



SPC42xx/43xx/52xx/53xx/63xx

Installation & Configuration Manual

3.6

Copyright

Technical specifications and availability subject to change without notice.

© Copyright Vanderbilt

We reserve all rights in this document and in the subject thereof. By acceptance of the document the recipient acknowledges these rights and undertakes not to publish the document nor the subject thereof in full or in part, nor to make them available to any third party without our prior express written authorization, nor to use it for any purpose other than for which it was delivered to him.

Edition: 01.05.2016

Document ID: A6V10276959

Table of contents

1	Meaning of symbols.....	11
2	Security	12
2.1	Target group	12
2.2	General safety instructions	12
2.2.1	General information	12
2.2.2	Transport.....	12
2.2.3	Setup.....	13
2.2.4	Operation	13
2.2.5	Service and maintenance	13
2.3	Meaning of written warning notices	14
2.4	Meaning of hazard symbols	14
3	Directives and standards.....	15
3.1	EU directives	15
3.1.1	Overview of Conformity to EN50131 Standard.....	15
3.1.2	Compliance with EN50131 Approvals	19
3.1.3	Compliance with EN 50136-1:2012 and EN 50136-2:2014.....	21
3.1.4	Compliance with INCERT Approvals	21
3.1.5	PD 6662:2010 Conformance Guidelines	23
3.1.5.1	Product scope	23
3.1.5.2	Standards overview	23
3.1.5.3	Methods for the completion of setting and unsetting	23
3.1.5.4	Configuration requirements for PD 6662:2010 conformance	26
3.1.5.5	Additional commissioning requirements for PD 6662:2010 conformance	27
3.1.5.6	Additional information	28
3.1.6	Compliance with VDS approvals	28
3.1.7	Compliance with NF and A2P approvals	29
4	Technical Data	31
4.1	SPC4000	31
4.2	SPC5000	32
4.3	SPC6000	35
4.4	SPCP355.300.....	38
5	Introduction.....	39
6	Mounting system equipment.....	40
6.1	Mounting a G2 housing	40
6.2	Mounting a G3 housing	41
6.2.1	Mounting a Back Tamper Kit	43
6.2.2	Battery installation for EN50131 compliance	47
6.3	Mounting a G5 housing	48
6.3.1	Tamper protection	50
6.3.2	Mounting the housing with tamper protection	50
6.3.2.1	Tamper operation.....	51

6.3.3	Installing the batteries	53
6.4	Mounting a keypad	54
6.5	Mounting an expander.....	54
7	Smart PSU	55
7.1	SPCP355.300 Smart PSU.....	55
7.1.1	Supervised Outputs.....	57
7.1.2	Batteries	58
7.1.2.1	Installing Batteries.....	58
7.1.2.2	Testing Battery Voltage.....	60
7.1.2.3	Deep Discharge Protection	60
7.1.2.4	Battery Stand-By Times	60
7.1.3	Wiring the X-BUS Interface.....	60
7.1.3.1	Wiring the Inputs	61
7.1.3.2	Wiring the Outputs	62
7.1.4	Compliance with NF and A2P approvals	63
7.1.5	PSU LED Status.....	64
7.1.6	System Recovery	65
8	Controller hardware	66
8.1	Controller Hardware 42xx\43xx\53xx\63xx.....	66
8.2	Controller Hardware SPC5350 and 6350.....	69
9	Door Expander	71
10	Wiring the system.....	72
10.1	Wiring the X-BUS interface	72
10.1.1	Loop configuration.....	73
10.1.2	Spur configuration	74
10.1.3	Star and multi-drop configuration.....	75
10.1.3.1	Examples of correct wiring.....	78
10.1.3.2	Examples of incorrect wiring	79
10.1.4	Shielding	80
10.1.5	Cable Map.....	81
10.2	Wiring of branch expander	81
10.3	Wiring the system ground.....	82
10.4	Wiring the relay output.....	82
10.5	Wiring the zone inputs	83
10.6	Wiring an external SAB bell.....	86
10.7	Wiring an internal sounder	87
10.8	Wiring Glassbreak	87
10.9	Installing plug-in modules.....	87
11	Powering up the SPC controller	89
11.1	Powering from battery only.....	89
12	Keypad user interface	90
12.1	SPCK420/421	90
12.1.1	Introduction	90
12.1.2	Using the LCD keypad interface	92
12.1.3	Data entry on the LCD keypad.....	94

12.2	SPCK620/623.....	95
	12.2.1 Introduction	95
	12.2.2 LED description.....	98
	12.2.3 Viewing mode description.....	99
	12.2.4 Function keys in idle state.....	99
13	Software support tools	101
14	Starting the system	102
14.1	Engineer modes	102
	14.1.1 Engineer PINs.....	102
14.2	Programming tools	103
	14.2.1 Fast Programmer.....	103
14.3	Configuring start-up settings	103
14.4	Creating system users.....	105
14.5	Programming the portable ACE	105
14.6	Configuring wireless fob devices.....	106
	14.6.1 Clearing alerts using the fob	107
15	Soft Engineer programming via the keypad.....	109
16	Engineer programming via the keypad.....	110
16.1	System Status	110
16.2	Options	111
16.3	Timers.....	114
16.4	Areas	116
16.5	Area Groups	117
16.6	X-BUS.....	118
	16.6.1 X-BUS Addressing	118
	16.6.2 XBUS Refresh.....	118
	16.6.3 Reconfigure.....	119
	16.6.4 Keypads/Expanders/Door Controllers	120
	16.6.4.1 Locate	120
	16.6.4.2 Monitor	120
	16.6.4.3 Edit Keypads.....	121
	16.6.4.4 Edit Expanders.....	123
	16.6.4.5 Edit Door Controllers.....	127
	16.6.5 Addressing Mode	128
	16.6.6 XBUS Type	129
	16.6.7 Bus Retries	129
	16.6.8 Comms Timer	129
16.7	Wireless.....	130
	16.7.1 Add Sensors	130
	16.7.2 Edit Sensors (Zone Assignment).....	131
	16.7.3 Add WPA.....	131
	16.7.4 Edit WPA.....	132
16.8	Zones.....	132
16.9	Doors.....	133
	16.9.1 Doors.....	133

16.10	Outputs	136
16.10.1	Outputs types and output ports	137
16.11	Communication.....	140
16.11.1	Serial Ports.....	140
16.11.2	Ethernet Ports	140
16.11.3	Modems	141
16.11.3.1	Monitoring the transmission network interface	141
16.11.3.2	Configuring Modems	142
16.11.4	Central Station	143
16.11.4.1	Add	143
16.11.4.2	Edit	143
16.11.4.3	Delete	144
16.11.4.4	Make Test Call	144
16.11.5	Remote Maintenance	144
16.12	Test.....	145
16.12.1	Bell Test	145
16.12.2	Walk Test	145
16.12.3	Zone Monitor	145
16.12.4	Output Test	146
16.12.5	Soak Test	147
16.12.6	Audible Options.....	147
16.12.7	Visual Indicators.....	147
16.12.8	WPA Test.....	148
16.12.9	Seismic Test.....	148
16.13	Utilities	148
16.14	Isolate	149
16.15	Event Log	149
16.16	Access Log	150
16.17	Alarm Log	150
16.18	Change Engineer Pin	150
16.19	Users	150
16.19.1	Add	151
16.19.2	Edit	151
16.19.2.1	Access Control	151
16.19.3	Delete	153
16.20	User Profiles	154
16.20.1	Add	154
16.20.2	Edit	154
16.20.3	Delete	154
16.21	SMS.....	155
16.21.1	Add	155
16.21.2	Edit	156
16.21.3	Delete	156
16.22	X-10	156
16.23	Set Date/Time.....	157
16.24	Installer Text	157

16.25	Door Control	157
16.26	SPC Connect.....	158
17	Engineer programming via the browser	159
17.1	System Information	159
17.2	Ethernet interface	159
17.3	Connecting to the panel via USB	161
17.4	Logging into the browser	163
17.5	SPC Home.....	164
	17.5.1 System Summary.....	164
	17.5.2 Alarms Overview	165
	17.5.3 Viewing Video	165
17.6	Panel status.....	167
	17.6.1 Status.....	167
	17.6.2 X-Bus Status	167
	17.6.2.1 Expander Status	168
	17.6.2.2 PSU status	170
	17.6.2.3 Keypad Status.....	172
	17.6.2.4 Door Controller Status	173
	17.6.3 Wireless	175
	17.6.3.1 Log - Wireless sensor X.....	176
	17.6.4 Zones	176
	17.6.5 Doors.....	178
	17.6.6 FlexC Status	179
	17.6.7 System alerts	180
17.7	Logs.....	181
	17.7.1 System Log	181
	17.7.2 Access Log	181
	17.7.3 WPA Log.....	182
	17.7.4 ALARM LOG	182
17.8	Users	183
	17.8.1 Adding / Editing a User	183
	17.8.1.1 Unknown Devices	185
	17.8.2 Adding / Editing User Profiles	186
	17.8.3 Configuring SMS.....	190
	17.8.4 SMS Commands.....	191
	17.8.5 Deleting Web Passwords.....	193
	17.8.6 Configuring Engineer Settings	193
	17.8.6.1 Changing Engineer PIN and web password	194
17.9	Configuration	196
	17.9.1 Configuring controller inputs & outputs.....	196
	17.9.1.1 Editing an input	196
	17.9.1.2 Editing an output	197
	17.9.1.3 Configuring system latch and auto set outputs.....	202
	17.9.1.4 X10 Config - Settings	203
	17.9.2 X-BUS	204
	17.9.2.1 Expanders.....	204


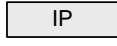




	17.9.2.2	Keypads	209
	17.9.2.3	Door Controllers	214
	17.9.2.4	Cable Map	215
	17.9.2.5	Settings	216
	17.9.3	Wireless	217
	17.9.3.1	Log - Wireless sensor X	218
	17.9.3.2	Configuring a WPA	218
	17.9.3.3	Changing wireless settings	221
	17.9.4	Changing system settings	222
	17.9.4.1	Options	222
	17.9.4.2	Timers	230
	17.9.4.3	Identification	233
	17.9.4.4	Standards	234
	17.9.4.5	Clock	235
	17.9.4.6	Language	236
	17.9.5	Configuring zones, doors and areas	237
	17.9.5.1	Editing a zone	237
	17.9.5.2	Adding / Editing an area	238
	17.9.5.3	Editing a door	246
	17.9.5.4	Adding an area group	251
	17.9.6	Calendars	251
	17.9.6.1	Adding / Editing a calendar	252
	17.9.6.2	Automatic setting/unsetting of areas	254
	17.9.6.3	Automatic setting/unsetting of other panel operations	254
	17.9.7	Change own PIN	255
	17.9.8	Configuring advanced settings	255
	17.9.8.1	Triggers	255
	17.9.8.2	Mapping Gates	256
	17.9.8.3	Audio/Video Verification	257
	17.9.8.4	Updating SPC Licenses	261
17.10		Configuring Communications	261
	17.10.1	Communications Settings	261
	17.10.1.1	Configuring the networking services of the panel	261
	17.10.1.2	Ethernet	262
	17.10.1.3	Modems	263
	17.10.1.4	Serial ports	272
	17.10.2	FlexC®	273
	17.10.2.1	Operation Mode	274
	17.10.2.2	Quick Start ATP Configuration for EN50136 ATS	274
	17.10.2.3	Configuring an EN50136-1 ATS or Custom ATS	276
	17.10.2.4	Configuring an SPC Connect ATS	285
	17.10.2.5	Exporting and Importing an ATS	285
	17.10.2.6	Configuring Event Profiles	286
	17.10.2.7	Configuring Command Profiles	290
	17.10.3	Reporting	292
	17.10.3.1	Alarm Reporting Centres (ARCs)	292

	17.10.3.2 EDP Setup	295
	17.10.4 PC Tools	302
	17.10.4.1 SPC Pro / SPC Safe	302
	17.10.4.2 SPC Manager	303
	17.10.4.3 Remote Maintenance	304
17.11	File Operations	304
	17.11.1 File Upgrade Operations	305
	17.11.1.1 Upgrading Firmware	305
	17.11.1.2 Upgrading Languages	308
	17.11.2 File Manager Operations	310
17.12	Using the Fast Programmer	311
	17.12.1 Connecting the Fast Programmer to the Controller	312
	17.12.2 Installing the Fast Programmer on a PC	312
	17.12.3 Fast Programmer File Operations	313
	17.12.3.1 Accessing the Fast Programmer using the Keypad	313
	17.12.3.2 Accessing the Fast Programmer using the Browser	313
18	Accessing web server remotely	315
18.1	PSTN connection	315
18.2	GSM connection	317
19	Intruder alarm functionality	320
19.1	Financial mode operation	320
19.2	Commercial mode operation	320
19.3	Domestic mode operation	321
19.4	Full and local alarms	321
20	System examples and scenarios	322
20.1	When to use a common area	322
21	Seismic Sensors	324
21.1	Seismic Sensor Testing	325
	21.1.1 Manual and Automatic Test Process	325
	21.1.2 Automatically Testing Sensors	326
	21.1.3 Manually Testing Sensors	327
22	Blocking Lock Operation	328
22.1	Blocking Lock	328
22.2	Authorized Setting of the Blocking Lock	329
22.3	Locking Element	330
23	Appendix	332
23.1	Network cable connections	332
23.2	Controller status LEDs	332
23.3	Powering expanders from the auxiliary power terminals	333
23.4	Calculating the battery power requirements	334
23.5	Domestic, Commercial and Financial mode default settings	336
23.6	Wiring of the X10 interface	337
23.7	SIA Codes	337
23.8	CID Codes	342
23.9	Overview of keypad types	343

23.10	User PIN combinations.....	344
23.11	Duress PINs	345
23.12	Automatic inhibits	345
	23.12.1 Zones	345
	23.12.2 Access PINs.....	345
	23.12.3 Engineer Access	345
	23.12.4 Keypad User Logoff	345
23.13	Wiring of mains cable to the controller	346
23.14	Maintenance controller	346
23.15	Maintenance Smart PSU	347
23.16	Zone types.....	347
23.17	Zone attributes.....	350
23.18	Applicable attributes to zone types.....	352
23.19	ATS levels and attenuation specifications.....	354
23.20	Supported card readers and card formats.....	354
23.21	SPC Support for E-Bus Devices.....	356
	23.21.1 Configuring and Addressing E-Bus Devices.....	356
	23.21.1.1 Addressing Transponders for SAP 8, SAP 14, and SAP 20.....	358
	23.21.1.2 Addressing Transponders for PSU SAP 25.....	358
23.22	FlexC Glossary	359
23.23	FlexC Commands.....	360
23.24	ATS Category Timings	362
23.25	ATP Category Timings	363

1 Meaning of symbols

There are several symbols in the document:

Symbol	Description
	Not available for SPC42xx, SPC43xx.
	Only available for SPC controller with IP interface (SPC43xx/SPC53xx/SPC63xx).
	Not available for installation type Domestic.
	Only available in unrestricted mode.
	Find further information about Security Grade, Region or Mode in text.
	See Appendix for further information.


2 Security

2.1 Target group

The instructions in this documentation are directed at the following target group:

Target readers	Qualification	Activity	Condition of the equipment
Installation personnel	Technical training for building or electrical installations.	Assembles and installs the hardware components on site.	Individual components that need to be assembled and installed.
Operational startup personnel	Has appropriate technical training with regard to the tasks and the products, devices or systems to be put in service.	Puts the device or system which is readily assembled and installed on site into service.	New, readily assembled and installed device or modified device.

2.2 General safety instructions

	⚠ WARNING
	<p>Before starting to install and work with this device, please read the Safety Instructions. This device shall only be connected to power supplies compliant to EN60950-1, chapter 2.5 ("limited power source").</p>

2.2.1 General information

- Keep this document for later reference.
- Always pass this document on together with the product.
- Please also take into account any additional country-specific, local safety standards or regulations concerning project planning, operation and disposal of the product.

Liability claim

- Do not connect the device to the 230 V supply network if it is damaged or any parts are missing.
- Do not make any changes or modifications to the device unless they are expressly mentioned in this manual and have been approved by the manufacturer.
- Use only spare parts and accessories that have been approved by the manufacturer.

2.2.2 Transport

Unit damage during transport

- Keep the packaging material for future transportation.
- Do not expose the device to mechanical vibrations or shocks.

2.2.3 Setup

Radio interference with other devices in the environment / EMS

- When handling modules that are susceptible to electrostatic discharge, please observe the ESD guidelines.

Damage due to unsuitable mounting location

- The environmental conditions recommended by the manufacturer must be observed.
See Technical Data.
- Do not operate the device close to sources of powerful electromagnetic radiation.

Danger of electrical shock due to incorrect connection

- Connect the device only to power sources with the specified voltage. Voltage supply requirements can be found on the rating label of the device.
- Ensure that the device is permanently connected to the electricity supply; a readily accessible disconnect device must be provided.
- Ensure that the circuit that the device is connected to is protected with a 16 A (max.) fuse. Do not connect any devices from other systems to this fuse.
- This device is designed to work with TN power systems. Do not connect the device to any other power systems.
- Electrical grounding must meet the customary local safety standards and regulations.
- Primary supply cables and secondary cables should be routed such that they do not run in parallel or cross over or touch one another inside the housing.
- Telephone cables should be fed into the unit separately from other cables.

Risk of cable damage due to stress

- Ensure that all outgoing cables and wires are sufficiently strain-relieved.

2.2.4 Operation

Dangerous situation due to false alarm

- Make sure to notify all relevant parties and authorities providing assistance before testing the system.
- To avoid panic, always inform all those present before testing any alarm devices.

2.2.5 Service and maintenance

Danger of electrical shock during maintenance

- Maintenance work must only be carried out by trained specialists.
- Always disconnect the power cable and other cables from the main power supply before performing maintenance.


Danger of electrical shock while cleaning the device


- Do not use liquid cleaners or sprays that contain alcohol, spirit or ammonia.

2.3 Meaning of written warning notices

Signal Word	Type of Risk
DANGER	Danger of death or severe bodily harm.
WARNING	Possible danger of death or severe bodily harm.
CAUTION	Danger of minor bodily injury or property damage
IMPORTANT	Danger of malfunctions

2.4 Meaning of hazard symbols

	⚠ WARNING
	Warning of hazard area

	⚠ WARNING
	Warning of dangerous electrical voltage

3 Directives and standards

3.1 EU directives

This product complies with the requirements of the European Directives 2004/108/EC “Directive of Electromagnetic Compatibility”, 2006/95/EC “Low Voltage Directive”, and 1999/5/EC on Radio and Telecommunications Terminal Equipment (R&TTE). The EU declaration of conformity is available to the responsible agencies at <http://pcd.vanderbiltindustries.com/doc/SPC>

European Directive 2004/108/EC „Electromagnetic Compatibility”

Compliance with the European Directive 2004/108/EC has been proven by testing according to the following standards:

emc emission	EN 55022 Class B
emc immunity	EN 50130-4

European Directive 2006/95/EC „Low-Voltage Directive”

Compliance with the European Directive 2006/95/EC has been proven by testing according to the following standard:

Safety	EN 60950-1
--------	------------

3.1.1 Overview of Conformity to EN50131 Standard

This section gives an overview of the SPC compliance to the EN50131 standard.

Address of Certifying Body
VDS (VDS A / C / EN / SES Approval) AG Köln HRB 28788 Sitz der Gesellschaft: Amsterdamer Str. 174, 50735 Köln Geschäftsführer: Robert Reineremann Jörg Wilms-Vahrenhorst (Stv.)

SPC products listed have been tested according to EN50131-3:2009 and all relevant RTC specifications.

Product Type	Standard
<ul style="list-style-type: none"> ● SPC6350.320 ● SPC6330.320 ● SPC5350.320 ● SPC5330.320 ● SPCP355.300 ● SPCP333.300 ● SPCE652.100 ● SPCK420.100 ● SPCK421.100 ● SPCE452.100 ● SPCE110.100 ● SPCE120.100 ● SPCA210.100 ● SPCK620.100 ● SPCK623.100 ● SPCN110.000 ● SPCN310.000 	EN50131 Grade 3

Product Type	Standard
<ul style="list-style-type: none"> ● SPC5320.320 ● SPC4320.320 ● SPCP332.300 	EN50131 Grade 2

Specific information in relation to EN50131 requirements can be found in the following sections in this document.

EN50131 Requirement	SPC Installation & Configuration Manual
Operating temperature and humidity range	Technical data SPC4000 [→ 31] Technical data SPC5000 [→ 32] Technical data SPC6000 [→ 35]
Weights and dimensions	Technical data SPC4000 [→ 31] Technical data SPC5000 [→ 32] Technical data SPC6000 [→ 35]
Fixing details	Mounting system equipment [→ 40]
Installation, commissioning and maintenance instructions, including terminal identifications	Mounting system equipment [→ 40] Controller hardware [→ 66]
Type of interconnections (refer to 8.8);	Technical data SPC4000 [→ 31] Technical data SPC5000 [→ 32] Technical data SPC6000 [→ 35] Wiring the X-Bus Interface [→ 72]
Details of methods of setting and unsetting possible (see 11.7.1 to 11.7.3 and Tables 23 to 26);	User programming via the keypad Areas – Setting/Unsetting [→ 243] Configuring a keyswitch expander [→ 207] Configuring a wireless fob [→ 106] Triggers [→ 255]
Serviceable parts	Technical data SPC4000 [→ 31] Technical data SPC5000 [→ 32] Technical data SPC6000 [→ 35]
Power supply requirement if no integrated PS	See installation instructions for SPCP33x and SPCP43x Expander PSUs.
Where PS is integrated, the information required by EN 50131-6:2008, Clause 6	Technical data SPC4000 [→ 31] Technical data SPC5000 [→ 32] Technical data SPC6000 [→ 35]
Maximum number of each type of ACE and expansion device.	Wiring the X-Bus Interface [→ 72] Technical data SPC4000 [→ 31] Technical data SPC5000 [→ 32] Technical data SPC6000 [→ 35]
Current consumption of the CIE and each type of ACE and expansion device, with and without an alarm condition.	See relevant installation instructions.
Maximum current rating of each electrical output	Technical data SPC4000 [→ 31] Technical data SPC5000 [→ 32] Technical data SPC6000 [→ 35]
Programmable functions provided	Engineer programming via the keypad [→ 110] Engineer programming via the browser [→ 159]

EN50131 Requirement	SPC Installation & Configuration Manual
How indications are made inaccessible to level 1 users when level 2, 3 or 4 user is no longer accessing the information (see 8.5.1)	Keypad user interface [→ 90] Standard keypad settings [→ 121] Comfort keypad settings [→ 122] Configuring an Indicator Expander [→ 206]
Masking/reduction of range signals/messages processed as “fault” or “masking” events (see 8.4.1, 8.5.1 and Table 11);	System Options [→ 222] Wiring the zone inputs [→ 83] SIA Codes [→ 337] PIR masking is always reported as a zone masked event (SIA - ZM). Additionally, anti-mask can cause an alarm, tamper, trouble or no additional action depending on configuration Current defaults of PIR addition effect: Ireland Unset - None Set - Alarm UK, Europe, Sweden, Swiss, Belgium Unset - Tamper Set - Alarm
Prioritization of signal and message processing and indications (see 8.4.1.2, 8.5.3);	Standard keypad display [→ 92] Comfort keypad display [→ 95]
Minimum number of variations of PIN codes, logical keys, biometric keys and/or mechanical keys for each user (see 8.3);	User PIN combinations [→ 344]
Method of time-limiting internal WD for level 3 access without level 2 authorization (see 8.3.1);	Not supported - Engineer cannot access system without permission.
Number and details of disallowed PIN codes (see 8.3.2.2.1);	Automatic inhibits [→ 345]
Details of any biometric authorization methods used (see 8.3.2.2.3);	Not applicable
Method used to determine the number of combinations of PIN codes, logical keys, biometric keys and/or mechanical keys (see 11.6);	User PIN combinations [→ 344]
Number of invalid code entries before user interface is disabled (see 8.3.2.4);	Access PINs [→ 345]
Details of means for temporary authorization for user access (see 8.3.2);	User Menus – Grant Access
if automatic setting at pre-determined times provided, details of pre-setting indication and any automatic over-ride of prevention of set (see 8.3.3, 8.3.3.1);	Areas – Setting/Unsetting [→ 243]
Details of conditions provided for the set state (see 8.3.3.4);	Setting and unsetting the system Standard keypad configuration [→ 121] Comfort keypad configuration [→ 122] Outputs [→ 198] Zone types [→ 347]
Notification of output signals or messages provided (see 8.6);	Outputs [→ 198] Areas – setting/unsetting [→ 243] User rights [→ 187]

EN50131 Requirement	SPC Installation & Configuration Manual
Other output configurations to interface with I&HAS components (see 8.2);	Outputs [→ 198] Zone types [→ 347] Test [→ 145] Keypad user interface [→ 90]
Criteria for automatic removal of “soak test” attribute (see 8.3.9);	Timers [→ 230]
Number of events resulting in automatic inhibit	Automatic Inhibits [→ 345]
If ACE is Type A or Type B (see 8.7) and whether portable or moveable (see 11.14);	All devices are hardwired and powered by system PSUs. Refer to relevant technical data on PSUs.
Component data for non-volatile memory components (see Table 30, step 6);	See user documentation for SPCK420/421 and SPCK620/623 keypads.
Life of memory support battery (see 8.10.1);	N/A. Stored in non-volatile memory.
Optional functions provided (see 4.1);	Engineer programming via the keypad Engineer programming via the browser [→ 159]
Additional functions provided (see 4.2, 8.1.8);	Grade - Unrestricted Policies – System options [→ 222]
Access levels required to access such additional functions provided;	User configuration (keypad) [→ 151] User configuration (browser) [→ 183]
Details of any programmable facility that would render an I&HAS non-compliant with EN 50131-1:2006, 8.3.13 or compliant at a lower security grade, with instruction on consequent removal of compliance labeling (see 4.2 and 8.3.10).	Grade - Unrestricted Policies – System options [→ 222] EN50131 Compliance [→ 19]

SPC products listed have been tested according to EN50131-6, and all relevant RTC specifications.

Product Type	Standard
<ul style="list-style-type: none"> ● SPC6350.320 ● SPC6330.320 ● SPC5350.320 ● SPC5330.320 ● SPCP355.300 ● SPCP333.300 ● SPCP355.300 ● SPCE652.100 ● SPCK420.100 ● SPCK421.100 ● SPCE452.100 ● SPCE110.100 ● SPCE120.100 ● SPCA210.100 ● SPCK620.100 ● SPCK623.100 ● SPCN110.000 ● SPCN310.000 	EN50131-6

Product Type	Standard
<ul style="list-style-type: none"> ● SPC5320.320 ● SPC4320.320 ● SPCP332.300 	EN50131-6

3.1.2 Compliance with EN50131 Approvals

Software Requirements



It is not possible to change the Region or Grade in SPC Pro. It is only possible to change these settings in the browser or keypad.

The screenshot shows the 'Standards' settings page. At the top, there is a navigation bar with tabs for Hardware, System, Inputs, Outputs, Doors, Areas, Calendars, Change own PIN, and Advance. Below this, there are sub-tabs for System Options, System Timers, Identification, Standards (selected), Clock, and Language. The main content area is titled 'Standard compliance settings' and contains three sections: 'Installation Type' with radio buttons for Domestic, Commercial, and Financial (selected); 'Region' with radio buttons for various regional requirements, with 'Select for compliance to European requirements' selected; and 'Grade' with radio buttons for EN50131 Grade 2, EN50131 Grade 3, and Unrestricted (selected). A 'Save' button is located at the bottom left. A gear icon is visible on the right side of the page.

- In the **Standards** settings page, select **Europe** under **Region** to implement EN50131 requirements.
- Select **Grade 2** or **Grade 3** to implement the grade of EN50131 compliance.
- The **Wireless** settings **Prevent Setting Time** and **Device Lost Time** must be set to a value other than 0.
- Select **Synchronization Time with Mains** under **Clock** settings to use mains as clock master.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
System Options	System Timers	Identification	Standards	Clock	Language			

Current Time and Date

Time: Hour: 15 : Minute: 18 : Second: 18

Date: Day: 7 / Month: Jul / Year: 2014

Automatic Daylight Saving Time:

Synchronize Time with Mains:

Save

- DO NOT select the attribute **Setting State** in the **Keypad** configuration settings for **Visual indications**.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Expanders	Keypads	Door Controllers	Cable Map	X-Bus Settings				

Keypad Configuration

Keypad ID: 1
 S/N: 559907
 Description: KEY 1 Enter keypad description.

Function Keys (in idle state)

Panic: Disabled Panic alarm by pressing the two Soft keys together.

Verification

Verification: Unassigned Verification will be triggered on keypad for duress or alert activated from keypad

Visual Indications

Backlight: On when key is pressed Select keypad LCD backlight option.

Indicators: Enable visible indicators (LED's).

Setting State: Check if setting state should be indicated in idle mode (LED).

Audible Indications

Buzzer: Enable keypad buzzer

Partset buzzer: Enabling will sound exit timer during Partset

Keypress: Check if keypress should be audible.

Deactivation

Calendar: None Check if keypad should be limited by calendar.

Mapping gate: None Check if keypad should be limited by a mapping gate.

Keyswitch: None Check if keypad should be limited by a keyswitch.

PACE Entry: Disable keys during entry time.

Areas

Location: 1: Marketing Select secured area where the keypad is located.

Areas: Select which areas can be controlled through keypad.

1: Marketing 3: Finance 5: Meeting Room
 2: Reception 4: Cafeteria


Options

Delay Fullset: Will use exit timer across all area

Save Back

Hardware Requirements

- The back tamper kit (SPCY130) must be installed for panels and power supplies for compliance with EN50131 Grade 3.
- EN50131 Grade 3 compliant components must be installed for EN50131 Grade 3 compliant systems.
- Either EN50131 Grade 2 or 3 compliant components must be installed for EN50131 Grade 2 compliant systems.
- It is not possible to enrol a wireless device with a signal strength lower than 3.
- The recommended ratio of wireless receivers to transmitters is no more than 20 transmitters for every one receiver.
- Glassbreak must be used with an EN-compliant glassbreak interface.
- To comply with EN50131-3:2009, do not set or unset the system using the SPCE120 (Indicator Expander) or the SPCE110 (Keypad Expander).

	NOTICE
	The SPCN110 PSTN module and SPCN130 GSM/GPRS module are tested with EN50131 approved Grade 2 and Grade 3 panels and can be used with these approved panels.

3.1.3 Compliance with EN 50136-1:2012 and EN 50136-2:2014

SPC products listed have been tested according to EN 50136-1:2012 and EN 50136-2:2014.

3.1.4 Compliance with INCERT Approvals

Software Requirements

Selecting Belgium (*) under **Region** implements local or national requirements which supercede EN50131 requirements.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advance
System Options	System Timers	Identification	Standards	Clock	Language			

Standard compliance settings**Installation Type:**

- Domestic
 Commercial
 Financial

Region:

- Select for compliance to UK requirements
 Select for compliance to Irish requirements
 Select for compliance to Swedish requirements
 Select for compliance to European requirements
 (*) Select for compliance to Swiss requirements
 (*) Select for compliance to Belgium requirements
 (*) Select for compliance to Spanish requirements
 (*) Select for compliance to German requirements
 (*) Select for compliance to French requirements

Grade

- EN50131 Grade 2
 EN50131 Grade 3
 Unrestricted

(*) Selecting this regional standard will implement local or national requirements which supersede EN50131 requirements

Save

Selecting **Grade 2** or **Grade 3** selects EN50131 compliance plus any additional INCERT requirements:

- Only an engineer can restore a tamper. For INCERT, this applies across all grades.
This is normally only a requirement for Grade III En50131.
- A tamper on an Inhibited / Isolated zone must be sent to an ARC and displayed to the user.
For INCERT, tampers are processed for isolated zones. On all other standard variations, tampers are ignored on isolated zones.
- User PIN codes must be defined with more than 4 digits.

Hardware Requirements

- The minimum battery capacity for SPC42xx/43xx/52xx/53xx/63xx is 10 Ah / 12 V. If a 10 Ah battery is used, then the battery is biased to the left of the cabinet and the bottom flap is bent to meet the battery.
- Fit jumper (J12) on the battery selector for 17/10 Ah battery use and remove for 7 Ah battery.
- The amount of current from Aux output using a 10 Ah battery for SPC42xx/SPC52xx is:

COMMS	NONE	PSTN	GSM	PSTN+GSM
Standby time				
12 h	568 mA	543 mA	438 mA	413 mA
24h	214 mA	189 mA	84 mA	59 mA
30 h	143 mA	118 mA	13 mA	N/A
60h	2mA	N/A	N/A	N/A

- The amount of current from Aux output using a 10 Ah battery for SPC43xx/SPC53xx/ SPC63xx is:

COMMS	NONE	PSTN	GSM	PSTN+GSM
Standby time				
12 h	538 mA	513 mA	408 mA	383 mA
24 h	184 mA	159 mA	54 mA	29 mA
30 h	113 mA	88mA	N/A	N/A
60 h	N/A	N/A	N/A	N/A

3.1.5 PD 6662:2010 Conformance Guidelines

This appendix contains all the criteria for the installation, and commissioning and maintenance of the SPC System to enable it to conform to the PD 6662:2010 Standard.

3.1.5.1 Product scope

The scope of this document is aimed at the following components of the SPC system:

SPC4320.320-L1 Grade 2 Controller	SPCE652.100 Expander, 8 Inputs / 2 Outputs
SPC5320.320-L1 Grade 2 Controller	
SPC5330.320-L1 Grade 3 Controller	SPCP332.300 Smart PSU with I/O Expander
SPC5350.320-L1 Grade 3 Controller	SPCP355.300 Smart PSU with 8 Inputs / 2 Outputs Expander
SPC6330.320-L1 Grade 3 Controller	SPCP333.300 Smart PSU with I/O Expander
SPC6350.320-L1 Grade 3 Controller	
SPCK420/421.100 LCD Keypad	SPCN110.000 PSTN Module
SPCE452.100 Expander, 8 Relay Outputs	SPCN310.000 GSM Module

3.1.5.2 Standards overview

Guidelines are provided for the implementation of PD 6662:2010 conformance for an SPC system to the following relevant standards:

PD 6662:2010	BS EN 50136-1-5:2008
BS 4737-3.1:1977	BS EN 50136-2-1:1998 +A1:1998
BS 8243:2010	BS EN 50136-2-2:1998
BS 8473:2006+A1:2008	BS EN 50136-2-3:1998
BS EN 50131-1:2006+A1:2009	BS EN 50131-3:2009
BS EN 50136-1-1:1998+A2:2008	BS EN 50131-6:2008
BS EN 50136-1-2:1998	DD 263:2010
BS EN 50136-1-3:1998	DD CLC/TS 50131-7:2008

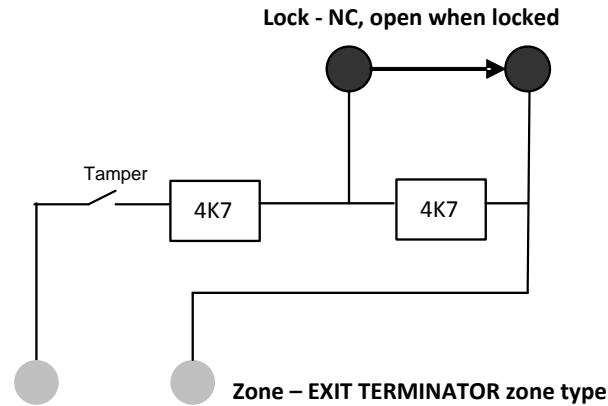
3.1.5.3 Methods for the completion of setting and unsetting

3.1.5.3.1 Methods of completion of setting (BS 8243:2010 - Clause 6.3)

Completion/Termination of the full setting procedure is achieved by any of the following methods:

a) Shunt lock fitted to the final exit door

A shunt lock must be installed by the installer as follows:



An EXIT TERMINATOR zone type must be configured for SPC.
Refer to the following section in this manual:
Zone types [→ 347]

b) Push button switch mounted outside the supervised premises
Connect the push button into an SPC zone input as follows:

An EXIT TERMINATOR zone type must be configured for SPC.
Refer to the following section in this manual:
Zone types [→ 347]

c) Protective switch (i.e. door contact) fitted to the final exit door of the alarmed premises or area
Connect the switch to the SPC System as follows:

The contact is fitted to the final exit door and is connected to an ENTRY/EXIT zone with a 'Final Exit' attribute.
Refer to the following section in this manual:
Zone types [→ 347]
Zone attributes [→ 350]

A misoperation signal is possible using the alarm abort feature. This is enabled by default.
Refer to the following section in this manual:
OPTIONS [→ 111] (Kypad)
Options [→ 222] (Browser)

d) Digital key
Not supported by SPC.

e) In conjunction with an ARC
This method of setting is supported by using SPC COM XT or other third party ARC software using EDP commands.

3.1.5.3.2 Methods of completion of unsetting (BS 8243:2010 - Clause 6.4)

Unsetting methods are complied with as follows:

6.4.1 For all the unsetting methods in the SPC system there is an audible indication to the user that the system has been unset successfully. This is in the form of a beep sequence from the CIE.

6.4.2 Prevention of entry to the supervised premises before the intruder alarm system (IAS) is unset:

a) Unlocking the initial entry door causes the IAS to be unset;

Compliance by SPC if KEYARM zone type is used with the UNSET attribute only. This zone type must not be used for setting.

b) Unsetting the IAS by the user before entering the supervised premises causes or permits the initial entry door to be unlocked.

Compliance by SPC by unsetting using an access card reader on an entry reader with the UNSET option, or an input from a third party access system to a KEYARM zone with an UNSET attribute.

6.4.3 Prevention of entry to the supervised premises before all means of intruder alarm confirmation have been disabled:

a) Unlocking the initial entry door causes all means of confirmation to be disabled
Operation not permitted by SPC.

b) Disabling all means of confirmation by the user before entering the supervised premises causes or permits the initial entry door to be unlocked

Operation not permitted by SPC.

6.4.4 Opening the initial entry door disables all means of intruder alarm confirmation

Operation not permitted by SPC.

6.4.5 Completion of unsetting using a digital key

a) Operation of a digital key before entering the supervised premises (for example, via radio)

SPC satisfies this clause when the installer installs a PACE reader (e.g. SPCK421) outside the premises.

b) Operation of a digital key after entering the supervised premises from a location as near as practicable to the initial entry door.

This functionality is provided by use of a PACE reader (e.g. SPCK421) near the entry door of a premises.

Refer to the following sections in this manual:

- Zone types [→ 347]
- Zone attributes [→ 350]



⚠ WARNING

Your attention is drawn to the fact that by allowing this method of unsetting, if an intruder succeeds in forcing the initial entry door, the police will not be called, regardless of the intruder's further progress through the premises.

This method of unsetting the intruder alarm system might be unacceptable to your insurers.

6.4.6 Unsetting in conjunction with an alarm receiving centre (ARC)

Compliance by SPC using third party ARC software. Indication external to the building must be provided by means of a timed buzzer/strobe, etc. that will operate on a system unset for a timed period e.g. 30 seconds.

Refer to the following sections in this manual:

Timers [→ 114]

3.1.5.4 Configuration requirements for PD 6662:2010 conformance

Recommendations for the recording of remotely notified alarm conditions (BS 8243:2010 - Annex G.1 and G.2)

Alarm conditions can be categorised for analysis in accordance with Annex G if the SPC system is configured so that the entry timer is less than 30 seconds, and the dialer delay is set to 30 seconds.

Refer to the following sections in this manual:

AREAS [→ 116]

Adding / Editing an area [→ 238]

Timers [→ 114]

Requirements for systems using dedicated alarm paths (BS EN 50136-1-2, 1998)

The SPC system should be configured to do an automated test call to the ARC.

The SPC system should be configured with a 'Fail to Communicate' output.

Refer to the following section in this manual:

Adding/Editing an ARC [→ 292]

Requirements for equipment used in systems with digital communicators using PSTN (BS EN 50136-2-2, 1998)

Fault Output

The SPC system should be configured with a 'Fail to Communicate' output.

Refer to the following sections in this manual:

OUTPUTS [→ 136] (Keypad)

Configuring controller inputs & outputs [→ 196] (Browser)

Adding/Editing an ARC [→ 292]

Retransmission Attempts

Retransmission attempts (Dial Attempts) are configured in this manual:

Adding/Editing an ARC [→ 292]

Editing EDP settings [→ 301]

A minimum of 1 and a maximum of 12 retransmissions are allowed.

Intrusion and hold-up - System design (DD CLC TS 50131-7, 2008)

Setting and unsetting

SPC system is configurable in such a way that the setting is completed by 'Final Exit'.

It is possible to configure the SPC so that a WD (Warning Device) is activated momentarily on setting.

Refer to the following sections in this manual:

Timers [→ 114]

Zone attributes [→ 350]

OUTPUTS [→ 136] (Keypad)

Editing an output [→ 197] (Browser)

Intrusion and confirmed hold-up alarm (BS8243:2010 Designation of hold-up alarm (HUA) signals for sequential confirmation)

SPC system is configurable in such a way that the following scenarios, when triggered more than two minutes apart from any hold-up zone or hold-up device (HD), will report a confirmed hold-up alarm event (HV for SIA and 129 for CID) to the CIE:

- two hold-up zone activations
- a hold-up zone and a panic zone activation

If a hold-up zone and a tamper zone or a panic zone and a tamper zone activation occurs within the two minute period, this will also send a confirmed hold-up alarm event.

A confirmed hold-up will not require an engineer restore even if engineer restore is enabled. A confirmed hold-up event is logged in the system log.

Security of communications for remote support and remote system checks (DD 263:2010)

Please ensure that SPC Pro is used within the guidelines specified in DD 263:2010.

3.1.5.5 Additional commissioning requirements for PD 6662:2010 conformance

Information to be included in the system design proposal and as-fitted document (BS 8243:2010 - Annex F)

- During the installation, configuration and commissioning of an SPC system, the installer must adhere to the following guidelines as required in the above annex:
- It is recommended that dual paths are used for signalling which are supported in the SPC system using GSM, PSTN and Ethernet options.
- The SPC system must be installed and configured to provide an effective confirmation facility. Any exceptions to this should be outlined in the 'As Fitted' document.
- Combinations and sequences which contribute to a confirmed alarm should be clearly notified to the end user.
- The intrusion confirmation time should be clearly notified to the end user.
- Methods of completion of setting and unsetting methods should be clearly described to the end user as detailed in this document.
- Ensure written arrangements are supplied to the end user in the event of a lock failure.



It is recommended that the enclosed PD 6662:2010 label is affixed in an appropriate position on the inside of the SPC housing beside the product type label.

3.1.5.6 Additional information

Transmission Network Requirements – Performance, Availability and Security Levels (BS EN 50136-1-2, 1998 and BS EN 50136-1-5, 2008)

The SPC System has been tested and approved to EN50136-1-1.

SPC levels are classified as follows:

Transmission time	D2 as max.
Transmission time, max. values	M0 - M4
Reporting time	T3 as max.
Availability	Refer to the following section in this manual: ATS levels and attenuation specifications [→ 354]
Signalling security level	Tested to EN50136-1-1 and classified as 'S0'.

3.1.6 Compliance with VdS approvals

This installation document encompasses the required product installation information for VdS approvals.

Vanderbilt

SPC42xx/43xx/53xx/63xx : VdS Approval Nr. G 112104, G112124, and G112128. VdS EN Certificates EN-ST000142, EN-ST000143, EN-ST000055, EN-ST000056, EN-ST000057, EN-ST000058, EN-ST000061, EN-ST000062.

Siemens

SPC42xx/43xx/53xx/: VdS Approval Nr. G116035. VdS EN Certificates EN-ST000225, EN-ST000226, EN-ST000227, EN-ST000228, EN-ST000229, EN-ST000230, EN-ST000231, EN-ST000232.

This section describes the compliance of this system with VdS approvals.

Software

To set the system for VDS compliance, do the following:

1. Log on to the panel with the browser.
2. Click Full Engineer.
3. Click Settings on the menu.
4. Click Standards.
5. Select the German region from the Region list.
6. Select the VDS grade required by your installation type.
 - Remote Isolations — It is not possible to deisolate isolated faults using the browser or SPCPro. Deisolation can only be performed on the keypads.
 - Remote Connections — it is not possible to use the browser or SPCPro to connect to an armed system.
 - Confirmed alarms — an internally set system cannot create a confirmed alarm.

- Hardware Fault reporting — in **Options**, you must select the **Enabled + Reporting (10s)** option from the **Watchdog Output Mode** drop-down list.
Note: Hardware faults are not reported if the Engineer is logged in to the system.

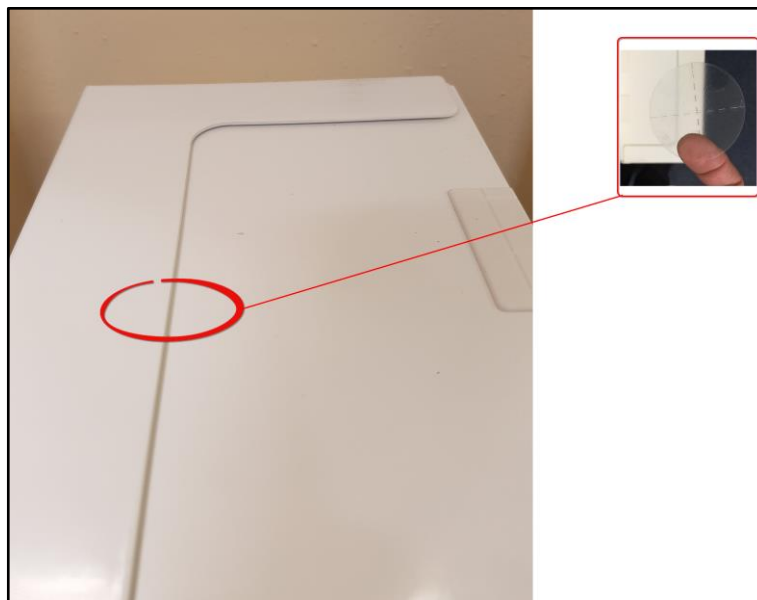
Hardware

VDS compliance requires the following:

- A G5 housing with Front tamper implemented as a minimum requirement.
- Keypads do not show status information if the system is armed.
- The number of supported zones is as follows:
 - 512 zones in ring configuration
 - 128 zones per X-Bus in multi-drop (spur) configuration
- The following end of line resistance combinations do not comply with VdS standards:
 - 1k, 470 ohm
 - 1k, 1k, 6k6 ohm





3.1.7 Compliance with NF and A2P approvals

Address of Certifying Body	
CNPP Cert Pôle Européen de Sécurité - Vernon Route de la Chapelle Réanville CD 64 - CS 22265 F-27950 SAINT MARCEL www.cnpp.com	AFNOR Certification 11 rue François de Pressensé 93571 Saint Denis La Plaine Cedex www.marque-nf.com



To comply with NF & A2P installation regulations, this enclosure must be sealed by affixing the accompanying Tamper Label after installation.

SPC products listed have been tested according to NF324 - H58, with reference to RTC50131-6 and RTC50131-3 and current EN certifications, see Compliance with EN50131 Approvals [→ 19].

Product Type	Configuration	Standard	Logo
SPC6350.320 + SPCP355.300 (Cert. 1233700001A0)	60h, unmonitored	NF Grade 3, Class 1	
SPC5350.320 + SPCP355.300 (Cert. 1233700001B0)	60h, unmonitored		
SPC6350.320 (Cert. 1233700001A0)	60h, unmonitored		
SPC5350.320 (Cert. 1233700001B0)	60h, unmonitored		
SPC6330.320 + SPCP333.300 (Cert. 1232200003)	60h, unmonitored	NF Grade 3, Class 1	
SPC5330.320 + SPCP333.300 (Cert. 1232200003)	60h, unmonitored		
SPC6330.320 (Cert. 1232200003)	30h, monitored		
SPC5330.320 (Cert. 1232200003)	30h, monitored		
SPC5320.320 (Cert. 1222200003)	36h, unmonitored	NF Grade 2, Class 1	
SPC4320.320 (Cert. 1222200003)	36h, unmonitored		
SPCN110.000 SPCN310.000 SPCK420.100 SPCK620.100 SPCK623.100 SPCE652.100 SPCE452.100 SPCE110.100 SPCE120.100		NF Grade 2 and 3, Class 1	

4 Technical Data

4.1 SPC4000

Programmable areas	4
Max. number of user PINs	100
Remote controls	Up to 32
Wireless Panic Alarm	Up to 128
Event memory	1000 intrusion events, 1000 access events
Number of on-board zones	8
Max. number of hardwired zones	32
Max. number of wireless zones	32 (take away wired zones)
Max. number of Intrunet wireless detectors per wireless receiver (recommended)	20
EOL resistor	Dual 4k7 (default), other resistor combinations configurable
Number of on-board relays	1 strobe (30 VDC / 1 A resistive switching current)
Number of on-board open coll.	2 internal / external bell, 3 freely programmable (each max. 400 mA resistive switching current, supplied via auxiliary output)
Firmware	V3.x
Door capacity	Max. 4 entry doors or 2 entry/exit doors
Number of card reader	Max. 4
Radio module	<ul style="list-style-type: none"> ● SPC4221: integrated SiWay RF receiver (868 MHz) ● SPC4320.220: Optional (SPCW111), ● SPC4320.320: Optional (SPCW110)
Verification	4 verification zones with max. 4 IP-cameras and 4 audio devices.
Video	Up to 16 pre / 16 post event images (by JPEG resolution 320 x 240, max. 1 frame / sec.)
Audio	Up to 60 sec. pre / 60 sec. post audio recording
Field bus 1)	X-BUS on RS-485 (307 kb/s)
Number of field devices 2)	Max. 11 (4 keypads, 2 door-expanders, 5 input/output expanders)
Connectable field devices	<ul style="list-style-type: none"> ● Keypads: SPCK42x, SPCK62x ● Door expanders: SPCA210, SPCP43x ● Expanders with I/O: SPCE65x, SPCE45x, SPCP33x, SPCE110, SPCE120, SPCV32x
Interfaces	<ul style="list-style-type: none"> ● 1 X-BUS (1 spur) ● 1 RS232 ● USB (PC connection) ● 1 SPC Fast Programmer ● SPC43xx: Additionally 1 Ethernet (RJ45)
Tamper contact	Front spring tamper, 2 auxiliary tamper contact inputs
Power supply	Type A (per EN50131-1)
Mains voltage	230 VAC, + 10%/ -15%, 50 Hz
Mains fuse	250 mA T (replaceable part on mains terminal block)
Power consumption	SPC42xx: Max. 160 mA at 230 VAC SPC43xx: Max. 200 mA at 230 VAC
Operating current	SPC42xx Controller: Max. 160 mA at 12 VDC SPC43xx Controller: Max. 200 mA at 12 VDC

Quiescent current	SPC42xx Controller: Max. 140 mA at 12 VDC (165 mA with PSTN, 270 mA with GSM, 295 mA with PSTN & GSM) SPC43xx Controller: Max. 170 mA at 12 VDC (195 mA with PSTN, 300 mA with GSM, 325 mA with PSTN & GSM)
Output voltage	13-14 VDC in normal conditions (mains powered and fully charged battery), min. 10.5 VDC when powered by secondary device (before system shut down to battery deep discharge protection)
Low voltage trigger	7.5 VDC
Overvoltage protection	15.7 VDC
Peak to Peak ripple	Max. 5 % of output voltage
Auxiliary power (nominal)	Max. 750 mA at 12 VDC
Battery type	SPC422x/4320: YUASA NP7-12FR (7 Ah), Battery not supplied
Battery charger	SPC422x/4320: Max. 72h to 80% of battery capacity
Battery protection	Current limited to 1 A (fuse protected), deep discharge protection at 10.5 VDC +/- 3 %
Software update	Local and remote upgrade for controller, peripherals and GSM/PTSN modems.
Calibration	No calibration checks required (calibrated at manufacturing)
Serviceable parts	No serviceable parts
Operating temperature	-10 ~ +50 °C
Relative humidity	Max. 90 % (non condensing)
Colour	RAL 9003 (signal white)
Weight	SPC422x/4320: 4.500 kg
Dimensions (W x H x D)	SPC422x/4320: 264 x 357 x 81 mm
Housing	SPC4320.320: Small metal housing (1.2 mm mild steel) SPC422x.220: Small housing with metal base (1.2 mm mild steel) and plastic lid
Housing can contain up to	SPC422x/4320: 1 additional expander (size 150 mm x 82 mm)
IP rating	30
ATS	2
ATP	4
Event Profiles	5
Event Exceptions	10
Command Profiles	5

1) Max. 400 m between devices / cable types IYSTY 2 x 2 x Ø 0.6 mm (min.), UTP cat5 (solid core) or Belden 9829.

2) More I/O expanders can be addressed instead of a keypad or door expander, but number of programmable inputs / outputs cannot exceed specified system limits.

4.2 SPC5000

Programmable areas	16
Max. number of user PINs	500
Remote controls	Up to 100
Wireless Panic Alarm	Up to 128

Event memory	10,000 intrusion events, 10,000 access events
Number of on-board zones	<ul style="list-style-type: none"> ● SPC5320\5330 — 8 ● SPC5350 — 16
Max. number of hardwired zones	128
Max. number of wireless zones	120 (take away wired zones)
Max. number of Intrunet wireless detectors per wireless receiver (recommended)	20
EOL resistor	Dual 4k7 (default), other resistor combinations configurable
Relay Outputs	<ul style="list-style-type: none"> ● SPC5320\5330 — 1 strobe (30 VDC/1A resistive switching current) ● SPC5350 — 4 (single-pole changeover, 30VDC/ maximum 1A resistive switching current)
Electronic Outputs	<ul style="list-style-type: none"> ● SPC5320\5330 — 5 outputs: <ul style="list-style-type: none"> – 2 internal/external bells – 3 programmable. Maximum 400 mA resistive switching current per output, supplied by auxiliary output. ● SPC5350 — 8 outputs. Maximum 400mA resistive switching current per output <ul style="list-style-type: none"> – 5 standard power outputs – 3 supervised outputs
Firmware	V3.x
Door capacity	Max. 16 entry doors or 8 entry/exit doors
Number of card reader	Max. 16
Radio module	Optional (SPCW110)
Verification	16 verification zones with max. 4 IP-cameras and 16 audio devices.
Video	Up to 16 pre / 16 post event images (by JPEG resolution 320 x 240, max. 1 frame / sec.)
Audio	Up to 60 sec. pre / 60 sec. post audio recording
Field bus 1)	X-BUS on RS-485 (307 kb/s)
Number of field devices 2)	Max. 48 (16 keypads, 8 door-expanders, 16 input/output expanders)
Connectable field devices	<ul style="list-style-type: none"> ● Keypads: SPCK42x, SPCK62x ● Door expanders: SPCA210, SPCP43x ● Expanders with I/O: SPCE65x, SPCE45x, SPCP33x, SPCP35x, SPCE110, SPCE120, SPCV32x
Interfaces	<ul style="list-style-type: none"> ● 2 X-BUS (2 spurs or 1 loop), ● 2 RS232 ● 1 USB (PC connection), ● 1 SPC Fast Programmer, ● SPC53xx: Additionally 1 Ethernet (RJ45)
Tamper contact	<ul style="list-style-type: none"> ● SPC5320/5330: Front spring tamper, 2 auxiliary tamper contact inputs ● SPC5350: Front/back tamper switch
Power supply	Type A (per EN50131-1)
Mains voltage	230 VAC, + 10%/ -15%, 50 Hz

Mains fuse	<ul style="list-style-type: none"> ● SPC5320/5330: 250 mA T (replaceable part on mains terminal block) ● SPC5350 : 800mA T (replaceable part on mains terminal block)
Power consumption	<ul style="list-style-type: none"> ● SPC5320/5330: Max. 200 mA at 230 VAC ● SPC5350: Max. 500mA at 230 V AC
Operating current	<ul style="list-style-type: none"> ● SPC5320/5330: Controller: Max. 200 mA at 12 VDC ● SPC5350: Max. 210 mA at 12 VDC
Quiescent current	SPC53xx Controller: Max. 170 mA at 12 VDC (195 mA with PSTN, 300 mA with GSM, 325 mA with PSTN & GSM)
Output voltage	13-14 VDC in normal conditions (mains powered and fully charged battery), min. 10.5 VDC when powered by secondary device (before system shut down to battery deep discharge protection)
Low voltage trigger	11 VDC
Overvoltage protection	<ul style="list-style-type: none"> ● SPC5320/5330: 15.7 VDC ● SPC5350: 15 VDC nominal
Peak to Peak ripple	Max. 5 % of output voltage
Auxiliary power (nominal)	<ul style="list-style-type: none"> ● SPC5320/5330: Max. 750 mA at 12 VDC ● SPC5350: Max. 2200 mA at 12 VDC (8 separately fused outputs, 300 mA per output)
Battery type	<ul style="list-style-type: none"> ● SPC5320: YUASA NP7-12FR (7 Ah), ● SPC5330: YUASA NP17-12FR (17 Ah) ● SPC5350: YUASA NP24-12 (12 V 24 Ah), Alarmcom AB1227-O (12 V 27 Ah) ● SPC5350: FIAMM FGV22703 (12V 27Ah) Battery not supplied
Battery charger	<ul style="list-style-type: none"> ● SPC5320: Max. 72h, ● SPC5330/5350: Max. 24h to 80% of battery capacity
Battery protection	<ul style="list-style-type: none"> ● SPC5320/5330: Current limited to 1 A (fuse protected), deep discharge protection at 10.5 VDC +/- 3 % ● SPC5350: Current limited to 2 A (protected by PTC resettable fuse), deep discharge protection at 10.5 VDC
Software update	Local and remote upgrade for controller, peripherals and GSM/PTSN modems.
Calibration	No calibration checks required (calibrated at manufacturing)
Serviceable parts	<ul style="list-style-type: none"> ● SPC5320/5330: No serviceable parts ● SPC5350: 8 glass fuses (400mA AT) for 12 VDC outputs
Operating temperature	-10 ~ +50 °C
Relative humidity	Max. 90 % (non condensing)
Colour	RAL 9003 (signal white)
Weight	<ul style="list-style-type: none"> ● SPC5320: 4.500 kg ● SPC5330: 6.400 kg ● SPC5350: 18.600 kg

Dimensions (W x H x D)	<ul style="list-style-type: none"> ● SPC5320: 264 x 357 x 81 mm ● SPC5330: 326 x 415 x 114 mm ● SPC5350: 498 x 664 x 157 mm
Housing	<ul style="list-style-type: none"> ● SPC5320: Small metal housing, (1.2 mm mild steel) ● SPC5330: Hinged metal housing, (1.2 mm mild steel) ● SPC5350: Metal housing (1.5 mm mild steel)
Housing can contain up to	<ul style="list-style-type: none"> ● SPC5320: 1 additional expander, ● SPC5330: 4 additional expanders (size 150 mm x 82 mm) ● SPC5350: 4 additional expanders (150 x 82 mm)
IP / IK Rating	30 / 06
ATS	5
ATP	15
Event Profiles	10
Event Exceptions	50
Command Profiles	8

1) Max. 400 m between devices / cable types IYSTY 2 x 2 x Ø 0.6 mm (min.), UTP cat5 (solid core) or Belden 9829.

2) More I/O expanders can be addressed instead of a keypad or door expander, but number of programmable inputs / outputs cannot exceed specified system limits.

4.3 SPC6000

Programmable areas	60
Max. number of user PINs	2500
Remote controls	Up to 100
Wireless Panic Alarm	Up to 128
Event memory	10,000 intrusion events, 10,000 access events
Number of on-board zones	<ul style="list-style-type: none"> ● SPC6320\6330 — 8 ● SPC6350 — 16
Max. number of hardwired zones	512
Max. number of wireless zones	120 (take away wired zones)
Max. number of Intrunet wireless detectors per wireless receiver (recommended)	20
EOL resistor	Dual 4k7 (default), other resistor combinations configurable
Relay Outputs	<ul style="list-style-type: none"> ● SPC6320\6330 — 1 strobe (30 VDC/1A resistive switching current) ● SPC6350 — 4 (single-pole changeover, 30VDC/ maximum 1A resistive switching current)

Electronic Outputs	<ul style="list-style-type: none"> ● SP6320\6330 — 5 outputs: <ul style="list-style-type: none"> – 2 internal/external bells – 3 programmable. Maximum 400 mA resistive switching current per output, supplied by auxiliary output. ● SPC6350 — 8 outputs. Maximum 400mA resistive switching current per output <ul style="list-style-type: none"> – 5 standard power outputs – 3 supervised outputs
Firmware	V3.x
Door capacity	Max. 64 entry doors or 32 entry/exit doors
Number of card reader	Max. 64
Radio module	Optional (SPCW110)
Verification	32 verification zones with max. 4 IP-cameras and 32 audio devices.
Video	Up to 16 pre / 16 post event images (by JPEG resolution 320 x 240, max. 1 frame / sec.)
Audio	Up to 60 sec. pre / 60 sec. post audio recording
Field bus 1)	X-BUS on RS-485 (307 kb/s)
Number of field devices 2)	Max. 128 (32 keypads, 32 door-expanders, 64 input/output expanders)
Connectable field devices	<ul style="list-style-type: none"> ● Keypads: SPCK42x, SPCK62x ● Door expanders: SPCA210, SPCP43x ● Expanders with I/O: SPCE65x, SPCE45x, SPCP33x, SPCP35x, SPCE110, SPCE120, SPCV32x
Interfaces	<ul style="list-style-type: none"> ● 2 X-BUS (2 spurs or 1 loop), ● 2 RS232 ● 1 USB (PC connection), ● 1 SPC Fast Programmer, ● SPC63xx: Additionally 1 Ethernet (RJ45)
Tamper contact	<ul style="list-style-type: none"> ● SPC6330: Front spring tamper, 2 auxiliary tamper contact inputs ● SPC6350: Front/back tamper switch
Power supply	Type A (per EN50131-1)
Mains voltage	230 V AC, + 10% / -15%, 50 Hz
Mains fuse	<ul style="list-style-type: none"> ● SPC6330 : 250 mA T (replaceable part on mains terminal block) ● SPC6350 : 800mA T (replaceable part on mains terminal block)
Power consumption	<ul style="list-style-type: none"> ● SPC6330: Max. 200 mA at 230 V AC ● SPC6350: Max. 500mA at 230 V AC
Operating current	<ul style="list-style-type: none"> ● SPC6330: Max. 200 mA at 12 V DC ● SPC6350: Max. 210 mA at 12 V DC
Quiescent current	SPC63xx Controller: Max. 170 mA at 12 V DC (195 mA with PSTN, 300 mA with GSM, 325 mA with PSTN & GSM)

Output voltage	<ul style="list-style-type: none"> ● SPC6330: 13-14 V DC in normal conditions (mains powered and fully charged battery), min. 10.5 V DC when powered by secondary device (before system shut down to battery deep discharge protection) ● SPC6350: 13-14 V DC in normal conditions (mains powered and fully charged battery), min. 10.5 V DC when powered by secondary device (before system shut down to battery deep discharge protection)
Low voltage trigger	11 V DC
Overvoltage protection	<ul style="list-style-type: none"> ● SPC6330: 15.7 V DC ● SPC6350: 15 V DC nominal
Peak to Peak ripple	Max. 5 % of output voltage
Auxiliary power (nominal)	<ul style="list-style-type: none"> ● SPC6330: Max. 750 mA at 12 V DC ● SPC6350: Max. 2200 mA at 12V DC (8 separately fused outputs, 300 mA per output)
Battery type	<ul style="list-style-type: none"> ● SPC6330: YUASA NP17-12FR (17 Ah) ● SPC6350: YUASA NP24-12 (12 V 24 Ah), Alarmcom AB1227-O (12 V 27 Ah) ● SPC6350: FIAMM FGV22703 (12V 27Ah) <p>Battery not supplied</p>
Battery charger	SPC63xx: Max. 24h to 80% of battery capacity
Battery protection	<ul style="list-style-type: none"> ● SPC6330: Current limited to 1 A (fuse protected), deep discharge protection at 10.5 V DC +/- 3 % ● SPC6350: Current limited to 2 A (protected by PTC resettable fuse), deep discharge protection at 10.5 V DC, low voltage indicator at 11 V DC
Software update	Local and remote upgrade for controller, peripherals and GSM/PTSN modems.
Calibration	No calibration checks required (calibrated at manufacturing)
Serviceable parts	<ul style="list-style-type: none"> ● SPC6330: No serviceable parts ● SPC6350: 8 glass fuses (400mA AT) for 12 V DC outputs
Operating temperature	-10 ~ +50 °C
Relative humidity	Max. 90 % (non condensing)
Colour	RAL 9003 (signal white)
Weight	<ul style="list-style-type: none"> ● SPC6330: 6.400 kg ● SPC6350: 18.600 kg
Dimensions (W x H x D)	<ul style="list-style-type: none"> ● SPC6330: 326 x 415 x 114 mm ● SPC6350: 498 x 664 x 157 mm
Housing	<ul style="list-style-type: none"> ● SPC6330: Hinged metal housing (1.2 mm mild steel) ● SPC6350: Metal housing (1.5 mm mild steel)
Housing can contain up to	<ul style="list-style-type: none"> ● SPC6330: 4 additional expanders (size 150 mm x 82 mm) ● SPC6350: 6 additional expanders (150 x 82 mm) or 1 additional controller + 4 expanders
IP / IK Rating	30 / 06
ATS	10
ATP	30
Event Profiles	20
Event Exceptions	100

Command Profiles	10
------------------	----

1) Max. 400 m between devices / cable types IYSTY 2 x 2 x Ø 0.6 mm (min.), UTP cat5 (solid core) or Belden 9829.

2) More I/O expanders can be addressed instead of a keypad or door expander, but number of programmable inputs / outputs cannot exceed specified system limits.

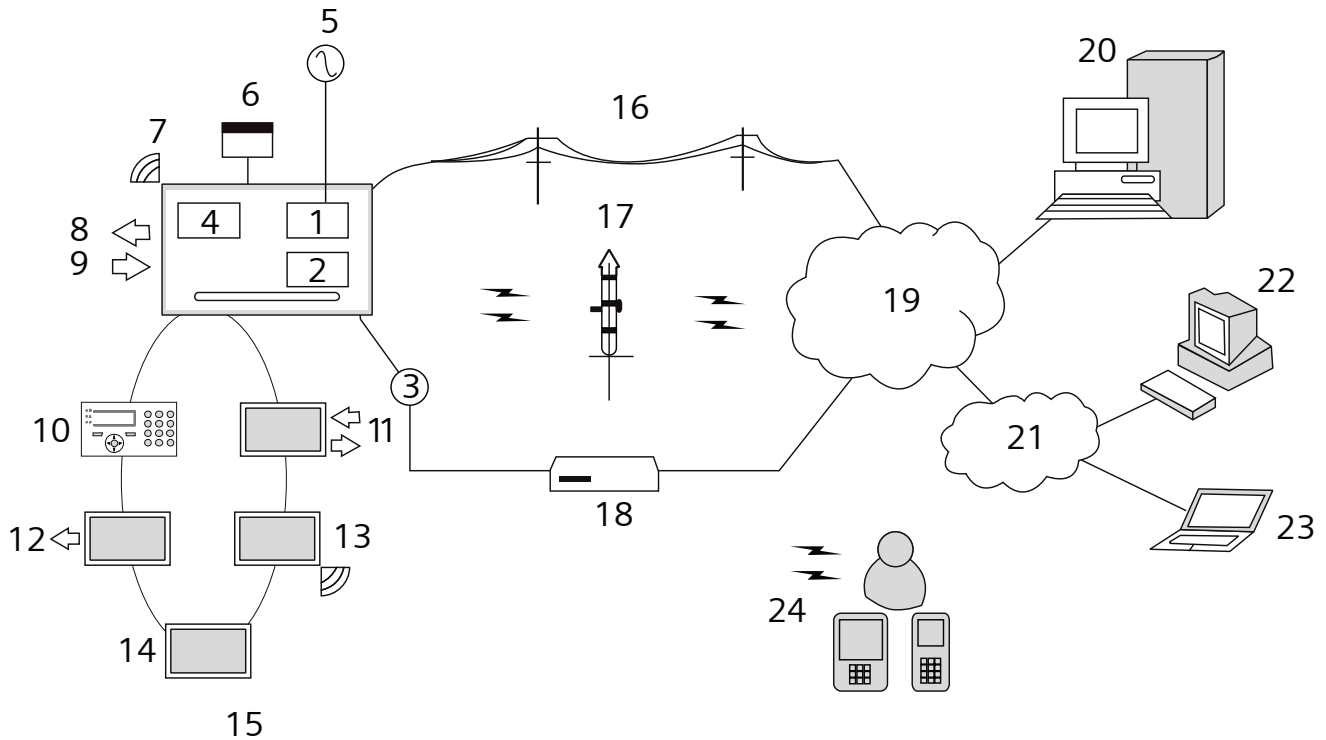
4.4 SPCP355.300

Number of on-board zones	8
EOL resistor	Dual 4K7 (default), other resistor combinations selectable
Relay Outputs	3 (single-pole changeover, 30 V DC/max. 1 A resistive switching current)
Electronic Outputs	3 supervised (each max. 400 mA resistive switching current),
Interfaces	X-BUS (in, out, branch)
Mains Voltage	230 V AC, +10 to -15 %, 50 Hz
Operating Current	Max. 245 mA at 12 V DC (all relays activated)
Quiescent Current	Max. 195 mA at 12 VDC
Output voltage	13-14 V DC in normal conditions (mains powered and fully charged battery),
Auxiliary power (nominal)	Max. 2360 mA at 12 V DC (8 separately fused outputs, max. 300mA per output)
Battery type	<ul style="list-style-type: none"> ● YUASA NP24-12 (12 V 24 Ah) ● Alarmcom AB1227-0 (12 V 27 Ah) ● FIAMM FGV22703 (12V 27Ah) Battery not supplied
Tamper contact	Front/back tamper switch
Operating temperature	0 to +40 °C
Housing	Metal housing (1.5 mm mild steel)
Colour	RAL 9003 (signal white)
Dimensions	498 x 664 x 157mm
Weight (without batteries)	18.400 kg (housing incl. cover), 11.300 kg (housing without cover)
IP / IK Rating	30 / 06

5 Introduction

The SPC series controller is a true hybrid controller with 8 on-board wired zones that communicate with intruder devices.

The flexible design of the controller allows the functional components (PSTN/GSM/RF) to be mixed and matched, improving the capability of the system. Using this approach, an installer can ensure that an efficient installation with minimal wiring is achieved.



Overview

1	PSTN	13	Wireless expander
2	GSM	14	PSU
3	Ethernet	15	Loop configuration
4	Wireless Receiver	16	PSTN network
5	AC mains	17	GSM network
6	Battery 12 V	18	Broadband router
7	RF	19	Network
8	Wired outputs (6)	20	Central
9	Wired inputs (8)	21	LAN/WLAN
10	Keypads	22	Service desk
11	IO expander	23	Remote user
12	Output Expander	24	Mobile interfaces

6 Mounting system equipment

6.1 Mounting a G2 housing

The SPC G2 housing is supplied with a metallic or plastic cover. The cover is attached to the base of the housing by 2 securing screws located on the top and bottom of the front cover.

To open the housing, remove both screws with the appropriate screwdriver and lift the cover directly from the base.

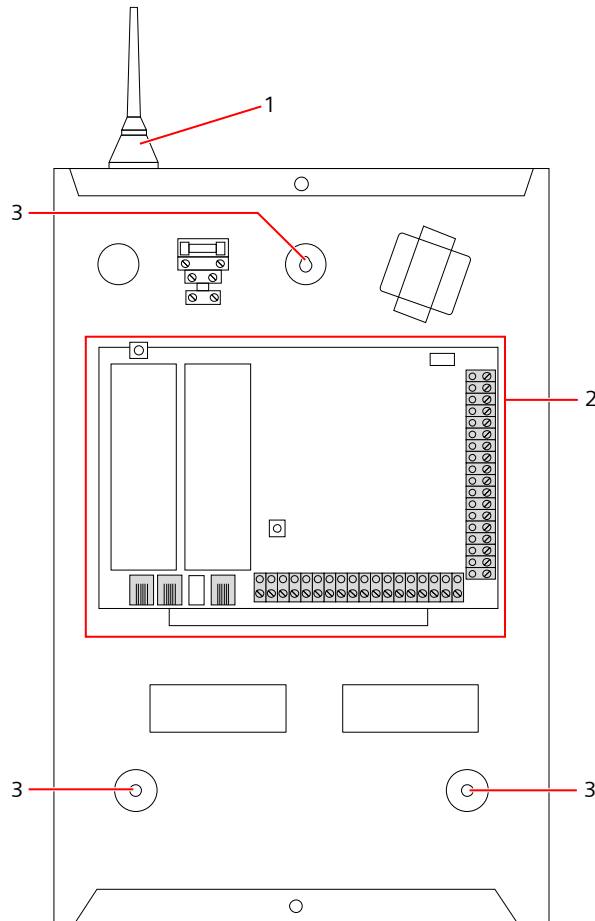
The G2 housing contains the controller PCB (**P**rinted **C**ircuit **B**oard) mounted on 4 support pillars. An optional input/output module can be mounted directly beneath the controller PCB. A battery with capacity of 7 Ah max. can be accommodated below the controller.

An optional external antenna must be fitted to housings with metallic lid if the wireless functionality is required. If an antenna is fitted to the unit, it must be enabled in the firmware.

The SPC G2 housing provides 3 screw holes for wall mounting the unit.

To wall mount the housing, remove the cover and locate the initial fixing screw hole at the top of the cabinet. Mark the position of this screw hole on the desired location on the wall and drill the initial screw hole. Screw the unit to the wall and mark the position of the bottom 2 screw hole positions with the unit vertically aligned.

Screws with a 4-5 mm shank, a minimum head diameter of 8 mm and a minimum length of 40 mm are recommended for mounting the housing. Additional expansion plugs or fixings may be required depending on the construction of the wall.



Standard housing

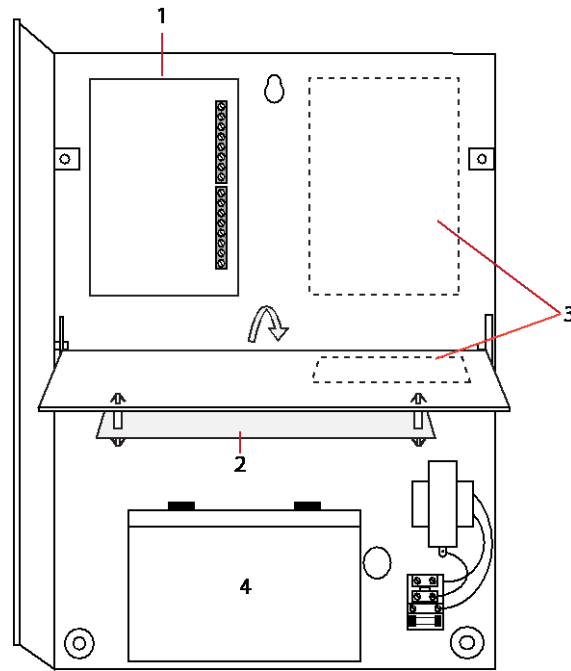
1	Wireless antenna
2	SPC controller
3	Wall mounting screw holes

6.2 Mounting a G3 housing

The SPC G3 housing is supplied with a metallic front cover. The cover is attached to the base of the housing by hinges and secured with one screw on the right hand side of the front cover.

To open the housing, remove the screws with the appropriate screwdriver and open the front cover.

The G3 housing contains the controller PCB (Printed Circuit Board) mounted on a hinged mounting bracket. Expanders and PSUs can be mounted on the underside of the hinged mounting bracket and also on the back wall of the housing underneath the mounting bracket.

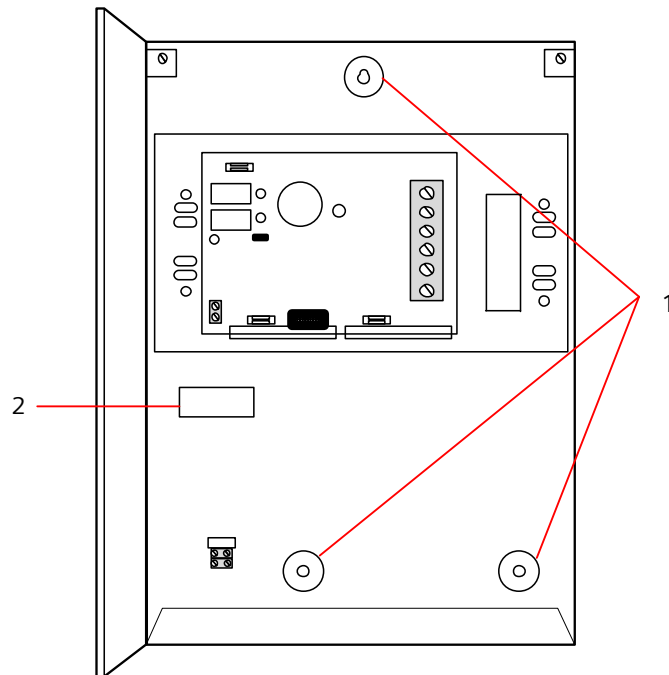


- 1 Expanders/PSU
- 2 Controller
- 3 Expanders/PSU
- 4 Battery

An optional external antenna must be fitted to housings with metallic lid if the wireless functionality is required. If an antenna is fitted to the unit, it must be enabled in the firmware.

The SPC G3 housing provides 3 screw holes for wall mounting the unit (see item 1 below).

Screws with a 4-5 mm shank, a minimum head diameter of 8 mm and a minimum length of 40 mm are recommended for mounting the housing. Additional expansion plugs or fixings may be required depending on the construction of the wall.



To wall mount the housing:

1. Open the cover and locate the initial fixing screw hole at the top of the cabinet.
2. Mark the position of this screw hole on the desired location on the wall and drill the initial screw hole.
3. Screw the unit to the wall and mark the position of the bottom 2 screw hole positions with the unit vertically aligned.

Back Tamper Requirements

A back tamper switch may be required by your local approval.

The back tamper switch is delivered with SPC panels in G3 housings or is available as an optional extra with a mounting kit (SPCY130). EN50131 G3 panels (SPCxx3x.x20) are supplied with a back tamper kit as standard.

6.2.1 Mounting a Back Tamper Kit

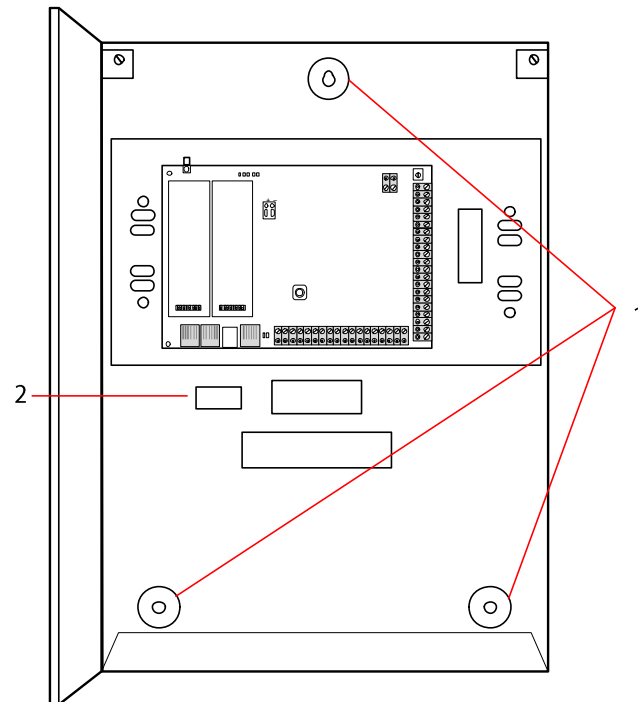
The SPC back tamper kit provides SPC control panels and power supplies with the option of having back tamper as well as front tamper.

The back tamper kit comprises the following parts:

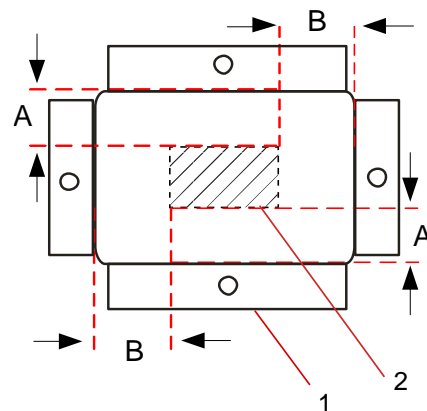
- Tamper switch
- Leads for connecting the back tamper switch to the controller
- Wall fixing plate

Mounting the Wall Fixing Plate

1. Mount the SPC in the appropriate position on the wall using all three fixings (see item 1 below).



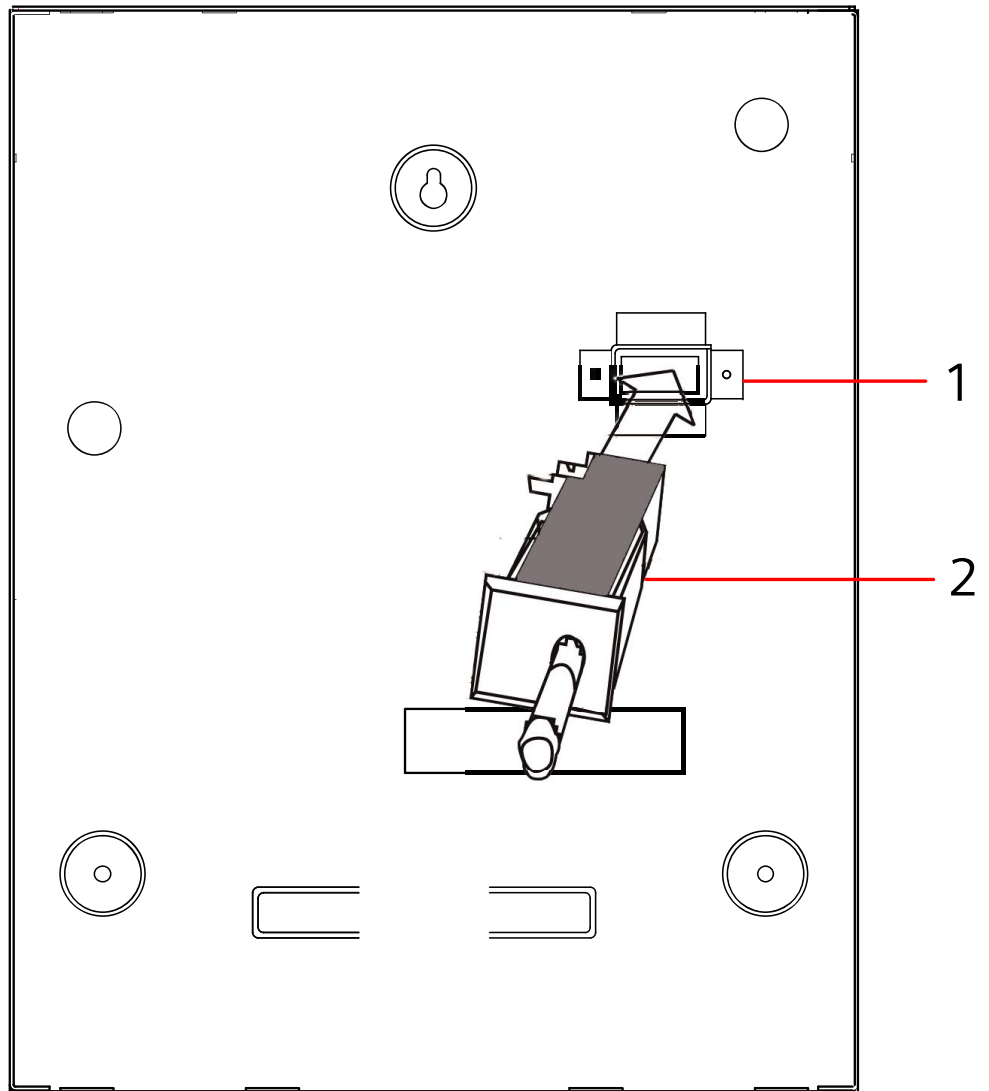
2. Draw a line around the inside of the back tamper cut out (See item 2 above) to provide a guide for the wall plate on the fixing wall. Remove the enclosure from the wall.
3. Place the wall plate (See item 1 below) on the wall centering it precisely around the rectangle previously drawn (See item 2 below).



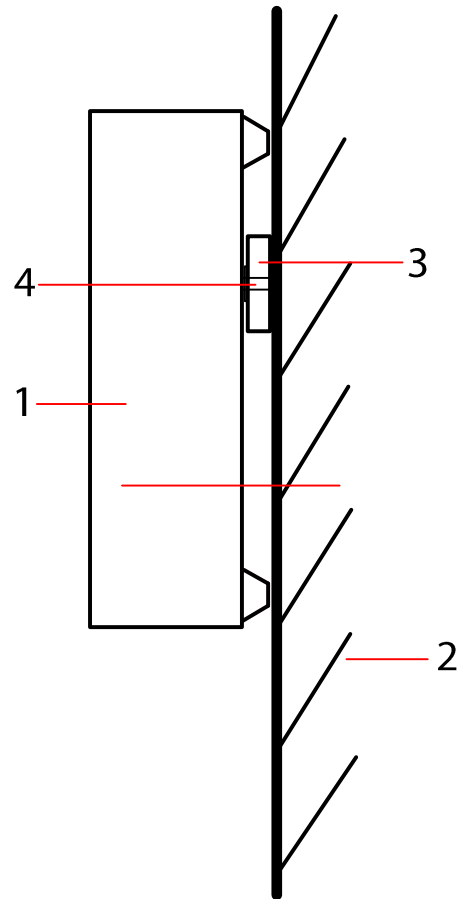
4. Ensure all four flanges on the wall plate are flush with the wall.
5. Mark the four fixings on the wall plate.
6. Drill and use suitable screws (max. 4 mm) for the wall substrate.
7. Fit the wall plate to the wall.

Fitting the Back Tamper Switch

1. Insert the tamper switch (See item 2 below) into the back of the enclosure so that the plunger faces outwards (See item 1 below).



2. Fit the enclosure back onto the wall using the three fixings previously removed (See item 2 below). Visually check to ensure there is a flush finish between the wall plate and the enclosure metalwork.



1 Enclosure

2 Wall

3 Wall Fixing Plate

4 Tamper Switch

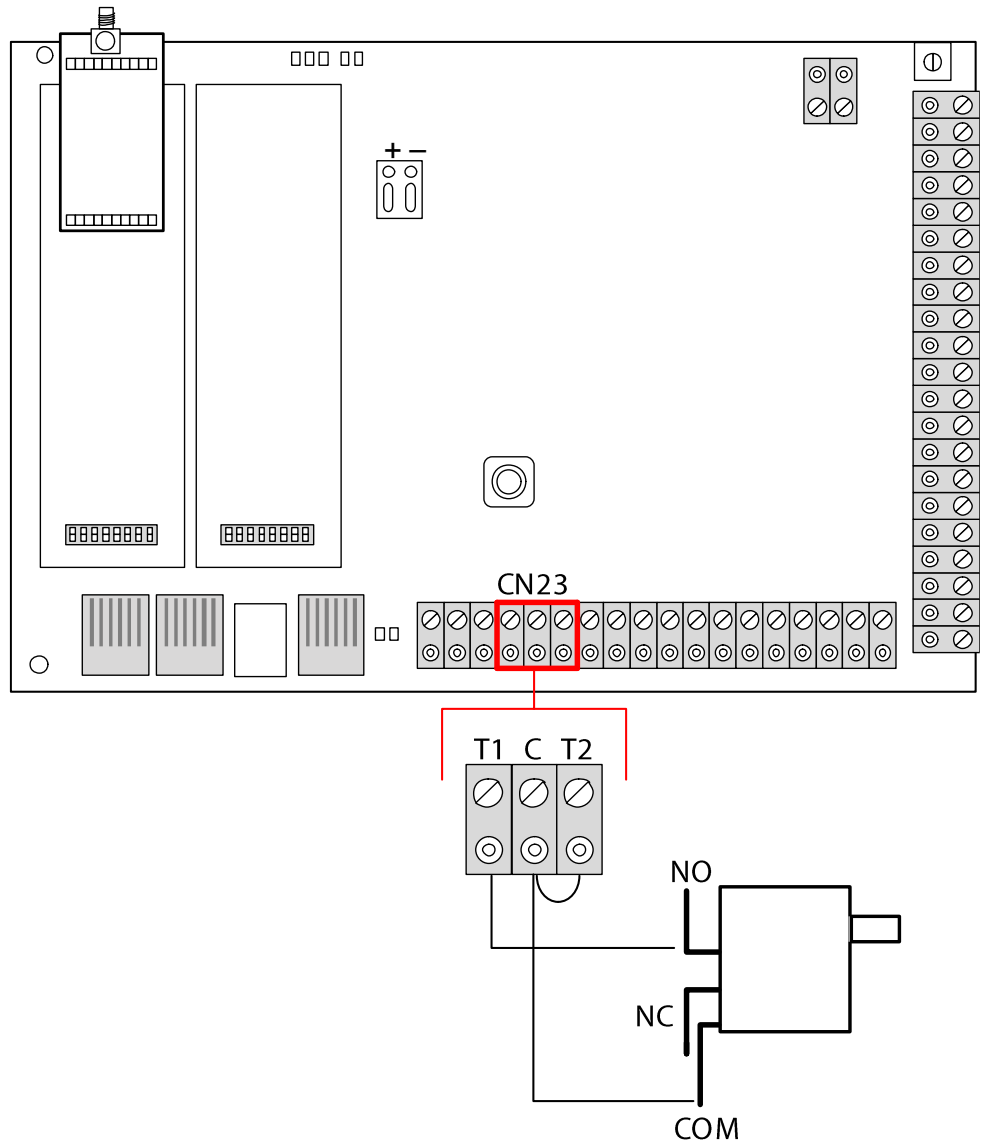
**⚠ WARNING**

If the wall fixing plate is not accurately aligned then the enclosure will not sit properly on its fixings.

Wiring the Back Tamper Switch to the Control Panel

All control panels have spare inputs configured as tamper inputs that are designed for wiring the tamper switch and do not require any programming.

This tamper switch will be referred to as 'Aux Tamper 1' by the system.



1. Connect NO on the tamper switch to T1 on the controller.
2. Connect COM on the tamper switch to C on the controller. Ensure the T2 jumper is not removed.
3. When the tamper switch is wired, the controller can be commissioned in the normal manner.

6.2.2 Battery installation for EN50131 compliance

For EN50131 compliance the battery needs to be retained within the housing to stop movement. This is achieved by bending out the flaps in the rear of the Hinged Enclosure so that the battery is retained.

If a 7 Ah battery is used then the battery is biased to the left of the cabinet and bottom flap is bent to meet the battery.

If a 17 Ah battery is used then the battery is biased to the right of the cabinet and middle flap is bent to meet the battery.



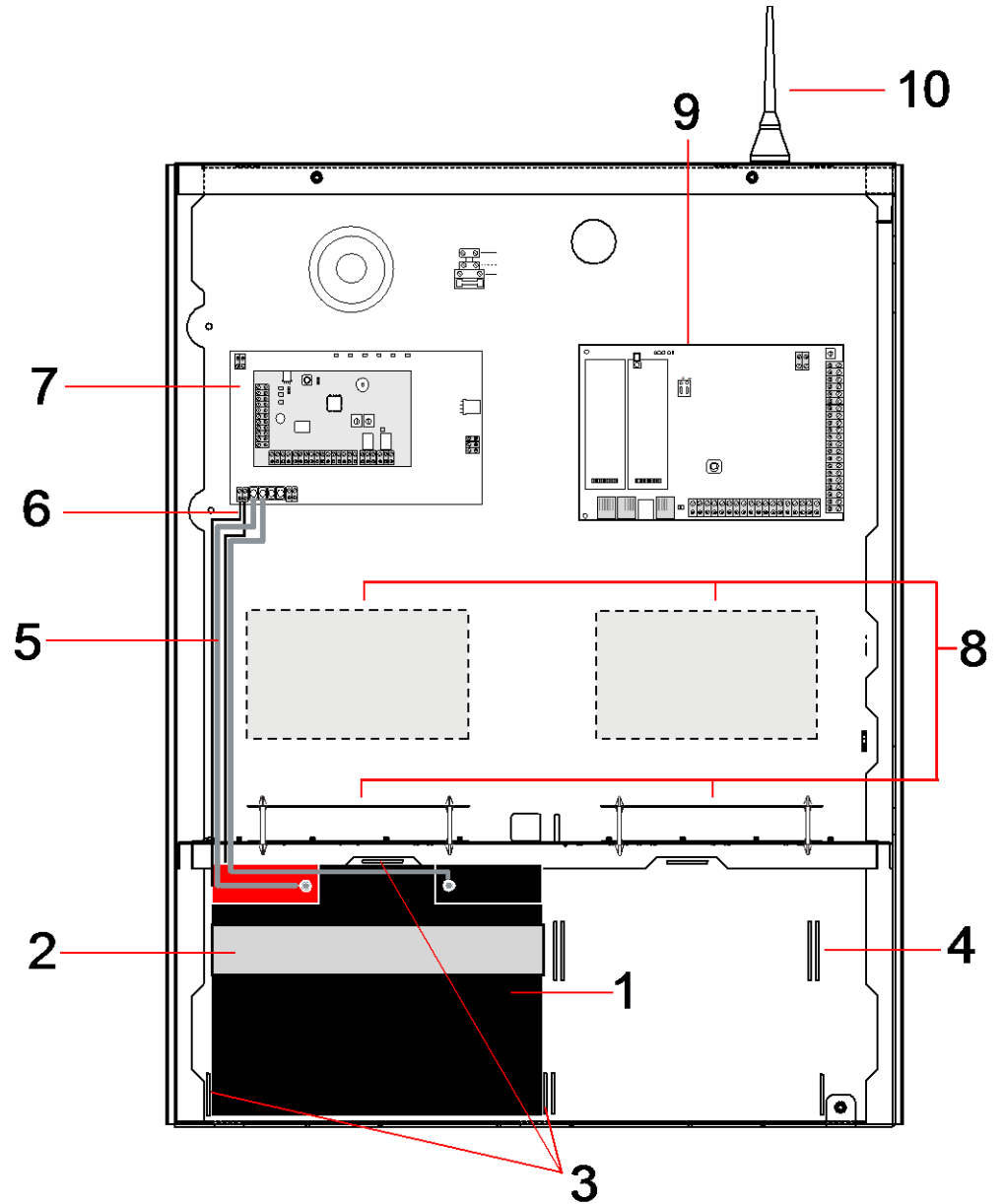
The battery flaps should be bent carefully as not to damage the battery. If any signs of a damaged battery exist or any leakage of the electrolyte then the battery should be discarded as per the current regulations and a new battery fitted.

6.3 Mounting a G5 housing

The SPC G5 housing comprises of a metallic base and front cover. The cover is attached to the base of the housing by 4 securing screws located on the top and bottom of the front cover.

To open the housing, remove all the screws with the appropriate screwdriver and lift the cover directly from the base.

The G5 housing contains the controller PCB (**P**rinted **C**ircuit **B**oard) and the SPCP355.300 Smart PSU, both mounted on 4 support pillars. An 8 In/2 Output Expander is mounted on top of the PSU. Four extra pillars are included to give you the option to mount the 8 In/2 Output Expander below the PSU board in the G5 cabinet. Additional expanders can be installed in the housing as shown.

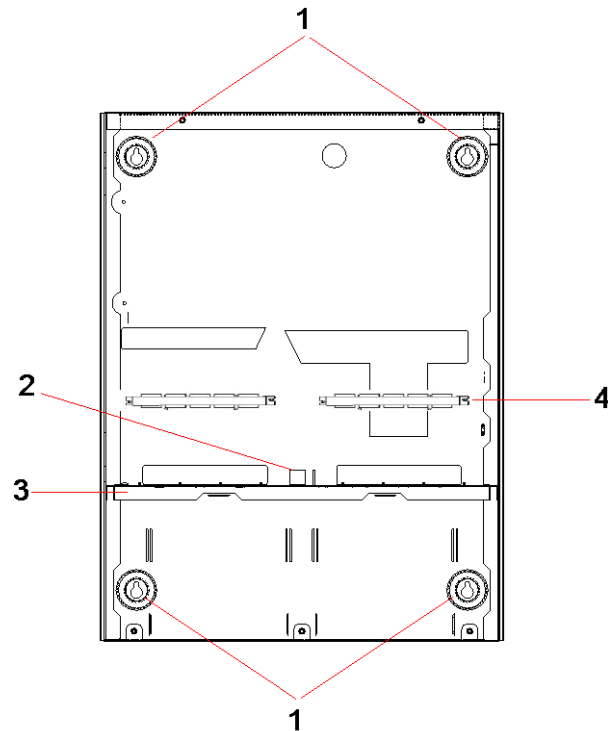


Number	Description	Number	Description
1	Battery	6	Battery temperature leads
2	Battery strap	7	PSU
3	Fixing tabs	8	Optional expander positions
4	Strap holes	9	Controller
5	Battery leads	10	Antenna

Two batteries, with a maximum capacity of 27 Ah, can be accommodated in the battery compartment at the bottom of the housing.

An optional external antenna must be fitted to a metallic housing if wireless functionality is required. Knockout holes are available in three positions on the top of the housing where the antenna can be installed. If an antenna is fitted to the unit, it must be enabled in the firmware.

The SPC G5 housing provides 4 screw holes for wall mounting the unit.



Number	Description
1	Corner fixings
2	Tamper cutout
3	Shelf separating battery compartment
4	Telecom socket cutout

6.3.1 Tamper protection

The tamper switch and back tamper bracket are fitted to the housing. The switch is used on its own for front tamper purposes only or used with the back tamper bracket for both front and back tamper protection. Either back or front tamper protection is required depending on local approval.

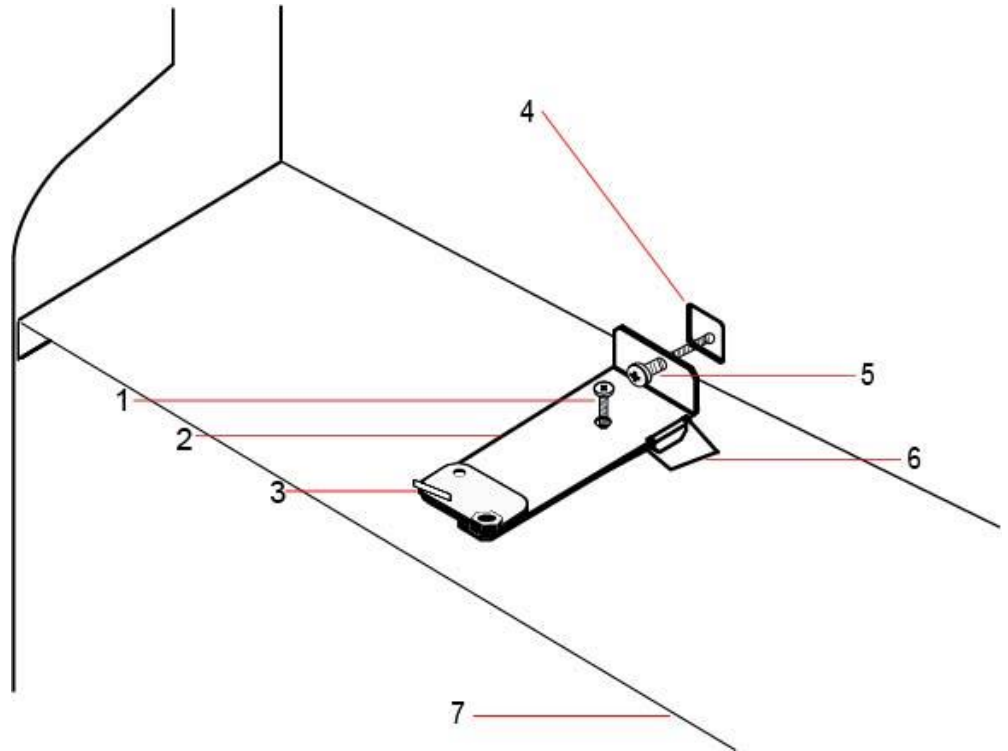
The tamper bracket is held firmly in place with a securing screw. Remember to remove this screw if commissioning the system for back tamper protection. Do not remove this screw if using front tamper only.

6.3.2 Mounting the housing with tamper protection

To mount the housing:

1. Using the supplied mounting template, mark the 4 drill positions for fixing the housing to the wall.
2. Drill and install suitable screws (see enclosed template) into the wall. Leave the screws protruding 1.5cm from the wall.
3. The G5 housing is pre-configured for front tamper only. To configure the housing for both front and back tamper, remove the front tamper securing screw (item 1).
 - ⇒ The tamper bracket swings to the far right of the orientation slot (item 6).

4. Mount the G5 housing in the appropriate position on the wall and tighten the 4 mounting screws. Ensure that the housing is flush with the wall surface.
5. Move the tamper bracket to the far left of the orientation slot and tighten the back tamper screw (item 5) to the wall. The tamper bracket should be perpendicular to the back wall of the housing.
6. Install the lid on the housing to test the tamper switch connection. Lift the lid by approximately 1 mm to activate the tamper switch.



Number	Description	Number	Description
1	Front tamper securing screw	5	Back tamper screw
2	Tamper bracket	6	Orientation slot
3	Tamper switch	7	Shelf separating battery compartment
4	Back tamper cutout		

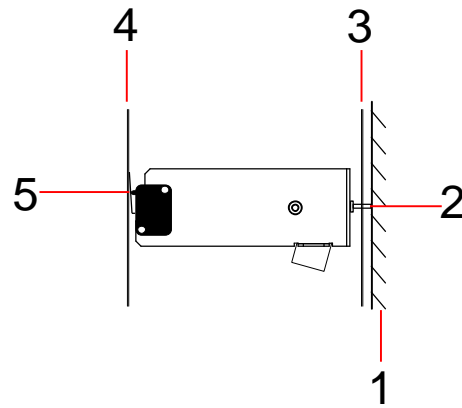


⚠ WARNING

If the back tamper screw is not secure against the wall, then tamper protection is compromised. If the housing is removed from the wall or displaced, the back tamper contact needs to be tested again for proper functionality and re-adjusted if required.

6.3.2.1 Tamper operation

Tamper switch - normal



1 Wall

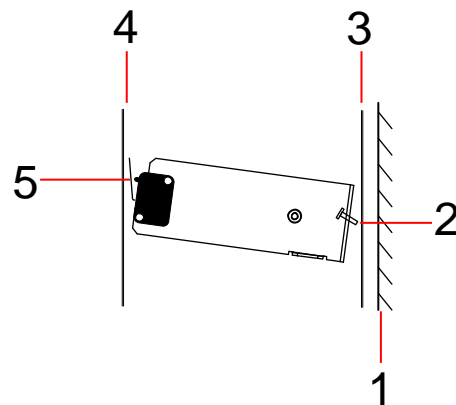
2 Back tamper screw

3 Back wall of housing

4 Housing lid

5 Tamper switch contact closed

Tamper switch – displaced



1 Wall

2 Back tamper screw

3 Back wall of housing

4 Housing lid

5 Tamper switch contact open

If the housing is removed from the wall or displaced, the tamper bracket screw is no longer secure against the wall, causing the bracket to pivot. This in turn causes the tamper switch to swivel away from the lid and opens the switch contact.

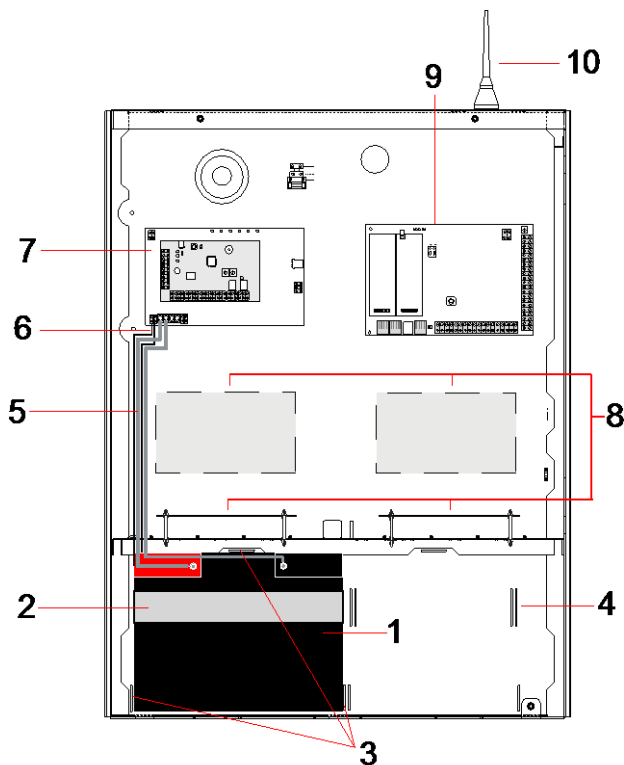


⚠ WARNING

If the tamper bracket screw is not secure against the wall, then tamper protection is compromised.

6.3.3 Installing the batteries

!	NOTICE
	If using two batteries in the G5 housing, it is recommended that both batteries should be the same Ah rating.



- | | |
|-----------------------|-------------------------------|
| 1 Battery | 6 Battery temperature lead |
| 2 Fixing strap | 7 PSU |
| 3 Battery fixing tabs | 8 Optional expander positions |
| 4 Strap holes | 9 Controller |
| 5 Battery leads | 10 Antenna |

To install the batteries:

1. Place the batteries into the battery compartment.
2. Press the metal tabs at the top and either side of the batteries in towards the batteries.
3. Secure each battery to the housing using a battery strap. Ensure that the strap is thread through the battery strap holes at the back of the battery compartment and around the battery, with the two ends of the strap at the front of the battery.
4. Fasten the two ends of the strap firmly using the Velcro strip. Ensure that the strap is tight around the battery.

5. Connect one end of the battery leads to the battery + and - terminals and the other ends to the corresponding + and - inputs of the PSU.

**⚠ CAUTION**

When installing the battery, always connect the positive (+) lead to the battery first before connecting the negative (-) lead. When removing the battery, always remove the negative (-) lead first before removing the positive (+)

6. Connect the loose ends of the attached temperature monitoring leads to the battery temperature monitoring inputs on the PSU.

6.4 Mounting a keypad

Please refer to corresponding installation instruction.

6.5 Mounting an expander

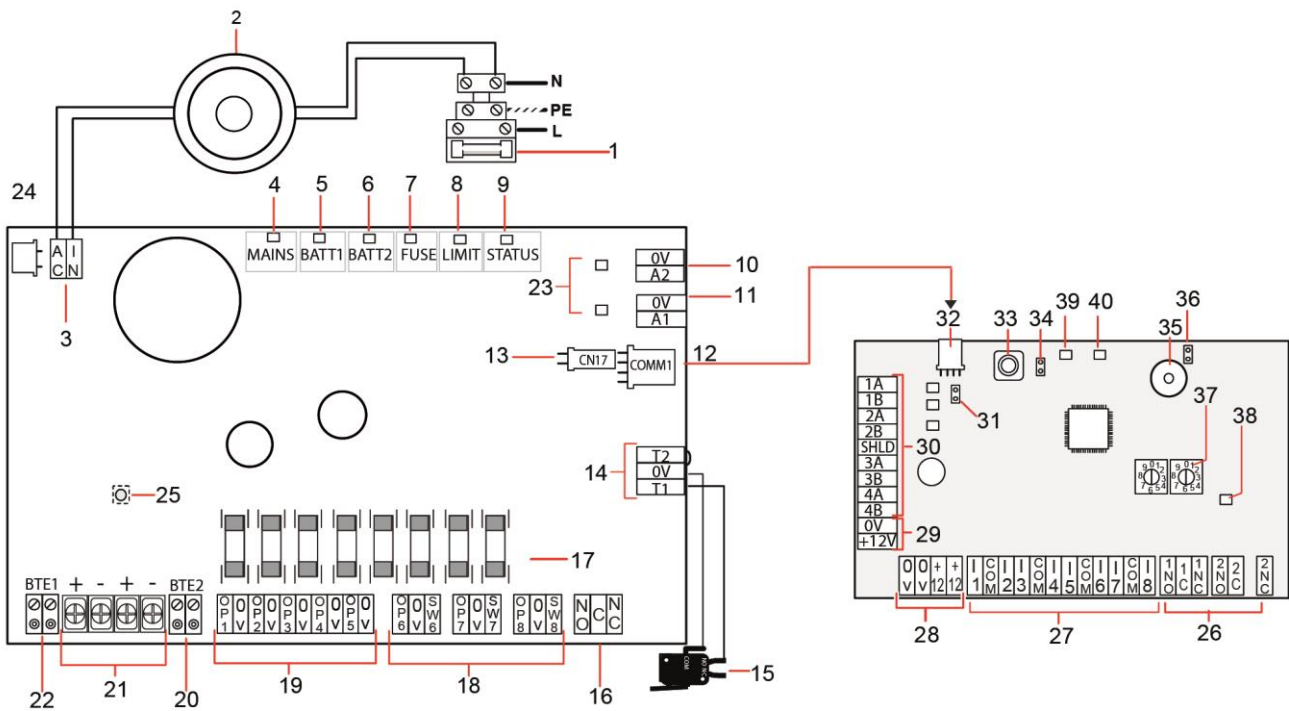
Please refer to corresponding installation instruction.

7 Smart PSU

This section describes the components and wiring of the Smart PSU.

7.1 SPCP355.300 Smart PSU


The SPCP355.300 Smart PSU is a power supply combined with an 8-input/2-output expander, contained in a G5 housing. The PSU is backed up by either 2x24Ah, or 2x27Ah batteries, and provides eight power and four logical outputs. The expander monitors the PSU for overcurrent, fuse failures, AC voltage, communications, and battery output. The expander is powered by, and receives data from, the PSU via a connector cable. It also interfaces with the SPC controller over the SPX X-BUS.



Number	Description
SPCP355.300 Smart PSU	
1	Mains input and fuse block
2	Input transformer
3	AC IN — AC power input
4	MAINS — Mains power LED
5	BATT1 — Battery 1 charge state LED
6	BATT2 — Battery 2 charge state LED
7	FUSE — Fuse fail LED
8	LIMIT — Current limit LED
9	STATUS — Status LED
10	A2 — 14.5V power output. <ul style="list-style-type: none"> ● Not backed up by battery ● Protected by PTC resettable fuse, rated at 300mA (Item 23 in image above)

Number	Description
11	A1 — Connects to the power input (+/-) on the SPC5350/6350.
12	COMM1 — Expander 4-pin interface. Connects to item 32, power and data connection, in image above, with a straight-through cable.
13	Clock Reference — Connects to Clock Reference on SPC5350/6350.
14	T1, T2 — Tamper switch inputs. Connect these to the Front/Back tamper switch. See Mounting the housing with tamper protection [→ 50].
15	Front back tamper switch. See Mounting the housing with tamper protection [→ 50].
16	NO/NC — Configurable NO/NC logical relay output. See Wiring the Outputs [→ 62] for more information.
17	Glass fuses — 400 mA T fuses for outputs 1-8.
18	OP 6 – 8 and SW 6 – 8 — Combined power outputs (OP) and logical outputs (SW). Standard 12V DC power outputs combined with configurable, open-drain, logical outputs (4K7 EoL supervised/unsupervised).
19	OP 1 – 5 — Standard 12V DC power outputs. See Warning note below table for more information.
20	BTE2 — Battery 2 temperature monitoring input.
21	BATT1 and BATT2 — Battery 1 and 2 connectors.
22	BTE1 — Battery 1 temperature monitoring input.
23	PTC fuses — Fuses rated at 300mA. Protecting the A1 and A2 outputs. For more information see System Recovery [→ 65].
24	PTC fuse — Fuse rated at 5A. Protects the AC power input (item 3 in image above). For more information see System Recovery [→ 65].
25	PSU Kickstart Switch — For more information see System Recovery [→ 65].
Expander	
26	NO/NC — Logical relay outputs. The expander provides two configurable NO/NC logical relay outputs. For more information, see Wiring the Inputs [→ 61]
27	I 1 – 8 — Inputs. The expander has 8 on-board inputs which can be configured as intruder alarm zones on the SPC system. For more information, see Wiring the Inputs [→ 61]
28	Auxiliary power supply 12V — Do not use. Expander is powered through COMM1 on the SPCP355.300 Smart PSU.
29	X-BUS Input power — Do not use. Expander is powered through COMM1 on the SPCP355.300 Smart PSU.
30	X-BUS Interface — The communications bus connects expanders on the SPC system.
31	Termination Jumper — This jumper is always fitted, by default. For more information, see Wiring the X-BUS Interface [→ 60].
32	PSU 4-pin interface — Connects to COMM1 on the SPCP355.300 Smart PSU (item 12 in image above), power and data connector, with a straight-through cable.
33	Front tamper switch — Not used. The Front/Back tamper connected to T1 and T2 of the SPCP355.300 Smart PSU is the only tamper required by this installation.

Number	Description
34	JP1 — Front tamper bypass must be fitted.
35	Buzzer — Activated to locate the expander. See the X-BUS menu LOCATE [→ 120] for more information.
36	JP6 — Back tamper bypass. Must be fitted.
37	Manual addressing switches — Enable manual setting of the ID of the expander.
38	X-BUS Status LED — Indicates the X-BUS status, when the system is in Full Engineer mode, as follows: <ul style="list-style-type: none"> ● Slow flash (every 1.5 seconds) — X-BUS communications status is OK. ● Quick flash (every 0.2 seconds) — Indicates one of the following: <ul style="list-style-type: none"> – Indicates the last-in-line expander for spur configurations. – Indicates a communications problem between two expanders. If two adjacent expanders are flashing quickly, the problem exists between those two expanders.
39	LED — Not used.
40	PSU Status LED.

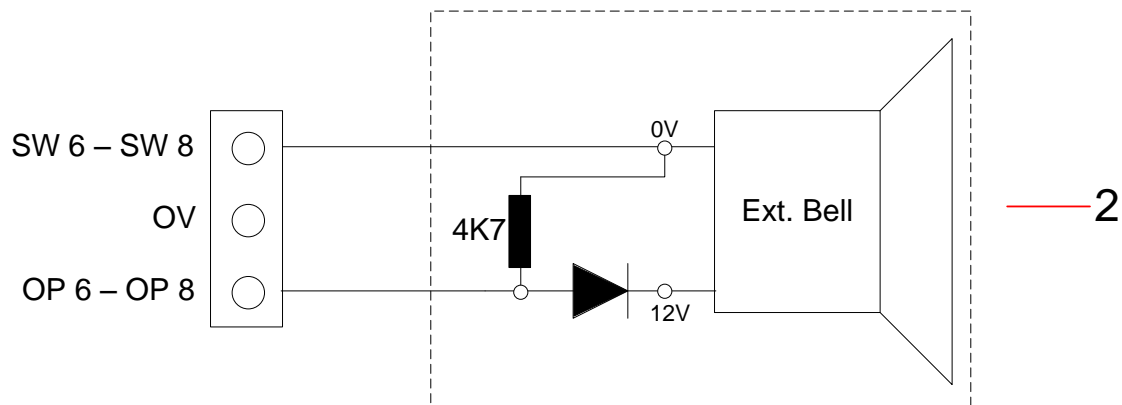
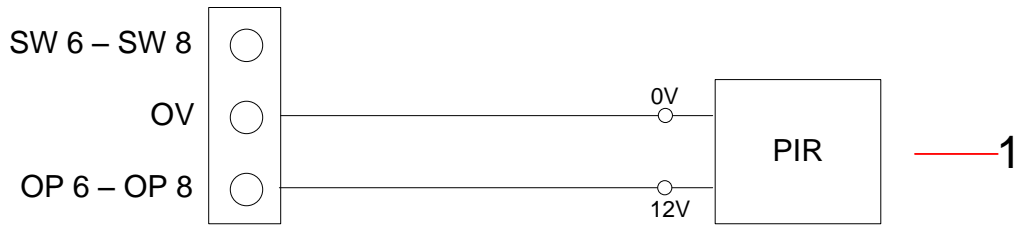
	⚠ WARNING
	<p>The combined maximum load current drawn from all 12V DC outputs (OP 1 - 8) plus COMM1, should not exceed 2.4A. Each individual output, and output A2, should not exceed 300mA. If the device current requires more than 300mA, it is recommended to parallel the outputs.</p>

Adding extra expanders

If adding extra expanders to the G5 enclosure, you must ensure the front and back tampers are deactivated by fitting the appropriate jumpers. In a G5 enclosure, the front and back tamper is handled by the enclosure itself and the SPCP355.300 Smart PSU.

7.1.1 Supervised Outputs

The SPCP355.300 Smart PSU supports three, open-drain, logical outputs, which can be supervised for tamper detection. Output tamper detection is enabled by configuration. Output tamper detection is enabled by connecting a 4K7 EoL resistor in parallel with the load device, such as an external bell. A power diode (1N4001 for example, or similar) is also required, if not already present in the external device.

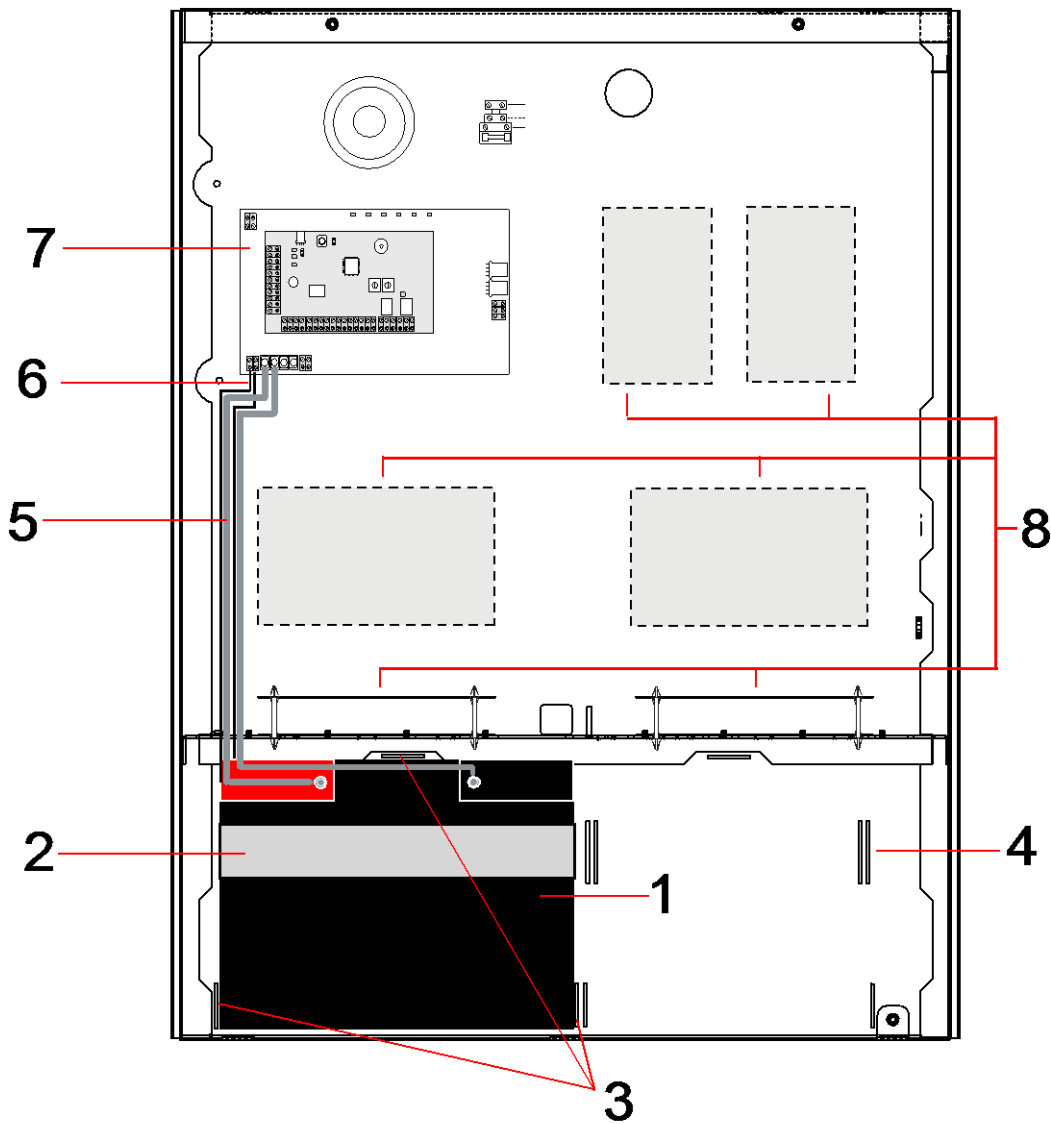


Number	Description
1	Standard 12V Power output
2	Configurable, supervised, 12V DC logical switched output.

7.1.2 Batteries

7.1.2.1 Installing Batteries

This section describes the battery installation for the SPCP355.300 Smart PSU and G5 Enclosure.



Number	Description
1	Battery
2	Battery strap
3	Fixing holes
4	Strap holes
5	Battery leads
6	Battery temperature leads
7	PSU Expander
8	Mounting positions for additional expanders.



It is recommended that two batteries are used. These batteries must be of the same type and capacity.

1. Install the batteries in the battery compartment.

2. Secure each battery using the battery straps provided, ensuring the strap is threaded through the battery strap holes at the back of the battery and around the battery.
3. Secure the two ends of the battery strap at the front of the battery, ensuring the battery strap is firmly tightened.
4. Connect the leads from the SPCP355.300 Smart PSU to the batteries in the following order:
 - Connect the positive (red) wire first.
 - Connect the negative (black) wire second.



⚠ DANGER

When removing the battery leads, always disconnect the negative (black) lead before disconnecting the positive (red) lead.

7.1.2.2 Testing Battery Voltage

The SPCP355.300 Smart PSU performs a load test on each battery by placing a load resistor across the battery terminals and measuring the resultant voltage. This battery test is performed every five seconds.

7.1.2.3 Deep Discharge Protection

If mains power to the SPCP355.300 Smart PSU fails for a prolonged period, each battery supplies power to the PSU 12V DC power outputs for a finite time. The batteries eventually discharge. To prevent a battery discharging beyond recovery, the SPCP355.300 Smart PSU disconnects the battery if the measured voltage drops below 10.5V DC. The battery can then be recharged after the mains power is restored.

7.1.2.4 Battery Stand-By Times

See Calculating the battery power requirements [→ 334] for the battery stand-by information.

7.1.3 Wiring the X-BUS Interface

The X-BUS interface connects expanders and keypads to the SPC controller. The X-BUS can be wired in a number of different configurations, depending on the installation requirements.

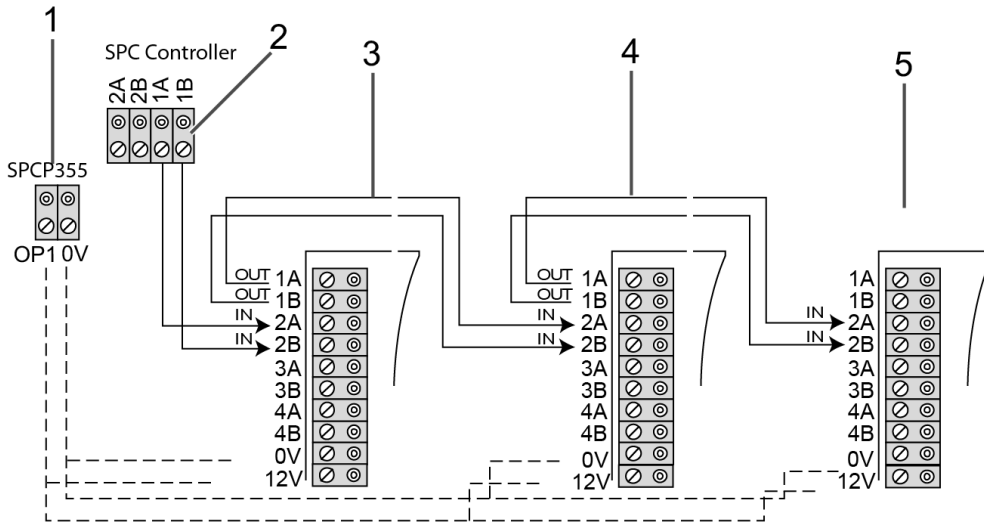
The following table lists the cable types and distances recommended:



Maximum cable length = (number of expanders and keypads in the system) x (maximum cable distance for each cable type)

Cable Type	Distance
CQR Standard Alarm Cable	200m
UTP Cat-5 Solid core	400m
Belden 9829	400m
IYSTY 2x2x0.6(min)	400m

The following diagram shows an example of wiring the X-BUS:



Number	Description
1	SPCP355.300 Smart PSU outputs
2	SPC Controller
3	SPCP355.300 Input/Output expander
4	Next expander
5	Next expander

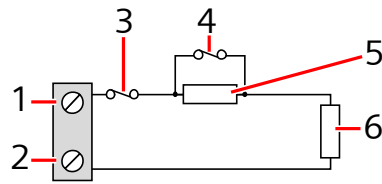
7.1.3.1 Wiring the Inputs

The expander has 8 on-board zone inputs which can be configured as one of the following:

- No End of Line
- Single End of Line
- Dual End of Line
- Anti-Masking PIR

Default Configuration

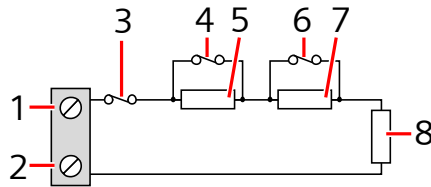
The following diagram shows the default configuration, Double EOL 4K7:



Number	Description
1	Input 1
2	COM
3	Tamper
4	Alarm
5	4K7
6	EOL 4K7

Anti-Masking PIR

The following diagram shows the Anti-Masking PIR configuration:



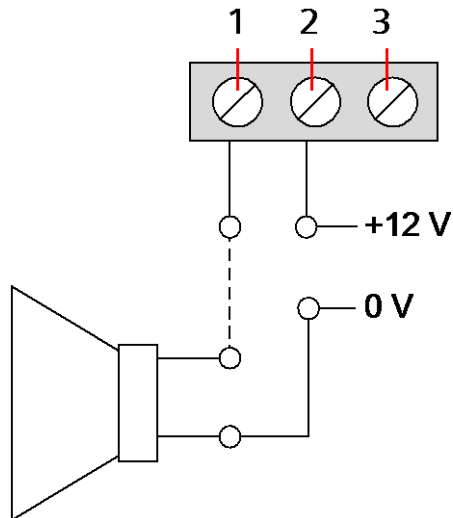
Number	Description
1	Input 2
2	COM
3	Tamper
4	Alarm
5	4K7
6	Detector Fault
7	2K2
8	EOL 4K7

7.1.3.2 Wiring the Outputs

The expander and PSU relay logical outputs can be assigned to any of the SPC system outputs. The relay outputs can switch a rated voltage of 30V DC at 1A (non-inductive load).

When the relay is activated, the Common terminal connection (COM) is switched from the Normally Closed (NC) to the Normally open (NO) terminal.

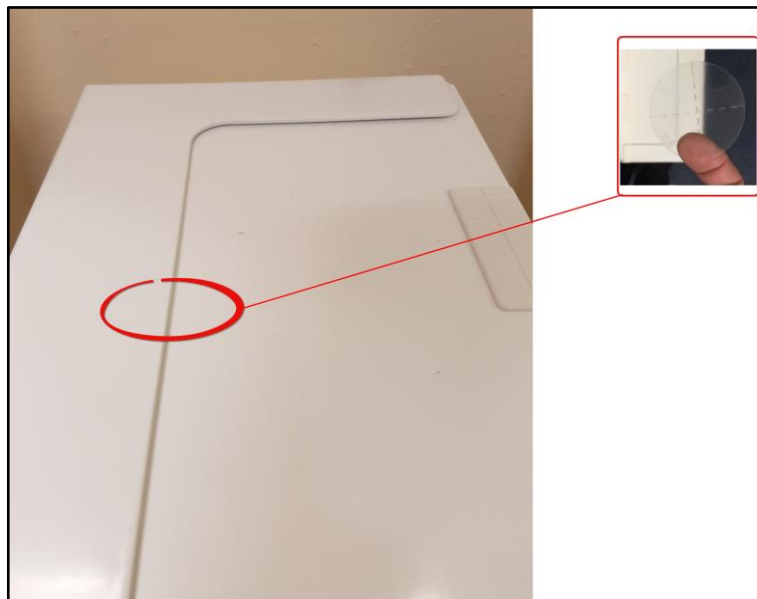
The following diagram shows the wiring of an active, high output:



Number	Description
1	Normally Open terminal
2	Common terminal connection (COM)
3	Normally Closed terminal (NC)

7.1.4 Compliance with NF and A2P approvals



Address of Certifying Body	
<p>CNPP Cert Pôle Européen de Sécurité - Vernon Route de la Chapelle Réanville CD 64 - CS 22265 F-27950 SAINT MARCEL www.cnpp.com</p>	<p>AFNOR Certification 11 rue François de Pressensé 93571 Saint Denis La Plaine Cedex www.marque-nf.com</p>





To comply with NF & A2P installation regulations, this enclosure must be sealed by affixing the accompanying Tamper Label after installation.

SPC products listed have been tested according to NF324 - H58, with reference to RTC50131-6 and RTC50131-3 and current EN certifications, see Compliance with EN50131 Approvals [→ 19].

Product Type	Configuration	Standard	Logo
SPC6350.320 + SPCP355.300 (Cert. XXXXXXXXXXXX)	60h, unmonitored	NF Grade 3, Class 1	
SPC5350.320 + SPCP355.300 (Cert. XXXXXXXXXXXX)	60h, unmonitored		
SPC6330.320 + SPCP333.300 (Cert. 1232200003)	60h, unmonitored	NF Grade 3, Class 1	
SPC5330.320 + SPCP333.300 (Cert. 1232200003)	60h, unmonitored		

7.1.5 PSU LED Status

The following table lists the Smart PSU LED status information:

LED	MAINS	BATT 1 & 2	FUSE	LIMIT	STATUS
COLOUR	Green	Green	Red	Red	Green
Condition					
Normal	On	On	Off	Off	On
Mains OK, battery charging	On	Flash			On
Mains Fail, Battery OK	Off	On			On
Mains OK, battery faulty or not present	On	Off			On
Mains OK, battery faulty, not present, or in deep discharge protection mode	All LEDs Off.				
Fuse Fail			On		On
Total Load Current exceeded				On	On
PSU switcher failure	Off				Flash

7.1.6 System Recovery

Mains and Battery Failure

In the event of both mains and battery power failure, the PSU kickstart switch (item 25 in SPCP355.300 Smart PSU [→ 55]) enables the system to be restarted if only battery power is reinstated. To kickstart the system, do the following:

- ▷ Mains power has failed
 - ▷ Battery power has failed
 - ▷ New batteries are available
1. Attach the battery leads.
 2. Press and hold the PSU Kickstart button.
 - ⇒ All LEDs flash.
 3. Hold the PSU Kickstart button until the LEDs stop flashing.
 4. Release the PSU Kickstart button.

PTC Fuse Reset

In the event of one of the PTC fuses resetting, you must manually disconnect then reconnect the mains and battery connections.

8 Controller hardware

This section describes the controller hardware.

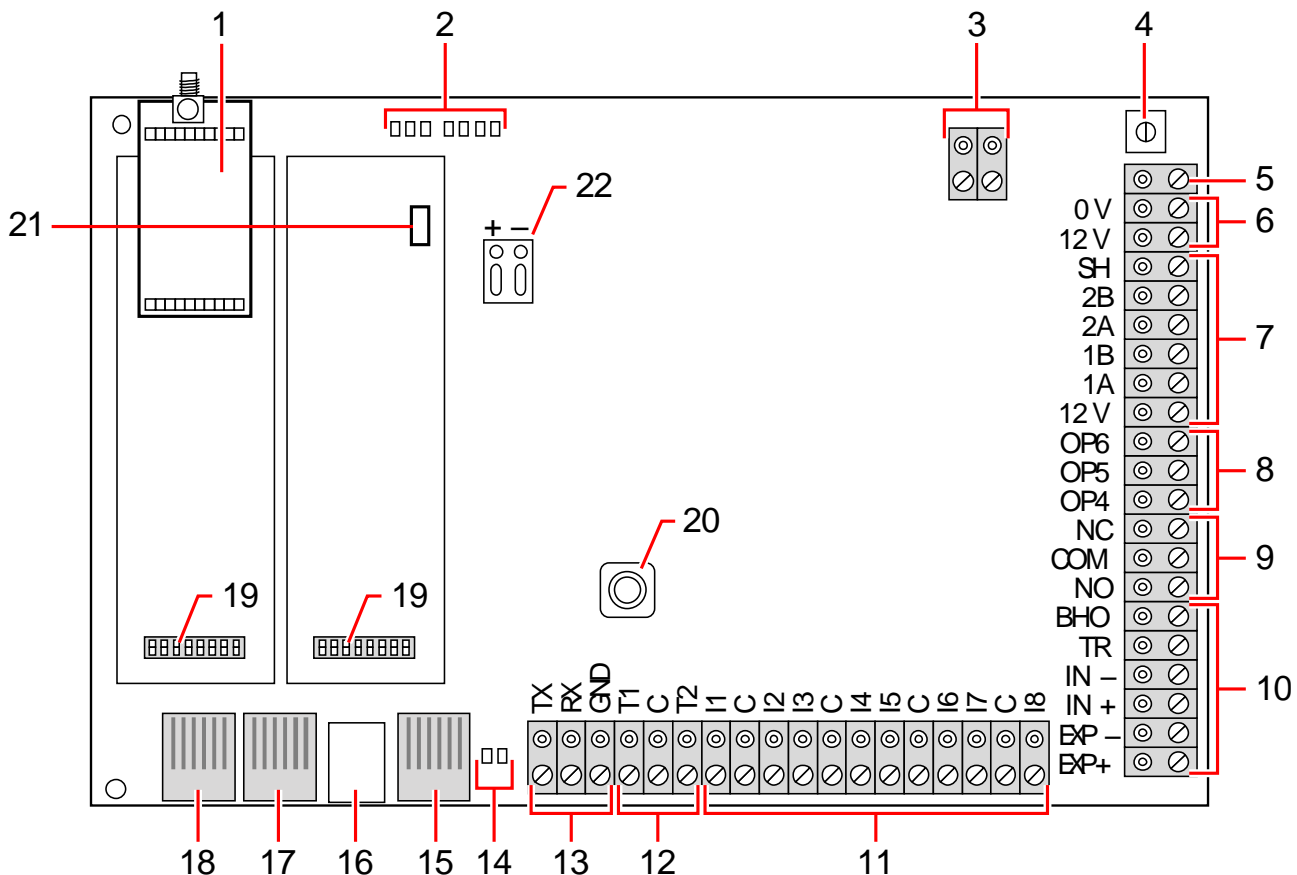
See also

- ▣ Powering expanders from the auxiliary power terminals [→ 333]
- ▣ Wiring the X-BUS interface [→ 72]
- ▣ Wiring an internal sounder [→ 87]
- ▣ Wiring the zone inputs [→ 83]
- ▣ Controller status LEDs [→ 332]
- ▣ Controller status LEDs [→ 332]
- ▣ Powering expanders from the auxiliary power terminals [→ 333]
- ▣ Wiring the X-BUS interface [→ 72]
- ▣ Wiring an internal sounder [→ 87]
- ▣ Wiring the zone inputs [→ 83]


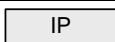

8.1 Controller Hardware 42xx\43xx\53xx\63xx


This section describes the controller for the SPC42xx, 43xx, 53 xx and 63xx models. The SPC5350 and 6350 are described in Controller Hardware SPC5350 and 6350 [→ 68].

The SPC controller provides 8 on-board wired zones and optional wireless zones.



1	Optional wireless module	The controller PCB can be factory fitted with a wireless module for use with wireless (868 MHz) sensors.
2	SPC status LEDs	These 7 LEDs display the status of various system parameters as

		described on page [→ 332].
3	AC power input	<p>A/C Mains Input: The mains AC input voltage is applied to this 2-pin connection via a transformer contained in the SPC enclosure. The earth lead from the mains supply is wired to a connection point on the metal cabinet.</p> <p>Clock Reference*: A clock reference signal can also be applied to this 2-pin connector to maintain accurate system time.</p>
4	Reset button	<ul style="list-style-type: none"> ● To reset the controller: <ul style="list-style-type: none"> – Press this switch once. ● To reset the programming settings to default and reboot the controller: <ul style="list-style-type: none"> – Hold down the button until you are asked if a factory reset is desired. – Select YES to reset to factory defaults. <p>Warning: Defaulting the controller to factory settings deletes all configuration files, including backups, stored on the controller. All isolates and inhibits are also deleted. It is recommended you backup your configuration to a PC before defaulting the controller.</p> <p>Note: This feature is not available if engineer lockout is enabled.</p>
5	Earth connection terminal	This terminal is not required and should not be connected.
6	Auxiliary 12 V output	<p>The SPC controller provides an auxiliary 12 V DC output that can be used to supply power to expanders and devices such as latches, bells, etc. See page [→ 333]. The maximum deliverable current is 750 mA.</p> <p>Please Note: The amount of current drawn is subject to the amount of time to be held up under battery conditions.</p>
7	X-BUS interface	This is the SPC communications bus used to network expanders together on the system. See page [→ 72]. SPC4000 only has 1 X-BUS interface.
8	On-board outputs	Outputs OP4, OP5, and OP6 are 12 V open collector resistive outputs that share a 400 mA current rating with the auxiliary 12 V output. If the outputs are not connected to the 12 V of the controller and are powered from an external power source the 0 V of the power source needs to be connected to the controller 0 V and the external power source cannot exceed 12 V.
9	Relay output	The SPC controller provides a 1 A, single-pole, changeover relay that can be used to drive the strobe output on the external bell.
10	Internal bell / external bell	Internal and external bell outputs (INT+, INT-, EXT+, EXT-) are resistive outputs with a 400 mA current rating. The BHO (B ell H old O ff), TR (T amper R eturn), and EXT outputs are used to connect an external bell to the controller. The INT+ and INT- terminals are used to connect to internal devices such as an internal sounder. See page [→ 87].
11	Zone inputs	The controller provides 8 on-board zone inputs that can be monitored using a variety of supervision configurations. These configurations can be programmed from system programming. The default configuration is Dual End of Line (DEOL) using resistor values of 4K7. See page [→ 83].
12	Tamper terminals	The controller provides 2 additional tamper input terminals that can be connected to auxiliary tamper devices to provide increased tamper protection. These terminals should be shorted when not in use.
13	Serial port 2 terminal block	<p>Serial port 2 terminal block (TX, RX, GND) may be used to interface to an external modem or PC terminal program. Serial port 2 shares a communications channel with the back-up modem. If a back-up modem is installed, ensure that no devices are connected to this serial port.</p> 
14	 Ethernet connectivity LEDs	The 2 Ethernet LEDs indicate the status of the Ethernet connection. The left LED indicates data activity on the Ethernet port; the right LED indicates the Ethernet link is active.
15	 Ethernet interface	The Ethernet interface provides for the connection of a PC to the controller for the purposes of programming the system.

16	USB interface	This USB interface is used to access browser programming or a terminal program.
17	Serial port 2 	This RS232 serial port may be used to interface to an external modem or PC terminal program. Serial port 2 shares a communications channel with the back-up modem. If a back-up modem is installed, ensure no devices are connected to this serial port.
18	Serial port 1	This RS232 serial port may be used to interface to an X10 protocol device.
19	Optional plug-in modules	A primary (left slot) and back-up (right slot) module can be connected to the controller. These modules can be GSM or PSTN modems offering increased communication functionality. The back-up modem should not be connected if serial port 2 interface is connected to an external modem or other device.
20	Front tamper	This on-board front tamper (switch & switch) provides the cabinet tamper protection. Note: The front tamper is not used in the G5 housing.
21	Battery selector	J12: Fit jumper for 17 Ah battery use and remove for 7 Ah battery. Please Note: This selector is only available on 2.3 revision controller PCB. (Not applicable for SPC5350 and SPC5360 panels)
22	Auxiliary power input	12 v input from battery or PSU**.

* Default setup for SPC5350 and SPC5360 panels

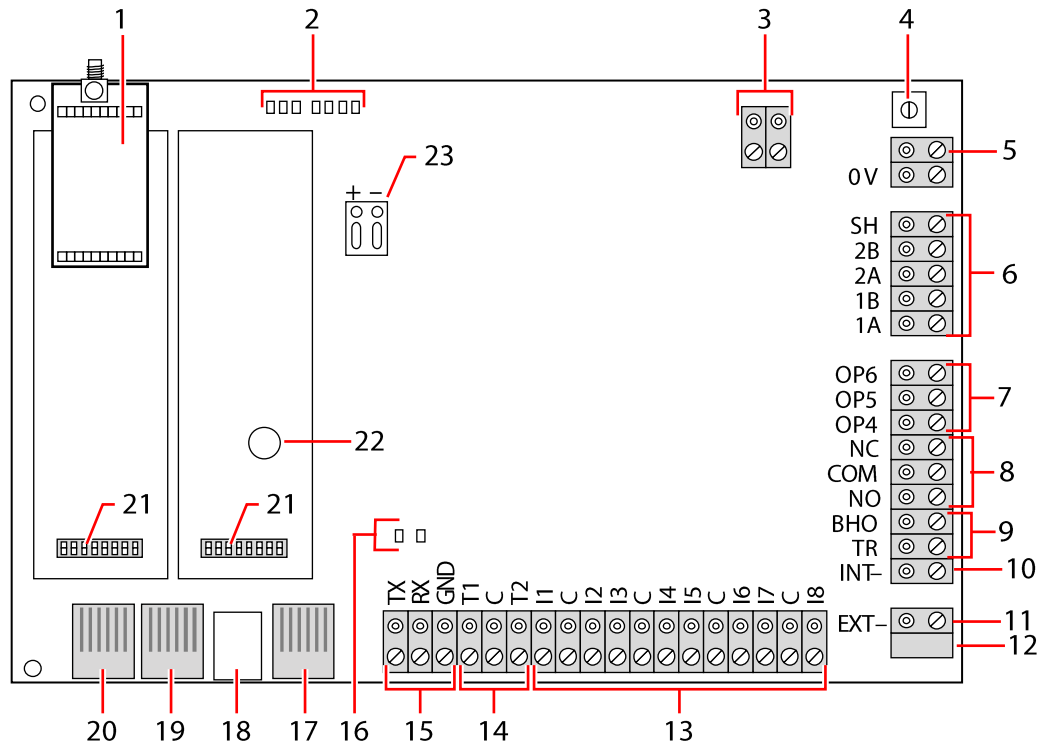
** PSU only applies to SPC5350 and SPC6350 panels.

8.2 Controller Hardware SPC5350 and 6350

This section describes the SPC5350 and SPC6350.




The expander that is connected to the power supply within the G5 is set to ID1 by default. This setting should not be changed.



1	Optional wireless module	The controller PCB can be factory fitted with a wireless module for use with wireless (868 MHz) sensors.
2	SPC status LEDs	These 7 LEDs display the status of various system parameters as described on page [→ 332].
3	Clock Reference	A clock reference signal can also be applied to this 2-pin connector to maintain accurate system time. Connect to Clock Reference CN17 on SPCP355.300 Smart PSU.
4	Reset button	<ul style="list-style-type: none"> ● To reset the controller: <ul style="list-style-type: none"> – Press this switch once. ● To reset the programming settings to default and reboot the controller: <ul style="list-style-type: none"> – Hold down the button until you are asked if a factory reset is desired. – Select YES to reset to factory defaults. <p>Warning: Defaulting the controller to factory settings deletes all configuration files, including backups, stored on the controller. All isolates and inhibits are also deleted. It is recommended you backup your configuration to a PC before defaulting the controller.</p> <p>Note: This feature is not available if engineer lockout is enabled.</p>
5	Earth connection terminal	This terminal is not required and should not be connected.
6	X-BUS interface	This is the SPC communications bus used to network expanders together on the system. See page [→ 72]. Terminals 1B and 1A must be connected to SPCP355.300 I/O Expander

		terminals 2B and 2A, respectively Terminals 2A and 2B must be connected to terminals 2A and 2B, respectively, of the next expander on the X-BUS.
7	On-board outputs	Outputs OP4, OP5, and OP6 are 12 V open collector resistive outputs with a 300 mA current rating. The OP4 load must be connected to the SPCP355.300 Smart PSU.
8	Relay output	The SPC controller provides a 1 A, single-pole, changeover relay that can be used to drive the strobe output on the external bell.
9	Bell Hold-Off (BHO) and Tamper Return (TR)	The BHO (B ell H old O ff) and TR (T amper R eturn) (and EXT output) are used to connect an external bell to the controller. See page [→ 87].
10	Internal Bell (negative)	The INT- terminal is used to connect to internal devices such as an internal sounder. The power for the internal sounder must be connected to the SPCP355.300 Smart PSU.
11	External Bell (negative)	The Ext- terminal is used to connect to external devices such as an external bell. The power for the external sounder must be connected to the SPCP355.300 Smart PSU.
12	Do not use.	Do not use.
13	Zone inputs	The controller provides 8 on-board zone inputs that can be monitored using a variety of supervision configurations. These configurations can be programmed from system programming. The default configuration is Dual End of Line (DEOL) using resistor values of 4K7. See page [→ 83].
14	Tamper terminals	The controller provides 2 additional tamper input terminals that can be connected to auxiliary tamper devices to provide increased tamper protection. These terminals should be shorted when not in use.
15	Serial port 2 terminal block	Serial port 2 terminal block (TX, RX, GND) may be used to interface to an external modem or PC terminal program. Serial port 2 shares a communications channel with the back-up modem. If a back-up modem is installed, ensure that no devices are connected to this serial port.
16	Ethernet connectivity LEDs	The 2 Ethernet LEDs indicate the status of the Ethernet connection. The left LED indicates data activity on the Ethernet port; the right LED indicates the Ethernet link is active.
17	Ethernet interface	The Ethernet interface provides for the connection of a PC to the controller for the purposes of programming the system.
18	USB interface	This USB interface is used to access browser programming or a terminal program.
19	Serial port 2	This RS232 serial port may be used to interface to an external modem or PC terminal program. Serial port 2 shares a communications channel with the back-up modem. If a back-up modem is installed, ensure no devices are connected to this serial port.
20	Serial port 1	This RS232 serial port may be used to interface to an X10 protocol device.
21	Optional plug-in modules	A primary (left slot) and back-up (right slot) module can be connected to the controller. These modules can be GSM or PSTN modems offering increased communication functionality. The back-up modem should not be connected if serial port 2 interface is connected to an external modem or other device.
22	Real-time clock battery	Battery for real-time clock (RTC).
23	Auxiliary power input	12 v input from A1 on SPCP355.300 Smart PSU.

See also

-  Powering expanders from the auxiliary power terminals [→ 333]

9 Door Expander

The two door expander can handle up to two doors and two card readers. Configuration of the operation mode is done via the two door I/Os. Each of the two door I/Os is responsible for the functionality of two inputs and one output of the door controller. A specific door number can be assigned to a door I/O, which gives the inputs and output predefined functionality. If no door number is assigned to neither of the door I/Os (option "Zones" is selected), the inputs and outputs of the door controller can be used like inputs and outputs on the control panel. Thus, no access functionality is available on this two door controller.

If a door number is assigned only to the first door I/O of the two door controller, the first reader is used as entry reader for this door. If a second reader is available, it is used as exit reader for the configured door. Two inputs and one output have predefined functionality and two inputs and one output can be configured by the user. Additionally, the door position sensor input of the first door can be used as intrusion zone but only with limited functionality.

If a door number is assigned to each of the two door I/Os, the two doors are handled independently. The first card reader is used as entry reader for the first door and the second card reader is used as entry reader for the second door. All inputs and outputs have predefined functionality. The door position sensor inputs of the two doors can additionally be used as intrusion zones but only with limited functionality.

Refer to the Appendix [→ 354] for details of currently supported card readers and card formats.



Each free zone number can be assigned to the zones. But the assignment is not fixed. If number 9 was assigned to a zone, the zone and an input expander with the address 1 is connected to the X-Bus (which is using the zone numbers 9-16). The assigned zone from the two door controller will be moved to the next free zone number. Configuration will be adapted accordingly.

10 Wiring the system

10.1 Wiring the X-BUS interface

The X-BUS interface provides for the connection of expanders to the controller. The X-BUS can be wired in a number of different configurations depending on the installation requirements. The X-BUS interface baud rate is 307 kb.



NOTICE

The X-BUS is an RS-485 bus with a baud rate of 307 kb. The full performance is only supported in loop [→ 73] and spur [→ 74] wiring configuration (best signal quality due to daisy chain of isolated sections with 1 transmitter / 1 receiver and balanced terminating resistors on each end).

The performance in star [→ 75] or multi-drop [→ 75] configuration wiring is limited due to non-optimal conditions of the RS-485 bus specification (reduced signal quality due to multiple receivers / transmitters in parallel with unbalanced terminating resistors).



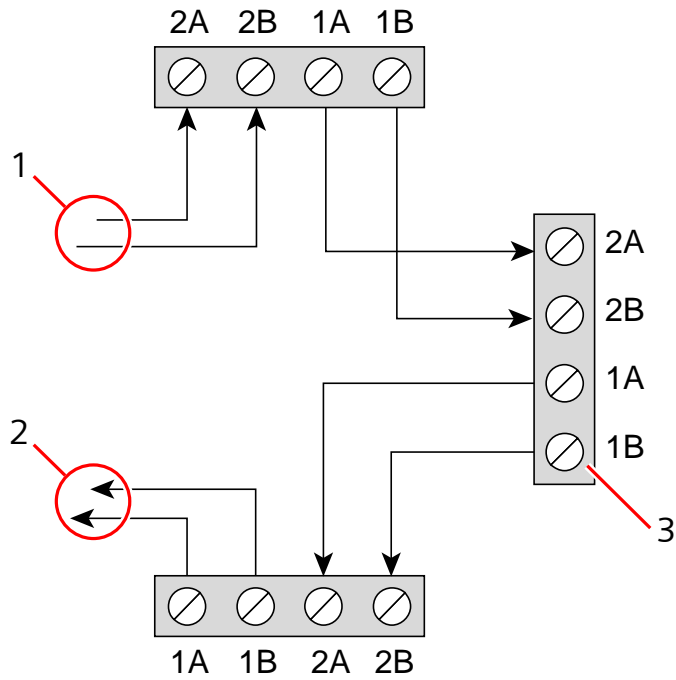
NOTICE

It's strongly recommended to use loop [→ 73] or spur [→ 74] configuration.

The table below shows the maximum distances between controller / expander or expander / expander for all cable types in loop and spur configuration.

Cable Type	Distance
CQR standard alarm cable	200 m
UTP Category: 5 (solid core)	400 m
Belden 9829	400 m
IYSTY 2 x 2 x 0.6 (min)	400 m

Each device has 4 terminals (1A, 1B, 2A, 2B) for connection to expanders via the X-BUS cable. The controller initiates a detection procedure on power up to determine the number of expanders connected on the system and the topology in which they are connected.



Wiring expander

1	Previous expander
2	Next expander
3	SPC controller

Most expanders are equipped with additional terminals 3A/3B and 4A/4B for branch expander wiring. See page [→ 81] for instructions on branch expander wiring.

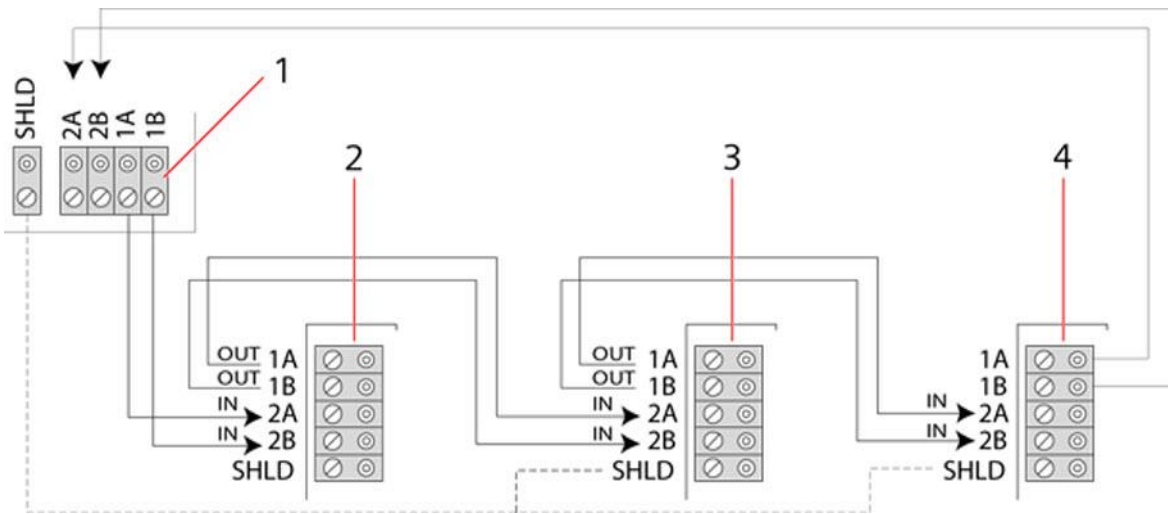
10.1.1 Loop configuration

i	NOTICE
	4000 The SPC42xx/43xx doesn't support loop configuration (only 1 X-BUS port).

i	NOTICE
	All expanders/keypads are fitted with a termination jumper by default. In loop configuration it's imperative to have these jumpers fitted.

The loop (or ring) cabling method offers the highest security by providing fault tolerant communications on the X-BUS. All keypads and expanders are supervised and in case of a X-BUS fault or break, the system continues to operate and all

detectors are monitored. This is achieved by connecting 1A, 1B on the controller to 2A, 2B on the first keypad or expander. The wiring continues with connection 1A, 1B to 2A, 2B on the next expander and so on to the last keypad or expander. The last connection is 1A, 1B of the last expander to 2A, 2B of the controller. See wiring configuration in the figure below.



1	Controller
2-4	Expanders

10.1.2 Spur configuration



NOTICE

SPC52xx/53xx/63xx supports 2 spurs (2 X-BUS ports).
SPC42xx/43xx supports 1 spur (1 X-BUS port).



NOTICE

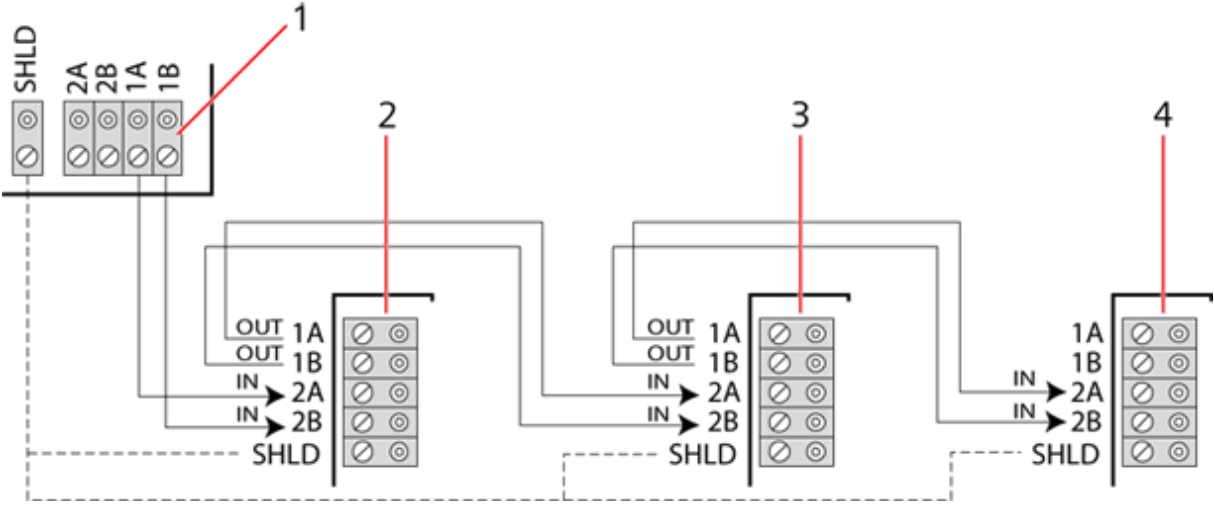
All expanders/keypads are fitted with a termination jumper by default. In spur configuration it is imperative to have these jumpers fitted.

The spur (or open loop) cabling method offers a high level of fault tolerance and may be more convenient on certain installations. In the case of a X-BUS fault or break, all expanders and detectors up to the fault continue to be supervised.

In this configuration, the SPC controller uses a single the X-BUS port (1A/1B or 2A/2B) to support a group of expanders. See wiring configuration in the figure below. The last expander in an open loop configuration is not wired back to the controller and can be identified by the fast LED flashing light (one flash every 0.2 seconds approx) when in Full Engineer programming.

In automatic mode, the expander numbering commences at the expander nearest to the controller and ends with the expander connected farthest from the controller. E.g. if 6 expanders are connected in an open loop configuration, then the nearest expander on the X-BUS connection is expander 1, the second nearest expander is 2, etc. ending with the expander wired farthest from the controller, which is expander 6.

All expanders/keypads are fitted with termination jumpers, as default, allowing termination on all the devices. This is imperative for the spur (chain) configuration, as the jumper acts as a resistive terminator cancelling echoes on the line. Within the loop wiring configuration all expanders/keypads are fitted with a jumper, as default, allowing termination on the device.



Spur configuration

1	Controller
2-4	Expanders

10.1.3 Star and multi-drop configuration

i	NOTICE
	Please read the section for wiring examples [→ 79] and the section Shielding [→ 80] before starting the installation.

The star and multi-drop cabling methods enables takeover of existing wirings with four-core cables in small buildings (typically homes) with low electrical noise environment. These wiring methods are limited to the specifications below:

	SPC42xx/SPC43xx	SPC52xx/SPC53xx/SPC63xx
Max. expanders/keypads	8	16 (8 per X-BUS port)
Total cable length	200 m	200 m

i	NOTICE
	The performance in star or multi-drop configuration wiring is limited due to non-optimal conditions of the RS-485 bus specification (reduced signal quality due to multiple receivers/transmitters in parallel with unbalanced terminating resistors).

Star configuration

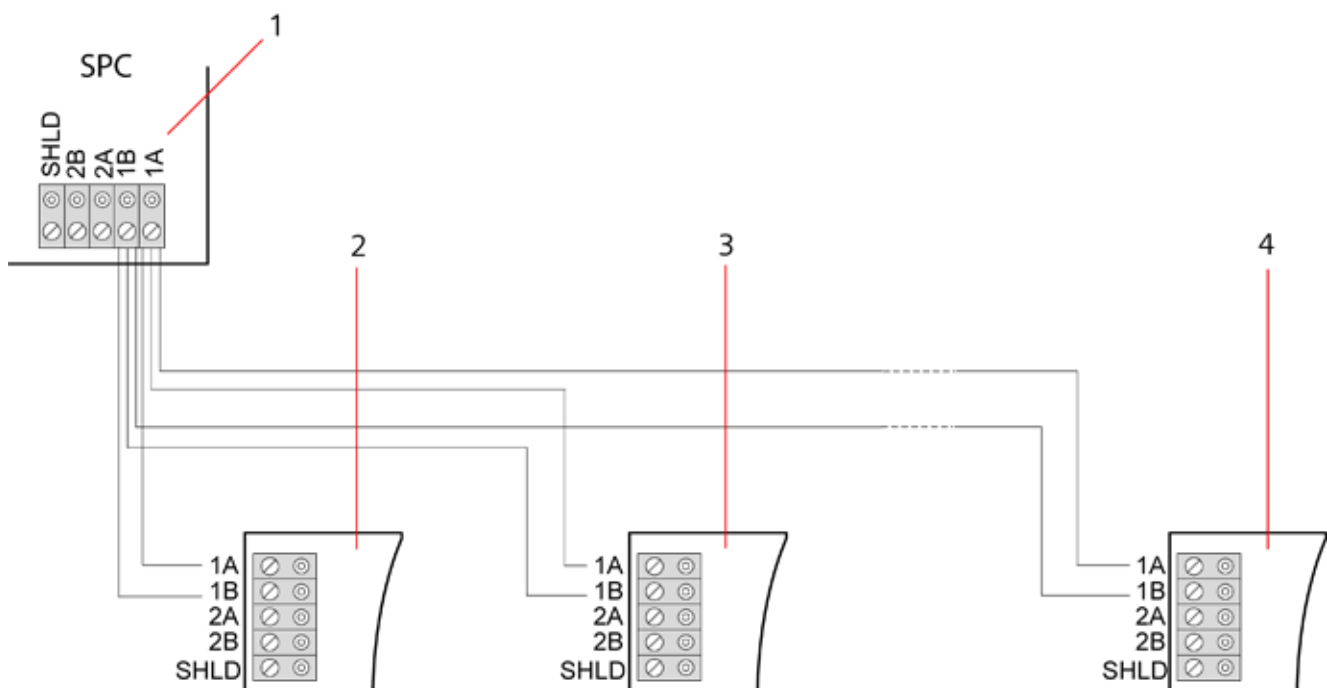


NOTICE

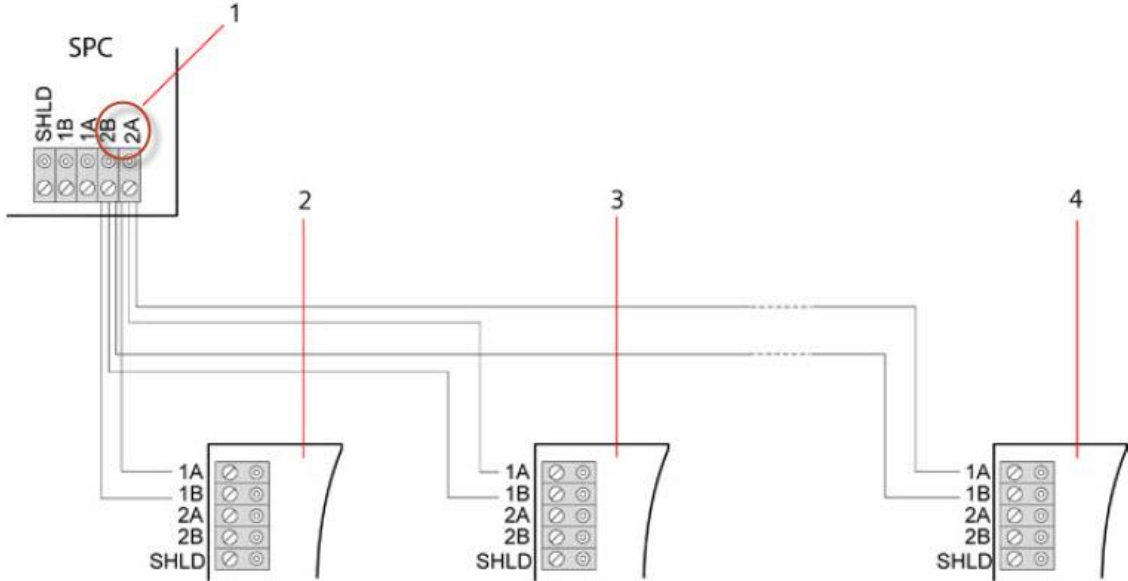
All expanders/keypads are fitted with a termination jumper by default. In star configuration it's imperative to **remove** these jumpers.

A star configuration is established when multiple expanders are wired back to the same X-BUS port on the SPC controller. Depending on controller type 2 ports may exist (1A/1B, 2A/2B), however only one port (1A/1B) is to be used on each keypad or expander.

In the case of a X-BUS break the single will be disconnected, all other expanders and detectors continue to be supervised. A short in the cable renders all expanders disabled.



Star configuration



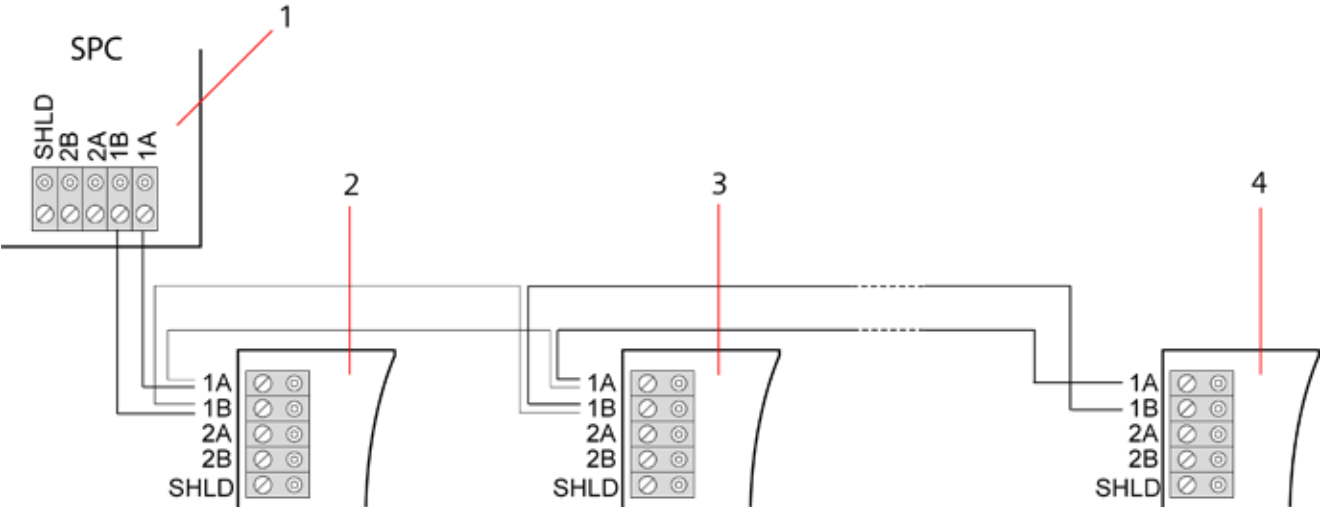
Star configuration 2

1	SPC Controller
2-4	Expanders

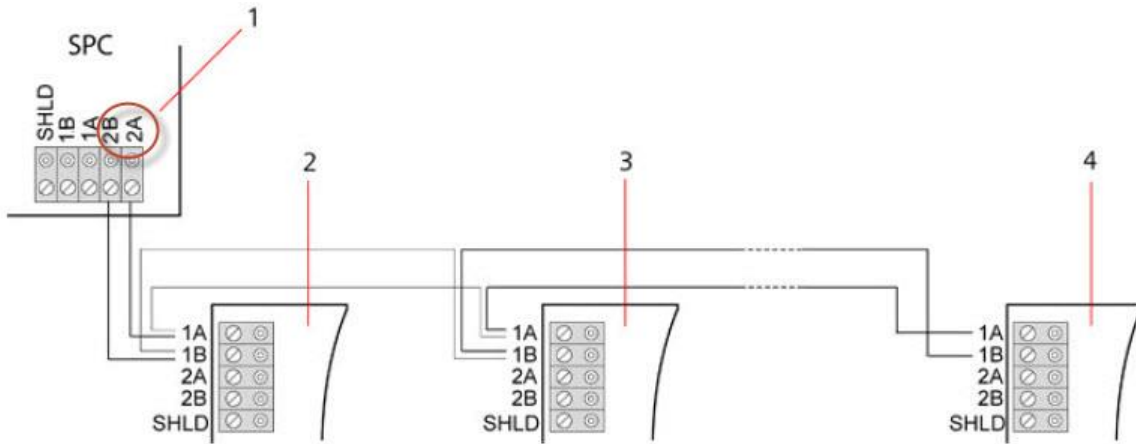
Multi-drop configuration

i	NOTICE
	All expanders/keypads are fitted with a termination jumper by default. In multi-drop configuration it's imperative to remove these jumpers with exception of last keypad or expander.

The multi-drop configuration varies in that each expander uses the same communication channel as it wires onto the next expander, with all expanders using the same input channel. See multi-drop configuration in the second figure. In the case of a X-BUS break, all expanders and detectors up to the fault continues to be supervised. A short in the cable renders all expanders disabled.



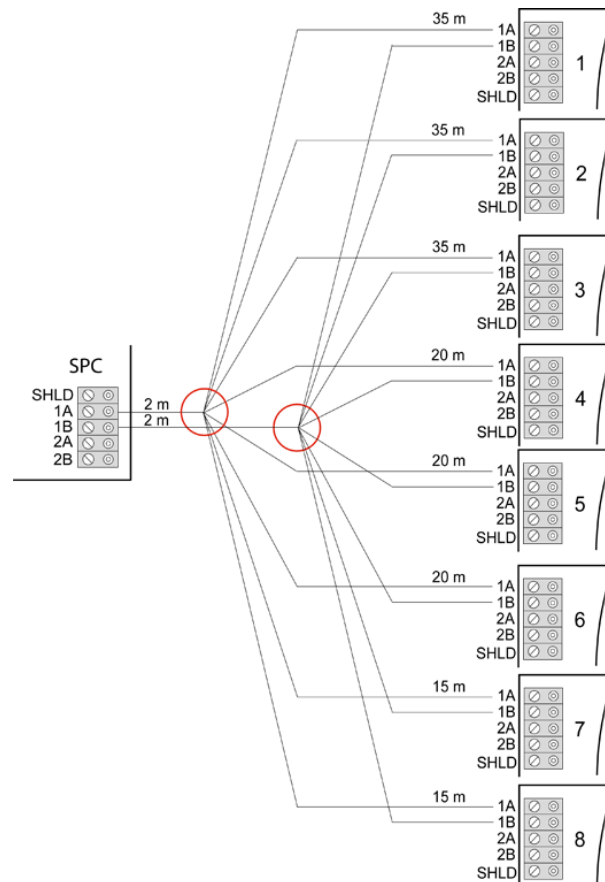
Multi-drop configuration



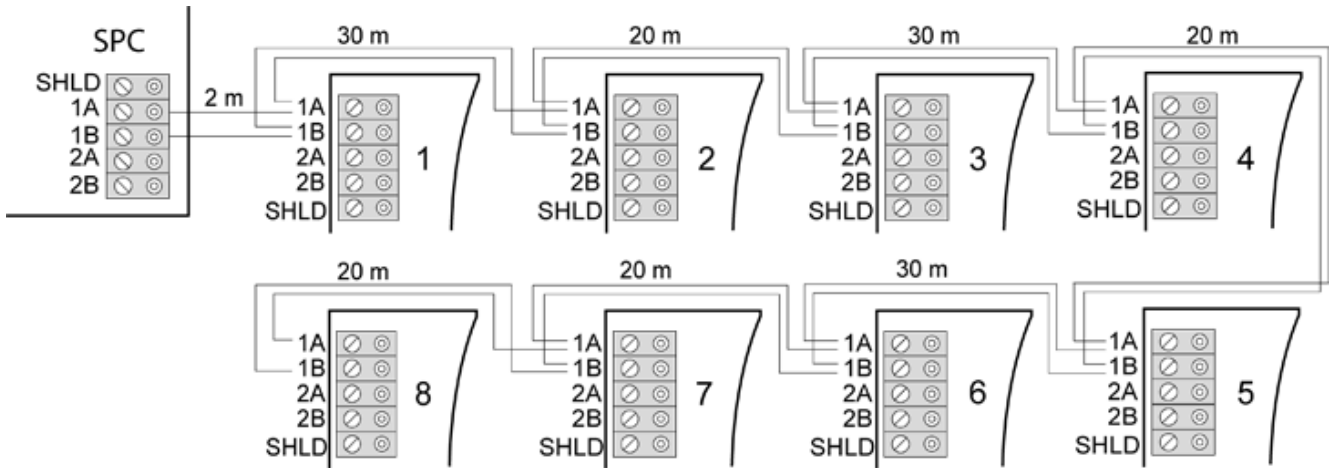
Multi-drop configuration 2

1	SPC controller
2-4	Expanders

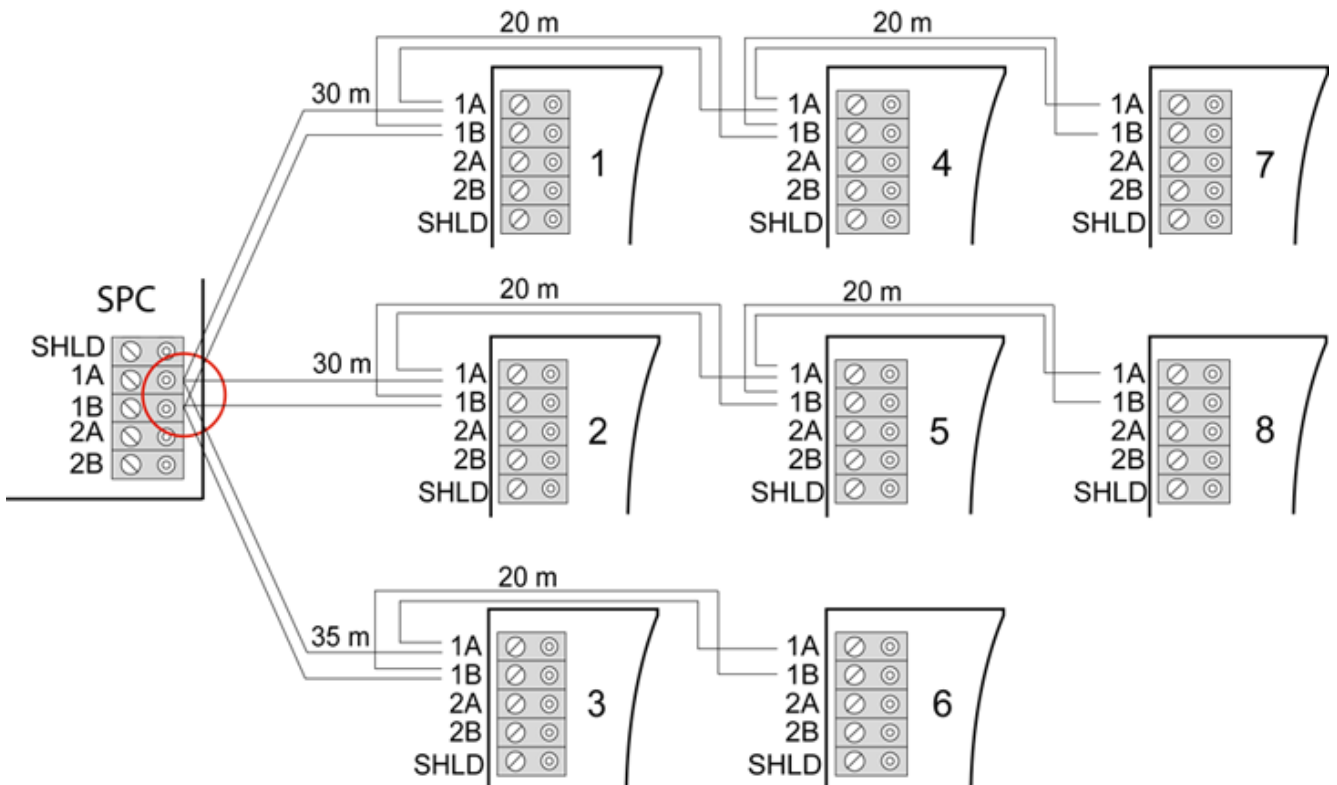
10.1.3.1 Examples of correct wiring



Star wiring




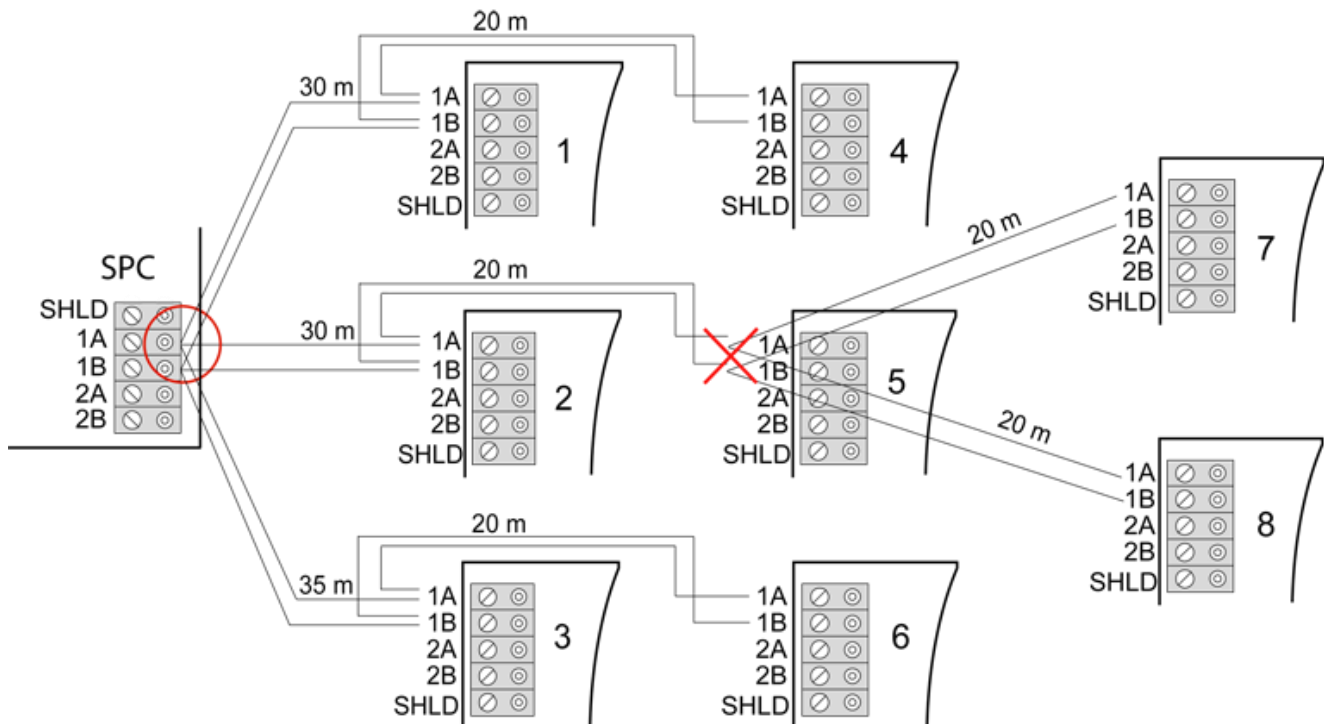
Multi-drop wiring



Mixed wiring

10.1.3.2 Examples of incorrect wiring

	<p>NOTICE</p> <p>A mix of star and multi-drop configuration is only allowed if the star point is at the controller X-BUS port. In this case, all expanders/keypads must be wired in multi-drop configuration without any other star points in the wiring.</p>
---	--



Not allowed wiring with a second star point



NOTICE

If the mix of star and multi-drop configuration is not properly wired the reduced signal quality may lead to slow reaction time of connected devices (e.g. keypad operation) or even loss of communication to devices. If such behavior is observed a wiring in loop OR star configuration is strongly recommended.

10.1.4 Shielding



The shielding terminals (SHLD) should only be used for cables types with shielding (e.g. Belden 9829). If shielding is required (i.e. sites with high electric field interference): connect the cable shield to the SHLD terminals on the controller and all networked expanders. If the shield needs to be connected to earth then a cable needs to be connected from the SHLD terminal on the controller to the chassis earth stud. Do NOT earth the SHLD terminal on any of the expanders.



NOTICE

For star and multi-drop wiring

It's not recommended to use shielded cables due to disadvantageous electrical characteristics (higher capacitance) in star and multi-drop wiring configuration. However, if shielding is required (i.e. sites with high electric field interference) a new wiring in proper spur or loop configuration with appropriate installation cable configuration has to be done.

10.1.5 Cable Map

Identification and numbering order for expanders and keypads differ depending on automatic or manual addressing of the expanders. For information on manual and automatic configuration, see page [→ 118].

For a system with manual addressing, expanders and keypads have a separate numbering sequence and are defined by the engineer manually. I.e., expanders are numbered 01, 02, 03, and so on as desired. Using same numbers, keypads may be numbered as desired.

In the manual configuration, the system automatically allocates zones to each expander. For this reason, devices with no zones, such as 8 output expanders should be addressed last.

For a system with automatic addressing, expanders and keypads belong to the same numbering group and are assigned by the controller. I.e., expanders and keypads are together numbered 01, 02, 03, in the order that they are detected relative to the location of the controller.

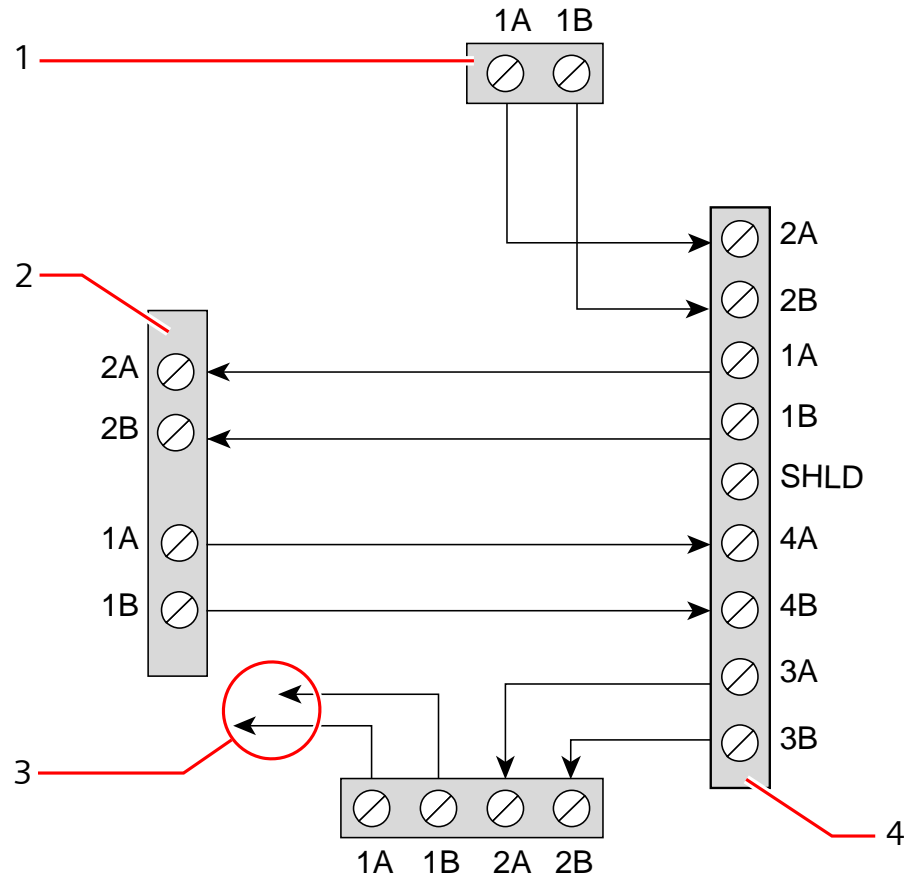
10.2 Wiring of branch expander

The wiring of the X-BUS interface with 8 terminals 1A/1B to 4A/4B provides for the connection of an additional branch expander.

If the branch is not used then the terminals 1A/1B are used to connect to the next expander/keypad. Terminals 3A/3B and 4A/4B are then not used.

The following modules have branch expander wiring capability (additional terminals 3A/B and 4A/B):

- 8 Input / 2 Output Expander
- 8 Output Expander
- PSU Expander
- Wireless Expander
- 2-door Expander



Wiring of a branch expander

1	Previous expander
2	Expander connected to branch
3	Next expander
4	Expander with branch

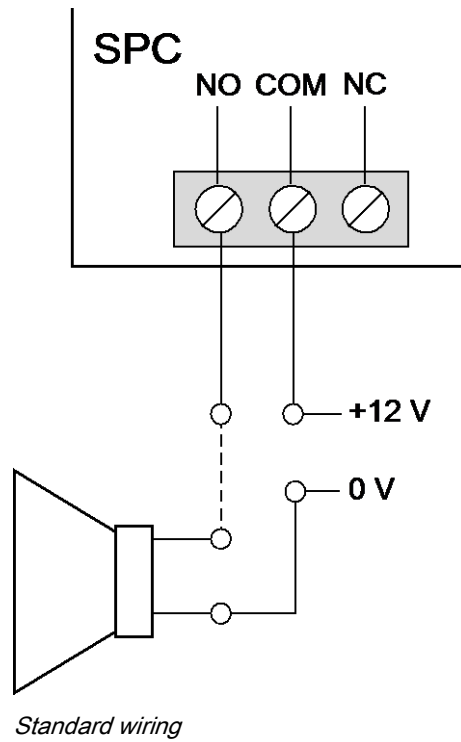
10.3 Wiring the system ground

0V of Smart PSU's, Keypads and Expanders must be connected to the SPC controller 0V (System GND).

10.4 Wiring the relay output

The SPC controller has one on-board 1 A single pole changeover relay that can be assigned to any of the SPC system outputs. This relay output can switch a rated voltage of 30 V DC (non-inductive load).

When the relay is activated the common terminal connection (COM) is switched from the **Normally Closed** terminal (NC) to the **Normally Open** terminal (NO).

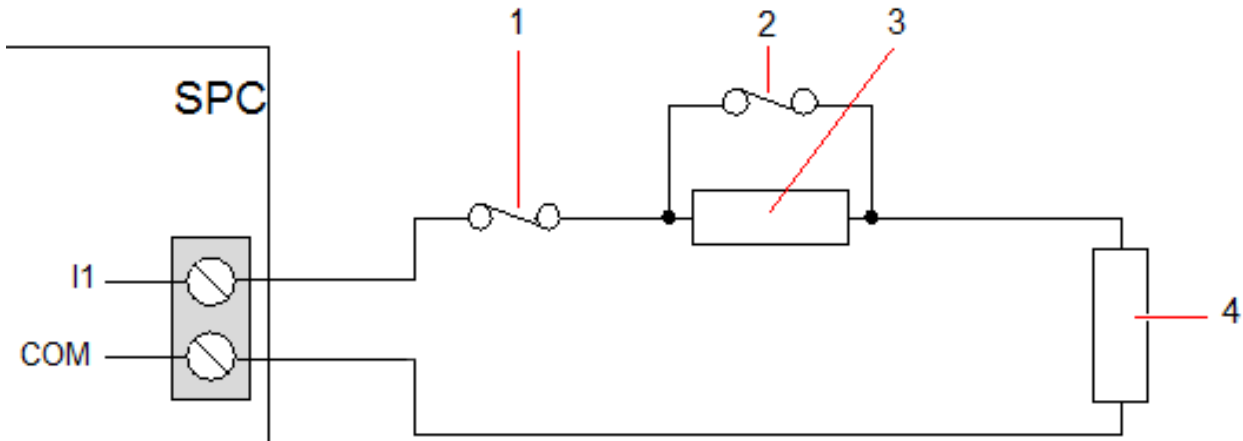


NO	Normally open terminal
COM	Common terminal connection
NC	Normally closed terminal

10.5 Wiring the zone inputs

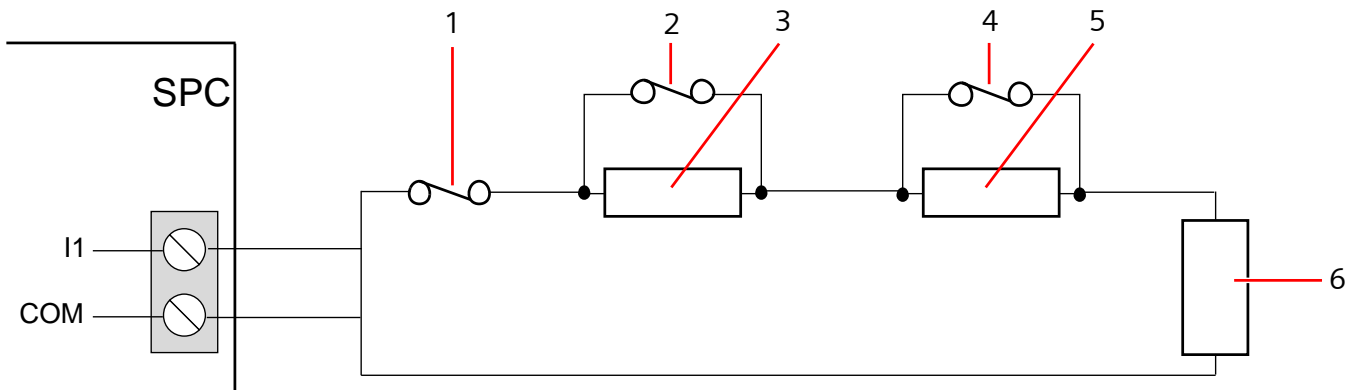
The SPC controller has 8 on-board zone inputs. By default these inputs are monitored using end of line supervision. The installer can choose from any of the following configurations when wiring the inputs:

- No End of Line (NEOL)
- Single End of Line (SEOL)
- Dual End of Line (DEOL)
- Anti-masking PIR



Default configuration (DEOL 4K7)

1	Tamper
2	Alarm
3	EOL 4K7
4	EOL 4K7



Anti-Masking PIR configuration

1	Tamper
2	Alarm
3	EOL 4K7
4	Fault
5	EOL 2K2
6	EOL 4K7

The following table shows the resistance ranges associated with each configuration.

Single EOLs

EOL Type	Quiescent			Alarm		
	Min	Nom	Max	Min	Nom	Max
NONE	0Ω (-100%)	150Ω	300Ω (+100%)	300Ω (+100%)	N/A	Infinite
SINGLE_1K	700Ω	1kΩ	1.3kΩ	23kΩ	N/A	Infinite

	(-30%)		(+30%)			
SINGLE_1K5	1.1k Ω (-27%)	1.5k Ω	2.1k Ω (+40%)	23k Ω	N/A	Infinite
SINGLE_2K2	1.6k Ω (-28%)	2.2k Ω	2.9k Ω (+32%)	23k Ω	N/A	Infinite
SINGLE_4K7	3.1k Ω (-22%)	4.7k Ω	6.3k Ω (+24%)	23k Ω	N/A	Infinite
SINGLE_10K	7k Ω (-30%)	10k Ω	13k Ω (+30%)	23k Ω	N/A	Infinite
SINGLE_12K	8.5k Ω (-30%)	12k Ω	15.5k Ω (+30%)	23k Ω	N/A	Infinite

Dual EOLs with PIR Masking and Fault

EOL Type	Quiescent			Alarm		
	Min	Nom	Max	Min	Nom	Max
Mask_1K_1K_6K8 (1K / 1K / 6K8)	700 Ω (-30%)	1k Ω	1.3k Ω (+30%)	1.5k Ω (-25%)	2k Ω	2.5k Ω (+25%)
Mask_1K_1K_2K2 (1K / 1K / 2K2)	700 Ω (-30%)	1k Ω	1.3k Ω (+30%)	1.5k Ω (-25%)	2k Ω	2.6k Ω (+30%)
Mask_4K7_4K7_2K2 (4K7 / 4K7 / 2K2)	3.9k Ω (-18%)	4.7k Ω	5.6k Ω (+20%)	8.4k Ω (-11%)	9.4k Ω	10.3k Ω (+10%)

EOL Type	Fault			Masking		
	Min	Nom	Max	Min	Nom	Max
Mask_1K_1K_6K8	2700 Ω (-69%)	8.8k Ω	12.6k Ω (+20%)	-	-	-
Mask_1K_1K_2K2	2.8k (-13%)	3.2k	3.6k (+13%)	3.8k (-10%)	4.2k	4.8k (+15)
Mask_4K7_4K7_2K2	6k (-14%)	6.9k	7.8k (+14%)	10.8k (-7%)	11.6k	12.6k (+9%)

Dual EOLs

EOL Type	Quiescent			Alarm		
	Min	Nom	Max	Min	Nom	Max
DUAL_1K0_470	400 Ω (-20%)	470 Ω	700k Ω (+40%)	1.1k Ω (-27%)	1.5k Ω	2k Ω (+34%)
DUAL_1K0_1K0	700 Ω (-30%)	1k Ω	1.3k Ω (+30%)	1.5k Ω (-25%)	2k Ω	2.6k Ω (+30%)
DUAL_1k0_2k2	1.6k Ω (-28%)	2.2k Ω	2.9k Ω (+32%)	2.3k Ω (-29%)	3.2k Ω	4.2k Ω (+32%)
DUAL_1k5_2k2	1.6k Ω (-28%)	2.2k Ω	2.9k Ω (+32%)	2.7k Ω (-28%)	3.7k Ω	4.8k Ω (+30%)
DUAL_2K2_2K2	1.6k Ω (-28%)	2.2k Ω	2.9k Ω (+32%)	3.4k Ω (-23%)	4.4k Ω	5.6k Ω (+28%)
DUAL_2k2_4k7	4.1k Ω (-13%)	4.7k Ω	5.4k Ω (+15%)	6k Ω (-14%)	6.9k Ω	7.9k Ω (+15%)
DUAL_2K7_8K2	7.2 k Ω (-13%)	8.2k Ω	9.2k Ω (+13%)	9.9k Ω (-10%)	10.9k Ω	11.9k Ω (+10%)
DUAL_3K0_3K0	2.1k Ω	3.0k Ω	3.9k Ω	4.5k Ω	6k Ω	7.5k Ω

	(-30%)		(+30%)	(-25%)		(+25%)
DUAL_3K3_3K3	2.3k Ω (-26%)	3.3k Ω	4.3k Ω (+31%)	4.9k Ω (-26%)	6.6k Ω	8.3k Ω (+26%)
DUAL_3K9_8K2	7.0 k Ω (-15%)	8.2k Ω	9.5k Ω (+16%)	10.5k Ω (-14%)	12.1k Ω	13.8k Ω (+15%)
DUAL_4K7_2K2	1.6k Ω (-28%)	2.2K Ω	2.9k Ω (+32%)	5k Ω (-28%)	6.9k Ω	8.8k Ω (+28%)
DUAL_4K7_4K7	3.3k Ω (-30%)	4.7k Ω	6.1k Ω (+30%)	7k Ω (-26%)	9.4k Ω	11.9k Ω (+27%)
DUAL_5K6_5K6	4.0k Ω (-26%)	5.6k Ω	7.2k Ω (+29%)	8.3k Ω (-26%)	11.2k Ω	14.1k Ω (+26%)
DUAL_6K8_4K7	3.3k Ω (-30%)	4.7k Ω	6.1k Ω (+30%)	8.1k Ω (-30%)	11.5k Ω	14.9k Ω (+30%)
DUAL_2k2_10K	9.2k Ω (-8%)	10k Ω	10.8k Ω (+8%)	11.3 k Ω (-8%)	12.2k Ω	13.2k Ω (+9%)
DUAL_10k_10k	7.5k Ω (-25%)	10k Ω	12.5k Ω (+25%)	17k Ω (-15%)	20k Ω	23k Ω (+15%)

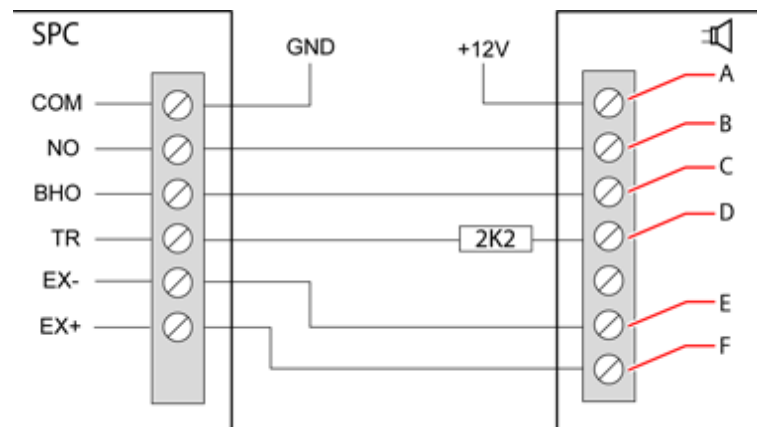


For all EOL types, a resistance below 300 Ω is considered a short. If the resistance is not within the thresholds stated, this is treated as a disconnection.

10.6 Wiring an external SAB bell

On an external bell to the SPC controller board the relay output is wired to the strobe input with **Bell Hold Off (BHO)** and **Tamper Return (TR)** connected to their respective inputs on the external bell interface.

A resistor (2K2) is pre-fitted on the controller board between the BHO and TR terminals. When wiring an external bell, connect this resistor in series from the TR terminal on the controller to the TR terminal on the external bell interface.

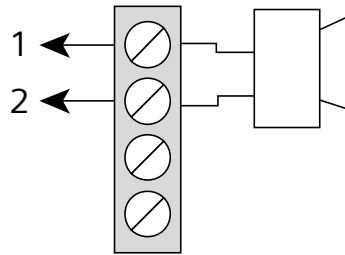


External bell wiring

A	Strobe +
B	Strobe -
C	Hold off
D	Tamper return
E	Bell -
F	Bell +

10.7 Wiring an internal sounder

To wire an internal sounder to the SPC controller connect the IN+ and IN- terminals directly to the 12 V sounder input.



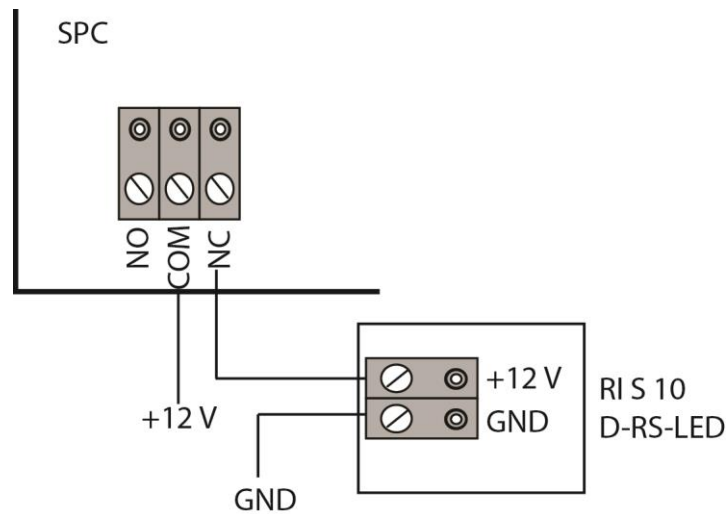
Internal sounder wiring (12 V)

IN-	IN- (SPC controller)
IN+	IN+ (SPC controller)

10.8 Wiring Glassbreak

SPC supports the RI S 10 D-RS-LED glassbreak interface in combination with GB2001 glassbreak detectors.

The following diagram shows how the glassbreak interface is wired to the SPC controller for power, or to an 8-in/2-out expander:



For information on wiring the glassbreak interface to a zone, see the product-specific documentation.

For information on wiring the glassbreak sensors to the glassbreak interface, see the product-specific documentation.

10.9 Installing plug-in modules

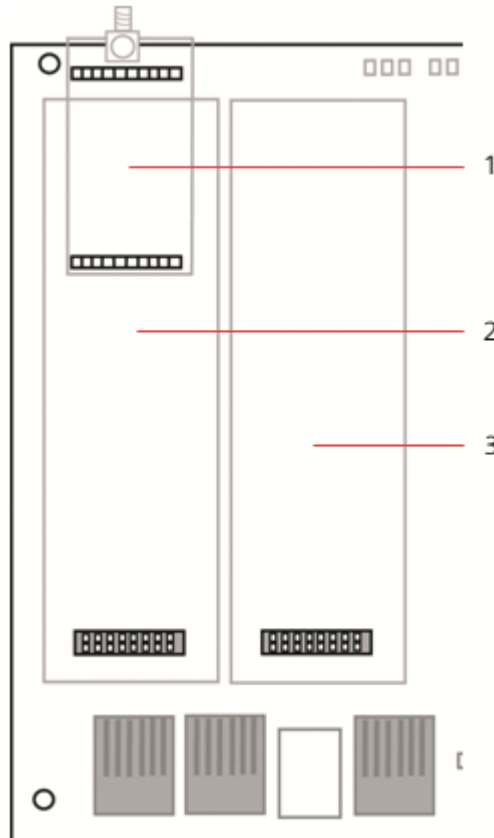
2 modems (PSTN or GSM) may be installed on the controller board to increase functionality. The picture below shows the 2 slots available for each modem, the primary (left) slot and the back-up (right) slot.

If both modem slots are available, always install the plug-in module in the primary slot; the system always attempts to make PSTN or GSM calls on a modem installed on the primary slot before attempting to use the back-up slot.



⚠ WARNING

Modems are not plug and play. You must log on to the panel as Full Engineer, then power the controller board down before installing, removing or moving modems from one position to the other. After completing the modem task, reconnect the system to the power supply and log on to the controller as Full Engineer again. Configure and save the configuration. Failure to follow this process results in a CRC error.



Plug-in modules

1	Wireless receiver slot
2	Primary modem slot
3	Back-up modem slot



For installation please refer to the corresponding Installation Instruction.


11 Powering up the SPC controller

The SPC controller has two power sources, the mains supply and the integral standby battery. A qualified electrician should undertake connection to the mains and the mains supply should be connected from a spur that can be isolated. See Page [→ 346] for full details of conductor sizes / fuse ratings etc.

The SPC should be powered from the mains first and then the internal standby battery. For compliance to EN only one battery should be fitted of the appropriate capacity.

11.1 Powering from battery only

It is recommended that when powering a system from battery only, the battery should be in a fully charged state (>13.0 V). The system will not power up when using a battery with less than 12 V and no mains is applied.

	<p>NOTICE</p>
	<p>The battery will continue to power the system until deep discharge level (10.5 V to 10.8 V) has been detected. The time duration that the system will hold up on battery will depend on the external loading and Ah rating of the battery.</p>

12 Keypad user interface

The following keypad models are available:

- SPCK420/421 — referred to throughout this document as the LCD Keypad
- SPCK620/623 — referred to throughout this document as the Comfort Keypad

12.1 SPCK420/421

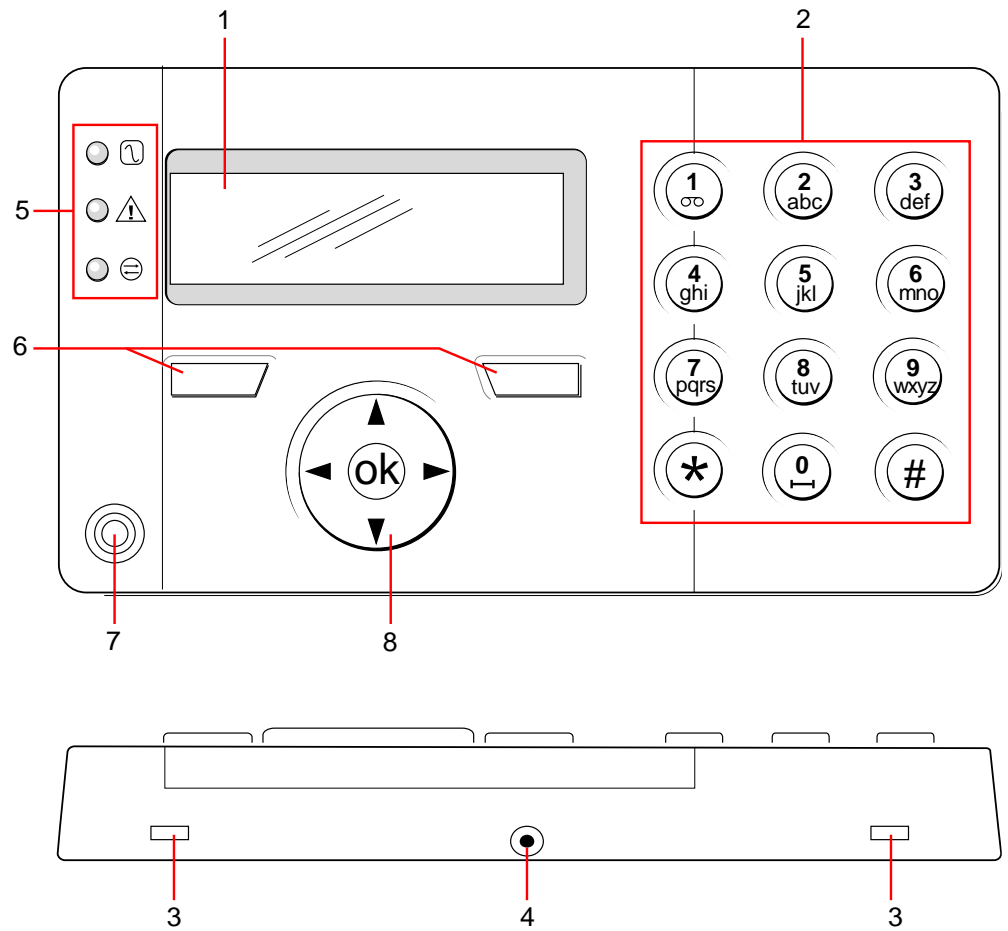
12.1.1 Introduction

The LCD keypad is a wall-mounted interface that allows:

- **Engineers** to program the system through the Engineer Programming menus (password protected) and to set/unset the system; a user can control the system on a day-to-day basis.
- **Users** to enter User Programming menus (password protected), and to perform operational procedures (set/unset) on the system. (Please refer to the SPCK420/421 User Manual for more details of user programming.)

The LCD keypad unit includes an integral front tamper switch and has a 2 line x 16 character display. It features an easy-to-use navigation key to assist in locating required programming options, and has 2 context sensitive soft keys (left and right) for selecting the required menu or program setting. 3 LEDs on the keypad provide an indication of AC power, system alerts, and communications status.




The LCD keypad may be factory fitted with a Portable ACE (PACE) proximity device reader (see page [→ 343]).



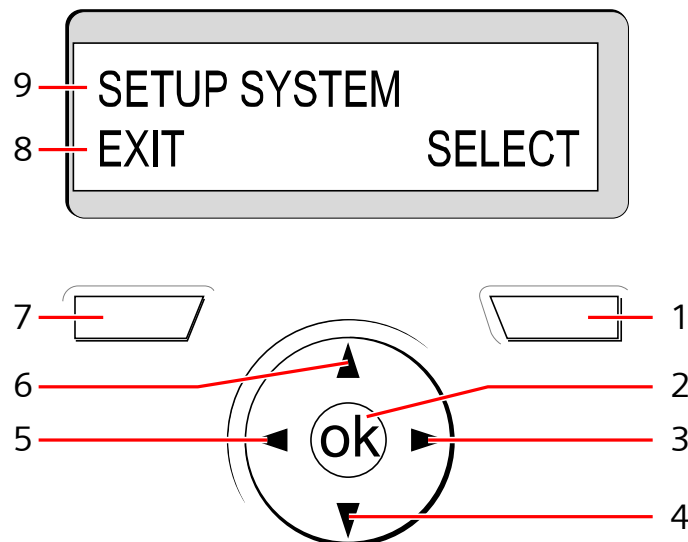
LCD keypad

1	LCD display	The keypad display (2 lines x 16 characters) shows all alert and warning messages and provides a visual interface for programming the system (engineer programming only). The display can be adjusted for contrast and under which conditions the backlight comes on.
2	Alphanumeric keys	Alphanumeric keypad allow for both text and numeric data entry during programming. Alphabetic characters are selected by applying the appropriate number of key presses. To switch between upper and lower case characters, press the hash (#) key. To enter a numeric digit, hold down the appropriate key for 2 seconds.
3	Leverage access tabs	The leverage access tabs provide access to the keypad back assembly clips. Users can unhinge these clips from the front assembly by inserting a 5mm screwdriver into the recesses and pushing gently.
4	Back assembly securing screw	This screw secures the front and back assemblies on the keypad. This screw must be removed to open the keypad.
5	LED status indicators	The LED status indicators provide information on the current status of the system as detailed in the table below.
6	Soft function keys	The left and right soft function keys are context sensitive keys to navigate through menus/programming.
7	Proximity device receiver area	If the keypad has been fitted with a proximity device receiver (see page [→ 343]), users should present the Portable ACE Fob to within 1 cm of this area to SET/UNSET the system.
8	Multi-functional navigation Key	The multi-functional navigation key in combination with the keypad display provides an interface for programming the system.



LED	Status
-----	--------

AC mains (Green)		Indicates the presence or failure of the mains supply FLASHING: AC mains fault detected STEADY: AC mains OK
System alert (Yellow)		Indicates a system alert FLASHING: System alert detected; display indicates the location and nature of alert. If the system is SET, then NO indication is given of system alerts OFF: No alert detected; If a keypad is assigned to more than one area, LED does not indicate an alert condition if any of those areas is SET
X-BUS Status (Red)		Indicates the status of the X-BUS communications when in FULL ENGINEER programming Flashes regularly: (once every 1.5 seconds approx) indicates communications status is OK Flashes quickly: (once every 0.25 seconds approx) indicates the keypad is the last expander on the X-BUS If the keypad is being installed for the first time and power is supplied to it before a connection to the controller X-BUS interface is made, the LED remains in the ON state

12.1.2 Using the LCD keypad interface



Keypad display

1	RIGHT SOFT KEY	This key is used to select the option presented on the right side of the bottom line display. Possible values are: → SELECT to select the option displayed on the top line → ENTER to enter the data displayed on the top line → NEXT to view the next alert after the one displayed on the top line → CLEAR to clear the alert displayed on the top line → SAVE to save a setting
2	OK	The OK button acts as a SELECT key for the menu option displayed on the top line and also as an ENTER/SAVE key for data displayed on the top line.
3		In Programming mode, the right arrow key advances the user through the menus in the same way as pressing the SELECT option (right soft key). In data entry mode, press this key to move the cursor one position to the right.
4		In Programming mode, the down arrow key moves the user to the next programming option in the same menu level. Continually press this key to scroll through all programming options available on the current menu level. In alphanumeric mode, press this key over an upper case character to change the character to lower case.

		When alerts are displayed, the down arrow key moves the user to the next alert message in the order of priority. (See section on Prioritization of Display Messages)
5	◀	In Programming mode, the left arrow key returns the user to the previous menu level. Pressing this key when in the top menu level exits the user from programming. In data entry mode, press this key to move the cursor one position to the left.
6	▲	In Programming mode, the up arrow key moves the user to a previous programming option in the same menu level. Continually press this key to scroll through all programming options available on the current menu level. In Alphanumeric mode, press this key over a lower case character to change the character to upper case.
7	LEFT SOFT KEY	This key is used to select the option presented on the left side of the bottom line display. Possible values are: → EXIT to exit programming → BACK to return to previous menu
8	BOTTOM LINE OF DISPLAY	In the IDLE state, this line is blank. In Programming mode, this line displays options available to the user. These options align over the left and right soft keys for selection as required.
9	TOP LINE OF DISPLAY	In the IDLE state, displays the current date and time. In Programming mode, this line displays one of the following: → The programming feature to be selected → The current setting of the selected feature → The nature of the current alert during an alert condition. (See Prioritization of Display Messages below)

Prioritization of display messages

Trouble messages and alerts are displayed on the keypad in the following order:

- Zone
 - Alarms
 - Tamper
 - Trouble
- Area Alerts
 - Fail to set
 - Entry time out
 - Code tamper
- System Alerts
 - Mains
 - Battery
 - PSU fault
 - Aux fault
 - External bell fuse
 - Internal bell fuse
 - Bell tamper
 - Cabinet tamper
 - Aux tamper 1
 - Aux tamper 2
 - Wireless jamming
 - Modem 1 fault
 - Modem 1 line
 - Modem 2 fault
 - Modem 2 line

- Fail to communicate
- User panic
- XBUS cable fault
- XBUS communications fault
- XBUS mains fault
- XBUS battery fault
- XBUS power supply fault
- XBUS fuse fault
- XBUS tamper fault
- XBUS antenna fault
- XBUS wireless jamming
- XBUS panic
- XBUS fire
- XBUS medical
- XBUS Power supply link
- XBUS output tamper
- XBUS Low voltage
- Engineer restore Required
- Autoarm
- System information
 - Soaked zones
 - Open zones
 - Area state
 - Low battery (sensor)
 - Sensor lost
 - WPA low battery
 - WPA lost
 - WPA test overdue
 - Camera offline
 - Fob low battery
 - Xbus over current
 - Installer name
 - Installer phone
 - Engineer enable
 - Manufacture enable
 - Reboot
 - Hardware fault
 - Aux over current
 - Battery low
 - Ethernet link
 - System name

12.1.3 Data entry on the LCD keypad

Entering data and navigating the menus on the LCD keypad is facilitated through the use of the programming interface. The use of the interface for each type of operation is detailed below.

Entering numeric values

In Numeric Entry mode, only the numeric digits (0 - 9) can be entered.

- To move the position of the cursor one character to the left and right respectively, press the left and right arrow keys.
- To exit from the feature without saving, press the BACK menu key.
- To save the programmed setting press ENTER or OK.

Entering text

In Text Entry mode, both alphabetic characters (A-Z) and numeric digits (0 – 9) can be entered.

- To enter an alphabetic character, press the relevant key the required number of times.
- To enter a language specific special character (ä, ü, ö...) press button 1 to cycle through the special characters.
- To enter a space + special characters (+, -/[...] press button 0.
- To enter a digit, hold the relevant key down for 2 seconds and release.
- To move the position of the cursor one character to the left and right respectively, press the left and right arrow keys.
- To exit from the feature without saving, press BACK.
- To save the programmed setting press ENTER or OK.
- To change the case of an alphabetic character, press the up/down arrow keys when the character is highlighted by the cursor.
- To toggle between upper and lower case for all subsequent characters, press the hash (#) key.
- To delete character to the left of the cursor, press the star key(*).

Selecting a programming option

In navigation mode, the Engineer/User selects one of a number of pre-defined programming options from a list.

- To scroll through the list of options available for selection, press the up and down arrow keys.
- To exit from the feature without saving, press BACK.
- To save the selected option, press SAVE or OK.

12.2 SPCK620/623

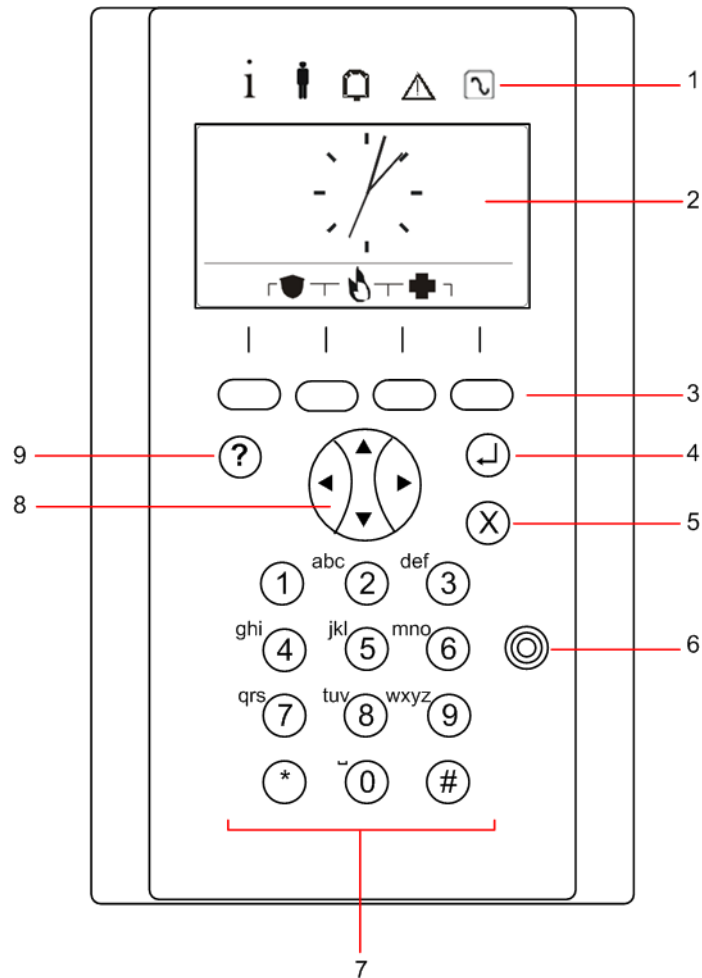
12.2.1 Introduction

The Comfort keypad is a wall-mounted interface that allows:

- Engineers to program the system through the Engineer Programming menus (password protected) and to set/unset the system; a user can control the system on a day-to-day basis.
- Users to enter User Programming menus (password protected), and to perform operational procedures (set/unset) on the system. (Please refer to the SPC620/623 User Manual for more details of user programming)

The SPCK620 is equipped with soft keys and large graphical LCD for easy operation. The functionality can be enhanced with key switch expander SPCE110 or indication expander SPCE120.

The SPCK623 is equipped with a proximity card reader (125 kHz EM 4102) for easy user access, soft keys, large graphical LCD and voice annunciation support. The functionality can be enhanced with key switch expander SPCE110 or indication expander SPCE120.



1	LED status indicators	The LED status indicators provide information on the current status of the system as detailed in the table below.
2	LCD display	The keypad display shows all alert and warning messages and provides a visual interface for programming the system (engineer programming only). (See section on Display Message Prioritization) The display can be configured under which conditions the backlight comes on.
3	Soft function keys	Context sensitive keys to navigate through menus/programming.
4	Enter key	Confirm display or input.
5	Back menu key	<ul style="list-style-type: none"> ● Go back in the menu Reset buzzers, siren and alarms in the memory.
6	Proximity device receiver area	Only SPCK 623: If the keypad has been fitted with a proximity device receiver, users should present the Portable ACE Fob to within 1 cm of this area.
7	Alphanumeric keys	Alphanumeric keypad allow for both text and numeric data entry during programming. Alphabetic characters are selected by applying the appropriate number of key presses. To switch between upper and lower case characters, press the hash (#) key. To enter a numeric digit, hold down the appropriate key for 2 seconds.
8	Multi-functional navigation key	Navigation through menus and to scroll through alert messages. (See Display Message

		Prioritization below)
9	Information key	Displays information.






Prioritization of display messages

Trouble messages and alerts are displayed on the keypad in the following order:


- Zone
 - Alarms
 - Tamper
 - Trouble
- Area Alerts
 - Fail to set
 - Entry time out
 - Code tamper
- System Alerts
 - Mains
 - Battery
 - PSU fault
 - Aux fault
 - External bell fuse
 - Internal bell fuse
 - Bell tamper
 - Cabinet tamper
 - Aux tamper 1
 - Aux tamper 2
 - Wireless jamming
 - Modem 1 fault
 - Modem 1 line
 - Modem 2 fault
 - Modem 2 line
 - Fail to communicate
 - User panic
 - XBUS cable fault
 - XBUS communications fault
 - XBUS mains fault
 - XBUS battery fault
 - XBUS power supply fault
 - XBUS fuse fault
 - XBUS tamper fault
 - XBUS antenna fault
 - XBUS wireless jamming
 - XBUS panic
 - XBUS fire
 - XBUS medical
 - XBUS Power supply link
 - XBUS output tamper
 - XBUS Low voltage
 - Engineer restore Required

- Autoarm
- System information
 - Soaked zones
 - Open zones
 - Area state
 - Low battery (sensor)
 - Sensor lost
 - WPA low battery
 - WPA lost
 - WPA test overdue
 - Camera offline
 - Fob low battery
 - Xbus over current
 - Installer name
 - Installer phone
 - Engineer enable
 - Manufacture enable
 - Reboot
 - Hardware fault
 - Aux over current
 - Battery low
 - Ethernet link
 - System name

12.2.2 LED description

Description	Symbol	Color	Operation	Description
Information		Blue	On	The system or area cannot be set. Forced setting is possible (faults or open zones can be inhibited).
			Flashing	The system or area cannot be set or forced set (faults or open zones cannot be inhibited).
			Off	The system or area can be set.
		Amber	Flashing	Engineer is on site.
User		Green	On	Assigned area is unset.
			Flashing	Assigned area is Partset A / B
			Off	Assigned area is fullset
Alarm		Red	On	Alarm
			Flashing	-
			Off	No alarm
Alert		Amber	On	-
			Flashing	Trouble
			Off	No trouble
Mains		Green	On	System ok
			Flashing	Mains fault


			Off	No bus connection
--	--	--	-----	-------------------

	NOTICE
	The LED indications for information, area status, alarm and fault is deactivated in idle state of the keypad. A valid user PIN has to be entered. It is configurable if the power indication can be seen in idle state.

12.2.3 Viewing mode description

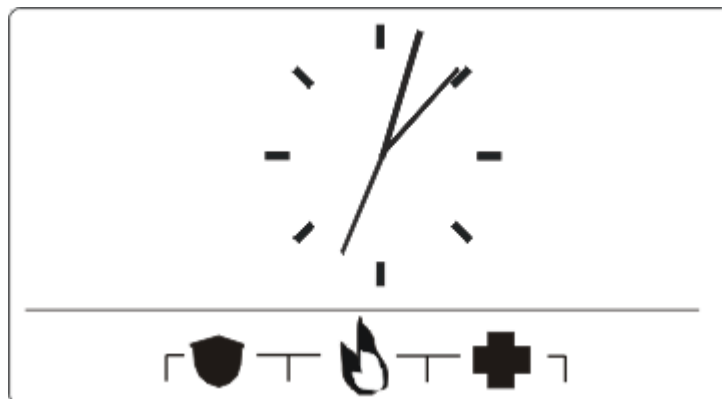
There are 2 viewing modes (automatic):

- Multi area view: User has access to several areas. Displaying the areas is done via area groups. If no area group is configured, only the general group “All my areas” is displayed.
- Single area view: The user has only rights for 1 area. In the single area view, only one area is displayed in large fonts and can be controlled directly.



	NOTICE
	The rights of a user can be restricted by the user settings or the settings of the keypad the user is logging in to. Only if the user and the keypad that is being used for logging in have the right for an area, the area is displayed. If the user has the right for several areas but the keypad has only the right for one area, the user will also see the single area view.

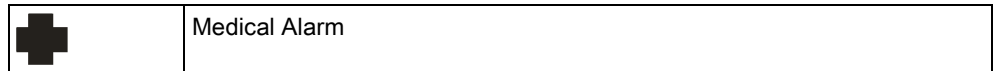
12.2.4 Function keys in idle state

Emergency Keys



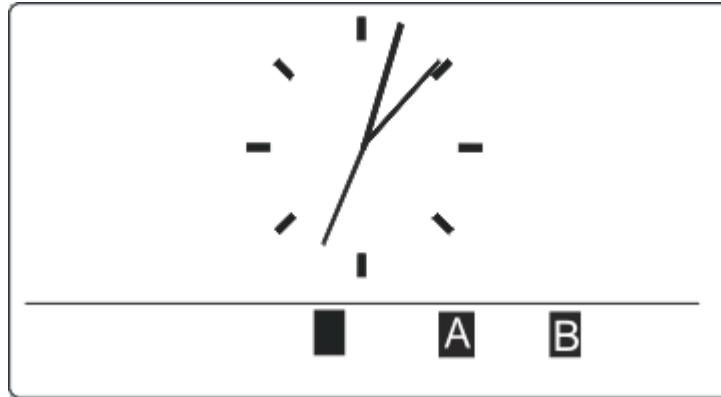
Depending on configuration, emergency keys are displayed. A simultaneous pressing of the keys activates an emergency call.

	Panic Alarm
	Fire alarm



The activated process depends on the system configuration. Please ask the installer for details.

Direct Settings



Depending on configuration, the direct set option is displayed. A forced set / part set without PIN is possible of the area the keypad is assigned to.

13 Software support tools

The following PC based software tools are available to remotely manage an SPC panel:

- **SPC Manager**
Enables the remote creation, control and modification of access based functionality within the SPC system.
- **SPC Safe**
Provides automated remote site administration of an SPC system.
- **SPC Remote Maintenance**
Provides automated remote monitoring and servicing of an SPC system.

14 Starting the system



⚠ CAUTION

The SPC system must be installed by an authorised installation engineer.

1. Wire the keypad to the X-BUS interface on the controller.
2. Enter Engineer Programming by entering the default Engineer PIN (1111). For more details, see Engineering PINs [→ 102].

14.1 Engineer modes

The SPC system works under 2 programming modes for authorised installation engineers: Full and Soft. In the browser, log off is only permitted in Soft Engineer mode.

Full Engineer Mode



All alerts, faults and tampers must first be isolated or cleared before exit from the Full Engineer mode is allowed.

Full Engineer mode provides extensive programming functionality. However, programming in Full Engineer mode disables all alarm settings, reports and output programming for the system. For full review of Full Engineer menu options, refer to page [→ 110].

[Soft] Engineer mode

Soft Engineer mode provides fewer programming functions and does not affect any outputs programmed in the system. For full review of [Soft] Engineer menu options, refer to page [→ 109].

14.1.1 Engineer PINs

The start up Engineer default programming PIN is '1111'.

If an installation is changed from Grade 2 to Grade 3 at any time after start-up, all PINs are prefixed with a 0. Therefore, the default Engineer PIN will be '01111'.

Increasing the number of digits for the PIN (see System Options [→ 222]) will add the relevant number of zeros to the front of an existing PIN (for example, 001111 for a 6 digit PIN).



NOTICE

If the default PIN 1111 is enabled, for example, a new SPC installation, you must change the engineer PIN at the panel. If you do not change your PIN, you will get an information message forcing you to change your default PIN before logging out of full engineer mode.

14.2 Programming tools

Keypad

The keypad provides quick onsite access to system menus and programming. The authorised installation engineer must set initial default configurations using the keypad. Programming of proximity card/device reader and assignment to users also must be done using the keypad.

SPC Pro

SPC Pro is a software application enabling you to configure SPC systems either online or offline. The SPC Pro programming tool provides additional advanced communication and X10 functionality not found on the keypad. Firmware upgrades can also be performed using SPC Pro.

SPC Pro supports USB, Serial, Ethernet and PSTN/GSM modem connectivity to an SPC controller.

14.2.1 Fast Programmer

The SPC Fast Programmer is a portable storage device that provides the engineer with the ability to upload and download configuration files in a quick and convenient manner. Fast Programmer can be used in conjunction with all of the above programming tools. For more details, see page [→ 311].

Fast Programmer may perform firmware upgrades.

14.3 Configuring start-up settings

The following start-up settings can be changed at a later time when programming the system functionality.



If powering up the panel the version number of the SPC system will be displayed on the keypad.

Prerequisite:

- ▷ To initialize the start-up configuration press the reset button on the PCB for at least 6 seconds.
- 1. Press a key on the keypad.
 - Press NEXT after each setting to move to the next setting.
- 2. Choose the LANGUAGE in which the configuration wizard will be displayed.
- 3. Choose the appropriate REGION.
 - EUROPE, SWEDEN SWITZERLAND, BELGIUM SPAIN UK IRELAND ITALY, , , , CANADA, USA
- 4. Choose a TYPE of installation:
 - DOMESTIC: is appropriate for home use (houses and apartments).
 - COMMERCIAL: provides additional zone types and commercial zone default descriptions for the first 8 zones.
 - FINANCIAL: is specific for banks and other financial institutions and includes features such as auto-setting, time locks, interlock groups and a seismic zone type.



For more details of default zone descriptions see Domestic, Commercial and Financial mode default settings [→ 336].

5. Choose the Security Grade of your installation.
6. LANGUAGE View the default languages available on the system. The following shows the default languages available for each region:
 - IRELAND/UK -English, French, German
 - EUROPE/SWITZERLAND/SPAIN/France/GERMANY – English, French, German, Italian, Spanish
 - BELGIUM – English, Dutch, Flemish, French, German
 - SWEDEN – English, Swedish, Danish, French, German



NOTICE

If the system is defaulted, and the REGION is changed on start up, only the languages that are currently on the system for the previous REGION will be available for the new REGION.

7. Select the languages you require for your installation. Selected languages are prefixed with an asterisk (*). To remove, or select, a language, press hash (#) on the keypad.
 - ⇒ The unselected languages are deleted from the system and will be unavailable if you default the system.
 - ⇒ To add other languages, refer to the sections on 'Upgrading Languages' for the keypad, browser and SPC pro.
8. Enter the DATE and TIME.
 - ⇒ The system scans the X-BUS for modems.
9. Enable SPC CONNECT to allow a panel to communicate with <https://www.spcconnect.com> once the panel IP address is configured.
10. Enable DHCP to automatically assign an available network IP address to the panel. If you've enabled SPC CONNECT and DHCP, an SPC CONNECT ATS is now added to the panel to complete the connection to <https://www.spcconnect.com>
11. For DHCP enabled panels, the automatically assigned IP address displays in the IP ADDRESS menu. If DHCP is not enabled, the default IP address displays. Choose SELECT to continue. In Engineer Programming mode, under COMMUNICATIONS, you must manually enter the static IP address for the panel.
12. Choose the X-BUS addressing mode:
 - MANUAL: is recommended for most installation types, especially when doing a preconfiguration.
 - AUTO: is recommended only for very small installations.
13. Choose the installation topology: LOOP (Ring) or SPUR (Chain).
 - ⇒ The system scans for the quantity of keypads, expanders, door controllers and available zone inputs.
14. Press NEXT to scan all X-BUS devices.

- ⇒ PROGRAMMING MODE will be displayed.
- ⇒ The Start-up setting is complete.

15. Check the alerts in the menu SYSTEM STATUS > ALERTS. Otherwise you will not be allowed to exit the Engineer Mode.
16. Configure the system by keypad, SPC Pro or web browser.

See also

- 📖 Domestic, Commercial and Financial mode default settings [→ 336]

14.4 Creating system users

By default the SPC system only allows engineer access on the system. The engineer must create Users to allow on-site personnel to set, unset, and perform basic operations on the system as required. Users are restricted to a set of panel operations by assigning them to specific User Profiles.

The system allows all user PINs within the allowed PIN range i.e. if a 4 digit PIN is used then all user PINs between 0000 and 9999 would be permissible.

Refer to the section on Adding Users:



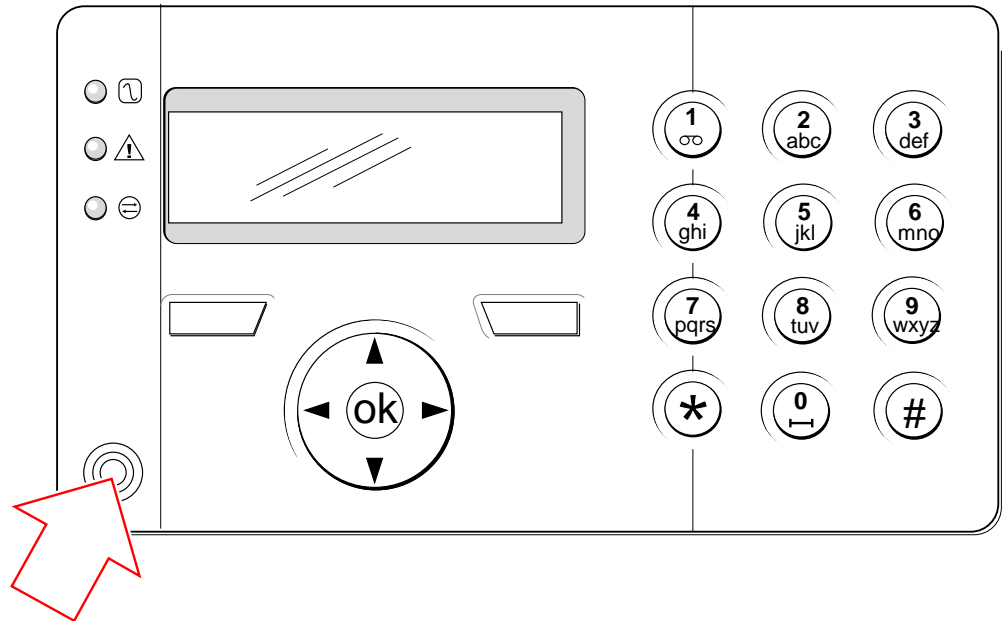
The ability to grant manufacturer access to the system (i.e. allow a firmware upgrade of the panel) is configured as a user right for a user profile. If a user is going to be enabling firmware upgrades, ensure that the user has the correct profile for this purpose.

See also

- 📖 Engineer PINs [→ 102]

14.5 Programming the portable ACE

The SPC keypad can be configured with a proximity card/device reader. Users whose profiles are configured as such may remotely set or unset the system, as well as conduct programming, depending on the level of profile. When a proximity device has been programmed on the keypad, the user has the ability to set or unset the system or enter the user programming by presenting the device within 1 cm of the receiver area on the keypad.



Receiver area on the keypad

To program a portable ACE on the keypad:

1. Enter the Engineer Programming PIN. (Default PIN is 1111. See Engineer PINs [→ 102])
2. Scroll to USERS.
3. Press SELECT.
4. Select EDIT and select USER1 from the list.
5. Scroll to PACE and press SELECT.
6. Toggle for ENABLE and DISABLE of the PACE functionality.
 - ⇒ The keypad flashes PRESENT PACE on the top line display.
7. Position the PACE fob within 1 cm of the receiver area on the keypad.
 - ⇒ The keypad indicates that the device has been registered by displaying PACE CONFIGURED.

To disable a portable ACE on the system:

1. Enter the Engineer Programming PIN. (Default PIN is 1111. See Engineering PINs [→ 102])
2. Scroll to USERS.
3. Press SELECT.
4. Select EDIT and select USER1 from the list.
5. Scroll to PACE and press SELECT.
6. Toggle to DISABLED.
 - ⇒ The keypad indicates UPDATED.

14.6 Configuring wireless fob devices

If an 868 MHz wireless receiver module is installed on the keypad or controller, a wireless fob device can be programmed via the keypad.

To program a wireless fob device on the system:

1. Enter the Engineer Programming PIN (Default PIN is 1111. See Engineering PINs [→ 102]).
2. Using the up/down arrow keys, scroll to the USERS option.
3. Press SELECT.
4. Select the EDIT option and press SELECT.
5. Scroll to the preferred user and press SELECT.
6. Scroll to the RF FOB option and press SELECT.
7. Toggle the setting to ENABLED and press SELECT.
⇒ The message PRESS KEY ON FOB flashes on the top line.
8. Position the fob to within 8 meters of the keypad and press one of the keys.
⇒ The message FOB CONFIGURED displays to indicate that the device has been registered.

To disable the wireless fob device on the system:

1. Enter the Engineer Programming PIN (Default PIN is 1111. See Engineering PINs [→ 102]).
2. Using the up/down arrow keys, scroll to the USERS option.
3. Select the EDIT option and press SELECT.
4. Scroll to the preferred user and press SELECT.
5. Scroll to the RF FOB option and press SELECT.
6. Toggle to DISABLED and press SAVE.



If no 868MHz wireless receiver is detected on the system, the RF FOB option is not displayed in the keypad menu.



Number of RF fobs per user: Only one fob device can be programmed for each user. To change fob devices among users, repeat the programming procedure for any new devices. Old fob devices become available for use by different users.

14.6.1 Clearing alerts using the fob

Alerts on the SPC system are normally cleared using the keypad RESTORE option. Clearing alerts can also be performed by using the wireless fob device.

If an active alert is displayed on the keypad when the system is UNSET, the alert can be cleared or restored by pressing the UNSET key on the wireless fob five seconds after the system has been unset.

To enable this functionality, the KEYFOB RESTORE option must be enabled in System Options:

1. Login to the keypad with an Engineer PIN.
2. Scroll to FULL ENGINEER > OPTIONS.
3. Press SELECT.
4. Scroll to KEYFOB RESTORE and press SELECT.

5. Toggle the setting to ENABLED and press SAVE.

15 Soft Engineer programming via the keypad

This section provides [Soft] Engineer programming options using the LCD keypad. For each menu option, the keypad must be in Engineer programming:

1. Enter a valid Engineer PIN (Default Engineer PIN is 1111. For more details, see Engineering PINs [→ 102]).
 2. Using the up/down arrow keys, scroll to the desired programming option.
 3. It is also possible to select a programming option using the keypad digits, enter the Engineer programming PIN plus the digit as shown in the table below.
- ⇒ If you change one of the programming options, the keypad displays UPDATED momentarily.

1	SETTING	Performs an Unset, Fullset or Partset on the system. See page
2	INHIBIT	Displays a list of the Inhibited zones on the system. See page
3	ISOLATE	Allows the engineer to isolate zones on the system. See page [→ 149]
4	EVENT LOG	Displays a list of the most recent events on the system. See page [→ 149]
5	ACCESS LOG	Displays a list of the most recent access to the system. See page
6	ALARM LOG	Displays a list of recent alarms.
7	CHANGE ENG PIN	Allows the engineer to change the Engineer PIN. See page [→ 150]
8	USERS	Allows the engineer to add, edit or delete users. See page [→ 150]
9	SMS	Allows the user to add, edit or delete SMS details for users.. See SMS [→ 155]

See also

- 📖 TEST [→ 145]
- 📖 DOOR CONTROL [→ 157]
- 📖 Engineer programming via the keypad [→ 110]
- 📖 INSTALLER TEXT [→ 157]
- 📖 SET DATE/TIME [→ 157]
- 📖 SMS [→ 155]

16 Engineer programming via the keypad

This section provides [Full] Engineer programming options using the LCD keypad. For each menu option, the keypad must be in Full Engineer programming:

1. Enter a valid Engineer PIN (Default Engineer PIN is 1111. For more details, see Engineering PINs [→ 102]).
 2. Press SELECT for FULL ENGINEER programming.
 3. Using the up/down arrow keys, scroll to the desired programming option.
 4. A quick select function is implemented. Press # to select a parameter (e.g. a zone attribute). The selected parameter is displayed with a * (e.g. *Inhibit).
- ⇒ Upon completion of the programming options, the keypad displays UPDATED momentarily.

16.1 System Status

The System Status feature displays all faults on the system.

To view these faults:

1. Scroll to SYSTEM STATUS.
 2. Press SELECT.
- ⇒ The status of the following items is displayed.
- ⇒ Click on each item to display further details.

OPEN ZONES	Displays all open zones.
ALERTS	Displays current alerts on the system.
SOAK	Displays all zones on soak test.
ISOLATIONS	Displays zones that are isolated.
FAIL TO SET	Displays all areas that have failed to set. Select each area to display details of why the area failed to set.
BATTERY	Displays remaining battery time, voltage and current of battery. You must enter the Battery capacity and Max current values in OPTIONS to view the remaining battery time on the keypad in the event of mains failure. This is indicated under the STATUS - BATTERY - BATT TIME menu. This menu also indicates if there is a battery fault.
AUX	Displays voltage and current of auxiliary power.



NOTICE

Users cannot exit from FULL ENGINEER programming if any fault conditions exist. The first fault will display on the keypad when you attempt to leave engineer mode. You can view and isolate all faults within the System Status menu under Alerts and Open Zones.

16.2 Options

1. Scroll to OPTIONS and press SELECT.
2. Scroll to the desired programming option:
 - ⇒ The programming options displayed in the OPTIONS menu vary depending on the security grade of the system (see right column)



▲ WARNING

To change the region on your panel, it is strongly recommended that you default your panel and select a new region as part of the start up wizard.

Variable	Description	Default
SECURITY GRADE	<p>Determines the Security Grade of the SPC Installation.</p> <ul style="list-style-type: none"> ● Irish and European Regions: <ul style="list-style-type: none"> – EN50131 Grade 2 – EN50131 Grade 3 – Unrestricted ● UK Region: <ul style="list-style-type: none"> – PD6662 (EN50131 Grade 2 based) – PD6662 (EN50131 Grade 3 based) – Unrestricted ● Swedish Region: <ul style="list-style-type: none"> – SSF1014:3 Larmclass 1 – SSF1014:3 Larmclass 2 – Unrestricted ● Belgium Region: <ul style="list-style-type: none"> – TO-14 (EN50131 Grade 2 based) – TO-14 (EN50131 Grade 3 based) – Unrestricted ● Switzerland Region: <ul style="list-style-type: none"> – SWISSI Cat 1 – SWISSI Cat 2 – Unrestricted ● Spanish Region <ul style="list-style-type: none"> – EN50131 Grade 2 – EN50131 Grade 3 ● German Region <ul style="list-style-type: none"> – VdS Class A – VdS Class C – Unrestricted ● France <ul style="list-style-type: none"> – NFtyp2 – NFtyp3 – Unrestricted 	Grade: 2 Country: n/a
REGION	Determines the specific regional requirements that the installation complies with. Options are UK, IRELAND, EUROPE, SWEDEN, SWITZERLAND, BELGIUM, GERMANY and FRANCE	
APPLICATION	Determines whether SPC is being installed for use in a commercial business or a private residence. Choose between COMMERCIAL (see page [→ 321]), DOMESTIC (see page [→ 320]) or FINANCIAL.	Domestic

Refer to the section System Options [→ 222] for more details of the following OPTIONS.

PARTSET A	RENAME TIMED ACCESS to E/EXIT E/EXIT to ALARM LOCAL
PARTSET B	RENAME TIMED ACCESS to E/EXIT E/EXIT to ALARM LOCAL
CALL ARC MESSAGE	DISPLAY MESSAGE (ENABLED/DISABLED)
CONFIRMATION	VDS DD243: GARDA EN50131-9
CONFIRM ZONES	Select NO. OF ZONES.
AUTO RESTORE	ENABLED/DISABLED
KEYFOB RESTORE	ENABLED/DISABLED
USER DURESS	DISABLED PIN +1 PIN +2
RETRIGGER BELL	ENABLED/DISABLED
BELL ON 1ST	ENABLED/DISABLED
BELL ON FTS	ENABLED/DISABLED
STROBE ON FTS	ENABLED/DISABLED
ALARM ON EXIT	ENABLED/DISABLED Only available in ENGINEER CONFIG mode as setting is not in accordance with EN50131.
LANGUAGE	SYSTEM LANGUAGE IDLE STATE :LANGUAGE
PIN DIGITS	4 DIGITS 5 DIGITS 6 DIGITS 7 DIGITS 8 DIGITS
CODED RESTORE	ENABLED/DISABLED
WEB ACCESS	ENABLED/DISABLED Allows/restricts access to the web browser.
OPEN ZONES	ENABLED/DISABLED
ALLOW ENGINEER	ENABLED/DISABLED
ALLOW MANUFACT. *	ENABLED/DISABLED
SHOW STATE	ENABLED/DISABLED
EOL RESISTANCE	NONE

	SINGLE 1K SINGLE 1K5 SINGLE 2K2 SINGLE 4K7 SINGLE 10K SINGLE 12K DUAL 1K / 470R DUAL 1K / 1K DUAL 2K2 / 1K0 DUAL 2K2 / 1K5 DUAL 2K2 / 2K2 DUAL 2K2 / 4K7 DUAL 2K7 / 8K2 DUAL 2K2/ 10K DUAL 3K0 / 3K0 DUAL 3K3 / 3K3 DUAL 3K9 / 8K2 DUAL 4K7 / 2K2 DUAL 4K7 / 4K7 DUAL 5K6 / 5K6 DUAL 6K8 / 4K7 DUAL 10K / 10K MASK_1K_1K_6K8 MASK_1K_1K_2K2 MASK_4K7_4K7_2K2
SMS AUTH MODE	PIN ONLY CALLER ID ONLY PIN + CALLER ID SMS PIN ONLY SMS PIN + CALLER ID
PACE AND PIN	ENABLED/DISABLED
RESTORE ON UNSET	ENABLED/DISABLED Note: To comply with PD6662, you must disable this option.
ENGINEER RESTORE	ENABLED/DISABLED
OFFLINE TAMPER	ENABLED/DISABLED
ENGINEER LOCK	ENABLED/DISABLED If enabled, system cannot be reset using yellow button on controller unless an Engineer PIN is input on the keypad.
SECURE PIN	ENABLED/DISABLED
CLOCK SETTINGS	AUTOMATIC DST MAINS TIME SYNC
SUSPICION AUDIBLE	ENABLED/DISABLED
SHOW CAMERAS	ENABLED/DISABLED
SEIS TEST ON SET	ENABLED/DISABLED
ALERT FORBID SET	ENABLED/DISABLED
ANTIMASK SET	DISABLED TAMPER FAULT ALARM
ANTIMASK UNSET	DISABLED TAMPER FAULT ALARM

RETRIGGER DURESS	ENABLED/DISABLED
RETRIGGER PANIC	ENABLED/DISABLED
SILENCE AUD VER.	ENABLED/DISABLED
ENGINEER EXIT	ENABLED/DISABLED

* Not available for SPC42xx, SPC43xx.

16.3 Timers

1. Scroll to TIMERS and press SELECT.
2. Scroll to the desired programming option:


Timers

Designation of the functions in the following order:

- 1st row: Web/SPC Pro
- 2nd row: Keypad

Timer	Description	Default
Audible		
Internal Bells INT BELL TIME	Duration that internal sounders will sound when alarm is activated. (1 – 15 minutes; 0 = never))	15 min.
External Bells EXT BELL TIME	Duration that external sounders will sound when alarm is activated. (1 – 15 minutes; 0 = never)	15 min.
External Bell Delay EXT BELL DELAY	This will cause a delayed activation of the external bell. (0 – 600 seconds)	0 sec.
Chime CHIME TIME	Number of seconds that a chime output will activate, when a zone with chime attribute opens. (1 – 10 seconds)	2 sec.
Confirmation		
Confirm CONFIRM TIME	<ul style="list-style-type: none"> ● Note: Only available when Security Grade is 'Unrestricted' and 'DD243' is selected for 'Confirmation' variable. (See System Options [→ 222]) This timer applies to the alarm confirmation feature and is defined as the maximum time between alarms from two different non overlapping zones that will cause a confirmed alarm. (30 – 60 minutes)	30 min.
Confirmed holdup	This timer applies to the confirmed holdup feature and is defined as the maximum time between alarms from two different non-overlapping zones that will cause a confirmed alarm. (480 - 1200 minutes)	480 min.
Dialer Delay DIALER DELAY	When programmed, the dialler delay initiates a predefined delay period (0 -30 seconds) before the system dials out to an Alarm Receiving Centre (ARC). This is specifically designed to reduce unwarranted responses from Alarm Receiving Centres and the constabulary. In the event of a subsequent zone being tripped the dialler delay period is ignored and the dialler dials out immediately. (0 – 30 seconds)	30 sec.
Alarm abort ALARM ABORT	Time after a reported alarm in which an alarm abort message can be reported. (0 – 999 seconds))	30 sec.
Setting		
Setting Authorisation SETTING AUTH	Period for which Setting Authorisation is valid. Enter a value between 10 and 250 seconds.	20 secs
Final Exit	The Final Exit time is the number of seconds that arming is delayed after a zone programmed with the final exit attribute	7 sec.

Timer	Description	Default
FINAL EXIT	is closed. (1 – 45 seconds)	
Bell on Fullset FULLSET BELL	Activates the external bell momentarily to indicate a full set condition. (0 – 10 seconds)	0 sec.
Strobe on Fullset FULLSET STROBE	Activates the strobe on the external bell momentarily to indicate a full set condition. (0 – 10 seconds)	0 sec.
Fail To Set FAIL TO SET	Number of seconds to display fail to set message on keypads (0 until valid PIN is entered). (0 – 999 seconds)	10 sec.
Alarm		
Double Knock DKNOCK DELAY	The maximum delay between activation's of zones with the double attribute, which will cause an alarm. (1 – 99 seconds)	10 sec.
Soak SOAK DAYS	The number of days a zone remains under soak test before it automatically returns to normal operation. (1 – 99 days)	14 days
Seismic Test Interval SEISMIC AUTOTEST	The average period between seismic sensor automatic tests (12 – 240 hours) Note: To enable automatic testing, the Automatic Sensor Test attribute must be enabled for a seismic zone.	168 hours.
Seismic Test Duration SEISMIC TEST DUR	Maximum time (in seconds) that a seismic sensor takes to trigger an alarm in response to the 'Seismic Test' output. (3 - 120 seconds)	30 sec.
Lockout Post Alarm LOCKOUT POST ALARM	Duration after alarm that access will be denied.	0 mins
External Bell Strobe STROBE TIME	Duration that the strobe output will be active when an alarm is activated. (1 – 15 minutes; 0 = indefinitely)	15 min.
Alerts		
Mains Delay MAINS SIG DELAY	The time after a mains fault has been detected before an alert is activated by the system. (0 – 60 minutes)	0 min.
Engineer		
Engineer Access ENGINEER ACCESS	The timer for the Engineer access starts as soon as the user enables the Engineer Access. (0 – 999 minutes. '0' indicates no time limitation for system access)	0 min.
Engineer auto log out ENG AUTO LOG OUT	Duration of inactivity after which the engineer will be automatically locked out	0 mins.
Keypad		
Keypad Timeout KEYPAD TIMEOUT	The number of seconds that an RKD will wait for key entry before it leaves the current menu. (10 – 300 seconds)	30 sec.
Keypad Language KEYPAD LANGUAGE	The duration a keypad will wait in idle before switching language to default (0 - 9999 seconds; 0 = never).	10 secs
Fire		
Fire Pre-alarm FIRE PRE-ALARM	Number of seconds to wait before reporting fire alarm for zones with 'Fire pre-alarm' attribute set. (1 – 999 seconds) See Editing a Zone [→ 237].	30 sec.
Fire recognition FIRE RECOGNITION	Extra time to wait before reporting file alarm for zones with 'Fire pre-alarm' and 'Fire Recognition' attributes set. (1 – 999 seconds). See Editing a Zone [→ 237].	120 sec.
PIN		
PIN Valid PIN VALID	Period for which pin is valid in days (1 - 330)	30 days
PIN Changes Limit PIN CHANGES LIMIT	Number of changes within a valid period (1 - 50)	5
PIN Warning PIN WARN	Time before PIN expiry after which a warning will be displayed (1 - 14)	5 days

Timer	Description	Default
General Settings		
RF Output Time RF OUTPUT	The time that the RF output will remain active on the system. (0 – 999 seconds)	0 sec.
Time Sync Limit TIME SYNC LIMIT	Time limit within which no event will be reported. (0 – 999 secs) Time synchronization only takes place if system time and update time are outside this limit.	0 sec.
Link Timeout LINK TIMEOUT	Timeout for Ethernet link fault (0 = Disabled) (0 - 250)	0 secs
Camera Offline CAMERA OFFLINE	Time for camera to go offline (10 - 9999)	10 secs
Tech. delay TECH. DELAY	Number of seconds to delay triggering of tech. zones with tech. delay attribute. (0 – 9999 seconds)	0 sec.
Frequent FREQUENT 	This attribute only applies to Remote Maintenance. The number of hours a zone must open within if the zone is programmed with the Frequent use attribute. (1 – 9999 hours)	336 hours (2 weeks)
Duress silent	Time when duress will remain silent and not restorable from keypad (0 - 999).	0 Minutes
Holdup/panic silent	Number of minutes that a holdup/panic will remain silent and cannot be restored from the keypad (0 - 999).	0 Minutes



Default times are dependent upon the Engineer configuration. The default times denoted may or may not be allowable and is dependent on the configuration by the engineer

16.4 Areas

1. Scroll to AREAS and press SELECT.
2. Scroll to the desired programming option:

ADD	For Domestic and Commercial Mode, the area type defaults to Standard. In Financial Mode, select area type STANDARD, ATM, VAULT or ADVANCED. Enter the name of the area and the preferred entry/exit time.
EDIT	Edit the following settings: <ul style="list-style-type: none"> ● DESCRIPTION ● ENTRY EXIT <ul style="list-style-type: none"> - ENTRY TIMER - EXIT TIMER - NO EXIT TIMER - FOB ENTRY ACTIVE ● PARTSET A/B <ul style="list-style-type: none"> - ENABLED/DISABLED - TIMED - ACCESS TO E/EXIT - E/EXIT TO ALARM - LOCAL - NO BELLS

	<ul style="list-style-type: none"> ● LINKED AREAS <ul style="list-style-type: none"> - AREA - FULLSET - FULLSET ALL - PREVENT FULLSET - PREVENT FULLSET ALL - UNSET - UNSET ALL - PREVENT UNSET - PREVENT UNSET ALL ● SCHEDULE <ul style="list-style-type: none"> - CALENDAR - AUTOMATIC SET/UNSET - TIME LOCKED - VAULT ACCESS ● REPORTING <ul style="list-style-type: none"> - EARLY TO SET - LATE TO SET - EARLY TO UNSET - LATE TO UNSET ● SET/UNSET <ul style="list-style-type: none"> - AUTO SET WARNING - AUTO SET CANCEL - AUTO SET DELAY - KEYSWITCH - DELAY INTERVAL - DELAY COUNTER - DELAYED UNSET - UNSET DURATION - INTERLOCK - DUAL PIN ● RF OUTPUT
DELETE	Select the area to be deleted.

See Adding / Editing an area [-> 238] for further details on these options.

16.5 Area Groups

1. Scroll to AREA GROUPS and press SELECT.
2. Scroll to the desired programming option:

ADD	Enter the name of the area group.
EDIT	GROUP NAME - Rename the group as required. AREAS - Scroll to an area and select it. Choose ENABLED or DISABLED as required to add it or remove it from the group. An asterisk (*) indicates if an area is part of the group.
DELETE	Select the area to be deleted.

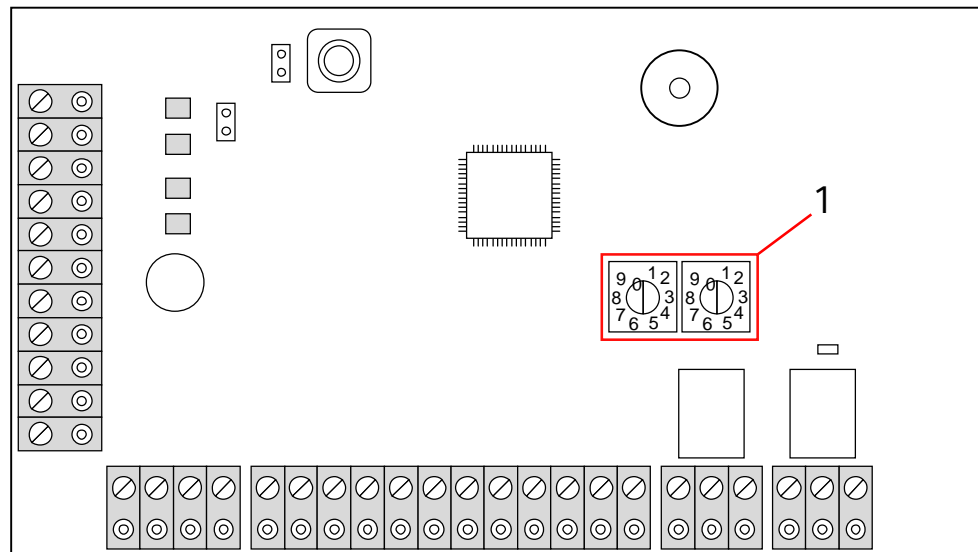
16.6 X-BUS

1. Scroll to XBUS and press SELECT.
2. Scroll to the desired programming options as shown below.

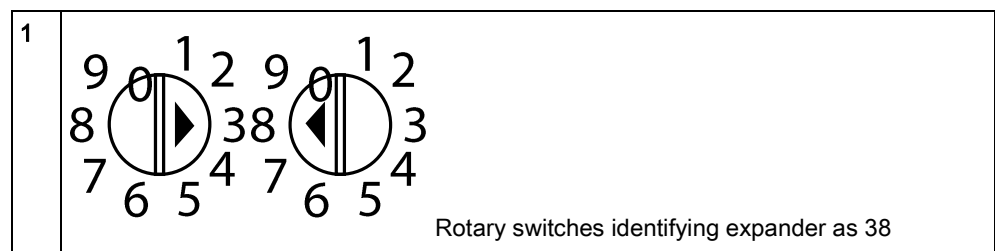
16.6.1 X-BUS Addressing

Expanders, keypads and subsequent zones may be configured, located and monitored, with the steps provided in this section. X-BUS settings such as type, communication times and retries are also accessed within this menu.

The figure below shows each rotary switch with an arrow symbol pointing to a number for identification (i.e. 3, 8). The right switch is the first unit digit and the left switch is the 10s digit. The expander in the figure below is identified as 38.



Rotary switches



For a system with automatic addressing, expanders and keypads belong to the same numbering sequence. E.g. expanders and keypads are automatically numbered 01, 02, 03, etc., by the controller in the order in which they are detected, e.g. its relevant location to controller. In this configuration, zones are allocated to each input expander.



Automatically addressed expanders are not supported by SPC41xx.

16.6.2 XBUS Refresh

The X-Bus Refresh utility performs a discovery of the current status of the X-Bus and displays the current X-Bus configuration.

To refresh the X-Bus status:

1. Scroll to XBUS REFRESH.
2. Press SELECT.
 - ⇒ The number of online keypads is displayed.
3. Press the right soft key on the keypad after each display to view expanders, zones and offline items.
4. Press this key again to exit.



Refresh makes no changes to the system, but is useful for detecting system faults, such as loose connections, or inactive expanders, before performing a **Reconfigure**.

16.6.3 Reconfigure



NOTICE

A reconfigure only applies to wired zones on an expander. Wireless zones on an expander and controller zones will not be brought online after a reconfigure. To bring controller zones online, you must apply a zone type other than 'Unused' using the zones menu on the keypad or web browser.

If the system has a mixture of expander types (with and without rotary switches) then the system can only be automatically reconfigured. If the system has all expanders with rotary switches, the system can still be automatically reconfigured and the system will ignore the rotary switches and auto addresses all the expanders on the system.



It is recommended that you perform a **Refresh** before a **Reconfigure**.

To reconfigure keypads/expanders:

1. Scroll to RECONFIGURE.
2. Press SELECT.
 - ⇒ The number of online keypads is displayed.
3. Press NEXT.
 - ⇒ The number of online expanders is displayed.
4. Press NEXT
 - ⇒ The number of online zones is displayed.
5. Press BACK to exit.

16.6.4 Keypads/Expanders/Door Controllers



NOTICE

You must upgrade to version 1.1 of firmware before adding door controllers. With earlier firmware versions, the door controllers are seen by the panel as normal I/O expanders and doors must be added manually.

16.6.4.1 Locate

To locate a keypad/expander/door controller:

1. Scroll to KEYPADS, EXPANDER or DOOR CONTROLLER and press SELECT.
2. Scroll to LOCATE and press SELECT.
3. Scroll to the expander/keypad/door controller to be located and press SELECT.
 - ⇒ The selected device beeps and the LED flashes allowing Engineer to locate it.
4. Press BACK to exit.
 - ⇒ Locate keypads using the same menus and following the keypad choice instead of expander.

16.6.4.2 Monitor

To obtain an overview of the keypads/expanders/door controller connected to the system:

1. Scroll to KEYPADS, EXPANDER or DOOR CONTROLLER and press SELECT.
2. Scroll to MONITOR and press SELECT.
3. Scroll to desired Monitor programming option.
4. Press SELECT.
 - ⇒ A list of detected keypads/expanders is displayed.
5. Scroll through the list and press SELECT on preferred expander/keypad/door controller.
 - ⇒ Parameters and details, if applicable, are displayed for editing as shown in the table below.
6. Press BACK to exit.

STATUS	Online or offline
S/N	Serial number (used to track and identify)
VER	Firmware version
POWER	Power parameters: real-time voltage and current readings
ADDRESS INFO	The addressing mode and the address of the keypad\expander\door controller.
AUX FUSE	The status of the auxiliary fuse on the expander\door controller

PSU	The type and status of the PSU. (PSU expanders only) Scroll to display the voltage and current load on the outputs, the battery status. The Mode Link option is also available, which shows the jumper setting on the panel for the Ah setting. 7Ah and 17Ah are the available options. (This jumper is not present on the 5350 or 6350 models) If you are using the SPC 5360 or 6350, this menu displays the battery status, and the status of the fuses on the outputs.
BATTERY	Battery voltage: battery voltage level (PSU expanders only)
INPUT STATE	State of each zone input associated with an expander as follows: C: Closed, O: Open, D; Disconnected, S: Short (Expanders with inputs only)

16.6.4.3 Edit Keypads

To edit keypads:

1. Scroll to KEYPADS > EDIT.
2. Press SELECT.
3. Scroll to the device to be edited and press SELECT.
 - ⇒ The configuration settings for a standard keypad and comfort keypad are described in the sections below.
4. Press BACK to exit the menu.

LCD Keypad Settings

Configure the following settings for the keypad.

Description	Enter a unique description to identify the keypad.
Function Keys (in idle state)	
Panic	Select Enable, Disable or Enabled Silent. If enabled, panic alarm is activated by pressing the 2 soft keys together.
Verification	If you assign a verification zone to the keypad, when a panic alarm is triggered by pressing 2 soft keys together or by entering a duress code, audio and video events are activated.
Visual Indications	
Backlight	Select when keypad backlight is on. Options are: - On after key is pressed; Always on; Always off..
Indicators	Enable or disable the LED's on the keypad.
Setting state	Select if setting state should be indicated in idle mode.
Audible Indications	
Buzzer	Enable or disable the buzzer on the keypad.
Partset Buzzer	Enable or disable buzzer during exit time on Partset.
Keypress	Select if the speaker volume for the key presses should be activated.
Deactivation	
Calendar	Select if the keypad should be limited by calendar. See Calendar [→ 251].
Mapping gate	Select if keypad should be limited by a mapping gate.
Keyswitch	Select if keypad should be limited by a keyswitch.
PACE Entry	Tick this box to disable the keys on the keypad during the entry time when a PACE is configured on the keypad.
Areas	
Location	Select the secured area where the keypad is located.
Areas	Select which areas can be controlled through keypad.
Options	

Delay Fullset	Select to configure a delayed set across all keypads. The location of the keypad is ignored and all areas will perform a full exit time count down.
---------------	---

**NOTICE**


An area should be assigned to a keypad only if the keypad is inside the assigned area, and if an entry/exit route is defined. If an area is assigned, when the particular area is set or unset then entry and exit timers are used (if configured). Other features related to entry/exit routes also become available. If no area is assigned, the area is set or unset immediately and other entry/exit features are not available

Comfort Keypad Settings

Configure the following settings for the comfort keypad.

Description	Enter a unique description to identify the keypad.
Function Keys (in idle state)	
Panic	Select Enable, Disable or Enabled Silent. If enabled, panic alarm is activated by pressing F1 and F2 soft keys together.
Fire	Enable to allow fire alarm to be activated by pressing F2 and F3 soft keys together.
Medical	Enable to allow medical alarm to be activated by pressing F3 and F4 soft keys together.
Fullset	Enable to allow Fullset to be activated by pressing F2 key twice.
Partset A	Enable to allow Partset A to be activated by pressing F3 key twice.
Partset B	Enable to allow Partset B to be activated by pressing F4 key twice.
Verification	If you assign a verification zone to the comfort keypad, when a Medical, Panic or Fire event is triggered, or if a user enters a duress code, then audio and video events are activated.
Visual indications	
Backlight	Select when keypad backlight is on. Options are: - On after key is pressed; Always on; Always off.
Backlight Level	Select the intensity of illumination of the backlight. Range 1 - 8 (High).
Indicators	Enable or disable the LED's on the keypad.
Setting state	Enable if setting state should be indicated in idle mode. (LED)
Logo	Enable if logo should be visible in idle mode.
Analog Clock	Select position of clock if visible in idle mode. Options are Left Aligned, Center Aligned, Right Aligned or Disabled.
Emergency	Enable if Panic, Fire and Medical function keys should be indicated in the LCD display.
Direct Set	Enable if Fullset/Partset function keys should be indicated in the LCD display.
Audible indications	
Alarms	Select speaker volume for alarm indications or disable sound.
Entry/Exit	Range is 0 – 7 (Max volume)
Chime	Select speaker volume for entry & exit indications or disable sound.

Keypress	Range is 0 – 7 (Max volume)
Voice Annunciation	Select speaker volume for chime or disable sound.
Partset Buzzer	Range is 0 – 7 (Max volume)
Deactivation	
Calendar	Select if the keypad should be limited by calendar. See Calendar.
Mapping gate	Select if keypad should be limited by a mapping gate.
Keyswitch	Select if keypad should be limited by a keyswitch.
PACE Entry	Tick this box to disable the keys on the keypad during the entry time when a PACE is configured on the keypad.
Areas	
Location	Select the secured area where the keypad is located.
Areas	Select which areas can be controlled through keypad.
Options	
Delay Fullset	Select to configure a delayed set across all keypads. The location of the keypad is ignored and all areas will perform a full exit time count down.

	NOTICE
	An area should be assigned to a keypad only if the keypad is inside the assigned area, and if an entry/exit route is defined. If an area is assigned, when the particular area is set or unset then entry and exit timers are used (if configured). Other features related to entry/exit routes also become available. If no area is assigned, the area is set or unset immediately and other entry/exit features are not available.

16.6.4.4 Edit Expanders

To edit expanders:

1. Scroll to EXPANDERS > EDIT.
2. Press SELECT.
3. Scroll to the device to be edited and press SELECT.
 - ⇒ Parameters and details, if applicable, are displayed for editing.
4. Press BACK to exit the menu.



For naming and identifying, expanders are allocated zones (in groupings of 8) with subsequent identities of 1 to 512. (The greatest number in zone identification is 512.) Therefore, any expander named or identified by a number greater than 63 has no allocated zones.

16.6.4.4.1 Editing IO Expanders

The following table lists the available options for IO expanders:

Function	Description
Description	Edit the description of the expander.

16.6.4.4.2 Editing Audio Expanders

The following table lists the options available in the **Edit** menu for Audio Expanders:

Name	Description
DESCRIPTION	Enter or edit a description for the audio expander.
INPUT	Select the zone's input.
VOLUME LIMIT	Select the volume limit.

16.6.4.4.3 Editing Wireless Expanders

The following table lists the available options for Wireless expanders:

Function	Description
Description	Edit the description of the expander.

16.6.4.4.4 Editing Analysed IO Expanders

The following table lists the available options for IOA expanders:

Name	Description
Description	Edit the description of the expander.

16.6.4.4.5 Editing Indicator Expander Modules

The following table lists the available options for Indicator Expander modules:

Name	Description
DESCRIPTION	Enter or edit a description for the expander.
LOCATION	Select a location for the expander from the list of available areas.
FUNCTION KEYS	Enables you to assign behaviour to specific keys for specific areas. Select an area and assign one of the following options to that area: <ul style="list-style-type: none"> ● None

Name	Description
	<ul style="list-style-type: none"> ● Unset ● Partset A ● Partset B ● Fullset ● Toggle Unset/Fullset ● Toggle Unset/Partset A ● Toggle Unset/Partset B ● All Okay ● Setting Authorisation
VISUAL INDICATIONS (Flexible Mode only)	Enables you to assign specific behaviour to each LED on the indicator module. Each of the LEDs has the following options: <ul style="list-style-type: none"> ● FUNCTION — the following options are available: <ul style="list-style-type: none"> – KEYSWITCH — select a keyswitch and the position of the key. – DISABLED — select to disable the LED. – SYSTEM — select the alarm type which triggers the LED. – AREA — select the area which triggers the LED. – ZONE — select the zone which triggers the LED – DOOR — select the door and the door option which triggers the LED. ● ON – COLOR — specify the activation colour ● ON – FLASH — specify the behaviour of the LED in active state. Available options are: <ul style="list-style-type: none"> – Permanent — always on. – Flash Fast\Medium\Slow — varying speed of the flashing. ● OFF – COLOR — specify the deactivation colour. ● OFF – FLASH — specify the behaviour of the LED in the inactive state. Available options are: <ul style="list-style-type: none"> – Permanent — always on. – Flash Fast\Medium\Slow — varying speed of the flashing.
LED ALWAYS	Enable if LED indicators remain active when keys are deactivated.
AUDIBLE IND. (Flexible Mode only)	Select the audible indicators for alarms, entry/exit, and keypresses,
DEACTIVATION (Flexible Mode only)	Choose one, or more, of the following deactivation options: <ul style="list-style-type: none"> ● Calendar – select a calendar from the available options. ● Keyswitch – select a keyswitch from the available options. ● Keypad - select a keypad from the available options. ● Card Reader – enable or disable deactivation using a keypad.
MODE	Select Linked or Flexible. Linked mode reduces the number of options available in the Expander Edit menu.
INPUT	Select the zone

16.6.4.4.6 Editing Keyswitch Expanders

The following table lists the available options for keyswitch expanders:

Name	Description
DESCRIPTION	Enter or edit a description for the expander.
LOCATION	Select a location for the expander from the list of defined areas.
LATCH	Enable or disable the latch on the key position.
VISUAL INDICATIONS (Flexible mode only)	<p>Enables you to assign specific behaviour to each LED on the keyswitch expander. Each of the LEDs has the following options:</p> <ul style="list-style-type: none"> ● FUNCTION — the following options are available: <ul style="list-style-type: none"> – KEYSWITCH — select a keyswitch and the position of the key. – DISABLED — select to disable the LED. – SYSTEM — select the alarm type which triggers the LED. – AREA — select the area which triggers the LED. – ZONE — select the zone which triggers the LED – DOOR — select the door and the door option which triggers the LED. ● ON – COLOR — specify the activation colour ● ON – FLASH — specify the behaviour of the LED in active state. Available options are: <ul style="list-style-type: none"> – Permanent — always on. – Flash Fast\Medium\Slow — varying speed of the flashing. ● OFF – COLOR — specify the deactivation colour. ● OFF – FLASH — specify the behaviour of the LED in the inactive state. Available options are: <ul style="list-style-type: none"> – Permanent — always on. – Flash Fast\Medium\Slow — varying speed of the flashing.
DEACTIVATION (Flexible mode only)	<p>Select a deactivation method from the available options:</p> <ul style="list-style-type: none"> ● Calendar — select a calendar.
KEY POSITIONS	<p>Enables you to assign behaviour to specific key positions for specific areas.</p> <p>Select an area for the key position, and assign one of the following options to that area:</p> <ul style="list-style-type: none"> ● None ● Unset ● Partset A ● Partset B ● Fullset ● Toggle Unset/Fullset ● Toggle Unset/Partset A ● Toggle Unset/Partset B ● All Okay ● Setting Authorisation

16.6.4.5 Edit Door Controllers

For further information about Door controller see page [→ 71].

1. Scroll to DOOR CONTROLLERS > EDIT.
 2. Press SELECT.
 3. Scroll to the device to be edited and press SELECT.
- ⇒ Parameters and details, if applicable, are displayed for editing as shown in the table below.

DESCRIPTION	Name of the door controller
DOORS	Configuration of Door I/O 1 & Door I/O 2.
READERS	Configuration of Reader Profiles

To edit a DOOR I/O:

1. Scroll to DOORS.
 2. Press SELECT.
 3. Scroll to the DOOR I/O to be edited and press SELECT.
- ⇒ Parameters and details, if applicable, are displayed for editing as shown in the table below.

ZONES	No access functionality is realized. The inputs and outputs can be used normally.
DOOR 1 – DOOR 64	The selected door number is assigned to the DOOR I/O.

If the option “ZONES” is selected for a DOOR I/O the two inputs of this door I/O must be configured:

To edit the two zones of a DOOR I/O:

1. Scroll to the DOOR I/O to be edited and press SELECT
⇒ The option “Zones” is selected.
 2. Press SELECT.
 3. Select which Zone should be edited (DPS or DRS zone).
 4. Press SELECT.
- ⇒ Parameters and details, if applicable, are displayed for editing as shown in the table below.

UNASSIGNED	This zone is not assigned and can not be used.
ZONE 1 – ZONE 512	The zone which is edited is assigned to this zone number. If the zone is assigned to a specific zone number, it can be configured like a normal zone.



The zones can be assigned to each free zone number. But the assignment is not fixed. If the zone was assigned to zone number 9 and an input expander with the address 1 is connected to the X-Bus (which is using the zone numbers 9-16) the assigned zone from the two door controller will be moved to the next free zone number. The configuration will be adapted accordingly.

To edit a READER PROFILE:

1. Scroll to READERS.
 2. Press SELECT.
 3. Scroll to the READER to be edited and press SELECT.
- ⇒ Select any of the following profiles for the reader:

1	For readers with a green and a red LED.
2	For VANDERBILT readers with a yellow LED (AR618X).
3	Profile 3 is used with HID readers that send a PIN to the panel as a card reading with a predefined site code (0)
4	Profile 4 is used with HID readers that send a PIN to the panel as a card reading with a predefined site code (255).
5	Select to enable Sesam readers. For VdS compliance, ensure you select the Override Reader Profile option on the browser to provide feedback on the setting process.

See also

 Door Expander [→ 71]

16.6.5 Addressing Mode

X-BUS addressing can be configured in one of the 2 following ways:

Automatic addressing

rotary switch expanders. With automatic addressing, the controller over-rides rotary switches and automatically assigns expanders and keypads in the system unique IDs in sequential order

Manual addressing

Manual addressing allows manual determination of each expander/keypad ID in a system. All devices should be installed where required and each ID set manually using the rotary switches. The zones to ID can be calculated using the following formula: $((ID \text{ value} \times 8) + 1) = \text{first zone number}$ and then the next 7 sequential zones. For example $((ID2 \times 8) + 1) = 17$. Zone 17 is allocated to input 1 on ID2. Each input has the next sequential zone allocated to it, in this case up to zone 24. Note: ID limit for zone allocation SPC 4000: Expander ID 1 – 3. SPC 5000: Expander ID 1 – 15. SPC 6000: Expander ID 1 – 63.

ID	Zone	ID	Zone	ID	Zones	ID	Zones	ID	Zones
1	9-16	14	113-120	27	217-224	40	321-328	53	425-432
2	17-24	15	121-128	28	225-232	41	329-336	54	433-440
3	25-32	16	129-136	29	233-240	42	337-344	55	441-448
4	33-40	17	137-144	30	241-248	43	345-352	56	449-456
5	41-48	18	145-152	31	249-256	44	353-360	57	457-464
6	49-56	19	153-160	32	257-264	45	361-368	58	465-472
7	57-64	20	161-168	33	265-272	46	369-376	59	473-480
8	65-72	21	169-176	34	273-280	47	377-384	60	481-488
9	73-80	22	177-184	35	281-288	48	385-392	61	489-496
10	81-88	23	185-192	36	289-296	49	393-400	62	497-504
11	89-96	24	193-200	37	297-304	50	401-408	63	505-512

12	97-104	25	201-208	38	305-312	51	409-416		
13	105-112	26	209-216	39	313-320	52	417-424		



If 2 devices of a kind (e.g. expanders) are set to same ID, upon configuration, both expanders beep and the flashing LED indicates conflict. Reset the switches and the system rescans.

On a device, if both rotary switches are set to zero (0, 0), the full configuration becomes an automatic addressing configuration.

To select the ADDRESS MODE:

1. Scroll to ADDRESS MODE.
2. Press SELECT.
3. Toggle for appropriate address mode: AUTOMATIC or MANUAL
4. Press SELECT to update the setting.

16.6.6 XBUS Type

To program the X-BUS type from the keypad:

1. Scroll to XBUS TYPE.
2. Press SELECT.
3. Scroll to select desired configuration:
 - LOOP
 - SPUR
4. Press SELECT to update the setting.

16.6.7 Bus Retries

To program the number of times the system attempts to retransmit data on the X-BUS interface before a communications fault is generated:

1. Scroll to BUS RETRIES.
2. Press SELECT.
3. Enter the preferred number of times the system retransmits data.
4. Press SELECT to update the setting.

16.6.8 Comms Timer

To designate the length of time before a communication fault is recorded:

1. Scroll to COMMS TIMER.
2. Press SELECT.
3. Enter the preferred time setting.
4. Press ENTER to update the setting.

16.7 Wireless

1. Scroll to WIRELESS and press SELECT.
2. Scroll to the desired programming option:

SENSORS	<p>It may be necessary to change the type of sensor enrolled on the system if the sensor type was incorrectly identified in the enrolment process.</p> <p>If no wireless detectors are enrolled, the keypad displays NO ACTIVE SENSORS.</p> <p>The following options are available for sensors:</p> <ul style="list-style-type: none"> ● ADD See ADD SENSORS [→ 130] ● EDIT (Change zone assignment) See EDIT SENSORS (ZONE ASSIGNMENT) [→ 131] ● REMOVE Select the device or sensor to be deleted.
WPA	<p>Add, edit or remove a WPA (Wireless Personal Alarm).</p> <ul style="list-style-type: none"> ● ADD See ADD WPA [→ 131] ● EDIT See EDIT WPA [→ 132] ● REMOVE Select the WPA to be deleted.
EXTERNAL ANTENNA	Enable or disable the external antenna.
SUPERVISION	Enable or disable tamper supervision.
FILTER LOW SIGNAL	Enable or disable the filter low signal (RF strengths 0 and 1).
DETECT RF JAM	Enable or disable the RF JAM.
RFFOB PANIC	Enable or disable the RFFob Panic or enable silent mode for the RFFob Panic.
WPA TEST SCHEDULE	Enter a maximum period (in days) between WPA tests. Max is 365 days.
PREVENT SET TIME	Enter a time in minutes after which, if the sensor or WPA fails to report, a setting is prevented for an area where the wireless zone is. Max is 720 minutes.
DEVICE LOST TIME	Enter the number of minutes after which the wireless device is reported as lost if it fails to report within this timeframe. (Min is 20 and max is 720 minutes)

16.7.1 Add Sensors

To add a wireless sensor device:

1. Scroll to ADD and press SELECT.
 - ⇒ The prompt ACTIVATE ENROL is displayed.
2. Press SELECT.
 - ⇒ The top line of the display flashes the text ACTIVATE DEVICE.
3. Activate the wireless device between 3 and 5 times in succession to allow the keypad receiver to detect the wireless transmission of the device.

- ⇒ The display indicates that the device has been detected by flashing the text FOUND SENSOR. The device TYPE and ID information is displayed alternately.
- 4. Press ENROL.
- ⇒ A prompt to select the zone type is displayed.
- 1. Press SELECT.
- 2. Scroll to the required zone type and press SELECT.



To add a device by TAMPER ENROL, scroll to this option in step 2. The enrolment process is identical except a prompt to define an area type is displayed before the zone type prompt.

16.7.2 Edit Sensors (Zone Assignment)

It may be necessary to change the zone assignment of sensor enrolled on the system.

To change the zone assignment of a wireless detector:

1. Scroll to EDIT and press SELECT.
2. Scroll to the sensor to be changed and press SELECT.
3. Scroll to ZONE.
4. Scroll to the appropriate zone number (only unoccupied zone numbers are displayed).
5. Press SELECT.

16.7.3 Add WPA

!	NOTICE
	You can only configure a WPA or check its status on the keypad if there is a wireless module fitted on the panel or any of its expanders and the panel is licensed for the type of module(s) fitted.

A WPA is not assigned to a user. Usually, a WPA is shared by several people, for example, security guards working in shifts or, alternatively, WPAs may be permanently attached to a surface such as under a desk or behind a till.

A maximum of 128 WPAs is allowed per panel.

To configure a WPA with the keypad:

1. Select WIRELESS and then WPA.
2. Select ADD to add a WPA.
3. Select MANUALLY to manually enter a WPA ID.
The ID can also be entered automatically by the panel by selecting the LEARN WPA option. One of the WPAs buttons must be pressed when the ACTIVATE WPA message is displayed, in order for the panel to identify the WPA. The panel will not accept a WPA if it's ID is a duplicate of a currently configured WPA.

- Exit the ADD menu and select the EDIT menu to configure the WPA.

16.7.4 Edit WPA

To configure a WPA with the keypad:

- Select WIRELESS and then WPA.
- Select EDIT to configure a WPA.

DESCRIPTION	Enter a description to uniquely identify the WPA.
TRANSMITTER ID	Enter the WPA Id. The panel will not accept a WPA if it's ID is a duplicate of a currently configured WPA.
FUNC TO BUTTONS	<p>Use this section to assign functions to button combinations. Available functions are Panic, Panic Silent, Holdup, Suspicion, RF User Output, Medical. More than one button combination can be selected for the same function. For example:</p> <ul style="list-style-type: none"> ● Yellow - Suspicion ● Red + Green – Holdup ● For Commercial or Domestic installations, the default is: Red + Green – Panic <p>Note: If no function is assigned to a button combination, it is still possible use that combination by using a trigger. See Triggers [→ 255]</p>
SUPERVISE	<p>The WPA may be configured to send periodic supervision signals. If supervision is enabled on the WPA (with the jumper), the WPA sends out a supervision message about every 7.5 minutes. The time between messages is randomized to decrease the chances of collision with other WPAs.</p> <p>The supervision function also needs to be enabled on the panel for the particular WPA for correct supervision operation. If the panel does not get a supervision signal, it raises an alarm that is shown in the keypad and logged.</p> <p>If supervision is not enabled, the WPA sends out a supervision message about every 24 hours to transmit the WPA battery status to the panel. This message is also randomized to decrease the chances of collision with other WPAs.</p> <p>Select ENABLE if supervision has been enabled for that particular WPA.</p>
TEST	Enables testing of the WPA signal.

See also

Triggers [→ 255]

Configuring WPA Timers [→ 130]

Testing a WPA from the Keypad [→ 148]

16.8 Zones

- Scroll to ZONES and press SELECT.
- Scroll to the desired zone (ZONE 1-x).
- Scroll to the desired programming option:

DESCRIPTION	Used to help identify the zone: enter a specific and descriptive name.
ZONE TYPE	Determines the zone type. See page [→ 347].
ATTRIBUTES	Determines the attributes of the zone. See page [→ 350].
TO AREA	Determines which zone is mapped to which area. This menu option is only displayed if multiple areas are defined on the system. Selecting this feature allows

users to build a set of zones that are identified with a particular area in the building.



The number and type of attributes displayed in the keypad menus for a particular zone vary depending on the type of zone that is selected. See page.

16.9 Doors

16.9.1 Doors

1. Scroll to DOORS and press SELECT.
2. Scroll to the door to be programmed and press SELECT.
3. Parameters and details, if applicable, are displayed for editing as follows:
 - Description
 - Door Inputs
 - Door Group
 - Door Attributes
 - Door Timers
 - Reader Information (Display only - format of last card used with configured reader)

Door inputs

Each door has 2 inputs with predefined functionality. These two inputs, the door position sensor and the door release switch can be configured.

Name	Description
Zone	<p>The door position sensor input can be used for the intrusion part as well. If the door position sensor input is used also for the intrusion part, the zone number it is assigned to has to be selected. If the door position sensor is used only for the access part, the option "UNASSIGNED" has to be selected.</p> <p>If the door position sensor is assigned to an intrusion zone, it can be configured like a normal zone but only with limited functionality (e.g. not all zone types are selectable).</p> <p>If an area or the system is set with the card reader, the door position sensor input has to be assigned to a zone number and to the area or the system which have to be set.</p>
Description (Web and SPC Pro only)	Description of the zone the door position sensor is assigned to.
Zone Type (Web and SPC Pro only)	Zone type of the zone the door position sensor is assigned to (not all zones types are available).
Zone attributes (Web and SPC Pro only)	The attributes for the zone the door position sensor is assigned to can be modified.
Area (Web and SPC Pro only)	The area the zone and the card reader are assigned to. (If the card reader is used for setting & unsetting, this area will be set / unset).
Door Position (Web)	The resistor used with the door position sensor. Choose

Name	Description
DPS End Of Line (keypads) Door Position EOL (SPC Pro)	the used resistor value / combination.
DPS Normal Open	Select if the door release switch is to be a normally open or normally closed input.
Door Release (Web) DRS END OF LINE (Keypads) Door Position EOL (SPC Pro)	The resistor used with the door release switch. Choose the used resistor value / combination.
DRS Normal Open	Select if the door release switch is a normally open input or not.
No DRS (Web and SPC Pro only)	Select to ignore DRS. If a DC2 is used on the door, this option MUST be selected. If not selected, the door will open.
Reader Location (Entry/Exit) (Web and SPC Pro only)	Select the location of the entry and exit readers.
Reader formats (Web) READER INFO (Keypads)	Displays format of last card used with each configured reader. (not available in SPC Pro)



Each free zone number can be assigned to the zones but the assignment is not fixed. If the number '9' is assigned to a zone, the zone and an input expander with the address '1' is connected to the X-Bus (which is using the zone numbers 9-16). The assigned zone from the two door controller will be moved to the next free zone number. Configuration will be adapted accordingly.

Door Groups

The different doors can be assigned to door groups. This is needed if one of the following functionalities is activated:

- Custodian
- Soft Passback
- Prevent Passback
- Interlock

Door attributes



If no attribute is activated, a valid card can be used.

Attribute	Description
Void	The card is temporarily blocked.
Door Group	Used when multiple doors are assigned to the same area and/or anti passback, custodian, or interlock functionality is required.
Card and PIN	Card and PIN are required to gain entry.
PIN Only	PIN is required. No card will be accepted.
PIN Code or Card	PIN or card are required to gain entry
PIN to Exit	PIN is required on exit reader. Door with entry and exit reader is required.

Attribute	Description
PIN to Set/Unset	PIN is required to set and unset the linked area. The card has to be presented before the PIN is entered.
Unset outside (Browser) Unset on Entry Reader (SPCPro)	Panel/area will unset, when card is presented at entry reader.
Unset inside (Browser) Unset on Exit Reader (SPCPro)	Panel/area will unset, when card is presented at exit reader.
Bypass alarm	Access is granted if an area is set and the door is an alarm or an entry zone type.
Fullset outside (Browser) Fullset on Entry Reader (SPCPro)	Panel/area will fullest, when card is presented twice at entry reader.
Fullset inside Full set on Exit Reader (SPCPro)	Panel/area will fullest, when card is presented twice at exit reader.
Force Fullset	If the user has rights, they can force set from entry reader.
Emergency	Door lock opens if a fire alarm is detected within the assigned area.
Emergency any	Fire in any area will unlock the door.
Escort	The escort feature enforces privileged card holders to escort other card holders through specific doors. If this feature is assigned to a door, a card with the "escort right" has to be presented first, to allow other cardholders without this right to open the door. The time period in which cardholders are able to present their cards after a card with escort right was presented, can be configured per door.
Prevent Passback*	Anti-passback should be enforced on the door. All doors must have entry and exit readers and must be assigned to a door group. In this mode, cardholders must use their access card to gain entry into and exit from a defined door group. If a valid cardholder has presented his access card to enter a door group and not presented the card to exit it, the cardholder is in breach of the Anti-Passback rules. Next time the cardholder attempts to enter the same door group, a hard Anti-Passback alarm will be raised and the cardholder will not be permitted entry to the door group.
Soft Passback*	Anti-passback violations are only logged. All doors must have entry and exit readers and must be assigned to a door group. In this mode, cardholders must use their access card to gain entry to and exit from a defined door group. If a valid cardholder has presented his access card to enter a door group and not presented the card to exit it, the cardholder is in breach of the Anti-Passback rules. Next time the cardholder attempts to enter the same door group, a Soft Anti-Passback alarm will be raised. However, the cardholder will still be permitted entry to the door group.
Custodian*	The custodian feature allows a card holder with custodian right (the custodian) to give other cardholders (non-custodians) access to the room. The custodian must be the first to enter the room. The non-custodians are only allowed to enter if the custodian is in the room. The custodian will not be allowed to exit until all non-custodians have left the room.

Attribute	Description
Door Sounder	Door controller PCB mounted sounder sounds on door alarms.
Ignore Forced	Door forced open is not processed.
Interlock* (Browser) Limit Interlocked Door Access (SPCPro)	Only one door in an area will be allowed open at a time. Requires Door Group.
Setting Prefix	Authorisation with prefix (A,B,* or #) key to set system
* Require door group	

Door timers

Timer	Min.	Max.	Description
Access granted	1 s	255 s	The time the lock will remain open after granting access.
Access deny	1 s	255 s	The duration after which the controller will be ready to read the next event after a invalid event.
Door open	1 s	255 s	Duration within which the door must be closed to prevent a "door open too long" alarm.
Door left open	1 min	180 min	Duration within which the door must be closed to prevent a "door left open" alarm.
Extended	1 s	255 s	Additional time after granting access to a card with extended time attribute.
Escort	1 s	30 s	Time period after presenting a card with escort attribute within a user without escort right can access the door.

16.10 Outputs

Each zone type on the SPC system has an associated output type (an internal flag or indicator). When a zone type is activated, i.e. a door or window opens, smoke is detected, an alarm is detected, etc., the corresponding output is activated.

1. Scroll to OUTPUTS and press SELECT.
2. Scroll to CONTROLLER or EXPANDER and press SELECT.
3. Scroll to the expander/output to be programmed and press SELECT.

⇒ If the output activations are recorded in the system event log (i.e. enabled, items recorded / disabled, items) the programming options are available as shown in the table below.

NAMES	Used to help identify the output; enter a specific and descriptive name.
OUTPUT TYPE	Determines the output type; see the table in page [→ 137], for a description of output types.
OUTPUT MODE	Determines the style of the output: continuous, momentary or pulsed.
POLARITY	Determines whether the output is activated on a positive or negative polarity.
LOG	Determines if system log is enabled or disabled.



For the output test procedure, see page [→ 146].

16.10.1 Outputs types and output ports

Each output type can be assigned to one of the 6 physical output ports on the SPC controller or to an output on one of the connected expanders. Output types that are not assigned to physical outputs act as indicators of events on the system and may be logged and/or reported to remote central stations if required.

The output ports on the expanders are all single pole relay type outputs (NO, COM, NC); therefore, output devices may need external power sources to activate if they are wired to expander outputs.

The activation of a particular output type depends on the zone type (see page [→ 347]) or alert condition that triggered the activation. If multiple areas are defined on the system then the outputs on the SPC are grouped into system outputs and area outputs; the system outputs are activated to indicate a system wide event (e.g. mains fault) whereas the area outputs indicate events detected in one or more of the defined areas on the system. Each area has its own set of area outputs; if the area is a common area for other areas, then its outputs will indicate the state of all the areas it is common for, including its own state. For example, if Area 1 is common for Area 2 and 3, and Area 2 Ext. Bell is active, then the Area 1 Ext Bell output is also active.



Some output types can only indicate system wide events (no specific area events). Please refer to the table below for further information.

Output Type	Description
External Bell	This output type is used to activate the system external bell and is active when any Area External Bell is active. By default, this output is assigned to the first output on the controller board (EXT+, EXT-). Note: An external bell output is automatically activated whenever a zone programmed as an Alarm zone triggers an alarm in Fullset or Partset modes.
External Bell Strobe	This output type is used to activate the strobe on the system external bell and is active when any area strobe is active. By default, this output is assigned to the strobe relay output (Output 3) on the Controller board (NO, COM, NC). Note: An external bell strobe output is automatically activated whenever a zone programmed as an alarm zone triggers an alarm in Fullset or Partset modes. The external bell strobe activates on a 'Fail to Set' condition if the strobe on the 'Fail to Set' option is checked in system options.
Internal Bell	This output type is used to activate the internal bell and is active when any area Internal Bell is active. By default, this output is assigned to the second output on the controller board (INT+, INT-). Note: An internal bell output is automatically activated whenever a zone programmed as an Alarm zone type triggers an alarm in Fullset or Partset modes. The internal Bell activates on a 'Fail to Set' condition if the Bell on the 'Fail to Set' option is checked in system options.
Alarm	This output turns on following alarm zone activation on the system or from any area defined on the system.
Alarm Confirmed	This output turns on when an alarm has been confirmed. An alarm is confirmed when 2 independent zones on the system (or within the same Area) activate within a set time period).
Panic*	This output turns on following activation of panic alarm zone types from any area. A panic alarm output is also generated if a user duress event is generated or if the panic option for the keypad is enabled.

Hold-up	This output turns on whenever a zone programmed as a Hold-up type zone triggers an alarm from any area
Fire	This output turns on following a fire zone activation on the system (or from any area)
Tamper	This output turns on when a tamper condition is detected from any part of the system. For a grade 3 system, if communication is lost to an XBUS device for greater than 100s, a tamper is generated and SIA and CIR reported events will send a tamper.
Medical	This output turns on when a medic zone is activated
Fault	This output turns on when a technical fault is detected
Technical	This output follows tech zone activity
Mains Fault*	This output activates when Mains power is removed
Battery Fault*	This output activates when there is a problem with the backup battery. If the battery voltage drops below 11 V this output activates. The 'Restore' option for this fault is only presented when the voltage level rises to above 11.8 V.
Partset A	This output is activated if the system or any area defined on the system is in Partset A mode
Partset B	This output is activated if the system or any area defined on the system is in Partset B mode
Fullset	This output is activated if the system is in Fullset mode
Fail to set	This output activates if the system or any area defined on the system failed to set; it clears when the alert is restored
Entry/Exit	This output activates if an Entry/Exit type zone has been activated; i.e. a system or area Entry or Exit timer is running
Latch	This output turns on as defined in the system latch output configuration (see Configuring system latch and auto set outputs [→ 202]). This output can be used to reset latching sensors as smoke or inertia sensors.
Fire Exit	This output turns ON if any Fire-X zones on the system are activated
Chime	This output turns on momentarily when any zone on the system with chime attribute opens
Smoke	This output turns on momentarily(3 seconds) when a user unsets the system; it can be used to reset smoke detectors The output will also activate when the zone is restored When using the zone to reset latched smoke detectors the first code entry will not activate the smoke output but will silence bells, on the next code entry if the fire zone is in the open state the smoke output will activate momentarily. This process is repeatable until the fire zone is closed.
Walk Test*	This output turns on momentarily when a walk test is operational and a zone becomes active. This output can be used, for example, to activate functional tests of connected detectors (if available).
Auto Set	This output turns on if the Auto Set feature has been activated on the system.
User Duress	This output turns on if a user duress state has been activated (PIN code + 1 has been entered on the keypad)
PIR Masked	This output turns on if there are any masked PIR zones on the system. It generates a fault output on the keypad led. This output is latched so it will remain active until restored by a level 2 user. PIR Masking is logged by default. The number of log entries do not exceed 8 between arming periods.
Zone Omitted	This output turns on if there are any inhibited, isolated, or walk test zones on the system
Fail to Communicate	This output turns on if there is a failure to communicate to the central station
Man Down Test	This output turns on a 'Man Down' wireless device which is activated during a 'Man Down' test.

Unset	This output is activated if the system is in Unset mode.
Alarm Abort	This output activates if an alarm abort event occurs i.e. when a valid user code is entered via the keypad after a confirmed or unconfirmed alarm. It is used, for example, with external dialers (SIA, CID, FF)
Seismic Test	This output is used to activate a manual or automatic test on a seismic zone. Seismic sensors have a small vibrator that will be attached to the same wall as the sensor and is wired to an output on the panel or one of its expanders. During the test, the panel waits up to 30 seconds for the seismic zone to open. If it does not open, the test fails. If it opens within 30 seconds the panel then waits for the zone to close within 10 seconds. If that doesn't happen, the test fails. The panel then waits a further 2 seconds before reporting the test result. The result of the test, either manual or automatic, is stored in the system event log
Local Alarm	This output activates on a local intrusion alarm.
RF Output	This output activates when a Fob or WPA button is pressed.
Modem 1 Line Fault	This output activates when there is a line fault on the primary modem..
Modem 1 Failure	This output activates when the primary modem fails.
Modem 2 Line Fault	This output activates when there is a line fault on the secondary modem.
Modem 2 Failure	This output activates when the secondary modem fails.
Battery Low	This output activates when the battery is low,
Entry Status	This output activates if an 'All Okay' entry procedure is implemented and there is no alarm generated i.e. the 'All Okay' button is pressed within the configured time after the user code is entered.
Warning Status	This output activates if an 'All Okay' entry procedure is implemented and a silent alarm generated i.e. the 'All Okay' button is not pressed within the configured time after the user code is entered.
Ready to Set	This output activates when an area is ready to set.
Setting ACK (SPC Pro — Setting Complete)	This output signals the setting status. The output toggles for 3 seconds to signal that the setting has failed. The output remains on for 3 seconds if setting is successful.
Fullset Done (SPC Pro — Setting Success)	This output activates for 3 seconds to signal that the system has been fullest.
Blockschloss 1	Used for normal Blockschloss devices. When all zones in an area are closed, and there are no pending faults, the 'Blockschloss 1' output is activated. If the lock on the Blockschloss is closed, a 'Keyarm' input is activated, the relevant area is set and the 'Setting Ack' output is activated for 3 seconds to signal that the setting was successful. 'Blockschloss 1' is not deactivated. If the Blockschloss is unlocked, the Blockschloss device deactivates the Keyarm input to the unset state (closed) and the area is unset. 'Blockschloss 1' is then deactivated.
Blockschloss 2	Used for Blockschloss device type - Bosch Blockschloss, Signalock Plus, E4.03. When all zones in an area are closed, and there are no pending faults, the 'Blockschloss 2' output is activated. If the lock on the Blockschloss is closed, a 'Keyarm' input is activated, the relevant area is set and the 'Setting Ack' output is activated for 3 seconds to signal that the setting was successful. 'Blockschloss 2' is then deactivated. If the Blockschloss is unlocked, the Keyarm zone is switched to unset (closed) and the area is unset. 'Blockschloss 2' is activated (if area is ready to set).
Lock Element	Activates if the Lock Element is in the 'locked' position.
Unlock Element	Activates if the Lock Element is in the 'unlocked' position.
Code Tamper	Activates if there is a code tamper in the area. Clears when state is reset.
Trouble	Activates if any zone is in trouble state.
Ethernet Link	Activates if there is a fault on the Ethernet link.
Network Fault	Activates if there is an EDP communications fault.

Glass Reset	Used to switch on the power for the glassbreak interface module and to remove power in order to reset the device. The output is reset if a user enters their code, the zone is not in the closed state, and the bells deactivated.
Confirmed holdup	Activates in the following scenarios for PD6662 compliance: <ul style="list-style-type: none"> ● two hold-up zone activations more than two minutes apart ● a hold-up zone and a panic zone activation more than two minutes apart ● If a hold-up zone and a tamper zone or a panic zone and a tamper zone activation occurs within the two minute period
Full Engineer	Activates if an engineer is on site and the system is in full engineer mode.

** This output type can only indicate system wide events (no area specific events).*

See also

📖 [Configuring system latch and auto set outputs \[→ 202\]](#)

16.11 Communication

1. Scroll to COMMUNICATION and press SELECT.
2. Scroll to the desired programming option.

16.11.1 Serial Ports

The serial ports allow older style PCs to be connected to the system or other peripheral equipment like printers.

1. Scroll to SERIAL PORTS.
2. Press SELECT.
3. Scroll to the serial port to be programmed.
4. Select the desired programming option shown in the table below.
5. Press BACK to exit.

TYPE	Determines if type is TERMINAL (system information) or PRINTER (SPC event log)
BAUD RATE	Determines the speed of the communication between the panel and the peripheral equipment. Please note that the baud rate must be set the same as both items of equipment.
DATA BITS	Determines the length of data packet to be transferred between the panel and the peripheral equipment. Please note that the data bits must be set the same for both items of equipment.
STOP BITS	Determines the number of stop bits at the end of the data packet. Please note that the stop bits must be set the same for both items of equipment.
PARITY	Determines the parity (odd/even) of the data packet. Please note that the parity must be set the same for both items of equipment.
FLOW CONTROL	Determines if the data is under hardware (RTS, CTS) or software control (None). Please note that the flow control must be set the same for both items of equipment.

16.11.2 Ethernet Ports

To program the Ethernet port:

1. Scroll to ETHERNET PORT.

2. Press SELECT.
 - ⇒ The IP ADDRESS option displays, XXX.XXX.XXX.XXX For single digits, leading zero(s) are required. I.e., 001
3. Press SELECT and enter the preferred IP address.
 - ⇒ When the ENTER key is operated, the system beeps twice and states UPDATED if the IP address is valid. If the IP address is allocated manually, then this must be unique on the LAN or VLAN, connected to panel. A value is not entered if the DHCP option is used.
4. Scroll to IP NETMASK.
5. Press SELECT and enter the IP NETMASK format XXX.XXX.XXX.XXX. (For single digits, leading zero(s) are required. I.e., 001) When the ENTER key is operated, the system beeps twice and states UPDATED if the IP NETMASK is valid.
6. Scroll to GATEWAY. Note the gateway needs to be programmed for access outside the network (for use with the Portal).
7. Press SELECT and enter the GATEWAY format XXX.XXX.XXX.XXX. (For single digits, leading zero(s) are required. I.e., 001) When the ENTER key is operated, the system beeps twice and states UPDATED if the GATEWAY is valid.
8. Scroll to DHCP. The DHCP is enabled if the LAN has a DHCP server to allocate the IP address. The IP address is to be enabled manually. Note the gateway needs to be programmed if the panel needs access outside the network (for Portal service).
9. Press SELECT and enter the GATEWAY format XXX.XXX.XXX.XXX. (For single digits, leading zero(s) are required. I.e., 001)
 - ⇒ When the ENTER key is operated, the system beeps twice and states UPDATED if the GATEWAY is valid.
 - ⇒ The DHCP option is displayed.
10. Toggle between DHCP ENABLED and DISABLED for preferred option.
11. Press SELECT.

16.11.3 Modems

The SPC system supports SPC intelli-modems for communications with analogue lines and mobile network interfacing for enhanced communications and connectivity. The SPC system must be configured accordingly.


16.11.3.1 Monitoring the transmission network interface


The SPC Alarm System sends a poll to SPC Com XT, which responds with a poll acknowledge (ACK). On receipt of a valid poll ACK the SPC Alarm System updates its status to OK and resets its polling interval timer (depending on the ATP category).

If the SPC Alarm System does not receive a polling ACK within the timeout (depends on ATP category), the SPC Alarm System updates its status to DOWN.

SPC supports the following transmission interfaces:

- Ethernet
- GSM with GPRS enabled
- PSTN modem.

	NOTICE
	Before changing PIN or new SIM card, ensure all power sources are disconnected (AC mains and battery) or card will not be activated.

	NOTICE
	After a factory default, during the process of initial setup of the system with the keypad, the panel detects if it has a primary or backup modem fitted, and if so, it displays its type and automatically enables it (or them) with the default configuration. No other modem configuration is allowed at this stage.

16.11.3.2 Configuring Modems

To configure a GSM or PSTN modem:

1. Scroll to MODEMS and press SELECT.
2. Toggle between PRIMARY and BACKUP for correct modem slot and press SELECT.
 - ⇒ The ENABLE MODEM option is displayed.
3. ENABLE or DISABLE the modem as required.
4. Scroll to MODEM STATUS, TYPE, FIRMWARE VERSION and SIGNAL LEVEL and press SELECT to view details of the modem.
5. Configure the following modem settings from the menu as follows and press ENTER after each selection:

Menu Option	Description
COUNTRY CODE	Select a country from the list.
GSM PIN	(GSM modem only) Enter a GSM PIN for the SIM card.
ANSWER MODE	Select to select the mode in which the modem answers incoming calls: NEVER ANSWERS or ALWAYS ANSWERS
ANSWER ENG. ACC.	Select ENABLE to only answer when engineer access is granted.
SETUP SMS	Select ENABLE SMS to enable SMS for this modem. (Only for PSTN.) Select SMS SERVER to enter an appropriate phone number of the SMS service provider that is accessible in your location, if required. This number automatically displays the default number for SMS for the country selected. To manually test SMS, select TEST SMS and enter the SMS NUMBER. To automatically test SMS at specific time intervals, select AUTOMATIC TEST , select a TEST INTERVAL and enter the SMS NUMBER.
PREFIX DIALLING	(PSTN modem only) Enter a prefix number to include before the SMS number, if required.
LINE MONITORING	For PSTN: Enable this feature to monitor the voltage of the line connected to the modem.

Menu Option	Description
	<p>GSM Modem: Enable this feature to monitor the signal level from the GSM mast connected to the modem. Select a monitoring MODE (ALWAYS ON, FULLSET, DISABLED). The FULLSET option only enables this feature while the system is Fullset.</p> <p>Enter the number of seconds for the monitoring TIMER (0 – 9999 sec)</p> <p>Note : EN 50131-9 Confirmation configuration In order for EN50131-9 Confirmation to operate correctly, line monitoring must be enabled. (refer to System Options)</p>



GSM Modem only. If SMS enabled, and if an incorrect PIN is sent to the SIM card three times, the SIM is blocked. If this happens, it is recommended that the SIM card be removed and unblocked using a mobile phone. If the SIM card is being changed on the GSM module or if a SIM card is being used with a PIN, it is recommended that the PIN code be programmed before it is placed in the SIM holder, to ensure that incorrect PINs are not sent to it. All power should be removed (AC mains and battery) when loading the SIM card into the SIM holder.

16.11.4 Central Station

16.11.4.1 Add

To program the central station settings:

1. Scroll to CENTRAL STATION > ADD.
2. Press SELECT.
3. Select the desired programming option shown in the table below.
4. After programming is complete, the option to make a test call to the station is displayed on the keypad.

ACCOUNT ID	This information should be available from the receiving station and is used to identify users each time a call is made to the ARC
ACCOUNT NAME	Description of the Remote Alarm Receiving Centre
PROTOCOL	The communication protocol to be used (SIA, Contact ID, Fast Format)
1ST PHONE NUMBER	The first number to be dialled to contact the ARC
2ND PHONE NUMBER	The second number to be dialled to contact the ARC; the system only attempts to contact the ARC on this number if the first contact number did not successfully connect
PRIORITY	The modem (primary or back-up) to be used to communicate with the ARC

16.11.4.2 Edit

To edit the central station settings:

1. Scroll to CENTRAL STATION >EDIT.
2. Press SELECT.
3. Select the desired programming option shown in the table below.

4. After programming is complete, the option to make a test call to the station is displayed on the keypad.

ACCOUNT ID	This information should be available from the receiving station and is used to identify users each time a call is made to the ARC
ACCOUNT NAME	Description of the Remote Alarm Receiving Centre
PROTOCOL	The communication protocol to be used (SIA, Contact ID, Fast Format)
1ST PHONE NUMBER	The first number to be dialled to contact the ARC
2ND PHONE NUMBER	The second number to be dialled to contact the ARC; the system only attempts to contact the ARC on this number if the first contact number did not successfully connect
DIAL ATTEMPTS	Enter the number of times that the system will attempt to make a call to the receiver.
DIAL INTERVAL	Enter the number of seconds to delay between failed dial attempts. (0 - 999)
ASSIGN AREA	Assign the areas for which events are reported to the ARC.
REPORTED EVENTS	Define the types of events reported to the ARC.
PRIORITY	The modem (primary or back-up) to be used to communicate with the ARC
AUTOMATIC TEST	Defines a schedule for testing the connection to the ARC. Possible values range from every hour to once every 30 days.

16.11.4.3 Delete

Enables you to delete a configured ARC.

16.11.4.4 Make Test Call

Enables you to test the connection with the ARC.

To make a test call, do the following:

1. Select MAKE TEST CALL.
 2. Select the ARC name.
 3. Click SELECT.
 4. Select the modem to use for the text call.
- ⇒ The test call is performed.

16.11.5 Remote Maintenance

1. Scroll to REMOTE MAINT.>ENABLE REMOTE MAINT
2. Press Select.
3. Toggle between ENABLED and DISABLED.
4. Select the desired programming option shown in the table below.

ID	Remote Maintenance ID. Must match that at SPC Pro (1 - 999999).
PASSWORD	Password for Remote Maintenance. Must match that at SPC Pro.
IN CONN. SETTS.	Incoming Connection Settings. You can enable IN IP ENABLE to allow incoming IP connections from the Remote Maintenance server. If not enabled, only modem connections are possible. Enter the IN TCP/IP PORT on which the panel listens to incoming IP connections from the Remote Maintenance server.

OUT CONN. SETTS	Outgoing Connection Settings. Choose how to make outgoing connections to the Remote Maintenance server from the options DISABLED, OVER MODEM or OVER IP.
-----------------	--

16.12 Test

1. Scroll to TEST and press SELECT.
2. Scroll to the desired programming option.

16.12.1 Bell Test

To perform a bell test:

1. Scroll to TEST > BELL TEST.
2. Press SELECT.


⇒ When BELL TEST is selected, the following options available: EXTERNAL BELLS, STROBE, INTERNAL BELLS and BUZZER. When each of these options is selected, the device sounds to verify it is operating correctly.

16.12.2 Walk Test

A walk test ensures that the sensors are operating correctly on the SPC system.

To perform a walk test:

1. Scroll to TEST > WALK TEST.
2. Press SELECT.
3. The display indicates the number of zones to be tested on the system with the text TO TEST XX (where XX is the number of valid walk test zones). Locate the sensor on the first zone and activate it (open the door or window).
 - ⇒ The keypad buzzer sounds continuously for approximately 2 seconds to indicate that the zone activation has been detected and the number of zones left to test (displayed on the keypad) decreases.
4. Continue with the remaining zones on the system until all zones have been tested. If a zone activation does not get acknowledged by the system, check the wiring of the sensor and/or replace with another sensor if necessary.

	NOTICE
	All zones can be included in an Engineer walk test.

16.12.3 Zone Monitor

The Zone Monitor option displays status information on each of the zones on the system.

To view zone status information:

1. Scroll to TEST > ZONE MONITOR.

2. Press SELECT.
 3. Scroll to a preferred zone and press SELECT.
 - ⇒ The status of the zone and its associated resistance value is displayed.
 4. Press NEXT to locate the zone (e.g. CONTROLLER 1 = first zone on Controller).
- ⇒ Refer to the table below for correlating status information (valid for Dual EOL resistors).

Zone status	Abbreviation
UNKNOWN	UK
CLOSED	CL
OPEN	OP
SHORT	SH
DISCONNECTED	DI
PULSE	PU
GROSS	GR
MASKED	AM
FAULT	FA
DC SUB	DC
OUT OF BOUNDS	OB
UNSTABLE	US

All zones on a system can be monitored for correct operation by performing a monitoring test.

To perform a zone monitoring test:

1. Scroll to ZONE MONITOR.
2. Press SELECT.
3. Scroll to a preferred zone and press SELECT, or enter the zone number directly.
 - ⇒ If the zone is located close to the keypad, the status of the keypad can be viewed as it changes. The Zone status and resistance value displays on the top right.
4. Change the state of the sensor; e.g. for a door contact sensor, open the door.
 - ⇒ The keypad buzzer beeps and the status of the sensor changes from CL (Closed) to OP (Open). The corresponding resistance value changes to a value that depends on the EOL resistance scheme.



It is advisable to check the operation of all zones on the system after installation is complete. To locate the zone select NEXT (bottom right) on the keypad. A zone status value of SH or DI indicates that the zone is shorted or disconnected.

16.12.4 Output Test

To perform an output test:

1. Scroll to OUTPUT TEST.
2. Press SELECT.
3. Toggle between CONTROLLER and EXPANDER for preferred option.

4. If testing the controller outputs, scroll to the preferred output and press SELECT. If testing the expander outputs, select the expander and then the output.
 - ⇒ The keypad display indicates the current state of the output on the top line.
5. Toggle the output state ON/OFF.
6. Check that the device connected to the selected output changes state accordingly.

16.12.5 Soak Test

A Soak Test provides a method of putting selected zones on test. Zones on soak test do not cause any alarms but are recorded in the event log. Zones on soak test will remain on soak test until the soak test timer expires as in the timers default (14 days).

To perform a soak test:

1. Scroll to SOAK TEST and press SELECT.
 2. Toggle between ENABLE SOAK and CANCEL SOAK for preferred option.
 3. Scroll to preferred zone and press SELECT.
- ⇒ A message confirming that the zone is in soak is displayed.



NOTICE

All zone types can be included in a Soak test.

16.12.6 Audible Options

The audible options are applied as indicators within a walk test.

To set the audible options:

1. Scroll to AUDIBLE OPTIONS.
2. Press SELECT.
3. Scroll to one of the following options: ALL, INT BELL, EXT BELL, KEYPAD
4. Press SAVE.
5. Press BACK to exit.

16.12.7 Visual Indicators

This test is used to test all the pixels on the LCD Keypad and all the pixels and LED indicators on the Comfort Keypad, Indicator module and Keyswitch.

To test a keypad:

1. Scroll to VISUAL IND.
2. Press SELECT.
3. Press ENABLE.

On the LCD keypad, two rows of continuously changing characters are displayed.

On the Comfort keypad, all the LED indicators are lit and all screen pixels are displayed.

1. Press BACK to disable the test.

2. Press BACK to exit.

16.12.8 WPA Test

!	NOTICE
	This test can be only be performed by an engineer or user that has a 'WPA Test' right assigned to them. See User rights

To test the WPA from the keypad:

1. Scroll to WPA TEST and press SELECT.
2. When prompted with ACTIVATE WPA, press the three buttons simultaneously on the WPA.
 - ⇒ If the test succeeded, a WPA *n* OK message will be shown where *n* is the number of WPA being tested.
1. Repeat the test if required.
2. Press BACK or X to end the test.

16.12.9 Seismic Test

To perform a seismic test:

1. Scroll to TEST > SEISMIC TEST.
2. Press SELECT.
3. Select TEST ALL AREAS, or select an individual area to test.
4. If you select an individual area to test, you can select either TEST ALL ZONES or select a specific seismic zone to test.
 - ⇒ The message 'SEISMIC TEST' is display on the keypad while the test is being performed,
 - ⇒ If the test fails, the message 'SEISMIC FAIL' is displayed. If the "i" or VIEW key is pressed, a list of the failed zones is displayed which can be scrolled through.
 - ⇒ If the test succeeds, 'SEISMIC OK' is displayed.

See also Seismic Sensor Testing [→ 325].

16.13 Utilities

1. Scroll to UTILITIES and press SELECT.
2. Scroll to the desired programming option:

SYSTEM SOFTWARE	To view the current software version.
DEFAULTS	To reset users or return the system to factory setting.
BACKUP CONFIG	To back-up a configuration.
RESTORE CONFIG	To restore a configuration.
FAST PROGRAMMER	<ul style="list-style-type: none"> ● DATA FROM PANEL: Transfer data from the controller to the Fast Programmer. You are prompted to confirm if the new

	<p>configuration file name is the same as a file name already existing in the fast programmer to prevent configuration files from being overwritten.</p> <ul style="list-style-type: none"> ● DATA TO PANEL: Transfer data to the controller from the Fast Programmer. ● DELETE FILES: ● FIRMWARE UPGRADE. Note: If you downgrade the firmware (i.e. install an older version of firmware) the system will default all current configuration settings. Also, when downgrading firmware, it is important to downgrade the corresponding peripheral firmware otherwise zones may appear disconnected, opened or closed. ● PERIPHERAL UPGRADE: ● LANGUAGE UPGRADE:
SPC PRO/SPC SAFE	<p>To program the following SPC Pro options:</p> <ul style="list-style-type: none"> ● ENABLE ACCESS: Determine if SPC Pro is enabled or disabled. ● ENGINEER ACCESS: Determine if engineer access is enabled or disabled. ● PASSWORD: Edit the existing system password. ● IP ENABLE: Enable to connect to the system via IP. ● IP PORT: Select which IP Port SPC Pro/SDK will connect through.
SYSTEM RESTART	To restart the system.
LICENSE	Enter a license number to change the SPC license key. The system does not log or report a license change.

16.14 Isolate

Zones, system alerts or alerts from X-BUS devices can be manually isolated from the keypad. Isolating a zone removes that zone from the system until the user de-isolates it.

To isolate zones, system alerts or alerts from X-BUS devices:

1. Scroll to ISOLATE and press SELECT.
2. Scroll to the desired option in the table below and press SELECT.

ZONE	Select the required zone and toggle the setting from NOT ISOLATED to ISOLATED.
SYSTEM	Isolate the desired system alert.
XBUS	<p>Isolate the desired alert from EXPANDERS or KEYPADS:</p> <ul style="list-style-type: none"> ● XBUS COMMS LOST ● XBUS FUSE FAULT (Expanders only) ● X-BUS TAMPER
VIEW ISOLATIONS	To view a list of the isolated zones, system alerts and X-BUS devices alerts.

16.15 Event Log

Recent events on the system are displayed in the EVENT LOG option. Events flash in one second intervals.

1. Scroll to EVENT LOG and press SELECT.
2. To view an event from a particular date, enter the date with the numeric keys.

- ⇒ The most recent events are displayed on the bottom line of the display. All previous events are displayed for one second in turn.

16.16 Access Log

Zone access on the system is displayed in the ACCESS LOG option.

1. Scroll to ACCESS LOG and press SELECT.
2. Select a door on the system for which you want to display access events.

⇒ The most recent access events are displayed with a date and time.
3. Scroll down through the access events or enter a date and press ENTER to find a particular access event.

16.17 Alarm Log

The ALARM LOG displays a list of alarm events.

- Select **Log > System Log > Alarm Log**.

The following types are displayed in this log:

- Zones
 - Alarm
 - Panic
- System Events
 - Confirmed Alarm
 - User Duress
 - XBus Panic
 - User Panic
 - RPA Panic

16.18 Change Engineer Pin

To change the Engineer PIN:

1. Scroll to CHANGE ENG PIN and press SELECT.

⇒ A randomly generated PIN appears.
2. Enter a new PIN if required by overwriting the displayed PIN and press ENTER.

⇒ The minimum number of digits required for this code depends on the security setting of the system or on the selected length of the PIN Digits in the browser (Panel Settings > System Settings > Options) The system will not accept a PIN with fewer numbers than it is set to receive
3. Confirm the new PIN, press SAVE.
4. Press BACK to return to the previous screen to amend the PIN.

⇒ If the display times out during the process, the old PIN remains valid.

16.19 Users

Only users with the appropriate user right enabled in their profile have the ability to add, edit, or delete users:

16.19.1 Add

To add users to the system:

1. Scroll to USERS > ADD.
 - ⇒ Select a user ID from the available IDs on the system and press SELECT.
2. Press ENTER to accept the default user name or enter a customized user name and press ENTER.
3. Scroll to the preferred user profile type and press ENTER to select.
 - ⇒ The system generates a default PIN for each new user.
4. Press ENTER to accept the default user PIN or enter a new user PIN and press ENTER.

The keypad confirms that the new user has been created.

16.19.2 Edit

To edit users on the system:

1. Scroll to USERS > EDIT.
2. Press SELECT.
3. Edit the desired user setting shown in the table below.

CHANGE NAME	Edit the current user name
USER PROFILE	Select the appropriate profile for this user.
USER DURESS	Enable or disable duress for this user.
DATE LIMIT	Enable this if the user can only access the system for a specified period of time. Enter a FROM and TO date and press ENTER.
PACE	Enable or disable PACE capability
RF FOB	Enable or disable RF Fob access (wireless keypad, remote control)
MAN-DOWN (MDT)	Enables the man-down test.
ACCESS CONTROL	If no card assigned to the user: <ul style="list-style-type: none"> ● ADD CARD ● LEARN CARD If a card assigned to the user: <ul style="list-style-type: none"> ● EDIT CARD <ul style="list-style-type: none"> – CARD NUMBER – CARD ATTRIBUTES (see Access Control) ● RESET CARD ● DELETE CARD
LANGUAGE	Select a language for this user that will be displayed on the system.

16.19.2.1 Access Control

One access card can be assigned to each of the users on the control panel.

To configure the access control for a user:

1. Scroll to USERS > EDIT.
2. Press SELECT.
3. Select the user which should be configured and press SELECT.

4. Scroll to ACCESS CONTROL and press SELECT.


The following sections provide programming steps found within the access control option of the selected user.

16.19.2.1.1 Add Card manually

If the card format of the card number is known, the card can be created manually. The site code of the card is configured for the user profile that is assigned for this user.


1. Scroll to ADD CARD
 2. Press SELECT.
- ⇒ An empty card has been added and can now be edited.

16.19.2.1.2 Learn Card

	NOTICE
	Only cards with supported card formats can be learned.

If the card number or the card format is not known, the card can be read and its information learned.

1. Scroll to LEARN CARD.
2. Press SELECT.
3. Select the door that the card will be presented.
4. Press SELECT.

	NOTICE
	The new card can be presented at the entry or the exit reader of the selected door.

5. Present the card at a card reader at the selected door.
- ⇒ The information for the new card is learned.

16.19.2.1.3 Edit Card

If an access card is already assigned to a user it can be changed via the keypad:

1. Scroll to EDIT CARD.
2. Press SELECT.
3. Edit the desired user setting shown in the table below.
4. Press BACK to exit.

Access Control

Attribute	Description
Card Number	Enter card number. Enter 0 to unassign this card.

Attribute	Description
Void Card	Check to temporarily disable this card.
Extended Time	Extend door timers when this card is present.
PIN bypass	Access a door without PIN on a door with PIN reader.
Priority	Priority cards are stored locally in the door controllers and will grant access in case of a technical fault where the door controller cannot communicate with the control panel. The maximum number of priority users is: <ul style="list-style-type: none"> ● SPC4xxx – all users ● SPC5xxx – 512 ● SPC6xxx - 512
Escort	The escort feature enforces privileged card holders to escort other card holders through specific doors. If this feature is enabled on a door, a card with the “escort” right has to be presented first, to allow other cardholders without this right to open the door. The time period in which cardholders are able to present their cards after a card with escort right was presented, can be configured per door.
Custodian	The custodian feature enforces a card holder with custodian privilege to always be inside a room (door group) when other card holders are inside. The custodian must be the first to enter the room. Only if a custodian is in the room other cardholders are allowed to enter. The cardholder with the custodian right will not be allowed to exit until all non-custodian cards left the room. Identifies this card holder as a custodian. The user with the custodian attribute has to be the first who enters a door group which requires a custodian card holder and has to be the last that is leaving this door group.

16.19.2.1.4 Delete Card

If an access card is no longer needed it can be deleted via the keypad.

1. Scroll to DELETE CARD.
2. Press SELECT.

16.19.2.1.5 Reset Card

If the ‘Prevent Passback’ feature is activated in a room and a user leaves this room without using the exit reader, he is not allowed to enter this room again. The user’s card can be reset to allow him to present his card once without a passback check.

To reset the card via the keypad:

1. Scroll to RESET CARD.
2. Press SELECT.

16.19.3 Delete

To delete users on the system:

1. Scroll to USERS > DELETE.
2. Press SELECT.
 - ⇒ A prompt displays, confirming command to delete.
3. Press YES to delete the user.

16.20 User Profiles

See also

 Adding / Editing User Profiles [→ 187]

16.20.1 Add

To add user profiles to the system:



The creator must be a user profile type MANAGER.

1. Scroll to USERS PROFILES > ADD.
 - ⇒ The option NEW NAME is displayed. Press SELECT.
2. Enter a customized user profile name and press ENTER.
 - ⇒ The keypad confirms that the new user profile has been created.

16.20.2 Edit

To edit user profiles on the system:

1. Scroll to USER PROFILES > EDIT.
2. Press SELECT.
3. Edit the desired user profile setting shown in the table below.

CHANGE NAME	Edit the name of the profile if required.
CHANGE AREAS	Select the areas relevant to this profile.
CALENDAR	Select a configured calendar or NONE.
RIGHT	Enable or disable system features for this profile. See User Rights [→ 187].
DOOR	Select the type of access available to this profile for the configured doors. Options are NONE, NO LIMIT or CALENDAR.
SITE CODE	Enter a site code for all cards using this profile.

16.20.3 Delete

To delete user profiles on the system:

1. Scroll to USER PROFILES > DELETE.
2. Scroll through the user profiles to the required profile.
3. Press SELECT
 - ⇒ You are prompted to confirm deletion.

4. Press SELECT to delete the user profile.

16.21 SMS

The SPC system support SMS alerts to be communicated from the panel to the engineer and selected users' mobile phones (SMS events) in addition to allowing users to control the SPC system remotely via SMS (SMS control). These two features work hand in hand as it allows the user to respond to a SMS notification without the need to be physically at the premises.

A maximum of 32 (SPC4xxx), 50 (SPC5xxx) or 100 (SPC6xxx) SMS IDs can be configured for each panel. An SMS-enabled modem and an appropriate system and user configuration are required to enable SMS communications.

Depending on the SMS AUTHENTICATION mode selected (see OPTIONS [→ 111] menu), SMS user authentication can be configured to use various combinations of the user's PIN and Caller ID or SMS PIN and Caller PIN.



The SMS notification can operate with a PSTN modem if the PSTN operator supports SMS over PSTN whereas SMS control will need a GSM modem at the panel. A GSM modem will support both SMS notification and control.

SMS control

The SMS control can be set up so that a remote user can send an SMS message to perform the following actions at the panel:

- Setting / unsetting
- Enable / disable engineer
- Enable / disable manufacturer access.
- Mapping gate on/off.

SMS events

The SMS notification can be set up to send a range of events that occur on the system such as:

- Alarm activation
- Confirmed alarms
- Fault & tamper
- Setting & unsetting
- Inhibit & isolate
- All other types of events

16.21.1 Add

- ▷ A modem is installed and identified by the system.
 - ▷ The function **SMS Authentication** is activated in OPTIONS [→ 111].
1. Scroll to SMS -> ADD and press SELECT.
 2. Select a user to add for SMS operation.
 3. Enter an SMS NUMBER for this user and press ENTER.
 4. Enter an SMS PIN for this user and press ENTER.
- ⇒ Keypad indicates that SMS details are updated.

16.21.2 Edit

- ▷ A modem is installed and identified by the system.
 - ▷ The function **SMS Authentication** is activated in OPTIONS [→ 111].
1. Scroll to SMS -> EDIT and press SELECT.
 2. Select an engineer or user SMS ID to edit.

SMS ID	System generated ID.
SMS Number	Enter the number to which the SMS will be sent (requires three-digit country code prefix). Note: Engineer SMS number can be deleted by resetting it 0. User SMS numbers cannot be deleted.
User	Select a new user for this SMS ID if required.
SMS Events	Select the panel events which the user or engineer will receive via SMS.
SMS Control	Select the operations that the user or engineer can perform remotely on the panel through SMS. See SMS Commands [→ 191]



NOTICE

HOLDUP alarm events are not transmitted via SMS.



If the phone line is connected to the PSTN network via a PBX, the appropriate line access digit should be inserted before the called party number. Ensure that **Calling Line Identity (CLI)** is enabled on the line selected to make the call to the SMS network. Consult the PBX administrator for details.

16.21.3 Delete

1. Scroll to SMS -> DELETE.
 2. Scroll to the required SMS ID.
 3. Press SELECT.
- ⇒ The keypad indicates that the SMS information is updated.

16.22 X-10



As of version 3.4, X-10 is in maintenance. The functionality remains in the product for backward compatibility.

X10 is a technology that allows peripheral devices, such as lights or appliances, to be controlled by the system and system events can be used to trigger outputs on the X10 devices. The SPC controller provides a dedicated serial port (serial port 1) for interfacing directly with standard X10 equipment.

1. Scroll to X-10 and press SELECT.

2. Scroll to the desired programming option:

ENABLE X-10	To enable or disable the X-10 functionality on the system.
DEVICES	To add, edit, delete or test X-10 devices.
LOGGING	To enable or disable the X-10 logging.

16.23 Set Date/Time

The date and time can be manually entered on the system. The time and date information is displayed on the keypad and browser and is used on time-related programming features.

1. Scroll to SET DATE/TIME and press SELECT.
 - ⇒ The date displays on the top line of the display.
2. To enter a new date, press the required numeric keys. To move the cursor to the left and right, press the left and right arrow keys.
3. Press ENTER to save the new date.
 - ⇒ If an attempt is made to save an invalid date value, the text INVALID VALUE is displayed for 1 second and the user is prompted to enter a valid date.
4. To enter a new time, press the required numeric keys. To move the cursor to the left and right, press the left and right arrow keys.
5. Press ENTER to save the new time.
 - ⇒ If an attempt is made to save an invalid time value, the text INVALID VALUE is displayed for 1 second and the user is prompted to enter a valid time.

16.24 Installer Text

This setting allows the engineer to enter system information and engineer contact information.

1. Scroll to INSTALLER TEXT and press SELECT.
2. Scroll to the desired programming option:

SYSTEM NAME	Used to help identify the system; use a clear and descriptive name for the installation.
SYSTEM ID	Used to help identify the installation when connected to a central station (max. 10 digits).
INSTALLER NAME	Used for contact purposes.
INSTALLER PHONE	Used for contact purposes.
DISP. INSTALLER	Setting to display installer details can during the idle state.



The installer contact details programmed in these menu options should also be entered on the keypad pull-down label on completion of the installation.

16.25 Door Control

This option allows you to control all the doors of the system.

1. Scroll to DOOR CONTROL and press SELECT.
2. Select the door which should be controlled and press SELECT.
3. Select one of the door states listed below as new door state and press SELECT.

NORMAL	The door is in normal operation mode. A card with the corresponding access rights is needed to open the door.
MOMENTARY	The door is opened only for a timed interval to allow access.
LOCKED	The door is locked. The door remains closed even if a card with the corresponding access rights is presented.
UNLOCKED	The door is unlocked.

16.26 SPC Connect

Add an SPC Connect ATS to set up a connection between a panel and the SPC Connect website <https://www.spconnect.com>. This enables a panel user to register and access their panel remotely using the SPC Connect website. If SPC Connect is not enabled during the start up wizard sequence, you can use this menu to add an SPC Connect ATS. If SPC Connect was enabled during start up, this menu shows the Registration ID for a panel.

ADD	If SPC CONNECT was disabled during the start up wizard, the ADD menu displays. Select ADD to create an SPC Connect ATS. This allows a panel user to register their panel and access their panel remotely using the SPC Connect website, https://www.spconnect.com
REGISTRATION ID	If SPC CONNECT was enabled during the start up wizard, the panel registration ID displays. Provide this information to an end user to allow them to register their panel with the SPC Connect website, https://www.spconnect.com , for remote access to their panel.
COMPANY ID	For future use.
DELETE	To remove an SPC Connect ATS from a panel, select DELETE.

17 Engineer programming via the browser

Engineer programming options on the SPC panel can be accessed via any standard web browser on a PC and is PIN protected.

You can access Engineer Programming via the browser by entering the default Engineer PIN (1111). For more details, see Engineering PINs [→ 102].

This web server provides access to the complete set of programming features used to install and configure the SPC system.



This programming option should only be provided to authorized installers of the SPC system.

Engineer Programming features on the SPC are divided into the following categories:

Soft Engineer Features

These features can be programmed without requiring the alarm system to be deactivated; they are accessible directly upon entering Engineer mode.

Full Engineer Features

These features require the alarm system to be deactivated before programming can commence; these features are accessible under the Full Engineer menu.

!	NOTICE
	If 'Engineer Exit' option is enabled in System Options, the engineer is allowed leave Full Engineer mode with alerts active but must acknowledge all alerts listed on the keypad or in the browser before switching from Full Engineer mode to Soft Engineer mode.

The web server on SPC controller can be accessed using either the Ethernet or USB interface.



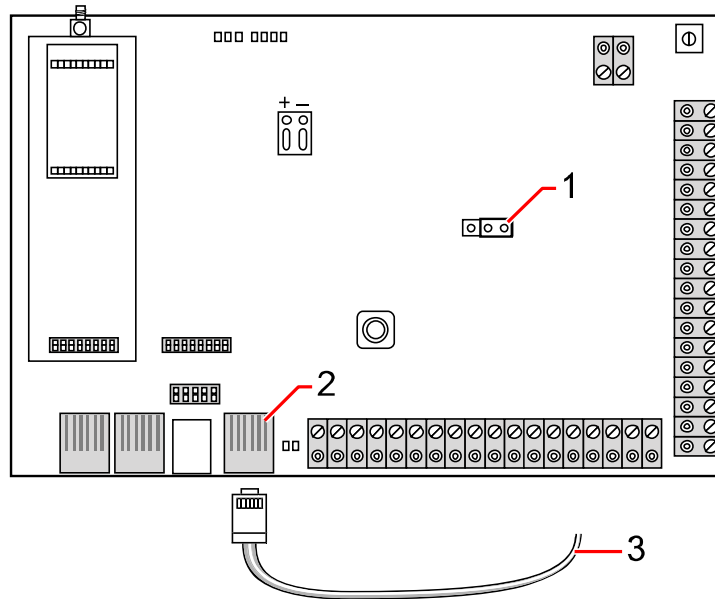
If programming with a browser interface, click **Save** when making changes. Click **Refresh** to view the current programming values on a web page.

17.1 System Information

Click the ? icon to view the Help menu which provides up-to-date information about the panel and the functionality that is currently licensed on the system.

17.2 Ethernet interface

IP



Connect

1	JP9 SPC4xxx
2	Ethernet port
3	To Ethernet port on PC



If the SPC Ethernet interface is connected to an existing **Local Area Network (LAN)**, please consult the network administrator for that LAN before connecting to the panel. Default IP Address: 192.168.1.100

Connect the cable

- Connect an Ethernet cable from the Ethernet interface on the PC to the Ethernet port on the controller board
– OR –
If connecting directly from a PC then a cross over-cable must be used. See page [→ 332].
- ⇒ The LEDs to the right of the Ethernet interface indicate a successful data connection (Right LED on) and Ethernet data traffic (Left LED flashing).

Determine the IP address of the SPC controller

1. Entering the Engineer mode (See Engineering PINs [→ 102]).
2. Using the up/down arrow keys, scroll down COMMUNICATION option and press SELECT.
3. Scroll to ETHERNET PORT and press SELECT.
4. Scroll to IP ADDRESS and press SELECT.

17.3 Connecting to the panel via USB



If the panel is reset while the USB cable is connected, the cable must be unplugged and plugged in again.

The USB port on the controller connects to a PC via a standard USB type A or type B cable. Drivers must be installed to make a USB connection from the controller to the PC.

- ▷ SPC Pro must be installed on your PC.
- ▷ USB cable connecting your PC to the panel.
- 1. Connect the USB cable from the controller to a USB interface on the PC.
 - ⇒ The **Found New Hardware** wizard is displayed.
- 2. Press **Next** .
 - ⇒ Windows XP detects a Generic USB hub.
- 3. Click Finish.
 - ⇒ Windows XP detects the SPC – Advanced Security System on COM port N, where N is the number of the COM port assigned to the device.
- 4. Make a note of the COM port assigned to the device, it is required later in the process.
 - ⇒ The **Found New Hardware** wizard is displayed again.
- 5. Select **Install the software automatically**.
- 6. If the Windows XP driver installation wizard asks you to select the best match from a list, choose the following option:
 - ⇒ **Vanderbilt Intrunet SPC USB Local Connection**
- 7. Click **Next**.
 - ⇒ A dialog box regarding Windows certification appears. Vanderbilt deems this acceptable to continue. For further queries, please contact network administrator or a Vanderbilt technician.
- 8. Click **Continue Anyway**.
 - ⇒ The installation finishes.
- 9. Click Finish.
 - ⇒ The driver is installed.

Configuring the connection on Windows XP

To set up the new connection on the PC:

1. Click on the Start command.
2. Select **Connect To > Show All Connections > Create A New Connection**.
3. In the New Connection Wizard, select **Setup an advanced connection**.
4. Select the Advanced Connection Option, **Connect directly to another computer**.
5. Select **Guest** as the role for this PC.
6. Enter a name for the connection.
7. Select an available serial port for use with the connection. This port should be the COM port that the USB device is using.

8. Select if this connection is available to all users or just yourself.
9. On the last dialog of the wizard, click **Finish**.
10. The PC prompts for username and password for the USB connection. Enter the following details:
 - Username: SPC
 - Password: password (default)
11. Click **Connect**.
 - ⇒ The PC initiates a data link with the controller. When the link has been established, a connection icon appears on the task bar at the bottom of the PC screen.
12. Right-click the link and select **Status**.
 - ⇒ A server IP address is displayed in the details window.
13. Enter this address into the address bar of an internet browser using the **hyper text transfer protocol secure** (e.g. <https://192.168.5.1>).
14. Login into the SPC browser application using your user PIN.



Your default PIN should be changed immediately and noted. Forgotten PINs are remedied only by a factory default of the system, resulting in a reset of the system configuration. The configuration can be restored if a backup is available.

Windows 7

- ▷ Perform all actions described in USB Connection on Windows 7 for SPCPro
 - ▷ You must have Local Administrator rights to perform the actions in this task.
1. Open the Windows 7 Control Panel.
 2. Select **Phone and Modem**.
 - ⇒ The **Phone and Modem** window is displayed,
 3. Select the **Modems** tab and click **Add**.
 - ⇒ The **Add Hardware Wizard – Install New Modem** window is displayed.
 4. Click **Next** twice.
 - ⇒ The **Add New Hardware** wizard displays a list of modems.
 5. Select **Communications cable between two computers**.
 6. Click **Next**.
 7. Select the COM port assigned in USB Connection on Windows 7 for SPCPro.
 8. Click **Next**, then **Finish**.
 9. Return to the **Modems** tab of the **Phone and Modem** window.
 10. Select the new modem and click **Properties**.
 - ⇒ The **Communications cable between two computers Properties** window is displayed.
 11. In the **General** tab, click **Change Settings** to allow editing of the properties.
 12. Select the **Modem** tab.
 13. Change the value in the **Maximum Port Speed** to **115200** and click **OK**.

14. From the **Control Panel**, open the **Network and Sharing Center**.
15. Click **Change Adapter Settings**. If a new modem is present in the list of available connections, proceed to step 23. If the modem is *not* present, perform the following steps.
16. In the **Network and Sharing Center**, click **Set up a new connection or network**.
17. Select **Set up a dial-up connection** and click **Next**.
18. Enter any values in the **phone number**, **User name** and **Password** fields and enter a name in the **Connection Name** field.
19. Click **Connect**.
 - ⇒ Windows 7 creates the connection.
20. Skip the **Testing Internet Connection** process.
21. Click **Close**.
22. In the **Network and Sharing Center**, click **Change adapter settings**.
23. Double-click on the new modem.
 - ⇒ The **Connect *ConnectionName*** window opens, where *ConnectionName* is the name you defined for the modem.
24. Click **Properties**.
25. Ensure the **Connect using:** field contains the correct information, Communications cable between two computers (COM3), for example.
26. Open your browser and enter the IP address of the Controller using https as the connection protocol.
27. Click **Continue Anyway** if the browser displays a certificate error page.
28. Log on to the panel.

17.4 Logging into the browser

To log into the browser:

1. When an Ethernet or USB link is established and the IP address of the controller determined, open the PC browser.
2. Enter the IP address in the address bar of the browser using the **hyper text transfer protocol secure**. (e.g. https:// 192.168.1.100) See table below.
 - ⇒ A window with a security message is displayed.
3. Click **Continue to this website**.
 - ⇒ The login screen is displayed.

4. Enter the following:
 - **User ID:** user or engineer name
 - **Password:** User or Engineer PIN.
5. Select a language in which to display the browser screens. The default language setting 'Auto' will automatically load the language assigned to this user ID.
6. Click **Login**.

Default settings for WEB server address

Connection	IP address Web server
Ethernet	192.168.1.100 (default)
RS232	192.168.2.1 (fixed)
Backup Modem / RS232	192.168.3.1 (fixed)
Primary Modem	192.168.4.1 (fixed)
USB	192.168.5.1 (fixed)

17.5 SPC Home

The SPC Home page has a **System Summary** tab, **Alarms** tab and **Video** tab.

17.5.1 System Summary

The **System Summary** tab is divided into the following three sections:

- **System:** shows the status of all areas, active system alerts and warnings and information for the system.
- **Areas:** shows the status of each area defined on the system with up to 20 alarm events. You can set or unset an area and the area status displays here.
- **Inhibits and Isolates:** Lists all the isolated zones and allows you to deisolate or bypass before setting.

System Summary	Alarms	Video
System		
All Areas	Partial Set	Unset
Active System Alerts		
None		
Areas		
Area 1: Marketing	Fullset	Unset
Preventing Setting		
Area -Vault 7	Information	
Area 2: Cafeteria	Unset	Fullset
Area 3: Finance	Unset	Fullset
Area 7: Vault	Unset	Fullset
Inhibits and Isolates		
Zone: Front door - Isolated	Isolated	Deisolate
Zone: Vault - Isolated	Isolated	Deisolate
Zone: Window 2 - Isolated	Isolated	Deisolate

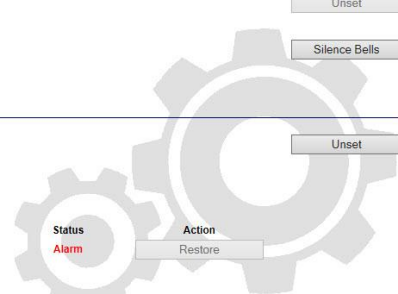
!	<p>NOTICE</p> <p>If there are alarms on the system, the information message See alarm tab displays.</p>
----------	---

17.5.2 Alarms Overview

The **Alarms** tab shows the following system information:

- **Alarm Set State** - shows whether the system was partial or fullset at the time the alarm was triggered.
- **Alarm Status** - shows the type of alarm (alarm, confirmed alarm etc.)
- **Bells active** - shows if the alarm activated the bells. Click the **Silence Bells** button to cancel.

For each area, the **Alarm Set State**, **Alarm Status**, **Alarm Activations** and **Alarm log** displays. The **Alarm Activations** show a list of zones in alarm state ordered by activation. Click the **Restore** button to clear. The **Alarm log** shows up to 20 events.

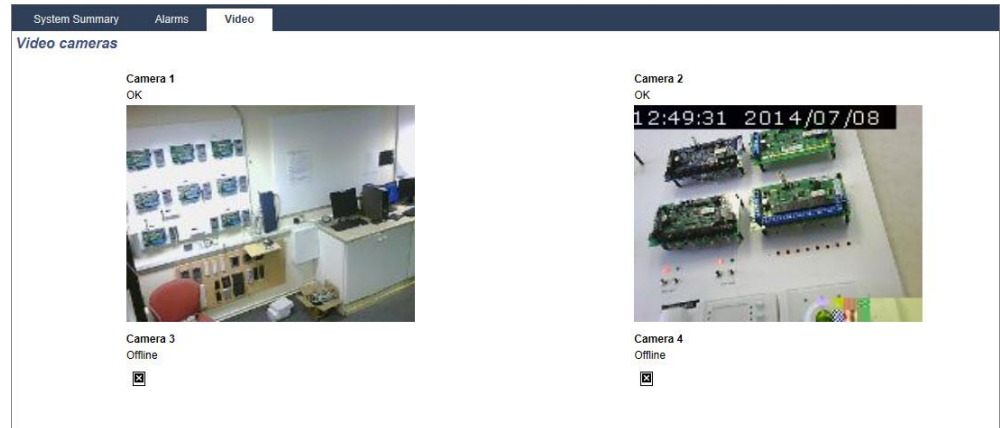
System Summary	Alarms	Video
Refresh		
System		
Alarm Set State	Fullset	Unset
Alarm Status	Alarm	
Bells active	Bells active	Silence Bells
Area 1: Marketing		
Alarm Set State	Fullset	Unset
Alarm Status	Alarm	
Area 1 Alarm Activations		
Activation Time	Zone	Zone Type
Today 12:52:37	35: Zone 35	Alarm
		Input
		Open
<div style="display: flex; justify-content: space-between;"> Area 1 Alarm log <div style="text-align: right;">  </div> </div>		

17.5.3 Viewing Video

The **Video** tab displays images from up to 4 IP cameras.

- In Full Engineer, Soft Engineer and User mode, select **SPC Home > Video**.

⇒ All the configured and operational cameras (up to the maximum of four) are displayed in the **Video Cameras** page. Only two cameras are available in the following example.



The images are automatically refreshed as per the interval settings for the camera. (See Configuring Video [→ 257])

Click on the **Pause Refresh** button to retain the current image on the screen and pause refreshing. Click on the **Resume Refresh** button to enable the panel to resume refreshing the images.

Note: Ensure that a resolution of 320 x 240 is selected for the cameras that will be displayed in the browser otherwise images may not be displayed correctly. The higher resolution of 640 x 480 can be used for operation with SPC Pro and SPC Com.

Video Fault Reporting

A video fault report is displayed above the camera image. The following table lists the possible messages:

Message	Description
OK	The camera is behaving normally
Timeout	Camera connection timed out.
Socket Invalid	Internal socket handling error
Image too small	Received image too small
Buffer too small	Received image is too large. Lower the resolution in the Camera configuration.
Format incorrect	Invalid format received.
Abort	TCP connection disconnected
Internal	Alarm panel has insufficient memory to complete the request.
Bad request	A badly formed request was sent to the camera. Check your camera configuration settings.
Client error	The camera returned a client error. Check your camera configuration.
Authorization error	User name and/or password are incorrect
Unknown	An unknown error was returned. The camera may be an unsupported model.

17.6 Panel status

17.6.1 Status

This page displays the status and summary of the main SPC components, including system, power, X-BUS and communications.

1. Select **Status > Hardware > Controller Status**.
2. See tables below for further information.

Hardware	Inputs	Outputs	Doors	FlexC	System Alerts
Controller Status					
System			Ethernet		
System Time:	Mon, 07 Jul 2014 10:24:53		MAC Address:	00:0F:B6:03:1A:F1	
Cabinet Tamper:	Isolate		IP Address:	10.100.82.181	
Aux. Tamper 1:	OK		Netmask:	255.255.0.0	
Aux. Tamper 2:	OK		Gateway:	0.0.0.0	
Bell Tamper:	Isolate		Receive:	21 M Packets, 3199 M Bytes	
Wireless Module:	SiWay - V5		Transmit:	4 M Packets, 366 M Bytes	
Antenna Tamper:	OK				
Power			Modem 1		
Mains:	OK		Modem Status:	Line Fault	
Mains time sync.:	OK (50Hz)		Type fitted:	IntelliModem PSTN	
Battery:	Isolate		Line Status:	Fault	
Battery Voltage:	N/A		Incoming Calls:	0 (0 Seconds)	
Battery Current:	N/A		Outgoing Calls:	0 (0 Seconds)	
Aux. Voltage:	13.6V		Incoming SMS:	0	
Aux. Current:	200mA		Outgoing SMS:	0	
Aux. Fuse:	OK		Failed Dial Attempts:	0	
Ext. Bell Fuse:	OK				
Int. Bell Fuse:	OK				
X-BUS			Modem 2		
Cable status:	OK		Modem Status:	Fault: E51 [Isolate]	
Devices: Online:	11		Type fitted:	IntelliModem GSM	
Devices: Comms:	OK		Line Status:	Isolate	
Devices: Lid tamper:	Isolate		Incoming Calls:	0 (0 Seconds)	
Devices: Ant. Tamper:	OK				

Performable actions

The following actions are only possible if a connection has been established.

Restore All Alerts <input type="button" value="Pro"/>	Restores all active alerts on the panel. These alerts messages are displayed in red text opposite the relevant item.
Refresh	Updates any changes in panel status. You must refresh the status window to display the actual panel status at any particular moment.
Full Engineer / Soft Engineer	To toggle between Soft- and Full Engineer modes. Full Engineer mode disables alarms and prevents reporting of events to a central station.

17.6.2 X-Bus Status

1. Select **Status > Hardware > X-Bus Status**.

⇒ The following window with the status of the different X-Bus devices is displayed. All detected expanders are listed as default.

Hardware	Inputs	Outputs	Doors	FlexC	System Alerts		
Controller Status							
X-Bus Status			Wireless Status				
Expanders							
ID	Description	Type	SIN	Version	Comms.	Status	PSU
1	IND 1	Indicator [1 Input]	223387801	1.03 [13MAR13]	Online	OK	Not Fitted
2	KSW 2	Keyswitch [1 Output]	226593801	1.01 [11NOV10]	Online	Isolate	Not Fitted
3	IO 3	I/O [8 Output]	443907	1.11 [07AUG13]	Online	OK	Not Fitted
4	IOA 4	I/O Analyzed [8 Input / 2 Output]	165074801	2.00 [09Apr14]	Online	Isolate	Not Fitted
5	WIR 5	Wireless	489907	1.11 [07AUG13]	Online	Isolate	Not Fitted
6	AEX 6	Audio [4 Input / 1 Output]	37070907	1.03 [13MAR13]	Online	OK	Not Fitted
7	AEX 7	Audio [4 Input]	1434900	1.03 [13MAR13]	Online	OK	Not Fitted
8	IO 8	I/O [8 Input / 2 Output]	11327907	1.11 [07AUG13]	Online	Isolate	Type 1 - V4
<input type="button" value="Refresh"/>							

2. Select one of the following tabs.

- Expanders (for programming expanders see page [→ 204]).

- Keypads (for programming keypads see page [→ 209]).
 - Door controllers (for programming door controllers see page [→ 214]).
3. Click any of the keypad/expander/door controller identifying parameters (ID, description, type, serial number) to displayed further status details.

17.6.2.1 Expander Status

1. Select **Status > Hardware > X-Bus Status**.
2. Select the **Expanders** tab.

⇒ A list of detected expanders and any associated PSUs is displayed.

Hardware							
Controller Status							
X-Bus Status							
Wireless Status							
Expanders							
Keypads							
Door Controllers							
ID	Description	Type	S/N	Version	Comms.	Status	PSU
1	IND 1	Indicator [1 Input]	223387801	1.03 [13MAR13]	Online	OK	Not Fitted
2	KSW 2	Keyswitch [1 Output]	226593801	1.01 [11NOV10]	Online	Isolate	Not Fitted
3	IO 3	I/O [8 Output]	443907	1.11 [07AUG13]	Online	OK	Not Fitted
4	IOA 4	I/O Analyzed [8 Input / 2 Output]	165074801	2.00 [09Apr14]	Online	Isolate	Not Fitted
5	WIR 5	Wireless	489907	1.11 [07AUG13]	Online	Isolate	Not Fitted
6	AEX 6	Audio [4 Input / 1 Output]	37079907	1.03 [13MAR13]	Online	OK	Not Fitted
7	AEX 7	Audio [4 Input]	1434900	1.03 [13MAR13]	Online	OK	Not Fitted
8	IO 8	I/O [8 Input / 2 Output]	11327907	1.11 [07AUG13]	Online	Isolate	Type 1 - V4

Refresh

Expander ID	This ID number is a unique identifier for the expander.
Description	Text description of the expander. This text will also appear on the browser and keypad.
Type	The type of expander detected (I/O, PSU, keypad etc.).
S/N	The serial number of the expander.
Version	The firmware version of the expander.
Comms	The status of the expander (online or offline).
Status	The status of the expander (OK, Fault, OP Tamper).
PSU	The type of PSU that is fitted to the expander, if applicable. Click on the PSU to view the PSU status.

Performable actions

Refresh	Click the button to update the status of the X-BUS.
---------	---

To view more status information:

- Click on any of the expander's identifying parameters (ID, description, type, serial number) to display further status details.

	Input	Status	Action
Communication	OK	OK	Inhibit Isolate
Cabinet Tamper	Fault	Isolate	Deisolate
Fuse Fault	OK	OK	Inhibit Isolate
Mains Fault	OK	OK	Inhibit Isolate
Battery Fault	Fault	Isolate	Deisolate
PSU Fault	Fault	Isolate	Deisolate

Name	Description
Communication	The physical status (OK, Fault) and the programmed status (OK, Isolated, Inhibited) of the X-BUS cable connection to the expander.
Cabinet Tamper	The physical and programmed status of the expander cabinet tamper.
Fuse Fault	The physical and programmed status of the expander fuse.
Controller Mains Fault	The physical and programmed status of the mains supply to the controller.
Battery Fault	The physical and programmed status of the battery.
PSU Fault	The physical and programmed status of the PSU.
OP Tamper	The physical and programmed status of the tamper outputs on the PSU.
Low Voltage	Indication of battery low voltage status.

Performable actions

Name	Description
Restore Alerts	Click the button to restore all alerts on the panel.
Inhibit ⓘ	Click this button to inhibit a fault condition. The inhibit operation will disable that fault or zone for one arming period only. Inhibit operation is not available in Security Grade EN 50131 Grade 3.
Isolate	Click this button to isolate that zone. Isolating a zone will deactivate that zone until such time as the zone is explicitly de-isolated again. It is recommended that you exercise caution when isolating zones as those zones will not be active every time the system is SET.

See also

 [PSU status \[→ 170\]](#)

17.6.2.2 PSU status

The **PSU Status** window displays details of the current status of the PSU and its outputs in addition to the status of any connected batteries.

The following PSU types are supported:

- SPCP332/333 Smart PSU
- SPCP355.300 Smart PSU

SPCP332/333 Smart PSU Status

The following image shows the Smart PSU status:



PSU Status	
Type	1
Version	4
Mains status	OK
Battery link	7Ah Battery
Battery status	Fully charged
Battery Voltage	13.4V
Battery Current	0mA

Name	Description
Type	The type of power supply unit (PSU).
Version	The version of the PSU.
Mains Status	Displays the condition of the mains connection. Possible values are Fault or OK.
Battery Link	Displays the type of battery connected.
Battery Status	Displays the condition of the battery connection. Possible values are Fault or OK.
Battery Voltage	Displays the voltage reading of the battery.
Battery Current	Displays the current taken from the battery.

Name	Description
Outputs	Displays the voltage on the outputs, the current drawn by the output and the condition of the fuse on the output.

SPCP355.300 Smart PSU Status

The following image shows the SPCP355.300 Smart PSU status.

PSU Status			
Type	Vds PSU		
Version	Hardware Version: 1 Firmware Version: 1.1 [04JUL13]		
Mains status	OK		
Temperature	23 °C		
Load Voltage	14.4 V		
Load current	16 mA		
Charge status	N/A		
Primary Circuit	OK		
Charge Circuit	OK		
Battery			
		Voltage	Current
Battery 1	Fault or Missing	0.0V	0mA
Battery 2	Fault or Missing	0.0V	0mA

Name	Description
Type	The type of power supply unit (PSU).
Version	The version of the PSU.
Mains Status	Displays the condition of the mains connection. Possible values are Fault or OK.
Temperature	Displays the temperature of the PSU.
Load voltage	The voltage on the PSU
Load Current	The current drawn by the PSU.
Charge Status	Displays the condition of the battery charge.
Primary Circuit	Displays the condition of the primary circuit which supplies power when the mains is connected.
Charge Circuit	Displays the condition of the charge circuit which charges the batteries when the mains

Name	Description
	is connected.
Battery	Displays the charge status, voltage and current available from the batteries.
Outputs	Displays the voltage, fuse condition and tamper condition of the PSU outputs.

17.6.2.3 Keypad Status

1. Select **Status > Hardware > X-Bus Status**.

2. Select the **Keypads** tab.

⇒ A list of detected keypads is displayed.

ID	Description	Type	S/N	Version	Comms.	Status
1	KEY 1	Keypad	559907	2.09 [13MAR13]	Online	OK
2	CKP 2	Comfort Keypad	227361801	1.02 [13MAR13]	Online	OK

Refresh

Name	Description
Expander ID	This ID number is a unique identifier for the keypad.
Description	Text description of the keypad (max. 16 characters).
Type	The type of expander detected (=keypad).
S/N	The serial number of the keypad.
Version	The firmware version of the keypad.
Comms	The status of the keypad (online or offline).
Status	The status of the keypad (OK, Fault).

Performable actions

Refresh	Click on the refresh button to update the list of detected keypads and their status.
---------	--

To view more status information:

- Click on a keypad's identifying parameters (ID, description, type, serial number) to display further status details.

Communication	The physical status (OK, Fault) and the programmed status (OK, Isolated, Inhibited) of the keypad cable connection to the expander.
Cabinet Tamper	The physical and programmed status of the expander cabinet tamper.
PACE	Applies only to Keypads with a PACE receiver installed.
Panic	Keypad panic alarm status.
Fire	Keypad Fire alarm status.
Medical	Keypad medical alarm status.
Code Tamper	Keypad PIN tamper alarm status

Performable actions

Restore Alerts	Click the button to restore all alerts on the panel.
Inhibit ⓘ	Click this button to inhibit a fault condition. The inhibit operation will disable that fault or zone for one arming period only. Inhibit operation is not available in Security Grade EN 50131 Grade 3.
Isolate	Click this button to isolate that zone. Isolating a zone will de-activate that zone until such time as the zone is explicitly de-isolated again. It is recommended that you exercise caution when isolating zones as those zones will not be active every time the system is SET.

17.6.2.4 Door Controller Status

1. Select **Status > Hardware > X-Bus Status**.
2. Select the **Door Controllers** tab.
⇒ A list of detected door controllers is displayed.

Expander ID	This ID number is a unique identifier for the door controller.
-------------	--

Description	Text description of the door controller (max. 16 characters).
Type	The type of expander detected (=door controller).
S/N	The serial number of the door controller.
Version	The firmware version of the door controller.
Comms	The status of the door controller (online or offline).
Status	The status of the door controller (OK, Fault).
PSU	Specifies if the door controller has a PSU.

Performable actions

Refresh	Click on the refresh button to update the status of the system alerts.
---------	--

To view more status information:

- Click on a door controller's identifying parameters (ID, description, type, serial number) to display further status details.

	Input	Status	Action
Communication	OK	OK	Inhibit Isolate
Cabinet Tamper	Fault	Isolate	Deisolate
Fuse Fault	OK	OK	Inhibit Isolate
Code Tamper	OK	OK	Inhibit Isolate

Communication	The physical status (OK, Fault) and the programmed status (OK, Isolated, Inhibited) of the keypad cable connection to the expander.
Cabinet Tamper	The physical and programmed status of the expander cabinet tamper.
Fuse Fault	The physical and programmed status of the door controller fuse.
Code Tamper	Status of the user's PIN. Multiple failed attempts result in an alert.

Performable actions

Restore Alerts	Click the button to restore all alerts on the panel.
Inhibit ⓘ	Click this button to inhibit a fault condition. The inhibit operation will disable that fault or zone for one arming period only. Inhibit operation is not available in Security Grade EN 50131 Grade 3.
Isolate	Click this button to isolate that zone. Isolating a zone will de-activate that zone until such time as the zone is explicitly de-isolated again. It is recommended that you exercise caution when isolating zones as those zones will not be active every time the system is SET.

17.6.3 Wireless

Wireless sensor detection (868 MHz) on the SPC panel is provided by wireless receiver modules which may be factory fitted on the keypad or on the controller, or by installing a wireless expander.

1. Select **Configuration > Hardware > Wireless > Wireless**.
2. See table below for further information.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Wireless		WPA	Wireless Settings					
Sensor ID	Type	Received	Status	Receiver	Signal	Enrol		
26662468	Magnetic contact	07/07/2014 15:00:50	Close	Wireless 5	High (9)	Enrol		
58749154	PIR	07/07/2014 14:59:28	Open	Wireless 5	High (9)	Enrol		
26589639	Magnetic contact	07/07/2014 14:59:08	Close	Wireless 5	High (9)	Enrol		
58906531	PIR	07/07/2014 14:58:04	Close	Wireless 5	High (9)	Enrol		
26329994	Magnetic contact	07/07/2014 14:57:50	Close	Controller	High (9)	Enrol		
26422346	Magnetic contact	07/07/2014 14:57:36	Close	Wireless 5	High (9)	Enrol		
26661509	Magnetic contact	07/07/2014 14:56:12	Close	Wireless 5	High (9)	Enrol		
26220868	Magnetic contact	07/07/2014 14:55:13	Close	Wireless 5	High (9)	Enrol		
58749154	PIR	07/07/2014 14:54:28	Close	Wireless 5	High (9)	Enrol		
58732159	PIR	07/07/2014 14:54:26	Close	Wireless 5	High (9)	Enrol		
26661909	Magnetic contact	07/07/2014 14:54:02	Open	Wireless 5	High (9)	Enrol		
26661450	Magnetic contact	07/07/2014 14:53:27	Open	Wireless 5	High (9)	Enrol		

Sensor	The number of the sensor enrolled on the system (1 = first, 2 = second, etc.)
ID	A unique identity number for that sensor.
Type	The type of wireless sensor detected (magnetic contact, inertia/shock, etc.)
Zone	The zone to which the sensor has been enrolled.
Battery	The status of the battery in the sensor (if fitted).
Supervise	The status of the supervisory operation (OK = supervisory signal received, Not Supervised = no supervisory operation).
Signal	The signal strength received from the sensor (01=low, 09=high). Note: Although it is not possible to enroll a device with a signal strength less than 3, devices whose signal drops below 3 after enrollment are not dropped.

Performable actions

Log	Click to view the wireless sensor Log. See page [→ 176].
Enrol	Click to open the list of unenrolled wireless devices.

1. Select **Status > Hardware > Wireless > WPA**.
2. The identity of each enrolled WPA and its status displays.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Wireless	WPA	Wireless Settings						

Configure Wireless Personal Alarm (WPA)

WPA: 1

Description:

Transmitter ID:

Supervise: Check if WPA should be supervised. (Note: This requires the supervision link to be fitted on the WPA.)

Test: Check if the WPA requires a manual test according to test schedule.

Assignment of Functions to Buttons

Red:

Green:

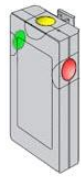

Yellow:

Red + Green:

Red + Yellow:

Yellow + Green:

Red + Yellow + Green:

17.6.3.1 Log - Wireless sensor X

To view a quick log of events for a wireless sensor:

1. Click the **Log** button.
2. See table below for further information.
3. Create a text file of the log by clicking **Text File**.

Date/Time	The date and time of the logged event.
Receiver	The wireless receiver location, i.e. wireless module mounted on the keypad, controller or wireless expander.
Signal	The signal strength received from the sensor (01=low, 09=high).
Status	The physical status of the sensor.
Battery	The status of the battery connected to the sensor (OK, Fault).

17.6.4 Zones




For configuration see page [→ 237].

1. To view all zones, select **Status > Inputs > All Zones**. To view X-Bus only zones, select the **X-Bus Zones** tab or to view wireless zones only, select the **Wireless Zones** tab.
2. See tables below for further information.

Hardware	Inputs	Outputs	Doors	FlexC	System Alerts				
All Zones		X-Bus Zones	Wireless Zones						
Zones Active 37, Max Zones 512									
Zone	Area	Zone Type	EOL Quality	Input	Status	Log	Action		
1 Front door	2 Reception	Entry/Exit	Good [4.7kΩ]	Closed	Isolate	Log	Deisolate		
2 Fire Exit	4 Cafeteria	Entry/Exit	Good [4.7kΩ]	Closed	Isolate	Log	Deisolate		
3 Window 2	5 Meeting Room	Alarm	Good [4.7kΩ]	Closed	Isolate	Log	Deisolate		
4 PIR 1	1 Marketing	Alarm	Good [4.7kΩ]	Closed	Isolate	Log	Deisolate		
5 PIR 2	3 Finance	Alarm	- [∞]	DISCON	Isolate	Log	Deisolate		
6 Fire Exit	1 Marketing	Fire Exit	- [∞]	DISCON	Isolate	Log	Deisolate		
7 Fire alarm	1 Marketing	Fire	- [∞]	DISCON	Isolate	Log	Deisolate		
8 Panic Button	1 Marketing	Panic	- [∞]	DISCON	Isolate	Log	Deisolate		
9 Zone 9	1 Marketing	Alarm	Good [4.6kΩ]	Closed	Normal	Log	Inhibit	Isolate	Soak
10 Entry	1 Marketing	Entry/Exit	Good [4.7kΩ]	Closed	Normal	Log	Inhibit	Isolate	Soak
12 DOOR 2	1 Marketing	Entry/Exit	Good [4.7kΩ]	Closed	Normal	Log	Inhibit	Isolate	Soak
33 Zone 33	1 Marketing	Alarm	Good [4.7kΩ]	Closed	Isolate	Log	Deisolate		
34 Zone 34	1 Marketing	Alarm	Good [4.7kΩ]	Closed	Isolate	Log	Deisolate		
35 Zone 35	1 Marketing	Alarm	Good [4.7kΩ]	Closed	Post alarm	Log	Restore		
36 Zone 36	1 Marketing	Alarm	Good [4.7kΩ]	Closed	Normal	Log	Inhibit	Isolate	Soak










Auto Status Refresh <input type="button" value="Pro"/>	Tick this button to activate an automatically refreshing of the zone summary. This can only be done for all zones, and not for filter zones.
Zone Description	Text description of the zone (max. 16 characters).
Area	Areas to which this zone is assigned.
Zone Type	The type of zone (Alarm, Entry/Exit, etc.).
EOL Quality	<p>Displays the EOL quality for the zone state resistance range. Possible values are:</p> <ul style="list-style-type: none"> ● Good — Nominal value +/-25% of the defined range. ● OK — Nominal value +/- 50% of the defined range. ● Poor — Nominal value +/- 75% of the defined range. ● Unsatisfactory — any other value. ● Noisy — indicates a problem detecting the signal. The cabling may be in close proximity to a mains cable or other source of interference. <p>This column is only visible in Engineer mode. For more information on nominal resistance values and their defined ranges, see Wiring the zone inputs [→ 83].</p>
Input	<p>The detected input state of that zone (Unknown, Open, Closed, Disconnect, Short, Pulse, Gross, Masked, Fault, Out of bounds, Unstable, DC Sub, Noisy).</p> <p>DC Sub is an input tamper alert. DC substitution performs a periodic check to ensure that no external voltages are being applied to that circuit.</p> <p>Unstable: An unstable state occurs when the zone input resistance value is not stable over a defined sampling period.</p> <p>Noisy: A Noisy state occurs when an external interference is induced onto the input circuit over a defined sampling period.</p> <p>Out Of Bounds: An Out of Bounds state will occur when the resistance value on the zone input does not come within accepted tolerances of the present EOL values.</p>
Status	<p>The programmed status of that zone. A status value of Normal means that the zone is programmed to operate normally. The following is a complete list of possible values:</p> <p>Isolate, Soak, Inhibit, Tamper, Alarm, Fire Exit, Warning Fault, Holdup Fault, Detector Fault, Line Fault, Panic, Hold Up, Tech, Medic, Lock, Fire, Trouble, PIR Masked, Normal, Actuated, Tamper, Post Alarm. A zone is in the post alarm status if an alarm occurred and the confirmed alarm timed out. This reinstates the zone, however it also flags that an alarm did occur.</p>


Performable actions

Refresh	Updates the status information displayed for the panel.
Log	Click on the Log button to view a log of the input status of that zone.
Inhibit 	Click this button to inhibit a fault or open zone. The inhibit operation will disable that fault or zone for one arming period only. Inhibit operation is not available in Security Grade EN 50131 Grade 3.
Restore	Click this button to restore the alarm condition of the panel.
Isolate	Zone . Isolating a zone will deactivate that zone until such time as the zone is explicitly deisolated again. It is recommended that you exercise caution when isolating zones as those zones will not be active every time the system is SET.
Soak	Highlight a zone and click this button to perform a Soak test on that zone.
Seismic Test 	Click this button to initiate a test of the selected seismic sensor. For more information on seismic sensors, see Seismic Sensors [→ 324].
Hide Closed	Click this button to hide all closed inputs.
Filter Zones 	Select a zone type from the dropdown menu. Only the summary of this zone type will be displayed.

17.6.5 Doors

1. Select **Status > Doors**.
2. See tables below for further information.

Hardware		Inputs	Outputs	Doors	FlexC	System Alerts			
Door	Zone	Area	DPS	DRS	Status	Log	Action		
1	10 Entry	1 Marketing	Closed	Short	Door Normal				
2	12 DOOR 2	1 Marketing	Closed	Closed	Door Normal				
									

Door	This ID number is a unique identifier for the door.
Zone	The zone number the door position sensor is attached to (only if the door position sensor input is also used as intrusion zone).
Area	The area the door position sensor input and the card reader are assigned to.
DPS	Status of the door position sensor.
DRS	Status of the door release switch.
Status	The status of the door (OK, fault).
Door Mode 	Specifies the door operate mode.

Performable actions

Refresh	Updates the door summary.
Log	Displays a log of events for the selected door.
Lock	Locks the selected door.
Unlock	Unlocks the selected door.
Normal	Returns the door to normal system control.
Momentary	Unlocks the door for one timed interval.

17.6.6 FlexC Status

This screen displays the status of each ATS configured on your system.

1. To view the status of an ATS, go to **Status - FlexC**.
2. The table below describes the status criteria available for each ATS.

Hardware Inputs Outputs Doors **FlexC** System Alerts

FlexC Status

FlexC ATS: ATS 1

ATS Registration ID	T578-G5R9-92XG-SP2G	The unique registration ID of the ATS allows the panel to be uniquely identified at the RCT.
ATS Status	Fault	The Status of the ATS
Time since last Poll	4 Days 17hr 30min 51s	The time since the last poll on any ATP in the ATS.
Event Queue Count	250	No. of events in the event queue waiting to be transmitted
Event Queue	<input type="button" value="Event Queue"/>	List of the events currently in the Event Queue
Event Log	<input type="button" value="Event Log"/>	Event log history for all the events that have occurred on the ATS
Network Log	<input type="button" value="Network Log"/>	Network Log for the ATS

Status of ATPs within ATS

Seq No	ATP Name	Communications Interface	ATP Status	Last successful transmission	Network Log	ATP Log	Test call
1	Primary ATP 1	Ethernet	Fault	-	<input type="button" value="Network Log"/>	<input type="button" value="ATP Log"/>	<input type="button" value="Manual Test"/>
2	Backup ATP 2	Ethernet	Fault	-	<input type="button" value="Network Log"/>	<input type="button" value="ATP Log"/>	<input type="button" value="Manual Test"/>

ATS Registration ID	The unique registration ID of the ATS allows the panel to be uniquely identified at the RCT.
ATS Status	The status of the ATS, for example, initializing.
Time since last poll	The time since the last poll on any ATP in the ATS.
Event Queue Count	Number of events in the event queue waiting to be transmitted.
Event Queue Count	No. of events in the event queue waiting to be transmitted.
Event Queue	List of the events currently in the Event Queue. The tables shows the following: <ul style="list-style-type: none"> ● Event Seq No. ● Event Timestamp ● Event Description ● Additional Event Info ● Start Timestamp ● Report Duration
Event Log	Event log history for all the events that have occurred on the ATS. The table shows the same fields as Event Queue above and the following additional field: <ul style="list-style-type: none"> ● Event Seq No. ● Event Timestamp ● Event Description ● Additional Event Info ● Result ● Reported ATP ● Start Timestamp ● ACK/Fail Timestamp ● Report Duration
Network Log	Network log for the ATS showing the configured polling interval.

Status of ATPs within ATS	<p>This table shows each ATP in the ATS. For each ATP, the table shows the ATP sequence number, the ATP name, the communications interface, ATP Status, Last successful transmission, Network Log, ATP Log and Test Call button.</p> <p>Network Log: Click this button to show the network log.</p> <p>ATP Log: Shows a list of poll transmissions. Click the Refresh button to update the log. Click the Most Recent Last button to change the viewing order. By default the most recent event displays first.</p> <p>Manual Test button: Click this button to force a test call. The Event is added to the event queue.</p>
---------------------------	--

17.6.7 System alerts

1. Select **Status > System Alerts**.
2. See tables below for further information.

Hardware	Inputs	Outputs	Doors	FlexC	System Alerts			Action
Alert					Input	Status		Inhibit Isolate
Controller Mains Fault					OK	OK		Deisolate
Controller Battery Fault					Fault	Isolate		Inhibit Isolate
Controller PSU Fault					OK	OK		Inhibit Isolate
Controller Aux. Fuse Fault					OK	OK		Inhibit Isolate
Controller External Bell Fuse Fault					OK	OK		Inhibit Isolate
Controller Internal Bell Fuse Fault					OK	OK		Inhibit Isolate
Bell Tamper					Fault	Isolate		Deisolate
Controller Cabinet Tamper					Fault	Isolate		Deisolate
Controller Aux. Tamper 1					OK	OK		Inhibit Isolate
Controller Aux. Tamper 2					OK	OK		Inhibit Isolate
Controller Antenna Tamper					OK	OK		Inhibit Isolate
Controller RF Jamming					OK	OK		Inhibit Isolate
Modem 1 Fault					OK	OK		Inhibit Isolate
Modem 2 Fault					Fault	Isolate		Deisolate
Fail to communicate					OK	Isolate		Deisolate
User Duress					OK	OK		
User RF FOB Panic					OK	OK		
User Man Down Alarm					OK	OK		

Alert	Description of the system alert.
Input	The actual state of the alert that was detected on the panel (OK, Fault).
Status ⚠	The programmed status of the system alert, i.e. whether the alert has been isolated or inhibited. A status value of OK is displayed if the alert condition has not been disabled in any way (see page).

Performable actions

Refresh	Click this button to update the status of the system alerts.
Restore	Click this button to restore an alert on the panel
Inhibit !	Click this button to inhibit a fault condition. The inhibit operation will disable that fault or zone for one arming period only. Inhibit operation is not available in Security EN 50131 Grade 3.
Isolate	Click this button to isolate the zone. Isolating a zone will de-activate that zone until such time as the zone is explicitly de-isolated again. It is recommended that you exercise caution when isolating zones as those zones will not be active every time the system is SET.

17.7 Logs

17.7.1 System Log

This log displays all the system events of the SPC system.

1. Select **Log > System Log > System Log**.
2. Create a text file of the log by clicking **Text File**.
3. The logging of individual zone state changes is enabled by setting the log attribute for that zone in the Zone Attributes configuration page.

System log	Access log	Modem 1	Modem 2
System log	Alarm log	WPA Log	
System log			
04/07/2014 10:33:39 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 10:43:39 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 10:53:39 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 11:03:38 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 11:13:38 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 11:22:29 User 9999 WEB PASSWORD ADDED By User 9999 Engineer 04/07/2014 11:23:37 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 11:33:37 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 11:43:36 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 11:53:36 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 12:03:35 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 12:13:35 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 12:19:58 Panel in Soft eng mode 04/07/2014 12:19:58 Configuration changed 04/07/2014 12:20:01 WWW END, User 9999 Engineer 04/07/2014 12:20:08 WWW LOGIN FAILED INVALID ENTRY, IP 10.100.82.253 04/07/2014 12:20:17 WWW LOGIN FAILED INVALID ENTRY, IP 10.100.82.253 04/07/2014 12:20:23 WWW LOGIN OK, User 9999 Engineer, IP 10.100.82.253 04/07/2014 12:23:35 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 12:33:34 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 12:43:34 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 12:53:34 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 13:03:34 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 13:13:34 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)] 04/07/2014 13:23:34 FlexC ATS Event Timeout. [ATS=1, Event ID=6002 (FlexC ATP Down)]			



In order to avoid multiple events from the same source filling the log, the SPC system, in accordance with standards, permits the logging of only 3 activations of the same zone in one set period.

17.7.2 Access Log

The log provides all the access events of the SPC system.

- Select **Log > Access log**.
- ⇒ The following window will be displayed:

System log	Access log	Modem 1	Modem 2
Access log			
Time	Event	Door	User
26/07/2012 16:01:17	Unknown card	1- Entry	
26/07/2012 16:01:17	Entry Denied - CARD NOT ON SYSTEM	1- Entry	
26/07/2012 16:01:36	Unknown card	1- Entry	
26/07/2012 16:01:36	Entry Denied - CARD NOT ON SYSTEM	1- Entry	
26/07/2012 16:02:07	User 11 Card added By User 1		1 User 1
26/07/2012 16:02:11	Entry Granted	1- Entry	11
08/08/2012 12:43:17	User 9 Card added By User 1		1 User 1
08/08/2012 15:57:42	Unknown card	2- DOOR 2	
08/08/2012 15:57:42	Entry Denied - CARD NOT ON SYSTEM	2- DOOR 2	
08/08/2012 15:57:46	Unknown card	1- Entry	
08/08/2012 15:57:46	Entry Denied - CARD NOT ON SYSTEM	1- Entry	
08/08/2012 16:02:27	User 7 Card added By User 1		1 User 1
08/08/2012 16:02:55	Unknown card	1- Entry	
08/08/2012 16:02:55	Entry Denied - CARD NOT ON SYSTEM	1- Entry	
08/08/2012 16:03:11	User 8 Card added By User 1		1 User 1
10/08/2012 12:37:29	Entry Granted	2- DOOR 2	11
10/08/2012 12:37:34	Entry Granted	2- DOOR 2	11

- Create a text file of the log by clicking on the **Text File** button.

17.7.3 WPA Log

This log displays all the WPA events on the system.

- Select **Log > System Log > WPA log**.
⇒ The following window will be displayed:

System log	Access log	Modem 1	Modem 2
System log	Alarm log	WPA Log	
WPA Log			
10/06/2014 11:06:07 Alert: WPA SUPERVISION 1 WPA 1			
10/06/2014 11:06:31 Alert: WPA SUPERVISION 1 WPA 1			
17/06/2014 11:07:27 Alert: WPA SUPERVISION 1 WPA 1			
25/06/2014 09:34:02 Alert: WPA SUPERVISION 1 WPA 1			

17.7.4 ALARM LOG

The ALARM LOG displays a list of alarm events.

- Select **Log > System Log > Alarm Log**.
The following types are displayed in this log:
- Zones
 - Alarm
 - Panic
- System Events
 - Confirmed Alarm
 - User Duress
 - XBus Panic
 - User Panic
 - RPA Panic

17.8 Users

The following table shows the maximum number of users, user profiles and user devices for the panel:

Maximum No.	SPC4xxx	SPC5xxx	SPC6xxx
Users	100	500	2500
User Profiles	100	100	100
User Profiles per User	5	5	5
PACE Devices	32	250	250
SMS IDs	32	50	100
Web Passwords	32	50	100
RF Fobs	32	50	100
MDT Devices	32	32	32



⚠ WARNING

If upgrading from a firmware version prior to version 3.3, please note the following:

- The Engineer web password, if configured, is deleted and must be reentered after upgrade.
- All existing users will be assigned to new user profiles corresponding to their previous user access levels. If max. number of user profiles is exceeded, no profile is assigned (see User Profiles [→ 186]). Please review all user configuration after a firmware upgrade.
- The default Engineer ID is changed from 513 to 9999.

17.8.1 Adding / Editing a User

1. Select **Users > Users > Add User**.

⇒ A list of configured users is displayed.

Edit	Delete	User	Name	Alerts	Card number	FOB	Pace	User Profiles
		1	User 1	OK	-	OK	-	- Manager [2]
		2	User 2	OK	-	-	-	- Standard user [1] - Manager [2]

Buttons: Add User, Sort by Name

2. Click on the **Add** button or click on the **Edit** button of the required user.

⇒ The following screen is displayed.

3. Enter a **User ID** that is not currently being used. If you enter an ID that is already used, an 'ID Unavailable' message is displayed.
4. Provide a **User Name** (maximum 16 characters and case sensitive).
5. To automatically generate a **User PIN** for a new user, click the **Generate PIN** button. Change the PIN if required. Enter 0 if PIN is not required.
 - ⇒ **Note:** To comply with INCERT approvals, the user's PIN code must contain more than 4 digits.
6. You can also limit access to the system for this user by ticking the **Date Limit** box and entering a **To** and **From** date in the date fields.
 - ⇒ **User Alerts** displays the status of the user's PIN. For example, It displays the number of days remaining before the PIN expires, if Periodic changes are enabled in the system PIN Policy.
7. Select the appropriate User Profile [→ 186] for this user.
8. Select **Duress Enable** for this user if required. The number of PINs allocated for duress (PIN +1 or PIN+2) is set in System Options [→ 222].



Duress option only available on this screen if 'User Duress' is enabled for the system in System Options. If Duress is enabled for this user, then consecutive user PINs for other users (i.e. 2906, 2907) are not permitted, as entering this PIN from the keypad would activate a user duress event.

Access Control

Attribute	Description
Card Number	Enter card number. Enter 0 to unassign this card.
Void Card	Check to temporarily disable this card.
Extended Time	Extend door timers when this card is present.
PIN bypass	Access a door without PIN on a door with PIN reader.
Priority	Priority cards are stored locally in the door controllers and will grant access in case of a technical fault where the door controller cannot communicate with the control panel. The maximum number of priority users is:

Attribute	Description
	<ul style="list-style-type: none"> ● SPC4xxx – all users ● SPC5xxx – 512 ● SPC6xxx - 512
Escort	<p>The escort feature enforces privileged card holders to escort other card holders through specific doors. If this feature is enabled on a door, a card with the “escort” right has to be presented first, to allow other cardholders without this right to open the door. The time period in which cardholders are able to present their cards after a card with escort right was presented, can be configured per door.</p>
Custodian	<p>The custodian feature enforces a card holder with custodian privilege to always be inside a room (door group) when other card holders are inside.</p> <p>The custodian must be the first to enter the room. Only if a custodian is in the room other cardholders are allowed to enter. The cardholder with the custodian right will not be allowed to exit until all non-custodian cards left the room.</p> <p>Identifies this card holder as a custodian. The user with the custodian attribute has to be the first who enters a door group which requires a custodian card holder and has to be the last that is leaving this door group.</p>

17.8.1.1 Unknown Devices

If an unknown device, such as a fob, PACE, or card, has been scanned but not assigned to a user, a button is displayed in the relevant section of the users page.

- **RF- FOB — Unknown Fob** button or, if the device is assigned to the user, **Delete FOB** button
- **Pace — Unknown Pace** button or, if the device is assigned to the user, **Delete Pace** button
- **Access Control — Unknown card** button

To assign a fob, PACE or card to the user:

1. Click the **Unknown** button for the device. The User page displays the list of unknown devices.
2. Click **Add** to assign the device to the user.

Note: To assign a card to the user, the associated user profile must have the correct site code defined.

To unassign a fob or Pace from a user:

1. Click the **Delete** button.
The device is unassigned from the user and also deleted from the system.
2. To add the device again, you must rescan it.

To unassign a card from a user:

1. Change the card number to zero (0).
2. Click **Save**.
The card is unassigned from the user and deleted from the system.
3. To add the card again, you must rescan it.

17.8.2 Adding / Editing User Profiles



NOTICE

Global user profiles cannot be edited in the browser or SPC Pro and must be edited in SPC Manager

1. Select **Users** -> **User Profiles**

⇒ A list of configured profiles is displayed with the number of users assigned to each profile.

Users		User Profiles	Users SMS	Web Passwords	Engineer
		ID	User Profile Name	User Count	
		1	Standard user	1	
		2	Manager	2	
		3	Limited user	0	
		4	Access User	0	
<input type="button" value="Add User Profile"/>					

2. Select **Add User Profile** or click on the **Edit** button of the required profile.

The following screen is displayed with the configuration options categorized as follows:

- General Settings
- User/Panel Rights
- Access Control

Users		User Profiles	Users SMS	Web Passwords	Engineer
Add a new User Profile to the system					
General Settings					
User Profile ID:	<input type="text" value="5"/>				
User Profile Name:	<input type="text" value="User Profile 5"/>	Name of User Profile on system			
Areas					
<input checked="" type="checkbox"/> 1: Marketing	<input type="checkbox"/> 2: Reception	<input type="checkbox"/> 3: Finance	<input type="checkbox"/> 4: Cafeteria	<input type="checkbox"/> 5: Meeting Room	
Calendar					
Calendar:	<input type="text" value="None"/>	Daily time limits of user on system are specified by the selected calendar			
User Rights - Intruder					
Unset	<input type="checkbox"/>	User can unset the system.			
Partset A	<input type="checkbox"/>	User can Partset A the system.			
Partset B	<input type="checkbox"/>	User can Partset B the system.			
Fullset	<input type="checkbox"/>	User can Fullset the system.			

General Settings

1. Enter a **User Profile ID** that is not currently being used. If you enter an ID that is already used, an 'ID Unavailable' message is displayed.
2. Provide a **User Profile Name** (maximum 16 characters and case sensitive).
3. Select all **Areas** that will be controlled by this user profile.
4. Select a **Calendar** to set the time limitations of this profile on the system.

User/Panel Rights

- Select the required user rights that are to be assigned to this user profile.

User rights

Right	User Profile Type Default	Description
User Rights - Intruder		
Fullset	Limited Standard Manager	The FULLSET operation fully sets the alarm system and provides full protection to a building (opening of any alarm zones activates the alarm). On selecting FULLSET, the buzzer sounds and the keypad display counts down the exit time period. Exit the building before this time period has expired. When the exit time period has expired, the system is set and opening of entry/exit zones starts the entry timer. If the system is not Unset before the entry timer expires, the alarm is activated.
Partset A	Standard Manager	The PARTSET A option provides perimeter protection to a building while allowing free movement through the access areas. Zones that have been classified as EXCLUDE A remain unprotected in this mode. By default, there is no exit time; the system sets instantly on selection of this mode. An exit timer can be applied to this mode by enabling the Partset A timed variable.
Partset B	Standard Manager	The PARTSET B option applies protection to all zones except those that have been classified as EXCLUDE B. By default there is no exit time; the system sets instantly on selection of this mode. An exit timer can be applied to this mode by enabling the Partset B timed variable.
Forceset	Standard Manager	The FORCESET option is presented on the keypad display when an attempt is made to set the system while an alarm zone is faulty or still open (the top line of the display shows the open zone). Selecting this option sets the alarm and inhibits the zone for that set period.
Unset	Limited Standard Manager	The UNSET operation unsets the alarm. This menu option is only presented on the keypad after an Entry/Exit zone has been activated and a valid user code has been entered.
Delay Auto Set	Standard* Manager	User can delay or cancel autosetting..
Bypass Delay	Standard Manager	User can automatically override the Unset Delay. Only available for Financial installations. See Setting/Unsetting [→ 243]
Restore	Standard Manager	The RESTORE operation restores an alert condition on the system and clears the alert message associated with that alert condition. An alert condition can only be cleared after the zone(s) or fault(s) that triggered the alert condition have been restored to their normal operating state and the CLEAR ALERT option in user programming is selected for that zone.
Inhibit	Standard Manager	Inhibiting a zone deactivates that zone for one alarm set period. This is the preferred method of deactivating a faulty or open zone as the fault or open condition is displayed

Right	User Profile Type Default	Description
		on the keypad each time the system is being set to remind the user to attend to that zone.
Isolate	Standard* Manager	<p>Isolating a zone deactivates that zone until such time as the zone is de-isolated. All zone types on the controller can be isolated.</p> <p>Use of this feature to deactivate faulty or open zones should be considered carefully; once a zone is isolated, it is ignored by the system and could be overlooked when setting the system in the future, compromising the security of the premises.</p>
User Rights - System		
Web Access	Standard* Manager	User can access panel through web browser.
View Log	Standard Manager	This menu option displays the most recent event on the keypad display. The event log [→ 149] details the time and date of each logged event.
Users	Manager	User can create and edit other users on the panel but with only the same or less rights than this user.
SMS	Standard* Manager	This feature allows users to set up the SMS messaging service if a modem is installed on the system.
Set Date	Standard Manager	<p>Use this menu option to program the time and date on the system [→ 157].</p> <p>Ensure the time and date information is accurate; these fields are presented in the event log when reporting system events.</p>
Change PIN	Standard Manager	<p>This menu option allows users to change their user PINS [→ 150].</p> <p>Note: To comply with INCERT approvals, the user's PIN code must contain more than 4 digits.</p>
View Video/Video in Browser	Standard Manager	<p>User can view video images via the web browser.</p> <p>Note: The Web Access right must also be enabled for this function.</p>
Chime	Standard Manager	<p>All zones that have the CHIME attribute set generate a short burst of audible tone on the keypad buzzer when they are opened (while the system is unset).</p> <p>This menu option allows for enabling or disabling of the chime feature on all zones.</p>
Engineer	Manager	<p>This option allows users to grant access to engineer programming.</p> <p>For Swiss CAT 1 and CAT 2 regional requirements, when Engineer Access is granted, all areas must be unset otherwise the engineer will be denied access.</p>
Upgrade	Manager	User can grant manufacturer access to panel to perform firmware upgrade.
User Rights - Control		
Outputs	Standard Manager	User can activate/deactivate configured outputs (mapping gates). See Editing an Output [→ 197].
X-10	Standard Manager Access Control	<p>User can activate/deactivate configured X-10 devices.</p> <p>Note: X-10 is in maintenance. The functionality remains in the system for backward compatibility.</p>
Door Control	Standard* Manager Access Control	User can lock/unlock doors.

Right	User Profile Type Default	Description
RF Control	Standard Manager Access Control	User can control RF output
User Rights - Test		
Bell Test:	Standard Manager	User can perform a bell test to test the external bells, strobe, internal bells and buzzer to ensure their correct operation.
Walk Test	Standard Manager	User can perform a walk test to allow for testing of the operation of all alarm sensors on a system.
WPA Test	Standard Manager	User can test a WPA.
Seismic Test	Standard Manager	User can test the seismic detector.
User Rights – Service Engineer		
Set Users (Master)		User can create and edit other users on the system with no restriction on user rights.
Set User Profiles		User can create and edit user profiles on the system.
Set Calendars		User can configure calendars.
Set Doors		User can edit doors.
* Functions not enabled by default for this user but can be selected.		

Access Control

Access Control

Site Code: Site code of all cards using this user profile

Door Access List:	Door ID	Door Name	Access / Calendar
	1	Door 1	No time limit ▾
	2	Door 2	No time limit ▾
	3	Door 3	No time limit ▾
	4	Door 4	No time limit ▾
			No access
			No time limit
			1:

1. Enter a **Site Code**, if required, for all cards assigned to this user profile. Refer to the appendix section on Card Readers and Formats [→ 354].
2. Select the **Access** rights of this user profile for the doors configured on the system. Options are:
 - No access
 - No time limit (i.e. 24 hour access)
 - Calendar (if configured)

Users

A list of users assigned to this profile is displayed. Click on a user to view or edit the user's details.

You can create a new user profile based on an existing profile by clicking **Replicate**. A new User Profile page is displayed.

See also

- 📄 Adding / Editing User Profiles [→ 187]
- 📄 Adding / Editing an area [→ 238]

17.8.3 Configuring SMS

The SPC system allows remote (SMS) messaging on systems with installed modems.

- ▷ A modem is installed and identified by the system.
- ▷ The function **SMS Authentication** is activated. See page [→ 222].

1. Select Users > Users SMS.

⇒ The Engineer SMS ID and a list of user SMS IDs with corresponding SMS details are displayed.

**2. Click on the Test button to test an SMS number.****3. Click Add to add a new SMS ID or click Edit beside the required SMS ID.**
4. Configure the SMS details as follows:

SMS ID	System generated ID.
SMS Number	Enter the number to which the SMS will be sent (requires three-digit country code prefix). Note: Engineer SMS number can be deleted by resetting it 0. User SMS numbers cannot be deleted.
User	Select a new user for this SMS ID if required.

SMS Events	Select the panel events which the user or engineer will receive via SMS.
SMS Control	Select the operations that the user or engineer can perform remotely on the panel through SMS. See SMS Commands [→ 191]

!	NOTICE
	HOLDUP alarm events are not transmitted via SMS.



If the phone line is connected to the PSTN network via a PBX, the appropriate line access digit should be inserted before the called party number. Ensure that Calling Line Identity (CLI) is enabled on the line selected to make the call to the SMS network. Consult the PBX administrator for details.

17.8.4 SMS Commands

When the SMS setup and configuration is complete, SMS features may be activated. Commands, depending on SMS configuration, are sent using a PIN or caller ID. The type of PIN depends on what is set for SMS Authentication.

The table below provides all available SMS commands. Subsequent action and response are also provided.

SMS Commands are sent as texts to the phone number of the SIM card on the controller.

For commands using a PIN, the format of the text is:

****.command or **** command

where **** is the PIN and “command” is the command i.e. the PIN followed by either a space or a full stop. For example, the command “FSET” is entered as: **** FSET or ****.FSET. The full version of the command, where listed, can also be used. For example, ****.FULLSET.

If the user does not have sufficient rights to perform a command, the system returns ACCESS DENIED.

If Caller ID is enabled, and the sender’s SMS number is configured, the PIN prefix is not required.

COMMANDS (**** = code)			
Using Code	Using Caller ID	Action	Response
**** HELP ****.HELP	HELP	All available commands displayed	All available commands
**** FSET ****.FSET ****.FULLSET	FSET FULLSET	Sets all areas the user has access to.	Time/date of system set. If applicable, responds with open zones/force set zones
**** UNSET ****.UNSET ****.UNSET	UNSET UNSET	Unsets all areas the user has access to.	System Unset
**** SSTA ****.SSTA ****.STATUS	SSTA STATUS	Retrieves the status of areas.	Status of system and applicable areas <ul style="list-style-type: none"> ● For a single area system, system and mode are returned, where mode is the set status of the system

			<ul style="list-style-type: none"> For a multi-area system, the status of each area is returned.
**** XA1.ON (X10) ****.XA1.ON		Where X10 device is identified as "A1", it is triggered on.	Status of "A1"
**** XA1.OFF ****.XA1.OFF		Where X10 device is identified as "A1", it is triggered off.	Status of "A1"
**** LOG ****.LOG		Up to 10 recent events displayed	Recent events
**** ENGA.ON (ALLOW ENGINEER) ****.ENGA.ON	ENGA.ON	Enable Engineer access	Allow Engineer
**** ENGA.OFF ****.ENGA.OFF	ENGA.OFF	Disable Engineer access	Revoke Engineer
**** MANA.ON ****.MANA.ON		Enable Manufacturer access	Manufacturer status
**** MANA.OFF ****.MANA.OFF		Disable Manufacturer access	Manufacturer status
**** O5.ON ****.O5.ON ****.OUTPUT		Where mapping gate is identified as "O5", it is triggered on.	Status of "O5" For example: <ul style="list-style-type: none"> Output O5 on. Output heating on (where heating is the name of the output.)
**** O5.OFF ****.O5.OFF		Where mapping gate is identified as "O5", it is triggered off	Status of "O5" For example: Output O5 off
****.ASET (PARTSET A)		Allows Partset A of alarm by SMS It is also possible to specify the custom name defined in the PARTSET rename field of the Options window. See Options [→ 222]	System set.
****.BSET (PARTSET B)		Allows Partset B of alarm by SMS It is also possible to specify the custom name defined in the PARTSET rename field of the Options window. See Options [→ 222] For example: ****.ASET NIGHT	System set.
****.CLR ****.RESTORE		Allows clear alerts by SMS	



For SMS recognition, mapping gate identification uses the format ONNN, where O stands for mapping gate, and NNN are the numeric placeholders, of which not all are necessary.

(Example: O5 for mapping gate 5)

For SMS recognition, X-10 device uses the format: XYNN, where X stands for X-10; Y stands for the alphabetic identity and NN are the available numeric placeholders. (Example: XA1)

The SMS operates using a standard protocol that is used in SMS telephones. Please note that some PSTN operators do not provide the service of SMS over PSTN. For SMS to operate over PSTN, the following criteria are required:

- Caller ID needs to be enabled on the telephone line.
- Direct telephone line – not through PABX or other communications equipment.
- Please also note that most Service Providers only allow SMS to a telephone registered in the same country. (This is due to billing issues)

17.8.5 Deleting Web Passwords

This screen lists the engineer and any user and Engineer password that has been created for accessing the Web browser.

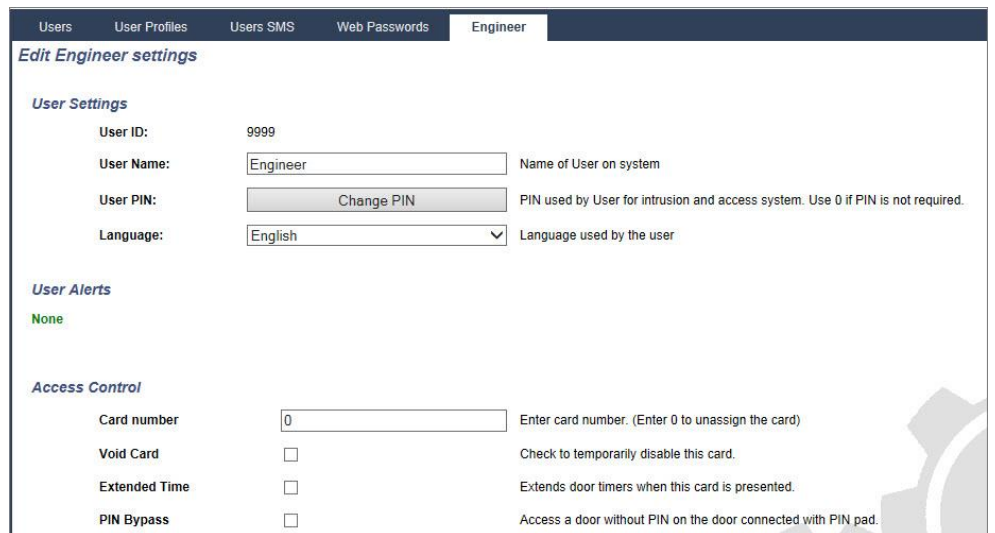
1. Select **Users -> Web Passwords**



2. Click on the **Delete** button beside the Engineer or user to delete the password.

17.8.6 Configuring Engineer Settings

1. Select **Users -> Engineer**.



2. Change the 'Engineer' **User Name** if required.
3. Click on the Change PIN [→ 194] button to change the Engineer PIN.
 - ⇒ **Note:** To comply with INCERT approvals, the user's PIN code must contain more than 4 digits.
4. Select the **Language** that will be used by the engineer. (Only displayed if multiple languages available – see Upgrading Languages [→ 308])

Access Control

Attribute	Description
Card Number	Enter card number. Enter 0 to unassign this card.
Void Card	Check to temporarily disable this card.
Extended Time	Extend door timers when this card is present.
PIN bypass	Access a door without PIN on a door with PIN reader.
Priority	<p>Priority cards are stored locally in the door controllers and will grant access in case of a technical fault where the door controller cannot communicate with the control panel.</p> <p>The maximum number of priority users is:</p> <ul style="list-style-type: none"> ● SPC4xxx – all users ● SPC5xxx – 512 ● SPC6xxx - 512
Escort	<p>The escort feature enforces privileged card holders to escort other card holders through specific doors. If this feature is enabled on a door, a card with the “escort” right has to be presented first, to allow other cardholders without this right to open the door. The time period in which cardholders are able to present their cards after a card with escort right was presented, can be configured per door.</p>
Custodian	<p>The custodian feature enforces a card holder with custodian privilege to always be inside a room (door group) when other card holders are inside.</p> <p>The custodian must be the first to enter the room. Only if a custodian is in the room other cardholders are allowed to enter. The cardholder with the custodian right will not be allowed to exit until all non-custodian cards left the room.</p> <p>Identifies this card holder as a custodian. The user with the custodian attribute has to be the first who enters a door group which requires a custodian card holder and has to be the last that is leaving this door group.</p>

17.8.6.1 Changing Engineer PIN and web password

This screen enables you to change the PIN for accessing the keypad and also the password for accessing the Web browser for Engineer level only.

The screenshot shows a web interface with a navigation bar containing 'Users', 'User Profiles', 'Users SMS', 'Web Passwords', and 'Engineer'. The 'Engineer' menu is active. Below the navigation bar, there are two main sections:

Change PIN

User PIN

Old PIN: 5 Numeric digits

New PIN: 5 Numeric digits

Confirm new PIN: 5 Numeric digits

Change Web Password (use a more secure password instead of PIN for user authentication)

Old Password:

New Password:

Confirm new Password:

- Change the PIN as follows:

Old PIN	Enter the existing Engineer PIN code. (Numeric digits only)
New PIN	Enter the new Engineer PIN code. (Numeric digits only)
Confirm New PIN	Re-enter the New Engineer PIN code.

1. Click on the **Change PIN** button to activate the new PIN.



The minimum number of digits required for this code depends on the security setting of the system or on the selected length of the **PIN Digits** in the menu **Panel Settings > System Settings > Options**.

2. Change the Web password to a more secure password for accessing the Web browser.

New Password	Enter the new web access password (alphabetic characters A-Z, numeric digits 0-9).
Confirm New Password	Re-enter the new web access password.

- Click on the **Change Password** button to activate the new password.



This password is case sensitive – ensure that you enter the correct upper or lower case alphabetic characters in your new password.

17.9 Configuration

17.9.1 Configuring controller inputs & outputs

17.9.1.1 Editing an input

1. Select **Configuration > Hardware > Controller**.
⇒ The following window will be displayed.
2. Configure the fields as described in the table below.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Controller Input & Output								
Input	End of Line	Zone	Description	Type	Area	Attributes		
1	Dual 4K7 / 4K7	1	Front door	Entry/Exit	2: Reception	...		
2	Dual 4K7 / 4K7	2	Fire Exit	Entry/Exit	4: Cafeteria	...		
3	Dual 4K7 / 4K7	3	Window 2	Alarm	5: Meeting Room	...		
4	Dual 4K7 / 4K7	4	PIR 1	Alarm	1: Marketing	...		
5	Dual 4K7 / 4K7	5	PIR 2	Alarm	3: Finance	...		
6	Dual 4K7 / 4K7	6	Fire Exit	Fire Exit	1: Marketing	...		
7	Dual 4K7 / 4K7	7	Fire alarm	Fire	1: Marketing	...		
8	Dual 4K7 / 4K7	8	Panic Button	Panic	1: Marketing	...		
Output	Description	Type	Change type	Attributes	Test			
1	Ext. Bell	System - External Bell			
2	Int. Bell	System - Internal Bell			
3	Strobe	System - Ext. Bell Strobe			
4	Fullset	System - Fullset			
5	Alarm	System - Alarm			
6	Alarm Confirmed	System - Alarm Confirmed			

Input	The number is presented for reference and can not be programmed.
End of Line	Select the End of Line (EOL) for the zone input (default: 4K7).
Analyzed <input type="checkbox"/> Pro	Displays if the sensor is an inertia/shock type sensor
Pulse count <input type="checkbox"/> Pro	Pulse count programmed on the panel that will trigger an alarm from an inertia / shock sensor.
Gross Attack <input type="checkbox"/> Pro	The Gross attack programmed on the panel that will trigger an alarm from an inertia/shock sensor
Zone	Number of the zone on the panel
Description	Enter a text describing the input (max. 16 characters). This text will also appear on the browser and keypad.
Type	The type of zone (see page [→ 347]).
Area	Only if (multiple) Areas is activated in menu Panel Settings > System Settings > Options. Select the areas to which this zone has been assigned.
Attributes	An icon in this field indicates that attributes have been programmed for this zone (see page [→ 197]).

17.9.1.1.1 Input zones: attributes

Each zone on the SPC can be assigned an attribute that determines the properties of that zone.

To assign an attribute to a zone:

1. Select **Configuration > Hardware > Controller > Attributes**.

⇒ The following window will be displayed:

Attribute	Description
<input type="checkbox"/> Exclude A	If checked then an alarm will not be generated if that zone opens while the system is in the Partset A mode.
<input type="checkbox"/> Exclude B	If checked then an alarm will not be generated if that zone opens while the system is in the Partset B mode.
<input type="checkbox"/> Local	If checked an alarm generated by the zone opening will NOT result in the reporting of the event.
<input type="checkbox"/> Chime	If checked then opening that zone during the Unset mode will cause the internal buzzers to activate for a short period.
<input checked="" type="checkbox"/> Inhibit	If checked a user may inhibit this zone.
<input type="checkbox"/> Normal Open	If checked the system expects that a connected detector/sensor is a Normally Open device.
<input type="checkbox"/> Log	If checked then all zone state changes are logged.
<input type="checkbox"/> Final Exit	If checked then closing that zone will terminate the exit timer 6 seconds after all exit routes have been closed.
<input type="checkbox"/> Shunt	If checked then an active shunt zone will inhibit this zone.
<input type="checkbox"/> Frequent	Zone must open within the 'frequent time period', for service purposes.
<input type="checkbox"/> Exit open	If checked then zone will be indicated if open during setting.
<input type="checkbox"/> Analyzed	Select this option if Inertia sensor is used.
<input type="text" value="5"/> Pulse Count	Pulse count trigger level for Analyzed inertia sensors
<input type="text" value="5"/> Gross attack	Gross attack trigger level for Analyzed inertia sensors

Calendar:

Verification:

2. Check the box beside the preferred attribute.



The attributes presented on this page will depend on the type of zone selected. For a list of assignable attributes see page [→ 352].

17.9.1.2 Editing an output

1. Select **Configuration > Hardware > Controller**.
2. Configure the fields as described in the table below.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Controller Input & Output								
Input	End of Line	Zone	Description	Type	Area	Attributes		
1	Dual 4K7 / 4K7	1	Front door	Entry/Exit	2: Reception	...		
2	Dual 4K7 / 4K7	2	Fire Exit	Entry/Exit	4: Cafeteria	...		
3	Dual 4K7 / 4K7	3	Window 2	Alarm	5: Meeting Room	...		
4	Dual 4K7 / 4K7	4	PIR 1	Alarm	1: Marketing	...		
5	Dual 4K7 / 4K7	5	PIR 2	Alarm	3: Finance	...		
6	Dual 4K7 / 4K7	6	Fire Exit	Fire Exit	1: Marketing	...		
7	Dual 4K7 / 4K7	7	Fire alarm	Fire	1: Marketing	...		
8	Dual 4K7 / 4K7	8	Panic Button	Panic	1: Marketing	...		
Output	Description	Type	Change type	Attributes	Test			
1	Ext. Bell	System - External Bell			
2	Int. Bell	System - Internal Bell			
3	Strobe	System - Ext. Bell Strobe			
4	Fullset	System - Fullset			
5	Alarm	System - Alarm			
6	Alarm Confirmed	System - Alarm Confirmed			

Output Type	<ul style="list-style-type: none"> ● System Output: Select the type from the dropdown menu. (See Output Types and Output Ports [→ 198]) ● Area Output: Only if (multiple) Areas is activated in menu Panel Settings > System Settings > Options. Select an area and the type of system output for this area. (See Output Types and Output Ports [→ 198]) ● Zone Mapping: Select which zone should be mapped. ● Mapping Gate: Select which mapping gate should be mapped. ● Door Output: Select the door number and the type of system output for the door. (See Output Types and Output Ports [→ 198]) ● Keyswitch: Select the node ID for the required keyswitch and the required key position to map to this output.
Description	Enter a text describing the output (max. 16 characters). This text will also appear on the browser and keypad.
Output Configuration	<ul style="list-style-type: none"> ● Mode: Select the operational mode. Continuous follows output type; Pulsed toggles on and off when output type is active; Momentary generates a pulse when output type activates. ● Retrigger: Tick the box to retrigger momentary outputs. ● On Time: Enter the On time that applies to momentary and pulsed outputs. ● Off Time: Enter the Off time that applies to pulsed outputs. ● Invert: Tick this box to invert the physical output. ● Log: Tick this box to log the output state changes to the event log. ● Calendar: Select if necessary the desired calendar. See page [→ 251].

See also

📖 Calendars [→ 251]

17.9.1.2.1 Outputs types and output ports

Each output type can be assigned to one of the 6 physical output ports on the SPC controller or to an output on one of the connected expanders. Output types that are not assigned to physical outputs act as indicators of events on the system and may be logged and/or reported to remote central stations if required.

The output ports on the expanders are all single pole relay type outputs (NO, COM, NC); therefore, output devices may need external power sources to activate if they are wired to expander outputs.

The activation of a particular output type depends on the zone type (see page [→ 347]) or alert condition that triggered the activation. If multiple areas are defined on the system then the outputs on the SPC are grouped into system outputs and area outputs; the system outputs are activated to indicate a system wide event (e.g. mains fault) whereas the area outputs indicate events detected in one or more of the defined areas on the system. Each area has its own set of area outputs; if the area is a common area for other areas, then its outputs will indicate the state of all the areas it is common for, including its own state. For example, if Area 1 is common for Area 2 and 3, and Area 2 Ext. Bell is active, then the Area 1 Ext Bell output is also active.



Some output types can only indicate system wide events (no specific area events). Please refer to the table below for further information.

Output Type	Description
External Bell	This output type is used to activate the system external bell and is active when any Area External Bell is active. By default, this output is assigned to the first output on the controller board (EXT+, EXT-). Note: An external bell output is automatically activated whenever a zone programmed as an Alarm zone triggers an alarm in Fullset or Partset modes.
External Bell Strobe	This output type is used to activate the strobe on the system external bell and is active when any area strobe is active. By default, this output is assigned to the strobe relay output (Output 3) on the Controller board (NO, COM, NC). Note: An external bell strobe output is automatically activated whenever a zone programmed as an alarm zone triggers an alarm in Fullset or Partset modes. The external bell strobe activates on a 'Fail to Set' condition if the strobe on the 'Fail to Set' option is checked in system options.
Internal Bell	This output type is used to activate the internal bell and is active when any area Internal Bell is active. By default, this output is assigned to the second output on the controller board (INT+, INT-). Note: An internal bell output is automatically activated whenever a zone programmed as an Alarm zone type triggers an alarm in Fullset or Partset modes. The internal Bell activates on a 'Fail to Set' condition if the Bell on the 'Fail to Set' option is checked in system options.
Alarm	This output turns on following alarm zone activation on the system or from any area defined on the system.
Alarm Confirmed	This output turns on when an alarm has been confirmed. An alarm is confirmed when 2 independent zones on the system (or within the same Area) activate within a set time period).
Panic*	This output turns on following activation of panic alarm zone types from any area. A panic alarm output is also generated if a user duress event is generated or if the panic option for the keypad is enabled.
Hold-up	This output turns on whenever a zone programmed as a Hold-up type zone triggers an alarm from any area
Fire	This output turns on following a fire zone activation on the system (or from any area)
Tamper	This output turns on when a tamper condition is detected from any part of the system. For a grade 3 system, if communication is lost to an XBUS device for greater than 100s, a tamper is generated and SIA and CIR reported events will send a tamper.
Medical	This output turns on when a medic zone is activated
Fault	This output turns on when a technical fault is detected
Technical	This output follows tech zone activity
Mains Fault*	This output activates when Mains power is removed

Battery Fault*	This output activates when there is a problem with the backup battery. If the battery voltage drops below 11 V this output activates. The 'Restore' option for this fault is only presented when the voltage level rises to above 11.8 V.
Partset A	This output is activated if the system or any area defined on the system is in Partset A mode
Partset B	This output is activated if the system or any area defined on the system is in Partset B mode
Fullset	This output is activated if the system is in Fullset mode
Fail to set	This output activates if the system or any area defined on the system failed to set; it clears when the alert is restored
Entry/Exit	This output activates if an Entry/Exit type zone has been activated; i.e. a system or area Entry or Exit timer is running
Latch	This output turns on as defined in the system latch output configuration (see Configuring system latch and auto set outputs [→ 202]). This output can be used to reset latching sensors as smoke or inertia sensors.
Fire Exit	This output turns ON if any Fire-X zones on the system are activated
Chime	This output turns on momentarily when any zone on the system with chime attribute opens
Smoke	This output turns on momentarily(3 seconds) when a user unsets the system; it can be used to reset smoke detectors The output will also activate when the zone is restored When using the zone to reset latched smoke detectors the first code entry will not activate the smoke output but will silence bells, on the next code entry if the fire zone is in the open state the smoke output will activate momentarily. This process is repeatable until the fire zone is closed.
Walk Test*	This output turns on momentarily when a walk test is operational and a zone becomes active. This output can be used, for example, to activate functional tests of connected detectors (if available).
Auto Set	This output turns on if the Auto Set feature has been activated on the system.
User Duress	This output turns on if a user duress state has been activated (PIN code + 1 has been entered on the keypad)
PIR Masked	This output turns on if there are any masked PIR zones on the system. It generates a fault output on the keypad led. This output is latched so it will remain active until restored by a level 2 user. PIR Masking is logged by default. The number of log entries do not exceed 8 between arming periods.
Zone Omitted	This output turns on if there are any inhibited, isolated, or walk test zones on the system
Fail to Communicate	This output turns on if there is a failure to communicate to the central station
Man Down Test	This output turns on a 'Man Down' wireless device which is activated during a 'Man Down' test.
Unset	This output is activated if the system is in Unset mode.
Alarm Abort	This output activates if an alarm abort event occurs i.e. when a valid user code is entered via the keypad after a confirmed or unconfirmed alarm. It is used, for example, with external dialers (SIA, CID, FF)
Seismic Test	This output is used to activate a manual or automatic test on a seismic zone. Seismic sensors have a small vibrator that will be attached to the same wall as the sensor and is wired to an output on the panel or one of its expanders. During the test, the panel waits up to 30 seconds for the seismic zone to open. If it does not open, the test fails. If it opens within 30 seconds the panel then waits for the zone to close within 10 seconds. If that doesn't happen, the test fails. The panel then waits a further 2 seconds before reporting the test result. The result of the test, either manual or automatic, is stored in the system event log
Local Alarm	This output activates on a local intrusion alarm.

RF Output	This output activates when a Fob or WPA button is pressed.
Modem 1 Line Fault	This output activates when there is a line fault on the primary modem..
Modem 1 Failure	This output activates when the primary modem fails.
Modem 2 Line Fault	This output activates when there is a line fault on the secondary modem.
Modem 2 Failure	This output activates when the secondary modem fails.
Battery Low	This output activates when the battery is low,
Entry Status	This output activates if an 'All Okay' entry procedure is implemented and there is no alarm generated i.e. the 'All Okay' button is pressed within the configured time after the user code is entered.
Warning Status	This output activates if an 'All Okay' entry procedure is implemented and a silent alarm generated i.e. the 'All Okay' button is not pressed within the configured time after the user code is entered.
Ready to Set	This output activates when an area is ready to set.
Setting ACK (SPC Pro — Setting Complete)	This output signals the setting status. The output toggles for 3 seconds to signal that the setting has failed. The output remains on for 3 seconds if setting is successful.
Fullset Done (SPC Pro — Setting Success)	This output activates for 3 seconds to signal that the system has been fullest.
Blockschloss 1	Used for normal Blockschloss devices. When all zones in an area are closed, and there are no pending faults, the 'Blockschloss 1' output is activated. If the lock on the Blockschloss is closed, a 'Keyarm' input is activated, the relevant area is set and the 'Setting Ack' output is activated for 3 seconds to signal that the setting was successful. 'Blockschloss 1' is not deactivated. If the Blockschloss is unlocked, the Blockschloss device deactivates the Keyarm input to the unset state (closed) and the area is unset. 'Blockschloss 1' is then deactivated.
Blockschloss 2	Used for Blockschloss device type - Bosch Blockschloss, Signalock Plus, E4.03. When all zones in an area are closed, and there are no pending faults, the 'Blockschloss 2' output is activated. If the lock on the Blockschloss is closed, a 'Keyarm' input is activated, the relevant area is set and the 'Setting Ack' output is activated for 3 seconds to signal that the setting was successful. 'Blockschloss 2' is then deactivated. If the Blockschloss is unlocked, the Keyarm zone is switched to unset (closed) and the area is unset. 'Blockschloss 2' is activated (if area is ready to set).
Lock Element	Activates if the Lock Element is in the 'locked' position.
Unlock Element	Activates if the Lock Element is in the 'unlocked' position.
Code Tamper	Activates if there is a code tamper in the area. Clears when state is reset.
Trouble	Activates if any zone is in trouble state.
Ethernet Link	Activates if there is a fault on the Ethernet link.
Network Fault	Activates if there is an EDP communications fault.
Glass Reset	Used to switch on the power for the glassbreak interface module and to remove power in order to reset the device. The output is reset if a user enters their code, the zone is not in the closed state, and the bells deactivated.
Confirmed holdup	Activates in the following scenarios for PD6662 compliance: <ul style="list-style-type: none"> ● two hold-up zone activations more than two minutes apart ● a hold-up zone and a panic zone activation more than two minutes apart ● If a hold-up zone and a tamper zone or a panic zone and a tamper zone activation occurs within the two minute period
Full Engineer	Activates if an engineer is on site and the system is in full engineer mode.

** This output type can only indicate system wide events (no area specific events).*

See also

📖 [Configuring system latch and auto set outputs \[→ 202\]](#)

17.9.1.3 Configuring system latch and auto set outputs

- Under **Policy**, click on the **Edit** button for the **Output Configuration** option in **System Options**.

⇒ The following screen is displayed:

The screenshot shows a web interface with a navigation bar at the top containing tabs: Hardware, System, Inputs, Outputs, Doors, Areas, Calendars, Change own PIN, and Advanced. The 'System' tab is selected, and a sub-menu below it includes System Options, System Timers, Identification, Standards, Clock, and Language. The 'System Options' sub-menu is active, displaying two sections:

Latch Output Configuration

Entry Time	<input checked="" type="checkbox"/>	Turns on at end of exit time and off at beginning of entry time
Fire Exit	<input type="checkbox"/>	Turns on if any Fire X zones are active
Unset	<input type="checkbox"/>	Turns on if user Unsets systems, momentary
Alarm Reset	<input type="checkbox"/>	Turns on when an alarm is reset , momentary
Resetting Alarm	<input type="checkbox"/>	Turns on during setting procedure if glass break /smoke open and not in alarm
Engineer Exit	<input type="checkbox"/>	Turns on when engineer leaves engineer mode, momentary
Keypad valid PIN	<input type="checkbox"/>	Valid user code entered on keypad and fire zone active

Auto Set Output Configuration

On Output will remain on if auto set active

Keypad Output will follow keypad operation

Progressive Output will give progressive warning of auto set

Pulse Time Duration Auto Set output will remain active when pulsed (in 100ms increments)

Buttons: Save, Cancel

- Select the condition under which the latch output is activated:

Entry Time	Output turns on at the end of Exit time and off at the beginning of Entry time.
Fire Exit	Output turns on if any fire exit zones are active.
Unset	Output turns on if any user unsets system momentary
Alarm Reset	Output turns on if an alarm is reset momentary.
Resetting Alarm	Output turns on during a setting procedure if glass break/smoke open and not in alarm.
Engineer Exit	Output turns on when an engineer exits from Engineer mode momentary.
Keypad Valid PIN	Output turns on when valid user PIN entered on keypad and fire zone is active

- Select the behavior of the output.

On	Output will remain on if auto set is active.
Keypad	Output will follow keypad operation.

Progressive	Output will give progressive warning of auto set.
Pulse Time	Select the duration that the auto set output will remain active when pulsed.

17.9.1.4 X10 Config - Settings

The X10 settings window allows you to configure the operation of X10 on the panel.

1. Select **Configuration > Outputs > X-10**.

⇒ The following window will be displayed:

2. Activate the checkbox **Enable** to enable X10 operation on the panel.
3. Activate the checkbox **Log** to enable logging of all X10 events on the panel.
4. Click **Save**.
5. Click an alphabetic tab (A-P) to program X10 device triggers.

⇒ A list of programmable device triggers (1-16) will be presented for that alphabetic character:

Unit	Active	Description	Triggers	Quick Key	Test
1	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
2	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
3	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
4	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
5	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
6	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
7	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
8	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
9	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
10	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
11	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off
12	<input type="checkbox"/>	<input type="text"/>	Edit	None	On Off

Unit number	This is the number (1-16) that is assigned to the device.
Active	This field indicates if the device is active or not.
Description	This field displays a description that is used to help identify the device – e.g. downstairs light (16 characters max).

Quick key	This field indicates if the X10 device activation can be toggled by entering a code from the keypad.
-----------	--

To edit a X-10 device

1. Click **Edit**.

⇒ The following window will be displayed:

2. For further programming refer to page [→ 255].

17.9.2 X-BUS

17.9.2.1 Expanders

1. Select **Configuration > Hardware > X-Bus > Expanders**.

⇒ The following window will be displayed:

ID	Description	Status	Type	S/N	Version	Reader	Wireless	PSU
1	IND 1	Online	Indicator [1 Input]	223387801	1.03 [13MAR13]	EM4100	Not Fitted	Not Fitted
2	KSW 2	Online	Keyswitch [1 Output]	226593801	1.01 [11NOV10]	Not Fitted	Not Fitted	Not Fitted
3	IO 3	Online	I/O [8 Output]	443907	1.11 [07AUG13]	Not Fitted	Not Fitted	Not Fitted
4	IOA 4	Online	I/O Analyzed [8 Input / 2 Output]	165074801	2.00 [09Apr14]	Not Fitted	Not Fitted	Not Fitted
5	WIR 5	Online	Wireless	489907	1.11 [07AUG13]	Not Fitted	SIWay - V5	Not Fitted
6	AEX 6	Online	Audio [4 Input / 1 Output]	37070907	1.03 [13MAR13]	Not Fitted	Not Fitted	Not Fitted
7	AEX 7	Online	Audio [4 Input]	1434900	1.03 [13MAR13]	Not Fitted	Not Fitted	Not Fitted
8	IO 8	Online	I/O [8 Input / 2 Output]	11327907	1.11 [07AUG13]	Not Fitted	Not Fitted	Type 1 - V4



For naming and identifying:

In loop configuration, each expander is numbered consecutively from the first (expander connected to the 1A 1B on the controller) to the last (expander connected to the 2A 2B on the controller).

Example for SPC63xx: Expanders, when numbered 1 through 63, are allocated zones (in groupings of 8) in subsequent identities of 1 to 512 (the greatest number in zone identification is 512). Therefore, any expander named or identified by a number greater than 63 has no allocated zones.

2. Click on one of the expander identifying parameters to display the **Expander Configuration** screen.

- Configure the following fields:


Description	For appearance on device LEDs.
Volume Limit	Audio Expander Only: Speaker volume for the Audio Expander and satellites (WAC 11). They are all wired in parallel. Note that the speaker on WAC 11 has a potentiometer for fine-tuning the volume. Range is 0 min - 7 max or disabled.
Auxillary Channnel	Audio Expander Only: This option should be enabled if satellites (WAC11) are connected to this expander. Note: This option, if enabled, powers the satellite microphones. The satellite speakers are always enabled regardless of this setting.
End Of Line	Select the correct End of Line (default: DEOL 4K7). This setting should match the actual wiring of the input on the controller or expander. See page [→ 72].
(Zone) Description	Provide a description for allocated zone.
(Zone) Type	Select the zone type. See page [→ 350].
Area	Select the area.
Attributes	Assign attributes as desired. See page [→ 347].
Outputs / PSU outputs (Displayed for the SPCP355.300 Smart PSU ONLY)	
Output	The numbered output. The value in parentheses corresponds to the physical output on the PSU board.
Description	Provide description for output.
Change type	Change the type of output as necessary.
Attributes	Assign attributes to the output.
Test	Test the output.
Output monitor	Select which outputs are to be monitored. Note: The parallel resistor, diode and required load must be applied before enabling this option. The SPCP355.300 must perform a calibration before monitoring starts. See Supervised Outputs [→ 57] for more information.
Primary battery only	Tick this box if there is no secondary battery connected to the PSU

When expanders are added or removed:

- Click **Reconfigure** to implement changes.

See also

Wiring the system [→ 72]

 [Zone attributes \[→ 350\]](#)

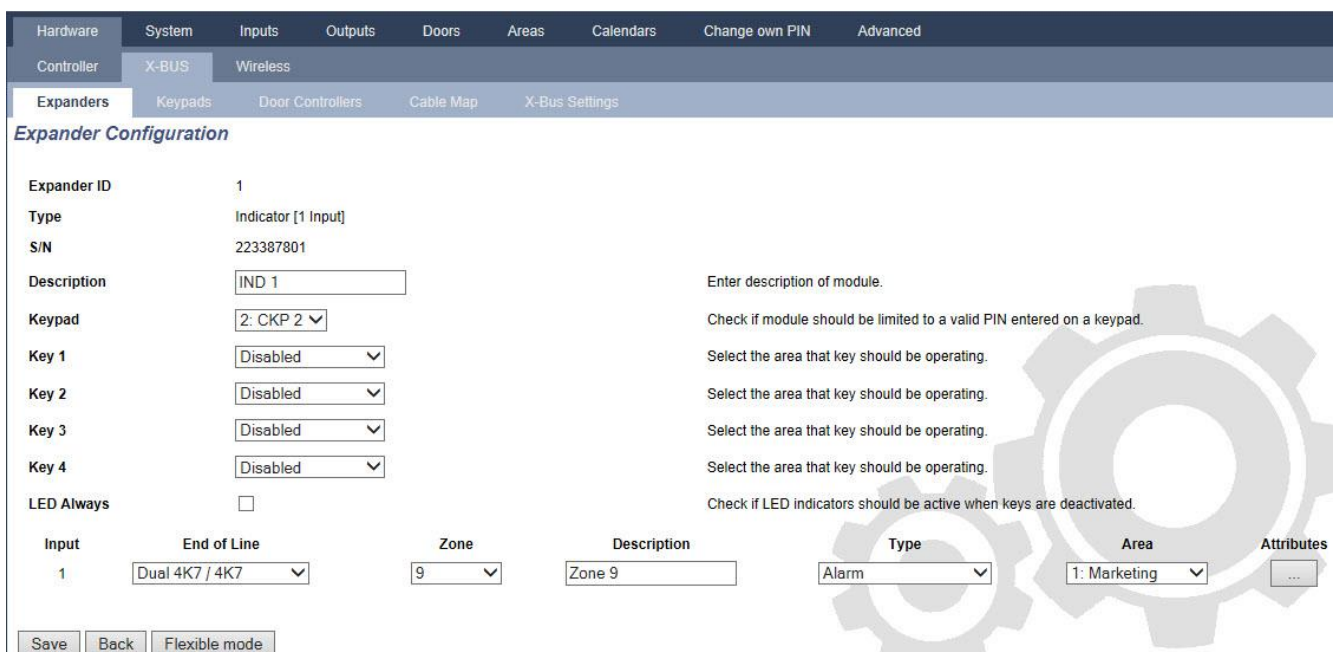
 [Zone types \[→ 347\]](#)

17.9.2.1.1 Configuring an Indicator Expander

There are 2 possible configuration modes for the indication expander:

- Linked Mode
- Flexible Mode

1. Select **Configuration > Hardware > X-Bus > Expanders**.
 2. Click one of the indicator identifying parameters.
- ⇒ The following screen is displayed for **Linked Mode** configuration.



Expander Configuration

Expander ID: 1
 Type: Indicator [1 Input]
 S/N: 223387801
 Description: IND 1
 Keypad: 2: CKP 2
 Key 1: Disabled
 Key 2: Disabled
 Key 3: Disabled
 Key 4: Disabled
 LED Always:

Input	End of Line	Zone	Description	Type	Area	Attributes
1	Dual 4K7 / 4K7	9	Zone 9	Alarm	1: Marketing	...

Save Back Flexible mode

Enter description of module.
 Check if module should be limited to a valid PIN entered on a keypad.
 Select the area that key should be operating.
 Select the area that key should be operating.
 Select the area that key should be operating.
 Select the area that key should be operating.
 Check if LED indicators should be active when keys are deactivated.

Linked Mode

1. Enter a description.
2. Select if indicator module should be limited to a valid code entered on a keypad.
3. Select the areas that are to be controlled by the 4 functions keys.
4. Configure the input.

Flexible Mode

1. Click the **Flexible Mode** button.
2. Configure the fields described in the tables below.
3. Configure the input.



▲ WARNING

Your system will not comply with EN standards if you enable a function key to set the system without a valid PIN being required.

Function Keys	
Area	Select the area is to be controlled by the function key.
Function	Select the function to be performed by this key in this area..
Area	Select an area if the indicator module is located in a secure area.
Visual Indication	
Indicator	There are 8 indicators / LEDs on the right and 8 indicators / LEDs on the left side.
Function	The function that is indicated by this LED.
Function On	Select the colour and the state for every indicator if the selected function is ON.
Function Off	Select the colour and the state for every indicator if the selected function is OFF.
Change function	Press this button to change the function for this indicator. The function can be enabled or used for a system, area, zone or keyswitch.
Audible Indications	
Alarms	Select if the alarms should be audible.
Entry / Exit	Select if entry / exit should be audible.
Key press	Select if keypress should be audible.
Deactivation	
Calendar	Select if indicator expander should be limited by calendar.
Mapping gate	Select if indicator module should be limited by a mapping gate.
Keyswitch	Select if indication module should be limited by a keyswitch.
Keypad	Select if indicator module should be limited to a valid PIN entered on a keypad. (see warning above)
Card reader	Select if indicator module should not be activated until a valid card/fob is presented to the built-in card reader.

17.9.2.1.2 Configuring a Keyswitch Expander

1. Select **Settings > X-Bus > Expanders**.
2. Click one of the keyswitch identifying parameters.
 - ⇒ The following dialog is displayed.

Expander Configuration

Expander ID: 2
 Type: Keyswitch
 SIN: 226593801
 Description: KSW 2

Keyswitch Options

Latch: Check if key position should be latched.
 Latch Timer: 0 Enter duration of latch in seconds. (0 - 9999, 0 = latch lasts until key reactivates same position or is turned to other position).

Areas

Location: None Select secured area where the keyswitch is located.

Visual Indications

Indicator	Function	Function On		Function Off	
Left	Disabled	Green	Permanent	Off	Permanent
Right	Disabled	Green	Permanent	Off	Permanent

Deactivation

Calendar: None Check if module should be limited by calendar.
 Mapping gate: None Check if module should be limited by a mapping gate.

Output

Output	Description	Type	Change type	Attributes	Test
1		Disabled

Keyswitch Functions

Key	Area	Function
Center position	1: Marketing	None
Right Position	1: Marketing	None
Left Position	1: Marketing	None

Save Back

- Configure the fields described in the tables below.

Description	Enter a description for the keyswitch expander.
Key Options	
Latch	Select if key position should be latched.
Latch timer	Enter duration of latch in seconds (0 - 9999, 0 means latch lasts until key is turned the other way).
Areas	
Location	Select the area where the keyswitch is located.
Visual Indications	
Indicator/LED	There is 1 indicator / LED on the right and 1 indicator / LED on the left side.
Function	The function for this indicator / LED.
Function On	Select the colour and the state for every indicator if the selected function is ON.
Function Off	Select the colour and the state for every indicator if the selected function is OFF.
Change function	Press this button to change the function for this indicator. The function can be enabled or used for a system, area, zone or keyswitch.
Deactivation	
Calendar	Select if the keyswitch module should be limited by calendar.
Mapping gate	Select if the keyswitch module should be limited by a mapping gate.
Output	
Output x	Configure and text the outputs for the keyswitch. See Outputs [→ 198] for more details
Keyswitch Functions	

Centre, Right and Left Positions	Select the Function that that this keyswitch position will perform and the relevant Area .
----------------------------------	--



⚠ WARNING

Your system will not comply with EN standards if you enable a keyswitch function to set the system without a valid PIN being required.

17.9.2.2 Keypads

17.9.2.2.1 Editing a Standard Keypad

1. Select **Configuration > Hardware > X-Bus > Keypads**.
2. Click one of the standard keypad identifying parameters.
3. Configure the fields as described in the table below.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Expanders	Keypads	Door Controllers	Cable Map	X-Bus Settings				

Keypad Configuration

Keypad ID: 1
 S/N: 559907
 Description: Enter keypad description.

Function Keys (in idle state)

Panic: Panic alarm by pressing the two Soft keys together.

Verification

Verification: Verification will be triggered on keypad for duress or alert activated from keypad

Visual Indications

Backlight: Select keypad LCD backlight option.

Indicators: Enable visible indicators (LED's).

Setting State: Check if setting state should be indicated in idle mode (LED).

Audible Indications

Buzzer: Enable keypad buzzer

Partset buzzer: Enabling will sound exit timer during Partset

Keypress: Check if keypress should be audible.

Deactivation

Calendar: Check if keypad should be limited by calendar.

Mapping gate: Check if keypad should be limited by a mapping gate.

Keyswitch: Check if keypad should be limited by a keyswitch.

PACE Entry: Disable keys during entry time.

Areas

Location: Select secured area where the keypad is located.

Areas: Select which areas can be controlled through keypad.


1: Marketing 3: Finance 5: Meeting Room
 2: Reception 4: Cafeteria

Options

Delay Fullset: Will use exit timer across all area

Description	Enter a unique description to identify the keypad.
Function Keys (in idle state)	
Panic	Select Enable, Disable or Enabled Silent. If enabled, panic alarm is activated by pressing the 2 soft keys together.
Verification	If you assign a verification zone to the keypad, when a panic alarm is triggered by pressing 2 soft keys together or by entering a duress code, audio and video events are activated.
Visual Indications	
Backlight	Select when keypad backlight is on. Options are: - On after key is pressed; Always on; Always off..
Indicators	Enable or disable the LED's on the keypad.
Setting state	Select if setting state should be indicated in idle mode.
Audible Indications	
Buzzer	Enable or disable the buzzer on the keypad.
Partset Buzzer	Enable or disable buzzer during exit time on Partset.
Keypress	Select if the speaker volume for the key presses should be activated.
Deactivation	

Calendar	Select if the keypad should be limited by calendar. See Calendar [→ 251].
Mapping gate	Select if keypad should be limited by a mapping gate.
Keyswitch	Select if keypad should be limited by a keyswitch.
PACE Entry	Tick this box to disable the keys on the keypad during the entry time when a PACE is configured on the keypad.
Areas	
Location	Select the secured area where the keypad is located.
Areas	Select which areas can be controlled through keypad.
Options	
Delay Fullset	Select to configure a delayed set across all keypads. The location of the keypad is ignored and all areas will perform a full exit time count down.

	NOTICE
	An area should be assigned to a keypad only if the keypad is inside the assigned area, and if an entry/exit route is defined. If an area is assigned, when the particular area is set or unset then entry and exit timers are used (if configured). Other features related to entry/exit routes also become available. If no area is assigned, the area is set or unset immediately and other entry/exit features are not available

See also

 [Calendars \[→ 251\]](#)

17.9.2.2.2 Editing a Comfort Keypad

1. Select **Configuration > Hardware > X-Bus > Keypads**.
2. Click one of the comfort keypad identifying parameters.
3. Configure the fields as described in the table below.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Expanders	Keypads	Door Controllers	Cable Map	X-Bus Settings				

Keypad Configuration

Keypad ID: 2
 S/N: 227361801
 Description: Enter keypad description.

Function Keys (in idle state)

Panic: Enabled (Silent) Panic alarm by pressing function keys F1 and F2 together.
 Fire: Fire alarm by pressing function keys F2 and F3 together.
 Medical: Medical alarm by pressing function keys F3 and F4 together.
 Fullset: Fullset by pressing function key F2 twice.
 Partset A: Partset A by pressing function key F3 twice.
 Partset B: Partset B by pressing function key F4 twice.

Verification

Verification: Unassigned Verification will be triggered on keypad for duress or alert activated from keypad

Visual Indications

Backlight: On when key is pressed Select keypad LCD backlight option.
 Backlight Intensity: 8 - High Select intensity of keypad backlight.
 Indicators: Enable visible indicators (LED's).
 Setting State: Check if setting state should be indicated in idle mode (LED).
 Logo: Check if logo should be visible in idle mode.
 Analog Clock: Centred Analog clock visible in idle mode.
 Emergency Keys: Check if Panic / Fire / Medical function keys should be indicated.
 Direct Set: Check if the Fullset / Partset function keys should be indicated.

Audible Indications

Alarms: 6 Select speaker volume for alarm indications.
 Entry/Exit: 6 Select speaker volume for entry & exit indications.
 Chime: 6 Select speaker volume for chime.
 Keypress: 2 Select speaker volume for key presses.
 Voice Annunciation: Disabled Select speaker volume for voice annunciation.
 Partset buzzer: Enabling will sound exit timer during Partset

Deactivation

Calendar: None Check if keypad should be limited by calendar.
 Mapping gate: None Check if keypad should be limited by a mapping gate.
 Keyswitch: None Check if keypad should be limited by a keyswitch.
 PACE Entry: Disable keys during entry time.

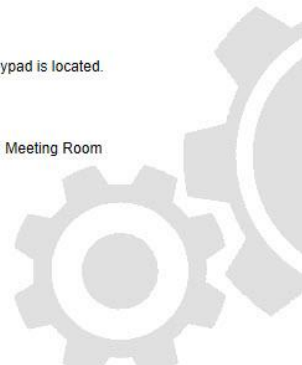
Areas

Location: 1: Marketing Select secured area where the keypad is located.

Areas: Select which areas can be controlled through keypad.
 1: Marketing 3: Finance 5: Meeting Room
 2: Reception 4: Cafeteria

Options

Delay Fullset: Will use exit timer across all area



Description	Enter a unique description to identify the keypad.
Function Keys (in idle state)	
Panic	Select Enable, Disable or Enabled Silent. If enabled, panic alarm is activated by pressing F1 and F2 soft keys together.
Fire	Enable to allow fire alarm to be activated by pressing F2 and F3 soft keys together.
Medical	Enable to allow medical alarm to be activated by pressing F3 and F4 soft keys together.
Fullset	Enable to allow Fullset to be activated by pressing F2 key twice.
Partset A	Enable to allow Partset A to be activated by pressing F3 key twice.
Partset B	Enable to allow Partset B to be activated by pressing F4 key twice.
Verification	If you assign a verification zone to the comfort keypad, when a Medical, Panic or Fire event is triggered, or if a user enters a duress code, then audio and video events are activated.
Visual indications	
Backlight	Select when keypad backlight is on. Options are: - On after key is pressed; Always on; Always off.
Backlight Level	Select the intensity of illumination of the backlight. Range 1 - 8 (High).
Indicators	Enable or disable the LED's on the keypad.
Setting state	Enable if setting state should be indicated in idle mode. (LED)
Logo	Enable if logo should be visible in idle mode.
Analog Clock	Select position of clock if visible in idle mode. Options are Left Aligned, Center Aligned, Right Aligned or Disabled.
Emergency	Enable if Panic, Fire and Medical function keys should be indicated in the LCD display.
Direct Set	Enable if Fullset/Partset function keys should be indicated in the LCD display.
Audible indications	
Alarms	Select speaker volume for alarm indications or disable sound.
Entry/Exit	Range is 0 – 7 (Max volume)
Chime	Select speaker volume for entry & exit indications or disable sound.
Keypress	Range is 0 – 7 (Max volume)
Voice Annunciation	Select speaker volume for chime or disable sound.
Partset Buzzer	Range is 0 – 7 (Max volume)
Deactivation	
Calendar	Select if the keypad should be limited by calendar. See Calendar.
Mapping gate	Select if keypad should be limited by a mapping gate.
Keyswitch	Select if keypad should be limited by a keyswitch.
PACE Entry	Tick this box to disable the keys on the keypad during the entry time when a PACE is configured on the keypad.
Areas	
Location	Select the secured area where the keypad is located.
Areas	Select which areas can be controlled through keypad.

Options	
Delay Fullset	Select to configure a delayed set across all keypads. The location of the keypad is ignored and all areas will perform a full exit time count down.



NOTICE

An area should be assigned to a keypad only if the keypad is inside the assigned area, and if an entry/exit route is defined. If an area is assigned, when the particular area is set or unset then entry and exit timers are used (if configured). Other features related to entry/exit routes also become available. If no area is assigned, the area is set or unset immediately and other entry/exit features are not available.

17.9.2.3 Door Controllers

17.9.2.3.1 Editing a door controller

1. Select **Configuration > Hardware > X-Bus > Door Controllers**.
2. Click on one of the blue marked data (e.g. serial number).
3. Configure the fields as described in the table below.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Expanders	Keypads	Door Controllers		Cable Map	X-Bus Settings			

Door controller configuration

Expander ID	1
Type	DC-2 [4 Input / 2 Output]
S/N	195309801
Description	<input type="text" value="DC2 1"/>
Door I/O 1 (*)	<input type="text" value="Door 1"/> <input type="button" value="Edit"/>
Door I/O 2 (*)	<input type="text" value="Door 2"/> <input type="button" value="Edit"/>
Reader 1 (**)	<input type="text" value="AR618X"/>
Reader 2 (**)	<input type="text" value="AR618X"/>

(*) Selecting 'Zones / Outputs' makes a door unassigned. Making door 2 of a door controller unassigned means it is now the exit reader for door 1.

(**) Defines the behaviour of the reader functionality and indicators. Profile 3 + 4 should be used with HID readers with PIN that sends the PIN with a pre-defined site code.



For naming and identifying:

In loop configuration, each expander is numbered consecutively from the first (expander connected to the 1A 1B on the controller) to the last (expander connected to the 2A 2B on the controller).

Example for SPC63xx: Expanders, when numbered 1 through 63, are allocated zones (in groupings of 8) in subsequent identities of 1 to 512 (the greatest number in zone identification is 512). Therefore, any expander named or identified by a number greater than 63 has no allocated zones.

Expander ID	ID of the door controller set with the rotary switches.
Type	Type of the door controller.
S/N	Serial number of the door controller.
Description	Description of the door controller..
Door I/O 1	<ul style="list-style-type: none"> ● If a door is assigned to the door I/O, select the corresponding door number. If the two inputs and outputs are configurable, select Zones / Outputs. ● If a door number is selected for the door I/O, the door settings can be changed by clicking on the edit button. This is equal to Settings > Doors. ● If Zones / Options is selected, the two zones and the one output can be configured by clicking the edit button.
Door I/O 2	
Profile 1	For readers with a green and a red LED.
Profile 2	For VANDERBILT readers with a yellow LED (AR618X).
Profile 3	Profile 3 is used with HID readers that send a PIN to the panel as a card reading with a predefined site code (0)
Profile 4	Profile 4 is used with HID readers that send a PIN to the panel as a card reading with a predefined site code (255).
Profile 5	Select to enable Sesam readers. It is also recommended that you select the Override Reader Profile option to provide feedback on the setting process.

Editing Zones/Outputs for a Door I/O

1. Select a Zone/Output for the door I/O.
2. Click the **Edit** button.
3. The 2 inputs and the output belonging to this door I/O can be configured as normal door inputs and outputs. See page [→ 246].
4. In order to use the inputs, they have to be assigned to a zone number.

17.9.2.4 Cable Map

For a list of the expanders/keypads in the ordered they are configured on the SPC system:

- Select **Configuration > Hardware > X-BUS > Cable Map**.
⇒ The following window will be displayed:

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Expanders	Keypads	Door Controllers	Cable Map	X-Bus Settings				

X-BUS Cable Map

Position	ID	Status	Type	S/N	Description
1	8	Active	I/O [8 Input / 2 Output]	11327907	IO 8
2	7	Active	Audio [4 Input]	1434900	AEX 7
3	6	Active	Audio [4 Input / 1 Output]	37070907	AEX 6
4	5	Active	Wireless	489907	WIR 5
5	4	Active	I/O Analyzed [8 Input / 2 Output]	165074801	IOA 4
6	1	Active	DC-2 [4 Input / 2 Output]	195309801	DC2 1
7	3	Active	I/O [8 Output]	443907	IO 3
8	2	Active	Keyswitch [1 Output]	226593801	KSW 2
9	1	Active	Indicator [1 Input]	223387801	IND 1
10	2	Active	Comfort Keypad	227361801	CKP 2
11	1	Active	Keypad	559907	KEY 1

Reconfigure



For more detail on X-BUS interfacing, see page [→ 72].

17.9.2.5 Settings

To configure X-BUS connections:

1. Select **Configuration > Hardware > X-BUS > X-Bus Settings**.
⇒ The following window will be displayed.
2. Configure the fields as described in the table below.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Expanders	Keypads	Door Controllers	Cable Map	X-Bus Settings				

X-BUS Settings

Addressing Mode

Manual - Use switches on expanders/keypads to assign Id
 Automatic - ID will be assigned automatically (required for expanders without Id switches)

X-BUS Type

Loop
 Spur

Retries Number of attempted retransmissions in case of interference. (Default is 25).

Comms timer Number of seconds that interconnect interference must be present before alert is triggered. (Default is 10).

Save

Addressing Mode	Select if expanders/keypads are either manually or automatically addressed on the X-BUS .
X-BUS Type	Select Loop or Spur configuration.
Retries	The number of times the system attempts to re-transmit data on the X-BUS interface before a communications fault is generated. (1 – 99: default is 25)
Comms Timer	The length of time before a communication fault is recorded.

17.9.3 Wireless

Wireless sensor detection (868 MHz) on the SPC panel is provided by wireless receiver modules which may be factory fitted on the keypad or on the controller, or by installing a wireless expander.

1. Select **Configuration > Hardware > Wireless > Wireless**.
2. See table below for further information.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Wireless	WPA	Wireless Settings						
Sensor ID	Type	Received	Status	Receiver	Signal	Enrol		
26662468	Magnetic contact	07/07/2014 15:00:50	Close	Wireless 5	High (9)	Enrol		
58749154	PIR	07/07/2014 14:59:28	Open	Wireless 5	High (9)	Enrol		
26589639	Magnetic contact	07/07/2014 14:59:08	Close	Wireless 5	High (9)	Enrol		
58906531	PIR	07/07/2014 14:58:04	Close	Wireless 5	High (9)	Enrol		
26329994	Magnetic contact	07/07/2014 14:57:50	Close	Controller	High (9)	Enrol		
26422346	Magnetic contact	07/07/2014 14:57:36	Close	Wireless 5	High (9)	Enrol		
26661509	Magnetic contact	07/07/2014 14:56:12	Close	Wireless 5	High (9)	Enrol		
26220868	Magnetic contact	07/07/2014 14:55:13	Close	Wireless 5	High (9)	Enrol		
58749154	PIR	07/07/2014 14:54:28	Close	Wireless 5	High (9)	Enrol		
58732159	PIR	07/07/2014 14:54:26	Close	Wireless 5	High (9)	Enrol		
26661909	Magnetic contact	07/07/2014 14:54:02	Open	Wireless 5	High (9)	Enrol		
26661450	Magnetic contact	07/07/2014 14:53:27	Open	Wireless 5	High (9)	Enrol		

Sensor	The number of the sensor enrolled on the system (1 = first, 2 = second, etc.)
ID	A unique identity number for that sensor.
Type	The type of wireless sensor detected (magnetic contact, inertia/shock, etc.)
Zone	The zone to which the sensor has been enrolled.
Battery	The status of the battery in the sensor (if fitted).
Supervise	The status of the supervisory operation (OK = supervisory signal received, Not Supervised = no supervisory operation).
Signal	The signal strength received from the sensor (01=low, 09=high). Note: Although it is not possible to enroll a device with a signal strength less than 3, devices whose signal drops below 3 after enrollment are not dropped.

Performable actions

Log	Click to view the wireless sensor Log. See page [→ 218].
Enrol	Click to open the list of unenrolled wireless devices.

1. Select **Status > Hardware > Wireless > WPA**.
2. The identity of each enrolled WPA and its status displays.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Wireless	WPA	Wireless Settings						

Configure Wireless Personal Alarm (WPA)

WPA: 1

Description:

Transmitter ID:

Supervise: Check if WPA should be supervised. (Note: This requires the supervision link to be fitted on the WPA.)

Test: Check if the WPA requires a manual test according to test schedule.

Assignment of Functions to Buttons

Red:

Green:

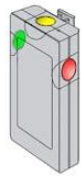

Yellow:

Red + Green:

Red + Yellow:

Yellow + Green:

Red + Yellow + Green:

17.9.3.1 Log - Wireless sensor X

To view a quick log of events for a wireless sensor:

1. Click the **Log** button.
2. See table below for further information.
3. Create a text file of the log by clicking **Text File**.

Date/Time	The date and time of the logged event.
Receiver	The wireless receiver location, i.e. wireless module mounted on the keypad, controller or wireless expander.
Signal	The signal strength received from the sensor (01=low, 09=high).
Status	The physical status of the sensor.
Battery	The status of the battery connected to the sensor (OK, Fault).

17.9.3.2 Configuring a WPA



NOTICE

The WPA configuration and status page is displayed only if there is a wireless module fitted on the panel or any of its expanders, and the panel is licensed for the type of module(s) fitted.

A WPA is not assigned to a user. Usually, a WPA is shared by several people, for example, security guards working in shifts or, alternatively, WPAs may be permanently attached to a surface such as under a desk or behind a till. A maximum of 128 WPAs is allowed per panel.

To configure a WPA from the browser:

- Select Full Engineer mode and select the following options **Configuration > Hardware > Wireless > WPA**.

WPA	Description	Transmitter ID	Battery	Supervise	Status	Edit	Delete
1	WPA 1	3002	OK	OK	---	Edit	Delete
2	WPA 2	0	OK	Disabled	---	Edit	Delete

Add

The following items can be checked or configured from this page:

- **Battery Status**
The panel receives the battery status from the WPA in every frame. The battery status can be either OK or Low.
Battery monitoring requires a WPA fitted with the PCB revision E-PC138612 or later.
 - **Supervise Status**
The Supervise status can be any of the following:
 - Fault
The panel has not received a supervision message from the WPA in the period configured in the Wireless Settings page.
 - Disabled
Supervision is not configured.
 - OK
Supervision is transmitting normally.
 - **Test Status**
The Test Status can be any of the following:
 - Overdue
The WPA has not been tested in the period configured in the Wireless Settings page.
 - Disabled
Supervision is not configured.
 - OK
The WPA test is ok.
1. Click on the **Edit** button to edit the WPA configuration.
 2. Click on the **Delete** button to delete a WPA from the system.

17.9.3.2.1 Adding a WPA

To add a WPA to the system:

- Click the **Add** button in the main WPA Configuration and Status page.
- ⇒ The Configure WPA page is displayed for the new WPA.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Controller	X-BUS	Wireless						
Wireless	WPA	Wireless Settings						

Configure Wireless Personal Alarm (WPA)

WPA: 1

Description:

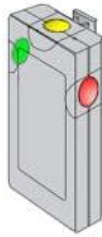
Transmitter ID:

Supervise: Check if WPA should be supervised. (Note: This requires the supervision link to be fitted on the WPA.)

Test: Check if the WPA requires a manual test according to test schedule.

Assignment of Functions to Buttons

Red	<input type="text" value="None"/>
Green	<input type="text" value="None"/>
Yellow	<input type="text" value="RF User Output"/>
Red + Green	<input type="text" value="Panic"/>
Red + Yellow	<input type="text" value="None"/>
Yellow + Green	<input type="text" value="None"/>
Red + Yellow + Green	<input type="text" value="Panic silent"/>



- Configure the WPA using the following details:

Description/Name	Enter a Description or Name to uniquely identify a WPA.
Transmitter ID	The transmitter ID is printed on the WPA casing and can be entered manually here. You can also identify the ID remotely by pressing any button on the WPA and then clicking the Learn button. The panel automatically enters this ID in this field providing no other WPA is currently defined with it
Supervise	The WPA may be configured to send periodic supervision signals. Supervision is enabled on the WPA with a jumper. The supervision function also needs to be enabled on the panel for the particular WPA for correct supervision operation. If the panel does not get a supervision signal, it raises an alarm that is shown in the keypad and logged. If supervision is not enabled, the WPA sends out a supervision message about every 24 hours to transmit the WPA battery status to the panel. This message is also randomized to decrease the chances of collision with other WPAs. Tick the Supervise box if supervision has been enabled for that particular WPA.
Test	Tick the Test box if a periodic WPA test is required. The timeframe for periodic testing is configured on the Changing wireless settings [→ 221] page.
Button Assignment	Use this section to assign functions to button combinations. Available functions are Panic, Panic silent, Holdup, Suspicion, RF User Output and Medical. More than one combination can be selected for the same function. The screen above shows the defaults for the panel for a Financial installation: ● Yellow - Suspicion

	<ul style="list-style-type: none"> ● Red + Green - Holdup <p>For Commercial or Domestic installations, the default is:</p> <ul style="list-style-type: none"> ● Red + Green - Panic <p>Note: If no function is assigned to a button combination, it is still possible to use that combination by using a trigger. See Triggers [→ 255]</p>
--	---

- Click on the **Save** button to save the settings.

See also

- 📄 Changing wireless settings [→ 221]
- 📄 Changing wireless settings [→ 221]
- 📄 Triggers [→ 255]

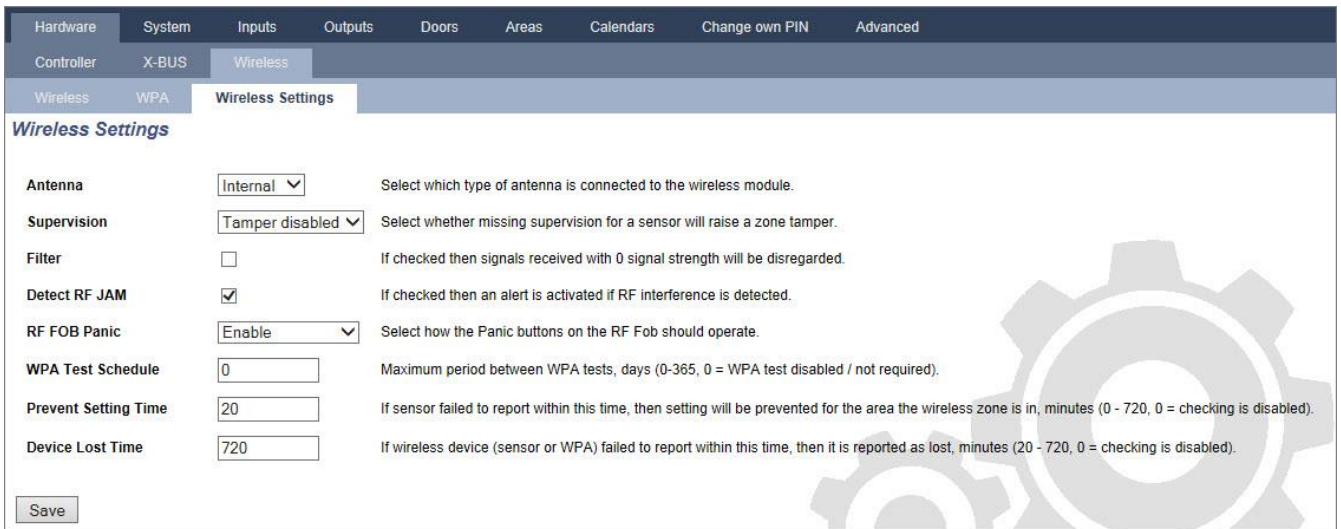
17.9.3.2.2 Editing a WPA

To edit a WPA, click the **Edit** button in the main WPA Configuration and Status page.

The **Edit** page is similar to the **Add** page except that it does not contain the Learn button for automatically entering the WPA ID.

17.9.3.3 Changing wireless settings

1. Select **Configuration > Hardware > Wireless > Wireless Settings**.



2. See table below for further information.

Antenna	Select the type of antenna connected to the wireless module (internal or external) from the drop down menu. The type of antenna required for the wireless module depends on the type of wireless module fitted.
Supervision	Select whether a wireless sensor that is reported as missing registers a tamper condition on the signet panel. A wireless sensor is reported as missing when no supervision signal has been received from the sensor for a period greater than the programmed Wireless Lost timer. See page [→ 230].
Filter	Tick to filter low strength RF signals.
Detect RF Jam	Tick to activate an alert if RF interference is detected.
RF FOB SOS	Select how the SOS buttons on the RF Fob should operate.:

	<ul style="list-style-type: none"> ● Disable ● Enable ● Enabled Silent ● User Medic ● User Holdup ● RF Output
WPA Test Schedule	Enter a maximum period (in days) between WPA tests.
Prevent Setting Time	<p>Enter a time in minutes after which, if the sensor fails to report, a setting is prevented for an area where the wireless zone is.</p> <p>This setting applies to the following intrusion zones only:</p> <ul style="list-style-type: none"> ● Alarm ● Entry/Exit ● Exit Term ● Panic ● Hold up ● Tamper ● Lock Supervision ● Seismic ● All OK ● Setting Authorisation ● Lock Element
Device Lost Time	Enter a number of minutes after which the wireless device (sensor or WPA) device is reported as lost.

17.9.4 Changing system settings

17.9.4.1 Options

1. Select **Configuration > System > System Options**.
2. Configure the fields as described in the table below.

System Options



The options displayed vary depending on the Security Grade of the system.

Restriction	System Option	Description
General Settings		
	Areas	Select to enable multiple areas on the system. Note: This option is displayed for the Domestic and Commercial installation types, only.
	Code Restore	Grade 3 only: A user, who does not have the right to restore an alarm, is able to restore the alarm with this feature. On resetting an alarm, a 6 digit code is required. The user must call the installer to generate a restore code, with which the user is able to restore the alarm.
	Offline Tamper	Enable this for offline expander zones to generate a zone tamper.
	Keyfob Restore	If enabled, key fob is enabled to restore alerts by pressing the Unset key.


Restriction	System Option	Description
Web and SPC Pro Only	Audio Expander LED	If enabled, audio expander will not turn on LED when microphone active.
	Report in Eng mode	If enabled, the panel will always report alarm activations and panic alarms.
	Outputs in Eng Mode	If selected, the following are not deactivated in Full Engineer mode: <ul style="list-style-type: none"> ● Controller outputs ● Expander outputs ● Indicator LEDs ● Keyswitch LEDs
	Alarm on Reporting Fail	If a 'Fail to Communicate' alert is raised, external bells will activate.
	Retrigger Duress	If enabled, duress alarm will retrigger.
	Retrigger Panic	If enabled, panic alarm will retrigger.
	Override Reader Profile	If enabled, the LED behavior of readers will be controlled by the panel.
	Silence Audio Verification	If enabled, then the internal and external bells (system and area), the keypad buzzers and annunciation messages on the Comfort Keypad will be silenced during audio verification.
	Watchdog Output Mode	Enables output 6 on the SPC controller board to be used for monitoring purposes. The following modes of operation of the watchdog output can be selected: <ul style="list-style-type: none"> ● Disable — Output 6 is available as a general purpose output. ● Enabled — Output 6 is normally OFF but is turned ON when a watchdog fault occurs. ● Pulsed — Output 6 is PULSED at 100ms intervals. ● Enabled Inverted — Output 6 is normally ON but is turned OFF when a watchdog fault occurs. <p>The following options combine the Enabled option with hardware-fault reporting in the event of a main microprocessor failure. If such a failure occurs, a SIA event is sent to ARC1.</p> <p>Note: The ARC must be configured to use SIA and SIA Extended 1 or 2. CID and FF are not supported by this reporting method.</p> <ul style="list-style-type: none"> ● Enabled + Reporting (10s) — The failure event is sent to ARC1 10 seconds after the fault is detected. This option must be used to comply with VdS 2252. ● Enabled + Reporting (60s) — The failure event is sent to ARC1 60 seconds after the fault is detected. <p>The SIA event reported is HF and Extended SIA reports Hardware Fault.</p> <p>Note: Hardware faults are not reported if the Engineer is logged in to the system.</p> <p>For more information on ARCs, see Alarm Reporting Centres (ARCs) [→ 292].</p>
	SPCP355	Enable VDS power supply. For VdS installations, this option is automatically selected.
	Bell on Fail to Set (FTS)	Enable to activate the internal bell if the system fails to set.
	Strobe on Fail to	Enable to activate the strobe if the system fails to set.

Restriction	System Option	Description
	Set (FTS)	
Ⓣ	Hide bypass	If enabled, the bypass messages will no longer be displayed on keypad.
	Battery capacity	Total batteries capacity in AH, for panel only (3 - 100 Ah). You must enter this value and Max current value to view the remaining battery time on the keypad in the event of mains failure. This is indicated under the STATUS - BATTERY - BATT TIME menu.
	Max current	The total current draw from batteries when mains fail occurs (30 - 20000 mA). You must enter this value and the Battery capacity value to view the remaining battery time on the keypad in the event of mains failure. This is indicated under the STATUS - BATTERY - BATT TIME menu.
Partset		
	Partset A Rename	Enter a new name for your PARTSET A mode (e.g. Night Mode).
	Partset B Rename	Enter a new name for your PARTSET B mode (e.g. Floor 1 only).
Alarm		
	Bell on First	Enable to activate relevant bells/sirens on an unconfirmed alarm. When this option is disabled, the relevant bells/sirens will only activate on a confirmed alarm or if the detector that caused the unconfirmed alarm is reactivated.
	Bell Retrigger	Enable to resound bells/sirens if a second zone activation is detected (after the bell time has elapsed). If not checked then the external bells will only trigger once.
Ⓣ Web Only	Alert Forbid Set	If enabled, a user cannot set an area if there is an area or system alert present on the system. Note: This option is only available when the Standards -> Region selected is Switzerland or Security Grade selected is 'Unrestricted'.
	Restore on Unset	Enable for alerts to auto clear after 30 seconds in Unset mode. Note: To comply with PD6662, you must disable this option.
Ⓣ	Antimask Set	Select the type of event reported resulting from antimask detection when panel is Set. Options are Disabled, Tamper, Trouble or Alarm. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: <ul style="list-style-type: none"> ● Ireland - Alarm ● All other regions - Alarm
Ⓣ	Antimask Unset	Select the type of event reported resulting from antimask detection when panel is Unset. Options are Disabled, Tamper, Trouble or Alarm. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: <ul style="list-style-type: none"> ● Ireland - Disabled ● All other regions - Tamper


Restriction	System Option	Description
Ⓣ	Out of bounds EOL unset	Select the type of event reported resulting from Out of Bounds EOL detection when the panel is unset. Options are: Disabled, Tamper and Trouble. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: <ul style="list-style-type: none"> ● Germany VDS – Tamper ● All other regions - Trouble
Ⓣ	Out of bounds EOL set	Select the type of event reported resulting from Out of Bounds EOL detection when the panel is set. Options are: Disabled, Tamper and Trouble. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: <ul style="list-style-type: none"> ● Germany VDS – Tamper ● All other regions – Trouble
Ⓣ	Zone Unstable unset	Select the type of event reported resulting from Zone Unstable detection when the panel is unset. Options are: Disabled, Tamper and Trouble. A zone is unstable if a valid sample cannot be obtained within 10 seconds. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: <ul style="list-style-type: none"> ● Germany VDS – Tamper ● All other regions – Trouble
Ⓣ	Zone Unstable set	Select the type of event reported resulting from Zone Unstable detection when the panel is set. Options are: Disabled, Tamper and Trouble. A zone is unstable if a valid sample cannot be obtained within 10 seconds. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: <ul style="list-style-type: none"> ● Germany VDS – Tamper ● All other regions – Trouble
Ⓣ	EOL Wide	If enabled, EOL wide bands are used.
	Suspicion Audible	If enabled then WPA Suspicion alerts have audible and visible indicators on the keypad. (Financial mode only).
Pro	End Of Line (EOL RESISTANCE)	Select the End Of Line termination resistors that will apply to either all zones on the system or new zones added to the system. Select a value to enable the appropriate feature. To apply a new EOL setting to all existing zones, select the Update all zones checkbox. If you change the End of Line value but do not select this checkbox, the new setting applies only to zones added after changing the value.
	Seismic Test on Set	If enabled, all seismic sensors in any area that is being set will be tested before area or system set. (Financial mode only).
Ⓣ	Auto Restore	Enable this feature to automatically restore alerts on the system i.e. when the open zone that triggered an alarm is

Restriction	System Option	Description
		closed, a manual restore operation on the keypad/browser is not required. If disabled it prevents the user from restoring alerts by resetting the input that triggered the alert.
⏴	Alarm on Exit	<p>Enabled: If a non-entry/exit zone is activated during the exit timer countdown, a local alarm is raised by sounding the bells.</p> <p>Disabled: If a non-entry/exit zone is activated during the exit timer countdown, an alarm is not raised.</p> <p>Note: This option only displays when the Unrestricted grade is selected as enabling it is not in accordance with EN50131. When you choose the Swiss or Belgium Region under Standard Compliance Settings, this option is automatically enabled but it is not visible under Options.</p>
⏴	Alarm on Entry	<p>Enabled: If a non-entry/exit zone is activated during the entry timer countdown, a local alarm is raised by sounding the bells.</p> <p>Disabled: If a non-entry/exit zone is activated during the entry timer countdown, an alarm is not raised.</p> <p>Note: This option only displays when the Unrestricted grade is selected as enabling it is not in accordance with EN50131. When you choose the Swiss Region under Standard Compliance Settings, this option is automatically enabled but it is not visible under Options.</p>
Confirmation		
⏴	Confirmation	<p>The Confirmation variable determines when an alarm is deemed to be a confirmed alarm.</p> <ul style="list-style-type: none"> ● BS8243: This will enforce compliance with the UK Police requirements, and is a specific requirement for UK Commercial installations. The requirement stipulates that an alarm will only be deemed to be a confirmed alarm if it meets the following condition: After an initial zone alarm has been activated and before the alarm confirmation time has expired, a second zone alarm is activated. The alarm confirmation time must be between 30 and 60 minutes. (See Timers [→ 230]) <p>If a second zone alarm is not activated within the Alarm confirmation time, then the first zone alarm will be inhibited. The BS8243 confirmation option is automatically set whenever the Standards -> Region option is set to UK.</p> <ul style="list-style-type: none"> ● Garda: This will enforce the policies for confirmed alarms required by the Irish Garda. The requirement stipulates that an alarm will be deemed to be a confirmed alarm as soon as a second zone alarm is activated on the system within the one alarm set period. The Garda confirmation option is automatically set whenever the Standards -> Region option is set to Ireland. ● EN-50131-9 This will enforce compliance with the EN-50131-9 standard and the Spanish "INT/316/2011 Order of 1 February on the operation of alarm systems in the field of private security". This requirement stipulates that an alarm will only be deemed to be a confirmed alarm if it meets the following conditions: - 3 zone activations in 30 minutes (default), whereby

Restriction	System Option	Description
		<p>two activations may come from the same device if the activations differ in type, i.e. alarm / tamper.</p> <p>- 1 Alarm activation followed by an ATS[1] Fault within 30 minutes (default).</p> <p>- ATS fault followed by a tamper or alarm condition within 30 minutes (default).</p> <p>If the 30 minutes expires and the zone is restored to its normal physical state, then the zone's alerts will be restored if a level 2 user can restore this alert. In this case, the zone will accept a new alert condition which will cause a new activation.</p> <p>Alternatively, if the zone has not been restored to its normal physical state then that zone will be inhibited if that zone is allowed to be inhibited.</p> <p>If an alert (ATS) reoccurs after the 30 minute window (default), then the 30 minute timer will restart.</p> <p>The EN50131-9 confirmation option is automatically set whenever the Standards -> Region option is set to Spain.</p> <ul style="list-style-type: none"> ● VDS This will enforce compliance with the VDS standard.
Keypad		
ⓘ	Always Show State (SHOW STATE)	If enabled, the setting status of the system (Fullset / Partset / Unset) is permanently displayed in the bottom line of the keypad display. If unchecked the setting status will disappear from the keypad display after 7 seconds.
	Show Open Zones	If enabled, open zones will display on keypad in Unset mode.
	Call ARC Message	If enabled, the ARC message will be displayed for 30 seconds after Unset, if confirmed alarm has been reported..
	Call ARC Line 1	ARC message in line 1 of display (16 chars).
	Call ARC Line 2	ARC message in line 2 of display (16 chars).
	Show Cameras	If enabled, offline cameras will be displayed on the keypad in Unset mode.
	Idle State Language	<p>Select the language displayed in idle state.</p> <ul style="list-style-type: none"> ● System Language: Language in which menus and texts on the keypads, the web interface and the event log will be displayed. ● Last Used: Last used language is displayed in idle state.
PIN		
	PIN Digits	<p>Enter the number of digits for user PINs (max. 8 digits). Increasing the number of digits will add the relevant number of zeros to the front of an existing PIN, e.g. an existing user PIN of 2134 (4 digits) will change to 00002134 if the PIN digits is set to 8. If you decrease the number of PIN digits, existing PINs will have their leading digits removed, e.g. an existing user PIN of 00002134 (8 digits) will change to 02134 if the PIN digits is set to 5.</p> <p>Note: This option cannot be changed if an SPC Manager PIN digit mode is set. Refer to page [→ 303]</p> <p>Note: To comply with INCERT approvals, the user's PIN code must contain more than 4 digits.</p>

Restriction	System Option	Description
	PACE and PIN	If enabled, both PACE and PIN are required.
	User Duress	<p>Select one of the following Duress options to activate this function on the system.</p> <ul style="list-style-type: none"> ● PIN + 1 (system reserves the PIN before and after the user PIN for duress. ● PIN + 2 (system reserves two PINs before and after the user PIN for duress. <p>Duress must be enabled for individual users. See section on Adding/Editing a User.</p>
	PIN Policy	<p>Click on the Edit button to select options for PIN usage.</p> <ul style="list-style-type: none"> ● Periodic changes required – enforces scheduled changes to the user's PIN. The period is defined in the PIN Valid field of Timers. See Timers [→ 230]. ● Warn if changes required – generates a user alert if the user's PIN is about to expire, or has expired. The warning period is defined in the PIN Warning field of Timers. See Timers [→ 230]. ● User selects the last digit – enables the user to select the last digit of their pin. The preceding digits are automatically generated by the system. ● User selects the 2 digits - enables the user to select the last two digits of their PIN. The preceding digits are automatically generated by the system. ● Limit Changes – limits the number of changes possible within a valid PIN period. This value is defined in the PIN Changes Limit field of Timers. See Timers [→ 230] ● Secure PIN - If enabled the PIN will be automatically generated by the panel.
Door		
	Reset Cards	If enabled, access cards passback state will be reset every day at midnight.
	Ignore site code	If enabled, the access system will ignore site codes. By ignoring the site code, you only add the card number and increase the card users on the system from 100 to 2,500.
	Card Formats	<p>Click on the Edit button to select the card formats that will be allowed on this panel.</p> <p>Refer to the Appendix in the SPC Installation & Configuration Guide for details of currently supported card readers and card formats.</p> <p>Note: Selecting Wiegand enables all Wiegand card formats.</p>
Web and SPC Pro Only	Door Mode Set	Select the required user identification to unlock door when area is set. Options are Default, Card and PIN, Card Or PIN.
Web and SPC Pro Only	Door Mode Unset	Select the required user identification to unlock door when area is unset. Options are Default, Card and PIN, Card Or PIN.
Engineer		
	Engineer Restore	(Impact only if Region "UK" is chosen): If this option is enabled, then the engineer has to restore the confirmed alarms. This option works together with the function "Confirmation".
	Engineer Exit	If enabled, the engineer is allowed to leave Full Engineer mode with alerts active.

Restriction	System Option	Description
Ⓣ	Allow Engineer	Enable this feature to ensure that the engineer can only access the system if the user allows it. If disabled, ENABLE ENGINEER menu option on keypad is not available. Note: Only available if Security Grade is 'Unrestricted'. For Grade 2 / 3, user control of engineer access to system is always available.
Ⓣ	Allow Manufacturer	Enable this feature to ensure that the engineer can only access the system if the user allows it. If disabled, ENABLE MANUFACTURER menu option on keypad is not available. Note: Only available if Security Grade is 'Unrestricted'. For Grade 2 / 3, user control of engineer access to system is always available if user type is 'Manager'.
SMS		
	SMS Authentication	Select one of the following options: <ul style="list-style-type: none"> ● PIN Code Only: This is a valid user code. See page. ● Caller ID Only: This is the phone number (including three-digit country prefix code) as configured for user SMS control. SMS control will only be available for configuration by the user when this option is selected. ● PIN and Caller ID ● SMS PIN Code Only This is a valid PIN code configured for the user which is different from the user's login code. SMS controls will only be available for configuration by the user when this option is selected. ● SMS PIN Code & Caller ID.
Policy		
Web Only	System Policy	Configure engineer login and tamper reporting behavior for system.
Web Only	Timing Policy	Display system timing policy.
Web and SPC Pro Only	Output Configuration	Click on the Edit button to configure latch and autoselect output settings [→ 202].
Web Only Ⓣ	System Alert Policy	This programming option allows you to restrict the user and engineer's ability to restore, Isolate and inhibit alerts. The manner in which the system reacts to alerts can also be programmed.
Web Only Ⓣ	Zone Alarm Policy	Select whether particular zone alarms can be restored, inhibited or isolated by the user and engineer.
Web Only Ⓣ	Zone Tamper Policy	Select whether particular zone tampers can be restored, inhibited or isolated by the user and engineer.
Web Only Ⓣ	Keypad Display Policy	Select events to be displayed on keypads in both Set and Unset modes.
Web Only Ⓣ	Keypad LED Policy	Select which LEDs will be displayed on keypads in both Set and Unset modes.
Web Only Ⓣ	System General Policy	Select options to manage remote control of the system and alarm and bell settings from the following: - No confirmed alarms if internally set

Restriction	System Option	Description
		- Block remote restore - Block remote isolates - Block remote inhibits - No external bell if internal set - Delay reporting if entry active - Confirmed alarm cancels delay
Web Only 	Confirmed Alarms System Alerts	Select which system alerts cause a confirmed alarms when at least one alarm is active, and which system alerts cause the panel to enter the tentative state.
Hold-up Data		
Web Only	Hold-up keyword 1	Enter the first hold-up keyword to send to the CMS in a Holdup Information (HD) event.
Web Only	Hold-up keyword 2	Enter the second hold-up keyword to send to the CMS in a Holdup Information (HD) event.
Web Only	Phone number 1	Enter the first site phone number to send to the CMS in a Holdup Information (HD) event.
Web Only	Phone number 2	Enter the second site phone number to send to the CMS in a Holdup Information (HD) event.

See also

 Adding / Editing an area [→ 238]

17.9.4.2 Timers

This window gives an overview about identified timer defaults and their description.



These settings, which vary depending on the defined Security Grade of the system, should only be programmed by an authorised installation engineer. Changing settings could render the SPC system noncompliant with security standards. Setting the Security Grade back to EN 50131 Grade 2 or EN 50131 Grade 3 overwrites any changes made on this page.

1. Select **Configuration > System > SystemTimers**.
⇒ The following window will be displayed.
2. Configure the fields as described in the table below.

Timers

Designation of the functions in the following order:

- 1st row: Web/SPC Pro
- 2nd row: Keypad

Timer	Description	Default
Audible		
Internal Bells INT BELL TIME	Duration that internal sounders will sound when alarm is activated. (1 – 15 minutes; 0 = never)	15 min.
External Bells EXT BELL TIME	Duration that external sounders will sound when alarm is activated. (1 – 15 minutes; 0 = never)	15 min.

Timer	Description	Default
External Bell Delay EXT BELL DELAY	This will cause a delayed activation of the external bell. (0 – 600 seconds)	0 sec.
Chime CHIME TIME	Number of seconds that a chime output will activate, when a zone with chime attribute opens. (1 – 10 seconds)	2 sec.
Confirmation		
Confirm CONFIRM TIME	<ul style="list-style-type: none"> Note: Only available when Security Grade is 'Unrestricted' and 'DD243' is selected for 'Confirmation' variable. (See System Options [→ 222]) This timer applies to the alarm confirmation feature and is defined as the maximum time between alarms from two different non overlapping zones that will cause a confirmed alarm. (30 – 60 minutes)	30 min.
Confirmed holdup	This timer applies to the confirmed holdup feature and is defined as the maximum time between alarms from two different non-overlapping zones that will cause a confirmed alarm. (480 - 1200 minutes)	480 min.
Dialer Delay DIALER DELAY	When programmed, the dialler delay initiates a predefined delay period (0 -30 seconds) before the system dials out to an Alarm Receiving Centre (ARC). This is specifically designed to reduce unwarranted responses from Alarm Receiving Centres and the constabulary. In the event of a subsequent zone being tripped the dialler delay period is ignored and the dialler dials out immediately. (0 – 30 seconds)	30 sec.
Alarm abort ALARM ABORT	Time after a reported alarm in which an alarm abort message can be reported. (0 – 999 seconds)	30 sec.
Setting		
Setting Authorisation SETTING AUTH	Period for which Setting Authorisation is valid. Enter a value between 10 and 250 seconds.	20 secs
Final Exit FINAL EXIT	The Final Exit time is the number of seconds that arming is delayed after a zone programmed with the final exit attribute is closed. (1 – 45 seconds)	7 sec.
Bell on Fullset FULLSET BELL	Activates the external bell momentarily to indicate a full set condition. (0 – 10 seconds)	0 sec.
Strobe on Fullset FULLSET STROBE	Activates the strobe on the external bell momentarily to indicate a full set condition. (0 – 10 seconds)	0 sec.
Fail To Set FAIL TO SET	Number of seconds to display fail to set message on keypads (0 until valid PIN is entered). (0 – 999 seconds)	10 sec.
Alarm		
Double Knock DKNOCK DELAY	The maximum delay between activation's of zones with the double attribute, which will cause an alarm. (1 – 99 seconds)	10 sec.
Soak SOAK DAYS	The number of days a zone remains under soak test before it automatically returns to normal operation. (1 – 99 days)	14 days
Seismic Test Interval SEISMIC AUTOTEST	The average period between seismic sensor automatic tests (12 – 240 hours) Note: To enable automatic testing, the Automatic Sensor Test attribute must be enabled for a seismic zone.	168 hours.
Seismic Test Duration SEISMIC TEST DUR	Maximum time (in seconds) that a seismic sensor takes to trigger an alarm in response to the 'Seismic Test' output. (3 - 120 seconds)	30 sec.
Lockout Post Alarm LOCKOUT POST ALARM	Duration after alarm that access will be denied.	0 mins
External Bell Strobe STROBE TIME	Duration that the strobe output will be active when an alarm is activated. (1 – 15 minutes; 0 = indefinitely)	15 min.
Alerts		

Timer	Description	Default
Mains Delay MAINS SIG DELAY	The time after a mains fault has been detected before an alert is activated by the system. (0 – 60 minutes)	0 min.
Engineer		
Engineer Access ENGINEER ACCESS	The timer for the Engineer access starts as soon as the user enables the Engineer Access. (0 – 999 minutes. '0' indicates no time limitation for system access)	0 min.
Engineer auto log out ENG AUTO LOG OUT	Duration of inactivity after which the engineer will be automatically locked out	0 mins.
Keypad		
Keypad Timeout KEYPAD TIMEOUT	The number of seconds that an RKD will wait for key entry before it leaves the current menu. (10 – 300 seconds)	30 sec.
Keypad Language KEYPAD LANGUAGE	The duration a keypad will wait in idle before switching language to default (0 - 9999 seconds; 0 = never).	10 secs
Fire		
Fire Pre-alarm FIRE PRE-ALARM	Number of seconds to wait before reporting fire alarm for zones with 'Fire pre-alarm' attribute set. (1 – 999 seconds) See Editing a Zone [→ 237].	30 sec.
Fire recognition FIRE RECOGNITION	Extra time to wait before reporting fire alarm for zones with 'Fire pre-alarm' and 'Fire Recognition' attributes set. (1 – 999 seconds). See Editing a Zone [→ 237].	120 sec.
PIN		
PIN Valid PIN VALID	Period for which pin is valid in days (1 - 330)	30 days
PIN Changes Limit PIN CHANGES LIMIT	Number of changes within a valid period (1 - 50)	5
PIN Warning PIN WARN	Time before PIN expiry after which a warning will be displayed (1 - 14)	5 days
General Settings		
RF Output Time RF OUTPUT	The time that the RF output will remain active on the system. (0 – 999 seconds)	0 sec.
Time Sync Limit TIME SYNC LIMIT	Time limit within which no event will be reported. (0 – 999 secs) Time synchronization only takes place if system time and update time are outside this limit.	0 sec.
Link Timeout LINK TIMEOUT	Timeout for Ethernet link fault (0 = Disabled) (0 - 250)	0 secs
Camera Offline CAMERA OFFLINE	Time for camera to go offline (10 - 9999)	10 secs
Tech. delay TECH. DELAY	Number of seconds to delay triggering of tech. zones with tech. delay attribute. (0 – 9999 seconds)	0 sec.
Frequent FREQUENT ⓘ	This attribute only applies to Remote Maintenance. The number of hours a zone must open within if the zone is programmed with the Frequent use attribute. (1 – 9999 hours)	336 hours (2 weeks)
Duress silent	Time when duress will remain silent and not restorable from keypad (0 - 999).	0 Minutes
Holdup/panic silent	Number of minutes that a holdup/panic will remain silent and cannot be restored from the keypad (0 - 999).	0 Minutes



Default times are dependent upon the Engineer configuration. The default times denoted may or may not be allowable and is dependent on the configuration by the engineer

17.9.4.3 Identification

1. Select **Configuration > System > Identification**.
⇒ The following window will be displayed.
2. Configure the fields as described in the table below.

Option	Value	Description
Installation ID	1	Unique identification number of the panel (used by FlexC and SPC Pro/SPC Safe). (1 - 999999)
Installation Name		Description of this installation.
Installation Date	Day: 1 / Month: Jan / Year: 2006	
Installer Name		Name of installer for support purposes.
Installer Phone		Phone number of installer for support purposes.
Display Installer	<input type="checkbox"/>	If checked installer details are displayed on keypads.
Engineer Lock	<input type="checkbox"/>	If checked the Engineer lock PIN is required to factory default the panel.
Engineer Lock PIN	1111	Four digit Engineer Lock PIN.

Installation ID	Enter a unique number for each installation This number identifies the installation (1 – 999999).
Installation Name	Enter the name of the installation. An installation name must be entered before the installation is saved on the system. The installation can be viewed from the keypad.
Installation Date	Select the date from the dropdown menu that the installation was completed.
Installer Name	Enter the name of the person who installed the system (for support purposes).
Installer Phone	Enter the contact phone number of the person who installed the system (for support purposes).
Display Installer	Tick this box to display the installation details on the keypad connected to the panel when in the idle condition.
Engineer Lock	Tick this box to require use of the engineer lock PIN to factory default the panel.
Engineer Lock PIN	Enter value for lock PIN (4 digits).

17.9.4.4 Standards



All alarm systems must comply with defined security standards. Each standard has specific security requirements that apply to the market/country in which the alarm system is installed.

1. Select **Configuration > System > Standards**.

⇒ The following window will be displayed.

2. Configure the fields as described in the table below.



Standard compliance settings

Installation Type:

- Domestic
- Commercial
- Financial

Region:

- Select for compliance to UK requirements
- Select for compliance to Irish requirements
- Select for compliance to Swedish requirements
- Select for compliance to European requirements
- (*) Select for compliance to Swiss requirements
- (*) Select for compliance to Belgium requirements
- (*) Select for compliance to Spanish requirements
- (*) Select for compliance to German requirements
- (*) Select for compliance to French requirements

Grade

- EN50131 Grade 2
- EN50131 Grade 3
- Unrestricted

(*) Selecting this regional standard will implement local or national requirements which supersede EN50131 requirements

Save

Installation Type	Select the type of installation. Options are Domestic, Commercial or Financial.
Region	To change the region on your panel, it is strongly recommended that you default your panel and select a new region as part of the start up wizard. Select the region in which the installation is installed and the regional requirements it complies with. Options are UK, Ireland, Sweden, Europe, Switzerland, Belgium (INCERT), Spain, and Germany (VDS).
Grade	Select the Security Grade that applies to the installation. <ul style="list-style-type: none"> ● Irish and European Regions: <ul style="list-style-type: none"> – EN50131 Grade 2 – EN50131 Grade 3 – Unrestricted ● UK Region: <ul style="list-style-type: none"> – PD6662 (EN50131 Grade 2 based) – PD6662 (EN50131 Grade 3 based)

	<ul style="list-style-type: none"> - Unrestricted ● Swedish Region: <ul style="list-style-type: none"> - SSF1014:3 Larmclass 1 - SSF1014:3 Larmclass 2 - Unrestricted ● Belgium Region: <ul style="list-style-type: none"> - TO-14 (EN50131 Grade 2 based) - TO-14 (EN50131 Grade 3 based) - Unrestricted ● Switzerland Region: <ul style="list-style-type: none"> - SES EN-CH-Grad 2 - SES EN-CH-Grad 3 - Unrestricted ● Spanish Region <ul style="list-style-type: none"> - EN50131 Grade 2 - EN50131 Grade 3 ● German Region <ul style="list-style-type: none"> - VdS Class A - VdS Class C - Unrestricted ● France <ul style="list-style-type: none"> - NF&A2P - Grade 2 - NF&A2P - Grade 3 - Unrestricted
--	--

Unrestricted Grade

A Security Grade setting of **Unrestricted** does not apply to any regionally approved security restrictions of the installation. Instead, the Unrestricted setting enables an engineer to customize the installation by changing security policy options and configuring additional options which do not comply with the selected regional security compliance.

Unrestricted configuration options are denoted in this document by the following symbol: Ⓡ

See System Options for details of configuring system policies.

17.9.4.5 Clock

This window allows you to program the date and time on the panel. The controller contains a **Real-Time Clock (RTC)** that is battery backed to preserve the time and date information in the event of power failure.

1. Select **Configuration > System > Clock**.

⇒ The following window will be displayed.

Current Time and Date

Time: Hour: 15 : Minute: 18 : Second: 18

Date: Day: 7 / Month: Jul / Year: 2014

Automatic Daylight Saving Time:

Synchronize Time with Mains:

Save

2. Select the **Time** and **Date** from the drop down menus.
3. Configure the following fields:

Automatic Daylight Saving Time	If selected, the system will automatically switch to summer time
Synchronize time with Mains	If selected, the RTC synchronizes itself with the sine wave in the power line



The selected time and date will be displayed on the keypad, the web interface and the event log.

17.9.4.6 Language

- Select **Configuration > System > Language**.

⇒ The following window is displayed:

Language Option

Option	Value	Description
Language	English	Select language used on the keypads, web interface and event log. The web interface language will be updated as soon as a new browser session is initiated.
Idle language	Use system language	Select the display language for idle mode.

Save

- For the **Language** option, select a language from the dropdown menu.
- ⇒ This option determines the system language in which the texts and menus on the keypads, the web interface and the event log will be displayed.
- For the **Idle Language** option, select either 'Use System Language' or 'Last Used'.

- ⇒ Idle Language determines the language which is displayed on the keypads when the panel is in its idle state. If 'Last Used' is selected, the language displayed is the language that is associated with the last user login.



The language used in the keypads and browser depends on the language selection made for each user. For example, if the system language is set to French, but the individual user's language is set to English, English is the language used in both keypads and browser for that user, regardless of the specified system language.

See also

- 📄 Language [→ 236]
- 📄 OPTIONS [→ 111]

17.9.5 Configuring zones, doors and areas

17.9.5.1 Editing a zone

Engineer and User actions include Log, Isolate/Deisolate and Soak/Desoak for each zone as allowable by the Security Grade EN 50131 Grade 2 and EN 50131 Grade 3.

1. Select **Configuration > Inputs > All Zones**.

⇒ The following window will be displayed.





You can select **Configuration > Inputs > X-Bus Zones** to configure wired zones only or **Configuration > Inputs > Wireless Zones** to configure wireless zones only.

2. Configure the fields as described in the table below.

Hardware System Inputs Outputs Doors Areas Calendars Change own PIN Advanced					
All Zones X-Bus Zones Wireless Zones					
Zone	Input	Description	Type	Area	Attributes
1	Controller - Input 1	Front door	Entry/Exit	2: Reception	...
2	Controller - Input 2	Fire Exit	Entry/Exit	4: Cafeteria	...
3	Controller - Input 3	Window 2	Alarm	5: Meeting Room	...
4	Controller - Input 4	PIR 1	Alarm	1: Marketing	...
5	Controller - Input 5	PIR 2	Alarm	3: Finance	...
6	Controller - Input 6	Fire Exit	Fire Exit	1: Marketing	...
7	Controller - Input 7	Fire alarm	Fire	1: Marketing	...
8	Controller - Input 8	Panic Button	Panic	1: Marketing	...
9	Expander 1 - Input 1	Zone 9	Alarm	1: Marketing	...
10	Door Controller 1 - Door I/O 1	Entry	Entry/Exit	1: Marketing	...
11	Door Controller 1 - Door I/O 3		Unused	1: Marketing	...
12	Door Controller 1 - Door I/O 2	DOOR 2	Entry/Exit	1: Marketing	...
13	Door Controller 1 - Door I/O 4		Unused	1: Marketing	...

Zone	The number is presented for reference and can not be programmed.
Description	Enter a text (max. 16 characters) that serves to uniquely identify the zone.

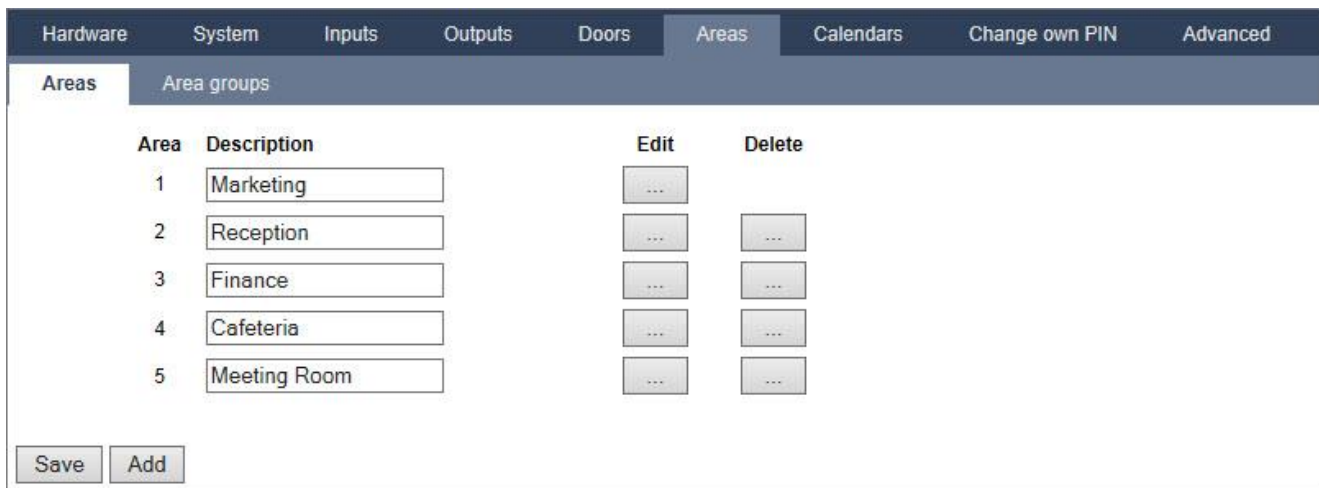
Input	The physical input is displayed for reference and is not programmable.
Type	Select a type of zone from the drop down menu (see page [→ 347]).
Area	Only if (multiple) Areas is activated. Select an area to which the zone is assigned from the drop down menu.
Calendar	Select if necessary the desired calendar (see page [→ 251]).   For Security Grade 2 / 3 a calendar can be assigned only to zones of type Exit Terminator, Technical, Key Arm, Shunt and X-Shunt. For Security Grade Unrestricted a zone of any type can be associated with a calendar.
Attributes	Tick the relevant checkbox for the zone. Only attributes that apply that type of zone will be presented (see Zone Attributes [→ 350])

17.9.5.2 Adding / Editing an area

▷ Only if (multiple) **Areas** is activated.

1. Select **Configuration > Areas > Areas**.

⇒ The following window will be displayed:



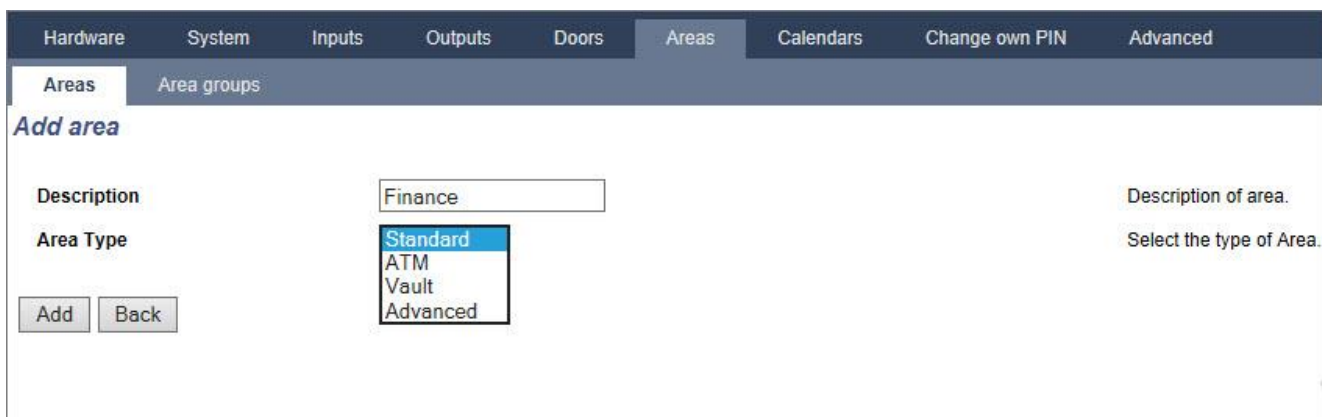
The screenshot shows the 'Areas' configuration window. At the top, there is a navigation bar with tabs: Hardware, System, Inputs, Outputs, Doors, Areas (selected), Calendars, Change own PIN, and Advanced. Below the navigation bar, there is a sub-tab 'Area groups'. The main content area contains a table with the following columns: Area, Description, Edit, and Delete. The table lists five areas: 1 Marketing, 2 Reception, 3 Finance, 4 Cafeteria, and 5 Meeting Room. Each row has an 'Edit' button (represented by three dots) and a 'Delete' button (represented by three dots). At the bottom left of the table, there are 'Save' and 'Add' buttons.

2. Press **Edit** to edit an existing area.

3. Press **Add** to add a new area. If the Installation Type is *Domestic* or *Commercial*, an area is automatically added and the Edit Area Settings window is displayed.

Note that the area type for the new area is automatically set to Standard.

If the Installation Type is *Financial*, the following window is displayed and the area must be added manually.



The screenshot shows the 'Add area' configuration window. At the top, there is a navigation bar with tabs: Hardware, System, Inputs, Outputs, Doors, Areas (selected), Calendars, Change own PIN, and Advanced. Below the navigation bar, there is a sub-tab 'Area groups'. The main content area is titled 'Add area'. It contains two input fields: 'Description' with the value 'Finance' and 'Area Type' with a dropdown menu showing 'Standard' (selected), 'ATM', 'Vault', and 'Advanced'. To the right of the 'Description' field, there is a label 'Description of area.' and to the right of the 'Area Type' field, there is a label 'Select the type of Area.'. At the bottom left, there are 'Add' and 'Back' buttons.

4. Enter a description for the new area and select an area type from one of the following:
 - Standard - Suitable for most areas.
 - ATM - Provides settings and defaults relevant to ATMs.
 - Vault - Provides settings and defaults relevant to vaults.
 - Advanced – Provides all area settings (Standard, ATM and Vault).
5. Click on the **Add** button to add the area.
 - Configure the settings for each installation type as per the following sections:

17.9.5.2.1 Entry/Exit

Configure the following Entry/Exit settings:

Entry time	The time period (in seconds) allowed for the user to UNSET the alarm after opening an entry/exit zone of an armed system. The entry time applies to all entry/exit zones in that area (default: 45 seconds).
Exit time	The time (in seconds) allowed for a user to leave a protected area before setting is complete. The exit time will be counted down at the keypad as the buzzer beeps to indicate to the user that the system will arm when the exit timer reaches zero. The exit time applies to all entry/exit zones in that area (default: 45 seconds).
Disable Exit Time	Select if no exit timer is required and setting is activated by 'Exit term' zone or 'Entry exit' zone with 'Final exit' attribute. See Timers [→ 230].
Fob Unset Entry	FOB will only unset when entry timer is running. Default is enabled.
Access Denied on Alarm	Access is temporarily denied to the area for the amount of time specified in the Lockout Post Alarm timer.
Prevent Setting	If enabled, setting prevented from keypad
Prevent Unsetting	If enabled, unsetting prevented from the keypad.
Setting Authorisation	Used for configuring Blocking Lock operation. Options are: <ul style="list-style-type: none"> ● Disabled ● Set ● Unset ● Set and Unset If the Disabled option is selected (default) then the system will set and unset normally with no change of operation. If the Set option is selected, a "Setting Authorisation" signal is required to set this area which can be received from keypads or a zone input (see Authorised Setting of the Blocking Lock) The user cannot set the system from the keypad. Any area that requires setting authorisation will appear as locked on the comfort keypad and will not appear on the standard keypad when setting. If the Unset option is selected, the user cannot unset the area from keypads but can use the keypad to generate the setting authorization signal. For the set and unset options, the user will be unable to change the state of the area at any stage from the keypad. A timer for setting authorisation can be configured. See Timers [→ 230].

17.9.5.2.2 Partset Options

Configure the operation of particular zones for both Partset A and Partset B modes as detailed below:

Partset Enable	Enable PartSet for A and B operation as required.
Partset Timed:	Tick the relevant checkbox (Partset A or B) to apply the exit timer to the Partset A or B mode.
Partset Access:	Tick the relevant checkbox to change access zones into entry/exit type zones for either Partset A or B operation. This feature is useful for a domestic installation where a Passive Infrared (PIR) sensor is located in the hallway. If the user partsets the system at night and returns downstairs during the night, he/she may unintentionally activate the PIR sensor in the hallway and trigger the alarm. By setting the partset access option, the buzzer will sound for the entry time period when the PIR sensor is activated thereby warning the user that the alarm will activate if no action is taken.
Partset Exit/Entry:	Tick the relevant checkbox to change the behaviour of entry/exit zones to alarm zones when in Partset A or B mode. This feature is useful for a domestic installation when the system has been set in partset mode. If the user partsets the system at night he/she may wish the alarm to activate immediately if the front or back door is opened during the night.
Partset Local:	Tick the relevant checkbox to restrict the reporting of alarms in Partset Mode to local reporting only (No remote reporting).
No Bells	If ticked, no bells will be activated for partset A or B.

17.9.5.2.3 Linked Areas

This section enables you to link areas for setting and unsetting purposes:

Fullset	Fullset this area when all linked areas are Fullset.
Fullset All	Fullset all areas when this area is Fullset.
Prevent Fullset	Prevent this area from Fullset if all linked areas are Fullset.
Prevent Fullset All	Prevent linked areas from Fullset if this area is not Fullset.
Unset	Unset this area when all linked areas are Unset.
Unset All	Unset all areas when this area is Unset.
Prevent Unset	Prevent this area from Unset if any linked areas are Fullset.
Prevent Unset All	Prevent linked areas from Unset if this area is Fullset.
Authorise Setting	Enable authorised setting for linked areas. Refer Authorised Setting of the Blocking Lock.
Linked Areas	Click on the areas that you wish to link to this area.

17.9.5.2.4 Schedule

Configure scheduling with the following settings:

Calendar	Select a calendar to control scheduling.
Unset	Select if area should automatically Unset as per the time specified in the selected calendar.
Fullset	Select this option to Fullset the area as per

	the time specified in the selected Calendar. The area will also set when the Unset Duration or Delay Interval has elapsed (See Setting and Unsetting [→ 243] section). If the Unset Duration overlaps the scheduled time, the area will use the calendar settings.
Time Locked	Select this option to time lock the area as per the selected Calendar. (Vault type area in Financial mode only)
Vault Access	Enter the number of minutes (0 – 120) to activate this timer at the end of a Time Locked Unset period. If the area is not unset after this timer expires, the area cannot be unset until the start of the next Time Locked Unset period. (Vault type area in Financial mode only)

17.9.5.2.5 Reporting



The Reporting configuration settings are applicable for Standard Areas in Commercial and Financial installations only and are only relevant if a calendar has been selected. (See Schedule [→ 240] section)

These settings enable a report to be sent to the Control Centre or nominated personnel if the panel is Set or Unset outside scheduled calendar times.

Early to Set	Enables a report to be sent if the panel is manually Fullset before a scheduled Set and before the number of minutes entered in the Timer field.
Late to Set	Enables a report to be sent if the panel is manually Fullset after a scheduled Set and after the number of minutes entered in the Timer field.
Early to Unset	Enables a report to be sent if the panel is manually Unset before a scheduled Unset and before the number of minutes entered in the Timer field.
Late to Unset	Enables a report to be sent if the panel is manually Unset before a scheduled Unset and before the number of minutes entered in the Timer field.

Reporting is done via SMS or to the ARC via SIA and Contact ID. An event is also stored in the system log.

Only events configured for late or early reporting for the area will be reported. Event reporting must also be enabled for an ARC or SMS, as described in the following sections.

Enabling Reporting of Unusual Setting/Unsetting for an ARC

To configure event reporting for an ARC configured to communicate over SIA or CID, select **Communications>Reporting>Analog ARC> Edit>Filter** to display the Event Filter page for an ARC.

Communications	FlexC	Reporting	PC Tools
Analog ARC	EDP	CEI-ABI	
Event Filter			
Alarms	<input checked="" type="checkbox"/>	Alarm activation	
Alarm Restores	<input checked="" type="checkbox"/>	Reported alarms being restored	
Confirmed alarms	<input checked="" type="checkbox"/>	Alarms confirmed by multiple zones	
Alarm Abort	<input type="checkbox"/>	Report Alarm Abort event if valid PIN is entered on keypad after alarm report	
Faults	<input checked="" type="checkbox"/>	Fault or Tamper activations	
Fault restore	<input checked="" type="checkbox"/>	Fault or Tamper restores	
Setting	<input type="checkbox"/>	Setting and Unsetting	
Early / Late	<input type="checkbox"/>	Report if Setting/Unsetting is not according to schedule	
Inhibits	<input type="checkbox"/>	Inhibit and Isolate	
Door events	<input type="checkbox"/>	Access control door events	
Other	<input type="checkbox"/>	All other types of events	
Network	<input type="checkbox"/>	Report IP Network Polling Up/Down events	
Areas	<input checked="" type="checkbox"/> 1: Marketing <input checked="" type="checkbox"/> 2: Reception	<input checked="" type="checkbox"/> 3: Finance <input checked="" type="checkbox"/> 4: Cafeteria	<input checked="" type="checkbox"/> 5: Meeting Room <input checked="" type="checkbox"/> 6: Finance
<input type="button" value="Save"/> <input type="button" value="Back"/>			

The **Early/Late** parameter is enabled to report any setting or unsetting which differs from the schedule.

Enable Reporting of Unusual Setting/Unsetting for SMS

SMS Events can be configured using both Engineer and User configuration pages. For Engineer configuration, select **Users > Users SMS > Engineer SMS > Edit:**

Users	User Profiles	Users SMS	Web Passwords	Engineer
Edit SMS settings				
General Settings				
SMS ID	9999			
User	Engineer			
SMS Number	<input type="text" value="0"/>	Phone number SMS messages will be sent to / received from		
SMS Events				
Alarms	<input type="checkbox"/>	Alarm activation		
Alarm Restores	<input type="checkbox"/>	Reported alarms being restored		
Confirmed alarms	<input type="checkbox"/>	Alarms confirmed by multiple zones		
Faults	<input type="checkbox"/>	Fault or Tamper activations		
Fault restore	<input type="checkbox"/>	Fault or Tamper restores		
Setting	<input type="checkbox"/>	Setting and Unsetting		
Early / Late	<input type="checkbox"/>	Report if Setting/Unsetting is not according to schedule		
Inhibits	<input type="checkbox"/>	Inhibit and Isolate		

Enable Early/Late to report any setting and unsetting which is not according to schedule.

17.9.5.2.6 Setting/Unsetting

The following parameters (with the exception of the Interlock parameter) are only relevant in the following cases:

- A Calendar is selected (see Schedule [→ 240]), or
- **Unset Duration** is enabled (has a value greater than zero), or
- Both of the above conditions are met.

Auto Set Warning	Enter the number of minutes to display a warning before Auto Setting. (0 - 30) Note that the panel sets either at the scheduled time or at the time defined by the Delay Unset parameter. The first warning is displayed at the configured time before the scheduled time. There are further warnings starting at one minute before setting time.
Auto Set Cancel	Enables the user to cancel Auto Setting by entering a code in the keypad.
Auto Set Delay	Enables a user to delay Auto Setting by entering a code in the keypad.
Keyswitch	Enables Auto Setting to be delayed using Keyswitch Expander.
Delay Interval	Enter the number of minutes by which to delay Auto Set. (1 - 300)
Delay Counter	Enter the number of times that Auto Setting can be delayed. (0 – 99: 0 = unlimited)
Delay Unset	Enter the number of minutes by which to delay an Unset. (0 = no delay)
Interlock Group	Select an Interlock Group to assign to this area. Interlocking only allows one area within the group to be Unset at any time. Typically used in ATM areas.
Unset Duration	If area is Unset for longer than this it will Set

	automatically. (Range 0 – 120 mins: 0 = not active).
Dual PIN	<p>If this option is enabled, two PINs are required to Set or Unset the area with the keypad. Both PINs must belong to users who have the required user right for the operation (Setting or Unsetting).</p> <p>If the second PIN is not entered within 30 seconds, or it is wrong, then the area cannot be Set or Unset.</p>

Late Working Support

An example of using the setting and unsetting parameters is for late working situations where a calendar has been configured for automatic setting of a premises at a particular time but staff may need to work late on occasion and the automatic setting needs to be delayed.

Each delay is determined by the amount configured in the **Delay Interval** parameter, and the **Delay Counter** parameter determines the number of times that setting can be delayed. A user needs the correct value in the **Auto Set Delay** in order to use this feature.

There are three ways to delay setting:

1. Entering the PIN on the keypad.
 DELAY is a menu option on the standard keypad. The buttons at the top of the comfort keypad are used to operate the delay feature
2. Using the keyswitch.
 Turning the key to the right delays setting the system by the configured delay if the maximum number of times that setting can be delayed (**Delay Counter**) has not been exceeded. Turning the key to the left sets the delay to three minutes (non-configurable). This can be done regardless of how many times setting was delayed.
3. Using a FOB, WPA or button which activates a **Delay AutoSet** trigger action. (See page 172)

Temporary Unset

To allow a system to be temporarily unset in a time period specified by a calendar, the following three parameters need to be configured:

1. **Calendar**
 A calendar needs to be configured and selected for this area.
2. **Time Locked**
 This box needs to be ticked so that the area can be unset only when allowed as per the configured calendar.
3. **Unset Duration**
 This parameter needs to be set to a value greater than zero to set an upper limit on the time the area will be unset.

The following screen shows these parameters configured with appropriate settings:

17.9.5.2.7 All Okay

All Okay Required	If selected, user must confirm 'All okay' input or silent alarm is generated. See Editing a Zone [→ 237] for details on configuring an 'All Okay' zone input.
-------------------	---

All Okay Time	Time (in seconds) in which 'All okay' must be confirmed before alarm is raised. (Range 1 – 999 seconds)
All Okay Event	Select the event type to be sent when the 'All okay' timer expires. Options are Panic (Silent), Panic and Duress.

17.9.5.2.8 RF Output

RF Output Time	Enter the number of seconds that the RF Output will remain on for. 0 seconds will toggle the output on and off.
----------------	--



The other Miscellaneous options are described in Entry/Exit [→ 239] for SPC Pro

17.9.5.2.9 Fire Exit Route

Fire exit route Doors which will open when fire occurs in this area

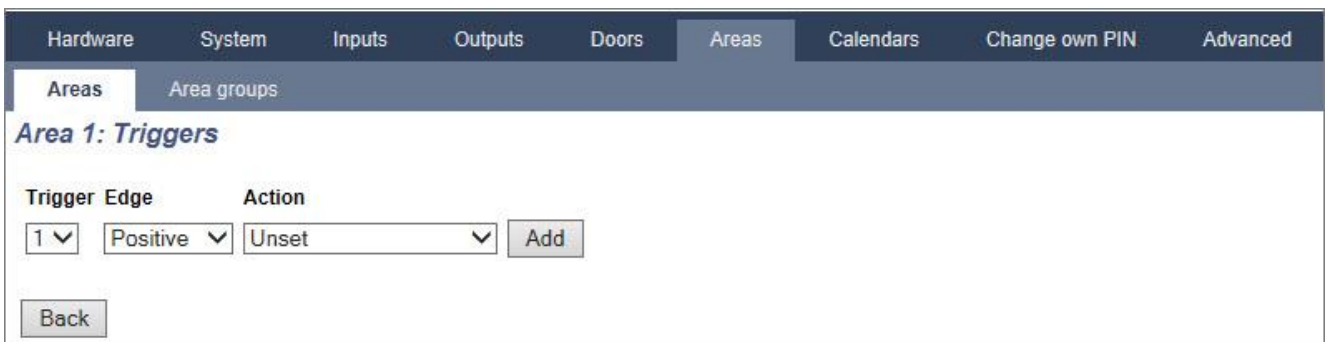
1 Entry

2 DOOR 2

Fire exit route	Select the doors which will open when fire occurs in this area. This option does not display in domestic mode.
-----------------	--

17.9.5.2.10 Area Triggers

The Triggers section is only displayed if triggers have been defined previously. (See section on Triggers)
Click on the **Edit** button to add, edit or delete trigger conditions for the area. The following page is displayed:



Configure the trigger for the area using the following parameters:

Trigger	Select a trigger from the drop down list.
Edge	The trigger can activate from either the positive or negative

	edge of the activation signal.
Action	<p>This is the action that is performed when the trigger is activated. Options are:</p> <ul style="list-style-type: none"> ● Unset ● Partset A ● Partset B ● Fullset ● Delay autose <p>This action will delay alarm setting when the autose timer is running. The trigger will only add time if the Delay Limit has not been exceeded and each trigger activation will delay setting by the time defined in Delay Interval (see section Setting/Unsetting [→ 243]).</p> <ul style="list-style-type: none"> ● Restore alarms <p>This action will clear all alarms in the configured zone.</p>

Note: Triggers cannot be configured from a keypad.

See also

📖 Triggers [→ 255]

17.9.5.3 Editing a door

1. Select **Configuration > Doors**.
⇒ A list of configured doors is displayed.
2. Click the **Edit** button.
3. Configure the fields as described in the tables below.

Door inputs

Each door has 2 inputs with predefined functionality. These two inputs, the door position sensor and the door release switch can be configured.

Name	Description
Zone	<p>The door position sensor input can be used for the intrusion part as well. If the door position sensor input is used also for the intrusion part, the zone number it is assigned to has to be selected. If the door position sensor is used only for the access part, the option "UNASSIGNED" has to be selected.</p> <p>If the door position sensor is assigned to an intrusion zone, it can be configured like a normal zone but only with limited functionality (e.g. not all zone types are selectable).</p> <p>If an area or the system is set with the card reader, the door position sensor input has to be assigned to a zone number and to the area or the system which have to be set.</p>
Description (Web and SPC Pro only)	Description of the zone the door position sensor is assigned to.
Zone Type (Web and SPC Pro only)	Zone type of the zone the door position sensor is assigned to (not all zones types are available).
Zone attributes (Web and SPC Pro only)	The attributes for the zone the door position sensor is assigned to can be modified.

Name	Description
Area (Web and SPC Pro only)	The area the zone and the card reader are assigned to. (If the card reader is used for setting & unsetting, this area will be set / unset).
Door Position (Web) DPS End Of Line (keypads) Door Position EOL (SPC Pro)	The resistor used with the door position sensor. Choose the used resistor value / combination.
DPS Normal Open	Select if the door release switch is to be a normally open or normally closed input.
Door Release (Web) DRS END OF LINE (Keypads) Door Position EOL (SPC Pro)	The resistor used with the door release switch. Choose the used resistor value / combination.
DRS Normal Open	Select if the door release switch is a normally open input or not.
No DRS (Web and SPC Pro only)	Select to ignore DRS. If a DC2 is used on the door, this option MUST be selected. If not selected, the door will open.
Reader Location (Entry/Exit) (Web and SPC Pro only)	Select the location of the entry and exit readers.
Reader formats (Web) READER INFO (Keypads)	Displays format of last card used with each configured reader. (not available in SPC Pro)



Each free zone number can be assigned to the zones but the assignment is not fixed. If the number '9' is assigned to a zone, the zone and an input expander with the address '1' is connected to the X-Bus (which is using the zone numbers 9-16). The assigned zone from the two door controller will be moved to the next free zone number. Configuration will be adapted accordingly.

Door attributes



If no attribute is activated, a valid card can be used.

Attribute	Description
Void	The card is temporarily blocked.
Door Group	Used when multiple doors are assigned to the same area and/or anti passback, custodian, or interlock functionality is required.
Card and PIN	Card and PIN are required to gain entry.
PIN Only	PIN is required. No card will be accepted.
PIN Code or Card	PIN or card are required to gain entry
PIN to Exit	PIN is required on exit reader. Door with entry and exit reader is required.
PIN to Set/Unset	PIN is required to set and unset the linked area. The card has to be presented before the PIN is entered.
Unset outside (Browser) Unset on Entry Reader (SPCPro)	Panel/area will unset, when card is presented at entry reader.

Attribute	Description
Unset inside (Browser) Unset on Exit Reader (SPCPro)	Panel/area will unset, when card is presented at exit reader.
Bypass alarm	Access is granted if an area is set and the door is an alarm or an entry zone type.
Fullset outside (Browser) Fullset on Entry Reader (SPCPro)	Panel/area will fullest, when card is presented twice at entry reader.
Fullset inside Full set on Exit Reader (SPCPro)	Panel/area will fullest, when card is presented twice at exit reader.
Force Fullset	If the user has rights, they can force set from entry reader.
Emergency	Door lock opens if a fire alarm is detected within the assigned area.
Emergency any	Fire in any area will unlock the door.
Escort	The escort feature enforces privileged card holders to escort other card holders through specific doors. If this feature is assigned to a door, a card with the "escort right" has to be presented first, to allow other cardholders without this right to open the door. The time period in which cardholders are able to present their cards after a card with escort right was presented, can be configured per door.
Prevent Passback*	Anti-passback should be enforced on the door. All doors must have entry and exit readers and must be assigned to a door group. In this mode, cardholders must use their access card to gain entry into and exit from a defined door group. If a valid cardholder has presented his access card to enter a door group and not presented the card to exit it, the cardholder is in breach of the Anti-Passback rules. Next time the cardholder attempts to enter the same door group, a hard Anti-Passback alarm will be raised and the cardholder will not be permitted entry to the door group.
Soft Passback*	Anti-passback violations are only logged. All doors must have entry and exit readers and must be assigned to a door group. In this mode, cardholders must use their access card to gain entry to and exit from a defined door group. If a valid cardholder has presented his access card to enter a door group and not presented the card to exit it, the cardholder is in breach of the Anti-Passback rules. Next time the cardholder attempts to enter the same door group, a Soft Anti-Passback alarm will be raised. However, the cardholder will still be permitted entry to the door group.
Custodian*	The custodian feature allows a card holder with custodian right (the custodian) to give other cardholders (non-custodians) access to the room. The custodian must be the first to enter the room. The non-custodians are only allowed to enter if the custodian is in the room. The custodian will not be allowed to exit until all non-custodians have left the room.
Door Sounder	Door controller PCB mounted sounder sounds on door alarms.
Ignore Forced	Door forced open is not processed.

Attribute	Description
Interlock* (Browser) Limit Interlocked Door Access (SPCPro)	Only one door in an area will be allowed open at a time. Requires Door Group.
Setting Prefix	Authorisation with prefix (A,B,* or #) key to set system
* Require door group	

Door timers

Timer	Min.	Max.	Description
Access granted	1 s	255 s	The time the lock will remain open after granting access.
Access deny	1 s	255 s	The duration after which the controller will be ready to read the next event after a invalid event.
Door open	1 s	255 s	Duration within which the door must be closed to prevent a "door open too long" alarm.
Door left open	1 min	180 min	Duration within which the door must be closed to prevent a "door left open" alarm.
Extended	1 s	255 s	Additional time after granting access to a card with extended time attribute.
Escort	1 s	30 s	Time period after presenting a card with escort attribute within a user without escort right can access the door.

Door calendar

Door locked	Select a calendar which should lock the door during the configured time. No card / pin will be accepted during this time.
Door locked	Select a calendar which should unlock the door. The door will be unlocked during the configured time.

Door triggers

Trigger	Description
Triggers that will Momentarily Unlock door	If the assigned trigger is activated, the door will unlock for a defined period, then lock again.
Trigger that will lock the door	If the assigned trigger is activated, the door will get locked. No card / PIN will be accepted.
Trigger that will unlock the door	If the assigned trigger is activated, the door will get unlocked. No card / PIN will be needed to open the door.
Trigger that will set the door to normal	If the assigned trigger is activated, the door will get back to normal operation. This is to undo locking / unlocking of the door. A card / will be is needed to open the door.

17.9.5.3.1 Door Interlock

Door interlock is feature that prevents the remaining doors in an interlock group from opening if any one door in the group is open.

The following are example of how this feature is used:

- In two-doors entry systems used in some banks and other buildings. Usually push buttons or card readers are used to gain entrance, and red and green LEDs show if the door can be opened or not.
- In ATM technical areas connecting ATM doors. Typically all the ATM doors in addition to the door that gives access to the area would be interlocked.

To create a door lock:

1. Create a Door Group. See Editing a door [→ 246].
2. Set the **Interlock** attribute for the required doors in the group. See Editing a door [→ 246].
3. Configure a door output for door interlock operation. This output becomes active for all the doors of the interlock group whenever a door belonging to the group is open, including the open door itself.
This output could be connected, for example, to a red LED or light to indicate that the door could not be opened, and if inverted could be connected to a green LED or light.

To configure an output for door interlock.

1. In Full Engineer mode, select **Configuration > Hardware > X-BUS > Expanders**.
2. In the **Expander Configuration** page, click on the **Change Type** button for the required output.
3. Select **Door** as the output type.
4. Select the required door and **Interlocked** as the output type.

Hardware System Inputs **Outputs** Doors Areas Calendars Change own PIN Advanced

Outputs X-10

Output Type

Disabled

System

External Bell

Area

1: Marketing

External Bell

Zone

1 Front door

Door

Door 1 Entry

Interlocked


17.9.5.4 Adding an area group

You can use area groups for configuring multiple areas. So the configuration must not be done for every single area.

▷ Only if the option (multiple) **Areas** is activated.

- Select **Settings > Areas > Area groups**.

1. Click on the **Add** button.
2. Enter a description for the group.
3. Select the areas that are to be assigned to this group.
4. Click **Add**.

	NOTICE
	To use the area groups for the Comfort Keypad, activate all Areas in the Areas field under Configuration > Hardware > X-BUS > Keypads > Type: Comfort Keypad .

17.9.6 Calendars

Calendars are used for scheduling time-based control for multiple panel operations as follows:

- Automatic setting and/or unsetting of areas
- Automatic setting and/or unsetting of other panel operations including triggers, enabling of users, zones, physical outputs, etc.

At any particular time, any schedule within the calendar can be 'active' if its time conditions are satisfied.

Each week of the year is assigned an ordinal number. Depending on the fall of days within a month, there may be 52 or 53 weeks in one year. The SPC calendar implementation conforms to the ISO8601 international standard.

Configuring calendars

- Select **Configuration > Calendars**.
⇒ A list of configured calendars is displayed:

Calendar	Description	Edit	Delete
1	Calendar_1	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
2	Calendar 2	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Performable actions

Add	Add a new calendar.
Exceptions	Configure setting schedules for exceptional circumstances outside of the normal weekly schedules
Edit/View	Edit or view the selected calendar.
Delete	Delete the selected calendar. The calendar cannot be deleted if it is currently assigned to an SPC configuration item i.e. zone, area, user profile, output, trigger, door or X-Bus component. A message is displayed indicating the assigned item.



Global calendars created using SPC Manager cannot be deleted as shown with Calendar 3 above.

17.9.6.1 Adding / Editing a calendar

- Select **Configuration > Calendars > Add**.
⇒ The following window will be displayed:

Hardware System Inputs Outputs Doors Areas **Calendars** Change own PIN Advanced

Calendar Added

Configure Calendar - 3

Description

Week Schedule:

Week 1:	<input type="text" value="Type 1"/>	Week 15:	<input type="text" value="Type 1"/>	Week 29:	<input type="text" value="Type 1"/>	Week 43:	<input type="text" value="Type 1"/>
Week 2:	<input type="text" value="Type 1"/>	Week 16:	<input type="text" value="Type 1"/>	Week 30:	<input type="text" value="Type 1"/>	Week 44:	<input type="text" value="Type 1"/>
Week 3:	<input type="text" value="Type 1"/>	Week 17:	<input type="text" value="Type 1"/>	Week 31:	<input type="text" value="Type 1"/>	Week 45:	<input type="text" value="Type 1"/>
Week 4:	<input type="text" value="Type 1"/>	Week 18:	<input type="text" value="Type 1"/>	Week 32:	<input type="text" value="Type 1"/>	Week 46:	<input type="text" value="Type 1"/>
Week 5:	<input type="text" value="Type 1"/>	Week 19:	<input type="text" value="Type 1"/>	Week 33:	<input type="text" value="Type 1"/>	Week 47:	<input type="text" value="Type 1"/>
Week 6:	<input type="text" value="Type 1"/>	Week 20:	<input type="text" value="Type 1"/>	Week 34:	<input type="text" value="Type 1"/>	Week 48:	<input type="text" value="Type 1"/>
Week 7:	<input type="text" value="Type 1"/>	Week 21:	<input type="text" value="Type 1"/>	Week 35:	<input type="text" value="Type 1"/>	Week 49:	<input type="text" value="Type 1"/>
Week 8:	<input type="text" value="Type 1"/>	Week 22:	<input type="text" value="Type 1"/>	Week 36:	<input type="text" value="Type 1"/>	Week 50:	<input type="text" value="Type 1"/>
Week 9:	<input type="text" value="Type 1"/>	Week 23:	<input type="text" value="Type 1"/>	Week 37:	<input type="text" value="Type 1"/>	Week 51:	<input type="text" value="Type 1"/>
Week 10:	<input type="text" value="Type 1"/>	Week 24:	<input type="text" value="Type 1"/>	Week 38:	<input type="text" value="Type 1"/>	Week 52:	<input type="text" value="Type 1"/>
Week 11:	<input type="text" value="Type 1"/>	Week 25:	<input type="text" value="Type 1"/>	Week 39:	<input type="text" value="Type 1"/>	Week 53:	<input type="text" value="Type 1"/>
Week 12:	<input type="text" value="Type 1"/>	Week 26:	<input type="text" value="Type 1"/>	Week 40:	<input type="text" value="Type 1"/>		
Week 13:	<input type="text" value="Type 1"/>	Week 27:	<input type="text" value="Type 1"/>	Week 41:	<input type="text" value="Type 1"/>		
Week 14:	<input type="text" value="Type 1"/>	Week 28:	<input type="text" value="Type 1"/>	Week 42:	<input type="text" value="Type 1"/>		

- Provide a **Description** for the calendar (max. 16 characters)

Copying a Calendar

To make a copy of this calendar structure, click on the **Replicate** button.

A new calendar is created with the same configuration as the original calendar. You can provide a new description for the new calendar and edit the calendar configuration as required.

Week Types

Calendars are configured by assigning an optional Week Type for each calendar week. Up to three Week Types may be defined for each calendar. Not all weeks must have a Week Type (i.e. a Week Type may be 'None'). There is a system maximum number of 64 calendar configurations.

To configure a week type

1. Click **Week Types**.
2. Enter the desired times for setting / unsetting or for triggers. Use time guidelines for Automatic Setting/Unsetting of Areas (see page [→ 254]), or for Automatic Setting/Unsetting of other Panel Operations (see page [→ 254]).
⇒ Up to three week types may be configured.
3. Click **Save** and then **Back**.
4. Select the desired week type from the drop down menu for each of the required scheduled weeks in the calendar.
5. Click **Save**.
6. Click **Back**.

See also

- 📖 Automatic setting/unsetting of areas [→ 254]
- 📖 Automatic setting/unsetting of other panel operations [→ 254]

17.9.6.1.1 Exceptions

Exceptions or exception days are used to configure automatic setting schedules for exceptional circumstances outside of the normal weekly schedules defined in the calendars. Exceptions are defined with a start and end date (day/month/year) and up to four on/off timing periods for different panel operations including automatic setting/unsetting of areas or the switching on/off of triggers or outputs. A maximum of 64 exceptions can be configured on the system.

Exceptions are generic entities that can be assigned to one or more calendars. When an exception is assigned to a calendar, the exception settings override any calendar configuration for that start and end date period with both dates inclusive.

Configuring Exception Days

1. Select **Configuration > Calendars > Exceptions > Add**.
⇒ The following window will be displayed.
2. Configure the fields as described in the table below.

Hardware	System	Inputs	Outputs	Doors	Areas	Calendars	Change own PIN	Advanced
Calendar Exceptions								
Description: <input type="text"/>								
Start date: Day: <input type="text" value="1"/> / Month: <input type="text" value="Jan"/> / Year: <input type="text" value="2014"/>								
End date: Day: <input type="text" value="1"/> / Month: <input type="text" value="Jan"/> / Year: <input type="text" value="2014"/>								
Times: On / Unset hh:mm <input type="text"/> Off / Set hh:mm <input type="text"/> On / Unset hh:mm <input type="text"/> Off / Set hh:mm <input type="text"/> On / Unset hh:mm <input type="text"/> Off / Set hh:mm <input type="text"/> On / Unset hh:mm <input type="text"/> Off / Set hh:mm <input type="text"/>								
Calendars: <input type="checkbox"/> 1: Calendar_1 <input type="checkbox"/> 2: Calendar_2 <input type="checkbox"/> 3: Calendar_3 <input type="checkbox"/> 4: Calendar_4								
Save Back								

Description	Enter a name for the exception (16 characters max).
Start Date/End Date	Select the start and end date.
On Time/Off Time	Select the desired times for setting / unsetting or for triggers. Use time guidelines for Automatic Setting/Unsetting of Areas (see page [→ 254]), or for Automatic Setting/Unsetting of other Panel Operations (see page [→ 254]).
Calendars Assigned to	Select the desired calendar(s) for effect.

!	NOTICE
	Global exception days created remotely using the SPC Manager tool cannot be deleted or removed.

17.9.6.2 Automatic setting/unsetting of areas

A calendar can be configured for area auto-sets or auto-unsets.

For any day of the week, a configuration can have a maximum of 4 set times and 4 unset times. Configured times use the 24 hour clock (hh:mm). If the hour is 24, then minutes must be 00, such as midnight is 24:00. It is possible to define a set time without an unset and vice-versa. Configured times trigger the area to either set or unset (provided all conditions are satisfied). Times entered are not considered as a duration of time, rather they are a point in time that said action (set/unset) will occur. If the controller is powered up or reset, the set/unset status is kept and subsequent set or unset times occur according to configuration.

17.9.6.3 Automatic setting/unsetting of other panel operations

Panel operations including triggers, enabling of users, zones, physical outputs can be automatically set or unset using On/Off, True/False or Active/Inactive state configurations.

On/Off, True/False or Active/Inactive states can be assigned to an output that effectively turns on or off and can be configured for any day of the week. State configurations have a maximum of 4 set times and 4 unset times. Configured times use the 24 hour clock (hh:mm). If the hour is 24, then minutes must be 00, such as midnight is 24:00. Each configuration consists of a pairing of settings for On/Off, True/False, Active/Inactive states. Any one setting without a respective corresponding setting is disregarded.

17.9.7 Change own PIN

To change a PIN, see Changing Engineer PIN and web password [→ 194].

17.9.8 Configuring advanced settings

17.9.8.1 Triggers

A trigger is a system state (e.g. zone closing / time / system event (alarm) etc.) that can be used as inputs to the Cause & Effects. The triggers can be logically assigned together using the logical operators and / or to create user outputs. The system supports up to a maximum of 1024 triggers across all its Cause & Effects system.

1. Select **Configuration > Advanced > Triggers**.
⇒ The following window will be displayed.
2. Configure the fields as described in the table below.

Trigger	System generated number for new trigger. Trigger will only become active if one of the 2 optional steps (calendar/time limitation) is configured
Description	Enter a text description for the trigger
Calendar	Select a calendar, if required. If selected, the trigger will only be in effect during this calendar period. See page [→ 251].
Active Time/Timer	Enter the number of seconds that the trigger conditions must be true before the trigger will activate
Time limited	Select a time period between 00:00 and 24:00 during which the trigger will only be in effect. The Start time is inclusive, the end time is exclusive. Note: This parameter delays a trigger transition from ON to OFF only; from OFF to ON is immediate.
Trigger conditions	The trigger is ON if the following conditions are satisfied (i.e. a logical AND operation is performed): Zone – the trigger is ON if the configured zone is in one of the following states - open, closed, short or disconnected. Door – the trigger is ON if the any of the following door options are configured; Entry granted, Entry denied, Exit granted, Exit denied, Door open too long, Door left open, Door forced open, Door normal, Door Locked, Door unlocked System - the trigger is on if the system output is in the configured state, which can be on or off. Possible system outputs are “External Bell”, “Alarm”, etc. Area - the trigger is ON if the area output is in an ON or OFF state. Possible

	<p>area outputs are “External Bell”, “Alarm”, etc.</p> <p>Wireless FOB – this condition can be configured for a particular user or for any user. With this configuration, if the configured user (or any user) presses the ‘*’ key on the FOB, it will cause an instantaneous pulse OFF/ON/OFF. This only applies for FOBs that have been registered with the system.</p> <p>Wireless FOB Panic – this condition can be configured for a particular user or for any user. With this configuration, if the configured user (or any user) presses the ‘*’ key on the FOB Panic, it will cause an instantaneous pulse OFF/ON/OFF. This only applies for FOB Panics that have been registered with the system.</p> <p>WPA – the trigger is activated if a button or combination of buttons is pressed. It is possible to assign a trigger condition to all WPAs or just to one specific WPA. When a trigger with a WPA trigger condition is defined, it can be assigned to a mapping gate for many purposes including arming a system, turning on lights or opening a door.</p> <p>Keypad valid PIN – this condition can be configured for a particular user or for any user. With this configuration, if the configured user (or any user) enters a valid PIN, or presents a configured PACE, it will cause an instantaneous pulse OFF/ON/OFF.</p> <p>Keyswitch – the trigger can be configured for a specific key position on the keyswitch.</p> <p>Time Trigger – the trigger is on at the specific time entered in the box provided, in the format hh:mm.</p>
--	---



⚠ WARNING

Your system will not comply with EN standards if you enable a trigger to set the system without a valid PIN being required.

17.9.8.2 Mapping Gates

Triggers are used with Mapping Gates, which are virtual outputs defined by the user that can be mapped to a physical output. There can be a maximum of 512 Mapping Gates.



For continuous output, when the trigger is a valid user code, both states must be the same, either both negative or both positive.

1. Select **Configuration > Advanced > Mapping Gates**.

⇒ The following window will be displayed.

Gate	Description	Protected	Quick Key	Timer	Triggers	Delete
1	MG1	<input type="checkbox"/>	#1	0 * 100ms	Edit	Delete
2	MG2	<input type="checkbox"/>	#2	0 * 100ms	Edit	Delete

Save Add

2. Enter a **Description** for the gate. This is important as no mapping gate number, only the description, is displayed on the **Outputs** user page for turning on and off gates.

3. Tick the **Protected** check box if you do not want to allow users to turn on and off this gate, even if they have the right to do so. A protected gate does not appear in the **Outputs** setting page for users.
4. Select desired **Quick Key**.
A quick key is a '#' followed by a single digit pressed at the keypad. If a shortcut is configured and is pressed at the keypad, the user is prompted to turn the output on or off.



There may be many outputs activated by one shortcut, both X-10 and Mapping Gates.

5. Add a **Timer** for the gate. Time quantity used is 1/10 of a second.
6. Click on the **Triggers** button to configure triggers for turning the output on and turning it off. In both cases, a positive or negative edge of the trigger needs to be defined. See Triggers [→ 255] for details of configuring triggers.
7. Click **Add** to add a new gate or **Save** to save the new settings for an existing gate.

See also

Triggers [→ 255]

17.9.8.3 Audio/Video Verification

To set up Audio/Video Verification on an SPC system:

1. Install and configure Audio Expander (s)
2. Install and configure Video Camera(s).
3. Install and configure Audio Equipment.
4. Configure Verification Zone(s).
5. Test audio playback from verification zones.
6. Assign Verification Zone(s) to physical zone(s).
7. Configure Verification Settings.
8. View images from verification zones in web browser or SPC Pro.

!	NOTICE
	Keypads and access control may be disabled for several minutes while sending an audio file to the panel, depending on the size of the file.

17.9.8.3.1 Configuring Video

Overview

Cameras are used for video verification. The SPC panel supports a maximum of four cameras. Only IP cameras are supported and the panel must have an Ethernet port.

**NOTICE**

Cameras must not be shared with other CCTV applications.

Cameras can only be configured with the web browser or SPC Pro. Configuration with the keypad is not supported. SPC Pro provides an easier method of configuration and is recommended.

The panel supports two camera resolutions:

- 320X240
This setting is recommended if you want to view images on the browser)
- 640X480 (with some restrictions).

The following cameras are supported in addition to other generic cameras:

- Vanderbilt CCIC1410 (1/4" VGA IP Colour Camera)
- Vanderbilt CFMC1315 (1/3" 1.3 MP Indoor Dome Colour Camera)

A command string is available as a default to access configuration details for the above cameras directly. Other generic IP cameras require a command string to be entered manually.

Adding Camera

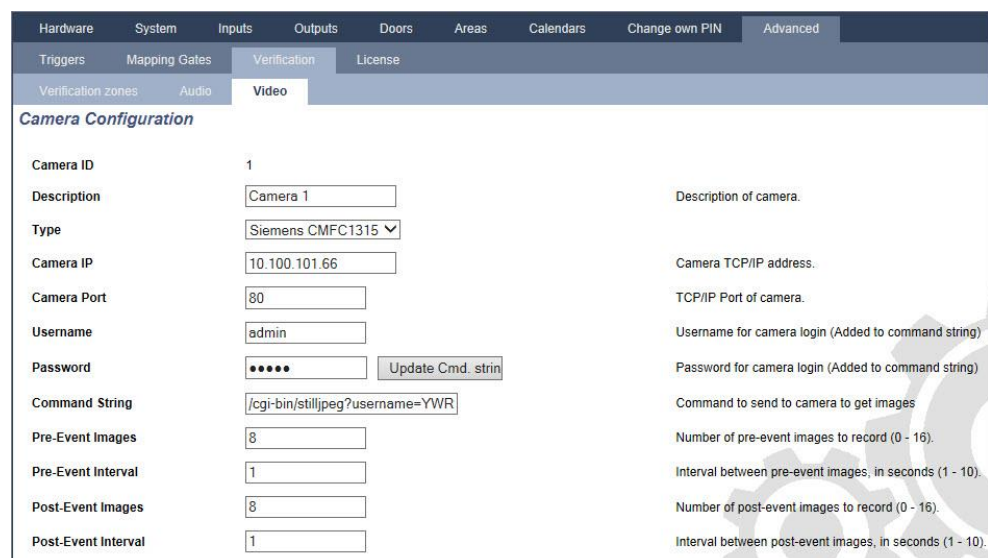
1. Select **Configuration > Advanced > Verification > Video**.

⇒ A list of any previously configured cameras is displayed and their online or offline status. A camera is online if an image was obtained from the camera in the previous 10 seconds.



2. Click on the **Add** button to add a new camera or the **Edit** button to edit an existing camera.

⇒ The following screen is displayed.



3. Configure the camera with the following parameters:

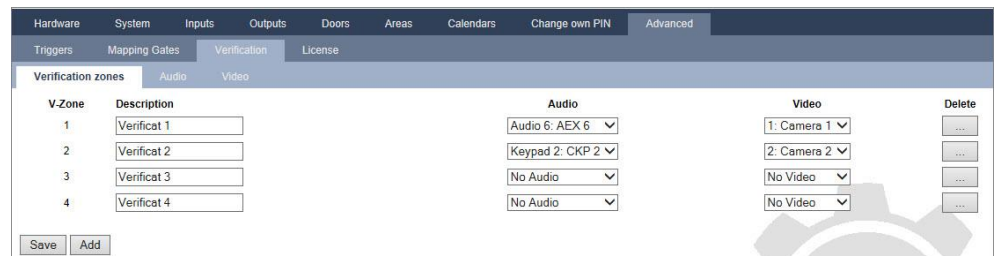
Camera ID	System generated Camera ID.
Description	Enter a description to identify this camera.
Type	Select from one of the following camera types: <ul style="list-style-type: none"> ● Generic ● Vanderbilt CCIC1410 ● Vanderbilt CFMC1315
Camera IP	Enter the IP address of the camera.
Camera Port	Enter the TCP port the camera listens on. Default is 80. Note: The CCIC1410 camera can only be used over port 80 only.
Username	Vanderbilt CCIC1410 and CFMC1315 cameras only. Enter a login username for the camera which will be added to the command string below when the Update Cmd. String button is pressed.
Password	Vanderbilt CCIC1410 and CFMC1315 cameras only. Enter a login password for the camera which will be added to the command string below when the Update Cmd. String button is pressed.
Command String	Enter the command string to be sent to the HTTP server on the camera in order to obtain images. This string should include the user name and password for the camera. Consult the camera documentation for the specific string required for the camera type selected. SPC Pro can configure this automatically if connected to a Vanderbilt CCIC1410 or CFMC1315 camera over a LAN. The default command string for a Vanderbilt CCIC1410 or CFMC1315 camera with no password is "/cgi-bin/stilljpeg".
Pre-event images	Enter the number of pre-event images to record (0 - 16). Default is 8.
Pre-event interval	Enter the time interval, in seconds, between pre-event images (1 - 10). Default is 1 second.
Post-event images	Enter the number of post-event images to record (0 - 16). Default is 8.
Post-event interval	Enter the time interval, in seconds, between post-event images, in seconds (1 - 10). Default is 1 second.

17.9.8.3.2 Configuring Verification Zones

To create a verification zone

- Go to **Configuration > Advanced > Verification > Verification zones**.

⇒ A list of any existing verification zones is displayed.



- Click on the **Add** button.
- Enter a **Description** for the zone.
- Select an **Audio** expander from the drop down list.

5. Select a **Video** from the drop down list.
6. Click on the **Save** button.
7. Assign this verification zone to a physical zone on the SPC system. (See Editing a Zone [→ 237])



The audio input and output for the verification zone can be tested by the engineer only in SPC Pro.

See also

- Editing a zone [→ 237]

17.9.8.3.3 Configuring Verification Settings

Note: The following settings apply to all verification zones [→ 259].

1. Select **Configuration > Advanced > Verification > Audio**.

⇒ The following screen is displayed.

The screenshot shows the 'Verification settings' page in the SPC Pro interface. The navigation menu at the top includes Hardware, System, Inputs, Outputs, Doors, Areas, Calendars, Change own PIN, and Advanced. Under 'Advanced', there are tabs for Triggers, Mapping Gates, Verification, and License. The 'Verification' tab is active, and within it, there are sub-tabs for Verification zones, Audio, and Video. The 'Audio' sub-tab is selected, showing the 'Audio Settings' section. It contains two rows of settings: 'Pre-Event Recording' with a value of 10 and 'Post-Event Recording' with a value of 30. Both values are followed by the word 'Seconds'. To the right of each input field is a small text description: 'Duration of pre-event recording in seconds. (0 - 120)' and 'Duration of post-event recording in seconds. (0 - 120)'. A 'Save' button is located at the bottom left of the settings area.

2. Configure the following settings.

Pre-event recording	Enter a required duration of pre-event audio recording, in seconds (0 - 120). Default is 10.
Post-event recording	Enter a required duration of post-event audio recording, in seconds (0 - 120). Default is 30.

17.9.8.3.4 Viewing Video Images

Video images from the configured cameras can be viewed in the web browser in Full or Soft Engineer modes. This functionality is also available to users that have the View Video right in their profile. (See Setting User Rights [→ 183]) The Web Access right must also be enabled for this functionality.

The View Video right can also be set on the keypad and in SPC Pro ('Video in Browser' setting).

To view images, go to **SPC Home > Video**. See Viewing Video [→ 165].

See also

- Adding / Editing a User [→ 183]
- Configuring Video [→ 257]

17.9.8.4 Updating SPC Licenses

The **License Options** feature provides a mechanism for the user to update or add functionality to the SPC system, for example, for migrations, where installed peripherals, which are not licensed for SPC, need to be supported by an SPC controller.

1. Select **Configuration > Advanced > License**.

2. Contact technical support with the requested functionality and quote current license key as displayed.
 - ⇒ If request is approved, a new license key is issued.
3. Enter the new key in the field provided.

17.10 Configuring Communications

17.10.1 Communications Settings

17.10.1.1 Configuring the networking services of the panel

1. Select **Communications > Communications > Services**.
 - ⇒ The following window will be displayed.
2. Configure the fields as described in the table below.

Communications	FlexC ®	Reporting	PC Tools
Services	Ethernet	Modems	Serial ports

Network Services

HTTP Enabled	<input checked="" type="checkbox"/>	Check to enable web server
HTTP Port	<input type="text" value="443"/>	Port web server is listening on
TLS Enabled	<input checked="" type="checkbox"/>	Check to enable the encrypted web server
Telnet Enabled	<input type="checkbox"/>	Check this to enable telnet server
Telnet Port	<input type="text" value="23"/>	Port telnet server is listening on
SNMP Enabled	<input type="checkbox"/>	Check to enable Simple Network Management Protocol
SNMP Community	<input type="text" value="public"/>	Community ID for SNMP protocol
ENMP Enabled	<input checked="" type="checkbox"/>	Check to enable Enhanced Network Management Protocol
ENMP Port	<input type="text" value="1287"/>	Port ENMP is listening on
ENMP Password	<input type="text" value="password"/>	Password used to encrypt ENMP packets
ENMP Change Enabled	<input checked="" type="checkbox"/>	Check to enable network config changes through ENMP

HTTP Enabled	Tick this box to enable the embedded web server on the panel.
HTTP Port	Enter the Port number that the web server is 'listening' on. By default this is set to 443.
TLS Enabled	Tick this box to enable encryption operation on embedded web server. By default this is enabled. With TLS enabled, web pages can only be accessed by using 'https://' prefix before typing the IP address.
Telnet Enabled	Tick this box to enable the Telnet server. (Default: Enabled) Note: Using Telnet without a comprehensive knowledge can damage the controller configuration; this should only be used if the user has sufficient knowledge or is being instructed by someone with such knowledge.
Telnet Port	Enter the number of the Telnet port.
SNMP Enabled	Tick this box to enable Simple Network Management Protocol (SNMP). (Default: Disabled)
SNMP Community	Enter the Community ID for the SNMP protocol. (Default : Public)
ENMP Enabled	Tick this box to enable Enhanced Network Management Protocol (ENMP). (Default : Disabled)
ENMP Port	Enter the ENMP port number (default: 1287).
ENMP password	Enter the password for the ENMP protocol.
ENMP change enabled	Check this box to enable network changes to be made with ENMP protocol.

17.10.1.2 Ethernet

The Ethernet port on the controller can be configured from both the browser and keypad interfaces. An Ethernet connection with the SPC controller can be established using a direct connection or a LAN connection.

1. Select **Communications > Communications > Ethernet**.
⇒ The following window will be displayed.
2. Configure the fields as described in the table below.

IP address	Enter the IP address of the panel.
IP Network	Enter the subnet mask that defines the type of network address structure implemented on the Local Area Network (LAN).
Gateway IP Address	Enter the IP address of the IP gateway if one exists. This is the address that IP packets will be routed through when accessing external IP addresses on the internet.
Enable DHCP	Click this Button to enable dynamic address assignment on the panel.
DNS Server	Enter the IP address of the DNS server.

17.10.1.3 Modems

The SPC panel provides two on-board modem interface connectors (primary and backup) that allow you to install PSTN or GSM onto the system.



After a factory default, during the process of initial setup of the system with the keypad, the panel detects if it has a primary or backup modem fitted, and if so, it displays the modem type and automatically enables it (or them) with the default configuration. No other modem configuration is allowed at this stage.

To program the modem(s):

Note: A modem must be installed and identified. (See section Installing plug-in modules [→ 87])

1. Select **Communications > Communications > Modems**.
2. Click **Enable** and **Configure**.

Communications		FlexC	Reporting	PC Tools
Services	Ethernet	Modems	Serial ports	Portal
Modem 1 Primary		Modem 2 Backup		
Status:	Line Fault	Status:	Fault: E51	
Type:	IntelliModem PSTN	Type:	IntelliModem GSM	
Firmware Version:	2.09 [28MAR14]	Firmware Version:	3.08 [13NOV13]	
Hardware Version:	---	Hardware Version:	---	
<input type="button" value="Configure"/> <input type="button" value="Disable"/>		<input type="button" value="Configure"/> <input type="button" value="Disable"/>		



SMS detection and configuration is not available unless modems that are configured and enabled.

17.10.1.3.1 SMS test

Once the SIM feature is enabled for a modem, a test may be performed to desired recipient number with a composed message.

1. Enter the mobile phone number (including 3-digit country prefix) in the number field and a short text message in the message box.
2. Click **Send SMS** and verify the message is received on the mobile phone.



The SMS test is provided only for the purpose of ensuring the SMS feature is operating correctly. A short text message using alphabetic characters (A-Z) should be used to test this feature.

The SMS operates using a standard protocol that is used in SMS telephones. Please note that some PSTN operators do not provide the service of SMS over PSTN. For SMS to operate over PSTN the following criteria is required:

- Caller ID needs to be enabled on the telephone line.
- Direct telephone line – not through PABX or other comms equipment.
- Please also note that most Service Providers only allow SMS to a telephone registered in the same country (this is due to billing issues).

17.10.1.3.2 SMS feature

The SPC controller allows remote (SMS) messaging on systems with installed modems. Once a modem is installed, the following configurations are necessary for SMS:

- SMS-enabled modem. See page.
- SMS Authentication. See page.
- Engineer SMS Control. See page.
- User SMS Control. See page.

Depending on configurations, features include these SMS abilities:

- Event notification. See page.
- Remote Commands (users may be assigned select remote commands. See page.

17.10.1.3.3 SMS system options

Once a modem is installed and the SMS feature enabled, for SMS operations the SPC system must apply the SMS Authentication.

1. Select **Configuration > System > System Options**.
2. Select the desired option from the drop-down menu **SMS Authentication**:
 - **PIN Only**: This is a valid user code. See page [→ 105].
 - **Caller ID Only**: This is the phone number (including 3-digit country prefix code) as configured for User SMS Control. Only when this option is selected will the SMS Control be available for configuration by the user.
 - **PIN and Caller ID**
 - **SMS PIN Code Only**: This is a valid PIN code configured for the user which different from the user's login code. See page. Only when this option is selected will the SMS Controls be available for configuration by the user.
 - **SMS PIN Code & Caller ID**

17.10.1.3.4 SMS commands

Once the SMS setup and configuration is complete, SMS features may be activated. Commands, depending on SMS configuration are sent using a code or caller ID. The type of code depends on what is set for SMS Authentication. For more information on SMS Authentication, see page [· 136]).

The table below provides all available SMS commands. Subsequent action and response are also provided.

SMS Commands are sent as texts to the phone number of the SIM card on the controller.

For commands using code, the format of the text is the code followed by either a space or a full stop. Where **** is the code and "command" is the command: ****.command or **** command.

For example, the command "HELP" is this text: **** HELP or ****.HELP.

COMMANDS (**** = code)			
Using Code	Using Caller ID	Action	Response
**** HELP ****.HELP	HELP	All available commands displayed	All available commands
**** FSET (FULLSET) ****.FSET	FSET	Fullset Alarm	Time/date of system set. If applicable, responds with open zones/forceset zones
****ASET (PARTSET A) ****.ASET		Allows Partset A of alarm by SMS	
**** BSET (PARTSET B) ****.BSET			
**** USET ****.USET	USET	Unset Alarm	System Unset
**** SSTA (STATUS) ****.SSTA	SSTA	Status displayed	Status of system and applicable areas
**** XA1.ON		Where X10 device is identified as "A1", it is	Status of "A1"

****.XA1.ON		triggered on.	
**** XA1.OFF ****.XA1.OFF		Where X10 device is identified as "A1", it is triggered off.	Status of "A1"
**** LOG ****.LOG		Up to 10 recent events displayed	Recent events
**** ENG.ON ****.ENG.ON	ENG.ON	Enable Engineer access	Engineer status
**** ENG.OFF ****.ENG.OFF	ENG.OFF	Disable Engineer access	Engineer status
**** MANA.ON ****.MANA.ON		Enable Manufacturer access	Manufacturer status
**** MAN.OFF ****.MAN.OFF		Disable Manufacturer access	Manufacturer status
**** O5.ON ****.O5.ON		Where output is identified as "O5", it is triggered on	Status of "O5"
**** O5.OFF ****.O5.OFF		Where output is identified as "O5", it is triggered off	Status of "O5"



For SMS recognition, output identification uses the format ONNN, where O stands for output, and NNN are the numeric placeholders, of which not all are necessary. Example: O5 for Output 5.

For SMS recognition, X-10 device uses the format: XYNN, where X stands for X-10; Y stands for the alphabetic identity and NN are the available numeric placeholders. Example: XA1.

17.10.1.3.5 PSTN modem

1. Select **Communications > Communications > Modems > Configure**.
2. Configure the fields as described in the table below.

Communications	FlexC	Reporting	PC Tools
Services	Ethernet	Modems	Serial ports
Portal			

PSTN Modem settings [Primary]

Country: Ireland

Incoming Calls:

- Don't answer incoming calls
- Answer after: 1 Ring
- Answer when after one ring phone is hung up, then immediately dialled again.

Prefix: 086

Line Monitoring: Enable

Monitoring timer: 0

Modem Fault Time: 60

SMS Enable:

SMS Server: 17409900

Automated SMS: Disabled

Automated SMS Number:

Test Call Time: ---

Dial Up Internet Configuration


Dial Up Internet Enable:

Phone Number:

Username:

Password:

Save Back Test SMS



Modem settings

Country	Select the country that the SPC is installed in.
SIM PIN	Only for GSM. Enter the PIN for the SIM card installed in the GSM module.
Allow Roaming	Select to enable GSM roaming. Note: Changing this setting resets the modem. Note: Supported on GSM modems v3.08 or higher.
Incoming Calls	The modem can be programmed to answer calls based on the following conditions: <ul style="list-style-type: none"> ● Don't answer calls: Modem never answers calls. ● Answer after 'x' rings: Select the number of rings after which the modem answers the incoming call. ● Answers after the calling party calls the modem, hangs up after 1 ring burst only and then immediately re-calls the modem. The SPC system knows to automatically answer the call in this condition. ● Only answer when 'Engineer Access' is granted.
Prefix	Enter the number required to access a line. (e.g. if connected to a PBX)
Line Monitoring	PSTN Modem: Enable this feature to monitor the voltage of the line connected to the modem. GSM Modem: Enable this feature to monitor the signal level from the GSM mast connected to the modem. The Fullset option only enables this feature while the system is Fullset. Note : EN 50131-9 Confirmation configuration In order for EN50131-9 Confirmation to operate correctly, line monitoring must be enabled. (refer to System Options [→ 222])
Monitor Timer	Select the period (in seconds) for which the line voltage must be seen

	as being incorrect before the line is deemed by the SPC to be faulty.
Modem Fault Time	Time delay for a system alert (0 - 9999 seconds). Default 60 seconds.
SMS Enable	<p>Tick this checkbox to enable the SMS feature on the system.</p> <p>Note: The SMS operates using a standard protocol that is used in SMS telephones. Please note that some PSTN operators do not provide the service of SMS over PSTN. For SMS to operate over PSTN the following criteria is required:</p> <p>Caller ID needs to be enabled on the telephone line.</p> <p>Direct telephone line – not through PABX or other comms equipment.</p> <p>Please also note that most Service Providers only allow SMS to a telephone registered in the same country (this is due to billing issues).</p> <p>Note: SMS over PSTN is no longer supported. The functionality remains in the product for backward compatibility.</p>
SMS Server Number	Only for PSTN. This number automatically displays the default number for SMS for the country selected. Enter an appropriate phone number of the SMS service provider that is accessible in your location.
Automated SMS	Select the timing for automated SMS messages.
Automated SMS Number	Enter SMS number to receive automated SMS messages.
Test Call Time	Displays time of last SMS test call.
GSM Chip Version	<p>Displays the GSM WISMO version number.</p> <p>If no version number is available, "---" is displayed.</p>
GPRS Access Point (APN)	Only for GSM. Access Point Details must be provided by service provider.
GPRS Access Point User Name	Only for GSM. Access Point Details must be provided by service provider.
GPRS Access Point Password	Only for GSM. Access Point Details must be provided by service provider.

Click the **Test SMS** button to send a short text message for the purposes of testing the system.

Note: The SMS test is provided only for the purpose of ensuring the SMS feature is operating correctly. A short text message using alphabetic characters (A-Z) should be used to test this feature.



The SMS test is provided only for the purpose of ensuring the SMS feature is operating correctly. A short text message using alphabetic characters (A-Z) should be used to test this feature.

When using the SMS message feature over a PSTN line, it is necessary to program the phone number of the SMS service provider that services the area in which the SPC is installed. The SPC system automatically dials this number to contact the SMS server whenever the SMS feature is activated. Calling line identity **MUST** be enabled on the PSTN line for this feature to operate. Each country will have its own SMS service provider with a unique phone number.



This feature is not released in all countries. Please contact your local supplier for more information (support of feature, recommended service provider).



Check with country specific service providers for availability of service and SMS server number.
Some SMS servers may have additional technical requirements for the correct operation of the service. Check with the local SMS service provider for details on these requirements.

17.10.1.3.6 GSM modem

- ▷ A GSM modem must be properly installed and functioning correctly.
- 1. Select **Communications > Communications > Modems > Configure**.
 - ⇒ The following window will be displayed:

Communications	FlexC	Reporting	PC Tools
Services	Ethernet	Modems	Serial ports
Portal			

GSM Modem settings [Backup]

Country: Ireland

SIM PIN: 1234

Allow Roaming:

Incoming Calls: Don't answer incoming calls
 Answer incoming calls

Line Monitoring: Disabled

Monitoring timer: 0 0 to 9999 Seconds

Modem Fault Time: 60 Time delay for system alert. 0 to 9999 Seconds

SMS Enable:

Automated SMS: 1 Hour

Automated SMS Number: 132345

Test Call Time: ---

GSM Chip Version: ---

GPRS Configuration

GPRS Access Point (APN):

GPRS Access Point User Name:

GPRS Access Point Password:

Dial Up Internet Configuration

Dial Up Internet Enable:

Phone Number:

Username:

Password:

Save Back Test SMS

2. Configure the following fields:

Modem settings

Country	Select the country that the SPC is installed in.
SIM PIN	Only for GSM. Enter the PIN for the SIM card installed in the GSM module.
Allow Roaming	Select to enable GSM roaming. Note: Changing this setting resets the modem. Note: Supported on GSM modems v3.08 or higher.
Incoming Calls	The modem can be programmed to answer calls based on the following

	<p>conditions:</p> <ul style="list-style-type: none"> ● Don't answer calls: Modem never answers calls. ● Answer after 'x' rings: Select the number of rings after which the modem answers the incoming call. ● Answers after the calling party calls the modem, hangs up after 1 ring burst only and then immediately re-calls the modem. The SPC system knows to automatically answer the call in this condition. ● Only answer when 'Engineer Access' is granted.
Prefix	Enter the number required to access a line. (e.g. if connected to a PBX)
Line Monitoring	<p>PSTN Modem: Enable this feature to monitor the voltage of the line connected to the modem.</p> <p>GSM Modem: Enable this feature to monitor the signal level from the GSM mast connected to the modem.</p> <p>The Fullset option only enables this feature while the system is Fullset.</p> <p>Note : EN 50131-9 Confirmation configuration In order for EN50131-9 Confirmation to operate correctly, line monitoring must be enabled. (refer to System Options [→ 222])</p>
Monitor Timer	Select the period (in seconds) for which the line voltage must be seen as being incorrect before the line is deemed by the SPC to be faulty.
Modem Fault Time	Time delay for a system alert (0 - 9999 seconds). Default 60 seconds.
SMS Enable	<p>Tick this checkbox to enable the SMS feature on the system.</p> <p>Note: The SMS operates using a standard protocol that is used in SMS telephones. Please note that some PSTN operators do not provide the service of SMS over PSTN. For SMS to operate over PSTN the following criteria is required:</p> <p>Caller ID needs to be enabled on the telephone line. Direct telephone line – not through PABX or other comms equipment. Please also note that most Service Providers only allow SMS to a telephone registered in the same country (this is due to billing issues).</p> <p>Note: SMS over PSTN is no longer supported. The functionality remains in the product for backward compatibility.</p>
SMS Server Number	Only for PSTN. This number automatically displays the default number for SMS for the country selected. Enter an appropriate phone number of the SMS service provider that is accessible in your location.
Automated SMS	Select the timing for automated SMS messages.
Automated SMS Number	Enter SMS number to receive automated SMS messages.
Test Call Time	Displays time of last SMS test call.
GSM Chip Version	<p>Displays the GSM WISMO version number.</p> <p>If no version number is available, "--" is displayed.</p>
GPRS Access Point (APN)	Only for GSM. Access Point Details must be provided by service provider.
GPRS Access Point User Name	Only for GSM. Access Point Details must be provided by service provider.
GPRS Access Point Password	Only for GSM. Access Point Details must be provided by service provider.

Click the **Test SMS** button to send a short text message for the purposes of testing the system.

Note: The SMS test is provided only for the purpose of ensuring the SMS feature is operating correctly. A short text message using alphabetic characters (A-Z) should be used to test this feature.

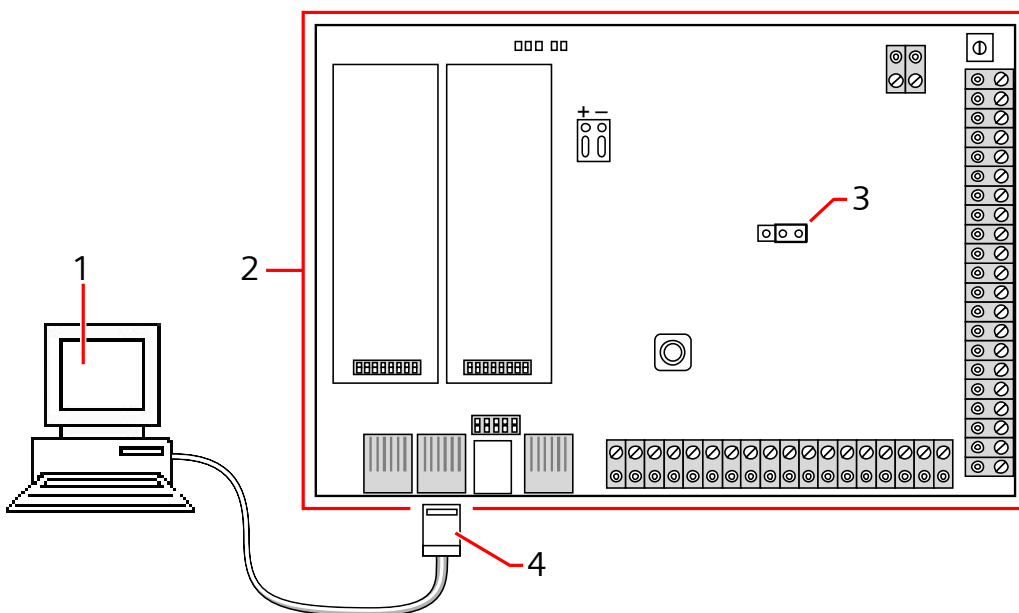



The SMS test is provided only for the purpose of ensuring the SMS feature is operating correctly. A short text message using alphabetic characters (A-Z) should be used to test this feature.

17.10.1.4 Serial ports

The SPC controller provides 2 serial ports (RS232) that offer the following functionality:

- **X10:** Serial port 1 is a dedicated interface that supports the X10 protocol. This protocol allows for use of the existing power cables of a building to transport control information to X10 devices providing the ability to trigger and monitor these devices via the SPC Controller programming interface.
- **Logging of Events:** The Serial port 2 interface provides the ability to connect to a serial port on a PC or a printer. With this connection, a terminal program can be configured to receive a log of System Events or Access Events from the SPC controller.
- **System Information:** Serial port 2 also provides an interface via a terminal program that allows for the execution of a set of commands to interrogate the controller for specific system information. This facility is available only as a tool for debug and information purposes and should only be used by experienced installers.



1	PC with serial port running hyperterminal
2	SPC controller
3	JP9 
4	RS232

To configure the serial ports:

- Select **Communications > Communications > Serial Ports**.
⇒ The following window will be displayed:

Communications		
Services	Ethernet	Modems
<p>Portal registration</p> <p>Enable <input checked="" type="checkbox"/> Check to enable portal registration</p> <p>Portal URL or IP Address <input type="text" value="87.192.253.140"/> URL or IP address of portal service</p> <p>Portal Port <input type="text" value="80"/> Port portal server is listening on</p> <p>WAN IP Address <input type="text" value="217.91.58.61"/> IP address of SPC from external network</p> <p>WAN Port <input type="text" value="443"/> Port address of SPC from external network</p> <p>Update interval <input type="text" value="2"/> Registration interval in minutes</p> <p>Registration ID: 135482801</p> <p>Last Registration:</p> <p><input type="button" value="Refresh"/> <input type="button" value="Save"/></p>		

The settings displayed will depend on the type of connection that the ports are used for. The settings are described in the following sections:

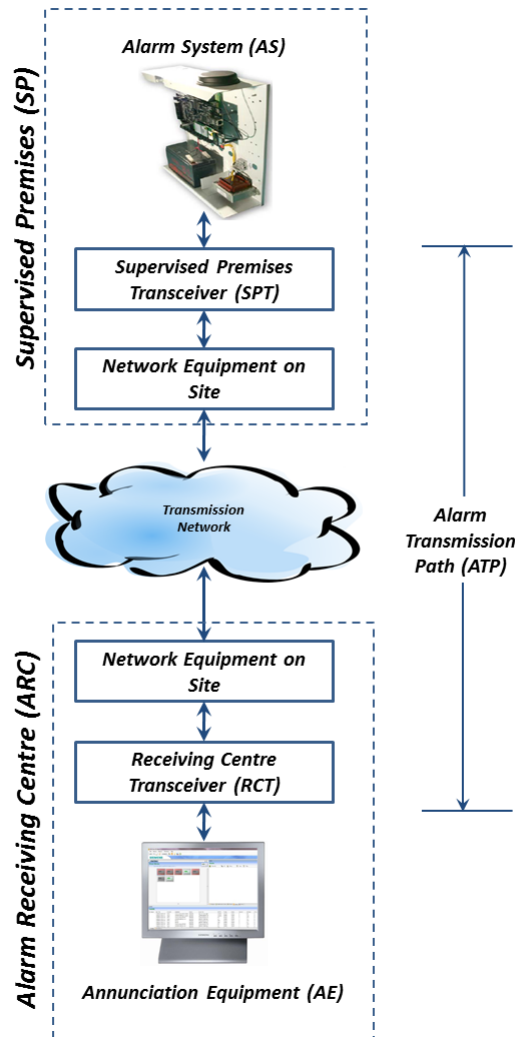
17.10.2 FlexC®

The SPC Flexible Secure Communications Protocol (FlexC) enables communications for an Internet Protocol (IP) based single or multiple path Alarm Transmission System (ATS). An ATS is a reliable communications link between a Supervised Premises Transceiver (SPT e.g. Ethernet integrated onto the SPC panel) and a Receiving Centre Transceiver (RCT e.g. SPC Com XT or the SPC Connect server, www.spconnect.com). A FlexC ATS consists of a primary Alarm Transmission Path (ATP) and up to nine backup Alarm Transmission Paths (ATPs). It enables:

- Two-way transfer of data between the SPT, for example the SPC panel over Ethernet, and the RCT, for example, the SPC Com XT server or the SPC Connect server, www.spconnect.com.
- Communication monitoring of a complete ATS and individual ATPs.

SPC intrusion panels support FlexC over IP with any of the following interfaces:

- Ethernet
- GSM modem with GPRS enabled
- PSTN modem



See also

- 📄 Quick Start ATP Configuration for EN50136 ATS [→ 274]
- 📄 Configuring Event Profiles [→ 286]
- 📄 Event Exception Definition [→ 288]
- 📄 Configuring Command Profiles [→ 290]
- 📄 FlexC Status [→ 179]
- 📄 Configuring an EN50136-1 ATS or Custom ATS [→ 276]

17.10.2.1 Operation Mode

The system uses the store-and-forward method when communicating events.

The SPC Alarm System sends events to SPC Com XT and requires an acknowledgment from SPC Com XT before the SPC Alarm System considers the event to have been successfully transmitted. SPC Com XT only acknowledges the event after it has successfully written the event to the SQL database. SPC Com XT then forwards the event to the SPC Com XT Client and Sur-Gard interfaces.

17.10.2.2 Quick Start ATP Configuration for EN50136 ATS

FlexC provides the following out of the box features that enable you to get FlexC up and running quickly:

- Quick start configuration screen for an EN50136 **Single Path ATS**, **Dual Path ATS** and **Dual Path Dual Server ATS**
 - Default Event Profile
 - Default Command Profile (this does not support audio video verification)
 - Default **FlexC Command User Name** (FlexC) and **Command Password** (FlexC) for controlling the panel from the RCT (e.g. SPC Com XT)
 - Auto Encryption with no password
1. To quickly configure a FlexC connection between a panel and an RCT (e.g. SPC Com XT), go to **Communications - FlexC - FlexC ATS**.
 2. Under **Add EN50136-1 ATS**, choose one of the following to display the **ATP Configuration** screen:
 - **Add Single Path ATS** - primary ATP only
 - **Add Dual Path ATS** - primary and backup ATPs
 - **Add Dual Path Dual Server ATS** - primary and backup ATPs, primary and backup servers

Communications		FlexC	Reporting	PC Tools
FlexC ATS		Event Profiles	Command Profile	FlexC Help
ATP Configuration - EN50136 ATS				
<i>Panel Identification</i>				
ATS Name	<input type="text" value="ATS 3"/>	The name of the ATS		
SPT Account Code	<input type="text" value="0"/>	The number that uniquely defines the panel to the RCT (1-99999999, 0 = Aut)		
<i>RCT Identification</i>				
RCT ID	<input type="text" value="1"/>	The unique ID of the RCT (e.g. RCT ID of SPC ComXT) (1-99999999)		
RCT URL or IP Address	<input type="text" value="0.0.0.0"/>	URL or IP address of the RCT (e.g. SPC ComXT)		
RCT TCP Port	<input type="text" value="52000"/>	The TCP Port of the RCT (e.g. The TCP Port that SPC ComXT is listening on)		
<i>Backup RCT Identification</i>				
RCT ID	<input type="text" value="1"/>	The unique ID of the RCT (e.g. RCT ID of SPC ComXT) (1-99999999)		
RCT URL or IP Address	<input type="text" value="0.0.0.0"/>	URL or IP address of the RCT (e.g. SPC ComXT)		
RCT TCP Port	<input type="text" value="52000"/>	The TCP Port of the RCT (e.g. The TCP Port that SPC ComXT is listening on)		
<i>ATP Interface</i>				
EN50136 ATS Category	<input type="text" value="Dual Path ATS: DP3"/>	Select the ATS Category as defined in the EN50136-1:2012 specification		
Primary Interface	<input type="text" value="Ethernet"/>	Interface used by Primary ATP for communication		
Backup Interface	<input type="text" value="Dial Up Internet: Modem 1"/>	Interface used by Backup ATP for communication		
<input type="button" value="Back"/>		<input type="button" value="Save"/>		

1. Complete the fields on the **ATP Configuration - EN50136 ATS** screen shown in the table below. At a minimum, you must complete the field **RCT URL or IP Address** to save. If you do not enter an **SPT Account Code**, you can commission the panel using the **ATS Registration ID** which is automatically generated when you save. The RCT operator must enter this **ATS Registration ID**, for example, in SPC Com XT.
2. Click **Save**. The **ATS Configuration** screen displays showing the **ATS Registration ID** and the configured primary ATP or primary and backup ATPs in the **Event Sequence Table**.
3. On the **ATS Configuration** screen, click **Save** to accept the default settings, for example, the **Default Event Profile**, the **Default Command Profile** (including the **FlexC Command User Name** and **FlexC Command Password**), and **Auto Encryption** with no password. To change the settings, see **Configuring an EN50136-1 ATS or Custom ATS** [→ 276].
4. Click **Back**. The ATS displays in the **Configured ATS** table.

Panel Identification

ATS Name	Enter the name of the ATS. If you do not enter a value, the ATS name defaults to ATS 1, ATS 2 etc.
SPT Account Code	The number that uniquely identifies the panel to the RCT. Enter 0 if you do not have the SPT Account Code. In this case, you can commission the panel using the ATS Registration ID . For an EN50136 ATS, the ATS Registration ID is automatically generated when you click Save . The RCT can send the SPT Account Code to the panel when it is available.
RCT Identification & Backup RCT Identification (Dual Path Dual Server Only)	
RCT ID	Enter the RCT ID that uniquely identifies the RCT (e.g. SPC Com XT) to the panel. This must match the value entered in the SPC Com XT Server Configuration Manager tool in the Server RCT ID field in the Server Details tab. See the <i>SPC Com XT Installation & Configuration Manual</i> .
RCT URL or IP Address	Enter the RCT URL or IP Address for the RCT server location (e.g. SPC Com XT server).
RCT TCP Port	Enter the TCP port for the RCT (e.g. SPC Com XT). This must be the same value entered for the field Server FlexC Port in the SPC Com XT Server Configuration Manager tool.
ATP Interface	
EN50136 ATS Category	Select the EN50136 ATS Category (SP1-SP6, DP1-DP4). For a description of categories, see ATS Category Timings [→ 362] .
Primary Interface	Select the Primary Interface to apply to the primary communications path from the following: <ul style="list-style-type: none"> ● Ethernet ● GPRS: Modem 1 ● GPRS: Modem 2 ● Dial Up Internet: Modem 1 ● Dial Up Internet: Modem 2
Backup Interface	For a Dual Path ATS , select the Backup Interface to use for the backup communications path from the following: <ul style="list-style-type: none"> ● Ethernet ● GPRS: Modem 1 ● GPRS: Modem 2 ● Dial Up Internet: Modem 1 ● Dial Up Internet: Modem 2

17.10.2.3 Configuring an EN50136-1 ATS or Custom ATS

An ATS comprises an alarm panel, network paths and an RCT (e.g. SPC Com XT). It combines one or multiple paths between an SPC panel and an RCT. You can add up to 10 ATPs to an ATS.

!	<p>NOTICE</p> <p>For an EN50136-1 ATS, the ATS set up sequence starts with configuring an ATP for an ATS. This provides you with a quick set up feature. See Quick Start ATP Configuration for EN50136 ATS [→ 274].</p>
----------	--

1. To configure an ATS, go to **Communications - FlexC - FlexC ATS**.
2. Choose from one of the following options:
 - **Add Single Path ATS**
 - **Add Dual Path ATS**
 - **Add Dual Path Dual Server ATS**
 - **Add Custom ATS**.
1. For an EN50136 ATS, you must configure the settings on the **ATP Configuration - EN50136** screen first. See Quick Start ATP Configuration for EN50136 ATS [→ 274].
2. The **ATS Configuration** screen displays. An EN50136-1 ATS will display a primary or primary and backup ATP in the **Event Sequence Table**.

1. Enter an **ATS Name** to identify the ATS. If you do not enter a value, the ATS name defaults to ATS 1, ATS 2 etc.
2. To add 1 primary and up to 9 backup ATPs to an ATS, click **Add ATP to FlexC RCT**, see Add ATP to FlexC RCT [→ 278] or click **Add ATP to Analog ARC**, see Add ATP to Analog ARC [→ 282].
3. Select an **Event Profile** from the dropdown menu. To customise how events are transmitted on an ATS, see Configuring Event Profiles [→ 286].
4. Select a **Command Profile** from the dropdown menu. To customise the commands enabled for an RCT to control a panel, see Configuring Command Profiles [→ 290].
5. Complete the **ATS Faults** fields as shown in the table below.
6. Click the **Edit Installation Details** button to complete the settings to identify the panel to the RCT operator. See Edit Installation Details [→ 284].

7. Click **Save** and **Back** to return to the **ATS Configuration** page. The new ATS displays in the **Configured ATS** table.
8. For multiple ATPs, you can use the up and down arrows in the **Event Sequence Table** to reorder the ATP sequence.

!	NOTICE
	The ATS Registration ID is automatically generated for an ATS. It uniquely identifies the panel to the RCT. If you do not know the SPT Account Code , you can commission the panel using this ATS Registration ID . The CMS operator must also enter this ATS Registration ID at the RCT (e.g. SPC Com XT. See the <i>SPC Com XT Installation & Configuration Manual</i>).

ATS Polling Timeout	This field is automatically calculated by adding the values of the Active Polling Timeout column in the Event Sequence Table, that is, for all ATPs in an ATS. You can manually overwrite this field. For example, CAT 2 [Modem] has an Active Polling Timeout of 24 hours 10 minutes (87000 seconds). To allow a shorter reaction time, enter a lower value.
ATS Event Timeout	The amount of time after an event has been raised and not successfully transmitted before the ATS gives up. Default: 300 seconds.
Generate FTC	Select whether the system generates a FTC on an ATS event timeout.
Re-queue Events	Select this to re-queue events after an ATS Timeout.
Re-queue Event Delay	Delay after an ATS Event Timeout before the re-queued event is attempted again. Default: 300 seconds.
Re-queue Event Duration	Amount of time that the event will be re-queued before the event is deleted. Default: 86400 seconds.

See also

 [ATS Category Timings \[→ 362\]](#)

17.10.2.2.1 Add ATP to FlexC RCT

Add ATP to FlexC RCT allows you to configure an ATP between the SPC panel and the RCT (e.g. SPC Com XT). You can configure up to 10 ATPs for each ATS.

1. Click the button **Add ATP to FlexC RCT**.

1. Complete the ATP fields described in the table below.
2. If required, click **Advanced ATP Settings**, for example, if you are using auto encryption you can optionally enter a password in the **Encryption Password** field. See Configure Advanced ATP Settings [→ 280].
3. Click **Save**.




WARNING

It is not recommended to change **Advanced ATP Settings**. Changes must only be made by expert users.

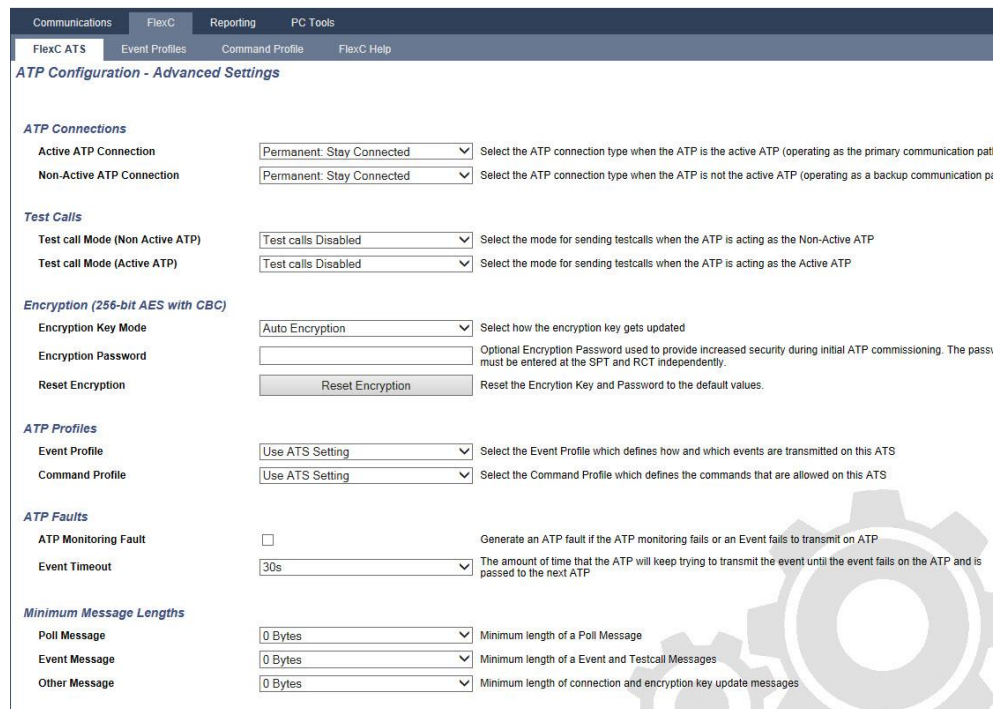
Panel Identification	
ATP Sequence No.	This field displays the sequence number of the ATP in the ATS configuration. Number 1 is primary, numbers 2 - 10 are backup.
ATP Unique ID	When you save an ATP, the system assigns a unique ID to an ATP. This is the unique ID of the ATP so it can be recognised by the RCT.
ATP Name	Enter a name for the ATP.
SPT Account Code	Enter a number to uniquely identify the panel to the RCT.
RCT Identification	
RCT ID	Enter the number that uniquely identifies the RCT (for example, SPC Com XT) to the panel. This must match the number entered in the field Server RCT ID in the SPC Com XT Server Configuration Manager tool.
RCT URL or IP Address	Enter the URL or IP address of the RCT (for example, SPC Com XT).
RCT TCP Port	Enter the TCP Port that the RCT (for example, SPC Com XT) listens on. The default is 52000. This must match the value in the field Server FlexC Port in the Server Configuration Manager tool. See the <i>SPC Com XT Installation & Configuration Manual</i> .
ATP Interface	
Communications Interface	From the dropdown list, select the interface this ATP uses for communication. <ul style="list-style-type: none"> ● Ethernet ● GPRS: Modem 1 ● GPRS: Modem 2

	<ul style="list-style-type: none"> ● Dial Up Internet: Modem 1 ● Dial Up Internet: Modem 2
ATP Category	Select the category to apply to this ATP. For information on ATP Categories, see ATP Category Timings [→ 363].
Advanced	
Advanced ATP Settings	It is not recommended to change advanced settings. Changes must only be made by expert users.

17.10.2.2.1.1 Configure Advanced ATP Settings

	<p>⚠ WARNING</p> <p>It is not recommended to change Advanced ATP Settings. Changes must only be made by expert users.</p>
---	--

1. Click the **Advanced ATP Settings** button.



The screenshot shows the 'ATP Configuration - Advanced Settings' page. It includes sections for:

- ATP Connections:** Active ATP Connection (Permanent: Stay Connected), Non-Active ATP Connection (Permanent: Stay Connected).
- Test Calls:** Test call Mode (Non Active ATP) (Test calls Disabled), Test call Mode (Active ATP) (Test calls Disabled).
- Encryption (256-bit AES with CBC):** Encryption Key Mode (Auto Encryption), Encryption Password (Optional Encryption Password), Reset Encryption (Reset Encryption button).
- ATP Profiles:** Event Profile (Use ATS Setting), Command Profile (Use ATS Setting).
- ATP Faults:** ATP Monitoring Fault (checkbox), Event Timeout (30s).
- Minimum Message Lengths:** Poll Message (0 Bytes), Event Message (0 Bytes), Other Message (0 Bytes).

1. Configure the fields described in the table below.
2. Click **Save**.

ATP Connections	
Active ATP Connection	Select the ATP connection type when the ATP is operating as the primary communication path. <ul style="list-style-type: none"> ● Permanent: Stay Connected ● Temporary: Hangup 1second ● Temporary: Hangup 20 second ● Temporary: Hangup 80 second ● Temporary: Hangup 3 minutes ● Temporary: Hangup 10 minutes ● Temporary: Hangup 30 minutes

Non-active ATP Connection	<p>Select the ATP connection type when the ATP is operating as a backup communication path.</p> <ul style="list-style-type: none"> ● Permanent: Stay Connected ● Temporary: Hangup 1second ● Temporary: Hangup 20 seconds ● Temporary: Hangup 80 seconds ● Temporary: Hangup 3 minutes ● Temporary: Hangup 10 minutes ● Temporary: Hangup 30 minutes
Test Calls	
Test Call Mode (Non Active ATP)	<p>Select the mode for sending test calls when the ATP is the non-active ATP.</p> <ul style="list-style-type: none"> ● Test calls Disabled ● Test call every 10 minutes ● Test call every 1 hour ● Test call every 4 hours ● Test call every 24 hours ● Test call every 48 hours ● Test call every 7 days ● Test call every 30 days
Test Call Mode (Active ATP)	<p>Select the mode for sending test calls when the ATP is the active ATP.</p> <ul style="list-style-type: none"> ● Test calls Disabled ● Test call every 10 minutes ● Test call every 1 hour ● Test call every 4 hours ● Test call every 24 hours ● Test call every 48 hours ● Test call every 7 days ● Test call every 30 days
Encryption (256-bit AES with CBC)	
Encryption Key Mode	<p>Select how the encryption gets updated.</p> <ul style="list-style-type: none"> ● Auto Encryption ● Auto Encryption with Updates ● Fixed Encryption <p>Note: Auto Encryption uses the default key and updates it once. Auto Encryption with Updates changes the encryption key every 50,000 messages or once per week, whichever comes first.</p>
Encryption Password	<p>Optional password used to provide increased security during initial ATP commissioning. The password must be entered at the SPT or RCT independently.</p>
Reset Encryption	<p>Reset the Encryption Key and password to the default values.</p>
ATP Profiles	
Event Profile	<p>Select the Event Profile which defines how and which events are transmitted on this ATS.</p> <ul style="list-style-type: none"> ● Use ATS Setting ● Default Event Profile ● All events

Command Profile	Select the Command Profile which defines the commands that are allowed on this ATS. <ul style="list-style-type: none"> ● Use ATS Setting ● Default Command Profile ● Custom Command Profile
ATP Faults	
ATP Monitoring Fault	Select to generate an ATP fault if the ATP monitoring fails or an event fails to transmit on the ATP.
Event Timeout	The amount of time that the ATP will keep trying to transmit the event until the event fails on the ATP and is passed to the next ATP. <ul style="list-style-type: none"> ● 30 seconds ● 60 seconds ● 90 seconds ● 2 minutes ● 3 minutes ● 5 minutes ● 10 minutes
Minimum Message Lengths	
Poll Message	Minimum length of a poll message. <ul style="list-style-type: none"> ● 0 Bytes ● 64 Bytes ● 128 Bytes ● 256 Bytes ● 512 Bytes
Event Message	Minimum length of an event and test call message. <ul style="list-style-type: none"> ● 0 Bytes ● 64 Bytes ● 128 Bytes ● 256 Bytes ● 512 Bytes
Other Message	Minimum length of connection and encryption key and update messages. <ul style="list-style-type: none"> ● 0 Bytes ● 64 Bytes ● 128 Bytes ● 256 Bytes ● 512 Bytes

17.10.2.2.2 Add ATP to Analog ARC

If a connection between the SPC panel and RCT (e.g. SPC Com XT) goes down, FlexC has the ability to switch to a backup ATP connection between the SPC panel and an Analog ARC. You can configure up to 10 ATPs for each ATS.

1. To configure an ATP between an SPC panel and an Analog ARC, click the button **Add ATP to Analog ARC**.
2. Complete the ATP fields described in the table below.
3. Click **Save**.

Panel Identification

ATP Sequence No.	This field displays the sequence number of the ATP in the ATS configuration. Number 1 is primary, numbers 2 - 10 are backup
ATP Unique ID	This ID uniquely identifies the ATP to the RCT
ATP Name	Enter a name for the ATP
SPT Account Code	Enter a number to uniquely identify the panel to the RCT (1 - 999999)
ARC Connection	
Number 1	Phone number 1
Number 2	Phone number 2
Modem Select	Select the modem to be used. <ul style="list-style-type: none"> ● Modem 1 ● Modem 2
Test Calls	
Test Call Mode (Non-active ATP)	Select the mode for sending test calls when the ATP is in non-active mode. Default: 24 hours. <ul style="list-style-type: none"> ● Test calls disabled ● Test call every 10 minutes ● Test call every 1 hour ● Test call every 24 hours ● Test call every 48 hours ● Test call every 7 days ● Test call every 30 days.
Test Call Mode (Active ATP)	Select the mode for sending test calls when the ATP is an active ATP. Default: 24 hours. <ul style="list-style-type: none"> ● Test calls disabled ● Test call every 10 minutes ● Test call every 1 hour ● Test call every 24 hours ● Test call every 48 hours ● Test call every 7 days ● Test call every 30 days.
Time of first test call	Time of first test call after reset or ATS initialization. <ul style="list-style-type: none"> ● Send Immediately (default) ● or ● Select a half hour interval between 00:00 and 23:30
Event Protocol	
Protocol	Protocol used in communication. <ul style="list-style-type: none"> ● SIA ● SIA Extended 1 ● SIA Extended 2 ● Contact ID
Event Profile	Select the Event Profile which defines how and which events are transmitted on this ATS. <ul style="list-style-type: none"> ● Use ATS Setting ● Default Event Profile ● Default Portal Event Profile ● All events ● Custom Event Profile
ATP Faults	
ATP Monitoring Fault	Select to generate an ATP fault if the ATP

	monitoring fails or an event fails to transmit on the ATP.
Event Timeout	<p>The amount of time that the ATP will keep trying to transmit the event until the event fails on the ATP and is passed to the next ATP. Default: 2 minutes.</p> <ul style="list-style-type: none"> ● 30 seconds ● 60 seconds ● 90 seconds ● 2 minutes ● 3 minutes ● 5 minutes ● 10 minutes

17.10.2.2.3 Edit Installation Details

The installation details are passed to the RCT to help the operator to identify the panel.

1. Click the **Edit Installation Button**.

The following installation details are passed to the RCT to help the Operator at the RCT to identify the panel.

ATS Installation ID	<input type="text" value="0"/>	The ID of the ATS Installation (1-999999999)
Company ID	<input type="text" value="0"/>	ID of the Company
Company Name	<input type="text"/>	Name of the Company
ATS Installation Address	<input type="text"/>	The address of the ATS Installation
GPS Coordinates	<input type="text"/>	The GPS Coordinates of the installation.
ATS Installer Name	<input type="text"/>	The name of the installer of the ATS
Installer Phone Number 1	<input type="text"/>	The phone number of the installer of the ATS
Installer Phone Number 2	<input type="text"/>	The phone number of the installer of the ATS
Notes	<input type="text"/>	Any additional information for the RCT

Back Save

1. Complete the fields in the table below.
2. Click **Save**.

ATS Installation ID	The ID of the ATS Installation (1 - 999999999).
Company ID	For future use.
Company Name	Name of the company.
ATS Installation Address	The address of the ATS installation.
GPS Coordinates	The GPS coordinates of the installation.
ATS Installer Name	The name of the installer of the ATS.
Installer Phone Number 1	The phone number of the installer of the ATS.
Installer Phone Number 2	The phone number of the installer of the ATS.

Notes	Any additional information for the RCT.
-------	---

17.10.2.4 Configuring an SPC Connect ATS

The **Add SPC Connect** ATS functionality opens a communication between the panel (SPT) and the **SPC Connect** server (RCT), www.spconnect.com. Using the generated SPC Connect ATS Registration ID, a panel user can register a user account and panel with the SPC Connect website to access their panel remotely.

1. To configure an SPC Connect ATS, go to **Communications - FlexC - FlexC ATS**.
 2. In the ATS Configuration screen, click **Add SPC Connect** to open a communication path with the SPC Connect server.
- ⇒ An SPC Connect ATS is added to the **Event Sequence Table** with the following attributes:
- SPC Connect ATS Registration ID
 - Default ATP over Ethernet. For information on ATP fields, see Add ATP to FlexC RCT [→ 278]
 - Default Events Profile for SPC Connect
 - Default Commands Profile for SPC Connect
 - Default RCT URL is www.spconnect.com
 - The SPT Account Code for the ATP is populated.
 - Make a note of the SPC Connect **ATS Registration ID** and provide this to the customer along with the *SPC Connect User Guide*.

The screenshot shows the 'ATS Configuration' screen. At the top, there are tabs for 'FlexC ATS', 'Event Profiles', 'Command Profile', and 'FlexC Help'. Below the tabs is a table titled 'Configured ATS' with the following data:

Edit	Delete	Export ATS	ID	ATS Name	ATS Registration ID	ATP Count	Event / Command Profiles	ATS Polling Timeout	ATS Event Timeout	Generate FIC
			1	SPC Connect	T578-G5R9-92XG-SP2G	1	- Default Events [SPC Connect] - Default Commands [SPC Connect]	86400	300	No
			2	ATS Dual Path	K6PG-K87Y-T866-385Y	2	- Default Events - Default Commands	360	300	Yes

Below the table, there are four sections for adding ATSs:

- Add SPC Connect:** Add an ATS to the SPC Connect Server. Button: Add SPC Connect
- Add EN50136-1 ATS:**
 - Add an EN50136-1:2012 single path ATS to the system. Button: Add Single Path ATS
 - Add an EN50136-1:2012 dual path ATS to the system. Button: Add Dual Path ATS
 - Add an EN50136-1:2012 dual path and dual Server ATS to the system. Button: Add Dual Path Dual Server ATS
- Add Custom ATS:** Add a custom ATS to the system. Up to 10 ATPs may be added to the ATS. Button: Add Custom ATS
- Import ATS:** Import an ATS to the system. Includes a 'Browse...' button and an 'Import ATS' button.

17.10.2.5 Exporting and Importing an ATS

ATS files have a .xml extension. You must create the ATS in the SPC browser and export it before you can import it to a system.

1. To export an ATS, go to **Communications - FlexC - FlexC ATS**.
2. In the **Configured ATS** table, locate the ATS to export and click the **Export ATS** button (green arrow).

Communications FlexC Reporting PC Tools

FlexC ATS Event Profiles Command Profile FlexC Help

ATS Configuration

Configured ATS

Edit	Delete	Export ATS	ID	ATS Name	ATS Registration ID	ATP Count	Event / Command Profiles	ATS Polling Timeout	ATS Event Timeout	Generate FTC
			2	ATS Dual Path	K6PG-K87Y-T866-385Y	2	- Default Events - Default Commands	360	300	Yes
			3	ATS Single Path	TTS9-7Y45-X2YP-SS56	1	- Default Events - Default Commands	180	300	Yes

Add SPC Connect
Add an ATS to the SPC Connect Server

Add EN50136-1 ATS
Add an EN50136-1:2012 single path ATS to the system.
Add an EN50136-1:2012 dual path ATS to the system.
Add an EN50136-1:2012 dual path and dual Server ATS to the system.

Add Custom ATS
Add a custom ATS to the system. Up to 10 ATPs may be added to the ATS.

Import ATS
Import an ATS to the system.

3. Save the file with the default filename **export_flexc.xml** or rename the file.
 4. To view the file, open in Notepad.
 5. To import an ATS into the system, go to **Communications - FlexC - FlexC ATS**.
 6. Scroll down to **Import ATS**.
 7. Click the **Browse** button and select an ATS to import (.xml file extension).
 8. Click **Import ATS**.
- ⇒ The ATS displays in the **Configured ATS** table with the next available ID.



When you export an ATS, the SPT Account Code changes to 0. This prevents an ATS being exported and then imported and replicating an existing ATS.

17.10.2.6 Configuring Event Profiles

The event profile defines which events are transmitted on an ATS, the reporting status for an event and event exceptions. Event exceptions allow you to remap default values for events to customised values. For more information, see Event Exception Definition [→ 288].



NOTICE

To see a list of all events, go to **Communications - FlexC - Event Profiles**. Click **Edit** (blue pencil) for an event profile. Scroll to the end of the screen and click **Show Complete Event Table**.

!	<p>NOTICE</p> <p>To quickly create a new event profile, go to Communications - FlexC - Event Profiles. In the Event Profiles table, select an event profile and click the edit button (blue pencil). Scroll to the bottom of the screen and click Replicate. You can now make the changes you require.</p>
----------	--

1. To configure FlexC event profiles step by step, go to **Communications - FlexC - Event Profiles**.
2. Click **Add**. The **Event Profiles** window displays.

1. Enter a **Name** to identify the event profile.
2. Select the event filter groups to report for this profile by ticking the **Report Event** checkboxes.
3. To prevent reporting of certain events or addresses within an event, select the event from the corresponding **Add Event Exception** dropdown list.
4. Click **Add** to view the **Event Exception Definition** screen. See Event Exception Definition [→ 288].
5. To apply an event profile to an area, select the area under **Area Filter**.
6. Click **Save** and **Back**. The new profile displays in the **Event Profiles** table.



You can view a list of all event exceptions for an event profile under **Event Exceptions** on the **Event Profiles** screen.



NOTICE

You cannot delete the **Default Event Profile**, the **Default Portal Event Profile** or an event profile that is assigned to an ATS. If you try to delete an event profile that is in use, you will get an error.

17.10.2.5.1 Event Exception Definition

Event exceptions allow you to change the following settings for a range of addresses within an event:

- Report Event
- SIA Code
- CID Code
- Event Address (e.g. Zone IDs, Area IDs, User IDs)

For example, in the Filter Group **Intruder Alarms** you could define an event exception for a range of Zone IDs in the Burglary Alarm (BA) event as follows:

- Do not report BA events for Zone ID 1 - 9
- Remap the SIA Code from BA to YZ
- Remap the CID from 130 / 1 to 230 / 1
- Remap the Zone ID 1 - 9 to Zone ID 101 - 109

Communications FlexC Reporting PC Tools

FlexC ATS Event Profiles Command Profile FlexC Help

Event Exception Definition

Configuration saved OK

Identification

Name: Burglarly Alarm (Name of the Event Exception)

Event ID: 1000 (Event ID of the event on the system)

Event Description: Burglary Alarm [Alarm Zone] (Description of the event)

Event Filter

Report Event: (Check if the event is normally reported)

Filter Exception Enable: (Check to enable the filter exception)

DISABLED="disabled"

if (1 ≤ Zone ID ≤ 9)
then Don't Report Event

Event Format

SIA Event Code: BA (SIA event code that is transmitted to represent the event)

Contact ID Event Code / Qualifier: 130 / 1 (Contact ID Event Code / Qualifier transmitted to represent the event)

Remap Exception Enable: (Check to enable the remap exception)

if (1 ≤ Zone ID ≤ 9)
then Remap SIA Event Code to YZ
and Remap Contact ID Event Code / Qualifier to 230 / 1
and Remap Event Address to 101 - 109

1. To configure an **Event Exception Definition**, complete the fields described in the table below.
2. Click **Save**.

- Click **Back** to return to the **Event Profiles** screen.
 - ⇒ The name of each exception displays in the **Event Exceptions** table at the bottom of the screen. The table shows the settings for the fields **Report Event**, **Filter Exception**, **Event Code (SIA/CID)** and **Remap Exception** for the event.

Area Filter

1: Area 1

Event Exceptions

Edit	Delete	Event Exception Name	Report Event	Filter Exception	Event Code (SIA / CID)	Remap Exception
<i>Event ID 1000 :Burglary Alarm [Alarm Zone]</i>						
		Burglary Alarm	Yes	Don't Report Event [1-9]	BA / 130	[1-9] → YZ/230 [101-109]

- Click the **Edit** icon to make changes or the **Delete** icon to remove an **Event Exception**.
- To apply the event profile to an area, select the area checkbox.
- Click **Save** to save the event profile.
- Click **Back** to view the profile in the **Event Profiles** table.

Identification	
Name	Enter the name of the Event Exception.
Event ID	Event ID of the event on the system. This is display only.
Event Description	Description of the event. This is display only.
Event Filter	
Report Event	Check to report the event. This overrides the reporting value set for the event Filter Group. For example, if the Filter Group Intruder Alarms is set to report, you can exclude the BA event or by disabling this setting.
Filter Exception Enable	Check to exclude a range of addresses, for example Zone IDs, from the Report Event field setting.
if (0 ≤ Zone ID ≤ 9999) then Report Event/Don't Report Event	Enter a range of addresses to exclude from the Report Event setting. For example, if you choose to report the event type BA, you may choose not to report <i>Zone ID 1 - 9</i> for that event. Alternatively, if you choose not to report the event type BA, you may choose to report <i>Zone ID 1- 9</i> for that event.
Event Format	
SIA Event Code	Default SIA event code that is transmitted to represent the event. This field is display only.
Contact ID Event Code / Qualifier	Default Contact ID Event Code / Qualifier transmitted to represent the event. This field is display only.
Remap Exception Enable	Check to remap the default SIA, CID code / Qualifier and Event Address to customised values, for example, to remap <i>Zone ID 1 - 9</i> to <i>Zone ID 101 - 109</i> . When enabled, the fields below display.
if (0 ≤ Zone ID ≤ 9999)	Enter the range of addresses to remap for an event, for example, if you want to remap <i>Zone ID</i>

	1 - 9 to Zone ID 101 - 109, enter 1 and 9. The quantity of addresses in the range must be equal to the quantity of addresses defined in the field Remap Event Address below.
then Remap SIA Event Code to BA	Remap the default SIA code to a customised SIA code.
and Remap Contact ID Event Code / Qualifier to	Remap the default CID Event Code / Qualifier to a customised CID Event Code / Qualifier.
and Remap Event Address to	Enter the new range of addresses, for example, if you are remapping Zone ID 1 - 9 to Zone ID 101 - 109, enter 101 and 109.

17.10.2.7 Configuring Command Profiles

The command profile defines the commands that are allowed on an ATS. This profile determines how a CMS can control a panel. The default command profile does not support video verification.

!	<p>NOTICE</p> <p>To quickly create a new command profile, go to Communications - FlexC - Command Profiles. In the Command Profiles table, select a command profile and click the edit button (blue pencil), Scroll to the bottom of the screen and click Replicate. You can now make the changes you require.</p>
----------	---

- To add a command profile step by step, go to **Communications - FlexC - Command Profiles**.

Edit	Delete	ID	Command Profile Name	Commands Enabled	Commands Logged
	-	1	Default Commands	49	40
	-	2	Default Commands [SPC Connect]	75	40
		3	Command Profile 3	38	40
		4	Command Profile 4	38	37

Add

- Click **Add**.

Communications	FlexC	Reporting	PC Tools
FlexC ATS	Event Profiles	Command Profile	FlexC Help

Command Profiles

Identification

Name Name of the Command Profile

Command Profile Authentication

Authentication Mode Mode used to authenticate the rights of the user using the Command Profile

Command User Name Name of the Command Profile user

Command Password Password of the Command Profile user

Live streaming

Live Streaming Mode Select Live Streaming privacy options

Command Filter

	Command Enable	Log Command
System Commands		
Get Panel Summary	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Set the System Time and Date	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Grant Engineer Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Grant Manufacturing Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1. Enter a **Name** to identify the command profile.
2. Select an **Authentication Mode** (Command User or Panel User, Command User Only, or Any Panel User) from the dropdown menu.

!	<p>NOTICE</p> <p>The default Command User Name provides an out of the box user that quickly and easily enables control of the panel from SPC Com XT. It enables a broad range of commands. For example, the default command user can set all areas or control all zones. For tighter control, for example to only allow setting of certain areas, you can set up a customised command profile with a defined set of rights. You cannot delete the Default Command Profile, the Default Portal Command Profile or a command profile that is assigned to an ATS.</p>
----------	--

3. Enter the name of the command profile user in the **Command User Name** field. This must match the **Authentication User Name** field in SPC Com XT.
4. Enter the password of the command profile user in the **Command Password** field. This must match the authentication **User PIN or Password** field in SPC Com XT.
5. Select the **Live Streaming Mode** (Disabled, Only after alarm event, Always available, System is fullset) to determine the streaming privacy options. **Always Available** generates the highest volume of data.
6. Under **Command Filter**, select the commands to enable. For a full list of commands, see FlexC Commands [→ 360].
7. Select the commands to log.
8. Click **Save**.
9. Click **Back** to view the command profile in the **Command Profiles** table.
10. To change a command profile, click the **Edit** button (pencil icon) next to a command profile.

17.10.3 Reporting

17.10.3.1 Alarm Reporting Centres (ARCs)

The SPC panel has the facility to communicate information to a remote receiving station when a specific alarm event on the panel has occurred.

These Alarm Reporting Centres must be configured on the panel to allow this remote communication to operate.

17.10.3.1.1 Adding / Editing an ARC using SIA or CID

▷ A PSTN or GSM modem is installed and functioning correctly.

1. Select **Communications > Reporting > Analog ARC**.

⇒ The following window will be displayed:

Communications		FlexC	Reporting	PC Tools					
Analog ARC		EDP	CEI-ABI						
ID	Account	Description	Last Dial	Last Dial Status	Test Calls	Test Call Time	Log	Edit	Delete
1	1	ABC	03/07/2014 17:59:31	Modem Fault	Modem 1	---
2	2	CMS	07/07/2014 15:24:09	Modem Fault	Modem 1	---
3	2	XYZ	03/07/2014 17:59:31	Modem Fault	Modem 1	---

Refresh Add

2. Click on the **Modem1/2** button to make a test call to the ARC from the either modem 1 or modem 2.

3. Click on the **Log** button to receive a log file. A window with the logs from all automatic and manual test calls will be displayed.

4. To add or edit an ARC, click **Add**. – OR -
Click **Edit**.

⇒ The following window will be displayed.

5. Configure the fields as described in the table below.

Communications	FlexC	Reporting	PC Tools
Analog ARC EDP CEI-ABI			
Add Alarm Receiving Center			
Description	<input type="text"/>	Identification of Alarm Receiving Center	
Account	<input type="text" value="1"/>	Account number	
Protocol	<input type="text" value="SIA"/>	Protocol used in communication	
Priority	<input type="text" value="Primary"/>	Priority of ARC	
Number 1	<input type="text"/>	Phone number 1	
Number 2	<input type="text"/>	Phone number 2	
Dial Attempts	<input type="text" value="8"/>	Number of dial attempts to connect to receiver	
Dial Delay	<input type="text" value="0"/>	Number of seconds to delay between failed dial attempts. (0 - 999)	
Test Calls	<input type="text" value="Disabled"/>	Interval between automatic test calls	
	<input type="checkbox"/>	Check if all modems should be tested	
<input type="button" value="Add"/>			

Description	Enter a description of the remote Alarm Receiving Centre.
Account	Enter your account number. This information should be available from the receiving station and is used to identify you each time you make a call to the ARC. For a Contact ID account, a maximum of 6 characters is allowed.
Protocol	Enter the communication protocol that you intend to use (SIA, SIA Extended, Contact ID, Fast Format). Note: SPC supports the extended SIA protocol. Select this protocol to support additional textual descriptions of the SIA events being sent to the Alarm Receiving Station.
Priority	Select the priority for the ARC in terms of primary or back-up reporting.
Number 1	Enter the first number to be dialled to contact the ARC. This system will always attempt to contact the ARC on this number before attempting another number.
Number 2	Enter the second number to be dialled to contact the ARC. The system will only attempt to contact the ARC on this number if the first contact number did not successfully establish a call.
Dial Attempts	Enter the number of times that the system will attempt to make a call to the receiver. (Default is 8)
Dial Delay	Number of seconds to delay between failed dial attempts (0 - 999).
Dial Interval	Enter the number of seconds to delay between failed dial attempts. (0 - 999)
Test Calls	Enable the test call by choosing a time interval. This will send out an automatic test call from modem 1 to the primary ARC.
Test All	Check this box if you want to initiate also an automatic test call from modem 2 to the backup ARC.

- Click on the **Add** button to enter those details on the system.
 - ⇒ A list of the configured ARC accounts will be displayed on the browser screen along with the account information, description, protocol, dial-up status and time and date of the last call to the ARC.

17.10.3.1.2 Editing an ARC filter using SIA or CID

To configure the events on the SPC that will trigger the call to the ARC:

1. Select **Communications - Reporting - Analog ARC - Edit - Filter..**

⇒ The following window will be displayed:

Event Type	Checked	Description
Alarms	<input checked="" type="checkbox"/>	Alarm activation
Alarm Restores	<input checked="" type="checkbox"/>	Reported alarms being restored
Confirmed alarms	<input checked="" type="checkbox"/>	Alarms confirmed by multiple zones
Alarm Abort	<input type="checkbox"/>	Report Alarm Abort event if valid PIN is entered on keypad after alarm report
Faults	<input checked="" type="checkbox"/>	Fault or Tamper activations
Fault restore	<input checked="" type="checkbox"/>	Fault or Tamper restores
Setting	<input type="checkbox"/>	Setting and Unsetting
Early / Late	<input type="checkbox"/>	Report if Setting/Unsetting is not according to schedule
Inhibits	<input type="checkbox"/>	Inhibit and Isolate
Door events	<input type="checkbox"/>	Access control door events
Other	<input type="checkbox"/>	All other types of events
Network	<input type="checkbox"/>	Report IP Network Polling Up/Down events

Area	Checked	Area	Checked	Area	Checked
1: Marketing	<input checked="" type="checkbox"/>	3: Finance	<input checked="" type="checkbox"/>	5: Meeting Room	<input checked="" type="checkbox"/>
2: Reception	<input checked="" type="checkbox"/>	4: Cafeteria	<input checked="" type="checkbox"/>	6: Finance	<input checked="" type="checkbox"/>

2. Configure the following fields:

Check any of the following boxes if you want to initiate a remote call to the ARC to notify it of the particular event.

Alarms	Alarms are activated.
Alarm Restores	System alarms are restored.
Confirmed Alarms	Alarms confirmed by multiple zones
Alarm Abort	Alarm Abort events. Alarms are aborted after a valid user code is entered via the keypad after a confirmed or unconfirmed alarm,
Faults	Faults and tampers are activated.
Fault Restores	Fault or tamper alarms are restored.
Settings	System is Set and Unset.
Early/Late	Unscheduled setting and unsetting of the system.
Inhibits	Inhibit and isolate operations are performed on the system.
Door Events	Door events are activated. Only works with SIA protocol.

Other	All other types of events are detected on the system.
Network	Report IP Network Polling Up/Down events.
Areas	Select specific areas to which above events apply.



By adding a separate Alarm Receiving Centre (ARC) for each area defined on the system and programming each area to report it's own separate ARC receiver, the system can approximate a multi-tenanted system in that a high degree of autonomy is assigned to each area.

17.10.3.1.3 Editing an ARC Filter using Fast Format

To configure the events on the SPC that will trigger the call to the ARC when **Fast Format** is the selected protocol:

- Select **Communications - Reporting - Analog ARC - Edit - Filter**.
- 1. A list of the eight channels is displayed along with the alarm conditions that can be programmed for each channel. Select the alarm conditions for each channel as required. For a description of each, see Outputs types and output ports [→ 198].
- 2. From the **Scope** dropdown menu, select **System** or a specific area to apply your selected settings.
- 3. Click the **Test** button located next to the first channel to test the alarm activation.
 - ⇒ The light bulb icon is switched on.
- 4. Wait approximately five seconds and click the **Test** button again for the same channel. This sends a channel restore to the ARC and the light bulb icon is switched off.
- 5. Continue to test the other channels.

17.10.3.2 EDP Setup

IP

The system has the facility to communicate information to the SPC Com server remotely using Vanderbilt's own protocol, the EDP (**Enhanced Datagram Protocol**). By correctly configuring an EDP receiver on the system, it can be programmed to automatically make data calls to the SPC Com server in a remote location whenever events such as alarm activations, tampers, or arming/disarming occur. The engineer can configure the system to make calls to the remote server via the following routes:

- **PSTN** (PSTN modem required)
- **GSM** (GSM modem required)
- **Internet** (Ethernet interface)

If using the PSTN network, ensure the PSTN modem is properly installed and functioning correctly and that a functioning PSTN line is connected to the A, B terminals on the PSTN modem.

If using the GSM network, ensure the GSM module is properly installed and functioning correctly. An IP connection can be made across the internet to a server with a fixed public IP address.

If an IP connection is required, ensure the Ethernet interface is correctly configured (see page [→ 159]) and that internet access is enabled at the router.

17.10.3.2.1 Adding an EDP Receiver

1. Select **Communications > Reporting > EDP**.

⇒ The following window will be displayed:

Communications FlexC Reporting PC Tools							
Analog ARC EDP CEI-ABI							
ID	Receiver	Description	Network Status	Dial-up status	Last Dial	Test	Edit
1	1	EDP	Fault	N/A	None

Refresh Settings Add



Max. 8 receivers can be added to the SPC system.

2. Click on the **Add** button.

⇒ The following window will be displayed.

Communications FlexC Reporting PC Tools		
Analog ARC EDP CEI-ABI		
Add receiver		
Description	<input type="text" value="EDP"/>	Description of receiver.
Receiver Id	<input type="text" value="3"/>	Unique identification number of EDP receiver used by this panel.
Save Back		

3. See table below for further information.

Description	Enter a text description of the receiver.
Receiver ID	Enter a unique number which will be used by the EDP to identify the receiver.

See also

[Editing EDP Receiver Settings \[→ 296\]](#)

17.10.3.2.2 Editing EDP Receiver Settings

1. Select **Communications > Reporting > EDP > Edit**.

⇒ The following window will be displayed.

2. Configure the fields as described in the table below.

Communications FlexC Reporting PC Tools
Analog ARC EDP CEI-ABI

Edit Receiver

Description Description of receiver.
Receiver Id Unique identification number of EDP receiver used by this panel. (1 - 999997)
Protocol version Select version of EDP protocol to use with this receiver

Security

Commands Enable Check if incoming commands are allowed from this receiver.
Change user PINs Check if changing user PINs is allowed from this EDP receiver.
Virtual Keypad Check to allow virtual keypad access from this EDP receiver.
Live streaming Select Live Streaming privacy options
Encryption Enabled Check if data to and from this receiver is encrypted.

Network

Network Enable Check if events can be reported through Network

Dial-up

Dial-up Enable Check if events can be reported through dial-up

Events

Primary Receiver Check if primary, clear for backup
Re-queue Events Check if events that fail to report are to be requeued for transmission.
Verification Check if Audio/Video verification should be sent to this receiver.
Event Filter Configure which events are reported to this receiver

Description	Edit the name of the EDP receiver. Maximum 16 characters.
Receiver ID	Edit the EDP receiver ID. Range is 1 to 999997 (999998 and 999999 are reserved for special purposes)
Protocol Version	Select the EDP protocol version to use with this EDP receiver. Options are Version 1 or Version 2. Version 2 is recommended if supported by the receiver, as it is a more secure protocol.
VdS 2471 Compatible	(Vds standard only) If this option is selected then the EDP receiver will enforce the following settings for that receiver: <ul style="list-style-type: none"> ● 8s polling interval ● TCP protocol enforced ● TCP retries will fail before 10s (9s approx) ● EDP event retries are set to 1 independent of the global "Retry Count" setting in "EDP Settings" ● FTC will be generated within 20s of network failure.

Security

Commands Enable	Check this box to allow commands to be accepted from the receiver.
Change User PINs	Check this box to allow user PINs to be changed from a remote location. This feature is applicable only if commands are enabled from the receiver.
Encryption Enable	Check this box to enable encryption on data to and from the receiver.
Encryption Key	Enter a hexadecimal key (max. 32 digits) that will be used to encrypt the data. Note: The same key will need to be used at the receiver.
Virtual Keypad	Enables access to the panel with a virtual keypad i.e. a PC software module that looks and behaves like an SPC keypad. It is available with the SPC Com client.
Live Streaming/Streaming Mode	Specifies when live streaming of audio and video is available. Options are Never, Always or Only after an alarm event. Default is 'Only after an alarm event'. Note: This setting has obvious privacy implications and therefore should be enabled only where appropriate and subject to local laws and regulations.
Network (Applies to the Ethernet connection only)	
Network Enable	Check this box to allow events to be reported through the network.
Network Protocol	Select the type of network protocol for the receiver. Options are UDP and TCP. TCP is recommended if supported by the receiver.
Receiver ID Address	Enter the IP address of the receiver.
Receiver IP Port	Enter the IP port that the EDP receiver is listening on.
Always Connected	If enabled the panel will keep a permanent connection to the receiver. If disabled, the panel will only connect to the receiver after an alarm event.
Panel Master	If enabled the panel is master of polling messages. Only applicable to UDP connections.
Polling Interval	Enter the number of seconds between polls.
Polling Trigger	Enter the number of missing polls before a network connection fail is registered. Only applicable to UDP connections.
Generate a Network Fault	If polling fails, a network fault alert is generated.
Dial-up (Applies to the GPRS modem connection only)	
Dial-up Enable	Check this box to report events through a dial-up connection.
Call type	Select type of call to use when dial up is enabled. Select GPRS.
GPRS protocol	Select the transport layer protocol used over the GPRS connection. Options are UDP or TCP. Only applicable if Call Type is GPRS.
GPRS address	Enter the IP address of EDP receiver for GPRS connections. Only applicable if Call Type is GPRS.
GPRS port	Enter the port that the EDP receiver is listening on for GPRS connections Options are UDP or TCP. Only applicable if Call Type is GPRS. Default is 50000.
GPRS Hangup Timeout	Enter the time in seconds after which the GPRS call will hang up. (0 = stay connected until IP connection is up)
GPRS Autoconnect	Check this box to automatically trigger a GPRS call to the server if an IP network fault occurs.
Dial-up on Net Fault	Check this box to report network faults on a dial-up test call.
Dial-up Interval 1*	Enter the number of minutes between dial-up test calls when network link is up.

Dial-up Interval 2*	Enter number of minutes between dial-up test calls when network link is down.
Network Address*	Enter the IP address of the receiver. This is only required if the connection to the EDP receiver is being made over the Ethernet interface. If using one of the on-board modems then leave this field blank.
Phone Number*	Enter the first phone number that the modem(s) will dial to contact the receiver.
Phone Number 2*	Enter a second phone number that the modem(s) will dial in the event that the first number dialled did not result in a call being successfully established.
Events	
Primary Receiver	Check this box to indicate that this is the primary receiver. If unchecked, this is a backup receiver.
Re-queue Events	Check this box if events that failed to report are to be re-queued for transmission
Verification	Check this box if Audio/Video verification is to be sent to this receiver.
Event Filter	Click this button to edit the filter events that will trigger an EDP call. Refer to Editing Events Filter Settings [→ 299].



* EDP dial-up over PSTN is not supported in this release.

See also

[Configuring SMS \[→ 190\]](#)

17.10.3.2.3 Editing Event Filter Settings

1. Select **Communications > Reporting > EDP > Edit > Filter**
⇒ The following window will be displayed.
2. Configure the fields as described in the table below.

Communications		FlexC	Reporting	PC Tools
Analog ARC		EDP	CEI-ABI	
Event Filter				
Alarms	<input checked="" type="checkbox"/>	Alarm activation		
Alarm Restores	<input checked="" type="checkbox"/>	Reported alarms being restored		
Confirmed alarms	<input checked="" type="checkbox"/>	Alarms confirmed by multiple zones		
Alarm Abort	<input type="checkbox"/>	Report Alarm Abort event if valid PIN is entered on keypad after alarm report		
Faults	<input checked="" type="checkbox"/>	Fault or Tamper activations		
Fault restore	<input checked="" type="checkbox"/>	Fault or Tamper restores		
Zone state	<input type="checkbox"/>	Report all state changes of inputs		
Setting	<input type="checkbox"/>	Setting and Unsetting		
Early / Late	<input type="checkbox"/>	Report if Setting/Unsetting is not according to schedule		
Inhibits	<input type="checkbox"/>	Inhibit and Isolate		
Door events	<input type="checkbox"/>	Access control door events		
Other	<input type="checkbox"/>	All other types of events		
Other (Non Standard)	<input type="checkbox"/>	Non Standard SIA codes		
Network	<input type="checkbox"/>	Report IP Network Polling Up/Down events		
Areas	<input checked="" type="checkbox"/> 1: Marketing <input checked="" type="checkbox"/> 2: Reception	<input checked="" type="checkbox"/> 3: Finance <input checked="" type="checkbox"/> 4: Cafeteria	<input checked="" type="checkbox"/> 5: Meeting Room <input checked="" type="checkbox"/> 6: Finance	
<input type="button" value="Save"/> <input type="button" value="Back"/>				

Check any of the following boxes if you want to initiate a remote call to an EDP Receiver to notify it of the particular event.

Alarms	Alarms are activated.
Alarm Restores	System alarms are restored.
Confirmed Alarms	Alarms confirmed by multiple zones
Alarm Abort	Alarm Abort events. Alarms are aborted after a valid user code is entered via the keypad after a confirmed or unconfirmed alarm,
Faults	Faults and tampers are activated.
Fault Restores	Fault or tamper alarms are restored.
Zone state	Report all zone input state changes.
Settings	System is Set and Unset.
Early/Late	Unscheduled setting and unsetting of the system.
Inhibits	Inhibit and isolate operations are performed on the system.
Door Events	Door events are activated. Only works with SIA protocol.
Other	All other types of events are detected on the system.
Other (Non standard)	Non supported SIA codes used with SPC COM XT including Camera Online/Offline events.

Network	Report IP Network Polling Up/Down events.
Areas	Select specific areas to which above events apply.

17.10.3.2.4 Editing EDP settings

1. Select **Communications > Reporting > EDP > Settings**.
⇒ The following window will be displayed.
2. Configure the fields as described in the table below.

EDP Settings (Panel)

Enable	<input type="checkbox"/>	Check this to enable EDP.
EDP Panel ID	<input type="text" value="1000"/>	Unique identification number used by EDP receiver for this panel. (1 - 999997)
Panel Port	<input type="text" value="50000"/>	IP port for receiving IP packets (Default is 50000). (1 - 65535)
Packet Size Limit	<input type="text" value="1440"/>	Maximum number of bytes in an EDP packet for transmission. (500 - 1440)
Event Timeout	<input type="text" value="10"/>	Number of seconds between retransmissions of unacknowledged events. (1 - 199)
Retry Count	<input type="text" value="10"/>	Max number of event retransmissions. (0 - 199)
Dial Attempts	<input type="text" value="10"/>	Max number of failed dial attempts before Modem lockout. (1 - 199)
Dial Delay	<input type="text" value="30"/>	Seconds to wait before redialling after a failed dial attempt. (1 - 199)
Dial Lockout	<input type="text" value="480"/>	Seconds to suspend dialling when max number of failed dial attempts are reached (0 = don't suspend dialling). (0 - 999999)

Event Logging Options

Comms Status	<input type="checkbox"/>	Log all changes to communication availability.
EDP Commands	<input type="checkbox"/>	Log all commands executed through EDP.
A/V Events	<input type="checkbox"/>	Log when Audio/Video verification events are sent to receiver.
A/V Streaming	<input type="checkbox"/>	Log when Audio/Video live streaming begins.
Keypad Use	<input type="checkbox"/>	Log when remote keypad is activated.

Save Back

Enable	Tick this checkbox to enable EDP operation on the system.
EDP Panel ID	Enter a numeric identifier that is used by the EDP Receiver to identify the panel uniquely.
Panel Port	Select the IP port for receiving IP packets. Default is 50000.
Packet Size Limit	Enter the maximum number of bytes in an EDP packet for transmission.
Event timeout	Enter the timeout period (in seconds) between retransmissions of unacknowledged events.
Retry Count	Enter the maximum number or event retransmissions allowed by the system.
Dial Attempts	Enter the maximum number of failed dial attempts accepted by the system before the modem is locked out (prevented from making further attempts to dial). The lockout period is defined in the option Dial Lockout.

Dial Delay	Enter the time period (in seconds) that the system will wait before redialling after a dial attempt has failed.
Dial Lockout	Enter the time period (in seconds) that the system will suspend dialling when the maximum number of failed dial attempts is reached. Enter a value of '0' to continually attempt dialling.

Event Logging Options

Comms Status	Log all communication availability.
EDP Commands	Log all commands executed through EDP.
A/V Events	Log when Audio/Video verification events are sent to Receiver.
A/V Streaming	Log when Audio/Video live streaming begins.
Keypad Use	Log when remote keypad is activated.

17.10.4 PC Tools

17.10.4.1 SPC Pro / SPC Safe

1. Select **Communications > PC Tools > SPC Pro/SPC Safe**.
2. Configure the fields as described in the table below.

Enable	Tick this box to enable SPC Pro to connect to the panel.
Engineer Access	Tick this box if engineer access must be granted to allow SPC Pro to connect to the panel.
Password	Enter the password for SPC Pro connection. The password is checked by the panel every time SPC Pro attempts to connect to it. If the password programmed in this field matches the password programmed on the panel, then the connection will be allowed (default:).
Enable IP	Tick this box to enable a connection to the panel using Internet Protocol (IP).
IP Port	Select the IP port that SPC Pro will use to connect to the panel.

SPC Safe

For further information about configuration of the SPC Safe please refer to the *SPCS410 Installation & Configuration Manual*.

1. Click the **Enable SPC Safe** button.
2. Configure the fields as described in the table below.

Communications FlexC® Reporting **PC Tools**

SPC Pro/SPC Safe SPC Manager Remote Maintenance

SPC Pro/SPC Safe

General Settings

- Enable Access** Check to allow SPC Pro/SPC Safe to connect to panel.
- Engineer Access** Check if engineer access must be granted for SPC Pro/SPC Safe to connect
- Password** Password used by SPC Pro/SPC Safe.

Incoming connections settings (Panel is receiving)

- Enable IP (*)** Check to allow SPC Pro/SPC Safe to connect through IP.
- Panel IP Port (*)** TCP port panel listens to incoming connections from SPC Pro/SPC Safe.

(*) Note: this also affects Remote Maintenance.

Enable	Tick this box to enable Pro to connect to the panel.
Engineer Access	Tick this box if engineer access must be granted to allow Pro to connect to the panel.
Password	Enter the password for the Pro connection. The password is checked by the panel every time the Pro attempts to connect to it. If the password programmed in this field matches the password programmed on the panel, then the connection will be allowed (default:).
Installation ID	Enter the numeric identification of this installation (can also be set in System Identification page).
Enable Reporting	Check to allow the panel to contact the server after its configuration has been changed.
Reporting Timer	Enter the minutes how long after the last configuration change the panel should contact the server to report its configuration (min: 1, max.: 120).
Enable IP	Tick this box to enable a connection to the panel using Internet Protocol (IP).
TCP/IP Port	Enter the IP port that SPC Safe will use to connect to the panel (the IP port of the panel).
Server address	Enter the Hostname, URL or IP address of the SPC Safe server (e.g the IP address of your PC).
Server TCP/IP Port	Enter theTCP port of the SPC server (e.g .the IP port of your PC).

17.10.4.2 SPC Manager

The SPC manager mode setting determines the number of digits for user PINs and therefore the number of available PINs on a global system controlled by SPC Manager.

- Mode41: 4-digit PIN enables 1,000 global users
- Mode51: 5-digit PIN enables 10,000 global users
- Mode61: 6-digit PIN enables 100,000 global users

Mode71: 7-digit PIN enables 1000,000 global users

Mode81: 8-digit PIN enables 10,000,000 global users

When you set an SPC Manager mode, additional zeros are added to the front of existing 4 or 5 digits user PINs which modify the PIN for global use. For example, if **Mode71: 7-PIN Digit** is selected, 3 zeros are added to existing 4 digit PINs - 2222 will become 0002222.

To set the SPC Manager Mode:

1. Select **Communications > PC Tools > SPC Manager**.

2. Select the SPC Manager global user mode from the drop down list.
3. Click on the **Save** button.
 - ⇒ The mode cannot be saved if a conflict exists between a local existing user PIN and another user PIN on the global system. An 'Invalid PIN' error is displayed.
4. Click on the appropriate button to delete the PIN and save the new mode or change the PIN to the randomly generated new PIN displayed and then save the new mode.



NOTICE

SPC Manager modes cannot be changed if global users exist on the system.

17.10.4.3 Remote Maintenance

For further information please refer to the Remote Maintenance Configuration Manual.

17.10.4.3.1 Remote Maintenance Report

A Remote Maintenance Report can be obtained directly by SPC Pro from the panel.

- ▷ SPC Pro must be online with the panel.
- ▷ **Remote Maintenance** must be enabled.

1. Click on the **Advanced** menu .
2. Select the **Get Service Report from Panel** menu option.

For further details on Remote Maintenance, refer to the SPC Remote Maintenance manual.

17.11 File Operations

To perform operations on the panel files and configuration:

- **Select File.**
⇒ The following tabs are displayed:

Upgrade	Options for upgrading the controller and peripheral firmware, and languages on the panel. See File Upgrade Operations [→ 305].
File Manager	Options for managing the system configuration file and uploading and downloading users data to and from the panel. See File Manager Operations [→ 310].
Audio	Upload an audio file to the SPC. The file must be created by the SPC Pro Audio Manager. Click Browse and click Upload to add the audio file to the SPC. After upload, click the Test button to validate the audio file.
Fast Programmer	Fast Programmer File Operations. See Using the Fast Programmer [→ 311].
Default	Restores the SPC system to factory defaults. NOTICE! The IP address is maintained for connecting to the web interface after a factory default from the web page
Reset	Restarts the panel.
Policy Text	This tab summarises the configuration for your SPC product settings based on selected Region, Grade and Type .

17.11.1 File Upgrade Operations

To upgrade firmware and languages on the system:

- **Select File > Upgrade.**
⇒ The following page is displayed:

See also

- 📖 Options [→ 222]
- 📖 Using the Fast Programmer [→ 311]


17.11.1.1 Upgrading Firmware

	NOTICE
	Manufacturer Access is required for firmware upgrade operations and when enabled, is available for the completion of both controller and peripheral firmware upgrades. See System Options [→ 222].

Firmware for SPC is contained in two separate files:

- **Controller Firmware File**
Contains the firmware for the controller's CPUs only. Filename has the extension *.fw.
- **Peripheral Firmware File**
Contains the firmware for the X-BUS nodes, plus PSTN and GSM modems. Filename has the extension *.pfw.

The two files are upgraded separately.

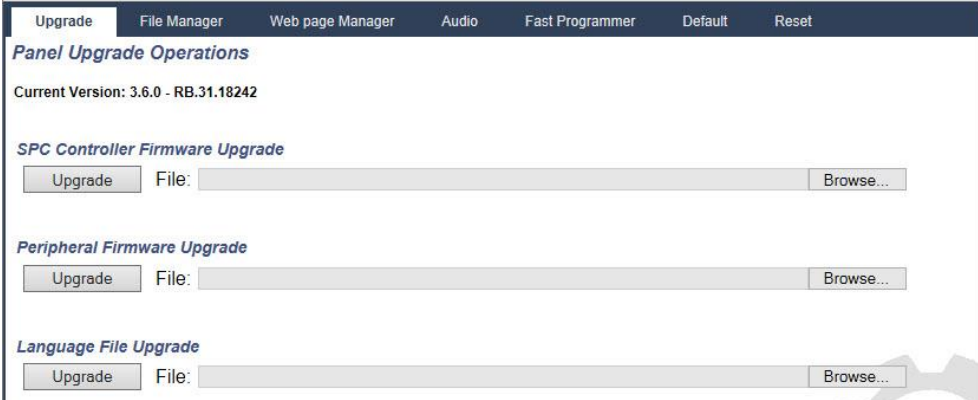
	<p>NOTICE</p> <p>It is recommended that all peripheral firmware is upgraded after a new controller firmware upgrade.</p>
---	---

Note: Firmware can also be upgraded using the keypad, SPC Pro and the Fast Programmer.


Controller Firmware

To upgrade controller firmware on the system:

1. Select the **Panel Upgrade Operations** option from the **File** page.
⇒ The following page is displayed:



2. Select the firmware file to upgrade by clicking the **Browse** button for the appropriate option, selecting the required firmware file and then clicking on the appropriate **Upgrade** button.
⇒ A confirmation screen is displayed.
3. Click on the **Confirm** button to confirm the upgrade to the new version of the controller firmware.
⇒ When the controller firmware is upgraded, the system will display a message to indicate that the system is resetting. You must login to the system again to continue operation.

	<p>WARNING</p> <p>If you downgrade the controller firmware (i.e. install an older version of firmware), the system defaults all current configuration settings. Also, when downgrading firmware, it is important to downgrade the corresponding peripheral firmware otherwise zones may appear disconnected, opened or closed.</p>
---	---



WARNING

If upgrading from a firmware version prior to version 3.3, please note the following:

- The Engineer web password, if configured, is deleted and must be reentered after upgrade.
- All existing users will be assigned to new user profiles corresponding to their previous user access levels. If max. number of user profiles is exceeded, no profile is assigned (see User Profiles [→ 186]). Please review all user configuration after a firmware upgrade.
- The default Engineer ID is changed from 513 to 9999.

Peripheral Firmware Upgrade

Upgrade the peripheral firmware using the same procedure as for the controller firmware.

The peripheral firmware file is only stored temporarily in the file system. When a new peripheral firmware file is uploaded, the current and new versions of the firmware for each peripheral and modem is displayed as shown:

ID	Type	SIN	Current Version	Upgrade Version	Action
8	I/O [8 Input / 2 Output]	11327907	1.11 [07AUG13]	1.11 [07AUG13]	Identical
7	Audio [4 Input]	1434900	1.03 [13MAR13]	1.03 [13MAR13]	Identical
6	Audio [4 Input / 1 Output]	37070907	1.03 [13MAR13]	1.03 [13MAR13]	Identical
5	Wireless	489907	1.11 [07AUG13]	1.11 [07AUG13]	Identical
4	I/O Analyzed [8 Input / 2 Output]	165074801	2.00 [09Apr14]	2.00 [09Apr14]	Identical
1	DC-2 [4 Input / 2 Output]	195309801	2.00 [07APR14]	2.00 [07APR14]	Identical
3	I/O [8 Output]	443907	1.11 [07AUG13]	1.11 [07AUG13]	Identical
2	Keyswitch [1 Output]	226593801	1.01 [11NOV10]	1.01 [11NOV10]	Identical
1	Indicator [1 Input]	223387801	1.03 [13MAR13]	1.03 [13MAR13]	Identical
2	Comfort Keypad	227361801	1.02 [13MAR13]	1.02 [13MAR13]	Identical
1	Keypad	559907	2.09 [13MAR13]	2.09 [13MAR13]	Identical

Modem Slot	Type	Current Version	Upgrade Version	Action
Modem Slot 1	IntelliModem PSTN	2.09 [28MAR14]	2.09 [28MAR14]	Identical
Modem Slot 2	IntelliModem GSM	3.08 [13NOV13]	3.09 [23Jan14]	Upgrade

- Click on the **Upgrade** button for the peripherals that require upgrading or click on the **Upgrade All** button to upgrade all peripherals.
- ⇒ If the firmware for a peripheral device in the pfw file is older than the existing firmware of that device, a **Downgrade** button is available.

During upgrade, the panel checks if the firmware in the peripheral file supports the particular hardware versions of the installed peripherals and does not allow an upgrade for those peripherals which are not supported.

If the pfw file version differs from the controller version, a warning message is displayed

If the major version number of the firmware available for a device differs from the existing major number of a device, a warning message is also displayed.

The peripheral firmware can also be upgraded with SPC Pro or using the Fast Programmer [→ 311].

Upgrading the SPCP355.300 Smart PSU Firmware

To upgrade the SPCP355.300 Smart PSU you must ensure the following:



The SPCP355.300 Smart PSU firmware can only be updated through the browser. It cannot be upgraded using SPCPro.

- The mains power must be connected.



The upgrade procedure can take up to 2 minutes to complete. Do not perform any actions within the browser, restart or shut down the system until the upgrade completes. A message will be displayed when the process is complete.

See also

Adding / Editing User Profiles [→ 186]

17.11.1.2 Upgrading Languages

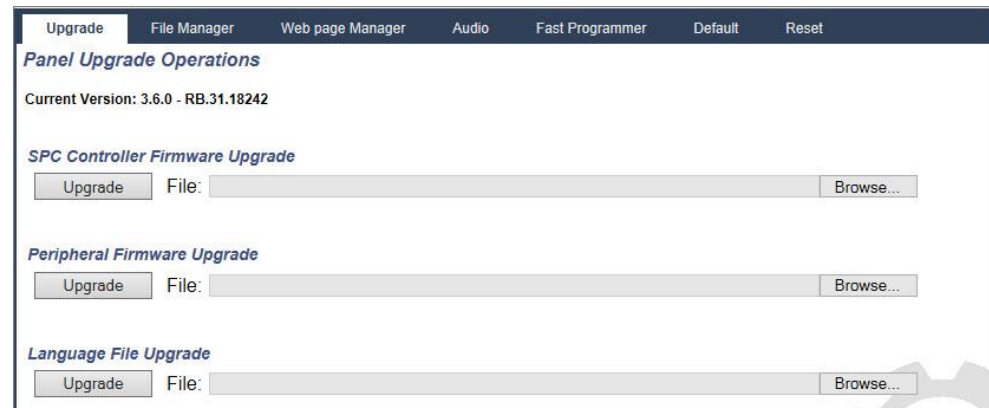
A custom language file (*.clng) can be uploaded to the panel. This file applies to the panel firmware only and is not available for SPC Pro or SPC Safe.

!	<p>NOTICE</p> <p>The panel must be licensed for use of custom languages and other languages.</p>
----------	---

To upgrade languages on the system:

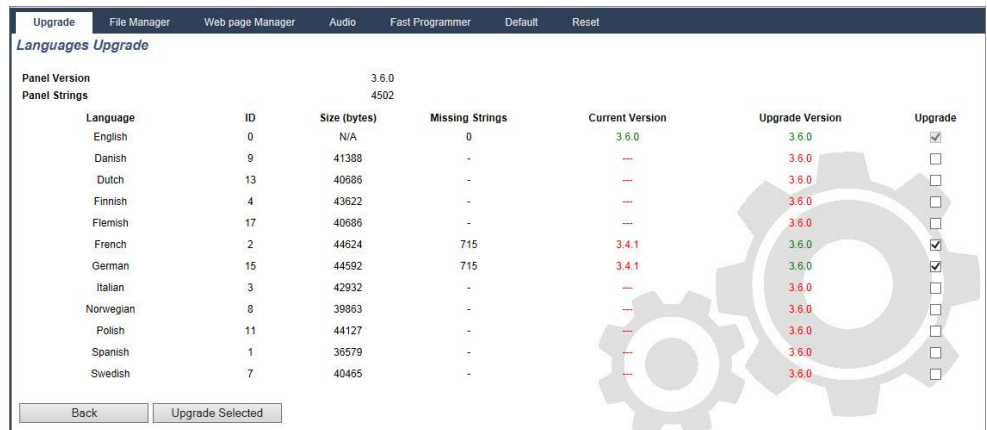
1. Select **File** -> **Upgrade**.

⇒ The **Panel Upgrade Operations** page is displayed:



2. Select the language file to upgrade by clicking the **Browse** button for the **Language File Upgrade** option, selecting the required language file and then clicking on the appropriate **Upgrade** button.

⇒ A list of available languages in this file is displayed.



3. Tick the box beside the language to be installed.



A maximum of 4 languages can be installed.

4. Click on the **Upgrade Selected** button.

⇒ The **Confirm Language Upgrade** screen is displayed showing any languages that are being installed.

5. Click on the **Confirm** button.

A message is displayed to indicate if the language upgrade was successful or if it failed.

Deleting Languages

To delete languages from the language file:

1. Select the language file to upgrade by clicking the **Browse** button for the **Language File Upgrade** option, selecting the required language file and then clicking on the appropriate **Upgrade** button.

⇒ A list of available languages in this file is displayed.

2. Uncheck the boxes for each of the languages that you want to delete.

3. Click on the **Upgrade Selected** button.

⇒ The **Confirm Language Upgrade** screen is displayed. When deleting a language, the panel deletes all languages and reinstalls only the languages required. In the example below, Flemish is being deleted.

Upgrade	File Manager	Web page Manager	Audio	Fast Programmer	Default	Reset
Confirm Language Upgrade						
Language files being deleted:						
ID	Language	Current Version				
2	French	3.4.1				
15	German	3.4.1				
Language files being installed:						
ID	Language	Upgrade Version				
2	French	3.6.0				
15	German	3.6.0				
Size (bytes)			109852			
Free space after upgrade (bytes)			405397			
<input type="button" value="Cancel"/>		<input type="button" value="Confirm"/>				

4. Click on the **Confirm** button to confirm the languages being deleted.

Language files can also be imported using the Fast Programmer [→ 311].

See Language [→ 236] for details of selecting the panel 'System' and 'Idle State' languages in the browser.

See OPTIONS [→ 111] for details of selecting the panel 'System' and 'Idle State' languages on the keypad.

See also

 Language [→ 236]

17.11.2 File Manager Operations

- Select **File -> File Manager**.

⇒ A screen displays showing details of the system configuration, language and trace files.

Upgrade	File Manager	Web page Manager	Audio	Fast Programmer	Default	Reset
System Files						
Description	Size (bytes)	Date	Delete			
System Configuration file	8059	04/07/14 15:44:50	-			
Backup System configuration file	671	07/06/12 12:37:01	<input type="button" value="..."/>			
Languages file	89070	17/06/14 11:16:09	<input type="button" value="..."/>			
Total Used		97800				
Free Space		426191				
System Configuration file						
<input type="button" value="Download"/>		Downloads the file to the PC where it can be saved as a backup.				
<input type="button" value="Upload"/>		Uploads a file from the PC to the panel				
<input type="button" value="Backup"/>		Creates a backup file on the panel, which can be used to restore the panel at a later date.				

System Configuration File

The following options are available to manage the system configuration file:

Download	Downloads a configuration file from the controller. Note: If an error message appears after clicking the download button, proceed as follows: <ol style="list-style-type: none"> 1. Select Internet Options in the Tools menu. 2. Select the Advanced tab. 3. Mark the checkbox Do not save encrypted pages to disk. 4. Click Apply. 5. Click OK. 6. Click Download again. <p>When downloading a configuration file, the configuration settings are stored in a .cfg file. This file can then be uploaded to other controllers to avoid lengthy programming procedures.</p>
Upload	Uploads a configuration file to the controller.
Backup	Stores a backup copy of the current configuration to flash.
Restore	Restores a backup copy of the current configuration from flash.

Users Data

The following options are available to manage users data:

Download	Click the button to Download the users data from the panel. A dialog box asks you where you would like to save the users.csv file.
Upload	Click the Browse button to Upload users data to the panel. This must be a .csv file format.

17.12 Using the Fast Programmer

The SPC Fast Programmer is a portable storage device that provides the engineer with the ability to upload and download configuration files in a quick and convenient manner. The Fast Programmer has two interfaces located on opposite ends of the device:

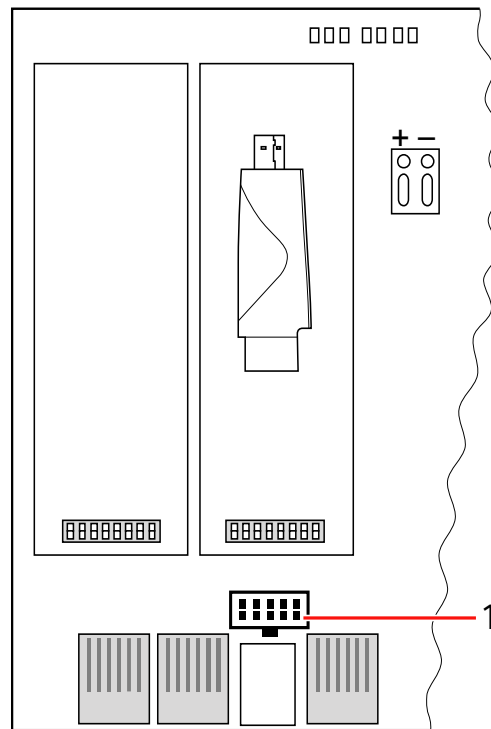
SPC controller interface

This 10-pin serial interface is located at the top of the Fast Programmer and connects directly to the Fast Programmer interface on the controller board. Once connected, the engineer can upload and download files directly from the Fast Programmer via the browser and keypad programming tools.

PC USB interface

This USB interface is located at the bottom of the Fast Programmer and connects directly to the USB interface on a PC. Configuration and other files can only be copied between the PC and the Fast Programmer using the SPC Pro programming tool.

17.12.1 Connecting the Fast Programmer to the Controller



Fast Programmer interface

1	Fast Programmer interface
---	---------------------------

To connect the SPC Fast Programmer to the controller:

1. Open the SPC controller enclosure and locate the Fast Programmer interface.
NOTICE! Do not power down the controller.
2. Align the Fast Programmer over the Fast Programmer interface on the SPC controller board with the 10-pin serial interface facing down.
3. Ensure the pins match up correctly with the holes in the socket and firmly but gently press into place.
 - ⇒ The LED on the Fast Programmer flashes momentarily as the data is accessed.
CAUTION! Do not remove the Fast Programmer while the LED is flashing.
 - ⇒ The Fast Programmer is now connected to the controller.



To remove the Fast Programmer - gently pull the device out of the Fast Programmer interface.

17.12.2 Installing the Fast Programmer on a PC

For Windows XP

- ▷ SPCPro must be installed on the Windows XP PC.
- 1. Connect the Fast Programmer to a USB interface on the PC.
 - ⇒ The **Found New Hardware** wizard is displayed.

2. Press **Next**.
3. Click **Continue Anyway**.
 - ⇒ At the end of the installation process, a window indicates that the installation process is complete.
4. Click **Finish**.

For Windows 7

- ▷ You have administration privileges.
- ▷ SPCPro must be installed on the Windows 7 PC.
- Connect the Fast Programmer to a USB interface on the PC.
- ⇒ The drivers are installed automatically

View SPC Fast Programmer

- Open the Windows menu **Start > Control panel > System > Device Manager**.
- ⇒ The Fast Programmer driver will be listed under the Ports (COM & LPT) directory as **SPC USB Fast Programmer (COM X)** (X = com port number).

17.12.3 Fast Programmer File Operations

Controller and peripheral firmware upgrades and custom language imports may be done using the Fast Programmer and SPC Pro.

17.12.3.1 Accessing the Fast Programmer using the Keypad

1. Enter Full Engineer and scroll to UTILITIES > FAST PROGRAMMER.
2. Press SELECT.
3. Scroll and select the desired option:

DATA FROM PANEL	Select desired file from list.
DATA TO PANEL	Select desired file from list.
DELETE FILES	Select desired file from list.
FIRMWARE UPGRADE	The panel searches for a valid controller firmware file. Once it finds the firmware file, it will allow the user to select it and upgrade the panel.
PERIPHERAL UPGRADE	The panel searches for a valid peripheral firmware file. Once it finds the firmware file, it will allow the user to select it and upgrade the panel.
LANGUAGE UPGRADE	A list of the language files available on the Fast Programmer is displayed. Select the language required and press SELECT to import the file.

17.12.3.2 Accessing the Fast Programmer using the Browser

1. Enter Full Engineer in browser programming and select the **File** programming page.
2. Click **Fast Programmer**.
- ⇒ The options to upload and download files are displayed.

Upgrade	File Manager	Web page Manager	Audio	Fast Programmer	Default	Reset
Fast Programmer						
Version: 0.1						
Type: 8 M Bytes used: 707 K Bytes free: 7 M						
Configuration files stored on Fast Programmer: No files on Fast Programmer						
Upload configuration file from SPC to Fast Programmer						
File name		<input type="text"/>	Upload			
Firmware files stored on Fast Programmer:						
SPC_2.2.0		Upgrade	Delete			
Language files stored on Fast Programmer: No files on Fast Programmer						
Upload language file from SPC to Fast Programmer						
File name		<input type="text"/>	Upload			

Downloading Configuration Files to the Panel

A list of the configuration files stored on the fast programmer is displayed along with the options to download or delete them.

Uploading Configuration Files to the Fast Programmer

When uploading files from the SPC to the Fast programmer, you will be prompted to delete the existing file on the programmer before the new file can be saved.

To upload a configuration file from the Fast Programmer to the SPC, enter the file name in the file name box and click **Upload**.

For complete details on using the Fast Programmer with SPC Pro, consult the *SPC Pro Configuration Manual*.

Upgrading Firmware



NOTICE

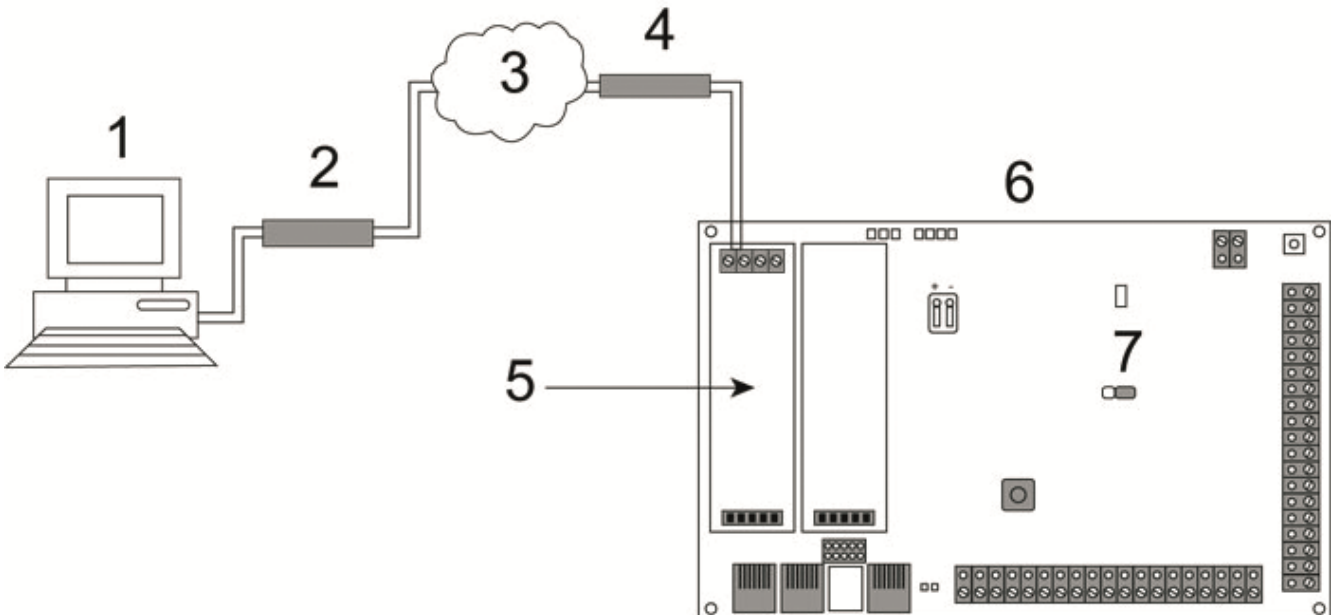
Manufacturer Access is required for firmware operations.

A list of the firmware files stored on the Fast Programmer is displayed.

To upgrade firmware, click on the **Upgrade** button beside the required firmware file.

18 Accessing web server remotely

18.1 PSTN connection



PSTN Connection

1	Remote PC with browser
2	PSTN modem
3	PSTN network
4	Telephone line
5	PSTN modem
6	SPC controller
7	JP9 SPG4xxx

The web server on the controller can be accessed via a remote connection over a PSTN telephone line. A PSTN module and a PSTN line must be connected to the controller as shown above to provide remote access to the controller.

On the remote side of the connection the user must have a PSTN modem installed on a PC with access to a PSTN line.

To connect remotely to the controller:

1. Install a PSTN modem on the controller (please refer to corresponding installation instruction).
2. Connect the phone line to the A/B screw terminals on the connector at the top of the modem.
3. Enter Engineer programming from the keypad and configure the modem (primary or backup) to answer an incoming call.
4. On the keypad, scroll to **Full Engineer Mode > Comms > Modems**
5. Select the following settings:
 - **Enable Modem:** Set to enabled
 - **Type:** Displays the type of modem (PSTN)

- **Country Code:** Select the relevant country code (Ireland, UK, Europe)
 - **Answer mode:** Select numbered rings; this tells the modem to wait for a number of rings before answering the incoming call
 - **Modem Rings:** Select the number of rings to allow before answering the call (8 rings max)
6. Create a dial-up connection on the remote PC using the phone number of the telephone line connected to the PSTN module on the controller. The instructions to do this on windows XP operating system are listed below:

On Windows XP:

1. Open the New Connection Wizard by browsing to **Control Panel > Network Connections > Create New Connection** (in the Network Tasks window).
2. In the **Network Connection Type** window, select **Connect to the Internet**.
3. In the **Getting Ready** window, choose **Setup my connection manually**.
4. In the **Internet Connection** window, choose **Connect using Dialup modem**.
5. In the **Connection Name** window enter the connection name e.g. SPC remote connection.
6. In the **Phone Number to Dial** window, enter the phone number of the PSTN line connected to the PSTN modem.
7. In the **Connection Availability** window, choose whether this connection is available to all users.
8. In the **Internet Account Information** window, enter the following details:
 - Username : SPC
 - Password: password (default)
 - Confirm Password: password⇒ The **Completing the New Connection Wizard** window is displayed.
9. Click **Finish** to save the Dial-up connection to the PC.



Default code should be changed and noted accordingly as Vanderbilt is unable to retrieve this new code. Forgotten codes are remedied only by a factory default of the system, rendering loss of programming. Programming can be restored if a backup is available.

To activate this dial-up connection:

- Click on the icon located in the **Control Panel > Network Connections** window.
 - ⇒ The PC makes a data call to the PSTN line connected to the SPC PSTN module.
 - ⇒ The SPC PSTN module answers the incoming data call after the designated number of rings and establishes an IP link with the remote computer.
 - ⇒ The SPC system automatically assigns an IP address to the remote PC.



For some Windows operating systems, a dialog box regarding Windows certification appears. Vanderbilt deems this acceptable to continue. For further queries, please contact network administrator or a Vanderbilt technician.

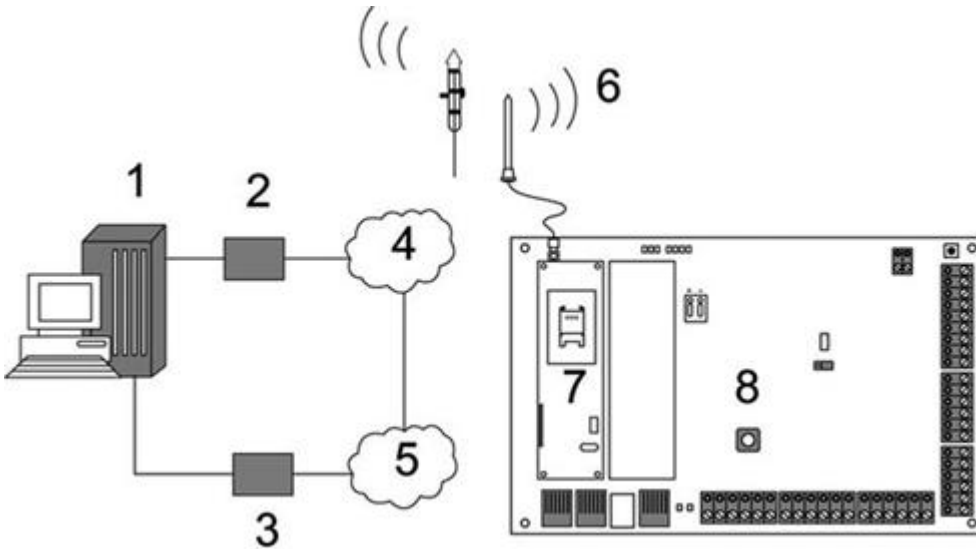
To obtain this IP address:

1. Right click the dial-up icon.
2. Click on the **Details** tab.
 - ⇒ The IP address is displayed as the Server IP address.
1. Enter this IP address in the address bar of the browser and click.
2. When the Dial-up connection icon is displayed on the task bar of the PC, open the browser and enter the IP address of the SPC.
 - ⇒ The browser logon screen is displayed.



To set up a dial-up connection on another operating system, consult the help menu of that operating system.

18.2 GSM connection



GSM Connection

1	Remote PC with browser
2	GSM modem
3	PSTN modem
4	GSM network
5	PSTN network
6	External antenna
7	GSM modem
8	SPC controller

The web server on the controller can be accessed via a remote connection over the GSM network. A GSM module (with SIM card) must be installed on the controller as shown above to provide remote access to the SPC. The data option of the SIM card must be activated and the data number must be used.

On the remote side of the connection the user must have a PSTN or GSM modem installed on a PC with browser. If a PSTN modem is installed then it must be connected to a working PSTN line.

To connect remotely to the controller:

1. Install a GSM modem on the controller (please refer to corresponding installation instruction).
2. Enter Full Engineer programming from the keypad and configure the modem (primary or backup) to answer an incoming call.
3. On the keypad, scroll to the following menu: FULL ENGINEER > COMMUNICATION > MODEMS, and select the settings listed:

Enable Modem	Set to Modem Enabled.
Type	Displays the type of modem (GSM).
Country Code	Select the relevant country code.
Answer Mode	Select numbered rings; this tells the modem to wait for a number of rings before answering the incoming call.
Modem Rings	Select the number of rings to allow before answering the call (8 rings max).

On Windows XP:

1. Open the New Connection Wizard by browsing to **Control Panel > Network Connections > Create New Connection** (in the Network Tasks window).
2. In the **Network Connection Type** window, select **Connect to the Internet**.
3. In the **Getting Ready** window, choose **Setup my connection manually**.
4. In the **Internet Connection** window, choose **Connect using Dialup modem**.
5. In the **Connection Name** window enter the connection name e.g. SPC remote connection.
6. In the **Phone Number to Dial** window, enter the phone number of the PSTN line connected to the PSTN modem.
7. In the **Connection Availability** window, choose whether this connection is available to all users.
8. In the **Internet Account Information** window, enter the following details:
 - Username : SPC
 - Password: password (default)
 - Confirm Password: Vanderbilt
 - ⇒ The **Completing the New Connection Wizard** window is displayed.
9. Click **Finish** to save the Dial-up connection to the PC.



Default code should be changed and noted accordingly as Vanderbilt is unable to retrieve this new code. Forgotten codes are remedied only by a factory default of the system, rendering loss of programming. Programming can be restored if a backup is available.

To activate this dial-up connection:

- Click on the icon located in the **Control Panel > Network Connections** window.
 - ⇒ The PC makes a data call to the PSTN line connected to the SPC PSTN module.
 - ⇒ The SPC PSTN module answers the incoming data call after the designated number of rings and establishes an IP link with the remote computer.
 - ⇒ The SPC system automatically assigns an IP address to the remote PC.



For some Windows operating systems, a dialog box regarding Windows certification appears. Vanderbilt deems this acceptable to continue. For further queries, please contact network administrator or a Vanderbilt technician.

To obtain this IP address:

1. Right click the dial-up icon.
2. Click on the **Details** tab.
 - ⇒ The IP address is displayed as the Server IP address.
1. Enter this IP address in the address bar of the browser and click.
2. When the Dial-up connection icon is displayed on the task bar of the PC, open the browser and enter the IP address of the SPC.
 - ⇒ The browser logon screen is displayed.



To set up a dial-up connection on another operating system, consult the help menu of that operating system.

19 Intruder alarm functionality

The SPC system can accommodate 3 distinct modes of intruder alarm operation, **Financial**, **Commercial** or **Domestic** mode, all of which support multiple areas.

Each area in turn can support 4 different alarm modes. Commercial and Financial mode present more programmable alarm types than Domestic mode. The default zone name and type settings for each mode is listed in page [→ 336].

19.1 Financial mode operation

Financial mode is suitable banking and financial businesses that have special secure areas such as vaults and ATMs.

Each area defined on the system supports the alarm modes listed below.

Alarm Mode	Description
UNSET	Area is disarmed, only alarm zones classified as 24Hour will activate the alarm.
PARTSET A	This mode provides perimeter protection to a building while allowing free movement through the exit and access areas. Zones that have been classified as EXCLUDE A remain unprotected in this mode. By default there is no exit time (the system instantly sets on selection of this mode). An exit timer can be applied to this mode by enabling the Partset A Timed variable.
PARTSET B	This setting mode applies protection to all zones except those that have been classified as EXCLUDE B. By default there is no exit time (the system instantly sets on selection of this mode). An exit timer can be applied to this mode by enabling the Partset B Timed variable.
FULL SET	Area is fully armed; opening of entry/exit zones starts the entry timer. If the alarm is not unset before entry timer expires, the alarm is activated.

19.2 Commercial mode operation

Commercial mode is suitable for business installations with multiple areas and a large number of alarm zones. Each area defined on the system supports the alarm modes listed below.

Alarm Mode	Description
UNSET	Area is disarmed, only alarm zones classified as 24Hour will activate the alarm.
PARTSET A	This mode provides perimeter protection to a building while allowing free movement through the exit and access areas. Zones that have been classified as EXCLUDE A remain unprotected in this mode. By default there is no exit time (the system instantly sets on selection of this mode). An exit timer can be applied to this mode by enabling the Partset A Timed variable.
PARTSET B	This setting mode applies protection to all zones except those that have been classified as EXCLUDE B. By default there is no exit time (the system instantly sets on selection of this mode). An exit timer can be applied to this mode by enabling the Partset B Timed variable.
FULL SET	Area is fully armed; opening of entry/exit zones starts the entry timer. If the alarm is not unset before entry timer expires, the alarm is activated.

19.3 Domestic mode operation

Domestic mode is suitable for residential installations with one or more areas and a small-to-moderate number of alarm zones. Each area defined on the system supports the alarm modes listed below.

Alarm Mode	Description
UNSET	Area is disarmed, only alarm zones classified as 24Hour will activate the alarm.
PARTSET A	This mode provides perimeter protection to a building while allowing free movement through the exit and access areas (for example front door and hall) Zones which have been classified as EXCLUDE A remain unprotected in this mode. There are no Exit times associated with this mode and protection is applied instantly on selection of this mode.
PARTSET B	This setting mode applies protection to all zones except those that have been classified as EXCLUDE B. By default there is no exit time (the system setting instantly on selection of this mode). An exit timer can be applied to this mode by enabling the Partset B Timed variable.
FULL SET	Area is fully armed, opening of Entry/Exit zone start the Entry timer. If the alarm is not unset before the Entry timer expires then the alarm is activated.

19.4 Full and local alarms

The type of alarms generated by the SPC system can vary depending on the type of zone that triggered the alarm activation. The vast majority of alarms require a visual (strobe) and audible (bell) indication of an intrusion to the premises or building.

By default, the first 3 physical outputs on the SPC controller are assigned to the external bell, internal bell, and external bell strobe. When activated, these 3 outputs together provide sufficient warning of an alarm condition to persons located inside or within the immediate environment of the building or premises where the intrusion has taken place.

Full and local alarms on the SPC activate the following physical outputs:

- Controller Output 1: External Bell
- Controller Output 2: Internal Bell
- Controller Output 3: Strobe

For details on how to wire the bells and strobe see page [→ 72].

A **Full Alarm** activation reports the alarm to the Alarm Receiving Centre (ARC) if one has been configured on the system.

A **Local Alarm** activation does not attempt to call the ARC even if one has already been configured.

A **Silent Alarm** activation does not activate outputs 1 – 3 (no visual or audible indications of the alarm). The alarm event is reported to the ARC. Silent alarms are only generated when alarm zones with the Silent attribute have been opened when the system is set.

20 System examples and scenarios

20.1 When to use a common area

Common areas provide a convenient way of setting multiple areas within a single installation. A user assigned to a common area has the ability to SET ALL areas within that common area (even those areas that have not been assigned to that user). However, the users can only UNSET areas assigned to them.

Common areas should only be used when a single keypad is installed at the primary access location and is shared by all users within the building (defining a common area on a system with multiple keypads in different areas is not recommended).

Scenario: 2 departments of a business (Accounts and Sales) share a common access point (front door)

In this case, create 3 areas on the system (Common Area, Accounts, and Sales). The Common Area must include the main access point (front door). Assign the zones in Accounts to Area 2 and the zones in Sales to Area 3. Install a keypad at the front door and assign it to all 3 areas. Define 2 users (minimum) on the system, one for each department, and assign the users to their respective areas and the common area.

Operation: Setting the system

The Accounts Manager leaves the office at 5 pm. When he enters his code at the keypad, the FULLSET option presents the following 3 sub-menus:

- ALL AREAS: sets all areas assigned to the common area (Common Area, Accounts, and Sales) and any additional areas assigned to the account manager; in this case there are no additional areas. The exit timer for the front door informs the user to exit the building.
- COMMON: sets all areas assigned to the Common Area (Common Area, Accounts and Sales) and starts the exit timer for the front door
- ACCOUNTS: sets the Accounts area only; the Sales area remains unset and access is still permitted through the front door

When the last worker in the Sales department is leaving the building, he/she closes all doors and windows in AREA 3 and enters his/her code at the keypad. The FULLSET option presents the following 3 sub-menus:

- ALL AREAS: sets all areas assigned to the Common Area (Common area, Accounts, and Sales) and any additional areas assigned to the sales worker; in this case there are no additional areas. The exit timer for the front door informs the user to exit the building.
- COMMON: sets all areas assigned to the Common Area (Common Area, Accounts, and Sales) and starts the exit timer for the front door.
- SALES: sets ALL areas assigned to the Common Area (Common area, Accounts and Sales); this is because there are no other unarmed sub-areas on the system

Operation: Unsetting the system

When the Accounts Manager returns to open the building and enters his code on the keypad, the UNSET option presents the following 3 sub-menus:

- ALL AREAS: unsets all areas assigned to the accounts worker (Common Area, Accounts) and any additional area assigned to the accounts worker. In this case there are no additional areas. NOTE: The accounts worker cannot UNSET the Sales area.
- COMMON: unsets ONLY the Common Area (Reception). This provides the option to unarm the reception area only while leaving the Accounts and Sales offices set.

- ACCOUNTS: unsets the Accounts area and the Common Area (Reception). In this case the Sales area remains set while access is still permitted through the front door.

Use of common areas:

- Keyarm zone

If the entry/exit route in the common area is programmed as a keyarm zone, when it is activated all areas in the Common area are SET. Deactivating the keyarm zone UNSETS all areas in the Common Areas.

- Multiple keypads

If areas assigned to the common area have their own keypads for entry/exit, it is important that the exit times associated with those areas provide sufficient time to allow the user to reach the common area exit. This is in case the area being armed is the last un-armed area on the system and therefore will trigger arming of the entire common area.



As a rule it is advisable to use common areas in installations that have only one keypad located at the common access point, i.e. front door access to the entire building.

21 Seismic Sensors

Vibration sensors, also called seismic sensors, are used to detect intrusion attempts by mechanical means, such as drilling or making holes through walls or safes.

Support for seismic sensors is available only if the installation type for the panel is 'Financial'.

There are several ways to test seismic sensors. The simplest way to test seismic sensors is by hitting a wall or safe and seeing if the zone opens during a walk test. This means of testing is available with all types of seismic sensors.

If the seismic sensor is installed with a test transmitter, the following test options are available:

- Manual testing initiated at the keypad or with SPC Pro (not supported by the browser);
- Automatic testing on a periodic basis or when the panel is set using the keypad.

The test transmitter is a small high frequency vibrator that is attached a short distance from the sensor on the same wall. The test transmitter is wired to an output on the panel or an expander.

Configuring Seismic Sensors in the Panel

1. Configure a seismic zone. Seismic sensors must be assigned to a zone. (See Editing a Zone [→ 237])

Zone	Input	Description	Type	Area	Attributes
1	Controller - Input 1	Front door	Entry/Exit	2: Reception	...
2	Controller - Input 2	Vault	Seismic	7: Vault	...

2. Set the attributes for the zone.

Attribute	Description
<input type="checkbox"/> 24 Hour	If checked the zone opening will activate the alarm in all modes.
<input type="checkbox"/> Unset local	When the Unset Local attribute is set, an alarm generated by the zone opening will result in the reporting of the event only when the area is Fullset or Partset.
<input checked="" type="checkbox"/> Inhibit	If checked a user may inhibit this zone.
<input type="checkbox"/> Log	If checked then all zone state changes are logged.
<input type="checkbox"/> Seismic Test	If checked then the seismic sensor will be automatically tested at an interval as set in Timers 'Seismic Test Interval'
Calendar	
<input type="text" value="5: Vault"/>	Check if zone is limited by calendar.
Verification	
<input type="text" value="1: Verificat 1"/>	Check if input is to be included in a verification zone, and trigger audio/video verification.
<input type="button" value="Save"/> <input type="button" value="Back"/>	

3. Enable automatic testing of the sensor with the **Seismic Test** attribute.
4. Select a calendar to control the seismic zone, if required.
5. Assign this zone to a verification zone if audio/video verification is required..
6. Configure timers to specify how often to test seismic zones (default is 7 days) and the duration of the tests. (Automatic Seismic Test zone attribute must be set). (See Timers [→ 230])

Seismic Test Interval	<input type="text" value="168"/> Hours	Average test period for seismic sensor automatic tests (the test period is randomized). To enable automatic tests the 'Seismic Test' attribute of the 'Seismic' zone type must be enabled. (12 - 240)
Seismic Test Duration	<input type="text" value="30"/> Seconds	Maximum time (in seconds) that a seismic sensor takes to trigger an alarm in response to the 'Seismic Test' output. (3 - 120)

7. Configure an output for testing a seismic zone. (See Output Types and Output Ports [→ 198])

The output can be assigned to either the system or an area, if the panel is

configured to use areas as is usually the case in financial environments. The output should only be assigned to the system if the panel does not use areas.

Hardware System Inputs Outputs Doors Areas Calendars Change own PIN Advanced

Controller X-BUS Wireless

Output Type

Disabled

System

External Bell

Area

7: Vault

Seismic Test

Using the Keypad

1. Select FULL ENGINEER->ZONES->(select zone)->ZONE TYPE->SEISMIC
2. Select FULL ENGINEER->ZONES->(select zone)->ATTRIBUTES->SEISMIC AUTOTEST

See also

- 📄 Timers [→ 230]
- 📄 Outputs types and output ports [→ 198]
- 📄 Editing a zone [→ 237]

21.1 Seismic Sensor Testing

Seismic zones must be configured in order for both manual and automatic tests to be available. The results of either manual or automatic testing are stored in the system event log.

During a seismic test, one or more seismic zones are tested. When a zone is tested, all other zones in the same area are temporarily disabled as there is a single seismic test output per area

21.1.1 Manual and Automatic Test Process

A manual or automatic test operates as follows:

1. The panel activates the Seismic Test Output for the appropriate area(s) in which the seismic zone(s) are to be tested.
2. The panel then waits for all seismic zones under test to open and then verifies that all seismic sensors in the area enter the alarm state within the time configured for the '**Seismic Test Duration**'. Any zone(s) that have not opened within the maximum period are deemed to have failed the test.
3. When all seismic zones in the area are open or the maximum Seismic Test Duration has been reached (whichever comes first), the panel will clear the Seismic Test Output for that area.
4. The panel then waits a fixed time for all seismic detectors in the area to close. Any zone(s) that have not closed are deemed to have failed the test.
5. The panel then waits another fixed period before reporting the test result. The result of the test, either manual or automatic, is stored in the system event log.

The seismic output is normally high, and goes low during tests (i.e. when it is active). If this signal is not suitable for a particular sensor then the physical output can be configured to be inverted.

21.1.2 Automatically Testing Sensors

Seismic sensors are tested either periodically or after the system is set using the keypad.

Periodic Automatic Testing

Periodic automatic tests are performed on all seismic zones for which automatic tests are enabled.

Automatic tests are randomized within the configured test period and are done independently for each area.

All seismic zones in the same area (for which automatic tests are enabled) are tested simultaneously.

The **Seismic Test Interval** configuration option in the Timers [→ 230] menu determines the average test period for seismic sensors automatic tests. The default value is 168 hours (7 days) and the allowed values are in the range 12 – 240 hours.

The test time is random within the specified range +/- 15%. For example, if a test is scheduled every 24 hours, a test may be performed between 20.4 and 27.6 hours after the last test.

A seismic test is performed after a reboot if automatic tests are enabled. If the panel was in Full Engineer mode before reboot, then the test is performed only after the panel is out of Full Engineer mode after a reboot.

If a seismic test fails, a Trouble event is reported (SIA code "BT"). There is also a corresponding Restoration event (SIA code "BJ").

Automatic Test on Setting

The option **Seismic Test on Set** is configurable in the System Options [→ 222] menu. If enabled, all seismic zones in all areas that are to be set are tested before the usual setting sequence. This applies to keypad operation only.

While the test is being performed, 'SEISMIC AUTOTEST' is displayed on the keypad. If the seismic test succeeds, the setting proceeds as normal.

If all areas or an area group or a single area are selected to be set, and a seismic test fails, then 'SEISMIC FAIL' will be displayed. Pressing **Return** displays a list of the failed zones which can be scrolled through using the up and down arrow keys.

Depending on the **Inhibit** settings for the failed seismic zones and your user profile, the following can occur:

- If all of the seismic zones that failed the test have the **Inhibit** attribute set, and your user profile user is configured with the **Inhibit** right:
 1. Press **Return** on any of the failed zones.
 - ⇒ The message "FORCE SET ALL?" is displayed.
 2. Press **Return** again to inhibit all seismic zones that failed the test. (Alternatively, go back to the previous menu.)
 - ⇒ Setting proceeds as normal.
- If some of the seismic zones that failed the test do not have the **Inhibit** attribute set or your user profile user does not have the **Inhibit** right:
- Press **Return**.
 - ⇒ The message 'FAIL TO SET' will be displayed and no areas will be set.

There is no automatic seismic test for areas that are auto-set for any reason (for example, areas activated by a calendar or trigger). Likewise there is no automatic seismic test when the system is set with SPC Com, with SPC Pro or the browser. However, there is an automatic seismic test when a virtual keypad is used with SPC Com or SPC Pro.

No event is reported if seismic testing on set fails.

The periodic automatic system test timer restarts after a test is performed after setting.

21.1.3 Manually Testing Sensors

To manually test sensors, select the TEST>SEISMIC TEST option from the TEST menu on the keypad.

A seismic manual test with the keypad can be done by the engineer in Full Engineer mode, and also by a user of type Manager or type Standard:

- An engineer is able to test all sensors in all areas configured in the system using any keypad.
- A user is able to test only the sensors in areas that are both assigned to him and to the particular keypad he is using.

To perform a seismic test in Engineer mode, select FULL ENGINEER ⇒ TEST ⇒ SEISMIC TEST

To perform a seismic test in User mode, select MENUS ⇒ TEST ⇒ SEISMIC TEST

Note: The following instructions apply to both engineer and user modes but please note that only a subset of options may be available to a user.

The following options are available in the SEISMIC TEST menu:

- TEST ALL AREAS
Tests seismic zones in all available areas if there is more than one area that contains seismic zones.
- 'AREA NAME'
The names of the areas containing seismic zones are listed individually. When a specific area is selected, the following options are available:
 - TEST ALL ZONES
Test all seismic zones in this area if there is more than one seismic zone.
 - 'ZONE NAME'
The names of all seismic zones are listed and can be selected for testing individually.

The message 'SEISMIC TEST' is display on the keypad while the test is being performed,

If the test fails, the message 'SEISMIC FAIL' is displayed. If the "i" or VIEW key is pressed, a list of the failed zones is displayed which can be scrolled through.

If the test succeeds, 'SEISMIC OK' is displayed.

Entries are recorded in the event log with the following details:

- user who initiated the test
- result (OK or FAIL)
- area and zone number and name.

No events are reported for manual tests.

22 Blocking Lock Operation

Blocking Lock operation and the Authorized Setting operation of a Blocking Lock is supported by the SPC intrusion panel.

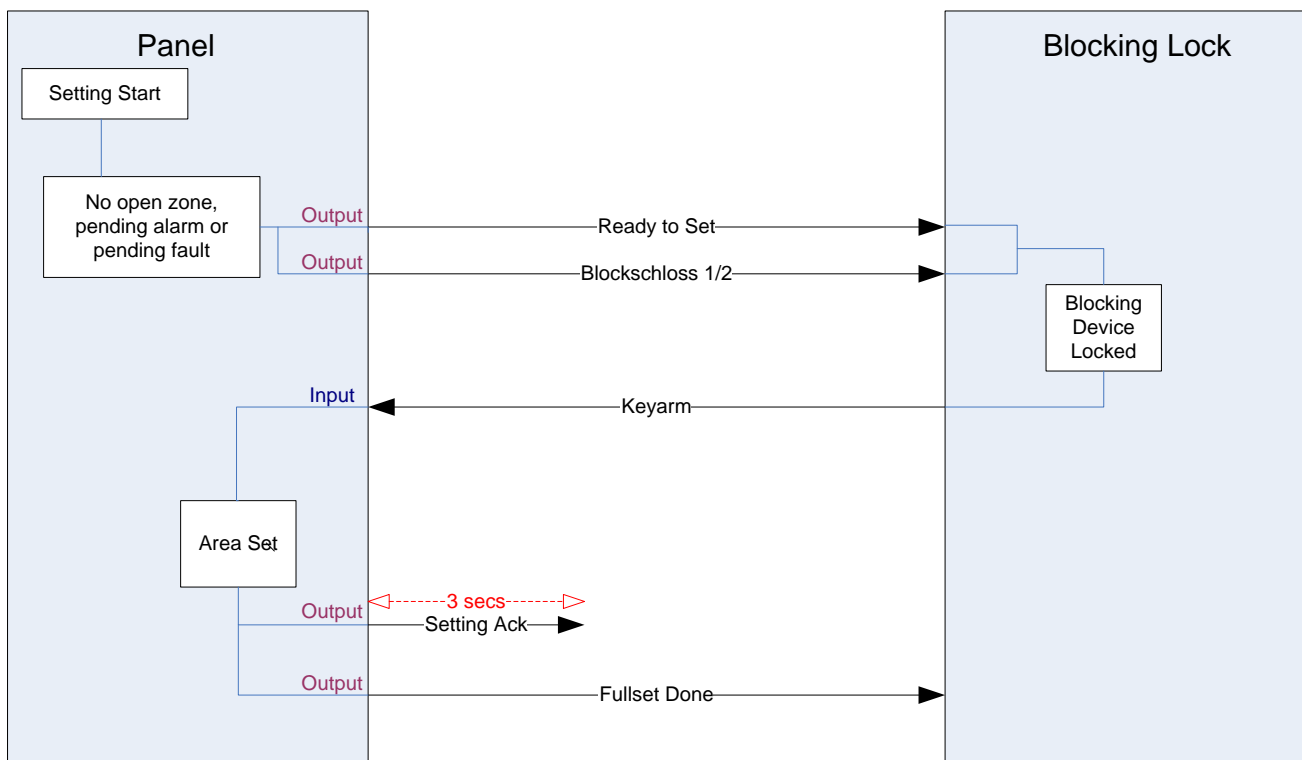
22.1 Blocking Lock

A Blocking Lock is a mechanical lock which is mounted into a door in addition to the normal lock and is used to set and unset the intrusion system. SPC support normal Blocking Lock devices (Blockschloss 1) and also the Bosch Blockschloss, Sigalock Plus, E4.03 device (Blockschloss 2).

Depending on the kind of Blocking Lock, a signal is needed to enable locking and unlocking the lock i.e. the Blocking Lock can only be locked and the system set if the signal Ready to Set is available from the control panel. This is controlled by a magnetic switch.

The operation of a Blocking Lock is as follows:

1. If there is no open zone, pending alarm or pending fault in the area, the area is ready to set and the Ready to Set signal is sent from the panel.
2. If the Blocking Lock device is then locked, the Blockschloss 1/2 output is activated.
3. Following the corresponding change on the Keyarm input type, the respective area is set.
4. The Setting Ack output is activated for 3 seconds to signal a successful setting of the area. Blockschloss 1 output is deactivated when the system is set. Blockschloss 2 stays activated when the system is set.
5. If the Blocking Lock is unlocked, the Keyarm input is switched to the unset state (closed).
6. Following the change on the Keyarm input type, the area is unset. Blockschloss 1 is deactivated if the area is ready to set while Blockschloss 2 is activated if the area is ready to set.



The configuration requirements for a Blocking Lock are as follows:

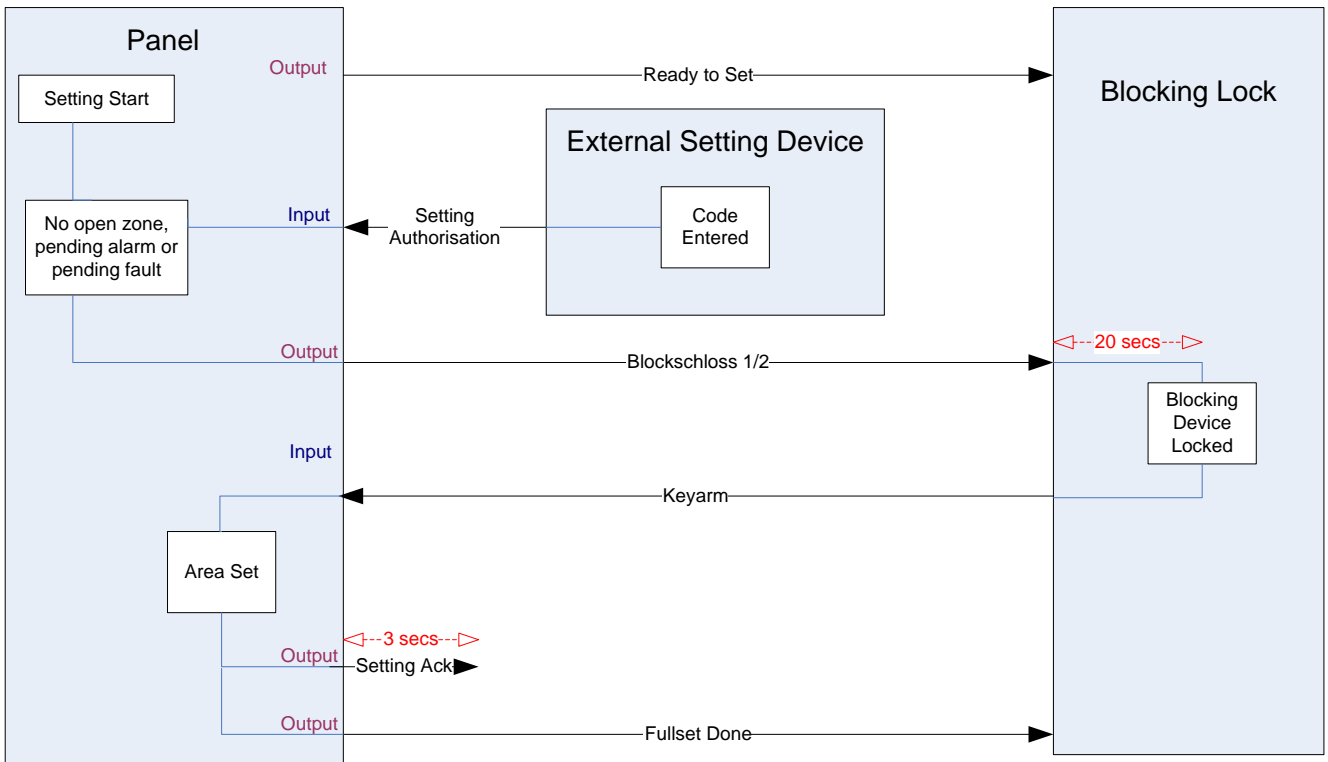
- Outputs:
 - Ready to set
 - Setting Ack
 - Fullset Done
 - Blockschloss 1/2
- Inputs
 - Keyarm

22.2 Authorized Setting of the Blocking Lock

The 'Authorised Setting' functionality extends the setting and unsetting procedure for a Blocking Lock with a second security level. Before the system can be set or unset, a code must be entered on an external setting device such as a card or pin reader with a separate controller. This controller can be connected to any kind of intrusion system using inputs and outputs.

Operation is as follows:

1. The panel signals to the external setting device when it is possible to set using a Ready To Set output.
2. When the code is entered, the Setting Authorisation input is activated and Blockschloss 1/2 is activated.
3. The blocking lock opens a control panel input (Keyarm) which initiates the setting procedure of the panel.
4. The external setting device waits up to 8 seconds for Fullset Done output signal to be activated from the control panel.
5. If this signal is not received, the setting fails and the external setting device unsets the system again.



The configuration requirements for Authorised Setting are as follows:

- Area Attributes:
 - Setting Authorisation
 - Set
 - Set and Unset (required for VdS)
 - Unset
- Outputs:
 - Ready to set
 - Setting Ack
 - Fullset Done
- Inputs
 - Keyarm

22.3 Locking Element

For VdS, it is mandatory to prevent entering a set area. This is done by using a Lock Element which is mounted in the doorframe. The lock element consists of a small plastic bolt which locks the door in a SET state. The position of the bolt is signaled by **Lock element – Lock** or **Lock element – Unlock** outputs. This signal is checked during the setting process. If the “locked” information is not received, the setting fails.

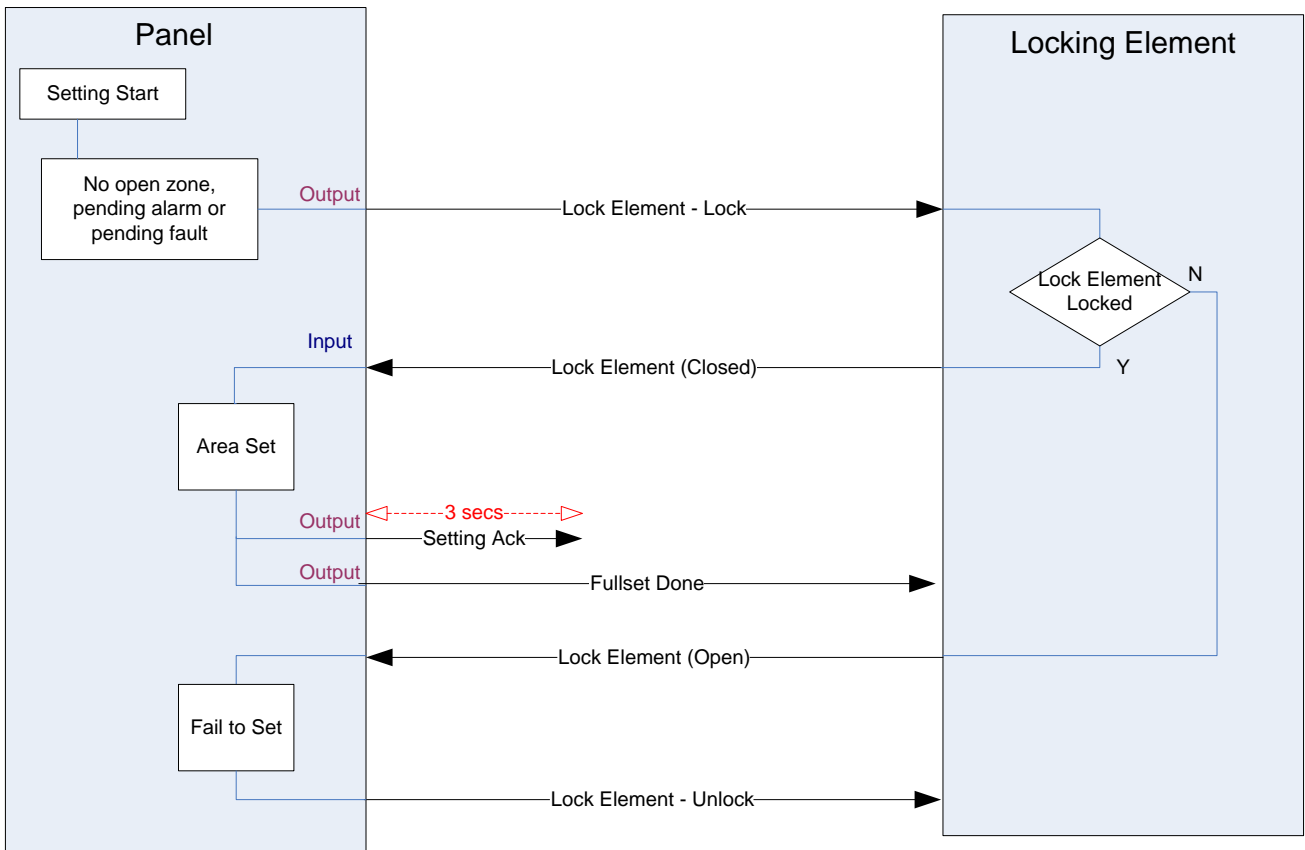
If a lock element is located within an area, the exit timer will be restricted to a minimum of 4 seconds so that the lock element can be activated. When the exit timer reaches four seconds, the lock element will be activated for three seconds. When the exit timer expires, the Lock Element input must be in the closed state then the system will set.

If a lock element is opened during a set period it will be handled as an alarm zone.

If a lock element is closed during an unset process then it will be considered to be tampered and raise a tamper on the zone.

If the lock element fails to open after the unlock signal is sent to the device, then a trouble will be raised on that zone to signal that a mechanical failure has occurred.

If the Lock Element input (if configured) is not in the closed state when the exit timer expires, then the system will not set and a Fail to Set signal will be raised. The Lock Element – Unlock output will be activated.



The configuration requirements for the lock element are as follows:

- Outputs:
 - Lock Element – Lock
 - Lock Element – Unlock
- Inputs
 - Lock Element

23 Appendix

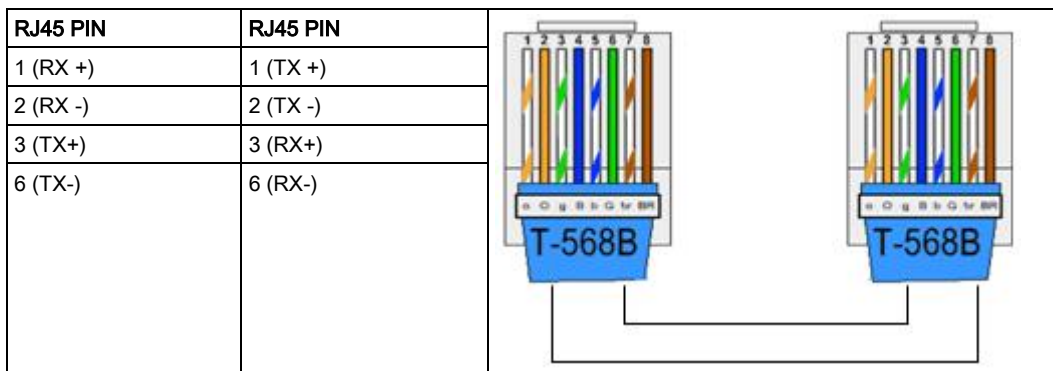
23.1 Network cable connections

IP

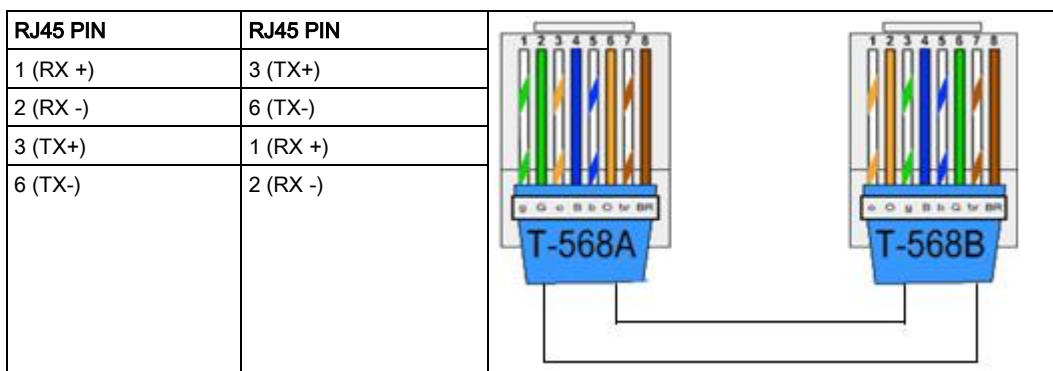
A PC can be connected directly to the Ethernet interface of the SPC controller or via a LAN connection. The tables below show the 2 possible connection configurations.

- If the SPC is connected to an existing network via a hub, then connect a straight through cable from the hub to the SPC and another from the hub to the PC.
- If the controller is not connected to a network (i.e. a hub or switch is not used), then a crossover cable should be connected between the SPC controller and the PC.

Use the straight through cable for connecting the SPC controller to a PC via a hub.






Use the crossover cable for connecting the SPC controller directly to a PC.



23.2 Controller status LEDs

LED	Function
LED 1	Wireless Data FLASHING: wireless data is being received by the wireless module OFF: no wireless data is being received
LED 2	Battery Status ON: battery voltage has dropped below the deep discharge level (10.9 V) OFF: battery status OK

LED 3	Mains Supply ON: Mains failure OFF: Mains OK
LED 4	X-BUS Status ON: X-BUS configuration is a loop configuration OFF: X-BUS configuration is an spur configuration FLASHING: Detects end of line Expanders or break in wiring.
LED 5	System Fault ON: a hardware fault has been detected on the board OFF: no hardware fault has been detected
LED 6	Writing to Flash ON: system is writing to flash memory OFF: system is not writing to flash memory
LED 7	Heartbeat FLASHING: system is functioning normally

ON 	OFF 	FLASHING 
--	---	--

23.3 Powering expanders from the auxiliary power terminals

To calculate the number of expanders/keypads that can safely be powered from the auxiliary 12 VDC power terminals, add the total maximum current draw from all of the expanders/keypads to be powered and determine if this total is less than the specified 12VDC auxiliary power.

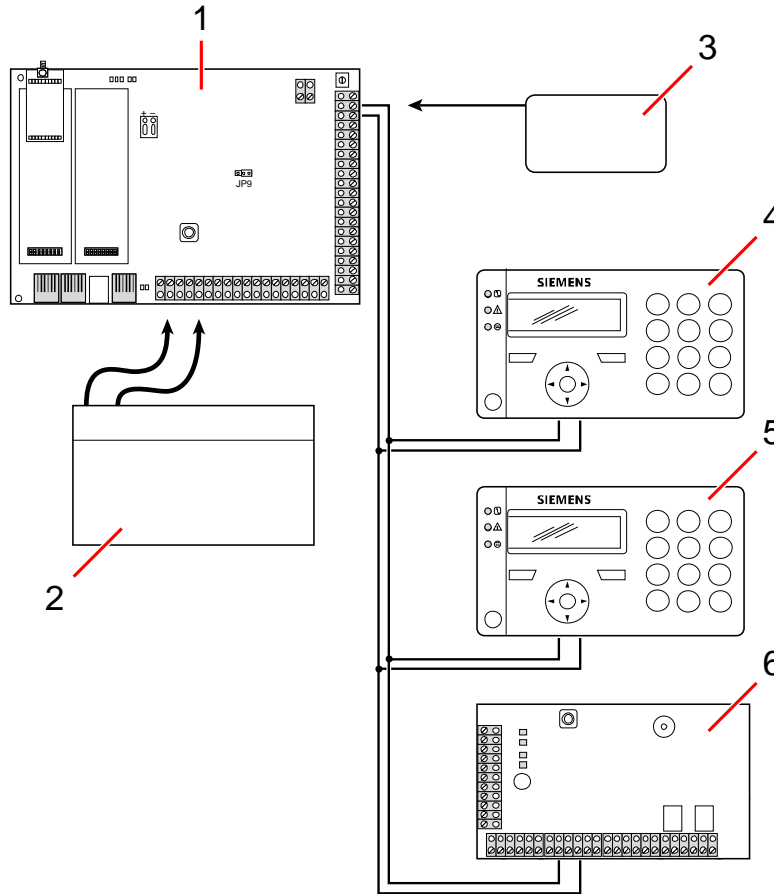


Please refer to Technical data for the specific auxiliary current and to the corresponding installation instruction or data sheet of modules, keypads and expanders for current consumption.

$$\text{Expander 1 Current (mA)} + \text{Expander 2 Current (mA)} + \dots < \text{Auxiliary Power}$$

If the electronic or relay outputs are already powering external devices, the power supplied to these devices must be subtracted from the 12VDC auxiliary power supply to determine the amount of available power from the auxiliary power terminals (0 V 12 V).

If the total maximum current draw from the expanders exceeds the auxiliary power, a PSU expander should be used to provide additional power.



Powering expanders from the auxiliary power terminals

1	SPC controller
2	Battery
3	Auxiliary 12 V power terminals
4	Keypad
5	Keypad
6	I/O expander

23.4 Calculating the battery power requirements

It is important that adequate stand-by power is available to supply all devices in the event of a mains supply failure. To ensure that enough power is available, always connect the appropriate back-up battery and PSU.

The table below gives an approximation of the maximum load current that can be drawn from each type of battery over the given stand-by periods.

The approximations below assume that the SPC controller PCB is drawing its maximum load (all wired inputs have their EOL resistors fitted) and that the usable output power from the battery is 85 % of its maximum capacity.

0.85 x battery size (Ah)	-	(Icont + Ibell)	=	I _{max}
Time (hours)				

Battery size = Capacity, in Ah, depending upon SPC enclosure chosen

Time = backup time, in hours, depending upon Security grade

I_{cont} = Quiescent current (in A) for the SPC controller

I_{bell} = Quiescent current (in A) for the attached external and internal bells

I_{max} = the maximum current that can be drawn from the auxiliary power output

Amount of current from Aux output using a 7 Ah battery (SPC422x/522x)

COMMS	NONE	PSTN	GSM	PSTN+GSM
Standby time				
12 h	356 mA	331 mA	226 mA	201 mA
30 h	58 mA	33 mA	N / A	N / A

Amount of current from Aux output using a 17 Ah battery (SPC523x)

COMMS	NONE	PSTN	GSM	PSTN+GSM
Standby time				
12 h	750 mA	750 mA	750 mA	750 mA
30 h	342 mA	317 mA	212 mA	187 mA

Amount of current from Aux output using a 7 Ah battery (SPC432x/532x)

COMMS	NONE	PSTN	GSM	PSTN+GSM
Standby time				
12 h	326 mA	301 mA	196 mA	171 mA
30 h	28 mA	N / A	N / A	N / A

Amount of current from Aux output using a 17 Ah battery (SPC533x/633x)

COMMS	NONE	PSTN	GSM	PSTN+GSM
Standby time	mA	mA	mA	mA
12 h	750	750	750	750
30 h	312	287	182	157

Amount of current from Aux output using a 24 Ah battery (SPC535x/635x)

COMMS	NONE	PSTN	GSM	PSTN+GSM
Standby time	mA	mA	mA	mA
12 h	1650	1625	1610	1585
24 h	650	625	610	585
30 h	450	425	410	385
60 h	50	25	10	N/A

Amount of current from Aux output using two 24 Ah batteries (SPC535x/635x)

COMMS	NONE	PSTN	GSM	PSTN+GSM
Standby time	mA	mA	mA	mA
12 h	2205	2180	2165	2140
24 h	1650	1625	1610	1585
30 h	1250	1225	1210	1185
60 h	450	425	410	385

Amount of current from Aux output using a 27 Ah battery (SPC535x/635x)

COMMS	NONE	PSTN	GSM	PSTN+GSM
Standby time	mA	mA	mA	mA
12 h	1900	1875	1860	1835
24 h	775	750	735	710
30 h	550	525	510	485
60 h	100	75	60	35

Amount of current from Aux output using two 27 Ah batteries (SPC535x/635x)

COMMS	NONE	PSTN	GSM	PSTN+GSM
Standby time	mA	mA	mA	mA
12 h	2205	2180	2165	2140
24 h	1900	1875	1860	1835
30 h	1450	1425	1410	1385
60 h	550	525	510	485

Values listed as N / A indicate that the selected battery does not have the capacity to power the minimum load of just the SPC controller for the given standby time. See page [→ 334] for maximum load of devices and modules.



Only sealed cell valve regulated battery types to be used.

For EN compliance the supplied current needs to be supported by the battery for required stand by time.

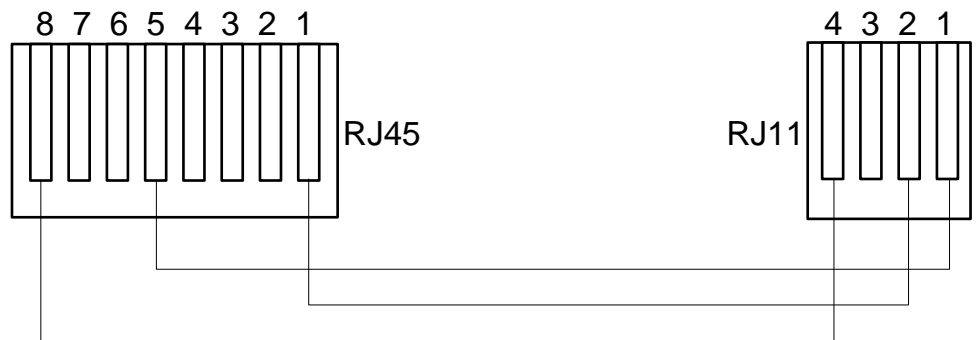
23.5 Domestic, Commercial and Financial mode default settings

This table gives the default zone name and types on the controller for each mode of operation. All zones on connected expanders are be categorized as unused until explicitly configured by the installation engineer.

Feature	Domestic mode	Commercial mode	Financial mode
<i>Zone Names</i>			

Controller - Zone 1	Front door	Front door	Front door
Controller - Zone 2	Sitting room	Window 1	Window 1
Controller - Zone 3	Kitchen	Window 2	Window 2
Controller - Zone 4	Upstairs front	PIR 1	PIR 1
Controller - Zone 5	Upstairs rear	PIR 2	PIR 2
Controller - Zone 6	PIR hallway	Fire exit	Fire exit
Controller - Zone 7	PIR landing	Fire alarm	Fire alarm
Controller - Zone 8	Panic button	Panic button	Panic button
<i>Zone Types</i>			
Controller - Zone 1	ENTRY/EXIT	ENTRY/EXIT	ENTRY/EXIT
Controller - Zone 2	ALARM	ALARM	ALARM
Controller - Zone 3	ALARM	ALARM	ALARM
Controller - Zone 4	ALARM	ALARM	ALARM
Controller - Zone 5	ALARM	ALARM	ALARM
Controller - Zone 6	ALARM	FIRE EXIT	ALARM
Controller - Zone 7	ALARM	FIRE	ALARM
Controller - Zone 8	PANIC	PANIC	ALARM

23.6 Wiring of the X10 interface



X10 wiring to the controller

PIN	RJ45	RJ11
TX	8	4
GND	5	1
RX	1	2

23.7 SIA Codes

DESCRIPTION	CODE
AC RESTORAL	AR
AC TROUBLE	AT
BURGLARY ALARM	BA
BURGLARY BYPASS	BB
BURGLARY CANCEL	BC

DESCRIPTION	CODE
SWINGER TROUBLE	BD
SWINGER TROUBLE RESTORE	BE
BURGLARY TROUBLE RESTORE	BJ
BURGLARY RESTORAL	BR
BURGLARY TROUBLE	BT
BURGLARY UNBYPASS	BU
BURGLARY VERIFIED	BV
BURGLARY TEST	BX
CLOSING DELINQUENT	CD
FORCED CLOSING	CF
CLOSE AREA	CG
FAIL TO CLOSE	CI
EARLY TO CLOSE	CK
CLOSING REPORT	CL
AUTOMATIC CLOSING	CP
REMOTE CLOSING	CQ
CLOSING KEYSWITCH	CS
LATE TO OPEN	CT
ACCESS CLOSED	DC
ACCESS DENIED	DD
DOOR FORCED	DF
ACCESS GRANTED	DG
ACCESS DENIED PASSBACK	DI
DOOR LEFT OPEN	DN
ACCESS OPEN	DO
DOOR RESTORAL	DR
REQUEST TO EXIT	DX
EXIT ALARM	EA
EXPANSION TAMPER RESTORE	EJ
EXPANSION MISSING	EM
EXPANSION MISSING RESTORE	EN
EXPANSION RESTORAL	ER
EXPANSION DEVICE TAMPER	ES
EXPANSION TROUBLE	ET
FIRE ALARM	FA
FIRE BYPASS	FB
FIRE CANCEL	FC
FIRE TROUBLE RESTORE	FJ
FIRE RESTORAL	FR
FIRE TROUBLE	FT
FIRE UNBYPASS	FU

DESCRIPTION	CODE
HOLDUP ALARM	HA
HOLDUP BYPASS	HB
HOLDUP TROUBLE RESTORE	HJ
HOLDUP RESTORAL	HR
HOLDUP TROUBLE	HT
HOLDUP UNBYPASS	HU
CONFIRMED HOLDUP	HV
USER CODE TAMPER ¦WEB or ¦XBUS	JA
TIME CHANGED	JT
LOCAL PROGRAMMING	LB
MODEM RESTORAL ¦ 1 or 2	LR
MODEM TROUBLE ¦ 1 or 2	LT
LOCAL PROGRAMMING ENDED	LX
MEDICAL ALARM	MA
MEDICAL BYPASS	MB
MEDICAL TROUBLE RESTORE	MJ
MEDICAL RESTORAL	MR
MEDICAL TROUBLE	MT
MEDICAL UNBYPASS	MU
PERIMETER ARMED	NL
NETWORK LINK IP RESTORE	NR
NETWORK LINK GPRS RESTORE	NR
NETWORK LINK IP FAIL	NT
NETWORK LINK GPRS FAIL	NT
AUTOMATIC OPENING	OA
OPEN AREA	OG
EARLY OPEN	OK
OPENING REPORT	OP
OPENING KEYSWITCH	OS
LATE TO CLOSE	OT
REMOTE OPENING	OQ
DISARM FROM ALARM	OR
PANIC ALARM	PA
PANIC BYPASS	PB
PANIC TROUBLE RESTORE	PJ
PANIC RESTORAL	PR
PANIC TROUBLE	PT
PANIC UNBYPASS	PU
RELAY CLOSE	RC
REMOTE RESET	RN
RELAY OPEN	RO

DESCRIPTION	CODE
AUTOMATIC TEST	RP
POWERUP	RR
REMOTE PROGRAM SUCCESS	RS
DATA LOST	RT
MANUAL TEST	RX
TAMPER	TA
TAMPER BYPASS	TB
TAMPER RESTORAL	TR
TAMPER UNBYPASS	TU
TEST CALL	TX
UNTYPED ALARM	UA
UNTYPED BYPASS	UB
UNTYPED TROUBLE RESTORE	UJ
UNTYPED RESTORAL	UR
UNTYPED TROUBLE	UT
UNTYPED UNBYPASS	UU
BELL FAULT	YA
RF JAM RESTORAL	XH
RF TAMPER RESTORAL	XJ
READER LOCKED	RL
READER UNLOCKED	RG
KEYPAD UNLOCKED	KG
RF JAM FAULT	XQ
RF TAMPER	XS
COMMUNICATION FAIL	YC
CHECKSUM FAULT	YF
BELL RESTORED	YH
COMMUNICATION RESTORAL	YK
BATTERY MISSING	YM
PSU TROUBLE	YP
PSU RESTORAL	YQ
BATTERY RESTORAL	YR
COMMUNICATION TROUBLE	YS
BATTERY TROUBLE	YT
WATCHDOG RESET	YW
SERVICE REQUIRED	YX
SERVICE COMPLETED	YZ
SPECIAL SIA EVENTS	
USER DURESS	HA
USER DURESS RESTORE	HR
ENET PANIC ALARM	PA

DESCRIPTION	CODE
ENET PANIC RESTORAL	PR
USER PANIC ALARM	PA
ENET FIRE ALARM	FA
ENET FIRE RESTORAL	FR
ENET MEDICAL ALARM	MA
ENET MEDICAL RESTORAL	MR
MDT PANIC	PA
MDT TILT	MA
MDT BELT CLIP	HA
MDT PANIC RESTORE	PR
MDT TILT RESTORE	MR
MDT BELT CLIP RESTORE	HR
RPA PANIC	PA
RPA PANIC RESTORE	PR
RPA HOLDUP	HA
RPA HOLDUP RESTORE	HR
USER CODE CHANGE	JV
CODE DELETED	
NON-STANDARD SIA CODES FOR ZONE STATE REPORTING	
ZONE OPEN	ZO
ZONE CLOSE	ZC
ZONE SHORT	ZX
ZONE DISCON	ZD
ZONE MASKED	ZM
ZONE WALKED	TP
WALKTEST START	ZK
WALKTEST END	TC
ZONE LOW BATT	XT
ZONE LOW BATTERY RESTORAL	XR
OTHER NON-STANDARD SIA CODES	
CAMERA ONLINE	CU
CAMERA OFFLINE	CV
ALERT CLOSE	SD
ALERT REOPEN	SO
XBUS ALERT CLOSE	NB
XBUS ALERT REOPEN	NO
UNKNOWN CARD	AU
USER ACCESSING	JP
USER ACCESSING END	ZG
LOW VOLTAGE	XD
LOW VOLTAGE RESTORAL	XG

DESCRIPTION	CODE
DEEP CHARGE	XK
LOCKED OUT	WW

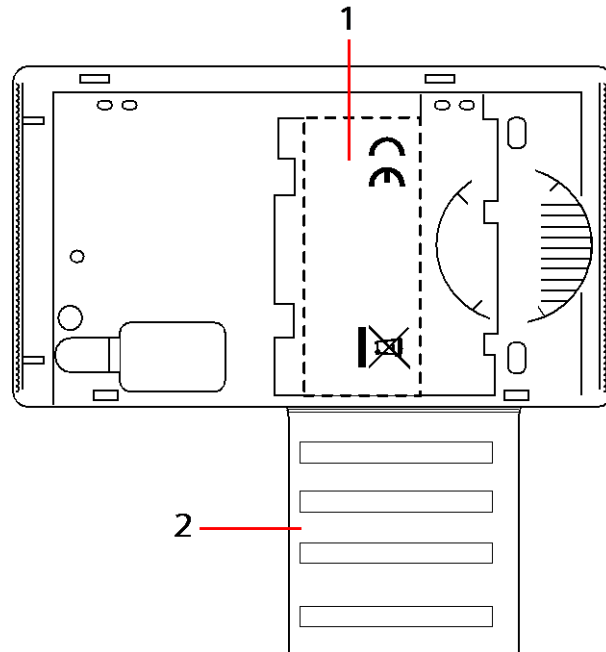
23.8 CID Codes

CODE	CID EVENT	DESCRIPTION
100	MEDICAL	Medical and man down alarm and restore.
110	FIRE	
120	PANIC	
121	DURESS	
129	CONFIRMED HOLDUP	See Configuration requirements for PD 6662:2010 conformance [→ 26]
130	BURGLARY	
134	ENTRYEXIT	
137	TAMPER	Cabinet and auxiliary tamper fail and restore.
139	VERIFIED	Confirmed alarm.
144	SENSOR TAMPER	Zone tamper fail and restore.
150	NON BURGLARY	
300	SYSTEM TROUBLE	PSU fault and restore.
301	AC LOSS	PSU mains fail and restore.
302	BATTERY LOW	
305	RESET	System reset.
311	BATTERY FAIL	PSU battery fail and restore.
312	PSU OVERCURRENT	PSU internal, external and auxiliary fuse fail and restore.
320	SOUNDER	Bell tamper fail and restore.
330	SYSTEM PERIPHERAL TROUBLE	PSU fault and restore.
333	EXP FAIL	X-Bus cable and node communications fault and restore.
338	EXP BATT	X-Bus node battery fault and restore.
341	EXP TAMPER	X-Bus tamper and RF antenna tamper alarm and restore.
342	EXP AC	X-Bus node mains fault and restore.
344	RF JAM	RF jam fault and restore.
351	TELCO 1	Primary modem fault and restore.
352	TELCO 2	Secondary modem fault and restore.
376	HOLDUP TROUBLE	
380	SENSOR TROUBLE	
401	OPENCLOSE	Unset, post alarm and fullset.
406	ALARM ABORT	Cancel alarm.
451	EARLY OPENCLOSE	

452	LATE OPENCLOSE	
453	FAIL TO OPEN	Late to unset.
454	FAIL TO CLOSE	Late to set.
456	EVENT PARTSET	Partset A and B.
461	CODETAMPER	User code tamper.
466	SERVICE	Engineer mode enabled and disabled.
570	BYPASS	Zone inhibited and uninhibited, zone isolated and un-isolated.
601	MANUAL TEST	Modem manual test.
602	AUTO TEST	Modem automatic test.
607	WALK TEST	
613	ZONE WALKED	
614	FIRE ZONE WALKED	
615	PANIC ZONE WALKED	
625	TIME RESET	Time set.

23.9 Overview of keypad types

Keypad type	Model no.	Basic Functionality	Proximity Detection	Audio
Standard Keypad	SPCK420	✓	-	-
Keypad with PACE	SPCK421	✓	✓	-
Comfort Keypad	SPCK620	✓		-
Comfort Keypad with Audio/CR	SPCK623	✓	✓	✓



Keypad Label SPCK420/421

1	Label on inside of Keypad
2	Pull-down label for providing installer details. Fill in all relevant details when installation is complete.

23.10 User PIN combinations

The system supports 4, 5, 6, 7 or 8 PIN Digits for each user (User or Engineer PINs). The maximum number of logical combinations/variations for each number of PIN digits can be found in the table below.

Number of digits	Number of variations	Last valid user codes
4	10,000	9999
5	100,000	99999
6	1,000,000	999999
7	10,000,000	9999999
8	100,000,000	99999999

The maximum number of logical combinations/variations is calculated by:

$10^{\text{No of digits}} = \text{Number of variations (including the User or Engineer PIN)}$

Note: To comply with INCERT approvals, the user's PIN code must contain more than 4 digits.



The default Engineer PIN is 1111. See Engineer PINs [→ 102] for more details.

23.11 Duress PINs

A user PIN with duress cannot be configured for the last user PIN in an allocation of PINs for a specific number of PIN digits. Configuring duress with 'PIN+1' or 'PIN+2' requires either 1 or 2 additional PINs to be available after a specific PIN. For example, for an allocation of 4 digit PINs, the total number of PINs available is 10,000 (0 – 9999), in this case, if using 'PIN +1' duress configuration, the last user PIN that can be allocated duress is 9998. If 'PIN+2' is used then 9997 is the last user PIN that can be allocated duress.

Also, if the duress feature is enabled then consecutive user codes (i.e. 2906, 2907) are not permitted, as entering this code from the keypad would activate a user duress event.

Once the system is configured for PIN +1 or PIN +2 in System Options [→ 222] and specific users enabled for duress (see Users [→ 183]), it **must** not be changed unless all the users are deleted and re-allocated user PINs.

23.12 Automatic inhibits

The system supports automatic inhibits in the following instances.

23.12.1 Zones

When the UK & Commercial are selected (see Standards [→ 234]), the system will provide DD243 functionality. In this instance the system will inhibit zones under the following conditions:

- Entry zone will not cause an alarm signal to the central station and cannot be part of a confirmed alarm and hence will be effectively inhibited as required by DD243.
- If a single zone is triggered and another zone is not triggered within the confirmation time (30 min default) but the first zone is still triggered, then the first zone will be automatically be inhibited and no further alarms will be triggered from this zone during the set period.

23.12.2 Access PINs

For Grade 2 systems: After 10 unsuccessful attempts with the incorrect PIN, the keypad or browser will be disabled for 90 s; after a further 10 attempts with the incorrect PIN, the keypad or browser will be disabled for a further 90 s. Once a correct PIN has been entered, it will reset the counter back to zero allowing for a further 10 attempts before disablement.

For Grade 3 systems: After 10 unsuccessful attempts with the incorrect PIN, the keypad or browser will be disabled for 90 s; after each further attempt with an incorrect PIN the keypad or browser will be disabled for a further 90 s. Once a correct PIN has been entered it will reset the counter back to zero allowing for a further 10 attempts before disablement.

23.12.3 Engineer Access

An Engineer can only access the system if permitted by a 'Manager' user type (see 'Engineer' attribute in User Rights) and only for a specified time duration (see 'Engineer Access' in Timers [→ 230]).

23.12.4 Keypad User Logoff

If no keys are pressed on a keypad for a specific duration (see 'Keypad Timeout' in Timers [→ 230]), the user is automatically logged off.

23.13 Wiring of mains cable to the controller

Requirements:

A readily accessible approved disconnect device must be incorporated in the building installation wiring. This must disconnect both phases at the same time. Acceptable devices are switches, circuit breakers, or similar devices

- The disconnect device must have at least 3 mm distance between the contacts
- Minimum size conductor used for connecting mains is 1.5 mm square
- The circuit breakers must have a maximum rating of 16 A

The mains cable is secured to the metal V shaped bend in the base plate via a tie wrap such that the metal bend is between the cable and the tie wrap. Ensure that the tie wrap is applied to the supplementary insulation of the mains cable i.e. the outer PVC cable sleeve. The tie wrap must be pulled extremely tightly such that when the cable is tugged there is no movement in the cable relative to the tie wrap.

The Protective Earthing conductor should be fitted to the terminal block in such a way that if the mains cable should slip in its anchorage, placing a strain on the conductors, the Protective Earthing conductor will be the last item to take the strain.

The mains cable must be an approved type and marked HO5 VV-F or HO5 VVH2-F2.

The plastic tie wrap must be flammability rated V-1.

23.14 Maintenance controller

The system should be serviced in accordance with the service schedule that is in place. The only replaceable parts on the controller are the mains fuse, standby battery and the time & date battery (PCB mounted).

It is recommended that during a service the following be checked:

- The Event Log to check if any standby battery tests have failed since last service – if standby battery tests have failed then the standby battery should be checked.
- The standby battery should be replaced as per the servicing schedule to ensure that it has sufficient capacity to hold the system up for the time defined in the system design. The battery should be physically inspected for any deformation of the casing or any sign of leakage; if any of these conditions exist the battery should be immediately replaced.



NOTICE

The new battery should be of the same capacity or greater (up to the maximum the system can accommodate).

- If the main fuse blows then the system should be checked for any reasons. The fuse should be replaced by a fuse with the same rating. The rating is stated on the system label in the rear of the cabinet.
- The time & date onboard PCB lithium battery is only used when the system is left un-powered; in this state that battery has a life of approximately 5 years. The battery should be visually checked once a year and all power removed from the system to ensure that system retains the time & date. If the system does not retain the time and date the battery should be replaced with a new Lithium cell type CR1216.
- All electrical connections should be checked to ensure that the insulation is in place and there is no risk of shorting or becoming disconnected.
- It is also recommended that any firmware update release notes be checked for any additional updates that may improve the security of the system.


- Check all physical mountings are intact. Any broken mountings should be replaced with the same parts.

23.15 Maintenance Smart PSU

The system should be serviced in accordance with the service schedule that is in place. The only replaceable parts on the Smart PSU are the mains fuse and standby battery.

It is recommended that during a service the following be checked:

- The controller Event Log to check if any standby battery tests have failed since last service – if standby battery tests have failed then the standby battery should be checked.
- The standby battery should be replaced as per the servicing schedule to ensure that it has sufficient capacity to hold the system up for the time defined in the system design. The battery should be physically inspected for any deformation of the casing or any sign of leakage; if any of these conditions exist the battery should be immediately replaced.

	NOTICE
	The new battery should be of the same capacity or greater (up to the maximum the system can accommodate).

- Check the LEDs on the PSU control board are in the expected state. See Smart PSU document for LED details.
- If the main fuse blows then the system should be checked for any reasons. The fuse should be replaced by a fuse with the same rating. The rating is stated on the system label in the rear of the cabinet.
- All electrical connections should be checked to ensure that the insulation is in place and there is no risk of shorting or becoming disconnected.
- It is also recommended that any firmware update release notes be checked for any additional updates that may improve the security of the system.
- Check all physical mountings are intact. Any broken mountings should be replaced with the same parts.

23.16 Zone types

The zone types on the SPC system are programmable from both the browser and keypad. The table below gives a brief description of each zone type available on the SPC system. Each zone type activates its own unique output type (an internal flag or indicator) that can then be logged or assigned to a physical output for activation of a specific device if required.

Zone Type	Processing Category	Description
ALARM	Intruder	This zone type is the default zone type setting and is also the most frequently used zone type for standard installations. An Open, Disconnected, or Tamper activation in any mode (except unset) causes an immediate full alarm. In the Unset mode, Tamper conditions are logged, causing the alert message ZONE TAMPER and triggering a local alarm. In Partset A, Partset B and Full Set modes, all activity is logged.
ENTRY/EXIT	Intruder	This zone type should be assigned to all zones on an entry/exit route (i.e. a front door or other access area to the building or premises). This zone type provides an entry and exit time delay. The entry timer controls this delay. When the system is being full set, this zone type provides an exit delay allowing time to vacate an area. The

		exit timer controls this delay. In Part set A mode, this zone type is inactive.
EXIT TERMINATOR	Intruder	This zone type is used in conjunction with a push button on an exit route and acts as an exit terminator – that is, it provides an infinite exit delay period and will not allow the system to set until the button is pressed.
FIRE	Hold-up	Fire zones are 24-hour zones for fire monitoring and their response is independent of panel operating mode. When any fire zone opens, a full alarm is generated and the FIRE output type is activated. If the 'Report only' attribute is set then activation will only be reported to the central station and a Full Alarm will not be generated.
FIRE EXIT	Hold-up	This is a special type of 24-hour zone for use with fire exit doors that should never be opened. In Unset mode, an activation of this zone will trip the Fire-X output, causing alert messages.
LINE	Fault	Telemetry line monitoring input. This is usually used in conjunction with a telephone line health output from an external digital dialer or direct line communication system. When activated, it produces a local alarm in Unset mode and a full alarm in all other modes.
PANIC ALARM	Hold-up	This zone type is active on a 24-hour basis and activated via a panic button. When a Panic zone is activated it will report a Panic event, independent of panel arming mode. All activation's are logged and reported if log attribute is active. If the SILENT attribute is set then the alarm will be silent (Activation is reported to ARC), otherwise it will generate a Full alarm.
HOLD-UP ALARM	Hold-up	This zone type is active on a 24-hour basis and activated via a button. When a Hold-up zone is activated it will report a Hold-up event, independent of panel arming mode. The SILENT attribute is set by default therefore the alarm will be silent. If unset, it will generate a full alarm. All activations are logged and reported if log attribute is active.
TAMPER	Tamper	When open in the Unset mode, a Local Alarm is generated but no external bell will activate. If the system is Full Set, a Full alarm is generated. If the Security Grade of the system is set to Grade 3 then an engineer code is required to restore the alarm.
TECHNICAL	Intruder	The tech zone controls a dedicated tech zone output. When a tech zone changes state, the tech zone output will follow. That is: <ul style="list-style-type: none"> ● When the tech zone opens, tech zone o/p triggers on ● When the tech zone closes, tech zone o/p goes off If more than one tech zone has been assigned, the tech zone output will remain on until all tech zones are closed.
MEDICAL	Hold-up	This zone type is used in conjunction with radio or hardwired medical switches. Activation in any mode will: <ul style="list-style-type: none"> ● Trigger the medical digital communicator output (unless Local attribute is set) ● Cause the panel buzzer to sound (unless Silent attribute is set) ● Display the message Medic Alarm
KEYARM	Intruder	This zone type is normally used in conjunction with a key lock mechanism. A Keyarm zone will SET the System / Area / Common Areas when it is OPENED and will UNSET the System/Area/Common Areas when it is CLOSED. <ul style="list-style-type: none"> ● If the zone with the keyarm zone type is assigned in a non area system then the keyarm operation will SET/UNSET the system. ● If the zone with the keyarm zone type is assigned to an area then the keyarm operation will SET/UNSET the area. ● If the zone with the keyarm zone type is assigned to a common area then the keyarm operation will SET/UNSET all the areas in the common area. ● If the 'Open only' attribute is set then the armed status of the System / Area / Common Areas will toggle on each opening of the key lock. (

		<p>i.e. Open once to SET the system, Close and Open again to UNSET)</p> <ul style="list-style-type: none"> ● If the 'Fullset Enable' attribute is set then zone activation will only Fullset the system. ● If the 'Unset Enable' attribute is set then zone activation will only unset the system. <p>Keyarming will force set the system/area and auto-inhibit any open zones or fault conditions.</p> <p>Note: Your system will not comply with EN standards if you enable this zone type to set the system without first entering a valid PIN on an external device.</p>
SHUNT	Intruder	<p>This zone type is only available in Commercial Mode of operation. Though the Shunt Alarm Zone type can be set in Domestic Mode of operation, it has no effect.</p> <p>This zone type when opened inhibits all zones that have the shunt attribute set. This operation applies for both SET and UNSET modes. As soon as the shunt zone is closed, the zones with the shunt attribute set will become un-inhibited again.</p>
X-SHUNT	Intruder	<p>This zone type is only available in Commercial Mode of operation.</p> <p>A zone programmed with the x-shunt zone type inhibits the next consecutive zone on the system whenever it is opened. This operation applies for both SET and UNSET modes. As soon as the x-shunt zone type is closed the next zone becomes de-inhibited again.</p>
DETECTOR FAULT	Fault	<p>Detector Fault zones are 24 hour zones that are applicable to a detector device, for example, a PIR. The fault zone type triggers the Fault output.</p> <p>When the system is armed, a fault output is triggered. Both the keypad LED and the buzzer are activated when Unarmed.</p>
LOCK SUPERVISION	Intruder	<p>Only available in Commercial mode.</p> <p>Used to monitor a door lock. System can be programmed not to set unless door is locked.</p>
SEISMIC	Intruder	<p>Only available if the panel is in Financial mode of operation. Vibration sensors, also called seismic sensors, are used to detect intrusion attempts by mechanical means, such as drilling or making holes through walls or safes.</p>
ALL OKAY	Intruder	<p>This zone type enables a special entry procedure to be implemented using a user code and 'All Okay' input. A silent alarm is generated if an All Okay button is not pressed within a configurable time after a user code is entered. (See Areas [→ 238] for details of 'All Okay' configuration)</p> <p>All Okay uses two outputs, Entry Status (Green LED) and Warning Status (Red LED), to indicate entry status using LEDs on the keypad.</p>
UNUSED	Intruder	<p>Allows a zone to be disabled without the need for each zone to have EOL resistors fitted. Any activation on the zone will be ignored.</p>
HOLDUP FAULT	Fault	<p>Holdup Fault zones are 24 hour zones that are applicable to a holdup signaling device, for example, a WPA. The fault zone type triggers the Fault output.</p> <p>When the system is armed, a fault output is triggered. Both the keypad LED and the buzzer are activated when Unarmed.</p> <p>This zone type will report the SIA messages, HT (Holdup Trouble) and HJ (Holdup Trouble Restore) and for CID, a sensor trouble event (380) is produced.</p>
WARNING FAULT	Fault	<p>Warning Fault zones are 24 hour zones that are applicable to a warning signaling device, for example, an internal or external bell. The fault zone type triggers the Fault output.</p> <p>When the system is armed, a fault output is triggered. Both the keypad LED and the buzzer are activated when Unarmed.</p> <p>This zone type will report the SIA messages, YA (Bell Fault) and YH (Bell Restore) and for CID, a sensor trouble event (380) is produced.</p> <p>Note: On a grade 2 system, a cable fault will cause a fault and not an</p>

		alarm.
SETTING AUTHORISATION.	Intruder	Applicable to Blockschloss operation. This zone type is used to send a setting authorisation signal to the panel that the Blockschloss is ready to set. The Set option must be selected for the 'Setting Authorisation' attribute for the area
LOCK ELEMENT	Intruder	If using a Lock Element (bolt) with a Blockschloss, this zone type signals the position of the lock element to the panel (locked or unlocked). This bolt locks the door in the set state. This signal is checked during setting process. If the 'locked' information is not received, the setting will fail.
GLASSBREAK	Intruder	<p>Zone is connected to an RI S 10 D-RS-LED glassbreak interface in combination with GB2001 glassbreak detectors.</p> <ul style="list-style-type: none"> ● This zone type is available on controllers and expanders. It is not available as wireless or as a door zone type if the DC2 is configured as a door. ● The zone type reports in the same way as an alarm zone over SIA and contact ID. ● The rights to restore/inhibit/isolate glassbreak are the same as the alarm zone type ● Power up condition — As the power is supplied by the panel any state changes within the first 10 seconds are ignored in order to allow the device to settle. ● Reset condition — Signals are ignored from the glassbreak interface for 3 seconds after the device has been reset. ● Exiting engineer mode — The glassbreak output may be toggled when exiting engineer mode, in which case the signals from this sensor will be temporarily ignored for 3 seconds.

23.17 Zone attributes

The zone attributes on the SPC system determine the manner in which the programmed zone types function.

Zone attribute	Description
Access	<p>When the 'Access' attribute on a zone is set, then on opening that zone, an alarm will not be generated if either the entry or exit timer is running. When the system is full set the Access attribute is not active and opening the zone will initiate a full alarm. The 'Access' attribute is most often used for PIR sensors located close to an entry/exit zone. It allows the user free movement within the access area while the entry or exit timer is counting down.</p> <p>The 'Access' attribute is only valid for Alarm zone types.</p> <p>All connected devices (Bells - Internal & External, Buzzers, Strobe) are activated.</p> <p>NOTE: An alarm zone with Access attribute can automatically be changed to an entry/exit zone in Partset mode if the Partset Access Option is set.</p>
Exclude A	<p>If the 'Exclude A' attribute on a zone is set, then an alarm will not be generated by that zone opening while the panel is in the Partset A mode. The 'Exclude A' attribute is valid for Alarm zone type and Entry/Exit zones only.</p> <p>A FULL alarm is generated if a zone with the EXCLUDE A attribute is opened while the system is in FULLSET or PARTSET B Mode (Bells - Internal & External, Strobe).</p>
Exclude B	<p>When the 'Exclude B' attribute is set, the zone opening will not generate an alarm while the panel is in the Partset B mode. The 'Exclude B' attribute is valid for Alarm zone type and E/Exit zones only.</p> <p>A FULL alarm is generated if a zone with the EXCLUDE B attribute is opened while the system is in FULLSET or PARTSET A Mode (Bells - Internal & External, Strobe).</p>
24 Hour	If a Zone is assigned the '24 Hour' attribute, then it is active at all times and


	<p>will cause a full alarm if opened in any mode. This attribute can only be assigned to the ALARM zone type. Generates a FULL Alarm in UNSET, SET and PARTSET modes.</p> <p>NOTE: The 24 Hour attribute overrides the settings of any of the other attributes for a particular alarm zone.</p>
Local	<p>When the 'Local' attribute is set, an alarm generated by a zone opening will not result in the external reporting of the event. The 'Local' attribute is valid for Alarm, E/Exit, Fire, Fire Exit and Medic zone types.</p>
Unset Local	<p>When this attribute is set, an alarm generated by the zone opening when the area is fullset or partset will be reported in the usual way. However, if the area is unset there will be only a local alarm i.e keypad buzzer, LED flash and zone display. This attribute is only applicable to Alarm, Fire and Seismic zones.</p>
Double Knock	<p>Use this attribute to deal with troublesome detectors. (i.e. some detectors may generate activation signals spuriously, thereby inadvertently trigger alarms on the system).</p> <p>If the same double knock zone activates twice during the double knock period, then an alarm is generated. Double knock time is set in seconds (see page [→ 230]). Two open actions within that time period will generate an alarm. All open double knock zones are logged when the system is armed.</p>
Chime	<p>When the 'Chime' attribute is set for a zone, any opening of the zone during the Unset mode will cause the internal buzzers to activate for a short period (2 seconds approx.).</p> <p>The Chime attribute is valid for Alarm, Entry/Exit, and Tech. zones types.</p>
Inhibit	<p>When the 'Inhibit' attribute is set, a user may inhibit this zone. The inhibit operation will disable that fault or zone for one setting period only.</p>
Normal Open	<p>When the 'Normal Open' attribute is set, the system expects that a connected detector/sensor is a Normally Open device. (i.e. a sensor is deemed to be activated whenever the contacts are closed on the device).</p>
Silent	<p>If the 'Silent' attribute is set then there will be no audio or visual indications of the Alarm. The alarm activation will be sent to the Receiver station. If the system is unset then a warning message is shown on the display.</p>
Log	<p>If this attribute is set then all zone state changes are logged.</p>
Exit Open	<p>If set then zone will be indicated if open during setting.</p>
Frequent	<p>This attribute only applies to Remote Maintenance*. If this attribute is set for a zone, the zone must open for remote service purposes within the defined frequent time period.</p>
End of Line	<p>The End Of Line (EOL) attribute provides a number of input zone wiring configurations on the system.</p>
Analysed	<p>The Analysed Attribute must be set for a zone if that zone is wired with an inertia sensor. The Pulse count and Gross attack values should be programmed for each inertia sensor on the system in accordance with the results of a simple calibration of the device.</p>
Pulse Count	<p>Pulse count trigger level for analysed inertia sensors.</p>
Gross Attack	<p>Gross attack trigger level for analysed inertia sensors</p>
Final Exit	<p>The Final Exit attribute can only be assigned to an Entry/Exit Zone type. Use this attribute to override the standard process of counting down the exit timer whenever the system is full set. When all other entry/exit routes in the premises are closed, fullset the system and close the final exit/entry zone. As soon as the door is closed the Final Exit time will count down to setting the system.</p>
Shunt	<p>A zone with the shunt attribute set will be inhibited whenever a shunt type zone is opened. This provides a mechanism to group the inhibition of zones with the opening of the shunt zone type.</p>
Report Only	<p>This attribute only applies to the FIRE zone type. If this attribute is set, then activation of the fire zone will only report the activation to the central station. No alarms will be generated on site.</p>

Open Only	This attribute only applies to the KEYARM zone type. If set then the setting state of the building will toggle on openings only.
Fullset Enable	This attribute only applies to the KEYARM zone type. If this attribute is set then zone activation will Fullset the system/area. Apply this attribute if it is intended that the user should only have the ability to FULLSET the system from a keyarm zone.
Unset Enable	This attribute only applies to the KEYARM zone type. If set then zone activation will Unset the system/area. Apply this attribute if it is intended that the user should only have the ability to UNSET the system from a keyarm zone.
Tech Zone Report	Allows a zone when opened, regardless of the mode to send an alarm to the ARC in FF, CID, SIA and SIA extended. When areas are selected, the alarm will only be sent to the ARC to which the area has been assigned to. This would be a "UA" Unknown Alarm followed by the zone number and text if SIA extended is selected. It will also send an SMS to the end user and engineer if select to do so when the unconfirmed alarm filter is selected.
Tech Zone Display	Allows an opening zone to be displayed on the system keypad. The alert led should also activate. When areas are selected it will only be displayed on the keypad which is assigned to the area in which the zone has been selected. The alert may only be displayed on the keypad when the area is in the unset mode and not in the Part A, Part B and set mode.
Tech Zone Audible	Allows an activated zone to operate the buzzer. This will operate the same as the Tech Zone Display in the different setting modes and on systems with areas.
Tech Zone Delay	Allows the zone to have a programmable delay. The delay is variable from 0 to 9999 seconds and will apply to all Tech Zones. The operation is the same as the Mains Delay timer, if the zone is closed within the delay time, then no alarm is sent to the ARC, no SMS is sent to the user and the Technical Output will not trip. NOTE: The Technical Output will not trip until the delay timer has expired.
Armed report only	Openings are reported only in armed mode.
Fire pre-alarm	If enabled and a fire alarm occurs, a Fire Pre-alarm timer is started and internal bells and buzzers are activated. (See Timers [→ 230].) If the alarm is not cancelled within the timer duration, a fire alarm is confirmed, internal and external bells are triggered and an event is sent to ARC.
Fire Recognition	If enabled, a Fire Recognition timer is activated which adds extra time to the Fire Pre-alarm timer duration until a fire alarm is reported for the zone. See Timers [→ 230].
Seismic Test/Automatic Sensor Test	A Seismic zone type may be tested manually or automatically. This attribute allows automatic testing to be enabled. Refer to the section on timers [→ 230] for details of how to configure the timer that determines how often the panel tests any seismic zones that have this attribute set. The default value for the timer is 7 days.
Timed	The 'Timed' attribute is used for Key Arm zones to delay the setting of an area. The delay follows the exit timer for the area to which the key arm is associated.
Verification	Select the configured verification zone to assign to this zone to trigger audio/video verification.
Force Set	If enabled, the keyarm device can set the system, automatically inhibiting all open zones.

23.18 Applicable attributes to zone types

The following table shows which attributes are applicable to each zone type:

Zone Type																									
	Alarm	Entry/Exit	Exit Term	Fire	Fire Exit	Line	Panic	Holdup	Tamper	Tech	Medical	Keyarm	Unused	Shunt	X-Shunt	Detector Fault	Lock Supervision	Seismic **	All Okay	Hold-up Fault	Warning Fault	Setting Authorisation	Lock Element	Glass Break	
Access	v																							v	
Exclude A	v	v																						v	v
Exclude B	v	v																						v	v
24 Hour	v																	v						v	
Local	v	v		v	v						v						v				v	v		v	v
Unset Local	v			v															v					v	
Double Knock	v																							v	
Chime	v	v									v												v	v	
Inhibit	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v		v	v	
Normal Open	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v	v	v	v	v
Silent	v						v	v																	v
Log	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v	v	v	v	v
Shunt	v	v			v																				v
Frequent *	v	v	v							v		v		v	v										v
Analyzed	v	v			v																				
Pulse Count	v	v			v																				
Gross attack	v	v			v																				
Calendar	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v	v	v	v	v
Verification	v	v		v	v		v	v		v	v								v						v
Exit Open		v																							
Seismic Test																			v						
Timed												v													
Report Only				v																					
Open Only													v										v		
Final Exit		v																							v
Fullset enable													v												
Unset enable													v												
Shunt	v	v			v																				v
Report (Tech)											v														
Display(Tech)											v														
Audible (Tech)											v														
Delay (Tech)											v														
Report When Set											v														
Fire Pre-alarm				v	v																				
Fire Recognition				v	v																				
Force set												v													

 Only available in Commercial Mode.
 * Only in conjunction with Remote Maintenance.
 ** Only available in Financial Mode

23.19 ATS levels and attenuation specifications

ATS (Alarm Transmission System) Levels

The following table lists the ATS levels required for the panel when communicating over:

- GSM to Alarm Reporting Centre (ARC)
- PSTN to Alarm Reporting Centre (ARC)
- Ethernet to SPC Comm receiver software
- GPRS to SPC Comm receiver software

	GSM ARC	PSTN ARC	Ethernet	GPRS
ATS Level	ATS 2	ATS 2	ATS 6	ATS 5

Attenuation of PSTN

For a PSTN dialer, a CW1308 Internal Telecom or equivalent cable should be used to connect the modem to the phone line. The cable length should be between 0.5 – 100m.

Attenuation of Ethernet

For Ethernet, a Cat 5 cable should be used with its length between 0.5 – 100m.

Attenuation of GSM

The field strength of the GSM signal needs to at least -95dB. Below this level the modem will flag a low signal fault to the panel. This is handled in the same way as other faults on the system.

Monitoring and watchdog of PSTN (SPCN110) and GSM (SPCN310)

A failure of the interface between the PSTN modem and the panel will be detected after 30 seconds, after which an ATS fault will occur.

A failure of the interface between the GSM modem and the panel will be detected after 30 seconds, after which an ATS fault will occur.

23.20 Supported card readers and card formats

The following card readers and formats are supported on the SPC system:

Reader	Card Format
HD500-EM PR500-EM SP500-EM PM500-EM	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
AR6181-RX AR6182-RX	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG

Reader	Card Format
	ABR5100-PR
HD500-Cotag PR500-Cotag SP500-Cotag PM500-Cotag HF500-Cotag	IB928 IB911 IB968 IB961 IB958M
PP500-Cotag	IB928 IB911 IB968 IB961 IB958M
PP500-EM	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
AR6181-MX AR6182-MX	ABP5100-BL Mifare Classic 1K ABR5100-PR Mifare Classic 4K
iClass R10 iClass R15 iClass R30 iClass R40 iClassRK40	ABP5100-BL Default 32 bit MiFare Only
MultiClass RP40 MultiClass RP15 MultiClass RPK40	ABP5100-BL Default 32 bit MiFare Only IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
HID Prox Pro	26 bit Wiegand EPX 36 bit Wiegand

Site codes and restrictions

Reader Format	Side Code Available	Restrictions
EM4102	No	Max card no. 9999999999
COTAG	No	Max card no. 9999999999
Wiegand 26 bit	Yes	Max site code. 255 Max card no. 65535
Wiegand 36 bit	Yes	Max site code.. 32767 Max card no. 524287
HID Corporate 1000	Yes	Max site code.. 4095 Max card no.. 1048575

Reader Format	Side Code Available	Restrictions
HID 37	No	Max card no. 34359738370
HID 37F	Yes	Max site code. 65535 Max card no. 5242875
HID 37BCD	No	Max card no. 99999999
HID ICLASS MIFARE	No	Max card no. 4294967295
HID ICLASS DESFIRE	No	Encrypted card number. Max card no. 72×10^{16} . This number must be learned on the panel
AR618 WIE BCD 52 BIT	No	Max card no. 4294967295
AR618 OMRON 80 BIT	No	Max card no. 999999999999

23.21 SPC Support for E-Bus Devices

The SPC E-Bus Gateway (SPCG310) is an X-Bus expander that enables communication between an SPC controller and Sintony E-Bus devices. Sintony E-BUS addressing permits duplicate addresses for E-Bus devices across different E-BUS sections. X-Bus devices require unique addresses. To support this conflict, E-BUS peripheral readdressing may be required. For more information, see ADDRESSING MODE [→ 128].



NOTICE

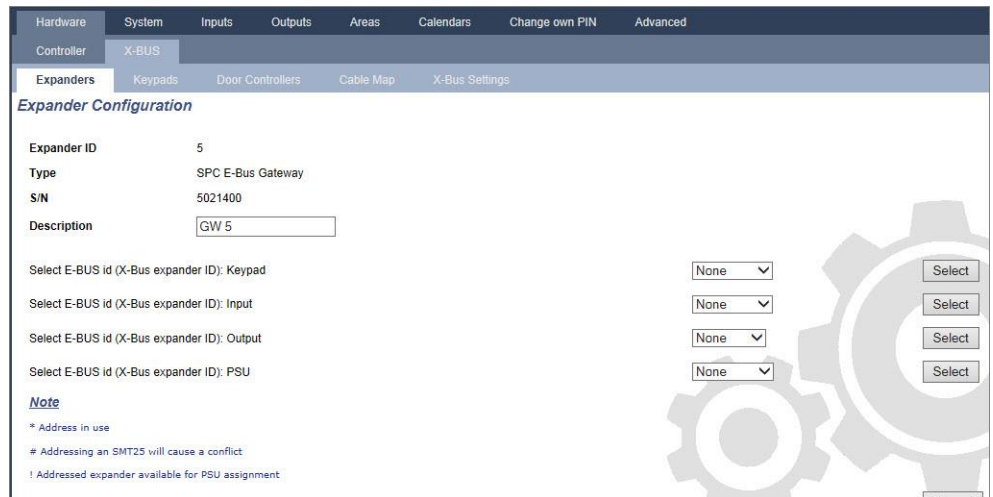
Vanderbilt recommends you read the **Sintony System Migration** document before configuring E-Bus devices.

23.21.1 Configuring and Addressing E-Bus Devices

You can configure and address the following Sintony E-Bus devices to communicate with the SPC controller:

- Sintony keypads
- Sintony input transponders
- Sintony output transponders
- Sintony PSUs: SAP 8, SAP 14, SAP 20, and SAP 25

1. In the browser, go to **Settings - X-BUS - Expanders**.
⇒ A list of **Configured Expanders** displays.
2. Select an **SPC E-Bus Gateway**.
3. In the **Expander Configuration** screen, enter a **Description** for the **SPC E-Bus Gateway**. For more information on configuring expanders, see Expanders [→ 204].



4. To address an E-Bus device, select an ID from the relevant dropdown menu described in the table below. An asterisk (*) prefixes an ID that is in use. You cannot select this ID.
5. Click the **Select** button.
 - ⇒ Address in progress.....Reconfiguration of Xbus will be required displays at the top of the screen.
 - ⇒ The SPC E-Bus Gateway beeps repeatedly.
6. Depending on the E-Bus device, hold the addressing button as described in the **Addressing** column in the table below.
 - ⇒ The SPC E-Bus Gateway beeps continuously to indicate the ID is now associated with the E-Bus device.
7. Go to **Settings - X-BUS - Expanders**.
8. Click the **Reconfigure** button.
 - ⇒ Reconfiguration completed displays at the top of the screen. E-Bus inputs and outputs display in the list of **Configured Expanders**. If an input transponder has an associated PSU, the PSU type displays in the **PSU** column. Keypads display in the list of **Configured Keypads**.
9. To complete the manual addressing steps to add the SAP 8, SAP 14, and SAP 20 PSU devices to the list of **Configured Expanders**, see Addressing Transponders for SAP 8, SAP 14, and SAP 20 [→ 358].
10. If the X-BUS has addressing conflicts, the warning *Invalid* or *Duplicate ID for Expander IDx* displays. Repeat the addressing steps above until there is no addressing conflict.

E-Bus Device: Dropdown Menu	Description	ID Format	Addressing
Keypad	IDs to assign to Sintony keypads	E-BUS ID (X-BUS ID)	Hold keys 1 and 3 simultaneously until the SPC E-Bus Gateway beeps continuously.
Input	IDs to assign to Sintony input transponders	E-BUS ID (X-BUS ID)	Hold the addressing button for 5 seconds and release to hear a continuous beep.
Output	IDs to assign to Sintony output transponders	E-BUS ID (X-BUS ID)	Hold the addressing button for 5 seconds

			and release to hear the SPC E-Bus Gateway beeps continuously.
PSU	IDs to assign to Sintony PSU devices SAP 8, SAP 14, SAP 20, and SAP 25	E-BUS ID (X-BUS ID of associated transponder)	Hold the addressing button until the SPC E-Bus Gateway beeps continuously..

See also

 ADDRESSING MODE [→ 128]

23.21.1.1 Addressing Transponders for SAP 8, SAP 14, and SAP 20

After assigning a PSU ID to an SAP 8, SAP 14, or SAP 20, see *Configuring and Addressing E-Bus Devices* [→ 356], you must assign an input transponder to the PSU. This simulates communication to the SPC controller via an expander.

1. In the **Configured Expanders** list, select the **SPC E-Bus Gateway**.
 - ⇒ The **Expander Configuration** screen displays.
2. From the dropdown list, view the newly assigned PSU ID.
 - ⇒ An exclamation mark (!) prefixes the PSU ID you assigned to the device. This indicates that there is an input transponder available to assign to the PSU.
3. Take a note of the number in brackets next to the PSU ID. This number is the ID you must assign to the input transponder. For example, if the PSU ID is **ID 14 (27)**, you must manually select a transponder with **ID 27** from the **Input** dropdown list.
4. From the **Input** dropdown list, select the transponder ID indicated in brackets next to the PSU ID.
5. Click the **Select** button.
6. Go to **Settings - X-BUS - Expanders**.
7. Click **Reconfigure**.
 - ⇒ The PSU device displays in the list of **Configured Expanders**.

23.21.1.2 Addressing Transponders for PSU SAP 25

The Sintony PSU SAP 25 has two internal transponders. Each transponder requires an ID. These two IDs are assigned automatically when you complete the addressing steps described in *Configuring and Addressing E-Bus Devices* [→ 356]. The formula $2n - 1$ applies where n is the value of the PSU ID. For example, if you assign ID 10 to an SAP 25, each transponder will be assigned the X-BUS IDs 19 and 20.

!	NOTICE
	In the PSU dropdown list, a hash (#) symbol prefixes an SAP 25 ID to indicate that the automatic addressing of transponders will conflict with existing input transponders. To resolve this conflict, you must readdress one of the conflicting devices.

23.22 FlexC Glossary

Acronym	EN50136-1 Description	FlexC Example
AE	Annunciation Equipment Equipment located at an ARC which secures and displays the alarm status, or the changed alarm status of ASs in response to the receipt of incoming alarms before sending a confirmation. The AE is not part of the ATS.	SPC Com XT Client
ARC	Alarm Receiving Centre Continuously manned centre to which information concerning the status of one or more AS is reported.	SPC Com XT would be installed in an ARC.
AS	Alarm System Electrical installation, which responds to the manual or automatic detection of the presence of a hazard. The AS is not part of the ATS.	SPC Panel
ATE	Alarm Transmission Equipment Collective term to describe SPT, MCT (Monitoring Centre Transceiver) and RCT.	-
ATP	Alarm Transmission Path Route an alarm message travels between an individual AS and its associated AE. The ATP starts at the interface between AS and SPT and ends at the interface between RCT and AE. For notification and surveillance purposes the reverse direction may also be used.	A defined path between the SPC panel and SPC Com XT. e.g. A system with ethernet as the primary path and GPRS as a backup path would be two separate ATPs of an ATS.
ATS	Alarm Transmission System ATE and networks used to transfer information concerned with the state of one or more ASs at a supervised premises to one or more AEs of one or more ARCs. An ATS may consist of more than one ATP.	A system combining one or multiple paths between SPC panel and SPC Com XT.
RCT	Receiving Centre Transceiver ATE at the ARC including the interface to one or more AE(s) and the interface to one or more transmission networks and being part of one or more ATPs. In some systems this transceiver may be able to indicate changes of the status of an AS and to store log-files. This may be needed to increase the ATS availability in case of AE failure.	SPC Com XT Server
SPT	Supervised Premises Transceiver ATE at the supervised premises including the interface to the AS and the interface to one or more transmission networks and being	Integrated onto SPC Panel using Ethernet, GPRS, PPP over PSTN.

	part of one or more ATPs.	
--	---------------------------	--

FlexC also uses the following acronyms.

Acronym	Description
ASP	Analogue Security Protocols The analogue security protocols traditionally used for alarm transmission over the telephone network e.g. SIA, Contact ID.

23.23 FlexC Commands

The following table lists the commands that you can enable for a command profile. The command profile you assign to an ATS defines how you can control a panel from SPC Com XT.

Command Filter	Commands
System Commands	Get Panel Summary
	Set the System Time and Date
	Grant Engineer Access
	Grant Manufacturing Access
Intruder Commands	Get the Area Status
	Get the Change Mode Status of an Area
	Change the mode (Set/Unset) of an Area
	Get Status of Panel Alerts
	Perform actions on Alerts
	Silence Bells
	Get Zone Status
	Control a Zone
	Get the System Log
	Get the Log for a Zone
	Get the Wireless Log
Output Commands	Get Mapping Gate Status
	Control Mapping Gates
User Commands	Verify a User on the Panel
	Get a User Configuration
	Add a User
	Edit a User
	Delete a User
	Get a User Profile Configuration
	Add a User Profile
	Edit a User Profile
	Delete a User Profile
Change a User's own PIN	
Calendar Commands	Read Calendar Configuration
	Add a Calendar
	Edit a Calendar
	Edit a Calendar Week

	Delete a Calendar
	Add a Calendar Exception Day
	Edit a Calendar Exception Day
	Delete a Calendar Exception Day
Communication Commands	Get the status of the Ethernet
	Get the status of a modem
	Get the log for a modem
	Get the log for a ARC receiver
FlexC Commands	Get the status of a FlexC ATS
	Get the Network Log for a FlexC ATS
	Get the Event Log for a FlexC ATS
	Get the log for a FlexC ATP
	Get the Network log for a FlexC ATP
	Export a FlexC ATS configuration file
	Import a FlexC ATS configuration file
	Delete a FlexC ATS
	Delete a FlexC ATP
	Delete a FlexC Event Profile
	Delete a FlexC Command Profile
	Request a testcall for a FlexC ATP
Access Control Commands	Get the Configuration for a Door
	Read the Status for a Door
	Control a Door
	Get the Access Log
Verification Commands	Read a Camera Image
	Get the Status of a Verification Zone
	Get the data for a Verification Zone
	Send data to a Verification Zone
Virtual Keypad Commands	Control keypad
File Commands	Upgrade the Panel Firmware
	Upgrade Peripheral Firmware
	Upload a File
	Download a File
	Saves the Panel Configuration
	Reset the Panel
Legacy Commands	Get Panel Info
	Get Panel Status
	Get Headers of Configuration Files
	Get Language Configuration
	Get Intruder Configuration
	Get Status of X-BUS Devices
	Get the Area Configuration

23.24 ATS Category Timings

This table describes the EN50136-1 ATS Category Timings laid down in the standard and how the FlexC implementation meets these standards under the categories SP1-SP6, DP1-DP4.

		EN50136-1 ATS Category Timing Requirements				FlexC Implementation of ATS Category Timing Requirements			
ATS Category	Default Interfaces	Event Timeout	Primary Polling Timeout	Backup ATP Polling Timeout (Primary OK)	Backup ATP Polling Timeout (Primary Down)	Event Timeout	Primary Polling Timeout	Backup ATP Polling Timeout (Primary OK)	Backup ATP Polling Timeout (Primary Down)
SP1	Cat 1 [Ethernet]	8 min	32 days	-	-	2 min	30 days	-	-
SP2	Cat 2 [Ethernet]	2 min	25 hr	-	-	2 min	24 hr	-	-
SP3	Cat 3 [Ethernet]	60 s	30 min	-	-	60 s	30 min	-	-
SP4	Cat 4 [Ethernet]	60 s	3 min	-	-	60 s	3 min	-	-
SP5	Cat 5 [Ethernet]	30 s	90 s	-	-	30 s	90 s	-	-
SP6	Cat 6 [Ethernet]	30 s	20 s	-	-	30 s	20 s	-	-
DP1	Cat 2 [Ethernet] Cat 2 [Modem]	2 min	25 hr	50 hr	25 hr	2 min	24 hr	24 hr 30 min	24 hr 10 min
DP2	Cat 3 [Ethernet] Cat 3 [Modem]	60 s	30 min	25 hr	30 min	60 s	30 min	24 hr 30 min	30 min
DP3	Cat 4 [Ethernet] Cat 4 [Modem]	60 s	3 min	25 hr	3 min	60 s	3 min	24 hr 30 min	3 min
DP4	Cat 5 [Ethernet] Cat 5 [Modem]	30 s	90 s	5 hr	90 s	30 s	90 s	4 hr 10 min	90 s

23.25 ATP Category Timings

The following table shows the settings applied for event timeouts, polling intervals (active and non-active) and polling timeouts (active and non-active) for each ATP category. For the purpose of ethernet, polling interval and retry interval are identical. To reduce costs related to GPRS calls, the interval and retry interval for GPRS paths differ, for example, Cat 3 [Modem] polls once every 25 minutes and thereafter it polls every 60s for 5 minutes until it times out after 30 minutes. For a visual overview of the configured polling interval, go to **Status - FlexC - Network Log**.



If an ATP is up and active and then goes down, it will remain on active polling rates for two more polling cycles before converting to the **ATP Down** polling intervals.

<i>Ethernet ATP Categories</i>		Polling when ATP Active			Polling when ATP Non-active			Polling when ATP Down	
ATP Category	Event Timeout	Polling Interval	Retry Interval	Polling Timeout	Polling Interval	Retry Interval	Polling Timeout	Polling Interval	Timeout
Cat 6 [Ethernet]	30 s	8 s	30 s	20s	8 s	30 s	20 s	30 s	30 s
Cat 5 [Ethernet]	30 s	10s	30 s	90s	10s	30 s	90 s	30 s	30 s
Cat 4 [Ethernet]	60 s	30 s	30 s	3 min	30 s	30 s	3 min	30 s	30 s
Cat 3 [Ethernet]	60 s	60 s	60 s	30 min	60 s	60 s	30 min	60 s	30 s
Cat 2A [Ethernet]	2 min	2 min	2 min	4 hr	2 min	2 min	4 hr	2 min	30 s
Cat 2 [Ethernet]	2 min	2 min	2 min	24 hr	2 min	2 min	24 hr	2 min	30 s
Cat 1 [Ethernet]	2 min	2 min	2 min	30 days	2 min	2 min	30 days	2 min	30 s
<i>Modem ATP Categories</i>									
Cat 5 [Modem]	30 s	10 s	30 s	90 s	4 hr	2 min	4hr 10 min	10 min	90 s
Cat 4A [Modem]	60 s	60 s	60 s	3 min	4 hr	2 min	4hr 10min	30 min	90 s
Cat 4 [Modem]	60 s	60 s	60 s	3 min	24 hr	2 min	24 hr 30 min	1 hr	90 s
Cat 3 [Modem]	60 s	25 min	60 s	30 min	24 hr	2 min	24 hr 30 min	4 hr	90 s
Cat 2A [Modem]	2 min	4 hr	2 min	4hr 10min	24 hr	2 min	24 hr 30 min	4 hr	90 s
Cat 2 [Modem]	2 min	24 hr	2 min	24hr 10min	24 hr	2 min	24 hr 30 min	24 hr	90 s
Cat 1 [Modem]	2 min	24 hr	10 min	25 hr	30 days	10 min	30 days 1 hr	7 days	90 s

Issued by
Vanderbilt

© Vanderbilt, 2015
Technical specifications and availability subject to change without notice.

Clonshaugh Business and Technology Park
Clonshaugh
Dublin
D17 KV84
www.service.vanderbiltindustries.com