

VANDERBILT



KNX

ASHRAE BACnet

Modbus

# SPCway SPCway Plus Setup guide

---

Adapted for SPCway Plus firmware 2.0

## Table of contents

Adapted for SPCway Plus firmware 2.0.....	1
Table of contents.....	2
1 Create the EDP client on the SPC panel .....	4
2 Hook up the SPCway.....	7
3 Logon to the SPCway website .....	8
4 Configure the network IP address .....	10
5 Configure the device physical KNX address .....	11
6 Set the EDP client settings in the SPCway .....	13
7 Configure the communication objects and group addresses .....	15
7.1 General information.....	16
7.2 Event.....	19
7.3 Status.....	21
7.4 Command .....	23
7.4.1 Watchdog command .....	25
8 Modbus.....	26
8.1 Modbus configuration.....	26
8.1.1 Modbus connection.....	26
8.1.2 Communication objects.....	27
8.1.3 Profile parameters.....	27
8.2 Modbus profile.....	28
8.3 Application level datatypes .....	30
9 BACnet & API (Plus features).....	32
9.1 BACnet.....	33
9.2 API.....	35
10 Visualization (Plus feature).....	36
11 Security considerations .....	38
12 Interface language.....	40
13 Supplementary features.....	41
13.1 KNX Objects.....	41
13.2 Objects Logging .....	43
13.3 Alerts, Logs and Error log .....	44
13.4 Back-up and restore .....	44

14	Advanced settings .....	45
14.1	Hostname .....	45
14.2	KNX-IP router & filtering.....	45
14.3	Advanced General settings.....	46
14.4	Firmware upgrade .....	46
14.5	Resetting password .....	47
Annex 1:	Event definitions .....	48
Annex 2:	Status definitions.....	53
Annex 3:	Command definitions.....	55
Annex 4:	BACnet.....	56



For a typical setup, you only need to go through steps 1 till 7.

# 1 Create the EDP client on the SPC panel

The first step is to define an EDP receiver configuration for the SPCway, inside the SPC panel.

The manual will focus on the use of the web interface to do so, but it is equally possible with the other SPC configuration tools.

First logon locally to the SPC website as 'Engineer' and go into 'Full Engineer' mode in the upper right corner. Then go to 'Communications' > 'Reporting' > 'EDP'.



Figure 1: EDP screen

Click on the general 'Settings' button in order to:

- Verify the EDP is enabled
- To set/modify/consult & note the SPC **EDP Panel ID**

You should see the following screen. Click 'Save' and 'Back' to return to the EDP window.

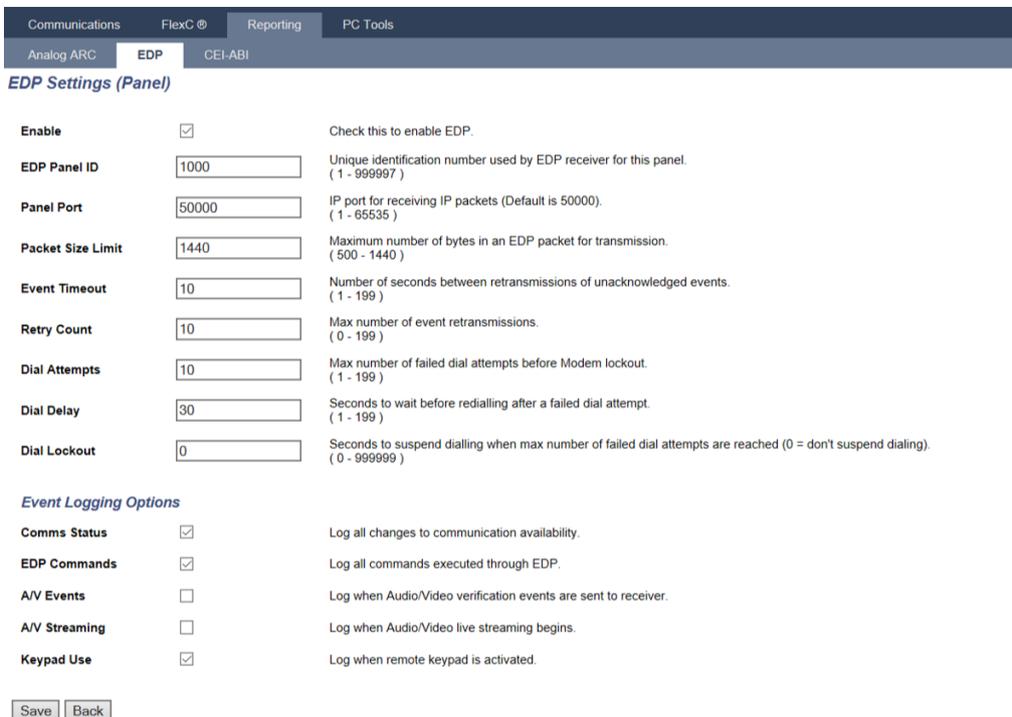


Figure 2: EDP settings

Click the 'Add' button to open the EDP Receiver editing window.

The following parameters are particularly important:

- **Receiver Id**: this is the SPCway EDP ID. E.g.: 99
- Protocol version: Version 2
- Commands enable: check if you want to allow the SPCway to send commands to the panel
- **Encryption key**: you can enable the encryption and specify the key (optionally)
- Network enable: check
- Network protocol: TCP/IP
- **Receiver IP address**: the IP address you will assign to the SPCway, e.g.: 192.168.255.110
- **Receiver IP port**: the port the SPCway needs to listen on: e.g. 50000
- Always connected: check
- Primary receiver: check, if events are needed. See note below\*
- Event filter: turn on those events you need. IP Network congestion might be a consideration for not enabling all events. See note below\*



Note: events are used for true event forwarding, but also to optimise fast status updates (~ 100 ms). If for instance zone events are filtered, then the zone updates will have a typical maximal two second lag. This interval can be changed if needed. (See chapter 14 'Advanced Settings'.)

Before logging off, do not forget to exit the 'Full Engineer' mode.

The 5 values indicated in **bold red** above are needed to configure the SPCway.

This is what the form would typically look like:

Description	<input type="text" value="SPCway"/>	Description of receiver.
Receiver Id	<input type="text" value="99"/>	Unique identification number of EDP receiver used by this panel. (1 - 999997)
Protocol version	<input type="text" value="Version 2"/>	Select version of EDP protocol to use with this receiver
<b>Security</b>		
Commands Enable	<input checked="" type="checkbox"/>	Check if incoming commands are allowed from this receiver.
Change user PINs	<input checked="" type="checkbox"/>	Check if changing user PINs is allowed from this EDP receiver.
Virtual Keypad	<input checked="" type="checkbox"/>	Check to allow virtual keypad access from this EDP receiver.
Live streaming	<input type="text" value="Only after alarm event"/>	Select privacy options for live streaming to this receiver.
Encryption Enabled	<input type="checkbox"/>	Check if data to and from this receiver is encrypted.
<b>Network</b>		
Network Enable	<input checked="" type="checkbox"/>	Check if events can be reported through Network
Network Protocol	<input type="text" value="TCP/IP"/>	Select transport layer protocol over Ethernet.
Receiver IP Address	<input type="text" value="192.168.255.110"/>	IP address of receiver.
Receiver IP Port	<input type="text" value="50000"/>	IP port of receiver.
Always Connected	<input checked="" type="checkbox"/>	Check if panel should keep a permanent connection to the receiver. If not checked then panel will only connect to the receiver after an alarm event.
Panel Master	<input checked="" type="checkbox"/>	Check this to make the panel master of polling messages.
Polling Interval	<input type="text" value="10"/>	Seconds between polls
Generate a Network Fault	<input type="checkbox"/>	A polling failure will generate a network fault
<b>Dial-up</b>		
Dial-up Enable	<input type="checkbox"/>	Check if events can be reported through dial-up
<b>Events</b>		
Primary Receiver	<input checked="" type="checkbox"/>	Check if primary, clear for backup
Requeue Events	<input checked="" type="checkbox"/>	Check if events that fail to report are to be requeued for transmission.
Verification	<input type="checkbox"/>	Check if Audio/Video verification should be sent to this receiver.
Event Filter	<input type="text" value="Filter"/>	Configure which events are reported to this receiver

Figure 3: EDP receiver form

## 2 Hook up the SPCway

Three connections are to be made

- 1) Power supply to the 'DC 24V + & -' terminals.  
Any supply in the 'DC 12V - 24V' range will work. The typical power consumption approximately 1W. There are three possibilities to provide power to your SPCway:
  - A separate PSU (recommended)
  - The 12V connection from your SPC panel. If you were to choose this option, be sure to consider power consumption in the battery load calculation.
  - The third possibility is 24V passive power-over-Ethernet
- 2) LAN: plug in your Ethernet cable to connect the SPCway to the same LAN and subnet as the SPC panel.
- 3) KNX-EIB: Optionally, connect the KNX bus cable to the SPCway. You can also connect to the bus line (or to several lines in larger installations) through the KNX-IP (EIBnet/IP) protocol.

Your device is now starting up and ready in roughly one minute.

### 3 Logon to the SPCway website

Default configuration information of the SPCway:

Parameter	Value
Default IP address	Fixed IP: 192.168.0.10 Subnet: 255.255.255.0
Configuration login: Username & password	admin & admin
Hostname:	SPCway

Assure your pc (or tablet) is on the same subnet as your SPCway. In other words, it needs a similar IP address: 192.168.0.xxx. You can do so by configuring a fixed IP address for your LAN adapter (example 192.168.0.9).



**Note:** Google for 'assign static IP address windows' or 'assign static IP address iPad' if you need assistance with this.

Now open your browser and surf to <http://192.168.0.10> or to <http://SPCway.local/>

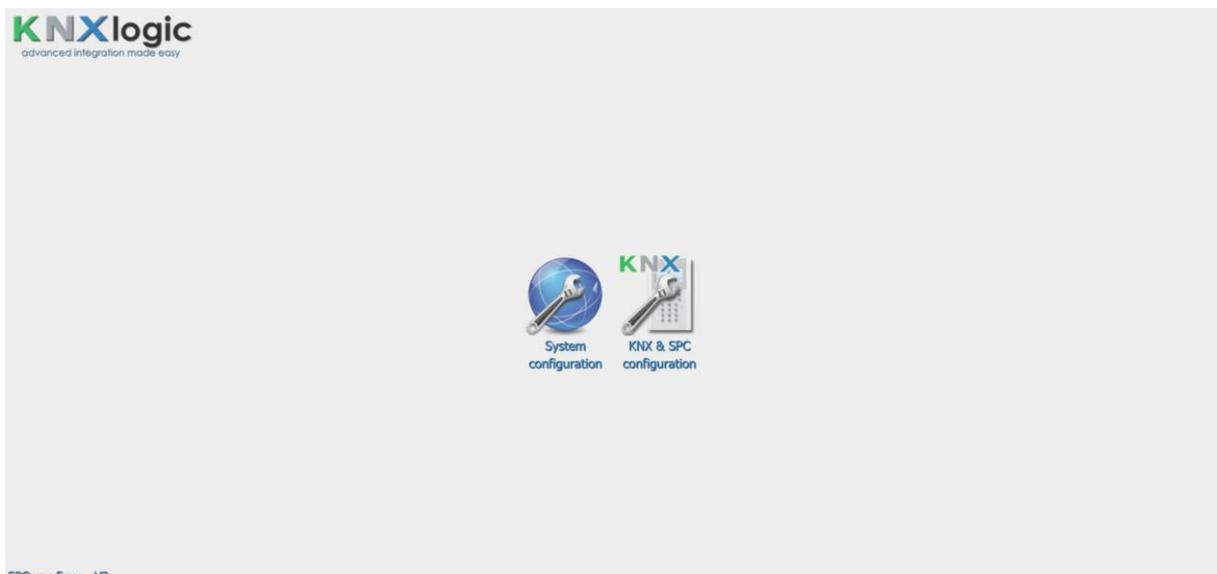


Figure 4: SPCway homepage

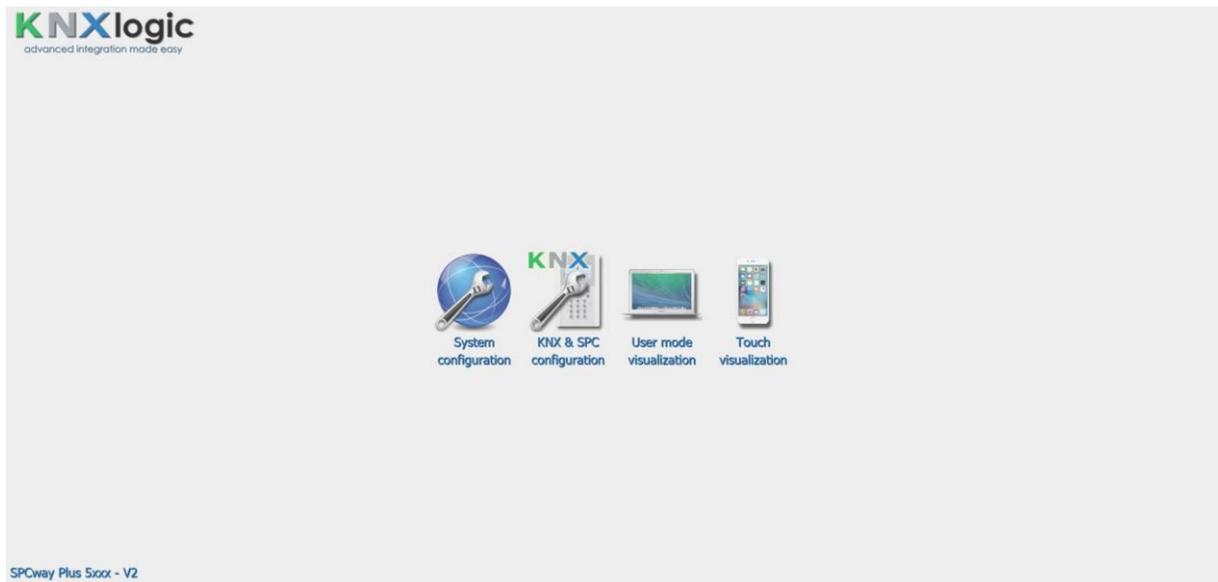


Figure 5: SPCway Plus homepage



**Note:** The two rightmost icons to access the visualization engine are only present on the SPCway Plus homepage.

All common configuration can be accessed from the '*KNX & SPC configuration*' page.

The '*System configuration*' page is only needed for very specific tasks or when instructed to do so.



**Note:** the use of the Hostname to surf to the device (SPCway.local by default) will only work from a tablet/pc/phone with '*zero config support*':

- Apple enabled devices: iPad, iPhone, Mac or PC with iTunes
- Android devices: Android is gradually adding '*zero config support*' to its operating system. From a device which is not yet enabled: install the free app 'ZeroConf Browser'. Under HTTP you'll find the SPCway with its IP-number. Surf to that IP number with any internet browser.
- From a PC without any Apple support: install '*Bonjour for Windows*' from Apple (or install '*iTunes*') and proceed as above.
- From a Linux device: assure you have a '*zero config service*' running such as '*Ahavi*'

## 4 Configure the network IP address

You will probably want a different network IP address. Contact your network administrator if you need assistance.

From the homepage open the 'KNX & SPC configuration' and log in.

Select tab 'KNX & SPC configuration' > 'Utilities' > 'System' > 'IP interface'. (or 'System configuration' > 'Network' > 'Interfaces') and click on the first and only interface 'eth0' to get the configuration window:

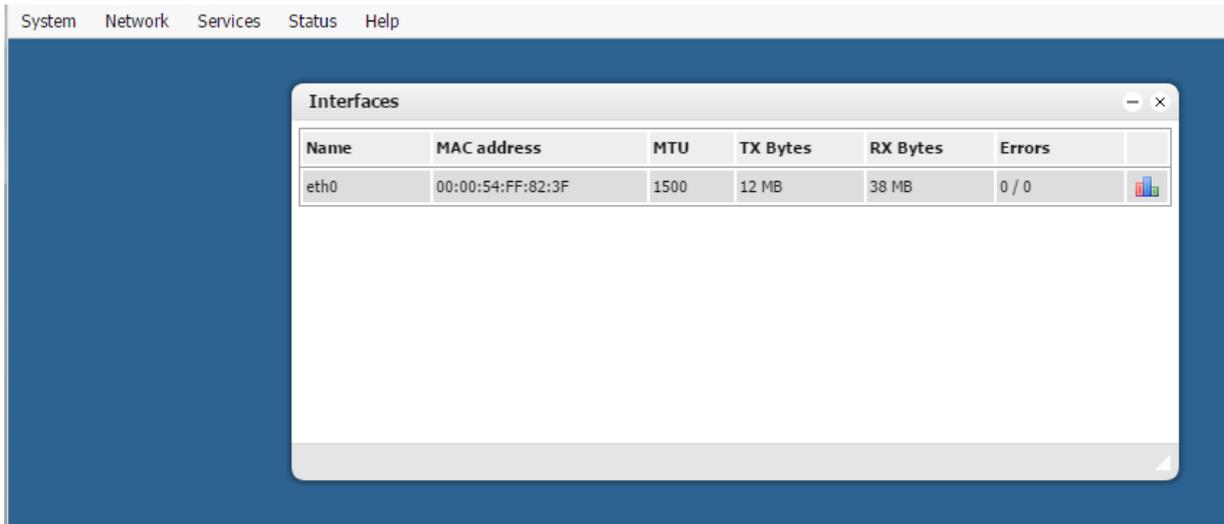


Figure 6: Network settings

This will open the interface configuration form:

Interface eth0

Protocol: Static IP

IP address: 192.168.255.110

Network mask: 255.255.255.0

Gateway IP: 192.168.255.1

DNS server 1: 8.8.8.8

DNS server 2: 8.8.4.4

MTU: [ ]

OK Cancel

Figure 7: Interface eth0

Now set the IP address in line with the **EDP client IP address** you entered earlier in the SPC panel.

## 5 Configure the device physical KNX address

The physical KNX/EIB address configuration is done through the web interface. ETS is not needed to configure the device.

From the Configuration page, go to: 'KNX & SPC configuration' > 'Utilities' > 'System' > 'KNX connection' (or: 'System configuration' > 'Network' > 'KNX connection').

The following screen will pop up.

KNX connection	
General   IP > TP filter   TP > IP filter	
Mode	TP-UART
ACK all group telegrams	<input type="checkbox"/>
KNX address	15.15.255
KNX IP features	<input type="checkbox"/>
Multicast IP	224.0.23.12
Multicast TTL	1
Maximum telegrams in queue	100

Figure 8: KNX connection

- 1) 'KNX address' (physical address): assign in line with your KNX line addressing.
- 2) 'Mode': If you have the KNX/EIB bus connected directly to the SPCway (on the red and black connector), then 'Mode' needs to be set to 'TP-UART'. If you want to connect through KNX-IP without a direct bus connection, then put 'Mode' on 'EIBnet/IP routing'.
- 3) 'KNX IP features': with a TP KNX/EIB connection, you can switch on/off the KNX-IP features if you wish. (when using any other mode, KNX IP is always required).

You don't need to change the other settings in this tab.



Note: when logging in to the configuration page, you will be prompted with a warning if no TP connection was found while mode is set to TP-UART. When confirming the popup, the configuration will be changed (mode= EIBnet/IP routing, KNX-IP features=enabled).



Note: When neither communication over TP or KNX-IP is possible, an error will be flagged in the Configuration page, at the bottom right corner:

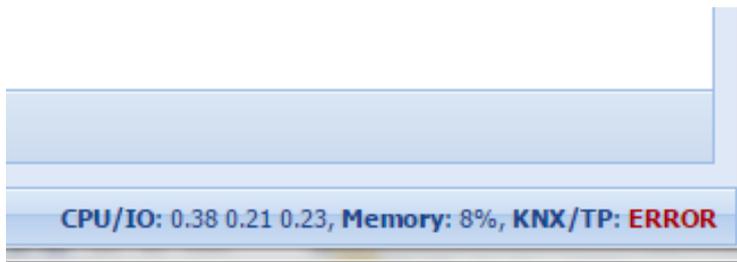


Figure 9: Error

## 6 Set the EDP client settings in the SPCway

From the configuration homepage select the 'KNX & SPC configuratie' > 'KNX SPC config' tab.

Select the listing of 'General' parameters:

Name	Value	Description
Panel ID	1000	The EDP ID of the SPC panel
SPCway ID	99	The EDP client ID for the SPCway
TCP port	50000	The TCP port, used by the panel to poll the connection

Figure 10: Tab 'General'

Here you can set the three remaining EDP client settings as configured in the SPC panel.

To set a parameter, click in the listing, fill in the value in the popup window and click 'Save'.

To configure the optional EDP encryption key, click 'Add new' and select 'Encryption' in the name field from the drop down menu:

Configure General SPCway parameter

Name: Encryption

Value: 0123456789ABCDEF0123456789ABCDEF

Description: The EDP encryption Key for the SPCway

Save Cancel

Figure 11: Encryption configuration

Once all three parameters are set, click the *'Reload configuration'* button (see above) in order to activate the changes.

Look in the *'Alerts'* tab to see if a stable connection is established.

You can now click the *'Panel config data'* button to see the element info retrieved from the panel. This info gets updated automatically every 10 minutes.

## 7 Configure the communication objects and group addresses

The SPCway offers the possibility to create group addresses in a very flexible way. Even for a small installation (4xxx based), one can easily imagine over thousand different communication objects to suit every possible need you might have.

Due to this extreme flexibility, communication objects and group addresses are configured through the web interface. ETS cannot be used to configure the device.

There are three types of communication objects you can create:

- Events (SPC -> KNX/Modbus)
- Statuses (SPC -> KNX/Modbus)
- Commands (KNX/Modbus -> SPC)

A status is an information regarding the **state** of an element. An essential concept of a state is that a state is always valid. Any event that invalidates the state (as defined) will result in a change of state. The only limitation on this is related to the polling and update frequency of a state. For more information regarding status update frequency see section 14.3 '*Advanced General settings*'.

Events and Commands are linked to **an event** of the SPC panel. An essential concept of an event is that it is only valid at the moment of the event. It loses its meaning immediately after that moment because another event can have occurred invalidating the former event. Example: a command 'arm perimeter' @ 10:00:00 only means that at that moment such command was raised (and may or may not have changed a state of the SPC). Looking at the value of the command @ 10:00:01 doesn't tell anything about the state of the SPC panel, since another command might have been given in the mean while (through another KNX command, direct user interaction ...)

### Terminology:

- 1) Further in this document, the term '*element*' is used. Referring to such '*element*', refers to one of the 'assets' managed by the SPC panel: a zone, an area, a door, a user, an output, a camera, an expander, a node or a modem.
- 2) When referring to the element type '*Output*', we refer to the broadest meaning of the term, in line with the SPC Installation manual term '*Output*': a Mapping gate (see section '*Configuring advanced settings*' of the SPC Installation manual). Such a mapping gate may be linked inside the SPC panel to a physical output, but this is not required.

For the first 5 '*element*' types listed above, the SPCway will get the list of configured elements from the SPC panel. This information is consultable on the '*Panel config data*' button and in the form control tip texts.

## 7.1 General information

For each type of communication objects there is a separate listing on the 'KNX SPC config' tab. Click the button to show the listing.

To add a new communication object, click 'Add new'

Class	Event	Element ID	Option	KNX object	KNX value	Description	Dupl...	Active	
Doors	Access Granted	1	*	1/2/3	1	send 1 in case somebody gets access at door 1			

Figure 12: Object row

**Duplicate Communication Object** ✕

Number of duplicates:  

Increment object GA's (ID):  

Figure 13: Duplicate form

From the listing you can:

- edit the object: click any text field on the row. (See figure 12)
- duplicate a communication object: click the duplication icon of the row, you can adjust the number of duplicates and the increment object GA's (ID)
- activate/deactivate a communication object: click the red/green round
- delete a communication object: click the delete icon of the row
- sort the objects: click on the required sort field in the header.

## Editing generalities

When editing or creating a new communication object an edit form will appear:

Figure 14: Object configuration screen

- The first field is always the 'Class'. Since there are many commands, events and statuses, the *Class* allows to reduce the long list and find what you need faster.
- The second field is always the selected event, status or command.
- 'Active' field: you can have the communication object active or inactive. When inactive, the SPCway will not consider the communication object.
- 'Description' field: a free text field.
- After making changes, you need to 'Reload' the configuration in order to take effect.

For most of the fields, there are control tip text boxes that appear when moving your cursor/mouse over the field. They give additional help to fill in the field. Example: when you need to fill in a zone ID, the tip text will show the list of all existing zones in the panel.

Doors	▼	ess door 2
Access Granted	▼	it door 2
1		it door 2
1		* : All
<input checked="" type="checkbox"/>		n, m, ... : multiple ID's
1/2/1		it door 2
		it door 1
		it door 1

Figure 15: Tiptext



**Note:** In annex 1, 2 and 3, you can find the tables with the possible objects.

## 7.2 Event

Events are raised on a given moment and indicate that something happens at a given moment in time. Once the event has been sent on the KNX bus, the last value of the event will persist, however, this might no longer represent the actual status. Events are in line with the SIA event definitions.

There are 135 different types of events distributed over 15 classes. See annex 1 for more information on the possible events.

After selecting the *Class* and *Event* field:

- Specify the *element ID*: most events are raised for a specific Element type (see annex 1). In most cases you can identify for which element you want to create a communication object. This is what you put in the third form field.

Allowed values:

- a single element ID: e.g. '2' to report an event on door 2 only
  - a comma separated list of element ID: e.g. '2, 4'
  - '\*' to trigger the communication object on all elements
- Filter, for specific events: a limited number of events can be filtered even further because they are associated with a secondary element type (see annex 1). E.g., the *door open event* can be filtered on the user who triggers the event. When filtering is possible, the field in the form will be enabled after choosing the event type. If filtering is possible then the *Filter* field is mandatory. The Field description indicates on what element type you can filter, e.g. '*Filter on Area ID*'.

Allowed values:

- The filter can only be one element ID.
- If you do not want filtering, set it to '\*'.



**Note:** If you want to filter on multiple ID's, then duplicate the communication object configuration and modify the filter value.

- '*KNX group address*', '*KNX data type*': specify on which group address and with what data type the event needs to be reported. Even if you only need the Modbus side of the interface you still have to specify these values: the Modbus object (register/coil) definition is mirrored with the KNX objects.

- 'KNX value': the value to be sent when the event occurs. It can be :
  - an explicit numeric value (in line with data type) e.g. '1'
  - an explicit string value (data type *string* required)
  - IV: **ID Value** = textual description/name of ID (data type *string* required)
  - FV: **Filter Value** = textual description/name of the Filter (data type *string* required), if present
  - SV: **SIA** 2 letter code, followed by the **ID Value** (data type *string* required)
  - SI: **SIA** 2 letter code, followed by the **ID number** (data type *string* required)
  - TS: the **TimeStamp** of the event in time of the SPC panel (data type *time* required)



Note: multiple events can report to the same address. In that case different events can send different values



Note: one event can be linked to multiple communication objects. If the event is raised, all objects will be verified and sent when applicable.

## 7.3 Status

A status describes at any moment in time the actual state of an element or the system.

A status telegram is, by default, only sent when the status changes. The gateway will also respond to a read request on the configured group address.

There are 25 types of states grouped in 6 classes.

The status form upper part is similar to the event form, see section ‘General info’ above.

Figure 16: Configure status

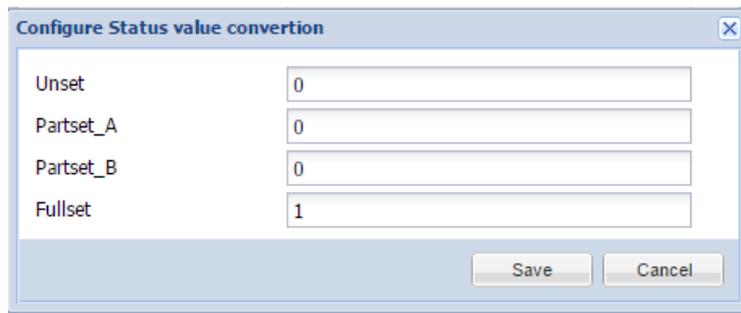
The specific fields for the status communication objects are:

- ‘Possible values’: this lists the native possible values of the status. Information only, see Annex 2. When there is no limitative list of possible values, this field is blank; e.g. the name of a User.
- ‘Resend interval’: if specified, the telegram will be resend periodically with this interval (seconds), even if the value did not change.
- ‘Resend @ value’: if a ‘resend interval’ is specified, and if also this value is specified, then the resend will only occur if the value to be send corresponds to the ‘Resend @ value’. If left blank, the periodic resend will occur for any value.

- '*Status type*': defines what needs to be done with the raw status value received from the SPC panel.

Possible values:

- '*Status string*': try to convert the raw value to a string and then send.
- '*Status value*': try to convert to a numeric value, then send.
- '*Converted*': define a conversion table. For every possible predefined value you can specify what value needs to be send.
- '*Conversion table*': the button will enable when the Converted status type was selected. This opens a form such as this (for the example form above):



Label	Value
Unset	0
Partset_A	0
Partset_B	0
Fullset	1

Figure 17: Configure conversion



**Note:** after the '*Status type*' based convention, the gateway will try to translate the value into a KNX telegram of the specified KNX data type and send it on the KNX bus.

## 7.4 Command

The SPCway can send 22 different types of commands, grouped in 5 classes. See Annex 3 for a list of these commands.

Upon receiving a value or telegram on the KNX bus or Modbus, the command will be executed on the panel. Optionally a command feedback can be reported on a feedback communication object.

The status form upper part is similar to the event form, see section 'General info' above.

Figure 18: Configure command

On top of the generic fields like the *Class* and the command name, the command specific fields are:

- '*Element ID*': for most commands, it needs to be specific on which element (e.g. which door) it needs to be applied.

Possible values:

- one element ID
- a comma separated list of element ID's: the command is applied to all listed
- the predefined value 'CV' = **Command Value**: the value received on the command object is used as *element ID* for the command

- '*Option*': on certain specific commands a second option argument is needed (see annex 3). When available, the *option* field becomes enabled and is mandatory.

Allowed values are:

- the explicit value to be used, e.g. '1' for audio message 1
- the predefined value 'CV' = **Command Value**: the value received on the command object is used as *option* for the command
- '*Send value filter*': when specified, the command will only be executed when the command telegram value corresponds to the value. If not matching, then the command request is discarded for this configuration (and reported on the feedback).
- '*KNX feedback object*': when a group address is specified, it creates a communication object to report the error/success of the command. The datatype of this communication object is always 8bit-Unsigned Integer.

Possible values are:

- 0 = success
- 2 = error, due to configuration
- 12 = error, panel in full engineer mode
- 13 = error, panel not ready to receive such command
- 14 = error, command not enabled
- 15 = error, command not implemented
- 16 = command not initiated: filtered out (*Send value filter*)
- 17 = command issued but no panel reply



#### Advanced ETS

In case you want to rely on certain advanced ETS functions (filter tables) then use a dummy KNX device to virtually assign group addresses. Read the similar instructions in the document '[ComfoWay – KNX and ETS usage](#)' which you find on our website.

### 7.4.1 Watchdog command

The watchdog command (in the *System* Class) is a special command. This command is processed internally by the SPCway only and is not forwarded to the SPC panel.

The purpose is to be able to verify from an external source if the SPCway is still functional.

When send a command value to this command, the value is echoed onto its feedback object, so the feedback object values defined above do not apply to this object.

Since the feedback object is fixed at datatype 'unsigned byte', the most common sense choice for the command object datatype is 'unsigned byte'. However, this is no absolute requirement.

The SPCway will try to convert the incoming value of the command to a unsigned integer for feedback: if a command string type is used, and the string '12' is sent, the feedback object will still echo integer 12.

Typical delay between command and echo should be less than 200 ms.

## 8 Modbus

### 8.1 Modbus configuration

The Modbus configuration consists of three aspects:

- The modbus connection
- The Modbus communication objects
- The Modbus profile parameters

#### 8.1.1 Modbus connection

The Modbus connection can be configured with four parameters.

In the '*General configuration settings*', the following modbus parameters are available. They can be added by using the '*Add*' button.

- modbus.connect.type

Meaning: identification of the physical/logical layer of the communication.

Allowed values: rtu or tcp; rtu uses the rs-485 terminals

Default (if not specified): tcp

- modbus.connect.params

Meaning: configuration of the communication.

Allowed values: a comma separated list of parameter-value pairs: parameter='value'.

The allowed parameters depend on the modbus.connect.type setting

- In case of rtu :

- rsport: which physical serial port to use RS485 or RS232

Default value: RS485

- baud

Allowed values: 110, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 500000

Default value: 9600

- databits

Default Value: 8

- stopbits

Default Value: 1

- parity: the parity bit used

Allowed values: E (even), O (odd), N (none)

Default Value: E

- duplex: the duplex setting used

Allowed values: H (half), F (full)

Default Value: H

- In case of tcp :

- ip : IP address or FQN of master/server

Default value: 192.168.0.20

- ipport: IP port listening for Modbus communication

Default value: 502

- modbus.connect.slaveid

Meaning: identification the Modbus slave-id of the SPCway

Allowed values: integer values

Default (if not specified): 10

- modbus.connect.disabled

Meaning: used to enable/disable the Modbus feature

Allowed values: true or false

Default (if not specified): false

### 8.1.2 Communication objects

The application layer Modbus communication objects are mirrored on the KNX communication objects: they are identical to the KNX communication objects as configured on the '*KNX SPC config*' tab, resulting in the automatically generated Objects listed on the '*KNX objects*' tab.

Objects added manually on the '*KNX objects*' tab, or added by the KNX buss sniffer, but which are not the SPC configured objects will not be mirrored in the Modbus profile.

### 8.1.3 Profile parameters

The following parameters can also be added to the '*General*' parameters.

- modbus.profile.usecoils

Meaning: indicates if coils are to be used (for the 'bit' application data type objects), or always use registers including for 'bit' objects.

Allowed values: true or false

Default (if not specified): false

- modbus.profile.stable

Meaning: indicates how the Modbus profile file and addresses needs to be organized. In a 'stable' profile, the object base address only depends on the internal configuration ID of the object. As a result, in such profile the addresses of objects will never change when changing (adding/deleting/modifying) the SPCway objects configuration. In a 'non-stable' profile the objects are grouped per coil/register datatype, Read/Write property and application datatype. This results in an easier to read profile. Small changes are unlikely to modify the addresses of the objects, but large changes will most certainly change also Modbus addresses of unmodified objects.

Allowed values: true or false

Default (if not specified): false

## 8.2 Modbus profile

The Modbus objects are mirrored with the KNX objects. All Modbus relevant data of these objects are stored in a 'Modbus profile'.

From the SPC KNX config tab the description of the Modbus interface in terms of communication objects can be downloaded through the appropriated button.

The profile can be downloaded as text/html or as a csv file for easy editing.



**Note:** in any case, only the readable-writeable coils and registers are used. In other words: only 'discrete inputs' and 'holding registers' are used. 'Coils' and 'input registers' are not used. The 'Read/Write' property of an object does not change that.

The profile is a table with the following columns, each representing a property of the objects listed as rows:

- '*Name*': name of the communication object, identical to the name found/generated in the 'KNX objects' tab.
- '*Type*': indicates if the raw Modbus datatype used is a coil or register.

- *'Read/Write'*: indicates if the object is R = Read only or W(R) = Write / Read. This property has no raw Modbus meaning (see note above). It only has a meaning at application level: when a value is written to a 'discrete coil' or 'holding register' which is not of type 'W', the received value will be dropped by the SPCway and the internal data table will not be updated. (When reading the value subsequently, it will still hold the old internally written value.)
- *'Address'*: the Modbus address of the first element of the object, in the 'true sense' of the protocol description. One object can be represented by several elements (see Length), depending on application data type used. (See *'Data Type'*)
- *'Address'*: the 2<sup>nd</sup> address columns holds a combination of the object Modbus type number and the address number.
- *'Data Type'*: the application datatype use to represent the object value. (See next chapter)
- *'Length'*: the number of elements (coils or registers) to represent this object. The address range start with the *'Address'* and continues till offset *'Length -1'*, relative to the *'Address'*.
- *'ID'*: internal unique and fixed ID of the object. When the option 'stable profile' is used, the *'Address'* solely depends on this *'ID'*.
- *'GA'*: KNX object Group Address, corresponding to this object, as listed in the *'KNX Objects'* tab.

#### Modbus SPC panel profile

Name	Type	Read/Write	Address	Address	Data Type	Length	ID	GA
CMD Set an area on id 1,2 (on CV 1)	register	W(R)	0	4x00001	bit	1	17	1/0/2
CMD Unset an area on id 1,2 (on CV 1)	register	W(R)	1	4x00002	bit	1	18	1/0/3
CMD Set a door to normal mode on id 1 (on CV 0, #2)	register	W(R)	2	4x00003	bit	1	78	1/0/40

Figure 19: Modbus profile

### 8.3 Application level datatypes

The Modbus protocol only consists of 2 formal base datatypes: bit (=coil) and 2-byte (=register)

However, on application level one or more bits/bytes are given a specific meaning. How to interpret these bits/bytes is determined by the application level datatypes. The datatypes used in the Modbus interface are specified below.

All register example values in in hexadecimal notation where the 16 bits are listed as 4 4-bit hex values with a 'h' suffix: 1234h =  $1*16^3 + 2*16^2 + 3*16^1 + 4$



**Note:** when an application datatype such as uint16 is used, it doesn't mean that all integer values that can be represented are valid values: this depends on the objects settings in the KNX SPC configuration.

The following application datatypes are currently used in the Modbus interface:

- bit: represents a binary value 1 or 0 equivalent to true or false. Depending on the modbus.profile.usecoils parameter, this datatype is mapped to either 1 coil or 1 register. When a register is used only the LSB is considered.

coil offset 0: bit

register offset 0: LSB

examples: A001h = true, 26F0h = false

- uint16: this datatype is mapped to 1 register. It represents an integer value 0-65535.
  - register offset 0 : integer 2-Byte value
  - example: 1001h =  $1*16^3 + 1$
- uint32: this datatype is mapped to 2 registers. It represents an integer value 0 – 4294967295.
  - register offset 0 : Least Significant 2-Byte value
  - register offset 1 : Most Significant 2-Byte value (is shifted 16 bits)
  - example: 0001h 1001h =  $1 + (1*16^3 + 1)* 2^{16}$

- string14: this datatype is mapped to 7 registers. It represents a 14-character string in 7-Bit ASCII codes

register offset 0 : MSByte = char 2; LSByte = char 1

...

register offset 6 : MSByte = char 14; LSByte = char 13

example: 6854h 7369h 6920h 2073h 6574h 7473h 0021h = 'This is test!'

- datetime: this datatype is mapped to 7 registers. It represents a time and date indication.

register offset 0 : Byte representing year

register offset 1 : Byte representing month

register offset 2 : Byte representing day

register offset 3 : Byte representing weekday (1-7 = sun-sat)

register offset 4 : Byte representing hours

register offset 5 : Byte representing minutes

register offset 6 : Byte representing seconds

example: **07DFh 0003h 0009h 0004h 000Ch 0005h 0010h**

= **12:05:16 Wednesday 9 March 2015**

-



Note: there is no KNX datatype that can hold both time and date in a single object. As a result, not all subvalues of the type will contain data. In case of a dt.time KNX datatype object, only the last 4 contain info (others '0'). In case of dt.date only the 3 first contain info, whilst the others are '0'.

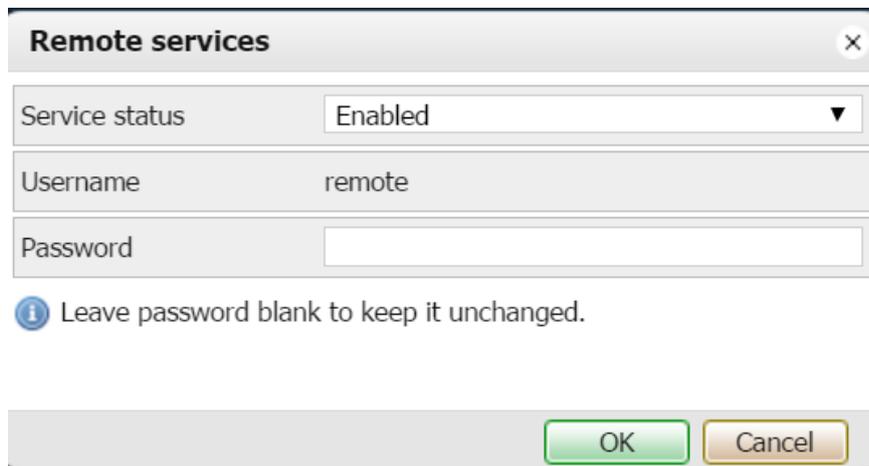
## 9 BACnet & API (Plus features)

The SPCway Plus product variant has two more protocol interfaces over and above the KNX and Modbus interface of the SPCway: BACnet and an API based interface.

Both interfaces work transparently with and just like the existing protocol interfaces. Any change that is made in either protocol is automatically synchronized with the other enabled protocols and objects.

Both protocols are part of the 'Remote Services' the SPCway Plus offers. To use any of these two, the following steps must be followed in order to make the configured communication objects available on the respective protocols:

- 1) Enable 'Remote Services' in 'System Configuration' > 'Services' > 'Remote services'.  
If desired, you can modify the default password (= 'remote'). This only applies to the API feature.



**Remote services** [X]

Service status: Enabled ▼

Username: remote

Password: [ ]

*i* Leave password blank to keep it unchanged.

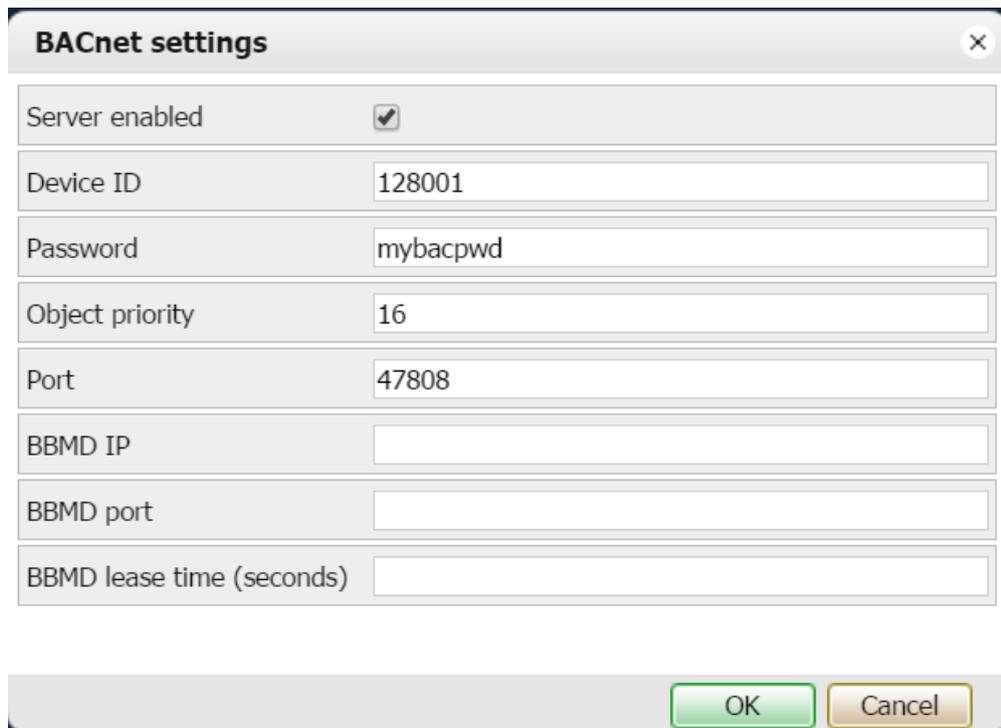
OK Cancel

Figure 20: Remote services

- 2) Select which of the Communication objects are to be exposed in the remote services: check the 'Remote' property of the objects in the 'KNX Objects' tab of the SPCway main configuration page.

## 9.1 BACnet

To configure BACnet, some additional parameters of the SPCway BACnet server can be set. First the BACnet service must be enabled. Both the enable and the general BACnet server settings can be made in 'System configuration' -> Network -> 'BACnet settings':



The image shows a dialog box titled "BACnet settings" with a close button (X) in the top right corner. The dialog contains several configuration fields:

Server enabled	<input checked="" type="checkbox"/>
Device ID	128001
Password	mybacpwd
Object priority	16
Port	47808
BBMD IP	
BBMD port	
BBMD lease time (seconds)	

At the bottom of the dialog, there are two buttons: "OK" (green) and "Cancel" (yellow).

Figure 21: BACnet settings

Once enabled, the list of BACnet objects can be consulted under: 'System Configuration' > 'Network' > 'BACnet objects'.

**BACnet objects**

Name: ComfoWayPlus\_128001 Download CSV

Device ID: 128001

Object priority: 16

Port: 47808

Type	Instance	Name	Current value
2 (AV)	12288	Volume control (6.0.0)	1
2 (AV)	12289	Comfort temperature (6.0.1)	23
5 (BV)	12290	Supply air (6.0.2)	true
5 (BV)	12291	Extract air (6.0.3)	true
5 (BV)	12293	Filter timer reset (6.0.5)	true
5 (BV)	12294	Error reset (of ComfoD) (6.0.6)	true
2 (AV)	12295	filter Dirty weeks (6.0.7)	17
5 (BV)	12297	Boost mode active (6.0.9)	true
2 (AV)	12298	Boost mode duration (6.0.10)	30
2 (AV)	12348	Manuel volume control (6.0.60)	1
5 (BV)	12349	Automatic volume control (6.0.61)	false
5 (BV)	12353	Manuel volume control - Away	true
5 (BV)	12354	Manuel volume control - pos 1	false

Figure 22: BACnet objects

With the Download CSV, an EDE-like file can be downloaded with the BACnet object definitions to be used/imported in other external BACnet configuration tools.



Note 1: Objects must be activated individually to participate in the remote services. See above. If an object is missing in the BACnet list, make sure you check the 'Remote' flag of the object.



Note 2: All BACnet objects are automatically generated: they are mapped from the base (KNX) objects to BACnet objects with corresponding analog or digital value type. KNX Boolean type become a digital value, all other numerical types become an analog value. KNX string objects are not mapped, since no string variable type exists in BACnet.



Note 3: BACnet object description length is limited. This may lead to duplicate (at first sight) objects. But this is due to length limitation. The order of the BACnet objects corresponds to the objects in the 'Objects' tab. The Objects address (in integer value notation) corresponds to the BACnet object identifier value.



In order for a BACnet device to be discovered, the appropriate IP settings must be made with matching network mask settings, since discovery of BACnet devices is by broadcast on the corresponding subnet.



Note: To verify BACnet functionality several freeware tools can be used to interrogate the SPCway BACnet server, such as 'Yabe' : 'Yet Enother BACnet Explorer' which can be found on sourceforge.

For further information, see also Annex 4.

## 9.2 API

It is possible to interact with the SPCway objects bidirectionally with an URI based API over http/https.

The supported data formats are json and XML.

The full description of this API is available in a dedicated document. Check the website documentation page or contact us on [info@KNXlogic.eu](mailto:info@KNXlogic.eu).

## 10 Visualization (Plus feature)

For the SPCway Plus two more icons appear on the landing webpage. They allow to login and use the visualisation engine/server embedded in the SPCway:

- In user mode: this mode is optimised for large screen (laptop, tablet, ...) utilisation, with full graphic layout possibilities
- In touch mode: this mode is optimised for smartphone use, with a tabular format and simplified graphics

No special or licenced application is required: the server is consulted through a web browser.

The visualisation engine can be entirely edited inside the SPCway, and a separate visualization manual exists explaining all the ins and outs.

The additional tabs appearing in the SPCway configuration page related to the visualization engine are:

- *'Vis. Structure'*:
  - allows to define the tree-like structure of buildings, floors or plans.
  - allows to set certain parameters for these items (visibility in the modes, pincode, name ...)
  - allows to import and export visualisation elements for faster configuration and reuse of existing layouts.
- *'Visualisation'*:
  - This is the main editor where the layout of the pages are configured
  - Different types of visualisation elements can be added and configured: objects, labels, graphs, links, gauges, frames (to embed other URL pages) and video.



Note: the engine will itself convert a 'User mode' page (as configured in the editor), into a Touch page. This conversion can be tuned in the editor (see separate manual)

- *'Vis. Graphics':*
  - Upload and manage icons to be used in the visualisation elements.
  - Upload and manage background images for the floors/plans.
  - Customise CSS stylesheet.
  
- *'Users':*
  - Allows to manage additional user profiles for the visualization access and specify their rights for all elements in the building/floor tree

A dedicated Visualisation Guide exists, as well as example layout and icon set, which can be downloaded from our site and directly imported into your SPCway Plus.

## 11 Security considerations

When interfacing the SPC panel certain security consideration and recommendations are relevant. Depending on LAN/BACnet/KNX/Modbus network architectures, one or more recommended measures are to be considered. It is up to the system integrator to assess the necessity of these and other measures. The present chapter is not meant to give an exhaustive list or a ready solution but rather to serve as a checklist starting point.

Possible security measures inside the SPCway:

- Use EDP encryption to create a safe tunnel between SPC panel and SPCway.
- Disable the use of all commands from the EDP client inside the panel.
- Only implement command objects required for the desired functionality. Do not expose commands which are not needed.
- Use obfuscation techniques on implemented command objects by using non obvious command datatypes and specific command values, aka. the command 'Send value filter'. E.g. telegram on object 1/2/3 with temperature datatype and 23°C value means 'Arm area 1'.
- Use the Command feedback telegram only during setup and commissioning, but rely on status changes for actual use.
- Use advanced obfuscation techniques and KNX sender address filtering/verification by using event scripts (with SPCLib solution only, contact us for information & assistance).
- Enabled remote services only when needed.
- Enable remote services only for those objects needed (in particular commands).
- Modify the default remote services password when using API remote services.
- Only use secure https API URI's.
- When not using KNX-IP, then disable the service.
- When using KNX-IP, then change the multicast address to a project specific address.
- When using KNX-IP between multiple SPCway's, then use multicast message encryption.
- When using KNX, use KNX-IP filtering rules and filtering at object level (with dedicated TP line) to limit object availability on the bus/IP.

- When enabling security sensitive commands or statuses in the SPCway visualization, use the available access control features:
  - Create user accounts per user or profile, with only the respective rights at floor level (and thus at object level)
  - Add pin codes (4, 6 digits or more) in line with local policies. These can be added at Building, floor and element level.
- Modify the default admin password.
- Only use https to login to the SPCway.
- Protect the SPCway from physical access.

## 12 Interface language

The default language of the user interface is English. If you need your user interface in another language, select one of the available languages in the top left corner of the 'KNX & SPC configuration' page.

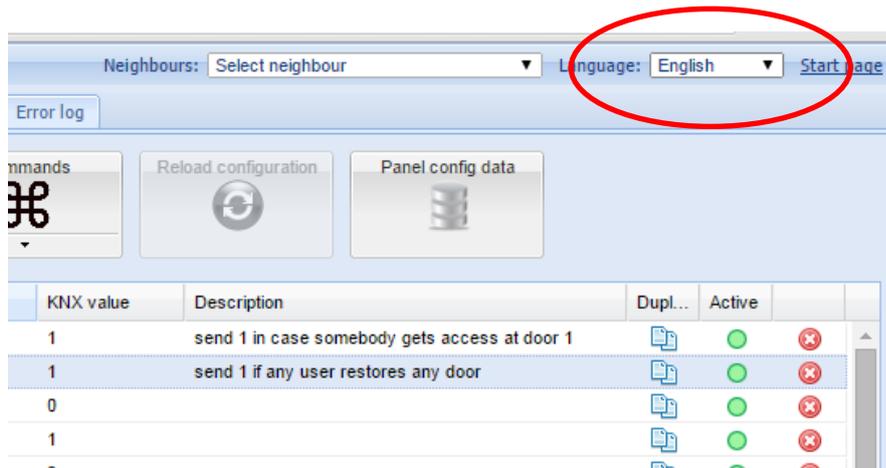


Figure 23: Change language

If you want to contribute a missing translation, please contact us for the conditions we offer.

## 13 Supplementary features

### 13.1 KNX Objects

A list of all managed KNX objects can be found in the ‘KNX objects’ tab.

The screenshot shows the 'KNX Objects' tab in the SPCway software. The interface includes a sidebar with filters and a main table listing various KNX objects. The table columns are: Group ad..., Object name, Data type, Current v..., IP > T..., TP > I..., Log, Ex..., Updated at, and Set v... The table contains 20 rows of data, including objects like 'EVT Door Restoral on id \* for id \*', 'CMD Open a door momentarily o...', 'CFB on command ga 3/3/1', 'EVT Zone Open on id 1, value 1 (...)', 'EVT Zone Open on id 9, value 1 (...)', 'EVT Zone Close on id 4, value 0', 'EVT Close Area on id 1, value 2 (...)', 'EVT Close Area on id 2, value 2 (...)', 'EVT Close Area on id 3, value 2 (...)', 'EVT Access Granted on id \* for i...', 'EVT Access Granted on id \*, valu...', 'EVT Access Granted on id \*, valu...', 'EVT Access Granted on id \*, valu...', 'EVT Zone Open on id 1, value TS', 'CMD Set an area on id CV', 'CMD Open a door momentarily o...', 'CMD Silence All Bells', 'CMD Audio Challenge on id 1, 2, ...', 'CMD Set a door to normal mode ...', and 'CMD Set an area on id 1, 2, 3 (on...'. The bottom of the interface shows a status bar with 'Page 1 of 3' and 'IP > TP policy: None; TP > IP policy: None Display'.

Figure 24: 'KNX objects' tab

In this tab you can:

- Consult the existing KNX objects.
- Add objects (which are not parts of the SPCway configuration)
- Modify object settings.



**Note:** for those objects created by the SPCway, you should not change the settings such as name or data type. When you do, they will be reset by the SPCway protocol daemon after some time.

- You can modify filtering.
- Write a value to the KNX bus: click on the 'set value' icon to the right of the row listing.

- Delete objects: again, for objects created by the SPCway: you should not delete. When an object is no longer configured, the SPCway daemon will remove it for you.
- Filter the list by the panel on the left.

### Object naming

When creating the objects, the SPCway will try to give a clear name to facilitate the use of the 'KNX objects' tab and the 'Logging' tab. When multiple events/status/command are linked to one object, this is indicated by '(# n)', where  $n$  is the number of links.

### Automatic object discovery

If you wish, you can have the SPCway discover and list all KNX objects it detects on the bus. For that purpose, you need to activate the bus sniffer. Go to 'Utilities' > 'General Configuration' > 'Bus sniffer'.

## 13.2 Objects Logging

All objects which are listed in the KNX objects tab, and for which the logging is activated, will be logged in the SPCway. The size of the Log can be set in the 'Utilities' tab.

**SPCway - Panel and Object Configuration** Neighbours: Select neighbour Language: English Start page

KNX SPC config KNX Objects **KNX Object logs** Utilities Alerts Logs Error log

Object log filter

Start date:

End date:

Name or group address:

Tags:

Value:

Source address:

Apply filter Cancel

Log time	Object add...	Object name	Type	Source ad...	Decoded value	Data type
14.01.2015 17:10:41	11/0/33	EVT Zone Open on id 1, value TS	write	15.15.255	17:09:42, Wednes...	10. 3 byte time / day
14.01.2015 17:10:41	11/0/3	EVT Zone Open on id 1, value 1 (#2)	write	15.15.255	1	01. 1 bit (boolean)
14.01.2015 17:10:38	11/3/11	STS Zone state on id 1	write	15.15.255	0	01. 1 bit (boolean)
14.01.2015 17:10:38	11/0/3	EVT Zone Open on id 1, value 1 (#2)	write	15.15.255	0	01. 1 bit (boolean)
14.01.2015 17:10:35	11/3/11	STS Zone state on id 1	write	15.15.255	1	01. 1 bit (boolean)
14.01.2015 17:10:35	11/0/33	EVT Zone Open on id 1, value TS	write	15.15.255	17:09:37, Wednes...	10. 3 byte time / day
14.01.2015 17:10:35	11/0/3	EVT Zone Open on id 1, value 1 (#2)	write	15.15.255	1	01. 1 bit (boolean)
14.01.2015 17:10:30	11/3/2	STS Area mode on id 1	write	15.15.255	0	01. 1 bit (boolean)
14.01.2015 17:10:28	11/3/12	STS Zone state on id 2	write	15.15.255	0	01. 1 bit (boolean)
14.01.2015 17:10:26	11/3/11	STS Zone state on id 1	write	15.15.255	0	01. 1 bit (boolean)
14.01.2015 17:10:26	11/0/3	EVT Zone Open on id 1, value 1 (#2)	write	15.15.255	0	01. 1 bit (boolean)
14.01.2015 17:10:25	11/3/12	STS Zone state on id 2	write	15.15.255	1	01. 1 bit (boolean)
14.01.2015 17:10:24	11/3/11	STS Zone state on id 1	write	15.15.255	1	01. 1 bit (boolean)
14.01.2015 17:10:24	11/0/33	EVT Zone Open on id 1, value TS	write	15.15.255	17:09:25, Wednes...	10. 3 byte time / day
14.01.2015 17:10:24	11/0/3	EVT Zone Open on id 1, value 1 (#2)	write	15.15.255	1	01. 1 bit (boolean)
14.01.2015 17:10:19	11/3/11	STS Zone state on id 1	write	15.15.255	0	01. 1 bit (boolean)
14.01.2015 17:10:19	11/0/3	EVT Zone Open on id 1, value 1 (#2)	write	15.15.255	0	01. 1 bit (boolean)
14.01.2015 17:10:16	11/3/11	STS Zone state on id 1	write	15.15.255	1	01. 1 bit (boolean)
14.01.2015 17:10:16	11/0/33	EVT Zone Open on id 1, value TS	write	15.15.255	17:09:18, Wednes...	10. 3 byte time / day
14.01.2015 17:10:16	11/0/3	EVT Zone Open on id 1, value 1 (#2)	write	15.15.255	1	01. 1 bit (boolean)

Clear Export all logs Page 16 of 51 Displaying logs 301 - 320 of 1001

Version: 20141127 CPU/IO: 0.11 0.13 0.18, Memory: 8%, KNX/TP: ERROR

Figure 25: 'Logging' tab

You can use the left pane to filter the log.

### 13.3 Alerts, Logs and Error log

In the interface you will also find three tabs; *'Alerts'*, *'Logs'* and *'Error log'*, which you normally do not need once everything runs fine. However, in order set up the SPCway, this can provide helpful information.

In normal operation, there will be very little messages in these three tabs.

However, if configuration issues are found, these will be reported here.

Example: if the EDP ID of the connected SPC panel does not match the configured ID, the connection will be stopped and reported in the *'Alerts'*.

This provides helpful information to diagnose the configuration.

If needed you can increase the verbosity of the alerts and logging. See the advanced settings section for more details.

### 13.4 Back-up and restore

It is recommended to often make a back-up of your data. This can be done via *'KNX & SPC configuration' > 'Utilities' > 'Back-Up'*. To restore a back-up on your device, click the *'Restore'* button, next to the *'Back-up'* button.

## 14 Advanced settings

### 14.1 Hostname

You can change the hostname (ie 'SPCway'): 'System Configuration' -> Menu 'System' -> 'Hostname'



**Note:** If you don't use an internal DNS service, then you can use the hostname of your SPCway. Simply go to <http://SPCway.local/> and all Apple enabled pc's and tablets will find your SPCway on the network. On Android, install the free 'Zero Config Browser' to easily find your SPCway



**Note:** If you have an internal DNS, then the network administrator can define a network name and IP-lease for your device.

### 14.2 KNX-IP router & filtering

The SPCway can be used as a KNX-IP router with advances filtering features.

When KNX-IP features are enabled, all telegram will be exchanged between the TP and the IP side.

In order to limit traffic in either or both directions, filters can be defined. These can be defined at:

- high level: go to the *System configuration page -> Network -> KNX connection*. Then modify the filtering tabs accordingly. If you need further assistance then please contact us for a detailed explanation,

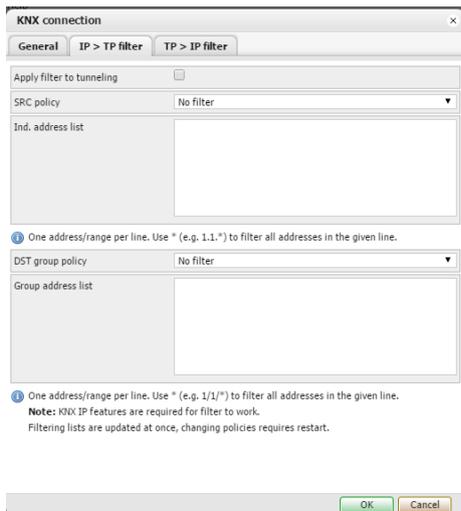


Figure 26: Configure KNX connection

- Object level: in the KNX objects tab of the 'KNX & SPC configuration' page, you can specify for every KNX object if and in which direction it can pass.

### 14.3 Advanced General settings

The following additional General parameters can be specified in the 'General' section of the 'KNX & SPC configuration' tab:

- DEBUG: when a value >0 is set, this will increase the amount of information that will be put in the alerts and logging tabs. This can help when diagnosing problems. It is suggested to not set the DEBUG value to a value larger than 1 for normal user purposes. Higher values are targeted for specialist review. The amount of logging will be so extensive that it can degrade responsiveness of the SPCway.
- UpdateInt.xxxx: For every type of element, there is a default polling interval for status updates. On top of that, updates are also triggered based on monitoring of specific related events. For network performance reasons, and depending on event management strategies, it might be necessary to reduce the default intervals. This can be achieved by specifying these general parameters.

If all events are forwarded to the SPCway (event forwarding active and no event filtering in the SPC panel), then increasing the default polling intervals should have no functional effect. The default values are:

- Zone: 2s
- Area: 4s
- Door: 2s
- Output: 2s
- System: 2s
- User: 600s

### 14.4 Firmware upgrade

The SPCway firmware can be upgraded. Upgrades are announced and available for download on our website. After downloading the most recent upgrade file from our website, the upgrade is initiated under 'System Configuration' -> Menu 'System' -> 'Upgrade firmware'

If your device does not have this menu option, then follow the instructions on our website to activate this upgrade feature, or contact us.



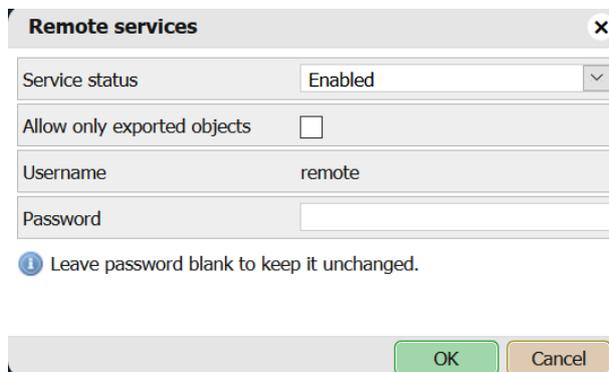
**Before upgrading always backup your configuration:** you find the Backup feature on the 'Utilities' tab of the main configuration page.

After upgrade, if the upgrade was unable to maintain your configuration, you can restore the backup through the same 'Utilities' tab, 'Restore' button.

## 14.5 Resetting password

If you forgot your password, there is a way to reset it via a factory reset. **If you do so, your whole device will be reset, and all data will be lost.** We recommend often making back-ups.

- Push the 'reset' button on your SPCway during 10 at least. Your device is now factory reset.
- The IP address, KNX address and username & login are changed to:
  - IP: 192.168.0.10
  - KNX: 15.15.255
  - Username & login: admin & admin
- Restore a back-up of your files. (See also 13.4 'Back-up and restore'.)
- If you don't have a back-up of your files, you have to restore a blank back-up file, 'Blank Back-up V2\_0.tar.gz', which can be found on our website <http://www.knxlogic.eu/firmwares/spcway-firmware/>.
- At last, you need to reenable 'Remote services'. This can be done via 'System configuration' > 'Services' > 'Remote services'.



Service status	Enabled
Allow only exported objects	<input type="checkbox"/>
Username	remote
Password	

 Leave password blank to keep it unchanged.

OK Cancel

Figure 27: Remote services



**Note:** If the remote services aren't enabled, BACnet won't work.

## Annex 1: Event definitions

Class	SIA Code	SIA event description	Element type	Filter Element type
Alarm Abort	BC	Burglary Cancel	User	
Alarm Restores	NB	Alert Close Node	Expander	
Alarm Restores	SD	Alert Close	Info	
Alarm Restores	YH	Bell Restored		
Alarm Restores	BR	Burglary Restoral	Zone	Area
Alarm Restores	BJ	Burglary Trouble Restore	Zone	Area
Alarm Restores	FR	Fire Restoral	Zone	
Alarm Restores	HR	Holdup Restoral		
Alarm Restores	HJ	Holdup Trouble Restore	Zone	Area
Alarm Restores	ZL	Keypad Unlocked	Expander	
Alarm Restores	MR	Medical Restoral		
Alarm Restores	PR	Panic Restoral	Expander	
Alarm Restores	LR	Phone Line Restoral		
Alarm Restores	TR	Tamper Restoral	Zone	
Alarm Restores	UR	Untyped Zone Restoral	Zone	
Alarm Restores	PH	User Panic Alarm Restoral	Zone	
Alarm Restores	WX	Web Unlocked		
Alarm Restores	PR	User Panic Alarm Restoral	User	
Alarm Restores	WX	Web Unlocked		
Alarms	NO	Alert Reopen Node	Expander	
Alarms	SO	Aller Reopen	Info	
Alarms	YA	Bell Fault		
Alarms	BA	Burglary Alarm	Zone	Area
Alarms	BT	Burglary Trouble	Zone	Area
Alarms	FA	Fire Alarm	Zone	Area
Alarms	HA	Holdup Alarm		
Alarms	HT	Holdup Trouble	Zone	Area
Alarms	ZE	Keypad Locked	Expander	
Alarms	MA	Medical Alarm		
Alarms	PA	Panic Alarm		
Alarms	LT	Phone Line Trouble		
Alarms	TA	Tamper Alarm		

<b>Alarms</b>	UA	Untyped Zone Alarm	Zone	
<b>Alarms</b>	WW	Web Locked		
<b>Confirmed alarms</b>	BV	Burglary Verified	Area	
<b>Doors</b>	DC	Access Closed	Door	User
<b>Doors</b>	DD	Access Denied	Door	User
<b>Doors</b>	DG	Access Granted	Door	User
<b>Doors</b>	DO	Access Open	Door	User
<b>Doors</b>	DF	Door Forced	Door	User
<b>Doors</b>	DN	Door Left Open	Door	User
<b>Doors</b>	DR	Door Restoral	Door	User
<b>Doors</b>	ZA	Reader Locked	Door	
<b>Doors</b>	ZB	Reader Unlocked	Door	
<b>Doors</b>	DX	Request to Exit	Door	
<b>Doors</b>	AU	Unknown Card	Door	
<b>Early / Late</b>	CK	Early Close	User	
<b>Early / Late</b>	OK	Early Open	User	
<b>Early / Late</b>	OT	Late To Close	Area	
<b>Early / Late</b>	CT	Late to Open	Area	
<b>Fault or Tamper Restores</b>	AR	AC Restoral		
<b>Fault or Tamper Restores</b>	YH	Bell Restored		
<b>Fault or Tamper Restores</b>	BJ	Burglary Trouble Restore	Zone	
<b>Fault or Tamper Restores</b>	YK	Communications Restoral	Modem	
<b>Fault or Tamper Restores</b>	EN	Expansion Missing Restore	Expander	
<b>Fault or Tamper Restores</b>	ER	Expansion Restoral	Expander	
<b>Fault or Tamper Restores</b>	EJ	Expansion Tamper Restore		
<b>Fault or Tamper Restores</b>	FJ	Fire Trouble Restore	Zone	Area
<b>Fault or Tamper Restores</b>	HJ	Holdup Trouble Restore		
<b>Fault or Tamper Restores</b>	MJ	Medical Trouble Restore	Zone	
<b>Fault or Tamper Restores</b>	XZ	Network Restoral		
<b>Fault or Tamper Restores</b>	PJ	Panic Trouble Restore	Zone	

<b>Faults or Tamper Restores</b>	LR	Phone Line Restore	Line Number	
<b>Fault or Tamper Restores</b>	YQ	Power Supply Restored		
<b>Fault or Tamper Restores</b>	XG	PSU Battery Low Restoral	Expander	
<b>Fault or Tamper Restores</b>	XC	PSU Output LV Close	Expander	
<b>Fault or Tamper Restores</b>	OV	PSU Tamper Close	Expander	
<b>Fault or Tamper Restores</b>	XH	RF Interference Restoral	Zone	
<b>Fault or Tamper Restores</b>	XJ	RF Receiver Tamper Restoral	Zone	
<b>Fault or Tamper Restores</b>	YR	System Battery Restoral		
<b>Faults or Tamper Restores</b>	TR	Tamper Restoral	Zone	
<b>Fault or Tamper Restores</b>	UJ	Untyped Trouble Restore	Zone	Area
<b>Fault or Tamper Restores</b>	XR	Wireless Battery Low Restoral		
<b>Faults or Tampers</b>	AT	AC Trouble		
<b>Faults or Tampers</b>	YA	Bell Fault		
<b>Faults or Tampers</b>	BT	Burglary Trouble	Zone	
<b>Faults or Tampers</b>	YS	Communications Trouble	Modem	
<b>Faults or Tampers</b>	EM	Expansion Device Missing	Expander	
<b>Faults or Tampers</b>	ES	Expansion Device Tamper		
<b>Faults or Tampers</b>	ET	Expansion Trouble	Expander	
<b>Faults or Tampers</b>	FT	Fire Trouble	Zone	Area
<b>Faults or Tampers</b>	HF	Hardware Fault		
<b>Faults or Tampers</b>	HT	Holdup Trouble	Zone	
<b>Faults or Tampers</b>	MT	Medical Trouble	Zone	
<b>Faults or Tampers</b>	XY	Network Fault		
<b>Faults or Tampers</b>	PT	Panic Trouble	Zone	
<b>Faults or Tampers</b>	YP	Power Supply Trouble		
<b>Faults or Tampers</b>	XK	PSU Battery Discharged	Expander	
<b>Faults or Tampers</b>	XD	PSU Battery Low	Expander	
<b>Faults or Tampers</b>	XB	PSU Output LV Open	Expander	
<b>Faults or Tampers</b>	OU	PSU Tamper Open	Expander	
<b>Faults or Tampers</b>	XQ	RF Interference	Zone	

<b>Faults or Tamper</b>	XS	RF Receiver Tamper	Zone	
<b>Faults or Tamper</b>	YT	System Battery Trouble		
<b>Faults or Tamper</b>	TA	Tamper Alarm		
<b>Faults or Tamper</b>	UT	Untyped Zone Trouble	Zone	Area
<b>Faults or Tamper</b>	XT	Wireless Battery Low		
<b>Inhibit and Isolate</b>	BB	Burglary Bypass	Zone	User
<b>Inhibit and Isolate</b>	BU	Burglary Unbypass	Zone	User
<b>Inhibit and Isolate</b>	FB	Fire Bypass	Zone	User
<b>Inhibit and Isolate</b>	FU	Fire Unbypass	Zone	User
<b>Inhibit and Isolate</b>	HB	Holdup bypass	Zone	User
<b>Inhibit and Isolate</b>	HU	Holdup Unbypass	Zone	User
<b>Inhibit and Isolate</b>	MB	Medical Bypass	Zone	User
<b>Inhibit and Isolate</b>	MU	Medical Unbypass	Zone	User
<b>Inhibit and Isolate</b>	PB	Panic Bypass	Zone	User
<b>Inhibit and Isolate</b>	PU	Panic Unbypass	Zone	User
<b>Inhibit and Isolate</b>	TB	Tamper Bypass	Zone	
<b>Inhibit and Isolate</b>	TU	Tamper Unbypass	Zone	
<b>Inhibit and Isolate</b>	UB	Untyped Zone Bypass	Zone	User
<b>Inhibit and Isolate</b>	UU	Untyped Zone Unbypass	Zone	User
<b>Network</b>	NT	Network Failure		
<b>Network</b>	NR	Network Restoral		
<b>Other</b>	JA	Code Tamper	Expander	
<b>Other</b>	LB	Local Program		
<b>Other</b>	LX	Local Programming Ended		
<b>Other</b>	RR	Power up		
<b>Other</b>	JT	Time changed		
<b>Other</b>	ZG	User accessing end	User	Node
<b>Other</b>	JP	User accessing system begin	User	Node
<b>Other</b>	JV	User Code Changed		
<b>Other</b>	JX	User Code Deleted		
<b>Other</b>	TC	Walktest End	Area	
<b>Other</b>	ZK	Walktest Start	Area	
<b>Other</b>	TP	Zone Walked	Zone	
<b>Other (Non- Standard)</b>	CV	Camera offline	Camera	

<b>Other (Non- Standard)</b>	CU	Camera online	Camera	
<b>Setting and Unsetting</b>	CG	Close Area	Area	User
<b>Setting and Unsetting</b>	CS	Closing Keyswitch	Zone	
<b>Setting and Unsetting</b>	CL	Closing Report	User	
<b>Setting and Unsetting</b>	CI	Fail to Close	Area	
<b>Setting and Unsetting</b>	OG	Open Area	Area	
<b>Setting and Unsetting</b>	OS	Opening Keyswitch	Zone	Area
<b>Setting and Unsetting</b>	OP	Opening Report	User	
<b>Setting and Unsetting</b>	NL	Perimeter Armed	Area	User
<b>Setting and Unsetting</b>	CQ	Remote Closing	User	
<b>Setting and Unsetting</b>	OQ	Remote Opening	User	
<b>Unfiltered</b>	RP	Automatic EDP-Modem Test	Modem	
<b>Unfiltered</b>	RX	Manual EDP-Modem Test	User	
<b>Zone State Changes</b>	ZC	Zone Close	Zone	Area
<b>Zone State Changes</b>	ZD	Zone Disconnect	Zone	Area
<b>Zone State Changes</b>	ZF	Zone Fault	Zone	Area
<b>Zone State Changes</b>	ZM	Zone Masked	Zone	Area
<b>Zone State Changes</b>	ZO	Zone Open	Zone	Area
<b>Zone State Changes</b>	ZI	Zone Out Of Bounds	Zone	Area
<b>Zone State Changes</b>	ZX	Zone Short	Zone	Area
<b>Zone State Changes</b>	ZN	Zone Unstable	Zone	Area

## Annex 2: Status definitions

Class	Status name	Element Type	Possible predefined values
<b>Area</b>	Area mode	Area	Unset, Partset_A, Partset_B, Fullset
<b>Area</b>	Area name	Area	
<b>Area</b>	All Area min mode	Area	Unset, Partset_A, Partset_B, Fullset
<b>Door</b>	Door status	Door	NORMAL, LOCKED, UNLOCKED, OPEN_TOO_LONG, LEFT_OPEN, FORCED, TAMPER, OFFLINE
<b>Door</b>	Door Zone state	Door	OPEN, CLOSED, SHORT, DISCON, DCSUB, OFFLINE
<b>Door</b>	Door name	Door	<i>First 14 characters of the name</i>
<b>Output</b>	Output status	Output	1, 0
<b>System</b>	Panel product name	System	<i>First 14 characters of the name</i>
<b>System</b>	Panel Firmware version	System	<i>First 14 characters of the version</i>
<b>System</b>	Panel Product ID	System	<i>First 14 characters of the ID</i>
<b>System</b>	Full engineer mode active	System	1, 0
<b>System</b>	System Tampered	System	1, 0
<b>System</b>	System General fault	System	1, 0
<b>System</b>	System Mains fault	System	1, 0
<b>System</b>	System Battery fault	System	1, 0
<b>System</b>	System Ext. Bell active	System	1, 0
<b>System</b>	System Ext. Strobe active	System	1, 0
<b>System</b>	System Int. Bell active	System	1, 0
<b>System</b>	Modem 1 not responding	System	1, 0
<b>System</b>	Modem 1 Line fault	System	1, 0
<b>System</b>	Modem 2 not responding	System	1, 0
<b>System</b>	Modem 2 Line fault	System	1, 0
<b>System</b>	EDP fault	System	1, 0
<b>System</b>	EDP Connection(*)	System	1, 0
<b>User</b>	User name	User	<i>First 14 characters of the name</i>
<b>Zone</b>	Zone state	Zone	OPEN, CLOSED, ALARM, ISOLATE, MASKED, INHIBIT, SOAK, OFFLINE, DCSUB, TROUBLE, SHORT, DISCON, FAULT
<b>Zone</b>	Zone type	Zone	ALARM, ENTRYEXIT, EXITTERM, FIRE, FIREX, LINE, PANIC, HOLDUP, TAMPER, FAULT1, FAULT_HOLDUP, FAULT_WARNING, TECH, MEDIC, KEYARM, SHUNT, XSHUNT, LOCKSUP, SEISMIC, ALL OKAY, SETTING_AUTH, LOCK_ELEMENT, GLASS
<b>Zone</b>	Zone name	Zone	<i>First 14 characters of the name</i>

\*: This is the status as perceived by the SPCway since the Panel EDP status cannot transmit its status when connection is lost.

## Annex 3: Command definitions

Class	Command Name	Element type	Option
Area	Force Set Area	Area	
Area	Partset A an area	Area	
Area	Partset B an area	Area	
Area	Set an area	Area	
Area	Unset an area	Area	
Verification Zone	Audio Challenge	Verification Zone	Number of the Audio message to be played
Door	De-inhibit door zones	Door	
Door	De-isolate door zones	Door	
Door	Inhibit door zones	Door	
Door	Isolate door zones	Door	
Door	Lock a door	Door	
Door	Open a door momentarily	Door	
Door	Open a door permanently	Door	
Door	Set a door to normal mode	Door	
Output	Reset outputs	Output	
Output	Set outputs	Output	
System	Restore alerts	System	
System	Silence All Bells	System	
System	Set SPCway Watchdog	System	
User	N/A	User	
Zone	De-inhibit zones	Zone	
Zone	De-isolate zones	Zone	
Zone	Inhibit zones	Zone	
Zone	Isolate zones	Zone	

## Annex 4: BACnet

### ANNEX A - PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (NORMATIVE)

(This annex is part of this Standard and is required for its use.)

#### **BACnet Protocol Implementation Conformance Statement**

**Date:** 1 juin 2019

**Vendor Name:** KNXlogic

**Product Name:** SPCway Plus

**Product Model Number:** SPCway Plus 4XXX, SPCway Plus 5XXX, SPCway Plus 6XXX

Application Software Version: 2.0      Firmware Revision: 1.15      BACnet Protocol Revision: 10

#### **Product Description:**

SPCway is a dedicated protocol gateway to allow the integration of Vanderbilt (former Siemens) SPC intrusion control panels to be integrated in a building management system over a series of supported protocols.

The SPCway Plus adds BACnet protocol support and a visualization server.

It is gateway between KNX, Modbus, BACnet & IP logic module providing memory function and event controller, user interface based on a web server application.

It can be used from local and mobile devices such as smartphones, tablets, PCs and touch panels.

#### **BACnet Standardized Device Profile (Annex L):**

**BACnet Operator Workstation (B-OWS)**

**BACnet Advanced Operator Workstation (B-AWS)**

**BACnet Operator Display (B-OD)**

**BACnet Building Controller (B-BC)**

**BACnet Advanced Application Controller (B-AAC)**

**[?] BACnet Application Specific Controller (B-ASC)**

**BACnet Smart Sensor (B-SS)**

**BACnet Smart Actuator (B-SA)**

**List all BACnet Interoperability Building Blocks Supported (Annex K):**

Data Sharing	ReadProperty-B	DS-RP-B
	ReadPropertyMultiple-B	DS-RPM-B
	WriteProperty-B	DS-WP-B
	COV-B	DS-COV-B
Device and Network Management	Dynamic Device Binding-B	DM-DDB-B
	Dynamic Object Binding-B	DM-DOB-B
	DeviceCommunicationsControl-B	DM-DCC-B
	TimeSynchronization-B	DM-TS-B
	UTCTimeSynchronization-B	DM-UTC-B
	ReinitializeDevice-B	DM-RD-B

**Segmentation Capability: NOT SUPPORTED**

Able to transmit segmented messages      Window Size \_\_\_\_

Able to receive segmented messages      Window Size \_\_\_\_

**Standard Object Types Supported:**

An object type is supported if it may be present in the device. For each standard Object Type supported provide the following data:

Whether objects of this type are dynamically creatable using the CreateObject service

Whether objects of this type are dynamically deletable using the DeleteObject service

List of the optional properties supported

List of all properties that are writable where not otherwise required by this standard

List of all properties that are conditionally writable where not otherwise required by this standard

List of proprietary properties and for each its property identifier, datatype, and meaning

List of any property range restrictions

Object Type	Required Properties	Optional Properties	Writable Properties
Device	Object_Identifier Object_Name Object_Type System_Status Vendor_Name Vendor_Identifier Model_Name Firmware_Revision Application_Software_Version Protocol_Version Protocol_Revision Protocol_Services_Supported Protocol_Object_Types_Supported Object_List Max_Apdu_Length_Accepted Segmentation_Supported Apdu_Timeout Number_Of_Apdu_Retries Device_Address_Binding Database_Revision	Description Local_Time Utc_Offset Local_Date Daylight_Savings_Status Profile_Name Location Active_Cov_Subscriptions	No

Object Type	Required Properties	Optional Properties	Writable Properties
AnalogValue	Object_Identifier Object_Name Object_Type Present_Value Status_Flags Event_State Out_Of_Service Units	Description Priority_Array Relinquish_Default Cov_Increment	Present_Value Cov_Increment Out_Of_Service

Object Type	Required Properties	Optional Properties	Writable Properties
BinaryValue	Object_Identifier Object_Name Object_Type Present_Value Status_Flags Event_State Out_Of_Service	Description Priority_Array Relinquish_Default	Present_Value Out_Of_Service

Note: The functional application consequence of writing a 'Present\_Value' depends on the actual configuration of the Object. This can be consulted in the configuration of the SPCway itself, or in the modbus profile csv file that can be downloaded from the SPCway

Data Link Layer Options:

BACnet IP, (Annex J)

BACnet IP, (Annex J), Foreign Device

ISO 8802-3, Ethernet (Clause 7)

ATA 878.1, 2.5 Mb. ARCNET (Clause 8)

ATA 878.1, EIA-485 ARCNET (Clause 8), baud rate(s) \_\_\_\_\_

MS/TP master (Clause 9), baud rate(s): \_\_\_\_

MS/TP slave (Clause 9), baud rate(s): \_\_\_\_

Point-To-Point, EIA 232 (Clause 10), baud rate(s): \_\_\_\_

Point-To-Point, modem, (Clause 10), baud rate(s): \_\_\_\_

LonTalk, (Clause 11), medium: \_\_\_\_

BACnet/ZigBee (ANNEX O)

Other: \_\_

Device Address Binding:

Is static device binding supported? (This is currently necessary for two-way communication with MS/TP slaves and certain other devices.)  Yes  No

Networking Options:

Router, Clause 6 - List all routing configurations, e.g., ARCNET-Ethernet, Ethernet-MS/TP, etc.

Annex H, BACnet Tunneling Router over IP

BACnet/IP Broadcast Management Device (BBMD)

Does the BBMD support registrations by Foreign Devices?  Yes  No Does the BBMD support network address translation?  Yes  No

Network Security Options:

Non-secure Device - is capable of operating without BACnet Network Security

Secure Device - is capable of using BACnet Network Security (NS-SD BIBB)

Multiple Application-Specific Keys:

Supports encryption (NS-ED BIBB)

Key Server (NS-KS BIBB)

Character Sets Supported:

Indicating support for multiple character sets does not imply that they can all be supported simultaneously.

ISO 10646 (UTF-8)  IBM<sup>®</sup>/Microsoft<sup>®</sup> DBCS  ISO 8859-1

ISO 10646 (UCS-2)  ISO 10646 (UCS-4)  JIS X 0208

If this product is a communication gateway, describe the types of non-BACnet equipment/networks(s) that the gateway supports:

See above