

IOT SCADA SOFTWARE INSTALLATION AND USER MANUAL





Index

1 Introduction	6
2 IOT SCADA software	7
2.1 General characteristics	
2.2 Models	7
2.3 Software and Gateway	8
3 Physical world and IoT	9
3.1 Analog inputs	9
3.2 Digital inputs	9
3.3 Ethernet ports	9
3.4 RS232/485 port	9
4 Access	10
4.1 First access to the software and related PC/gateway	
4.2 Wi-Fi access	14
4.2.1 Access with local/corporate Wi-Fi	14
4.2.2 Wi-Fi Access Point Gateway	14
4.3 Ethernet LAN access	15
4.3.1 Local/corporate LAN	15
4.3.2 Direct connection to a PC (LAN cable)	17
4.4 Setting up your operating system	17
4.4.1 Windows 7	17
4.4.2 Windows 10	20
4.4.2 Windows 10 4.4.3 Connection to an existing LAN network	20
4.4.2 Windows 104.4.3 Connection to an existing LAN network4.5 Software installation	
 4.4.2 Windows 10 4.4.3 Connection to an existing LAN network 4.5 Software installation	
 4.4.2 Windows 10 4.4.3 Connection to an existing LAN network 4.5 Software installation	
 4.4.2 Windows 10 4.4.3 Connection to an existing LAN network 4.5 Software installation 4.5.1 Provided files 4.5.2 Installation procedure 4.5.3 Update procedure 	
 4.4.2 Windows 10 4.4.3 Connection to an existing LAN network 4.5 Software installation 4.5.1 Provided files 4.5.2 Installation procedure 4.5.3 Update procedure 4.5.4 License activation. 	

5 Configuration	
5.1 Communication	34
5.1.1 TCP/IP Configuration	34
5.1.2 Connection to an existing Wi-Fi network	36



Index

5.1.3 Internet communication test	36
5.1.4 Port and communication parameters configuration	37
5.1.5 Modbus Gateway	38
5.1.5.1 Rules of automatic mapping	38
5.1.6 MQTT brokers configuration	39
5.2 Installation	40
5.2.1 System devices connection and configuration	40
5.2.1.1 Adding new devices	40
5.2.1.2 Removing a device	42
5.2.1.3 Installation support manuals	43
5.2.3 Devices measures setup	43
5.2.3.1 Measures offset	45
5.2.3.2 Measures scaling	45
5.2.4 General settings	46
5.2.5 Password change	46
5.3 Customization	47
5.3.1 Logos and title	47
5.3.2 Custom measures	47
5.3.3 Custom alarms	48
5.3.4 Events	52
5.3.5 Synoptics configuration	56
5.4 Interface and Cloud services	60
5.4.1 E-mail and SMS notifications	60
5.4.2 Dropbox connection	61
5.4.3 OneDrive account	65
5.4.4 FTP Backup	66
5.4.4.1 Details of the transferred files	67
5.4.5 Connection with Microsoft SQL Server	67
5.4.6 Connection to Azure IoT Hub	70
5.4.7 MQTT Service	72
5.4.7.1 Getting started	72
5.4.7.2 Configuration of the information to send on MQTT Broker	75
5.4.7.2 Final configuration	76
5.5 Information	80
5.5.1 Device catalogue	80
5.5.2 License management	81
5.5.3 Informations	82
5.5.4 Logs	82



Index

6 User interface	83
6.1 Synoptics	83
6.2 Devices	84
6.2.1 System measures display	84
6.2.1.1 Data and alarms display	85
6.2.2 Graphs	87
6.2.3 Measure write	88
6.2.4 Exporting data to Excel	89
6.3 Alarms	89
6.4 Alarms history	90
6.5 Report	91
6.6 Documents	93
6.7 Favourites	94

7 Troubleshooting – FAQ	95
7.1 Specific functions for Machine tools and Machining centres	95
7.2 Remote part program transfer (machine instructions)	95
7.3 IOT SCADA SERVER does not switch on	100
7.4 Unable to complete Internet communication test	100
7.5 Communication problems with serial devices	100
7.6 Unable to access IOT SCADA SERVER from the local network	100
7.7 Unable to access IOT SCADA SERVER from the Internet	100
7.8 Auto start of the IOT SCADA system and the gateway at power-up of the	
machine	100
7.9 System hotspot activation	101
7.10 System configuration	102

8 (Contacts	• • • • • • • • • • • • • • • • • •	•••••		
-----	----------	-------------------------------------	-------	--	--



1 Introduction

This manual is intended for installation, configuration and use of Alleantia's IOT SCADA Software (product codes ISS_YY) on hardware with Windows OS. If the system comes already pre-installed on IoT gateway hardware (appliance), go to Paragraph 4.4.

ISC web software is a monitoring system of operational parameters of plants, machines and industrial equipment, with additional functions as creation of alarms, synoptic, sending instant messages (email, sms) for alarms, data export to Excel, creation of graphs, etc.

In addition, if the system has optional plug-ins, it is able to send data to third party applications both on premise and on cloud is configured with: SQL, Rest API, IOT HUB AZURE, Dropbox, etc.

Finally, there are optional modules available:

- Energy Pack application to monitor energy production in solar PV plants and energy usage from many meters;
- Machining Pack application to control and account for the energy usage in production and operations of machine tools, combined with energy meter (Energy KIT).

For further details on these optional modules, please, refer to the user manuals, available at www.alleantia.com on Technical Documents page.



2 IOT SCADA software

2.1 General characteristics

The Alleantia ISC software license can be purchased and installed on a PC or a gateway with proper specifications on WINDOWS operating system, or it can be purchased already embedded on specific hardware (gateway DELL EG5000, Advantech UTX 3115, ISS Alleantia, etc.).

The last one is IOT Scada Server ISS (AL-ISS-XXX-YY products class).

There are different versions of software license depending on the following parameters:

- 1. Number of devices to connect to the software for monitoring and supervision;
- 2. Number of variables to read.

For example, the ISC 4 license (AL-ISC-4 product code) from the different connected devices allows to monitor up to 4 devices and 200 variables.

The variables are to be considered as the monitored values: speed, temperature, power, voltage, etc.

Recommended system requirements (hardware) to install the license:

- Windows 10 IoT 2016
- Processor 2 GB RAM
- Memory 32G SSD (4 GB suggested)

For the licenses that allow to monitor a large number of devices and variables (more than 15 devices and 1500 variables), it is recommended to increase the processor and memory capacity to improve the data processing capacity and system throughput.

The software works also on Windows 7 and Windows 10 but, in this case, the operating system requires more hardware resources.

2.2 Models

As mentioned in the previous paragraph, different versions are available, according to the variables and monitored devices.

Code	N°Variables	N°Devices
AL-ISC-60	3000	60
AL-ISC-45	2250	45
AL-ISC-30	1500	30
AL-ISC-15	750	15
AL-ISC-7	350	7
AL-ISC-4	200	4
AL-ISC-2	100	2
AL-ISC-1	50	1



2 IOT SCADA software

The devices include energy meters, PLC, CNC, inverter, etc.

The variables are the monitored values as speed, temperature, power, voltage, state, both cumulative alarms and specific alarms, etc.

2.3 Software and Gateway

As mentioned in Paragraph 2.1, the software licence can be installed on industrial gateway, to be deployed in plant, electric cabinet or machines, with various architectures, depending on the plant topology, number of connected devices, networking requirements, etc.

On the market, there are diverse kinds of gateways with different configurations of the processors and disk memory, with additional connection type (Wi-Fi, 3G, LAN), ports and inputs/outputs.

At the moment, Alleantia Srl certifies ISC software on the following devices:

- 1. ISS Alleantia: appliance equipped with analog and digital I/O terminal block. The documents can be downloaded from Alleantia website.
- 2. DELL Edge Gateway 5000 (for further details, visit DELL site and see Annex A);
- 3. Advantech UTX 3115 (for further details, visit ADVANTECH site and see Annex B).

Before exploring installation and the functioning of the system, in the following section there are characteristics related to the physical world, which are useful for IoT Scada software use.

On the Alleantia web site the list of certified software is periodically updated.



3 Physical world and IoT

The software allows the user to immerse themselves into IoT world thanks to its various functionalities: connections with the "physical" world, represented by plants, devices, probes in the field and besides monitoring and managing the values, allows to connect the physical production systems and plants with different IT systems and applications, on premise and on cloud.

The measured values can be sent, for example, to OneDrive, Dropbox and in SQL, Modbus or REST API format vs. the most varied applications.

In this paragraph, there are some concepts and a short overview of the values, read by the system and related to the "physical" world.

3.1 Analog inputs

The analog inputs are available on the hardware with the installed software, or remote expansion I/O modules, connected through available ports, which are used for the acquisition of voltage signals (0-10 V) or current (up to 20 mA).

All probes and sensors data will be displayed from the system in individual channels.

See the technical data sheet and user manuals of the used hardware and/or I/O expansion, for the types of inputs and outputs, and connect only supported ones, to avoid damaging the hardware.

3.2 Digital inputs

Usually, in the gateways and the I/O expansions, DC voltage from the physical world is interpreted as a valid signal that activates the input.

See the technical data sheet and user manuals of the used hardware and I/O expansion, for the types of inputs and outputs, and connect only supported ones, otherwise the hardware can be damaged.

3.3 Ethernet ports

When one or more Ethernet ports are available, it is possible to integrate the gateway into a network architecture and make it "visible" to other systems, after assigning an IP by the network operator.

Furthermore, this port is also used for connection of machines/devices in the field (PLC, CNC, etc.). See on www.alleantia.com site the library of products supported by Alleantia, also the drivers can be found there.

All the gateways, certified by Alleantia, are equipped or can be equipped with dual LAN to address many diverse networking requirements.

3.4 RS232/485 port

When this kind of ports is available, it is possible to connect systems that use RS232 or RS485 communication protocols, usually Modbus protocols supported by the systems as inverters, energy meters, PLC, etc. See on www.alleantia.com site the library of products supported by Alleantia, also the drivers can be found there.



4.1 First access to the software and related PC/gateway

To access the software you must first do some gateway installation, such as suitable electrical connection and to connect mouse, keyboard and monitor.

When it is supplied with power (see gateway manual of the manufacturer and Annex), it can be switched on.

In the event that the device turns on automatically when supplied with power, it means that auto start and auto off functions were activated in the BIOS.

Proceed with the following the steps:

- 1. Connect the device to its electrical outlet (see gateway manual of the manufacturer and Annex), paying attention to electrical protection.
- 2. Connect the monitor to the video output port on the gateway (see manual).
- 3. Connect a keyboard to the USB port on the gateway (see manual).
- 4. Connect a mouse to the USB port on the gateway (see manual).
- 5. Access to the desktop of Windows operating system and in the bottom right corner of the screen right click on "**Network and Internet**".





6. Select "Open Network and Sharing Center".



7. A window will open: click "Ethernet" at the top right of the window.



8. Click "Properties".

	15	1
General		
Connection —		
IPv4 Connect	ivity:	Internet
IPv6 Connect	ivity: No r	network access
Media State:		Enabled
Duration:		05:01:05
Speed:		1.0 Gbps
Activity —		
Activity ———	Sent — 💵 –	- Received
Activity	Sent — 🙀 – 7.492.706	- Received 76.798.793
Activity Byte:	Sent — 7.492.706 Diagnose	- Received 76.798.793



9. Select "Internet Protocol Version 4 (TCP/IPv4)", then click "Properties".



10. The window with IP addresses will open. Type here the static IP address you wish to give to your hardware gateway. If you don't know which IP address to set, ask your network administrator.

Fill in "Subnet mask", "Default gateway", "DNS" and other fields, to allow the device to access local networks, internet, etc.

These addresses and parameters can be used, for example, to enable the system to send automatic email notifications (e.g. alarms, reports, etc.), to view the software on smartphone and tablet, or for the remote support.

automatically if your network supports ed to ask your network administrator		Internet
atically	re	ork access
		Enabled
192.168.1.29	^	05:02:21
255.255.255.0		10 0000
192.168.1.1		
automatically		-
r addresses:	>	
8.8.8.8	ës	Received
8.8.4.4		5.801.045
Advanced] luit	
OK Cancel		
	automatically if your network supports ed to ask your network administrator atically : 192.168.1.29 255.255.255.0 192.168.1.1 automatically r addresses: 8.8.8.8 8.8.4.4 Advanced OK Cancel	automatically if your network supports ed to ask your network administrator atically : 192.168.1.29 255.255.0 192.168.1.1 automatically r addresses: 8.8.8.8 8.8.4.4 Advanced



11. Check Use the following IP address, click Ok and close the window.

When the correct IP address is assigned to the device, it can be displayed on the client's network. The addresses from the figure above can be modified by the corporate network administrator, in order to assign correct addressing and network property, web access, etc.

In case of connection to multiple networks, make sure that the assigned IP addresses are compatible. For example, connecting the device on the office PCs network may conflict with the IP of monitored CNC/PLC. In such situation, assign a compatible IP also to the CNC or PLC, making choices both on the CNC and the gateway and PCs that need it.

CAUTION

setting a wrong IP address can result in equipment malfunctioning. If you're not sure about the IP address setup, ask your network administrator and/or verify the machine vendor user manual.

12. Click the IoT WEB Scada icon on your desktop to start the software.

13. Log in, using username and password from the from the software license coupon provided by your supplier. Now the system is ready and settings and configuration can be done.

Remote Desktop

As an alternative to points 1, 2, 3 and 4, there is the possibility to connect to the gateway via laptop or PC, using a remote desktop system. It can be useful in next steps (after first configuration, the user can install remote desktop software on the gateway, such as TeamViewer or others, downloading it for free from the web).

If purchased directly from Alleantia or its distribution channels, the hardware comes with the preloaded remote desktop software, so you can follow these steps:

- 1. Download TeamViewer on your PC or laptop and install it;
- 2. Start the program and connect the PC with the gateway;
- 3. Insert password "alleantia";
- 4. Access the desktop of the gateway and follow with points 5,6,...,13.
- 1. Download and install on your PC **ULTRAVNC** from the official website: http://www.uvnc.com/downloads/ultravnc.html
- 2. Establish a direct connection point to point with a LAN cable from your PC to the gateway;
- On your PC set a static IP similar to 192.168.1.XX with two last numbers different from 29, following the procedures from n°6 to n°10 of the Section 4;
- 4. In the step n°10 do not set the "Default gateway";
- 5. Start ULTRAVNCVIEWER on your PC and insert the IP address of the gateway **192.168.1.29** and password **"alleantia"** (without quotes) for the remote access from your PC to the gateway.



In the next paragraph, we will see how to handle when the gateway is on-board machine and how to access monitoring IOT Scada Software from PC, tablet or smartphone.

4.2 Wi-Fi access

This option is available for gateways equipped with Wi-Fi and can be used in two cases:

- Local/corporate Wi-Fi network: if you want to install the gateway in places with no wired network but Wi-Fi. In this case, connecting the gateway to the network you will be able to access the software from any PC, if this PC is connected to the same Wi-Fi network.
- Connecting with your own device (laptop, tablet or smartphone) directly to the gateway, using not a local Wi-Fi network but access point function of the gateway. This function is available when the gateway has such characteristics, is correctly configured and is near enough to be able to connect.

4.2.1 Access with local/corporate Wi-Fi

Where there is a local/corporate Wi-Fi available, the gateway can be configured to connect to such Wi-Fi network. So you will be able to monitor without any additional cables.

To allow the gateway to use the Wi-Fi network, click the icon on your desktop and search for the available Wi-Fi networks.

Select the network and insert Wi-Fi security password. If you don't know the password, ask your network administrator.

The gateway will connect to the network and you will be able to access it from any PC, tablet or smartphone connected to the same Wi-Fi network.

See previous paragraph about settings of the IP address to the gateway.

Use your favourite browser (Google Chrome is recommended), type the assigned IP address in the address bar, for example

http://192.168.1.29

4.2.2 Wi-Fi Access Point Gateway

For the direct access to the system via Wi-Fi access point mode when near the gateway, using a PC, smartphone or tablet (IOS or Android), follow the steps below.

Set the gateway in Access Point mode when the operating system starts, as described in the operating system manual (NOTE: not all Windows systems allow this option). Make sure that the Access Point is not already active (after switching on the gateway and waiting for some minutes, check if IoT Scada wireless network is available, written below in bold).



Once activation of the Access Point mode, as described in Windows operating system manual, and settings have been completed (for example, it might be useful to set auto-start of access point, every time the gateway starts), the system will automatically create a wireless network to assign the SSID parameters, security password and network address to. For example:

Wi-Fi (SSID) network name: IoT-SCADA

Password: IoTSCADAwifi

Connect to this network, generated by the gateway, using PC, tablet or smartphone with the same settings when you want to connect your device to a local Wi-Fi network.

Once connected, use your favourite browser (Google Chrome is recommended) and type the default address for the gateway in the address bar:

http://10.10.0.1

CAUTION: the Wi-Fi network allows direct connection to the web software IOT SCADA and display of its monitoring interface, but not to the hardware's operating system, managing its settings and other devices, connected to the IOT SCADA via LAN.

Obviously, activation and configuration of gateway's Access Point should be done connecting a monitor, keyboard and mouse to the gateway and making settings to the operating system.

4.3 Ethernet LAN access

4.3.1 Local/corporate LAN

In the case where the gateway is inserted in a LAN network and you want to access IOT SCADA for monitoring from a PC (smartphone or tablet).

LAN Ethernet default configuration of the IOT SCADA is shown below. After inserting the gateway into the LAN network (connecting the network cable to the device's LAN port), ping the device by the IP address, shown below, to check if it responds. Then, copy this IP address in your browser's address bar to access the system.

IP address: 192.168.1.29 Subnet mask: 255.255.255.0 Gateway: 192.168.1.1 DNS 1: 208.67.222.222 DNS 2: 208.67.220.220

If the device does not respond, check whether the default IP address is correct and coherent with the LAN network (the PC should have a static IP from the same family).



Otherwise assign a correct IP.

User can assign an address to insert the gateway into the LAN network.

In this case, the network parameters and assigned IP address settings, provided by the administrator, will enable Internet access (for the software updates or upgrade by Alleantia), as well as to display the software on PC, tablet or smartphone.

This function is supported as it is web based software and remote support by Alleantia or others (e.g. maintenance company).

NOTE: IP addresses and network

The IP address of the gateway should be compatible with the addresses of other devices, you want to connect with. Also user PC should have a compatible IP in order to make settings, configure and access the software via LAN. If the user's IP address does not have compatible characteristics (same network), assign a compatible IP address (the user can reset the original IP on their PC after gateway setup).

If you do not want to modify your IP settings, you can access via remote desktop (this function is available with a direct purchase from Alleantia).

In the same way, IP of the monitored devices, connected to the gateway, should have a compatible IP address.

Then, assign IP addresses, meeting these requirements (see previous paragraphs).

For this purpose the gateway also has Dual LAN, which can be configured.

Verify that the monitored CNC or PLC, connected to the gateway, have a compatible IP address, ID and LAN port, see the document for the technical requirements for installation of "Machine 4.0", which can be downloaded from the site www.alleantia.com.

For example, in the case of CNC, the communication should be enabled in its settings, and/or specific modules of the CNC's software for communication with third parties. Refer to the manufacturers of the devices you want to connect (which can be downloaded from the site <u>www.alleantia.com</u>). Firstly, it is recommended to control Alleantia libraries to check the compatibility of protocols and the presence of drivers.



4.3.2 Direct connection to a PC (LAN cable)

This procedure requires a direct link (point to point) to a PC via an Ethernet cable, **not necessarily twisted**. The network configuration of the PC connecting to the IOT SCADA SERVER must be:

- **192.168.1.nnn** Static IP (with n between 2 and 254, with the exception of 29, which is already used by IOT SCADA SERVER)
- subnet mask 255.255.255.0

Otherwise, modify your PC configuration, following the indications in the next paragraphs.

Then, it will be possible to access the web interface of the IOT SCADA SERVER using the preferred internet browser and entering the following URL in the address bar:

http://192.168.1.29

4.4 Setting up your operating system

The gateway or PC with the installed system, as mentioned in the previous paragraphs, can be configured and installed in a corporate network, connecting it to CNC or PLC with IP addresses, etc.

4.4.1 Windows 7

Access the "Start" menu and then click on "Control panel"





Click on "Network and Internet"



Click on "Network and sharing center"



Click on "Change adapter settings"

Control Panel Home	View your basic network information	on and set up connections
Change adapter settings	N	See full map
Change advanced sharing settings	QUATTRO-PC (This computer)	Rete 4 Internet
	View your active networks	Connect or disconnect
	Rete 4 Work network	Access type: Internet Connections: U Connessione alla rete locale (LAN)
	Change your networking settings	



Select the connection to be amended, usually "Local area connection (LAN)". Click mouse right button and select "Properties".



Select "Internet protocol version 4 (TCP/IPv4)" and click on "Properties".

Networking	one alla ret	te local	e (LAN) F	roperti	es	
Connect u	sing:					
Rea	altek PCIe G	BE Fami	ly Controll	er		
This conne	ection uses t	he follov	ving items	:	Configure	
	Client for Micr Shrew Soft Li NoS Packet S NoS Packet S No Printe Stemet Proto	osoft Ne ghtweig Schedul er Sharin col Vers	etworks ht Filter er ng for Micr	osoft Ne	tworks	
	nternet Proto ink-Layer To ink-Layer To	pology I pology I	ion 4 (TC Discovery Discovery	P/IPv4) Mapper Respon	170 Driver der	
Inst	all	l	Jninstall		Properties	
Descript Transm wide an across	ion ission Contro ea network p diverse intero	l Protocol protocol connecto	ol/Interne that provid ed networ	t Protoco des com ks.	ol. The default munication	•
<u>.</u>				OK	Ca	ncel



Set the network parameters as in the figure, namely:

IP address: 192.168.1.29 Subnet mask: 255.255.255.0

eneral	
You can get IP settings assigned this capability. Otherwise, you r for the appropriate IP settings.	d automatically if your network supports need to ask your network administrator
Obtain an IP address auto	matically
• Use the following IP addres	ss:
IP address:	192.168.1.29
Subnet mask:	255.255.255.0
Default gateway:	
Obtain DNS server address	s automatically
Use the following DNS serv	ver addresses:
Preferred DNS server:	
Alternate DNS server:	• • •
Validate settings upon exi	Advanced

The addresses from the figure above can be modified by the corporate network administrator, in order to assign correct addressing and network property, web access, etc.

In case of connection to multiple networks, make sure that the assigned IP addresses are compatible.

For example, connecting the device on the office PCs network may conflict with the IP of monitored CNC/ PLC. In such situation, assign a compatible IP also to the CNC or PLC, making choices both on the CNC and the gateway and PCs that need it.

4.4.2 Windows 10

1. On the Windows OS desktop, in the bottom right corner right click on "Network and Internet" icon.





2. Select "Open Network and Sharing Center".



3. A window will open: click "Ethernet" at the top right of the window.

Network and Sharing Center		
	Panel > All Control Panel Items > Network and	Sharing Center
Control Panel Home	View your basic network informa	tion and set up connections
	View your active networks	
Change adapter settings		
Change advanced sharing	Network 2	let
ettings	Private network	HomeGroup: Ready to create
		Connections.
	Unidentified network	Access type: No network access
	Public network	Connections: 🚇 Ethernet 3
	Change your networking settings	
	Set up a new connection or netwo	ork
	Set up a new connection of netwo	DN compactions as active a souther as access as int
	Set up a broadband, dial-up, or vi	Pro connection; or set up a router or access point.
	Troubleshoot problems	
	Diagnose and repair network prob	plems, or get troubleshooting information.

4. Click "Properties".

	15	1
General		
Connection —		
IPv4 Connect	ivity:	Internet
IPv6 Connect	ivity: No r	network access
Media State:		Enabled
Duration:		05:01:05
Speed:		1.0 Gbps
Activity —		
Activity ———	Sent — 💵 –	- Received
Activity	Sent — 🙀 – 7.492.706	- Received 76.798.793
Activity Byte:	Sent — 7.492.706 Diagnose	- Received 76.798.793



5. Select "Internet Protocol Version 4 (TCP/IPv4)", then click "Properties".



6. The window with IP addresses will open. Type here the static IP address you wish to give your device.

Fill in **"Subnet mask"**, **"Default gateway"**, **"DNS"** and other fields, to allow the device to access local networks, internet, etc.

These addresses and parameters can be used, for example, to enable the system to send automatic email notifications (e.g. alarms, reports, etc.), to view the software on smartphone and tablet, or for the remote support.

neral				
ou can get IP settings assigned nis capability. Otherwise, you ne or the appropriate IP settings.	automatically if your network supports eed to ask your network administrator			Internet
Obtain an IP address autom	atically	r	e	ork access
• Use the following IP address				Enabled
IP address:	192.168.1.29		^	05:02:21
Subnet mask:	255.255.255.0			1.0 3005
Default gateway:	192.168.1.1			
Obtain DNS server address	automatically			
Use the following DNS serve	r addresses:		>	
Preferred DNS server:	8.8.8.8		is	Received
Alternate DNS server:	8.8.4.4			5.801.045
Validate settings upon exit	Advanced]	ult	
	OK Cancel			



7. Check "Use the following IP address", click Ok and close the window.

When the correct IP address is assigned to the device, it can be displayed on the client's network.

The addresses from the figure above can be modified by the corporate network administrator, in order to assign correct addressing and network property, web access, etc.

In case of connection to multiple networks, make sure that the assigned IP addresses are compatible.

For example, connecting the device on the office PCs network may conflict with the IP of monitored CNC/ PLC. In such situation, assign a compatible IP also to the CNC or PLC, making choices both on the CNC and the gateway and PCs that need it.

4.4.3 Connection to an existing LAN network

As mentioned in previous paragraphs (4.1, 4.2, 4.3 etc.), it is necessary that the default IP address of the purchased device is compatible with the devices in the existing network. If so, connect it directly to the switch/ router, or modify the gateway network configuration. Follow the procedure described in Section 5.1.

The configuration of the network to assign to IOT SCADA SERVER cannot be determined beforehand. Please, contact your system administrator to obtain the necessary parameters.

Once you have obtained the network configuration for the IOT SCADA SERVER, modify it, accessing the web interface via one of the methods described in previous paragraphs, and then connect the IOT SCADA SERVER to the existing LAN.

If the LAN is equipped with a firewall to filter access to Internet, the following TCP and UDP ports used by IOT SCADA SERVER should be opened to outbound traffic, to ensure proper operation:

- 123 TCP (NTP) to synchronise the date and time
- 53 UDP (DNS) for domain names resolution, which is essential for the connection to the remote support VPN
- 443 TCP and 1194 UDP for the connection to the VPN of Alleantia remote support
- 21 TCP (FTP) for remote backup on FTP if enabled on a server not within the LAN network
- 25 TCP (SMTP) to send email notifications if enabled by a server not within the LAN network. Some SMTP servers may use a different TCP port. In this case open the specific port to traffic

If you want to remotely view the Web interface, enable the port to inbound traffic:

• 80 TCP (HTTP)

The configuration includes the setup of IOT SCADA SERVER communication, connection to devices through different available interfaces and GUI customization.



4.5 Software installation

If the IOT SCADA Server system is already installed on a device (PC, Gateway, etc.), to access and configure it, see **paragraph 4.1**.

Otherwise, if you need to install the software and license, follow these steps:

- Install the software;
- Activate license.

4.5.1 Provided files

The IOT SCADA is supplied as .exe file to install on Windows systems. It creates web server that you can access via browser at http://localhost (80 port can be modified during installation).

As regards the license, the provider sends a file with extension .lic that enables and activates the IOT SCADA.

4.5.2 Installation procedure

Copy the .exe file to the Windows system where you want to install the IOT SCADA and launch it.

Select the installation language.



Click "Next".

Specify an installation type:

- Standard: the files will be installed with default options (in "**Program files (x86)**" folder on Windows); the webserver port will be **:80** on the localhost.

- Custom: you can choose the installation directory and the webserver port.

Alleantia



Two following windows appear only if custom installation is selected.







Click on "Next".

мат Setup		_		×
Ready to Install				
Setup is now ready to begin installing IoT SC	ADA on your com	puter.		
InstallBuilder	< Back	Next >	Car	ncel

In the end two icons will be created on the Desktop:



Alleantia

To activate the webserver, double-click on "Start IoT SCADA". To open the browser and access web, click "IoT SCADA web interface". These commands can be found in Windows start menu.



You can set the auto start of the webserver:

- Windows 7 and Windows 8.1 - copying the "Start IoT SCADA" shortcut in Windows "Start-up" folder.

- Windows 10:
- 1. Open Task Scheduler, create new task.

Task Scheduler File Action View He Connect to And	lp other Computer			– – ×
Create Basic Tai Create Basic Tai Create Task Import Task Display All Run Enable All Task: AT Service Acco Refresh Help	ning Tasks s History punt Configuration Sta Last 24 Summary: 0 tot	ary (Last refree heduler e Task to create ge asks that uter will ally at the hours tal - 0 running, 0	• • • • • • • • • • • • • • • • • • •	Actions Task Scheduler (Local) Connect to Another Computer Create Basic Task Create Task Create Task Display All Running Tasks Enable All Tasks History AT Service Account Configuration View Refresh
Creates a customized task fo	Last refreshed at 2	17/06/2017 17:43:	→ 36 R	



2.	Setup as in t	the figure l	below: c	reate a name	, check I	Run with	highest privileg	es, choose	Windows	10 from
th	e dropdown li	ist.								

General Trigg	gers Actions Cond	itions Settings	
Name:	IoT SCADA Start		
Location:	/		
Author:	DESKTOP-KSP8EGR	loT SCADA Server	
Description:			
Security opt	ons		
When runni	ng the task, use the f	ollowing user account:	
DESKTOP-K	SP8EGR\IoT SCADA S	erver	Change User or Group
Run only	when user is logged	on	
O Run whe	ther user is logged or ot store password. Th	or not ne task will only have access to l	ocal computer resources.
Run with	highest privileges		
	Configure for:	Windows 10	~
Hidden			

3. Go to Trigger tab. In the section "Begin the task" select At startup.

	Begin the task: On a schedule	~
General Trigge When you crea	Settings On a schedule At log on Image: One time Daily Daily Weekly Monthly Monthly	Synchronize across time zones
	Advanced settings Delay task for up to (random delay): 1 hour Repeat task every: 1 hour Stop all running tasks at end of repetition duration	for a duration of: 1 day
New	□ Stop task if it runs longer than: 3 days □ Expire: 30/06/2018 □ Enabled	Synchronize across time zones



4. Go to Actions tab. Create new action.

Browse the file C:\Program Files (x86)\Alleantia\IoTSCADA\yajsw\bat\runConsoleW.bat

Unate Date				
Create Tasl	k		New Action	>
General Trig When you	ggers Actions create a task, yo	Condi ou must tails	You must specify what action this task will perform. Action: Start a program Settings	~
Action			Program/script: "C:\Program Files (x86)\Alleantia\IoTSCADA\yajsw\bat\rt Add arguments (optional): Start in (optional):	
New	Edit		OK Cance	1

5. In the Conditions tab, in Power section, uncheck Start the task only if the computer is on AC power.

eneral	Triggers	Actions	Conditions	Settings		
Specify run if a Idle	the condi	tions that, ion specifi	along with the	ne trigger, dete t true.	rmine whether the task shou	ld run. The task will not
Star	t the task o	only if the	computer is i	dle f <mark>or:</mark>	10 minutes	~
Wait for idle for:					1 hour	~
🖂 S	top if the o	computer	ceases to be i	dle		
	Restart if	the idle s	tate resumes			
Power	-					
Star	t the task o	only if the	computer is a	on AC power		
⊻ S	top if the o	computer	switches to b	attery power		
Wak	the com	puter to r	un this task			
Netwo	rk —	6 H -	1		7.11	
Star	t only if th	e followin	g network co	nnection is ava	ilable:	
Any	connectio	n				~



6. In the Settings tab, uncheck Stop the task if it runs longer than:.

eneral	Triggers	Actions	Conditions	Settings			
Specify	additional	<mark>l settin</mark> gs t	hat affect the	e behavior of the t	ask.		
	ow task to	be run on	demand				
Rur	n task as so	oon <mark>as pos</mark>	sible after a s	cheduled start is	missed		
] ft	he task fail:	s, restart e	very:		1 minute $ \sim $		
Att	empt to re	start up to	t.		3 times		
Sto	p the task	if <mark>it ru</mark> ns le	onger than:		3 days \sim		
☐ If the second sec	he running	task does	not end whe	en requested, forc	e it to stop		
ft	ne task is n	ot schedu	led to run ag	ain, del <mark>e</mark> te it after		30 days	×
f the ta	ask is alread	dy running	g, <mark>then the f</mark> o	llowing rule appli	es:		
Do not	start a nev	v instance		~			

To stop/restart the active webserver, you can use "IoT SCADA" icon in Windows Task Bar.



4.5.3 Update procedure

If the .exe file has been launched on the system where there is already an installed copy, it will be updated.



Alleantia

Click "OK", then "Next".



You will be asked to load new device mapping files, if in doubt, select "No".

of Setup		-		Х
Device catalogue				
Mapping files have all informations needed to get alarms. Loading new files contained in this installa already presents in existing installation and any cu	data from d tion program stomization	evices and th n will overwri will be lost.	eir defau ite mapp	ilt ings
Load new device mapping files?				
⊖ Yes				
No				
nstallBuilder				

Click "Next" to start the update procedure.

4.5.4 License activation

Together with the product the activation code, consisting of xxxx numbers, is provided.

To activate the license, login to http://cloud.alleantia.com/login/login.zul





Sign in with email or social networks. You will receive an email to confirm the registration.

After you log in, the next screen will appear.

	Download & install the license	Search your device from catalogue	Plug it on USB, Serial or LAN	Monitor it!
Turn your PC int object to internet objects, i	to the web interface that conr t. Catalog with hundreds of rr including your Arduino proje faxBox download Version 2.4.2 (~137 MB)	nects every aady to use cts.		
for Wind Manu Max	ows XP, Vista, 7, 8, Server 20	nooting		
Activation co	ode		•	Go to online demo
DOLLAR STREET, STREET, ST		_		



Insert your activation code in **"IOT SCADA license activation"** field. File .lic will be automatically sent to your email for system activation.

4.5.5 Uninstallation process

To uninstall the program and delete the data, run "Uninstall IoT SCADA" from the Windows start menu.



CAUTION All data will be deleted without the possibility to recover



In the end of uninstallation, desktop icons and shortcuts from Windows menu will be removed.



5 Configuration

Access the "Configuration" section from the main navigation bar and enter the following credentials:

Username: admin Password: webloggerSU

A screen will appear as in Figure 1:

Communication	Installation	Customization	Cloud services	10 Information
TCP / IP configuration	Devices configuration	Logos and title	E-mail and SMS	Device catalogue
TCP / IP Test	Devices, measures and rights setup	Synoptics measures configuration	Cropbox	License management
COM and Ethernet configuration	General configuration	Custom alarms	Microsoft OneDrive	Informations
Modbus Gateway		Events	Microsoft IoT Hub	Logs
MQTT brokers configuration		Synoptics configuration	Y ← Yammer	
			FTP remote backup	
			Microsoft SQL Server	
			MOTT Service	

Figure 1. System configuration

5.1 Communication

5.1.1 TCP/IP Configuration

If the IOT SCADA SERVER is connected to a LAN network with other devices, its default settings could cause a conflict. If so, change the settings in the "Communication" -> "TCP / IP Configuration" section. A screen as shown in Figure 2 will be displayed:

Documents Favorites	Configuration							
Configurable network interfaces Installed network interfaces								
Realtek PCIe GBE Family Controller								
Microsoft Wi-Fi Direct Virtual Adapter #2								
rt	rt Documents Favorites							



Alleantia

5 Configuration

Synoptics Devices Alarms	Alarm History	Report	Do	cuments	Favorites	Configuration		
TCP / IP configuration								
Cancel								
onfigurable network interfaces			Insta	alled netwo	ork interface	s		
			Θ	Realtek F	PCIe GBE Fa	mily Controller		
				State:	State: Active interface			
				IP Addres	ss: 1	92.168.1.47		
				Net mask	: 2	55.255.255.0		
				MAC add	ress: 0	0:0B:AB:9E:68:F5		
			Ξ	Microsof	crosoft Wi-Fi Direct Virtual Adapter #2			
				State:	A	ctive interface		
				IP Addre	ss: 1	92.168.137.1		
				Net mask	: 2	55.255.255.0		
				MAC add	ress: 0	2:03:8C:4A:65:33		

Figure 3. Network card data and setup of Ethernet and Wi-Fi

To modify the device's IP addresses on Windows 10 OS, see **paragraph 4.4.3**. For other Windows versions refer to **paragraphs 4.4.2** and **4.4.1**.

If there is a DHCP server in the LAN network to which the IOT SCADA SERVER is connected, you can check the **"Obtain an IP address automatically"** and click **Ok**.

Internet Pro	tocol Version 4 (TCP/I	Pv4) Prop	ert	ies			_			×
internet Pro		ir v4) riop	cit	ics.						~
General										
You can ge this capabi for the app	et IP settings assigned a lity. Otherwise, you ne propriate IP settings.	automatica ed to ask y	ly i our	f yo ne	tw	net ork	ad	ork supp ministra	oorts ator	
Obtai	n an IP address automa	atically								
🔘 Use t	he following IP address									
IP addre	ess:									
Subnet	mask:									
Default	gateway:									
Obtai	n DNS server address a	automatical	ly							
🔘 Use t	he following DNS server	r addresse:	s: -							
Preferre	ed DNS server:	8		8		8		8		
Alternat	e DNS server:	8		8		4	•	4		
🗌 Valid	ate settings upon exit						P	dvanc	ed	
			Г	18	OK	:		(Cancel	

The IOT SCADA SERVER will lease the IP configuration directly from the DHCP server.

If the DHCP server is not available or you prefer to set the IP address manually, check the **"Use the following IP address"** and enter all the **"IP Parameters"** including the IP addresses of the DNS servers that may coincide with that of the gateway in simple network configuration.



5 Configuration

The right area **"Network Interface"** displays the current network configuration for both the wired interface (LAN) as well as the Alleantia VPN (Virtual Private Network) through which the IOT SCADA SERVER communicates with any centralised server (optional service) and the remote support, where available.



If the network to which you are connected has internet access, refer to paragraph 5.1.3 to verify the correctness of the LAN configuration set.

5.1.2 Connection to an existing Wi-Fi network

If there is a Wi-Fi, you can easily connect the gateway in order to monitor without laying additional cables.

To connect to Wi-Fi, click the desktop icon and search for available networks.

Select the network and insert the password.

The device will connect to the network and it will be possible to query it from any device, connected to the same Wi-Fi.

To connect to the device, open the browser and insert the static IP, assigned to the gateway, for example

http://192.168.1.29

Refer to previous paragraphs for the assigning IP to the gateway.

5.1.3 Internet communication test

G TCP / IP Test										
Host Reachabi	Host Reachability									
Host Name	Host	Host Por	Host State							
Google DNS	8.8.8.8			🔮 Test						
Google	www.google.com	80		🔮 Test						
VPN Alleantia	vpn.alleantia.com	443		😔 Test						
Test web		80		🔮 Test						
Modbus Test		502		🔮 Test						
😌 Test all										
Ping				💽 Test						

Figure 4. Internet communication test

In the "Communication" - > "TCP / IP test" section you can test the reachability of some default hosts and others of your choice.

Alleantia
By pressing the **"Test"** button next to each host or **"Test all"**, the reachability of these hosts can be verified and the result of the test will be shown in the **"Host state"** column. In the event that the host cannot be reached, check the configuration of the network, the network wiring or contact your network administrator.

5.1.4 Port and communication parameters configuration

To connect devices or machinery to the device's serial ports with installed IOT SCADA SERVER, make the following settings.

The default configuration of the ports is carried out in the section "Communication" -> "COM and Ethernet configuration" and is illustrated in Figure 5.

Syr	noptics Devic	es Alarms	Alarm His	tory Report	Documents	Favorites	Configura				
G	COM and E	thernet conf	figuration								
50	ancel										
, s	can serial ports]									
Com	munication port	s parameters									
Ξ	COM1 Deactivate										
	Timeout (ms)	3000		Poll pause (ms)	10000						
	Retries	1		Baud rate (bps)	9600	•					
	Data bits	8	•	Parity	None	•					
	Stop Bits	1	۲	Flow control	None	•					
Ð	COM2				De	eactivate					
Ŧ	Ethernet	hernet									

Figure 5. Communication ports configuration

First, click Scan serial ports.

The system will automatically find the serial connections of the gateway.

When connecting a device to one of the gateway's ports (PLC, energy meters, CNC, etc.), setup the port parameters.

Setup every port (for example, baud rate, parity, stop bit, data bit) according to the characteristics of the connected devices, referring to their installation manuals. The Ethernet port is associated to the RJ45 connector of the IOT SCADA SERVER.

To create the COM ports click **"Scan serial ports" (NOTE**: the converters should be physically connected to the IOT SCADA SERVER). When scanning is complete, new found ports are displayed on green background. Remember to save new configuration before leaving the page.

The system provides for the polling of all devices on each communication line, inserting a pause between one cycle and the next equal to the **"Poll pause (ms)"** value (can be set in web interface).



In the event that the polling of a device is not successful within the "Timeout (ms)", the system performs a number of attempts equal to "Retries" before highlighting a communication error and moving on to the next device.

In the event of communication problems, increase this value by up to a few seconds in order to avoid underperforming electronic systems being overloaded by repeated polling.

The non-functioning device will be called up in each scan cycle. Click **"Save"** to apply changes when the configuration is complete.

5.1.5 Modbus Gateway

The Modbus gateway feature makes the system data accessible to external software via the Modbus protocol enabling, for example, the integration with SCADA systems, regardless of the protocol used by devices to which the IOT SCADA SERVER is connected upstream.



Figure 6. Modbus Gateway

To create automatically the Modbus map with information and download it in Excel format, including the configured information set, click the **Download Modbus map (Excel. XLSX)** button, which is enabled when the gateway is enabled.

5.1.5.1 Rules of automatic mapping

The mapping of the measures of the devices on the Modbus gateway follows the following rules:

• For each IO SCADA SERVER serial port where devices are connected and configured, a TCP Modbus slave is created on a different TCP port:

o COM1 -> TCP 502 port o COM2 -> TCP 503 port o COM3 -> TCP 504 port o COM4 -> TCP 505 port o COM5 -> TCP 506 port o Ethernet -> TCP 565 port

- Within each Modbus slave the devices keep the address configured on the physical device. If, however, this address is greater than 247, the maximum permitted by the Modbus protocol, it will be arbitrarily reassigned.
- The Modbus devices maintain the same identical mapping of the original device, both in respect of the areas as well as the addresses, data types etc. Byte and word swaps will not be considered.
- Non-Modbus devices will show the Boolean types in the coil area and numeric types both in Holding as well as in Input. The number will be in 2-word float format. The register address will be calculated arbitrarily.

Alleantia

- The bits within a word of the gateway are in Big-Endian format (More Significant Byte First) and the word in data types in 32 or 64 bits are in Little Endian format (Less Significant Word First).
- If a physical device goes offline, it will not respond when contacted through the gateway and the request will time out.
- If the value of a register containing a measure not read by IOT SCADA SERVER (see **paragraph 5.2.3**), is requested, the gateway responds with a default value of 0 for numeric data types and false for Boolean
- If the value of a non-existent Modbus register is requested, the gateway responds with the exception code "2", that is "Illegal Data Address".
- The gateway does not support writing, so if these are carried out by an external Modbus master, the Modbus register values are immediately restored to the value prior to the writing.

5.1.6 MQTT brokers configuration

In **"MQTT brokers configuration"** section, enter the connection parameters of MQTT brokers, where the data from MQTT Service will be forwarded (see Section 5.4.7).

Click "Add Broker", then insert necessary parameters to establish a connection with the broker.

G	MQTT Brokers				
	Cancel Save				
Ð	Broker name: Alleantia Bro	oker			Delete
	IP address or hostname*:	127.0.0.1	Port (default 1883)*:	1883	
	Username:	italtel	Password:	••••	
	Test Co	onnection	Add	Certificate	

Figure 7. Brokers MQTT configuration

First, create a name for the selected broker. This will appear in the list of the selectable brokers, as MQTT service is being configured.

Subsequently, enter the IP address and the Port, through which the data exchange between broker and IoT SCADA Server application will take place.

IoT SCADA application supports brokers either with no authentication, or the ones which require a normal type of authentication (Username and Password), or SSI type (Secure Sockets Layer). In the latter case, click "Add certificate" to upload a digital certificate that will allow MQTT service to authenticate and communicate with the broker.

When the configuration is done, click "Test Connection" to test the reachability of the broker. If the test succeeds, you will receive the message "Successful connection".

Click "Save" to apply changes.



5.2 Installation

5.2.1 System devices connection and configuration

This section describes how to add and remove new devices connected to the IOT SCADA SERVER via the RS485 serial interface or via Ethernet.

The examples below are valid for any kind of device or machinery you want to connect: PLC, inverter, CNC, remote modules with digital and analog input and outputs, etc. in the library or created new drivers.

5.2.1.1 Adding new devices

Any device from which you want the IOT SCADA SERVER to collect measures must be inserted in the section **Installation -> Devices configuration**.



Figure 8. System devices configuration

To add a device, press the **"Add"** button. A popup window appears as in Figure 8, showing device drivers loaded in the IOT SCADA SERVER catalogue. To add new devices please refer to Section 5.5.1



Add device to	system	Communication Port	ID II	P Address	TCP/UDP Port	×
Filter devices:	socomed	*				
Supplier	÷	Model	÷	Version	÷	
Socomec		Countis E43		Post 01/2009		
Socomec		Countis ECi2				
Socomec		DIRIS A10		Post 01/2009	×	
Socomec		DIRIS A40		Post 01/2009	×	
Socomec		ITY-TW020B				
Socomec		SUNSYS B15			×	
Socomec		SUNSYS B20			8	
Socomec		Sunsys IFB				
Socomec		SUNSYS PRO 18K				
Socomec		SUNSYS PRO 24K				-
Select a device	e from the list					
					< 🗸 Ok	ncel

Figure 9. List of supported devices

The list contains all of the devices supported by IOT SCADA SERVER and can be sorted and filtered by manufacturer, model and version in order to facilitate the search.

To add a device to the system configuration, select it, set the number of identical devices present and press the "Add" button. The number of devices selected will be inserted in the main page and will appear with a green background to indicate that they have just been added:

Devices Alarms Alarm History F	teport Documents Favorites	Configuration							🕧 License	🕧 License 🛛 Logo	🕖 License 🛛 🔙 Logou
G Devices configuration											
🔊 Cancel 📔 Save											
🐈 Add							\delta Trouble	shooting			
Device	Description	Communication Port	ID	IP Address	TCP/UDP Port						
🖉 Inverter											
Socomec - SUNSYS STATION P03 (66kW)	Inverter 1	COM1	1 🗘		502	Encap	× 1	Delete			
Socomec - SUNSYS STATION P03 (66kW)	Inverter 2	COM1	2 🗘		502	Encap	× 🗎	Delete			
Other											
Alleantia - IoT Server 10×		IoT SCADA	2			Encap	9				
Alleantia - IoT Server 10x (Configuration)		IoT SCADA	1 🗘			Encap	7				



Each new device shall be assigned a unique name to be recognised in the user interface (e.g. West Inverter 1), a unique numeric identifier to allow addressing on the RS232/485 bus or Ethernet (the ID in the case of the Modbus protocol) and the communication port to poll. For the list of existing ports or to add new ones using converters, refer to **Section 5.1**.

The device parameters can be inserted directly on the line. The "IP Address" and "TCP / UDP Port" fields will also be completed for the devices with Ethernet interface which, in the case of Modbus TCP / IP, is generally "502".

Repeat the operation for all devices to add.

CAUTION:

The identifier must be assigned to the first device (e.g. Inverter) according to the procedure described in the device's manual, and then copied in the configuration section of the IOT SCADA SERVER.



The devices with "<disconnected>" communication port are not "polled" as they are not associated with any communication line (Ethernet or serial). If a device is out of service its communication port can be set to "<disconnected>" to avoid any communication errors and speed up the reading of data from the system without changing the configuration.

Once the system configuration is complete, press the **"Save"** button at the top to make the changes effective. After a few moments the IOT SCADA SERVER will begin to poll the devices and an icon will appear next to each representing the communication status with the device itself.

If the configuration and wiring are correct the icon will be green: 🐙, while if the device is not reachable the



Devices Alarms Alarm History Report	t Documents Favorites Configura	tion					
G Devices configuration							
🔊 Cancel 🔚 Save							
🛉 Add							Stroubleshooting
Device	Description	Communication Port	ID	IP Address	TCP/UDP Port		
Inverter							
Socomec - SUNSYS STATION P03 (66kW)	Inverter 1	COM1 •	1 🗘			Encap	💻 🔀 👘 Delete
Socomec - SUNSYS STATION P03 (66kW)	Inverter 2	COM1 T	2			Encap	💻 🔀 👘 Delete

Figure 11. System configured

The measures collected by the devices will appear in the **Devices** section in the main menu, see **Section 6.2.1**. Each device provides a number of measures that can be appropriately chosen by the user to facilitate the readability of the synoptics, as explained in **Section 5.2.3**.

5.2.1.2 Removing a device

If a device is no longer present in the system it can be removed from the configuration by pressing the "**Delete**" button at the end of device line. The device will disappear from the list and the change will become effective after pressing the "**Save**" button.

CAUTION:

Deleting a device will cause the loss of all of its recorded data. If you no longer wish to poll the device but keep the collected data, set its communication port to "<disconnected>".







5.2.1.3 Installation support manuals

During both the device selection, as shown in Figure 7, as well as in the device list as shown in Figure 8, two icons can appear next to each device that allow to download and view the help documentation during installation:



User manual



Quick installation guide

The **User Manual** is the same as that provided by the device manufacturer configured in IOT SCADA SERVER, while the **Quick Start Guide** is a concise guide created by Alleantia to help you configure the device and IOT SCADA SERVER.

In the event of communication problems between the IOT SCADA SERVER devices, refer to the troubleshooting guide that can be downloaded by pressing the button:



5.2.3 Devices measures setup

Devices Alarms Alarm History	Report	Docur	ments	Favorites	Configuration			🥡 License	🕜 Manual 👌	Logou	t 🚺 📑
G Devices measures setup											
🔊 Cancel 📔 Save											
Measures and Devices		«	Cate	gory: Inver	ter						
🗆 Inverter			Devi	ce: Inverter	1						ONLINE
Inverter 1			Model	SUNSYS STAT	ION PD3				at	11/3/14 5	:18:10 PM
⊞⊡Inverter 2		2	inouci.		10111100						
			Filter m	easure:							
						Measure		Value	8	1	
			🛛 Sy	stem							^
			A	C Mains Cos p	ohi			0	1		
		e.		C Mains Input	Frequency			0 Hz			
				C Mains R-S \	/oltage			0 V			
				C Mains S-T V	/oltage			0 V			
			A	C Mains T-R V	/oltage			0 V			
				C side lightnin	g protection			false	\$	1	
				DC Roards 120	C communication t	fault		falca		1	•

Figure 13. Devices measures setup



Each device supported by IOT SCADA SERVER carries all information about any measure provided by the device. In order to avoid showing too many measures and slow down the scanning of the devices, only the measures actually considered useful for the monitoring are read when the device is added.

To change the default configuration, access the **Installation** -> **Devices measures setup** section; there is a tree menu on the left where all devices that the IOT SCADA SERVER is polling can be seen, organised by category. Once you have selected a device, all available measures will appear on the right.

Checking the boxes at the beginning of each line enables the reading of a single measure. Unchecking disable reading check boxes in the column with the symbol, it is possible to enable or disable measure logging in the IOT SCADA SERVER.

CAUTION:

Graphs can only be generated for the measures with enabled logging

Nel caso in cui la misura rappresenti un allarme, sarà presente anche una casella di spunta nella colonna con il simbolo *d*, spuntandola l'IOT SCADA SERVER visualizzerà un allarme quando la misura assumerà un valore all'interno della soglia impostata oppure sarà un allarme automaticamente generato (PLC, CNC, etc). Il sistema provvederà all'invio di mail in automatico per notifica allarme ai destinatari impostati. È possibile modificare il nome della misura direttamente nella casella di testo, per modificare invece le altre impostazioni, se presenti, è possibile aprire un popup dedicato cliccando sul pulsante *d*.

Advanced measure configuration										
Range Offs	set Scaling									
Min:		kWh								
Max:		kWh								
		🛛 🖉 Ok 🖉 🧐 Cancel								

Figure 14. Measure range configuration popup window

By specifying a minimum and maximum value in the popup window "**Range**" tab it will be possible to make the screen reading of the measure easier (see, for example, the horizontal bars of some measures in Figure 16).

Álleantia

5.2.3.1 Measures offset

Cange Onset Ocami	<u>, </u>	
Configure offset	ble offset 💷	
Value read from device:	0 kWh	
Lodged value:	0 kWh	

Figure 15. Measure offset configuration popup window

The measure offset feature is very useful in the case of network analysers that measure the energy produced or consumed. These devices are in fact often installed in parallel to an exchange meter and begin counting from 0 kWh, while the meter has a higher value. To facilitate the reading it can be aligned with that of the existing meter "correcting" the value displayed and recorded.

In the advanced configuration popup window "Offset" tab (see Figure 16) a value can be set in the "Aligned offset" box. The IOT SCADA SERVER will calculate the difference between the actual value and that desired, and this will be applied to the measures read by the device from that moment on. The values of the measures so aligned will appear in italic as a reminder that these values are not the real ones read but those purposefully modified by the user.

5.2.3.2 Measures scaling

_(Configu	re scaling	Enable	scaling 🔲	
١	Value re	ead from d	1.98 kW		
1	Logged	value:		1.98 kW	
1	Transfo	rmation ra	tio:		

Figure 16. Measures scaling configuration popup window

The measure scaling feature is very useful in the case of fiscal meters that measure energy through external current transformer. The measured value is a fraction of the real value, i.e. 1 / K, with K the transformation ratio of the current transformer.

In the advanced configuration popup window **"Scaling"** tab (see Figure 16) a value can be set in the **"Transformation ratio"**. The IOT SCADA SERVER will multiply the value aligned (see Section 5.2.3.1) for the transformation ratio set.

The values of the measures scaled in this manner will appear in italic as a reminder that these are not real values but those purposefully modified by the user.



5.2.4 General settings

Devices	Alarms	Alarm History	Report	Docume
Ger Ger	neral con	figuration		
Data sampl	ing period			
Sample eve	ry	300 second	s 📔 Save	2
Date/time s	et			
1/17/1	7 [10:33 AM ᅌ	📔 Save]
Reset confi	guration			
		Reset		
System reb	oot			
		Reboot		

Figure 17. Data sampling configuration

Data sampling will affect the accuracy of the measure as it will increase or decrease the number of samples available to be analysed. A too high number of samples could excessively slow the processing.

On the same page you can set the system date and time: **Date-Time Set, System Reset** and **System Reboot**. It's even possible to reset IOT SCADA SERVER configuration by clicking on the **Reset** button, in this case:

CAUTION: In case of reset all data and configurations of devices, alarms and notifications WILL BE LOST without possibility to recover

5.2.5 Password change

To change the access password to the configuration section, go to the **Installation** -> **Password Change** section and enter the old password (the initial installation default password is webloggerSU, as specified in **Section 5**). Select the new password and re-enter to confirm the selection. When finished, press the **Save** button.

Devices	Alarms	Alarm History	Report	Documents	Favorites	Configuratio
G Pas	sword cl	nange				
Password mu	ist have len	gth between 5 an	d 15 charao	ters, and can in	clued letters a	and numbers
Change pas	sword					
Old passwor	rd					
New passwo	ord					
Confirm new	password					
				📔 Sa	ave	

Figure 18. Password change

CAUTION:

For security reasons it is strongly recommended to change the IOT SCADA SERVER admin password immediately

Alleantia

5.3 Customization

5.3.1 Logos and title

Devices Alarm	s Alarm History	Report	Documents	Favorites	Configuration	
G Logos an	d title					
Title	anto				Save	
						Max size: 2MB
Upper left logo						Upper right logo

Figure 19. System logos and title customization

In the Customization -> Logos and title section the IOT SCADA SERVER interface can be customized:

- in the Title section the upper title present in all the pages of the interface can be set,
- in the Logo section 2 logos can be entered, one on the upper right and one on the upper left. These are also always present in all the pages GUI.

5.3.2 Custom measures

In addition to the measures read by the devices, you can define custom measures (such as, for example, sums of other measures): clicking the Add button in the Configuration > Synoptic measures configuration -> Custom measures section (Figure 19) a popup menu will open that allows you to enter the name of the new measure and select the existing ones which, when summed, will contribute to its value (Figure 20).

Syn	optics	Devices	Alarms Alarm History Report Documents Heic	lenhain Part Programs	Favorites	Configuration
9	Syr	noptics me	asures configuration			
usto	om me	asures				
	Abil	Global Id	Measure			1
Ð	I	G_TV101	test_custom_messaure	Modify	Delete	
Ð	2	G_TV100	test_power	Modify	Delete	-
_			Add			

Figure 20. Custom measures





Figure 21. Custom measures popup window

For example, if the system is divided into two levels, you can create the custom measures "East Power" and "West Power" and select the power of the inverters associated to each level for each one. Please note that it is only possible to choose measures with the same measure units. Therefore, after selecting the first one, an automatic filter will remove all those that have different units of measures from the list on the right.

5.3.3 Custom alarms

Devices	Alarms	Alarm History	Report	Documents	Favorites	Configuration
G Custo	om alarr	ns				
🔊 Cancel	금 Save]				
📥 Add						
3		Name			Delay	
				No custom a	larm	

Figure 22. Custom alarms start screen

By accessing the **Customization** -> **Custom alarms** section it is possible to define new and more complex alarm conditions, in addition to those that are already set in the device. For example, if you want to create a new alarm condition that notifies an anomalous situation of low production on a solar inverter. Pressing the **Add** button will open a popup menu that allows you to configure the new alarm in detail:

Alleantia

New alarm	
- Alarm name	
- Alarm notification text	
- Alarm condition	
Aan conduon	
alarm if sum of values of	
is v	
enabling condition: not 📃	
Time condition	
Enable alarm condition	
From: To:	
Enable weekly condition	
✓ Mon ♥ Tue ♥ Wed ♥ Thu ♥ Fri ♥ Sat ♥ Sun	
	Ok Cancel

Figure 23. New custom alarm configuration

In the popup window insert the name for the alarm and text description that will be used during the notification

to the user. Below, in the Alarm Condition section proceed to the selection of all the measures that you intend

to monitor by pressing the ... button. In this case we select only the power of inverter 1. Following the selection, the list of measures selected will appear next to the button. The check boxes enable the control types to be performed on the measure value. In this case the alarm will be triggered if the power of the inverter 1 falls below a certain threshold:



New alarm	
- Alarm name]
Low Production (Inverter 1)	
Alarm notification text	
Low Production on Inverter 1	
Alarm condition	
Inverter 1 - System - Inverters Active Power	
alarm if sum of values of	
0 kW is less than ▼ 3 kW	
enabling condition: not	
Time condition	
Enable alarm condition 🖉	
From: 11:00 AM 🗘 To: 2:00 PM 🗘	
	🖋 Ok 🄄 🔊 Cancel

Figure 24. Low production alarm

A time range for the control can be specified. In this case, to avoid the control perform during the night when the solar inverter is not active. To save and activate the alarm, press **Ok** and then click on **Save** in the **Custom alarms** screen.

Once this alarm is entered, it is displayed on the main screen where it can be enabled or disabled using the checkbox and it is possible to set the delay time before which the alarm is to be considered as true (for example, 5 minutes), thus limiting the effect of transients:

-	Name	Delay	
	Low Production (Inverter 1)	5 minutes	🖋 Modify 👔 Delete 🔋 Duplicate

Figure 23 - New alarm

It is also possible to enable an alarm in relation to another: for example, using a pyranometer the alarm previously created can be reinforced by connecting the value of irradiation and then testing the low production only at times when it is expected to be high. To do this, simply create a new alarm to act as an "enabling condition", an alarm that shall not be notified and, therefore, without the relevant box being checked:

4	Name	Delay	
	Low Production (Inverter 1)	5 minutes	📝 Modify 👔 Delete 🖺 Duplicate
	High Irradiance	0 minutes	📝 Modify 👔 Delete 🖺 Duplicate

Figure 25. Multiple custom alarms



High Irradiance	
- Alarm name	License
High Irradiance	
Alarm notification text	
High Irradiance	
Alarm condition	
Solarimeter - Current irradiation level	
alarm if sum of values of	···]
is greater then	
enabling condition: not	····
Time condition	
Enable alarm condition	
From: 🗘 To:	
	🛷 Ok 🏼 🥱 Cancel

Figure 26. High irradiance condition

The alarm condition is unusual in this case (and is, in fact, not notified), but allows the user to avoid the application of a time condition: a "low irradiance" condition without a time slot would be triggered every night. Once the alarm condition has been saved, change the low production alarm to link it to that of the irradiation thanks to the *"enabling condition"*:

Low Production (Inverter 1)	
Alarm name	
Low Production (Inverter 1)	
- Alarm notification text	
Low Production on Inverter 1	
Alayee aan diilan	
Ararm condition	
alarm if sum of values of	
0 kW is less than v 3 kW	
High Irradiance	1
enabling condition: not	
Time condition	
Enable alarm condition 🕑	
From: 11:00 AM 🗘 To: 2:00 PM 🔇	
V OK Cance	el

Figure 27. Change low production alarm enabling condition



At this point the time condition can be removed from this alarm as well given that there will not be high irradiation during the night and the low production alarm will not be enabled.



It is useful to create an alarm that acts as an enabling condition for many others. If there are 10 inverters it would then be possible to insert the "High irradiance" condition only once and use it in the 10 "Low production" alarms.

5.3.4 Events

In the section **Customisation > Events** it is possible to define one or more events.

The set *Events* monitor the happening of a given set condition on a single variable - or on a combination of variables - and in the same moment "to photograph" the value acquired by any variable, configured in the application.

The occurrence of an event will not be shown on the application's interface, unlike *Custom alarms* (see Section 5.3.2), nevertheless the software keeps track of it in its archiving database, and offers the possibility to transfer the data, associated to them, through the cloud services *Microsoft IoT Hub, SQL, MQTT Service*.

Click "Add" to create new event and to open the configuration window (see Figure 28).

Synoptics Devices Alarms	Alarm I	History	Report	Documents	Heidenhain Part Programs	Favorites	Configuration	Ucense	🚮 Logou	t 🚺 !		
Devices and system measures	*	C	ategory: C evice: Sigr	NC ma Compact 3						ONLIN	E	
System variables	_	M(3)	odel: Heidenhai	n - iTNC530 (Sigma C	ompact							
CNC	Ŧ	Filte	r measure:	ns	No.						_	
🗄 Sigma Compact 3			1	Measure	Va	alue	Min	Range	Max			
Operating	8	0	Active tool			8	1			8	-	
Consumo macchina			Execution E	Block Nr		67,30	D			8		
			Execution Mode			Automatic				8		
		4	Execution N	Name Active Progr	am Compact\MECS	TNC:\Programm SPE\01_Sgrossa	ii tu					
		:	Execution N	Name Selected Pro	gram Compact\MECS	TNC:\Programm SPE\01_Sgrossa	ii tu			8		
i Idle Compact/MECSPE\01_		fals	e			🦪 💾						
			Operating			true	e			8	-	
			Override: F	eed		47.5	5			8		
Override: Rapid		apid		47.5	5			8				
	Override: Speed 109.19 Program Status Started			Override: S	peed		109.1	9			B	
		d			B							
			S Actual			2,98	1			8		

Figure 28. Events: selection of the chosen variable to set the event condition



Click **Ok**, then the system will select the chosen variable, entering the corresponding *Globalld* inside *condition bar* and *Globalld*, *Description* and *Total value* of the variable chosen inside **Variables summary** field (see Figure 29).

vent			
-Event nam	e		
Machine op	perating		
Event cond (+) x AND (Add v Condition	dition	Condition v	Expression result: true
- Variables s	summary		1
Globalld	Description	Actual value	
G_4_71	SigmaCompact - Operating	true	
]
- Variables to Select at le	o observe	dition trigger	
Globalld	Description	Actual value	
Add v	variable		Vk Cancel

Figure 29. Events: Condition bar (red) and Variables summary window (blue).

Then, set the condition that determines the happening of the event. Select "equal to" condition from the dropdown menu (see Figure 30).

In the field next to it, enter the value 1 that corresponds to the boolean value *True*. On the right, a text line reports *currently acquired value* of the event as it has just been configured.

In the conditions of the example, the event will be verified at the moment of its creation (*Condition value: True*) (see Figure 31).



Machine operating				
Event condition —				
(+ -				
		Condition		
		G_4_71		
AND OR N	OT			
Add variable				
Condition				
-		Con		
augi ta				
different from				
ess than	ption	Actual valu		
equal to different from less than greater than less or equal than	ption	Actual va		



vent - Event name			
Machine operating			
Event condition	Condition		
AND OR NOT Add variable	G_4_71	Expre	ession result: true
Variables summary			
Globalld Description		Actual value	
G_4_71 SigmaCompact -	Operating	true	
Variables to observe	nake a snanshot on condition	trigger	

Figure 31. Defined event condition and currently acquired value of the event (red)

Alleantia

Finally, it is **compulsory** to specify a **snapshot variable**: the value of this variable will be registered, if the set condition of the event is verified. Click "Add variable" to enter the **snapshot variables** into "Variables to **observe**" section.

A pop-up window shows up, select the variable to set the event's condition (see Figure 30). It is possible to select more than one **snapshot variable**.

For example, it is interesting to know which program is running at the moment of the actual machine operation. To get this information select the variable **Execution Name active Program** as **snapshot variable**, in this way when the machine starts production, the event will report the program's name running in the machine. Chosen snapshot variable will be displayed in "Variables to observe" section, with *GlobalID*, *Description*, *Actual value* (see Figure 32).

Globalld	Description	Actual value	
3_4_53	SigmaCompact - Execution Name Active Program	TNC:\Program Compact\MEC	
Add v	variable 🔀		

Figure 32. Summary of variables to observe

In this example, the event's condition was defined as a single variable, it is possible to combine more variables in one condition, using the editor on the configuration screen. The editor has traditional mathematical operators (+,-,x,/), logical operators **AND**, **OR**, and **NOT**, and rounded brackets, so, everything to combine the variables according to the standards of *Regular Expression (Regex)* (see Figure 33).

Click and to scroll through the **Condition bar**, selecting the elements of the **Regex** (selection with the blue background). To delete any element of the expression, select it and click

() + -	Condition			
) x /	(G_4_51 *	G_4_71)	and	G_4_78
AND OR NOT Add variable	(*)	Exp	ression result	:
Condition	c	ondition value:		





The created event will be displayed on the main Events panel *(Configuration > Events)*. Enable or disable the event checking the box, click **Modify** to modify it, or click **Delete** to delete it (see Figure 34).

S	ynoptics Devices	Alarms	Alarm History	Report	Documents	Heidenhain Part Programs	Favori
G	Events						
5	Cancel 📔 Save						
+	Add						
Abil		N	ame				
	Machine Operating				1	Modify 📄 👚 Delete	

Figure 34. Events: the created event is displayed on the main Events panel

In the end, click Save to apply the changes.

5.3.5 Synoptics configuration



Figure 35. Creation of system synoptics

In the **Customization** -> **Synoptics configuration** section you can create custom synoptics with a personalised background and measures.

To create a new synoptic, click on the <u>+</u> tab. A popup window will appear as in Figure 35, to choose the screen sizes most commonly used for tablets and monitors, the background and the title.

New synoptic properti	es	x
Size	HD 16:9 (1280x720)	▼
Show background		
Background image	safe_image.jpg	📄 Select 🛛 🙀 Upload
Title	Distribution	_
		🕜 Ok 🎦 🔊 Cancel

Figure 37.Image catalogue

The IOT SCADA SERVER contains a catalogue of reusable images. In order to load an image in the catalogue, press the **Upload** button and choose the file from the hard drive of your PC/tablet. This will be loaded into the IOT SCADA SERVER and will be available for the creation of more synoptics. To reuse, press the **Select** button and choose from the catalogue images, as in Figure 37:

1	Ima	e catalog 🛛 🛛 🗙
D	0	
D	0	
	∢	
		V Ok Cancel

The image is uploaded in the original size and automatically resized depending on the size chosen for the synoptic.

At the end of the changes the empty synoptic will be displayed, as shown in Figure 30:





Figure 38. Empty synoptic

To change the properties of the synoptic double click on the corresponding tab or on the background. The popup window in Figure 39 will appear again.

To delete the synoptic, click on the "X" in the upper right corner of the corresponding tab.

From now on it is possible to add the displays that will show the values of the measures in the system, which are of 2 types: numeric and visual (lamp) displays. The numeric display shows just numeric values, while the lamp display shows Boolean values.

These two displays are shown on the left side of the page. To add one, simply drag it on to the synoptic into the position where you want it to be shown. Once released, a popup window will appear as in Figure 38 and Figure 39 to change its properties.

Display properties	
Measure:	
Upper title:	
Lower title:	
Background color:	White
Lamp ON color:	Red
Lamp OFF color:	Green
	V Ok Cancel

Figure 39. Lamp type display properties



Display properties	×
Measure:	
Upper title:	
Lower title:	
Background color:	White
	🛷 Ok 🏼 崎 Cancel

Figure 40. Numeric type display properties

The measure to be shown, the upper (first line) and lower (second row) title, the colours of the background and of any lamp displays can be chosen.

Once the parameters have been entered, the synoptic will appear for example as shown in Figure 41:

G Synoptics configuration								
Synoptics configuration								
Cancel 🔄 Save								
Lamp display Distribution × +								
WXYZ Show bit status switching lamp color Numeric display Image: Color Animations Power 0 kW 0 kW								

Figure 41. Synoptic with display

To subsequently change the properties of the display, double click on the displays themselves. The popup window in Figure 40 and Figure 41 will appear again, from which it is possible to delete the properties.

In the **Animations** section the synoptic in the home page can be automatically changed by selecting the check box **Enable synoptic rotation** and defining an interval in seconds.

Once defined the synoptic will appear in **Synoptic** window of the graphic interface (see Figure 41 at the top left).



5.4 Interface and Cloud services

5.4.1 E-mail and SMS notifications

The IOT SCADA SERVER can automatically send e-mail and SMS notifications in the following cases:

- an alarm condition occurs
- notification of the backup occurring (see Sections 5.4.2 and 5.4.3)

To take advantage of these features, Cloud Services -> E-mail and SMS configuration must be enabled.

Devices Alarms	Alarm History	Report	Documents	Favorites	Configurat	tion			
G E-mail and	SMS configurat	ion							
🔊 Cancel 📔 Sav	e								
Alarm notification ena	ablement								
Alarm notifications									
Backup and report notifications	Enable	e backup a	nd report notific	ations via e-m	ail				
E-mail notification pa	rameters					G	SM modem configur	ation	
Mail server configur	ation ———					Г	– SMS notification parameters –		
SMTP server:							Modem communica	tion port:	<pre><disconnected> ▼</disconnected></pre>
Port:							PIN code (opt.):		
Use SSL:							SMS center phone r	number (opt.):	
Username:						Destination numbers:			
Password:							(1 every line)		
From e-mail address:									
L							Modem status:	Disconnected	
Alarm notifications r	ecipients						Signal:	Disconnected	
To e-mail addresse	s [.]						-	20	Undete E Testand

Figure 42. Alarm and data logging configuration

After having ticked at least one checkbox to enable notifications, the email notification in the **E-mail notification** parameters and SMS notification in the **GSM modem configuration** can be configured.

For the e-mail notification the details of your SMTP server for sending email and that of the recipient must be included. At the end a test email can be sent to verify the correctness of the settings entered by pressing the corresponding **Send test mail** button.

For the SMS notification a GSM modem must first be connected to one of the IOT SCADA SERVER, serial ports, selecting from among those supported. The serial port must be properly configured according to the GSM modem manufacturer's instructions, see **Section 5.1.1**. The parameters of the recipients must subsequently be entered.

If the settings are correct, following the application of the changes, the IOT SCADA SERVER will connect to the modem and **Modem Status: Connected** will appear in the **Modem Test** box; then check the GSM signal strength in the appropriate **Signal** indicator and evaluate the displacement of the GSM antenna or the purchase of a magnified one if the signal is low, otherwise an SMS alarm notification may not be received.

You can send a test SMS to check the correctness of the settings entered by pressing the corresponding **Send** test mail button.



5.4.2 Dropbox connection

An existing Dropbox account can be indicated as an additional destination for the backup files. This account can also be used to upload the documents generated by IOT SCADA SERVER on the Dropbox by pressing

the send to Dropbox buttons in the application (for example, in energy reports). Before connecting a Dropbox account make sure internet connection is available on the device from which you are configuring.

Devices Alarms Alarm Hist	ory Report	Documents	Favorites	Configura				
G Dropbox								
Cancel 🔄 Save								
Dropbox link								
No user connected 📾 Connection								
Real Verify								
Remote backup service								
Enable Dropbox remote backup 📃								
Dropbox destination folder *								
Send a test file	Send							

Figure 43. Dropbox account configuration

Go to **Configuration -> Cloud Services -> Dropbox** and press the **Connection...** button to start the connection procedure of the IOT SCADA SERVER to a Dropbox account. The popup window of Figure 44 will open.

Connection to Dropbox folder
Request Dropbox authorization code
► Request code
Enter authorization code
Ok Sancel

Figure 44. Authorization code request



Press the **Request code** button to access your Dropbox account, if necessary by entering your email and password (Figure 45).

Try Dropbox Business	Second Se
	Sign in or create an account G Sign in with Google or or Email Password Remember me Sign in
	Get Dropbox on your desktop — download now

Figure 45. Dropbox account access

On the subsequent screen, click **Allow** to allow the IOT SCADA SERVER access to your Dropbox folder (Figure 46).



Figure 46. Authorization

Enter the code shown in Figure 47 in the start popup window (Figure 48).



Enter this code into Alleantia IOT SCADA SERVER to finish the process.

dlu6C4DU0jEAAAAAAAAJeB4n-WJK1_06Mzcd3XkgR4s

Figure 47. Authorization code

Comgaration	
Connection to Dropbox folder	
Request Dropbox authorization code	
▶ Request code	
Enter authorization code	
dlu6C4DU0jEAAAAAAAAJeB4n-WJK1_06Mzcd3XkgR4s	
Ok Cancel]

Figure 48. Authorization code shown in IOT SCADA SERVER



Press **Ok** to end the procedure. If successful, the account appears correctly connected (Figure 49).



Figure 49. Dropbox account connected

At this point the **Send to Dropbox** buttons of IOT SCADA SERVER can already be used to send documents on Dropbox. To disconnect the account in the future, simply press the **Disconnect** button.

If you want to enable the sending of backups to Dropbox press **Enable Dropbox remote backup** (Figure 50) and choose a destination folder for the files by clicking on the button "...". To test the backup feature, send a test file to the specified folder by pressing the **Send** button. When finished, press the **Save** button to save the configuration.

Remote backup service							
Enable Dropbox remote backup 🖉							
Dropbox destination folder *	/Backups						
Send a test file	Send Send						

Figure 50. Backup parameters

The backup files sent to Dropbox are not related to those of any FTP backup: in other words, <u>complete</u> backups of IOT SCADA SERVER will be present on both Dropbox as well as FTP.

Alleantia

5.4.3 OneDrive account

An existing OneDrive for Business account can be indicated as an additional destination for the backup files. This account can also be used to upload the documents generated by IOT SCADA SERVER on the Microsoft cloud. Before connecting OneDrive for Business account **make sure internet connection is available on the device from which you are configuring.**



Figure 51. OneDrive for Business account

CAUTION:

it is possible to synchronize OneDrive Business account only

Press the **Connect Account** button. The popup window will open with a request to insert email and password of the account to be synchronized. If successful, the account appears correctly connected. The IOT SCADA SERVER will synchronize with the OneDrive for Business cloud for the backup saving.

At this point the **Send** button of IOT SCADA SERVER can already be used to send documents on OneDrive for Business. To disconnect the account in the future, simply press the **Disconnect** button.

If you want to enable the sending of backups to OneDrive for Business, press **Enable OneDrive remote backup** and choose a destination folder for the files by clicking on the button "...". To test the backup feature, send a test file to the specified folder by pressing the **Send** button. When finished, press the **Save** button to save the configuration.





5.4.4 FTP Backup

The remote backup function to FTP provides for the creation and sending of daily backups of IOT SCADA SERVER data and the configuration on an FTP server in order to ensure recovery in case of hardware failure of the internal hard disk.

To use this function an FTP server must be available on which to make the transfer, as well as all the parameters necessary for its access, which are to be entered in the **Configuration -> Cloud Services -> FTP remote backup** section:

Synoptics Devices Alarr	ns Alarm History Report Documents
G FTP remote backup	
Cancel	
FTP Backup	
Remote FTP	backup enabled
FTP server name:	
FTP port:	21
Username:	
Password:	
	🕞 Backup test

Figure 53. FTP remote backup configuration

A test file can be sent to check the correctness of the settings entered by pressing the corresponding **Backup** test button.

Alleantia

5.4.4.1 Details of the transferred files

IOT SCADA will send 3 files every night called: backup_date_hour.zip backup_date_hour.zip.md5 backup_date_hour.zip.sig in which date represents the date, and hour the UTC time in which the backup was made such as, for example, "backup_23062017_0144.zip".

The file with the zip extension contains the CSV file with the IOT SCADA data and an encrypted file with its configuration.

CAUTION

The backup performed by this IOT SCADA SERVER feature is incremental. To rebuild the system in the event of failure all the files transferred over time are required. The remote backup can be interrupted at any time by disabling it in the dedicated configuration section. If subsequently re-enabled, it will resume the backup of your data from where it was last interrupted.

The file with the md5 extension contains a signature with the MD5 algorithm to verify the correct transfer of the file. The file with the .sig extension contains a RSA signature to verify that the file was actually generated by an Alleantia product and has not been manipulated to alter the content.



The remote backup function is incremental in respect to the previous backup. If the previous backup is of the previous night, the zip will contain the data of a single day. If the previous backup does not exist, or it is the first run, the zip file will contain ALL the data of the system starting from the commissioning of the plant.

5.4.5 Connection with Microsoft SQL Server

It is possible to configure a database MySQL or Microsoft SQL Server as destination of all data, events and alarms, taken from the IOT SCADA.

First, select the type of database to connect to IoT SCADA application, from the dropdown menu in the configuration window (Database type).



	Overview	Alarms	Alarm History	Report	Documents	Favorites	Configura
a sq	L Service						
Cancel	Save						
QL Servic	e						
Sql_1	+						
				_			
Databas	e type:		SQL Server	-			
Databas	e address:		SQL Server MySql				
Databas	e port:		1433				
Databas	e name:		ALLEANTIA				
Tables s	uffix:						
Usernan	ne:		marcotest				
Passwor	rd:		•••••				
					11		
	1						
Conne	ction test						
Conne	ction test						
Conne	ction test ad script to cre	ate tables o	on server			Downloa	ad script
Conne Downloa Copy de	ction test ad script to cre vices and vari	ate tables c ables config	on server guration on server			Downloa	ad script
Conne Downloa Copy de Send da	ad script to cre vices and vari tas to the serv	ate tables c ables confi <u>c</u> er every	on server guration on server		0	Downloa Cc	ad script py m 0 💠 s
Conne Downloa Copy de Send da	ad script to cre vices and vari itas to the serv d only changed	ate tables c ables config er every 1 variables i	on server guration on server in the time interva	I	0	Downloa Cc	ad script py m 0 💠 s
Conne Downloa Copy de Send da Send Enat	ad script to cre vices and vari itas to the serv d only changed ble SQL servic	ate tables o ables config er every 1 variables i e	on server guration on server in the time interva	I	0	Downloa Cc h 1 0	ad script py m 0 💠 s

Figure 54. "SQL Service" configuration interface

Then, on MySQL or SQL Server database, create again a database with compatible structure with IoT SCADA application. Click **"Download script"** to download the script of creation of a new database on SQL platform, that contains the data from Alleantia application.

After having entered the connection parameters to the database (IP address, Port, Database name, Tables suffix, Username, Password), check the connection by clicking **"Connection test"**. the message "Connection success" will be shown.

Click "Copy", the configurations of variables and devices, configured in IoT SCADA application will be forwarded to SQL database.

The time interval for data forwarding can be set independently of the logging time of the variables. Set it in h, m and s fields.

Alleantia

Check "Send only changed variables in the time interval" box to forward only the variables, which did not changed their value during the fixed forwarding time, to SQL platform.

In addition, a line will appear, indicate there the number of periods (1 period=forwarding time), after this number of periods the variables will be forwarded to the database, even if their value remained the same as the last entry.

After that, the service is completely configured, so check "Enable SQL service" box to enable the service.

Click **Save** to apply the changes.

IoT SCADA software also sends registered data to more SQL platforms at the same time. The maximum number of SQL platforms to forward data depends on the purchased license.

If this number is exceeded, the message as in the figure below will be shown.



Figure 55. Error message shown when the number of available SQL platforms is exceeded

To add a new database to forward data, click "+" tab. To delete it, click "Delete" in right corner below.



5.4.6 Connection to Azure IoT Hub

In Microsoft Azure, after creating IoT Hub, get the connection string.



Figure 56. Microsoft Azure

Insert the string into the box in configuration panel. Then press **Create IoT Hub Identity** button to register the device in IoT Hub.

G Accou					1 di ontoo	oomgaration				
-	G Account Azure									
Azure service										
To start sending messages to Azure cloud you must create a device identity on IoT Hub. To do this, paste the connection string taken from your personal IoT Hub and push "Create IoT Hub Identity" button										
Connection string to IoT Hub HostName=AlleantiaHub.azure- devices.net:SharedAccessKeyName=iothubowner:SharedAccessKey=D8r0ObhnknYePM84 XWkxh92gm9zxTRQkFco2n6mSg3U=;										
Create IoT Hub Identity Delete IoT Hub Identity DeviceID: IOTSPI216060799										
Start IoT Hub se	ervice 🗌									



Alleantia

If the registration was successful, Device ID will be displayed next to the button.



Figure 58. Account Azure

Now you can set time interval between sending next telemetry message and mske other settings. It will send messages only for variables/alarms with read/write/alarm rights (Figure 59).

Devices Alarms Alarm History Report Documents Favorites Configuration								
G Devices, measures and rights se	etup							
Cancel 🔚 Save								
Measures and Devices	» چ	Category: Photovoltaic inverter Device: Fanue Moder Fanue-Fanue(Mater) Filter measure: Filter			ON (last answ	JLINE at erat)		
Energy meter Exa Seneca	÷.	Measure	Value	Azure R W A	8 🤞			
Seneca S504C	÷	Posizione asse C Posizione asse B			•			
-Test	÷.	Posizione asse X						
	Ť	Poszuone asse Y Poszuone asse Y Poszuone asse Z			 ✓ 			
Fanuc Test VV	≧ . ∰							

Figure 59. Devices, measures and rights setup



You can set these rights in **Devices**, measures and rights setup, Synoptics measures configuration and **Custom alarms** sections.

Write permission can be enabled only for measures which can be modified from outside. The alarms' permissions (A) can be enabled only for measures defined as an alarm in Xmod driver.

Finally, check the checkbox **Start IoT Hub service** to activate. Depending on the selected options, estimated messages sent per day will be shown (Figure 60).

Devi	ces	Alarms	Alarm History	Report	Documents	Favorites	Configuratio	1	
G	Syr	noptics m	neasures confi	guration					
Custo	m me	asures						I	
abil							Azure		
+	V	MisuraPers	3					nodify 🔪	💼 Delete
+	V	Test XVV							💼 Delete
					🕂 Add]			

Figure 60. Synoptics measures configuration

D	evices Alarms Alarm History Report I	Documents	Favorites	Configuration	
G	Custom alarms				
5	Cancel 📔 Save				
+	Add			-	
1	Name	Delay	Azure		
	sss	0 minut	es 📄	🥜 Modify 🥤	🖥 Delete 📔 Duplicate
	boh	0 minut	es 🔲	Modify 🥤	Delete Duplicate



Figure 61. Custom alarms

The service uses MQTT v3.1.1., to run this protocol the 8883 port or web socket of 443 port are needed. Make sure that these ports are open.

5.4.7 MQTT Service

5.4.7.1 Getting started

Through *MQTT Service*, IoT SCADA application can publish data collected from different devices and sensors on a listening MQTT broker.

The exchange through MQTT protocol happens according to *publish/subscribe* type, indicating with *publisher* a device that can publish the data on a specific broker, and *subscriber* a device that can "subscribe" to a broker to receive different messages from the publishers. The communications happen on various channels, in order to be grouped based on the type of exchanged information *(alarms, events).*

Each communication channel among these takes *topic* as name.


Go to **Configuration > MQTT service**.

Select the broker to forward data. From the dropdown menu, next to "Select Broker" line, select the broker among the ones configured in Communication > MQTT brokers configuration (see Section 5.1.6).

Synoptics Devices Alarms Alarm	History Report	Documents	Heidenhain Part Programs	Favorites	Configuration
A MQTT service					
Cancel Save					
MQTT service					
Broker_1 +					
Select Broker					
	Alleantia broker		L		
Telemetry	IoT SCADA bro	ker		Select var	riables
Publish alarms messages on topic:	IOTSPI218032	2301/alarms		Select custo	m alarms
Publish events messages on topic:	IOTSPI218032	2301/events		Select er	vents
Listen for input messages on topic:	IOTSPI218032	2301/command	ls		
Select delay time before send messages	0 🗘 h 1 🔇	m 0 🗘 s			
Enable MQTT service					
Disconnection management					
Stream datas without saving unsent met	ssages on disk				
Enable backup of unsent messages on	disk				
Select max space occupation on disk fo	r saving unsent mes	sages 512 3	MB		
Messages format					
Add device alias in the json message Send messages in format					
◯ JTS (Json Time Series)	netry				
Send only changed variables in the time	interval (Impossible	to use advanced	d studies)		

Figure 62. MQTT service: selection of the broker to forward data

IoT SCADA application contains four topics. *Telemetry, alarms, events* are used by MQTT Service to publish messages of the configured broker (*publisher*). While the application listens on *commands* topic, waiting for requests from the broker (*subscriber*).

Forwarded data and topics functions description:

- devSn/telemetry: measures sampled by IoT SCADA application are sent to this topic;
- devSn/alarms: in case of alarm, MQTT service will forward the relevant data regarding the alarm to the topic;
- devSn/events: all the data related to the events are forwarded to events topic;



devSn/commands: unlike the others, commands topic is subscriber topic type. It means that IoT SCADA application listens on the topic in order to find when messages from the broker arrive. For example, there is the possibility to ask the application the information on the software version, devices configuration and associated variables, publishing the request on commands topic. Based on the received request, the application will publish the response on telemetry topic (see Section 3 of "MQTT Protocol User Manual").

To customise the structure of the topic's name, enter a *personalTag* in the text field next to the standard name (see Figure 63).

Synoptics Devices Alarms	Alarm History Report	Documents	Heidenhain Part Program	s Favorites	Configuration
G MQTT service					
Cancel III Save					
Broker_1 +					
-					
Select Broker	IoT SCADA broker	•			
Telemetry	IOTSPI218032301/te	elemetry	Alleantia	Select va	riables
Publish alarms messages on topic:	IOTSPI218032301/a	larms	active	Select custo	om alarms
Publish events messages on topic:	IOTSPI218032301/e	vents	active	Select e	vents
Listen for input messages on topic:	IOTSPI218032301/c	ommands	config		
Select delay time before send message	ges 0 🗘 h 1 💈	🗘 m 0 💠 s			
Enable MQTT service					
Disconnection management					
Stream datas without saving unse	ent messages on disk				
Enable backup of unsent messag	es on dis <mark>k</mark>				
Select max space occupation on e	disk for saving unsent mes	sages 512	♦ MB		
Messages format					
Add device alias in the json messi Send messages in format	age				



For example, nelle condizioni della Figura 63, the topics will be labelled in the following way:

IOTSPI218032301/telemetry/Alleantia IOTSPI218032301/alarms/active IOTSPI218032301/events/active IOTSPI218032301/commands/config

Alleantia

The topic's name will have the following structure (e.g. general structure of *telemetry* topic):

devSn/telemetry/personalTag

5.4.7.2 Configuration of the information to send on MQTT Broker

After the initial configuration described before, select which information to forward to each topic.

Click **Select variables** on the right of the text field. A window will show up, select the variables to forward to *telemetry* topic (see Figure 64).

ID	Description 56 Ingresso temperatura 2			Read					
ID .		Actual	Min	Max	Avg	StdDev	white	Alami	
G_1_56	Ingresso temperatura 2								
G_5_90	Y axis position								
G_5_91	Z axis position								
G_2_16	Ingresso digitale 4, frequenza massima								
G_2_17	Ingresso digitale 5, frequenza massima								
G_1_46	Ingresso analogico 2, valore digitale								
G_2_14	Ingresso digitale 2, frequenza massima								
G_1_47	Ingresso temperatura 1	Ø							
G_2_15	Ingresso digitale 3, frequenza massima								
G_2_18	Ingresso digitale 6, frequenza massima								
G_1_103	Ingresso TA 1, Irms								
G_2_12	Uscita digitale 2, modalità								
G_5_86	X motor axis rpm								
G_2_13	Ingresso digitale 1, frequenza massima								
G 5 87	Y motor axis rpm								

Figure 64. Right selection for MQTT service

In this window, there is a list of the variables of every device configured in IoT SCADA application. The first column (*ID*) shows *Global_Id:* identification numbers of all variables, configured in the application.

Description column shows the variable description as it was configured in Xmod driver of the monitored device.

To enable MQTT broker, check the boxes in *Read* column, which is divided into 5 sections:

- Actual: selecting the boxes in *Actual* column, MQTT service will be given the permit to forward the *instantaneous value of* the variable to the broker;
- Min: forward minimum value acquired by the variable in time interval between forwards;
- Max: forward maximum value acquired by the variable;



- Avg: calculate *medium value* of the time interval between forwards;
- StdDev: calculate *standard deviation* of the variable.

WARNING:

Min, Max, Avg and StdDev are calculated on a quantity of measuring points equal to the number of statistical samples in the time interval. Therefore, in the case where the number of statistical samples is set to 1, these quantities will return the current value.

Check the box in *Write* column to give the possibility to MQTT service to set the variable's value, if it is of *read/ write* type; note how the box is not enabled for variables of type readOnly.

Finally, if an alarm is active on an *alarmed* variable, *Alarm* column allows to forward the information related to the current alarm on the topic *telemetry*. The box will be active only for the variables with a *default alarm* associated, that is a preconfigured alarm when generating the Xmod driver, which therefore does not need to be configured from the Custom Alarms section (see Section 5.3.3).

Click **Select Custom Alarms** and **Select Events** to enable MQTT service to forward the information related to the alarms and the events configured on the IoT SCADA application.

Right	ts selection for service MQTT	1
7	Machine in alarm	1
8	Machine in Emergency	
9	Battery Low Alarm	

Figure 65. MQTT Service: window for selecting the alarms to be sent to the broker

In each case a window will open, showing the list of alarms or events configured in the application. Just check the box related to the chosen events or alarms to send the associated information to the chosen MQTT broker.

The left column contains *alarmld* and *eventId* of each alarm or event.

5.4.7.2 Final configuration

Once the initial configurations have been completed and the permissions to send the information to MQTT broker have been set, it is necessary to complete the configuration of MQTT service by customizing the time the messages are sent, the behaviour of the application in case of an absent connection and the format of the forwarded messages.

It is possible to *set the time interval for forwarding to the broker* through the three windows *h*, *m* and *s* next to the dedicated line. MQTT Service will wait for the time set here before sending an additional message to the broker.

If there is no connection, the application can behave in two different ways. The user can choose from two modes (see Figure 66):

Alleantia

- Stream data without saving unsent messages on disk: in this case, when there is no internet connection, and, therefore, it will not be possible to reach the broker, all the data recorded up to that moment will not be forwarded to the broker and it will not be possible to restore them when the connection is restored (data will be saved only on the application's internal DB);
- Enable backup of unsent messages on disk: in this case, the data will be temporarily saved on the
 physical memory (hardware), when the connection is restored, the communication with MQTT broker
 will be re-established. In the window below it is possible to specify the maximum amount of memory (in
 Megabytes) that the data recorded in the absence of a connection can occupy. Once the set threshold
 has been reached, the data will be lost and the application will behave with the same logic as described
 in the previous point.

sconnection management		
Stream datas without saving unsent messages on disk		
Enable backup of unsent messages on disk		
Select max space occupation on disk for saving unsent messages	512	\$ MB



Finally, it is possible to customize the messages that will be forwarded to the broker, such as the quantity of parameters and the syntax.

Checking the box **"Add device alias in the json message"** will include the device alias among the components of the forwarded message.

It is possible to choose from two messages formats: "Normal telemetry" and "JTS" (see "MQTT Protocol User Manual" for more details).

Selecting JTS format for the forwarded messages, it will be possible to set only the number of *samplings in the time interval* (see Figure 67). This is equal to setting the number of points, that the application will calculate with *Min, Max, Avg* and *StdDev* (see Section 5.4.7.2).

Messa	ages f	ormat	
Ad Send r	d devi nessa	ice alia Iges in	s in the json message format
● JT	S (Jso	o <mark>n T</mark> ime	e Series) 🔘 Normal telemetry
Make	1	\$	samplings in the time interval

Figure 67. Avaliable settings when Json Time Series message format is selected



If the user chose **Normal telemetry** format message, besides the number of **samplings in the time interval**, it is possible to make other settings, customising the forwarded messages to the broker (see Figure 68).

Checking the box "Send only changed variables in the time interval", only the variables whose value is changed after a time equal to the *time interval* will be forwarded. When you check the box, you will see an extra line from which the user can set the periods' number, after which the variables will be forwarded send in any case, even if their value is not changed (see Figure 68). A period is equivalent to the *time interval between forward to the broker*.

It is specified that if this option is operative, the *additional statistical values*, set in the process of configuration of information to forward on broker, will not be calculated (see Section 5.4.7.2).

Messages form	at
Add device	alias in the json message
Send messages	in format
JTS (Json T	ïme Series) 🖲 Normal telemetry
Send only c	hanged variables in the time interval (Impossible to use advanced studies)
Send all me	essages regardless of the change every 10 I periods
Make 1	statistical samplings in the time interval
-	

Figure 68. Normal telemetry settings

Further to what said until now, the messages on the broker can be personalized sending all the information available on the variables, checking the dedicated box *(forward a json that include any information about variables).* The json structure will remain the same, but it will contain a bigger number of tags than before, since the number of forwarded information is greater (See par 2.1 *MQTT Protocol User Manual*).

At this point, the configurations are completed, so you only have to check the box **"Enable MQTT service"** to activate the service. Finally, click **"Save"**.

It is possible to configure a number of MQTT brokers same as those available in license. To know the number of brokers to add to the application IoT SCADA Server, go to **Configuration > License management** (See par. 5.5.2) and check the value shown in the line "**Number of configurable MQTT Services**" (See Figure 64).

Alleantia

Synoptics Devices Alarms Ala	Irm History Report	Documents Heid
G License management		
Activation code		
3fbafa731-b45f-3cf6-9985-b2c26a7aa13a		
e opioad		
Installed license information		
Feature	Available in license	Currently in use
Modbus Gateway	Yes	Yes
Modbus write	Yes	
Locked device catalogue	No	
Energy pack	No	
	No	
Machine pack	INU	
Machine pack REST API	Yes	
Machine pack REST API REST API write	Yes	
Machine pack REST API REST API write Yammer module	Yes Yes Yes	
Machine pack REST API REST API write Yammer module Azure IoT Hub service	Yes Yes Yes Yes	
Machine pack REST API REST API write Yammer module Azure IoT Hub service SQL Server service	Yes Yes Yes Yes Yes	
Machine pack REST API REST API write Yammer module Azure IoT Hub service SQL Server service Number of configurable MQTT services	Yes Yes Yes Yes Yes 3	1
Machine pack REST API REST API write Yammer module Azure IoT Hub service SQL Server service Number of configurable MQTT services Number di connected devices available	Yes Yes Yes Yes 3 7	1 4
Machine pack REST API REST API write Yammer module Azure IoT Hub service SQL Server service Number of configurable MQTT services Number di connected devices available Number of measures read	Yes Yes Yes Yes Yes 3 7 350	1 4 128
Machine pack REST API REST API write Yammer module Azure IoT Hub service SQL Server service Number of configurable MQTT services Number of connected devices available Number of measures read Max history days	Yes Yes Yes Yes Yes 3 7 350 60	1 4 128 60

Figure 69. Number of configurable MQTT services

In the column "Available in license", the number of brokers currently in use are shown.

If you have reached the maximum number of MQTT services available in license, you will see the pop-up error message, as shown in Figure 65.



Figure 70. Pop-up error message: maximum number of MQTT services, available in license, have been reached



5.5 Information

In Section Information you can find information about the system and change such its data as licence and device catalogue.

5.5.1 Device catalogue

Every IOT SCADA SERVER system is released with database of connected devices with default configurations. This may contain not all the devices of the Alleantia's Library of Things, which is continuously updated and is available here http://cloud.alleantia.com/info/products.zul. Therefore you can download one or more .xmod files of devices configuration and upload it in the used IOT SCADA SERVER system, using the functionality of this section. The user can, in the same way, insert in the system ad hoc configured devices (e.g. PLC) using the Alleantia's tool

http://cloud.alleantia.com/xmod/convert.zul which creates an .xmod file for every device.

In section Information -> Device catalogue a window with the existing library of devices will open.

Synoptics	Devices	Alarms	Alarm History	Report	Documents	Favorites	Configuration		
G Device catalogue									
🕂 Add									
Filter devices:			*						
Supplier	÷	Model					Version	÷	
ABB		A-41							
ABB		A-42							
ABB		A-43							
ABB		A-44							
ABB		ACS 800							
ABB		B-21							
ABB		B-23							
ABB		B-24							
ABB		DMTME-I-	485						
ABB		Fidas 24 E	EL3000						
ABB		REF601 C	EI 0-16						
Albatech		APL 15							
Albatech		APL 20							
Alleantia		Alleantia E	Bus for Arduino						
Allen Bradley		Power Mo	nitor 500						-

Figure 71. Device catalogue

Pressing the **Add** button a popup window will open, that allows you to select different types of files: .xmod files of device's library to connect, and .pdf files for device's user manual.

Alleantia

Devices Ala	arms Alarm History Report Docu	iments Favorites	Configuration	
	catalogue		Add device	×
Device	catalogue		- Device description	
🐈 Add 👔 D			Upload No file uploaded	
Filter devices:	×		User Manual	
Supplier	Model		Unload No file unloaded	
ABB	A-41		No lie uploaded	
ABB	A-42			
ABB	A-43		Installation Guide	
ABB	A-44		Unload No file unloaded	
ABB	ACS 800			
ABB	B-21			
ABB	B-23		se Inse	rt Cancel
ABB	B-24			
ABB	DMTME-I-485			
ABB	Fidas 24 EL3000			
ABB	REF601 CEI 0-16			
ABB	REF615		IEC	
Albatech	APL 15			
Albatech	APL 20			
Alleantia	Alleantia Bus for Arduino		*	

Figure 72. Add device

Pressing the **Upload** button it will be possible to navigate the file system and select the file you need. For the .xmod file, the system recognizes and verifies correctness of the file and will permit or not to insert it in the IOT SCADA SERVER system's database.

5.5.2 License management

In this section you can verify the license key or insert a new license (e.g. of updating or upgrading) and insert the related activation key provided by Alleantia or by its vendor.

In section **Information -> License management** a popup window will open with the activation key, possibility to upload a new license and the installed license characteristics, and options:



Devices	Alarms	Alarm History	Report	Documents	Favorites	Configuratio
G Lice	nse mar	agement				
Activation co	ode					
44120f54f-63	bf-3fb1-8a	15f-e1be85ec2dc	5			
🕞 Upload]					
	,					
Installed lice	neo inforn	astion				
Installed lice	nse inforn	nation			1	
Installed licer	nse inforn	nation	Avail	able in license	Currently i	in use
Installed licer Feature Modbus Gate	nse inforn eway	nation	Avail	able in license	Currently i	in use
Installed licer Feature Modbus Gate Modbus write	nse inforn eway e	nation	Avail Yes Yes	able in license	Currently i No	in use
Installed licer Feature Modbus Gate Modbus write Locked device	nse inforn eway e ce catalogi	nation	Avail Yes Yes No	able in license	Currently i No	in use
Installed licer Feature Modbus Gate Modbus write Locked devic Energy pack	nse inforn eway e ce catalogi	nation	Avail Yes Yes No No	able in license	Currently i No	in use
Installed licer Feature Modbus Gate Modbus write Locked devic Energy pack Machine pac	nse inforn eway e ce catalogi k	nation	Avail Yes Yes No No No	able in license	Currently i No	in use
Installed licer Feature Modbus Gate Modbus write Locked devic Energy pack Machine pac REST API	nse inforn eway e ce catalogi k	nation ue	Avail Yes Yes No No No No	able in license	Currently i No	in use

Figure 56- License management

5.5.3 Informations

In this section the version of installed software license is provided.

Devices Ala	arms Alarm History	Report	Documents	Favorites	Configuration
	ations				
Software inform	ation				
Version:	3.4.2				

Figure 57 - Informations

5.5.4 Logs

It is possible to generate audit log in different sections of software, useful to debug problems in different levels: communication protocols, devices, user interfaces.

Go to section Information -> Logs a page for the logs configuration will open.

Devices Alarms	Alarm History	Report	Documents	Favorites	Configuration		
G Logs							
File: 🔹 🗖 Lock 👶 Download							
Logging level: Apply							
Select a log fle from d	rop-down menu	50 1					

Figure 58 - Logs creation

3 logs files can be generated: "Logging engine", "Graphic interface" e "Protocol traffic". The levels of logging that can be selected are: ERROR, WARN and DEBUG. It is possible to download generated logs files, clicking the **Download** button.



6.1 Synoptics

Figure 59 shows a complete synopsis of a system in which the 2 synoptics have been created in section **Configuration -> Customization -> Synoptics configuration (**see Section 5.3**)**



Figure 59 - Home page with synoptics

This screen is automatically displayed on the HDMI output of the IOT SCADA SERVER.

The **Synoptics** tab is not shown if there are no configured synoptics, in which case the IOT SCADA SERVER home page becomes that of the **Devices** tab.



If a device in the system is in alarm, the "Alarms" text in the respective tab turns red.



The background of the text measures turns purple if at least one device from which they draw a value does not respond to requests.





6.2 Devices

6.2.1 System measures display

Home Devices Al	larms 🌔	Alarm Histo	ory	Report	Documents	Favorites	Config	guration				🕖 Lice	inse	🕜 Manual	🔙 Logou	t 📕	
Devices and system measu	ures	*	Ca	ategory: evice: In	Inverter verter 1		Inve Part	erters Activ tial Energ	re Power y Accumulated (today)		0 kW 0 kWh	-				ONLI	NE
System variables			Mo	odel: SUNS	YS STATION PO	3	Tota	al Energy /	Accumulated		0 kWh						
Inverter Inverter 1			D	ata Al	arms (1)												
		-	Filte	r measure	ə:		×										
Powermeter Power Meter						M	easure				Value	Mir	1	Range	Max		
Production Meter				Total En	ergy Accumula	ed				0 kWh						B	^
String String Control 1				Warning	present					false						B	
String Control 2		Ē		MPPT1													
				DC Input	t Voltage					0 V			0		900		1
				Inverter A	Active Power					0 kW			0		36		
				Module E	Board Tempera	ture				0 °C						B	
				Partial E	nergy Accumul	ated (today)				0 kWh						8	
				Total En	ergy Accumula	ed				0 kWh						8	
				Warning	present					false						H	
				MPPT2													
				DO Innui	Noltono					0.17			<u> </u>		000		

Figure 60 - System measures display

All of the devices being polled by the IOT SCADA SERVER can be seen in the tree menu structure on the left, sorted by category, and beside each device there is an icon that represents the reachability state. If operating normally the figured field fie

Once you select a device, the reachability state will be replicated in area on the right as well, together with the date and time of the last communication attempt made:



Alleantia

6.2.1.1 Data and alarms display

The device measures read are divided into the two tabs **Data** and **Alarms**. Information and icons can be associated with each:



During normal operation the **Alarms** tab will look the same as the **Data** tab. In the presence of active alarms, however, the text of the **Alarm** tab will appear in red and the number of active alarms will be indicated. Selecting this tab will display all the measures associated with an alarm and those in active alarm condition will have a red background:

Home	Devices	Alarms	Alarm Hist	огу	Report	Documents	Favorites	Configu	uration				👔 License	🕜 Manual	🚮 Logo	ut 🚺	
Devices and	d system m ⋈∰ Graph	easures	»	C D	ategory: evice: In	Inverter verter 1		Invert Partia	rters Activ ial Energy	e Power Accumulated (today)		0 kW 0 kWh				ONLIN	ΙE
System	i variable er ter 1	5	▲ 🖳		odel: SUNS Data Al	YS STATION P03		Total	i Energy A	Accumulated		0 KVVN]				
⊡ Rewert	ter 2			Filte	er measure	ə:		N.									
Powern Powern	er Meter				TEGRITI	aun	Me	easure			10100	Value	Min	Range	Max	V	
⊡ Produ	uction Mete	r			I Leak se	ensor Fault					false					⊲ 💾	1
String	g Control 1				Insulatio	n sensor fault					false					🦪 💾	
String	g Control 2				Interface	protection fault					false					🦪 💾	
					Low Imp	edance to Grou	nd				true					🔺 💾	
					Maintena	ance alarm					false					🦪 💾	
					Module *	1 in parallel gen	eral alarm				false					🦪 💾	
					Module 2	2 in parallel gen	eral alarm				false					🦪 💾	
					Module 3	3 in parallel gen	eral alarm				false					🦪 💾	
					Module i	n parallel with d	ifferent config	uration			false					🦪 💾	
					Modules	communication	fault				false					🦪 💾	
					Output A	C Mains Contac	tor fault				false					🦪 💾	-





In the event that the device is offline, the background colour of all its measures will be purple and the value displayed will be that related to the last valid reading, or a series of dashes if there has been no communication:

Home Devices Alarms	Alarm Histo	ry Report	Documents	Favorites	Configuration) License	🕜 Manual	🚮 Logou	t 🚺 📑
Devices and system measures	×	Category: Device: Pr	Powermeter roduction Me	ter					c	OFFLINE
System variables Model: DRIS A40										
Powermeter Power Meter	I I I I I I I I I I I I I I I I I I I	Filter measure	9:	Me	easure	Value	Min	Range	Max	
Production Meter String String Control 1 String Control 2		Controllo Partial Pe	energie ositive Active Ene	ergy (Ea+) Energy (Er+)		0 KWh				
	<u> </u>	Misure at	ffette da trasfor	matori		e wan				
		Current li	1 2			0 A 0 A				
		Current I	3 Phase Voltage	U12		0 A 0 V				
		Phase to	Phase Voltage Phase Voltage	U23 U31		0 V 0 V				
		S Active I	Power P +/-			0 KW				-

Figure 62 - Communication error device

To facilitate the search for a measure, it can be filtered by name with the appropriate field:

Filter measure:	×

Figure 63 - Measure name filter

Or use the breakdown in sections, if any, selecting a single section from the tree menu structure on the left, such as, for example, "MPPT2", which will result in the closure of all the sections except that selected, making visible only part of the device measures:

Measure	Value
System	
D MPPT1	
MPPT2	
DC Input Voltage	499 V
Inverter Active Power	13,4 KW
Module Board Temperature	24 °C
Partial Energy Accumulated (today)	118,4 kWh
Total Energy Accumulated	78.451 kWh

Figure 64 - Device sections



6.2.2 Graphs

To generate a graph of the time trend of one or more measures, select measures of interest by checking the appropriate box and then press the button:





Figure 65 - Graphs

The temporal controls for the generation of the graph are located at the top. The default date and time interval runs from the current date and time to midnight on the previous day. These can, however, be edited and a new graph generated by pressing the **Update graph** button.

To restore the default interval, press the Reset date button.

Once a graph has been created, the reference time interval can be changed using the buttons below:

	moves the time interval back by 90%
•	moves the time interval back by 40%
Q	decreases the time interval by 20%
•	increases the time interval by 20%
	moves the time interval forward by 40%
►	moves the time interval forward by 90%



The graph is automatically regenerated after pressing one of these buttons.

To change the selection of the measures to be plotted, return to the system and device measures display screen by pressing the button:

📋 Select

Select or clear the measure by using the check box again.

The measures currently selected are listed in the tree menu structure on the left. These can also be removed by pressing the icon:

6.2.3 Measure write

Some measures can be written, therefore it is possible to insert value to write into measure. To do it you should be authorized by logging in with user/password: go to section **Configuration**, login, and return to section **Devices**. Select a device to open the measures list. The writeable ones can be identified by the presence of a button on the row, see figure below.

Uscita digitale 1	false	8
Uscita digitale 2	false 🥒	8
Uscita relè 1	false	8
Uscita relè 2	false	8 -

Pressing the button a popup window will open that allows to insert new value.

Value write	×
Current measu	re value: false
Insert value to	write into measure "Uscita relè 2":
false ▼	
	Ok Cancel

Writing is carried out in few seconds and while waiting the selected measure's line turns orange, keeping the old value.

Uscita digitale 1	false 🖉	
Uscita digitale 2	false	8
Uscita relè 1	false	8
Uscita relè 2	false 🥓	8 -



Once writing is complete, the line turns white again and the value is updated.

Uscita digitale 1	true 🥒	8
Uscita digitale 2	false 🥖	8
Uscita relè 1	false	8
Uscita relè 2	false 🥒	8.

6.2.4 Exporting data to Excel

Once a graph has been generated, the data can be exported in Excel format by pressing the button:

🔜 Export data

You will be prompted to save the dataExport.xlsx file containing ALL of the values recorded by IOT SCADA SERVER for the measures that are currently selected within the selected time interval in Excel 2007 format. N.B. Excel 2007 limits the number of rows in an Excel spreadsheet to 65536. If the number of data exported is greater, the "excess" data will be automatically deleted.

6.3 Alarms

The current active alarms on all devices to which the IOT SCADA SERVER is connected can be viewed in the **Alarms** section. The list is sorted by date and time, but the order in any column can be changed by clicking on the corresponding heading.

Home	Devices	Alarms	Alarm H	listory	Report	Do	ocuments Favorit	es Config	guration	👔 Licen	se 🕜 Manual	📶 Logou	t 🚺 📕
Date ar	nd Time 🛛 💠	Devi	ce name	÷	Section	÷	Me	asure	÷	Alarm de	scription	÷	State
6/4/17 11	1:10:13 AM	In	verter 1		System		Low Imped	ance to Grou	und	Low Impeda	nce to Ground		Active

Figure 66 - Active alarms

If there is no alarm the message **No active alarm** will be displayed. If alarms are present, the text in the **Alarms** tab will be red, even when the tab is not open.

Custom alarms are also reported in this section.

6.4 Alarms history

To display a history of the alarms that were triggered in the devices connected to IOT SCADA SERVER enter the **Alarm history** section. If alarms are present, the screen that appears is like that in Figure 67:

Home Devices	Alarms Alarm His	story Report Doc	cuments Favorites C	Configuration		🕖 License 🕜 Manual ₫ Logout 📗 💻
Per event		 ♀ Alarm type filter ✓ Measure ✓ Device ✓ System 	- 💡 Date filter Start Date: Final Date:	11 × 11 ×	Ru Update	
Alarm Data (ON)	Alarm Data (OFF)	Alarm type	Device Description	Section	Alarm Description	Notification Timestamr Notification Timestamr Notification
6/4/17 11:10:13 AM		Measure	Inverter 1	System	Low Impedance to Ground	
6/4/17 11:05:14 AM		Measure	Inverter 1	System	Low Production on Inverter 1	
6/4/17 10:56:16 AM	6/4/17 11:00:54 AM	Measure	Inverter 1	System	Output Trasfo overtemperature	
6/4/17 10:56:16 AM	6/4/17 11:00:54 AM	Measure	Inverter 1	System	System AC Frequency fault	
6/4/17 10:56:16 AM	6/4/17 11:00:54 AM	Measure	Inverter 1	System	System AC Voltage fault	
6/4/17 10:56:16 AM	6/4/17 11:00:54 AM	Measure	Inverter 1	System	System AC Voltage Quality fault	
6/4/17 10:56:16 AM	6/4/17 11:00:54 AM	Measure	Inverter 1	System	Parallel fault	
6/4/17 10:56:16 AM	6/4/17 11:00:54 AM	Measure	Inverter 1	System	I Leak sensor Fault	
6/4/17 10:56:16 AM	6/4/17 11:00:54 AM	Measure	Inverter 1	System	External Shutdown Activated	
1 /27	 >> 					

Figure 67 - Alarm history per event

The list is sorted by date and time in descending order and the alarms displayed can be filtered based on a date interval to be specified in the **Date Filter** fields, and on the type of alarm, to be specified in the **Alarm type filter** box. Thereafter the alarm corresponding to the filters set will be displayed by clicking on the **Update** button.

There are 3 types of alarms in IOT SCADA:

Measure alarms

o These are default alarms set on catalogue device measures, or defined by the user as shown in Section 5.3.3.

Device alarms

o These are generated when a device does not respond to requests and becomes offline

System alarms

o These are generated by multiple abnormal situations, such as a backup failure, an improper shutdown of the IOT SCADA SERVER, an error while sending a notification, etc.

In Figure 67, **Per event** selected in the **Data sorting** box, the alarm ON and the corresponding OFF alarm, if any, are grouped together in the same row, thereby facilitating the relationship between alarm events.

If it is not possible to display all the alarms on the same page, the list can be scrolled by means of the page navigation controls at the bottom.

If the alarm notification has been configured (see Section 5.4.1), there is a button at the end of each row. If this is pressed, a popup window as in Figure 68 will be displayed, with details on the forwarding of the notification.

Notification D	etail	System	Low Impedance	to Ground 🛛 💌
Alarm State	Туре	Notified	Notification Date	Retries
ON	mail	No		1
				🔞 Close

Figure 68 - Notification details

The alarm history can also be viewed by sorting the data in a chronological manner (i.e. selecting the option **Chronology** in which the alarms are presented in the reverse order in which they occurred, that is with the most recent at the top of the list together with the information about the state of the alarm ON (device in alarm) separate from that of the alarm OFF status (device alarm over), as in Figure 69:

Home Devices	Alarms Alarm His	story Report Docum	ents Favorites	Configuration		🕧 Licer	nse 🕜 Manual <u>ब</u> Logout 📗 📕
Chronology		Image: Alarm type filter Image: System	P Date filter		R Update		
Alarm Timestamp	Alarm type	Device Description	Section		Alarm Description	Alarm State	Notification Timestamr Notificatio
6/4/17 11:10:13 AM	Measure	Inverter 1	System		Low Impedance to Ground	ON	
6/4/17 11:05:14 AM	Measure	Inverter 1	System		Low Production on Inverter 1	ON	
6/4/17 11:00:54 AM	Measure	Inverter 1	System		Output Trasfo overtemperature	OFF	
6/4/17 11:00:54 AM	Measure	Inverter 1	System		System AC Frequency fault	OFF	
6/4/17 11:00:54 AM	Measure	Inverter 1	System		System AC Voltage fault	OFF	
6/4/17 11:00:54 AM	Measure	Inverter 1	System		System AC Voltage Quality fault	OFF	
6/4/17 11:00:54 AM	Measure	Inverter 1	System		Parallel fault	OFF	
6/4/17 11:00:54 AM	Measure	Inverter 1	System		External Shutdown Activated	OFF	
6/4/17 11:00:54 AM	Measure	Inverter 1	System		I Leak sensor Fault	OFF	
1 / 30	► ►I						

Figure 69 - Chronological alarms history

6.5 Report

In the Report section of the main menu it is possible to choose the type of report to generate:

Synoptics	Devices Alarn	Alarm History	Report	Documents	Favorites	Configuration
Single me	easure reports	Comparison betwee	n measures	Compariso	n between pe	riods U →
Report param	neters					
Report on						
Period						
Day	1/19/17	<u> 11 11 11 11 </u>				
		📊 Ger	nerate			

Figure 70 - Types of report



Energy reports can be generated (growing monotonic measures), enabling the daily or monthly progress of the energy measures to be analysed in different ways:

- the single measure energy report represents the simplest type of energy reports focusing the analysis on a single energy measure. This is the most compact of the various reports as it is composed of a single page with a bar graph and data table.
- the energy report "comparison between measures" highlights the differences between energy measures
 over the same period of time. This is useful in comparing energy production and consumption in a system,
 as well as for discovering any inefficiencies in devices regarded as similar (e.g. different production by
 inverter of the same model connected to the same number of strings). This contains a line graph and one
 or more data comparison tables between different measures.
- the energy report "comparison between periods" analyses the performance of one energy measure over several days or several months. It enables, for example, the comparison between the energy produced in July 2016 with that produced in the same month of 2017. It contains a line graph and one or more data comparison tables between different periods.

The measures and the periods over which the analysis is to be performed must be defined in each of these reports by filling in a special form of input parameters.

Report parameter	Report parameters			
Report on				
Period	Daily Omega Monthly			
Day	1/19/17			
	Generate			

Figure 71 - Input parameters form for the single measure report

If the report is a comparison of several measures, then more than one measure can be chosen. Similarly, for the comparison report between several periods more than one period can be chosen.

Report param	Report parameters				
Measures	Inverter 2 - System - Total Energy Accumulated Inverter 1 - System - Total Energy Accumulated				
Period	Daily Monthly				
Month	June 2017				
Grafico 🖉 Include graph in report					
in Generate					

Measures	Inverter 1 - System - Total Energy Accumulated
Period	Daily Monthly
Months	May 2017 June 2017
Graph	Include graph in report

Figure 72 – Choice of multiple measures for the comparison report between different measures

Figure 73 – Choice of multiple periods for the comparison
report between different measures

After filling in the parameter input form, a preview of the report can be generated by pressing the **Generate** button. A few moments later a popup window will open displaying the generated document consisting of a graph and one or more tables; at the bottom of the popup window there are buttons that are used to save or forward the report displayed via email. The email forwarding occurs after the recipients of the mail have been entered in the appropriate popup window that appears after the **Send** button is pressed. To use this feature the notification parameters must be configured, as described in Section 5.4.1.





Figure 74 - Single measure energy report

6.6 Documents

Devices Alarms Alarm History Report	Documents Favo	orites Configuration	License 🕜 Manual <u> </u> I	ogout 📙 🗮
📥 Add				
Document name	\$ D	escription	Upload date	
536103A RS485.pdf	U	ser guide	11/3/17	💼 Delete

Figure 75 - System documents

For convenience, documents that are deemed useful to the system being monitored, such as wiring diagrams or other, can be loaded in IOT SCADA SERVER.

A popup window, as shown in Figure 75, opens when the **Add** button is pressed. Thereafter the **Upload** button must be pressed and the document to be loaded chosen. A description, such as **System Wiring** must be entered and subsequently the **Ok** button pressed.

You must be logged in to delete a document, in which case the **Delete** button next to each document will appear.

Document uple	pad 🔪
WARNING! For loaded: [exe, co	security reasons, files with the following extensions cannot be m, bat, cmd, htm, html, mht, js]
Document	Upload No file uploaded
Description	
	🛷 Ok 🕒 🎦 Cancel

Figure 76 - Document upload



6.7 Favourites

Devices Alarms Alarm History Report	Documents Fa	avorites	Configuration	🕧 License	🕜 Manual 🤞	📕 Logout 📕 💻
📥 Add						
Name	÷	Address				
IP Camera		http://192	2.168.2.34			💼 Delete



Favourites, that is addresses of IP cameras present in the system or of other sites that are of interest, can be entered in the IOT SCADA SERVER configuration.

By pressing the **Add** button a popup window opens as shown in Figure 77. A name must be entered to help understanding, such as **System cameras**, the address itself, and then the **Ok** button must be pressed.

You must be logged in to delete a favourite, in which case the **Delete** button next to each document will appear.

Favorite address	setup	http://192.168.1.23	\mathbf{x}
Name			
Address			
			🛷 Ok 🔊 Cancel

Figure 78 - Favourite addresses insertion

This will open in a new browser window when clicking on the address.



7.1 Specific functions for Machine tools and Machining centres

The IoT Scada Server system has specific functions to connect the device to CNC of machining tools or machining centres.

It supports drivers of primary brands, such as, for example CNC Siemens, Fanuc, and Heidenhain. When uploading this kind of drivers, there are additional functions available, as part program transfer and sending of working documents in **Documents** folder.

7.2 Remote part program transfer (machine instructions)

Not all families/versions of CNC support these functions (e.g. old CNC families).

When adding a device and choosing a driver of supported CNC brands (described in previous sections), Part Programs name CNC page will appear.



Follow this procedure:

- Connect gateway's Ethernet port to CNC's Ethernet port (very old CNC might not have Ethernet ports);

- Enable communication and connection ports from CNC: in some cases you should enable Ethernet port to allow the CNC to send data. Verify that the CNC can send data to the third parties (in some cases you should purchase additional optional functions of the CNC, provided by its manufacturer);

- Setup the Ethernet ports, as described in sections 4 and 5. Pay attention to the correct settings of assigned IPs to the CNC, gateway and local LAN network in order to avoid conflicts. The devices equipped with DUAL LAN allow the gateway to connect to CNC with IP of a certain family and, for ex., with the office PCs or servers with other IP, without coming into conflict;

- Make all communication **TCP/IP Tests** that can be found at **Configuration** tab (see section 5) and test a single IP address to ping on the CNC, office PC and server. In case of a successful outcome, the screen icon next to the device will turn green.



In case of communication problems the screen icon will turn red 💻. If the communication test succeeds but the icon remains red or the CNC icon remains red, it means that you should enable CNC's ports.



- After setting up the connections and the communication ports, click **Part Programs**. The screen as in figure below will appear.

	0:	Dete			
Par Program	Size	Date		-	
09100	2.0kB	02/01/2016 15:48:36	*		
O9101	2.0kB	02/01/2016 11:26:10			
O9102	1.0kB	02/01/2016 11:26:24			
O9200	2.0kB	02/01/2016 11:26:44			
01	1.0kB	14/01/2016 11:51:00			
TECNO	1.0kB	03/10/2015 17:43:50			
TEK	1.0kB	16/03/2017 12:55:44			
XIN-1	1.0kB	28/07/2016 15:00:54			
PROVA2	1.0kB	22/03/2017 12:11:22			
TEK2	1.0kB	28/03/2017 13:22:18			
TEKETE4	15.0kB	30/04/2017 15:18:38	_		
TEK1	1.0kB	25/06/2017 15:32:20	-		
📲 Upload 🛛	P Download				



In the box you will see all part programs on the monitored machine's PLC.

Then you can download and upload the part program files (machine instructions).

So it will be possible to send the instructions directly from a PC to the machine and transfer new part program.

- Click **Upload**, in the popup window select the file from your PC (as shown in the figure below) and click **Open**. The system in few seconds will transfer it to the machine's CNC, at any distance it is. In this example TEK1 part program was used.



- Click **Open**, wait for a few seconds.

- When the system has finished the file transfer (it depends on the file dimension and the kind of connection), you can check the transfer: click **F5** button to refresh the web page and scroll the list of part programs on the CNC. You will see TEK1 file in the list: the file transfer was successful.

	Par Program	Size	Date	
	O9153	2.0kB	14/11/2015 16:50:10	
	O9154	1.0kB	15/11/2015 08:53:16	
	O9100	2.0kB	02/01/2016 15:48:36	
	O9101	2.0kB	02/01/2016 11:26:10	
	O9102	1.0kB	02/01/2016 11:26:24	
	O9200	2.0kB	02/01/2016 11:26:44	
	01	1.0kB	14/01/2016 11:51:00	
	TECNO	1.0kB	03/10/2015 17:43:50	
	TEK	1.0kB	16/03/2017 12:55:44	
	TEK1	1.0kB	13/03/2017 18:43:16	_
4	XIN 4	1.0kB	28/07/2016 15:00:54	
	PROVA2	1.0kB	22/03/2017 12:11:22	-
	🕂 Upload	🐈 Download		



On-board controller can start the program or work.

The purpose of this function is to organize/program all sequences of working that the machine performs, to organize and plan the production, etc.

CAUTION:

If you are accidentally trying to transfer remotely a part program to the CNC, which is already on the machine, the operation will not have success, as the files are protected from being overwritten remotely. Rename the file, adding revision (TEK1rev, TEK1r1 and so on).

CAUTION:

The files that start with "O" cannot be downloaded and managed remotely, for security reasons. Rename the file (add another letter in the beginning).

- To download a part program from the machine's CNC (for ex., to modify the instructions remotely), select the file and click **Download**.

Choose the folder to save the file.

The file WILL NOT BE DELETED from the CNC. For security reasons, when working nothing is modified or overwritten.

Par Program	Size	Date	
O9153	2.0kB	14/11/2015 16:50:10	
D9154	1.0kB	15/11/2015 08:53:16	
O9100	2.0kB	02/01/2016 15:48:36	
09101	2.0kB	02/01/2016 11:26:10	
09102	1.0kB	02/01/2016 11:26:24	
09200	2.0kB	02/01/2016 11:26:44	
01	1.0kB	14/01/2016 11:51:00	
TECNO	1.0kB	03/10/2015 17:43:50	
TEK	1.0kB	16/03/2017 12:55:44	
TEK1	1.0kB	13/03/2017 18:43:16	
XIN-1	1.0kB	28/07/2016 15:00:54	
PROVA2	1.0kB	22/03/2017 12:11:22	
🐈 Upload 🔹	Download		



After that, on the on-board CNC screen you can easily check that the file has not been removed or modified.

CAUTION:

In some cases in might happen that, after selecting the part program to download, clicking the "Download" button, Google Chrome is set by default to download files in "Downloads" folder (see figure below).

Alleantia

O9100	2.0kB	02/01/2016 15:48:36		
09101		02/01/2010 13.40.30	*	
00101	2.0kB	02/01/2016 11:26:10		
O9102	1.0kB	02/01/2016 11:26:24		
O9200	2.0kB	02/01/2016 11:26:44		
01	1.0kB	14/01/2016 11:51:00		
TECNO	1.0kB	03/10/2015 17:43:50		
TEK	1.0kB	16/03/2017 12:55:44		
XIN-1	1.0kB	28/07/2016 15:00:54		
PROVA2	1.0kB	22/03/2017 12:11:22		
TEK2	1.0kB	28/03/2017 13:22:18		
TEKETE4	15.0kB	30/04/2017 15:18:38		
TEK1	1.0kB	25/06/2017 15:32:20	T	

To change the folder, go to Google Chrome settings, check **Ask where to save each file before downloading** box.

🌣 Settings	
\leftrightarrow \Rightarrow G \otimes	Chrome chrome://settings
Chrome	Settings
Extensions	Page zoom: 100%
Settings	Network
About	Google Chrome is using your computer's system proxy settings to connect to the network. Change proxy settings
	Languages Change how Chrome handles and displays languages. <u>Learn more</u> Language and input settings Ø Offer to translate pages that aren't in a language you read. Manage languages
	Downloads
	Download location: C:\Users\IoT SCADA Server\Down pads Change Ask where to save each file before downloading HTTPS/SSL Manage certificates



7.3 IOT SCADA SERVER does not switch on

For the Base and UPS models (code IxS_1y1), check there is 12 V direct current on jack with terminal positive on DC+ and negative on DC-. If voltage is over or below 12 V, change power supply or, if possible, adjust output voltage of existing one.

For the Multi and Multi+UPS models (code IxS_1y2, IxS_1y3), check there is between 12 V and 24 V direct current or between 15 V and 26 V alternating current on terminal DC+ and DC-. If the measured voltage is not comprised in the specified intervals, change power supply or, if possible, adjust output voltage of existing one.

7.4 Unable to complete Internet communication test

Verify that the Ethernet or Wi-Fi connections have been made correctly and check activity state of LED LAN or Wi-Fi on the IOT SCADA SERVER (Section 2.3.1) and the switch/router. If the IP address has been manually configured, verify the parameter configuration with your network administrator or with the router.

7.5 Communication problems with serial devices

In the event of communication problems with serial devices, refer to the troubleshooting guide in the section **Configuration -> Installation -> Devices configuration** that can be downloaded by pressing the button:



7.6 Unable to access IOT SCADA SERVER from the local network

Check that the IP address and subnet mask of the device from which you want to reach IOT SCADA SERVER are compatible with the IP address and the subnet mask of the IOT SCADA SERVER itself (see Sections 4.4 e 5.1)

7.7 Unable to access IOT SCADA SERVER from the Internet

Check that "NAT" has been configured on the local router on port 80 of the IP address of the IOT SCADA SERVER.

In the event that you are trying to access the IOT SCADA SERVER through a name, and not through an IP address (e.g. mymachine.no-ip.org), check the DDNS configuration of the router.

7.8 Auto start of the IOT SCADA system and the gateway at power-up of the machine

In order to allow the auto start when power up from the network when it is installed in machine or electric board, follow the procedure:

- Switch on the PC and press F2 several times, BIOS grey screen will appear

- Click Power management > AC recovery > Select Power on
- Click Apply
- Check the Save as custom user settings box > Click Ok > Exit

This procedure diables the gateway's power button. For the IOT SCADA auto start see **paragraph 4.1**.

Álleantia

7.9 System hotspot activation

To automatically activate the access point every time the gateway is powered up: access the IOT SCADA from a PC, laptop, tablet or smartphone, when in coverage of your gateway (see section 4 for the connection via Wi-Fi to the software).

This procedure can be activated only on the gateways with the appropriate hardware characteristics (if there is Wi/Fi card, possibility to set it up correctly, etc.).

This test has been done on Advantech UTX-3115.

- 1. Download Tool Connectify Hotspot 2017 (there is also a free version).
- 2. The Lite license has the following options:
 - the system generates "Connectify-me" hotspot
 - the hotspot password can be modified

3. In "Internet to share" section select Wi-Fi card. In our case (Advantech UTX-3115) it is "Realtek PCIe GBE Family Controller".

4. This tool can be set to start automatically along with Windows: go to **Settings** section in the upper right corner, click **Startup Options**, check **Start interface on login**. Select **Always** in **Resume hotspot on boot-up**.

5. Return to the beginning and check Start hotspot box to switch it on.

NOTE: these 5 steps should be done only once, during the device setup. Then the program will do it automatically.

The password can be modified.

Now you can use Wi-Fi:

a. Open IoTSCADA web interface.

b. Go to Configuration tab and log in:

username: admin password: webloggerSU

c. Click "TCP/IP configuration"

d. Select "Microsoft Wi-Fi Direct Virtual Adapter #2"

e. In the browser address bar copy 192.168.XXX.X IP address, shown in the table to access the IoTSCADA web interface from a mobile device, connected to **"Connectify-me"** Wi-Fi network.



7.10 System configuration

In the gateway, the following programs are already installed:

- TeamViewer
- UltraVnc
- OpenVpnGUI
- App. IoT SCADA Server

In addition, to ensure the best performance, the following Windows services were disabled:

- Windows Defender
- Windows Firewall

8 Contacts

Alleantia s.r.l.

www.alleantia.com

Registered offices: Via Tosco Romagnola, 136 56025 Pontedera (PI) Operating headquarters: Via Umberto Forti, 24/14 56121 Pisa VAT code/Tax code: IT 02011550502

info@alleantia.com







Alleantia s.r.l. www.alleantia.com

Registered offices: Via Tosco Romagnola, 136 - 56025 Pontedera (PI) Operating headquarters: Via Umberto Forti, 24/14 56121 Pisa VAT code/Tax code: IT 02011550502

 \mathcal{X}

....

 \odot

Ů

 \bigcirc

 \succ

@

Ö

÷

Ø

((

∦

O

SMS

:

57

Ç

Ð

>>

A

Tel: (+39) 050 9911933 Fax: (+39) 050 9655139 @: sales@alleantia.com

 \sim

. . .