

---

# SPC Bridge KNX User Manual

Revision 1.0

---



## History Record

Revision	Date	Author	Comment
1.0	Jan-2020	Lundix IT	First edition

©2020 Lundix IT

Lundix IT  
 Renvägen 22  
 S-433 70 Sävedalen  
 Sweden  
[info@lundix.se](mailto:info@lundix.se)

## Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>5</b>
1.1	SPC Bridge KNX.....	5
1.2	Main Features.....	5
1.3	Hardware Specification.....	5
<b>2</b>	<b>INSTALLATION.....</b>	<b>7</b>
2.1	Prerequisites.....	7
2.2	First Time Installation Workflow.....	7
<b>3</b>	<b>SYSTEM ADMINISTRATION.....</b>	<b>8</b>
3.1	System Administration Login.....	8
3.2	Static IP Address.....	9
3.3	Time Setting.....	9
3.4	Change Administration Password.....	9
<b>4</b>	<b>SPC BRIDGE CONFIGURATION.....</b>	<b>10</b>
4.1	SPC Bridge Sign In.....	10
4.2	SPC Communication (FlexC).....	10
4.2.1	SPC Panel - FlexC Settings.....	10
4.2.2	SPC Bridge - SPC Communication Settings.....	11
4.3	SPC Communication Test.....	12
4.4	KNX Interface Info (Programming Mode).....	12
4.5	KNX Scenes.....	13
4.6	KNX Datapoints.....	14
4.7	System Info.....	14
4.8	System User.....	15
<b>5</b>	<b>ETS KNX CONFIGURATION.....</b>	<b>16</b>
5.1	First Time Configuration.....	16
5.2	Communication Objects.....	16
5.2.1	KNX Datapoint Map.....	16
5.2.2	Global System Objects.....	17
5.2.3	SPC Area Commands.....	17
5.2.4	SPC Zone Commands.....	18
5.2.5	SPC Area Status Objects.....	19
5.2.6	SPC Zone Status.....	20
<b>6</b>	<b>ADVANCED USERS.....</b>	<b>21</b>
6.1	Backup of Configuration Settings.....	21
6.2	Upgrading software.....	21
6.3	SSH Access.....	21
6.4	Resetting the SPC Bridge.....	21
<b>7</b>	<b>APPENDICES.....</b>	<b>22</b>

7.1	SPC Command Error Codes .....	22
7.2	End-User License Agreement for SPC Bridge (EULA) .....	24
7.3	Open Source Software .....	25
7.4	Open Source Hardware .....	25

# 1 Introduction

## 1.1 SPC Bridge KNX



SPC Bridge

Weinzierl KNX interface 332

Weinzierl KNX interface 312

**SPC Bridge KNX** allows interfacing Vanderbilt SPC intrusion system to a KNX system. Using the SPC Bridge you are able to use events from all your SPC connected motion detectors, door/window contacts, fire detectors and alarm status for automations in your KNX system. SPC Bridge KNX includes a certified Weinzierl KNX interface (332 or 312) for a reliable and approved connection to the KNX bus.

## 1.2 Main Features

- Mirrors SPC zone and area states/status to KNX bus
- Support for area and zone commands from KNX bus, e.g arm/disarm, inhibit zone.
- SPC Panel Communication using FlexC
- Weinzierl KNX interface 332 or 312
- Communication objects configurable in KNX ETS.
- Web based Admin GUI
- Recommended for maximum 128 zones and 16 areas (The actual limit depends on the use case, e.g. how many motion detectors the SPC system has.)

## 1.3 Hardware Specification

SPC Bridge	
Processor	400MHz, 24K MIPS
Flash	16MB
RAM	64MB
Power input	9 – 12V DC
Network	2 x 10M/100M RJ45 Connectors
WiFi	802.11 b/g/n
USB	1 x USB 2.0 host connector
Type Approval	FCC Part15 Subpart B, Subpart C, CE NB, C-Tick

Weinzierl KNX interface 332	
Mechanical	Housing: plastic transparent, Dimensions: 58 mm x 12 mm x 18 mm

Indicators	LED (multicolor) for USB, LED (multicolor) for KNX
KNX	Medium TP, Interface protocol HID/xEMI, APDU length: 55,, Object Server: BAOS V2, Device model: System B
Power supply	USB < 10 mA, KNX < 3 mA
Connectors	KNX via pluggable screw terminal, USB connector type A
Compatibility	ETS (Engineering Tool Software) ETS4 or later

<b>Weinzierl KNX interface 312</b>	
Mechanical	Housing: plastic, DIN rail mounted device, width: 1TE
Indicators	LED (multicolor) for USB, LED (multicolor) for KNX
KNX	Medium TP, Long Frame, Object Server: BAOS V2, Device model: System B
Power supply	USB < 15 mA, KNX < 3 mA
Connectors	KNX connector, USB connector type B
Compatibility	ETS (Engineering Tool Software) ETS4 or later

## 2 Installation

### 2.1 Prerequisites

- Vanderbilt SPC panel with firmware  $\geq$  3.6 (3.6 was the first version with support for FlexC)
- Network router with DHCP server enabled
- SPC Bridge and SPC panel connected to same local network
- Internet access (to be able to use time synchronization via NTP)
- KNX system
- KNX configuration tool ETS v 5

### 2.2 First Time Installation Workflow

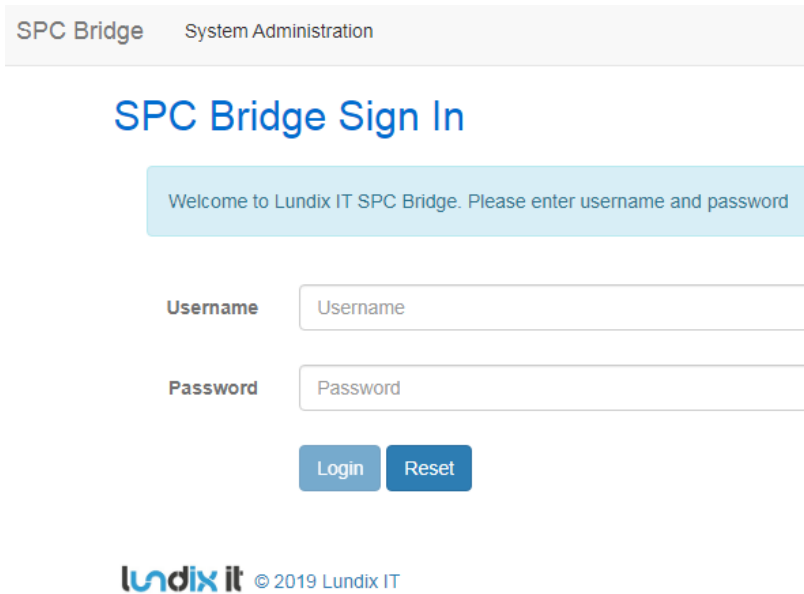
1. Read carefully **End-User License Agreement for SPC Bridge (EULA)** in last section in this document. If you do not agree to the terms of the EULA, do not install or use the SPC Bridge.
2. Connect the included KNX interface, Weinzierl 332 or 312, to the SPC Bridge USB port.
3. Connect the KNX bus cable to the KNX bus connector on the KNX interface. **NOTE!** The default individual device address of the KNX interface is **15.15.255**. If this address already is in use you should change the address (see section KNX Interface Info) before you connect the interface to the KNX-bus.
4. Connect the SPC Bridge LAN port, with a regular network cable, to your network switch or router.
5. Power up the device by connecting the included power adapter to a wall socket and then to the SPC Bridge.
6. Wait (~3 minutes) until the SPC Bridge has fully started.
7. Open a web browser and access your router (DHCP-server) to find the IP address assigned to the SPC Bridge. Type the IP address in the web browser to go to the SPC Bridge sign in page.
8. Assign a static IP address to the SPC Bridge. Follow instructions in section **System Administration, Static IP Address**.
9. Configure SPC communication. Follow the instructions in section **SPC Bridge Configuration, SPC Communication**.
10. Test the SPC Communication. See **SPC Communication Test**.
11. Configure the KNX interface. Follow the instructions in **ETS KNX configuration**

### 3 System Administration

The SPC Bridge is based on a standard Linux platform, OpenWrt, that is very common on routers. The System Administration Web GUI contains many settings intended only for advanced users. Only the settings described in this section should be changed by normal users.

#### 3.1 System Administration Login

Type IP address of the SPC Bridge in the web browser address field, go to SPC Bridge sign in page and click on **System Administration** in the **top bar**.



This will open the OpenWRT sign in page. Enter username (**root**) and password (default: **dragino**) and click on **Login**.

#### Authorization Required

Please enter your username and password.

Username

Password

**NOTE!** To return to SPC Bridge sign in page you need to type the SPC Bridge IP address in the web browser address field.



## 3.2 Static IP Address

Default will SPC Bridge use DHCP to get an IP Address. To be sure that the SPC Bridge keeps the IP address after a network/router restart you should assign the SPC Bridge a static IP Address. In the System Administration GUI, go to **Network -> Interfaces** and:

1. Select **LAN – Edit**.
2. In **Interfaces – LAN**, select **Static address** in the **Protocol** option menu
3. Click on **Switch Protocol**
4. In **Common Configuration – General Setup** fill in; IPv4 address, netmask, gateway and custom DNS servers.
5. In **DHCP Server – General Setup**; check the checkbox **Ignore interface**. **NOTE!** It is very important to disable the DHCP server in the SPC Bridge to avoid conflict with your normal DHCP server.
6. Click on **Save & Apply**.
7. Redirect your browser to the new IP Address.

## 3.3 Time Setting

To set correct Timezone, go to **System -> System** and select **Timezone** in section **System Properties – General Settings**.

The device is as default using NTP to synchronize time. This setting is in **System -> System** section **Time Synchronization**.

**NOTE!** The device has no RTC clock. During boot the device can have incorrect time. Some events in the system log can therefore have incorrect timestamps.

## 3.4 Change Administration Password

The default administration password for accessing the device is **dragino**. Of security reasons it is highly recommended to change the password as soon as possible. Go to **System -> Administration** section **Device Password** to change the password. The same password is used in both Administration Web GUI and for ssh access to the device.

## 4 SPC Bridge Configuration

### 4.1 SPC Bridge Sign In

Type IP address of the SPC Bridge in the web browser address field, go to SPC Bridge sign in page, enter username (**spcbridge**) and password (default **Spcbridge!**) and click **Login**.

SPC Bridge System Administration

### SPC Bridge Sign In

Welcome to Lundix IT SPC Bridge. Please enter username and password

Username

Password

Login Reset

Lundix IT © 2019 Lundix IT

### 4.2 SPC Communication (FlexC)

To setup the communication link between SPC Panel and SPC Bridge you have to configure the link in both SPC Panel and SPC Bridge ends.

#### 4.2.1 SPC Panel - FlexC Settings.

Use **Vanderbilt SPC Web interface** and define the FlexC communication following this instructions:

1. Select Full Engineer mode
2. Create a specific user for the SPC Bridge communication, e.g **spcbridge**. User profile should be Manager and you need also to define a web password for the user. (To be able to set a web password you need to login as the user in the SPC web interface).
3. Select **Communications -> FlexC -> Event Profiles**. Click on **Add** to add a new event profile. Give the event profile the name **SPC Bridge Events** and select (check) the report checkboxes for all event types. (You may consider reducing these settings later to just necessary events for the application)
4. Select **Communications -> FlexC -> FlexC ATS**. Select **Add Custom ATS** and change following from the default settings:
  - ATS Name = SPC Bridge
  - Event Profile = SPC Bridge Events (created in step 3)
  - ATS Polling Timeout = 60 seconds
  - Uncheck Generate FTC and Re-queue Events

5. Select **Add ATP to FlexC RCT** and change following from the default settings:
  - SPT Account Code = 999
  - RCT URL or IP Address = IP Address of the SPC Bridge
  - ATP Category = Cat 6 [Ethernet]
  
6. Open **Advanced ATP Settings** and change following from the default settings:
  - Encryption Key Mode = Fixed Encryption
  - Encryption key (64 hex digits) = Your own key. Must be exactly 64 hex digits (0-9, a-f).
  
7. Leave Full Engineer mode.

**NOTE!** In Full Engineer mode the SPC panel is not reporting any events to the SPC Bridge.

### 4.2.2 SPC Bridge - SPC Communication Settings

In the **SPC Bridge Web interface**, login and select **SPC ->SPC Communication** and fill in the form according to:

## SPC Communication

Configuration of FlexC, to be able to communicate with the Vanderbilt SPC Panel. The values must match the settings in the SPC Panel.

### FlexC Settings

<b>ATP Encryption Key</b>	Encryption Key (leave blank if you don't want to change it)	
<b>SPT Account Code</b>	999	^ v
<b>RCT ID</b>	1	^ v
<b>RCT TCP Port</b>	52000	^ v
<b>SPC Username</b>	spcbridge	
<b>SPC Password</b>	Password (leave blank if you don't want to change it)	

Save

Element	Description
ATP Encryption Key	ATP Encryption Key. 64 hex numbers (0-9, a-f, A-F). Must match corresponding key in SPC Panel FlexC settings. (Default key: 000011112222...ddddeeeeffff) <b>NOTE!</b> Of security reason a saved encryption key is never shown again. Just leave the field blank if you don't want to change the key.

SPC Account Code	ATP Account Code. Must match corresponding key in SPC Panel FlexC settings.
RCT ID	RCT Id. Must match corresponding id in SPC Panel FlexC settings.
RCT TCP Port	RCT TCP Port. Must match corresponding value in SPC Panel FlexC settings
SPC Username and Password	Credentials for FlexC communication. User must be defined in the SPC Panel and have a corresponding web password. <b>NOTE!</b> Of security reason a saved password is never shown again. Just leave the field blank if you don't want to change the password.

### 4.3 SPC Communication Test

To be sure that the communication between SPC Bridge and SPC panel is working properly you can use the tests provided in **SPC ->SPC Communication Test**. In the option menu you can choose between query SPC areas, zones or the system log.

#### SPC Communication Test

Test Case

GET SPC Areas

Raw JSON Reply

```
{
  "area_status": [
    {
      "area_id": "1",
      "area_name": "Area 1",
      "mode": "0",
      "partseta_enable": "1",
      "partsetb_enable": "1",
      "partseta_name": "Partset A",
      "partsetb_name": "Partset B",
      "last_set_time": "1573225019",
      "last_set_time_spc": "13565908112019",
      "last_set_user_id": "1",
      "last_set_user_name": "Go!",
      "last_unset_time": "1573225044",
      "last_unset_time_spc": "13572408112019",
      "last_unset_user_id": "1",
      "last_unset_user_name": "Go!",
      "last_alarm": "1573225178",
      "last_alarm_spc": "13593808112019",
      "internal_bells": "0",
      "external_bells": "0"
    },
    {
      "area_id": "2",
      "area_name": "Area 2",
      "mode": "0",
      "partseta_enable": "0",
      "partsetb_enable": "0",
      "last_set_time": "1573225009",
      "last_set_time_spc": "13564908112019",
      "last_set_user_id": "1",
      "last_set_user_name": "Go!",
      "last_unset_time": "1573225044",
      "last_unset_time_spc": "13572408112019",
      "last_unset_user_id": "1",
      "last_unset_user_name": "Go!",
      "internal_bells": "0",
      "external_bells": "0"
    }
  ]
}
```

Formatted Example

Area ID	Area Name	Mode	Last Set	Last Unset	Last Alarm
1	Area 1	Unset	2019-11-08 15:56:59 [Go!]	2019-11-08 15:57:24 [Go!]	2019-11-08 15:59:38
2	Area 2	Unset	2019-11-08 15:56:49 [Go!]	2019-11-08 15:57:24 [Go!]	-

### 4.4 KNX Interface Info (Programming Mode)

**Interface -> KNX Interface** shows some basic information about the KNX interface and is used to set the KNX interface in programming mode and change the address.

#### KNX Interface Info

Programming Mode:

Individual Address:

KNX Bus State:

Manufacturer:

Serial Number:

Protocol Version:

Configured Datapoints:

Element	Description
Programming Mode	Click on Activate/Deactivate button to set/unset the interface programming mode. NOTE! The interface has no physical programming mode button, so you need to use this feature when ETS ask you to set the interface in programming mode. Normally this will only happen when you do a full download.
Individual Address	Individual KNX address of the interface. Can also be changed using ETS.
KNX Bus State	Shows state of the KNX connection. Online or Offline.
Manufacturer	KNX interface manufacturer
Serial Number	KNX interface serial number
Protocol Version	KNC interface protocol version
Configured Datapoints	Number of datapoints that are linked to Group Addresses.

## 4.5 KNX Scenes

**Interface -> KNX Scenes** is used to configure KNX scene numbers that should be sent to the KNX-bus when different SPC events occur. The scene number is sent to the KNX-bus via a common datapoint (Scene Control Output), each time the assigned event occurs. The scene numbers are configured per alarm area and can have values between 1 to 64 (Set 0 will disable the event).

Area 1

Save Scene Numbers

<b>Area Unset Scene</b>	1	▲ ▼	Scene number to be sent when the area mode changes to unset (0 = disabled)
<b>Area Partset A Scene</b>	2	▲ ▼	Scene number to be sent when the area mode changes to partset A (0 = disabled)
<b>Area Partset B Scene</b>	3	▲ ▼	Scene number to be sent when the area mode changes to partset B (0 = disabled)
<b>Area Fullset Scene</b>	4	▲ ▼	Scene number to be sent when the area mode changes to fullset (0 = disabled)
<b>Intrusion Alarm Scene</b>	10	▲ ▼	Scene number to be sent when an intrusion alarm occurs (0 = disabled)
<b>Fire Alarm Scene</b>	12	▲ ▼	Scene number to be sent when a fire alarm occurs (0 = disabled)
<b>Tamper Alarm Scene</b>	0	▲ ▼	Scene number to be sent when a tamper alarm occurs (0 = disabled)
<b>Confirmed Alarm Scene</b>	0	▲ ▼	Scene number to be sent when a confirmed alarm occurs (0 = disabled)
<b>Alarm Restored Scene</b>	11	▲ ▼	Scene number to be sent when all alarms has been restored (0 = disabled)

An individual scene number can be assigned to following SPC events:

- Area becomes unset
- Area becomes partset A
- Area becomes partset B
- Area becomes fullset
- Area reports an intrusion alarm
- Area reports a fire alarm
- Area reports a tamper alarm
- Area reports a confirmed alarm
- Area reports all alarms are restored

## 4.6 KNX Datapoints

**Interface -> KNX Datapoints** shows the current values of the KNC communication objects and can be used for troubleshooting. The objects are divided in following categories:

- System objects
- SPC Area States
- SPC Zone States
- SPC Zone Status
- SPC Commands

### KNX Datapoints

SPC Area States ▾
  Hide unused datapoints

Datapoint #	Description	DPT	Value	KNX Update Status	Last update
31	Area 1 unset	DPT1	0	OK	2019-12-04 11:26:11
32	Area 1 partset A	DPT1	0	Not connected to Group Address	2019-12-04 11:26:11
33	Area 1 partset B	DPT1	0	Not connected to Group Address	2019-12-04 11:26:11
34	Area 1 fullset	DPT1	1	OK	2019-12-04 11:26:11
35	Area 1 intrusion alarm	DPT1	0	Not connected to Group Address	2019-12-04 11:26:11
36	Area 1 fire alarm	DPT1	0	Not connected to Group Address	2019-12-04 11:26:11
37	Area 1 tamper alarm	DPT1	0	Not connected to Group Address	2019-12-04 11:26:11
38	Area 1 confirmed alarm	DPT1	0	Not connected to Group Address	2019-12-04 11:26:11
44	Area 1 fullset user id	DPT5	0	Not connected to Group Address	2019-12-04 11:26:11
45	Area 1 fail to set reason	DPT5	255	OK	2019-12-04 11:26:11

Element	Description
Hide unused datapoints	If this is checked, only datapoints that have been accessed (from SPC side) is shown.
Datapoint #	Datapoint address
Description	Datapoint description
DPT	KNX data type
Value	Current value
KNX Update Status	Access status reported from the KNX interface. OK: The value was successfully sent to KNX bus Not connected Group Address: Datapoint isn't linked to a Group Address (by ETS)  Other possible error status (shouldn't normally appear) : Internal Error, Not found, Buffer Error, Write Error, Unsupported, Invalid service, Invalid command, Invalid length, Invalid message, Busy, Failed request
Last update	Last time the value was updated from the SPC system.

## 4.7 System Info

**System -> System Info** shows some basic information about the SPC Bridge hardware and software.

## System Info

System Name	dragino-18c950
Firmware Version	OpenWrt Chaos Calmer 15.05.1
Product Version	1.0-1
Uptime	93 days 04:58:22
Local Time	Mon Nov 18 2019 16:36:47 GMT+0100
Load Average	0.00 0.00 0.00
Total Memory	61124 kB
Free Memory	18568 kB

## 4.8 System User

To change the password for the SPC Bridge user (spcbridge) go to **System** -> **User** and enter a new password twice. **Note!** Username is not possible to change.

### User Credentials

Username	spcbridge
New Password	Password
Retype Password	Password
	<input type="button" value="Save"/>

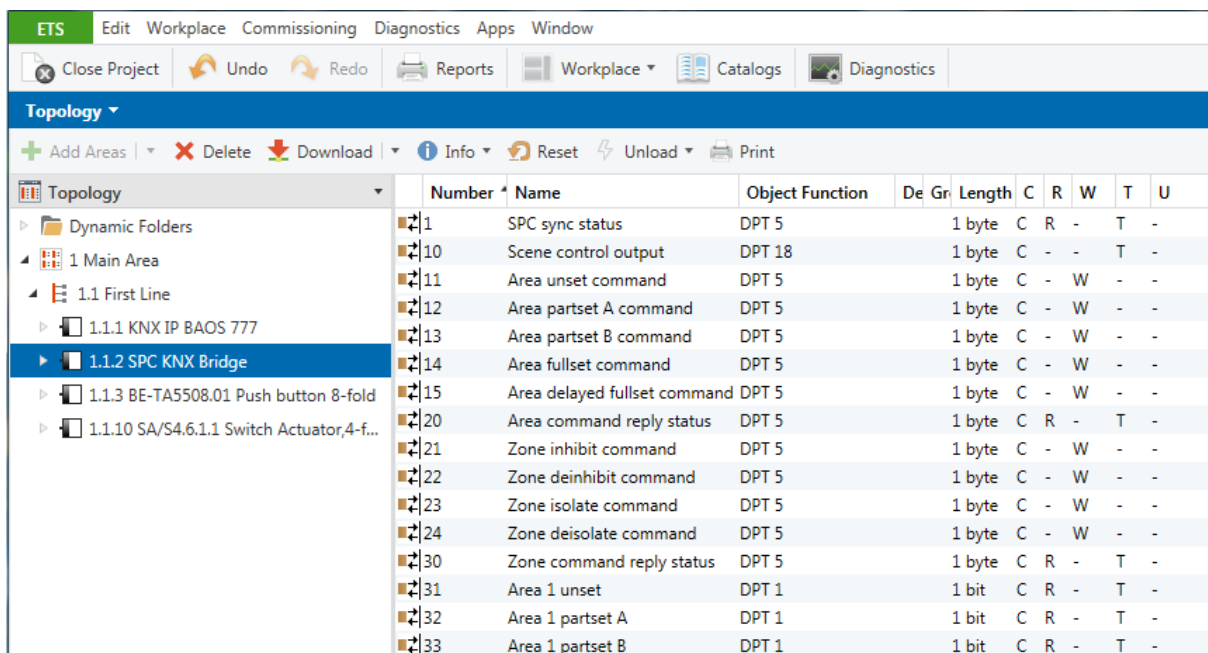
## 5 ETS KNX Configuration

### 5.1 First Time Configuration

To configure the KNX interface you should use the KNX standard configuration tool ETS. The configuration is based on a generic product database from Weinzierl, but adapted according to the Communication Objects below. For a quick start please copy and paste the configuration from one of the attached ETS project templates:

1. On **ETS project** page, import the template project file that best match your size of SPC system.
2. Open the template project. In the **Topology** tree, select and copy the item **1.1.1 SPC KNX SPC Bridge**.
3. Switch to your ordinary project and paste the copied item to the Topology tree (see example below).
4. Change the individual address to desired address of the KNX interface.
5. Download (full) configuration to the KNX interface. **NOTE!** To set the KNX interface in **programming mode** you need to use SPC Bridge Web GUI, see section **KNX Interface Info (Programming Mode)**.

After successful first time configuration you can link the communication objects (datapoints) to group addresses as usual.



## 5.2 Communication Objects

### 5.2.1 KNX Datapoint Map

States, status and commands from /to the SPC system are mapped to predefined datapoints/group objects on the KNX interface. The datapoint map has following main structure:



Datapoint Address	Usage
1 to 10	Global system objects
11 to 20	SPC area command objects
21 to 30	SPC zone command objects
31 to 270	SPC area status objects
301 to 556	SPC zone state objects
561 to 816	SPC zone status objects
817 to 1000	<i>Available for future features</i>

The map is designed for an absolute maximum of 16 areas and 256 zones.

### 5.2.2 Global System Objects

Following global system global Group Objects will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Flags
1	SPC com status	<p>0 = SPC communication is under initialization (datapoint values are not reliable),                      1 = SPC communication is OK,                      2 = SPC communication has failed (datapoint values are not reliable)</p> <p>To test SPC communication please see section 4.3.</p>	DPT 5	1-byte	CR-T-
10	Scene control output	<p>Common output for scene numbers sent to the KNX system when specified events occur. An individual scene number can be assigned to following SPC events:</p> <ul style="list-style-type: none"> <li>• Area X becomes unset</li> <li>• Area X becomes partset A</li> <li>• Area X becomes partset B</li> <li>• Area X becomes fullset</li> <li>• Area X reports an intrusion alarm *</li> <li>• Area X reports a fire alarm **</li> <li>• Area X reports a tamper alarm ***</li> <li>• Area X reports a confirmed alarm</li> <li>• Area X reports all alarms are restored</li> </ul> <p>(X = 1 to maximum number of areas, e.g. 16)</p> <p>The scene number is sent each time the assigned event occurs.</p>	DPT 18	1-byte	C—T-

\* Value is based on Alarm status for zone types Alarm, Exit/Entry, Glassbreak and Exit/Entry2.

\*\* Value is based on Alarm status for zone type Fire.

\*\*\* Value is based on Alarm status for zone type Tamper and Tamper status for all zone types.

### 5.2.3 SPC Area Commands

Common for all SPC areas following Group Objects for commands will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Flags
11	Area unset command	ID of area to unset  The success/error of the command is reported in "Area command reply status".	DPT 5	1-byte	C-W--
12	Area partset A command	ID of area to partset A  The success/error of the command is reported in "Area command reply status".	DPT 5	1-byte	C-W--
13	Area partset B command	ID of area to partset B  The success/error of the command is reported in "Area command reply status".	DPT 5	1-byte	C-W--
14	Area fullset command	ID of area to fullset (immediately)  The success/error of the command is reported in "Area command reply status".  The fail to set reason is reported in "Area fail to set reason"	DPT 5	1-byte	C-W--
15	Area delayed fullset command	ID of area to fullset when exit time has expired  The success/error of the command is reported in "Area command reply status".  The fail to set reason is reported in "Area fail to set reason" (after exit time has expired or been canceled)	DPT 5	1-byte	C-W--
20	Area command reply status	0 = Last area command succeeded, 1-255 = Area command failed error code.  Codes are listed in section 7.1 SPC Command Error Codes.	DPT 5	1-byte	CR-T-

Area ID = 1 to maximum number of areas (16).

### 5.2.4 SPC Zone Commands

Common for all SPC zones following Group Objects for commands will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Attributes
21	Zone inhibit command	ID of zone to inhibit  The success/error of the command is reported in "Zone command reply status".	DPT 5	1-byte	C-W--
22	Zone deinhibit command	ID of zone to deinhibit  The success/error of the command is	DPT 5	1-byte	C-W--

		reported in "Zone command reply status".			
23	Zone isolate command	ID of zone to isolate  The success/error of the command is reported in "Zone command reply status".	DPT 5	1-byte	C-W--
24	Zone deisolate command	ID of zone to deisolate  The success/error of the command is reported in "Zone command reply status".	DPT 5	1-byte	C-W--
30	Zone command reply status	0 = Last zone command succeeded, 1-255 = Zone command failed error code.  Codes are listed in section 7.1 SPC Command Error Codes.	DPT 5	1-byte	CR-T-

Zone ID = 1 to maximum number of zones (128).

### 5.2.5 SPC Area Status Objects

For each SPC area following Group Objects will be available:

Relative address *	Name	Values	Datapoint Type	Length	Flags
+1	Area X unset	0 = Area is not unset, 1 = Area is unset (disarmed)	DPT 1	1-bit	CR-T-
+2	Area X partset A	0 = Area is not partset A, 1 = Area is partset A	DPT 1	1-bit	CR-T-
+3	Area X partset B	0 = Area is not partset B, 1 = Area is partset B	DPT 1	1-bit	CR-T-
+4	Area X fullset	0 = Area is not fullset, 1 = Area is fullset (armed)	DPT 1	1-bit	CR-T-
+5	Area X intrusion alarm	0 = Area has no intrusion alarm **, 1 = Area has at least one intrusion alarm **	DPT 1	1-bit	CR-T-
+6	Area X fire alarm	0 = Area has no fire alarm ***, 1 = Area has at least one fire alarm ***	DPT 1	1-bit	CR-T-
+7	Area X tamper alarm	0 = Area has no tamper alarm ****, 1 = Area has at least one tamper alarm ****	DPT 1	1-bit	CR-T-
+8	Area X confirmed alarm	0 = Area has no confirmed alarm **, 1 = Area has at least one confirmed alarm **	DPT 1	1-bit	CR-T-
+13	Area X unset user id	1 – 255 = SPC User ID of user who last unset the area, 0 = User Id is unknown  For user ids > 255 (e.g the FlexC user) the value will be 255.  Will be sent to KNX bus every time Area mode changes to Unset and if value changes of other reason e.g at startup.	DPT 5	1-byte	CR-T-
+14	Area X fullset user id	1 – 255 = SPC User ID of user who last fullset the area, 0 = User Id is unknown	DPT 5	1-byte	CR-T-

		For user ids > 255 (e.g the FlexC user) the value will be 255.  Will be sent to KNX bus when Area mode changes to Fullset (and if value changes of other reason e.g at startup)			
+15	Area X fail to set reason	0 = Area fullset succeeded, 1 = Interlocked, 2 = Calendar was preventing area fullset, 100 (0x64) = An area was preventing area fullset, 101 (0x65) = A (open) zone was preventing area fullset, 102 (0x66) = An alert was preventing area fullset, 200 (0xC8) = Other reason was preventing area fullset  Will be sent to KNX bus every time Area mode changes to new value and if value changes of other reason e.g at exit delay and startup.	DPT 5	1-byte	CR-T-

X = 1 to maximum number of areas (16).

\* Datapoint address = 30 + (X-1) \* 15 + 'relative address'.

\*\* Value is based on Alarm status for zone types Alarm, Exit/Entry, Glassbreak and Exit/Entry2.

\*\*\* Value is based on Alarm status for zone type Fire.

\*\*\*\* Value is based on Alarm status for zone type Tamper and Tamper status for all zone types.

### 5.2.6 SPC Zone Status

For each SPC zone (input) following Group Objects will be available:

Datapoint Address	Name	Values	Datapoint Type	Length	Flags
300 + X	Zone X state	0 = Zone is Closed, 1 = Zone is Open	DPT 1	1-bit	CR-T-
560 + X	Zone X status	0 = OK, 1 = Inhibited, 2 = Isolated, 3 = Soak, 4 = Tamper, 5 = Alarm, 6 = OK, 7 = Trouble, 8 = Masked, 9 = Post Alarm	DPT 5	1-byte	CR-T-

X = 1 to maximum number of zones (256).

## 6 Advanced Users

### 6.1 Backup of Configuration Settings

In **System Administration -> System -> Backup / Flash Firmware**, section **Backup / Restore**, you can save a backup copy of your settings on your PC and later use it to restore the settings.

### 6.2 Upgrading software

In **System Administration -> System -> Backup / Flash Firmware**, you can upgrade the firmware to a new version. The firmware/image file should have the name **dragino-spc-bridge-knx-vX.X.X-squashfs-sysupgrade.bin**. For minor upgrades you can keep your current settings by selecting **Keep settings**. For major upgrades it is preferable to not keep the settings, because they can be incompatible with the new firmware.

1. Copy the image file provided by Lundix to the desktop of your PC.
2. In SPC Bridge **System Administration GUI**, go to **System->Backup/Flash firmware**
3. Just to be sure, do a backup copy of your settings with **Download backup**
4. Under **Flash new firmware image**
  - Check **Keep settings** if you would like to preserve your current settings.
  - Select **Image** file. Select and open the new image file.
  - Click on **Flash image**. The file is now uploaded and verified. Click **Proceed** to continue the installation
5. Wait at least 5 minutes until the installation is finished. (LED Power is ON and LED LAN is ON or Blinking)
6. Go back to sign in page, sign in again and check the settings

### 6.3 SSH Access

The device has as default **ssh** access enabled. Login using username **root** and same password as in the System Administration GUI (default **dragino**). The settings for the SSH access can be changed in the **System Administration->System -> Administration**, section **SSH Access**.

### 6.4 Resetting the SPC Bridge

The SPC Bridge has a toggle button which can be used to reset the device. When the SPC Bridge is **running in normal mode**, you can use a paper clip or similar to press and hold the toggle button.

- If pressing the toggle button and hold it for **5 seconds**, it will reset the **network settings** and other settings will be kept.
- If pressing the toggle button and hold it for **30 seconds**, it will reset **ALL settings** to factory default

## 7 Appendices

### 7.1 SPC Command Error Codes

Error Code	Error Message
0	OK: Command succeeded
10	ERROR: Generic
11	ERROR: Unknown
12	ERROR: Missing ID
13	ERROR: Invalid ID
14	ERROR: Unknown Tag
15	ERROR: Memory Full
16	ERROR: Invalid Data
17	ERROR: Missing Data
18	ERROR: Invalid CRC
19	ERROR: Invalid Length
20	ERROR: Not ready
21	ERROR: Invalid Sequence No
22	ERROR: Invalid Decryption
23	ERROR: Invalid Connection Details
24	ERROR: Invalid Username
25	ERROR: Invalid Password
40	ERROR: Generic check failed
50	ERROR: Active
51	ERROR: Inactive
52	ERROR: Invalid User
53	ERROR: Invalid Number
54	ERROR: Authentication Failed
55	ERROR: Engineer Not Authorized
56	ERROR: Invalid Name
57	ERROR: Invalid Profile
58	ERROR: Invalid Site Code
59	ERROR: Invalid PIN
60	ERROR: Duplicate
61	ERROR: Invalid Card Number
62	ERROR: In use
63	ERROR: Global ID in use
64	ERROR: Global Data Protected
65	ERROR: No Rights
66	ERROR: System Set
67	ERROR: Cannot delete
68	ERROR: Cannot delete last
69	ERROR: Date
70	ERROR: Calendar
71	ERROR: Area
72	ERROR: Door
73	ERROR: Web password not enabled

74	ERROR: Null data
75	ERROR: Bad Command
76	ERROR: Pin Expired
77	ERROR: Blocked
78	ERROR: Not allowed in Engineer mode
79	ERROR: Cannot delete default profile
80	ERROR: Cannot edit default profile
100	ERROR: XML – Buffer Fail
101	ERROR: XML – Bad Format
102	ERROR: XML – Bad Data
103	ERROR: XML – Unknown Tag
104	ERROR: XML – Compulsory Parameter Not Found
120	ERROR: File – Fail
121	ERROR: File – No Space
122	ERROR: File –Not Found
123	ERROR: File – Header
124	ERROR: File – Flash
125	ERROR: File – Flash Verify
126	ERROR: File – Flash Erase
140	ERROR: HTTP – Compulsory Parameter Not Found
160	ERROR: SAM – WD Output
255	ERROR: SPC Communication error

## 7.2 End-User License Agreement for SPC Bridge (EULA)

### **IMPORTANT PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SPC BRIDGE SOFTWARE OR HARDWARE.**

SPC Bridge End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Lundix IT, Sweden, for the SPC Bridge software and hardware product(s) (referred to as the "PRODUCT") which may also include associated software components, media, printed materials, and "online" or electronic documentation. By installing, copying, or otherwise using the PRODUCT, you agree to be bound by the terms of this EULA. This license agreement represents the entire agreement concerning the PRODUCT between you and Lundix IT (referred to as "licenser"), and it supersedes any prior proposal, representation, or understanding between the parties. If you do not agree to the terms of this EULA, do not install or use the PRODUCT.

The PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The software is licensed, not sold.

### **GRANT OF LICENSE.**

The PRODUCT is licensed as follows:

- The FlexC communication program is based on Vanderbilt propriety protocol FlexC and therefore **NOT open-source**.
- **All other software in SPC Bridge** is licensed under many different open source licenses.
- **Backup Copies.** You may make copies of the software as may be necessary for backup and archival purposes.

### **DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.**

- **Maintenance of Copyright Notices.**  
You must not remove or alter any copyright notices on any and all copies of the PRODUCT.
- **Prohibition on Reverse Engineering, Decompilation, and Disassembly.**  
You may not reverse engineer, decompile, or disassemble the program SPC Flex Gateway.
- **Support Services.**  
Lundix IT may provide you with support services related to the PRODUCT ("Support Services"). Any supplemental software code provided to you as part of the Support Services shall be considered part of the PRODUCT and subject to the terms and conditions of this EULA.
- **Compliance with Applicable Laws.**  
You must comply with all applicable laws regarding use of the PRODUCT.

### **COPYRIGHT**

All title, including but not limited to copyrights, in and to the PRODUCT and any copies thereof are owned by Lundix IT or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the PRODUCT is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. All rights not expressly granted are reserved by Lundix IT.

### **NO WARRANTIES**

Lundix IT expressly disclaims any warranty for the PRODUCT. The PRODUCT is provided 'As Is' without any express or implied warranty of any kind, including but not limited to any warranties of merchantability, noninfringement, or fitness of a particular purpose. Lundix IT does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the PRODUCT. Lundix IT makes no warranties respecting any harm that may be caused by the transmission of a computer virus, worm, time bomb, logic bomb, or other such



computer program. Lundix IT further expressly disclaims any warranty or representation to Authorized Users or to any third party.

### LIMITATION OF LIABILITY

In no event shall Lundix IT be liable for any damages (including, without limitation, lost profits, business interruption, or lost information) rising out of 'Authorized Users' use of or inability to use the PRODUCT, even if Lundix IT has been advised of the possibility of such damages. In no event will Lundix IT be liable for loss of data or for indirect, special, incidental, consequential (including lost profit), or other damages based in contract, tort or otherwise. Lundix IT shall have no liability with respect to the content of the PRODUCT or any part thereof, including but not limited to errors or omissions contained therein, libel, infringements of rights of publicity, privacy, trademark rights, business interruption, personal injury, loss of privacy, moral rights or the disclosure of confidential information.

## 7.3 Open Source Software

The SPC Bridge software is based on OpenWrt, a Linux distribution that bundles lots of third party software, under many different licenses. Source code for OpenWrt is available on <http://dev.openwrt.org>.

The most frequently used licenses are:

**GNU General Public License (GPL) and GNU Lesser General Public License (LGPL) version 2.** These firmware images contain software licensed under the GPLv2. A copy of that license can be found at <http://www.gnu.org/licenses/gpl-2.0.txt>.

**Apache License version 2.0.** These firmware images contain software licensed under the APLv2. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>. Modified files carry prominent notices stating who made the changes.

**MIT License.** Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## 7.4 Open Source Hardware

The SPC Bridge hardware is based on the open source hardware Dragino, <http://www.dragino.com>. The Dragino hardware design is released under the **Creative Commons License**, <https://creativecommons.org/licenses/>. The modular Dragino design enables rapid development cycles for commercial products.

END OF DOCUMENT