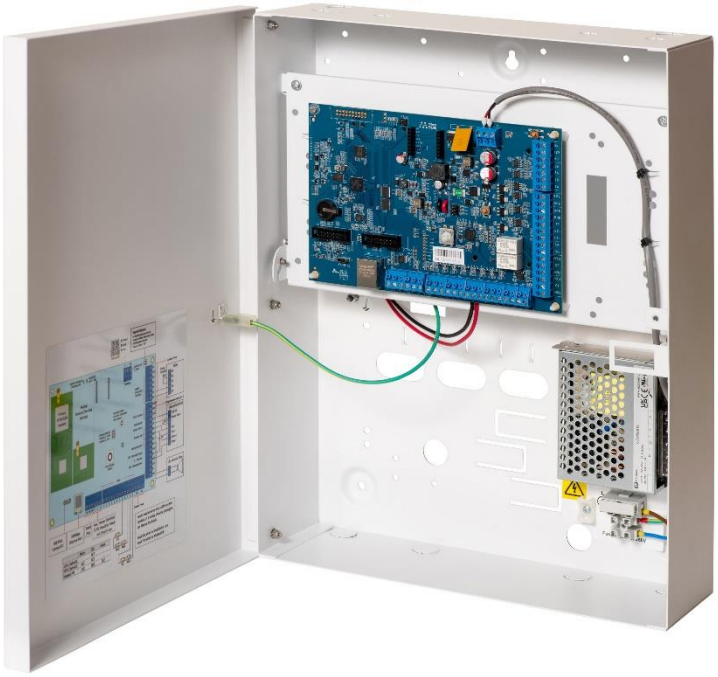
SPC42, SPC52, SPC53, SPC63

Installation & Configuration Manual



Document ID: I-200572
Edition date: 08.12.2023

Data and design subject to change without notice. / Supply subject to availability.

Table of Contents

1 Meaning of symbols

There are several symbols in the document:

Symbol	Description
IP	Only available for SPC controller with IP interface (SPC43/SPC52/SPC53/SPC63).
	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

This chapter covers:

2.1 Target group

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

Skilled Person:

Skilled person is a term applied to persons who have training or experience in the equipment technology, particularly in knowing the various energies and energy magnitudes used in the equipment. Skilled persons are expected to use their training and experience to recognize energy sources capable of causing pain or injury and to take action for protection from injury from those energies.

Skilled persons should also be protected against unintentional contact or exposure to energy sources capable of causing injury.

Instructed Person:

Instructed person is a term applied to persons who have been instructed and trained by a skilled person, or who are supervised by a skilled person, to identify energy sources that may cause pain and to take precautions to avoid unintentional contact with or exposure to those energy sources.

Under normal operating conditions, abnormal operating conditions or single fault conditions, instructed persons should not be exposed to parts comprising energy sources capable of causing injury.

2.2 General safety instructions

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

2.2.1 General information

- Keep this document for later reference.
- Always pass this document on together with the product.
- Also consider 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 230V 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, observe the ESD guidelines.

Damage due to unsuitable mounting location

- The environmental conditions recommended by the manufacturer must be observed. See *Technical Data* on page 21.
- 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 16A (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 and hazard symbols

2.3.1 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

2.3.2 Hazard symbols

WARNING: Warning of hazard area

WARNING: Warning of dangerous electrical voltage

3 Directives and standards

This chapter covers:

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”, and1999/5/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

3.2 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 Reinermann JörgWilms-Vahrenhorst (Stv.)

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

Product Type	Standard
• SPC53 • SPC63 • SPC6350.320 • SPC5350.320 • SPCP355.300 • SPCP333.300 • SPCE652.100 • SPCK420.100 • SPCK421.100 • SPCE452.100 • SPCE110.100 • SPCE120.100 • SPCA210.100 • SPCK620.100 • SPCK623.100 • SPCN110.000 • SPCN320.000 • SPCN340.000 • SPCN341.000 • SPCN342.000	EN50131 Grade 3
• SPC42 • SPC52 • SPCP332.300 • SPCW120.100	EN50131 Grade 2

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

Note: Compliance with Section 4.2.2 of EN 50131-5-3

Upon entering Engineer Walktest, the signals between the transmitter and the detectors are attenuated by 8dB. This provides immunity to attenuation as required by EN 50131-5-3.

EN50131 Requirement (and relevant section)	Relevant Vanderbilt documentation
Operating temperature and humidity range	Technical data: • SPC42/52 • SPC53 • SPC63

EN50131 Requirement (and relevant section)	Relevant Vanderbilt documentation
Weights and dimensions	Technical data: • SPC42/52 • SPC53 • SPC63
Fixing details	*Mounting system equipment* on page 23
Installation, commissioning, and maintenance instructions including terminal identifications	*Mounting system equipment* on page 23 *Controller hardware* on page 31
Type of interconnections (see 8.8)	Technical data: • SPC42/52 • SPC53 • SPC63 *Wiring the X-BUS interface* on page 35
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: • *Setting/Unsetting* on page 189 • *Configuring a Keyswitch Expander* on page 163 • *Configuring wireless fob devices* on page 63 • *Triggers* on page 201
Serviceable parts	Technical data: • SPC42/52 • SPC53 • SPC63
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: • SPC42/52 • SPC53 • SPC63
Maximum number of each type of ACE and expansion device.	*Wiring the X-BUS interface* on page 35 Technical data: • SPC42/52 • SPC53 • SPC63
Current consumption of the CIE and each type of ACE and expansion device, with and without an alarm condition.	See relevant installation instructions.

EN50131 Requirement (and relevant section)	Relevant Vanderbilt documentation
Maximum current rating of each electrical output	Technical data: • SPC42/52 • SPC53 • SPC63
Programmable functions provided	*Engineer programming via the keypad* on page 66 *Engineer programming via the browser* on page 122
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* on page 52 *LCD Keypad Settings* on page 79 *Comfort Keypad Settings* on page 80 *Configuring an Indicator Expander* on page 162
Masking/reduction of range signals/messages processed as “fault” or “masking” events (see 8.4.1, 8.5.1 and Table 11)	on page 169 *Wiring the zone inputs* on page 45 *SIA Codes* on page 267 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)	*Using the LCD keypad interface* on page 54 Using the Comfort keypad interface - see About the Comfort keypad
Minimum number of variations of PIN codes, logical keys, biometric keys and/or mechanical keys for each user (see 8.3)	*User PIN combinations* on page 275
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* on page 275
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* on page 275

EN50131 Requirement (and relevant section)	Relevant Vanderbilt documentation
Number of invalid code entries before user interface is disabled (see 8.3.2.4)	*Access PINs* on page 276
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)	*Setting/Unsetting* on page 189
Details of conditions provided for the set state (see 8.3.3.4)	*Setting/Unsetting* on page 189 *LCD Keypad Settings* on page 79 *Comfort Keypad Settings* on page 80 *Editing an output* on page 155 *Zone types* on page 278
Notification of output signals or messages provided (see 8.6)	*Editing an output* on page 155 *Setting/Unsetting* on page 189 *User rights* on page 141
Other output configurations to interface with I&HAS components (see 8.2)	*Editing an output* on page 155 *Zone types* on page 278 *Test* on page 113 *Keypad user interface* on page 52
Criteria for automatic removal of “soak test” attribute (see 8.3.9)	*Timers* on page 179
Number of events resulting in automatic inhibit	*Automatic inhibits* on page 275
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. See the relevant technical data on PSUs (separate documents).
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* on page 66 *Engineer programming via the browser* on page 122
Additional functions provided (see 4.2, 8.1.8)	*Unrestricted Grade* on page 184 *Options* on page 169
Access levels required to access such additional functions provided	*Edit* on page 89 User configuration (browser) - see *Adding/Editing a User* on page 139

EN50131 Requirement (and relevant section)	Relevant Vanderbilt documentation
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).	*Unrestricted Grade* on page 184 *Options* on page 169 *Compliance with EN50131 Approvals* below

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

Product Type	Standard
• SPC53 • SPC63 • SPC6350.320 • SPC5350.320 • 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
• SPC52 • SPC42 • SPCP332.300	EN50131-6

3.3 Compliance with VdS 2115:2015-12

Only VdS-approved maintenance-free batteries may be used for as a system standby backup.

3.3.1 Compliance with EN50131 Approvals

Software Requirements

- 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** setting **Prevent Setting Time** must be set to a value greater than 0 and less than 20.
- The **Wireless** setting **Device Lost Time** must be set to a value less than 120.

- The **X-BUS Settings, Retries**, must be set to a value of 10.
- The **X-BUS Settings, Comms timer**, must be set to a value of 5.
- DO NOT select the attribute **Setting State** in the **Keypad** configuration settings for **Visual indications**.
- Select **Network Time Protocol** to specify that the time is synchronized with the specified NTP server

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.
- 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 (Keyswitch Expander).

The SPCN110 PSTN module, the SPCN320 GSM/GPRS module, and the SPCN342 are tested with EN50131 approved Grade 2 and Grade 3 panels and can be used with these approved panels.

3.4 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.

3.5 Compliance with INCERT Approvals

Software Requirements

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

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

- Minimum battery capacity for the SPC42/43/53/63 is 10Ah/12V. If a 10Ah battery is used, then the battery is biased to the left of the housing and the bottom flap is bent to meet the battery.
- Fit jumper (J12) on the battery selector for 17/10Ah battery use and remove for 7Ah battery.

3.6 Compliance with NF and A2P approvals including CYBER requirements - SPC Products

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* on page 18.

Product Type	Configuration	Standard	Logo
SPC6350.320 + SPCP355.300 (Cert. 1233700001 + Cert.8033700002)	60h, unmonitored	NF Grade 3, Class 1	
SPC5350.320 + SPCP355.300 (Cert. 1233700001 + Cert.8033700002)	60h, unmonitored		
SPC6350.320 (Cert. 1233700001)	60h, unmonitored		
SPC5350.320 (Cert. 1233700001)	60h, unmonitored		
SPC63 + SPCP333.300 (Cert. 1233700001)	60h, unmonitored	NF Grade 3, Class 1	
SPC53 + SPCP333.300 (Cert. 1232200003)	60h, unmonitored		
SPC63 (Cert. 1233700001)	30h, monitored		
SPC5330.320 (Cert. 1232200003)	30h, monitored		
SPC53 (Cert. 1232200003)	36h, unmonitored	NF Grade 2, Class 1	
SPC42 (Cert. 1232200003)	36h, unmonitored		
SPCN110.000 SPCN320.000 SPCN341 SPCN342 SPCK420.100 SPCK620.100 SPCK623.100 SPCE652.100 SPCE452.100 SPCE110.100 SPCE120.100		NF Grade 2 and 3, Class 1	

4 Technical Data

The information in the following tables enable you to compare the technical data for the SPC42, SPC52, SPC53, and SPC63:

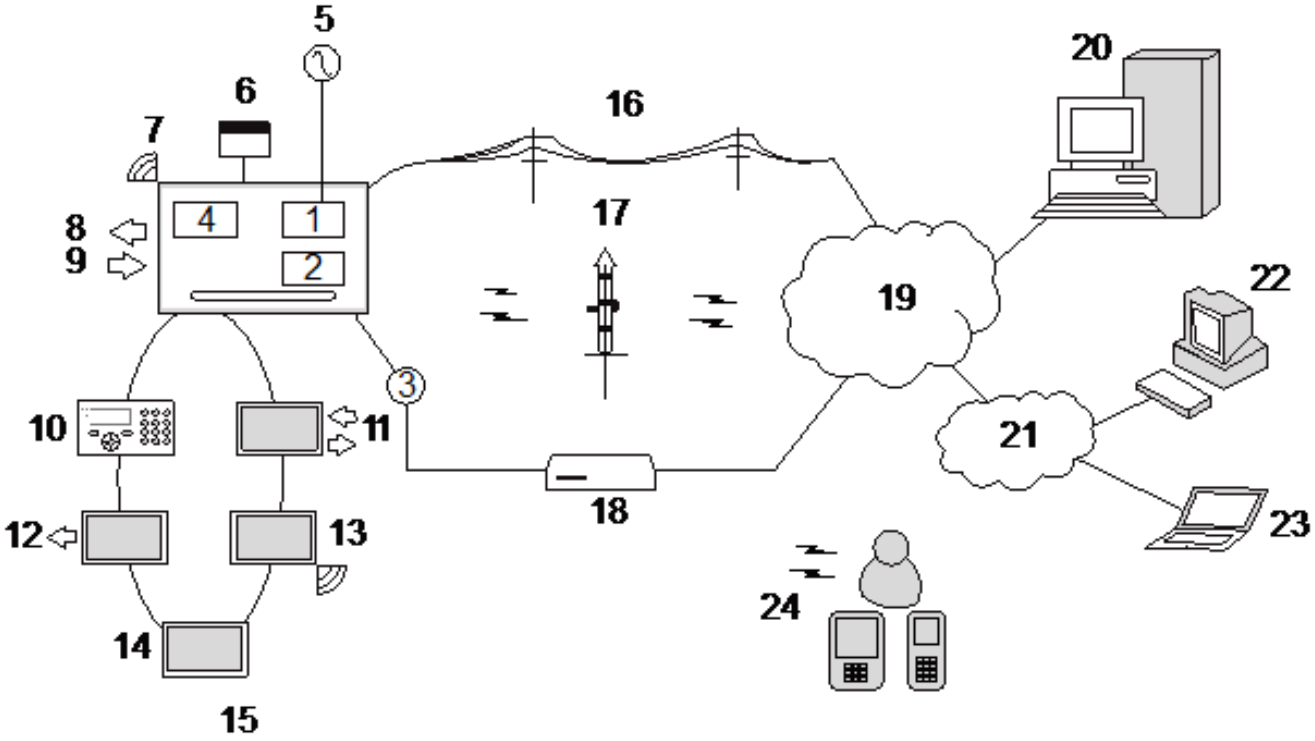
4.1 SPC Matrix

	Type	SPC42	SPC52	SPC53	SPC63
Controller details	Type	Main product	License upgrade via SPC Connect	Main product	License upgrade via SPC Connect
	Areas	4	16	16	60
	Supported Zones max. (wired & wireless)	40	128	128	512
	Number of on-board zones	8	8	8	8
	EOL resistor	Dual 4k7 (default), other resistor combinations configurable	Dual 4k7 (default), other resistor combinations configurable	Dual 4k7 (default), other resistor combinations configurable	Dual 4k7 (default), other resistor combinations configurable
	Supported Outputs max.	30	128	128	512
	Outputs on PCB	6	6	6	6
	Number of on-board relays	2 x 30V/3A resistive switching current	2 x 30V/3A resistive switching current	2 x 30V/3A resistive switching current	2 x 30V/3A resistive switching current
	Number of on-board open coll.	2 internal/external bell, 2 freely programmable (each supplied via auxiliary output)	2 internal/external bell, 2 freely programmable (each supplied via auxiliary output)	2 internal/external bell, 2 freely programmable (each supplied via auxiliary output)	2 internal/external bell, 2 freely programmable (each supplied via auxiliary output)
	Log Intrusion	1000	10000	10000	10000
	Log Access	1000	10000	10000	10000
	Calendars	4	32	32	64
	Triggers	8	512	512	1024
	Mapping Gates	8	128	128	512
	Virtual Zones	4	20	20	100
	Supported Active languages / System	EN + 4	EN + 4	EN + 4	EN + 4
	Security Grade	Grade 2	Grade 2	Grade 3	Grade 3
	Power supply	Type A (per EN50131-1)	Type A (per EN50131-1)	Type A (per EN50131-1)	Type A (per EN50131-1)
	Mains voltage	230V AC, + 10%/ -15%, 50Hz	230V AC, + 10%/ -15%, 50Hz	230V AC, + 10%/ -15%, 50Hz	230V AC, + 10%/ -15%, 50Hz
	Mains fuse	500mA T (replaceable part on mains terminal block)	500mA T (replaceable part on mains terminal block)	500mA T (replaceable part on mains terminal block)	500mA T (replaceable part on mains terminal block)
	Quiescent current min	38mA at 230V AC	38mA at 230V AC	38mA at 230V AC	38mA at 230V AC
	Quiescent current max	135mA at 12V DC	135mA at 12V DC	135mA at 12V DC	135mA at 12V DC
	Output voltage	13,8V DC in normal conditions (mains powered and fully charged battery), min. 10V DC when powered by secondary device (before system shut down to battery deep discharge protection)	13,8V DC in normal conditions (mains powered and fully charged battery), min. 10V DC when powered by secondary device (before system shut down to battery deep discharge protection)	13,8V DC in normal conditions (mains powered and fully charged battery), min. 10V DC when powered by secondary device (before system shut down to battery deep discharge protection)	13,8V DC in normal conditions (mains powered and fully charged battery), min. 10V DC when powered by secondary device (before system shut down to battery deep discharge protection)
	Low voltage trigger	7.5V DC	7.5V DC	7.5V DC	7.5V DC
	Overvoltage protection	14,75V DC	14,75V DC	14,75V DC	14,75V DC
	Peak to Peak ripple	Max. 5% of output voltage	Max. 5% of output voltage	Max. 5% of output voltage	Max. 5% of output voltage
	Auxiliary power (nominal)	Max. 1900mA at 12V DC (1500mA from CN14,CN12 & 400mA from CN15)	Max. 1900mA at 12V DC (1500mA from CN14,CN12 & 400mA from CN15)	Max. 1900mA at 12V DC (1500mA from CN14,CN12 & 400mA from CN15)	Max. 1900mA at 12V DC (1500mA from CN14,CN12 & 400mA from CN15)
	Supported battery capacity	7Ah	7Ah	17Ah	17Ah
	Battery type (Battery not supplied)	YUASA NP7-12FR (12V/7Ah) - NF PowerSonic PS1270 (12V/7Ah) YUASA Yucel Y7-12FR (12V/7Ah)	YUASA NP7-12FR (12V/7Ah) - NF PowerSonic PS1270 (12V/7Ah) YUASA Yucel Y7-12FR (12V/7Ah)	YUASA NP17-12FR (12V/17Ah) - NF YUASA Yucel Y17-12IFR (12V/17Ah) PowerSonic PS12170 (12V/17Ah)	YUASA NP17-12FR (12V/17Ah) - NF YUASA Yucel Y17-12IFR (12V/17Ah) PowerSonic PS12170 (12V/17Ah)
	Battery charger	Max. 72h to 80% of battery capacity	Max. 72h to 80% of battery capacity	Max. 24h to 80% of battery capacity	Max. 24h to 80% of battery capacity
	Battery protection	Current limited to 3A (fuse protected), deep discharge protection at 10V DC +/- 3%	Current limited to 3A (fuse protected), deep discharge protection at 10V DC +/- 3%	Current limited to 3A (fuse protected), deep discharge protection at 10V DC +/- 3%	Current limited to 3A (fuse protected), deep discharge protection at 10V DC +/- 3%
	Tamper contact	Front spring tamper, 2 auxiliary tamper contact inputs	Front spring tamper, 2 auxiliary tamper contact inputs	Front spring tamper, 2 auxiliary tamper contact inputs	Front spring tamper, 2 auxiliary tamper contact inputs
	Bootup time before fully operational	< 15 sec	< 15 sec	< 15 sec	< 15 sec
	Software update	Local and remote upgrade for controller, peripherals and GSM/PTSN modems.	Local and remote upgrade for controller, peripherals and GSM/PTSN modems.	Local and remote upgrade for controller, peripherals and GSM/PTSN modems.	Local and remote upgrade for controller, peripherals and GSM/PTSN modems.
	Calibration	No calibration checks required (calibrated at manufacturing)	No calibration checks required (calibrated at manufacturing)	No calibration checks required (calibrated at manufacturing)	No calibration checks required (calibrated at manufacturing)
	Serviceable parts	500mA T (replaceable part on mains terminal block)	500mA T (replaceable part on mains terminal block)	500mA T (replaceable part on mains terminal block)	500mA T (replaceable part on mains terminal block)
	Operating temperature	-10 to +55°C	-10 to +55°C	-10 to +55°C	-10 to +55°C
	Relative humidity	Max. 93% (non condensing)	Max. 93% (non condensing)	Max. 93% (non condensing)	Max. 93% (non condensing)
	Colour	RAL 9003 (signal white)	RAL 9003 (signal white)	RAL 9003 (signal white)	RAL 9003 (signal white)
	Weight	3.480kg	3.480kg	5.380kg	5.380kg
	Dimensions (W x H x D)	264 x 357 x 81mm	264 x 357 x 81mm	326 x 415 x 114mm	326 x 415 x 114mm
	IP rating	30	30	IP30/IK06	IP30/IK06
	Housing	Small metal housing (1.2mm mild steel)	Small metal housing (1.2mm mild steel)	Hinged metal housing (1.2mm mild steel)	Hinged metal housing (1.2mm mild steel)
	Housing can contain up to	1 additional expander (size 150 x 82mm)	1 additional expander (size 150 x 82mm)	4 additional expanders (size 150 x 82mm)	4 additional expanders (size 150 x 82mm)
User credentials	Users	100	500	500	2500
	Paces	32	250	250	250
	Access Cards	100	500	500	2500
	SMS	32	50	50	100
	Web passwords	32	50	50	100
	User Profiles	100	100	100	100
Connectivity	Web server	embedded	embedded	embedded	embedded
	RS232	1	1	2	1
	USB interface	1 (micro USB)	1 (micro USB)	1 (micro USB)	1 (micro USB)
	Ethernet 100Mbits full duplex Ethernet (RJ45)	1	1	1	1
X-Bus	X-Bus interface	2	2	2	2
	X-Bus devices max.	11	48	48	128
	X-Bus keypads	4	16	16	32
	X-Bus I/O devices	5	16	16	64
	X-Bus output devices	5	16	16	64
	X-Bus door expanders	2	8	8	32
Access Control	Doors only Entry	4	16	16	64
	Doors Entry / Exit	2	8	8	32
	Card readers max.	4	16	16	64
	Supported card technologies	Mifare, Classic 1k, Cotag, DESfire, EM4102, Wiegand (26 & 37 bits, HID Corp 1000	Mifare, Classic 1k, Cotag, DESfire, EM4102, Wiegand (26 & 37 bits, HID Corp 1000	Mifare, Classic 1k, Cotag, DESfire, EM4102, Wiegand (26 & 37 bits, HID Corp 1000	Mifare, Classic 1k, Cotag, DESfire, EM4102, Wiegand (26 & 37 bits, HID Corp 1000
2-Way Wireless	Wireless gateways	1	1	1	1
	Wireless keypads	2	4	4	4
	Wireless repeaters	4	4	4	4
	Wireless detectors max.	40	64	64	64
	Wireless output devices max. bells/strobes (int./ext.)	16	16	16	16
	FOBs max.	20	20	20	20
Transmission	IP dialer EDP / FlexC	on board	on board	on board	on board
	Internal modems max.	2	2	2	2
	PSTN modems max.	1 + 1	1 + 1	1 + 1	1 + 1
	GSM modems max. (2G/3G or 2G/4G support)	1 + 1	1 + 1	1 + 1	1 + 1
	FlexC max. no. of supported ATS	3	5	5	10
	FlexC max. no. of supported ATP	8	15	15	30
	Event Profiles	5	10	10	20
	Event Exceptions	10	50	50	100
	Command Profiles	5	8	8	10
Alarm verification	Verification zones	16	32	32	32
	IP cameras	4	4	4	4
	Video	Up to 16 pre/16 post event images (by JPEG resolution 320 x 240, max. 1 frame/sec.)	Up to 16 pre/16 post event images (by JPEG resolution 320 x 240, max. 1 frame/sec.)	Up to 16 pre/16 post event images (by JPEG resolution 320 x 240, max. 1 frame/sec.)	Up to 16 pre/16 post event images (by JPEG resolution 320 x 240, max. 1 frame/sec.)
	Audio	Up to 60sec. pre/60sec. post audio recording	Up to 60sec. pre/60sec. post audio recording	Up to 60sec. pre/60sec. post audio recording	Up to 60sec. pre/60sec. post audio recording
	X-BUS Audio exanders max.SPC340 / SPC341 / SPCV440	8	16	16	32
	Audio Satelites max .3 per X-BUS Audio expander	24	48	48	96

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, Ethernet) 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

Number	Description	Number	Description
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 12V	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

SPC Controllers should be installed in restricted access areas only. A restricted access area is an area accessible only to skilled persons and to instructed persons with the proper authorization.

This chapter covers:

6.1 Mounting a G2 housing

The SPC G2 housing is supplied with a metallic c 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 (Printed Circuit Board) mounted on 4 support pillars. An optional input/output module can be mounted directly beneath the controller PCB. A battery with capacity of 7Ah 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 housing. 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 4–5mm shank, a minimum head diameter of 8mm and a minimum length of 40mm are recommended for mounting the housing. Additional expansion plugs or fixings may be required depending on the construction of the wall.

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.

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 4–5mm shank, a minimum head diameter of 8mm and a minimum length of 40mm 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 housing.
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 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:

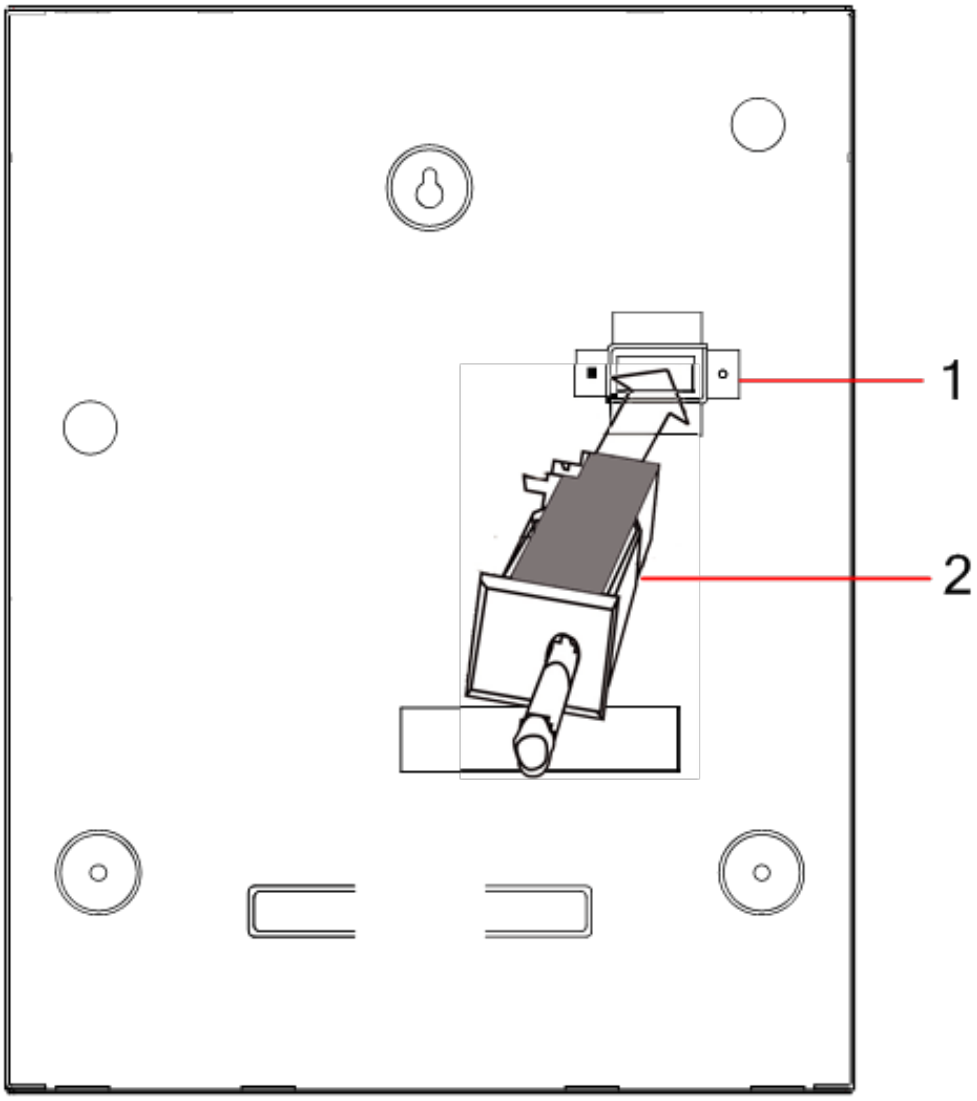
- Tamper switch
- Leads for connecting the back tamper switch to the controller
- Wall fixing plate

Mounting the Wall Fixing Plate

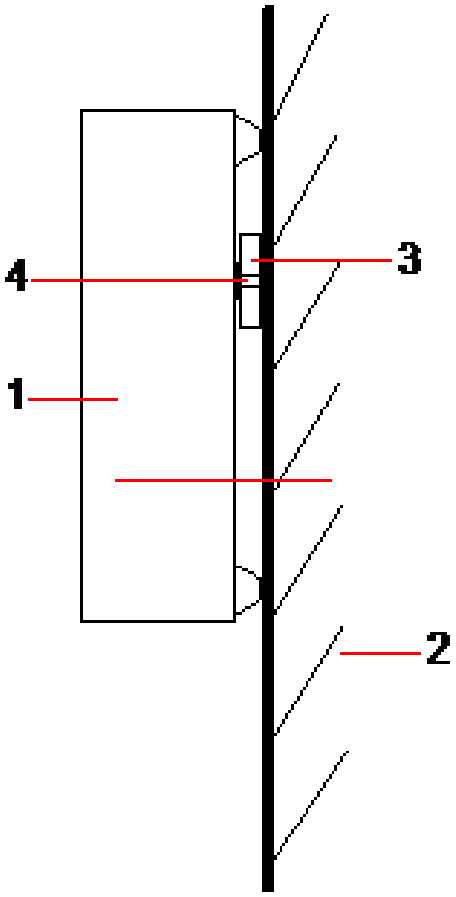
1. Mount the SPC in the appropriate position on the wall using all three fixings.
2. Draw a line around the inside of the back tamper cut out to provide a guide for the wall plate on the fixing wall. Remove the housing from the wall.
3. Place the wall plate on the wall centering it precisely around the rectangle previously drawn.
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. 4mm) 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 housing so that the plunger faces outwards (see item 1 below).


1
2

2. Fit the housing 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 housing metalwork.



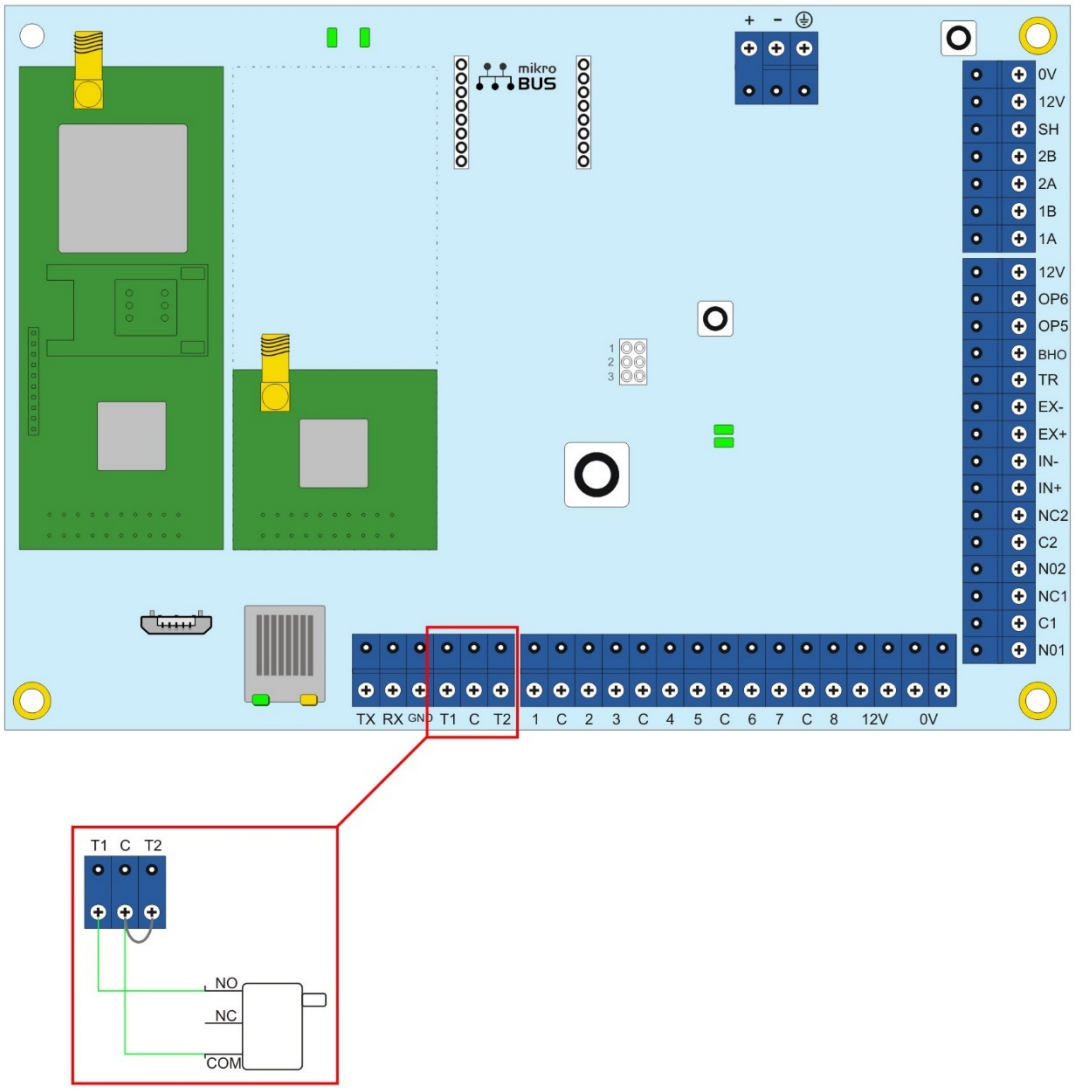
Number	Description
1	Housing
2	Wall
3	Wall Fixing Plate
4	Tamper Switch

WARNING: If the wall fixing plate is not accurately aligned then the housing 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 Housing so that the battery is retained.

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

If a 17Ah battery is used then the battery is biased to the right of the housing 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 keypad

See the corresponding installation instruction.

Installation guides are available at https://vanderbiltindustries.com/download-center.

6.4 Mounting an expander

See the corresponding installation instruction.

Installation guides are available at https://vanderbiltindustries.com/download-center.

6.5 Wiring the X-BUS Interface

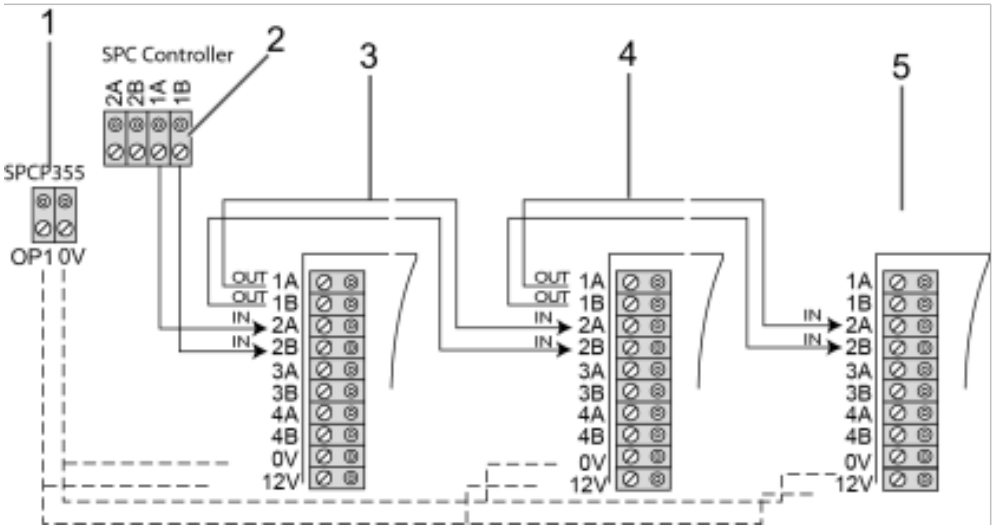
The X-BUS interface connects expanders and keypads to the SPC controller. The X-BUS can be wired in a number of different configurations, depending on the installation requirements.

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

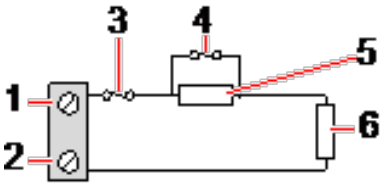
6.5.1 Wiring the Inputs

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

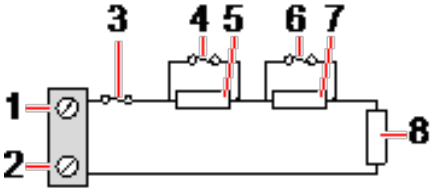
The following diagram shows the default configuration, Double EOL 4k7:



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

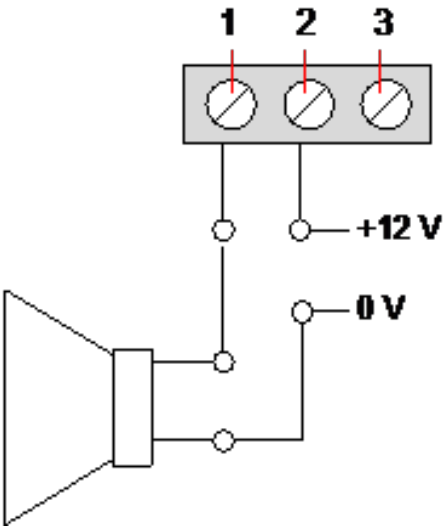
Number	Description
2	COM
3	Tamper
4	Alarm
5	4k7
6	Detector Fault
7	2K2
8	EOL 4k7

6.5.2 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 Controller hardware

This section describes the controller hardware.

See also

Powering expanders from the auxiliary power terminals on page 265

Wiring the X-BUS interface on page 35

Wiring an internal sounder on page 48

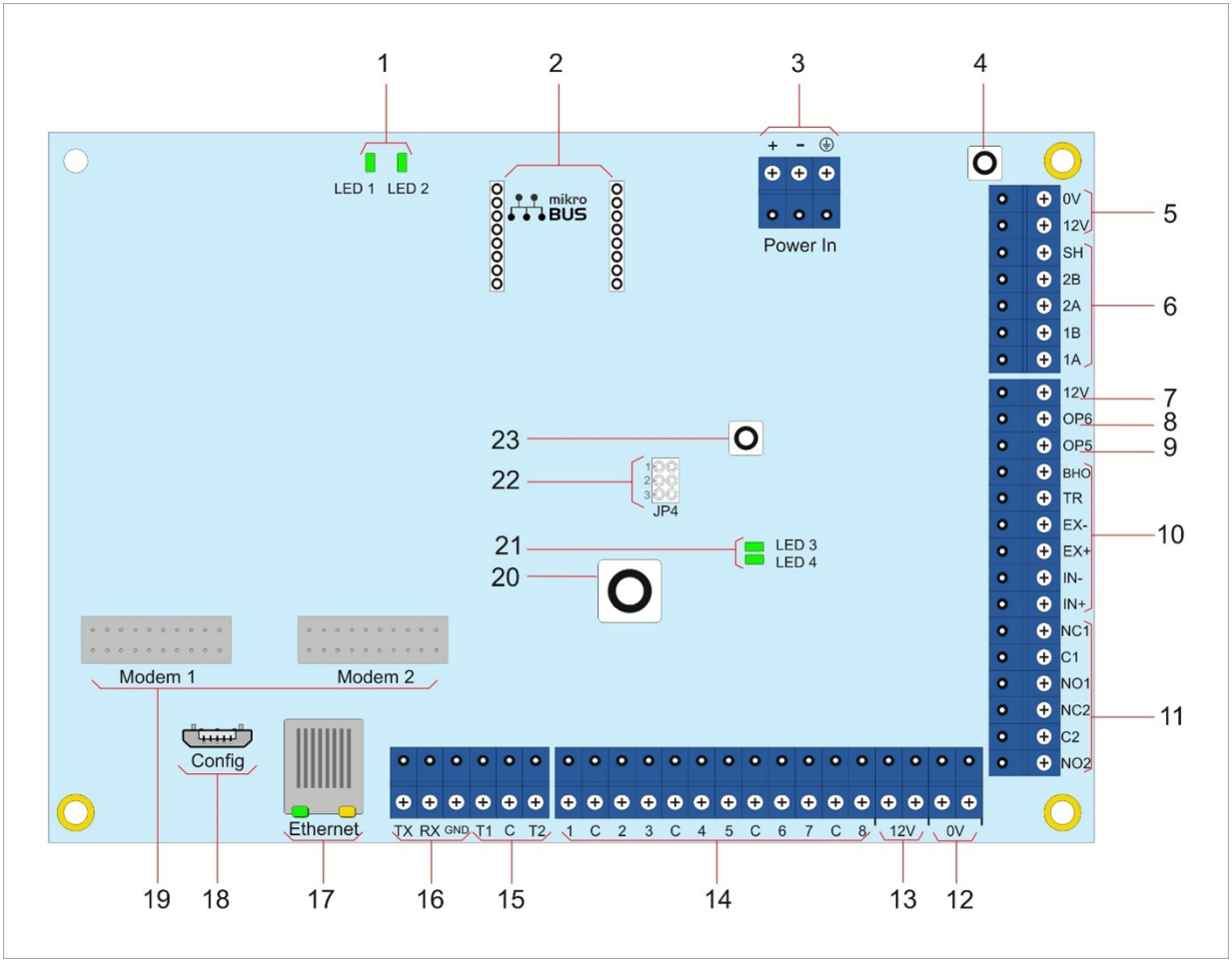
Wiring the zone inputs on page 45

Controller status LEDs on page 265

7.1 Controller Hardware SPC42/SPC52/SPC53/SPC63

This section describes the controller for the SPC42, SPC43, SPC53, and SPC63 models.

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



Number	Name	Description
1	SPC status LEDs	These LEDs display the status of various system parameters as described in *Controller status LEDs* on page 265.

Number	Name	Description
2	mikroBUS header	Reserved for future development.
3	Power supply	D/C Power Input: The DC input power supply is applied to this 3-pin connection. PE is connected to the earth lead from the mains supply which is wired to a connection point on the metal housing.
4	Reset button	• To reset the controller: – Press this switch once. • To reset the programming settings to default and reboot the controller: – Hold down the button until you are asked if a factory reset is desired. – Select YES to reset to factory defaults. **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. **Note:** This feature is not available if **Engineer Lock** is enabled.
5	Auxiliary 12V output	The SPC controller provides an auxiliary 12V DC output that can be used to supply power to expanders and devices such as latches, bells, etc. See *Powering expanders from the auxiliary power terminals* on page 265. The maximum deliverable current is 750mA. **Note:** The amount of current drawn is subject to the amount of time to be held up under battery conditions.
6	X-BUS interface	This is the SPC communications bus used to network expanders together on the system. See *Wiring the X-BUS interface* on page 35.
7	Auxiliary 12V output	Auxiliary 12V output An additional auxiliary 12V output provides power for outputs (8 and 9). The maximum deliverable current for Auxillary 12V outputs (5 and 7) is 1500mA.
8	On-board outputs	Output OP6 is a 12V open collector resistive output that shares a 400mA current rating with the auxiliary 12V output. If the output is not connected to the 12V of the controller and is powered from an external power source the 0V of the power source needs to be connected to the controller 0V and the external power source cannot exceed 12V.
9	ST- Output	The ST- Output is a 12V open collector resistive output that shares a 400mA current rating with the auxiliary 12V output.
10	Internal bell/external bell	Internal and external bell outputs (INT+, INT-, EXT+, EXT-) are resistive outputs with a 400mA current rating. The BHO (Bell Hold Off), TR (Tamper Return), 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 *Wiring an internal sounder* on page 48.
11	Relay Outputs	The SPCEvo controller provides two 3A, single pole, changeover relays that can be used to drive external bell strobes or other devices..
12, 13	Detector 12V outputs	The controller provides two 12V DC detector outputs that can be used to supply power to detectors. The maximum deliverable current is 400mA.

Number	Name	Description
14	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 *Wiring the zone inputs* on page 45.
15	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.
16	Serial port terminal block	Serial port terminal block (TX, RX, GND) may be used to interface to an external modem or PC terminal program. Serial port 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.
17	Ethernet interface	The Ethernet interface (100mbps) provides for the connection of a PC to the controller for the purposes of programming the system. 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.
18	USB Config	The micro USB Config interface is used to access browser programming, SPC Connect Pro, or a terminal program.
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 may also house a two-way wireless module.
20	Front tamper	This on-board front tamper (switch and switch) provides the housing tamper protection. **Note:** The front tamper is not used in the G5 housing.
21	Status LEDs	Two LEDs display the status of system parameters. See *Controller status LEDs* on page 265
22	Battery selector	JP4: • Fit jumper in position 1 for 17Ah battery use. • Fit jumper in position 3 for 7Ah battery use.
23	Kickstart Switch	See *Powering from battery only* on page 51.

8 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.

See *Supported card readers and card formats* on page 286 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.

9 Wiring the system

This chapter covers:

9.1 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 307kb.

NOTICE: The X-BUS is an RS-485 bus with a baud rate of 307kb. The full performance is only supported in loop (see *Loop configuration* on the next page) and spur (see *Spur configuration* on page 37) wiring configuration (best signal quality due to daisy chain of isolated sections with 1 transmitter/1 receiver and balanced terminating resistors on each end).

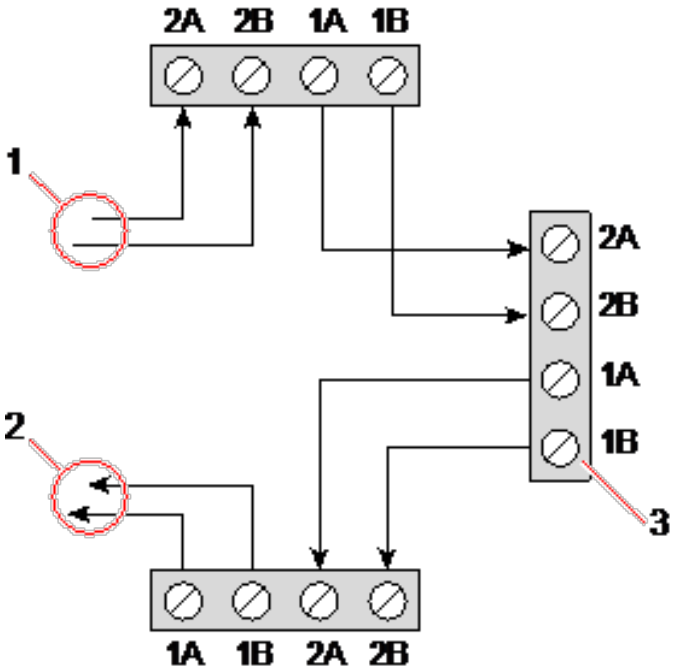
The performance in star or multi-drop configuration wiring (see *Star and multi-drop configuration* on page 38) is limited due to non-optimal conditions of the RS-485 bus specification (reduced signal quality due to multiple receivers/transmitters in parallel with unbalanced terminating resistors).

NOTICE: It is strongly recommended to use loop (see *Loop configuration* on the next page) or spur (see *Spur configuration* on page 37) 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

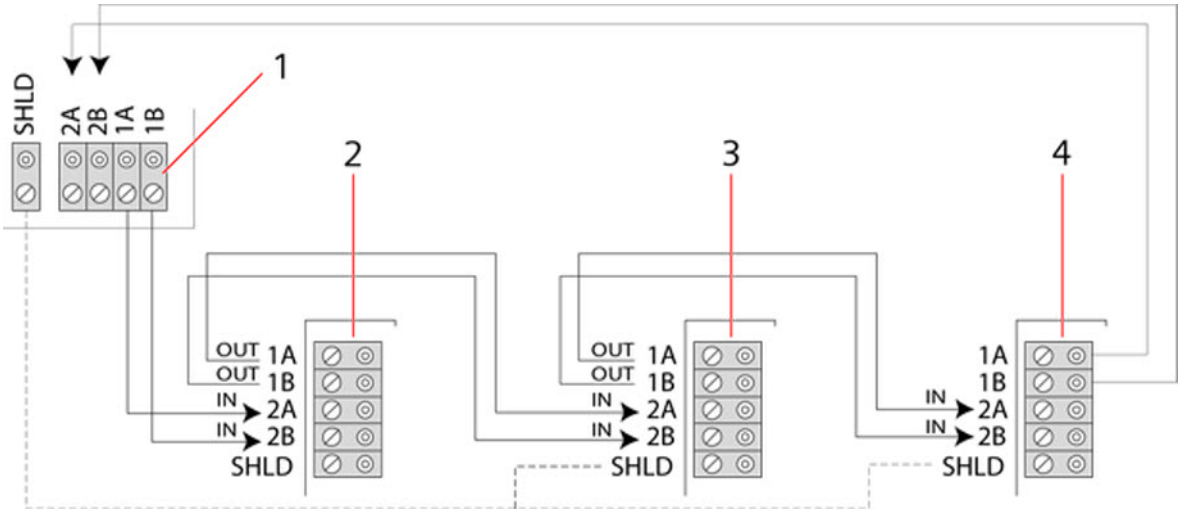
Number	Description
1	Previous expander
2	Next expander
3	SPC controller

Most expanders are equipped with additional terminals 3A/3B and 4A/4B for branch expander wiring. See *Wiring of branch expander* on page 43 for instructions on branch expander wiring.

9.1.1 Loop configuration

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 etc. 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.



Number	Description
1	Controller
2-4	Expanders

9.1.2 Spur configuration

NOTICE: SPC42, SPC52, SPC53, SPC63 support 2 spurs (2 X-BUS ports).

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

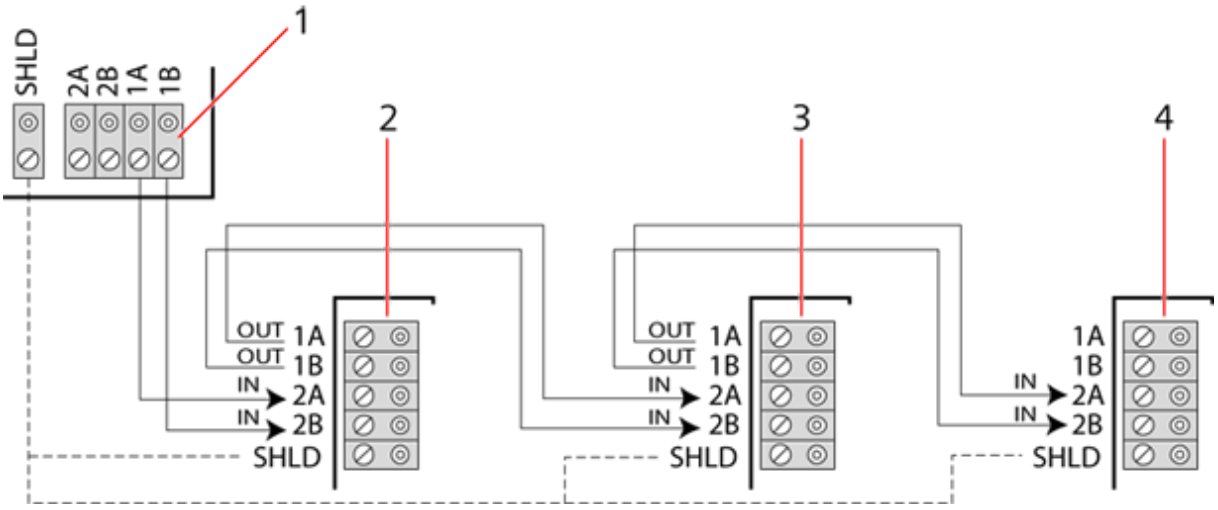
The spur (or open loop) cabling method offers a high level of fault tolerance and may be more convenient on certain installations. In the case of a X-BUS fault or break, all expanders and detectors up to the fault continue to be supervised.

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. For example, 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 resisting 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

Number	Description
1	Controller
2-4	Expanders

9.1.3 Star and multi-drop configuration

NOTICE: See *Examples of correct wiring* on page 41, *Examples of incorrect wiring* on page 42 and *Shielding* on page 43 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:

	SPC42/SPC52	SPC53/SPC63
Max. expanders/keypads	8	16 (8 per X-BUS port)
Total cable length	200 m	200 m

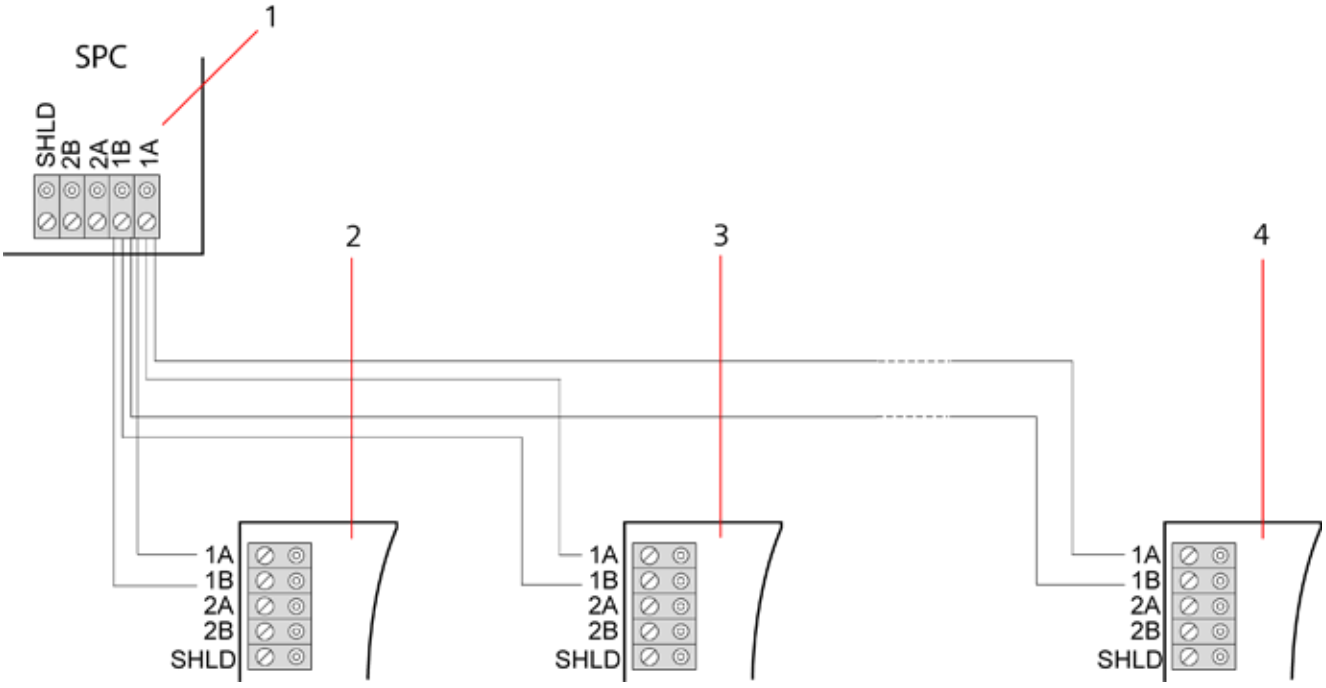
NOTICE: The performance in star or multi-drop configuration wiring is limited due to non-optimal conditions of the RS-485 bus specification (reduced signal quality due to multiple receivers/transmitters in parallel with unbalanced terminating resistors).

Star configuration

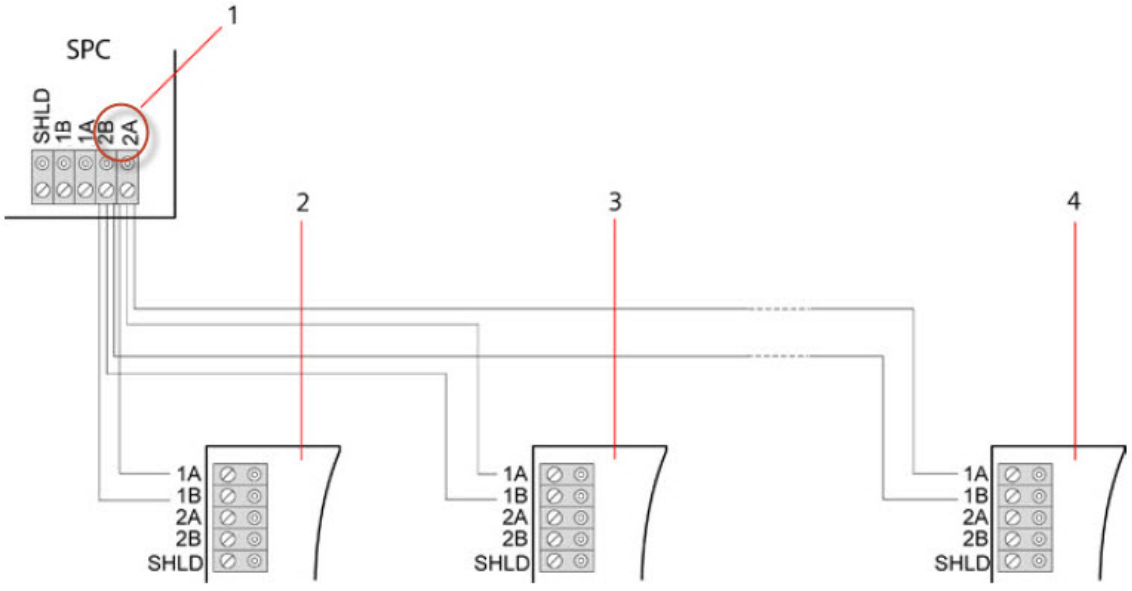
NOTICE: All expanders/keypads are fitted with a termination jumper by default. In star configuration it's imperative to **remove** these jumpers.

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

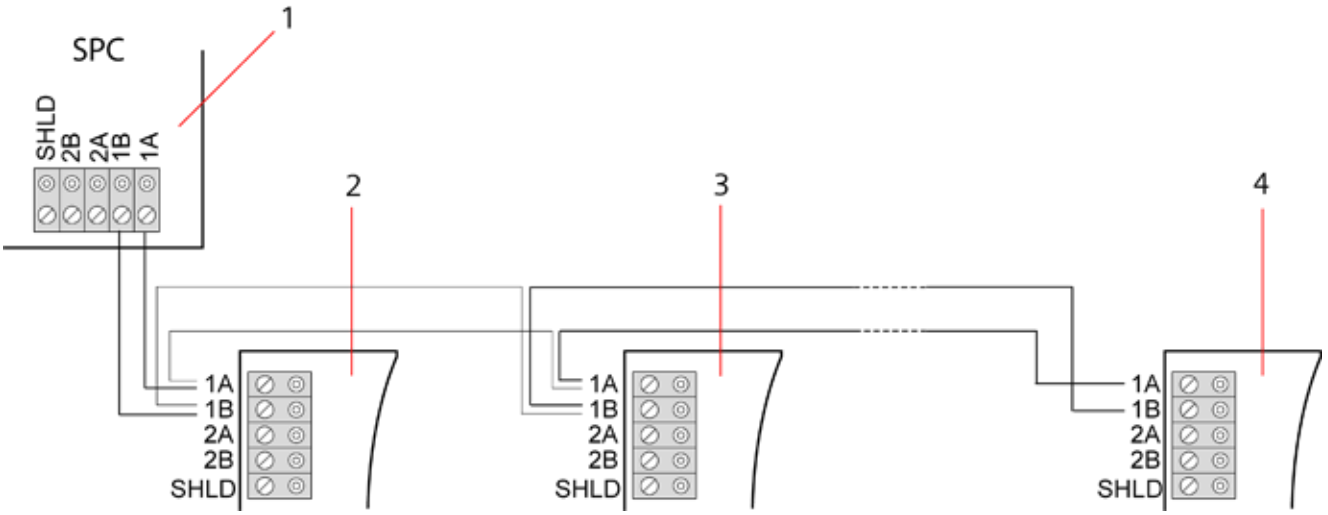
Number	Description
1	SPC Controller
2-4	Expanders

Multi-drop configuration

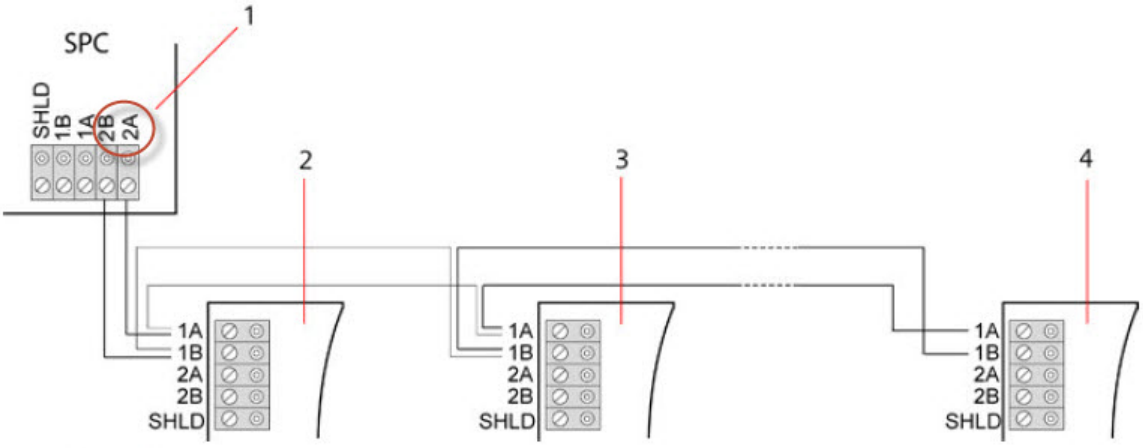
NOTICE: All expanders/keypads are fitted with a termination jumper by default. In multi-drop configuration it's imperative to **remove** these jumpers with exception of last keypad or expander on the line.

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.



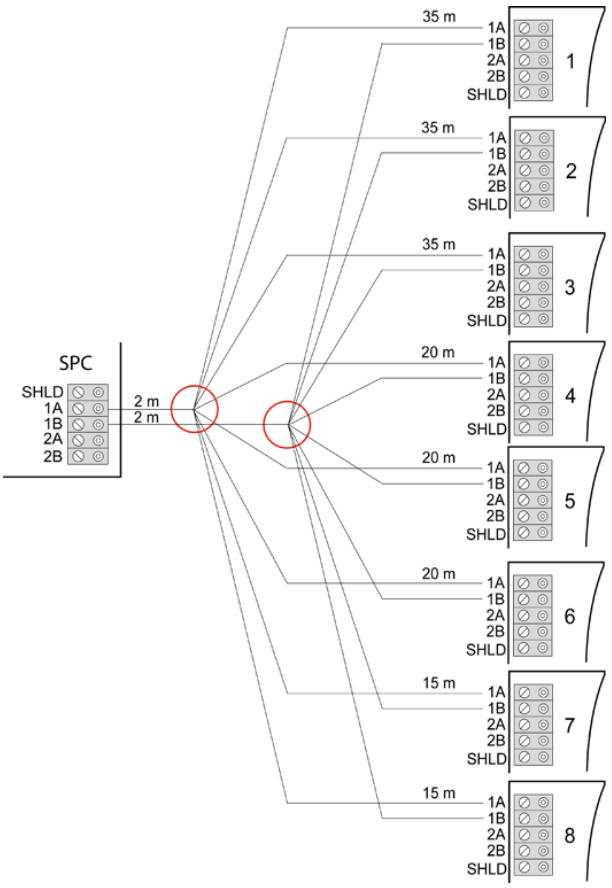
Multi-drop configuration



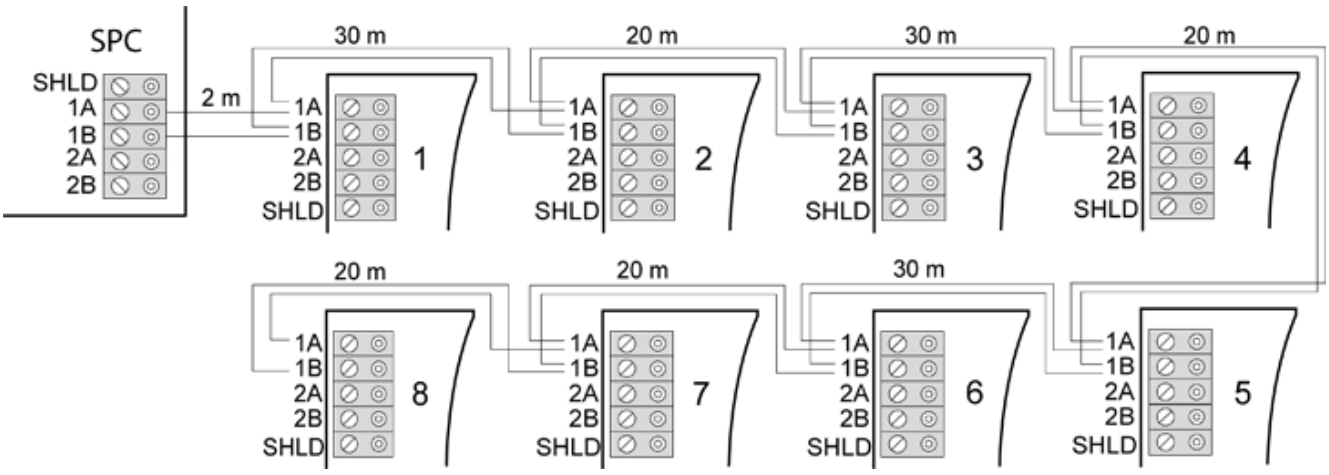
Multi-drop configuration 2

Number	Description
1	SPC controller
2-4	Expanders

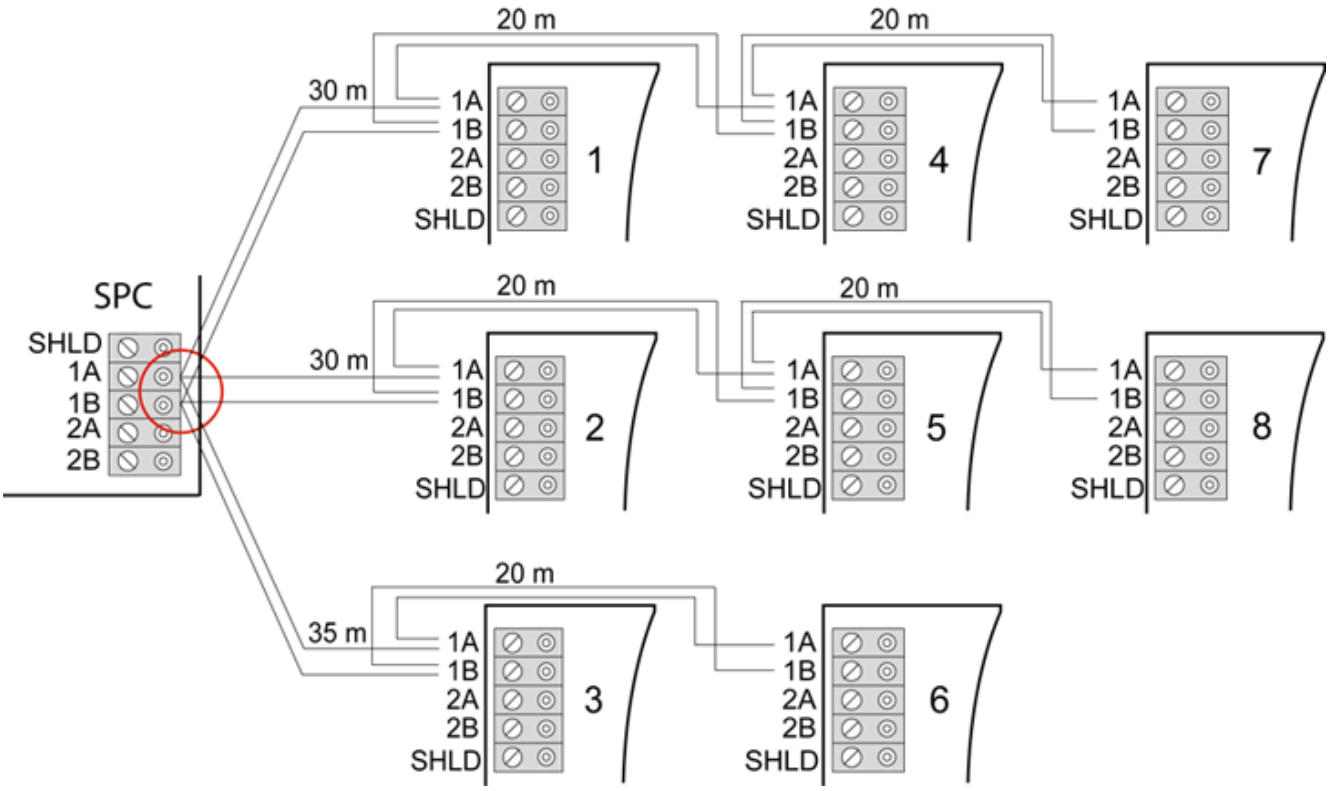
9.1.3.1 Examples of correct wiring



Star wiring



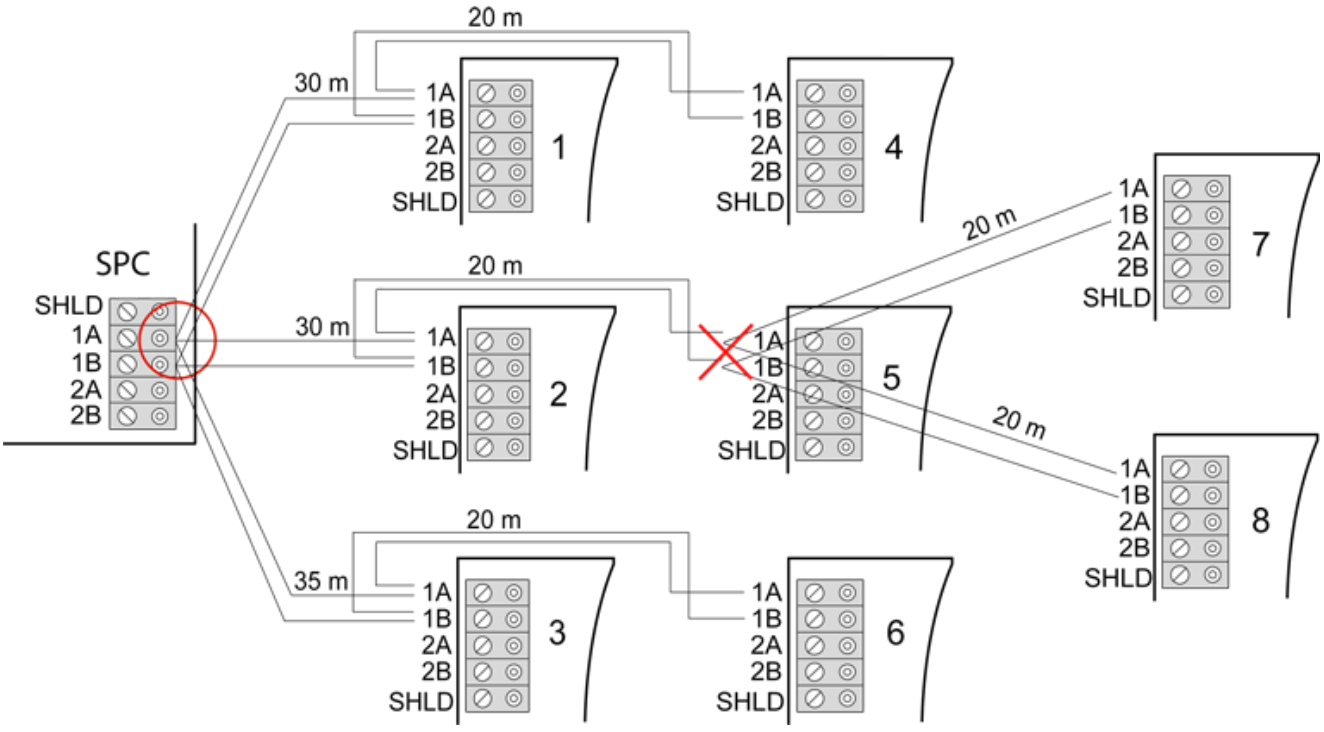
Multi-drop wiring



Mixed wiring

9.1.3.2 Examples of incorrect wiring

NOTICE: 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.



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 (for example, keypad operation) or even loss of communication to devices. If such behavior is observed a wiring in loop OR star configuration is strongly recommended.

9.1.4 Shielding

The shielding terminals (SHLD) should only be used for cables types with shielding (for example, Belden 9829). If shielding is required (that is, 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 is 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 (that is, sites with high electric field interference) a new wiring in proper spur or loop configuration with appropriate installation cable configuration has to be done.

9.1.5 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 *X-BUS* on page 77.

For a system with manual addressing, expanders and keypads have a separate numbering sequence and are defined by the engineer manually. That is, expanders are numbered 01, 02, 03, etc. 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. That is, expanders and keypads are together numbered 01, 02, 03, in the order that they are detected relative to the location of the controller.

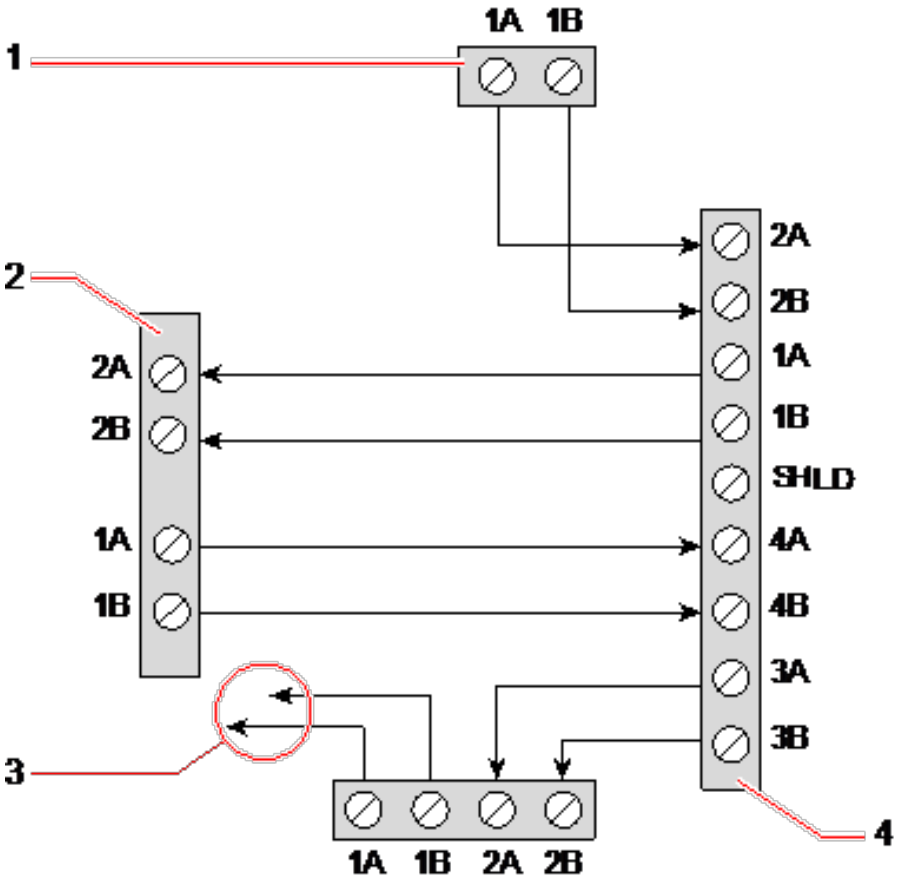
9.2 Wiring of branch expander

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

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

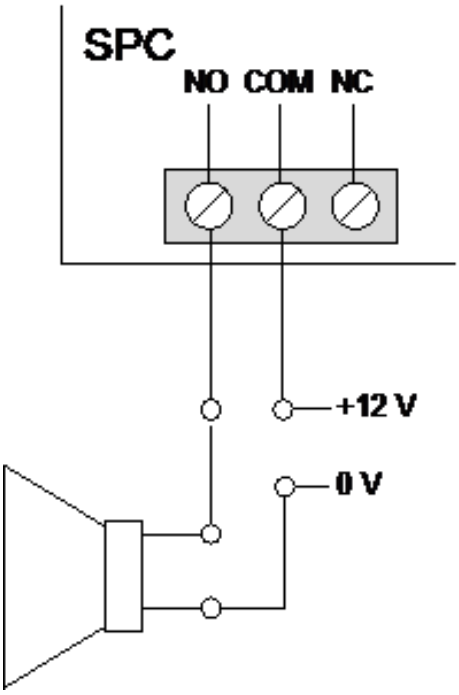
9.3 Wiring the system ground

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

9.4 Wiring the relay output

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

When a relay is activated the common terminal connection (COM) is switched from the **N**ormally **C**losed terminal (NC) to the **N**ormally **O**pen terminal (NO).



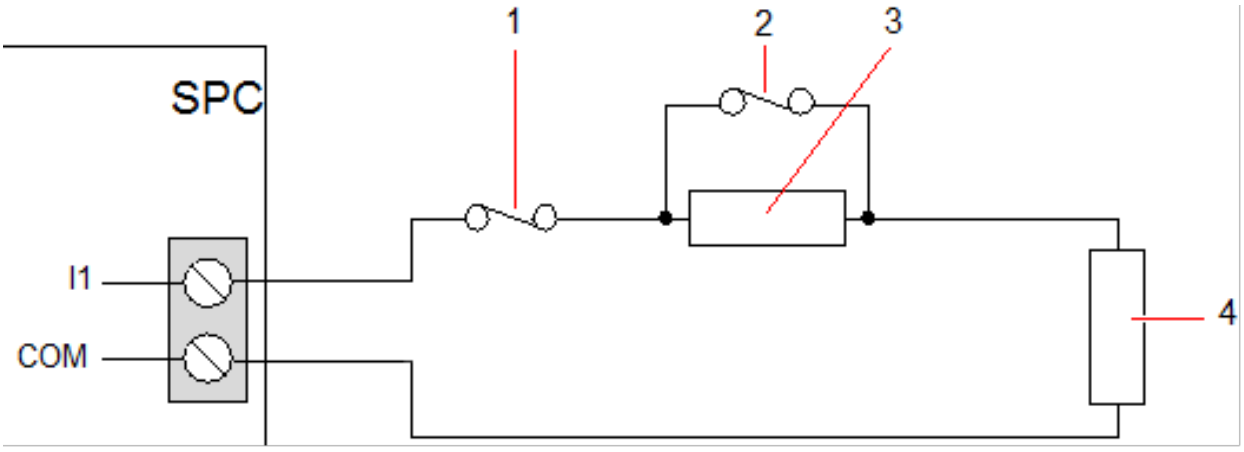
Standard wiring

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

9.5 Wiring the zone inputs

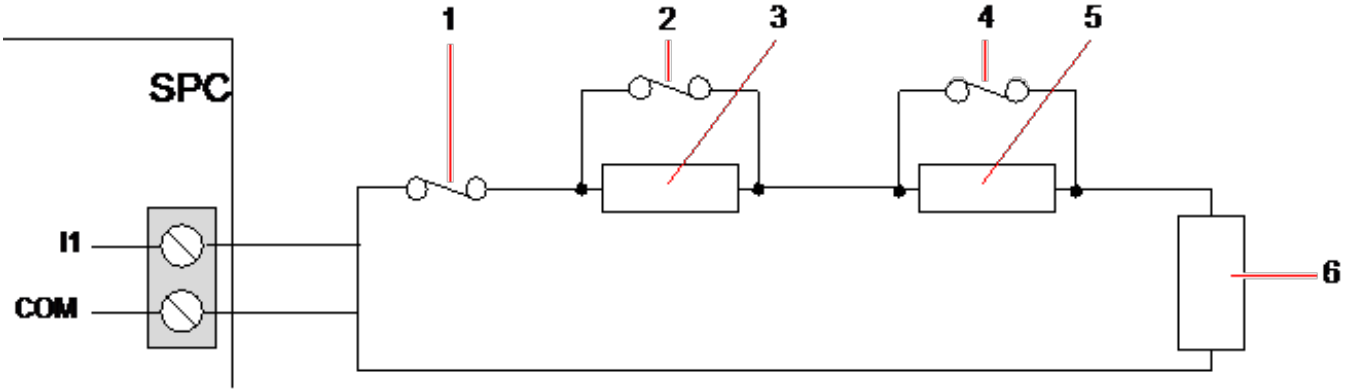
The SPC controller has 8 on-board zone inputs. By default these inputs are monitored using end of line supervision. The installer can choose from any of the following configurations when wiring the inputs:

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



Default configuration (DEOL 4k7)

Number	Description
1	Tamper
2	Alarm
3	EOL 4k7
4	EOL 4k7



Anti-Masking PIR configuration

Number	Description
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 (-30%)	1kΩ	1.3kΩ (+30%)	23kΩ	N/A	Infinite
SINGLE_1K5	1.1kΩ (-27%)	1.5kΩ	2.1kΩ (+40%)	23kΩ	N/A	Infinite
SINGLE_2K2	1.6kΩ (-28%)	2.2kΩ	2.9kΩ (+32%)	23kΩ	N/A	Infinite
SINGLE_4K7	3.1kΩ (-22%)	4.7kΩ	6.3kΩ (+24%)	23kΩ	N/A	Infinite

EOL Type	Quiescent			Alarm		
	Min	Nom	Max	Min	Nom	Max
SINGLE_10K	7kΩ (-30%)	10kΩ	13kΩ (+30%)	23kΩ	N/A	Infinite
SINGLE_12K	8.5kΩ (-30%)	12kΩ	15.5kΩ (+30%)	23kΩ	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)	700Ω (-30%)	1kΩ	1.3kΩ (+30%)	1.5kΩ (-25%)	2kΩ	2.5kΩ (+25%)
Mask_1K_1K_2K2 (1K / 1K / 2K2)	700Ω (-30%)	1kΩ	1.3kΩ (+30%)	1.5kΩ (-25%)	2kΩ	2.6kΩ (+30%)
Mask_4K7_4K7_2K2 (4K7 / 4K7 / 2K2)	3.9kΩ (-18%)	4.7kΩ	5.6kΩ (+20%)	8.4kΩ (-11%)	9.4kΩ	10.3kΩ (+10%)

EOL Type	Fault			Masking		
	Min	Nom	Max	Min	Nom	Max
Mask_1K_1K_6K8	2700Ω (-69%)	8.8kΩ	12.6kΩ (+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	400Ω (-20%)	470Ω	700kΩ (+40%)	1.1kΩ (-27%)	1.5kΩ	2kΩ (+34%)
DUAL_1K0_1K0	700Ω (-30%)	1kΩ	1.3kΩ (+30%)	1.5kΩ (-25%)	2kΩ	2.6kΩ (+30%)
DUAL_1k0_2k2	1.6kΩ (-28%)	2.2kΩ	2.9kΩ (+32%)	2.3kΩ (-29%)	3.2kΩ	4.2kΩ (+32%)
DUAL_1k5_2k2	1.6kΩ (-28%)	2.2kΩ	2.9kΩ (+32%)	2.7kΩ (-28%)	3.7kΩ	4.8kΩ (+30%)

EOL Type	Quiescent			Alarm		
	Min	Nom	Max	Min	Nom	Max
DUAL_2K2_2K2	1.6kΩ (-28%)	2.2kΩ	2.9kΩ (+32%)	3.4kΩ (-23%)	4.4kΩ	5.6kΩ (+28%)
DUAL_2k2_4k7	4.1kΩ (-13%)	4.7kΩ	5.4kΩ (+15%)	6kΩ (-14%)	6.9kΩ	7.9kΩ (+15%)
DUAL_2K7_8K2	7.2 kΩ (-13%)	8.2kΩ	9.2kΩ (+13%)	9.9kΩ (-10%)	10.9kΩ	11.9kΩ (+10%)
DUAL_3K0_3K0	2.1kΩ (-30%)	3.0kΩ	3.9kΩ (+30%)	4.5kΩ (-25%)	6kΩ	7.5kΩ (+25%)
DUAL_3K3_3K3	2.3kΩ (-26%)	3.3kΩ	4.3kΩ (+31%)	4.9kΩ (-26%)	6.6kΩ	8.3kΩ (+26%)
DUAL_3K9_8K2	7.0 kΩ (-15%)	8.2kΩ	9.5kΩ (+16%)	10.5kΩ (-14%)	12.1kΩ	13.8kΩ (+15%)
DUAL_4K7_2K2	1.6kΩ (-28%)	2.2KΩ	2.9kΩ (+32%)	5kΩ (-28%)	6.9kΩ	8.8kΩ (+28%)
DUAL_4K7_4K7	3.3kΩ (-30%)	4.7kΩ	6.1kΩ (+30%)	7kΩ (-26%)	9.4kΩ	11.9kΩ (+27%)
DUAL_5K6_5K6	4.0kΩ (-26%)	5.6kΩ	7.2kΩ (+29%)	8.3kΩ (-26%)	11.2kΩ	14.1kΩ (+26%)
DUAL_6K8_4K7	3.3kΩ (-30%)	4.7kΩ	6.1kΩ (+30%)	8.1kΩ (-30%)	11.5kΩ	14.9kΩ (+30%)
DUAL_2k2_10K	9.2kΩ (-8%)	10kΩ	10.8kΩ (+8%)	11.3 kΩ (-8%)	12.2kΩ	13.2kΩ (+9%)
DUAL_10k_10k	7.5kΩ (-25%)	10kΩ	12.5kΩ (+25%)	17kΩ (-15%)	20kΩ	23kΩ (+15%)

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

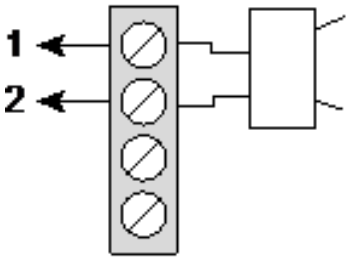
9.6 Wiring an external SAB bell

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.

9.7 Wiring an internal sounder

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



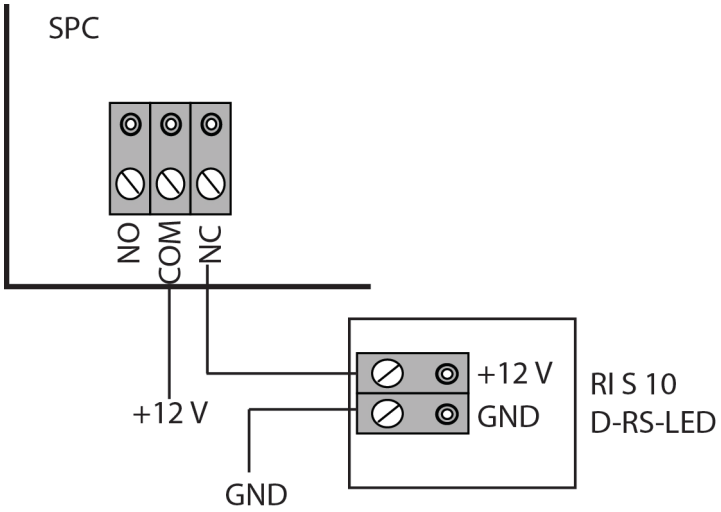
Internal sounder wiring (12V)

IN–	IN– (SPC controller)
IN+	IN+ (SPC controller)

9.8 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.

9.9 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 may result in a CRC error.

For installation details, see the corresponding Installation Instruction.

Installation guides are available at https://vanderbiltindustries.com/download-center.

10 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 *Wiring of mains cable to the controller* on page 276 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.

After the operating voltage is applied to the alarm panel, operational readiness is achieved after 15 seconds.

10.1 Powering from battery only

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

1. Press and hold the PSU Kickstart button (See *Controller Hardware SPC42/SPC52/SPC53/SPC63* on page 31).
   All PCB LEDs flash.
2. Release the PSU Kickstart button.

NOTICE: The battery will continue to power the system until deep discharge level (10.5V to 10.8V) 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.

11 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
- SPCK520/521 — referred to throughout this document as the Compact Keypad

11.1 SPCK420/421

This section covers:

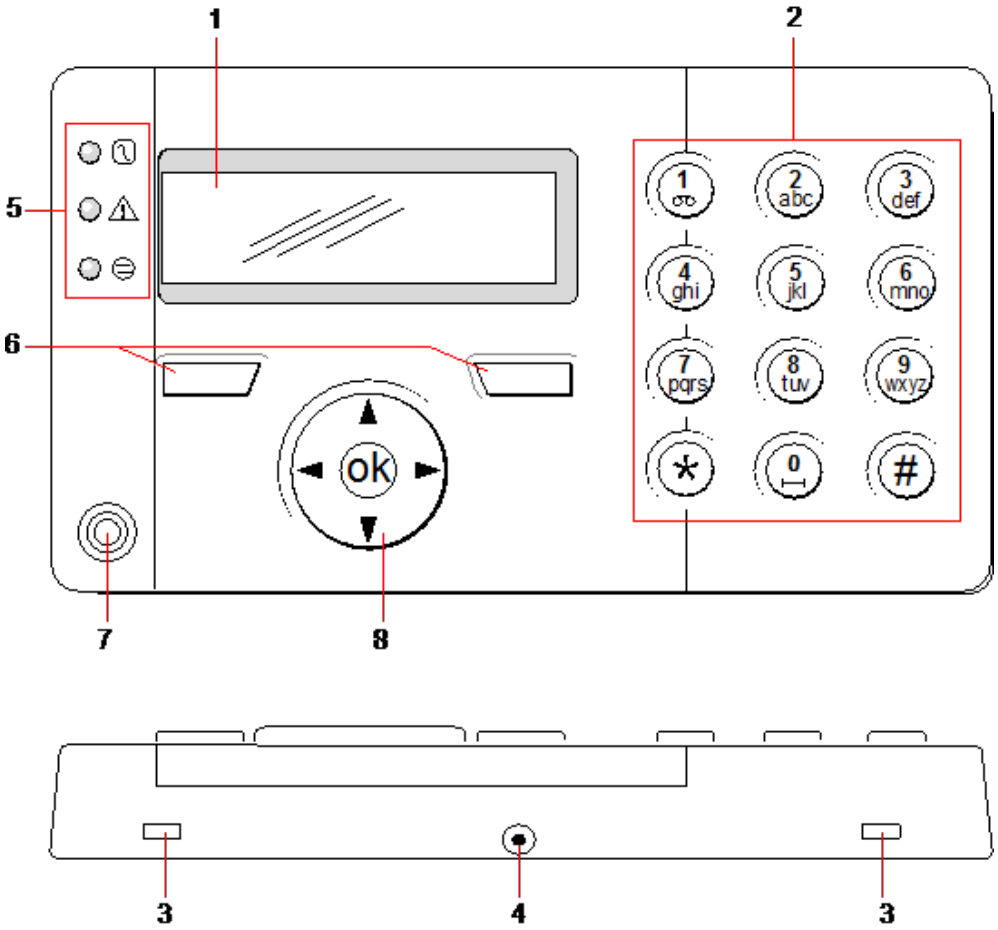
11.1.1 About the LCD keypad

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. (See 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).



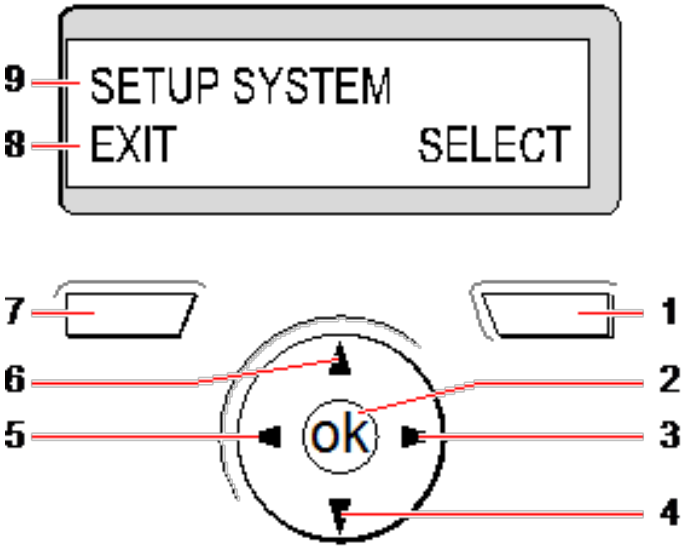
LCD keypad

Number	Name	Description
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.

Number	Name	Description
7	Proximity device receiver area	If the keypad has been fitted with a proximity device receiver (see), 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

11.1.2 Using the LCD keypad interface



Keypad display

Number	Name	Description
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 *Prioritization of display messages* on the facing page.)
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.

Number	Name	Description
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
  - – Housing 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

** A WPA is compatible with Wireless Module SPCW120,WRTX.*

11.1.3 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 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 *Engineer PINs* below.

12.1 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 a full review of Full Engineer menu options, see *Engineer programming via the keypad* on page 66.

[Soft] Engineer mode

Soft Engineer mode provides fewer programming functions and does not affect any outputs programmed in the system. For a full review of [Soft] Engineer menu options, see *Soft Engineer programming via the keypad* on page 65.

12.1.1 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 two digits. Therefore, the default Engineer PIN will be ‘001111’.

Increasing the number of digits for the PIN (see *Options* on page 169) 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.

12.2 Programming with the 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.

12.3 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 and hold the Reset button on the PCB .

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

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* on page 267.

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 to the panel, see *Upgrading Languages* on page 246. To add other languages to a keypad, see the documentation for that keypad. Installation guides are available at https://vanderbiltindustries.com/download-center.

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 or web browser.

See also

Domestic, Commercial and Financial mode default settings on page 267

12.4 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, that is, if a 4 digit PIN is used then all user PINs between 0000 and 9999 would be permissible.

See *Users* on page 88 or *Users* on page 138.

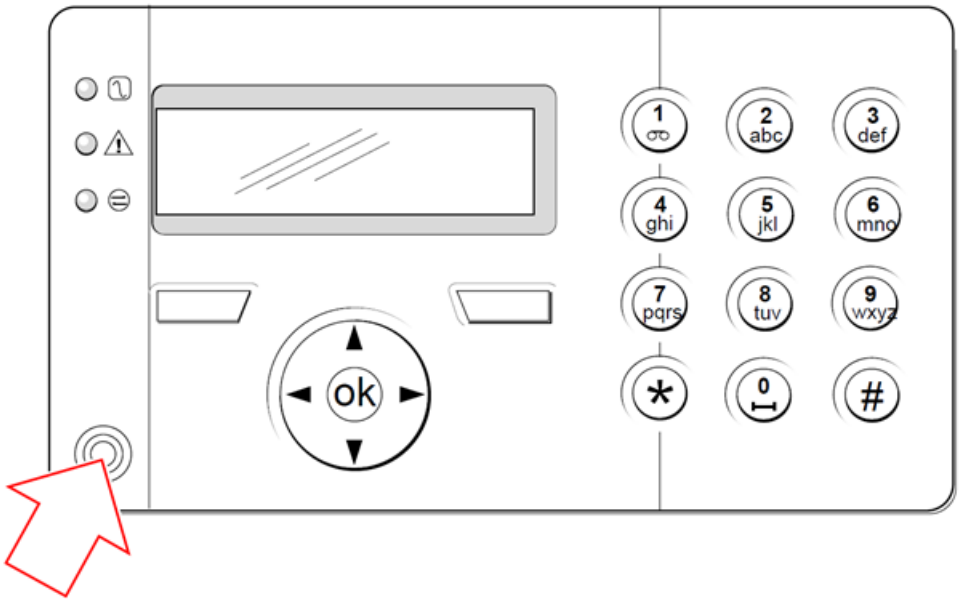
The ability to grant manufacturer access to the system (for example, allow a firmware upgrade of the panel) is configured as a user right for a user profile. If a user is going to be enabling firmware upgrades, ensure that the user has the correct profile for this purpose.

See also

Engineer PINs on page 59

12.5 Programming the portable PACE

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* on page 59.)
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 *Engineer PINs* on page 59.)
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.

12.6 Configuring wireless fob devices

If a wireless module SPCW120, WRTX 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 *Engineer PINs* on page 59.)
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 ENROL DEVICE displays.
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 *Engineer PINs* on page 59.)
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.

12.6.1 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.

13 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 *Engineer PINs* on page 59.)
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.

Number	Name	Description
1	SETTING	Performs an Unset, Fullset or Partset on the system.
2	INHIBIT	Displays a list of the Inhibited zones on the system.
3	ISOLATE	Allows the engineer to isolate zones on the system. See *Isolate* on page 116.
4	EVENT LOG	Displays a list of the most recent events on the system. See *Event Log* on page 117.
5	ACCESS LOG	Displays a list of the most recent access to the system. See *Access Log* on page 117.
6	ALARM LOG	Displays a list of recent alarms. See *Alarm Log* on page 117.
7	CHANGE ENG PIN	Allows the engineer to change the Engineer PIN. See *Change Engineer Pin* on page 118.
8	USERS	Allows the engineer to add, edit or delete users. See *Users* on page 88.
9	SMS	Allows the user to add, edit or delete SMS details for users. See *SMS* on page 118.

See also

Test on page 113

Door Control on page 121

Engineer programming via the keypad on page 66

Installer Text on page 120

Set Date/Time on page 120

SMS on page 118

14 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 *Engineer PINs* on page 59.)
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 (for example, a zone attribute). The selected parameter is displayed with a * (for example, *Inhibit).

   Upon completion of the programming options, the keypad displays UPDATED momentarily.

Please note that a * at the start of a menu item indicates that the item is already selected.

14.1 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 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.

14.2 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	Determines the Security Grade of the SPC Installation. • Irish and European Regions: –EN50131 Grade 2 –EN50131 Grade 3 –Unrestricted • UK Region: –PD6662 (EN50131 Grade 2 based) –PD6662 (EN50131 Grade 3 based) –Unrestricted • Swedish Region: –SSF1014:3 Larmclass 1 –SSF1014:3 Larmclass 2 –Unrestricted • Belgium Region: –TO-14 (EN50131 Grade 2 based) –TO-14 (EN50131 Grade 3 based) –Unrestricted • Switzerland Region: –SES Grade 2 –SES Grade 3 –Unrestricted • Spanish Region –EN50131 Grade 2 –EN50131 Grade 3 • German Region –VdS Class A –VdS Class C –Unrestricted • France –NFtyp2 –NFtyp3 –Unrestricted	Grade: 2 Country: n/a

Variable	Description	Default
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 *Commercial mode operation* on page 251), DOMESTIC (see *Domestic mode operation* on page 252) or FINANCIAL.	Domestic

See *Options* on page 169 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 3K3 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/1K8 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 NTP

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

14.3 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
- 2nd row: Keypad

Timer	Description	Default
Audible		
Internal Bells INT BELL TIME	Duration that internal sounders will sound when alarm is activated. (0–999 minutes; 0 = never)	15 min.
External Bells EXT BELL TIME	Duration that external sounders will sound when alarm is activated. (0–999 minutes; 0 = never)	15 min.

Timer	Description	Default
External Bell Delay EXT BELL DELAY	This will cause a delayed activation of the external bell. (0–999 seconds)	0 sec.
External Bell Delay Partset	Delay period before external bells are activated in partset mode.	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	**Note:** This option is only available for certain **Grade** and **Confirmation** option combinations. (See *Options* on page 169 and *Standards* on page 184.) 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. (0–60 minutes)	30 min.
Confirmed holdup	**Note:** This option is only available for certain **Grade** and **Confirmation** option combinations. (See *Options* on page 169 and *Standards* on page 184.) 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 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. (0–999 seconds)	30 sec.
Partset Dialer Delay	Delay period after a Partset alarm has been activated before system makes a call to ARC.	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. (10–250 seconds)	10 sec
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.

Timer	Description	Default
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.
Strobe on Fullset FULLSET STROBE	Activates the strobe on the external bell momentarily to indicate a full set condition. (0–10 seconds)	0 sec.
DELAY UNSET BUZZER TIME		1 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)	10sec.
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.
Auto Restore Delay	Time to delay auto restore after zone state returns to normal. (0–9999 seconds)	0 sec.
Lockout Post Alarm LOCKOUT POST ALARM	The duration of time after an alarm before the user can gain access. (1–120 minutes)	30 min.
Access Time	The duration of time the system can be accessed by an alarm access user after the Lockout Time has elapsed. (10–240 minutes)	120 min
External Bell Strobe STROBE TIME	Duration that the strobe output will be active when an alarm is activated. (1–999 minutes; 0 = indefinitely)	15min.
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)	0min.
RF Jamming Delay	The time after RF Jamming has been detected before an alert is activated by the system. (0–999 seconds)	0min.
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.

Timer	Description	Default
Engineer auto log out ENG AUTO LOG OUT	Duration of inactivity after which the engineer will be automatically logged out. (0–300 minutes)	0 min.
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 sec.
CODE LOCKOUT		10 sec
CODE LOCKOUT 2		10 sec
Lockout time		90 sec
Fire		
Fire Pre-alarm FIRE PRE-ALARM	Number of seconds to wait before reporting fire alarm for zones with ‘Fire pre-alarm’ attribute set. See *Editing a zone* on page 185. (1–999 seconds)	30sec.
Fire recognition FIRE RECOGNITION	Extra time to wait before reporting file alarm for zones with ‘Fire pre-alarm’ and ‘Fire Recognition’ attributes set. See *Editing a zone* on page 185. (1–999 seconds)	120sec.
PIN		
PIN Valid PIN VALID	Period for which pin is valid. (1–330 days)	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 days)	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 time synchronization will not take place. Time synchronization only takes place if system time and update time are outside this limit. (0–300 seconds)	0 sec.
Link Timeout LINK TIMEOUT	Timeout for Ethernet link fault. (0–250 seconds; 0 = Disabled)	0 sec.
Camera Offline CAMERA OFFLINE	Time for camera to go offline. (10–9999 seconds)	10 sec.

Timer	Description	Default
Frequent FREQUENT (!)	This attribute only applies to remote services. The number of hours within which a zone must open if the zone is programmed with the **Frequent** attribute. (1–9999 hours)	336 h (2 weeks)
Duress silent	Time when duress will remain silent and not restorable from keypad. (0–999 minutes)	0 min.
Holdup/panic silent	Number of minutes that a holdup/panic will remain silent and cannot be restored from the keypad. (0–999 minutes)	0 min.

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.

Valid settings/ranges may be dependent on the security grade specified under **Configuration > System > Standards**.

14.4 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: • DESCRIPTION • ENTRY EXIT – ENTRY TIMER – EXIT TIMER – NO EXIT TIMER – FOB ENTRY ACTIVE • PARTSET A/B – ENABLED/DISABLED – TIMED – ACCESS TO E/EXIT – E/EXIT TO ALARM – LOCAL – NO BELLS • LINKED AREAS – AREA – FULLSET – FULLSET ALL – PREVENT FULLSET – PREVENT FULLSET ALL – UNSET – UNSET ALL – PREVENT UNSET – PREVENT UNSET ALL • SCHEDULE – CALENDAR – AUTOMATIC SET/UNSET – TIME LOCKED – VAULT ACCESS • REPORTING – EARLY TO SET – LATE TO SET – EARLY TO UNSET – LATE TO UNSET • SET/UNSET – 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* on page 186 for further details on these options.

14.5 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.

14.6 X-BUS

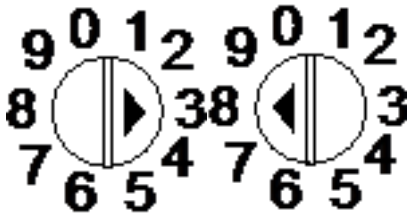
1. Scroll to XBUS and press SELECT.
2. Scroll to the desired programming options.

14.6.1 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 figures below show the rotary switches, and each rotary switch with an arrow symbol pointing to a number for identification (that is, 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

Number	Description
1	 Rotary switches identifying expander as 38.

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

14.6.2 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**.

14.6.3 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.

14.6.4 Keypads/Expanders/Door Controllers

14.6.4.1 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 to enable the Engineer to locate the device.
4. Press BACK to exit.

   Locate keypads using the same menus and following the keypad choice instead of expander.

14.6.4.2 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.

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)

6. Press BACK to exit.

14.6.4.3 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.

Setting	Description
Description	Enter a unique description to identify the keypad.

Setting	Description
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 *Calendars* on page 197.
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.

Setting	Description
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 and 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.
Mapping gate	Select if keypad should be limited by a mapping gate.

Setting	Description
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.

14.6.4.4 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.

Editing IO Expanders

The following table lists the available options for IO expanders:

Function	Description
Description	Edit the description of the expander.

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.

Name	Description
VOLUME LIMIT	Select the volume limit.

Editing Wireless Expanders

The following table lists the available options for Wireless expanders:

Function	Description
Description	Edit the description of the expander.

Editing Analysed IO Expanders

The following table lists the available options for IOA expanders:

Name	Description
Description	Edit the description of the expander.

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: • None • Unset • Partset A • Partset B • Fullset • Toggle Unset/Fullset • Toggle Unset/Partset A • Toggle Unset/Partset B • All Okay • Setting Authorisation

Name	Description
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: • FUNCTION — the following options are available: – 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: – 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: – 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: • 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

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.

Name	Description
VISUAL INDICATIONS (Flexible mode only)	Enables you to assign specific behaviour to each LED on the keyswitch expander. Each of the LEDs has the following options: • FUNCTION — the following options are available: – 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: – 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: – Permanent — always on. • Flash Fast/Medium/Slow — varying speed of the flashing.
DEACTIVATION (Flexible mode only)	Select a deactivation method from the available options: • Calendar — select a calendar.
KEY POSITIONS	Enables you to assign behaviour to specific key positions for specific areas. Select an area for the key position, and assign one of the following options to that area: • None • Unset • Partset A • Partset B • Fullset • Toggle Unset/Fullset • Toggle Unset/Partset A • Toggle Unset/Partset B • All Okay • Setting Authorisation

14.6.4.5 Edit Door Controllers

For further information about Door controllers, see *Door Expander* on page 34.

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 and 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 on page 34

14.6.5 Addressing Mode

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

Automatic addressing

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 value X 8)+1)= first zone number and then the next 7 sequential zones. For example ((ID2 x 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 42: Expander ID 1–3. SPC 52/53: Expander ID 1–15. SPC 63: 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 (for example, 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.

14.6.6 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.

14.6.7 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.

14.6.8 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.

14.7 Users

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

14.7.1 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 **OK**.

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.

14.7.2 Edit

To edit users on the system:

1. Scroll to **USERS>EDIT**.
2. Press **OK.**
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.
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: • ADD CARD • LEARN CARD If a card assigned to the user: • EDIT CARD – CARD NUMBER – CARD ATTRIBUTES • RESET CARD • DELETE CARD
LANGUAGE	Select a language for this user that will be displayed on the system.

14.7.2.1 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 **OK**.
3. Select the user which should be configured and press **OK**.
4. Scroll to **ACCESS CONTROL** and press **OK**.

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

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 **OK**.

   An empty card has been added and can now be edited.

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 **OK**.
3. Select the door that the card will be presented.
4. Press **OK**.

   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.

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 **OK**.
3. Edit the desired user setting shown in the table in *Access Control* below.
4. Press **BACK** to exit.

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.

Attribute	Description
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: • SPC42 – all users • SPC52/53 – 512 • SPC63 – 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.

Delete Card

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

1. Scroll to **DELETE CARD**.
2. Press **OK**.

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 **OK**.

14.7.3 Delete

To delete users on the system:

1. Scroll to **USERS>DELETE.**
2. Press **OK**.

   A prompt displays, confirming command to delete.
3. Press **YES** to delete the user.

14.8 User Profiles

See also

Adding/Editing User Profiles on page 141

14.8.1 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 **OK**.
2. Enter a customized user profile name and press **ENTER**.

   The keypad confirms that the new user profile has been created.

14.8.2 Edit

To edit user profiles on the system:

1. Scroll to **USER PROFILES>EDIT**.
2. Press **OK.**
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* on page 141.
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.

14.8.3 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 **OK**.

   You are prompted to confirm deletion.
4. Press **OK** to delete the user profile.

14.9 Wireless

Wireless sensor support on the SPC panel is provided by two way wireless modules SPCW120, WRXT (868MHz).

The SPC two way wireless module is fitted into modem slot 2 of the

control panel. See the table below for information on which devices can be enrolled with each type of SPCW120 Wireless Transceiver.

For CE regulatory compliance, the SPCW120 product can only be fitted to the following products:

- SPC53
- SPC63
- SPC42
- SPC52
- SPC5350.320-L1
- SPC6350.320-L1

Devices compatible with a two way transceiver

Sensors	**WPIR**	Wireless 12m PIR detector with pet immunity option
	WPIR-CRT	Wireless curtain PIR detector
	WMAG	Wireless magnetic contact (slim)
	WMAG-I	Magnetic contact with additional input
	WSMK	Wireless smoke detector
	WMAG-S	Wireless shock sensor
	WPIR-EXT	Wireless external PIR sensor
	WFLOOD	Wireless flood sensor
	WGB	Wireless Glass Break sensor
Outputs	**WSIR-INT**	Wireless indoor sounder
	WSIR-EXT	Wireless outdoor sounder
Repeaters	**WRPTR**	Wireless signal repeater plug
Keypads	**WKPD**	Wireless keypad
Fobs	**WRMT**	Remote control with 4 button control
	WPAN	Wireless personal alarm button

For instructional videos on wireless devices and transceivers please go to http://van.fyi?Link=Wireless_devices

14.9.1 Select a wireless programming option

To select a wireless programming option:

1. Scroll to **WIRELESS** and press **OK**.
2. Scroll to the desired programming option. Options are described in the following table:

SENSORS		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. The following options are available for sensors: • **ADD** See *16.7.1 Add Sensors* on page 1. • **EDIT** (Change zone assignment) See *Edit Sensors (Zone Assignment)* on page 1 • **REMOVE** Select the device or sensor to be deleted.
OUTPUTS		• **ADD** See on page 1. • **EDIT** See on page 1 • **REMOVE** Select the device or sensor to be deleted.
REPEATERS		• **ADD** See on page 1. • **EDIT** See on page 1 • **REMOVE** Select the device or sensor to be deleted.
WPA[1]		Add, edit or remove a WPA (Wireless Personal Alarm). • **ADD** See *16.7.3 Add WPA* on page 1. • **EDIT** See *16.7.4 Edit WPA* on page 1. • **REMOVE** Select the WPA to be deleted.
SETTINGS		
	2 WAY WIRELESS	Enable or disable two way wireless depending on the transceiver you are using. Enable two way wireless if you are using SPCW120 Wireless Transceiver. Disable two way wireless if you are using aSiWay RF Kit (SPCW120 or WRTX) and not using a SPCW120 Wireless Transceiver.
	FILTER LOW SIGNL	Enableto configure the panel to disregard low strength signals (RF strengths 0 and 1).
	DETECT RF JAM	Enable to activate an alert on detection of RF interference.

	WIRELESS LOST	Enable to send a Wireless Lost event over CID/SIA and FLexC on loss of wireless signal.
	SUPERVISION TIME	Browser option is **Supervision** ("Two way Wireless Supervision time in minutes")
	EXTERNAL ANTENNA	Enable an external antenna.
	SUPERVISION	Enable tamper supervision. Browser option is **Missing Supervision** ("Select whether missing supervision for a sensor will raise a zone tamper")
	RF FOB SOS	Disable the RF FOB SOS or specify the panel action from the following options: PANIC, PANIC SILENT, USER MEDIC, USER HOLDUP, RF OUTPUT.
	WPA TEST SCHED.	Enter a maximum period (in days) between WPA tests. Max is 365 days, 0 days means that the WPA test disabled.
	PREVENT SET TIME	Enter a time in minutes after which, if the sensor or WPA fails to report, setting is prevented for the area where the wireless zone is. Max is 720 minutes, 0 minutes means that checking is disabled.
	DEVICE LOST TIME	Enter the number of minutes after which the wireless device is reported as lost if it fails to report within this time frame. (Min is 20 and max is 720 minutes. 0 means that checking is disabled.)

[1]*A WPA is compatible with SiWay RF Kit (SPCW120 or WRTX) only.*

14.9.2 Two way wireless

The following devices can be enrolled on a two way wireless transceiver:

- Wireless sensors (motion detectors, magnetic contacts, smoke alarms)
- Wireless outputs (internal and external sirens)
- Wireless repeaters
- Wireless keypads
- WPAN personal alarm button
- WRMT remote control

Please note that you must enable two way wireless before enrolling these devices.

To enable two way wireless:

1. Scroll to **WIRELESS** and press **OK**.
2. Scroll to **SETTINGS** and press **OK**.
3. Scroll to **2 WAY WIRELESS** and select **ENABLE**

The SPCW120 Wireless Transceiver with firmware 4.7.x or later can support up to the following number of devices:

- 64 detectors
- 16 output sirens
- 8 wireless keypads
- 4 repeaters
- 20 fobs (personal alarm buttons and/or remote controls)

To upgrade the transceiver firmware to version 4.7.x, you must ensure that no more than 20 fobs (remote controls or personal alarm buttons) are configured on your SPC system. If there are more than 20 fobs configured, delete any excess fobs.

The combined maximum number of synchronous devices (wireless keypads and sirens) should not exceed 16 per transceiver.

14.9.2.1 Add wireless sensor

Add a wireless sensor using a keypad:

1. Login as **FULL ENGINEER**.
2. On the keypad, select **WIRELESS>SENSORS>ADD>ENROL**.
   The keypad displays the **ADD** screen with a flashing **ENROL DEVICE** message.
3. Open the detector.
4. Insert the battery taking care to observe correct polarity. Inserting the battery starts the discovery process from the device.
   The keypad displays the **FOUND SENSOR** message.
5. Click **OK**.
6. You can now enroll the device by configuring the **AREA, ZONE TYPE** and **ZONE** settings.
7. Click **OK**.
   The keypad displays the **UPDATED** message.

The wireless sensor is now enrolled on your SPC system. Please note that the initialization delay time can be up to 40 seconds.

14.9.2.2 Add wireless output

Add a wireless output using a keypad:

1. Login as **FULL ENGINEER**.
2. Select **WIRELESS > OUTPUTS > ADD > ENROL** to display the **ADD** screen with a flashing **ENROL DEVICE** message.
3. Remove the cover.
4. Power up the output by inserting and connecting the battery. Connecting the battery starts the discovery process.
5. When the discovery process succeeds, the keypad displays the **FOUND OUTPUT** screen with the device ID, the output TYPE, and the SIGNAL level.
6. Click **OK** to confirm and to display the **ADD** screen.
7. Identify the output by entering a description (maximum 16 characters) and click **OK** to display the **BELL TYPE** screen.
8. Select the **BELL TYPE** and click **OK**.
9. The keypad beeps twice and flashes the **UPDATED** message before returning to the **OUTPUTS** screen.

The output is now enrolled on your SPC system.

Select **EDIT** to configure the **VOLUME, AREA**, and **TAMPER OPTION** settings.

14.9.2.3 Add wireless repeater

Add a wireless repeater (WRPTR) using a wired keypad:

1. Login as **FULL ENGINEER**.
2. Select **WIRELESS > REPEATERS > ADD**.
   The keypad displays the **ADD** screen with a flashing **ENROL DEVICE** message.
3. Plug the WRPTR into an EU mains (220v AC) socket. Plugging in starts the discovery process from the WRPTR.
   When the discovery process succeeds, the keypad displays the **FOUND REPEATER** screen with the unique Repeater ID and the Signal Level.
4. Click **Enter** to confirm and to display the **ADD** screen.
5. (Optional) Enter up to 16 characters in the Description field to help identify the location of the WRPTR.
6. Click **Enter** to confirm and to display the **REPEATER TYP/LOC** screen.
7. Select **Standalone** in the **REPEATER TYP/LOC** drop-down.
8. Click **Enter**.
   The keypad briefly displays an **UPDATED** message and returns to the **REPEATERS** screen.

The WRPTR is now enrolled on your SPC system.

14.9.2.4 Add wireless keypad from a wired keypad

Add a wireless keypad using a wired keypad:

1. Login as **FULL ENGINEER**.
2. On the keypad, select **WIRELESS > KEYPADS > ADD > ENROL**.
   The keypad displays the **ADD** screen with a flashing **ENROL DEVICE** message.
3. Open the wireless keypad .
4. Insert the batteries taking care to observe correct polarity. Inserting the batteries starts the discovery process from the device.
   The keypad displays the **FOUND KEYPAD** message.
5. Click **OK**.
   You can now enroll the device by specifying the Description and the AREA settings.
6. Click **OK**.
   The keypad displays the **UPDATED** message.

The wireless keypad is now enrolled on your SPC system.

14.9.2.5 WPAN personal alarm button

The WPAN personal alarm button is a device that is used to transmit Panic Alarm messages to the SPC system.

The user can wear the WPAN in one of two ways:

- WPAN can be worn as a wrist watch (by inserting the wrist band into the two slits of the appropriate ring holder).
- WPAN can be worn as a pendant by removing the wrist ring holder and replacing it with the pendant ring holder.

Enrol a WPAN personal alarm button

To enrol the WPAN and assign it to a User(n):

1. Select **USERS > EDIT > USER(n) > RF FOB > ENABLED.**

   The keypad displays the **ADD** screen with a flashing **ENROL DEVICE** message.

2. On the WPAN, press and hold the button.

   The LEDs on the fob light in the following pattern: Red lights for 3 seconds, then no LED, then Red lights for 1 second, and then Green lights for 1 second. The WPAN is assigned to User (n).

Disable a WPAN personal alarm button

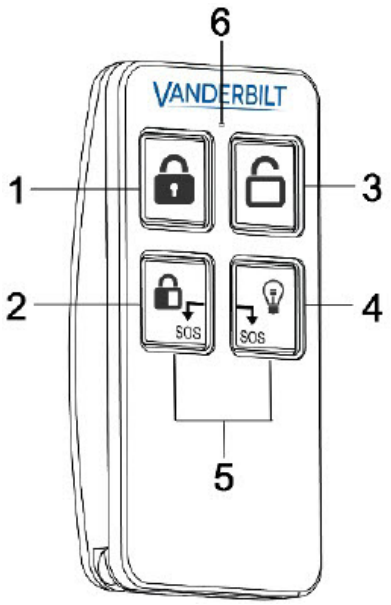
To disable the WPAN:

Select **USERS > EDIT > USER(n) > RF FOB > DISABLED.**

A message appears on-screen saying **UPDATED**.

14.9.2.6 WRMT remote control

The WRMT 4-button Remote is a device which allows a user to remotely operate the SPC system. The device supports **UNSET**, **FULLSET**, and **PARTSET** (A only) functionality, as well as the operation of defined outputs and an **SOS** feature.



1	Fullset
2	Partset (A only)
3	Unset
4	Output
5	Panic/SOS
6	LED

Enrol a WRMT remote control

To enrol the WRMT and assign it to a User (n):

1. Select **USERS > EDIT > USER (n) > RF FOB > ENABLED.**

   The keypad displays the **ADD** screen with a flashing **ENROL DEVICE** message.

2. On the WRMT, press and hold the two **SOS** buttons.

   The LED blinks Red once and then Green to confirm enrolment. A message appears on the keypad screen saying **FOB CONFIGURED**. The WRMT is assigned to the User (n).

Disable a WRMT remote control

To disable a WRMT:

- Select **USERS > EDIT > USER (n) > RF FOB > DISABLED.**

  A message appears on-screen saying **UPDATED**.

When you disable a WRMT from your system, you must also clear the internal registration in the WRMT before you can re-use the WRMT.

To clear the internal registration:

- On the WRMT, press and hold the **PARTSET** and **UNSET** buttons.

  The LED blinks Red and Orange to confirm that registration is cleared.

14.10 Zones

1. Scroll to ZONES and press OK.
2. Scroll to the desired zone (ZONE 1-x).
3. 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 *Zone types* on page 278.
ATTRIBUTES	Determines the attributes of the zone. See *Zone attributes* on page 283.
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.

14.11 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	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. If the door position sensor is assigned to an intrusion zone, it can be configured like a normal zone but only with limited functionality (for example, not all zone types are selectable). 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.
Description (Web only)	Description of the zone the door position sensor is assigned to.
Zone Type (Web only)	Zone type of the zone the door position sensor is assigned to (not all zones types are available).
Zone attributes (Web only)	The attributes for the zone the door position sensor is assigned to can be modified.
Area (Web only)	The area the zone and the card reader are assigned to. (If the card reader is used for setting and unsetting, this area will be set/unset).
Door Position (Web) DPS End Of Line (keypads)	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)	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.

Name	Description
No DRS (Web 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 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.

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)	Panel/area will unset, when card is presented at entry reader.
Unset inside (Browser)	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)	Panel/area will fullest, when card is presented twice at entry reader.
Fullset inside	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)	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.

14.12 Outputs

Each zone type on the SPC system has an associated output type (an internal flag or indicator). When a zone type is activated, that is, 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 (that is, 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 *Outputs types and output ports* on the facing page, 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 *Output Test* on page 115.

14.12.1 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 *Zone types* on page 278) 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 (for example, 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). See 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.

Output Type	Description
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 11V this output activates. The 'Restore' option for this fault is only presented when the voltage level rises to above 11.8V.
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; that is, 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* on page 159). 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.

Output Type	Description
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, that is, 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 WPA1 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.

Output Type	Description
Entry Status	This output activates if an ‘All Okay’ entry procedure is implemented and there is no alarm generated, that is, 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, that is, 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	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	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, Sigmalock 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: • 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).*

[1] A WPA is compatible with Wireless Module SPCW120,WRTX.

See also

Configuring system latch and auto set outputs on page 159

14.13 Communication

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

14.13.1 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.

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. 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. 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. 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. 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). Note that the flow control must be set the same for both items of equipment.

5. Press BACK to exit.

14.13.2 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, for example, 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 DCHP 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, for example, 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, for example, 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, for example, 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.

14.13.3 Modems

The SPC system supports SPC intelli-modems (PSTN, GSM, GSM (4G)) for communications with analogue lines and mobile network interfacing for enhanced communications and connectivity. The SPC system must be configured accordingly.

14.13.3.1 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

  GSM (4G)
- 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.

14.13.3.2 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, SIGNAL LEVEL, TYPE, and FIRMWARE VERSION then 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. **PSTN modem only** 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	**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. MODE or TIMER MODE - Select a monitoring MODE (DISABLED, ALWAYS ON, FULLSET). The FULLSET option only enables this feature while the system is Fullset. TIMER - Enter the number of seconds for the monitoring TIMER (0–9999 sec). **Note:** EN 50131-9 Confirmation configuration In order for EN50131-9 Confirmation to operate correctly, line monitoring must be enabled. (See on page 169.)

Menu Option	Description
USSD	**GSM Modem only** Enter the Unstructured Supplementary Service Data (**USSD**) code for your service provider in order to enable SMS-free credit checking for Pay As You Go SIMs. Note: This feature is not universally available. Please check with your service provider.
CHECK SIM CREDIT	Enable this feature to receive information on remaining credit balance for Pay As You Go SIMs (where available from your service provider).
NETWORK MODE	**GSM (4G) only** Select the signal type that you wish to the modem to use: • **2G Only** This option enables connection to 2G networks only. • **3G Only** This option enables connection to 3G networks only • **4G Only** This option enables connection to 4G networks only. • **Search 4G First** This option forces the modem to connect to 4G networks where available. If 4G is not available, the modem connects to 2G.

GSM Modem only

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

14.13.4 Central Station

This section covers how to add, edit, and delete a central station , and how to make a test call.

See:

- *Add* below
- *Edit* on the facing page
- *Delete* on the facing page
- *Make Test Call* on the facing page

14.13.4.1 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.

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.

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

14.13.4.2 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.

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.

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

14.13.4.3 Delete

Enables you to delete a configured ARC.

14.13.4.4 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.

14.13.5 SPC Connect PRO

SPC Connect PRO is a desktop application designed to support the installation and maintenance of SPC systems. Using SPC Connect PRO, you can create installations and configure them prior to arriving at site. The tool can also be used in conjunction with the SPC cloud service SPC Connect to remotely connect to customer sites and support them.

To enable and configure SPC Connect PRO support:

1. Scroll to SPC CONNECT PRO and press SELECT.
2. Enable the SPC CONNECT PRO option.
3. Scroll to INTERFACES and press SELECT.
4. Enable/disable the ETHERNET, USB, SERIAL, and MODEM interfaces as required.
5. To enable the TCP interface, select TCP PORT then enter the port number and press SELECT.

14.14 Test

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

14.14.1 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.

14.14.2 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.

14.14.3 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 (for example, CONTROLLER 1 = first zone on Controller).

   See 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; for example, 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.

14.14.4 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.

14.14.5 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.

14.14.6 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.

14.14.7 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.

14.14.8 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 on page 256.

14.15 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.
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.

14.16 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	Isolate the desired alert from EXPANDERS or KEYPADS: • 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.

14.17 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.

14.18 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.

14.19 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

14.20 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.

14.21 SMS

The SPC system support the communication of SMS alerts 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 (SPC4x), 50 (SPC5x) or 100 (SPC6x) 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* on page 67), 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 and tamper

- Setting and unsetting
- Inhibit and isolate
- All other types of events

14.21.1 Add

To add a user

Prerequisites

- A modem is installed and identified by the system.
- The function **SMS Authentication** is activated in OPTIONS (see *Options* on page 67).

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.

14.21.2 Edit

Prerequisites

- A modem is installed and identified by the system.
- The function **SMS Authentication** is activated in OPTIONS (see *Options* on page 67).

1. Scroll to SMS > EDIT and press SELECT.
2. Select an engineer or user SMS ID to edit.

SMS NUMBER	Enter the number to which the SMS will be sent (requires three-digit country code prefix). **Note:** Engineer SMS number can deleted by resetting it 0. User SMS numbers cannot be deleted.
EDIT USER	Select a new user for this SMS ID if required.
EVENT FITLTER	Select the panel events which the user or engineer will receive via SMS. Select ENABLED or DISABLED. Events that are enabled are indicated with an asterisk * before the event in the list.
CONTROL RIGHTS	Select the operations that the user or engineer can perform remotely on the panel through SMS. See *SMS Commands* on page 145

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 **C**alling **L**ine **I**dentity (CLI) is enabled on the line selected to make the call to the SMS network. Consult the PBX administrator for details.

14.21.3 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.

14.22 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.

14.23 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.

14.24 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.

14.25 SPC Connect

Add an SPC Connect ATS to set up a connection between a panel and the SPC Connect website https://www.spcconnect.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.spcconnect.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.spcconnect.com, for remote access to their panel.
COMPANY ID	For future use.
DELETE	To remove an SPC Connect ATS from a panel, select DELETE.

15 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 *Engineer PINs* on page 59.

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.

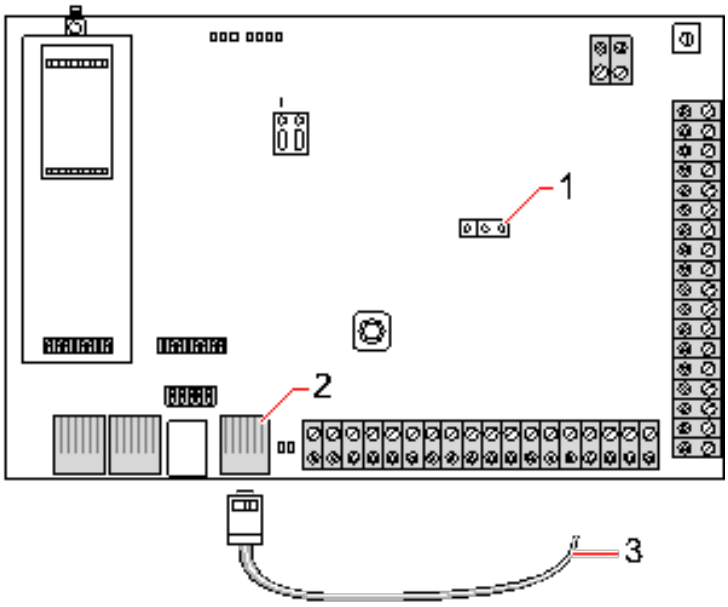
If programming with a browser interface, click **Save** when making changes.
Click **Refresh** to view the current programming values on a web page.

15.1 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.

15.2 Ethernet interface

IP



Connect

Number	Description
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), 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 *Network cable connections* on page 264.

  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 *Engineer PINs* on page 59).
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.

15.3 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 Micro USB type cable. Drivers must be installed to make a USB connection from the controller to the PC.

Prerequisites

- You must have a 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. Click **Next**.

   Windows detects a Generic USB hub.

3. Click **Finish**.

   Windows 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 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, contact your network administrator or a Vanderbilt technician.

8. Click **Continue Anyway**.

   The installation finishes.

9. Click **Finish.**
   The driver is installed.

15.4 Logging into the browser

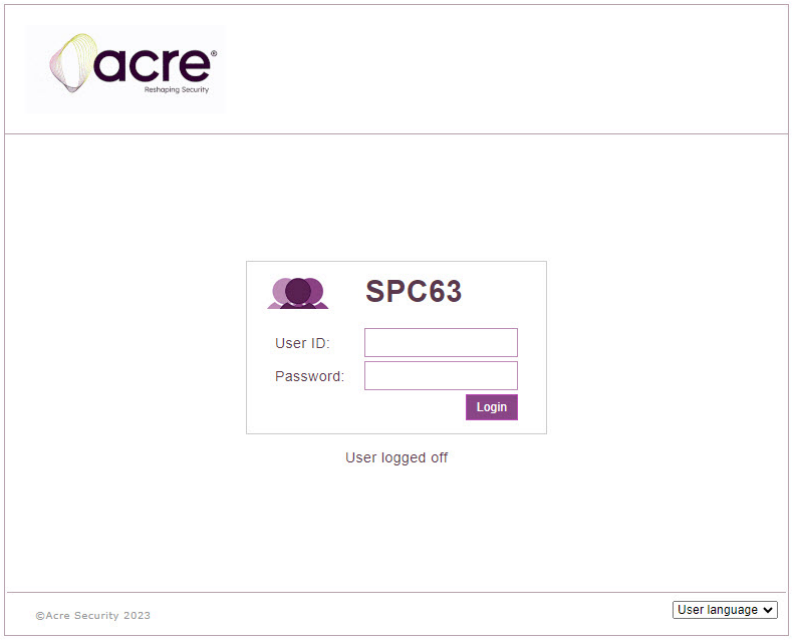
To log into the browser:

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. (For example, http://192.168.1.100.) See the table in *Default setting for WEB server address* on the next page.

   A page with a security message is displayed.

3. Click **Continue to this website**.

   The login page 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 pages. The default language setting ‘Auto’ will automatically load the language assigned to this user ID.
6. Click **Login**.

Default setting for WEB server address

Connection	IP address Web server
Ethernet	192.168.1.100 (default)

15.5 SPC Home

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

15.5.1 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.

NOTICE: If there are alarms on the system, the information message **See alarm tab** displays.

15.5.2 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.

15.5.3 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.

The images are automatically refreshed as per the interval settings for the camera. (See *Configuring Video* on page 205.)

Click the **Pause Refresh** button to retain the current image on the screen and pause refreshing.

Click 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 Com XT or equivalent FlexC supporting CMS software.

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.

Message	Description
Authorization error	User name and/or password are incorrect
Unknown	An unknown error was returned. The camera may be an unsupported model.

15.6 Panel status

This section covers:

15.6.1 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**.

   See following sections for further information.

Performable actions

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

Restore All Alerts	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 page 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.

15.6.2 X-Bus Status

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

   The X-Bus Status page displays showing a list of all detected expanders .

2. Select one of the following tabs.
   - **Expanders** (for programming expanders, see *Expanders* on page 160).
   - **Keypads** (for programming keypads, see *Keypads* on page 165).
   - **Door Controllers** (for programming door controllers, see *Door Controllers* on page 168).
3. Click any of the keypad/expander/door controller identifying parameters (ID, description, type, serial number) to displayed further status details.

15.6.2.1 Expander Status

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

   A list of detected expanders and any associated PSUs displays.
   The following table shows the information that is available.

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 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 any of the expander's identifying parameters (ID, description, type, serial number) to display further status details.
  The following table shows the information that is available.

Name	Description
Communication	The physical status (OK, Fault) and the programmed status (OK, Isolated, Inhibited) of the X-BUS cable connection to the expander.
Housing Tamper	The physical and programmed status of the expander housing 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.

Name	Description
Inhibit ⓵	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.

See also

PSU status below

15.6.2.2 PSU status

The **PSU Status** page 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 table shows the information that is available.

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.
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 table shows the information that is available.

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.

Name	Description
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 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.

15.6.2.3 Keypad Status

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

   A list of detected keypads is displayed.
   The following table shows the information that is available.

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 the **Refresh** button to update the list of detected keypads and their status.

To view more status information:

- Click a keypad's identifying parameters (ID, description, type, serial number) to display further status details.
  The following table shows the information that is available.

Communication	The physical status (OK, Fault) and the programmed status (OK, Isolated, Inhibited) of the keypad cable connection to the expander.
Housing Tamper	The physical and programmed status of the expander housing 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 ⓵	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.

15.6.2.4 Door Controller Status

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

   A list of detected door controllers is displayed.
   The following table shows the information that is available.

Name	Description
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 the **Refresh** button to update the status of the system alerts.

To view more status information:

- Click a door controller's identifying parameters (ID, description, type, serial number) to display further status details.
  The following table shows the information that is available.

Communication	The physical status (OK, Fault) and the programmed status (OK, Isolated, Inhibited) of the keypad cable connection to the expander.
Housing Tamper	The physical and programmed status of the expander housing 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.

15.6.3 Wireless

Wireless sensor detection (868MHz) on the SPC panel is provided by wireless modules. There are two types of wireless modules: one way SiWay RF Kit (SPCW120 or WRTX) and two way SPCW120 Wireless Transceiver. The SiWay RF Kit is fitted in the controller, on the keypad, or by installing a wireless expander. The SPC two way wireless module is fitted into modem slot 2 of the control panel. See the table below for information on which devices can be enrolled with each type of transceiver.

For CE regulatory compliance, the SPCW120 product can only be fitted to the following products:

- SPC42
- SPC52
- SPC53
- SPC62

Devices compatible with a two way transceiver

Wireless sensors	WPIR	Wireless 12m PIR detector with pet immunity option
	WPIR-CRT	Wireless curtain PIR detector
	WMAG	Wireless magnetic contact (slim)
	WMAG-I	Magnetic contact with additional input
WRMT		Remote control FOB with 4 button control
WPAN		Wireless personal alarm button
WSMK		Wireless smoke detector
WMAG-S		Wireless shock sensor with door contact
WFLOOD		Wireless flood sensor
WAGB		Wireless acoustic glass break detector
WPIR-EXT		Wireless external PIR detector
WSIR-INT		Wireless internal sounder
WSIR-EXT		Wireless external sounder
WRPTR		Wireless signal repeater plug
WKPD		Wireless keypad

For instructional videos on wireless devices and transceivers please go to http://van.fyi?Link=Wireless_devices.

15.6.3.1 View a list of wireless sensors

To view a list of wireless sensors and information about the sensors, select **Configuration > Hardware > Wireless**.
The following table shows the information that is available.

Wireless sensor information

Wireless 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.
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 enrolment are not dropped.
Version	The version details of the sensor.
Status	Actuated, Normal,Tamper, Unknown

Performable actions

Log	Click to view the wireless sensor Log. See *Log - Wireless sensor X* below.
Enrol New Sensor	Click to enrol a new sensor.
Refresh	Click to refresh the list of enrolled sensors.
Edit	Click to edit the sensor attributes.
Remove	Click to remove the sensor from the enrolled sensors list.

15.6.3.2 Log - Wireless sensor X

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

1. Click the Log button in the table row for that sensor.
2. The Message log for the sensor displays.
3. Optionally, you can create a text file of the log by clicking **Text File**.

Information provided in the message log

Time	The date and time of the logged event.
Receiver	The wireless receiver location, that is, 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).

15.6.4 Zones

For configuration, see *Editing a zone* on page 185.

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.
   The following table shows the information that is available.

Zone	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, Tech, etc.).
EOL Quality	Displays the EOL quality for the zone state resistance range. Possible values are: • 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. This column is only visible in Engineer mode. For more information on nominal resistance values and their defined ranges, see *Wiring the zone inputs* on page 45.
Input	The detected input state of that zone (Unknown, Open, Closed, Disconnect, Short, Pulse, Gross, Masked, Fault, Out of bounds, Unstable, DC Sub, Noisy). 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. Unstable: An unstable state occurs when the zone input resistance value is not stable over a defined sampling period. Noisy: A Noisy state occurs when an external interference is induced onto the input circuit over a defined sampling period. 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.
Status	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: 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.

Performable actions

Refresh	Updates the status information displayed for the panel.
Log	Click 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* on page 256.
Hide Closed	Click this button to hide all closed inputs.

15.6.5 Doors

1. To view all doors, select **Status > Doors**.

   The following table shows the information that is available.

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.

15.6.6 FlexC Status

This page 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.

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	List of the events currently in the Event Queue. The tables shows the following: • 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: • 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	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. **Network Log:** Click this button to show the network log. **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. **Manual Test** button: Click this button to force a test call. The Event is added to the event queue.

15.6.7 System alerts

1. Select **Status > System Alerts**.

   The following table shows the information that is available.

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, that is, 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.

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.

15.7 Logs

This section covers:

15.7.1 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.

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.

15.7.2 Access Log

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

1. Select **Log > Access log**.
2. Create a text file of the log by clicking on the **Text File** button.

15.7.3 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

15.8 Users

The following table shows the maximum number of users, user profiles and user devices for the panel:

Maximum No.	SPC4xx	SPC5xx	SPC6xx
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	20

WARNING: If upgrading from a firmware version prior to version 3.3, 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 *Adding/Editing User Profiles* on page 141). Review all user configuration after a firmware upgrade.

- The default Engineer ID is changed from 513 to 9999.

15.8.1 Adding/Editing a User

To add or edit a user:

1. Select **Users>Users**.

   A list of configured users displays.

2. Click the **Add User** button or click the **Edit** button of the required user.
3. Enter a **User ID** that is not currently being used. If you enter an ID that is already used, an 'Invalid ID' message is displayed when you select **Generate PIN**.
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. You can enable the **Alarm Access** option to grant time-limited access to the system for this user within a specific window.

   The time limits for this option are set in the **System Timers** page. Go to **Configuration>System>System Timers** to configure this option. See *Timers* on page 179.

   In normal mode any user with this attribute selected is unable to access the system.

8. Select the appropriate user profile (see *Adding/Editing User Profiles* on page 141) for this user.
9. 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 (see *Options* on page 169).

The **Duress** option is only available on this page 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 (for example, 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.

Attribute	Description
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: • 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.

15.8.1.1 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 edit user settings 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.

15.8.2 Adding/Editing User Profiles

NOTICE: Global user profiles cannot be edited in the browser and must be edited in SPC Manager.

To add or edit a user profile:

1. Select **Users>User Profiles**.

   A list of configured profiles displays with the number of users assigned to each profile.

2. Click **Add User Profile** or click the **Edit** button of the required profile.

   The configuration options are categorized as follows:

   - General Settings

   - User/Panel Rights

   - Access Control

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		
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.
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.

Right	User Profile Type Default	Description
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.
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.
Delay Auto Set	Standard* Manager	User can delay or cancel autosetting.
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 on the keypad each time the system is being set to remind the user to attend to that zone.
Isolate	Standard* Manager	Isolating a zone deactivates that zone until such time as the zone is de-isolated. All zone types on the controller can be isolated. 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.
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 (see *Event Log* on page 117) 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.

Right	User Profile Type Default	Description
Set Date	Standard Manager	Use this menu option to program the time and date on the system (see *Set Date/Time* on page 120). Ensure the time and date information is accurate; these fields are presented in the event log when reporting system events.
Change PIN	Standard Manager	This menu option allows users to change their user PINs (see *Change Engineer Pin* on page 118). **Note:** To comply with INCERT approvals, the user's PIN code must contain more than 4 digits.
View Video	Standard Manager	User can view video images via the web browser. **Note:** The Web Access right must also be enabled for this function.
Chime	Standard Manager	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). This menu option allows for enabling or disabling of the chime feature on all zones.
Engineer	Manager	This option allows users to grant access to engineer programming. 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.
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* on page 155.
Door Control	Standard* Manager Access Control	User can lock/unlock doors.
RF Output	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.
User Rights – Service Engineer		
Set Users [Master]		User can create and edit other users on the system with no restriction on user rights.

Right	User Profile Type Default	Description
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

1. Enter a **Site Code**, if required, for all cards assigned to this user profile. See *Supported card readers and card formats* on page 286.
2. Select the **Door Access List** rights of this user profile for the doors configured on the system. Options are:

   - No access

   - No time limit (that is, 24 hour access)

   - Calendar (if configured)
3. **Users using this User Profile**

A list of users assigned to this profile is displayed. Click 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 on page 141

Adding/Editing an area on page 186

15.8.3 Configuring SMS

The SPC system allows remote (SMS) messaging on systems with installed modems.

Prerequisites

- A modem is installed and identified by the system.
- The function **SMS Authentication** is activated. (See *Options* on page 169.)

1. Select **Users>Users SMS**.

   The Engineer SMS ID and a list of User SMS IDs with corresponding SMS details displays.
2. Click the **Test** button to test an SMS number.
3. Click **Add** to add a new SMS ID or click the **Edit** icon beside the required SMS ID to edit the SMS settings.
4. Configure the SMS details as follows:

SMS ID	System generated ID.
User	Select a new user for this SMS ID if required.

SMS Number	Enter the number to which the SMS will be sent (requires three-digit country code prefix). **Note:** Engineer SMS number can deleted by resetting it 0. User SMS numbers cannot be deleted.
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* below.

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 **C**alling **L**ine **I**dentity (CLI) is enabled on the line selected to make the call to the SMS network. Consult the PBX administrator for details.

15.8.4 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, that is, 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 are 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

Using Code	Using Caller ID	Action	Response
**** ASET ****.ASET		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** page. See *Options* on page 169.	System set
**** BSET ****.BSET		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** page. See *Options* on page 169. For example: ****.ASET NIGHT	System set
**** USET ****.USET ****.UNSET	USET 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 • For a single area system, system and mode are returned, where mode is the set status of the system. • For a multi-area system, the status of each area is returned.
**** LOG ****.LOG		Up to 10 recent events are displayed.	Recent events
**** ENGA.ON ****.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

Using Code	Using Caller ID	Action	Response
**** O5.ON ****.O5.ON ****.OUTPUT		Where output (mapping gate) is identified as “O5”, it is triggered on.	Status of “O5” For example: • Output O5 on. • Output heating on (where heating is the name of the output).
**** O5.OFF ****.O5.OFF		Where output (mapping gate) is identified as “O5”, it is triggered off.	Status of “O5” For example: Output O5 off
****.CLR ****.RESTORE		Allows clear alerts by SMS.	

For SMS recognition, output (mapping gate) 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)

The SMS operates using a standard protocol that is used in SMS telephones. 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.
- Also note that most Service Providers only allow SMS to a telephone registered in the same country. (This is due to billing issues.)

15.8.5 Deleting Web Passwords

This page 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 the **Delete** button beside the Engineer or User to delete the password.

15.8.6 Configuring Engineer Settings

To configure engineer settings:

1. Select **Users>Engineer**.
2. Change the ’Engineer’ **User Name** if required.
3. Click the **Change PIN** button to change the Engineer PIN (see *Changing Engineer PIN and web password* on the facing page).

   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* on page 246.)

Access Control

Attribute	Description
Card Number	Enter card number. Enter 0 to unassign the card.
Void Card	Check to temporarily disable the card.
Extended Time	Extend door timers when the 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: • SPC42 –500 • SPC52 – 500 • SPC53 – 500 • SPC62 – 500
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.

15.8.6.1 Changing Engineer PIN and web password

You can change the PIN for accessing the keypad and also the password for accessing the Web browser for Engineer level only.

1. 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.

2. Click the **Change PIN** button to activate the new PIN.

The minimum number of digits required for the 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**.

3. 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.

4. Click the **Change Password** button to activate the new password.

The password is case sensitive – ensure that you enter the correct upper or lower case alphabetic characters in your new password.

15.9 Wireless

Wireless sensor detection (868MHz) on the SPC panel is provided by wireless module. The SPC two way wireless module is fitted into modem slot 2 of the control panel. See the table below for information on which devices can be enrolled with each type of transceiver.

For CE regulatory compliance, the SPCW120 product can only be fitted to the following products:

- SPC42
- SPC52
- SPC53
- SPC63

Devices compatible with a two way transceiver

Sensors	**WPIR**	Wireless 12m PIR detector with pet immunity option
	WPIR-CRT	Wireless curtain PIR detector
	WMAG	Wireless magnetic contact (slim)
	WMAG-I	Magnetic contact with additional input
	WSMK	Wireless smoke detector
	WMAG-S	Shock sensor with door contact
	WFLOOD	Wireless flood sensor
	WAGB	Wireless acoustic glass break detector
	WPIR-EXT	Wireless external PIR detector
Outputs	**WSIR-INT**	Wireless indoor sounder
	WSIR-EXT	Wireless outdoor sounder
Repeaters	**WRPTR**	Wireless signal repeater plug
Keypads	**WKPD**	Wireless keypad
Fobs	**WRMT**	Remote control with 4 button control
	WPAN	Wireless personal alarm button

For instructional videos on wireless devices and transceivers please go to http://van.fyi?Link=Wireless_devices.

15.9.1 Two way wireless

The following devices can be enrolled and configured on a two way wireless transceiver:

- Wireless detectors (motion detectors, magnetic contacts, smoke alarms)
- Wireless outputs (internal and external sirens)
- Wireless repeaters
- Wireless keypads
- WPAN Personal alarm button
- WRMT Remote control

Note: You must enable two way wireless before enrolling these devices.

To enable two way wireless:

1. Select **Configuration > Hardware > Wireless > Wireless Settings**.
2. Enable **Two Way Wireless**.

The SPCW120 Wireless Transceiver can support (up to) the following number of devices

- 64 detectors
- 16 output sirens
- 8 wireless keypads
- 4 repeaters
- 20 fobs (personal alarm buttons and/or remote controls)

To upgrade the transceiver firmware to version 4.7.x, you must ensure that no more than 20 fobs (remote controls or personal alarm buttons) are configured on your SPC system. If there are more than 20 fobs configured, delete any excess fobs.

The combined maximum number of synchronous devices (wireless keypads and sirens) should not exceed 16 per transceiver.

15.9.1.1 Add wireless sensor

Add a wireless sensor using the browser

To add a wireless sensor using the browser:

1. Select **Configuration > Hardware > Wireless Settings**.
2. Enable **Two Way Wireless**.
3. Select **Configuration > Hardware > Wireless > Two Way** and click **Enrol New Device**.

4. Activate the wireless sensor by inserting the battery/batteries to enable the SPCW120 Wireless Transceiver to detect the wireless transmission of the device.
   When the sensor is detected, it is listed on the **Wireless - Discovering** page. The sensor information may display automatically after a few seconds or you may have to click the **Refresh** button to see the wireless sensor information.
5. Click **Add**.
6. Use the settings in the **Wireless Device Configuration** page to specify a Description and to configure the other settings for the wireless sensor.
   See *Configuring two way wireless attributes* on page 1 for more information.
7. Click **Save**.
   The wireless sensor is enrolled in your SPC system, and the device is added to the **Wireless - Enrolled List** page.

15.9.1.2 Configure wireless smoke detector LED

For more recent smoke detectors (v 0.2.0.3 and higher), you can configure the following settings

- Enable / disable LED
- Set the supervision time set to 1/2/4/7/10/15/20/30 minutes

In order to configure these settings, the smoke detectors must be communicating through a wireless transceiver with firmware version 4.7 or later, on anSPC system version 3.13.5 or later.

Go to **Hardware > Wireless > Two Way > Wireless Device Configuration** to configure the LED settings.

15.9.1.3 Add wireless output

Add a wireless output using the browser

To add a wireless output using the browser:

1. Select **Configuration > Hardware > Wireless Settings**.
2. Enable **Two Way Wireless**.
3. Select **Configuration > Hardware > Wireless > Two Way** and click **Enrol New Device**.
4. Activate the wireless output by inserting the battery/batteries to enable the SPCW120 Wireless Transceiver to detect the wireless transmission of the device.
   When the output is detected, it is listed on the **Wireless - Discovering** page. The output information may display automatically after a few seconds or you may have to click the **Refresh** button to see the wireless output information.
5. Click **Add**.
6. Use the settings in the **Wireless Device Configuration** page to specify a Description and to configure the other settings for the wireless output.
   See *Configuring two way wireless attributes* on page 1 for more information.
7. Click **Save**.
   The wireless output is enrolled in your system, and the device is added to the **Wireless - Enrolled List** page in the **Outputs List** section.

15.9.1.4 Add wireless repeater

Add a wireless repeater using the browser

To add a wireless repeater:

1. Select **Configuration > Hardware > Wireless Settings**.
2. Enable **Two Way Wireless**.

3. Select **Configuration > Hardware > Wireless > Two Way** and click **Enrol New Device**.
4. Activate the wireless repeater by inserting the battery/batteries and then plug the WRPTR into an EU mains (220v AC) socket.
   Activating the repeater enables the SPCW120 Wireless Transceiver to detect the wireless transmission of the device. When the repeater is detected, it is listed on the **Wireless - Discovering** page. The repeater information may display automatically after a few seconds or you may have to click the **Refresh** button to see the wireless repeater information.
5. Click **Add**.
6. Use the settings in the **Wireless Device Configuration** page to specify a Description and to configure the other settings for the wireless repeater.
   See *Configuring two way wireless attributes* on page 1 for more information.
7. Click **Save**.
   The wireless repeater is enrolled in your system, and added to the **Wireless - Enrolled List** page in the **Repeaters List** section.

15.9.1.5 Add wireless keypad

Add a wireless keypad using the browser

To add a wireless keypad using the browser:

1. Select **Configuration > Hardware > Wireless Settings**.
2. Enable **Two Way Wireless**.
3. Select **Configuration > Hardware > Wireless > Two Way** and click **Enrol New Device**.
4. Activate the wireless sensor by inserting the battery/batteries to enable the SPCW120 Wireless Transceiver to detect the wireless transmission of the device.
   When the keypad is detected, it is listed on the **Wireless - Discovering** page. The keypad information may display automatically after a few seconds or you may have to click the **Refresh** button to see the wireless keypad information.
5. Click **Add**.
6. Use the settings in the **Wireless Device Configuration** page to specify a Description and to configure the other settings for the wireless keypad.
   See *Configuring two way wireless attributes* on page 1 for more information.
7. Click **Save**.
   The wireless keypad is enrolled in your SPC system, and the device is added to the **Wireless - Enrolled List** page.

15.9.1.6 Add wireless personal alarm button

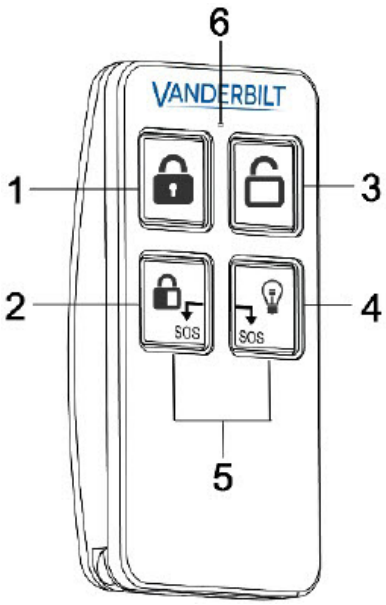
Add a wireless personal alarm button using the browser

To add a wireless personal alarm button using the browser:

1. Login as **Full Engineer**.
2. Select **Users > Wireless FOB**.
3. On the wireless personal alarm button, press and hold the centre button.
4. The Red LED lights for 3 seconds, then no LED, then Red LED once and then Green LED.
5. Click **Refresh** on the **Wireless FOB** page to display the wireless personal alarm button.
6. You can now assign the discovered wireless personal alarm button to a system user.

15.9.1.7 WRMT remote control

The WRMT 4-button Remote is a device which allows a user to remotely operate the SPC system. The device supports UNSET, FULLSET, and PARTSET (A only) functionality, as well as the operation of defined outputs and an SOS feature.



1	Fullset
2	Partset (A only)
3	Unset
4	Output
5	Panic/SOS
6	LED

Enrol a WRMT remote control

To enrol the WRMT:

1. In the SPC browser, select **Users > Wireless FOB**.
2. On the WRMT, press and hold both **SOS** buttons.

   The LED blinks Red once and then Green.
3. Click **Refresh** on the **Wireless FOB** page to display the WRMT.
4. You can now assign the discovered WRMT to a system user.

To assign the WRMT to a user:

1. Go to **Users > Users** and click the **Edit** button beside the user you want to assign the WRMT to.
2. On the **Edit user settings** page, click the **Unknown Fob** button.

   A list of unassigned fobs is displayed.
3. Click the **Add** button to assign the WRMT to the user.
4. On the **Edit user settings** page click **Save**.

Delete a WRMT remote control

To delete a WRMT:

1. Go to **Configuration > Hardware > Wireless > Transceiver list.**
2. Click the **Delete** button beside the WRMT that you want to delete.

When you delete a WRMT from your system, you must also clear the internal registration in the WRMT before you can re-use the WRMT.

To clear the internal registration:

- On the WRMT, press and hold the **PARTSET** and **UNSET** buttons.

  The LED blinks Red and Orange to confirm that registration is cleared.

15.10 Configuration

This section covers:

15.10.1 Configuring controller inputs and outputs

This section covers:

- *Editing an input* below
- *Editing an output* on the next page
- *Configuring system latch and auto set outputs* on page 159

15.10.1.1 Editing an input

1. Select **Configuration > Hardware > Controller**.
2. Configure the fields as described in the table below.

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).
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 *Zone types* on page 278).
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 *Input zones: attributes* on the next page).

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**.

   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 *Applicable attributes to zone types* on page 1.

15.10.1.2 Editing an output

1. Select **Configuration > Hardware > Controller**.
2. Configure the fields as described in the table below.

Output Type	• **System Output:** Select the type from the dropdown menu. (See *Outputs types and output ports* below.) • **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 *Outputs types and output ports* below.) • **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 *Outputs types and output ports* below.) • **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 Attributes	• **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 *Calendars* on page 197.

See also

Calendars on page 197

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 *Zone types* on page 278) 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 (for example, 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). See 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).

Output Type	Description
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 11V this output activates. The 'Restore' option for this fault is only presented when the voltage level rises to above 11.8V.
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; that is, 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* on page 159). 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).

Output Type	Description
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, that is, 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 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, that is, 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, that is, 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.

Output Type	Description
Setting ACK	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	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, Sigmalock 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: • two hold-up zone activations more than two minutes apart • a hold-up zone and a panic zone activation more than two minutes apart • 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 below

15.10.1.3 Configuring system latch and auto set outputs

1. Under **Policy**, click the **Edit** button for the **Output Configuration** option in **System Options**.
2. 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

3. 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.

15.10.2 X-BUS

This section covers:

- *Expanders* below
- *Keypads* on page 165
- *Door Controllers* on page 168
- *Cable Map* on page 168
- *Settings* on page 169

15.10.2.1 Expanders

1. Select **Configuration > Hardware > X-Bus > Expanders**.

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 one of the expander identifying parameters to display the **Expander Configuration** page.
3. 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 *Wiring the system* on page 35.
(Zone) Description	Provide a description for allocated zone.
(Zone) Type	Select the zone type. See *Zone attributes* on page 283.
Area	Select the area.
Attributes	Assign attributes as desired. See *Zone types* on page 278.
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 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 go to **Configuration > Hardware > X-BUS > Cable Map & Configuration**.

Click **Reconfigure** to implement changes.

When you click **Proceed Reconfiguration**, the whole X-BUS is reconfigured. If an expander is offline and the reconfigure button is pressed, the expander will disappear without notifying the user.

Reconfiguring the X-BUS

1. Select **Configuration > Hardware > X-BUS > Cable Map & Configuration**.
2. Click **Reconfigure**.

The X-Bus cable Map – Warning(s) page displays.

3. Click **Proceed Reconfiguration**.

   The X-BUS is reconfigured.

   If an expander is offline and the reconfigure button is pressed, the expander will disappear without notifying the user.

See also

- *Wiring the system* on page 35
- *Zone attributes* on page 283
- *Zone types* on page 278

Configuring an Indicator Expander

The LED indicator module has 1 input.

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 **Linked Mode** configuration page displays.

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. Select if LED indicators should be active when the keys are deactivated.
5. Configure the input.

Flexible Mode

1. Click the **Flexible Mode** button.
2. Configure the fields described in the table below.

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.
Location	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	Click this button to change the function for this indicator. The function can be enabled or used for a system, area, zone or keyswitch.
LED Always	Select if LED indicators should be active when the keys are deactivated.
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.
Card reader Trigger Mode	Select if card events can be used as triggger conditions, deactivation with the card reader becomes unavailable, and the reader cannot be deactivated.

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.

Configuring a Keyswitch Expander

1. Select **Settings > X-Bus > Expanders**.
2. Click one of the keyswitch identifying parameters.
3. 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). Default is 0.

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	Click 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 *Editing an output* on page 155 for more details.
Keyswitch Functions	
Centre, Right and Left Positions	Select the **Function** that that this keyswitch position will perform and the relevant **Area**. Keyswitch functions are: • None • Unset • Partset A • Partset B • Fullset • Toggle Unset / Fullset • Toggle Unset / Partset A • Toggle Unset / Partset B • All Okay • Setting authorisation • Shunt

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.

15.10.2.2 Keypads

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.

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 *Calendars* on page 197.
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 on page 197

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.

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.
Visual indications	
Backlight	Select when keypad backlight is on. Options are: On after key is pressed; Always on; Always off.
Backlight Intensity	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 Keys	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.
Human Icon	Enable if Mapping Gate should be indicated.

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 and 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)
Quiet Mode	Enable this setting to disable the buzzer during entry and exit when the keypad is in an armed area. **NOTE:** Keypad only audible for entry/exit/setting/unsetting if the area is the same as the keypad location, or if the keypad is performing the operation.
Deactivation	
Calendar	Select if the keypad should be limited by calendar. See *Calendars* on page 197.
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.
Keypad Access Level	Select keypad access level (1 to 3). Level 1 – All functions Level 2 – Arm, disarm, and restore only Level 3 – View only

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.

15.10.2.3 Door Controllers

Editing a door controller

1. Select **Configuration > Hardware > X-Bus > Door Controllers**.
2. Click one of the standard keypad identifying parameters (for example, serial number).
3. Configure the fields as described in the table below.

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).

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	• 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 *Editing a door* on page 192.
4. In order to use the inputs, they have to be assigned to a zone number.

15.10.2.4 Cable Map

For a list of the expanders/keypads in the order they are configured on the SPC system:

- Select **Configuration > Hardware > X-BUS > Cable Map & Configuration**.

For more detail on X-BUS interfacing, see *Wiring the X-BUS interface* on page 35.

15.10.2.5 Settings

To configure X-BUS connections:

1. Select **Configuration > Hardware >X-BUS > X-Bus Settings**.
2. Configure the fields as described in the table below.

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.

15.10.3 Changing system settings

This section covers:

- *Options* below
- *Timers* on page 179
- *Identification* on page 183
- *Standards* on page 184
- *Clock* on page 184
- *Language* on page 185

15.10.3.1 Options

1. Select **Configuration > System > System Options**.
2. Configure the fields as described in the table below.

The options that are 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.

Restriction	System Option	Description
	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.
Web 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: • 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.

Restriction	System Option	Description
	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: • 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. 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. **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. • 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. The SIA event reported is HF and Extended SIA reports **Hardware Fault**. **Note:** Hardware faults are not reported if the Engineer is logged in to the system. For more information on ARCs, see *Alarm Reporting Centres (ARCs)* on page 236.
	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 Set (FTS)	Enable to activate the strobe if the system fails to set.
	Hide bypass	If enabled, the bypass messages will no longer be displayed on keypad.
	Battery capacity	Total batteries capacity in AH, for panel only (3–100Ah). 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 (30–20000mA). 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.

Restriction	System Option	Description
Partset		
	Partset A Rename	Enter a new name for your PARTSET A mode (for example, Night Mode).
	Partset B Rename	Enter a new name for your PARTSET B mode (for example, 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: • 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: • Ireland - Disabled • All other regions - Tamper
	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: • Germany VDS – Tamper • All other regions - Trouble

Restriction	System Option	Description
⏻	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: • 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: • 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: • Germany VDS – Tamper • All other regions – Trouble
	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.
⏻	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).
	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, that is, when the open zone that triggered an alarm is 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.

Restriction	System Option	Description
	Alarm on Exit	**Enabled:** If a non-entry/exit zone is activated during the exit timer countdown, a local alarm is raised by sounding the bells. **Disabled:** If a non-entry/exit zone is activated during the exit timer countdown, an alarm is not raised. **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**.
	Alarm on Entry	**Enabled:** If a non-entry/exit zone is activated during the entry timer countdown, a local alarm is raised by sounding the bells. **Disabled:** If a non-entry/exit zone is activated during the entry timer countdown, an alarm is not raised. **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**.
Confirmation		
	Confirmation	The Confirmation variable determines when an alarm is deemed to be a confirmed alarm. • 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* on page 179.) 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. • 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 two activations

Restriction	System Option	Description
		may come from the same device if the activations differ in type, that is, alarm/tamper. - 1 Alarm activation followed by an ATS[1] Fault within 30 minutes (default). - ATS fault followed by a tamper or alarm condition within 30 minutes (default). 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. 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. If an alert (ATS) reoccurs after the 30 minute window (default), then the 30 minute timer will restart. The EN50131-9 confirmation option is automatically set whenever the **Standards > Region** option is set to Spain. • 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.
	Log Keypad Access	Enable this option to log users' keypad access (successful and failed log-in attempts).
	Idle State Language	Select the language displayed in idle state. • 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.
	Use Simplified Menu	Enable this option to use simplified set/unset menus on the 'Comfort' and 'Compact' Keypads (for one area configuration only).

Restriction	System Option	Description
PIN		
	PIN Digits	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, for example, 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, for example, an existing user PIN of 00002134 (8 digits) will change to 02134 if the PIN digits is set to 5. **Note:** This option cannot be changed if an SPC Manager PIN digit mode is set. See *SPC Manager* on page 244. **Note:** To comply with INCERT approvals, the user's PIN code must contain more than 4 digits.
	PACE and PIN	If enabled, both PACE and PIN are required.
	User Duress	Select one of the following Duress options to activate this function on the system. • 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. Duress must be enabled for individual users. See section on Adding/Editing a User.
	PIN Policy	Click the **Edit** button to select options for PIN usage. • Periodic changes required – enforces scheduled changes to the user's PIN. The period is defined in the **PIN Valid** field of **Timers**. See *Timers* on page 179. • 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* on page 179. • 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* on page 179. • Secure PIN - If enabled the PIN will be automatically generated by the panel.
Door & Reader		
	Reset Cards	If enabled, access cards passback state will be reset every day at midnight.

Restriction	System Option	Description
	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	Click the **Edit** button to select the card formats that will be allowed on this panel. See *Supported card readers and card formats* on page 286 for details of currently supported card readers and card formats. **Note:** Selecting **Wiegand** enables all Wiegand card formats.
Web 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 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**.
	Override Reader Profile	If enabled, Reader LEDs indicate setting confirmation and Card+PIN request.
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.
⏻	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'.

Restriction	System Option	Description
SMS		
	SMS Authentication	Select one of the following options: • PIN Code Only: This is a valid user code. • 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. Click **Edit** to configure general system behaviour. You can set Advanced system operations, or configure the reporting settings (**Report on close**, **Restore on close**, **Limit reporting**, and **Log on close**) for the Alert options.
Web Only	Timing Policy	Display system timing policy.
Web Only	Output Configuration	Click the **Edit** button to configure latch and autoset output settings (see *Configuring system latch and auto set outputs* on page 159).
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.

Restriction	System Option	Description
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 - 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.

**A WPA is compatible with SiWay RF Kit (SPCW120 or WRTX) only.*

See also

Adding/Editing an area on page 186

15.10.3.2 Timers

This page 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 > System Timers**.

   The **System Timers** page displays.
2. Configure the fields as described in the following table.

Timers

Designation of the functions in the following order:

- 1st row: Web
- 2nd row: Keypad

Timer	Description	Default
Audible		
Internal Bells INT BELL TIME	Duration that internal sounders will sound when alarm is activated. (0–999 minutes; 0 = never)	15 min.
External Bells EXT BELL TIME	Duration that external sounders will sound when alarm is activated. (0–999 minutes; 0 = never)	15 min.
External Bell Delay EXT BELL DELAY	This will cause a delayed activation of the external bell. (0–999 seconds)	0 sec.
External Bell Delay Partset	Delay period before external bells are activated in partset mode.	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	**Note:** This option is only available for certain **Grade** and **Confirmation** option combinations. (See *Options* on page 169 and *Standards* on page 184.) 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. (0–60 minutes)	30 min.
Confirmed holdup	**Note:** This option is only available for certain **Grade** and **Confirmation** option combinations. (See *Options* on page 169 and *Standards* on page 184.) 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 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. (0–999 seconds)	30 sec.
Partset Dialer Delay	Delay period after a Partset alarm has been activated before system makes a call to ARC.	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.

Timer	Description	Default
Setting		
Setting Authorisation SETTING AUTH	Period for which Setting Authorisation is valid. (10–250 seconds)	10 sec
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.
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.
Strobe on Fullset FULLSET STROBE	Activates the strobe on the external bell momentarily to indicate a full set condition. (0–10 seconds)	0 sec.
DELAY UNSET BUZZER TIME		1 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)	10sec.
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.
Auto Restore Delay	Time to delay auto restore after zone state returns to normal. (0–9999 seconds)	0 sec.
Lockout Post Alarm LOCKOUT POST ALARM	The duration of time after an alarm before the user can gain access. (1–120 minutes)	30 min.
Access Time	The duration of time the system can be accessed by an alarm access user after the Lockout Time has elapsed. (10–240 minutes)	120 min
External Bell Strobe STROBE TIME	Duration that the strobe output will be active when an alarm is activated. (1–999 minutes; 0 = indefinitely)	15min.

Timer	Description	Default
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)	0min.
RF Jamming Delay	The time after RF Jamming has been detected before an alert is activated by the system. (0–999 seconds)	0min.
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 logged out. (0–300 minutes)	0 min.
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 sec.
CODE LOCKOUT		10 sec
CODE LOCKOUT 2		10 sec
Lockout time		90 sec
Fire		
Fire Pre-alarm FIRE PRE-ALARM	Number of seconds to wait before reporting fire alarm for zones with ‘Fire pre-alarm’ attribute set. See *Editing a zone* on page 185. (1–999 seconds)	30sec.
Fire recognition FIRE RECOGNITION	Extra time to wait before reporting file alarm for zones with ‘Fire pre-alarm’ and ‘Fire Recognition’ attributes set. See *Editing a zone* on page 185. (1–999 seconds)	120sec.
PIN		
PIN Valid PIN VALID	Period for which pin is valid. (1–330 days)	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 days)	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 time synchronization will not take place. Time synchronization only takes place if system time and update time are outside this limit. (0–300 seconds)	0 sec.
Link Timeout LINK TIMEOUT	Timeout for Ethernet link fault. (0–250 seconds; 0 = Disabled)	0 sec.
Camera Offline CAMERA OFFLINE	Time for camera to go offline. (10–9999 seconds)	10 sec.
Frequent FREQUENT ⓘ	This attribute only applies to remote services. The number of hours within which a zone must open if the zone is programmed with the **Frequent** attribute. (1–9999 hours)	336 h (2 weeks)
Duress silent	Time when duress will remain silent and not restorable from keypad. (0–999 minutes)	0 min.
Holdup/panic silent	Number of minutes that a holdup/panic will remain silent and cannot be restored from the keypad. (0–999 minutes)	0 min.

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.

Valid settings/ranges may be dependent on the security grade specified under **Configuration > System > Standards**.

15.10.3.3 Identification

1. Select **Configuration > System > Identification**.
2. Configure the fields as described in the table below.

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).

15.10.3.4 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**.
2. Configure the fields as described in the following table.

Continent	Select the appropriate location for the installation. Options are Europe, Asia, North America, South America, or Oceania.
Installation Type	Select the type of installation. Options are Domestic, Commercial or Financial.
Region Compliance	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. Some selections will implement local or national requirements which supersede EN50131 requirements. The options in the **Grade** area will change depending on your selection in the **Region Compliance** area. Options are UK, Ireland, Europe General (EN), Italy, Sweden, Switzerland, Belgium, Spain, Germany (VDS), France, Norway, Denmark, Poland, Netherlands, Finland, Portugal, and Czech Republic.
Grade	Select the Security Grade that applies to the installation. The options in the **Grade** area change depending on your selection in the **Region Compliance** area.

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 on page 169 for details of configuring system policies.

15.10.3.5 Clock

This page enables you to program the date and time on the panel. The controller contains a **R**eal-**T**ime **C**lock (RTC) that is battery-backed to preserve the time and date information in the event of power failure.

1. Select **Configuration > System > Clock**.
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.
Network Time Protocol	If selected, time is synchronized with the specified NTP server.
IP or URL	
Time Zone	Select the UTC time zone.
Max Time Difference	Set the time difference before synchronization occurs.

The selected time and date will be displayed on the keypad, the web interface and the event log.

15.10.3.6 Language

1. Select **Configuration > System > Language**.
2. For the **Language** option, select a language from the drop-down 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.
3. 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

Options on page 67

15.10.4 Configuring zones, doors and areas

This section covers:

- *Editing a zone* below
- *Adding/Editing an area* on the facing page
- *Editing a door* on page 192
- *Adding an area group* on page 197

15.10.4.1 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.

Virtual zones can be created and edited , but a virtual zone must be associated with a mapping gate. For more information on Virtual Zones, see *Virtual Zones* on page 203

1. Select **Configuration > Inputs > All Zones**.

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.

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 *Zone types* on page 278).
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 *Calendars* on page 197). 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	Click the Attributes button to display the Attributes page for the zone. Only attributes that apply to that type of zone are displayed. See *Zone attributes* on page 283).

15.10.4.2 Adding/Editing an area

Prerequisite

- Only if (multiple) **Areas** is activated.

1. Select **Configuration > Areas > Areas**.
2. Click **Edit** to edit an existing area.
3. Click **Add** to add a new area. If the Installation Type is *Domestic* or *Commercial*, an area is automatically added and the **Edit Area Settings** page is displayed.

Tthe area type for the new area is automatically set to *Standard*.

If the Installation Type is *Financial*, the area must be added manually.

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 the **Add** button to add the area.

Configure the settings for each installation type as per the following sections.

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).
Entry Time 2	
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* on page 179.
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: • 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* on page 179.

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.

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 the areas that you wish to link to this area.

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/Unsetting* on the next page). 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)

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* on the previous page.)

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.

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**.

Enable **Early/Late** to report any setting and unsetting which is not according to schedule.

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* on the previous page), 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	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). If the second PIN is not entered within 30 seconds, or it is wrong, then the area cannot be Set or Unset.
Force Set Mode	Area options for Force-set operation (Normal or Blocked).
Auto Restore on Force Set	Check this option to auto-restore closed zones during force-set. If this option is selected, if an alert is active or a zone needs to be restored, then it will be automatically restored.

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.

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.

All Okay

All Okay Required	If selected, user must confirm 'All okay' input or silent alarm is generated. See *Editing a zone* on page 185 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.

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.

Fire Exit Route

Fire exit route	Select the doors which will open when fire occurs in this area. This option does not display in domestic mode.

Area Triggers

The Triggers section is only displayed if triggers have been defined previously. (See *Triggers* on page 201.)

Click the **Edit** button to add, edit or delete trigger conditions for the area.

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	This is the action that is performed when the trigger is activated. Options are: • Unset • Partset A • Partset B Fullset Delay autoset This action will delay alarm setting when the autoset 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 *Setting/Unsetting* on page 189). • Restore alarms This action will clear all alarms in the configured zone. • Cancel Delay Unset • Delay Fullset • Silence Bells

Note: Triggers cannot be configured from a keypad.

See also

Triggers on page 201

15.10.4.3 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	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. If the door position sensor is assigned to an intrusion zone, it can be configured like a normal zone but only with limited functionality (for example, not all zone types are selectable). 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.
Description (Web only)	Description of the zone the door position sensor is assigned to.
Zone Type (Web only)	Zone type of the zone the door position sensor is assigned to (not all zones types are available).

Name	Description
Zone attributes (Web only)	The attributes for the zone the door position sensor is assigned to can be modified.
Area (Web only)	The area the zone and the card reader are assigned to. (If the card reader is used for setting and unsetting, this area will be set/unset).
Door Position (Web) DPS End Of Line (keypads)	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.
DPS Delay	Specify a time (in seconds) for a delay to the DPS.
Door Release (Web) DRS END OF LINE (Keypads)	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.
DRS Single shot	Set Door release to momentary single use.
No DRS (Web 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 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.
DRS Single Shot	Changes operation of DRS to single shot instead of remain open.

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
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)	Panel/area will unset, when card is presented at entry reader.
Unset inside (Browser)	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.
Double unlocks	The door unlocks and stays unlocks when double-badged. Door must be double-badged after exit to reset. This option cannot be used with Settings options.
Fullset outside (Browser)	Panel/area will fullest, when card is presented twice at entry reader.
Fullset inside	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.

Attribute	Description
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.
Interlock* (Browser)	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
Code Tamper	Invalid cards contribute to code tamper.

** 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.

Timer	Min.	Max.	Description
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.
Dual Authorization			30 sec default
Delay DPS			0 ms default

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.

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* on page 192.
2. Set the **Interlock** attribute for the required doors in the group. See *Editing a door* on page 192.
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 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.

15.10.4.4 Adding an area group

You can use area groups for configuring multiple areas. So the configuration must not be done for every single area.

Prerequisite

- Only if the option (multiple) Areas is activated.

1. Select **Settings > Areas > Area groups**.
2. Click the **Add** button.
3. Enter a description for the group.
4. Select the areas that are to be assigned to this group.
5. 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**.

15.10.5 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 ISO8601international standard.

Configuring calendars

- Select **Configuration > Calendars**.

  A list of configured calendars is displayed.

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, that is, 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.

15.10.5.1 Adding/Editing a calendar

1. Select **Configuration > Calendars > Add**.
2. Provide a **Description** for the calendar (max. 16 characters).

Copying a Calendar

To make a copy of this calendar structure, click 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 (that is, 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 *Automatic setting/unsetting of areas* on the next page), or for Automatic Setting/Unsetting of other Panel Operations (see *Automatic setting/unsetting of other panel operations* on the next page).

   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 on the next page

Automatic setting/unsetting of other panel operations on the next page

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 > Exception Days > Add**.
2. Configure the fields as described in the table below.

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 *Automatic setting/unsetting of areas* below), or for Automatic Setting/Unsetting of other Panel Operations (see *Automatic setting/unsetting of other panel operations* below).
Calendars	Select the desired calendar(s) for effect.

NOTICE: Global exception days created remotely using the SPC Manager tool cannot be deleted or removed.

15.10.5.2 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.

15.10.5.3 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.

A valid On and Off time must be specified for this operation.

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.

15.10.6 Change own PIN

To change a PIN, see *Changing Engineer PIN and web password* on page 148.

15.10.7 Configuring advanced settings

This section covers:

- *Cause and Effect* below
- *Mapping Gates* below
- *Triggers* on the next page
- *Audio/Video Verification* on page 205
- *Updating SPC Licenses* on page 207

15.10.7.1 Cause and Effect

1. Select **Configuration > Advanced > Cause and Effect**.
2. Click an **Assign** button to perform one of the following actions:
   - **Output:** Assign a mapping gate (virtual output) to trigger a physical output. Select this option to display the **Mapping Gate - List** page. For more information see *Mapping Gates* below.
   - **Area:** Assign a trigger(virtual input) to trigger an area action. Choose an **Area** from the drop-down list before you click the **Assign** button. For more information see *Triggers* on the next page.
   - **Door:** Assign a trigger (virtual input) to trigger door action. Choose a **Door** from the drop-down list before you click the **Assign** button.

To display the list of configured triggers and actions, select **Configuration > Advanced > Cause & Effect > Cause & Effect List**.

The **Cause & Effect List** page displays only fully functioning cause & effects. For example, if a mapping gate is not assigned to a trigger or to a quick key, it is not displayed in the list.

WARNING: Your system will not comply with EN standards if you enable a trigger to set the system without a valid PIN being required.

15.10.7.2 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 > Cause & Effect > Mapping Gates**.
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. Enable the **Local** setting 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 local gate is not visible remotely.
4. Enable the **Report**setting to report the status of the mapping gate over FlexC.
5. 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.

6. Add a **Timer** for the gate. Time quantity used is 1/10 of a second.
7. Click 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* below for details of configuring triggers.
8. Select an output from the drop-down list.
9. Click **Add** to add a new gate or **Save** to save the new settings for an existing gate.

See also

Triggers below

15.10.7.3 Triggers

A trigger is a system state (for example, 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**.
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 *Calendars* on page 197.
Time limit	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.
Timer	Enter the number of seconds that the trigger conditions must be true before the trigger will activate.
Trigger Operation	• **All** All trigger conditions must be active for the system to activate the trigger. • **Any** Any trigger condition that is active enables the system to activate the trigger.
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.

Performable actions

Add	Add conditions for the trigger. Click this button to add one or more conditions for the selected trigger. See *Trigger conditions* below.

Trigger conditions

The following table lists the trigger conditions and the associated States, Outputs, Events, or Communication.

Trigger condition	States, Outputs, Events, or Communications
Zone	The trigger is ON if the following conditions are satisfied (i.e. a logical AND operation is performed): The trigger is ON if the configured zone is in one of the following states - **Open**, **Close**, **Short**, **Disconnected**, **Tamper**, **Bypass**, **Inhibited**, or **Alarm**.
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, Interlocked, and Door Buzzer**
Output	The trigger is ON if the system output is in the configured state, which can be **On** or **Off**: **System Output**, **Mapping gate**, **Area Output**.
System	The trigger is ON for the chosen system event and ID. IDs are: **System Reboot**, **Overcurrent**, **Engineer Access**, **Manufact. Access**, **XBUS cable fault**, **Xbus faults**. **Time Trigger** – the trigger is on at the specific time entered in the box provided, in the format hh:mm.
User	**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. **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. **Keypad 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. **Access card** – the trigger is activated when the selected user logs in using an access card. **Web Access** – the trigger is activated when the selected user logs in through the web browser. **Keypad Access** – the trigger is activated when any user logs into the selected keypad. **Indicator Access** – the trigger is activated by a specific function key..

Trigger condition	States, Outputs, Events, or Communications
Profile	**Keypad Pin** – if a user with the configured user profile enters a valid PIN, or presents a configured PACE, it will cause an instantaneous pulse OFF/ON/OFF. **Access card** – the trigger is activated when a user with the configured user profile logs in using an access card. **Web Access** – the trigger is activated when a user with the configured user profile logs in through the web browser.
Expander	**Keyswitch** – the trigger can be configured for a specific key position on the keyswitch. **Indicator** – the trigger can be configured for a specific function key.
Communication	**FlexC ATP** – the trigger activated by the selected ATS and ATP configuration. **FlexC ATS** – the trigger activated by the selected ATS configuration.

WARNING: Your system will not comply with EN standards if you enable a trigger to set the system without a valid PIN being required.

15.10.7.4 Virtual Zones

A virtual zone is associated with a mapping gate. Each mapping gate can have a number of triggers, and each trigger can be set off in multiple ways (for example, by events caused by other hardware or virtual zones). If the mapping gate is on, the virtual zone is usually open; if the mapping gate is off, the virtual zone is closed. The effect of the zone opening or closing depends on the zone type and, in more complex scenarios, if the zone is used in triggers.

Mapping gates can also have timers. Those timers are independent of the virtual zones timers. In some scenarios, it is valid to define separate timers for both a mapping gate and a virtual zone associated with that mapping gate.

The mapping gate for a virtual zone must be created and configured before you create the virtual zone. If you delete a mapping gate, then all of the virtual zones that are assigned to that mapping gate are automatically deleted.

See *Mapping Gates* on page 200 for more information on mapping gates.

See *Triggers* on page 201 for more information on triggers.

Virtual zones are reported to ARCs like hardware zones of the same type, if so configured. Virtual zones can be isolated or inhibited, like hardware zones.

Virtual zones have associated timers. By default the timer configuration value is zero, which means that the zone timer is inactive and the virtual zone being open or closed follows the mapping gate being on or off. If, however, the timer configuration has a value greater than zero, a timer is started when the virtual zone opens, and the virtual zone auto-closes after the time expires, even if the associated mapping gate is still in the on state. In this case, the virtual zone can open again only if the associated gate first closes and then opens.

Virtual zones are floating zones. If the X-BUS configuration is changed (for example by adding another I/O expander or by changing the rotary switch address of an existing I/O expander) all of the floating zones in the range used by the expander are moved up, including the virtual zones.

Virtual zones have by default the same attributes as hardware zones of the same type. Attributes for virtual zones can be configured in the Inputs page or through the keypad.

The maximum number of virtual zones is hardware-dependent:

- SPC 42 supports 4 virtual zones
- SPC 52 and SPC53 supports 20 virtual zones
- SPC62 supports 100 virtual zones

Select **Configuration > Advanced > Cause & Effect > Virtual Zones** to display the **Virtual Zones List** page.

The **Virtual Zones List** page displays the following information for your virtual zones:

ID	Unique ID for the virtual zone on the SPC Panel.
Zone	The zone number that is associated with the virtual zone. The zone number is reported in the event strings that are sent to ARCs.
Description	The name of the virtual zone.
Type	The type of the virtual zone.
Area	The area to which the virtual zone is assigned.
Mapping gate	The mapping gate assigned to the virtual zone. If this mapping gate is deleted, the virtual zone is automatically deleted.
Timer	The value of the timer of the virtual zone.

Adding a Virtual Zone

Virtual zones must be created via the panel web browser. When you have configured a virtual zone you can edit the properties (Description, Zone Type, Area and Attributes (if the zone is not unused) for the virtual zone through the panel web browser or through a keypad.

The mapping gate for a virtual zone must be created and configured before you create the virtual zone. If you delete a mapping gate, then all of the virtual zones that are assigned to that mapping gate are automatically deleted.

Add a Virtual Zone

1. Select **Configuration > Advanced > Cause & Effect > Virtual Zones**.

   The **Virtual Zones List** page displays.
2. Click **Add**

   The **Create/Edit Virtual Zone** page displays.
3. Enter/select values in the fields:

ID	Unique ID for the virtual zone on the SPC Panel.
Zone	The zone number that is associated with the virtual zone. The zone number is reported in the event strings that are sent to ARCs.
Description	The name of the virtual zone.
Type	The type of the virtual zone.
Area	The area to which the virtual zone is assigned.
Mapping gate	The mapping gate assigned to the virtual zone. If this mapping gate is deleted, the virtual zone is automatically deleted.

Timer	The value of the timer of the virtual zone (100 ms intervals). The zone toggles open/closed for the time entered.

4. Click **Save** to save the information entered and return to the **Virtual Zones List** page.

   Or

   Click **Add** to save the information entered and to re-populate the **Create/Edit Virtual Zone** page with details of a new virtual zone, with default values ready to be edited.

The **Description**, **Type** and **Area** values can be edited on the **Create/Edit Virtual Zone** page and on the **Inputs** page (**Configuration > Inputs**, or via the keypad . The **Zone**, **Mapping gate** and **Timer** values can only be changed on this page.

See also

Mapping Gates on page 200

Triggers on page 201

15.10.7.5 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.

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.

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. Configuration with the keypad is not supported.

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 the **Add** button to add a new camera or the **Edit** button to edit an existing camera.
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: • 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	Enter a login username for the camera which will be added to the command string below when the **Update Cmd. String** button is clicked.
Password	Enter a login password for the camera which will be added to the command string below when the **Update Cmd. String** button is clicked.
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. 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.

Configuring Verification Zones

To create a verification zone

1. Go to **Configuration > Advanced > Verification > Verification zones**.

   A list of any existing verification zones is displayed.
2. Click the **Add** button.
3. Enter a **Description** for the zone.
4. Select an **Audio** expander from the drop down list.
5. Select a **Video** from the drop down list.
6. Click the **Save** button.
7. Assign this verification zone to a physical zone on the SPC system. (See *Editing a zone* on page 185.)

See also

Editing a zone on page 185

Configuring Verification Settings

Note: The following settings apply to all verification zones (see *Configuring Verification Zones* above).

1. Select **Configuration > Advanced > Verification > Audio**.
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.

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 *Adding/Editing a User* on page 139.) The Web Access right must also be enabled for this functionality.

The View Video right can also be set on the keypad ('Video in Browser' setting).

To view images, go to **SPC Home > Video**. See *Viewing Video* on page 126.

See also

Adding/Editing a User on page 139

Configuring Video on page 205

15.10.7.6 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.

15.11 Configuring Communications

This section covers:

15.11.1 Communications Settings

This section covers:

- *Configuring the networking services of the panel* below
- *Ethernet* on the next page
- *Configuring Modems* on the next page
- *Serial ports* on page 215

15.11.1.1 Configuring the networking services of the panel

1. Select **Communications > Communications > Services**.
2. Configure the fields as described in the table below.

HTTP Enabled	Select this option 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	Select this option 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	Select this option 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.
GPRS DNS Enabled	Select this option to use DNS over GPRS
SNMP Enabled	Select this option to enable Simple Network Management Protocol (SNMP). (Default: Disabled)
SNMP Community	Enter the Community ID for the SNMP protocol. (Default : Public)
ENMP Enabled	Choose an option from the dropdown list to enable Enhanced Network Management Protocol (ENMP). (Default : Enabled in Full Engineer)
ENMP Port	Enter the ENMP port number (default: 1287).
ENMP password	Enter the password for the ENMP protocol.

ENMP change enabled	Selerct this option to enable network changes to be made with ENMP protocol.

15.11.1.2 Ethernet

IP

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**.
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.
DNS Server	Enter the IP address of the DNS server
Enable DHCP	Click this Button to enable dynamic address assignment on the panel.

15.11.1.3 Configuring Modems

The SPC panel provides two on-board modem interface connectors (primary and backup) that allow you to install GSM and/or PSTN modules onto the system.

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.

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* on page 49.)

1. Select **Communications > Communications > Modems**.
2. Click **Enable**.
3. Click **Configure**.
   - If you have installed a GSM Modem, the GSM Modem settings page displays.

     For more information, see *GSM modem* on page 211.
   - If you have installed a PSTN modem, the PSTN Modem settings page displays.

     For more information, see *PSTN modem* on page 213.

SMS detection and configuration is not available unless an SPC modem is correctly installed, configured and enabled.

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. 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.
- Also note that most Service Providers only allow SMS to a telephone registered in the same country (this is due to billing issues).

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
- SMS Authentication
- Engineer SMS Control
- User SMS Control

Depending on configurations, features include these SMS abilities:

- Event notification
- Remote Commands (users may be assigned select remote commands)

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 *Creating system users* on page 61.
   - **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 Only:** This is a valid PIN code configured for the user which different from the user's login code. Only when this option is selected will the SMS Controls be available for configuration by the user.
- **SMS PIN & Caller ID**

SMS commands

See *SMS Commands* on page 145 for more information.

GSM modem

Prerequisite

- A GSM modem must be properly installed and functioning correctly.

1. Select **Communications > Communications > Modems**.
2. Click **Configure**.
3. Configure the following fields.

GSM Modem settings

Country	Select the country that the SPC system is installed in.
SIM PIN	Enter the PIN for the SIM card installed in the GSM module.
Wireless Technology	**GSM only** Select the signal type that you wish to the modem to use: • **The SPC 320 is a 2G/4G Modem** • **The SPC342 is a 2G/3G/4G modem**
Allow Roaming	Select to enable GSM roaming. **Warning:** If this option is enabled, the modem can connect to a network in a different country. **Note:** Changing this setting resets the modem. **Note:** Supported on GSM modems v3.08 or higher.
USSD	**Pay-As-You-Go SIM only** Enter the code that the modem can use to query the network for the credit balance of the SIM. This code is network-dependent, please check with your service provider.
Incoming Calls	**Note:** Vanderbilt recommend that these options are not enabled for current systems. The modem can be programmed to answer calls based on the following conditions: • **Don't answer incoming calls:** The modem never answers calls. • **Answer incoming calls:** The modem answers incoming calls. • **Only answer when 'Engineer Access' is granted:** The modem only answers the call while engineer access is granted to the system.

Line Monitoring	• **Disabled** • **Enable** • **Fullset** 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. (See *Options* on page 169.)
Monitoring Timer	Enter the time period in seconds for which the signal level must drop to Low before the SPC system registers a fault. 0 to 9999 seconds range.
Modem Fault Time	Enter the time delay in seconds before the SPC system sends an alert. 0 to 9999 seconds range.
SMS Enable	Tick this checkbox to enable the transmission and reception of SMS messages and command control.
Automated SMS	• **Disabled** • **1 hour** • **24 Hours** • **48 Hours** • **7 Days** • **30 Days** Select the timing for automated SMS messages.
Automated SMS Number	Enter SMS number to receive automated SMS messages. Only one device can receive these messages.
Start Date/Time	Enter the start date and time from when the system will send automated SMS messages.
Mobile Data Configuration	
Access Point (APN)	Enter Access Point details to enable any IP communications. These details are service provider-dependent.
Access Point User Name	Enter Access Point details to enable any IP communications. These details are service provider-dependent.
Access Point Password	Enter Access Point details to enable any IP communications. These details are service provider-dependent.
Dial Up Internet Configuration	
Dial Up Internet Enable	Select this option to enable the modem to gain internet access through a dial-up connection
Phone Number	Enter the phone number for the dial-up connection.
Username	Enter the dial-up connection Username.
Password	Enter the dial-up connection Password.

Click the **Test SMS** button to send a short text message for the purposes of testing the system.

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.

PSTN modem

1. Select **Communications > Communications > Modems**.
2. Click **Configure**.
3. Configure the fields as described in the table below.

PSTN Modem settings

Country	Select the country that the SPC is installed in.
Incoming Calls	The modem can be programmed to answer calls based on the following conditions: • **Don't answer incoming calls** Modem never answers calls. • **Answer after 'x' rings** Select the number of rings (1 to 8) after which the modem answers the incoming call. • **Answer when after one ring phone is hung up, then immediately dialled again** If 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** The modem only answers the call while engineer access is granted to the system.
Prefix	Enter the number required to access a line (for example, if connected to a PBX).
Line Monitoring	Enable this feature to monitor the voltage of the line connected to the modem. **Note:** EN 50131-9 Confirmation configuration – In order for EN50131-9 Confirmation to operate correctly, line monitoring must be enabled. (See *Options* on page 169.)
Monitoring 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	Tick this checkbox to enable the SMS feature on the system. **Note:** The SMS operates using a standard protocol that is used in SMS telephones. 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. Also note that most Service Providers only allow SMS to a telephone registered in the same country (this is due to billing issues). **Note:** SMS over PSTN is no longer supported. The functionality remains in the product for backward compatibility.
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.
Dial Up Internet Configuration	
Dial Up Internet Enable	Select this option to enable the modem to gain internet access through a dial-up connection.
Phone Number	Enter the phone number for the dial-up connection.
Username	Enter the dial-up connection Username.
Password	Enter the dial-up connection Password.

Click the **Test SMS** button to send a short text message for the purposes of testing the system.

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. Contact your local supplier for more information (support of feature, recommended service provider).

15.11.1.4 Modem Status

Modem status

Status information for installed and configured modems is displayed on the main Status page.

The Modem 1 and Modem 2 areas of the Status page displays some or all of the following information, depending on the type of modem that is installed.

Modem Status	Indicates if the modem is Ready or if there is a Fault.
Modem Connection	Indicates the network operator, and the network type
IMSI	The international mobile subscriber identity (IMSI) is a unique number identifying a GSM subscriber
ICCID	The Integrated Circuit Card Identifier (ICCID) is a unique number associated with all physical SIM cards. It may be printed on the SIM card.
Type fitted	Identifies the type of modem (PSTN, GSM) that is fitted in this modem slot.

Line Status	Information on the signal strength (GSM), or the status of the phone line (PSTN).
Incoming Calls	Number count and (Duration) of incoming calls
Outgoing Calls	Number count and (Duration) of outgoing calls
Incoming SMS	Number count of incoming SMS
Outgoing SMS	Number count of outgoing SMS
Failed Dial Attempts	Number count of attempts to dial out that have failed.

15.11.1.5 Serial ports

The SPC controller provides a serial port (RS232) that offer the following functionality:

- **Logging of Events:** The Serial port 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:** The Serial port 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.

To configure the serial ports:

- Select **Communications > Communications > Serial Ports**.

  The settings displayed will depend on the type of connection that the ports are used for. The settings are described in the following sections.

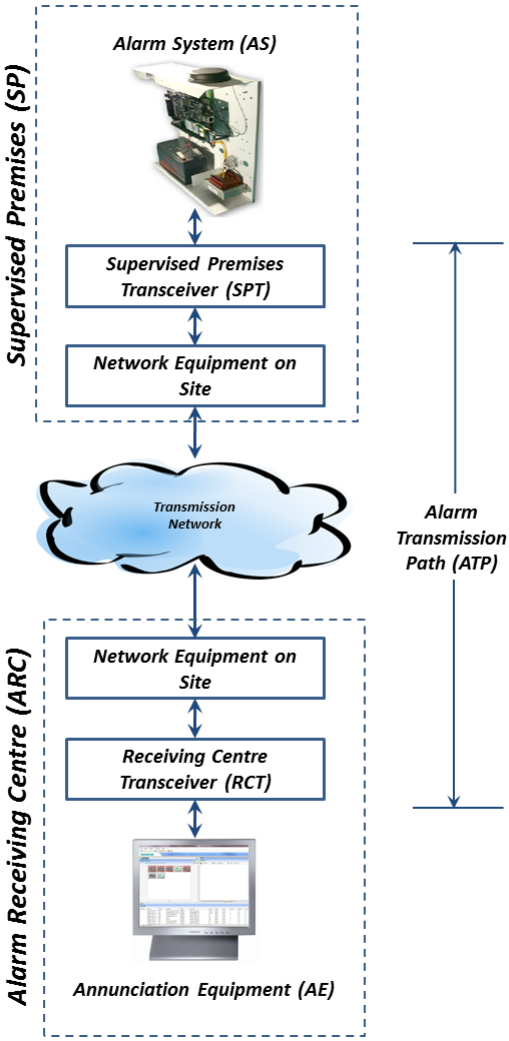
15.11.2 FlexC®

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, for example, Ethernet integrated onto the SPC panel) and a Receiving Centre Transceiver (RCT, for example, SPC Com XT or the SPC Connect server, www.spcconnect.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.spcconnect.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 below

Configuring Event Profiles on page 233

Event Exception Definition on page 233

Configuring Command Profiles on page 235

FlexC Status on page 136

Configuring an EN50136-1 ATS or Custom ATS on page 218

15.11.2.1 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.

15.11.2.2 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 page 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 (for example, SPC Com XT)
- Auto Encryption with no password

1. To quickly configure a FlexC connection between a panel and an RCT (for example, 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** :
   - **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
3. Complete the fields on the **ATP Configuration - EN50136 ATS** page as 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.
4. Click **Save**. The **ATS Configuration** page displays showing the **ATS Registration ID** and the configured primary ATP or primary and backup ATPs in the **Event Sequence Table**.
5. On the **ATS Configuration** page, 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* on the facing page.
6. 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 (for example, 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 *SPC Com XT Installation & Configuration Manual*.
RCT URL or IP Address	Enter the **RCT URL** or **IP Address** for the RCT server location (for example, SPC Com XT server).
RCT TCP Port	Enter the TCP port for the RCT (for example, 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* on page 292.
Primary Interface	Select the **Primary Interface** to apply to the primary communications path from the following: • 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: • Ethernet • GPRS: Modem 1 • GPRS: Modem 2 • Dial Up Internet: Modem 1 • Dial Up Internet: Modem 2

15.11.2.3 Configuring an EN50136-1 ATS or Custom ATS

An ATS comprises an alarm panel, network paths and an RCT (for example, 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.

NOTICE: 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* on page 216.

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
3. For an EN50136 ATS, you must configure the settings on the **ATP Configuration - EN50136** page first. See *Quick Start ATP Configuration for EN50136 ATS* on page 216.
4. The **ATS Configuration** page displays. An EN50136-1 ATS will display a primary or primary and backup ATP in the **Event Sequence Table**.
5. 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.
6. 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* on page 220) or click **Add ATP to Analog ARC** (see *Add ATP to Analog ARC* on page 229).

7. Select an **Event Profile** from the dropdown menu. To customise how events are transmitted on an ATS, see *Configuring Event Profiles* on page 233.
8. Select a **Command Profile** from the dropdown menu. To customise the commands enabled for an RCT to control a panel, see *Configuring Command Profiles* on page 235.
9. Complete the **ATS Faults** fields as shown in the table below.

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.
ATS/ATP Fault Events	Select to generate network events when this ATS or any other ATS on the system goes up or down. Default setting is off.
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.
Log ATS Faults	Select this to add ATS faults to the system log.

10. Click the **Edit Installation Details** button to complete the settings to identify the panel to the RCT operator. See *Edit Installation Details* on page 231.
11. Click **Save** and **Back** to return to the **ATS Configuration** page. The new ATS displays in the **Configured ATS table**.
12. 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 (for example, SPC Com XT). See the *SPC Com XT Installation & Configuration Manual*.

See also

ATS Category Timings on page 292

Add ATP to FlexC RCT

Add ATP to FlexC RCT allows you to configure an ATP between the SPC panel and the RCT (for example, SPC Com XT). You can configure up to 10 ATPs for each ATS.

1. Click the button **Add ATP to FlexC RCT**.
2. Complete the ATP fields described in the table below.

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 *SPC Com XT Installation & Configuration Manual*.
ATP Interface	
Communications Interface	From the dropdown list, select the interface this ATP uses for communication. • Ethernet • GPRS: Modem 1 • GPRS: Modem 2 • 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* on page 293.
Advanced	
Advanced ATP Settings	It is not recommended to change advanced settings. Changes must only be made by expert users.

3. 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* on the next page.
4. Click **Save**.

Configure Advanced ATP Settings

WARNING: It is not recommended to change **Advanced ATP Settings**. Changes must only be made by expert users.

1. Click the **Advanced ATP Settings** button.

   Configure the fields described in the table below.

ATP Connections	
Active ATP Connection	Select the ATP connection type when the ATP is operating as the primary communication path. • 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	Select the ATP connection type when the ATP is operating as a backup communication path. • 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)	Select the mode for sending test calls when the ATP is the non-active ATP. • 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)	Select the mode for sending test calls when the ATP is the active ATP. • 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	Select how the encryption gets updated. • Auto Encryption • Auto Encryption with Updates • Fixed Encryption **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.
Encryption Password	Optional password used to provide increased security during initial ATP commissioning. The password must be entered at the SPT or RCT independently.
Reset Encryption	Reset the Encryption Key and password to the default values.
ATP Profiles	
Event Profile	Select the Event Profile which defines how and which events are transmitted on this ATS. • Use ATS Setting • Default Event Profile • All events
Command Profile	Select the Command Profile which defines the commands that are allowed on this ATS. • 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. • 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. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes
Event Message	Minimum length of an event and test call message. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes
Other Message	Minimum length of connection and encryption key and update messages. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes

ATP Connections	
Active ATP Connection	Select the ATP connection type when the ATP is operating as the primary communication path. • 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	Select the ATP connection type when the ATP is operating as a backup communication path. • 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)	Select the mode for sending test calls when the ATP is the non-active ATP. • 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)	Select the mode for sending test calls when the ATP is the active ATP. • 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	Select how the encryption gets updated. • Auto Encryption • Auto Encryption with Updates • Fixed Encryption **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.
Encryption Password	Optional password used to provide increased security during initial ATP commissioning. The password must be entered at the SPT or RCT independently.
Reset Encryption	Reset the Encryption Key and password to the default values.
ATP Profiles	
Event Profile	Select the Event Profile which defines how and which events are transmitted on this ATS. • Use ATS Setting • Default Event Profile • All events
Command Profile	Select the Command Profile which defines the commands that are allowed on this ATS. • 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. • 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. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes
Event Message	Minimum length of an event and test call message. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes
Other Message	Minimum length of connection and encryption key and update messages. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes

ATP Connections	
Active ATP Connection	Select the ATP connection type when the ATP is operating as the primary communication path. • 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	Select the ATP connection type when the ATP is operating as a backup communication path. • 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)	Select the mode for sending test calls when the ATP is the non-active ATP. • 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)	Select the mode for sending test calls when the ATP is the active ATP. • 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	Select how the encryption gets updated. • Auto Encryption • Auto Encryption with Updates • Fixed Encryption **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.
Encryption Password	Optional password used to provide increased security during initial ATP commissioning. The password must be entered at the SPT or RCT independently.
Reset Encryption	Reset the Encryption Key and password to the default values.
ATP Profiles	
Event Profile	Select the Event Profile which defines how and which events are transmitted on this ATS. • Use ATS Setting • Default Event Profile • All events
Command Profile	Select the Command Profile which defines the commands that are allowed on this ATS. • 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. • 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. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes
Event Message	Minimum length of an event and test call message. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes
Other Message	Minimum length of connection and encryption key and update messages. • 0 Bytes • 64 Bytes • 128 Bytes • 256 Bytes • 512 Bytes

2. Click **Save**.

Add ATP to Analog ARC

If a connection between the SPC panel and RCT (for example, 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.

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. • 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. • 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. • 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. • Send Immediately (default) or • Select a half hour interval between 00:00 and 23:30

Event Protocol	
Protocol	Protocol used in communication. • 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. • 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	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. • 30 seconds • 60 seconds • 90 seconds • 2 minutes • 3 minutes • 5 minutes • 10 minutes

3. Click **Save**.

Edit Installation Details

The installation details are passed to the RCT to help the operator to identify the panel.

1. Click the **Edit Installation Details** button.
2. Complete the fields in the table below.

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.

3. Click **Save**.

15.11.2.4 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.spcconnect.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. On the **ATS Configuration** page, 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* on page 220.
   - Default Events Profile for SPC Connect
   - Default Commands Profile for SPC Connect
   - Default RCT URL is www.spcconnect.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 System User Guide*.

15.11.2.5 Exporting and Importing an ATS

ATS files have a .cxml 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.
3. Save the file with the default filename **export_flexc.cxml** 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 (.cxml 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.

15.11.2.6 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* below.

To see a list of all events, go to **Communications > FlexC > Event Profiles**. Click the **Edit** icon for an event profile. Scroll to the end of the page and click **Show Complete Event Table**.

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** icon. Scroll to the bottom of the page and click **Replicate**. You can now make the changes you require.

1. To configure FlexC event profiles step by step, go to **Communications > FlexC > Event Profiles**.
2. Click **Add**.
   The **Event Profiles** page displays.
3. Enter a **Name** to identify the event profile.
4. Select the event filter groups to report for this profile by ticking the **Report Event** checkboxes.
5. To prevent reporting of certain events or addresses within an event, select the event from the corresponding **Add Event Exception** dropdown list.
6. Click **Add** to view the **Event Exception Definition** page. See *Event Exception Definition* below.
7. Click **Back** to return to the **Event Profiles** page.
8. To apply an event profile to an area, select the area under **Area Filter**.
9. 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** page.

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.

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 (for example, 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

1. To configure an **Event Exception Definition**, complete the fields described in the table below.

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 *Zone ID 1 - 9* for that event. Alternatively, if you choose not to report the event type BA, you may choose to report *Zone ID 1- 9* 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 *Zone ID 1 - 9* to *Zone ID 101 - 109*. 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 *Zone ID 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*.

2. Click **Save**.
3. Click **Back** to return to the **Event Profiles** page.

The name of each exception displays in the **Event Exceptions** table at the bottom of the page. The table shows the settings for the fields **Report Event**, **Filter Exception**, **Event Code (SIA/CID)** and **Remap Exception** for the event.

4. Click the **Edit** icon to make changes or the **Delete** icon to remove an **Event Exception**.
5. To apply the event profile to an area, select the area checkbox.
6. Click **Save** to save the event profile.
7. Click **Back** to view the profile in the **Event Profiles** table.

15.11.2.7 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.

NOTICE: 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 page and click **Replicate**. You can now make the changes you require.

1. To add a command profile step by step, go to **Communications > FlexC > Command Profiles**.
2. Click **Add**.
3. Enter a **Name** to identify the command profile.
4. Select an **Authentication Mode** (Command User or Panel User, Command User Only, or Any Panel User) from the dropdown menu.

NOTICE: 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.

5. 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.
6. 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.
7. 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.
8. Under **Command Filter**, select the commands to enable. For a full list of commands, see *FlexC Commands* on page 289.
9. Select the commands to log.
10. Click **Save**.
11. Click **Back** to view the command profile in the **Command Profiles** table.
12. To change a command profile, click the **Edit** button next to a command profile.

15.11.3 Reporting

This section covers:

- *Alarm Reporting Centres (ARCs)* on the facing page
- *EDP Setup* on page 238

- *CEI-ABI Protocol Settings* on page 243

15.11.3.1 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.

Adding/Editing an ARC using SIA or CID

Prerequisite

- PSTN or GSM modem is installed and functioning correctly.

1. Select **Communications > Reporting > Analog ARC**.
2. Click the **Modem1/2** button to make a test call to the ARC from the either modem 1 or modem 2.
3. Click the **Log** button to receive a log file. A page 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**.
5. Configure the fields as described in the table below.

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.

6. Click the **Add** button to enter those details on the system.

   A list of the configured ARC accounts will be displayed in the browser along with the account information, description, protocol, dial-up status and time and date of the last call to the ARC.

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 **Select Communications > Reporting > Analog ARC > Edit > Filter**.
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.

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:

1. Select **Communications > Reporting > Analog ARC > Edit > Filter**.

   A list of the eight channels is displayed along with the alarm conditions that can be programmed for each channel.

2. Select the alarm conditions for each channel as required. For a description of each, see *Outputs types and output ports* on page 155.
3. From the **Scope** dropdown menu, select **System** or a specific area to apply your selected settings.
4. Click the **Test** button located next to the first channel to test the alarm activation.

   The light bulb icon is switched on.

5. 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.
6. Continue to test the other channels.

15.11.3.2 EDP Setup

IP

The system has the facility to communicate information to the SPC Com server remotely using Vanderbilt's own protocol, the EDP (**E**nhanced **D**atagram **P**rotocol). 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 *Ethernet interface* on page 122) and that internet access is enabled at the router.

Adding an EDP Receiver

1. Select **Communications > Reporting > EDP**.

   Max. 8 receivers can be added to the SPC system.

2. Click the **Add** button.

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 below

Editing EDP Receiver Settings

1. Select **Communications > Reporting > EDP > Edit**.
2. Configure the fields as described in the table below.

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: • 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, that is, 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. See *Editing Event Filter Settings* below.

* EDP dial-up over PSTN is not supported in this release.

See also

Configuring SMS on page 144

Editing Event Filter Settings

1. Select **Communications > Reporting > EDP > Edit > Filter**.
2. Configure the fields as described in the table below.

   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.

Editing EDP settings

1. Select **Communications > Reporting > EDP > Settings**.
2. Configure the fields as described in the table below.

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.

15.11.3.3 CEI-ABI Protocol Settings

1. Select **Communications > Reporting > CEI-ABI**.
2. Configure the fields as described in the table below.

Enable	Tick this box to enable CEI-ABI support.
Connection mode	• Select **Client** to connect the panel to the CEI-ABI receiver. • Select **Server** to enable the panel to listen for connections.
Server IP	If you select **Client** for **Connection mode**, enter the TCP/IP address of the CEI-ABI receiver.
Server Port	Enter the IP port for the server.
Physical address	Enter a physical address for the CEI-ABI on the panel.
Logical address	Enter a logical address for the CEI-ABI on the panel.

15.11.4 PC Tools

This section covers:

- *SPC Connect PRO* below
- *SPC Manager* on the facing page

15.11.4.1 SPC Connect PRO

SPC Connect PRO is a desktop application designed to support the installation and maintenance of SPC systems. Using SPC Connect PRO, you can create installations and configure them prior to arriving at site. The tool can also be used in conjunction with the SPC cloud service SPC Connect to remotely connect to customer sites and support them.

1. Select **Communications > PC Tools > SPC Connect PRO**.
2. Configure the fields as described in the table below then click **Save**.

SPC Connect PRO	Tick this box to enable SPC Connect PRO to connect to the panel.
Ethernet	Tick this box to allow SPC Connect PRO to connect over Ethernet.
TCP Port	Enter the TCP port on which the panel listens to incoming connections from SPC Connect PRO.
USB	Tick this box to allow SPC Connect PRO to connect over USB.

Modem 1	Tick this box to allow SPC Connect PRO to connect over Modem 1.

15.11.4.2 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 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 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.

15.12 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* on the next page.
File Manager	Options for managing the system configuration file and uploading and downloading users data to and from the panel. See *File Manager Operations* on page 247.
Audio	Upload an audio file to the SPC. Click **Browse** and click **Upload** to add the audio file to the SPC. After upload, click the **Test** button to validate the audio file.
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 summarizes the configuration for your SPC product settings based on selected **Region**, **Grade** and **Type**.

15.12.1 File Upgrade Operations

To upgrade firmware and languages on the system:

- Select **File > Upgrade**.

See also

Options on page 169

15.12.1.1 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 *Options* on page 169.

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, PSTN modem, GSM modems, and the SPCW120 Transceiver. Filename has the extension *.pfw.

The two files are upgraded separately.

NOTICE: It is recommended that all peripheral firmware is upgraded after a new controller firmware upgrade.

Note: Firmware can also be upgraded using the keypad.

Controller Firmware

To upgrade controller firmware on the system:

1. Select the **Panel Upgrade Operations** option from the **File** page.
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 page is displayed.
3. Click 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.

WARNING: If you downgrade the controller firmware (that is, 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.

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.

- Click the **Upgrade** button for the peripherals that require upgrading or click 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.

Upgrading the SPCP355.300 Smart PSU Firmware

To upgrade the SPCP355.300 Smart PSU you must ensure the following:

- 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 on page 141

15.12.1.2 Upgrading Languages

A custom language file (*.clng) can be uploaded to the panel.

NOTICE: The panel must be licensed for use of custom languages and other languages.

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 + English can be installed.

4. Click the **Upgrade Selected** button.

   The **Confirm Language Upgrade** page is displayed showing any languages that are being

installed.

5. Click 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 the **Upgrade Selected** button.

   The **Confirm Language Upgrade** page is displayed. When deleting a language, the panel deletes all languages and reinstalls only the languages required.

4. Click the **Confirm** button to confirm the languages being deleted.

See *Language* on page 185 for details of selecting the panel 'System' and 'Idle State' languages in the browser.

See *Options* on page 67 for details of selecting the panel 'System' and 'Idle State' languages on the keypad.

See also

Language on page 185

15.12.2 File Manager Operations

- Select **File > File Manager**.

  A page displays showing details of the system configuration, language and trace files.

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: 1. Select **Internet Options** in the **Tools** menu. 2. Select the **Advanced** tab. 3. Select the checkbox **Do not save encrypted pages to disk**. 4. Click **Apply**. 5. Click **OK**. 6. Click **Download** again. 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.
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 the save the **users.csv** file.
Upload	Click the **Browse** button to **Upload** users data to the panel. This must be a .csv file format.

16 Accessing web server remotely

This chapter covers:

16.1 PSTN connection

PSTN Connection

1	Remote PC with browser
2	PSTN modem
3	PSTN network
4	Telephone line
5	PSTN modem
6	SPC controller

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 (see the 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** page).
2. On the **Network Connection Type** page, select **Connect to the Internet**.
3. On the **Getting Ready** page, choose **Setup my connection manually**.

4. On the **Internet Connection** page, choose **Connect using Dialup modem**.
5. On the **Connection Name** page, enter the connection name, for example, SPC remote connection.
6. On the **Phone Number to Dial** page, enter the phone number of the PSTN line connected to the PSTN modem.
7. On the **Connection Availability** page, choose whether this connection is available to all users.
8. On the **Internet Account Information** page, enter the following details:

   - Username: SPC

   - Password: password (default)

   - Confirm Password: password

   The **Completing the New Connection Wizard** page 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 be 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 the icon located in the **Control Panel > Network Connections** page.

  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 it acceptable to continue. For further queries, contact your network administrator or a Vanderbilt technician.

To obtain this IP address:

1. Right click the dial-up icon.
2. Click the **Details** tab.

   The IP address is displayed as the Server IP address.
3. Enter this IP address in the address bar of the browser and click.
4. 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 page is displayed.

17 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 *Domestic, Commercial and Financial mode default settings* on page 267.

17.1 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.

17.2 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.

Alarm Mode	Description
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.

17.3 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.

17.4 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 *Wiring the system* on page 35.

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.

18 System examples and scenarios

This chapter covers:

18.1 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, that is, front door access to the entire building.

19 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 (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* on page 185.)
2. Set the attributes for the zone.
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* on page 179.)
7. Configure an output for testing a seismic zone. (See *Outputs types and output ports* on page 104.) 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.

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 on page 179

Outputs types and output ports on page 104

Editing a zone on page 185

19.1 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.

19.1.1 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 (that is, when it is active). If this signal is not suitable for a particular sensor then the physical output can be configured to be inverted.

19.1.2 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 **System Timers** menu (see *Timers* on page 179) 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 **Options** menu (see *Options* on page 169). 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 or the browser. However, there is an automatic seismic test when a virtual keypad is used with SPC Com.

No event is reported if seismic testing on set fails.

The periodic automatic system test timer restarts after a test is performed after setting.

19.1.3 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 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.

20 Blocking Lock Operation

Blocking Lock operation and the Authorized Setting operation of a Blocking Lock is supported by the SPC intrusion panel.

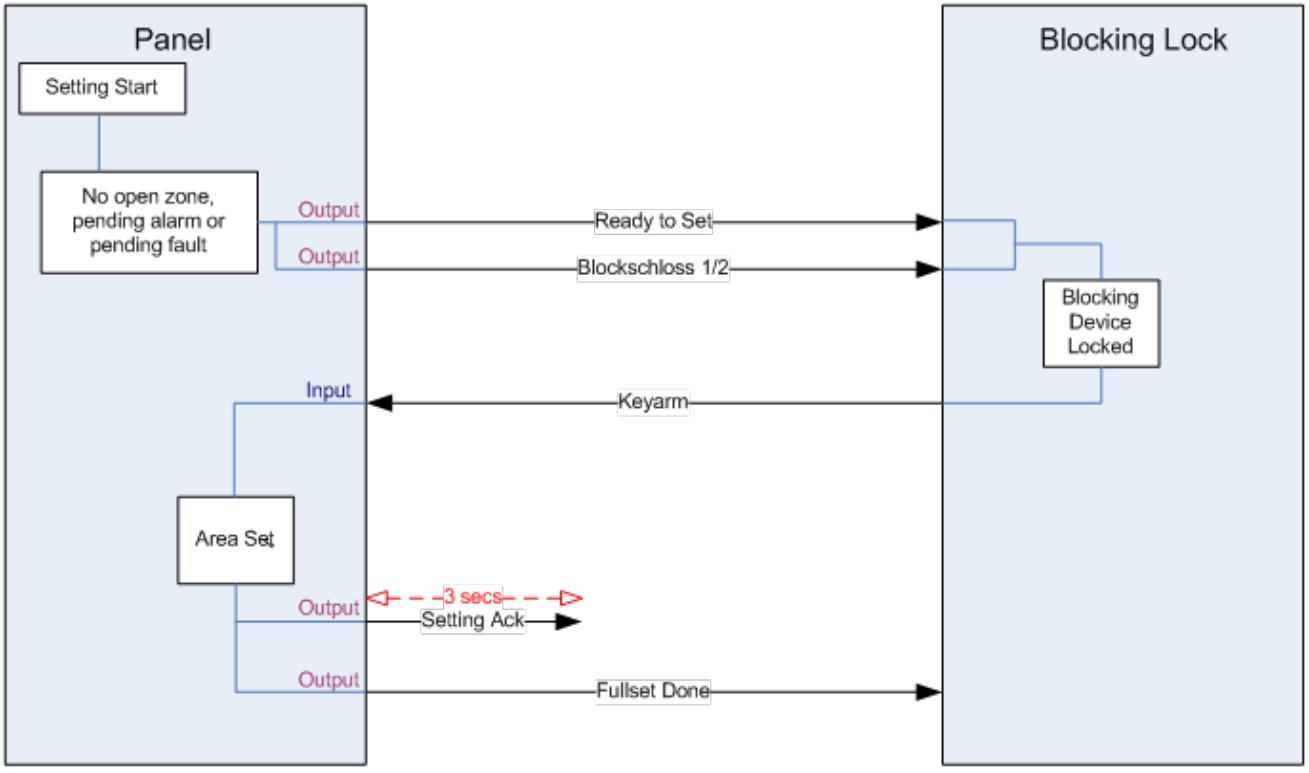
20.1 Blocking Lock

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, Sigmalock Plus, E4.03 device (Blockschloss 2).

Depending on the kind of Blocking Lock, a signal is needed to enable locking and unlocking the lock, that is, 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:

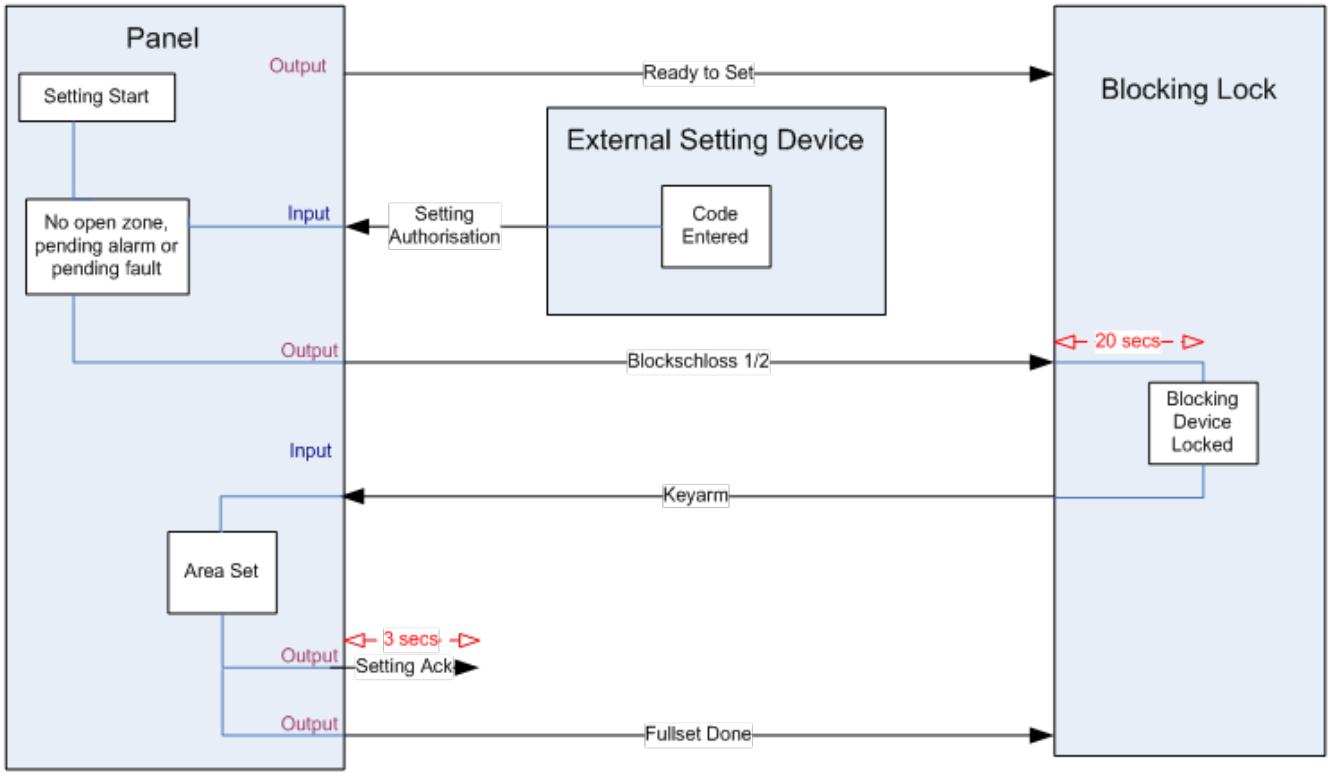
- Outputs:
  – Ready to set
  – Setting Ack
  – Fullset Done
  – Blockschloss 1/2
- Inputs
  – Keyarm

20.2 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

20.3 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.

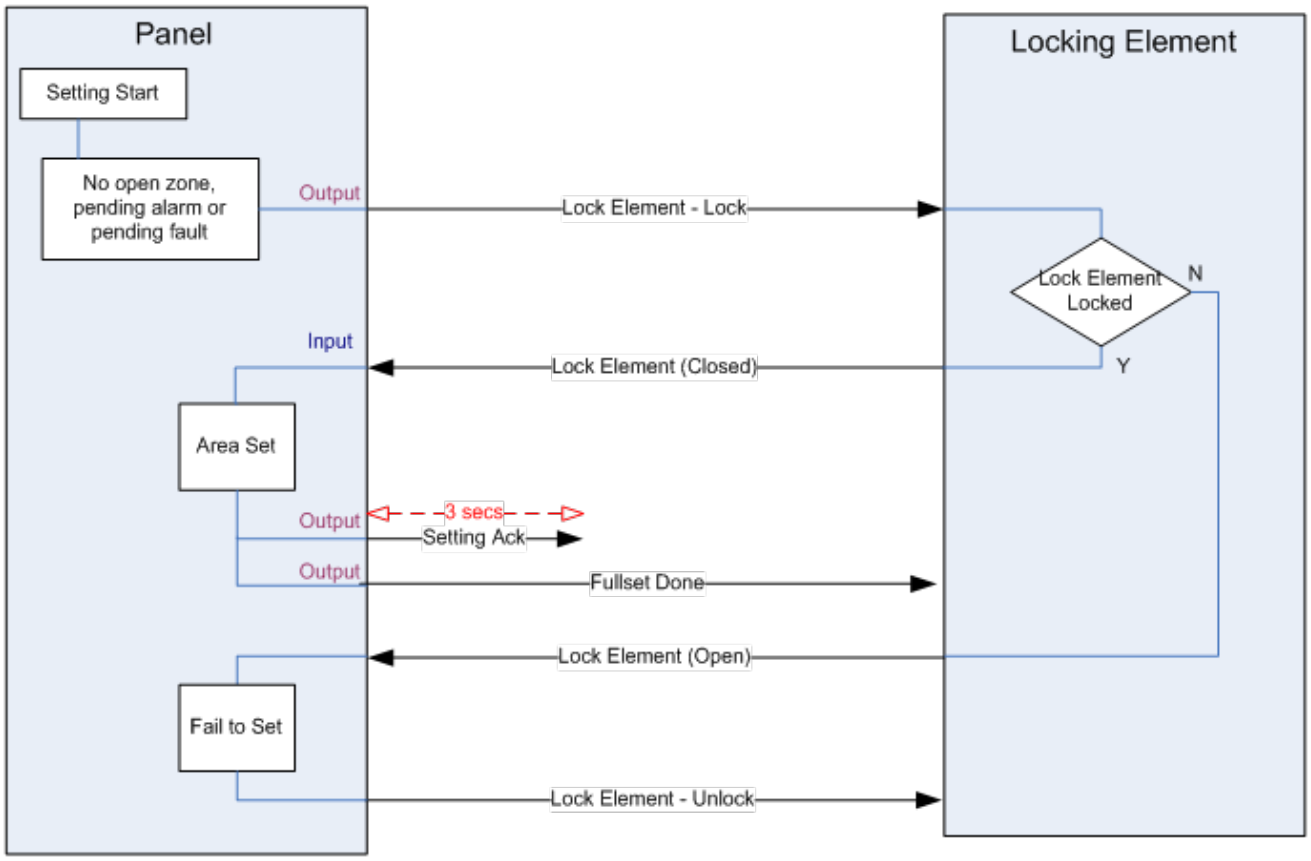
If a lock element is located within an area, the exit timer will be restricted to a minimum of 4 seconds so that the lock element can be activated. When the exit timer reaches four seconds, the lock element will be activated for three seconds. When the exit timer expires, the **Lock Element** input must 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

21 Appendix

This appendix covers:

21.1 Network cable connections

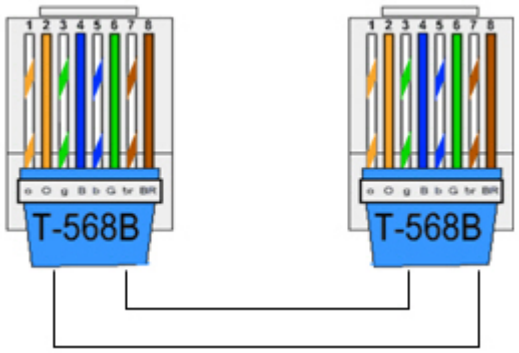
IP

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 (that is, a hub or switch is not used), then a crossover cable should be connected between the SPC controller and the PC.

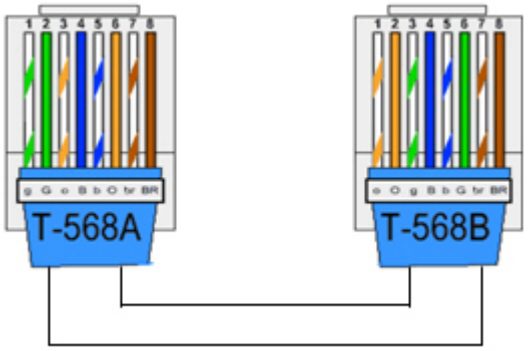
Use the straight through cable for connecting the SPC controller to a PC via a hub.

RJ45 PIN	RJ45 PIN
1 (RX +)	1 (TX +)
2 (RX -)	2 (TX -)
3 (TX+)	3 (RX+)
6 (TX-)	6 (RX-)



Use the crossover cable for connecting the SPC controller directly to a PC.

RJ45 PIN	RJ45 PIN
1 (RX +)	3 (TX+)
2 (RX -)	6 (TX-)
3 (TX+)	1 (RX +)
6 (TX-)	2 (RX -)



21.2 Controller status LEDs

LED	Function
LED 1	Main Processor Heartbeat FLASHING: system is functioning normally
LED 2	System Fault ON: A hardware fault has been detected on the board. OFF: No hardware fault has been detected.
LED 3	Secondary (Coprocessor) Heartbeat FLASHING: System is functioning normally.
LED 4	Mains Supply ON: Mains failure OFF: Mains OK

21.3 Powering expanders from the auxiliary power terminals

To calculate the number of expanders/keypads that can safely be powered from the auxiliary 12V DC 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 12V DC auxiliary power.

See the technical data for the specific auxiliary current and the corresponding installation instruction or data sheet of modules, keypads and expanders for current consumption.

Expander 1 Current (mA) + Expander 2 Current (mA) + ….. <Auxiliary Power

If the electronic or relay outputs are already powering external devices, the power supplied to these devices must be subtracted from the 12V DC auxiliary power supply to determine the amount of available power from the auxiliary power terminals (0V 12V).

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 12V power terminals
4	Keypad
5	Keypad
6	I/O expander

21.4 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 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.

$$\frac{0.85 \times \text{battery size (Ah)}}{\text{Time (hours)}} - (\text{Icont} + \text{Ibell}) = \text{Imax}$$

Battery size = capacity, in Ah, depending upon SPC housing chosen

Time = backup time, in hours, depending upon security grade

Icont = quiescent current (in A) for the SPC controller

Ibell = quiescent current (in A) for the attached external and internal bells

Imax = the maximum current that can be drawn from the auxiliary power output

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.

21.5 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
Zone Names			
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
Zone Types			
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

21.6 SIA Codes

DESCRIPTION	CODE
AC RESTORAL	AR
AC TROUBLE	AT
BURGLARY ALARM	BA
BURGLARY BYPASS	BB
BURGLARY CANCEL	BC
SWINGER TROUBLE	BD
SWINGER TROUBLE RESTORE	BE

DESCRIPTION	CODE
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

DESCRIPTION	CODE
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
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

DESCRIPTION	CODE
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
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

DESCRIPTION	CODE
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
ENET PANIC RESTORAL	PR
USER PANIC ALARM	PA
ENET FIRE ALARM	FA

DESCRIPTION	CODE
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

DESCRIPTION	CODE
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
DEEP CHARGE	XK
LOCKED OUT	WW

21.7 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* on page 1.
130	BURGLARY	
134	ENTRYEXIT	
137	TAMPER	Housing 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.

CODE	CID EVENT	DESCRIPTION
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.

21.8 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:

$10^{\text{No of digits}}$ = 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* on page 59 for more details.

21.9 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 (for example, 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** (see *Options* on page 169) and specific users enabled for duress (see *Users* on page 138), it must not be changed unless all the users are deleted and re-allocated user PINs.

21.10 Automatic inhibits

The system supports automatic inhibits in the following instances.

21.10.1 Zones

When the UK and Commercial are selected (see *Standards* on page 184), 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.

21.10.2 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.

21.10.3 Engineer Access

An Engineer can only access the system if permitted by a 'Manager' user type (see 'Engineer' attribute in *User rights* on page 141) and only for a specified time duration (see 'Engineer Access' in *Timers* on page 179).

21.10.4 Keypad User Logoff

If no keys are pressed on a keypad for a specific duration (see 'Keypad Timeout' in *Timers* on page 179), the user is automatically logged off.

21.11 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 3mm distance between the contacts
- Minimum size conductor used for connecting mains is 1.5mm square
- The circuit breakers must have a maximum rating of 16A

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, that is, 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.

21.12 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 and 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 housing.
- The time and 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 and 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.

21.13 Maintenance

The system should be serviced in accordance with the service schedule that is in place.

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).

- 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 housing.
- 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.

21.14 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 (for example, 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 Partset 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.

Zone Type	Processing Category	Description
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: • 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: • 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

Zone Type	Processing Category	Description
KEYARM	Intruder	This zone type is normally used in conjunction with a key lock mechanism. A Keyarm can be configured to perform the following **Setting Options**: • **Fullset** • **Partset A** • **Partset B** A Keyarm zone will SET the System/Area/Common Areas according to the selected **Setting Option** when it is OPENED and will UNSET the System/Area/Common Areas according to the selected **Setting Option** when it is CLOSED. • If the zone with the keyarm zone type is assigned in an 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 (that is, Open once to SET the system, Close and Open again to UNSET). • 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. Keyarming will force set the system/area and auto-inhibit any open zones or fault conditions. **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.**
SHUNT	Intruder	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. 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.
X-SHUNT	Intruder	This zone type is only available in Commercial Mode of operation. 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.

Zone Type	Processing Category	Description
DETECTOR FAULT	Fault	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. When the system is armed, a fault output is triggered. Both the keypad LED and the buzzer are activated when Unarmed.
LOCK SUPERVISION	Intruder	Only available in Commercial mode. Used to monitor a door lock. System can be programmed not to set unless door is locked.
SEISMIC	Intruder	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.
ALL OKAY	Intruder	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 *Adding/Editing an area* on page 186 for details of 'All Okay' configuration.) All Okay uses two outputs, Entry Status (Green LED) and Warning Status (Red LED), to indicate entry status using LEDs on the keypad.
UNUSED	Intruder	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.
HOLDUP FAULT	Fault	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. When the system is armed, a fault output is triggered. Both the keypad LED and the buzzer are activated when Unarmed. 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.
WARNING FAULT	Fault	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. When the system is armed, a fault output is triggered. Both the keypad LED and the buzzer are activated when Unarmed. 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. **Note:** On a grade 2 system, a cable fault will cause a fault and not an 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

Zone Type	Processing Category	Description
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	Zone is connected to an RI S 10 D-RS-LED glassbreak interface in combination with GB2001 glassbreak detectors. • 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.
WATER		This zone type follows the same behaviours as a Technical zone type.
HEAT		This zone type follows the same behaviours as a Technical zone type.
FRIDGE/FREEZER		This zone type follows the same behaviours as a Technical zone type.
GAS		This zone type follows the same behaviours as a Technical zone type.
SPRINKLER		This zone type follows the same behaviours as a Technical zone type.
CO		This zone type follows the same behaviours as a Technical zone type.
ENTRY/EXIT 2		This zone type follows the same behaviours as an Entry/Exit zone type with a separate Entry timer. This is so that there can be two entry timers to a building from different points.

21.15 Zone attributes

The zone attributes on the SPC system determine the manner in which the programmed zone types function. For more information on how to change the attributes for a zone, see *Editing a zone* on page 185).

Zone attribute	Description
Access	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. The 'Access' attribute is only valid for Alarm zone types. All connected devices (Bells - Internal and External, Buzzers, Strobe) are activated. **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.
Exclude A	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. 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 and External, Strobe).
Exclude B	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. 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 and External, Strobe).
24 Hour	If a Zone is assigned the '24 Hour' attribute, then it is active at all times and 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. **Note:** The 24 Hour attribute overrides the settings of any of the other attributes for a particular alarm zone.
Local	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.
Unset Local	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.
Double Knock	Use this attribute to deal with troublesome detectors (for example, some detectors may generate activation signals spuriously, thereby inadvertently trigger alarms on the system). 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 *Timers* on page 179). Two open actions within that time period will generate an alarm. All open double knock zones are logged when the system is armed.

Zone attribute	Description
Chime	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.). The Chime attribute is valid for Alarm, Entry/Exit, and Tech. zones types.
Inhibit	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.
Normal Open	When the 'Normal Open' attribute is set, the system expects that a connected detector/sensor is a Normally Open device (for example, a sensor is deemed to be activated whenever the contacts are closed on the device).
Silent	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.
Log	If this attribute is set then all zone state changes are logged.
Exit Open	If set then zone will be indicated if open during setting.
Frequent	This attribute only applies to remote services*. If this attribute is set for a zone, the zone must open for remote service purposes within the defined frequent time period.
End of Line	The End Of Line (EOL) attribute provides a number of input zone wiring configurations on the system.
Analysed	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.
Pulse Count	Pulse count trigger level for analysed inertia sensors.
Gross Attack	Gross attack trigger level for analysed inertia sensors
Final Exit	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.
Shunt	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.
Report Only	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.
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.

Zone attribute	Description
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* on page 179.) 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 file alarm is reported for the zone. See *Timers* on page 179.
Seismic Test/Automatic Sensor Test	A Seismic zone type may be tested manually or automatically. This attribute allows automatic testing to be enabled. See *Timers* on page 179 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.
Auto Restore	Enable this feature to automatically restore alerts on the system i.e. when the open zone that triggered an alarm is 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.

21.16 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 (SPCN320/SPCN340)

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.

21.17 Supported card readers and card formats

The following card readers and formats are supported on the SPC system:

Reader	Card Format
HD500-EM	IB41-EM
PR500-EM	IB42-EM
SP500-EM	IB44-EM
PM500-EM	IB45-EM
	ABR5100-BL
	ABR5100-TG
	ABR5100-PR
HD500-Cotag	IB928
PR500-Cotag	IB911
SP500-Cotag	IB968
PM500-Cotag	IB961
HF500-Cotag	IB958M

Reader	Card Format
PP500-Cotag	IB928 IB911 IB968 IB961 IB958M
PP500-EM	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
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 x 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. 9999999999999

21.18 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. For example, system with Ethernet as the primary path and GPRS as a backup path would be two separate ATPs of an ATS.

Acronym	EN50136-1 Description	FlexC Example
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 part of one or more ATPs.	Integrated onto SPC Panel using Ethernet, GPRS, PPP over PSTN.

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, for example, SIA, Contact ID.

21.19 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

Command Filter	Commands
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
	Get Holdup Data
	Edit Holdup Data
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
	Get User Status
	Clear All Alerts
	Get Unknown Cards

Command Filter	Commands
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
	Request an update of the FlexC Enc Key
Access Control Commands	Get the Configuration for a Door
	Read the Status for a Door
	Control a Door
	Get the Access Log

Command Filter	Commands
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
	Get a camera image
Virtual Keypad Commands	Control keypad
File Commands	Upgrade the Panel Firmware
	Upgrade Peripheral Firmware
	Upload Peripheral Firmware
	Upgrade PFW Progress
	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
	Reconfiguration Xbus
	Get the Area Configuration

21.20 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	-	-

		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)**
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

21.21 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.

Ethernet ATP Categories		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
Modem ATP Categories									
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	4 hr 10 min	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

22 Notes

Document ID: I-200572
Edition date: 18.09.2023