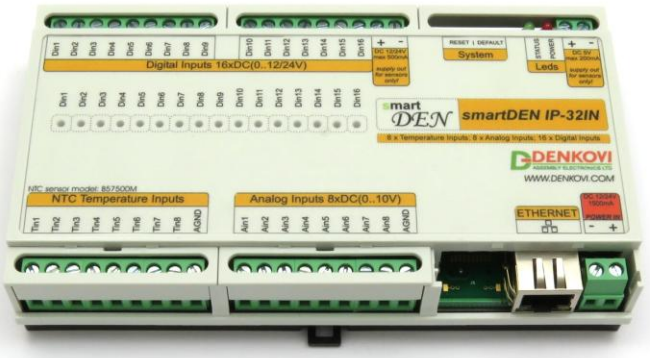
SmartDEN IP-32IN

Web enabled 32 Input Module

User Manual
Date: 28 Oct 2021

For firmware version: v1.28 / Oct 2021



Trademark Notices

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Apple, Mac, Mac OS, Mac OS logo are either trademarks or registered trademarks of Apple Computer Inc. in the United States and/or other countries.

smartDEN is registered trademark of Denkovi Assembly Electronics LTD in European Union.

Other product names and company names described in this document are trademarks or registered trademarks.

Content

1. Features

SmartDEN IP-32IN is an Ethernet input module designed especially for remote monitoring and logging. It provides 16 digital inputs (for motion detector sensors, dry contacts, switches, buttons), 8 analog inputs (for temperature, humidity, light, pressure sensors) and 8 NTC inputs especially designed for thermistors type B57500M. The integrated web server for set-up, SNMPv2c and HTTP/XML allow easy embedding in other systems. The module is able as well to control other remote relays based on input event or work in "Data Logging Mode" in order to post data in xml format on a remote server.

A list of **SmartDEN IP-32IN** features includes:

Inputs:

- 16 digital inputs (counters) with ON/OFF LED;
- 8 analog inputs 0-10V DC;
- 8 temperature inputs for NTC thermistors type B57500M;
- Linearization (scaling) for the analog inputs;

Communication:

- Fully Compatible with 10/100/1000 Base-T networks, Auto-MDIX;
- Protocols: TCP/IP, HTTP, DHCP, DNS, ICMP (ping), SNMPv2c;

Web Interface:

- Configuration of system parameters;
- Access current measurements;
- Secure login authorization;
- Access protection (by IP and MAC address);

TCP/IP Services:

- HTTP server: Access (GET) current measurements in XML/JSON format;
- Encrypted login process for reading inputs status and analog/temperature values;

SNMP:

- SNMP messages for configuration/monitoring (get, set, bulk, table, getnext, walk);
- SNMP trap messages (triggered by threshold events or periodically);

Web Services:

- Data Logging mode (push) mode: XML data is sent via HTTP post method to remote server periodically;
- Remote relay control mode: remote control of smartDEN Relay Modules, DAEnetIP3, DAEnetIP4 and Wi-Fi Relay Modules through Ethernet/Internet;

Power Supply:

- Supply voltage 10..28V DC;
- Additional source voltage 5V DC is provided to facilitate the sensors power supply;

Physical and Environment:

- Working temperature range: 0 to 70°C;
- DIN rail standard housing.

2. Application examples

SmartDEN IP-32IN could be used for home and industrial automation applications, datacenters monitoring, environmental monitoring and so on. Several application examples how **SmartDEN IP-32IN** could be used are shown bellow. The examples are only conceptual and an additional equipment/connections can be required in actual implementations.

2.1. Remote sensors monitoring

This mode of the module **SmartDEN IP-32IN** allows monitoring up to 32 different sensors in real time. Various kinds of sensors for temperature, humidity, distance, light and so on can be connected to the device. In this mode **SmartDEN IP-32IN** acts as a server**.** A custom client application can retrieve the current measurements using SNMPv2c or HTTP GET requests. Examples of client applications include our iOS and Android mobile apps, as well as custom monitoring applications with SNMPv2c /HTTP/XML/JSON support.

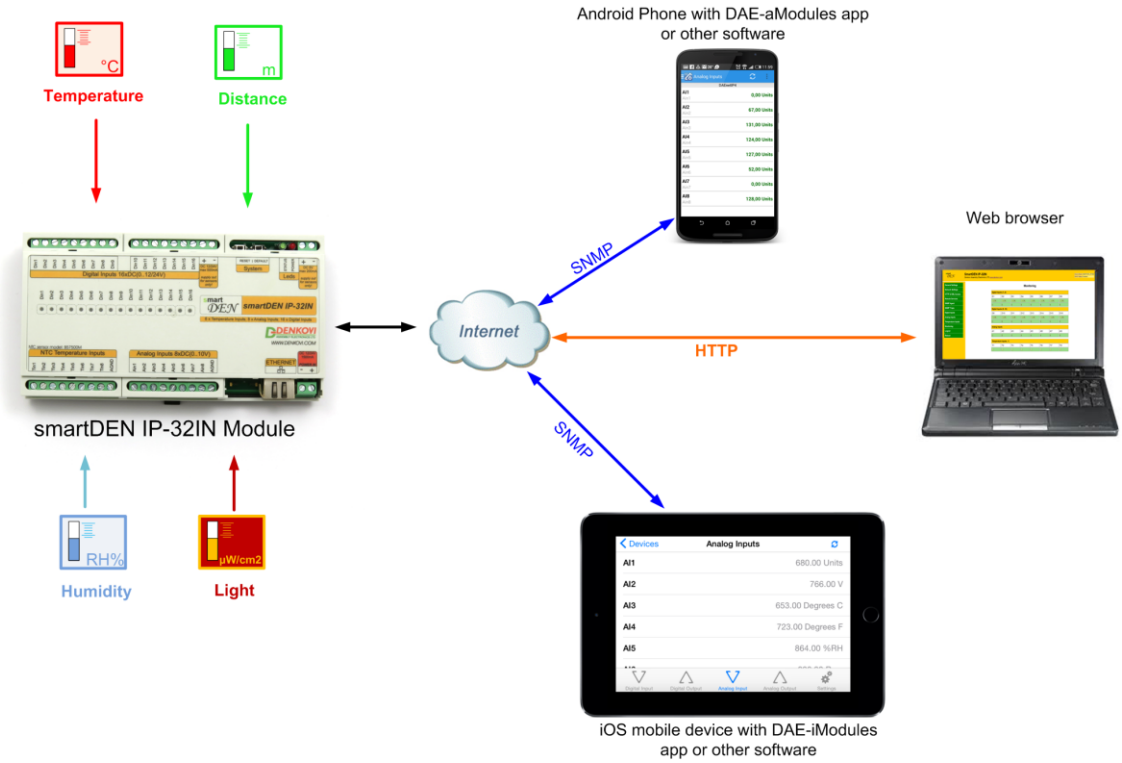


Figure 1. Remote sensors monitoring

2.2. Push messages and data logging

Another very useful mode of **SmartDEN IP-32IN** is sending "push" messages (notifications) to remote server without the need to be polled continuously. This is very suitable for organizing alert and logging systems. The module is able to send HTTP POST messages in XML format periodically. The SNMP traps can be triggered by events (for example when temperature is getting high) or send periodically. It is

also possible to control remote relay board over the LAN/WAN network again basing on input event via HTTP GET request.

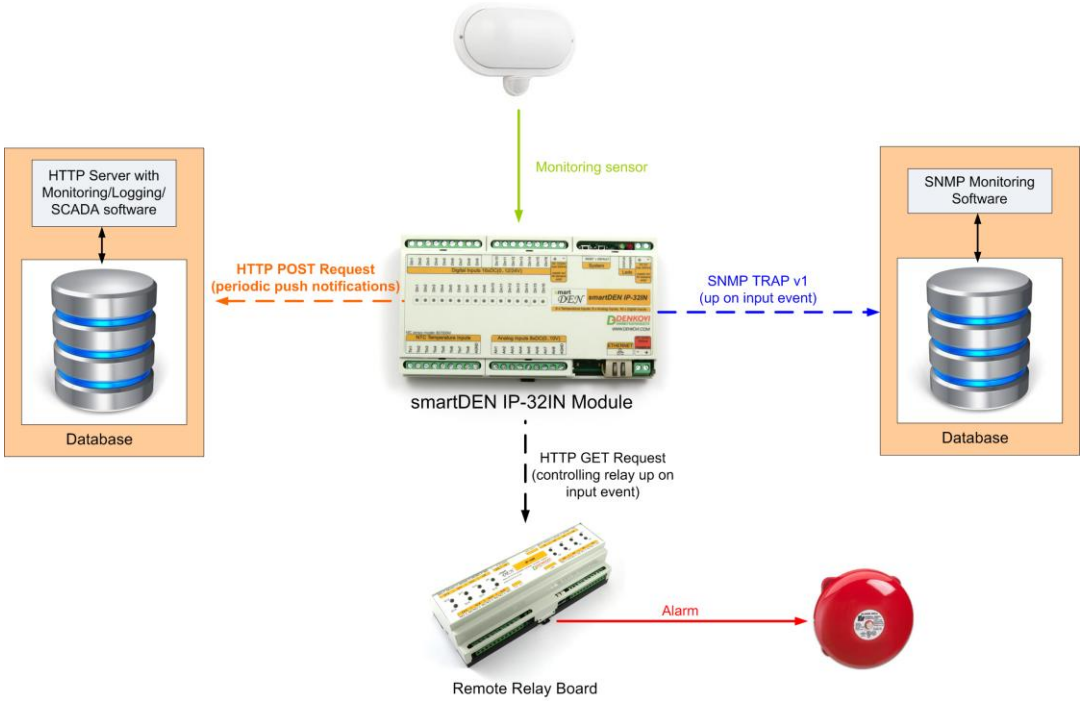


Figure 2. Alert and data log example system

2.3. Events counter

SmartDEN IP-32IN provides 16 x 16-bit counters (from 0 up to 65535) attached to the digital inputs that can be used to count various not fast events - for example detect when a person enters in a shop through the door (Fig. 3). Upon detecting the specified edge/level condition **SmartDEN IP-32IN** increments the corresponding counter. With suitable software and database one could easily organize a simple monitoring and statistic system.

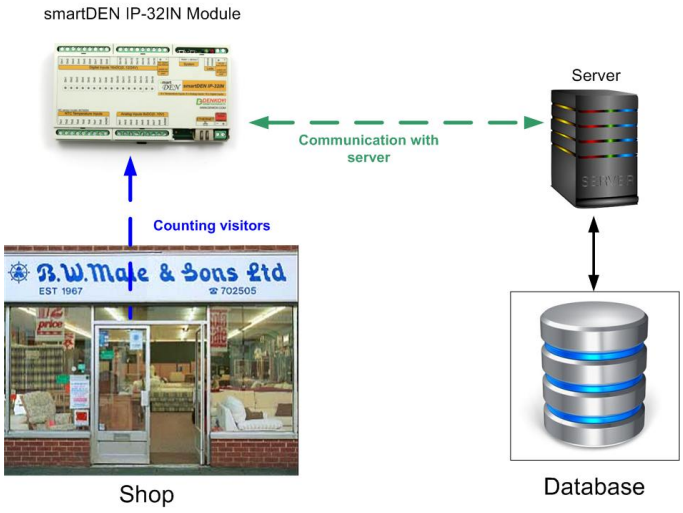


Figure 3. Counting visitors in shop

3. Technical parameters

Table 1. Physical parameters

Parameter	Value
Size (L / W / H), mm	157 / 89 / 31
Weight, g	205
Operating temperature, °C	0 to 70

Table 2. System parameters

Parameter	Value
Power supply voltage, VDC	10... 28 ± 5%
Maximum current consumption, mA	1500
Protection against reverse polarity	Yes
Default settings button	Yes
Reset button	Yes

Table 3. Analog Inputs

Parameter	Value
Analog inputs number	8
Analog inputs full scale voltage range, VDC	0 up to 10
Analog inputs absolute maximum non-destructive voltage, VDC	24
Analog inputs resolution, bits	10
Value of LSB, mV	~10
Input impedance, KΩ	1330
Sample period, ms	Min: 25*
	Max: 300**
Protection against reverse polarity	Yes

*No communication (HTTP, SNMP) is taking place with the module
**Intensive communication (HTTP, SNMP) with the module

Table 4. Digital Inputs

Parameter	Value
Digital inputs number	16
Digital inputs voltage range, VDC	0 up to 30
Input switching threshold from 0 to 1, VDC	>7.6
Input switching threshold from 0 to 1, mA	>3.2
Input switching threshold from 1 to 0, VDC	<4.5
Input switching threshold from 1 to 0, mA	<1.8
Supported sensor output type	PNP
Input type	Resistive with Schmitt trigger
Sample period, ms	Min: 25*
	Max: 300**
Protection against reverse polarity	Yes

*No communication (HTTP, SNMP) is taking place with the module
**Intensive communication (HTTP, SNMP) with the module

Table 5. Counters

Parameter	Value
Counters number	16
Max. pulses frequency, Hz	1 ..10*

*See point 7.9

Table 6. Temperature Inputs

Parameter	Value
NTC inputs number	8
Sensor type	B57500M
Units	Celsius/Fahrenheit
Sensor working temperature range	-55°C/-67°F to +155°C/311°F
Accuracy	±0.5°C
Sample period, ms	Min: 25*
	Max: 300**

*No communication (HTTP, SNMP) is taking place with the module
**Intensive communication (HTTP, SNMP) with the module

Table 7. Network

Parameter	Value
Network parameters	IP/Mask/Default gateway
MAC lock (protection)	Yes
DHCP	Yes
DNS	Yes
ICMP	Yes
SNMPv2c	Yes (set, get, table, walk, getnext, bulk)
Read-Write Community String	Yes
Read-Only Community String	Yes
SNMP traps	Yes
SNMP I/O access commands	Yes
Web server for configuration/access	Yes
Secure HTTP/XML/JSON access	Yes

4. Connectors, ports and led indicators

Bellow is shown a picture with the device connectors, ports and led indicators.

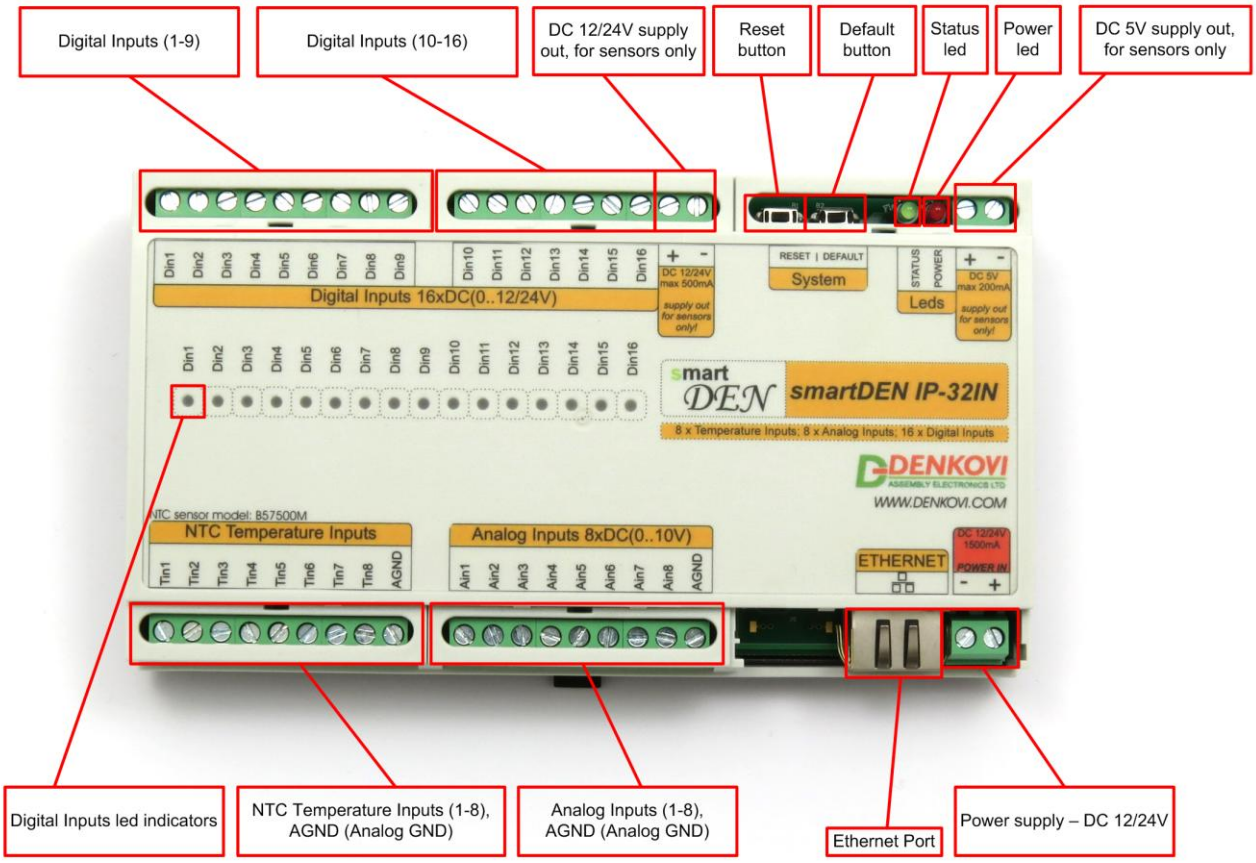


Figure 4. Device overview

5. Installation

- This device must be installed by qualified personnel;
- This device must not be installed directly outdoors;
- Installation consists of mounting the device, connecting to an IP network, connecting sensors, providing power and configuring via a web browser.

5.1. Box mounting

Figure 5. Mounting the device to DIN rail

SmartDEN IP-32IN can be mounted to a standard (35mm by 7.55mm) DIN rail. Attach the module to the DIN rail by hooking the hook on the back of the enclosure to the DIN rail and then snap the bottom hook into place.

5.2. Power supply

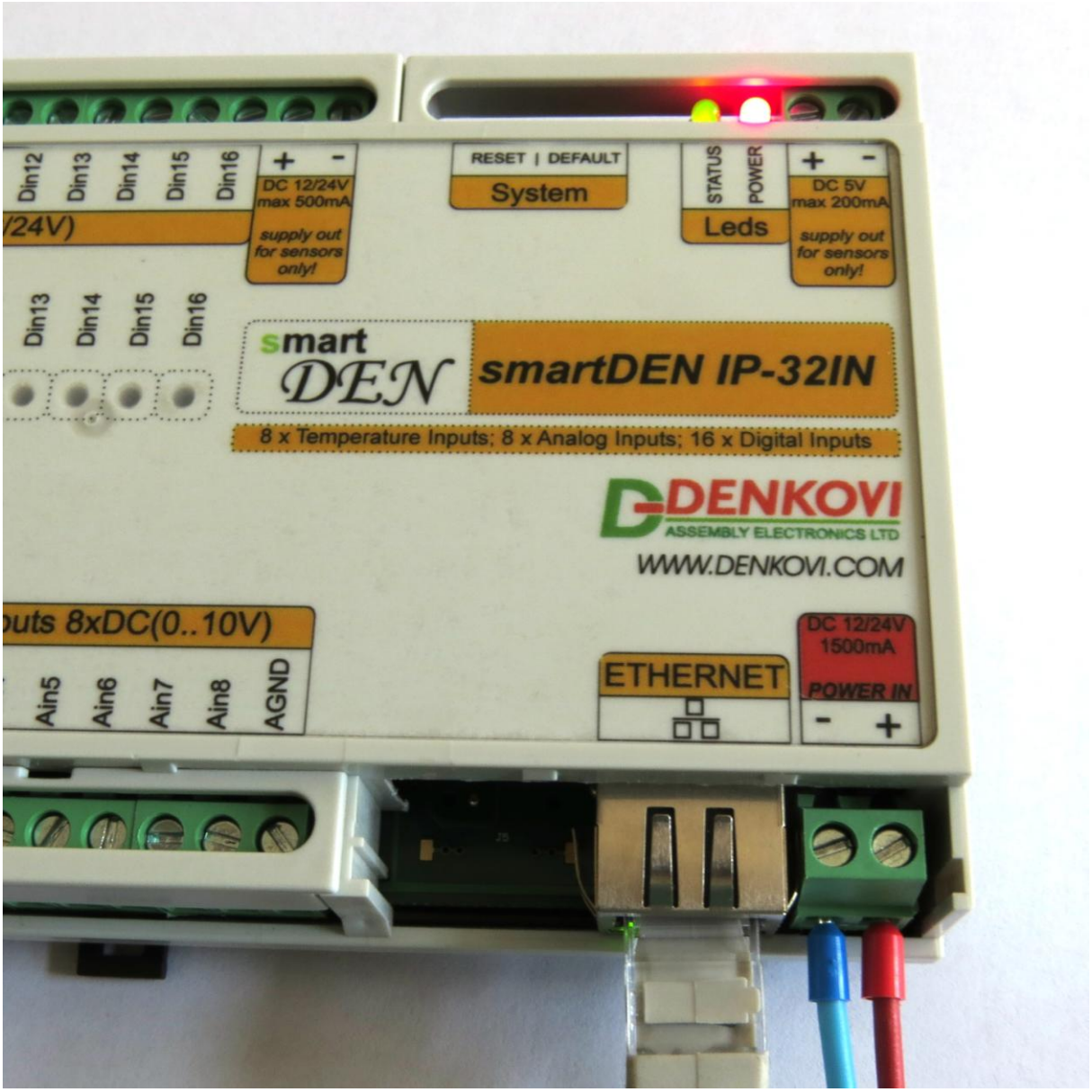


Figure 6. SmartDEN IP-32IN power supply

SmartDEN IP-32IN must be with voltage either **12VDC** or **24VDC** stabilized and filtered. After power on, the power led must be on and **STATUS indicator** must start blinking in 5 seconds which means the module is running normally.

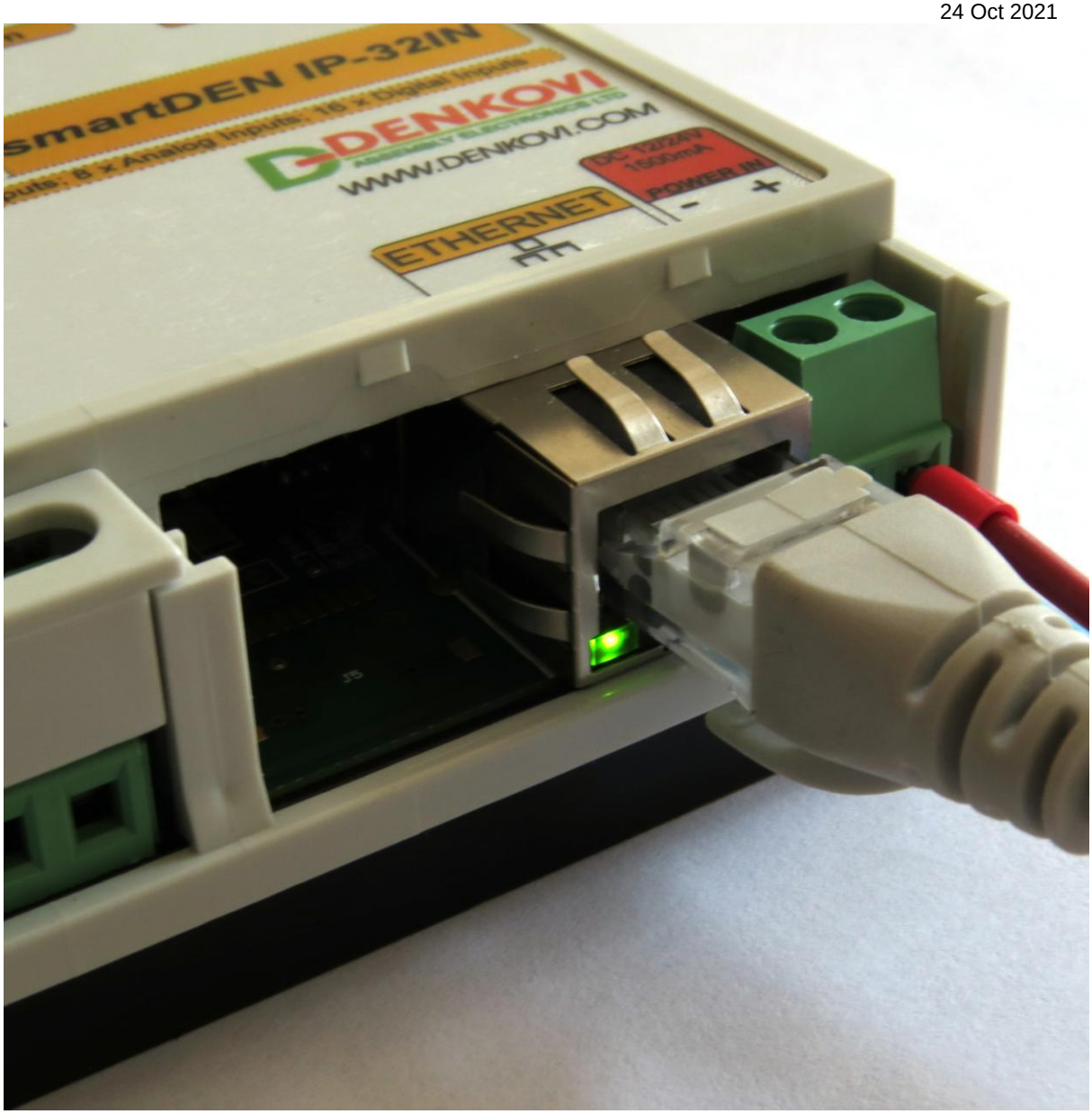


Figure 7. Connecting a LAN cable

- Please keep the polarity and supply voltage range!
- **SmartDEN IP-32IN** does not accept AC supply voltage. It is highly recommended to check the power supply source parameters before supply the module.
- The power supply equipment shall be resistant to short circuit and overload in secondary circuit.
- When in use, do not place the equipment so that it is difficult to disconnect the device from the power supply.

5.3. Connecting inputs

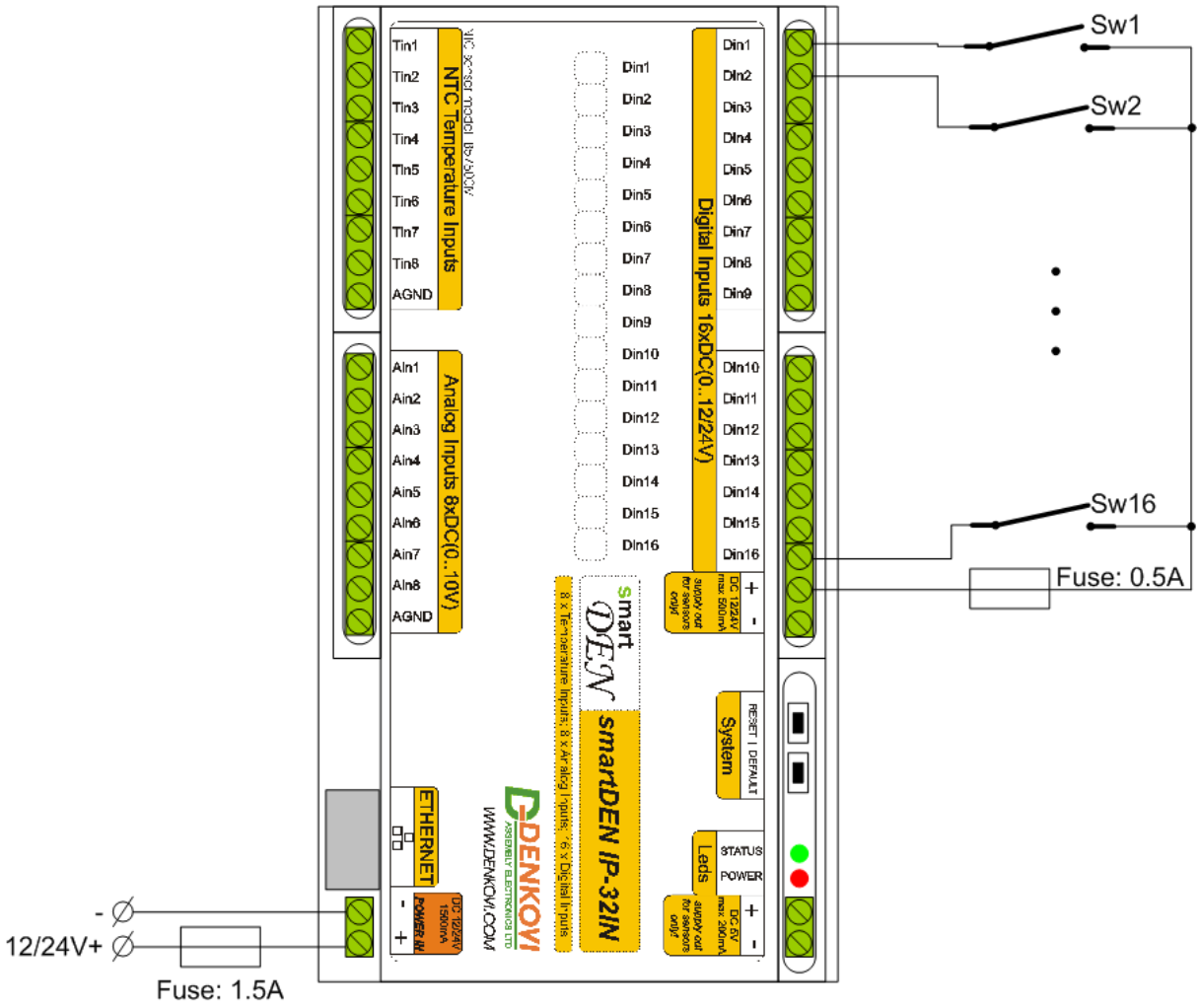


Figure 8. Connecting SPST NO output (dry contact) sensors, switches, buttons, door sensors and so on to the digital inputs.

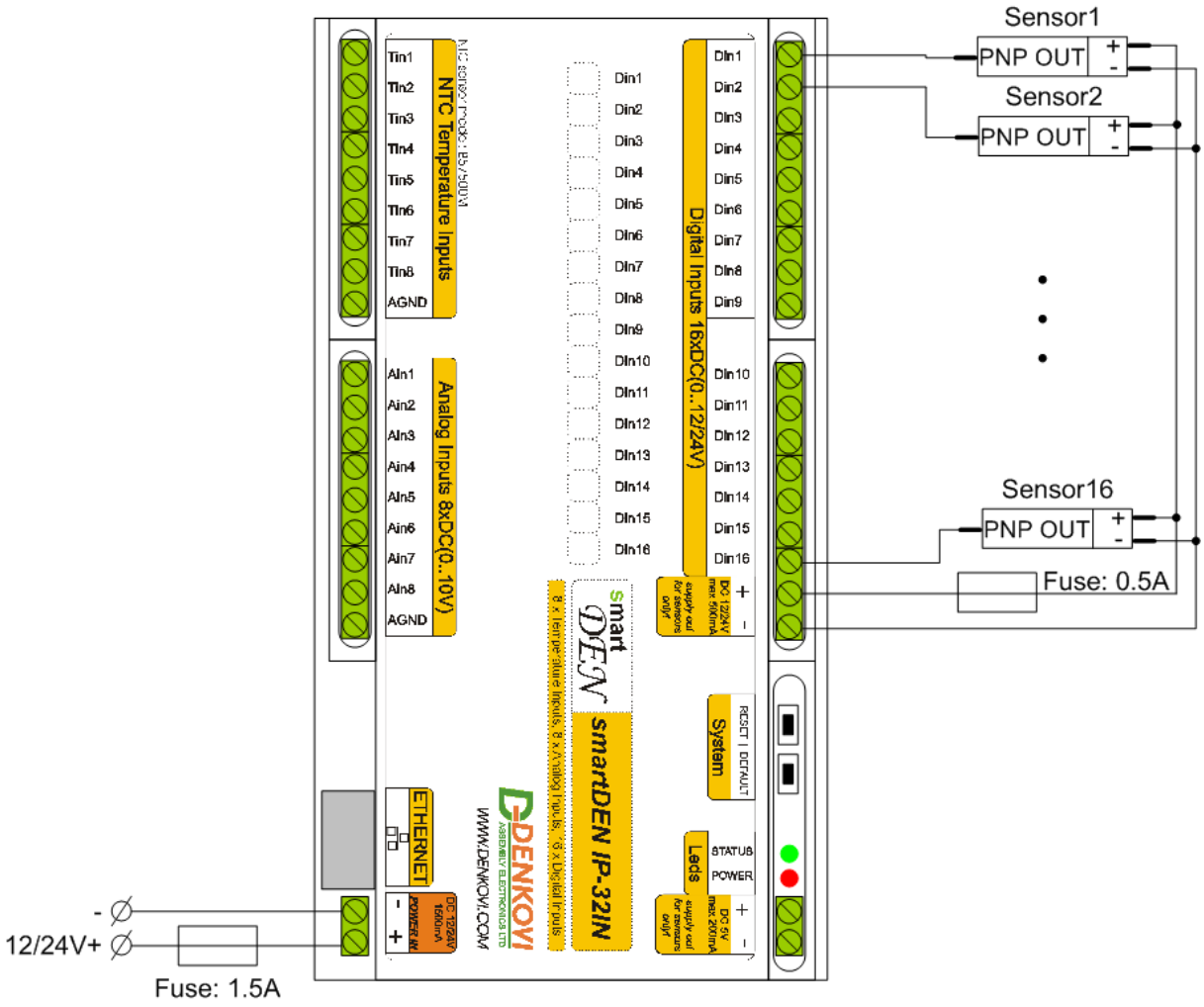


Figure 9. Connecting PNP output digital sensors requiring supply voltage 12/24V DC to the digital inputs.

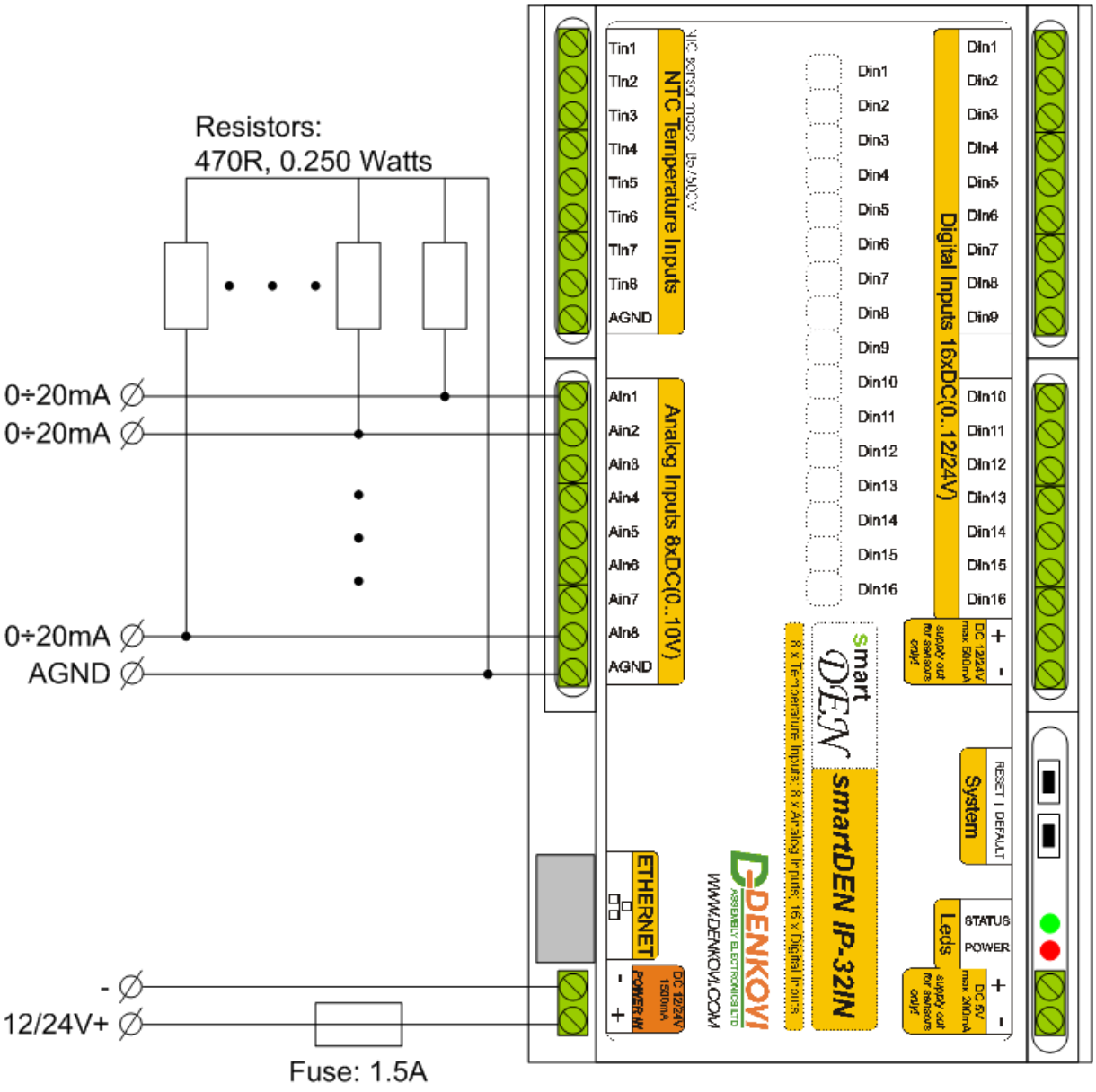


Figure 10. Connecting 0-20mA output analog sensors to the analog inputs.

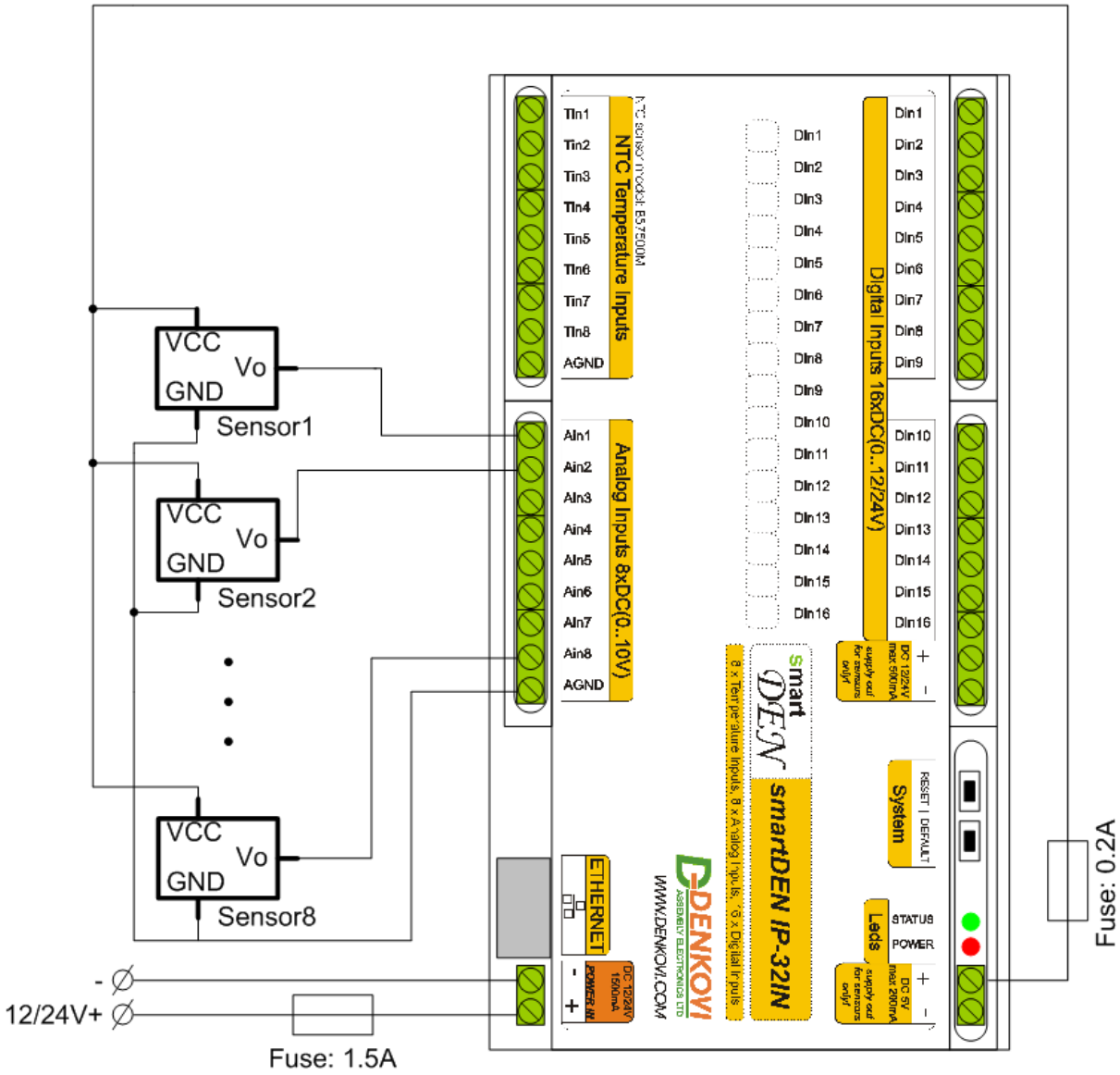


Figure 11. Connecting analog sensors with output from 0 up to 10V DC to the analog inputs requiring power supply voltage 5V DC.

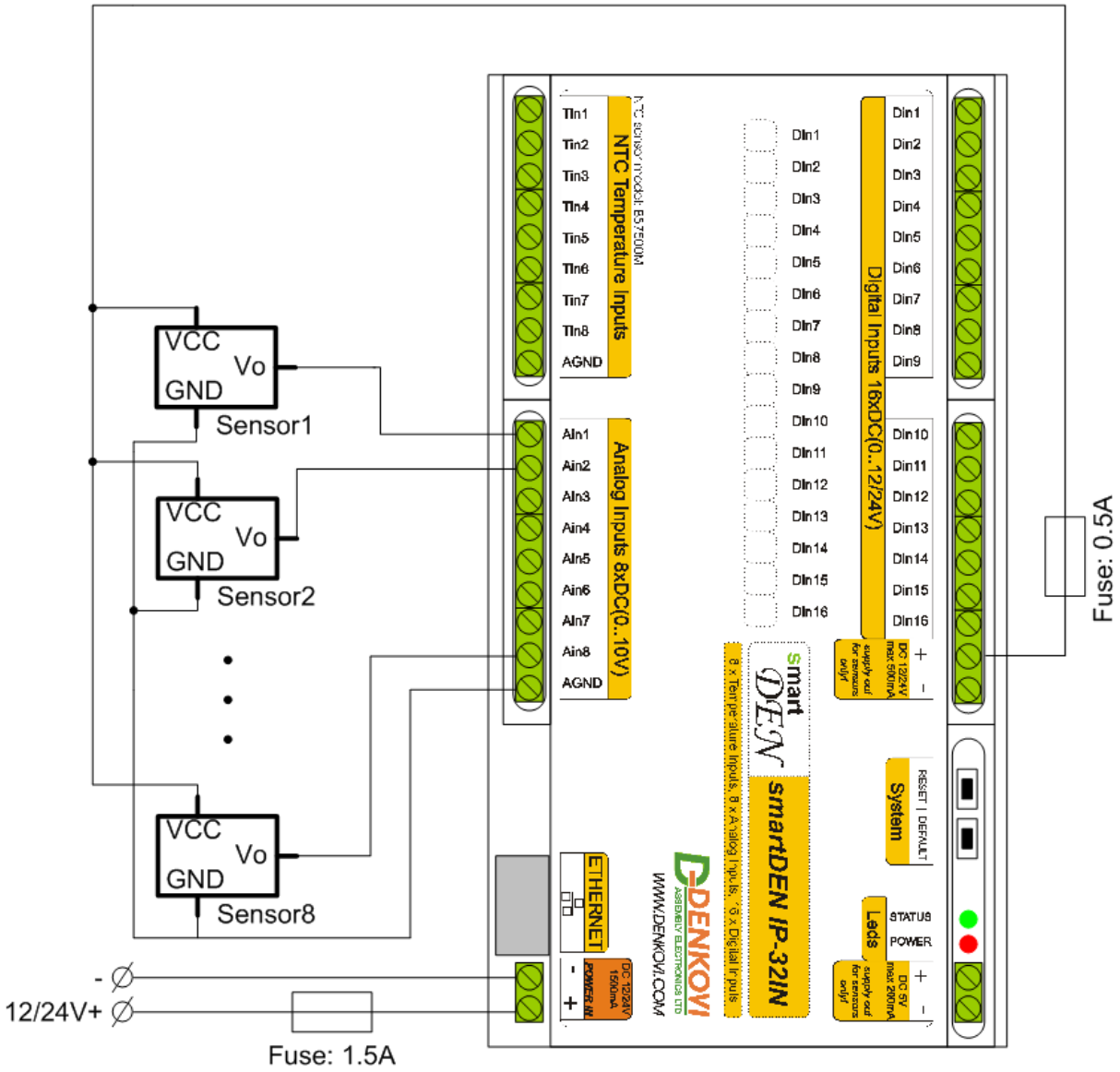


Figure 12. Connecting analog sensors with output from 0 up to 10V DC to the analog inputs requiring power supply voltage 12/24V DC.

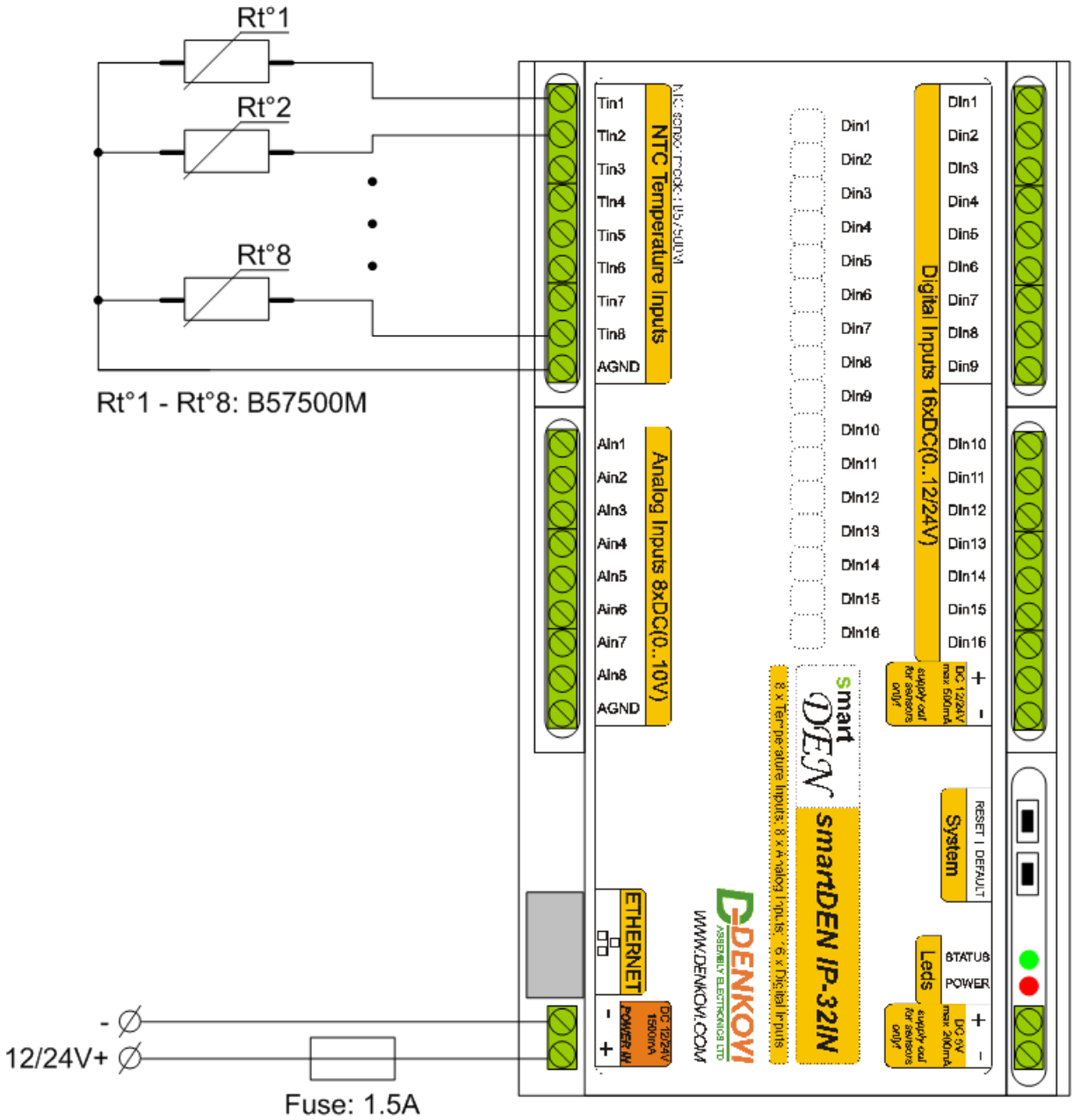


Figure 13. Connecting thermoresitor NTC sensors type B57500M to the analog inputs.

5.4. Network connection

SmartDEN IP-32IN supports AUTO-MDIX so either "crossover" or "straight-through" network cable can be used.

Figure 14. Connecting **SmartDEN IP-32IN** to a computer directly. This is the recommend initial connection

Figure 15. Connecting **SmartDEN IP-32IN** to a wireless router

5.5. Communication setup

SmartDEN IP-32IN is shipped with the following default parameters:

- IP address: **192.168.1.100**
- Subnet mask: **255.255.255.0**
- Gateway: **192.168.1.1**
- Web password: **admin**

Initially it is recommended to connect the module directly to the computer.

Next you have to change your PC's IP address.

You can google how to change you computer IP settings or just visit this web page: http://www.howtochangeipaddress.com/changeip.php

For Windows 7 OS for example you can do that in the following way:
Navigate to *Control Panel -> Network and Internet -> View network and status tasks -> Change adapter settings*

Then just select the local area connection with right click and select *Properties*:

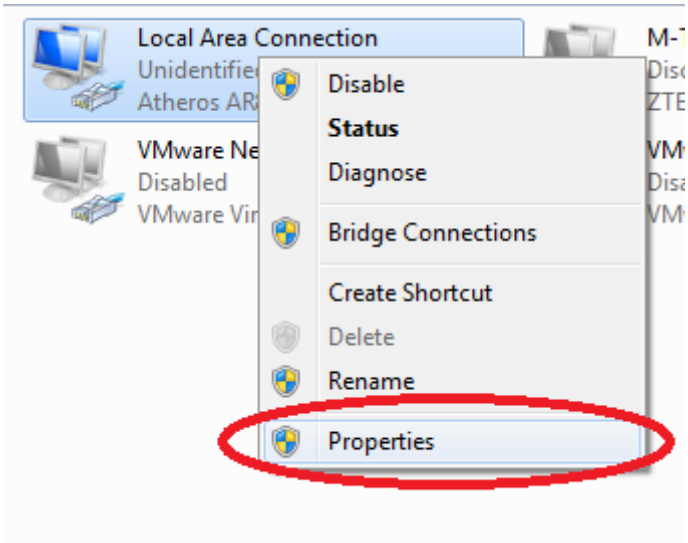


Figure 16. LAN card properties

The next step is to enter into IPv4 properties.

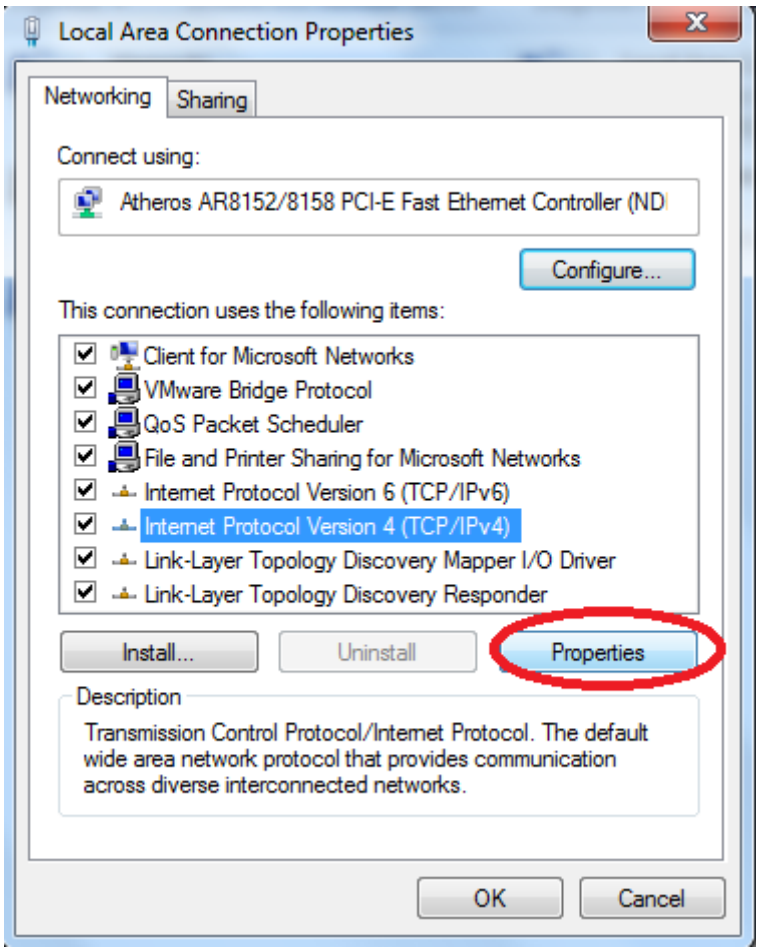


Figure 17. Enter in IPv4 properties section

Set the IP address of your PC to be in the same network.

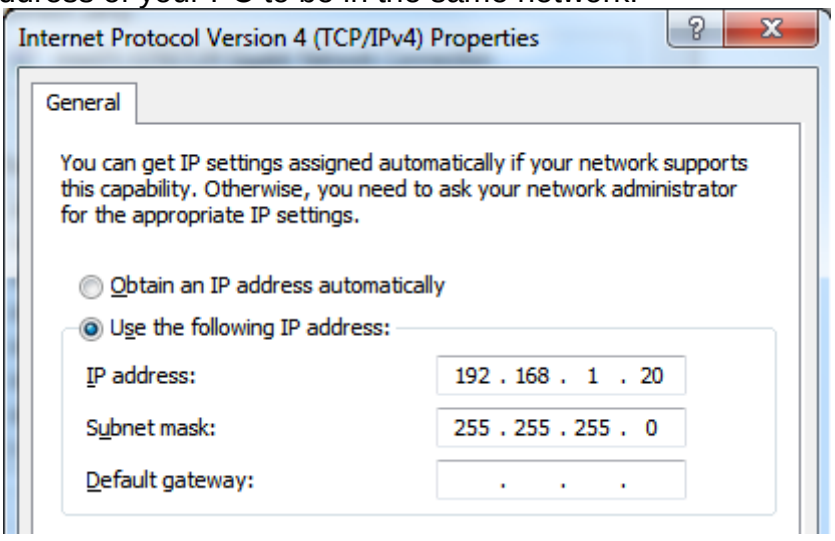


Figure 18. Set the IP address

Finally, in order to access **SmartDEN IP-32IN** just type in your browser 192.168.1.100

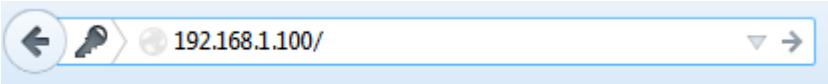


Figure 19. Open the device via browser

If the network settings are O'K, the log-in page should appear:

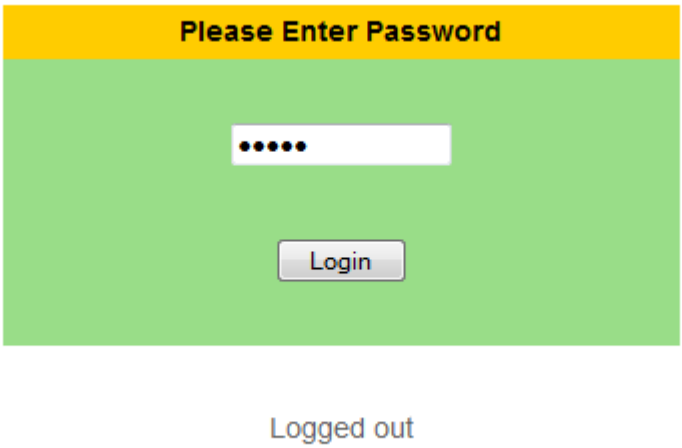


Figure 20. Login page

SmartDEN IP-32IN modules connected locally can be easily scanned and found via the tool ***Denkovi Finder*** as well.

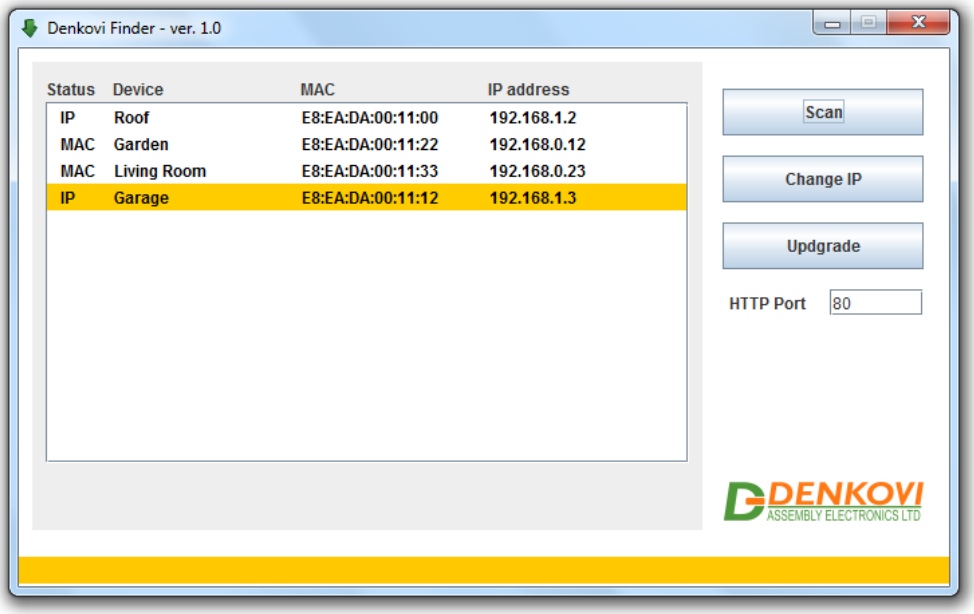


Figure 21. Denkovi Finder utility

6. Default settings

6.1. Table with default settings

The **SmartDEN IP-32IN** module is shipped with default (factory) settings shown in Table 2. The default settings can be reloaded, if necessary (see **point 6.2**).

Table 8. Default settings

Settings group	Parameter (according Web pages)	Value
General Settings	Device Name	SMARTDEN-IP-32IN
	Password	admin
	Temperature Scale	Celsius
	Analog Inputs Filter, sec	0
	Temperature Inputs Filter, sec	0
	Monitoring Timeout, sec	3
	Max. Monitoring Errors	5
Network Settings	DHCP	Disabled
	IP Address	192.168.1.100
	Gateway	192.168.1.1
	Subnet Mask	255.255.255.0
	Primary DNS	192.168.1.1
	Secondary DNS	0.0.0.0
HTTP/XML/JSON Settings	HTTP Port	80
	Access IP Address	192.168.1.0
	Access Mask	0.0.0.0
	Access MAC Address	00:00:00:00:00:00
	Session Timeout, min	3
	Enable Access	Enabled
	Encrypt Password	Disabled
	Multiple Access	Enabled
Data Logging Settings	Enable	Disabled
	HTTP Server Address / Path	0.0.0.0/current_state.xml
	Server Port	80
	Logging Period, sec	5
	Server Response Timeout, sec	2
Remote Relay Control	Enable	Disabled
	Remote Board Type	smartDEN IP-16R

	Remote Board Address	0.0.0.0
	Remote Board Port	80
	Remote Board Password	
	Remote Board Response Timeout, sec	2
SNMP Agent	Enable SNMP	Enabled
	SNMP Port	161
	Read-only Community1	public
	Read-only Community2	read
	Read-write Community1	private
	Read-write Community2	write
SNMP Traps	Enable Trap	Disabled
	Trap Receiver IP Address	0.0.0.0
	Trap Receiver Port	162
	Trap Community	
	Trap Sending	Level Triggered
Digital Inputs	Description	DI<n>, where <n> = 1..16
	Counter	0
	Filter (ms)	0
	SNMP Trap	Disabled
	SNMP Trap Value	0 (Off)
	Remote Relay Control	Disabled
	Remote Relay Mode	Normal
Analog Inputs	Description	AI<n>, where <n> = 1..8
	Min	0.0
	Max	10.0
	Label	Volt
	Low Threshold	0
	High Threshold	0
	SNMP Trap	Disabled
	Remote Relay Control	Disabled
	Remote Relay Mode	Normal
Temperature Inputs	Description	TI<n>, where <n> = 1..8
	Tolerance, %	0
	Low Threshold	0
	High Threshold	0
	SNMP Trap	Disabled
	Remote Relay Control	Disabled

	Remote Relay Mode	Normal

6.2. Steps for loading default settings

When necessary, the factory (default settings) may be applied so the module parameters will be returned back as those in **point 6.1** from the current document.

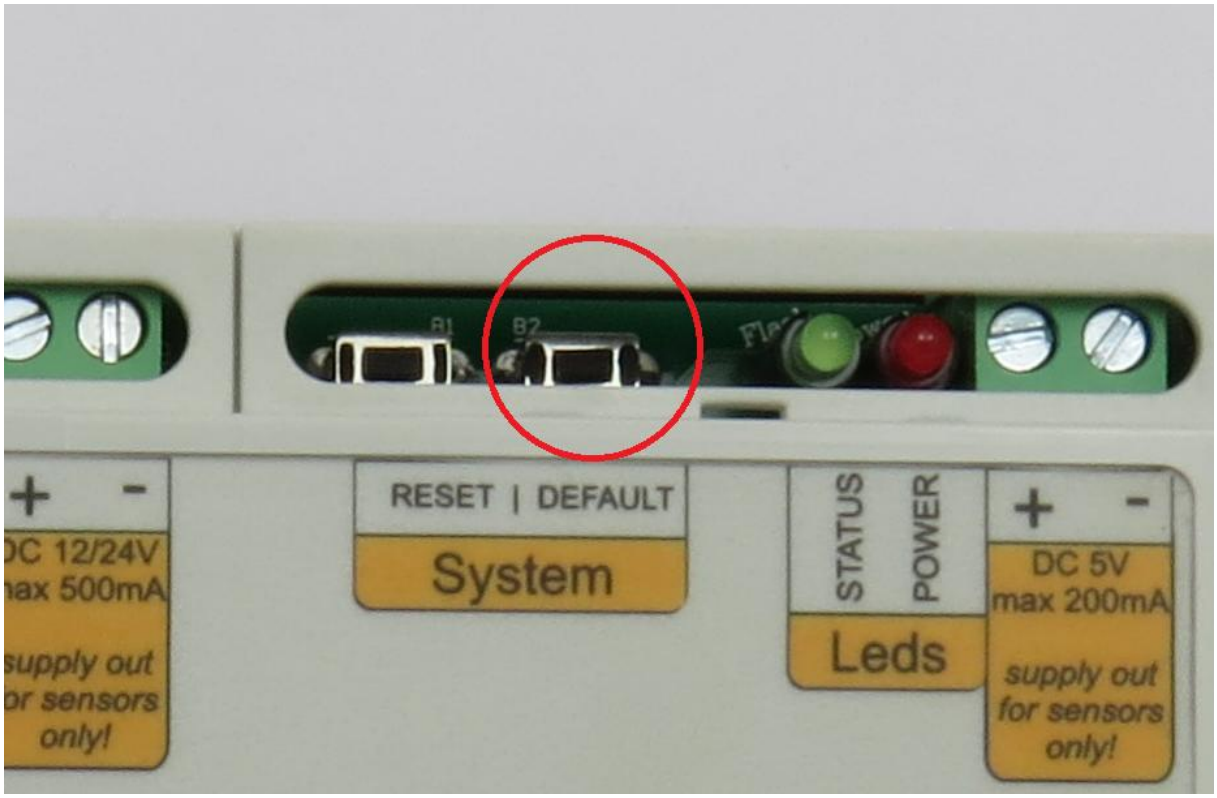


Figure 22. Loading the default settings

1. Turn off the power supply of the device;
2. Press and hold the default button;
3. Turn on the power supply of the device;
4. Wait for until STATUS led indicator become ON (approximately after 10 sec);
5. Release the default button;
6. The module is configured with default settings.

7. Web access

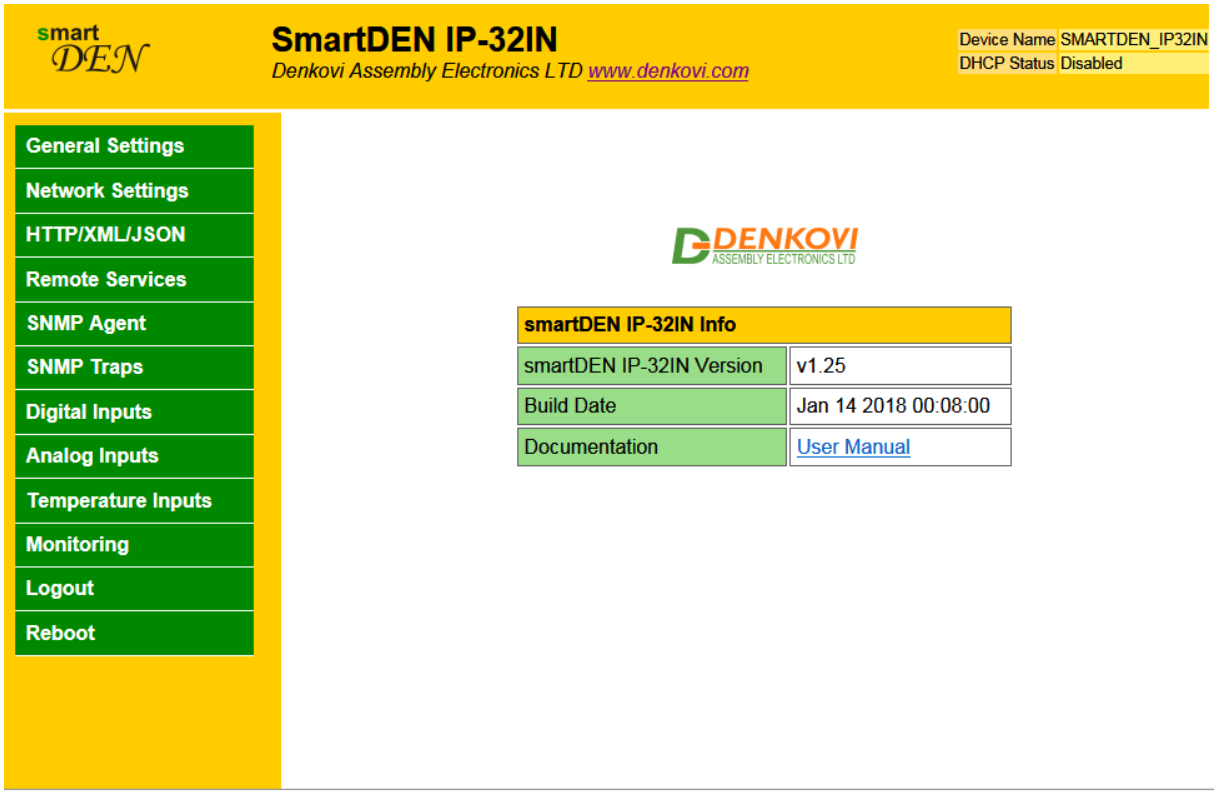


Figure 23. Web access

To access the setup pages, run a web browser (Internet Explorer, Mozilla Firefox or similar), and enter the **SmartDEN IP-32IN** IP address, for example: http://192.168.1.100

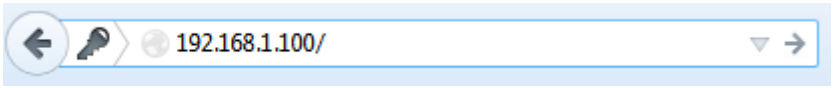


Figure 24. Open via browser

Note: You will need to have JavaScript enabled in your browser.

7.1. Login

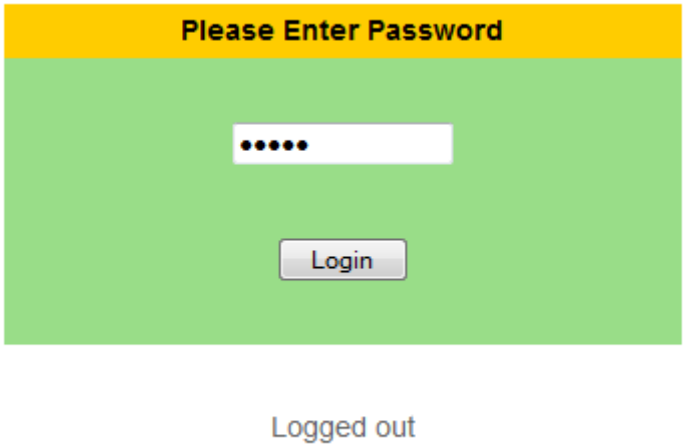


Figure 25. Login page

Enter the password and click "Login" button. This will bring you to the **SmartDEN IP-32IN** main configuration page which contains details for the current firmware version and build date and provides buttons and links to obtain further details.

Note: The default password is admin (passwords are case sensitive).

Note: When the password is entered, it is transmitted across the network in encrypted form, so eavesdropping on the data transmission will not reveal the password.

Note: In order to prevent setup/control conflicts, at any given moment, only one user can be logged in.

Note: If there is no data traffic between the Web-browser and the **SmartDEN IP-32IN** for time, specified by ***Session Timeout*** parameter, the session "times out" and a new login is required.

7.2. Menu

The main menu consists of the following items, located in the left window frame:

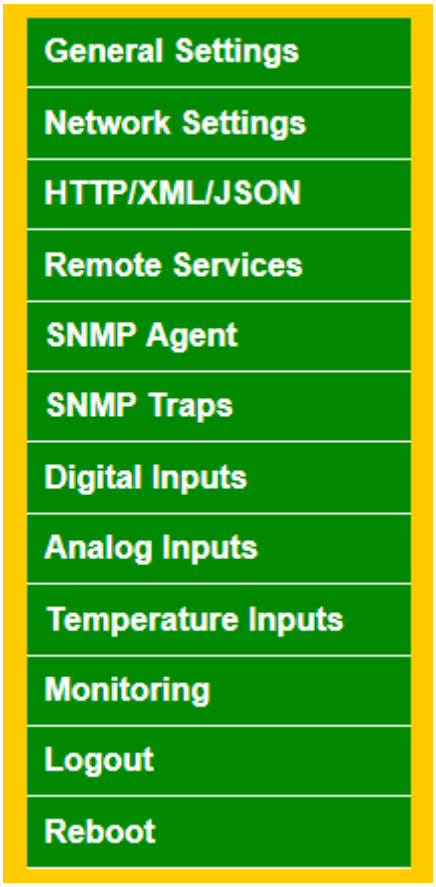


Figure 26. Navigation menu

7.3. General settings

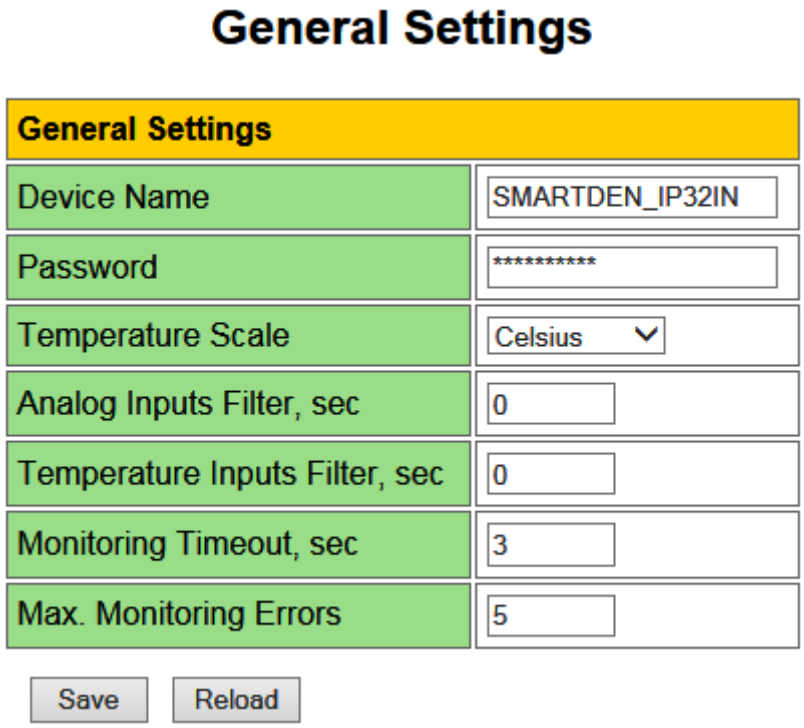


Figure 27. General settings

- **Device Name** - the name of the module (max 15 symbols). Every module can have different name in your network so they can be distinguished;
- **Password** - the password used for logging into the web admin and XML operation (max. 10 chars);

When typed, the password in this screen is not hidden. Only in this case, when the password is being changed, it is transmitted across the network "in the open". Therefore, set passwords in a secure environment where you can make sure that no one is "eavesdropping". Subsequent transmissions of the password to "login" onto the device are encrypted and "safe".

- **Temperature Scale** – Celsius / Fahrenheit;
- **Analog Inputs Filter, sec** – Analog Inputs filter constant (0 to 30 sec), 0 disables filtering;
- **Temperature Inputs Filter, sec** – Temperature Inputs filter constant (0 to 30 sec), 0 disables filtering;
- **Monitoring Timeout, sec** - the connection timeout for the Web-browser;
- **Max. Monitoring Errors** – the number of successive timeouts before the connection error is reported by the Web-browser;
- **Save button -** once you have changed the settings as required, click this button.

7.4. Network settings

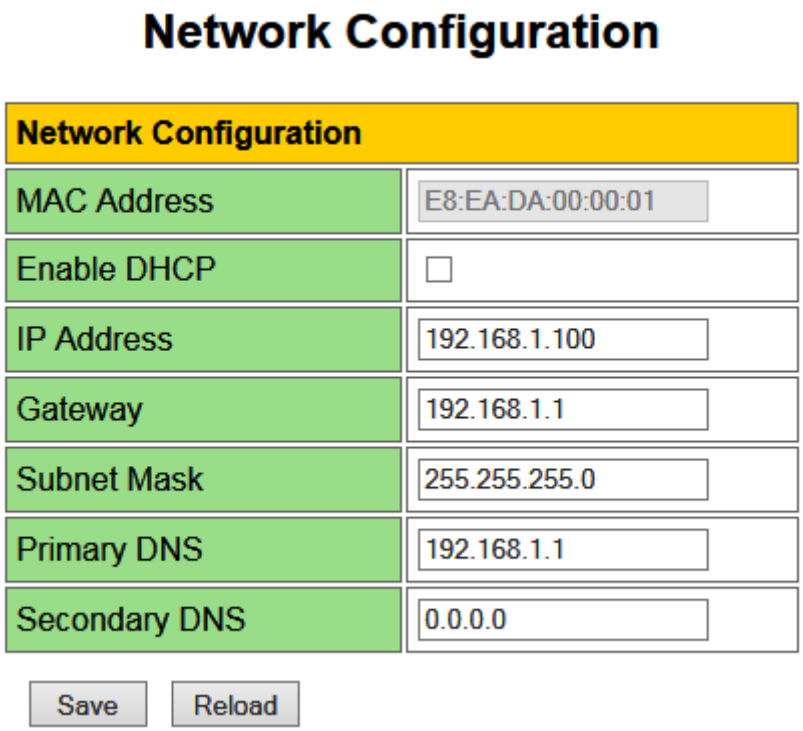


Figure 28. Network settings

This menu lets you configure the network settings of **SmartDEN IP-32IN** input module:

- **Enable DHCP** - this option allows DHCP to be enabled or disabled. If DHCP is set to Enabled, the Network page must be saved and **SmartDEN IP-32IN** must be rebooted before obtaining an IP address;
- **IP address** - this is the IP address of the **SmartDEN IP-32IN**. It needs to be manually assigned only if DHCP is disabled. With DHCP enabled, this field displays the currently assigned address;
- **Gateway** - this specifies the IP address of the gateway router. It is used for accessing public time servers for automatic time synchronization;
- **Subnet Mask** - this is the subnet mask for the network on which the **SmartDEN IP-32IN** is installed;
- **Primary DNS** - primary DNS (Domain Name Service) address;
- **Secondary DNS** - secondary DNS address;
- **Save button** - once you have changed the settings as required, click this button.

You have to reboot the device for these settings to apply.

7.5. HTTP/XML/JSON

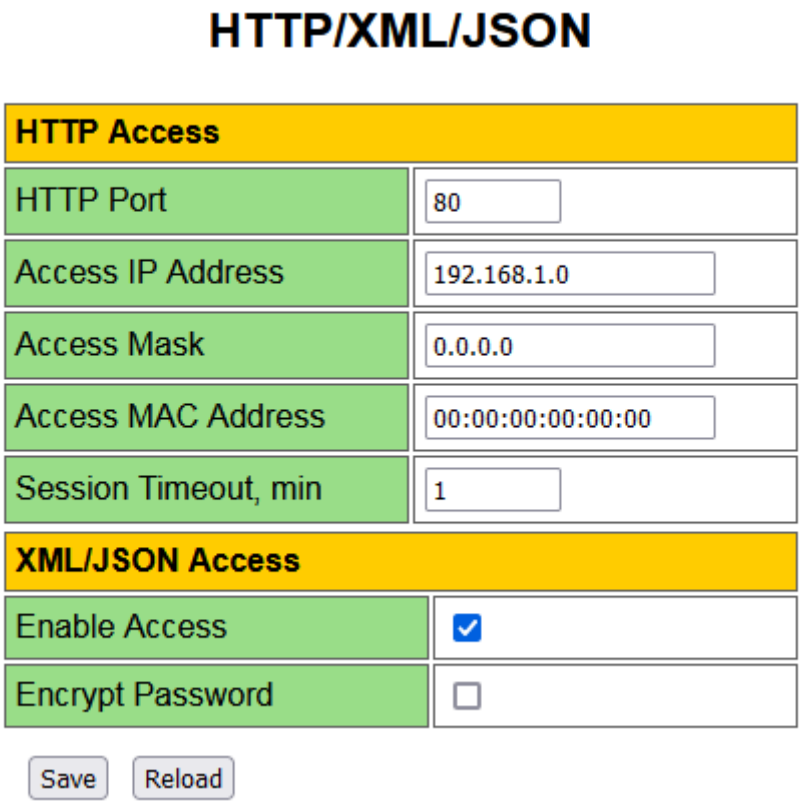


Figure 29. HTTP/XML/JSON access

These settings let you configure the HTTP and XML/JSON access parameters of **SmartDEN IP-32IN:**

- **HTTP Port** - port that the Web server listens for HTTP requests (default port is 80). You have to reboot the device for a new port setting to apply;
- **Access IP Address/Access Mask** - these fields can be used to restrict the HTTP/XML/JSON access by specifying the IP address and subnet mask of the HTTP client;
- **Access MAC Address** - this field can be used to restrict the HTTP/XML/JSON access by specifying the MAC address of the HTTP client;
- **Session Timeout, min** - Specifies the timeout period for HTTP and XML/JSON sessions in minutes;
- **Enable Access** - this option enables or disables XML/JSON access to the **SmartDEN IP-32IN**;
- **Encrypt Password** - when XML/JSON access is enabled, this option adds additional security level by encrypting the login password;
- **Save button** - once you have changed the settings as required, click this button.

You have to reboot the device for these settings to apply.

It is highly recommended to log out from the web server after finishing the parameters setup.

If you don't want to restrict the HTTP/XML/JSON access by IP address, set the **Access Mask** to 0.0.0.0.

If you don't want to restrict the HTTP/XML/JSON access by MAC address, set the MAC **Address** to 00:00:00:00:00:00.

Setting the **Access Mask** to 255.255.255.255 allows the HTTP/XML/JSON access only from the exactly specified **Access IP Address**.

You can allow the HTTP/XML/JSON access to a range of IP addresses by setting an appropriate value for **Access Mask**. For example setting the **Access IP Address** to 192.168.1.0 and **Access Mask** to 255.255.255.0 allows the access from IP addresses in range from 192.168.1.0 to 192.168.1.255.

7.6. Remote services

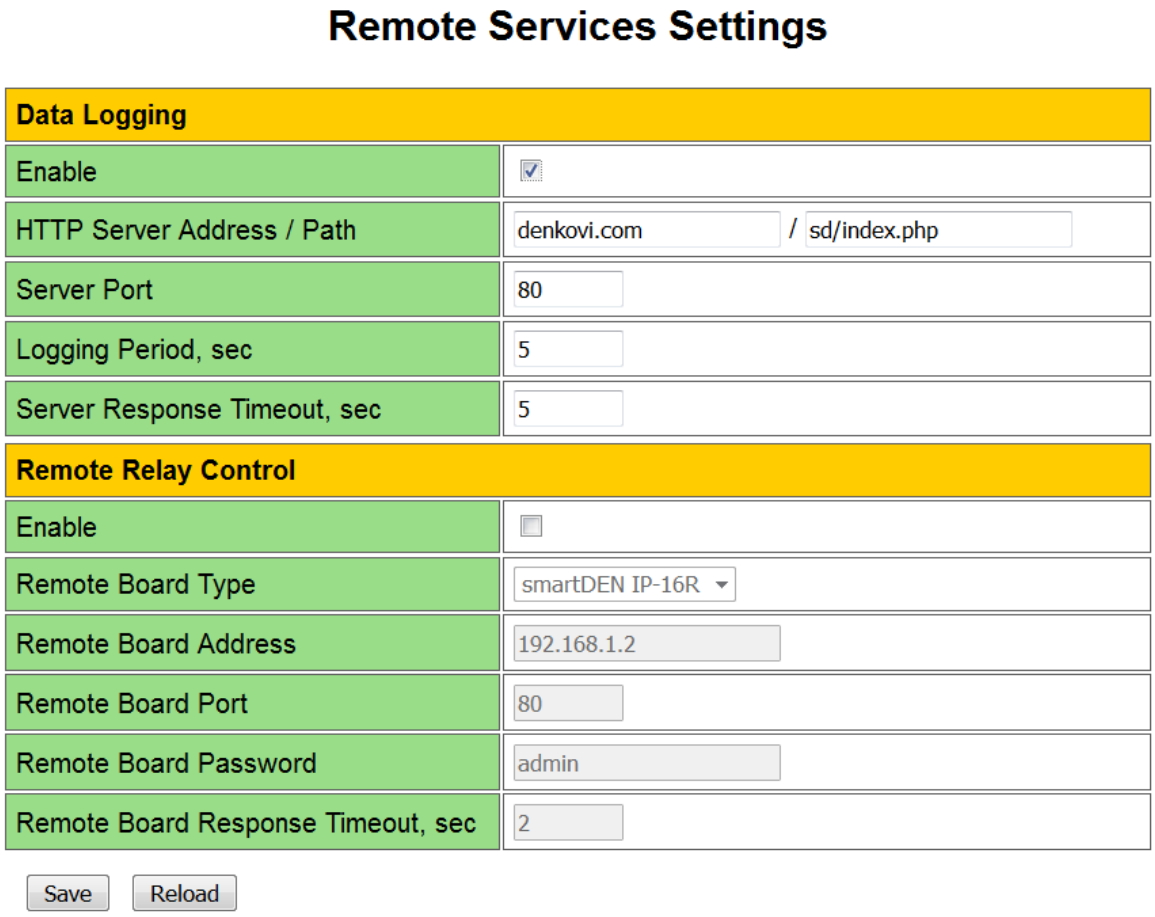


Figure 30. Remote services

SmartDEN IP-32IN supports sending HTTP GET/POST messages based on particular input events or periodically. This is so called "Remote Services" mode. In this mode the **SmartDEN IP-32IN** works as client and it sends messages to the server. From this page all the settings regarding this mode can be set. There are two modes available:

- **Data Logging** - in this mode the HTTP server is located on some remote machine and it must process the XML file containing the input values sent via POST request by the **SmartDEN IP-32IN** module. Parameters are:
  - **Enable** - activate this mode;
  - **HTTP Server Address** - the remote HTTP server IP address or domain name (max 22 chars);
  - **HTTP Server Path** - the remote path after the HTTP Server Address (max 22 chars);
  - **Server Port** - the remote HTTP server listening port;
  - **Logging period, sec** - the time interval in seconds between two sequential POST requests during the logging (from 1 to 250 seconds);
  - **Server Response Timeout, sec** - the timeout for the server response (from 1 to 250 seconds).

The timeout period must be less than the logging period!

- **Remote Relay Control** - In this mode the **SmartDEN IP-32IN** controls via HTTP GET request remote relays, located at our relay boards or IP controllers through the LAN network (or Internet). Parameters are:
  - **Enable** - activate this mode;
  - **Remote Board Type** - it can be: DAEnetIP3 and all *denkovi* devices based on this IP controller, DAEnetIP4 and all *denkovi* devices based on this IP controller, Wi-Fi Relays, and smartDEN relay modules;
  - **Remote Board Address** - the IP address or domain name of the remote board;
  - **Remote Board Port** - the remote board HTTP listening port;
  - **Remote Board Password** - the password for the remote board (max 10 chars);
  - **Remote Board Response Timeout, sec** - the timeout for the remote board response (from 1 to 250 seconds).

Please note the module can work only in one of the both modes at one moment!

7.7. SNMP agent

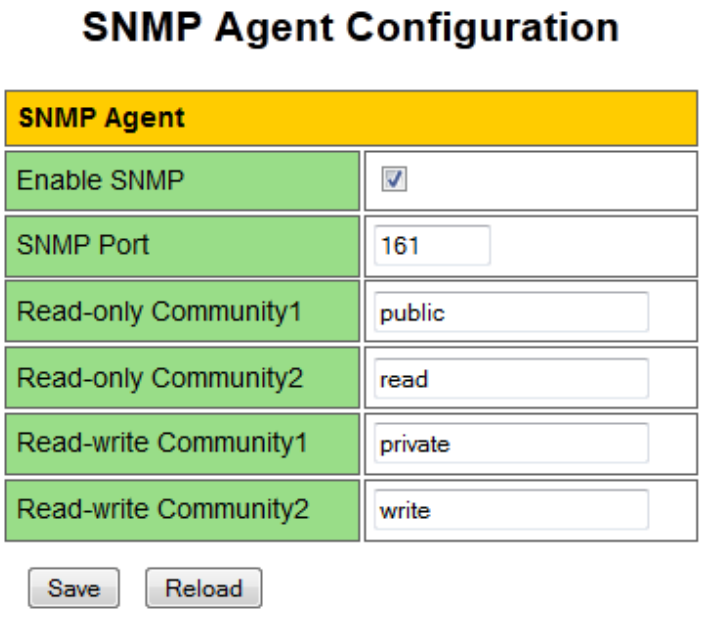


Figure 31. SNMP settings

These settings let you configure the SNMP (Simple Network Management Protocol) access to the **SmartDEN IP-32IN:**

- **Enable SNMP -** This option enables or disables SNMP access to the **SmartDEN IP-32IN**;

- **SNMP Port -** UDP port number the SNMP agent receives requests on (default port is 161);
- **Read-only Community1/2 -** Community string for client's authentication, used in read operations;
- **Read-write Community1/2 -** Community string for client's authentication, used in read/write operations.
- **Save button -** Once you have changed the settings as required, click this button.

You have to reboot the device for these settings to apply.

7.8. SNMP traps

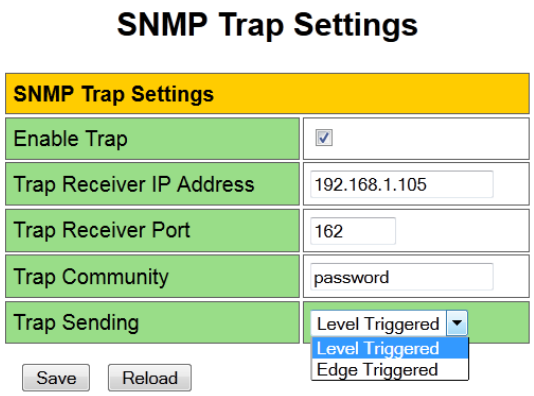


Figure 32. SNMP trap settings

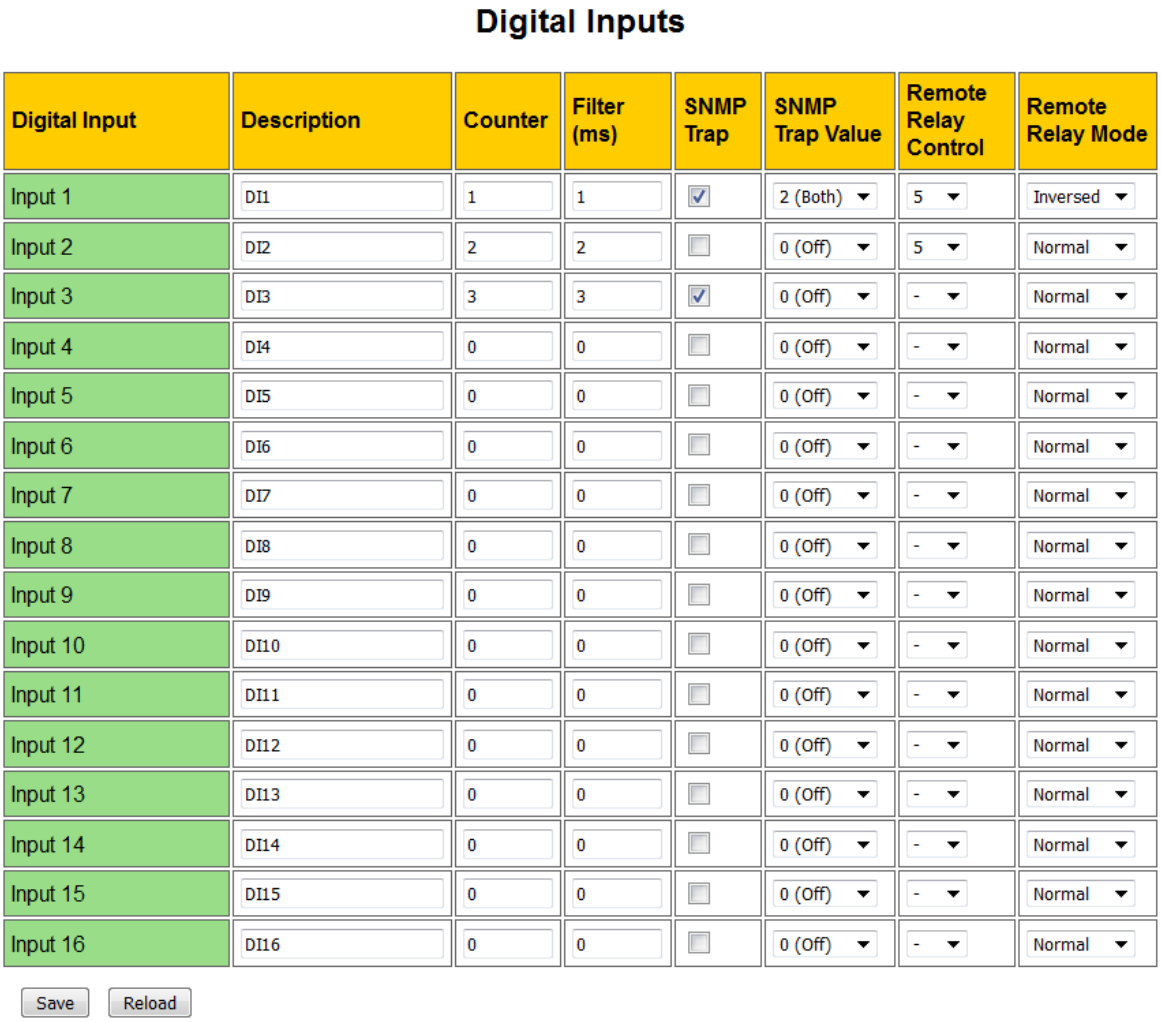
SmartDEN IP-32IN can send SNMP traps upon input event (detected by a Digital and/or Analog Input) to a Trap server and its parameters can be set from this web page:

- **Enable Trap** - global parameter that enables or disables sending traps to the server;
- **Trap Receiver IP Address** - the IP address of the trap server;
- **Trap Receiver Port** - determines the UDP port the trap message will be sent to;
- **Trap Community** - the trap community;
- **Trap Sending** - determines how the traps will be sent:
  - **Level Triggered** - the trap message will be sent every 5 seconds when the input is in position to generate traps. This is because the SNMP traps are UDP messages and UDP protocol does not guarantee that the packet will be received at all.
  - **Edge Triggered** - the trap message will be sent upon input event only once.

  Save button - once you have changed the settings as required, click this button.

If the traps are enabled, on boot so called "cold start" message is send indicating **SmartDEN IP-32IN** is started.

7.9. Digital Inputs



Digital Inputs

Digital Input	Description	Counter	Filter (ms)	SNMP Trap	SNMP Trap Value	Remote Relay Control	Remote Relay Mode
Input 1	DI1	1	1	☑	2 (Both)	5	Inversed
Input 2	DI2	2	2	☐	0 (Off)	5	Normal
Input 3	DI3	3	3	☑	0 (Off)	-	Normal
Input 4	DI4	0	0	☐	0 (Off)	-	Normal
Input 5	DI5	0	0	☐	0 (Off)	-	Normal
Input 6	DI6	0	0	☐	0 (Off)	-	Normal
Input 7	DI7	0	0	☐	0 (Off)	-	Normal
Input 8	DI8	0	0	☐	0 (Off)	-	Normal
Input 9	DI9	0	0	☐	0 (Off)	-	Normal
Input 10	DI10	0	0	☐	0 (Off)	-	Normal
Input 11	DI11	0	0	☐	0 (Off)	-	Normal
Input 12	DI12	0	0	☐	0 (Off)	-	Normal
Input 13	DI13	0	0	☐	0 (Off)	-	Normal
Input 14	DI14	0	0	☐	0 (Off)	-	Normal
Input 15	DI15	0	0	☐	0 (Off)	-	Normal
Input 16	DI16	0	0	☐	0 (Off)	-	Normal

Save Reload

Figure 33. Digital Inputs settings

- **Description** - digital input identification string (max 7 chars);
- **Counter** - every digital input works as a 16 bit software counter as well. The counter is incremented at rising, falling, or both edges depending on the **SNMP Trap Value** parameter. The counter is cyclic and it can be set or cleared by the user anytime via this parameter. The values which can be for this parameters are from 0 up to 65535;

The counters are software and not hardware. Due to this there are some considerations which must be taken in mind when work with them:

- In case of 0 ms for **Filter** and no requests are sent to the controller (no SNMP, no HTTP, logged out from web server) but just counting pulses, it is possible to achieve frequency about 10Hz or this is 50ms ON and 50ms OFF. This is the recommend state for counting pulses;
- In case of 0 ms for **Filter** but there is active web session in web server and the monitoring page is opened, then it is possible to

count pulses with frequency about 1Hz or this is 500ms ON and 500ms OFF;

- In case the controller is working with the EEPROM in that moment it is not possible to count pulses due to the blocking time which may be several seconds. This state is not suitable for counting pulses but only for adjustments!

- **Filter (ms)** - the input may be adjusted to work with a digital filter. It is valid for the input visualization, counting, SNMP traps and controlling the outputs as well. This parameter sets the time (in milliseconds) for this filter and it can be from 0 up to 200 ms;
- **SNMP Trap** - determines if the Digital Input will send traps or not;
- **SNMP Trap Value** - this parameter determines how the traps will be sent and how counter will work:
  - *0 (Off)* - If the parameter **Trap Sending** is set with value "Level Triggered" then the trap message is sent when the Digital Input is in low level (0) every 5 seconds. If the parameter **Trap Sending** is set with value "Edge Triggered" then the trap message is sent when the Digital Input's is falling edge (1->0); In this mode the counter will be increased when the Digital Input value transits from 1 to 0.

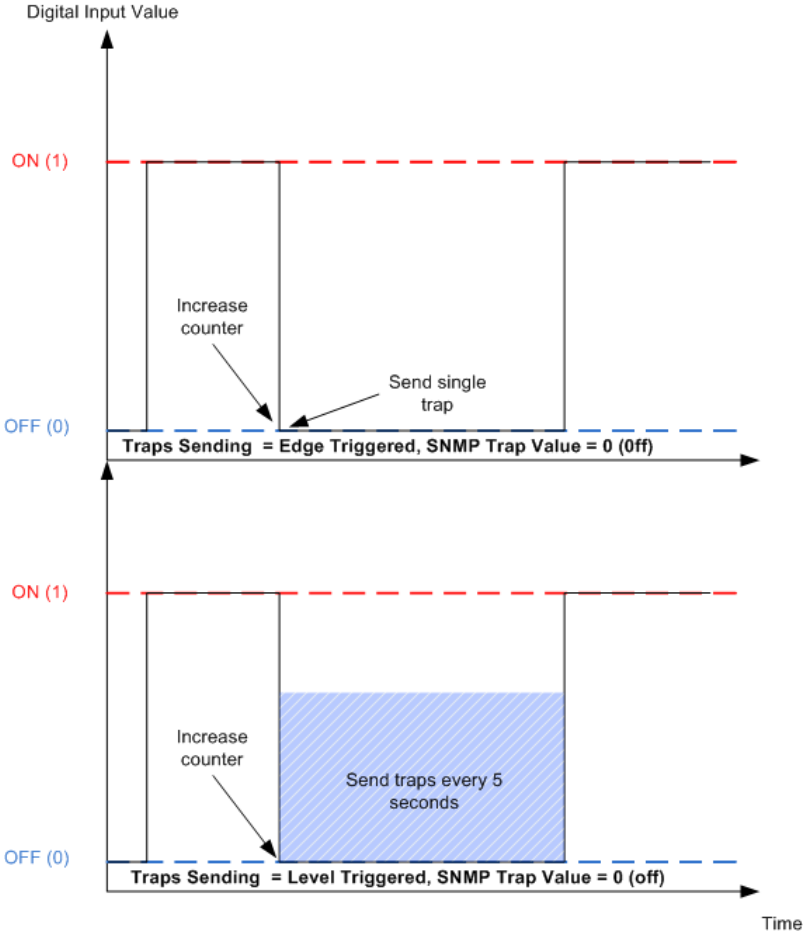


Figure 34. Traps and counter when SNMP Trap Value is "0 (off)"

  - *1 (On)* - If the parameter **Trap Sending** is set with value "Level Triggered" then the trap message is sent when the Digital Input is in high level (1)

every 5 seconds. If the parameter **Trap Sending** is set with value "Edge Triggered" then the trap message is sent during the Digital Input's rising edge (0->1); In this mode the counter will be increased when the Digital Input value transits from 0 to 1.

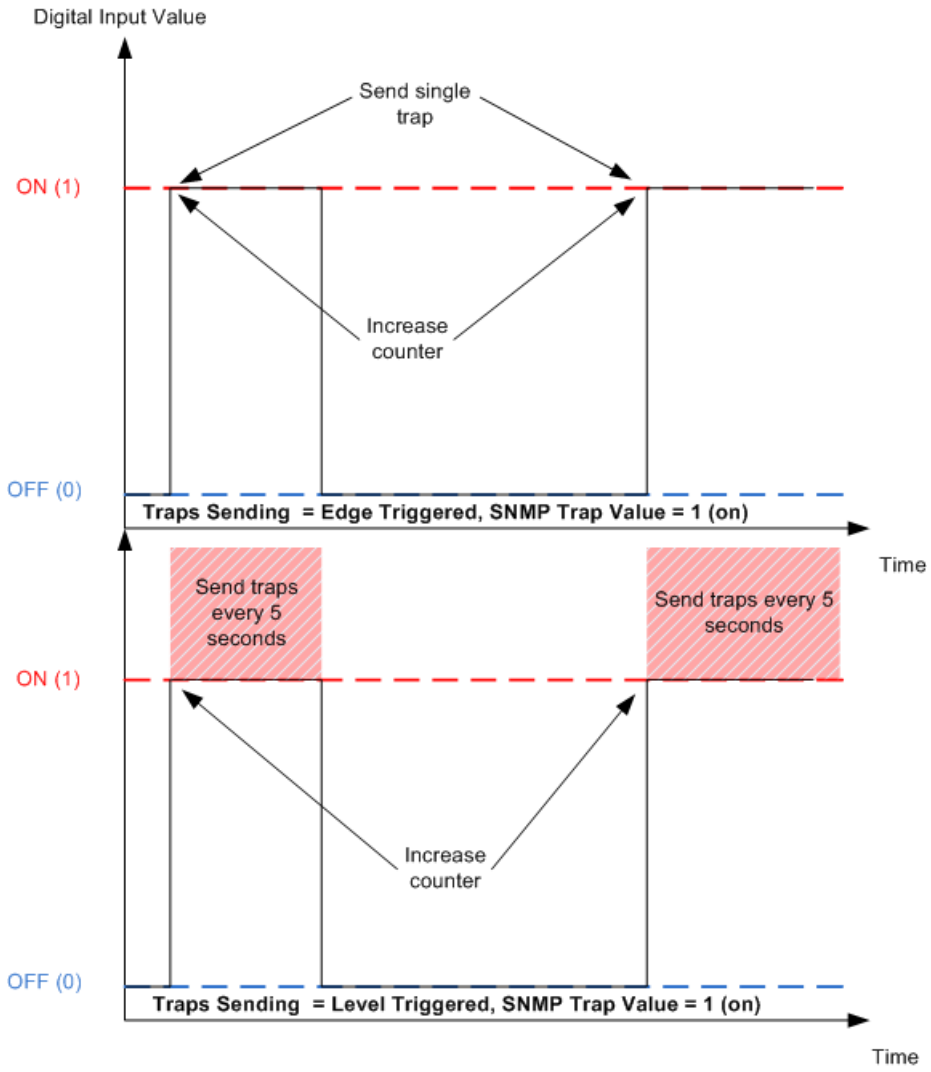


Figure 35. Traps and counter when SNMP Trap Value is "1 (on)"

- 2 (Both) - If the parameter **Trap Sending** is set with value "Level Triggered" then the trap message is sent constantly every 5 seconds. If the parameter **Trap Sending** is set with value "Edge Triggered" then the trap message is sent every time when the Input changes its state (falling and rising edge). In this mode the counter will be increased when the Digital Input value transits from 1 to 0 and from 0 to 1.

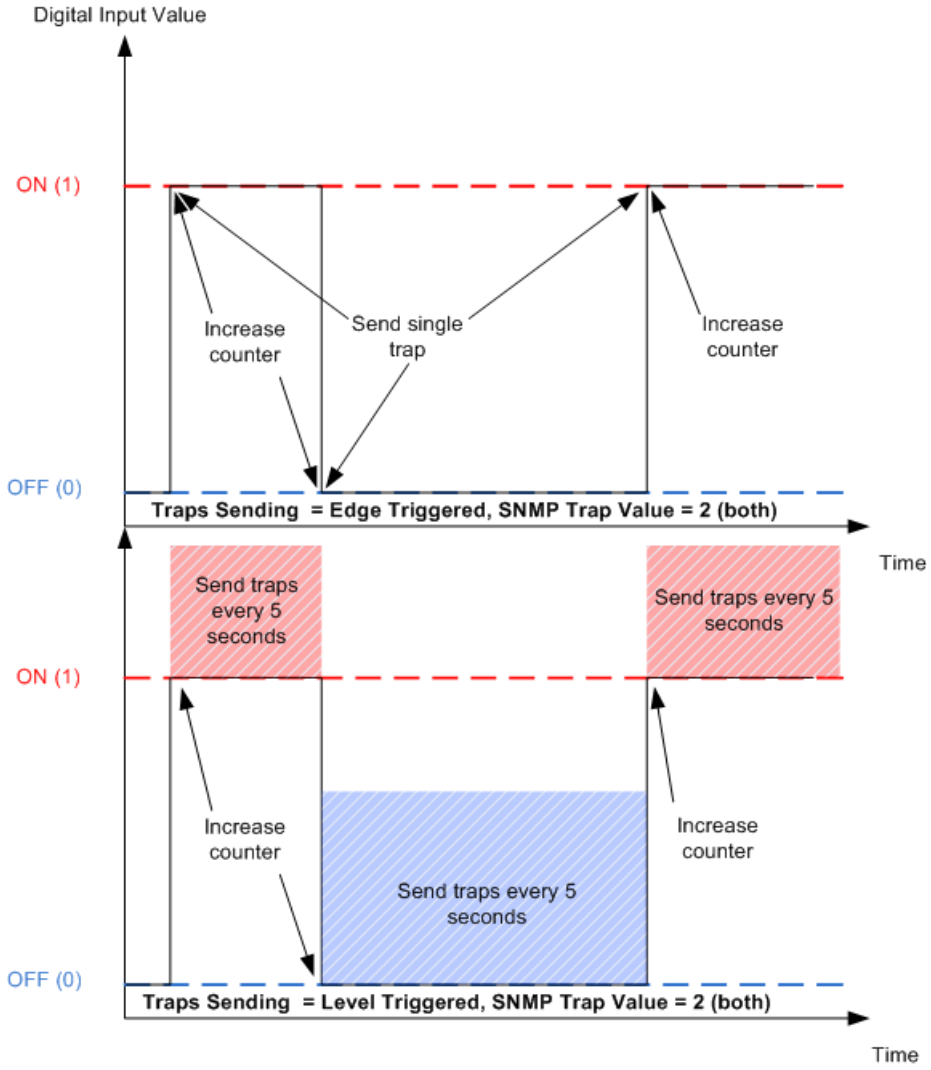


Figure 36. Traps and counter when SNMP Trap Value is "2 (both)"

- **Remote Relay Control** - this is the remote relay number "attached" to this digital input from the remote network device selected from the list from page "Remote Services". Commands for **Remote Relay Control** are sent:
  - When the digital input state is changed;
  - After reset of **SmartDEN IP-32IN**;
  - When new relay is selected from the field **Remote Relay Control**;
  - When **Remote Relay Mode** is changed;
- **Remote Relay Mode** - determines how the remote relay will be controlled:
  - *Normal* - when the digital input is ON, the relay will be ON. Then the input is OFF, the relay will be OFF as well;

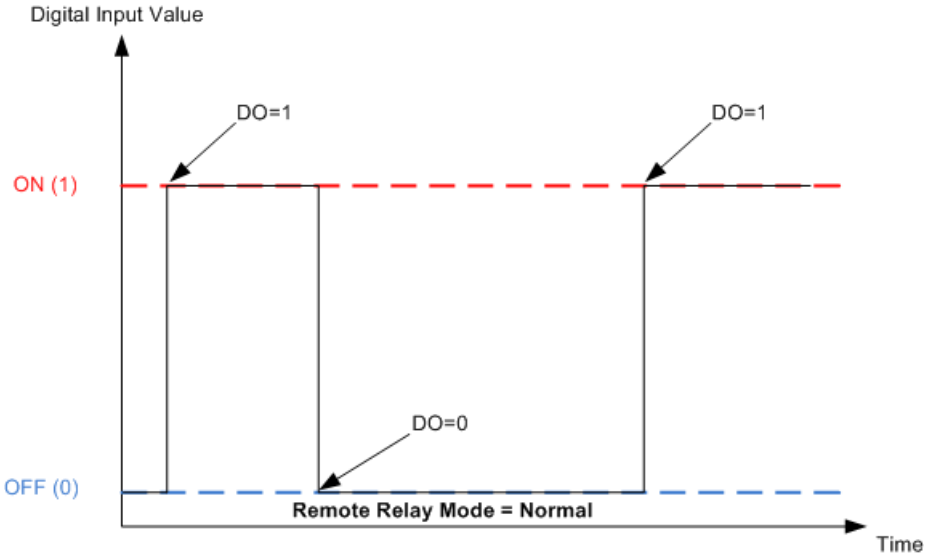


Figure 37. Controlling remote relay when **Remote Relay Mode** parameter is "Normal"

- *Inversed* - when the digital input is ON, the relay will be OFF. Then the input is OFF, the relay will be ON;

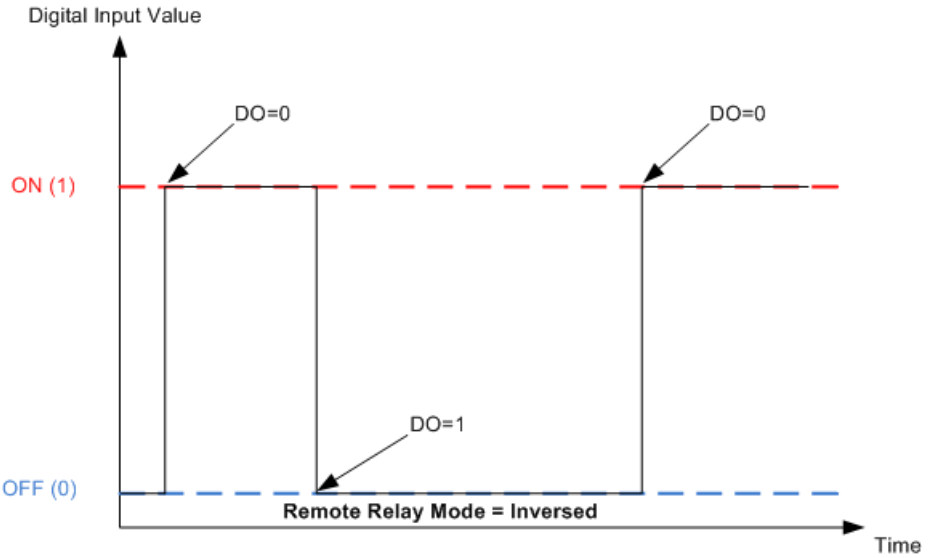


Figure 38. Controlling remote relay when **Remote Relay Mode** parameter is "Inversed"

- **Save button** - once you have changed the settings as required, click this button.

7.10. Analog Inputs

Analog Inputs

Analog Input	Description	Min	Max	Label	Low Threshold	High Threshold	SNMP Trap	Remote Relay Control	Remote Relay Mode
Input 1	AI1	0.0	50.0	Volt	0	0	☐	2	Normal
Input 2	AI2	0.0	30.0	DegC	0	0	☐	7	Inversed
Input 3	AI3	0.0	40.0	DegF	300	500	☑	3	Normal
Input 4	AI4	20.1	30.0	M	0	0	☐	-	Normal
Input 5	AI5	-1.2	100.0	%RH	0	0	☐	-	Normal
Input 6	AI6	0.0	10.0	cm	0	0	☐	-	Normal
Input 7	AI7	0.0	5.2	Kg	0	0	☐	-	Normal
Input 8	AI8	0.0	100.0	A	222	666	☑	2	Inversed

Save Reload

Figure 39. Analog Inputs

- **Description** - Analog Input identification string (max 7 chars);
- **Min** - the measured value used for scaling corresponding to analog input value = 0 (range: from -9999.9 to 9999.9);
- **Max** - the measured value used for scaling corresponding to analog input value = 1023 (range: from -9999.9 to +9999.9);
- **Label** - the label for the measured value for example: m,A,KG,V...(max 4 chars);
- **Low Threshold** - the low threshold for the measured value (range: from -9999 to **High Threshold**);
- **High Threshold** - the high threshold for the measured value (range: from **Low Threshold** to 9999);
- **SNMP Trap** - determines if the Analog Input will send traps or not. When this parameter is set, the trap(s) are sent in the following cases:
  - If **Traps Sending** parameter from web page "**SNMP Traps Settings**" is set to "**Level Triggered**" and if the Analog Input measured value is less or equal than **Low Threshold** or greater or equal than **High Threshold** traps will be sent every 5 seconds (Fig. 40);

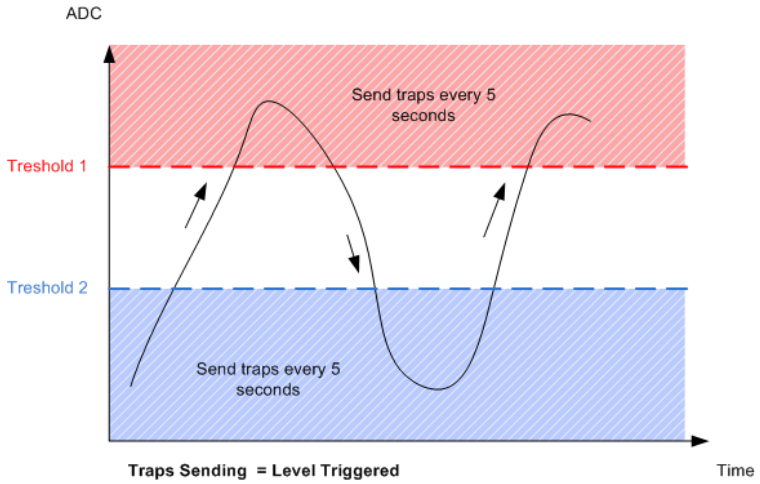


Figure 40. Sending tarps with **Traps Sending** = "**Level Triggered**"

- If **Traps Sending** parameter from web page "**SNMP Traps Settings**" is set to "**Edge Triggered**" a single trap is sent when measured value crosses over the **High Threshold** or below the **Low Threshold** values (Fig. 41).

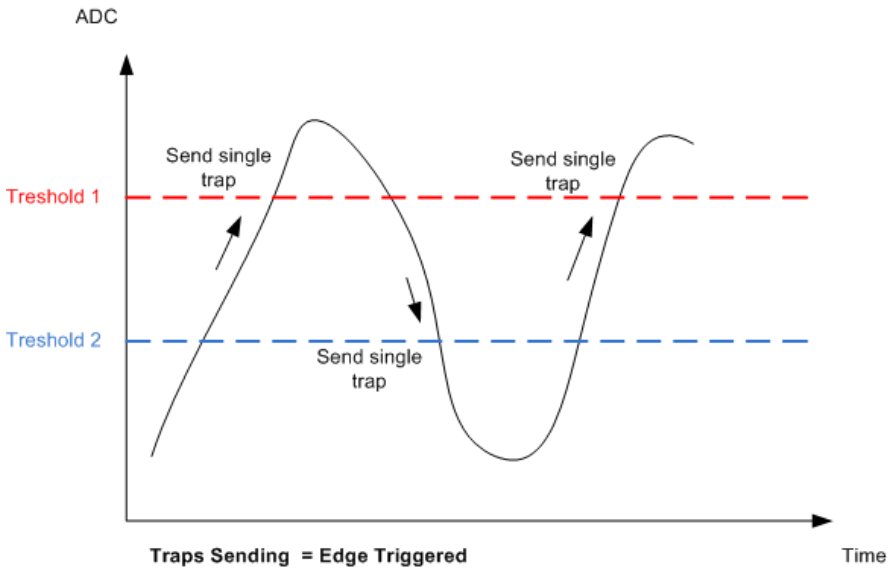


Figure 41. Sending tarps with **Traps Sending** = "Edge Triggered"

- When the parameter **Low Threshold** is changed and the Analog Input measured value is less or equal than the new value of **Low Threshold**;
- When the parameter **High Threshold** is changed and the Analog Input measured value is greater or equal than the new value of **High Threshold**;

- **Remote Relay Control** - this is the remote relay number "attached" to this analog input from the remote network device selected from the list from page "Remote Services". Commands for **Remote Relay Control** are sent:
  - When the Analog Input measured value is less or equal than **Low Threshold**;
  - When the Analog Input measured value is greater or equal than **High Threshold**;

- When parameter **Low Threshold** is changed and the measured value is less or equal than **Low Threshold**;
- When parameter **High Threshold** is changed and the measured value is greater or equal than **High Threshold**;
- After reset of **SmartDEN IP-32IN**;
- When new relay is selected from the field **Remote Relay Control**;
- When **Remote Relay Mode** is changed;

- **Remote Relay Mode** - determines what will be the control command for the remote relay:
  - *Normal* - when the rising analog input value crosses the **High Threshold**, the remote relay (digital output) will be OFF (0). When the falling value crosses the **Low Threshold** the remote relay (digital output) will be ON (1) (Fig. 42).

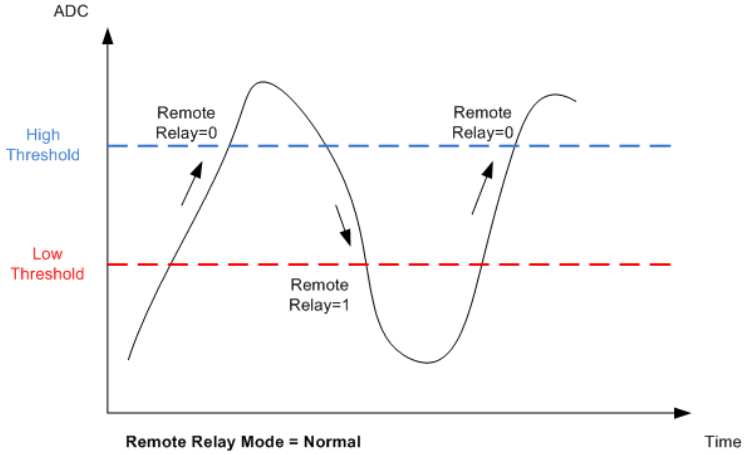


Figure 42. Controlling remote relay when **Remote Relay Mode** parameter is "Normal"

  - *Inversed* - when the rising analog input value crosses the **High Threshold**, the remote relay (digital output) will be ON (1). When the falling value crosses the **Low Threshold** the remote relay (digital output) will be OFF (0) (Fig. 43).

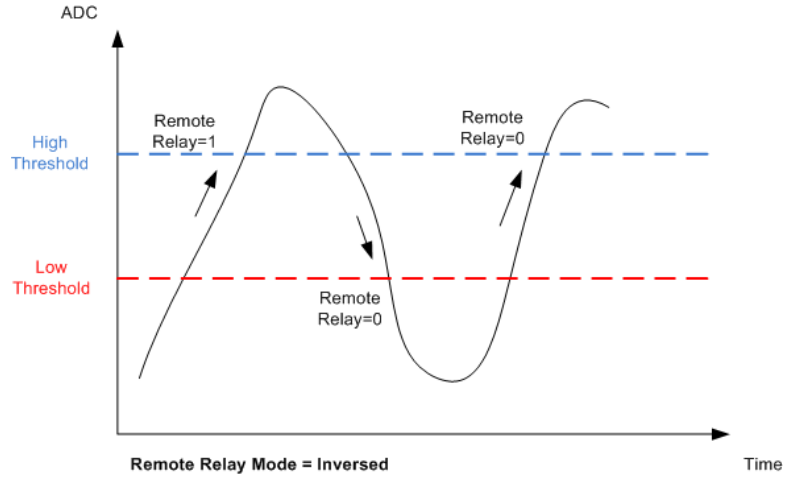


Figure 43. Controlling remote relay when **Remote Relay Mode** parameter is "Inversed"

- **Save button** - once you have changed the settings as required, click this button.

The measured value for the analog inputs is calculated in the following way:

$$MeasuredValue = Min + \frac{Max - Min}{1024} . ADCValue$$

7.11. Temperature Inputs

Temperature Inputs

Temp. Input	Description	Tolerance, %	Low Threshold, °C	High Threshold, °C	SNMP Trap	Remote Relay Control	Remote Relay Mode
Input 1	TI1	0	20	40	☑	5	Normal
Input 2	TI2	0	0	0	☐	-	Normal
Input 3	TI3	0	0	0	☐	-	Normal
Input 4	TI4	0	0	0	☐	-	Normal
Input 5	TI5	0	0	0	☐	-	Normal
Input 6	TI6	0	0	0	☐	-	Normal
Input 7	TI7	0	0	0	☐	-	Normal
Input 8	TI8	0	0	0	☐	-	Normal

Save Reload

Figure 44. Temperature Inputs

- **Description** - Temperature Input identification string (max 7 chars);
- **Tolerance, %**: The tolerance for the Temperature Input - from -5% to +5%; This can be set if there is significant difference in the sensor value otherwise must be left with value of 0;
- **Low Threshold, °C/°F** - the low threshold limit for this input (range: from -55°C/-67°F up to **High Threshold**);
- **High Threshold, °C/°F** - the high threshold limit for this input (from **Low Threshold** up to +155°C/ 311°F);
- **SNMP Trap** - determines if the Temperature Input will send traps or not. When this parameter is set, the trap(s) are sent in the following cases:
  - If **Traps Sending** parameter from web page "**SNMP Traps Settings**" is set to "**Level Triggered**" and if the Temperature Input value is less or equal than **Low Threshold** or greater or equal than **High Threshold** traps will be sent every 5 seconds (Fig. 45);

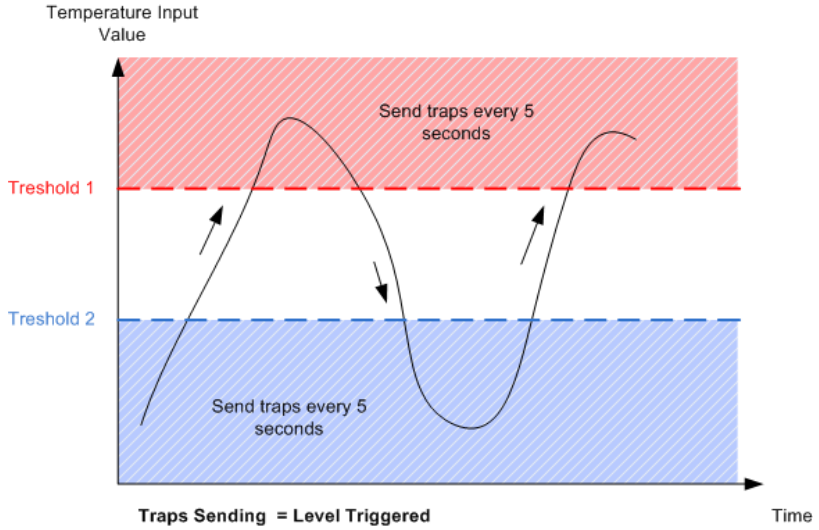


Figure 45. Sending tarps with **Traps Sending** = "Level Triggered"

- If **Traps Sending** parameter from web page "**SNMP Traps Settings**" is set to "**Edge Triggered**" and if the rising Temperature Input value the **High Threshold** or the falling Temperature Input value crosses the **Low Threshold,** a single trap will be sent (Fig. 46);

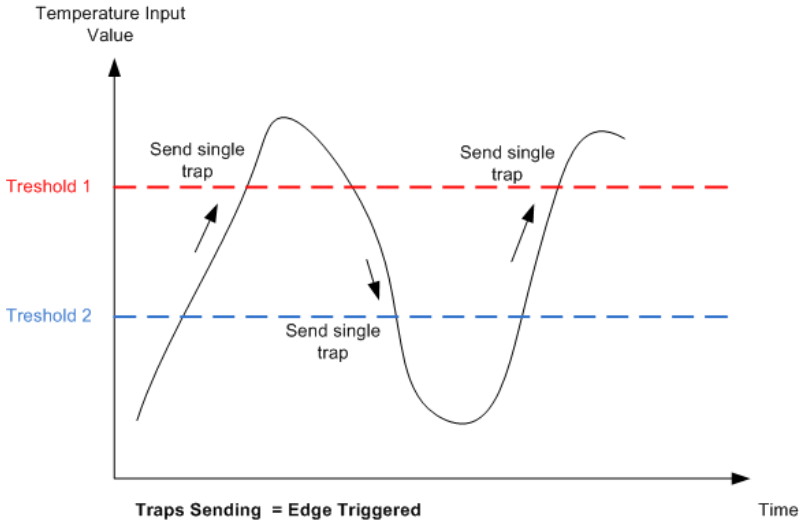


Figure 46. Sending tarps with **Traps Sending** = "Edge Triggered"

- When the parameter **Low Threshold** is changed and the Temperature Input value is less or equal than the new value of **Low Threshold**;
- When the parameter **High Threshold** is changed and the Temperature Input value is greater or equal than the new value of **High Threshold**;

- **Remote Relay Control** - this is the remote relay number "attached" to this Temperature Input from the remote network device selected from the list from page "Remote Services". Commands for **Remote Relay Control** are sent:
  - When the Temperature Input value is less or equal than **Low Threshold**;
  - When the Temperature Input value is greater or equal than **High Threshold**;
  - When parameter **Low Threshold** is changed and the input value is less or equal than **Low Threshold**;

- When parameter **High Threshold** is changed and the input value is greater or equal than **High Threshold**;
- After reset of **SmartDEN IP-32IN**;
- When new relay is selected from the field **Remote Relay Control**;
- When **Remote Relay Mode** is changed;

- **Remote Relay Mode** - determines what will be the control command for the remote relay:
  - *Normal* - when the rising Temperature Input value crosses the **High Threshold**, the remote relay (digital output) will be OFF (0). When the falling value crosses the **Low Threshold** the remote relay (digital output) will be ON (1) (Fig. 47).

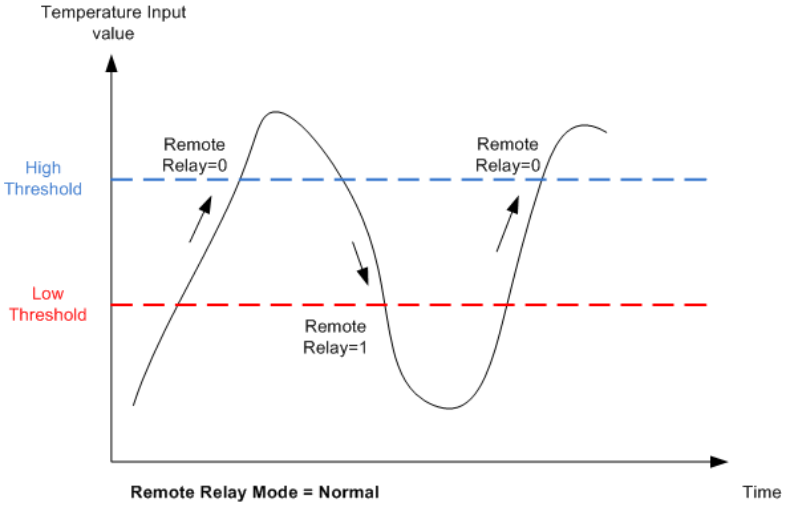


Figure 47. Controlling remote relay when **Remote Relay Mode** parameter is "Normal"

  - *Inversed* - when the rising Temperature Input value crosses the **High Threshold**, the remote relay (digital output) will be ON (1). When the falling value crosses the **Low Threshold** the remote relay (digital output) will be OFF (0) (Fig. 48).

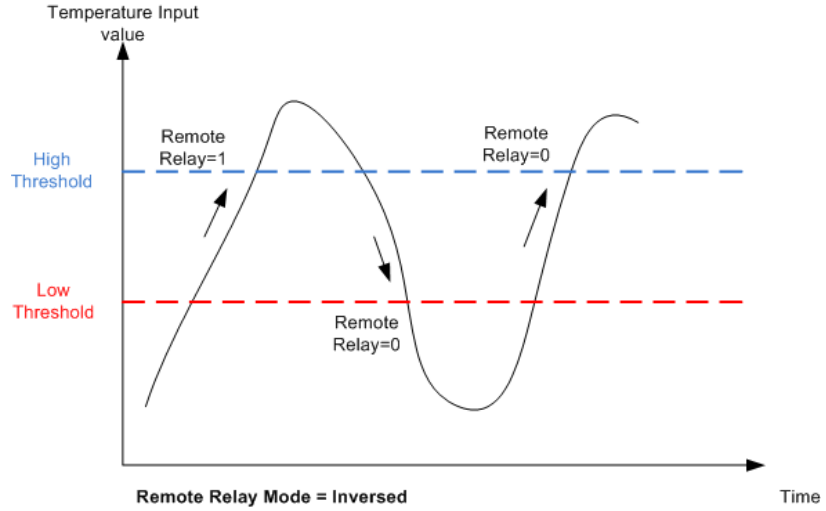


Figure 48. Controlling remote relay when **Remote Relay Mode** parameter is "Inversed"

- **Save button** - once you have changed the settings as required, click this button.

7.12. Monitoring

Digital Inputs (1..8)							
DIn1	DIn2	DIn3	Din4	DIn5	DIn6	DIn7	DIn8
0 (Off)	0 (Off)	0 (Off)	1 (On)	0 (Off)	1 (On)	0 (Off)	0 (Off)
8	12	110	108	0	0	0	0

Digital Inputs (9..16)							
DIn9	DIn10	DIn11	DIn12	DIn13	DIn14	DIn15	DIn16
0 (Off)	1 (On)	0 (Off)	0 (Off)	0 (Off)	0 (Off)	0 (Off)	0 (Off)
0	0	0	0	0	0	0	0

Analog Inputs							
AIn1	AIn2	AIn3	AIn4	AIn5	AIn6	AIn7	AIn8
0	0	0	0	504	0	0	0
0.0 Volt	0.0 mA	-9000.0 mV	0.0 Volt	49.2 %PH	0.0 Kg	0.0 Volt	0.0 Volt

Temperature Inputs, ℃							
TIn1	TIn2	TIn3	TIn4	TIn5	TIn6	TIn7	TIn8
-9.0	---	---	29.1	---	92.4	22.1	---

Figure 49. Monitoring page

7.13. Logout

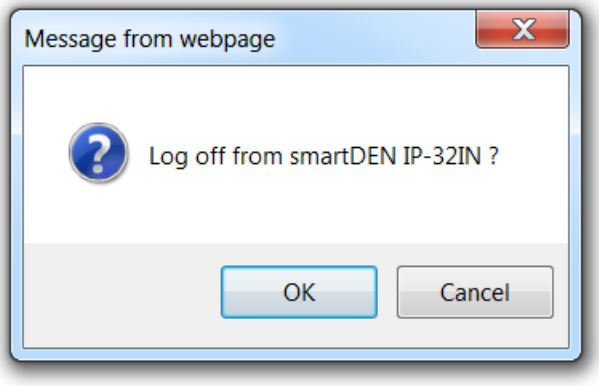


Figure 50. Log off

7.14. Reboot

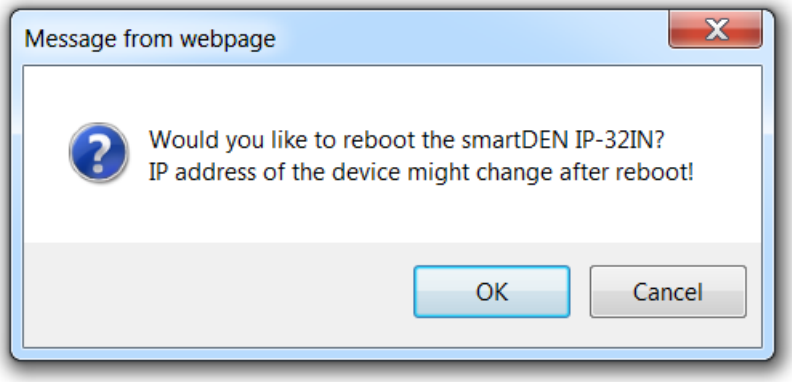


Figure 51. Reboot

8. HTTP server

This operation mode allows custom applications to obtain the input values from **SmartDEN IP-32IN** without using a Web-browser. The custom application acts as a HTTP client, sending HTTP GET requests to the **SmartDEN IP-32IN** (Fig. 52).

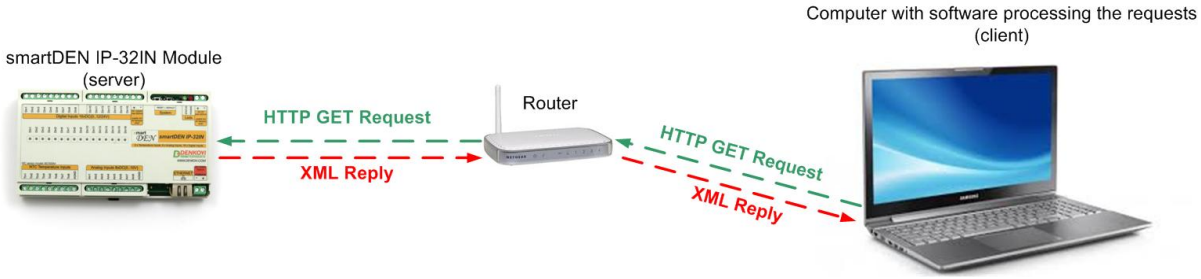


Figure 52. SmartDEN IP-32IN can work as HTTP server

To receive the current state of the **SmartDEN IP-32IN**, the application requests the page current_state.xml / current_state.json, for example:

http://192.168.1.100/current_state.xml
http://192.168.1.100/current_state.json

In order to use this mode, XML/JSON access should be enabled.

The login process differs depending on the selected **Encrypt Password** option.

8.1. XML access

8.1.1. XML login (encrypted password)

In this mode a two-step login sequence is provided as a protection against unauthorized access.

The first time the custom application requests the page current_state.xml, a random login key is issued in the reply. Next the custom application uses this key to encrypt the password. The encrypted password is sent as a parameter with the next request to the page current_state.xml.

Bellow is an example of login process:

Step 1:

Request
http://192.168.1.100/current_state.xml
Reply (login required):

```
<CurrentState>
    <LoginKey>65156</LoginKey>
</CurrentState>
```

Step 2:

Request (password is sent as a parameter)

http://192.168.1.100/current_state.xml?pw=28237099263eabfd88626124a822c64c

Reply (password is O'K, login accepted):

```
<CurrentState>
    <DigitalInput1>
        <Name>DIn1</Name>
        <Value>1</Value>
    </DigitalInput1>
...
</CurrentState>
```

Password encryption algorithm to be implemented in custom application is available upon request.

8.1.2. XML login (non-encrypted password)

In this mode the password is passed as non-encrypted parameter with the request:

http://192.168.1.100/current_state.xml?pw=admin

Getting the <LoginKey> in the answer in this mode means that the provided password is wrong or the login session has been expired.

If there is no data traffic between the custom application and the **SmartDEN IP-32IN** for time, specified by **Session Timeout** parameter, the session "times out" and a new login is required.

8.1.3. Retrieving current state in XML format

After successful login the custom application can obtain the **SmartDEN IP-32IN** current state by request to the current_state.xml page. The reply contains a page in XML format (Fig. 53).

```
▼<CurrentState>
  ▼<DigitalInput1>
      <Name>DIn1</Name>
      <Value>0</Value>
      <Count>92</Count>
    </DigitalInput1>
  ▶<DigitalInput2>...</DigitalInput2>
  ▶<DigitalInput3>...</DigitalInput3>
  ▶<DigitalInput4>...</DigitalInput4>
  ▶<DigitalInput5>...</DigitalInput5>
  ▶<DigitalInput6>...</DigitalInput6>
  ▶<DigitalInput7>...</DigitalInput7>
  ▶<DigitalInput8>...</DigitalInput8>
  ▶<DigitalInput9>...</DigitalInput9>
  ▶<DigitalInput10>...</DigitalInput10>
  ▶<DigitalInput11>...</DigitalInput11>
  ▶<DigitalInput12>...</DigitalInput12>
  ▶<DigitalInput13>...</DigitalInput13>
  ▶<DigitalInput14>...</DigitalInput14>
  ▶<DigitalInput15>...</DigitalInput15>
  ▶<DigitalInput16>...</DigitalInput16>
  ▼<AnalogInput1>
      <Name>AIn1</Name>
      <Value>504</Value>
      <Measure>3.9 Volt</Measure>
    </AnalogInput1>
  ▶<AnalogInput2>...</AnalogInput2>
  ▶<AnalogInput3>...</AnalogInput3>
  ▶<AnalogInput4>...</AnalogInput4>
  ▶<AnalogInput5>...</AnalogInput5>
  ▶<AnalogInput6>...</AnalogInput6>
  ▶<AnalogInput7>...</AnalogInput7>
  ▶<AnalogInput8>...</AnalogInput8>
  ▼<TemperatureInput1>
      <Name>TIn1</Name>
      <Value>23.4 ℃</Value>
    </TemperatureInput1>
  ▶<TemperatureInput2>...</TemperatureInput2>
  ▶<TemperatureInput3>...</TemperatureInput3>
  ▶<TemperatureInput4>...</TemperatureInput4>
  ▶<TemperatureInput5>...</TemperatureInput5>
  ▶<TemperatureInput6>...</TemperatureInput6>
  ▶<TemperatureInput7>...</TemperatureInput7>
  ▶<TemperatureInput8>...</TemperatureInput8>
  ▼<Device>
      <Name>SMARTDEN_IN</Name>
      <MAC>E8:EA:DA:00:00:01</MAC>
    </Device>
</CurrentState>
```


Figure 53. XML file with current measurements

8.2. JSON access

8.2.1. JSON login (encrypted password)

The encrypted login sequence is similar to the XML access:

Step 1:

Request
http://192.168.1.100/current_state.json
Reply (login required):

```
{
  "CurrentState": { "LoginKey": "65156" }
}
```

Step 2:

Request (password is sent as a parameter)
http://192.168.1.100/current_state.json?pw=28237099263eabfd88626124a822c64c
Reply (password is O'K, login accepted):

```
{
  "CurrentState": {
      "DigitalInput": [
            {"Name": "DIn1", "Value": "1"},
    ...
}
```

Password encryption algorithm to be implemented in custom application is available upon request.

8.2.2. JSON login (non-encrypted password)

The password should be passed as non-encrypted parameter with the request:

http://192.168.1.100/current_state.json?pw=admin

Getting the "LoginKey" in the answer means only that the provided password is wrong or the login session has been expired.

If there is no data traffic between the custom application and the **SmartDEN IP-32IN** for time, specified by **Session Timeout** parameter, the session "times out" and a new login is required.

8.2.3. Retrieving current state in JSON format

When logged, the custom application can get current measurements requesting the current_state.json page. The reply contains a page in JSON format (Fig. 54).

```
{
  "CurrentState": {
    "DigitalInput": [
      {"Name": "DIn1", "Value": "1"},
      {"Name": "DI2", "Value": "0"},
      {"Name": "DI3", "Value": "0"},
      {"Name": "DI4", "Value": "0"},
      {"Name": "DI5", "Value": "0"},
      {"Name": "DI6", "Value": "0"},
      {"Name": "DI7", "Value": "1"},
      {"Name": "DI8", "Value": "0"},
      {"Name": "DI9", "Value": "0"},
      {"Name": "DI10", "Value": "0"},
      {"Name": "DI11", "Value": "0"},
      {"Name": "DI12", "Value": "1"},
      {"Name": "DI13", "Value": "0"},
      {"Name": "DI14", "Value": "0"},
      {"Name": "DI15", "Value": "0"},
      {"Name": "DI16", "Value": "0"}
    ],
    "AnalogInput": [
      {"Name": "AI1", "Value": "249"},
      {"Name": "AI2", "Value": "190"},
      {"Name": "AI3", "Value": "13"},
      {"Name": "AI4", "Value": "505"},
      {"Name": "AI5", "Value": "1011"},
      {"Name": "AI6", "Value": "35"},
      {"Name": "AI7", "Value": "33"},
      {"Name": "AI8", "Value": "561"}
    ],
    "TemperatureInput": [
      {"Name": "TI1", "Value": "25.1"},
      {"Name": "TI2", "Value": "14.2"},
      {"Name": "TI3", "Value": "25.3"},
      {"Name": "TI4", "Value": "17.3"},
      {"Name": "TI5", "Value": "37.9"},
      {"Name": "TI6", "Value": "18.0"},
      {"Name": "TI7", "Value": "19.1"},
      {"Name": "TI8", "Value": "29.9"}
    ],
    "Device": {
      "Name": "SMARTDEN_IN",
      "MAC": "E8:EA:DA:00:00:01"
    }
  }
}
```


Figure 54. JSON file with current measurements

8.3. Multiple XML/JSON access

With the **Multiple Access** option selected the password should be passed as a non-encrypted parameter with each request:

http://192.168.1.100/current_state.xml?pw=admin
http://192.168.1.100/current_state.json?pw=admin

Multiple Access is not allowed when **Encrypt Password** option is enabled.

9. HTTP client

9.1. Data Logging mode

Data Logging mode (push notifications mode) is designed in order to help solving cases like remote monitoring and Internet/Ethernet logging. The **SmartDEN IP-32IN** acts like a client and it sends (pushes) HTTP POST messages in XML format to the HTTP server periodically (Fig. 55).

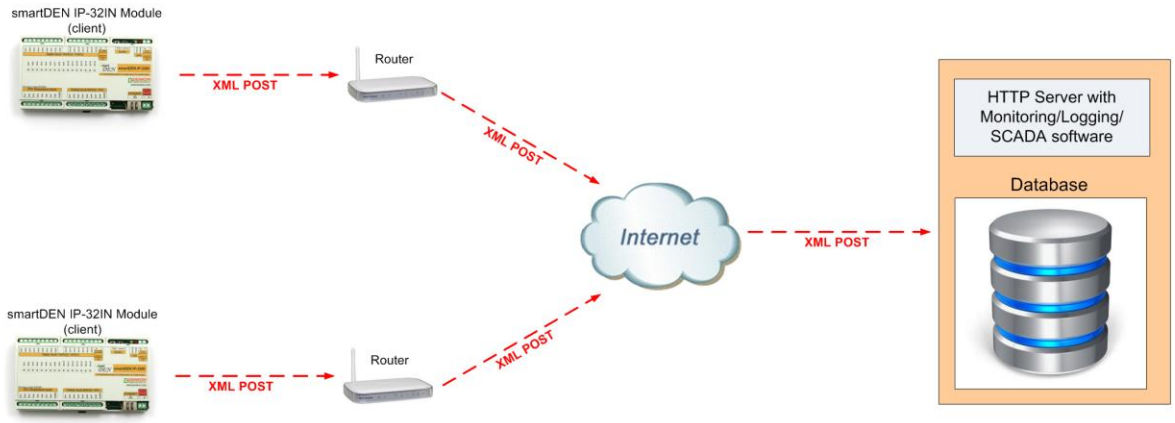


Figure 55. Data logging mode

Data Logging mode is adjusted from the "Remote Services Settings" web page -> "Data Logging" section.

Please note the module does not support internal memory data storage for logging, but it can send only messages to remote server-logger!

9.1.1. HTTP POST header

Bellow is shown the header of example POST message sent by **SmartDEN IP-32IN**:

```
POST /current_state.xml HTTP/1.0
Host: 192.168.1.124
Content-Type: text/xml; charset=UTF-8
Content-Length: 3046
Connection: close
```

Current_state.xml is actually the **HTTP Server Path** from the page "Remote Services Settings". *192.168.1.122* is the **HTTP Server Address**.

9.1.2. HTTP POST body

The body is actually the posted XML file content. Example body content is shown below:

```
<?xml version='1.0' encoding='UTF-8'?>
<CurrentState>
<DigitalInput1>
  <Name>DI1</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput1>
<DigitalInput2>
  <Name>DI2</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput2>
<DigitalInput3>
  <Name>DI3</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput3>
<DigitalInput4>
  <Name>DI4</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput4>
<DigitalInput5>
  <Name>DI5</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput5>
<DigitalInput6>
  <Name>DI6</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput6>
<DigitalInput7>
```

```
  <Name>DI7</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput7>
<DigitalInput8>
  <Name>DI8</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput8>
<DigitalInput9>
  <Name>DI9</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput9>
<DigitalInput10>
  <Name>DI10</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput10>
<DigitalInput11>
  <Name>DI11</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput11>
<DigitalInput12>
  <Name>DI12</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput12>
<DigitalInput13>
  <Name>DI13</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput13>
<DigitalInput14>
  <Name>DI14</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput14>
<DigitalInput15>
  <Name>DI15</Name>
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput15>
<DigitalInput16>
  <Name>123</Name>
```

```
  <Value>0</Value>
  <Count>0</Count>
</DigitalInput16>
<AnalogInput1>
  <Name>AI1</Name>
  <Value>0</Value>
  <Measure>0.0 Volt</Measure>
</AnalogInput1>
<AnalogInput2>
  <Name>AI2</Name>
  <Value>0</Value>
  <Measure>0.0 DegC</Measure>
</AnalogInput2>
<AnalogInput3>
  <Name>AI3</Name>
  <Value>0</Value>
  <Measure>0.0 DegF</Measure>
</AnalogInput3>
<AnalogInput4>
  <Name>AI4</Name>
  <Value>0</Value>
  <Measure>20.1 M</Measure>
</AnalogInput4>
<AnalogInput5>
  <Name>AI5</Name>
  <Value>0</Value>
  <Measure>-1.2 %RH</Measure>
</AnalogInput5>
<AnalogInput6>
  <Name>AI6</Name>
  <Value>0</Value>
  <Measure>0.0 cm</Measure>
</AnalogInput6>
<AnalogInput7>
  <Name>AI7</Name>
  <Value>0</Value>
  <Measure>0.0 Kg</Measure>
</AnalogInput7>
<AnalogInput8>
  <Name>AI8</Name>
  <Value>387</Value>
  <Measure>37.8 A</Measure>
</AnalogInput8>
<TemperatureInput1>
  <Name>TI1</Name>
  <Value>21.9</Value>
```

```
</TemperatureInput1>
<TemperatureInput2>
  <Name>TI2</Name>
  <Value>---</Value>
</TemperatureInput2>
<TemperatureInput3>
  <Name>TI3</Name>
  <Value>---</Value>
</TemperatureInput3>
<TemperatureInput4>
  <Name>TI4</Name>
  <Value>---</Value>
</TemperatureInput4>
<TemperatureInput5>
  <Name>TI5</Name>
  <Value>---</Value>
</TemperatureInput5>
<TemperatureInput6>
  <Name>TI6</Name>
  <Value>---</Value>
</TemperatureInput6>
<TemperatureInput7>
  <Name>TI7</Name>
  <Value>---</Value>
</TemperatureInput7>
<TemperatureInput8>
  <Name>TI8</Name>
  <Value>---</Value>
</TemperatureInput8>
<Device>
  <Name>SMARTDEN-IP32IN</Name>
  <MAC>E8:EA:DA:00:18:B7</MAC>
</Device>
</CurrentState>
```

9.2. Remote Relay Control mode

This mode allows you to control relays over the local network or Internet from some **SmartDEN IP-32IN** input up on input event like analog/temperature value threshold crossing or changing digital input value. **SmartDEN IP-32IN** sends specific HTTP GET message to the selected remote relay board.

Remote Relay Control mode is adjusted from the "Remote Services Settings" web page -> "Remote Relay Control" section.

Please note single **SmartDEN IP-32IN** input module can control only one remote relay board at a time.

SmartDEN IP-32IN input module must "see" the IP of the Remote Relay Board in order to work in this mode. In case of LAN, both modules must be in same local network segment. In case of WAN, the Remote Relay Board address must be static IP address.

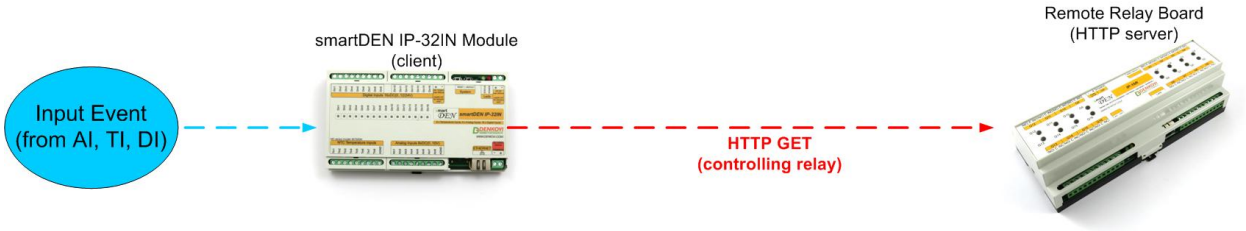


Figure 56. Controlling relay example (direct connection)

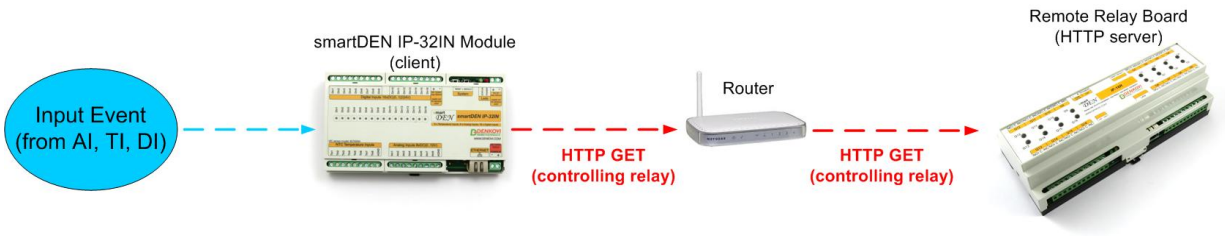


Figure 57. Controlling relay example (through router)

Figure 58. Controlling relay example (through Internet)

10. SNMP access

SmartDEN IP-32IN supports SNMP snmpget and snmpset commands. Most of the parameters can be configured/read via these commands. Read-only community string is used for reading and Read-Write Community String is used for changing the parameters. Parameters that can be changed, are grouped according to their functions in the tables below. To obtain a valid OID number it is necessary to replace the "x" symbol with the prefix "**.1.3.6.1.4.1.42505**". Also all the snmp commands are described in the MIB file**.**

During SNMP access, it must be used snmpget and snmpset only to one OID and not to group of OIDs.

10.1. Product

Table 9. Product OID-s

OID	Name	Access	Description	Syntax
x.7.1.1.0	Name	read-only	Description of the module	DISPLAYSTRING
x.7.1.2.0	Version	read-only	Current firmware version	DISPLAYSTRING
x.7.1.3.0	Date	read-only	Current firmware version build date	DISPLAYSTRING

10.2. Setup

Table 10. Digital Inputs OID-s

Start OID	End OID	Name	Access	Description	Syntax
x.7.2.1.1.2.0	x.7.2.1.1.2.15	DigitalInput Description	read-write	Digital Input Description (maxlen=7)	DISPLAYSTRING (SIZE (0..7))
x.7.2.1.1.3.0	x.7.2.1.1.3.15	DigitalInput Counter	read-write	Digital Input Counter (0..65535)	INTEGER32 (0..65535)
x.7.2.1.1.4.0	x.7.2.1.1.4.15	DigitalInput Filter	read-write	Digital Input Filter (0..200), ms	INTEGER (0..200)
x.7.2.1.1.5.0	x.7.2.1.1.5.15	DigitalInput TrapEnabled	read-write	Digital Input Trap Enable Flag (Disabled-0, Enabled-1)	INTEGER { no(0),yes(1) }
x.7.2.1.1.6.0	x.7.2.1.1.6.15	DigitalInput TrapValue	read-write	Digital Input Trap Value (off-0, on-1, both-2)	INTEGER { closed(0),open(1),both(2) }
x.7.2.1.1.7.0	x.7.2.1.1.7.15	DigitalInput State	read-only	Digital Input State (off-0,on-1)	INTEGER { closed(0),open(1) }

Table 11. Analog Inputs OID-s

Start OID	End OID	Name	Access	Description	Syntax
x.7.2.2.1.2.0	x.7.2.2.1.2.7	AnalogInput Description	read-write	Analog Input Description (maxlen=7)	DISPLAYSTRING (SIZE (0..7))
x.7.2.2.1.3.0	x.7.2.2.1.3.7	AnalogInputTrapLowThreshold	read-write	Analog Input Trap Low Threshold (0..1023)	INTEGER (0..1023)
x.7.2.2.1.4.0	x.7.2.2.1.4.7	AnalogInputTrapHighThreshold	read-write	Analog Input Trap High Threshold (0..1023)	INTEGER (0..1023)
x.7.2.2.1.5.0	x.7.2.2.1.5.7	AnalogInputTrapEnabled	read-write	Analog Input Trap Enable Flag (Disabled-0, Enabled-1)	INTEGER { no(0),yes(1) }
x.7.2.2.1.6.0	x.7.2.2.1.6.7	AnalogInput Value	read-only	Analogl Input Value	INTEGER (0..1023)
x.7.2.2.1.7.0	x.7.2.2.1.7.7	AnalogInput Min	read-write	Analog Input Min Value (maxlen=7)	DISPLAYSTRING (SIZE (0..7))
x.7.2.2.1.8.0	x.7.2.2.1.8.7	AnalogInput Max	read-write	Analog Input Max Value (maxlen=7)	DISPLAYSTRING (SIZE (0..7))
x.7.2.2.1.9.0	x.7.2.2.1.9.7	AnalogInputLabel	read-write	Analog Input Label (maxlen=4)	DISPLAYSTRING (SIZE (0..3))
x.7.2.2.1.10.0	x.7.2.2.1.10.7	AnalogInput Measure	read-write	Analog Input Measured Value	DISPLAYSTRING

Table 12. Temperature Inputs OID-s

Start OID	End OID	Name	Access	Description	Syntax
x.7.2.3.1.2.0	x.7.2.3.1.2.7	TemperatureInputName	read-write	Temperature Input Name (maxlen=7)	DISPLAYSTRING (SIZE (0..7))
x.7.2.3.1.3.0	x.7.2.3.1.3.7	TemperatureInputSensorTolerance	read-write	Temperature Input Sensor Tolerance (-5..+5)	INTEGER (-5..+5)
x.7.2.3.1.4.0	x.7.2.3.1.4.7	TemperatureInputTrapLowThreshold	read-write	Temperature Input Trap Low Threshold (-55..155)	INTEGER (-55..155)
x.7.2.3.1.5.0	x.7.2.3.1.5.7	TemperatureInputTrapHighThreshold	read-write	Temperature Input Trap Low Threshold (-55..155)	INTEGER (-55..155)

x.7.2.3.1.6.0	x.7.2.3.1.6.7	Temperature InputTrapEnabled	read-write	Temperature Input Trap Enable Flag (Disabled-0, Enabled-1)	INTEGER { no(0),yes(1) }
x.7.2.3.1.7.0	x.7.2.3.1.7.7	Temperature InputValue	read-only	Temperature Input Value	DISPLAYSTRING

10.3. Control

Table 13. Control OID-s

OID	Name	Access	Description	Syntax
x.7.3.1.0	DigitalInputsState	read-write	Digital Inputs State (0..65535)	INTEGER32 (0..65535)
x.7.3.2.0	Reboot	read-write	Reboot **smartDEN IP-32IN** Module	INTEGER (0..255)
x.7.3.3.0	sysUpTime	read-only	The time (in hundredths of a second) since the device was last re-initialized.	TIMETICKS
x.7.3.4.0	analogInputFilter	read-write	Analog Input Filter Constant (0..30), sec	Integer (0..30)
x.7.3.5.0	temperatureInputFilter	read-write	Temperature Input Filter Constant (0..30), sec	Integer (0..30)
x.7.3.6.0	temperatureScale	read-write	Temperature Scale	INTEGER { Celsius(0), Fahrenheit(1) }

To reboot the device via SNMP, set the Reboot value to the ASCII code of the first char of your Web password. For example, if this is the char 'a', code in decimal is 97.

10.4. Traps

Configuration parameters related with the SNMP traps are shown in the below **Table 14**.

Table 14. Traps parameters

Start OID	Name	Access	Description	Syntax
x.7.4.1.0	TrapEnabled	read-write	Trap Enable Flag (Disabled-0, Enabled-1)	INTEGER { no(0),yes(1) }
x.7.4.2.0	TrapReceiverIPAddress	read-write	Trap Receiver IP Address	IPADDRESS
x.7.4.3.0	TrapReceiverPort	read-write	Trap Receiver Port (0..65535)	INTEGER32 (0..65535)
x.7.4.4.0	TrapCommunity	read-write	Community in Sending Trap	DISPLAYSTRING (SIZE (0..7))

x.7.4.5.0	TrapSending	read-write	Trap Sending (Level Triggered-0, Edge Triggered-1)	INTEGER {(0),(1)}

SmartDEN IP-32IN generates SNMP v1 traps described in **Table 15.**

Table 15. SNMP v1 traps generated by **smartDEN IP-32IN**

Generic Type	Specific Type	Variable Bindings			Description
		No	Name	Value	
coldStart	0				Reboot trap
autenticationFailure	0				Wrong SNMP community request trap
enterpriseSpecific	1	1	x.7.2.1.1.7.0 - x.7.2.1.1.7.15	Digital Input State (off-0,on-1)	Digital Input trap
		2	x.7.2.1.1.2.0 - x.7.2.1.1.2.15	Digital Input Description (maxlen=7)	
enterpriseSpecific	2	1	x.7.2.2.1.10.0 - x.7.2.2.1.10.7	Analog Input Measured Value	Analog Input trap
		2	x.7.2.2.1.2.0 - x.7.2.2.1.2.7	Analog Input Description (maxlen=7)	
enterpriseSpecific	3	1	x.7.2.3.1.7.0 - x.7.2.3.1.7.7	Temperature Input Value	Temperature Input trap
		2	x.7.2.3.1.2.0 - x.7.2.3.1.2.7	Temperature Input Description (maxlen=7)	

11. Security considerations

The **SmartDEN IP-32IN** runs a special firmware and do not use a general-purpose operating system. There are no extraneous IP services found on general-purpose operating systems (e.g. Telnet, FTP, Finger, etc.) that can be particularly vulnerable. The only exception from this is the SNMP protocol that can be disabled.

Web-browser access
A challenge-response authentication is used in login process. When the password is entered, it is transmitted across the network in encrypted form, so eavesdropping on the data transmission will not reveal the password. Subsequent transmissions of the password to "login" onto the device are encrypted and "safe". The only case when the password is transmitted across the network "in the open", is when it is being changed and submitted in **General Setting** form. Therefore, you must set passwords in the secure environment where you can make sure that no one is "eavesdropping".

SNMP communication
SNMPv2c does not implement encryption. Authentication of clients is performed only by a "community string", which is transmitted in clear text. SNMP communication should be used in trusted networks and disabled if not used.

XML/JSON operation
A challenge-response authentication can be used in login process. The password can be transmitted by custom application across the network in encrypted form.

Web and XML/JSON access can be restricted by IP Address (range of IP Addresses) or by MAC Address.

12. Appendix 1. Mechanical drawing

Figure 59. Device size

13. Appendix 2. Disclaimer

Denkovi Assembly Electronics LTD products are not designed, authorized or warranted to be suitable for use in space, nautical, military, medical, life-critical or safety-critical devices or equipment.

Denkovi Assembly Electronics LTD products are not designed, authorized or warranted to be suitable for use in applications where failure or malfunction of an Denkovi Assembly Electronics LTD product can result in personal injury, death, property damage or environmental damage.

Denkovi Assembly Electronics LTD accepts no liability for inclusion or use of Denkovi Assembly Electronics LTD products in such applications and such inclusion or use is at the customer's own risk. Should the customer use Denkovi Assembly Electronics LTD products for such application, the customer shall indemnify and hold Denkovi Assembly Electronics LTD harmless against all claims and damages.