHCP Last Address 192.168			
SD File Manager	DHCP Lease Time (min) 15	15		
	Use Local Addresses through VPN	15	1	
	Enable OFF	OFF V		
	Mobile Network Firewall			
	Enable ON	ON T		
	Port Mapping / Virtual Server 1			
	Protocol TCP	TCP 🔻		
	External Port 8080	8080]	
	Server IP Address]	
	Internal Port 8080	8080]	
	Port Mapping / Virtual Server 2			
	Protocol TCP	TCP V		
	External Port 22	22]	
	Server IP Address			
	Internal Port 22	22		
	Port Mapping / Virtual Server 3			
	Protocol TCP/UE	P TCP/UDP V		
	External Port]	
	Server IP Address			
]	
	Internal Port			
	Port Mapping / Virtual Server 4			
	Protocol TCP/UD	P TCP/UDP V	1	
	External Port			
	Server IP Address			
	Internal Port]	
	Port Mapping / Virtual Server 5			
	Protocol TCP/UD	P TCP/UDP T		
	External Port			
	Server IP Address			
	Jukawa I Davk		1	•

19.1.6 OPC UA Server Configuration

By clicking on the "OPC UA Server Conf" link, in the "General Configuration" menu, you come to the following page:

	CURRENT		UPDATED
OPC-UA Server Conf.			
Enable NOTE: if ON, the server will be available at the following URL opc.tcp://IP_Address:Port/	ON	ON	~
Port	4840	484	10
Username			
Password			
Security Policy	None,Basic128Rsa15,Basic256	Sha256 No	ne,Basic128Rsa15,Basic256Sha256 🗸
Shared-Memory Type	Z-NET	Z-1	NET ~
APPLY			
	OPC-UA Server Certificates ust be in PEM (ASCII) format. Ist be in DER (binary) format.		
	Server certificate	Sfoglia	lessun file selezionato.
	Server private key	Sfoglia	lessun file selezionato.
	Trusted certificate 1	Sfoglia	lessun file selezionato.
	Trusted certificate 2	Sfoglia	lessun file selezionato.
	Trusted certificate 3	Sfoglia	lessun file selezionato.
	Trusted certificate 4	Sfoglia	lessun file selezionato.
	Trusted certificate 5	Sfoglia	lessun file selezionato.
UPLOAD SHOW CERT	IFICATE FILES RESET CERTI	IFICATE FILE	S

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

Field	Meaning	Default value
Enable	Enable or not	OFF
Port	The server port to use	4840
Username	The username provided with the service	empty
	subscription	
Password	The password provided with the service	empty
	subscription	
Security Policy	Select the security policy to use (support	None
	policies are:	
	None	
	Basic128Rsa15 / Sign	
	Basic128Rsa15 / Sign & Encrypt	
	Basic256Sha256 / Sign	
	Basic256Sha256 / Sign & Encrypt	
Shared Memory	Select which shared memory must	Z-NET
	access with the OPC-UA protocol.	
OPC-UA Server Certificates	Upload to the device the certificates for:	
	Server, Private key and Trusted	
	certifiactes (up to 5).	
	Press "Upload" to send the certificate to	

the device Press Show Certificate Files for show the actual loaded files	
Press Reset Certificate File for delete the actual loaded files	

Note that for access the server with a OPC UA client you must use the following url:

opc.tcp://IP_ADDR:PORT/

where:

IP_ADDR is the actual IP address

PORT is the configured port for the OPC UA serverOPC UA Client Configuration

By clicking on the "OPC UA Client Conf" link, in the "General Configuration" menu, you come to the following page:

Z-PASS2-	s			
OPC-UA	Client Conf. [user: admi	n] [logout]		
Firmware	Version: SW002940_36	0 [Modem:	UC20GQ	BR03A14E1G]
MAC Add	ress: C8F9811B02A0 [IN	/EI: 86107	50294940	02]
Internet /	Access: Ethernet			
Energy P	rotocols: none			
PLC Stat	us: running (app: znet_e	mpty)		
Router: n	unning			
	-			
	OPC-UA Cliem			
.crt,.cer,.k	ey,.pem files must be in PEM (A der files must be in DER (bii.	-		
	Clie	nt certificate	Sfoglia	Nessun file selezionato.
	Clier	it private key	Sfoglia	Nessun file selezionato.
	Trusted	certificate 1	Sfoglia	Nessun file selezionato.
	Trusted	certificate 2	Sfoglia	Nessun file selezionato.
	Trusted	certificate 3	Sfoglia	Nessun file selezionato.
	Trusted	certificate 4	Sfoglia	Nessun file selezionato.
	Trusted	certificate 5	Sfoglia	Nessun file selezionato.
	Trusted	certificate 6	Sfoglia	Nessun file selezionato.
	Trusted	certificate 7	Sfoglia	Nessun file selezionato.
	Trusted	certificate 8	Sfoglia	Nessun file selezionato.
	Trusted	certificate 9	Sfoglia	Nessun file selezionato.
	Trusted	certificate 10	Sfoglia	Nessun file selezionato.
UPLOAD	SHOW CERTIFICATE FILES	DECET CED	TIFICATE FI	

In this page, you can set the parameters related to the Certificates for the Client OPC Unified Architecture (Client OPC UA).

19.1.6.1 Using OPC-UA Client / Server Certificates

The Seneca devices are prepared with a couple of default certificates:

"server_cert.der" and "server_key.der" are provided in the default OPC-UA server configuration:

OPC-UA Server Certificates .crt,.cer,.key,.pem files must be in PEM (ASCII) format. .der files must be in DER (binary) format.
Server certificate Sfoglia Nessun file selezionato.
Server private key Sfoglia Nessun file selezionato.
Trusted certificate 1 Sfoglia Nessun file selezionato.
Trusted certificate 2 Sfoglia Nessun file selezionato.
Trusted certificate 3 Sfoglia Nessun file selezionato.
Trusted certificate 4 Sfoglia Nessun file selezionato.
Trusted certificate 5 Sfoglia Nessun file selezionato.
UPLOAD HIDE CERTIFICATE FILES RESET CERTIFICATE FILES
OPC-UA Server Certificate File
Files (size in byte NOTE: these files can be downloaded via FTP from 'home/config/opcua'' director
server_cert.der (102
server_key.der (121

And "client_cert.der" and "client_key.der" are provided in the default OPC-UA client configuration:

OPC-UA Clier .crt.cerkevpem files must be in PEM (nt Certificates		
.der files must be in DER (b			
Cli	ent certificate	Sfoglia	Nessun file selezionato.
Clie	ent private key	Sfoglia	Nessun file selezionato.
Truste	d certificate 1	Sfoglia	Nessun file selezionato.
Truste	d certificate 2	Sfoglia	Nessun file selezionato.
Truste	d certificate 3	Sfoglia	Nessun file selezionato.
Truste	d certificate 4	Sfoglia	Nessun file selezionato.
Truste	d certificate 5	Sfoglia	Nessun file selezionato.
Truste	d certificate 6	Sfoglia	Nessun file selezionato.
Truste	d certificate 7	Sfoglia	Nessun file selezionato.
Truste	d certificate 8	Sfoglia	Nessun file selezionato.
Truste	d certificate 9	Sfoglia	Nessun file selezionato.
Trusted	certificate 10	Sfoglia	Nessun file selezionato.
UPLOAD HIDE CERTIFICATE FILES	RESET CERT	IFICATE FILE	5
			OPC-UA Client Certificate Files
			Files (size in bytes)
NOTE: these files can be do	ownloaded via l	TP from '/ho	ne/config/opcua-client/" directory.
			client_cert.der (1020)
			client_key.der (1217)
REFRESH			

These files can be downloaded from the device using the ftp connection to /home/config/opcua-client.

If you want to allow only some clients to connect you must use the "OPC-UA Server/Client Trusted List".

For upload the Client/Server certificate to the trusted list use the "Trusted Certificate n" button, (max 5 Client certificates are allowed for the server and max 10 for the client).

Otherwise, if the trusted certificate lists are empty all clients are allowed to access to all the OPC-UA Servers.

Example 1 "Sign & Encrypt and allow all clients"

We need to connect 2 Seneca OPC-UA Client devices to one Seneca OPC-UA Server device with Sign&Encrypt but we don't need to restrict the access to only the 2 Clients.

In this case we must only connect the clients to the server without copy certificates.

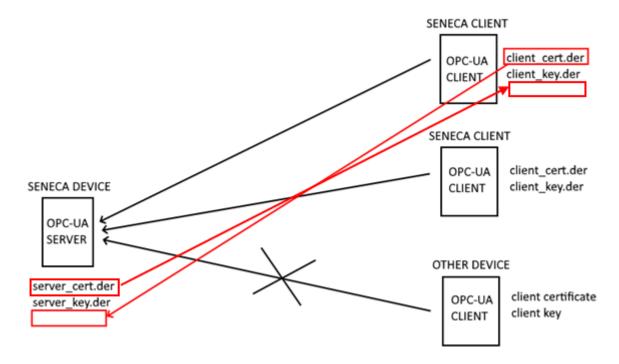
Example 2 "Sign & Encrypt and allow anly the 2 clients"

We need to connect 2 Seneca OPC-UA Client devices to one Seneca OPC-UA Server device with Sign&Encrypt but we need to restrict the access to only these 2 Clients.

In this case we must upload the "client_cert.der" to the Server Trusted certificate.

If you are using the default file you can upload only one file (because the 2 Seneca devices have the same certificates).

Also we must upload the "server_cert.der" to the Client Trusted certificate:



In this way the "Other device" is not allowed to connect to the OPC-UA server.

19.1.7 Users Configuration

By clicking on the "Users Configuration" link, in the "General Configuration" menu, you come to the following page:

In this page, you can change the "Web Administrator", "Web User", "Web Guest" and "FTP User" credentials, as explained in the following table:

Field Meaning Default value

WEB ADMINISTRATOR/Username	Username to access the web	admin
	configuration site (full access)	
WEB ADMINISTRATOR/Password	Password to access the web	admin
	configuration site (full access)	
WEB USER/Username	Username to access the web	user
	configuration site (limited access)	
	(see paragraph 19.2)	
WEB USER/Password	Password to access the web	user
	configuration site (limited access)	
	(see paragraph 19.2)	
WEB GUEST/Username	Username to access the web	guest
	configuration site, in "view-only	
	mode" (see paragraph 19.3)	
WEB GUEST/Password	Password to access the web	guest
	configuration site, in "view-only	
	mode" (see paragraph 19.3)	
FTP USER/Username	Username to access the Device	user
	FTP/SFTP site (see chapter 7)	
FTP USER/Password	Password to access the Device	123456
	FTP/SFTP site (see chapter 7)	

For all the fields in this page, the following characters are allowed:

```
a-zA-ZO-9-_|!@$%^&*?+{}<>;,:.
```

each field can contain up to 100 characters.

The same rules apply to the other "Username" and "Password" fields of the web pages and to the "Tag Name" field of the "VPN Configuration" page.

Please note that, after changing the Web Administrator credentials, a new login will be required to access any page.

19.1.8 FW Upgrade

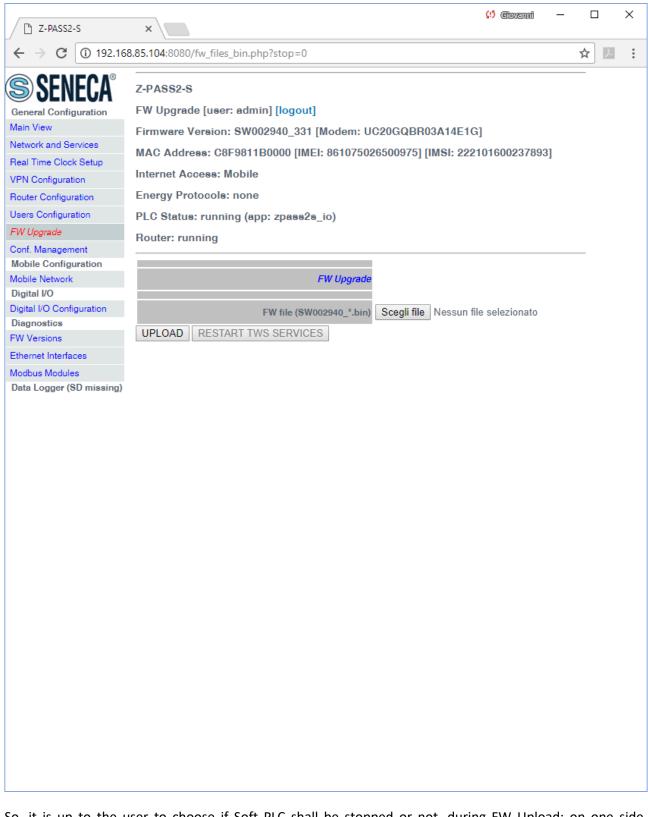
When clicking on the "FW Upgrade" link, in the "General Configuration" menu, the following pop-up is shown:

192.168.85.104:8080 dice:	×
Do you want to stop TWS services during upload ?	
(Once services are stopped, you can restart them by clicking on the 'RESTART TWS SERVICES' button.)	
OK Annulla	

If you click on the "OK" button, TWS Services (i.e. Soft-PLC) are stopped and you come to the "FW Upgrade" page, shown in the following figure.

Now, if you want to leave this page without performing the FW upgrade, the "RESTART TWS SERVICES" button lets you restart the TWS services which, otherwise, would remain in the "stopped" state.

Otherwise, if you click on the "Cancel" button of the pop-up, TWS Services are not stopped and you come to the same page where the "RESTART TWS SERVICES" button is disabled.



So, it is up to the user to choose if Soft PLC shall be stopped or not, during FW Upload; on one side, stopping it is more safe and let the upload be completed in a shorter time; on the other side, there are situations in which PLC stop time shall be as short as possible.

Since an erroneous use of the FW Upgrade functionality might compromise the proper Device operation, use this page only to apply upgrades provided by Seneca, with the support of Seneca personnel.

This page lets you browse your PC to select the file containing the FW, which shall have a name of the following type:

SW002940_xxx.bin¹⁴

If you select a file with a different name, an error will be shown at the end of the upload, as in the following figure.

¹⁴ The FW file can be downloaded from Seneca website (see chapter 18).

Z-PASS2-S	(1) Citoxenni — — >
← → C ① 192.16	8.85.104:8080/fw_upgrade_bin.php 🖈 🗵
SFNFCA®	Z-PASS2-S
General Configuration	FW Upgrade [user: admin] [logout]
Main View	Firmware Version: SW002940_331 [Modem: UC20GQBR03A14E1G]
Network and Services	
Real Time Clock Setup	MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237893]
VPN Configuration	Internet Access: Mobile
Router Configuration	Energy Protocols: none
Users Configuration	PLC Status: stopped
FW Upgrade	
Conf. Management	Router: running
Mobile Configuration	
Mobile Network	Invalid file 'disk.tar.gz' !
Digital I/O	
Digital I/O Configuration	A 'SW002940_*.bin' file is needed.
Diagnostics	
FW Versions	
Ethernet Interfaces	
Modbus Modules Data Logger (SD missing)	

Once a file is selected, you can start the upload, by pressing the "UPLOAD" button.

	×	- 🗆	Х
← → C ① 192.168.85.104:8080/fw_files_bin.php ☆ 🗵	192.168.85.104:8080/fw_files_bin.php	☆ 🗵	:
A Constraint of the second and second and the second	Xion Z-PASS2-S FW Upgrade [user: admin] [Firmware Version: SW00294 MAC Address: C8F9811B00 Internet Access: Mobile Energy Protocols: none PLC Status: stopped Router: running Internet Access: Stopped Router: running Internet Access Internet Access: Stopped Router: running Internet Access Internet Access Router: running Internet Access Internet Access Router: running Internet Access Internet Access Internet Access Router: running Internet Access Router: running Internet Access Internet Access		

Once the upload is successfully completed, the following page is shown:

Z-PASS2-S	× Giovanni —		×
	3.85.104:8080/fw_upgrade_bin.php	☆ //	
Configuration Several Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration <i>FW Upgrade</i> Conf. Management Mobile Configuration Mobile Network Digital I/O Digital I/O Digital I/O Configuration Diagnostics FW Versions Ethernet Interfaces Modbus Modules Data Logger (SD missing)	ZPASS2-S FW Upgrade [user: admin] [logout] Firmware Version: SW002940_331 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237893] Internet Access: Mobile Energy Protocols: none PLC Status: stopped Router: running File 'SW002940_331.bin' successfully uploaded ! Upgrade and Reboot Cancel and Reboot		

In this page, you can:

• press the "Upgrade and Reboot" button: this will start the upgrade procedure, which takes some minutes to be completed; during this time, the Device MUST NOT be switched off; during the

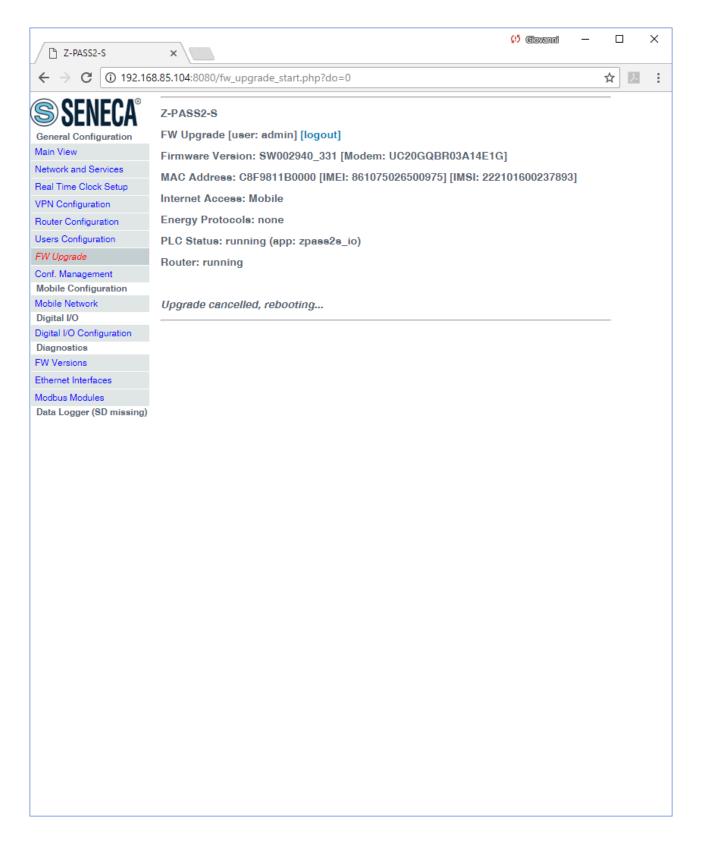
procedure, the Device will be rebooted several times; also, during the procedure, several LEDS will blink simultaneously¹⁵; the upgrade procedure is ended when only the LED "RUN" is blinking¹⁶;

Z-PASS2-S	(*) Ciovanni —]	×	(
	8.85.104:8080/fw_upgrade_start.php?do=3	☆	J.		0 0 0
SENELA	Z-PASS2-S				
General Configuration	FW Upgrade [user: admin] [logout]				
Main View	Firmware Version: SW002940_331 [Modem: UC20GQBR03A14E1G]				
Network and Services					
Real Time Clock Setup	MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237893]				
VPN Configuration	Internet Access: Mobile				
Router Configuration	Energy Protocole: none				
Users Configuration	PLC Status: stopped				
FW Upgrade	Router: running				
Conf. Management	Houter, Furning				
Mobile Configuration					
Mobile Network	Upgrading firmware, this will take some time				
Digital I/O					
Digital I/O Configuration Diagnostics					
FW Versions					
Ethernet Interfaces					
Modbus Modules					
Data Logger (SD missing)					

¹⁵ This applies only to products with HW revisions IO and R01; in details: for IO HW revision, all LEDs will blink simultaneously, except for Power, LAN/WAN, COM and modem LEDs; for R01 HW revision, RUN, VPN and SERV LEDs will blink.

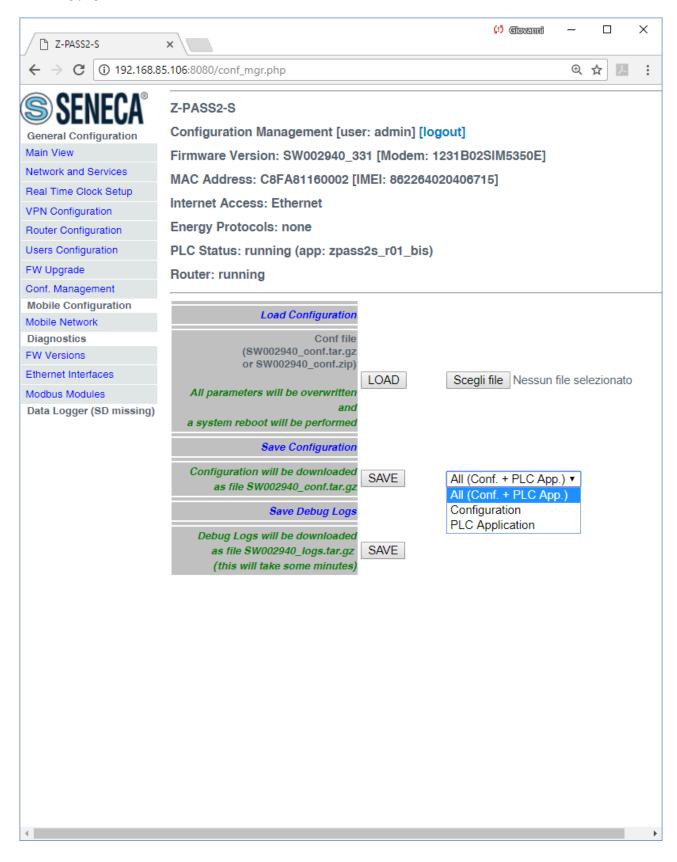
¹⁶ Also SERV and VPN LEDs might blink, depending on the Device configuration and status.

• press the "Cancel and Reboot" button: this will delete the uploaded file on the Device and perform the reboot.



19.1.9 Configuration Management

By clicking on the "Conf. Management" link, in the "General Configuration" menu, you come to the following page:



This page lets you save and load the whole Device configuration; this is very useful, for example, when you have to apply the same configuration to many devices.

The configuration archive file is named *SW002940_conf.tar.gz*; its contents depend on the selected option, as shown in the following table:

Option	Files	
All (Conf. + PLC App.)	- configuration parameters	
	- OpenVPN configuration (if present)	
	- PLC (Straton) application (if present)	
	- web user pages (if present)	
Configuration	- configuration parameters	
	- OpenVPN configuration (if present)	
PLC Application	- PLC (Straton) application (if present)	
	- web user pages (if present)	

The configuration archive, once created and downloaded by means of the "SAVE" button can be uploaded to the same or another device, in two ways:

- by means of the "LOAD" button, in this page
- by means of a USB pen

The procedure to load the configuration into the Device by means of a USB pen is the following:

- copy the *SW002940_conf.tar.gz* (or *SW002940_conf.zip*, see below) file into the root folder of the USB pen;
- switch off the Device;
- insert the USB pen into the USB#1 port of the Device;
- switch on the Device; the procedure will take some minutes to be completed; during this time, the Device MUST NOT be switched off; during the procedure, the Device will be rebooted;
- after the reboot, wait until you see the "RUN" LED blinking;
- remove the USB pen;
- the configuration has been applied to the Device.

The only care <u>when you carry the configuration archive from a device to another one is that the two</u> <u>devices should be the same product model</u>; for example, it's not safe to load the configuration archive saved on a Z-PASS2-S-R01 into a Z-PASS2-S.

This page lets you load also the configuration archive created by Z-NET4 SW (see chapter 21) as a zip file (*SW002940_conf.zip*).

Another useful feature available in this page is the one provided by the "Save Debug Logs / SAVE" button: when you click on it, a file named *SW002940_logs.tar.gz* is downloaded, which contains the debug logs stored by the CPU during its operation.

	(1) (flovanit	– 🗆 X
Z-PASS2-S	×	
$\boldsymbol{\leftarrow}$ \rightarrow \mathbf{C} (i) 192.168	8.85.106:8080/conf_mgr.php	☆ ▶ :
Configuration Second Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Conf. Management Mobile Configuration Mobile Network Diagnostics FW Versions Ethernet Interfaces Modbus Modules Data Logger (SD missing)	335.106:8080/conf_mgr.php Z-PASS2-S Configuration Management [user: admin] [logout] Firmware Version: SW002940_331 [Modem: 1231B02SiM5350E] MAC Addrese: C8FA81160002 [IMEI: 862264020406715] Internet Access: Ethernet Energy Protocols: none PLC Status: running (app: zpaes2s_r01_8) Router: running Load Configuration Conf file (SW002940_conf.zip) All parameters will be overwithen and a system reboot will be performed Save Configuration Configuration will be downloaded as file SW002940_conf.ar.gz SAVE All (Conf. + PLC App.) • Save Debug Logs Debug Logs will be downloaded as file SW002940_logs.tar.gz (this will take some minutes) SAVE	
SW002940_logs.tar.c	Jz ^	Mostra tutto 🗙

Please note that, to get detailed debug logs, the "DEBUG LOGS / Enable" parameter, in "Network and Services" page, shall be set to ON.

19.1.9.1 Factory reset by USB pen

A USB pen can be used also to reset the Device to its factory state; the procedure is the following:

- create an empty file named SW002940_reset_cmd into the root of the USB pen;
- switch off the Device;
- insert the USB pen into the USB#1 port of the Device;
- switch on the Device; the procedure will take some minutes to be completed; during this time, the Device MUST NOT be switched off; during the procedure, the Device will be rebooted;
- after the reboot, wait until you see the "RUN" LED blinking;
- remove the USB pen;
- the factory reset has been performed.

19.1.10 Modbus Configuration

By clicking on the "Modbus Configuration" link, in the "General Configuration" menu, you come to the following page:

Z-PASS2-S					
Modbus Configuration [user: admin] [logout]					
Firmware Version: SW002940_360 [Modem: UC20GQBR03A14E1G]					
MAC Address: C8F9811B02A0 [IMEI: 861075029494002]					
Internet Access: Ethernet	nternet Access: Ethernet				
Energy Protocols: none					
PLC Status: running (app: znet_empty)					
Router: running					
	CURRENT	UPDATED			
Modbus TCP Client		UPDATED			
Modbus TCP Client		UPDATED			
	127.0.0.1				
IP Address	127.0.0.1 502	127.0.0.1			
IP Address TCP Port	127.0.0.1 502	127.0.0.1			
IP Address TCP Port Modbus Pass-through	127.0.0.1 502 ON	127.0.0.1			

This page lets you change the IP Address and TCP Port of the Modbus TCP Client ("Open MODBUS") in the "Fieldbus Configurations" of the Straton project; the Modbus TCP Client change can be done without the need of recompiling the Straton project.

	10 Drivers				
E	Mg MODBUS Master	Name	Value		
恭		Mode	Open MODBUS		
•		Address	mbtcpcli_params		
	+0: VAR1	Port	1100		
10	- Error report: ErrorReport	Reconnect after error	Image: A start and a start		
	Mg MODBUS Slave	Slaves diagnostics			
		Delay between requests (ms)	0		
8		Disabled			
₫,					
Bt		1			

To apply the parameters set in this page to the "Open MODBUS" configuration, the string "*mbtcpcli_params*" shall be written in the "Address" field.

It should be noted that the value of the "Port" field is overwritten with the one set in the "Modbus TCP Client Configuration" web page.

In the following table, all configuration parameters available in the page are listed, with a short explanation and the parameter default value for each of them.

Field	Meaning	Default value
IP Address	IP Address of the Modbus TCP	127.0.0.1
	Server the client shall connect to	
TCP Port	TCP Port of the Modbus TCP Server	502
	the client shall connect to	

The Modbus Pass-through mode allows to change on the fly the Modbus TCP-IP to Modbus RTU protocol for access to the RS485 or RS232 devices using the Ethernet ports.

Field	Meaning	Default value
Enable	Enable or not the Modbus Pass-	OFF
	through	
TCP Port	TCP Port of the Modbus TCP for the	504
	Pass-through	

19.1.11 Mobile Network

By clicking on the "Mobile Network" link, in the "Mobile Configuration" menu, you come to the following page:

□ Z-PASS2-S	×		🤃 Ciovanni	-		×
← → C U 192.160	8.85.104:8080/mobile_network.php			\$:
S SENECA [®]	Z-PASS2-S					
General Configuration	Mobile Network [user: admin] [logout]				
Main View	Firmware Version: SW002940_	332 [Modem: LIC	20G0BB03A14E1G1			
Network and Services		-	_			
Real Time Clock Setup	MAC Address: C8F9811B0000	[IMEI: 861073026	500975]			
VPN Configuration	Internet Access: Ethernet					
Router Configuration	Energy Protocols: none					
Users Configuration	PLC Status: running (app: s203	3)				
FW Upgrade	Router: running	- /				
Conf. Management	Router: running					
Mobile Configuration		CURRENT	UPDATED		1	
Mobile Network		o o militi	VI DATED			
DDNS Configuration	SIM					
Digital I/O	PIN (if required by SIM)	8342	8342			
Digital I/O Configuration						
Diagnostics FW Versions	Operator Selection					
Ethernet Interfaces	Mode	Automatic	Automatic •			
Modbus Modules	Operator	[22201] I TIM (UMTS)	Operator list not available ▼			
Data Logger (SD found)	Data Connection					
Logs	Data Connection					
	Enable	OFF	OFF •			
	APN Mode	Automatic	Automatic ▼			
	APN	ibox.tim.it	ibox.tim.it			
	Authentication Type	None	None *			
	Username	user	user			
	Password	pass	pass		1	
	Ping Connection Testing IP				_	
	Address (if empty, testing is disabled)	www.google.com	www.google.com			
	APPLY SHOW MOBILE STATU		ORLIST			
			ONCLOT			

The above figure shows the "Mobile Network" page for Z-PASS2-S-IO.

For Z-PASS2-S-R01, Z-PASS2-S and S6001-RTU, the "Operator Selection" section and the "GET OPERATOR LIST" button are not available, so the page is as shown in the following figure.

			(!) Clovenni -	- 🗆 ×	(
Z-PASS2-S	×				
← → C (i) 192.168	8.85.105:8080/mobile_network.php			☆	:
SENECA °	Z-PASS2-S				
General Configuration	Mobile Network [user: admin] [logout]			
Main View	Firmware Version: SW002940_	332 [Modem: 123	31B02SIM5350E1		
Network and Services		-	_		
Real Time Clock Setup	MAC Address: C8F981160017 [IMEI: 862264020	382288]		
VPN Configuration	Internet Access: Ethernet				
Router Configuration	Energy Protocols: none				
Users Configuration	PLC Status: running (app: sms	blocks)			
FW Upgrade	Router: disabled				
Conf. Management	Router: disabled				
Mobile Configuration		CURRENT	UPDATED		
Mobile Network		CONNENT	OPDATED		
DDNS Configuration	SIM				
Diagnostics	PIN (if required by SIM)	1234	1234		
FW Versions	i in (in required by enity	1201	1204		
Ethernet Interfaces	Data Connection				
Modbus Modules	Enable	OFF	OFF •		
Data Logger (SD missing)	APN Mode	Automatic	Automatic T		
	APN	ibox.tim.it	ibox.tim.it		
	Authentication Type		None 🔻		
	Username		user		
	Password	0855	pass		
	Ping Connection Testing IP	paoo	pass		
	Address	www.google.com	www.google.com		
	(if empty, testing is disabled)				
	APPLY SHOW MOBILE STATU	5			
L					

In this page, you can change the parameters related to the Mobile Network, as listed in the following table:

Field	Meaning	Default value
SIM/PIN (if required by SIM)	PIN needed to unlock the SIM card,	1234
	if PIN locking functionality is enabled	

	on it ¹⁷	
Operator Selection/Mode (only on Z-PASS2-S-IO)	 This parameter tells if the modem shall select the Mobile Network Operator: automatically (Mode=Automatic) as selected by the user (Mode=Manual) reverting to "automatic" mode, if "manual" selection fails (Mode = Manual/ Automatic) 	Automatic
Operator Selection/Operator (only on Z-PASS2-S-IO)	 This parameter contains the list of the Mobile Network Operators currently available, that is detected by the modem. The list items are strings with the following format: the MCC+MNC¹⁸ code in square brackets (e.g.: "[22201]") the string identifying the operator (e.g.: "I TIM") the access technology, that is "GSM" or "UMTS", in brackets This list is initially empty: it shall be filled by clicking on the "GET OPERATOR LIST" button. 	"[22201] I TIM (UMTS)"
Data Connection/Enable	Flag to enable/disable the Mobile Network connectivity	OFF
Data Connection/APN Mode	This parameter tells if the APN and related parameters are automatically retrieved (based on SIM IMSI) (Mode=Automatic) or the values given in this page are used. When APN Mode = Automatic, APN, Authentication Type, Username and Password parameters are disabled.	Automatic
Data Connection/APN	Access Point Name, as given by the Mobile Network Operator	ibox.tim.it
Data Connection/Authentication Type	Type of authentication required; possible values are: "None", "CHAP/PAP", "CHAP only", "PAP only"	None
Data Connection/Username	Username needed for UMTS/GPRS connectivity, as given by the Mobile Network Operator; it may be empty, if "Authentication Type" parameter	user

¹⁷ Please note that the procedure to enable/disable the PIN locking functionality on the SIM is not performed by the Device.

¹⁸ MCC = Mobile Country Code, MNC = Mobile Network Code

	is "None"	
Data Connection/Password	Password needed for UMTS/GPRS	pass
	connectivity, as given by the Mobile	
	Network Operator; it may be empty,	
	if "Authentication Type" parameter	
	is "None"	
Data Connection/Ping Connection	FQDN or IP address used to	www.google.com
Testing IP Address (if empty, testing	periodically check, by means of	
is disabled)	"ping" packets, if the mobile	
	connection is actually working; if the	
	field is lefty empty, the check is not	
	performed.	
	It is important to note that the	
	FQDN or IP address specified must	
	be reachable from the Device mobile	
	network, otherwise the Device will	
	detect that the mobile connection is	
	not working and will drop it.	

In the "Mobile Network" page, when you click on the "SHOW MOBILE STATUS" button, a new section appears, named "Mobile Status", showing:

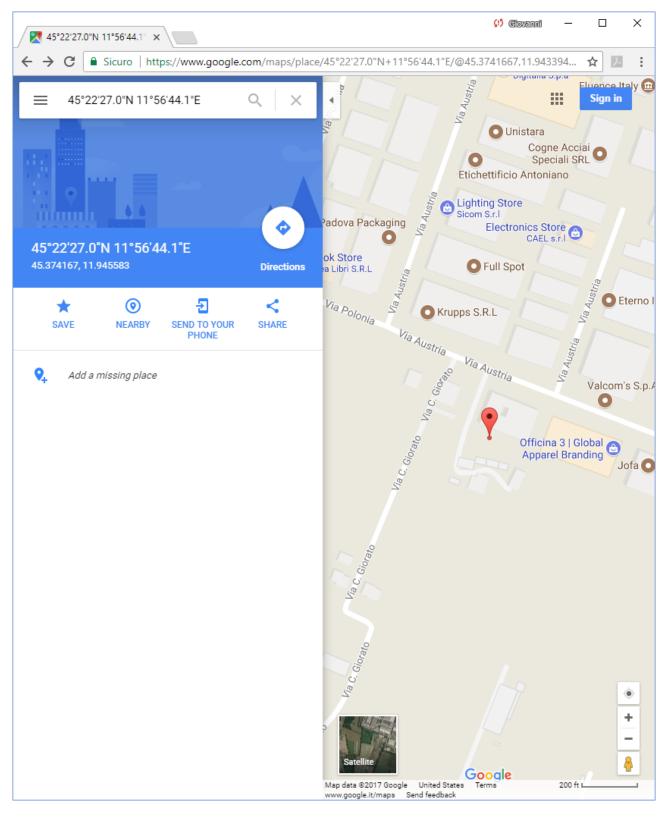
- the SIM/PIN Status; if an error in PIN setting has occurred or PUK/PUK2 setting is needed, this status is shown in red color
- the number of remaining attempts for PIN setting; when this value is less than 3 (shown in red color), it means that PIN setting has failed, that is the configured PIN value is wrong
- the radio "Signal Level", in the range [0..7]
- the selected operator (only for Z-PASS2-S-IO)
- the GSM "Registration Status"
- the Mobile Network "Connection Status" (i.e.: "Disconnected" or "Connected")
- the IP address assigned to the Mobile Network interface when connected, the "dummy" IP address "0.0.0.0" when disconnected
- the number of packets/bytes received from the Mobile Network interface, when connected; "0/0" when disconnected
- the number of packets/bytes sent to the Mobile Network interface, when connected; "0/0" when disconnected

as shown in the following couple of figures:

Z-PASS2-S	(1) (1)	Giovanni	-]	×
← → C ① 192	2.168.85.104:8080/mobile_network.php?showinfo=1		Q	☆	J.	0 0 0
S SENECA General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Conf. Management	Z-PASS2-S Mobile Network [user: admin] [logout] Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 2221016002374 Internet Access: Ethernet Energy Protocols: none PLC Status: running (app: s203) Router: running	890]				
Mobile Configuration Mobile Network	CURRENT UPDATED					
DDNS Configuration Digital I/O Digital I/O Configuration	SIM PIN (if required by SIM) 8342 8342					
Diagnostics FW Versions Ethernet Interfaces	Operator Selection Mode Automatic ✓ Operator [22201] I TIM Operator list not available ▼					
Modbus Modules Data Logger (SD found) Logs	Data Connection Enable OFF OFF APN Mode Automatic					
	APN ibox.tim.it ibox.tim.it Authentication Type None Username user User					
	Password pass pass Ping Connection Testing IP Address (if empty, testing is disabled) www.google.com www.google.com APPLY HIDE MOBILE STATUS GET OPERATOR LIST					
	Mobile Status SIM/PIN Status PIN required PIN Remaining Attempts 3 Signal Level [07] 6 Selected Operator "vodafone IT" (UMT Registration Status Disconnected O.0.0 IP Address 0.0.0 RX Packets / Bytes 0 / 0 TX Packets / Bytes 0 / 0 GP8 Location 45.37445,11.94516	network)				

Z-PASS2-S	×		(!) Ciovanai	_		Х
← → C ① 192.	.168.85.104:8080/mobile_network.p	php?showinfo=1		Q	☆ 🏸	:
SERVECA General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Conf. Management	Z-PASS2-S Mobile Network [user: admin] [lo Firmware Version: SW002940_33 MAC Address: C8F9811B0000 [IM Internet Access: Mobile Energy Protocols: none PLC Status: running (app: s203) Router: running	2 [Modem: UC20	-			
Mobile Configuration		CURRENT	UPDATED			
Mobile Network DDNS Configuration Digital I/O Digital I/O Configuration Diagnostics FW Versions	SIM PIN (if required by SIM) Operator Selection Mode	8342	8342			
Ethernet Interfaces	Operator	[22201] I TIM	Operator list not available V			
Modbus Modules	Data Connection	(UMTS)				
Data Logger (SD found) Logs	Enable		ON V			
		user pass	Automatic ibox.tim.it None user pass www.google.com LIST			
	Mobile 3 SIM/PIN 8 PIN Remaining Att Signal Level Selected Op Registration 8 Connection 9 IP Ad RX Packets / TX Packets / GPS Loc REFRESH	Status empts [07] erator Status Status dress Bytes Bytes	PIN required 3 6 "vodafone IT" (UMT8) Registered (home network) Connected 10.109.234.57 6 / 65 6 / 98 45.37433,11.94537 [Map]			

As shown in the above figures, only for Z-PASS2-S-IO, the last row of the "Mobile Status" gives the "GPS Location" as Latitude, Longitude values; clicking on the <u>Map</u> link, the Google Maps on the current position are shown.



If the GPS signal is not available, the "GPS Location" row contains the string "Not fixed" and the <u>Map</u> link is not shown.

The following figure shows the situation when an error in PIN setting has occurred, due to a wrong value of the PIN parameter.

Th Z-PASS2-S	×		(1) Elovand	-		>	×
	168.85.104:8080/mobile_network.p	hp?showinfo=1		Θ	☆	h.,	:
< 7 C 0 132.		np:snowinio=1		~	<u>м</u>	22	:
SERVECA® General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade	Z-PASS2-S Mobile Network [user: admin] [lo Firmware Version: SW002940_33 MAC Address: C8F9811B0000 [IM Internet Access: Ethernet Energy Protocols: none PLC Status: running (app: s203) Router: running	2 [Modem: UC20	-				
Conf. Management Mobile Configuration							
Mobile Network		CURRENT	UPDATED				
DDNS Configuration	SIM						
Digital I/O	PIN (if required by SIM)	1234	1234				
Digital I/O Configuration	Operator Selection						
Diagnostics			Automatic				
FW Versions		Automatic [22201] I TIM	Automatic •				
Ethernet Interfaces	Operator	(UMTS)	Operator list not available V				
Modbus Modules Data Logger (SD found)	Data Connection						
Logs	Enable	OFF	OFF V				
	APN Mode	Automatic	Automatic 🔻				
	APN	ibox.tim.it	ibox.tim.it				
	Authentication Type	None	None v				
	Username	user	user				
	Password		pass				
	Ping Connection Testing IP Address	www.google.com	www.google.com				
	(if empty, testing is disabled) APPLY HIDE MOBILE STATUS	GET OPERATOR					
		GET OF ERATOR					
	Mobile						
	SIM/PIN		PIN error 2				
	Signal Leve		4				
	Selected Op	erator	No operator				
	Registration Connection		Searching for network Disconnected				
		Idress	0.0.0				
	RX Packets /		0/0				
	TX Packets / GPS Lo		0 / 0 Not fixed				
	REFRESH		HULINGU				

It should be noted that, when the PIN is set during procedures automatically performed by the Device firmware, if the number of remaining attempts is 1, no more attempt is done to avoid blocking the SIM.

You can refresh the Mobile Network status, by clicking on the "REFRESH" button.

You can hide the "Mobile Status" section, by clicking on the "HIDE MOBILE STATUS" button.

As already told above, the "GET OPERATOR LIST" button lets you retrieve the list of the operators currently available, that is detected by the modem (only on Z-PASS2-S-IO).

When you click on the button, the following page is shown.

Z-PASS2-S	(!) Ciovanni —		×
	8.85.104:8080/mobile_network_scan.php	☆ 🗡	
SERNECA® General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration	Z-PASS2-S Mobile Network [user: admin] [logout] Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Internet Access: Ethernet Energy Protocols: none		
Users Configuration FW Upgrade Conf. Management Mobile Configuration Mobile Network	PLC Status: running (app: s203) Router: running		
DDNS Configuration Digital I/O Digital I/O Configuration Diagnostics FW Versions	Start retrieving operator list, please wait (this will take some minutes)		
Ethernet Interfaces Modbus Modules Data Logger (SD found) Logs			

Tipically, it takes about 1 minute to get the list, so the page shows the number of seconds elapsed.

Z-PASS2-S	(!) (Etovanni —]	×
	× \			
\leftrightarrow \rightarrow \times (i) 192.10	58.85.104:8080/mobile_network_scan.php	☆	J	:
SENECA [®]	Z-PASS2-S			
General Configuration	Mobile Network [user: admin] [logout]			
fain View	Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G]			
letwork and Services	MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]			
leal Time Clock Setup				
PN Configuration	Internet Access: Ethernet			
outer Configuration	Energy Protocols: none			
sers Configuration	PLC Status: running (app: s203)			
W Upgrade	Router: running			
onf. Management	i odoli i dining			
Iobile Configuration				
lobile Network	Operator list retrieval in progress, please wait			
DNS Configuration	(15 seconds elapsed)			
igital I/O ligital I/O Configuration				
)iagnostics				
W Versions				
thernet Interfaces				
lodbus Modules				
ata Logger (SD found)				
.ogs				
attesa di risposta da 192.1	58.85.104			

When the procedure is completed, the following page is shown.

🗅 Z-PASS2-S	(!) Ciovenni —		×
← → C ① 192.16	8.85.104:8080/mobile_network_scan.php	☆ 🔎	:
Seneral Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Conf. Management Mobile Configuration DDNS Configuration Digital I/O Digital I/O Digital I/O Configuration Diagnostics FW Versions Ethernet Interfaces Modbus Modules Data Logger (SD found) Logs	Z-PASS2-S Mobile Network [user: admin] [logout] Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 22210160023789 Internet Access: Ethernet Energy Protocols: none PLC Status: running (app: s203) Router: running <i>Operator list successfully retrieved</i> !		

After some seconds, the page automatically evolves to the "Mobile Network" page, with the operator list filled, as shown in the following figure.

Z-PASS2-S	×	(1) Civand — 🗆 🗙
	8.85.104:8080/mobile_network.php	☆ ▷ :
SERVECA® General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Conf. Management	Z-PASS2-S Mobile Network [user: admin] [logout] Firmware Version: SW002940_332 [Modem MAC Address: C8F9811B0000 [IMEI: 86107 Internet Access: Ethernet Energy Protocols: none PLC Status: running (app: s203) Router: running	-
Mobile Configuration	CURREN	T UPDATED
Mobile Network DDNS Configuration Digital I/O Digital I/O Configuration Diagnostics FW Versions Ethernet Interfaces Modbus Modules Data Logger (SD found) Logs	SillPIN (if required by SIM)1234Operator Selection4utomaticModeAutomaticOperator[22201] I TIMUMTS)Data ConnectionEnableOFFAPN ModeAutomaticAPN ModeAutomaticAuthentication TypeNoneUsernameuserPasswordpassPing Connection Testing IP Addresswww.google.(if empty, testing is disabled)GET OP	[22250] UIKINOWI (UMTS) [22288] I WIND (GSM) [22288] I WIND (UMTS) [22201] I TIM (UMTS) [22201] I TIM (GSM) [22210] vodafone IT (GSM) [22210] vodafone IT (UMTS) [22299] 3 ITA (UMTS) [22299] 3 ITA (UMTS)

You can choose an operator from the list, to perform "Manual" or "Manual/Automatic" selection.

19.1.12 DDNS Configuration

By clicking on the "DDNS Configuration" link, in the "Mobile Configuration" menu, you come to the following page:

 ← → C ① 192.168.85.104:8080/ddns_conf.php ☆ Z : SENECA® General Configuration Main View Network and Services 	🗋 Z-PASS2-S	×		(!) Cioxenni —		×
General Configuration DDNS Configuration [user: admin] [logout] Main View Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G] Network and Services Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G]	/ =			<u>م</u>	7	:
General Configuration DDNS Configuration [user: admin] [logout] Main View Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G] Network and Services Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G]	© SENEC A®	7-PΔSS2-S				
Main View Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G]	ULINLUA		l[logout]			
Firmware version: Sw002940_332 [Modem: 0C20GQBR03A14E1G]						
Network and Dervices		Firmware Version: SW002940_33	2 [Modem: UC2	20GQBR03A14E1G]		
Real Time Clock Setup		MAC Address: C8F9811B0000 [IM	IEI: 861075026	500975] [IMSI: 222101600237890]		
VPN Configuration Internet Access: Ethernet		Internet Access: Ethernet				
Router Configuration Energy Protocols: none		Energy Protocols: none				
EW Upgrade						
Conf. Management		Router: running				
Mobile Configuration			CURRENT			
Mobile Network CURRENT UPDATED			CURRENT	OPDATED		
DDNS Configuration DDNS Configuration	DDNS Configuration	DDNS Configuration				
Digital I/O Type None None		Туре	None	None 🔻		
Digital I/O Configuration Hostname		Hostname				
Diagnostics Hostname FW Versions Username	_					
Ethornat Interfaceo						
Password						
Data Logger (SD found)		APPLY				
Logs						
DDNS Update Status		DDNS Update \$	Status			
Status		5	Status			
IP Address		IP Ad	dress			

Field	Meaning	Default value
Туре	Type of Dynamic DNS service;	None
	possible values are:	
	- None	
	- dyndns.it	
	- dyndns.org	
	- no-ip.com	
Hostname	The hostname provided with the service	empty
	subscription	
Username	The username provided with the service	empty
	subscription	
Password	The password provided with the service	empty
	subscription	

In this page, you can set the parameters related to the Dynamic DNS service, as listed in the following table:

The parameters shall be set according to the DDNS service subscription; an example is given in the following figure.

🗋 Z-PASS2-S	×	(!) Ciovanti — 🗆 🗙
$\epsilon \rightarrow \mathbf{C}$ (i) Non si	curo 192.168.85.104:8080/ddns_conf.php	☆ 🗷 :
SERVECA® General Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration FW Upgrade Conf. Management	Z-PASS2-S DDNS Configuration [user: admin] [logout] Firmware Version: SW002940_332 [Modem: UC MAC Address: C8F9811B0000 [IMEI: 861075026 Internet Access: Ethernet Energy Protocols: none PLC Status: running (app: s203) Router: running	
Mobile Configuration Mobile Network DDNS Configuration Digital I/O Digital I/O Configuration	CURRENT DDNS Configuration Type dyndns.it	UPDATED dyndns.it T
Diagnostics FW Versions Ethernet Interfaces	Hostname zpasstest1.ns0.it Username gsp-seneca	zpasstest1.ns0.it gsp-seneca
Modbus Modules Data Logger (SD found) Logs	Password egdirba!	123456
	DDNS Update Status Status IP Address	

When an IP address assigned to the Mobile Network Interface has been bound with the hostname, the "DDNS Update Status" section appears like in the following figure.

← → C ① 192.168.85.104:8080/ddns_conf.php ★ → C ○ 198.2001 ★ → C ○ 198.2001 ★ → C ○ 198.2001 ↓ ← H → C ○ 198.2001 ↓ ←	1G] 22101600237890]
Seneral Configuration DDNS Configuration [user: admin] [logout] Main View Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G] Machad Services MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Real Time Clock Setup Internet Access: Mobile Router Configuration Energy Protocols: none PLC Status: running (app: s203) Router: running W Upgrade Outer: running Sonf. Management DDNS Configuration Mobile Configuration DDNS Configuration Digital I/O Type Digital I/O Type Digital I/O Type Objectal Logger (SD found) Username	22101600237890]
Main View Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G] Network and Services MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Real Time Clock Setup Internet Access: Mobile Real Time Configuration Energy Protocols: none Router Configuration PLC Status: running (app: s203) Router: running Router: running Conf. Management Mobile Configuration Mobile Network DDNS Configuration Digital VO Type Digital VO Type Oligital VO Type Oligital VO Spastest1.ns0.it PW Versions Username Ethernet Interfaces Password Modbus Modules Password Data Logger (SD found) APPLY	22101600237890]
Main View Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G] Network and Services MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Real Time Clock Setup Internet Access: Mobile VPN Configuration Energy Protocols: none Router Configuration PLC Status: running (app: s203) FW Upgrade Router: running Conf. Management Mobile Network DDNS Configuration DDNS Configuration Digital I/O Type Digital I/O Type Digital I/O Type FW Versions Username Ethernet Interfaces Password Modbus Modules Password Data Logger (SD found) APPLY	22101600237890]
Network and Services Real Time Clock Setup WAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890] Internet Access: Mobile Router Configuration Ruser Configuration Users Configuration FW Upgrade Conf. Management Mobile Network DDNS Configuration Digital I/O Diagnostics FW Versions Ethernet Interfaces Modbus Modules Data Logger (SD found)	22101600237890]
Real Time Clock Setup Internet Access: Mobile VPN Configuration Energy Protocols: none Router Configuration PLC Status: running (app: s203) FW Upgrade Router: running Conf. Management Mobile Configuration Mobile Configuration CURRENT UPDATED UPDATED DDNS Configuration OUPS Configuration Digital I/O Type Digital I/O Type Digital I/O Hostname Ethernet Interfaces Password Password egdirba! APPLY	
WPN Configuration Energy Protocols: none Router Configuration PLC Status: running (app: s203) FW Upgrade Router: running Conf. Management CURRENT Mobile Configuration DDNS Configuration Mobile Network DDNS Configuration Digital I/O Type Digital I/O Hostname Digital I/O Hostname Geger (SD found) Username APPLY APPLY	PDATED
Jsers Configuration FW Upgrade Conf. Management Mobile Configuration Mobile Network DDNS Configuration Digital I/O Digital I/O <td>PDATED</td>	PDATED
FW Upgrade Router: running Conf. Management Mobile Configuration Mobile Network DDNS Configuration Digital I/O Type Oigital I/O Configuration dyndns.it Digital I/O Configuration Hostname Diagnostics Username FW Versions Username Ethernet Interfaces Password Modbus Modules APPLY	2DATED
FW Upgrade Conf. Management Mobile Configuration Mobile Network DDNS Configuration Digital I/O Digital I/O Configuration Bigital I/O Configuration Digital I/O Configuration Bigital I/O Configuration Digital I/O Configuration Digital I/O Configuration Bigital I/O Configuration Bigital I/O Configuration Bigital I/O Configuration Digital I/O Configuration Bigital I/O Configuration Bigital I/O Configuration Bigital I/O Configuration Bigital I/O Configuration<	PDATED
Conf. Management Mobile Configuration Mobile Network DDNS Configuration Digital I/O	PDATED
Mobile Configuration CURRENT UPDATED Mobile Network DDNS Configuration DDNS Configuration UPDATED Digital I/O Digital I/O Type dyndns.it dyndns.it Digital I/O Hostname gsp-seneca gsp-seneca Ethernet Interfaces Password egdirba! egdirba!	PDATED
Mobile Network DDNS Configuration DDNS Configuration DDNS Configuration Digital I/O Type Origital I/O Configuration Type Digital I/O Configuration Hostname Two Password gsp-seneca Ethernet Interfaces Password Modbus Modules APPLY	
Digital I/O Type dyndns.it dyndns.it Digital I/O Configuration Hostname zpasstest1.ns0.it zpasstest1.ns0.it Diagnostics Username gsp-seneca gsp-seneca Ethernet Interfaces Password egdirba! egdirba!	
Digital I/O Configuration Type dynams.it dynams.it Diagnostics Hostname zpasstest1.ns0.it FW Versions Username gsp-seneca Ethernet Interfaces Password egdirba! Modbus Modules APPLY	
Diagnostics Hostname zpasstest1.ns0.it zpasstest1.ns0.it FW Versions Username gsp-seneca gsp-seneca Ethernet Interfaces Password egdirba! Modbus Modules APPLY APPLY	
Ethernet Interfaces Password egdirba! Modbus Modules APPLY	
Ethernet Interfaces Password egdirba! egdirba! Modbus Modules Data Logger (SD found)	
Modbus Modules APPLY APPLY APPLY	
Data Logger (SD found)	
DDNS Update Status	
Status good	boc
IP Address 2.45.73.76	45.73.76

19.1.13 Digital I/O Configuration

By clicking on the "Digital I/O Configuration" link, in the "Digital I/O" menu, you come to the page described in the following sub-paragraphs¹⁹; the page differs between Z-TWS4-IO and Z-PASS2-S-IO:

19.1.13.1 Z-PASS2-S-IO

¹⁹ This page is available only for Z-TWS4-IO and Z-PASS2-S-IO products.

D Z-PASS2-S	×				(!) Ciovanti	- □ >
\leftarrow \rightarrow C (i) 192.16	8.85.104:8080/digio	_conf.php				☆ 🗵
SENECA® General Configuration Main View Network and Services Real Time Clock Setup	Z-PASS2-S Digital I/O Confi Firmware Versic MAC Address: 0	on: SW00294	40_332 [Mod	em: UC20GQBR	03A14E1G] [IMSI: 2221016002	37890]
VPN Configuration Router Configuration Users Configuration FW Upgrade Conf. Management	Internet Access Energy Protoco PLC Status: run Router: running	ls: none ning (app: s	203)			
Mobile Configuration Mobile Network				CURRENT	UPDATED)
DDNS Configuration Digital I/O Digital I/O Configuration Diagnostics FW Versions Ethernet Interfaces Modbus Modules Data Logger (SD found) Logs	APPLY	((Input/ Input/	Dutput 2 Mode Dutput 1 Mode Dutput 2 Mode Security Leve	Remote connection disable Remote connection active General input General output General input General output	Remote connection Remote connection General input ▼ General output ▼ General output ▼ VPN Connection	
			Digital I/O	Status		
	DI 1	DO 1	DI 2	DO 2	DIDO 1	DIDO 2
	LOW	LOW	LOW	LOW	LOW	LOW

In this page, you can configure the operating modes of the Digital I/Os and the security level applied by the "Remote Connection Disable" feature (see chapter 13).

Field	Mear	ning			Default value
Input 1 Mode	This	parameter	represents	the	Remote connection disable

	an available of the Division of	
	operating mode of the Digital Input	
	1 (DI 1).	
	Since this is the digital input used for	
	"Remote Connection Disable"	
	feature, its value ("Remote	
	connection disable") cannot be	
	changed.	
Output 1 Mode	This parameter represents the	Remote connection active
	operating mode of the Digital	
	Output 1 (DO 1).	
	Since this is the digital output used	
	to monitor remote connection, its	
	value ("Remote connection active")	
	cannot be changed.	
Input 2 Mode	This parameter represents the	General input
	operating mode of the Digital Input	
	2 (DI 2).	
	Possible modes are: "General input"	
	"Local alarm".	
Output 2 Mode	This parameter represents the	General output
	operating mode of the Digital	
	Output 2 (DO 2).	
	Possible modes are: "General	
	output" "Remote toggle" ²⁰ .	
Input/Output 1 Mode	This parameter represents the	General input
	operating mode of the Digital	
	Input/Output 1 (first configurable	
	digital I/O) (DIDO 1).	
	Possible modes are: "General input"	
	"General output".	
Input/Output 2 Mode	This parameter represents the	General output
	operating mode of the Digital	Scheraroutput
	Input/Output 2 (second configurable	
	digital I/O) (DIDO 2).	
	Possible modes are: "General input"	
	"General output".	
Service Disable	This parameter determines which access	VPN Connection
	services are disabled when "Remote	
	Connection Disable" digital input is HIGH.	
	Possible values are: "VPN Connection"	
	"VPN Service" "Internet Connection"	
	"SMS Service".	
	See chapter 13, for a detailed	
	. ,	1

²⁰ "Remote toggle" function is still to be defined.

description of these values.

The "Digital I/O Status" section of the page gives the current status values ("LOW"/"HIGH") for each of the six available digital I/Os.



The status of the digital input configured as "Local Alarm" is reported in the "ALARM" column in the "Devices" tab of the "Seneca VPN Box Manager" and "Seneca VPN Client Communicator" applications.

_	SingleLan (tlc.sened Itente Connesso SUPERVIS	OR						SEN
s Dis	spositivi SENECA Accessi	/PN						
)isposi	itivo/î, 2 nuovi, 0 in aggiomar	nento, 5 configurati, 0 in alla	ame					€ Aggioma
	TAG	MAC	IMEI	STATUS	ALARM	SIGNAL	UPTIME	
۲	zpass1_C8F981160066	C8:F9:81:16:00:66	MODEM NON INSTALLA	SERVICE OFF - VPN DO	\circ	-		Reset
۲	ELTECO	C8:F9:81:1B:00:06	861075026509463	SERVICE OFF - VPN DO		-	-	Reset
۲	GREEN_METHANE2	C8:F9:81:02:01:D6	862264020120993	SERVICE ON - VPN UP	•	6/7	Last 06/10/2017 11.43.5	Reset
۲	Demo	C8:F9:81:16:00:9E	862264020393319	SERVICE OFF - VPN DO		-	-	Reset
•	zpass2s_C8F981160017	C8:F9:81:16:00:17	862264020382288	SERVICE OFF - VPN DO			-	Reset
•	ZEUS001	C8:F9:81:15:00:94	MODEM NON INSTALLA	SERVICE OFF - VPN DO			-	Reset
0	TOPCO	C8:F9:81:11:00:6D	862264020400825	SERVICE OFF - VPN DO		-		Reset
Configu	urazione CONFIGURED, u	timo refresh 27/09/2017 14	4.17.08	- DI1 NA		OFF	DIDO1 CONNECTION DISAE	☆ Configura
Conr	Network 192.168	.96.0/255.255.255.0 (VPN	10.9.1.133)	ON DO1 VP	N STATUS	OFF	DIDO2 INPUT	
	Versione ver. SW002940	331, hw Z-PASS1-R02, mod	le LAN/WAN	- DI2 NA				e Elimina

19.1.13.2 Z-TWS4-IO

Z-TWS4	×				(1) Ciovann	đ —			×	
	8.85.103:8080/dig	io_conf.php					☆	J.	:	
		F							•	
SENECA SENECA	Z-TWS4									
General Configuration	Digital I/O Configuration [user: admin] [logout]									
Main View	Firmware Vers	ion: SW00294	0_335							
Network and Services	MAC Address:	C8F9811B000	1							
Real Time Clock Setup VPN Configuration	Internet Acces	s: Ethernet								
Router Configuration	Energy Protoc	ols: none								
Users Configuration	PLC Status: ru		t rupping)							
FW Upgrade			(Tunning)							
Conf. Management	Router: disable	ea								
Digital I/O				CURRENT	UPDATED					
Digital I/O Configuration Diagnostics		DiottoLUO	Configuration							
FW Versions		Digital 1/0 0	Configuration							
Ethernet Interfaces		0		Remote connection active	Remote connection active •					
Modbus Modules		0	utput 2 Mode	General output	General output ▼					
Data Logger (SD missing)		Input/O	utput 1 Mode	Remote connection disable	Remote connection disable v					
		Input/O	utput 2 Mode	General output	General output *					
		8	Security Level							
		Se	rvice Disable	VPN Connection	VPN Connection •					
	APPLY									
			Digital I/O	Status						
	DO 1	DO 2	DIDO 1	DIDO 2						
	LOW	LOW	LOW	LOW						

In this page, you can configure the operating modes of the Digital I/Os and the security level applied by the "Remote Connection Disable" feature (see chapter 13).

Field	Meaning	Default value
Output 1 Mode	This parameter represents the operating mode of the Digital Output 1 (DO 1).	Remote connection active

	Since this is the digital output used	
	to monitor remote connection, its	
	value ("Remote connection active")	
	cannot be changed.	
Output 2 Mode	This parameter represents the	General output
	operating mode of the Digital	General output
	Output 2 (DO 2).	
	Possible modes are: "General	
land (Output 1 Mada	output" "Remote toggle" ²¹ .	Devente composition disable
Input/Output 1 Mode	This parameter represents the	Remote connection disable
	operating mode of the Digital	
	Input/Output 1 (first configurable	
	digital I/O) (DIDO 1).	
	Since this is used as an input for	
	"Remote Connection Disable"	
	feature, its value ("Remote	
	connection disable") cannot be	
	changed.	
Input/Output 2 Mode	This parameter represents the	General output
	operating mode of the Digital	
	Input/Output 2 (second configurable	
	digital I/O) (DIDO 2).	
	Possible modes are: "General input"	
	"General output" "Local alarm".	
Service Disable	This parameter determines which	VPN Connection
	access services are disabled when	
	"Remote Connection Disable" digital	
	input is HIGH.	
	Possible values are: "VPN	
	Connection" "VPN Service"	
	"Internet Connection" "SMS	
	Service".	
	See chapter 13, for a detailed	
	description of these values.	

The "Digital I/O Status" section of the page gives the current status values ("LOW"/"HIGH") for each of the four available digital I/Os.

19.1.14 I/O View (S6001-RTU)

In S6001-RTU CPU, one more page is available called "I/O View"; in this page, the current status of all the inputs/outputs is shown, along with some diagnostic information.

²¹ "Remote toggle" function is still to be defined.

🕒 S6001-RTU	×	Giovanni _	×
← → Ĉ 🗋 192.	.168.85.105:8080/io_view.php	Q	☆ =
	DIAGNOSTICS Error Status 0		
	CRC Error Counter 0		

The following parameters are shown:

Field	Meaning	Values
DIGITAL INPUTS/Input 1Input 15	Status of Digital Input	LOW/HIGH
DIGITAL OUTPUTS/Output	Status of Digital Output (relay)	OPEN/CLOSED
1Output 8		
DIGITAL OUTPUTS/12 Volt Enable	Status of Digital Output enabling 12	LOW/HIGH
Output	Vdc voltage on screw terminals 37	
	and 38	
ANALOG INPUTS/Current 1	Value of analog current input (in uA)	020000

Current 4		
ANALOG OUTPUT/Current	Value of analog current output (in	020000
	uA)	
ANALOG OUTPUT/Voltage	Value of analog voltage output (in	010000
	mV)	
ELECTRODES/Level	Liquid level value	0,1,2
ELECTRODES/Sensitivity	Sensitivity value applied in liquid	0255
	level measurement (in $k\Omega$)	
DIAGNOSTICS/Error Status	This parameter gives an information	0: no error
	about errors that might occur in the	Bit 9: flash memory error
	I/O board. The value is a bitmask, as	
	specified in the column "Values".	
DIAGNOSTICS/CRC Error Counter	This parameter counts the CRC	>= 0
	errors occurring in the	0 means "no CRC error"
	communication between the CPU	
	board and the I/O board; if the value	
	continuously increases, it means	
	that there is some HW problem	

If the Soft PLC application is not running, inputs/outputs values are not available, so the page appears like in the following figure:

19.1.15 FW Versions

By clicking on the "FW Versions" link, in the "Diagnostics" menu, you come to the following page:

Image: Partial state Image: Partial state
General Configuration FW Versions [user: admin] [logout] Main View Firmware Version: SW002940_332 [Modem: UC20GQBR03A14E1G] Network and Services MAC Address: C8F9811B0000 [IME1: 861075026500975] [IMSI: 222101600237890] Real Time Clock Setup Internet Access: Mobile VPN Configuration Energy Protocols: none Router Configuration PLC Status: running (app: s203) FW Upgrade Router: running Conf. Management Mobile Configuration Mobile Configuration HW Version Jogital I/O FW Components Versions Digital I/O FW Components Versions Digital I/O Linux Kernel Put Versions Linux Kernel Ethernet Interfaces Initial RAM Disk Modbus Modules Defaul Disk File System SW002940_332 Data Logger (SD found) Disk File System SW002940_332

In this page, the following information are shown:

- the product name along with its HW revision (in the above figure: "Z-PASS2-S-R01")
- the version strings of all the FW components, which are:
 - Linux Kernel (*kernel*)

- Initial RAM Disk (initrd)
- Root File System (rootfs)
- Default Disk File System (*diskdfl*)
- Disk File System (*disk*)

19.1.16 *Ethernet Interfaces*

By clicking on the "Ethernet Interfaces" link, in the "Diagnostics" menu, you come to the following page:

Z-PASS2-S	×		🤔 Giovanni	– 🗆 X
	8.85.103:8080/eth_stats.php			☆ :
SENECA [®]	Z-PASS2-S			
General Configuration	Ethernet Status [user: admin] [logout]			
Main View	Firmware Version: SW002940_310 [Moder	m: 1231B02SIM5350E]		
Network and Services	MAC Address: C8FA81160002	-		
Real Time Clock Setup				
VPN Configuration	Internet Access: Ethernet			
Router Configuration	Energy Protocole: none			
Users Configuration	PLC Status: running (app not running)			
FW Upgrade	Router: running			
Mobile Configuration	_			
Mobile Network Diagnostics	LAN ETHERNET			
Ethernet Interfaces	Link Status	Down		
Modbus Modules	RX Packets / Bytes	0/0		
Data Logger (SD found)	TX Packets / Bytes	0/0		
Logs	WAN ETHERNET			
	Link Status	Up		
	RX Packets / Bytes	11936 / 970.6K		
	TX Packets / Bytes	1533 / 492.0K		
	REFRESH			

The above figure applies to a Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO CPU, when the "Ethernet Mode" is "LAN/WAN".

In this page, for each of the two available Ethernet interfaces (LAN and WAN), the following information is shown:

- the Ethernet link status (i.e. "Down" or "Up")
- the number of packets/bytes received from the Ethernet interface, when the link is up; "0/0" when the link is down
- the number of packets/bytes sent to the Ethernet interface, when the link is up; "0/0" when the link is down

For Z-TWS4, Z-PASS2-S, S6001-RTU and for Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO when the "Ethernet Mode" is "Switch", the "Ethernet Interfaces" page is similar to the one shown in the following figure.

	0	5 Giovanni	– 🗆 X
🗋 Z-PASS2-S	×		
\leftarrow \rightarrow C (i) 192.16	58.85.103:8080/eth_stats.php		☆ :
SENECA® General Configuration	Z-PASS2-S Ethernet Status [user: admin] [logout]		
Main View Network and Services	Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]		
Real Time Clock Setup	MAC Address: C8FA81160002 Internet Access: Ethernet		
VPN Configuration Router Configuration	Energy Protocols: none		
Users Configuration	PLC Status: running (app not running)		
FW Upgrade Mobile Configuration	Router: running		
Mobile Network	ETHERNET		
Diagnostics Ethernet Interfaces			
Modbus Modules	RX Packets / Bytes 1658 / 160.8K		
Data Logger (SD found)	TX Packets / Bytes 199 / 36.3K		
Logs	REFRESH		
L			

In this page, for the one available Ethernet interface, the following information is shown:

- the number of packets/bytes received from the Ethernet interface
- the number of packets/bytes sent to the Ethernet interface

You can refresh the Ethernet status, by clicking on the "REFRESH" button.

19.1.17 Modbus Modules

By clicking on the "Modbus Modules" link, in the "Diagnostics" menu, you come to a page similar to the one in the following figure:

	CO OF 102-000		and a state of the				4			
← → C ① 192.1	68.85.103:808	J/modules_sta	tus_view.pnp				☆			
SENECA °	Z-PASS2-S	6								
General Configuration	Modules S	Modules Status View [user: admin] [logout]								
Main View	Firmware	Version: SW(02940_310 [Mode	m: 1231B02SIM5350E]						
Network and Services	MAC Add		160002							
Real Time Clock Setup		MAC Address: C8FA81160002								
VPN Configuration	Internet A	Internet Access: Mobile								
Router Configuration	Energy Pr	Energy Protocols: none								
Users Configuration	PLC Statu	s: running								
FW Upgrade Mobile Configuration	Router: di	sabled								
Mobile Network										
Diagnostics										
Ethernet Interfaces	INDEX	ADDRESS	PORT	ТҮРЕ	STATUS					
Modbus Modules	1	2	COM2 COM2	Z-10-DOUT Z-4AI 1	OK OK					
Data Logger (SD found)	2	3	COM2 COM2	Z-4AL1 Z-4AL1	OK					
Logs	4	5	COM2 COM2	Z-DAQ-PID	OK					
	-	-								

This page shows a table containing a row for each Modbus RTU Slave modules configured in the Z-NET4²²/Straton project; each row contains the following information:

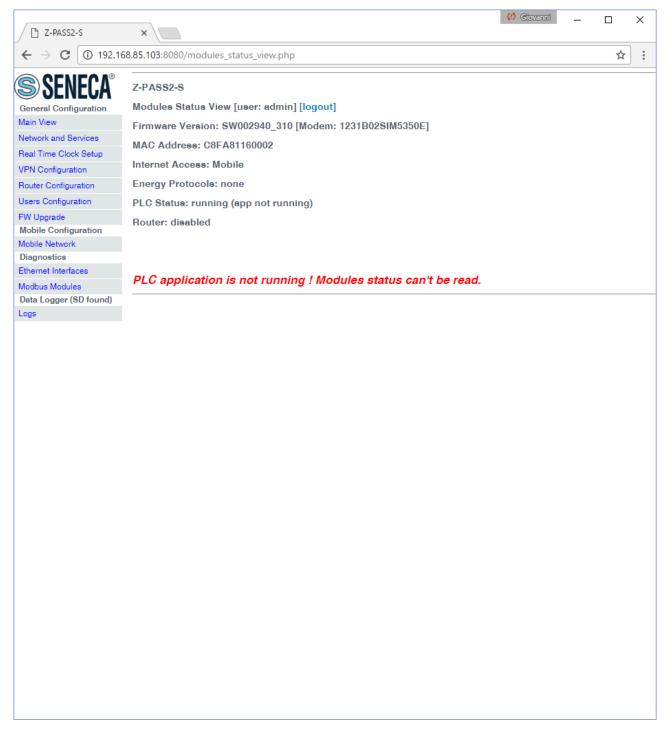
- a progressive index
- the Modbus Slave Address
- the name of the serial port (i.e. COM1/COM2/COM4) which the module is connected to
- the type of module
- the module status, which can be:
 - \circ "OK", if the module is correctly responding to Modbus requests
 - \circ "TIMEOUT", if the module is not responding to Modbus requests
 - "ERROR", if any other error occurs

The Modbus Modules page can't be shown in the following situations:

- if a Z-NET4 project is not loaded on the Device
- if TWS/PLC services are not running
- if a PLC application is not running, i.e. not present or stopped

As an example, for the third of the above cases, the following message is shown:

²² For information on Z-NET4 SW, please see chapter 21.



19.1.18 *M-Bus Scan*

By clicking on the "M-Bus Scan" link, in the "M-Bus" menu, you come to the following page.

SENECA®	Z-PASS2-	Z-PASS2-S								
General Configuration	M-Bus Sc	M-Bus Scan [user: admin] [logout]								
Summary	Firmware	Version: SW00294	0_344 [Mode	m: UC200	GQBR03A14E1G]					
Network and Services	MAC Add	ress: C8F9811B02	A0 [IME]: 861	07502949	40021 [IMSI: 240422600279769]					
Real Time Clock Setup										
VPN Configuration	Internet A	ccess: Ethernet								
Router Configuration	Energy Pr	otocols: none								
Users Configuration	PLC Statu	is: running (app: n	nbus_vars)							
FW Upgrade	Router: di	isabled								
Conf. Management										
Modbus TCP Client										
Mobile Configuration										
Mobile Network				s Scan Para						
DDNS Configuration	NC	OTE: only on serial po	rt COM1 with m	ode set to 2	z-mbus					
Digital I/O Configuration				Baud Rat						
Digital I/O Configuration		NOTE: "All" mea	ins all baud rate	es except fo	or 38400					
M-Bus			15,	Addres or secondar	ss Mask FFFFFFFFFFFFFFFF					
M-Bus Scan										
M-Bus Configuration		PRIMARY SCAN	SECONDAR	Y SCAN	CREATE CONFIGURATION					
Diagnostics										
FW Versions					1					
Ethernet Interfaces			RE	AD DATA						
Modbus Modules	#	Baud Ra	te		Address					
Data Logger (SD missing)										
					No device					

This page lets you run scan procedures to search for M-Bus devices and read data from the detected devices.

To let these procedures properly work, you have to:

- connect the Seneca "Z-MBUS" RS232-MBUS adapter to the COM1 serial port;
- set the COM1 mode to Z-MBUS (see paragraph 19.1.2).

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-rate²³; then click on the button; a confirmation pop-up will be shown.

192.168.85.106:8080 dice		
Run secondary scan for M-Bus devices with and address mask FFFFFFFFFFFFFFFFFFF ?) baud rate 2400	
	ок	Annulla

After confirming, the following page will be shown.

²³ Actually, the "All" option executes the scan for all possible baud-rates, except for 38400, that is: 300, 600, 1200, 4800, 9600, 19200; 38400 value can be selected separately.

SENECA	Z-PASS2-	s				
General Configuration	M-Bus Sc	an [user: admin] [logout]				
Summary	Firmware	Version: SW002940_344 [Mo	dem: UC20GQBR03A14E1G]			
Network and Services	MAC Add	ress: C8E9811B02A0 [IME]: 8	610750294940021 [IMSI: 24042260	02797691		
Real Time Clock Setup						
VPN Configuration	Internet A	Internet Access: Ethernet				
Router Configuration	Energy P	rotocols: none				
Users Configuration	PLC Statu	PLC Status: running (app: mbus_vars)				
FW Upgrade	Router: d	Router: disabled				
Conf. Management						
Modbus TCP Client						
Mobile Configuration	Start M-B	us scan, please wait				
Mobile Network	(this will t	ake some minutes)				
DDNS Configuration		-				
Digital I/O Configuration		5	TOP SCAN			
Digital I/O Configuration						
M-Bus	#	Baud Rate	Address			
M-Bus Scan					1	
M-Bus Configuration			No device			
Diagnostics						
FW Versions						
Ethernet Interfaces						
Modbus Modules						
Data Logger (SD missing)						

The scan procedure may take several minutes to be completed, so the page shows the number of seconds elapsed; the devices are shown in term of their secondary address and baud rate as soon as they are detected.

SENECA ®	Z-PASS2-	s					
General Configuration	M-Bus Scan [user: admin] [logout]						
Summary	Firmware	Version: SW002940_344 [M	Iodem: UC20GQBR03A14E1G]				
Network and Services		- • •					
Real Time Clock Setup	MAC Address: C8F9811B02A0 [IMEI: 861075029494002] [IMSI: 240422600279769]						
VPN Configuration	Internet Access: Ethernet						
Router Configuration	Energy P	Energy Protocols: none					
Users Configuration	PLC State	PLC Status: running (app: mbus vars)					
FW Upgrade		Router: disabled					
Conf. Management	Router, d	Isabled					
Modbus TCP Client							
Mobile Configuration	M-Bus sc	an in progress with baud r	ate 2400, please wait				
Vobile Network	(55 secor	nds elapsed)					
DDNS Configuration							
Digital I/O Configuration			STOP SCAN				
Digital I/O Configuration	#	Baud Rate (2400)	Address (Mask=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF				
M-Bus	1	2400	00008431614C0402				
M-Bus Scan		2400	00008431614C0402				
M-Bus Configuration	2	2.000					
Diagnostics	3	2400	00008434614C0402				
FW Versions	4	2400	00008435614C0402				
			00000 10001 100 100				
Ethernet Interfaces	5	2400	00008436614C0402				
Ethernet Interfaces Modbus Modules	5 6	2400 2400	00008436614C0402 00008441614C0402				
Modbus Modules		2100	0000010001100102				
	6	2400	00008441614C0402				
Nodbus Modules	6 7	2400 2400	00008441614C0402 00008444614C0402				
Nodbus Modules	6 7 8	2400 2400 2400	00008441614C0402 00008444614C0402 00008446614C0402				

The "STOP SCAN" button lets you abort the procedure; anyway, the partial results are kept.

At the end of the procedure the webserver indicate the end of the scan and then the following page is displayed:

SENECA [®]	Z-PASS2-S	6	
General Configuration	M-Bus Sca	an [user: admin] [logout]	
Summary	Firmware	Version: SW002940 344	[Modem: UC20GQBR03A14E1G]
Vetwork and Services		-	
eal Time Clock Setup		-	EI: 861075029494002] [IMSI: 240422600279769
PN Configuration	Internet A	ccess: Ethernet	
outer Configuration	Energy Pro	otocols: none	
Isers Configuration	PLC Statu	s: running (app: mbus \	ars)
W Upgrade	Router: di		,
onf. Management	Nouter. u.	Sabled	
lodbus TCP Client			
lobile Configuration			
Aobile Network		TE: only on serial port COM1	M-Bus Scan Parameters
DNS Configuration	NO	TE. only on senal port COM	
Digital I/O Configuration		NOTE: "All" means all b	Baud Rate (bit/s) All
igital I/O Configuration		NOTE. All means and	Address Maste
1-Bus Scan			(for secondary scan)
-Bus Configuration		PRIMARY SCAN SECO	ONDARY SCAN CREATE CONFIGURATION
iagnostics			
V Versions			
hernet Interfaces			READ DATA
dbus Modules	#	Baud Rate (2400)	Address (Mask=FFFFFFFFFFFFFFFFFF)
ta Logger (SD missing)	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
	20	2400	20884073C514010D
	20	2400	200040730314010D

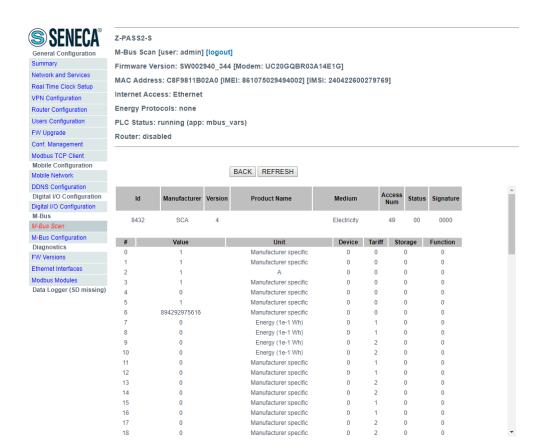
The baud rate value shown in the table header remembers the parameter choice for the last scan procedure.

The table with the detected M-Bus devices is stored in a permanent way, so after switching off and on the CPU, the results of the last scan are still available; they will be overwritten by the next scan or deleted by a factory reset ("FACTORY DEFAULT" button in "Main View" page).

In the same way the "PRIMARY SCAN" button lets you scan the bus, detecting M-Bus primary addresses; select the correct baud-rate for the COM1 serial port or select "All" to repeat the scan for any possible baud-rate²⁴.

You can read data from one of the devices, by selecting the corresponding row and clicking on the "READ DATA" button; you come to a page like the following.

²⁴Actually, the "All" option executes the scan for all possible baud-rates, except for 38400, that is: 300, 600, 1200, 4800, 9600, 19200; 38400 value can be selected separately.



In this page:

- the first table contains only one row, providing the "slave information";

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

By clicking on the "REFRESH" button, you can refresh the data; by clicking on the "BACK" button, you come back to the page with the devices table.

19.1.18.1 CREATE CONFIGURATION BUTTON

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

🤍 JEINEUA	2-FA33	2-0					
General Configuration	M-Bus S	can [user: admin] [logout]					
Summary	Firmwar	e Version: SW002940 344	[Modem: UC20GQBR03A14E1G]				
Network and Services		—					
Real Time Clock Setup	MAC AG	MAC Address: C8F9811B02A0 [IMEI: 861075029494002] [IMSI: 240422600279769]					
VPN Configuration	Internet	Internet Access: Ethernet					
Router Configuration	Energy	Energy Protocols: none					
Users Configuration	PLC Sta	PLC Status: running (app: mbus_vars)					
FW Upgrade	Router:	disabled					
Conf. Management							
Modbus TCP Client							
Mobile Configuration							
Mobile Network			M-Bus Scan Parameters				
DDNS Configuration		NOTE: only on serial port COM1	with mode set to Z-MBUS				
Digital I/O Configuration			Baud Rate (bit/s)				
Digital I/O Configuration		NOTE: "All" means all b	aud rates except for 38400				
M-Bus			Address Mask FFFFFFFFFFFFFFFF				
M-Bus Scan			(for secondary scan)				
M-Bus Configuration		PRIMARY SCAN SECO	ONDARY SCAN CREATE CONFIGURATION				
Diagnostics							
FW Versions							
Ethernet Interfaces			READ DATA				
Modbus Modules	#	Baud Rate (2400)	Address (Mask=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF				
Data Logger (SD missing)	1	2400	00008431614C0402				
	2	2400	00008432614C0402				
	3	2400	00008434614C0402				

In this way you have stored the actual M-BUS configuration. The webserver than move automatically to the next "M-Bus Configuration" page.

19.1.19 M-Bus Configuration

When you have pressed the "Create Configuration" in the M-Bus Scan page you will obtain the following page in the M-Bus Configuration:

M-Bus Configurat	ion [user: admin] [l	ogout]					
Firmware Version: SW002940 344 [Modem: UC20GQBR03A14E1G]							
	-	861075025454002J [IMISI. 2404	226002/9/69]				
Internet Access: E	Ethernet						
Energy Protocols:	Energy Protocols: none						
PLC Status: running (app: mbus_vars)							
Router: disabled							
ADD	DELETE	CREATE	TAGS				
NOTE: for each devi	ce tags will have the p	efix "MRUSy " where "y" is the val	ue in the "Tag Prefix				
column.	in nave the pr		Letter tog i fork				
		Address	Scan Rate (s				
MBUS 1	2400	00008431614C0402	60				
MBUS ₂	2400	00008432614C0402	60				
MBUS 3	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				
	2400	00008453614C0402	60				
	2400	00008454614C0402	60				
MBUS12	2400	00008458614C0402	60				
MBUS13	2400	00008461614C0402	60				
MBUS14	2400	00008464614C0402	60				
	2400	00008466614C0402	60				
MBUS 15							
	2400	00008470614C0402	60				
MBUS15 MBUS16 MBUS17		00008470614C0402 00008471614C0402	60 60				
MBUS16 MBUS17	2400	00008471614C0402	60				
MBUS 16	2400 2400						
	Firmware Version MAC Address: C8 Internet Access: E Energy Protocols PLC Status: runni Router: disabled ADD NOTE: for each devic column. Tag Prefix MBUS1 MBUS2 MBUS3 MBUS4 MBUS5 MBUS5 MBUS6 MBUS7 MBUS8 MBUS9 MBUS9 MBUS10 MBUS11 MBUS12 MBUS12 MBUS12 MBUS13	M-Bus Configuration [user: admin] [li Firmware Version: SW002940_344 [M MAC Address: C8F9811B02A0 [IMEI: Internet Access: Ethernet Energy Protocols: none PLC Status: running (app: mbus_var: Router: disabled ADD DELETE NOTE: for each device, tags will have the pr column. Tag Prefix Baud Rate MBUS[1 2400 MBUS[2 2400 MBUS[3 2400 MBUS[5 2400 MBUS[5 2400 MBUS[5 2400 MBUS[5 2400 MBUS[5 2400 MBUS[5 2400 MBUS[5 2400 MBUS[6 2400 MBUS[6 2400 MBUS[6 2400 MBUS[6 2400 MBUS[7 2400 MBUS[7 2400 MBUS[8 2400 MBUS[8 2400 MBUS[9 2400 MBUS[10 2400 MBUS[11 2400 MBUS[13 2400	M-Bus Configuration [user: admin] [logout] Firmware Version: SW002940_344 [Modem: UC20GQBR03A14E1G] MAC Address: C8F9811B02A0 [IMEI: 861075029494002] [IMSI: 2404 Internet Access: Ethernet Energy Protocols: none PLC Status: running (app: mbus_vars) Router: disabled ADD DELETE CREATE NOTE: for each device, tags will have the prefix "MBUSx_", where "x" is the value column. MBUS1 2400 00008431614C0402 MBUS2 2400 00008433614C0402 MBUS3 2400 00008433614C0402 MBUS5 2400 00008436614C0402 MBUS6 2400 00008436614C0402 MBUS6 2400 00008436614C0402 MBUS6 2400 00008446614C0402 MBUS6 2400 00008446614C0402 MBUS6 2400 00008446614C0402 MBUS6 2400 00008446614C0402 MBUS6 2400 00008446614C0402 <tr< td=""></tr<>				

The scan result can now be edited.

The 1st column represent the Straton Tag Prefix name for the device.

The 2nd column represent the Baud Rate to use.

The 3rd column represent the Device Address.

The 4th column represent the Scan Rate in seconds for this device.

19.1.19.1 Importing the M-BUS Configuration in Straton

First of all we must export the actual configuration:

memer Access. E				
Energy Protocols:	none			
PLC Status: runnin	ig (app: mbus_va	ars)		/
Router: disabled				
ADD	DELETE		CREATE TAG	s
NOTE: for each device column.	e, tags will have the	prefix "MBUSx_", where	"x" is the value in	the "Tag Prefix"
Tag Prefix	Baud Rate	Addres	S	Scan Rate (s)
MBUS1	2400	000084316140	0402	60

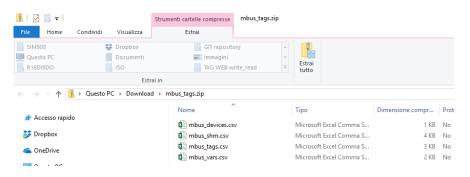
Now the tags automatic acquisition process will start:

reo status. running (app. nivus_vars)	
Router: disabled	
M-Bus tags creation in progress, please wait	
getting tags from device 3 with address 00008434614C0402 at baud rate 240	0 (3/21)
(10 seconds elapsed)	
STOP TAGS CREATION	

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

SENECA®	
General Configuration	M-Bus Configuration [user: admin] [logout]
Summary	Firmware Version: SW002940_344 [Modem: UC20GQBR03A14E1G]
Network and Services	MAC Address: C8F9811B02A0 [IMEI: 861075029494002] [IMSI: 240422600279769]
Real Time Clock Setup	Internet Access: Ethernet
VPN Configuration	Internet Access: Ethernet
Router Configuration	Energy Protocols: none
Users Configuration	PLC Status: running (app: mbus_vars)
FW Upgrade	Router: disabled
Conf. Management	TOWER, WINNING
Modbus TCP Client	
Mobile Configuration	M-Bus tags creation successfully performed.
Mobile Network	
DDNS Configuration	
Digital I/O Configuration	
Digital I/O Configuration	
M-Bus	
M-Bus Scan	
M-Bus Configuration	
Diagnostics	
FW Versions	
Ethernet Interfaces	
Modbus Modules	

The zip contain 4 files:



Two of these files must be used in Straton:

mbus_shm.csv (the shared memory configuration)

mbus_vars.csv (the M-Bus vars)

Extract the zip file in a directory.

Now launch Straton PLC:

Select Main then Global Variables:

STRATON - MBUS_test		- 0	×
<u>File Edit View</u> Insert Project	Iools Window Help		
🖆 🛃 🗃 🎒 🕹 🖪 🖎 🖎	(弐) 원 (의 연) 部 패 육 19 💀 🖞 🖻 🧊 🔡 📷 🖉		
Workspace	Main		H 🛛 X
⊟ 🗿 MBUS_test	S Type	Dim. Attrib.	Syb.
Exception programs	Carl Main	_	
Programs	🔐 🖸 🖸 🖓 🖓 🖓 🖓		
Main	RETAIN variables		
 Watch (for debugging) 			
Soft Scope			
El Initial values			
96 Binding Configuration			
in Sig Global defines	34		
Variables			
E Types			
	5		>
	1 (All)		
	(Project)		^
	E G (roject)		
1	Advanced		

Now click the right mouse button and select "Edit Variables as Text":

_	_	_		_		
^		Nam		уре		∡ × Syb.
	Ľ.,	Nai) Main	ype	Din. Attib.	<u>390.</u>
		-	Global variab	1		
			RETAIN varia		Undo	
				6	Redo	
				×	Cut	
					Сору	
					<u>P</u> aste	
				\times	Clear	
					Edit	
					C <u>a</u> ncel Sorting	
					E <u>n</u> able Changes	Space
		<			Swap Global <> Retain	
	Đ		(All)	8	A <u>d</u> d Variable	Ins
	Đ		(Project)		Add Multi Variables	
	Ð		Advanced		Edit Variables as Text	
	Ð		Arithmetic		Select Variables	
	Œ		Arrays		Rename Variables	
	±		AS-interface BACnet			
	E		Beoleans		Expand	
	E		CANbus		<u>C</u> ollapse	
	Đ		CANopen			
	Đ		Clock		Structures	
	÷		Comparisons Conversions		Ogen I/Os	
			Conversions			

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

Global variables	_		×
📁 🔜 🛃 🔺 👔 🖧 🗈 🛍 🕹 👘			
"name";"type";"len";"dim";"attr";"RO";"init";"tag";"de	sc";"	profil	e";' 🔺
"MB1_MANUFACTURER_SPECIFIC_0";"SINT";"";"";"";"NO";"";	"";"_	ZMBUS_	";"'
"MB1_MANUNACTURER_SPECIFIC_1";"INT";"";"";"";"NO";"";"	";"_Z	MBUS_"	;"";
"MB1_A_2";"SINT";"";"";"NO";"";"";"_ZMBUS_";"";"";			
"MB1_MANUFACTURER_SPECIFIC_3";"SINT";"";"";"";"NO";"";	"";"_	ZMBUS_	";"'
"MB1_MANUFACTURER_SPECIFIC_4";"SINT";"";"";"";"NO";"";	"";"	ZMBUS	";"'
"MB1_MANUFACTURER_SPECIFIC_5";"SINT";"";"";"";"NO";"";	"";"	ZMBUS	";"'
"MB1 MANUFACTURER SPECIFIC 6";"LINT";"";"";"";"NO";"";	"";"	ZMBUS	";"'
"MB1_ENERGY_7";"LINT";"";"";"";"NO";"";"";" ZMBUS_";"'	;"";"		
"MB1_ENERGY_8";"LINT";"";"";"";"NO";"";"";" ZMBUS_";"'	;"";"		
"MB1_ENERGY_9";"LINT";"";"";"";"NO";"";"";" ZMBUS_";"'	;"";"		
"MB1_ENERGY_10";"LINT";"";"";"";"NO";"";"";" ZMBUS_";"	";"";		
"MB1 MANUFACTURER SPECIFIC 11";"LINT";"";"";"";"","NO";"'	;"";"	ZMBUS	";'
"MB1 MANUFACTURER SPECIFIC 12";"LINT";"";"";"";"NO";"'	;"";"	ZMBUS	";'
"MB1 MANUFACTURER SPECIFIC 13";"LINT";"";"";"";"NO";"'	;"";"	ZMBUS	";'
"MB1 MANUFACTURER SPECIFIC 14";"LINT";"";"";"";"NO";"'	' , "","	ZMBUS	_";'
"MB1 MANUFACTURER SPECIFIC 15";"LINT";"";"";"";"NO";"'	' , "","	ZMBUS	";'
"MB1 MANUFACTURER SPECIFIC 16";"LINT";"";"";"";"NO";"'	',"","	ZMBUS	_";'
"MB1 MANUFACTURER SPECIFIC 17";"LINT";"";"";"";"";"NO";"'		ZMBUS	_"; ! ¥
<			>

NOTE: The first Line

"name";"type";"len";...

must be present only one time and only in the first row.

The variables are imported:

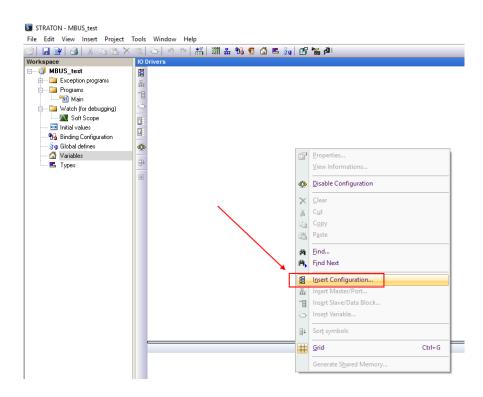
🝸 Name	Туре	Dim. At	trib. Syb.
🗋 Main			
🗉 🚮 Global variables			
MB1_MANUFACTURER_SPECIF	IC_0 SINT		
MB1_MANUFACTURER_SPECIF	IC_1 INT		
MB1A_2	SINT		
MB1_MANUFACTURER_SPECIF	IC_3 SINT		
MB1_MANUFACTURER_SPECIF	IC_4 SINT		
MB1_MANUFACTURER_SPECIF	IC_5 SINT		
MB1_MANUFACTURER_SPECIF	IC_6 LINT		
MB1_ENERGY_7	LINT		
MB1_ENERGY_8	LINT		
MB1_ENERGY_9	LINT		
MB1_ENERGY_10	LINT		
MB1_MANUFACTURER_SPECIF	IC_11 LINT		
MB1_MANUFACTURER_SPECIF	IC_12 LINT		
MB1_MANUFACTURER_SPECIF	IC_13 LINT		
MB1_MANUFACTURER_SPECIF	IC_14 LINT		
MB1_MANUFACTURER_SPECIF	IC_15 LINT		
MB1_MANUFACTURER_SPECIF	IC_16 LINT		
MB1 MANUFACTURER SPECIF	IC 17 LINT		
<			

Now we must create the shared memory used for sharing the data from M-BUS:

Click on fieldbus icon:

STRATON - MBUS_test		
File Edit View Insert Project	Tools Window Help	_
🖆 🛃 🛃 🛃 👗 🖻 🛍 🗙	🔨 🏷 🤊 🍽 🛗	品 😘 😨 🕼 🖪 💡 🗗 🕍 🔊
Workspace	IO Drivers	
MBUS_test Exception programs Programs Main Watch (for debugging)	2日 品品 ◆1日 ◎	

Click with the right mouse button and select "Insert Configuration":



Now create the Embedded Shared Memory:

Add Configuration	×
Choose a configuration	ОК
CAN Anybus CAN DNP3 Ethernet/IP IEC 60870 IEC 61850 MODBUS Profinet I0 Shared Memory Shared memory (embedded systems) Windows Shared memory	OK Cancel

Insert a Master/Port:



The Shared configuration MUST be (don't change any setting):

Shared memory	×
Identification	ОК
Name: MBUS_SHM	Cancel
Size: 16384 (bytes)	Cancel
Open mode Create (allocate memory) Link to existing memory Create if memory does not exist Access mode Create if access (synchronized with a mutex)	

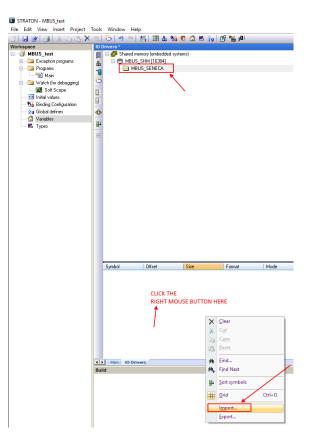
Now insert the data Block:

STRATON - MBUS_test			
File Edit View Insert Project	Tools Window Help		
121 🖬 🕑 🛃 🕹 🗈 🖎 🗙	🐟 🕒 🤊 🖭 🟭 🖩	11 🏔 % 😰 🕼 🛤 🚱 🕒 📽 🐜 🖉	
Workspace	IO Drivers *		
B 🗊 MBUS_test	📔 🖃 🚭 Shared memory (err	ibedded systems)	
Exception programs	MBUS_SHM [16	33841	
- Dia Programs		Properties	_
	-8	View Informations	
🚊 📴 Watch (for debugging)	6		
Soft Scope	FE 49	Disable Configuration	
🔛 Initial values			
👫 Binding Configuration			
🕉 g Global defines	👁 🕹	Cut	
🚰 Variables	B4 (2)	Сору	
🛋 Types		Paste	
	·		-
	24	Eind	
	24,	Find Next	
	8	Insert Configuration	
	24	Insert Master/Port	
	-8	Insert Slave/Data Block	
	0	Inse <u>r</u> t Variable	
	8+	Sor <u>t</u> symbols	
	#	Grid Ctrl+G	
		Generate Shared Memory	
		Renumber offsets	

Create a name group (use the name that you want):

Group			×
Description:	MBUS_SENECA	OK	

Then import the shared memory file:



Select the "mbus_shm.csv" file:

•	· ~ = 1	· · · · · · · · · · · · · · · · · · ·			
	IO Drivers *		1		
	1 HP	Shared memory (embedde	ed systems)		
	111	MBUS_SHM [16384]			
	*8	MBUS_SENECA			
	6		NUFACTURER_SPEI		
ng)			NUFACTURER_SPE	JHC_1	
		🔲 3[1]-MB1_A_			
			NUFACTURER_SPEI	-	
n			NUFACTURER_SPEI		
	¢¦p		NUFACTURER_SPEI	-	
	⊒ ∔		NUFACTURER_SPEI	CIFIC_6	
	H +	🔲 🔲 15 [8] · MB1_EN			
		- 🔲 23 [8] · MB1_EN			
		— 🛄 31 [8] · MB1_EN	IERGY_9		
		🔲 🔲 39 [8] • MB1_EN			
			ANUFACTURER_SPE		
		— 🔲 55 [8] · MB1_M/	ANUFACTURER_SPE	CIFIC_12	
		— 🔲 63 [8] · MB1_M/	ANUFACTURER_SPE	CIFIC_13	
		— 🔲 71 [8] · MB1_M/	ANUFACTURER_SPE	CIFIC_14	
		— 🔲 79 [8] · MB1_M/	ANUFACTURER_SPE	CIFIC_15	
		🔲 🔲 87 [8] • MB1_M/	ANUFACTURER_SPE	CIFIC_16	
		— 🔲 95 [8] · MB1_M/	ANUFACTURER_SPE	CIFIC_17	
		— 🔲 103 [8] - MB1_M	ANUFACTURER_SF	ECIFIC_18	
		🔲 🔲 111 [1] - MB1_E			
		— 🔲 112[1] · MB2_M	ANUFACTURER_SF	ECIFIC_0	
		— 🔲 113 [2] - MB2_M	ANUFACTURER_SF	ECIFIC_1	
		🔲 🔲 115 [1] - MB2			
		🗖 🔲 116 [1] - MB2_M	IANUFACTURER_SP	ECIFIC_3	
		— 🛄 117 [1] - MB2_N	ANUFACTURER_SP	ECIFIC_4	
		🔲 🔲 118 [1] - MB2_N	ANUFACTURER_SP	ECIFIC_5	
	Symbol	Offset	Size	Format	Mode
	MB1_M	ANUFAC 0	1	Signed integer	Input
	MB1_M	ANUFAC 1	2	Signed integer	Input
	MB1/		1	Signed integer	Input
		ANUFAC 4	1	Signed integer	Input
	_	ANUFAC 5	1	Signed integer	Input
	_	ANUFAC 6	1	Signed integer	Input
	_	ANUFAC 7	8	Signed integer	Input
	_	VERGY_7 15	8	Signed integer	Input
	_	VERGY_8 23	8	Signed integer	Input
	_	VERGY 9 31	8	Signed integer	Input
	_	VERGY 39	8	Signed integer	Input
	_	ANUFAC 47	8	Signed integer	Input
				origined integer	in ipse
	A > Main	IO Drivers			

19.1.19.2 Delete unused M-BUS variables

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

Tools Window Help					
🔜 🏷 이 이 部 井 유 % 😨 🖄 🛎 😼 🖻 🐂 🔊					
IO Drivers					
😫 🕀 🚰 Shared memory (embedded systems)		∧ Name	Value	Name Name	Type
👷 🗇 😇 MBUS_SHM [16384]		Description	MBUS_SENECA	Global variables	
MBUS_SENECA				MB1_MANUFACTU	
				MB1 MANUFACTU	INT
1 [2] • MB1_MANUFACTURER_SPECIFIC_1				MB1 A 2	SINT
□ 3[1]-MB1_A_2				MB1_MANUFACTU	SINT
				MB1 MANUFACTU	SINT
GITI-MBT_MANUFACTURER_SPECIFIC_3				MB1 MANUFACTU	SINT
G [1] · MB1_MANUFACTURER_SPECIFIC_5 G [1] · MB1_MANUFACTURER_SPECIFIC_5 G				MB1 MANUFACTU	
7 [8] - MB1_MANUFACTURER_SPECIFIC_6				MB1 ENERGY 7	LINT
				MB1 ENERGY 8	LINT
23 [8] - MB1_ENERGY_8				MB1 ENERGY 9	LINT
				MB1 ENERGY 10	LINT
- 39 [8] - MB1 ENERGY 10				MB1 MANUFACTU	
47 [8] - MB1_MANUFACTURER_SPECIFIC_11				MB1 MANUFACTU	
55[8] MB1_MANUFACTURER_SPECIFIC_12				MB1 MANUFACTU	
- G3181-MB1 MANUFACTURER SPECIFIC 13				MB1 MANUFACTU	
71 [8] - MB1_MANUFACTURER_SPECIFIC_14				MB1 MANUFACTU	
- 79 (8) - MB1 MANUFACTURER SPECIFIC 15				MB1 MANUFACTU	
- 87 [8] - MB1_MANUFACTURER_SPECIFIC_16				MB1_MANUFACTU	
- 9 95 (8) - MB1_MANUFACTURER_SPECIFIC_17				LIDY MANUEAOTU	LINT
- 103 [8] - MB1_MANUFACTURER_SPECIFIC_18				<	
- Itisigi-MBT_MANOPACTOREN_SPECIFIC_TO				Name Value	
III2[1] MB2_MANUFACTURER_SPECIFIC_0 III3[2] MB2_MANUFACTURER_SPECIFIC_1					
115[1]-MB2_A_2					
- IIG[1]-MB2_A_2					
TIS[1]-MB2_MANUFACTURER_SPECIFIC_3 TIS[1]-MB2 MANUFACTURER SPECIFIC 4					
- I18[1] - MB2_MANUFACTURER_SPECIFIC_5		~		_	
Symbol Offset Size Format	Mode				
MB1_MANUFAC 0 1 Signed integer	Input			^	
MB1_MANUFAC 1 2 Signed integer	Input				
MB1_A_2 3 1 Signed integer	Input 🔨				
MB1_MANUFAC 4 1 Signed integer	Input	/			
MB1_MANUFAC 5 1 Signed integer	Input				
MB1_MANUFAC 6 1 Signed integer	Input				

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

- 🖬 112 [1] - MB2 - 🔲 113 [2] - MB2 - 🔲 115 [1] - MB2 - 🔲 116 [1] - MB2 - 🔲 116 [1] - MB2 - 🔲 117 [1] - MB2 - 🔲 118 [1] - MB2	ERROR_REPORT MANUFACTURER_SI A_2 MANUFACTURER_SI MANUFACTURER_SI MANUFACTURER_SI MANUFACTURER_SI	PECIFIC_1 PECIFIC_3 PECIFIC_4 PECIFIC_5			*
iymbol Offset	Size	Format	Mode		
IB1_MANUFAC 0	1	Signed integer	Input		
IB1_MANUFAC 1	2	Signed integer	Input		
IB1_MANUFAC 4	1	Signed integer	Input		
IB1_MANUFAC 5	1	Signed integer	Input		
181_MANUFAC 6	1	Signed integer	Input	- \	
IB1_MANUFAC 7	8	Signed integer	Input		
B1_ENERGY_7 15	8	Signed integer	Input		
IB1_ENERGY_8 23	8	Signed integer	Input		
B1_ENERGY_9 31	8	Signed integer	Input		
81_ENERGY 39	8	Signed integer	Input		
B1_MANUFAC 47	8	Signed integer	Input		
IB1 MANUFAC 55	8	Signed integer	Input		

19.1.19.3 Replace a M-BUS Device

For Replace an existing M-BUS device (for example in case of a replace for failure)

- 1. Go to M-BUS Scan and make a Secondary or Primary Scan
- 2. Take note of the new address
- 3. Go to M-BUS Configuration and manually change the address from the old to the new device
- 4. Push the "Create Tag" button
- 5. You don't need to make any change in Straton

19.1.19.4Adding a M-BUS Device

- 1. Go to M-BUS Scan and make a Secondary or Primary Scan
- 2. Take note of the new address and baudrate
- 3. Go to M-BUS Configuration and manually add the address and baudrate of the new device with the "ADD" button
- 4. Push the "Create Tag" button
- 5. Import the shared memory file (see chapter 19.1.19.1)
- 6. Import the variable file (see chapter 19.1.19.1) without delete your local variable (use copypaste)

19.1.19.5Delete a M-BUS Device

- 1. Go to M-BUS Scan and make a Secondary or Primary Scan
- 2. Take note of the Device address to delete
- 3. Go to M-BUS Configuration and manually delete the device with the "DELETE" button
- 4. Push the "Create Tag" button
- 5. Import the shared memory file (see chapter 19.1.19.1)

6. Delete the variables from the deleted device

19.1.19.6Tag error report

When variable tags are imported in Straton a special tag is creted "Tag error report".

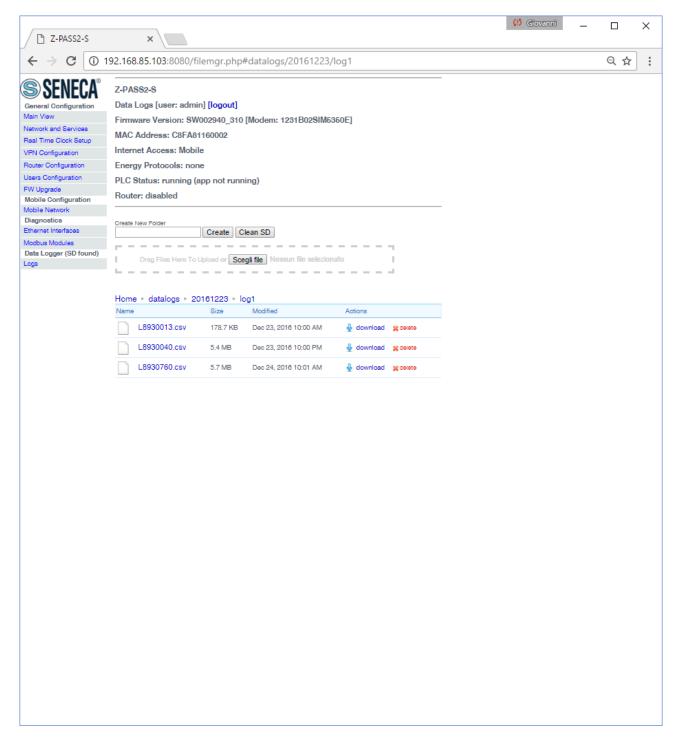
Use this tag for monitoring the device communication errors:

ERORR REPORT VALUE	MEANING
0	READ OK
-2	READ TIMEOUT, NO
	RESPONSE FROM DEVICE

19.1.20Data Logs

By clicking on the "Logs" link, in the "Data Logger" menu, you come to a page similar to those in the following figures:

🗋 Z-PASS2-S	×				🧭 Giovanni 🔤		>
← → C 🛈	192.168.85.103:8080)/filemgi	r.php#datalogs			९ ☆	
SENECA"	Z-PASS2-S				-		
ULNLUA	Data Logs [user: ad	lmin] [log	outl				
eneral Configuration ain View							
etwork and Services			0_310 [Modem: 1231B02S	M6360EJ			
al Time Clock Setup	MAC Address: C8F	A8116000)2				
PN Configuration	Internet Access: Mo	obile					
outer Configuration	Energy Protocols:	none					
ers Configuration	PLC Status: runnin		t rupping)				
V Upgrade		g (app no	(Turning)				
obile Configuration	Router: disabled				-		
obile Network iagnostics							
hernet Interfaces	Create New Folder	Cres	te Clean SD				
odbus Modules		Cicc					
ata Logger (SD found)		Talking	Caralifia Manua file anto				
iĝs	I Drag Files Here	ro upload (Scegli file Nessun file sele	21011810			
	Home ► datalogs Name	Size	Modified	Actions			
	20161223		Dec 23, 2016 10:00 AM	X delete			
	20161224		Dec 24, 2016 10:01 PM	🗶 delete			
	20161225		Dec 25, 2016 10:01 PM	💥 delete			
	20161226		Dec 26, 2016 10:01 PM	🗶 delete			
	20161227		Dec 27, 2016 10:02 PM	💥 delete			
	20161228		Dec 28, 2016 10:01 PM	💥 delete			
	20161229		Dec 29, 2016 10:01 PM	💥 delete			
	20161230		Dec 30, 2016 10:02 PM	🗶 delete			
	20161231		Dec 31, 2016 10:01 PM	💥 delete			
	20170101		Jan 1, 2017 4:22 PM Jan 2, 2017 10:01 PM	elete			
	20170102		Jan 3, 2017 10:02 PM	36 delete 36 delete			
	20170104		Jan 4, 2017 10:02 PM	adete			
	20170105		Jan 5, 2017 10:01 PM	X delete			
	20170106		Jan 6, 2017 10:01 PM	🗶 delete			
	20170107		Jan 7, 2017 10:01 PM	💥 delete			
	20170107						
	20170108		Jan 8, 2017 10:01 PM	💥 delete			



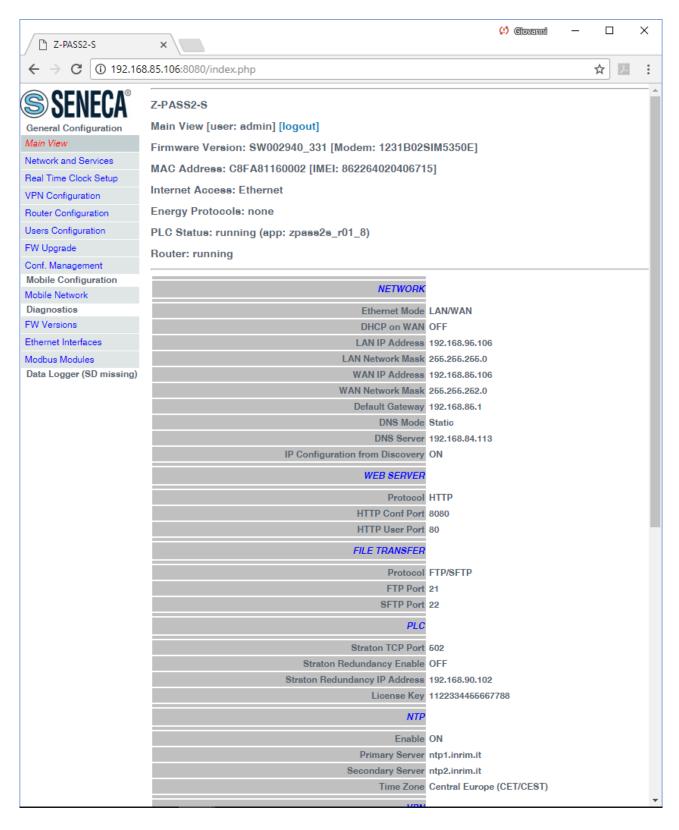
This page shows the contents of the SD card which, typically, is used to store "Data Logs" files; these files are created by the "Data Logger" functionality available in Z-NET4 "Telecontrol Functions" (see chapter 21).

The page lets you perform the following operations:

- browse the SD folder tree, clicking on the folder name links
- delete a folder, clicking on the "delete" link
- create a new folder, by means of the "Create New Folder" text-box and "Create" button; the new folder is created in the folder currently shown
- download a file, clicking on the filename link or on the "download" link
- delete a file, clicking on the "delete" link

- uploading a file, selecting it by means of the "Choose file" button or dragging it into the dashed area; the file is created in the folder currently shown
- clean the SD, by means of the "Clean SD" button; please note that this is done by formatting the SD, so all SD contents will be lost

If an SD card is not available on the Device, the "Logs" link is not shown, as in the following figure.



19.2 User pages

It is also possible to access the Device configuration site as a "non-administrator" user; this user is allowed to access only the "Main View" and "Network and Services" pages, viewing and setting only a limited number of configuration parameters; in S6001-RTU, the "I/O View" page is also available.

Also the "FW Versions", "Ethernet Interfaces" and "Modbus Modules" pages of the "Diagnostics" section are available for this kind of user; they will not be shown again here, as they are identical to those for administrator user.

To login as "non-administrator" user, connect the browser to the Device IP address on port 8080, e.g.:

http://192.168.90.101:8080

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

Username: user Password: user

You come to the "Main View" page, described in the following paragraph.

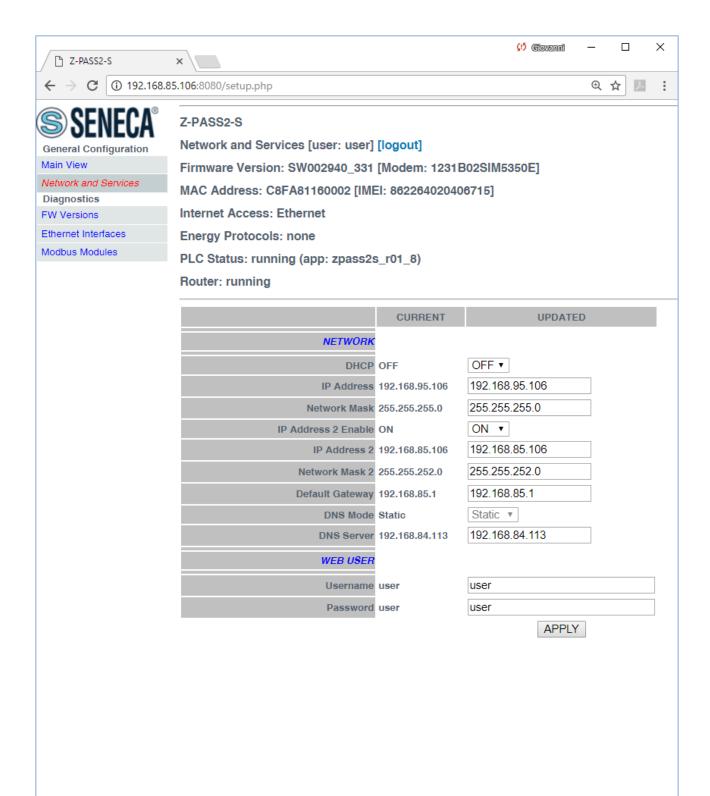
19.2.1 Main View

In this page, some Network parameters and the Web User credentials are shown, with their current values.

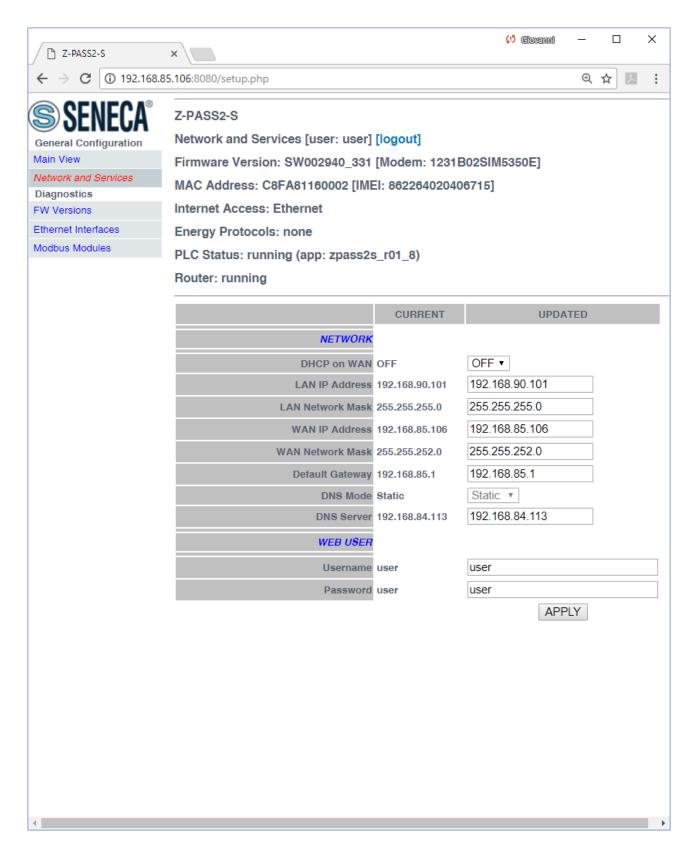
To change the parameter values, you have to go to the "Network and Services" page, described in the following paragraph.

19.2.2 Network and Services

The parameters shown in this page slightly change, depending on the HW version of the product (Z-TWS4/Z-PASS2-S or Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO) and, for new HW versions, on the selected "Ethernet Mode"; this is shown in the following figures.



The previous figure shows the "Network and Services" page for a Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO, when the "Ethernet Mode" parameter is set to "Switch"; it also applies to a Z-TWS4 and Z-PASS2-S (old versions) and to a S6001-RTU.



The previous figure shows the "Network and Services" page for a Z-PASS2-S-R01/Z-PASS2-S-IO/Z-TWS4-IO, when the "Ethernet Mode" parameter is set to "LAN/WAN".

There is an important difference between the parameter values shown in this page and those shown in the "Main View" page: the former are <u>configured</u> values, whereas the latter are <u>actual</u> values.

To better explain this difference, let's consider the case when the DHCP parameter is set to ON; in the "Network and Services" page, you may see the 192.168.90.101 default value for the "IP Address" parameter, whereas the "Main View" page shows the actual IP Address, assigned by the DHCP server.

In the following table, all configuration parameters available in this page are listed, with a short explanation and the parameter default value for each of them.

Note that "Ethernet Mode" parameter is not shown in user pages.

Field	Meaning	Default value		
Ethernet Mode = "Switch"				
NETWORK/DHCP	Flag to enable/disable the DHCP	OFF		
	functionality on the Ethernet			
	interface.			
NETWORK/IP Address	IP address of the Ethernet	192.168.90.101		
	interface (disabled when "DHCP"			
	is set to "ON")			
NETWORK/Network Mask	Network mask of the Ethernet	255.255.255.0		
	interface (disabled when "DHCP"			
	is set to "ON")			
NETWORK/IP Address 2 Enable	Flag to enable/disable the second	OFF		
	IP address on the Ethernet			
	interface.			
	Note that the second IP address			
	can be enabled also when the			
	DHCP functionality is active.			
NETWORK/IP Address 2	Second IP address of the Ethernet	192.168.100.101		
	interface			
NETWORK/Network Mask 2	Second network mask of the	255.255.255.0		
	Ethernet interface			
Ethernet Mode = "LAN/WAN"				
NETWORK/DHCP on WAN	Flag to enable/disable the DHCP	ON		
	functionality on the WAN			
	Ethernet interface			
NETWORK/LAN IP Address	IP address of the LAN Ethernet	192.168.90.101		
	interface			
NETWORK/LAN Network Mask	Network mask of the LAN	255.255.255.0		
	Ethernet interface			
NETWORK/WAN IP Address	IP address of the WAN Ethernet	192.168.100.101		

	interface (disabled when "DHCP			
	on WAN" is set to "ON")			
NETWORK/WAN Network Mask	Network mask of the WAN	255.255.255.0		
	Ethernet interface (disabled when			
	"DHCP on WAN" is set to "ON")			
NETWORK/Default Gateway	Default Gateway IP address	192.168.100.1 , for Z-TWS4-		
	(disabled when DHCP	R0x and Z-PASS2-S-R0x		
	functionality is enabled on any	(x=1,2)		
	interface).	192.168.90.1, for all other		
	When "Ethernet Mode" is set to	products		
	"LAN/WAN", the Default Gateway			
	shall be in the WAN subnet.			
NETWORK/DNS Mode	Tells if the DNS Server shall be set	DHCP, for Z-TWS4-R0x and		
	statically (value: "Static") or	Z-PASS2-S-R0x (x=1,2)		
	dinamically assigned by the DHCP	Static, for all other products		
	Server (value: "DHCP")			
NETWORK/DNS Server	DNS server IP address (disabled	192.168.100.1 , for Z-TWS4-		
	when DHCP functionality is	R0x and Z-PASS2-S-R0x		
	enabled on any interface and DNS	(x=1,2)		
	Mode = DHCP)	192.168.90.1, for all other		
		products		
WEB USER/Username	Username to access the web	User		
	configuration site (limited access)			
WEB USER/Password	Password to access the web	user		
	configuration site (limited access)			

Some notes about the "DHCP" parameters:

- the "DHCP" parameter can be set to "ON" only if the "DHCP Server" parameter of the "Router Configuration" page is set to "OFF";
- only the "DHCP on WAN" parameter can be set to "ON".

You can change any of the above parameters; to apply the changes, press the "APPLY" button.

Please note that, after changing the Web User credentials, a new login will be required to access any page.

19.2.3 I/O View (S6001-RTU)

This page is identical to that shown for "administrator user" (see 19.1.12).

🗅 \$6001-RTU	×	Giovanni 🗕 🗆 🗙
← → C 🗋 19	02.168.85.105:8080/io_view.php	ର 🏠 🚍
General Configuration Main View Network and Services S6001-RTU I/O View	S6001-RTU I/O View Firmware Version: SW002940_220 [Modem: 1231B02SIM5350E] MAC Address: C8F98100019B Internet Access: Ethernet Energy Protocols: none PLC Status: running Router: disabled	
	DIGITAL INPUTS Input 1 LOW Input 2 LOW Input 3 LOW Input 4 LOW Input 5 LOW Input 6 LOW Input 6 LOW Input 7 LOW Input 9 LOW Input 9 LOW Input 9 LOW Input 9 LOW Input 11 LOW Input 12 LOW Input 12 LOW Input 14 LOW Input 15 LOW Input 15 LOW Input 14 LOW Input 14 LOW Input 15 LOW Input 14 LOW Input 14 LOW Input 12 OPEN Output 2 OPEN Output 3 OPEN Output 3 OPEN Output 5 OPEN Output 6 OPEN Output 7 OPEN Output 7 OPEN Output 7 OPEN Output 8 UN Output 8 OPEN Current 1 (UA) 5 Current 3 (UA) 2 Current 3 (UA) 2 Current 3 (UA) 2 Current 4 (UA) 5 Cur	

19.3 Guest pages

It is also possible to access the Device configuration site as a "guest" user; this user is allowed to access all the pages except for "FW Upgrade", "Configuration Management"" and "Data Logs" pages, viewing all configuration parameters and status information, without changing any parameter; so, in all the pages, the "APPLY" buttons (and any other button used to perform changes) are disabled.

To login as "guest" user, connect the browser to the Device IP address on port 8080, e.g.:

http://192.168.90.101:8080

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

Username: guest Password: guest

You come to the "Main View" page, shown in the following figure.

🗋 Z-PASS2-S	×	(!) Clovenni	- 0	×
← → C 🛈	192.168.85.104:8080/index.php		Q 🕶 🕁	<i>J.</i> .
bile Network	Kouter: running			
DNS Configuration				
gital I/O	NETWORK			
ital I/O Configuration				
gnostics	Ethernet Mode LAN/WAN			
	DHCP on WAN OFF			
Versions	LAN IP Address 192.168.90.101			
ernet Interfaces	LAN Network Mask 255.255.255.0			
dbus Modules	WAN IP Address 192.168.85.104			
	WAN Network Mask 255.255.252.0			
	Default Gateway 10.64.64			
	DNS Mode Static			
	DNS Server 83.224.65.143 83.224.65.134			
	IP Configuration from Discovery ON			
	WEB SERVER			
	Protocol HTTP/HTTPS			
	HTTP Conf Port 8080			
	HTTP User Port 80			
	HTTPS Port 443			
	FILE TRANSFER			
	Protocol FTP/SFTP			
	FTP Port 21			
	SFTP Port 22			
	PLC			
	Straton TCP Port 502			
	Straton Redundancy Enable OFF			
	Straton Redundancy IP Address 192.168.90.102			
	License Key 1122334455667788			
	NTP			
	Enable ON			
	Primary Server ntp1.inrim.it			
	Secondary Server ntp2.inrim.it			
	Time Zone Central Europe (CET/CEST)			
	VPN			
	Made VDN Dev			
	Mode VPN Box			
	Enable OFF			
	Server 192.168.90.1			
	Password seneca			
	Tag Name zpasa2a			
	MOBILE NETWORK			
	Enable ON			
	APN Mode Manual			
	APN m2mbis.vodafone.it			
	Authentication Type None			
	Username user			
	Password pass			
	PIN 8342			
	Ping Connection Testing IP Address www.google.com			
	NETWORK REDUNDANCY			
	Enable OFF			
	Ping Address 8.8.4.4			
	WATCHDOG			
	E-H-OU			
	Enable ON			
	Timeout (8) 60			
	DEBUG LOGS			
	Enable ON			
	COM1			
	Mode RS485			
	FACTORY DEFAULT RESTART			
	CLEAN INTERNAL DATA LOGS			

Note that, as told above, the "FACTORY DEFAULT", "RESTART" and "CLEAN INTERNAL DATA LOGS" buttons are disabled.

Another example of a page accessed by the "guest" user is given in the following figure.

		🥵 Giovanni 💷 🗆 🗙
🗋 Z-PASS2-S	×	
$\boldsymbol{\leftarrow}$ \rightarrow \mathbf{C} (1) 192.16	8.85.103:8080/mobile_network.php?showinfo=1	☆ :
Seneral Configuration Main View Network and Services Real Time Clock Setup VPN Configuration Router Configuration Users Configuration Mobile Configuration Mobile Network Diagnostics Ethernet Interfaces	Z-PASS2-S Mobile Network [user: guest] [logout] Firmware Version: SW002940_310 [Modem: 1231B02S MAC Address: C8FA81160002 Internet Access: Mobile Energy Protocols: none PLC Status: running (app not running) Router: disabled CURRENT	IM5350E] UPDATED
Modbus Modules	Mobile Configuration Enable ON ON APN ibox.tim.it ibox.tim.it Authentication Type None None Username user user Password pass pass PIN (if required by SIM) 1234 1234	

In the "Mobile Network" page, the "APPLY" button is disabled, whereas the "SHOW MOBILE STATUS"/"HIDE MOBILE STATUS" and "REFRESH" buttons are enabled, letting the "guest" user to view the Mobile Status.

20 Seneca StratON Library

To let the users exploit Z-TWS4/Z-PASS2-S/S6001-RTU features in their IEC 61131-3 programs, Seneca has developed a set of "Function Blocks" and Functions, supplied with the Seneca library for StratON.

In this chapter, all the FBs and functions available on Z-TWS4/Z-PASS2-S/S6001-RTU are listed, providing a description of input/output parameters and some notes for each of them.

20.1 Function Blocks

20.1.1 General FB behavior

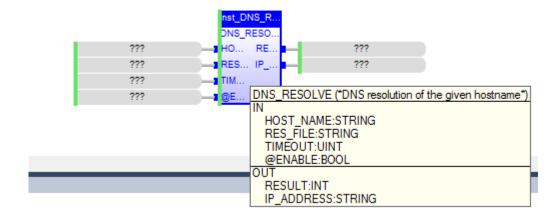
The description given in this paragraph apply to all the FBs available on Z-TWS4/Z-PASS2-S/S6001-RTU, except for the LINUX_SHELL FB, which has a particular behavior (see related paragraph).

All the FBs require more than one PLC cycle to be completed (Asynchronous Function Block); so, the application shall run them for a number of cycles until it detects that the FB execution has ended.

Every FB has an "ENABLE" parameter, which is an input/output parameter: to let the FB actually run, the application shall put ENABLE=TRUE (input), not changing the parameter value during the FB execution; when the execution is completed, the FB code itself will put ENABLE=FALSE (output); when the FB is called with ENABLE=FALSE, it does nothing and returns the *NOT_DONE* (-2) result value.

All the FBs return the *FAILED* (-1) result value to signal that the FB execution has failed, for a generic reason; some FBs provide further failure result values, in particular the *TIMEOUT* (2) result value.

All the FBs return the *RUNNING* (0) result value to tell the application that the FB processing is still running and the *DONE* (1) result value when the FB processing has successfully ended.



20.1.2 DNS_RESOLVE

The DNS_RESOLVE FB resolves a hostname into the corresponding IP address.

When first called, the FB runs a process which starts the DNS resolution; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

⁻ HOST_NAME : the hostname to be resolved

- RES_FILE : if this parameter is not empty, the resulting IP address will be written into /var/run/ file;

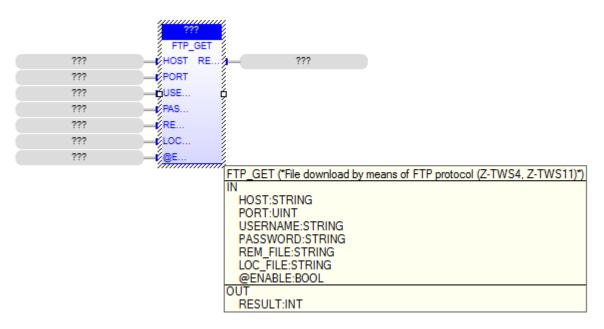
- if this is not needed, the parameter can be left empty
- TIMEOUT : timeout, in seconds
- @ENABLE : TRUE -> FB is executed

FALSE -> FB is skipped

The FB has the following output parameters:

- RESULT : -2, when called with ENABLE=FALSE
- -1, in case of any failure
- 0, if the process is still running
- 1, if the process has successfully finished
- 2, if timeout has expired
- IP_ADDRESS : the resulting IP address

20.1.3 FTP_GET

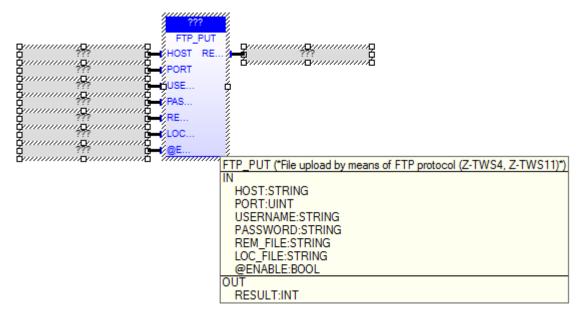


The FTP GET FB downloads a file, by means of the FTP protocol.

When first called, the FB runs a process which starts performing the download; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters: - HOST : IP address or host name of the FTP server : TCP port for the FTP protocol (normally: 21) - PORT - USERNAME : username for authentication - PASSWORD : password for authentication - REM FILE : name of the file (with path) on the remote server - LOC FILE : name of the file (with path) on the local device - @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped The FB has the following output parameter: - RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished.

20.1.4 FTP_PUT



The FTP_PUT FB uploads a file, by means of the FTP protocol.

When first called, the FB runs a process which starts performing the upload; on subsequent calls, it only checks if the process has finished its job.

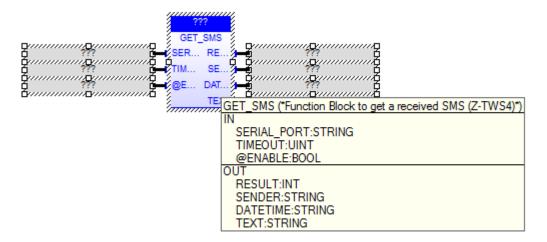
```
The FB has the following input parameters:
- HOST : IP address or host name of the FTP server
- PORT : TCP port for the FTP protocol (normally: 21)
- USERNAME : username for authentication
- PASSWORD : password for authentication
- REM_FILE : name of the file (with path) on the remote server
- LOC_FILE : name of the file (with path) on the local device
- @ENABLE : TRUE -> FB is executed
FALSE -> FB is skipped
The FB has the following output parameter:
- RESULT : -2, when called with ENABLE=FALSE
-1, in case of any failure
```

- 0, if the process is still running
- 1, if the process has successfully finished.

20.1.5 GET_ALARMS

```
st_GET_AL.
                          GET_ALARMS
                          STA...
                              RE.
               222
                                           222
               ???
                           SEP... FIR.
                                           ???
               ???
                           AX... LAS.
                                           ???
               ???
                           ۹L...
                              RE.
                                           222
               ???
                                 GET_ALARMS (*Retrieve alarms with the specified status from the DB.*)
                                 IN
                                  STATUS:USINT
                                  SEP_CHAR:USINT
                                  MAX_REC:UDINT
                                  FILENAME:STRING
                                  @ENABLE:BOOL
                                 00
                                  RESULT:INT
                                  FIRST_ID:UDINT
LAST_ID:UDINT
                                  REC_NUM:UDINT
This FB retrieves all alarm records with the specified status from the DB;
the records are written as lines into the specified file.
INPUTS:
- STATUS : this parameter is handled as a "negative bitmask", meaning that this
FB will provide alarm records such that:
  (alarms.stat & STATUS) = 0, where:
  alarms.stat: DB field
  STATUS: this parameter
- SEP CHAR : the field separator to be used in the file lines; possible values:
" "|","|";"
- MAX REC : the maximum number of records (lines) to be retrieved
- FILENAME : the file name, with absolute path
- @ENABLE: TRUE -> FB is executed
            FALSE -> FB is skipped
            the parameter is set to FALSE by the FB at the end of execution
OUTPUTS:
- RESULT: the FB result; possible values are:
   0: FB still running
   1: FB successfully executed
  -1: FB execution failed
  -2: FB execution timeout
- FIRST ID : the id of the first record retrieved; this value shall be passed as
an argument to the SET ALARMS STAT FB
- LAST ID : the id of the last record retrieved; this value shall be passed as
an argument to the SET ALARMS_STAT FB
- REC NUM : the number of records retrieved
```

20.1.6 GET_SMS



The GET_SMS FB gets an SMS, previously received, by means of a GSM modem; once read, the SMS is deleted.

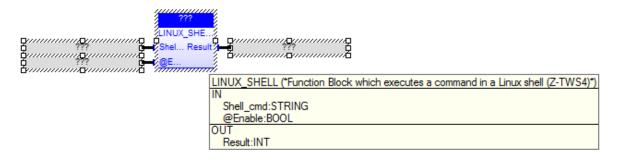
When first called, the FB runs a process which starts getting the SMS; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

 SERIAL PORT : this parameter is not used (it is still present only for compatibility reasons); it can be set to '' (empty string) TIMEOUT : timeout, in seconds @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped
The FB has the following output parameters:
<pre>- RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished and an SMS has been</pre>
found
2, if timeout has expired
3, if the process has successfully finished but no SMS has been
found 4, if PPP is active, on Z-MINIRTU 5, if MODEM_RESET FB is running CENDED - OVC condem (only if DECUUE-1)
 SENDER : SMS sender (only if RESULT=1) DATETIME : Date/time of SMS reception (only if RESULT=1) TEXT : SMS text (only if RESULT=1)

Please note that the GET_SMS FB can't be successfully executed while the PPP connection is active, on Z-MINIRTU.

20.1.7 LINUX_SHELL



Seneca FB for access to the Linux Shell. Max 255 command line characters. For access to the output use "> output.txt"

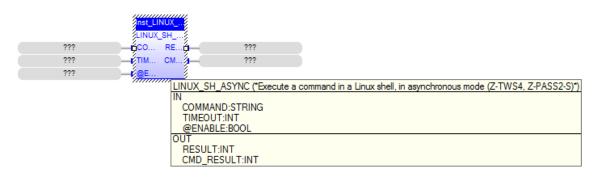
Shell_cmd : string command @Enable : if true execute the shell command Result : the return value of the "system" C function

Usage Example:

"ls > output1.txt"

create the directory list into output1.txt

20.1.8 LINUX_SH_ASYNC



The LINUX SH ASYNC FB executes a command in a Linux shell, in asynchronous mode.

When first called, the FB runs a Linux shell process which starts performing the command; on subsequent calls, it only checks if the process has finished the command execution.

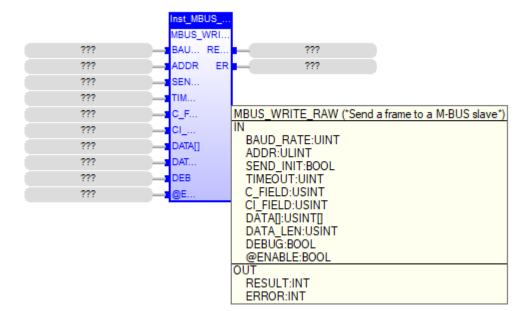
The FB has the following input parameters: - COMMAND : the command to be executed

- TIMEOUT : timeout, in seconds
- @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped

The FB has the following output parameters:

RESULT : -2, when called with ENABLE=FALSE
-1, in case of any failure
0, if the process is still running
1, if the process has successfully finished
2, if timeout has expired
CMD RESULT: command exit code

20.1.9 MBUS_WRITE_RAW



The MBUS_WRITE_RAW FB sends a frame to the specified M-Bus slave. A Control Frame or Long Frame can be sent with this FB.

When first called, the FB runs a process which starts the procedure; on subsequent calls, it only checks if the process has finished its job.

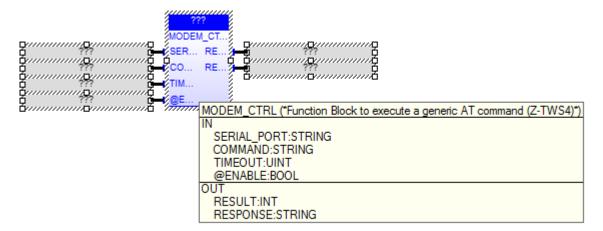
```
The FB has the following input parameters:
- BAUD RATE : the baud-rate on the serial port; possible values are:
              300, 600, 1200, 2400, 4800, 9600, 19200, 38400
- ADDR : M-Bus primary (<=255) or secondary address
- SEND INIT : flag to enable/disable the sending of the SND NKE reset frame, at
the beginning of the procedure
- TIMEOUT : timeout, in seconds
- C FIELD : the frame C Field value (see M-Bus protocol specification)
- CI FIELD : the frame CI Field value (see M-Bus protocol specification)
- DATA[] : the frame User Data field (see M-Bus protocol specification)
- DATA LEN : the length, i.e. the number of bytes, in the frame User Data field
- DEBUG : when this parameter is set to TRUE, the file /log/mbus prot.log is
created, which contains the M-Bus protocol frames dump; this file can be
retrieved via FTP/SFTP protocol
- @ENABLE : TRUE -> FB is executed
            FALSE -> FB is skipped
```

The FB has the following output parameters:

```
- RESULT : -2, when called with ENABLE=FALSE
           -1, in case of any failure
            0, if the process is still running
            1, if the process has successfully finished
            2, if timeout has expired
            5, if MBUS READ DATA or MBUS WRITE RAW FB is running
- ERROR : this parameter is meaningful when RESULT=-1; possible values are:
  0: none
  -1: invalid arguments (input parameters)
  -2: M-Bus protocol error
This FB can be used to send configuration commands to the slaves;
for example, to set the slave to primary address 8, the following values shall
be given:
 C FIELD = 53 (hex)
 CI FIELD = 51 (hex)
  DATA = 01 7A 08 (hex)
```

```
DATA_LEN = 3
```

20.1.10 MODEM_CTRL



The $\texttt{MODEM_CTRL}\ \texttt{FB}\ \texttt{sends}\ \texttt{a}\ \texttt{generic}\ \texttt{AT}\ \texttt{command}\ \texttt{to}\ \texttt{the}\ \texttt{GSM}\ \texttt{modem}\ \texttt{and}\ \texttt{receives}\ \texttt{the}\ \texttt{corresponding}\ \texttt{response}.$

When first called, the FB runs a process which starts sending the command; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

 SERIAL PORT : this parameter is not used (it is still present only for compatibility reasons); it can be set to '' (empty string) COMMAND : AT command to be executed TIMEOUT : timeout, in seconds @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped
<pre>The FB has the following output parameters: - RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished</pre>

(NOTE: this only means that the command was successfully sent and the response was successfully received;

it does not necessarily mean that the AT command was successfully executed;

in other words, it is up to the application to tell if the response means success or failure)

- 2, if timeout has expired
- 4, if PPP is active, on Z-MINIRTU
- 5, if MODEM RESET FB is running

- RESPONSE : the response to the AT command, as sent by the modem; it can contain more lines, separated by a '\' character;

if the whole response is longer than 255 characters, it will be truncated.

Please note that the MODEM_CTRL FB can't be successfully executed while the PPP connection is active, on Z-MINIRTU.

This FB cannot be used (i.e.: it won't work) in the following situations:

- if modem is set to send numeric result codes (see "ATV" command)

- for commands using a prompt (e.g.: "AT+CMGS" command)

- for call-handling commands (e.g.: "ATD", "ATA", "ATH").

20.1.11 MODEM_ONOFF

	Inst_MODEM MODEM_O		
???	ON RE	- ???	
???	— @E		
		IODEM_ONOFF (*Power on/of N ON_OFF:BOOL @ENABLE:BOOL UT RESULT:INT	ff the Modem (Z-TWS4, Z-PASS2-S, Z-MINIRTU)*)

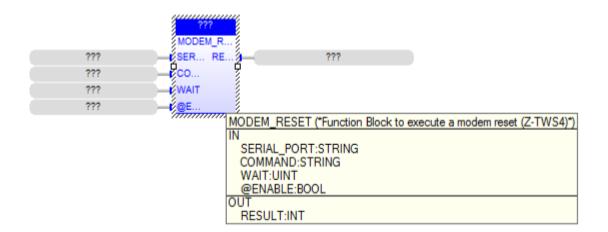
This FB permits to control the power ON/OFF digital input of the MODEM.

The params are :

ON_OFF : if True power-up the modem
@ENABLE : if True the FB is executed

RESULT : -2 FB executed with @ENABLE set to False -1 Error 0 operation not completed +1 OK +2 modem is already ON/OFF

20.1.12 MODEM_RESET



The MODEM_RESET FB sends an AT reset command to the GSM modem and waits for a specified time.

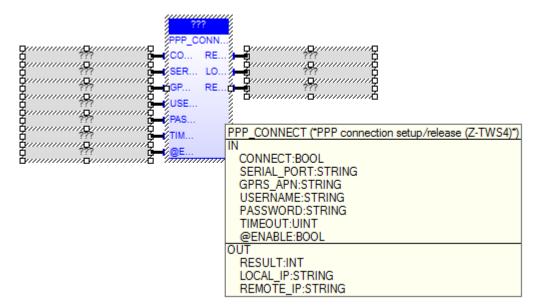
When first called, the FB runs a process which starts sending the command; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

- SERIAL PORT : this parameter is not used (it is still present only for compatibility reasons); it can be set to '' (empty string)				
- COMMAND : reset AT command to be sent;				
if left empty, the "AT+CFUN=1,1" command will be sent				
- WAIT : wait duration, in seconds, after sending the command;				
valid values are: [30300]				
- @ENABLE : TRUE -> FB is executed				
FALSE -> FB is skipped				
The FB has the following output parameter:				
- RESULT : -2, when called with ENABLE=FALSE				
-1, in case of any failure				
0, if the process is still running				
1, if the process has successfully finished				
2, if timeout has expired (timeout = WAIT + 5 seconds)				
4, if PPP is active, on Z-MINIRTU				
5, if MODEM RESET FB is already running				

Please note that the MODEM_RESET FB can't be successfully executed while the PPP connection is active, on Z-MINIRTU. Also note that, when MODEM_RESET FB is running, all other "modem related" FBs (PPP_CONNECT, SEND_SMS, GET_SMS, MODEM_CTRL and MODEM_RESET itself) are rejected.

20.1.13 PPP_CONNECT



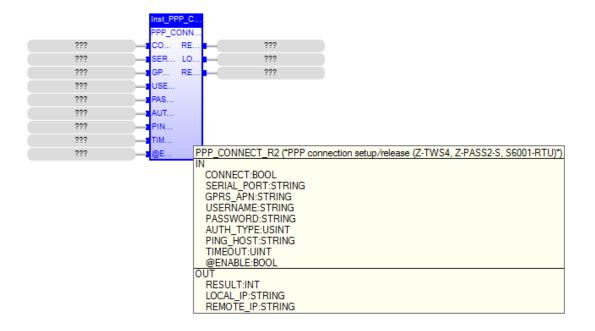
The PPP_CONNECT FB performs PPP connection setup or release, by means of a $\ensuremath{\mathsf{GPRS}}\xspace/\mathsf{UMTS}\xspace$ modem.

When first called, it runs a process which starts the connection setup or release; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

- CONNECT : TRUE -> connection setup FALSE -> connection release	
 SERIAL_PORT : this parameter is not used (it is still present only for compatibility reasons); it can be set to '' (empty string) GPRS_APN : GPRS Access Point Name (as given by the mobile operator); if this parameter is left empty, "Automatic APN" functionality 	7
is activated	
- USERNAME : username required for authentication (it can be empty, if authentication is not required);	
- PASSWORD : password required for authentication	
(it can be empty, if authentication is not required) not used with "Automatic APN" functionality	
- TIMEOUT : timeout, in seconds	
- @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped	
When CONNECT=FALSE, GPRS_APN, USERNAME and PASSWORD parameters can be empty.	
The FB has the following output parameters:	
- RESULT : -2, when called with ENABLE=FALSE	
-1, in case of any failure	
0, if the process is still running	
1, if the process has successfully finished 2, if timeout has expired	
5, if MODEM RESET FB is running	
- LOCAL IP : IP address assigned to the PPP network interface (only if	
RESULT=1, when CONNECT=TRUE)	
- REMOTE IP : IP address of the remote host (set as default gateway) (only if RESULT=1, when CONNECT=TRUE)	

20.1.14 **PPP_CONNECT_R2**



The PPP_CONNECT_R2 FB performs PPP connection setup or release, by means of a GPRS/UMTS modem.

When first called, it runs a process which starts the connection setup or release; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

- CONNECT	: TRUE -> connection setup FALSE -> connection release				
—	: this parameter is not used (it is still present only for reasons); it can be set to '' (empty string)				
—	: GPRS Access Point Name (as given by the mobile network				
activated	this parameter is left empty, "Automatic APN" functionality is				
- USERNAME	: username required for authentication				
	(it can be empty, if authentication is not required);				
	not used with "Automatic APN" functionality				
- PASSWORD	: password required for authentication				
	(it can be empty, if authentication is not required);				
	not used with "Automatic APN" functionality				
- AUTH_TYPE	: authentication type:				
	0 : None				
	1 : CHAP/PAP				
	2 : CHAP only				
	3 : PAP only				
	not used with "Automatic APN" functionality				
- PING HOST	: IP address or Host Name used to check that PPP connectivity is				
—	nning ping test;				
avarrabic, ra	if this parameter is left empty, ping test is not performed				
	II CHIS Parameter IS IEIC Empty, ping test IS not periormed				

- TIMEOUT : timeout, in seconds - @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped

When CONNECT=FALSE, GPRS APN, USERNAME, PASSWORD and PING HOST parameters can be empty.

The FB has the following output parameters: - RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished 2, if timeout has expired 5, if MODEM RESET FB is running - LOCAL IP : IP address assigned to the PPP network interface (only if RESULT=1, when CONNECT=TRUE) - REMOTE IP : IP address of the remote host (set as default gateway) (only if RESULT=1, when CONNECT=TRUE)

20.1.15 PPP_STATUS

	nst_PPP_ST GPPP_STATUSO
???	Ś <u>SER RE</u> ???
	PPP_STATUS (*PPP connection status (Z-TWS4, Z-PASS2-S, Z-MINIRTU)*)
	SERIAL_PORT:STRING
	OUT
	RESULT:INT

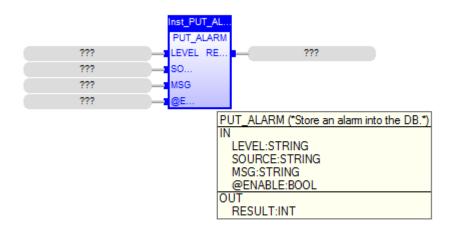
The PPP STATUS FB returns PPP connection status.

The FB has the following input parameters: - SERIAL PORT : this parameter is not used (it is still present only for compatibility reasons); it can be set to '' (empty string)

The FB has the following output parameters: - RESULT

- : 0, PPP DISCONNECTED
 - 1, PPP CONNECTED
 - 2, PPP CONNECTING
 - 3, PPP DISCONNECTING

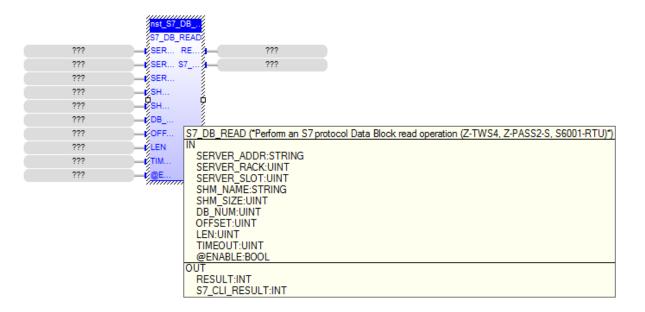
20.1.16 **PUT_ALARM**



This FB stores an alarm record into the DB; the "index" and "timestamp" fields are set by the FB; the "status" field is set to 0 by the FB. The FB is also responsible for keeping the DB size (number of records) under a specified limit (e.g.: 1000). INPUTS: - LEVEL: a string representing the alarm/event level (e.g.: "INFO") (max len=10); possible values are defined by the application - SOURCE: a string representing the alarm/event source (e.g.: "GRP1") (max len=10); possible values are defined by the application - MSG: the text message of the alarm (max len=255) - @ENABLE: TRUE -> FB is executed FALSE -> FB is skipped the parameter is set to FALSE by the FB at the end of execution OUTPUTS: - RESULT: the FB result; possible values are: 0: FB still running 1: FB successfully executed -1: FB execution failed

-2: FB execution timeout

20.1.17 S7_DB_READ



This FB performs an S7 protocol Data Block read operation. It connects to the specified S7 server IP address, rack and slot, performs the operation and then disconnects. The data read are written to the Straton shared-memory specified in the SHM NAME parameter. INPUTS: - SERVER ADDR: the S7 server IP address - SERVER RACK: the S7 server rack number - SERVER SLOT: the S7 server slot number - SHM NAME: name of the Straton shared-memory which the data are written to - SHM SIZE: size of the Straton shared-memory which the data are written to - DB NUM: the number of the Data Block to be read - OFFSET: start offset for the read operation in the Data Block - LEN: number of bytes to be read - TIMEOUT: timeout for the FB execution, in seconds - @ENABLE: TRUE -> FB is executed FALSE -> FB is skipped the parameter is set to FALSE by the FB at the end of execution OUTPUTS: - RESULT: the FB result; possible values are: 0: FB still running 1: FB successfully executed -1: FB execution failed -2: FB execution timeout - S7 CLI RESULT: the S7 Client result; possible values are: 0: no failure -1: invalid arguments failure -2: initialization failure (e.g.: error opening the shared-memory) -3: connection failure -4: read operation failure

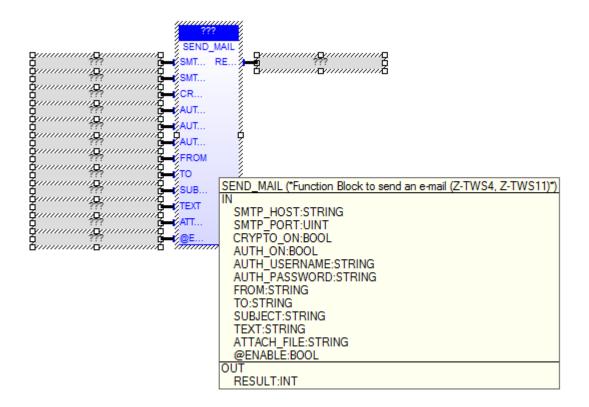
20.1.18 S7_DB_WRITE

		nst_S7_DB		
		S7_DB_WR		
	???	SER RE	???	
	???	SER S7	???	
	???	SER		
	???	SH		
	???	Сян У		
	???	CSH CSH CDB COFF		
	???	OFF		
	???	LEN		
	???			
	???	57_DI	B_WRITE (*Perform an S	7 protocol Data Block write operation (Z-TWS4, Z-PASS2-S, S6001-RTU)*)
		IN		
			RVER_ADDR:STRING	
			RVER_RACK:UINT RVER_SLOT:UINT	
			M_NAME:STRING	
			M_SIZE:UINT	
		DB	NUM:UINT	
			SET:UINT	
			I:UINT	
			IEOUT:UINT NABLE:BOOL	
		OUT	INADLE.DUUL	
			SULT:INT	
		S7_	CLI_RESULT:INT	
This F	B performs a	n S7 protoc	ol Data Blo	ck write operation.
	-	-		_
It con	nects to the	specified (S7 server I	P address, rack and slot, performs th
operat.	ion and then	disconnect	s.	
-				
ine da	ta to be wri	tten are rea	ad from the	Straton shared-memory specified in t
SHM NA	ME parameter			
		-		

```
INPUTS:
```

```
- SERVER ADDR: the S7 server IP address
- SERVER RACK: the S7 server rack number
- SERVER SLOT: the S7 server slot number
- SHM NAME: name of the Straton shared-memory which the data are read from
- SHM SIZE: size of the Straton shared-memory which the data are read from
- DB NUM: the number of the Data Block to be written
- OFFSET: start offset for the write operation in the Data Block
- LEN: number of bytes to be written
- TIMEOUT: timeout for the FB execution, in seconds
- @ENABLE: TRUE -> FB is executed
FALSE -> FB is skipped
the parameter is set to FALSE by the FB at the end of execution
OUTPUTS:
- RESULT: the FB result; possible values are:
   0: FB still running
  1: FB successfully executed
 -1: FB execution failed
  -2: FB execution timeout
- S7 CLI RESULT: the S7 Client result; possible values are:
  0: no failure
  -1: invalid arguments failure
  -2: initialization failure (e.g.: error opening the shared-memory)
  -3: connection failure
  -4: write operation failure
```

20.1.19 SEND_MAIL

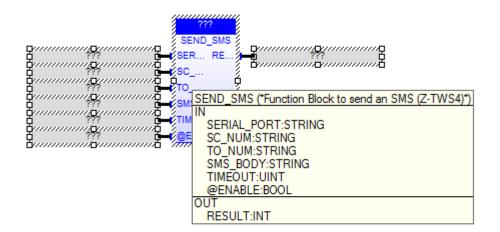


The SEND MAIL FB sends an e-mail, by means of the SMTP/SMTPS protocol.

When first called, the FB runs a process which starts sending the e-mail; on subsequent calls, it only checks if the process has finished its job.

```
The FB has the following input parameters:
- SMTP_HOST
             : IP address or host name of the SMTP/SMTPS server
- SMTP_PORT
                : TCP port for the SMTP/SMTPS protocol (normally: 25, for SMTP;
465, for SMTPS)
               : if cryptography (SSL) shall be used (FALSE -> SMTP, TRUE ->
- CRYPTO_ON
SMTPS)
                  (CRYPTO ON=TRUE is available only for Z-TWS4/Z-PASS2-S)
               : if authentication shall be executed
- AUTH ON
- AUTH USERNAME : username for authentication
- AUTH PASSWORD : password for authentication
- FROM
               : e-mail sender
- то
                : e-mail recipient
                 more than one recipient can be specified, using the ','
character as separator
- SUBJECT
               : e-mail subject
- TEXT
               : e-mail text
- ATTACH FILE
              : name of the file (with path) to be attached to the e-mail (it
can be empty)
- @ENABLE
               : TRUE -> FB is executed
                 FALSE -> FB is skipped
The FB has the following output parameter:
- RESULT : -2, when called with ENABLE=FALSE
           -1, in case of any failure
            0, if the process is still running
            1, if the process has successfully finished.
```

20.1.20 SEND_SMS



The SEND SMS FB sends an SMS, by means of a GSM modem.

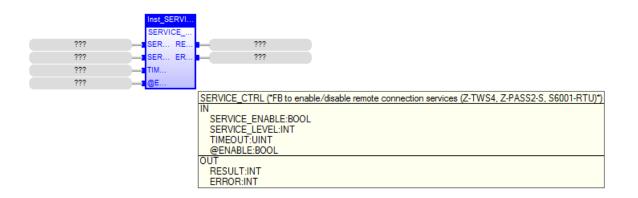
When first called, it runs a process which starts sending the SMS; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

- SERIAL_PORT : this parameter is not used (it is still present only for compatibility reasons); it can be set to '' (empty string) : SMS Service Center (as given by the mobile operator) (it can be - SC NUM empty, if the SC number is already set on the modem/SIM) : recipient number - TO NUM - SMS BODY : SMS text - TIMEOUT : timeout, in seconds : TRUE -> FB is executed - @ENABLE FALSE -> FB is skipped The FB has the following output parameter: - RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished 2, if timeout has expired 4, if PPP is active, on Z-MINIRTU 5, if MODEM RESET FB is running

Please note that the SEND SMS FB can't be successfully executed while the PPP connection is active, on $\overline{\rm Z}\mbox{-MINIRTU}.$

20.1.21 SERVICE_CTRL



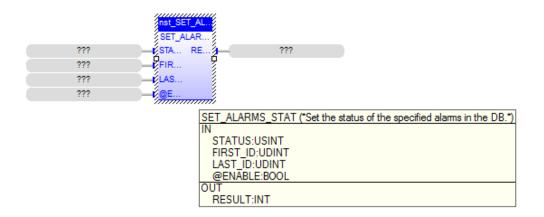
The SERVICE_CTRL FB enables or disables connection services, based on the required service level.

When first called, it runs a process which starts the procedure; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

- SERVICE ENABLE : TRUE -> enable connection services FALSE -> disable connection services - SERVICE LEVEL : this parameter defines the "Security Level", that is it tells which connection services shall be enabled/disabled; possible values are: 0: None 1: VPN Connection 2: VPN Service 3: Internet Connection 4: SMS Service -1: the value of the "Security Level / Service Disable" configuration parameter will be used - TIMEOUT : timeout, in seconds - @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped The FB has the following output parameters: - RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished 2, if timeout has expired - ERROR : this parameter is meaningful only when RESULT=-1; in all other cases, it is set to 0; possible values are: 1: the FB has been called with SERVICE LEVEL=0 2: the procedure to enable/disable the connection services is already running 3: the CPU configuration procedure is running -> FB execution has been aborted 4: connection services are disabled since Remote Connection Disable (RCD) digital input is HIGH -> FB execution has been aborted

20.1.22 SET_ALARMS_STAT



the passed arguments. INPUTS: - STATUS : this parameter is handled as a bitmask, meaning that the status of the relevant alarm records will be set as: alarms.stat = (alarms.stat | STATUS), where: alarms.stat: DB field STATUS: this parameter - FIRST_ID : the id of the first record retrieved by the GET_ALARMS FB - LAST ID : the id of the last record retrieved by the GET ALARMS FB - @ENABLE: TRUE -> FB is executed FALSE -> FB is skipped the parameter is set to FALSE by the FB at the end of execution OUTPUTS: - RESULT: the FB result; possible values are: 0: FB still running 1: FB successfully executed -1: FB execution failed -2: FB execution timeout

This FB sets the value of the "status" field for the alarm records specified by

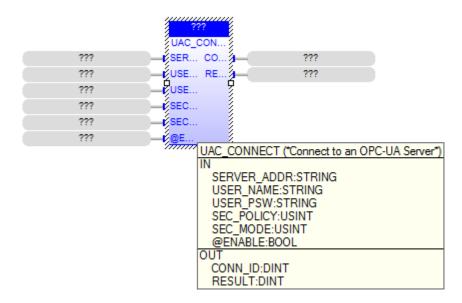
20.1.23 TIME_SYNC

TIME_SYNC ("Time synchronization by means of NTP protocol (Z-TWS4, Z-TWS11)")
IN
@ENABLE:BOOL
OUT
RESULT:INT

The TIME SYNC FB performs time synchronization, by means of the NTP protocol.

When first called, the FB runs a process which starts performing the synchronization; on subsequent calls, it only checks if the process has finished its job. The FB has the following input parameter: - @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped The FB has the following output parameter: - RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished.

20.1.24 UAC_CONNECT

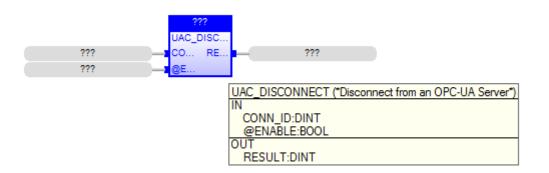


This Function Block can be used to connect to an OPC-UA Server.

When first called, it runs a process which starts the procedure; on subsequent calls, it only checks if the process has finished its job. The FB has the following input parameters: - SERVER ADDR : OPC UA Server URL (e.g.: opc.tcp://192.168.90.2:53530/OPCUA/SimulationServer) - USER NAME : user name for authentication - USER_PSW : password for authentication - SEC POLICY : numeric value for Security Policy: 1: None 2: Basic128Rsa15 3: Basic256 4: Basic256Sha256 all other values are invalid - SEC MODE : numeric value for Security Mode: 1: None 2: Sign 3: Sign and Encrypt all other values are invalid - @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped The FB has the following output parameters: - RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished - CONN ID : connection identifier, to be used in UAC READ, UAC WRITE and

20.1.25 UAC_DISCONNECT

UAC DISCONNECT FBs



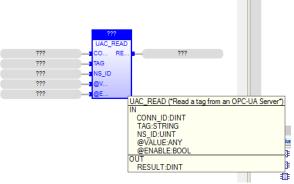
This Function Block can be used to disconnect from an OPC-UA Server.

When first called, it runs a process which starts the procedure; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters: - CONN_ID : connection identifier, given by the UAC_CONNECT FB - @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped

The FB has the following output parameters: - RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished

20.1.26 UAC_READ



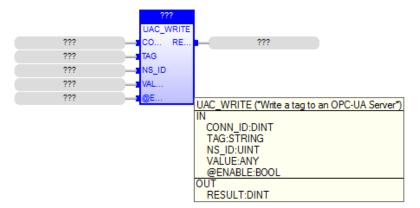
This Function Block can be used to read a tag from an OPC-UA Server.

When first called, it runs a process which starts the procedure; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters: - CONN_ID : connection identifier, given by the UAC_CONNECT FB - TAG : name of the tag to be read - NS_ID : tag name namespace index - @VALUE : variable to store the tag value - @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped

The FB has the following output parameters: - RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished

20.1.27 UAC_WRITE



This Function Block can be used to write a value to a tag of an OPC-UA Server.

When first called, it runs a process which starts the procedure; on subsequent calls, it only checks if the process has finished its job.

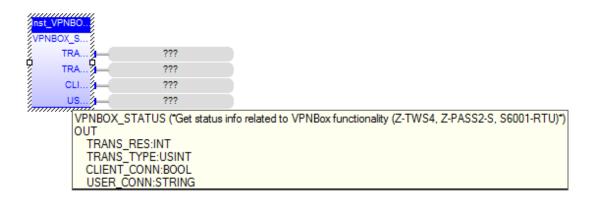
The FB has the following input parameters:

- CONN ID : connection identifier, given by the UAC CONNECT FB
- TAG : name of the tag to be written
- NS ID : tag name namespace index
- VALUE : variable to be written to the tag

- @ENABLE : TRUE -> FB is executed FALSE -> FB is skipped

The FB has the following output parameters: - RESULT : -2, when called with ENABLE=FALSE -1, in case of any failure 0, if the process is still running 1, if the process has successfully finished

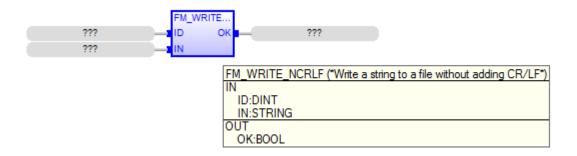
20.1.28 VPNBOX_STATUS



This FB provides information about the VPN Box functionality. INPUTS: none OUTPUTS: - TRANS RES : the result of the last VPN Box transaction performed by the CPU; possible values: -2: No response from VPN Box -1: Invalid response from VPN Box 0: OK 3: Wrong password 7: License limit reached 201: Generic error 202: VPN Box not configured 1000: No transaction has been performed (e.g.: VPN Box functionality is disabled) other: Unexpected response - TRANS TYPE : the type of the last VPN Box transaction performed by the CPU; possible values: 0: None (no transaction performed) 1: Register 2: Poll - CLIENT CONN : flag telling if a VPN Client is connected (meaningful only for "Point-to-Point" VPN Box) 0: no VPN client is connected 1: a VPN client is connected - USER CONN : if a VPN Client is connected, this parameter provides the authenticated username; otherwise, it is an empty string ('') (meaningful only for "Point-to-Point" VPN Box)

20.2 Functions

20.2.1 FM_WRITE_NCRLF

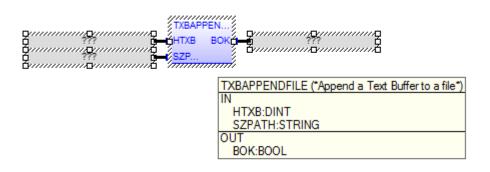


Same behaviour as FM_WRITE but without inserting final CR-LF $% \mathcal{M}_{\mathrm{CR}}$

Input parameters:
- ID: id of the file (already open)
- IN: string to write into the file

Output parameters:
- OK: boolean result value: (TRUE:success, FALSE:failure)

20.2.2 TXBAPPENDFILE



Append a Text Buffer to a file (without reloading the file).

Input parameters

- HTXB: Text Buffer handle
- SZPATH: file absolute path

Output parameters
- BOK: boolean result value: (TRUE:success, FALSE:failure)

20.2.3 GET_MIN_SINCE2K

GET_MIN_S. GET_MIN_S. GET_DAT MII	
	GET_MIN_SINCE2K (*Get the number of minutes since year 2000*)
	IN
	DATETIME:STRING
	OUT
	MIN:UDINT

This function returns the current number of minutes since January 1, 2000 0:00:00, if DATETIME is empty or DATETIME is not a valid date/time; otherwise, it returns the number of minutes since January 1, 2000 0:00:00, corresponding to DATETIME. DATETIME shall have the following format: "dd/mt/yyyy hh:mm:ss"

20.2.4 MBUS_READ_CTL

	MBUS_REA		
???		???	
	MBUS	_READ_CTL (*Function to	enable/disable the M-Bus read operations*)
	IN		
	ENA	ABLE:BOOL	
	OUT		
	RES	SULT:INT	

The ${\tt MBUS_READ_CTL}$ function can be used to enable/disable the M-Bus read operations.

It should be noticed that M-Bus read operations are enabled by default.

The function has the following input parameter: - ENABLE : TRUE, to enable read operations FALSE, to disable read operations

The function has the following output parameter:
- RESULT : 1: function has been successfully executed
-1: function execution failed

20.2.5 WDOG_KEEP_ALIVE

WDOG_KE... RE... ??? WDOG_KEEP_ALIVE ("Function to refresh the HW Watchdog (Z-TWS4, Z-PASS2-S, S6001-RTU)") OUT RESULT:INT

This function restarts the HW Watchdog timer.

NOTICE: once enabled, the HW Watchdog cannot be disabled; the WDOG_KEEP_ALIVE function shall be called to restart the timer; if timeout elapses, an HW reboot is triggered.

To let this function actually work, the "WATCHDOG/Enable" parameter in the CPU configuration shall be set to "OFF"; otherwise, the function will return the -2 value (see below).

INPUTS: none

OUTPUTS:

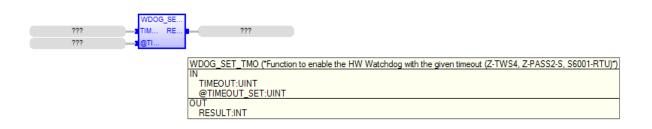
- RESULT: the function result; possible values are:

0: OK

-1: watchdog setting failed (WDOG_SET_TMO function has not been called or failed)

-2: watchdog controlled by system ("WATCHDOG/Enable" parameter set to "ON") -3: watchdog keep-alive failed

20.2.6 WDOG_SET_TMO



This function enables the HW Watchdog.

NOTICE: once enabled, the HW Watchdog cannot be disabled; the WDOG_KEEP_ALIVE function shall be called to restart the timer; if timeout elapses, an HW reboot is triggered.

The function can be called many times; if the timeout value is the same already set, it will do nothing; otherwise, the new timeout value will be set.

To let this function actually work, the "WATCHDOG/Enable" parameter in the CPU configuration shall be set to "OFF"; otherwise, the function will return the -2 value (see below).

INPUTS: - TIMEOUT: Watchdog timeout, in seconds; possibile values: [30..3600]; if an out-of-range value is given, the default value 60 will be set - @TIMEOUT_SET: at the end of the execution, this parameter will contain the timeout value actually set (in seconds) OUTPUTS: - RESULT: the function result; possible values are: 0: OK -1: watchdog setting failed

-2: watchdog controlled by system ("WATCHDOG/Enable" parameter set to "ON")

21 Z-NET4

When using Z-TWS4/Z-PASS2-S/S6001-RTU 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 let you:

- automatically discover the I/O modules available on the bus;
- configure the CPU (Z-TWS4/Z-PASS2-S/S6001-RTU) and the I/O modules;
- automatically create a StratON project containing the I/O variables, with the Modbus tasks needed to acquire/control them; for S6001-RTU, variables corresponding to the CPU I/Os are also inserted into the project
- automatically generate code for the StratON project, performing "Remote Control Functions", such as:
 - $\circ \quad \text{Data Logging} \quad$
 - \circ $\,$ Command and Status SMS $\,$
 - o Alarm generation
- easily create custom web pages, with graphic widgets, and upload them to the CPU (these pages can be accessed on the standard HTTP [80] TCP port).

The Z-NET4 SW is available at the following link:

http://www.seneca.it/products/z-net4

Please contact Seneca to get more information about the Z-NET4 suite.

22 Access to Straton variables

The aim of this chapter is to explain how an application (typically, web-based) can access the variables of the Straton Soft-PLC running on Z-TWS4/Z-PASS2-S/S6001-RTU.

Currently, there are two ways to access Straton variables:

- direct access to Straton shared-memory
- access by means of CGI

The main differences between the two methods is that the first requires developing a C program, running on the Device, typically invoked by the *lighttpd* web server, while the second does not require any changes in the Device FW, provided that the currently supported CGIs are used.

22.1 Shared Memory

Straton Workbench lets you define a shared-memory area and tell which PLC variables shall be put in it.

5	STRATON - test	_zpass2s_retain		- 🗆 🗙
File Edit View Insert Project Tools Wind	dow Help			
	이 어디 部長期 높 %6 😨 🕼 르 🐅 😗 🎽 🖉			
Workspace	IO Drivers			HZX
B 🗿 test_zpass2s_retain	🖀 🕀 Mo MODBUS Master	Name	Value	🍸 Name Type Dim. Attrib.
😑 📴 Exception programs	P Mg MODBUS Slave	Symbol	VarINT	🟠 Global variables
Cap pOnBadIndex	E C Shared memory (embedded systems)	Offset	0	🗉 🛃 RETAIN variables
pOnDivZero		Size	2	main (*main program*)
pShutDown	ZNET_VARIABLES	Format	Signed integer	"≓ pOnBadIndex
pStartup	0 [2] - VarINT	Mode	In/Out	PonDivZero
Graphic				pShutDown
😑 — 🧀 Programs	4 (4) - ValUN1 8 (2) - ValUNT			DStartup
Recipe				
- incope	Et Indial-vaniewe			
Soft Scope				
Spy				
String Tables				< >
Initial values				
				Name Value
😨 Profiles				
🚰 Variables				
L Types				
	A main IO Drivers			
	Build			×
	Build Cross references Runtime Call stack Breakpoints Digital sampling trace	Prompt HMI		
Ready	Cross references Huntime Cali stack Breakpoints Digital sampling trace	OffLine 192.168.85.105:502	۵,90 ا	184 x 18 0,0 100%
reduy		OTLUE 192.100.85.105:302	2 0,50 0	100 % (Mag)

For each variable in the shared-memory, the Workbench lets you define the following properties:

- Symbol: the name of a Straton variable defined elsewhere (Global Variables, Retain Variables etc.)
- *Offset*: the offset in the shared-memory
- Size: the variable size, in bytes
- Format: the kind of variable, i.e. "signed integer"
- *Mode*: if the variable is an *Input*, an *Output* or an *In/Out* (from the Straton point of view)

	Variable	×
Identification Symbol: Offset:	VarINT	OK Cancel
Format in shar Format: Select a pre	red memory Signed integer v Size: 2	
Output (de om shared memory to STRATON) from STRATON to shared memory) Bidirectional)	

The list of variables in the shared-memory, along with their properties, can be saved to / loaded from a *csv* file; the format of this file is as in the following example:

```
"NAME";"OFFSET";"SIZE";"FORMAT";"MODE";"ERROR_REPORT"
"VarINT";"0";"2";"0";"2";"CPU_ErrorReport_dummy"
"VarUINT";"2";"2";"1";"2";"CPU_ErrorReport_dummy"
"VarDINT";"4";"4";"0";"2";"CPU_ErrorReport_dummy"
"VarUDINT";"8";"4";"1";"2";"CPU_ErrorReport_dummy"
```

22.2 C program example

In this paragraph, an example is given of a simple C program which can be used to access a shared-memory.

The program arguments lets you specify:

- the shared-memory name
- the shared-memory size
- the offset, used to tell the program from which address in the shared-memory it shall start printing byte values

```
int main(int argc, char* argv[])
{
    long shmid;
    char *pMap;
    sem_t *sem;
    int i, iCpt ;
    for (i=1; i<argc; i++)
    {
        if (strcmp (argv[i], "?") == 0 || strcmp (argv[i], "/?") == 0)
        {
            printf ("Syntax: shmtest [options]\n");
            printf ("Options:\n");
            printf (" /name= Named memory\n");
            printf (" /size= Memory size\n");
        }
    }
}
</pre>
```

```
printf (" /offset=
                               Memory offset\n");
        return 0;
    }
    if (strncmp (argv[i], "/name=", 6) == 0)
    {
        strcpy (szName, (argv[i] + 6)) ;
    }
    else if (strncmp (argv[i], "/size=", 6) == 0)
    {
        wSize = atoi (argv[i] + 6);
    }
    else if (strncmp (argv[i], "/offset=", 8) == 0)
    {
        wOffset = atoi (argv[i] + 8);
    }
}
shmid = shm_open(szName, O_RDWR, S_IRWXO|S_IRWXG|S_IRWXU) ;
if (shmid < OL)
{
   printf("Error shm open : <%s>\n", szName) ;
   return 0;
}
ftruncate(shmid, wSize) ;
pMap = mmap(NULL, wSize, PROT READ | PROT WRITE, MAP SHARED, shmid, 0);
if (pMap == MAP FAILED)
{
   printf("Error mmap : <%s> size <%d>\n", szName, wSize) ;
   return 0;
}
sem = sem open(szName, O RDWR, S IRUSR | S IWUSR, 0);
if (sem == SEM FAILED)
{
   printf("Error sem_open : <%s>\n", szName) ;
   return 0;
}
init_keyboard() ;
iCpt = 0;
while( ShouldTerminate()==0)
{
    sem wait(sem) ;
    printf("Iteration %d\n", iCpt++) ;
   for (i=0+wOffset ; i<wSize ; i++)</pre>
     printf ("%02X ", (unsigned char)pMap[i]);
     if ((i+1)%16 == 0)
       printf("\n") ;
    }
    sem_post(sem);
   usleep(100*1000) ;
   system("clear") ;
}
close_keyboard() ;
munmap(pMap, wSize);
sem close(sem);
close (shmid) ;
return 0;
```

}

Note that the above code will print shared-memory byte values, without any knowledge of the variables properties.

Indeed, it is important to understand that <u>the shared-memory contains only the variables values</u>; the variables properties shall be retrieved, for example, by loading them from the *csv* file, shown above.

Below, some lines of code are given providing some definitions useful for variables properties handling.

```
#define VAR NAME MAX LEN 50
#define VAR MAX NUM 100
typedef enum
{
    VAR FORMAT INT,
   VAR FORMAT UINT,
   VAR_FORMAT_FLOAT,
   VAR_FORMAT_STRING,
   VAR FORMAT NUM
} VAR FORMAT T;
const char *var_format_str[] =
{
    "integer",
    "unsigned integer",
    "float",
    "string"
};
typedef enum
{
    VAR MODE IN,
    VAR MODE OUT,
    VAR MODE INOUT,
    VAR MODE NUM
} VAR MODE T;
const char *var_mode_str[] =
{
    "input",
    "output",
    "input/output"
};
typedef struct VarDescrS
{
    char name[VAR NAME MAX LEN+1];
    unsigned int offset;
   unsigned int size;
   VAR FORMAT T format;
    VAR MODE T mode;
} VarDescrT;
static VarDescrT *vars[VAR MAX NUM];
```

22.3 CGI

Another way to gain access to the Straton variables is by means of CGIs.

The variables that can be read/written by means of CGIs are those which are placed in the Straton sharedmemory. In the Device FW, a daemon is running which:

- parses the CGI requests
- reads/writes the requested variables from/to the shared-memory
- gives back the values/results in the CGI responses

Two CGIs are defined, one to read and one to write variables, as described in the following.

Both CGIs shall be inserted into HTTP POST requests.

It is important to note that, as far as the variables properties are concerned, normally the application sending the CGIs doesn't need to know the offset, size and format of a variable, while it needs to know the variables names and, possibly, the variables modes, to tell which variables can be read/written and which can only be read.

22.3.1 CGI "readVariable"

To read one variable:

```
request:
goform/readVariable?nVars=1&var1=<var name1>
response:
#<var name1>
                                <var code1> <var add info1>
<var value1>
Example:
request:
goform/readVariable?nVars=1&var1=M1 Output 1
response (successful case):
# M1 Output 1
                               0
1
response (failure case):
# M1 Output 1
                               5 Operation timeout
```

The CGI can be extended to read N variables (N>1), for example to read 2 variables:

goform/readVariable?nVars=2&var1=<var name1>&var2=<var name2>

The response contains N sections with the format described above.

22.3.2 CGI "writeVariable"

To write one variable:

Example:

request goform/writeVariable?nVars=1&var1=M1_Output_1&value1=1 response (successful case): # M1_Output_1 0 response (failure case): # M1_Output_1 5 Operation timeout

The CGI can be extended to write N variables (N>1), for example to write 2 variables:

```
goform/writeVariable?nVars=2&var1=<var_name1>&var2=<var_name2>&value1=<va
r_value1>&value2=<var_value2>
```

The response contains N sections with the format described above.

23 Glossary

<u>Router</u>: a networking device that forwards data packets between computer networks, e.g. between a LAN and a WAN (the Internet).

<u>Switch</u>: a networking device that connects devices together on a computer network, by using a form of packet switching to forward data to the destination device.

<u>VPN</u>: a Virtual Private Network extends a private network across a public network, such as the Internet. It enables a device to send and receive data across the public network as if it were directly connected to the private network. A VPN is created by establishing a virtual point-to-point connection through the use of tunnelling protocols, with traffic encryption.

<u>Tunnel</u>: an IP tunnel is an Internet Protocol (IP) network communications channel between two networks. It is used to transport another network protocol by encapsulation of its packets.