



**SPCS310**

**SPC Pro Programmier-Tool**

3.6

## Urheberrecht

Technische Spezifikationen und Verfügbarkeit können ohne vorherige Ankündigung geändert werden.

© Copyright Vanderbilt

Alle Rechte an diesem Dokument und dem darin behandelten Thema vorbehalten. Der Empfänger anerkennt diese Rechte und wird dieses Dokument nicht ohne unsere vorgängige schriftliche Ermächtigung ganz oder teilweise Dritten zugänglich machen oder außerhalb des Zweckes verwenden, zu dem es ihm übergeben worden ist.

Ausgabe: 01.10.2015

Dokument-ID: A6V10276928

# Inhalt

<b>1</b>	<b>Bedeutung der Symbole .....</b>	<b>8</b>
<b>2</b>	<b>Technische Daten.....</b>	<b>9</b>
<b>3</b>	<b>Softwarebeschreibung.....</b>	<b>10</b>
3.1	Betriebsarten .....	10
3.1.1	Offline-Modus.....	10
3.1.2	Online-Modus.....	10
3.2	Konnektivität.....	10
3.2.1	Ethernet-Schnittstelle .....	10
3.2.2	Direkt-USB .....	11
3.2.3	Direkt-Seriell .....	11
3.2.4	Modem .....	11
<b>4</b>	<b>Installation.....</b>	<b>13</b>
4.1	Neue SPC Pro-Software installieren .....	13
<b>5</b>	<b>Erste Schritte .....</b>	<b>14</b>
5.1	Anmelden .....	14
5.2	Installationen .....	15
5.2.1	Eine Installation hinzufügen .....	15
5.2.2	Konfigurieren einer Installation .....	17
5.2.3	Eine Installation kopieren.....	17
5.2.4	Eine Installation löschen .....	18
5.2.5	Installationsdetails bearbeiten .....	18
5.3	Konfigurationsfenster .....	18
5.3.1	Online-Statusinformationen .....	19
5.3.2	Symbolleiste.....	20
5.3.3	Programmmenüpunkte .....	21
<b>6</b>	<b>Programmierung - Übersicht.....</b>	<b>23</b>
6.1	Konfigurationsdateien.....	23
6.1.1	Speichern und Aufrufen in der Zentrale .....	23
6.1.2	Exportieren.....	23
6.1.3	Importieren.....	24
6.2	Konfigurationen offline programmieren .....	25
6.2.1	Speichern .....	26
6.2.2	Exportieren.....	26
6.3	Mit der Zentrale verbinden .....	26
6.3.1	Eine Verbindung in der Zentrale aktivieren.....	27
6.3.2	Eine Verbindung zur Zentrale herstellen .....	27
<b>7</b>	<b>Status der Zentrale.....</b>	<b>31</b>
7.1	Status .....	31
7.2	Meldegruppen .....	32
7.2.1	Quick Log - MG X .....	33
7.3	Bereiche .....	34

7.4	Systemalarme.....	35
7.5	X-BUS.....	36
	7.5.1 Netzteilstatus.....	39
7.6	Bedienteile.....	42
7.7	Türmodule.....	44
7.8	Türen.....	46
	7.8.1 Zutrittslogbuch – Tür X.....	47
7.9	Logbuch System.....	47
7.10	Logbuch der Zutrittskontrollfunktion.....	48
<b>8</b>	<b>Benutzer.....</b>	<b>51</b>
8.1	Hinzufügen/Bearbeiten von Benutzern.....	51
8.2	Hinzufügen/Bearbeiten von Profilen.....	55
8.3	Konfiguration von SMS.....	60
8.4	SMS-Befehle.....	62
8.5	Löschen von Web-Zugangscodes.....	64
8.6	Konfiguration der Technikereinstellungen.....	65
<b>9</b>	<b>Systemoptionen ändern.....</b>	<b>68</b>
9.1	Identifikation.....	68
9.2	Normen.....	69
	9.2.1 Installationstyp.....	70
9.3	Optionen.....	71
9.4	Timer.....	80
9.5	Uhrzeit.....	84
9.6	Sprache.....	85
9.7	SPC Pro / SPC Safe.....	86
9.8	SPC Manager.....	87
<b>10</b>	<b>Ein-/Ausgänge der Zentrale konfigurieren.....</b>	<b>89</b>
10.1	Ausgang bearbeiten.....	89
	10.1.1 MG-Einstellungen: Attribute.....	91
10.2	Bearbeiten eines Ausganges.....	92
	10.2.1 Ausgangstypen und Ausgangsschnittstellen.....	94
<b>11</b>	<b>Konfigurieren von Erweiterungen, Bedienteilen und Türsteuerungen.....</b>	<b>98</b>
11.1	Konfigurieren von Erweiterungen an einer SPC-Zentrale.....	98
11.2	Erweiterungen.....	99
	11.2.1 Hinzufügen und Konfigurieren von Erweiterungen.....	99
	11.2.1.1 Hinzufügen einer neuen Erweiterung.....	100
	11.2.1.2 Hinzufügen einer Erweiterung zur Konfigurationsdatenbank.....	101
	11.2.2 Konfigurieren einer Erweiterung.....	101
	11.2.2.1 Registerkarte PSU.....	105
	11.2.3 Konfigurieren eines Anzeigemoduls.....	106
	11.2.4 Konfigurieren eines Schlüsselschalter-Erweiterungsmoduls.....	108
	11.2.5 Erweiterungen neu zuweisen.....	110
	11.2.6 Bearbeiten der X-Bus-Einstellungen.....	111
11.3	Bedienteile.....	112
	11.3.1 Ein Bedienteil hinzufügen.....	112

	11.3.2	Bearbeiten eines Standard-Bedienteils .....	113
	11.3.3	Bearbeiten eines Komfort-Bedienteils .....	115
11.4		Türmodule .....	118
	11.4.1	Eine Türsteuerung hinzufügen.....	118
	11.4.2	Türsteuerung bearbeiten.....	119
<b>12</b>		<b>Funk.....</b>	<b>121</b>
12.1		Log - Funkmelder X.....	122
12.2		Nicht eingelernte Funkmelder .....	122
12.3		Konfiguration Funk ändern .....	122
12.4		Konfigurieren eines FÜ.....	124
	12.4.1	Hinzufügen eines FÜ .....	125
<b>13</b>		<b>Konfigurieren von Meldergruppen, Türen und Bereichen .....</b>	<b>127</b>
13.1		Meldergruppe bearbeiten .....	127
13.2		Bereich hinzufügen/bearbeiten .....	129
	13.2.1	Einbruch verzögert.....	131
	13.2.2	Intern-scharf-Optionen .....	132
	13.2.3	Verbundene Bereiche .....	133
	13.2.4	Plan .....	134
	13.2.5	Scharf-/Unscharfschalten.....	135
	13.2.6	Alles in Ordnung .....	139
	13.2.7	Übertragen .....	140
	13.2.8	Funk Ausgang.....	143
	13.2.9	Bereich gesteuert.....	143
	13.2.10	Kurzkonfigurationsprogramm für Tresor-/GAA-Bereiche.....	145
13.3		Bereichsgruppe hinzufügen.....	146
13.4		Tür bearbeiten .....	147
	13.4.1	Schleusenfunktion.....	152
<b>14</b>		<b>Kommunikation konfigurieren .....</b>	<b>155</b>
14.1		Serielle Schnittstellen .....	155
14.2		Modems.....	156
	14.2.1	SMS-Test .....	157
	14.2.2	SMS-Funktion .....	158
	14.2.3	SMS-Systemoptionen .....	158
	14.2.4	SMS-Befehle .....	158
	14.2.5	PSTN-Modem .....	160
	14.2.6	GSM-Modem.....	162
14.3		Empfänger (Alarm Reporting Centres, ARCs) .....	164
	14.3.1	Hinzufügen/Bearbeiten von Empfängern mithilfe von SIA oder CID	165
	14.3.2	Bearbeiten von Empfängerfiltern mithilfe von SIA oder CID.....	167
14.4		EDP-Einstellung .....	169
	14.4.1	Hinzufügen eines EDP-Empfängers .....	169
	14.4.2	Bearbeiten der Einstellungen des EDP-Empfängers.....	170
	14.4.3	Meldungsfiler-Einstellungen bearbeiten.....	175
	14.4.4	EDP-Einstellungen bearbeiten.....	176
14.5		"Fernwartung" .....	178
14.6		FlexC® .....	178

14.6.1	Schnellstart-ÜW-Konfiguration für EN50136 ATS .....	179
14.6.2	Konfigurieren eines EN50136-1-ATS oder kundenspezifischen ATS182	
14.6.2.1	ÜW zur FlexCom (AE).....	184
14.6.2.2	ÜW zu analogem Empfänger .....	189
14.6.2.3	Installationsdetails bearbeiten.....	191
14.6.3	Konfigurieren eines SPC-Connect-Übertragungssystems (ATS) .....	192
14.6.4	Konfigurieren von Ereignisprofilen .....	193
14.6.4.1	Ereignis Ausnahmendefinition .....	195
14.6.5	Konfigurieren von Steuerprofilen .....	198
<b>15</b>	<b>Kommunikationseinstellungen .....</b>	<b>201</b>
15.1	Ethernet .....	201
15.2	Konfigurieren der Netzwerkdienste der Zentrale .....	202
<b>16</b>	<b>Konfigurieren der erweiterten Einstellungen .....</b>	<b>204</b>
16.1	Cause & Effect.....	204
16.1.1	Einen Cause & Effect hinzufügen .....	205
16.1.2	Trigger erstellen/zuweisen .....	207
16.2	Kalender .....	209
16.2.1	Automatisches Scharf-/Unscharfschalten von Bereichen.....	210
16.2.2	Automatisches Scharf-/Unscharfschalten von anderen Funktionen der Zentrale .....	210
16.2.3	Kalender hinzufügen/bearbeiten .....	210
16.3	Trigger .....	212
16.4	Logische Ausgänge .....	215
16.5	X10 Konfiguration – Einstellungen .....	217
16.6	Konfiguration der Ausgänge für Systemverzögerung und automatische Scharfstellung.....	220
16.7	Logo-Konfiguration .....	221
16.8	Audio-Konfiguration .....	222
<b>17</b>	<b>Systemoptionen.....</b>	<b>225</b>
<b>18</b>	<b>Upgrade der Zentrale .....</b>	<b>226</b>
18.1	Upgrade Zentralen-Firmware .....	226
18.2	Upgrade der Peripherie-Firmware.....	227
18.3	Aktualisieren der SPC-Lizenzen.....	230
18.4	Import benutzerdefinierter Sprachen für die SPC Pro-Bedienoberfläche .....	231
<b>19</b>	<b>Bedienteil-Emulation aktivieren .....</b>	<b>234</b>
<b>20</b>	<b>Mit der Zentrale verbinden .....</b>	<b>236</b>
20.1	Ethernet-Schnittstelle .....	236
20.2	USB-Anschluss.....	237
20.3	Serielle Schnittstelle .....	238
20.4	PSTN-Modem .....	241
<b>21</b>	<b>Verwenden des Fast Programmer .....</b>	<b>245</b>
21.1	Installieren des Fast Programmer auf einem PC .....	245
21.2	Mit dem Fast Programmer verbinden.....	246
21.3	Importieren von Konfigurationsdateien aus dem Fast Programmer .....	248
21.4	Exportieren von Konfigurationsdateien zum Fast Programmer .....	249

21.5	Kopieren von Firmware- und Sprachdateien auf den Fast Programmer .....	250
<b>22</b>	<b>Audio/Video-Verifikation.....</b>	<b>253</b>
22.1	Konfigurieren von Video .....	253
22.1.1	Lese Kameraeinstellungen .....	254
22.1.2	Konfigurieren einer Kamera .....	255
22.2	Konfigurieren von Verifikationszonen.....	256
22.2.1	Testen des Audiosignals .....	258
22.2.1.1	Testen der Audiowiedergabe .....	258
22.2.1.2	Testen der Audioaufzeichnung .....	260
22.3	Konfigurieren der Verifikationseinstellungen.....	262
22.4	Anzeigen von Videobildern.....	262
<b>23</b>	<b>Körperschallmelder.....</b>	<b>264</b>
23.1	Testen der Körperschallmelder .....	267
23.1.1	Vorgang des manuellen und automatischen Tests .....	268
23.1.2	Automatisches Testen der Melder .....	268
23.1.3	Manueller Meldertest .....	269
<b>24</b>	<b>Anhang .....</b>	<b>271</b>
24.1	Netzwerk-Kabelverbindungen .....	271
24.2	Alarmempfangsstelle (Empfänger).....	271
24.3	EDP-Protokoll (Enhanced Datagram Protocol).....	272
24.4	Herstellen einer Fernverbindung zur Zentrale über GSM .....	274
24.5	Meldergruppentypen .....	278
24.6	MG-Attribute .....	281
24.7	Anwendbare Attribute nach Meldergruppentypen.....	284
24.8	FlexC-Glossar .....	285
24.9	FlexC-Steuerung .....	287
24.10	Zeiten für Übertragungssystemkategorien .....	289
24.11	ÜW Kategorie Zeiteinstellung.....	290

# 1 Bedeutung der Symbole

Im vorliegenden Dokument werden verschiedene Symbole verwendet:

Symbol	Beschreibung
	Nicht verfügbar für SPC42xx, SPC43xx.
	Nur bei SPC-Controller mit IP-Schnittstelle verfügbar (SPC43xx/SPC53xx/SPC63xx).
	Nicht verfügbar für Installationsart Privat.
	Nur verfügbar im uneingeschränkten Modus.
	Siehe Text für weitere Informationen zu Sicherheitsstufe, Region oder Modus.
	Siehe Anhang für weitere Informationen.

## 2 Technische Daten

Kommunikationsprotokoll	<ul style="list-style-type: none"><li>● Proprietär (über RS232, USB, TCP/IP im Ethernet, PSTN, GSM)</li><li>● Datenübertragung von/an SPC Fast Programmer</li></ul>
Systemkompatibilität	<ul style="list-style-type: none"><li>● Einzel-PC-Lösung</li><li>● Ausführung auf PCs mit Windows XP/Vista</li><li>● Vollständige Unterstützung von SPC42xx/SPC43xx/SPC52xx/SPC53xx/SPC63xx</li></ul>
Speicher	Min. 1 GB erforderlich
Datenbank	Dateien werden komprimiert lokal gespeichert.

## 3 Softwarebeschreibung

SPC Pro ist eine PC-basierte Softwareanwendung, die dem Benutzer die Möglichkeit gibt, SPC-Systeme zu vor Ort oder per Fernzugriff zu programmieren und zu konfigurieren. Alle Programmierfunktionen, die über die in SPC integrierte Browser-Oberfläche zugänglich sind, werden auch von SPC Pro zur Verfügung gestellt.

### 3.1 Betriebsarten

SPC Pro ermöglicht dem Benutzer, mehrere Installationsprofile zu erstellen. Jedes Profil besteht aus dem Namen der Installation, ihrer ID und Einzelheiten zur Verbindung, die nacheinander auf der Installationsseite von SPC Pro aufgeführt sind.

Nachdem ein Installationsprofil erstellt wurde, kann es im Konfigurationsmodus konfiguriert werden. Im Konfigurationsmodus können alle Programmfunktionen (Meldergruppen, Ausgänge, Timer usw.) nach Bedarf konfiguriert und gespeichert werden.

#### 3.1.1 Offline-Modus

Sie können neue Installationsprofile erstellen und vorhandene Profile bearbeiten oder löschen, ohne mit einer Installation verbunden zu sein. In diesem Modus kann jede Installation offline konfiguriert werden, und die Konfiguration kann später heruntergeladen werden, wenn sie gebraucht wird.

Wenn SPC Pro nicht mit einer Zentrale verbunden ist, wird das Symbol  in der Symbolleiste [→ 20] angezeigt.

Am oberen Rand jedes Programmierfensters wird der Text **offline** eingeblendet, um Sie daran zu erinnern, dass Sie noch nicht mit einem Installationsstandort verbunden sind. Alle Schaltflächen zum Aktualisieren des Status sind im Offline-Modus deaktiviert.

#### 3.1.2 Online-Modus

Wenn Sie den Konfigurationsmodus für eine vorhandene Installation aufrufen, wird die Option eingeblendet, sich mit einer Zentrale zu verbinden. In diesem Modus wird eine direkte Verbindung aufgebaut, die Ihnen ermöglicht, alle Programmfunktionen der gewählten Installation zu lesen und zu konfigurieren.

Wenn SPC Pro mit einer Zentrale verbunden ist, wird das Symbol  in der Symbolleiste [→ 20] angezeigt.

Am oberen Rand jedes Programmierfensters wird der Text **online** eingeblendet, um Sie daran zu erinnern, dass Sie mit einem Installationsstandort verbunden sind. Schaltflächen für Aktualisierung und Programmierung (wie Meldergruppe abschalten, sperren usw.) werden aktiviert, wenn Sie online sind.

### 3.2 Konnektivität

SPC Pro kann sich über folgende Schnittstellen mit der Zentrale SPC verbinden.

#### 3.2.1 Ethernet-Schnittstelle

IP

Ihr PC muss mit einer Ethernet-Netzwerkkarte ausgestattet sein, über die er lokal über ein LAN (Local Area Network), per Fernzugang über WAN (Wide Area Network) oder über ein Kreuzkabel direkt an den Ethernet-Port der Zentrale angeschlossen ist.

Einzelheiten zum Anschließen an die Zentrale über eine IP-Verbindung finden Sie auf Seite [→ 236].

### 3.2.2 Direkt-USB

Eine direkte Verbindung mit der Zentrale über einen USB-Port Ihres PC wird unterstützt. Der SPC USB-Treiber muss auf Ihrem PC installiert sein. Diese Treiber sind auf der SPC-CD enthalten.

Einzelheiten zum Anschließen an die Zentrale über eine USB-Verbindung finden Sie auf Seite [→ 237].

### 3.2.3 Direkt-Seriell

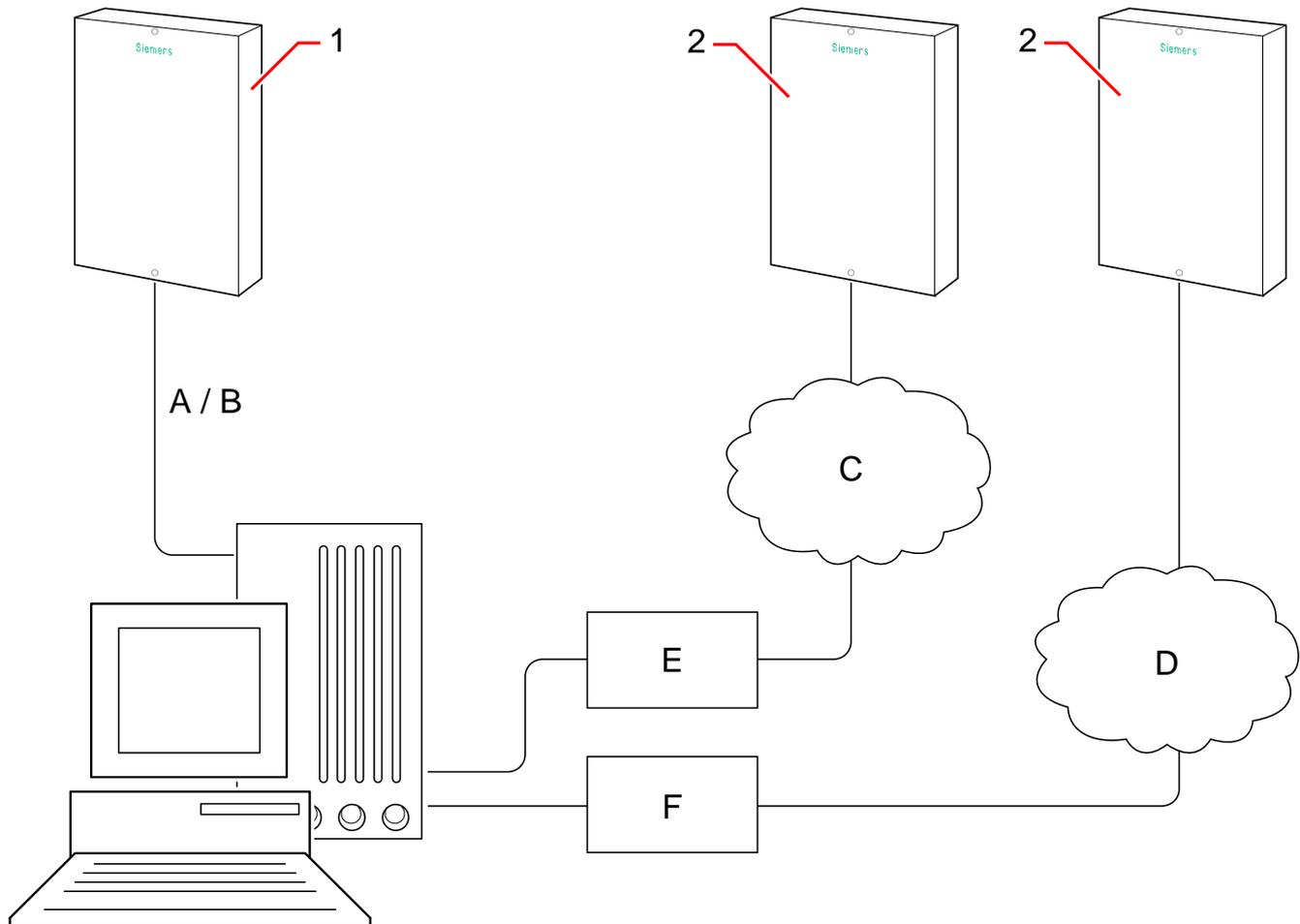
Eine direkte Verbindung von einem seriellen Port an Ihrem PC zur Zentrale wird von SPC Pro unterstützt.

Einzelheiten zum Anschließen an die Zentrale über eine serielle Verbindung finden Sie auf Seite [→ 238].

### 3.2.4 Modem

Eine Fernverbindung zur Zentrale über ein Festnetz- oder GSM-Modem wird ebenfalls unterstützt. Ihr PC muss mit einem funktionsfähigen PSTN/GSM-Modem ausgestattet sein, damit die Verbindung hergestellt werden kann. Um eine Verbindung über das Festnetz (PSTN) herstellen zu können, muss das Modem an die Telefonleitung angeschlossen sein. Am entfernten Standort muss auch die Zentrale mit einem Festnetz- oder GSM-Modem ausgestattet sein, das so konfiguriert ist, dass es eingehende Anrufe annimmt.

Einzelheiten zur Verbindung mit der Zentrale von einem entfernten Standort finden Sie auf Seite [→ 241].



1	Lokale SPC-Konnektivität
A	Ethernet
B	USB
2	Entfernte SPC-Konnektivität
C	IP-Netzwerk
D	PSTN/GSM-Netz
E	Router
F	Modem

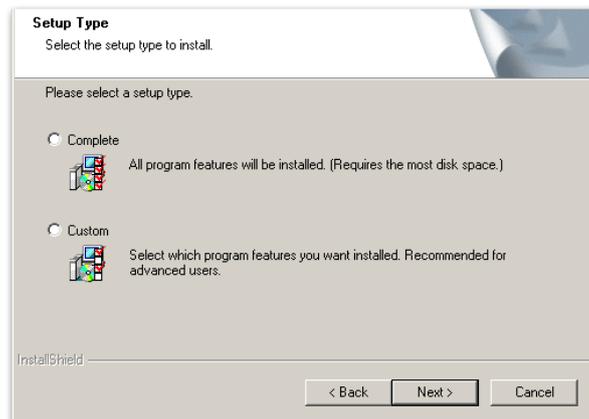
## 4 Installation

### 4.1 Neue SPC Pro-Software installieren

	 <b>WARNUNG</b>
	Bevor Sie die neueste Version von SPC Pro installieren, müssen Sie ältere Versionen zunächst deinstallieren.

Die neuesten Versionen des Konfigurationsprogramms für SPC Pro befinden sich auf der SPC-Support-CD, die zusammen mit der Zentrale geliefert wird.

1. Klicken Sie auf **setup.exe**.  
 ⇒ Der Setup-Assistent wird angezeigt.
2. Klicken Sie auf **Weiter**.
3. Geben Sie einen Benutzernamen und einen Firmennamen ein.
4. Klicken Sie auf **Weiter**.  
 ⇒ Das folgende Fenster wird angezeigt:



5. Wählen Sie den Installationstypen aus.
6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Installieren**.  
 ⇒ SPC Pro wird installiert.
8. Klicken Sie auf **Fertig stellen**.

	 <b>WARNUNG</b>
	Wenn Sie die SPC-Fernwartung unter Windows 7 (32-Bit- und 64-Bit-Version) oder Windows Vista verwenden, dürfen SPC Pro und -Fernwartung nicht im Ordner <i>Programme</i> bzw. <i>Programme (x86)</i> gespeichert werden.

## 5 Erste Schritte

### 5.1 Anmelden

1. Klicken Sie im Windows-Menü Programme auf das Symbol SPC Pro.

⇒ Das folgende Fenster wird angezeigt:



2. Klicken Sie auf die entsprechende Flagge, um die Sprache zu ändern.



Durch die Auswahl einer Flagge wird nur die in der Anwendung verwendete Sprache geändert. Informationen zum Wechseln der Sprache von Bedienteilen, Web-Schnittstelle und Logbuch finden Sie auf Seite [→ 85]. Beachten Sie, dass bei Änderung der Systemsprache von SPC Pro die Sprache für das Logbuch erst aktualisiert wird, nachdem die Verbindung zur Zentrale getrennt und anschließend wiederhergestellt wurde.

3. Geben Sie das werksseitig eingestellte Passwort (1111) in das Feld **Passwort** ein.

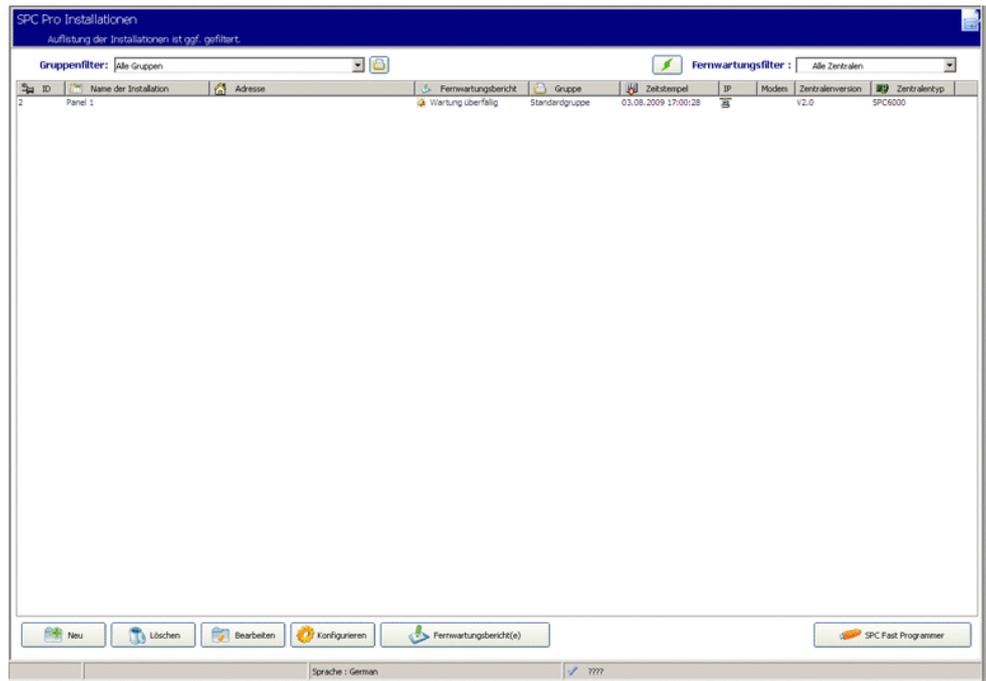


Das Kennwort zum Anmelden am Programm steht in keinem Zusammenhang mit dem Kennwort zum Verbinden mit der Zentrale (siehe Seite).

4. Klicken Sie auf die Schaltfläche **Anmelden**.

⇒ Daraufhin erscheint das folgende Fenster.

⇒ In dem Fenster werden die Installationsprofile aufgelistet, die im System erstellt wurden.



ID	Mit dieser Nummer wird die Installation eindeutig identifiziert (1–999999).
Installationsname	Der Name der Installation.
Adresse	Die Adresse der Installation.
Zentralentyp	Der Typ der Zentrale.
Gruppe	Jede Installation kann in unterschiedliche Gruppen eingeordnet sein, so dass der Benutzer Installationsstandorte mühelos nach Kunden unterscheiden kann.
Zeitstempel	Der letzte Zeitpunkt, zu dem die Anlage mit SPC Pro konfiguriert wurde.
IP	Die IP-Adresse der Installation.
Modem	Das Modem, das der Installation zugewiesen ist.
Zentralversion	Zeigt die Firmware-Version der Zentrale an.



Wenn diese Seite zum ersten Mal aufgerufen wird, ist die Liste leer, und Sie müssen ein Installationsprofil erstellen, um fortfahren zu können (siehe Seite [→ 15]).

## 5.2 Installationen

### 5.2.1 Eine Installation hinzufügen



In der Zentrale muss in der Techniker-Programmierung eine SPC Pro-Verbindung aktiviert sein, bevor eine Verbindung hergestellt werden kann (siehe Seite [→ 27]).

1. Klicken Sie auf **Neu**.  
⇒ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.
3. Klicken Sie auf **OK**.

Auflistung der Installationen

### Installationsdetails

Details für diese Installation eingeben...

SPC Pro ID :  Muss eindeutige ID sein (1-999999)

Installationsname:

Installationsadresse:

Zentralentyp:

Zentralenversion :

\*Region :

\*Grade :

Gruppe:

IP-Adresse:  IP-Port :

Telefonnummer 1:

Telefonnummer 2:

Passwort :

SPC Pro ID	Geben Sie für jede Installation eine eindeutige Nummer ein. Mit dieser Nummer wird die Installation eindeutig identifiziert (1-999999). <b>Hinweis:</b> Diese Nummer stimmt nicht mit der <b>Installations-ID</b> überein, die unter Panel Status\Summary (Zentralenstatus/Übersicht) angezeigt wird und die Zentrale eindeutig identifiziert.
Installationsname	Geben Sie einen Installationsnamen ein, bevor Sie die Installation im System speichern.
Installationsadresse (optional)	Geben Sie eine Adresse ein, die Ihnen dabei hilft, einzelne Standorte zu identifizieren.
Zentralentyp	Wählen Sie aus der Dropdown-Liste einen Zentralentyp.
Zentralenversion	Wählen Sie aus der Dropdown-Liste die Firmware-Version aus.
Region	Wählen Sie aus der Dropdown-Liste die Region aus.
Sicherheitsgrad	Wählen Sie aus der Dropdown-Liste den Grade (Sicherheitsgrad) aus.
Gruppe	Jede Installation kann in unterschiedliche Gruppen eingeordnet sein, so dass der Benutzer Installationsstandorte mühelos nach Kunden unterscheiden kann.
IP-Adresse <input type="text" value="IP"/>	Geben Sie eine IP-Adresse für die Installation ein.
IP-Port <input type="text" value="IP"/>	Geben Sie einen IP-Port für die Installation ein.

Telefonnummer 1	Geben Sie eine Telefonnummer ein, die zur PSTN- oder GSM-Nummer gehört, die dem Primär-Modem der SPC-Zentrale zugewiesen ist. SPC Pro wird versuchen, diese Nummer anzurufen, wenn von einem entfernten Standort über ein Modem eine Verbindung hergestellt werden soll. Wenn diese Verbindung nicht zustande kommt, wird Telefonnummer 2 gewählt.
Telefonnummer 2	Geben Sie eine Telefonnummer ein, die zu der PSTN- oder GSM-Nummer gehört, die dem Backup-Modem der -Zentrale zugewiesen ist. SPC Pro wird diese Nummer nur wählen, wenn zur Telefonnummer 1 keine Verbindung hergestellt werden kann.
Kennwort	Geben Sie ein Passwort ein, mit dem die Verbindung zur Zentrale ermöglicht wird. <b>Hinweis:</b> Dieses Passwort muss dem SPC Pro-Passwort entsprechen, das in der Zentrale programmiert ist.

## Zeitstempel

Neben den grundlegenden Installationsparametern wird ein Feld Zeitstempel angezeigt.

ID	Name der Installation	Adresse	Zentralentyp	Gruppe	Zeitstempel	IP	Modem	Zentralenversion
2	Installation2	Address 2	SPC6300	Standardgruppe	-			V3.2
3	Installation3	Address 3	SPC5300	Standardgruppe	-			V3.1
4	Installation4	Address 4	SPC6300	Standardgruppe	06/02/2013 15:59:48			V3.4

In diesem Feld wird Folgendes angezeigt:

- Der letzte Zeitpunkt, zu dem eine Konfiguration in eine Zentrale herauf- oder aus einer Zentrale heruntergeladen wurde.
- Der letzte Zeitpunkt, zu dem eine Installationskonfiguration lokal auf dem PC gespeichert wurde.

Zeitstempelfelder, die leer sind (-), weisen darauf hin, dass diese Installationen dem System hinzugefügt wurden, ohne konfiguriert oder an eine Zentrale gesendet worden zu sein (d. h. nur die grundlegenden Angaben für die Standortinitialisierung wurden konfiguriert und gespeichert).



Obwohl SPC Pro gestattet, eine große Anzahl von Installationen (1–999999) hinzuzufügen, können Sie sich jeweils immer nur mit einer Installation verbinden. Jeder Versuch, sich gleichzeitig mit mehr als einer Konfiguration zu verbinden, wird zurückgewiesen.

## 5.2.2 Konfigurieren einer Installation

1. Klicken Sie auf eine Installation in der Liste.
2. Klicken Sie auf die Schaltfläche **Konfigurieren**.  
⇒ Es erscheint das Konfigurationsfenster [→ 18].

## 5.2.3 Eine Installation kopieren

Installationsprofile können kopiert und bearbeitet werden, um ein neues Profil zu erstellen. Dies ist eine komfortable Methode zum Erstellen einer Reihe von ähnlichen Profilen.

1. Klicken Sie auf ein vorhandenes Profil.

2. Klicken Sie im Dropdown-Menü mit der rechten Maustaste auf **Neue Installation kopieren/erstellen**.
- ⇒ Es wird das Fenster **Installationsdetails** angezeigt, in dem Änderungen vorgenommen werden können.

## 5.2.4 Eine Installation löschen



Es empfiehlt sich, die Einzelheiten einer Installation, die Sie löschen zu notieren. Wenn eine Installation aus SPC

Pro gelöscht wurde, können Informationen für diese Installation nicht mehr aufgerufen werden.

Wenn Sie eine Installation löschen, wird auch die ID-Nummer für diese Installation gelöscht. Diese Nummer kann dann wieder für eine neue Installation verwendet werden.

1. Klicken Sie auf eine Installation in der Liste.
  2. Klicken Sie auf die Schaltfläche **Löschen**.
- ⇒ Daraufhin erscheint folgende Meldung:



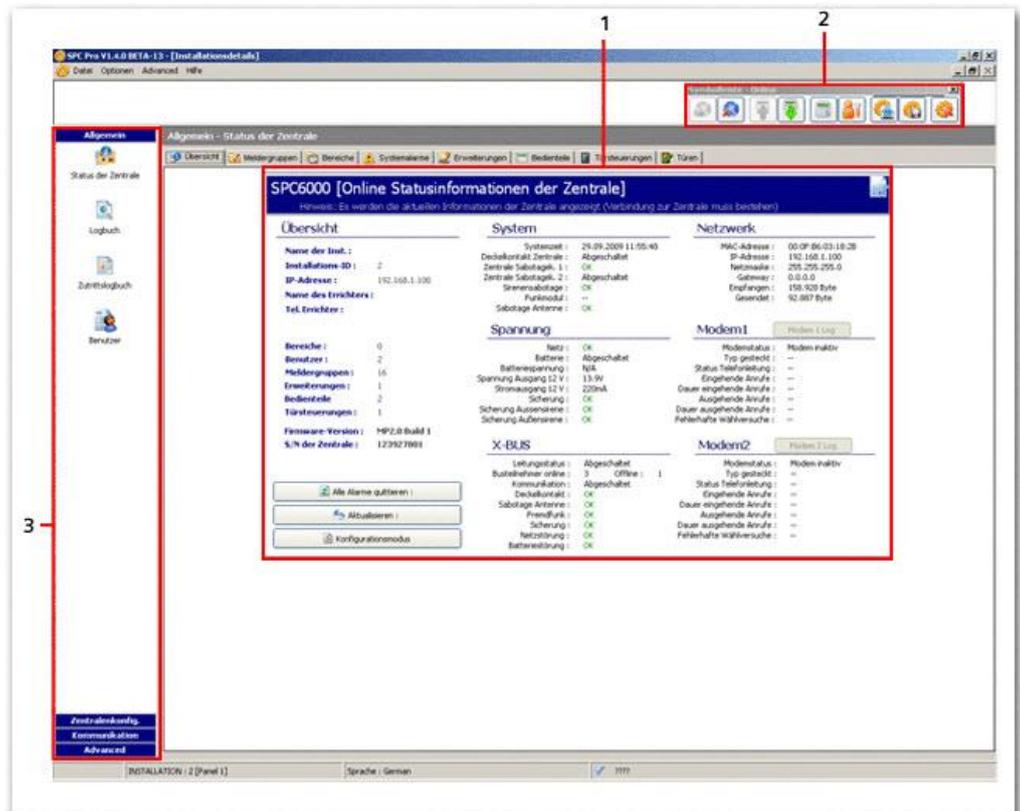
3. Klicken Sie auf **Ja**.
- ⇒ Die Installation wird gelöscht.

## 5.2.5 Installationsdetails bearbeiten

1. Klicken Sie auf eine Installation in der Liste.
  2. Klicken Sie auf die Schaltfläche **Bearbeiten**.
- ⇒ Das Fenster **Installationsdetails bearbeiten** wird angezeigt. Das Fenster **Installationsdetails bearbeiten** ist mit dem neuen Fenster **Installationsdetails** identisch. Die Einstellungen **Region** und **Grade** können für eine bestehenden Installation in SPC Pro jedoch nicht bearbeitet werden.
3. Geben Sie die neuen Daten ein.
  4. Klicken Sie auf **Installationsdetails speichern**.

## 5.3 Konfigurationsfenster

Wenn eine Installation zu SPC Pro hinzugefügt wurde, kann sie in folgendem Fenster nach Bedarf konfiguriert werden:



9.7

1	Aktuelle Statusinformationen (nur wenn SPC Pro mit der Zentrale verbunden ist).
2	Symbolleiste
3	Programmenüpunkte

### 5.3.1 Online-Statusinformationen

Systemübersicht	Übersicht über Sabotageeingänge, Funkeingänge und Zeit.
Energieversorgung	Übersicht über die elektrischen Parameter der Zentrale (Spannung, Strom) und den Status der Sicherungen (Hilfseingänge und Sirenen).
X-BUS	Übersicht über den X-BUS-Status und Online-Erweiterungen.
Ethernet	Übersicht über die Ethernet-Parameter der Zentrale.
Modem 1	Übersicht über die Modemparameter von Modem 1 (primärer Steckplatz).
Modem 2	Übersicht über die Modemparameter von Modem 2 (Backup-Steckplatz).

## 5.3.2 Symbolleiste



Schaltfläche	Funktion	Beschreibung
	Verbinde zu Zentrale	Diese Schaltfläche wird angezeigt wenn SPC Pro offline ist. Um SPC mit der Zentrale zu verbinden, klicken Sie auf diese Schaltfläche. Es erscheint das Fenster <b>Wähle Kommunikationspfad</b> und fordert dazu auf, einen der Kommunikationsmodi zu wählen, die für diese Installation programmiert wurden (IP, USB, seriell, Modem 1, Modem2).
	Trenne Verbindung zur Zentrale	Diese Schaltfläche wird angezeigt, wenn SPC Pro online ist (bereits mit einer Zentrale verbunden). Um SPC von der Zentrale zu trennen, klicken Sie auf diese Schaltfläche. SPC Pro fordert Sie auf zu bestätigen, dass Sie die Verbindung zur Zentrale trennen wollen. Klicken Sie auf die Schaltfläche Ja, um die Verbindung zu trennen.
	Sende Konfiguration zur Zentrale	Klicken Sie auf diese Schaltfläche, um die aktuelle Konfiguration an die Zentrale zu senden. Alle programmierten Einstellungen werden an die Zentrale übertragen. Stellen Sie sicher, dass Sie die Installation korrekt konfiguriert haben, bevor Sie auf diese Schaltfläche klicken. Diese Funktion steht nur im Konfigurationsmodus zur Verfügung.
	Konfiguration der Zentrale anfordern	Klicken Sie auf diese Schaltfläche, um die Konfigurationsdatei der Zentrale in Ihre Konfigurationsdatei zu laden. Alle programmierten Einstellungen werden in Ihre Konfigurationsdatei geladen. Konfigurationsdaten, die sich von der Konfiguration der Zentrale unterscheiden, werden überschrieben.
	Bedienteil - Emulation	Klicken Sie auf diese Schaltfläche um ein virtuelles SPC-Bedienteil auf Ihrem PC zu aktivieren. Dieses Bedienteil verhält sich genau so, als würden Sie ein reales Bedienteil betätigen. Es ermöglicht Ihnen, Informationen im Bedienteil-Display anzuzeigen und den Techniker- oder Benutzer-Programmiermodus aufzurufen, indem Sie auf die Tasten des Bedienteils klicken (siehe Seite [→ 234]).
	Wartungs- oder Konfigurationsmodus auswählen	Klicken Sie auf diese Schaltfläche, um zwischen Wartungs- und Konfigurationsmodus umzuschalten. Im Konfigurationsmodus werden alle Alarmer und Berichtsfunktionen deaktiviert. <b>Hinweis:</b> Wenn die standardmäßige PIN 1111 für beispielsweise eine neue SPC-Installation aktiviert ist, müssen Sie die Techniker-PIN an der Zentrale ändern. Wenn Sie Ihre PIN nicht ändern, erhalten Sie eine Informationsmeldung, in der Sie aufgefordert werden, Ihre voreingestellte PIN zu ändern, bevor Sie sich aus dem Konfigurationsmodus abmelden. Der „Wartungsmodus“ bietet einen geringeren Funktionsumfang und wird für den Betrieb des Systems verwendet. Im Wartungsmodus sind jedoch Scharfschalten und Testen des Systems möglich. Alle Alarmer bleiben aktiviert. <b>Hinweis:</b> Ist die Option „Konfig.mod.verlassen“ unter „Systemoptionen“ aktiviert, darf der Techniker den

Schaltfläche	Funktion	Beschreibung
		Konfigurationsmodus bei aktiven Alarmen verlassen, muss aber alle Alarme quittieren, bevor er vom Konfigurationsmodus in den Wartungsmodus wechselt.
	Speichern der Konfiguration	Klicken Sie auf diese Schaltfläche, um die von Ihnen programmierte Konfiguration zu speichern.
	Konfiguration beenden	Klicken Sie auf diese Schaltfläche, um den Konfigurationsmodus zu verlassen. Wenn Sie Ihre Änderungen vor dem Verlassen speichern möchten, klicken Sie auf <b>Konfiguration speichern</b> .

### 5.3.3 Programmmenüpunkte

Allgemein	Zentralenkonfig.	Kommunikation	Erweitert
 Status	 Systemoptionen	 Ser. Schnittstellen	 Cause & Effect
 Logbuch System	 Ein- & Ausgänge der Zentrale	 Modems	 Kalender
 Zutrittslogbuch	 Busteilnehmer	 Empfängereinstellungen	 Trigger
 Benutzer	 Alle MG	 EDP-Einstellungen	 Logische Ausgänge
	 Funk	 SPC Pro/SPC Safe*	 X-10
	 Alle Türen	 Fernwartungseinstellungen	 Erweiterte Ausgänge
	 Bereiche	 CEI-ABI	 Logo-Konfiguration
		 Netzwerk	 Audio-Konfiguration

Allgemein	Zentralenkonfig.	Kommunikation	Erweitert
			 Verifikation

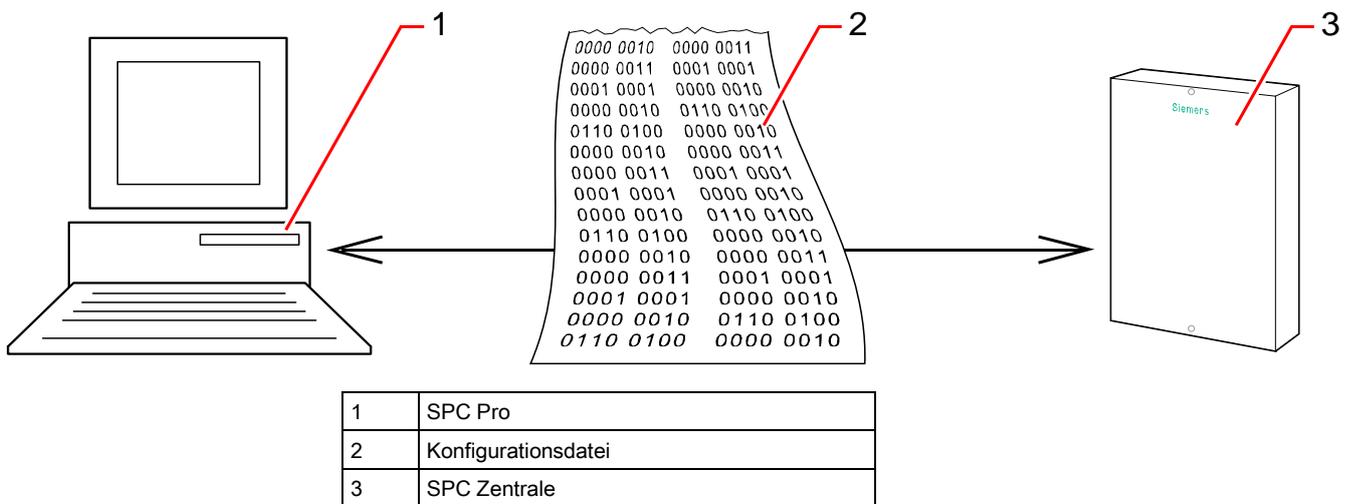
\* Siehe SPC-Fernwartungs- und SPC Safe-Konfigurationshandbuch.

## 6 Programmierung - Übersicht

### 6.1 Konfigurationsdateien

#### 6.1.1 Speichern und Aufrufen in der Zentrale

Programmierte Daten werden zwischen SPC Pro und der Zentrale über eine Konfigurationsdatei ausgetauscht. Wenn Sie eine Konfigurationsdatei herauf- oder herunterladen, werden ALLE Konfigurationsdaten an die Zentrale gesendet bzw. von ihr empfangen. Sie sollten daher sämtliche Konfigurationsdaten (nicht nur die, die Sie gerade eingesehen haben) überprüfen, bevor Sie eine Datei an die Zentrale senden.



Jede Konfigurationsdatei wird mit einem Zeit- und Datumsstempel gespeichert. Wenn SPC Pro sich mit der Zentrale verbindet, wird eine Überprüfung durchgeführt, um festzustellen, ob Ihre Konfigurationsdatei auf dem PC denselben Zeit- und Datumsstempel hat wie die Konfigurationsdatei in der Zentrale. Siehe Seite [→ 225].

Wenn Zeit- und Datumstempel der Konfigurationsdatei übereinstimmen, sind die Konfigurationsdaten in SPC Pro und der Zentrale identisch (siehe Hinweis weiter unten). Wenn die Zeit- und Datumstempel unterschiedlich sind, wird eine Warnung angezeigt, um Sie zu informieren, dass Ihre lokalen Konfigurationsdaten nicht mit der Konfiguration der Zentrale übereinstimmen.

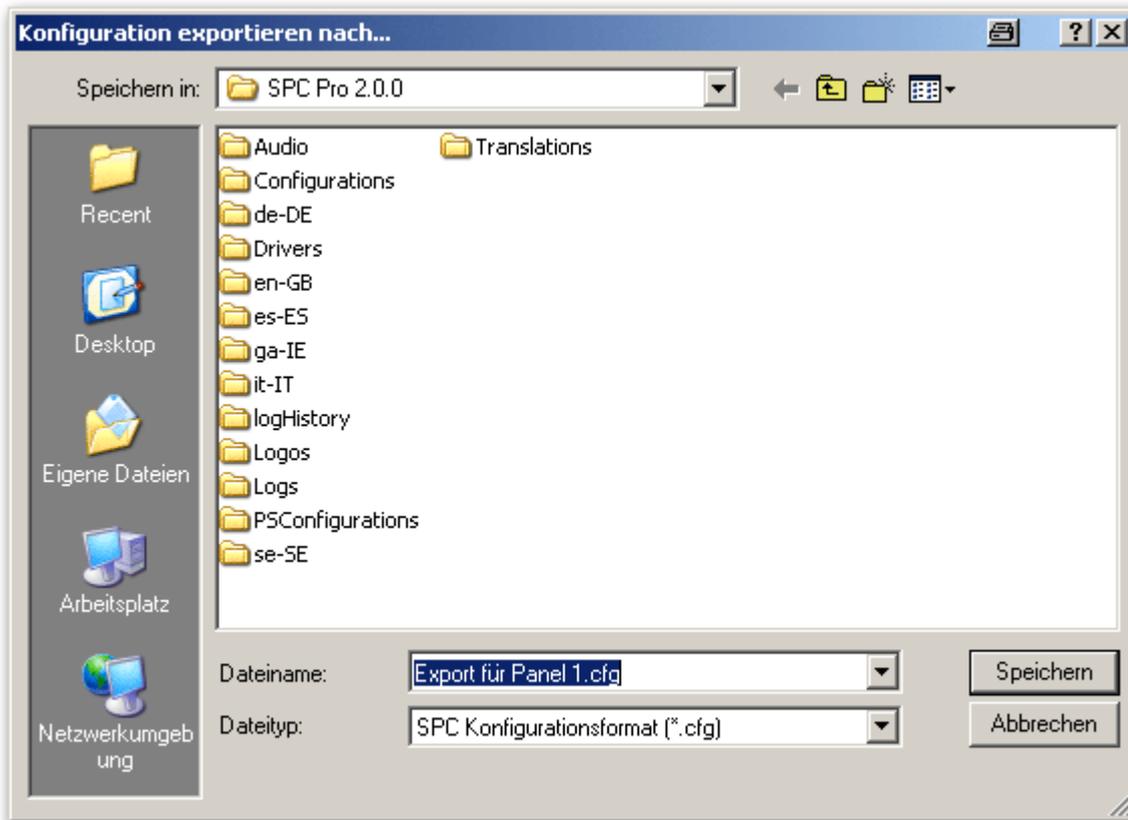


Wenn Sie die Konfigurationseinstellungen von der Zentrale heraufladen und in die Datei auf Ihrem PC speichern (ohne Änderungen vorzunehmen), wird der Zeit- und Datumsstempel geändert. Sie erhalten einen entsprechenden Warnhinweis, wenn Sie versuchen, dieselbe unveränderte Konfigurationsdatei wieder in die Zentrale zurückzuspeichern.

#### 6.1.2 Exportieren

Eine SPC-Konfigurationsdatei (.cfg) enthält alle Konfigurationsinformationen einer Zentrale in einem portierbaren Format, das gespeichert und an eine E-Mail angehängt oder zum Bearbeiten oder Herunterladen wieder in SPC Pro importiert werden kann. Der in der Zentrale integrierte Browser und der Fast Programmer speichern Konfigurationsinformationen in diesem Format und rufen sie in diesem Format wieder auf.

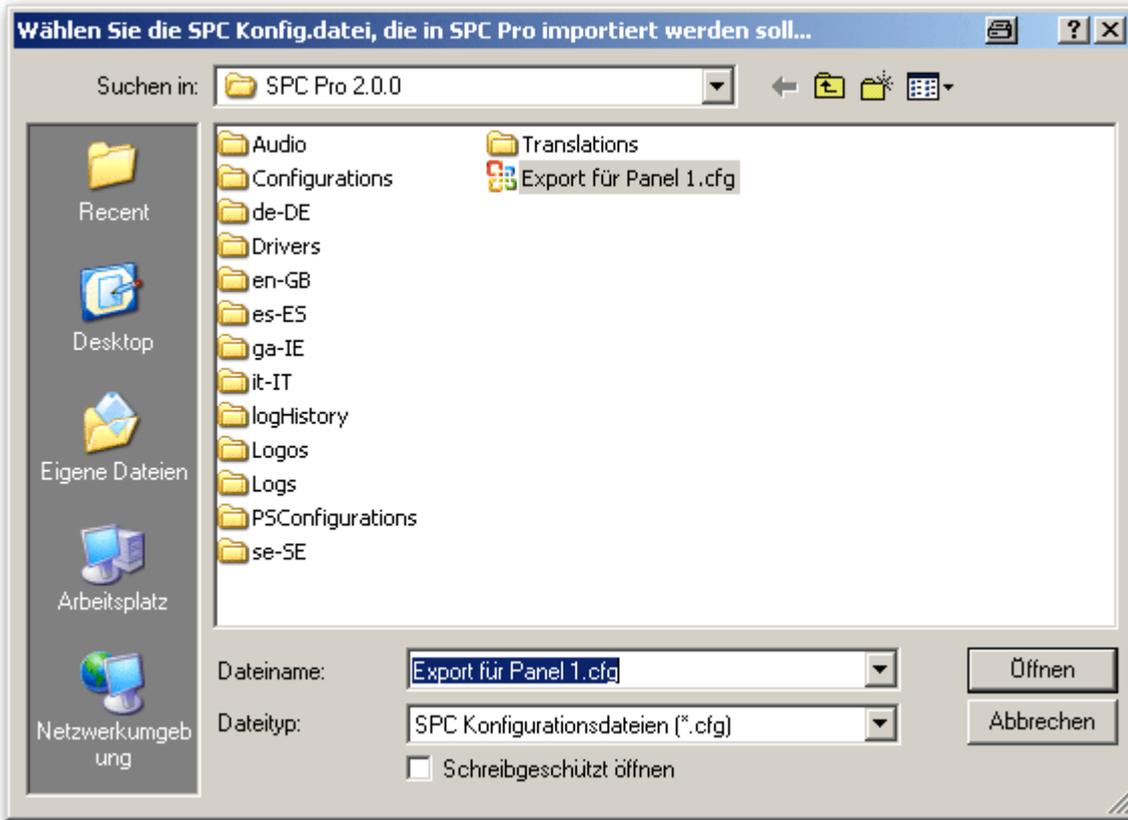
1. Öffnen Sie das Fenster SPC Pro-Installationen.
2. Markieren Sie die Installation, die Sie exportieren wollen.
3. Klicken Sie mit der rechten Maustaste.
4. Wählen Sie **Konfiguration auf Festplatte exportieren**.  
⇒ Daraufhin erscheint das folgende Fenster:



5. Geben Sie den Dateinamen ein.
6. Klicken Sie auf **Speichern**.

### 6.1.3 Importieren

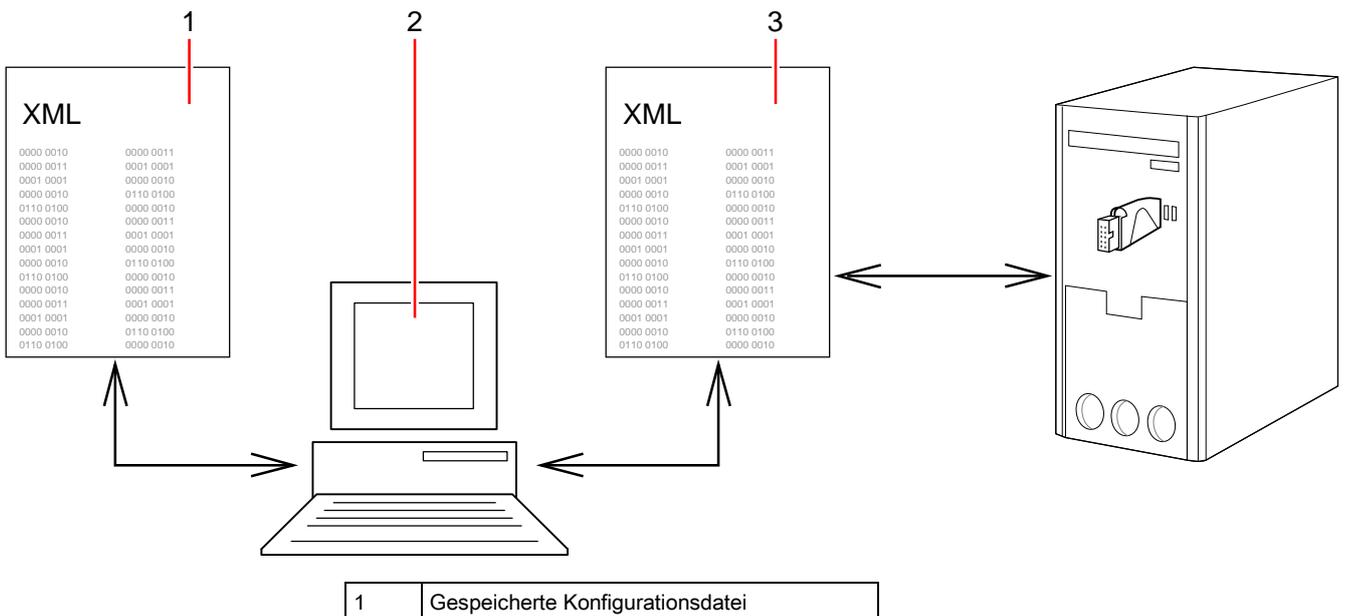
1. Öffnen Sie das Fenster SPC Pro-Installationen.
2. Wählen Sie die Option **Datei > Installation von Festplatte importieren**.  
⇒ Daraufhin erscheint das folgende Fenster:



3. Wählen Sie die .cfg-Datei.
4. Klicken Sie auf **Öffnen**.

## 6.2 Konfigurationen offline programmieren

SPC Pro bietet dem Benutzer die Möglichkeit, Konfigurationsdateien zu erstellen, zu bearbeiten und zu speichern, ohne dass eine Verbindung zu einer SPC-Zentrale besteht. In diesem Modus können Sie eine Installation erstellen und nach Bedarf konfigurieren und diese Konfiguration speichern, bis eine Verbindung zu einer Installation erforderlich wird.



2	SPC Pro
3	Exportierte Konfigurationsdatei

### 6.2.1 Speichern



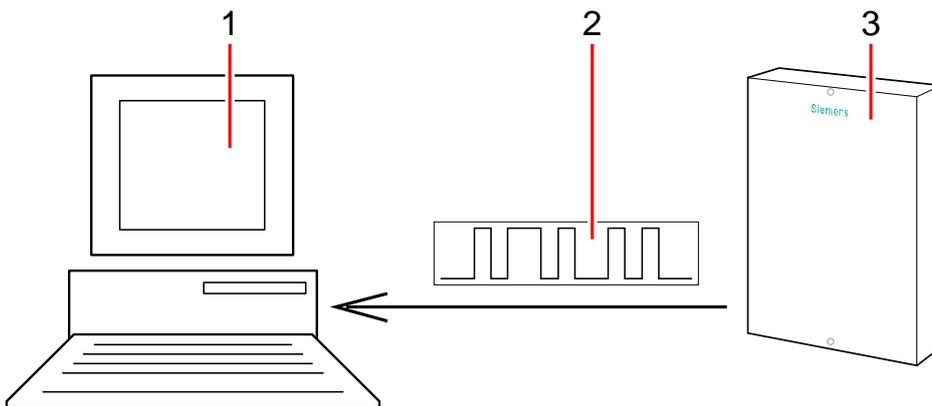
- Klicken Sie auf die Schaltfläche **Speichern der Konfiguration** in der Symbolleiste.
- ⇒ Die Datei wird lokal auf Ihrer Festplatte gespeichert und wird automatisch geladen, wenn Sie die Konfiguration mit SPC Pro aufrufen.

### 6.2.2 Exportieren

Installationskonfigurationen können in einem portierbaren Format für die Verwendung von Fast Programmer-Geräten oder zum E-Mail-Versand an entfernte Standorte exportiert werden.

Diese .config-Dateien können unter einem frei wählbaren Namen direkt auf Ihrer Festplatte gespeichert werden, so dass sie sich mühelos wieder aufrufen lassen. Um diese Dateien in SPC Pro zu laden, verwenden Sie die Option Konfiguration importieren.

## 6.3 Mit der Zentrale verbinden



1	SPC Pro
2	Statusinformationen
3	SPC-Zentrale

1. Verbinden Sie sich mit der gewünschten Installation.
2. Wählen Sie in SPC Pro die lokale Konfiguration der Installation.
3. Rufen Sie den Konfigurationsmodus auf.
4. Verbinden Sie die Zentrale über eine der möglichen Verbindungsarten (siehe Seite [→ 10]).

Wenn die Verbindung zur Zentrale hergestellt wurde, werden von der Zentrale folgende Statusinformationen an SPC Pro gesendet:

- Zentralenversion
- Zeit- und Datumsstempel der Konfigurationsdatei
- Hardware-Informationen: Modemstatus, Status des Funkempfängers, Stromversorgung, Sabotageeingänge des Systems

- X-BUS-Status
- Ethernet-Status
- Systemalarm-Status
- MG-Status
- Bereichsstatus
- Türstatus

Diese Statusinformationen vermitteln dem Benutzer einen Überblick über die wesentlichen Konfigurationsdaten der Zentrale, ohne dass die vollständige Konfiguration aus der Zentrale heraufgeladen werden muss.



SPC Pro lässt keine Verbindung zu einer Zentrale mit einer Firmware-Version zu, die nicht mit dem Programm kompatibel ist. Sie müssen sicherstellen, dass Sie über die richtige Firmware-Release von SPC verfügen.

### 6.3.1 Eine Verbindung in der Zentrale aktivieren

Um eine SPC Pro-Verbindung zu einer Zentrale zu aktivieren, müssen Sie die Zentrale so konfigurieren, dass sie eine Verbindung akzeptiert:

1. Rufen Sie über ein an die Zentrale angeschlossenes Bedienteil den Konfigurationsmodus auf.
2. Rufen Sie den **Konfigurationsmodus** auf.
3. Wählen Sie **Utilities** (Dienstprogramme).
4. Wählen Sie **SPC Pro**.
5. Wählen Sie **Enable SPC PRO** (SPC Pro aktivieren).
6. Wählen Sie **Enabled** (Aktiv).
7. Wählen Sie **Engineer Access** (Technikerzugang).
8. Wählen Sie **Enabled** (Aktiv).
9. Wählen Sie **Passwort**.
10. Geben Sie das Passwort ein, das für eine Verbindung benötigt wird (Standard-Passwort: password).

### 6.3.2 Eine Verbindung zur Zentrale herstellen

1. Klicken Sie in der Symbolleiste auf das Symbol .  
⇒ Daraufhin erscheint das folgende Fenster:



Es werden nur die Verbindungsmodi angezeigt, die für diese Installation programmiert wurden, als sie hinzugefügt oder bearbeitet wurde. Siehe Seite [→ 15].

2. Wählen Sie den gewünschten Verbindungsmodus.
3. Klicken Sie auf **Verbinden**.

### Firmware-Version

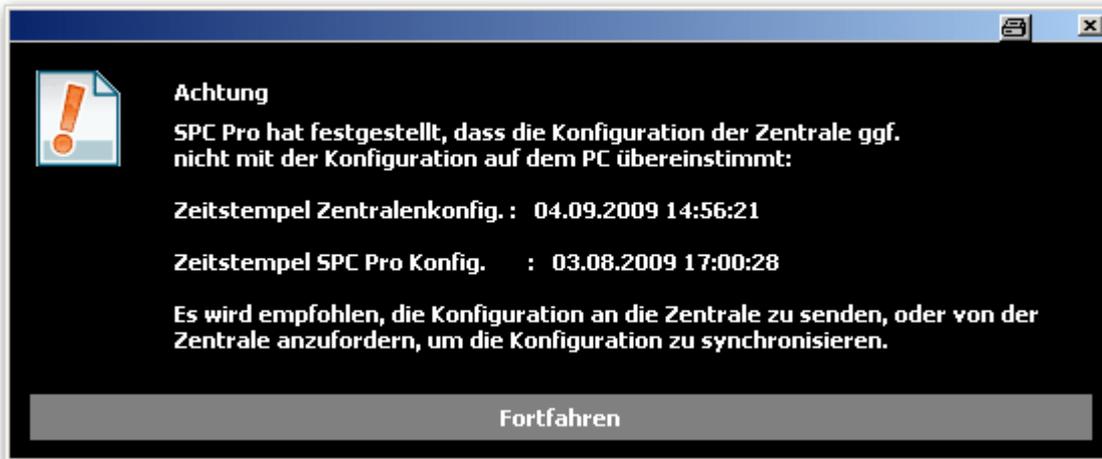
SPC Pro liest nach dem Verbinden mit der Anlage die Statusinformationen und zeigt eine Warnung an, wenn die erkannte Firmware-Version in der Zentrale nicht von SPC Pro unterstützt wird.



Wenn die Firmware-Version der Zentrale von SPC Pro nicht unterstützt wird, setzen Sie sich bitte mit Vanderbilt in Verbindung, um das jüngste Firmware-Upgrade für die Zentrale zu erhalten, indem Sie die Nummer Ihrer Version von X Pro angeben.

### Synchronisation der Konfigurationsdatei

Wenn die in der Zentrale erkannten Konfigurationsinformationen nicht den in SPC Pro programmierten Konfigurationsinformationen entsprechen, wird folgendes Fenster angezeigt:



Bevor Sie Konfigurationsdaten senden oder empfangen können, müssen Sie die Konfigurationsdatei auf Ihrem PC mit der Konfigurationsdatei in der Zentrale konfigurieren. Dies geschieht, indem Sie die eine Datei mit der anderen überschreiben.



Vanderbilt empfiehlt, die Konfigurationsdatei aus der Zentrale zu laden, BEVOR Sie Änderungen der Konfiguration an die Zentrale senden. Hierdurch wird sichergestellt, dass Sie mit einer exakten Kopie der aktuellen Installationskonfiguration arbeiten, BEVOR Sie Änderungen an der Konfiguration vornehmen.

Die Konfigurationsdateien von PC und Zentrale synchronisieren:

1. Klicken Sie auf die Schaltfläche **Continue** (Weiter).
2. Klicken Sie auf folgende Optionen:
  - Konfiguration der Zentrale anfordern: Die Konfiguration der Zentrale wird von der Zentrale auf den Computer hochgeladen.
  - Send Config file to panel (Konfigurationsdatei an Zentrale senden): Die Konfiguration zur Zentrale wird auf die Zentrale heruntergeladen.

### Konfiguration der Zentrale anfordern



Alle Konfigurationsänderungen, die über ein Bedienteil vor Ort vorgenommen werden, während eine Verbindung mit SPC Pro besteht, werden überschrieben, wenn Sie Ihre Konfigurationsdatei an die Zentrale senden.

Wenn Sie die Konfiguration nicht von der Zentrale heraufgeladen haben, empfiehlt es sich, dies noch zu tun. Sie können dann Ihre Konfigurationsänderungen in den heruntergeladenen Informationen programmieren. Wenn Sie alle Änderungen eingegeben haben, können Sie sie an die Zentrale senden. Nur die Konfigurationseinstellungen, die Sie geändert haben, werden auch in der Zentrale geändert.

---

## Konfiguration zur Zentrale senden

---



Sie können auch Ihre Konfigurationsdatei an die Zentrale senden, ohne Konfigurationsdaten von der Zentrale zu laden. In diesem Fall sollten Sie jedoch umfassende und präzise Kenntnisse zur Konfiguration der Zentrale haben, bevor Sie Ihre Konfigurationsdatei senden. SPC Pro lässt nicht zu, dass Sie Konfigurationsinformationen für eine Erweiterung an die Zentrale senden, die nicht der Konfiguration der Erweiterung an der Zentrale entsprechen. Siehe Seite [→ 98].

---

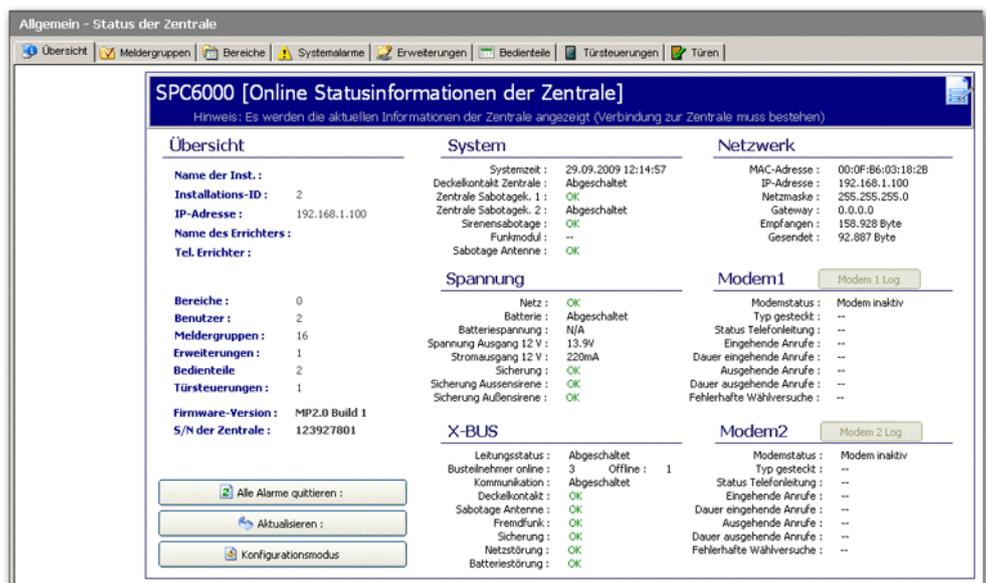
# 7 Status der Zentrale

## 7.1 Status

Diese Seite zeigt den Status und eine Übersicht der SPC-Hauptkomponenten einschließlich System, Stromversorgung, X-BUS und Kommunikation.



1. Klicken Sie auf die Registerkarte **Übersicht**.
2. Siehe die nachfolgende Tabelle für weitere Informationen.



Offline\Online Statusinformationen der Zentrale	Zeigt die Parameter an, die für die Installation programmiert wurden, als sie eingerichtet wurde (Installationsname, ID usw.). Diese Daten werden von den Daten der Zentrale aktualisiert, wenn Sie eine Verbindung mit der Zentrale herstellen. Die Firmware-Version und die S/N-Felder der Zentrale werden ebenfalls angezeigt, sobald eine Verbindung zur Zentrale hergestellt wurde.
---	--

### Ausführbare Aktionen

Die nachstehenden Aktionen können nur dann ausgeführt werden, wenn eine Verbindung aufgebaut wurde.

Alle Alarme quittieren	Quittiert alle aktiven Alarme auf der Zentrale. Die betreffenden Alarmmeldungen werden als roter Text gegenüber dem betreffenden Element angezeigt.
Aktualisieren	Aktualisiert alle Änderungen des Zentralenstatus. Sie müssen das Statusfenster aktualisieren, um den zum jeweiligen Zeitpunkt aktuellen Zentralenstatus anzuzeigen.
Konfiguration / Wartung	Zum Umschalten zwischen Konfigurations- und Wartungsmodus. Im Konfigurationsmodus werden alle Alarme deaktiviert, und es werden alle Meldungen an einen Empfänger unterdrückt.

## 7.2 Meldegruppen

Informationen zur Konfiguration finden Sie auf Seite [→ 127].

Allgemein



Status der  
Zentrale

1. Klicken Sie auf die Registerkarte **Meldergruppen**.
2. Siehe die nachfolgende Tabelle für weitere Informationen.

Online Übersicht Meldergruppen

Autom. Aktualisieren der Statusanzeige

ID	MG	Beschreibung	Bereich	MG-Typ	Phys....	Status
1		Front door	1 -	Einbruch verzögert	Geschlossen	OK
2		Sitting room	1 -	Einbruch	Geschlossen	OK
3		Kitchen	1 -	Einbruch	Geschlossen	OK
4		Upstairs front	1 -	Einbruch	Geschlossen	OK
5		Upstairs rear	1 -	Einbruch	Geschlossen	OK
6		PIR Hallway	1 -	Einbruch	Geschlossen	OK
7		PIR Landing	1 -	Einbruch	Geschlossen	OK
8		Panic button	1 -	Überfall	Geschlossen	OK
9			1 -	Einbruch	Geschlossen	OK
10			1 -	Einbruch	Geschlossen	OK
11			1 -	Einbruch	Geschlossen	OK
12			1 -	Einbruch	Geschlossen	OK
13			1 -	Einbruch	Geschlossen	OK
14			1 -	Einbruch	Geschlossen	OK
15			1 -	Einbruch	Geschlossen	OK
16			1 -	Einbruch	Geschlossen	OK

Filter MG:

Autom Aktualisieren der Statusanzeige	Aktivieren Sie dieses Kontrollkästchen, um die automatische Aktualisierung der MG-Übersicht zu aktivieren. Dies ist nur für alle MGs möglich, nicht für Filter-MGs.
MG-Beschreibung	Textbeschreibung der MG (max. 16 Zeichen).
Bereich	Bereiche, denen diese Meldergruppe zugewiesen ist.
MG Typ	Typ der Meldergruppe (Einbruch, Verzögert usw.).
EOL Wert	<p>Zeit den EOL-Wert für den Widerstandsbereich des Meldergruppenzustands an. Mögliche Werte sind:</p> <ul style="list-style-type: none"> <li>● Gut – Nomineller Wert +/- 25 % des definierten Bereichs</li> <li>● OK – Nomineller Wert +/- 50 % des definierten Bereichs</li> <li>● Schwach – Nomineller Wert +/- 75 % des definierten Bereichs</li> <li>● Ungenügend — jeder andere Wert</li> <li>● Laut – zeigt ein Problem bei der Signalerkennung an. Das Kabel könnte sich in der Nähe eines Hauptkabels oder einer anderen Interferenzquelle befinden.</li> </ul> <p>Diese Spalte ist nur im Techniker-Modus sichtbar. Weitere Informationen zu nominellen Widerstandswerten und deren definierte Bereiche finden Sie unter Verdrahtung Linieneingänge.</p>
Eingang	Der erkannte Eingabestatus dieser MG (Unbekannt, Offen, Geschlossen, Leitungsbruch, Kurzschluss, Impuls, Erschütterung, Abgedeckt, Störung, Ausserhalb d. Gr, Meldergruppen instabil schärfen, Fremdspannung, Laut).

	<p>Fremdspannung ist ein Eingabe-Sabotagealarm. Bei einem Fremdspannungsaustausch wird eine regelmäßige Überprüfung ausgeführt, um sicherzustellen, dass keine externen Spannungen an diesen Schaltkreis angelegt werden.</p> <p>Instabil: Ein instabiler Zustand tritt ein, wenn der Widerstandswert der Linieneingänge über einen definierten Probenzeitraum instabil ist.</p> <p>Laut: Ein lauter Zustand tritt ein, wenn während eines definierten Messintervalls eine externe Interferenz in den Eingangsschaltkreis induziert wird.</p> <p>Im Aus: Ein Im-Aus-Zustand tritt ein, wenn der Widerstandswert am Meldergruppeneingang nicht innerhalb der akzeptierten Toleranzen der aktuellen EOL-Werte liegt.</p>
Status	<p>Der programmierte Status einer MG. Der Statuswert Normal bedeutet, dass die MG für den normalen Betrieb programmiert ist. Nachstehend finden Sie eine vollständige Liste der möglichen Werte:</p> <p>Abschaltung, Dauertest, Sperrung, Sabotage, Alarm, Notausgang, Warnung Fehler, Bedrohung Fehler, Störung, Störung Telefonleitung, Überfall, Bedrohung, Technik, Medizin, Sperren, Feuer, Melder abgedeckt, Normal, Actuated (Ausgelöst), Nachalarm. Eine MG befindet sich im Nachalarmstatus, wenn ein Alarm eingetreten ist und eine Zeitüberschreitung des bestätigten Alarms vorliegt. Dadurch wird die MG neu gestartet, und es wird eine Kennzeichnung gesetzt, dass der Alarm aufgetreten ist.</p>

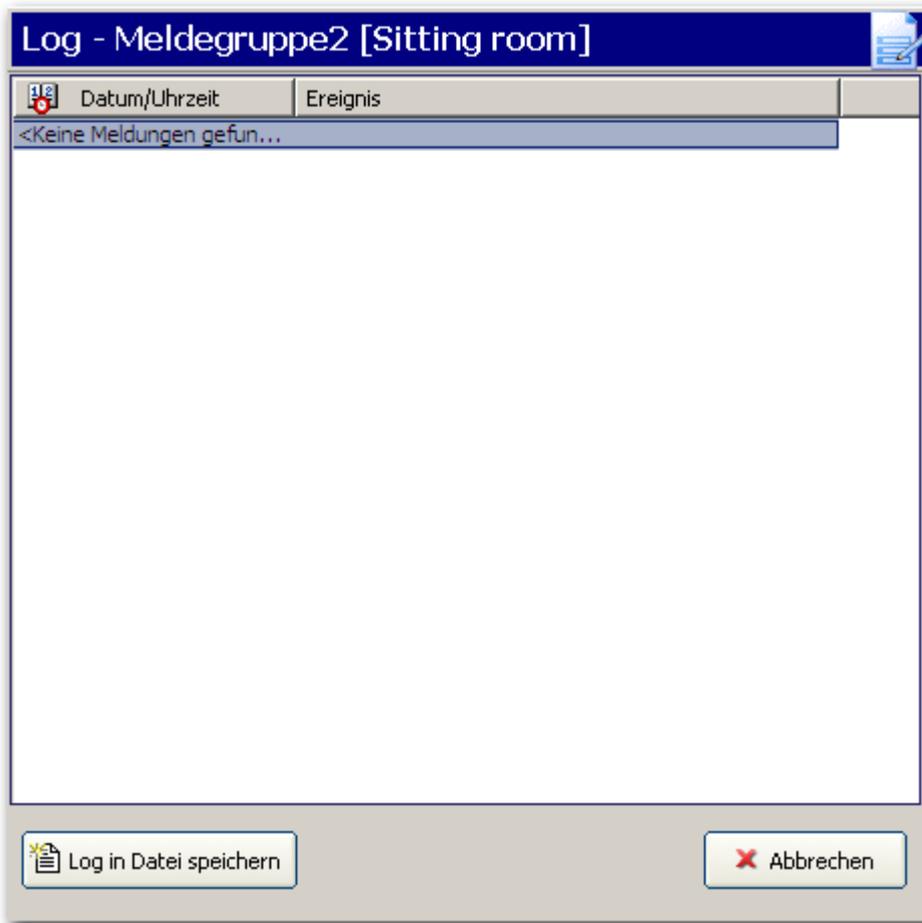
### Ausführbare Aktionen

MG aktualisieren	Aktualisiert die für die Zentrale angezeigten Statusinformationen.
Log (Protokoll)	Markieren Sie eine Meldergruppe (MG) und klicken Sie auf die Schaltfläche „Log“, um ein Protokoll des Eingangsstatus dieser MG anzuzeigen.. [→ 33]
Sperrung 	Klicken Sie auf diese Schaltfläche, um eine Störung oder eine offene Meldergruppe zu sperren. Durch das Sperren werden der Fehler oder die Meldergruppe nur für einen Scharfschaltungszeitraum gesperrt. Sperren steht bei Sicherheitsgrad 3 nach EN 50131 nicht zur Verfügung.
Alarmer quittieren	Klicken Sie auf diese Schaltfläche, um den Alarmzustand der Zentrale zu quittieren.
Abschalten	MG-Beschreibung. Nach Abschalten einer Meldergruppe bleibt diese solange deaktiviert, bis sie wieder explizit eingeschaltet wird. Es empfiehlt sich, beim Abschalten von Meldergruppen sehr vorsichtig vorzugehen, da diese Meldergruppen nicht aktiv sind, wenn das System SCHARFGESCHALTET wird.
Dauertest	Markieren Sie eine MG, und klicken Sie auf diese Schaltfläche, um mit dieser MG einen Dauertest auszuführen.
Körperschallmelder-Test	Klicken Sie auf diese Schaltfläche, um den ausgewählten Körperschallmelder zu testen. Weitere Informationen über Körperschallmelder finden Sie unter Körperschallmelder [→ 264].
Geschl Eingänge nicht anzeigen	Klicken Sie auf diese Schaltfläche, um alle geschlossenen Eingänge zu verbergen.
Filter-MG	Wählen Sie einen Meldergruppen -Typ aus dem Dropdown-Menü. Es wird nur die Übersicht für den gewählten Meldergruppen-Typ angezeigt.

## 7.2.1 Quick Log - MG X

Anzeigen eines Quick-Logs des Eingangsstatus einer Meldergruppe:

1. Markieren Sie die Meldergruppe.
  2. Klicken Sie auf die Schaltfläche **Log**.
- ⇒ Daraufhin erscheint das folgende Fenster:



Das neueste Ereignis wird am unteren Ende der Liste angezeigt.

## 7.3 Bereiche

Hier wird jeder im System angelegte Bereich mit seinem jeweiligen Status angezeigt.

Informationen zur Konfiguration finden Sie auf Seite [→ 129].

Allgemein



Status der  
Zentrale

1. Klicken Sie auf die Registerkarte **Bereiche**.  
⇒ Daraufhin erscheint das folgende Fenster.
2. Weitere Informationen finden Sie in der nachstehenden Tabelle.
3. Klicken sie auf **Aktualisieren**.

**Online Übersicht Bereiche**

Bereich	Beschreibung	Modus
1		Unscharf

Bereich	Bereichsnummer
Beschreibung	Textbeschreibung des Bereichs (max. 16 Zeichen).
Modus	Aktueller Aktivierungsmodus des Bereichs.

Den Zustand des Bereichs ändern:

1. Klicken Sie auf die Schaltfläche  auf die Schaltfläche **Wartungsmodus** in der Symbolleiste.
2. Wählen Sie einen Bereich aus der Liste.
3. Wählen Sie einen Modus für diesen Bereich per Klick auf die gewünschte Schaltfläche (Unscharf, Internscharf A, Internscharf B, Externscharf).

## 7.4 Systemalarme

**Allgemein**



Status der  
Zentrale

1. Klicken Sie auf die Registerkarte **Systemalarme**.
2. Siehe die nachfolgende Tabelle für weitere Informationen.

**Online Übersicht Systemalarme**

Alarm	Phy. Eingang	Status
Zentrale Netz	OK	OK
Zentrale Batterie	Störung	Abgeschaltet
Zentrale Sicherung Ausgang 12 V	OK	OK
Zentrale Sicherung Außensirene	OK	OK
Zentrale Sicherung Innensirene	OK	OK
Zentrale Sabotage Sirene	OK	OK
Zentrale Deckelkontakt	Störung	Abgeschaltet
Zentrale Sabotagek. 1	OK	OK
Zentrale Sabotagek. 2	Störung	Abgeschaltet
Zentrale Sabotage Antenne	OK	OK
Zentrale Fremdfunk	OK	OK
X-BUS Leitungsbruch	Störung	Abgeschaltet
Übertragungsstörung	OK	OK
Bedrohungspin	OK	OK
Überfall Fernbedienung	OK	OK
User Man Down Transmitter Alarm	OK	OK

Alarm	Beschreibung des Systemalarms.
Eingang	Der aktuelle Status des Alarms, der auf der Zentrale erkannt wurde (OK, Störung).
Status ⚠	Der programmierte Status des Systemalarms, d. h. ob der Alarm abgeschaltet oder gesperrt ist. Der Statuswert OK wird angezeigt, wenn die Alarmbedingung in keiner Weise deaktiviert wurde (siehe Seite).

**Ausführbare Aktionen**

Aktualisieren	Klicken Sie auf diese Schaltfläche, um den Status der Systemalarme zu aktualisieren.
Alarme quittieren	Klicken Sie auf diese Schaltfläche, um ALLE Alarme auf der Zentrale wiederherzustellen.
Sperren ⚠	Klicken Sie auf diese Schaltfläche, um eine Störungsbedingung zu sperren. Durch das Sperren werden der Fehler oder die Meldergruppe nur für einen Scharfschaltungszeitraum gesperrt. Die Funktion Sperren steht bei Sicherheitsgrad 3 nach EN 50131 nicht zur Verfügung.
Abschaltung	Klicken Sie auf diese Schaltfläche, um diese Meldergruppe abzuschalten. Durch Abschalten einer Meldergruppe wird diese solange deaktiviert, bis sie wieder explizit eingeschaltet wird. Es empfiehlt sich, beim Abschalten von Meldergruppen sehr vorsichtig vorzugehen, da diese Meldergruppen nicht aktiv sind, wenn das System SCHARFGESCHALTET wird.

## 7.5 X-BUS

**Allgemein**

 Status der  
 Zentrale

1. Klicken Sie auf das Register X-BUS.
2. Siehe die nachfolgende Tabelle für weitere Informationen.

Online Übersicht Erweiterungen

Erw.-ID	Beschreibung	Leitungsplan	Typ	Firmware	Komm.	Status	Ni
1	XBus 2 - Position 2	Erweiterung [8 Eingang / 2...		1.06.06MAY08	Online	OK	Ni

Leitungsbruch : zwischen [Zentrale - X-BUS 1] und [Zentrale - X-BUS 2]

Aktualisieren Leitungsplan

Erweiterungs-ID	Mit dieser ID wird die Erweiterung eindeutig gekennzeichnet.
Beschreibung	Beschreibungstext für die Erweiterung. Dieser Text erscheint auch im Browser und im Bedienteil.
Leitungsplan	Die Reihenfolge, in der das System die Erweiterungen am X-BUS erkennt.
Typ	Der Typ der erkannten Erweiterung (I/O, Netzteil, Bedienteil usw.).
Firmware-Version	Die Firmware-Version der Erweiterung.
Komm.	Der Status der Erweiterung (online oder offline).
Status	Der Status der Erweiterung (OK, Störung).
Netzteil	Typ und Version des Netzteils, soweit installiert.
Funk	Modell des Funkmoduls, soweit installiert

### Ausführbare Aktionen

Aktualisieren	Klicken Sie auf die Schaltfläche, um den Status von X-BUS zu aktualisieren.
Leitungsplan	Klicken Sie auf die Schaltfläche, um eine Liste von Erweiterungen/Bedienteilen zu erhalten, die physisch an die Zentrale angeschlossen sind.



Beim ersten Verbinden mit der Zentrale werden diese Informationen angezeigt und vermitteln Ihnen einen umfassenden Überblick über die X-BUS-Konfiguration, ohne dass Sie die Konfigurationsdatei von der Zentrale hochladen müssen. Diese Informationen sind besonders hilfreich, wenn Sie Erweiterungen an der Zentrale hinzufügen möchten. Siehe Seite [→ 98].

### Status Erweiterung

Um den Online-Status einer Erweiterung einzusehen, die mit dem X-BUS verbunden ist:

1. Klicken Sie auf eine Erweiterung in der Liste.
2. Siehe die nachfolgende Tabelle für weitere Informationen.

**Status Erweiterung**  
 Statusinformationen Erweiterung



**Erweiterungs-ID :** 1 Zeige NT Status  
**Typ :** Erweiterung [8 Eingang / 2 Ausgang]  
**S/N :** 9428901  
**Firmware-Version :** 1.10 Build32  
**Spannung :** 14.4V  
**Batteriespannung :** N/A  
**Strom :** 0mA  
**Funktyp :** Nicht gesteckt  
**Funkversion :** --  
**Lesertyp :** Nicht gesteckt

	Input	Status
Kommunikation	OK	OK
Deckelkontakt	OK	OK
Störung Sicherung	OK	OK
Netz	OK	OK
Batterie	OK	OK
Netzteil	OK	OK
PSU Ausgang Tamper	OK	OK
PSU Spannung zu niedrig	OK	OK

Alarmer quittieren
Sperren
Abschalten

Schließen

Kommunikation	Der physische Status (OK, Störung) und der programmierte Status (OK, ausgeschaltet, gesperrt) der X-BUS-Kabelverbindung zur Erweiterung.
Sabotage Deckelkontakt	Der physische und der programmierte Status des Sabotageschalters (Deckelkontakt) am Gehäuse des Erweiterungsmoduls.
Störung Sicherung	Der physische und der programmierte Status der Erweiterungssicherung.
Netz	Physischer und programmierter Status der Stromversorgung der Erweiterung.
Batterie	Physischer und programmierter Status der Batterie.
Netzteil	Physischer und programmierter Status des verbundenen Netzteils. Um weitere Informationen zum Status des Netzteils anzuzeigen, klicken Sie auf <b>Zeige NT Status</b> . (Siehe Netzteilstatus)

### Ausführbare Aktionen

Alarmer quittieren	Klicken Sie auf die Schaltfläche, um ALLE Alarmer auf der Zentrale zu quittieren.
Sperren 	Klicken Sie auf diese Schaltfläche, um eine Störungsbedingung zu sperren. Durch das Sperren werden der Fehler oder die Meldergruppe nur für einen Scharfschaltungszeitraum gesperrt. Die Funktion Sperren steht bei Sicherheitsgrad 3 nach EN 50131 nicht zur Verfügung.

Abschalten	Klicken Sie auf diese Schaltfläche, um diese Meldergruppe abzuschalten. Durch Abschalten einer Meldergruppe wird diese solange deaktiviert, bis sie wieder explizit eingeschaltet wird. Es empfiehlt sich, beim Abschalten von Meldergruppen sehr vorsichtig vorzugehen, da diese Meldergruppen nicht aktiv sind, wenn das System SCHARFGESCHALTET wird.
------------	--



Die Daten zum Erweiterungsstatus hängen von der Art der gewählten Erweiterung ab, d. h. das dargestellte Fenster zeigt den physischen und den programmierten Status einer Reihe von Parametern für eine Erweiterung an.

## 7.5.1 Netzteilstatus

Das Fenster **Status Netzteil** zeigt Informationen über den aktuellen Status des Netzteils und seine Ausgänge sowie den jeweiligen Status angeschlossener Batterien an.

Die folgenden Netzteiltypen werden unterstützt:

- SPCP332/333 Smart-Netzteil (als Smart-Netzteil bezeichnet)
- SPCP355 Smart-Netzteil

### Smart-Netzteilstatus

Die folgende Abbildung zeigt den Smart PSU-Status an:

**Status Netzteil**  
Status for PSU connected to Enetnode

 **Typ :** Typ1  
**Version :** V4  
**Mains :** OK  
**Batterie Link :** 7 Ah Batterie  
**Status Batterie :** OK  
**Batteriespannung :** 13.3V  
**Strom [Batterie] :** 0mA

	Spannung	Strom	Sicherung
<b>Ausgang 1</b>	13.7V	390mA	OK
<b>Ausgang 2</b>	13.7V	0mA	OK
<b>Ausgang 3</b>	13.7V	26mA	N/A

Geschlossen

Name	Beschreibung
Typ	Der Typ des Netzteils.
Version	Die Version des Netzteils.
Netz-Status	Zeigt den Zustand der Netzverbindung an. Mögliche Werte sind: Störung oder OK
Batterie Link	Zeigt den Typ der angeschlossenen Batterie an.
Status Batterie	Zeigt den Zustand der Batterieverbindung an. Mögliche Werte sind: Störung oder OK
Batteriespannung	Zeigt die gemessene Batteriespannung an.
Batterie Strom	Zeigt den Strom der Batterie an.
Ausgänge	Zeigt die Spannung an den Ausgängen, den Stromverbrauch der Ausgänge und den Status der Sicherung an den Ausgängen an.

### Status SPCP355 Smart PSU

Die folgende Abbildung zeigt den SPCP355-Netzteilstatus an:

## Status Netzteil

Status for PSU connected to Enetnode

**Typ :** Typ2  
**Version :** V2  
**Mains :** OK  
**Temperatur :** 23 Grad (C)  
**Ladespannung :** 14.4V  
**Ladestrom :** 18mA  
**Aufladestatus :** Vollständig geladen  
**Hauptstromkreis :** OK  
**Aufladestromkreis :** OK

**Batterie**

	Strom	Voltage	Current
<b>Batterie 1 :</b>	OK	13.6V	19mA
<b>Batterie 2 :</b>	OK	13.6V	36mA

**Ausgänge**

	Spannung	Sicherung	Sabotage
<b>Netzteil</b>	OK	OK	
<b>Netzteil</b>	OK	OK	OK
<b>Netzteil</b>	OK	OK	OK
<b>Netzteil</b>	OK	OK	OK
<b>NFAusgang :</b>	OK	OK	
<b>Netzteil</b>	OK		

Geschlossen

Name	Beschreibung
Typ	Der Typ des Netzteils.
Version	Die Version des Netzteils.
Netz-Status	Zeigt den Zustand der Netzverbindung an. Mögliche Werte sind: Störung oder OK.
Temperatur	Zeigt die Temperatur des Netzteils an.
Ladespannung	Zeigt die Spannung am Netzteil an.
Ladestrom	Zeigt den Stromverbrauch des Netzteils an.
Aufladestatus	Zeigt den Zustand der Batterieladung an.
Hauptstromkreis	Zeigt den Status des Hauptstromkreises an, der bei verbundenem Netzstrom für die

Name	Beschreibung
	Stromversorgung zuständig ist.
Aufladestromkreis	Zeigt den Status des Aufladestromkreises an, der bei verbundenem Netzstrom die Batterien auflädt.
Batterie	Zeigt den Aufladestatus, die Spannung und den Strom der Batterien an.
Ausgänge	Zeigt die Spannung, den Zustand der Sicherung und den Zustand des Sabotageschutzes des jeweiligen Netzteilausgangs an.

## 7.6 Bedienteile

Informationen zur Konfiguration finden Sie auf Seite.

**Allgemein**



Status der  
Zentrale

1. Klicken Sie auf das Register **Bedienteil**.
2. Siehe die nachfolgende Tabelle für weitere Informationen.

Online Übersicht Bedienteile							
Erw.-ID	Beschreibung	Leitungsplan	Typ	Firmware	Komm.	Status	
1		XBus 1 - Position 1	Bedienteil	2.07 19SEP08	Online	OK	
2		XBus 2 - Position 1	Bedienteil	2.07 19SEP08	Online	OK	

Erweiterungs-ID	Mit dieser ID wird das Bedienteil eindeutig gekennzeichnet.
Beschreibung	Beschreibungstext für das Bedienteil (max. 16 Zeichen).
Leitungsplan	Die Anordnung des Bedienteils auf dem X-BUS.
Typ	Der Typ der erkannten Erweiterung (= Bedienteil).
Firmware-Version	Die Firmware-Version des Bedienteils.
Komm.	Der Status des Bedienteils (online oder offline).
Status	Der Status des Bedienteils (OK, Störung).

## Ausführbare Aktionen

Aktualisieren	Klicken Sie auf die Schaltfläche Aktualisieren, um den Status der Systemalarme zu aktualisieren.
Leitungsplan	Klicken Sie auf die Schaltfläche, um eine Liste von Erweiterungen/Bedienteilen zu erhalten, die physisch an die Zentrale angeschlossen sind.

## Status Bedienteil

Den Online Status eines Bedienteils anzeigen:

1. Klicken Sie auf ein Bedienteil in Übersicht Bedienteile (siehe Seite [→ 42]).
2. Siehe die nachfolgende Tabelle für weitere Informationen.

### Status Bedienteil

Statusinformationen des Bedienteils



**Bedienteil-ID :** 1  
**Typ :** Bedienteil  
**S/N :** 119959801  
**Firmware-Version :** 2.07 195EP08  
**Spannung :** 13.3V  
**Batteriespannung :** N/A  
**Strom :** 0mA  
**Funktyp :** Nicht gesteckt  
**Funkversion :** --  
**Lesertyp :** EM4100

	Input	Status
Kommunikation	OK	OK
Deckelkontakt	OK	OK
Überfall	OK	OK

Kommunikation	Der physische Status (OK, Störung) und der programmierte Status (OK, ausgeschaltet, gesperrt) der Kabelverbindung zur Erweiterung.
Sabotage Deckelkontakt	Der physische und der programmierte Status des Sabotageschalters (Deckelkontakt) am Gehäuse des Erweiterungsmoduls.
TP	Betrifft nur Bedienteile, in denen ein Transpondersignalempfänger installiert ist.
Überfall	Status des Panikalarms im Bedienteil.

## Ausführbare Aktionen

Alarmer quittieren	Klicken Sie auf die Schaltfläche, um alle Alarmer auf der Zentrale zu quittieren.
Sperren ⓘ	Klicken Sie auf diese Schaltfläche, um einen Fehlerzustand zu sperren. Durch das Sperren werden der Fehler oder die Meldergruppe nur für einen Scharfschaltungszeitraum gesperrt. Sperren steht bei Sicherheitsgrad 3 nach EN 50131 nicht zur Verfügung.
Abschaltung	Klicken Sie auf diese Schaltfläche, um diese Meldergruppe abzuschalten. Durch das Abschalten einer Meldergruppe wird diese solange deaktiviert, bis sie explizit wieder eingeschaltet wird. Es empfiehlt sich, beim Abschalten von Meldergruppen sehr vorsichtig vorzugehen, da diese Meldergruppen nicht aktiv sind, wenn das System SCHARFGESCHALTET wird.

## 7.7 Türmodule

Allgemein



Status der  
Zentrale

1. Klicken Sie auf die Registerkarte **Türsteuerungen**.
2. Weitere Informationen finden Sie in der nachstehenden Tabelle.

Online Übersicht Türsteuerungen							
Erw.-ID	Beschreibung	Leitungsplan	Typ	Firmware	Komm.	Status	Nid
6			Türsteuerung [4 Eingang / ...	0.00	Online	abgeschalte	Nid

Erweiterungs-ID	Mit dieser ID wird die Türsteuerung eindeutig gekennzeichnet.
Beschreibung	Beschreibungstext für die Türsteuerung (max. 16 Zeichen).
Leitungsplan	Die Anordnung der Türsteuerung auf dem X-Bus.
Typ	Der Typ der erkannten Türsteuerung (= Türsteuerung).
Firmware-Version	Die Firmware-Version der Türsteuerung.
Komm.	Der Status der Türsteuerung (online oder offline).
Status	Der Status der Türsteuerung (OK, Störung).
Netzteil	Gibt an, ob die Türsteuerung mit einem Netzteil ausgestattet ist.

### Ausführbare Aktionen

Aktualisieren	Klicken Sie auf die Schaltfläche Aktualisieren, um den Status der Systemalarme zu aktualisieren.
Leitungsplan	Klicken Sie auf die Schaltfläche, um eine Liste von Erweiterungen/Bedienteilen zu erhalten, die physisch an die Zentrale angeschlossen sind.

### Status Türsteuerungen

Den Online-Status eines Bedienteils anzeigen:

1. Klicken Sie auf eine Türsteuerung in der Liste.
2. Siehe die nachfolgende Tabelle für weitere Informationen.

**Status Türsteuerungen**

Erweiterungs-ID : 9 Zeige NT Status

Typ : Türsteuerung [4 Eingang / 2 Ausgang]

S/N : 1

Firmware-Version : 1.08 Build28

Spannung : 13.2V

Batteriespannung : N/A

Strom : 0mA

Funktyp : Nicht gesteckt

Funkversion : --

	Input	Status
Kommunikation	OK	OK
Deckelkontakt	OK	OK
Störung Sicherung	OK	OK
Netz	OK	OK
Batterie	OK	OK
Netzteil	OK	OK

Alarmer quittieren    Sperren    Abschalten

Schließen

Kommunikation	Der physische Status (OK, Störung) und der programmierte Status (OK, ausgeschaltet, gesperrt) der Kabelverbindung zur Erweiterung.
---------------	--

Sabotage Deckelkontakt	Der physische und der programmierte Status des Sabotageschalters (Deckelkontakt) am Gehäuse des Erweiterungsmoduls.
Störung Sicherung	Physischer und programmierter Status der Sicherung der Erweiterung.

## Ausführbare Aktionen

Alarmer quittieren	Klicken Sie auf die Schaltfläche, um alle Alarmer auf der Zentrale zu quittieren.
Sperren ⚠	Klicken Sie auf diese Schaltfläche, um einen Fehlerzustand zu sperren. Durch das Sperren werden der Fehler oder die Meldergruppe nur für einen Scharfschaltungszeitraum gesperrt. Sperren steht bei Sicherheitsgrad 3 nach EN 50131 nicht zur Verfügung.
Abschaltung	Klicken Sie auf diese Schaltfläche, um diese Meldergruppe abzuschalten. Durch das Abschalten einer Meldergruppe wird diese solange deaktiviert, bis sie explizit wieder eingeschaltet wird. Es empfiehlt sich, beim Abschalten von Meldergruppen sehr vorsichtig vorzugehen, da diese Meldergruppen nicht aktiv sind, wenn das System SCHARFGESCHALTET wird.

## 7.8 Türen

Allgemein



Status der  
Zentrale

1. Klicken Sie auf die Registerkarte **Türemeldungen**.
2. Siehe die nachfolgende Tabelle für weitere Informationen.

Online Übersicht Türen

Tür	ID	MG	Bereich	MK (DPS)	REX (DRS)	Status	Türmodus

Türen aktuell. LOG Sperren Freigeben Normal Einm. Freigabe

Tür	Bei dieser ID-Nummer handelt es sich um eine eindeutige ID für die Tür.
Meldergruppe	Die MG-Nummer, welcher der Magnetkontakt zugewiesen ist (nur wenn der Magnetkontakt-Eingang auch als Einbruch-MG verwendet wird).
Bereich	Der Bereich, dem der Magnetschalter-Eingang und der Kartenleser zugewiesen sind.
MK (DPS)	Status des Magnetschalters.
REX (DRS)	Status des REX-Tasters.
Status	Der Status der Tür (OK, Störung).

REX (DRS)	Status des REX Tasters.
-----------	-------------------------

### Ausführbare Aktionen

Aktualisieren	Aktualisiert die Tür-Übersicht.
Log (Protokoll)	Zeigt ein Ereignisprotokoll der gewählten Tür an.
Sperrern	Sperrt die gewählte Tür.
Freigeben	Gibt die gewählte Tür frei.
Normal	Versetzt die Tür in die normale Systemsteuerung zurück.
Kurzzeitig	Gibt die Tür für ein definierten Zeitintervall frei.

## 7.8.1 Zutrittslogbuch – Tür X

Anzeigen eines Quick-Logs des Status einer Tür:

- ▷ SPC Pro ist an eine Zentrale angeschlossen.
- 1. Wählen Sie eine Tür aus der Liste.
- 2. Klicken Sie auf die Schaltfläche **Log**.



Das neueste Ereignis wird am unteren Ende der Liste angezeigt.

- 3. Klicken Sie auf die Schaltfläche **Log in Datei speichern**, um das aktuelle Ereignisprotokoll in einer Datei zu speichern (z. B. im Format .txt).
- ⇒ Sie können diese Protokolldatei öffnen, nachdem die Verbindung mit der Zentrale beendet wurde.

## 7.9 Logbuch System

Dieses Logbuch enthält alle Systemereignisse des SPC-Systems.

**Allgemein**



Logbuch  
System

- ▷ SPC Pro ist an eine Zentrale angeschlossen.
- Klicken Sie auf die Registerkarte **Logbuch System**.
- ⇒ Daraufhin erscheint das folgende Fenster:

Anzeigen von Ereignissen, die über bestimmte Zeiträume eingetreten sind:

1. Geben Sie das Startdatum und die Startzeit für das Logbuch im Dropdown-Menü **Von: Datum/Uhrzeit** ein.
2. Geben Sie das Enddatum und die Endzeit für das Log im Dropdown-Menü **Bis: Datum/Uhrzeit** ein.
3. Klicken Sie auf die Schaltfläche **Log anfordern**.
  - ⇒ Das aktuelle System-Ereignisprotokoll wird von der Zentrale heruntergeladen.
  - ⇒ Das System-Ereignisprotokoll für den angegebenen Zeitraum wird in der folgenden Reihenfolge angezeigt: Datum, Zeit, Ereignis und Beschreibung.



Um zu vermeiden, dass mehrere Ereignisse aus derselben Quelle das Protokoll füllen, lässt das SPC

-System gemäß den geltenden Normen nur die Protokollierung von maximal 3 Aktivierungen der gleichen Meldergruppe innerhalb eines Scharfschaltungszeitraums zu.

4. Klicken Sie auf die Schaltfläche **Log in Datei speichern**, um das aktuelle Ereignisprotokoll in einer Datei zu speichern (z. B. in „log.txt“).
  - ⇒ Sie können diese Protokolldatei öffnen, nachdem die Verbindung mit der Zentrale beendet wurde.



Wenn Sie SPC Pro zur Änderung der Systemsprache am Bedienteil verwenden, wird die Sprache für das Logbuch erst aktualisiert, nachdem die Verbindung zur Zentrale getrennt und anschließend wiederhergestellt wurde.

## 7.10 Logbuch der Zutrittskontrollfunktion

Das Protokoll informiert über alle Zutrittsereignisse des SPC-Systems.

Allgemein



Zutrittslogbuch

▷ SPC Pro ist an eine Zentrale angeschlossen.



Um zu vermeiden, dass mehrere Ereignisse aus der selben Quelle das Log füllen, lässt das SPC

gemäß geltenden Normen nur die Protokollierung von maximal 3 Aktivierungen der gleichen Meldergruppe innerhalb eines Alarmzeitraums zu.

- Klicken Sie auf die Registerkarte **Zutrittslogbuch**.  
 ⇒ Daraufhin erscheint das folgende Fenster:

Anzeigen von Zutrittsereignissen, die über bestimmte Zeiträume ausgegeben wurden:

1. Geben Sie das Startdatum und die Startzeit für das Logbuch im Dropdown-Menü Von: Datum/Uhrzeit ein.
2. Geben Sie das Enddatum und die Endzeit für das Logbuch im Dropdown-Menü Bis: Datum + Zeit ein. Datum/Uhrzeit ein.
3. Geben Sie den Benutzernamen aus dem Benutzer-Dropdown-Menü ein.
4. Geben Sie den Türnamen aus dem Tür-Dropdown-Menü ein.
5. Klicken Sie auf die Schaltfläche **Zutrittslog anfordern**.

- ⇒ Das aktuelle Systemlog der Zutrittsmeldungen wird von der Zentrale heruntergeladen.
  - ⇒ Das Systemlog für Zutrittsmeldungen für den angegebenen Zeitraum wird in der folgenden Reihenfolge angezeigt: Datum, Zeit, Benutzer, Tür und Meldung.
6. Klicken Sie auf die Schaltfläche **Log in Datei speichern** , um das aktuelle Ereignisprotokoll in einer Datei zu speichern (z. B. im Format .txt).
- ⇒ Sie können diese Protokolldatei öffnen, nachdem die Verbindung mit der Zentrale beendet wurde.

## 8 Benutzer

Die folgende Tabelle enthält die maximale Anzahl an Benutzern, Benutzerprofilen und Benutzergeräten für die Zentrale:

Max. Anzahl	SPC4xxx	SPC5xxx	SPC6xxx
Benutzer	100	500	2.500
Profile	100	100	100
Profile pro Benutzer	5	5	5
Transponder	32	250	250
SMS IDs	32	50	100
Web-Zugangscodes	32	50	100
Fernbedienungen	32	50	100
MDT-Geräte	32	32	32



### ⚠️ WARNUNG

Beim Upgrade von einer Firmware-Version vor Version 3.3 müssen Sie Folgendes beachten:

- Das Techniker-Web-Kennwort (falls konfiguriert) wird gelöscht und muss nach dem Upgrade erneut eingegeben werden.
- Alle bestehenden Benutzer werden neuen Profilen zugeordnet, die den vorherigen Zutritts-Leveln der Benutzer entsprechen. Bei Überschreitung der max. Anzahl an Profilen wird kein Profil zugewiesen (siehe Anwenderprofile [→ 55]). Prüfen Sie nach dem Firmware-Upgrade sämtliche Benutzerkonfigurationseinstellungen.
- Die Standard-Techniker-ID wird von 513 in 9999 geändert.

## 8.1 Hinzufügen/Bearbeiten von Benutzern



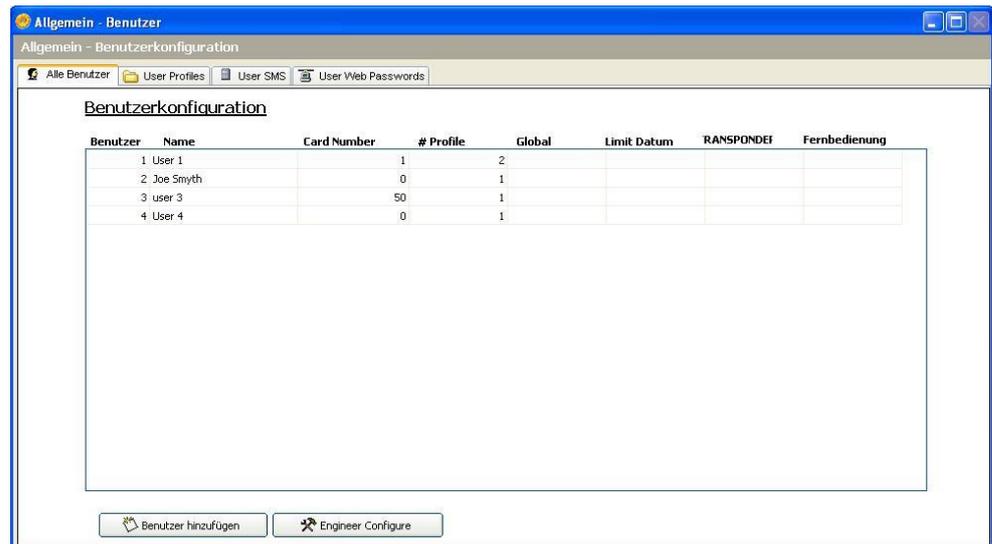
Allgemeine Informationen über die maximale Anzahl von Benutzern und die maximale Anzahl von Bereichen finden Sie im Installations- und Konfigurationshandbuch der betreffenden SPC-Zentrale

Allgemein



Benutzer

1. Klicken Sie auf das Register **Alle Benutzer**.
2. Weitere Informationen finden Sie in der nachstehenden Tabelle.



Benutzer hinzufügen	Klicken Sie auf diese Schaltfläche, um einen Benutzer zur Zentrale hinzuzufügen.
Engineer Configure (Techniker konfigurieren)	Klicken Sie auf diese Schaltfläche, um die PIN und den Webcode für den Technikerzugang zu ändern. Weitere Informationen finden Sie unter Konfiguration der Technikereinstellungen [→ 65].

## Benutzer hinzufügen

1. Klicken Sie auf die Schaltfläche **Benutzer hinzufügen**, um einen neuen Benutzer hinzuzufügen, ODER doppelklicken Sie auf einen Benutzer in der Benutzerliste, um ihn zu bearbeiten.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

Benutzerkonfig.
✖

## Benutzer konfigurieren

Ändern der Benutzereinstellungen, Profile, etc.

**Benutzer:**

**Benutzername:**

**Benutzer-PIN:**

**User Language :**

**Aktivieren Bedrohung :**

**Zeit-Limit :**  **Eingeschaltet**  bis

---

**Anwenderprofil :**

<b>Anwenderprofil 1</b>	<input type="text" value="--"/>	
<b>Anwenderprofil 2</b>	<input type="text" value="--"/>	
<b>Anwenderprofil 3</b>	<input type="text" value="--"/>	
<b>Anwenderprofil 4</b>	<input type="text" value="--"/>	
<b>Anwenderprofil 5</b>	<input type="text" value="--"/>	

---

**Zutrittskontrolle :**

**Ausweisnr. :**  Eingabe Ausweisnr.

**Karte ungültig**  Aktivieren um die Karte vorübergehend zu sperren.

**Verlängerte Zeit :**  Auswählen, um die Türöffnungszeit zu verlängern

**PIN-Bypass :**  Karte benötigt keine PIN and Türen, die zusätzl. eine PIN erfordern.

**Priorität :**  Karten mit Vorzug haben auch Zugang, wenn Türstrg n. verbunden ist.

**Begleitung :**  Karte kann Zutritt durch Türen mit Attrib. 'Begleitung' gewähren.

**Aufsicht :**  Aufsicht muss Türgruppe zuerst betreten, und als letztes verlassen.

Benutzer	Wählen Sie eine Benutzer-ID aus den auf dem System verfügbaren IDs aus.
Benutzername	Geben Sie einen eindeutigen Namen für diesen Benutzer ein (max. 16 Zeichen, mit Groß- und Kleinschreibung).
Benutzer-PIN	Geben Sie die Benutzerzugangs-PIN ein. <b>Hinweis:</b> Zur Einhaltung der INCERT-Genehmigungen muss die Benutzer-PIN mehr als 4 Zeichen enthalten.
Sprache	Sie können die Standardsprache der Zentrale ändern. Die Bedienteilmenüs werden in der gewählten Sprache angezeigt, wenn die PIN für diesen Benutzer eingegeben wird. Wenn die ausgewählte Sprache nicht auf der Zentrale verfügbar ist, werden die Menüs in der Standardsprache der Zentrale angezeigt. Wenn SPC Pro offline (nicht mit der Zentrale verbunden) ist, wird eine Liste mit den verfügbaren Sprachen der Zentrale angezeigt. Die tatsächlich verfügbaren Sprachen für die jeweilige Firmware-Version der Zentrale werden nur angezeigt, wenn SPC Pro online (mit der Zentrale verbunden) ist. Wenn SPC Pro offline ist, wird anstelle der kundenspezifischen Sprache der Hinweis ‚Custom‘ angezeigt.
Aktivieren Bedrohung	Aktivieren Sie für diesen Benutzer die Option Bedrohungspin ermöglichen, falls erforderlich. Die für Bedrohungs-PINs zugewiesene Anzahl an PINs (PIN +1 oder PIN+2) wird in System Optionen [→ 71] festgelegt. <b>Hinweis:</b> Die Bedrohungspin-Option steht in diesem Fenster nur zur Verfügung,

	wenn unter System Optionen die Option "Bedrohungspin" für das System aktiviert ist. Wenn die Bedrohungspin-Option für diesen Benutzer aktiviert ist, sind aufeinanderfolgende Benutzer-PINs für andere Benutzer (d. h. 2906, 2907...) nicht zulässig, da die Eingabe dieser PIN am Bedienteil einen Bedrohungsalarm auslösen würde.
Limit Datum	Aktivieren Sie das Kontrollkästchen Limit aktivieren, um diesem Benutzer den Zugriff für den Zeitraum innerhalb der vorgegebenen Werte zu verwehren.
Anwenderprofile	Wählen Sie Profile aus, die diesem Benutzer über die Dropdown-Liste zugewiesen werden können.
Zutrittskontrolle	Siehe Tabelle im nächsten Abschnitt für weitere Informationen.

## Zutrittskontrolle

Attribut	Beschreibung
Ausweisnummer	Eingabe Ausweisnr. Geben Sie 0 ein, wenn dieser Ausweis nicht zugewiesen werden soll.
Ung. Ausweis	Aktivieren, um den Ausweis vorübergehend zu sperren.
Verlängerte Türöffnungszeit	Verlängert die Türöffnungszeit, wenn der betreffende Ausweis vorgehalten wird.
PIN Bypass	Zutritt ohne Eingabe einer PIN an einer Tür mit PIN-Leser.
Priorität	Karten (Ausweise) mit Vorzug werden lokal in den Tür-Controllern gespeichert und haben auch dann Zutritt, wenn die Türsteuerung aufgrund einer technischen Störung keine Verbindung zur Zentrale hat. Die maximale Anzahl von Benutzern mit Vorzugsrechten ist wie folgt: <ul style="list-style-type: none"> <li>● SPC4xxx - Alle Benutzer</li> <li>● SPC5xxx - 512</li> <li>● SPC6xxx - 512</li> </ul>
Begleitung	Die Begleitungsfunktion erfordert, dass privilegierte Ausweisinhaber andere Ausweisinhaber durch bestimmte Türen begleiten. Wird diese Funktion an einer Tür aktiviert, muss zuerst ein Ausweis mit „Begleitrecht“ vorgehalten werden, bevor andere Ausweisinhaber ohne dieses Recht die Tür öffnen können. Die Zeitspanne, innerhalb der Ausweisinhaber ihre Ausweise vorhalten können, nachdem ein Ausweis mit Begleitrecht vorgehalten wurde, kann für jede Tür separat eingestellt werden.
Aufsicht	Die Aufsichtsfunktion berechtigt einen Ausweisinhaber mit Aufsichtsprivileg zum ständigen Aufenthalt in einem Raum (bzw. innerhalb einer Türgruppe), wann immer sich andere Ausweisinhaber dort aufhalten. Die Aufsichtsperson muss den betreffenden Raum zuerst betreten. Andere Ausweisinhaber dürfen den Raum nur betreten, wenn sich eine Aufsichtsperson im Raum befindet. Der Ausweisinhaber mit Aufsichtsrechten darf den Raum erst wieder verlassen, wenn alle beaufsichtigten Personen den Raum verlassen haben. Kennzeichnet den Ausweisinhaber als Aufsichtsperson. Der Benutzer mit dem Attribut „Aufsicht“ muss eine Türgruppe, die einen Karteninhaber mit Aufsichtsrecht erfordert, als erster betreten und muss die betreffende Türgruppe als letzter verlassen.

### Siehe auch

 Konfiguration von SMS [→ 60]

## 8.2 Hinzufügen/Bearbeiten von Profilen



### HINWEIS

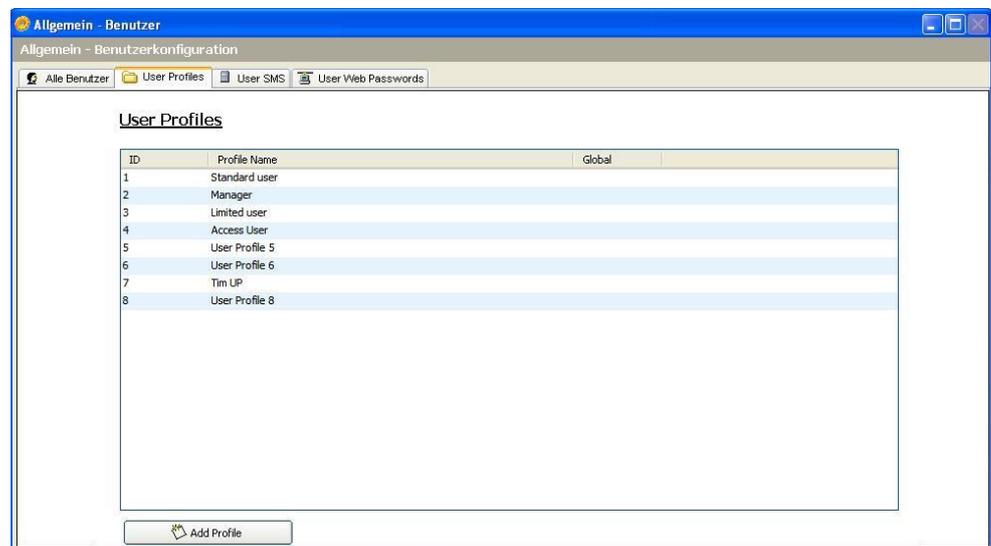
Globale Profile können nicht im SPC Webbrowser oder in der SPC Pro geändert werden, sondern müssen im SPC Manager bearbeitet werden

Allgemein



Benutzer

1. Klicken Sie auf die Registerkarte **User Profiles (Benutzerprofile)**.  
⇒ Eine Liste mit den bestehenden Benutzerprofilen wird angezeigt.



2. Wählen Sie **Add Profile (Profil hinzufügen)**, oder klicken Sie auf ein Profil, um es zu bearbeiten.

## Allgemeine Einstellungen

1. Geben Sie eine **Anwenderprofil ID** ein, die derzeit nicht verwendet wird. Sollten Sie eine ID eingeben, die bereits verwendet wird, wird die Meldung ‚ID nicht verfügbar‘ angezeigt.
2. Geben Sie unter **Name des Anwenderprofils** einen Namen ein (max. 16 Zeichen, mit Groß- und Kleinschreibung).
3. Wählen Sie alle **Bereiche**, die mit diesem Anwenderprofil gesteuert werden sollen.
4. Wählen Sie einen **Kalender** aus, um die Zeitbegrenzung für dieses Profil im System festzulegen.

## Benutzer-/Systemrechte

- Wählen Sie die erforderlichen Benutzerrechte, die diesem Profil zugewiesen werden sollen.

## Benutzerrechte

Recht	Standard-Anwenderprofiltyp	Beschreibung
<b>Anwenderrechte – Eindringling</b>		
Extern Scharf	Limited Standard	Im EXT SCHARF-Betrieb schaltet das Alarmsystem extern scharf und gewährleistet den umfassenden

Recht	Standard-Anwenderprofil	Beschreibung
	Manager	Schutz eines Gebäudes (beim Öffnen einer Meldergruppe wird ein Alarm ausgelöst). Nach dem Wählen von EXTERN SCHARF ertönt der Summer und das Bedienteil zeigt einen Countdown der verbleibenden Schärfungsverzögerung an. Das Gebäude muss vor Ablauf dieser Zeit verlassen werden. Wenn die Schärfungsverzögerung abgelaufen ist, wird das System scharfgeschaltet und das Öffnen von verzögerten Meldergruppen löst die Alarmverzögerung aus. Wenn das System nicht unscharf geschaltet wird, bevor die Alarmverzögerung abläuft, wird der Alarm ausgelöst.
Intern scharf A	Standard Manager	Die Option INTERNSCHARF A bietet Schutz für einen bestimmten Bereich des Gebäudes, während man sich im Ausgangsbereich frei bewegen kann. Meldergruppen, die als NICHT BEI INTERN A klassifiziert wurden, bleiben in diesem Modus ungeschützt. Standardmäßig gibt es keine Schärfungsverzögerung; das System wird beim Wählen dieses Modus automatisch scharf geschaltet. Es kann eine Scharfschaltungsverzögerung in diesem Modus verwendet werden, indem der Parameter Intern scharf A verzögert aktiviert wird.
Intern scharf B	Standard Manager	Durch die Option INTERN SCHARF B werden alle Meldergruppen geschützt mit Ausnahme derer, die als NICHT BEI INTERN B klassifiziert wurden. Standardmäßig gibt es keine Schärfungsverzögerung; das System wird beim Wählen dieses Modus automatisch scharf geschaltet. Es kann eine Scharfschaltungsverzögerung in diesem Modus verwendet werden, indem der Parameter Intern scharf B verzögert aktiviert wird.
Erzwungen scharf	Standard Manager	Die Option ERZWUNGEN SCHARF wird im Display des Bedienteils angezeigt, wenn versucht wird, das System scharfzuschalten, während ein Fehler an einer Meldergruppe vorliegt oder diese noch offen ist (die obere Zeile des Displays zeigt die betreffende offene Meldergruppe an). Durch Wählen dieser Option wird der Alarm scharfgeschaltet und für diese Meldergruppe um die eingestellte Zeit verzögert.
Unscharf	Limited Standard Manager	Die Option UNSCHARF deaktiviert den Alarm. Diese Menüoption wird auf dem Bedienteil nur angezeigt, nachdem eine Verzögerungs-Meldegruppe aktiviert und eine gültige Anwender-PIN eingegeben wurde.
Automatische Schärfung löschen	Standard* Manager	Der Anwender kann die automatische Scharfschaltung verzögern oder abbrechen.
Verzögerung abkürzen	Standard Manager	Die Unscharf-Verzögerung kann automatisch aufgehoben werden. Diese Option steht nur für Installationen im Finanzsektor zur Verfügung. Siehe Scharf-/Unscharfschalten [→ 135]
Quittieren	Standard Manager	Die Option QUITTIEREN quittiert einen Alarmzustand im System und löscht die zugehörige Alarmmeldung. Ein Alarmzustand kann nur quittiert werden, nachdem die Meldergruppe(n) oder der/die Fehler, die die Alarmbedingung ausgelöst haben, wieder in ihren normalen Betriebszustand versetzt wurden und in der

Recht	Standard-Anwenderprofiltyp	Beschreibung
		Benutzerprogrammierung für den gewählten Bereich die Option ALARME QUITTIEREN gewählt wurde.
Sperren	Standard Manager	MG sperren deaktiviert diese Meldergruppe für einen Alarmzeitraum. Diese Methode sollte bevorzugt zum Deaktivieren von fehlerhaften oder offenen Meldergruppen verwendet werden, da der Fehler oder der geöffnete Zustand jedes Mal auf dem Bedienteil angezeigt werden, um den Benutzer daran zu erinnern, dass er sich um diese Meldergruppe kümmern muss.
Abschaltung	Standard* Manager	Durch Abschalten einer Meldergruppe wird diese solange deaktiviert, bis sie wieder eingeschaltet wird. Alle Meldergruppen des Controllers können abgeschaltet werden. Die Verwendung dieser Funktion zum Deaktivieren von fehlerhaften oder offenen Meldergruppen sollte sorgfältig überdacht werden. Wenn eine Meldergruppe abgeschaltet ist, wird sie vom System ignoriert und könnte bei einem späteren Scharfschalten übersehen werden, womit die Sicherheit der Räumlichkeiten gefährdet würde.
<b>Anwenderrechte – System</b>		
Webzugang	Standard* Manager	Der Anwender kann über einen Browser auf die Zentrale zugreifen.
Log einsehen	Standard Manager	Mit dieser Menüoption wird das letzte Ereignis auf dem Display des Bedienteils angezeigt. Im Logbuch werden Uhrzeit und Datum jedes protokollierten Ereignisses angezeigt.
Benutzer	Manager	Der Anwender kann andere Anwender in der Zentrale erstellen und bearbeiten, jedoch nur mit denselben oder weniger Rechten als dieser Anwender besitzt.
SMS	Standard* Manager	Mit dieser Funktion kann der SMS-Benachrichtigungsdienst eingerichtet werden, wenn im System ein Modem installiert ist.
Datum/Uhrzeit stellen	Standard Manager	Hier können Systemzeit und Systemdatum eingestellt werden. Stellen Sie sicher, dass die Einstellungen von Uhrzeit und Datum korrekt sind. Diese Felder erscheinen im Logbuch, wenn Ereignisse berichtet werden.
PIN ändern	Standard Manager	Hier können Benutzer ihre Benutzer-PINs ändern. <b>Hinweis:</b> Zur Einhaltung der INCERT-Genehmigungen muss die Anwender-PIN mehr als 4 Zeichen enthalten.
Video anzeigen/Video im Browser anzeigen	Standard Manager	Videobilder können über den Webbrowser angezeigt werden. Hinweis: Zur Nutzung dieser Funktion muss auch das Recht für den Webzugriff zugewiesen sein.
Türglocke	Standard-Manager	Alle Meldergruppen mit dem Attribut TÜRGLOCKE erzeugen einen kurzen Ton des Bedienteilssummers, wenn die Meldegruppe geöffnet wird (nur bei unscharfem System). Mit dieser Menüoption kann in allen Meldegruppen die Türglockenfunktion aktiviert oder deaktiviert werden.
Techniker	Manager	Hier können Anwender Zugriff auf den Konfigurationsmodus gewähren. Zur Erfüllung der regionalen Schweizer CAT 1- und CAT 2-Anforderungen müssen sämtliche Bereiche

Recht	Standard-Anwenderprofil	Beschreibung
		unscharf gestellt werden, wenn Technikerzugang gewährt wird; andernfalls wird dem Techniker der Zugang verwehrt.
Upgrade	Manager	Der Anwender kann Herstellerzutritt gewähren, um ein Firmware-Upgrade zu ermöglichen.
<b>Anwenderrechte – Steuerung</b>		
Ausgänge	Standard Manager	Der Anwender kann konfigurierte Ausgänge ein-/ausschalten (logische Ausgänge). Siehe Bearbeiten eines Ausgangs [→ 92].
X-10	Standard Manager Zutrittskontrolle	Der Anwender kann konfigurierte X-10-Geräte ein- und ausschalten. <b>Hinweis:</b> X-10 ist im Wartungszustand. Die Funktion wird im System zur Wahrung der Rückwärtskompatibilität beibehalten.
Türsteuerung	Standard* Manager Zutrittskontrolle	Der Anwender kann Türen freigeben/sperren.
FUNKSTEUERUNG	Standard-Manager Zutrittskontrolle	Der Anwender kann den Funkausgang steuern.
<b>Anwenderrechte – Test</b>		
Sirenentest	Standard Manager	Der Anwender kann einen Signalgebertest zum Testen von externen Sirenen, Blitzleuchte, internen Sirenen und Summer durchführen, um sicherzustellen, dass sie ordnungsgemäß funktionieren.
Gehtest	Standard Manager	Mit dem Gehtest lässt sich die Funktionsfähigkeit aller Alarmmelder im System testen.
WPA Test	Standard Manager	Mit diesem Test kann der Anwender die Funktionsfähigkeit von FÜ überprüfen.
Körperschallmelder-Test	Standard Manager	Der Anwender kann den Körperschallmelder testen.
<b>Anwenderrechte – Service-Techniker</b>		
Gibt dem Anwender Managerrechte		Anwender können andere Anwender im System ohne Einschränkung von Anwenderrechten erstellen und bearbeiten.
Ändern von Anwenderprofilen		Anwender kann Anwenderprofile im System erstellen und ändern.
Gibt Kalenderrechte		Anwender kann Kalender konfigurieren.
Ändern der Türeinrichtungen		Anwender kann Einstellungen der Türen ändern.
* Funktionen sind für diesen Anwender nicht standardmäßig aktiviert, können aber ausgewählt werden.		

## Zutrittskontrolle

1. Geben Sie für alle Ausweise, die diesem Profil zugeordnet sind, eine **Anlagennummer** ein, falls erforderlich. Weitere Informationen finden Sie im Anhang im Abschnitt Unterstützte Ausweisleser und Ausweisformate.
2. Wählen Sie die **Zutrittsberechtigungen** dieses Profils für die im System konfigurierten Türen. Verfügbare Optionen sind:
  - Kein Zutritt
  - 24 Stunden
  - Kalender (sofern konfiguriert)

## Benutzer

Klicken Sie unten im Dialog auf **View Profile Usage** (Ansicht Profilnutzung), um eine Liste mit Benutzern anzuzeigen, denen dieses Profil zugewiesen wurde.

Mit der Option **Replizieren** können Sie ein neues Anwenderprofil auf Grundlage eines bereits vorhandenen Profils erstellen. Eine neue Anwenderprofil-Seite wird angezeigt

### Siehe auch

- 📄 Hinzufügen/Bearbeiten von Profilen [→ 56]
- 📄 Bereich hinzufügen/bearbeiten [→ 129]

## 8.3 Konfiguration von SMS

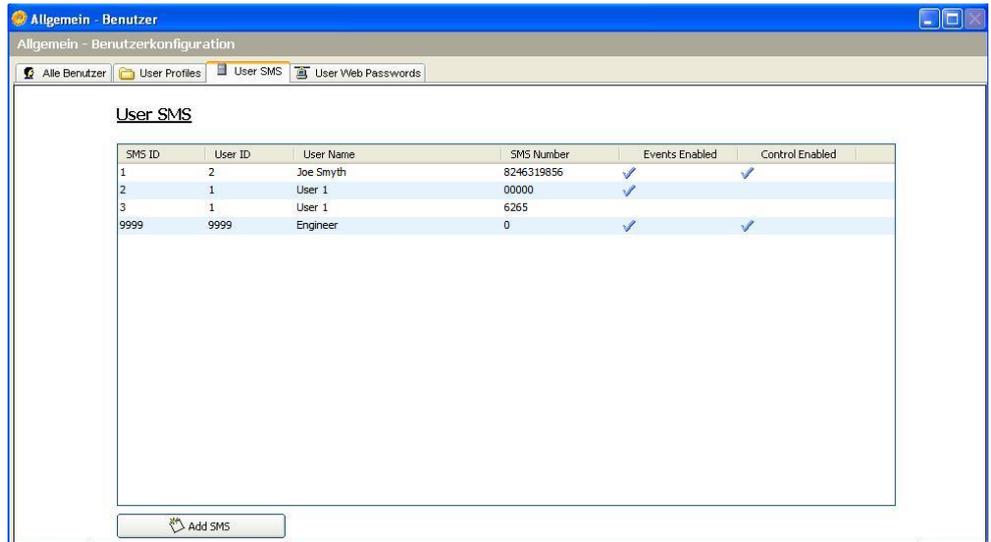
Das SPC-System unterstützt das Versenden von Textnachrichten (SMS) auf Systemen mit installierten Modems.

Allgemein

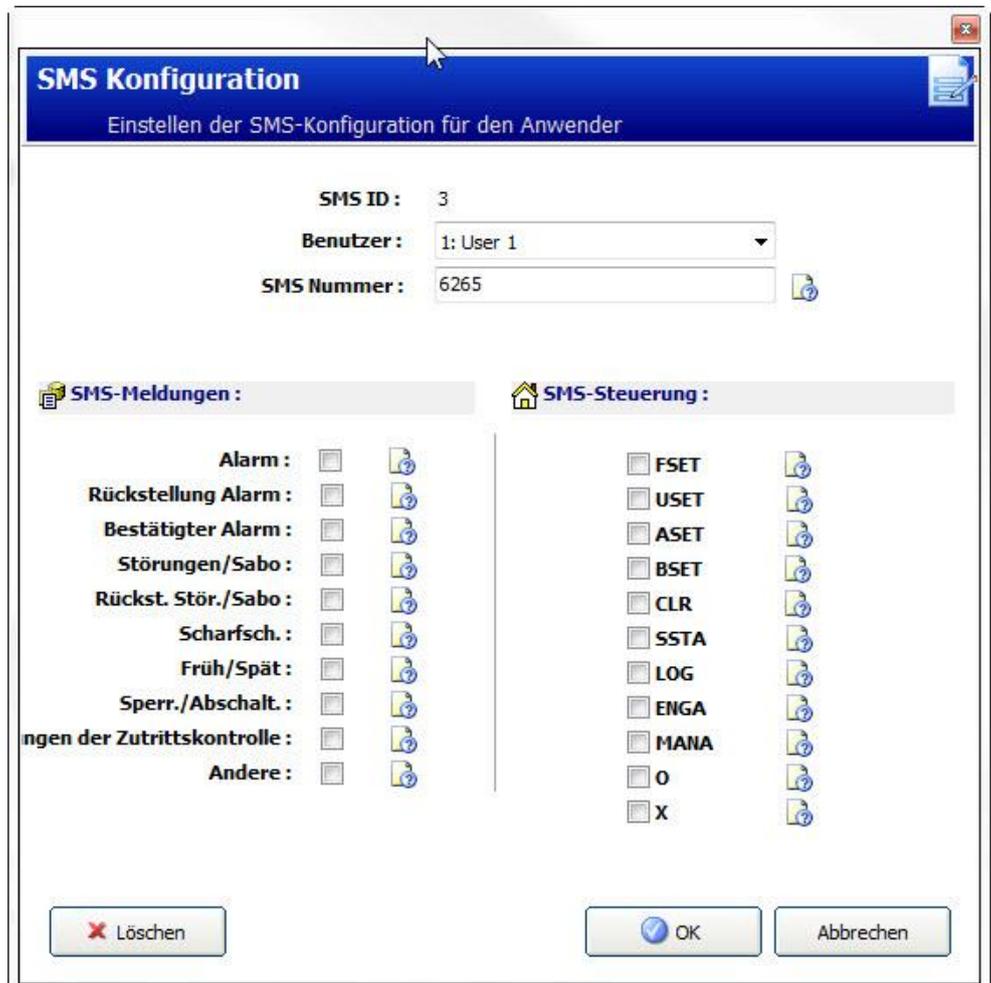


Benutzer

- ▷ Ein Modem ist installiert und vom System erkannt.
  - ▷ Die Funktion **SMS-Authentifizierung** ist aktiviert. Siehe Seite [→ 71].
1. Wählen Sie die Registerkarte **User SMS (Anwender SMS)**.
    - ⇒ Die SMS ID des Technikers sowie eine Liste mit SMS IDs und den entsprechenden SMS-Informationen werden angezeigt.



2. Klicken Sie auf **Add SMS (SMS hinzufügen)**, um eine neue SMS ID hinzuzufügen, oder klicken Sie auf einen SMS-Eintrag, um ihn zu bearbeiten.



3. Konfigurieren der SMS-Informationen:

SMS ID	Die vom System generierte ID.
SMS-Nummer	Geben Sie die Nummer ein, an welche die SMS gesendet werden soll (mit der dreistelligen Ländervorwahl). <b>Hinweis:</b> Die SMS-Nummer für Techniker kann gelöscht werden, wenn Sie

	auf 0 zurückgesetzt wird. SMS-Nummern für Benutzer können nicht gelöscht werden.
Benutzer	Wählen Sie einen neuen Benutzer für diese SMS ID, falls erforderlich.
SMS-Meldungen	Wählen Sie die Ereignisse der Zentrale, die der Benutzer oder Techniker per SMS erhält.
SMS-Strg	Wählen Sie die Vorgänge, die der Benutzer oder Techniker aus der Ferne via SMS in der Zentrale ausführen darf. Siehe SMS-Befehle [→ 62]

<b>!</b>	<b>HINWEIS</b>
	BEDROHUNG-Alarmereignisse werden nicht per SMS gemeldet.



Falls die Telefonleitung über eine Telefonanlage an das PSTN-Netz angeschlossen ist, muss ggf. die Amtskennziffer (für externe Gespräche) vor der Rufnummer des Empfängers eingefügt werden. Achten sie darauf, dass Calling Line Identity (CLI) am gewählten Anschluss aktiviert ist, damit Verbindungen zum SMS-Netz möglich sind. Setzen Sie sich für weitere Einzelheiten mit dem Telefonanlagenadministrator in Verbindung.

## 8.4 SMS-Befehle

Ist die SMS-Konfiguration abgeschlossen, können die SMS-Funktionen aktiviert werden. Befehle werden je nach SMS-Konfiguration über eine PIN oder eine Rufnummer an die Zentrale übertragen. Der Codetyp hängt von den Einstellungen für die SMS-Authentifizierung ab.

Die nachfolgende Tabelle enthält alle verfügbaren SMS-Befehle. Die auf einen Befehl folgenden Aktionen und Reaktionen sind ebenfalls aufgeführt.

SMS-Befehle werden als Texte an die Telefonnummer der SIM-Karte im Controller gesendet.

Für Befehle mit einer PIN lautet das Textformat wie folgt:

\*\*\*\*.Befehl oder \*\*\*\* Befehl

Dabei steht \*\*\*\* für die PIN und „Befehl“ ist der Befehl, d. h. die PIN gefolgt von einem Punkt oder einem Leerzeichen. Beispiel: Der Befehl „FSET“ wird wie folgt eingegeben: \*\*\*\* FSET oder \*\*\*\*.FSET. Soweit aufgelistet, kann auch die Vollversion des Befehls verwendet werden. Wie z. B. \*\*\*\*.EXTERN SCHARF.

Falls die Benutzerrechte nicht ausreichen, um einen Befehl auszuführen, zeigt das System ZUGANG VERWEIGERT an.

Falls eine Rufnummer aktiviert ist und die SMS-Nummer des Senders konfiguriert ist, wird das PIN-Präfix nicht benötigt.

BEFEHLE (**** = PIN)			
Mit PIN	Mit Rufnummer	Aktion	Reaktion
**** HILFE ****.HILFE	HILFE	Alle verfügbaren Befehle werden angezeigt.	Alle verfügbaren Befehle
**** FSET ****.FSET ****.EXT SCHARF	FSET EXT SCHARF	Schaltet alle Bereiche scharf, zu denen der Benutzer Zugang hat.	Datum/Uhrzeit der Systemaktivierung. Falls zutreffend: Anzeige offener/erzwungen scharfer MGs

**** USET **** USET **** . UNSCHARF	USET UNSCHARF	Schaltet alle Bereiche unscharf, zu denen der Benutzer Zugang hat.	System unscharf geschaltet
**** SSTA **** .SSTA **** . STATUS	SSTA STATUS	Liest den Status der Bereiche aus.	Status des Systems und der zugehörigen Bereiche <ul style="list-style-type: none"> <li>● Bei einem System mit nur einem Bereich werden das System und der Modus ausgegeben, wenn der Modus der Scharfschaltungsstatus des Systems ist.</li> <li>● Bei einem System mit mehreren Bereichen wird der Status jedes Bereichs ausgegeben.</li> </ul>
**** XA1.AN (X10) **** .XA1.AN		In den Fällen, in denen das X10-Gerät als „A1“ konfiguriert ist, wird es eingeschaltet.	Status von „A1“
**** XA1.AUS **** .XA1.AUS		In den Fällen, in denen das X10-Gerät als „A1“ konfiguriert ist, wird es ausgeschaltet.	Status von „A1“
**** LOG **** .LOG		Letzte Meldungen werden angezeigt (bis zu 10)	Letzte Meldungen
**** ENGA.AN (TECHNIKERZUGANG FREIGEBEN) **** .ENGA.AN	ENGA.AN	Technikerzugang freigeben	Technikerzugang freigeben
**** ENGA.AUS **** .ENGA.AUS	ENGA.AUS	Technikerzugang sperren	Technikerzugang sperren
**** MANA.AN **** .MANA.AN		Herstellerzugang freigeben	Herstellerstatus
**** MANA.AUS **** .MANA.AUS		Herstellerzugang sperren	Herstellerstatus
**** O.AN **** O.AN **** . AUSGANG		Wo der logische Ausgang als „O5“ konfiguriert ist, wird er eingeschaltet.	Status von „O“ Beispiel: <ul style="list-style-type: none"> <li>● Ausgang O5 aktiv.</li> <li>● Ausgang „Heizung“ aktiv (wobei „Heizung“ der Name des Ausgangs ist).</li> </ul>
**** O.AN **** O.AUS		Wo der logische Ausgang als „O“ konfiguriert ist, wird er ausgeschaltet.	Status von „O5“ Beispiel: Ausgang O5 inaktiv
**** ASET (INTERN SCHARF A)		Intern A Scharfsch via SMS zulassen Es kann auch der individuelle Name eingegeben werden, der im Feld INTERNSCHARF umbenennen des Optionsfensters definiert wurde. Siehe Optionen [→ 71]	System scharf.
**** BSET (INTERN SCHARF B)		Intern B Scharfsch via SMS zulassen Es kann auch der individuelle Name eingegeben werden, der im	System scharf.

		Feld INTERNSCHARF umbenennen des Optionsfensters definiert wurde. Siehe Optionen [→ 71] Beispiel: ****.ASET NIGHT	
****.ABBR ****.QUITTIEREN		Alarm quittieren via SMS zulassen	



Der logische Ausgang verwendet für die SMS-Erkennung das Format ONNN; O steht für den logischen Ausgang, NNN sind numerische Platzhalter, die nicht alle zwingend erforderlich sind.

(Beispiel: O5 = logischer Ausgang 5)

Das X-10-Gerät verwendet für die SMS-Erkennung das Format: XYNN; X steht dabei für X-10, Y steht für die alphabetische ID, und NN sind die verfügbaren numerischen Platzhalter. (Beispiel: XA1)

Die SMS-Funktion verwendet ein Standardprotokoll, das auch in SMS-fähigen Telefonen verwendet wird. Bitte beachten Sie, dass nicht alle PSTN-Betreiber den SMS-Dienst über PSTN anbieten. Damit SMS über PSTN funktioniert, müssen folgende Kriterien erfüllt sein:

- Die Rufnummernanzeige muss am Telefonanschluss aktiviert sein.
- Es muss sich um einen Direktanschluss handeln – nicht um einen Anschluss über eine Telefonanlage oder sonstige Telekommunikationsanlagen.
- Bitte beachten Sie auch, dass die meisten Telekommunikationsdiensteanbieter nur SMS an ein im gleichen Land angemeldetes Telefon zulassen. (Aus abrechnungstechnischen Gründen)

## 8.5 Löschen von Web-Zugangscodes

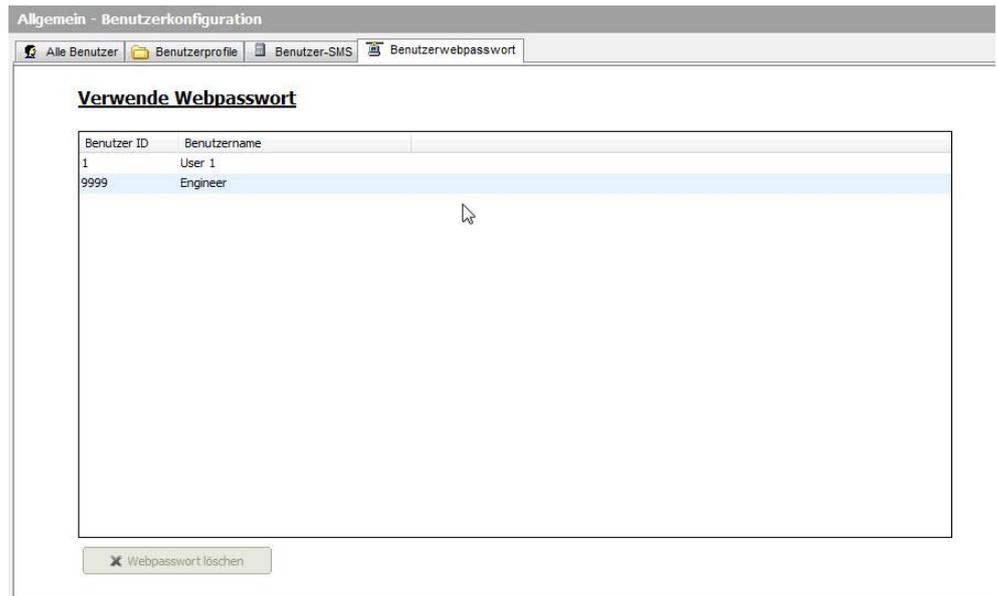
In diesem Fenster werden sämtliche Benutzer- und Techniker-Passwörter aufgelistet, die für den Zugriff über den Webbrowser erstellt wurden.

Allgemein



Benutzer

1. Wählen Sie die Registerkarte **User Web Passwords (Anwender Web-Zugangscodes)**.
2. Klicken Sie auf die Schaltfläche **Engineer Configure (Techniker Konfiguration)**.



3. Klicken Sie neben einem Benutzer oder Techniker auf die Schaltfläche **Delete Web Password (Löschen Web-Zugangscodes)**, um das Passwort zu löschen.

## 8.6 Konfiguration der Technikereinstellungen



1. Wählen Sie die Registerkarte **All Users (Alle Benutzer)**.
2. Klicken Sie auf die Schaltfläche **Engineer Configure (Techniker Konfiguration)**.

**Technikerkonfiguration**  
Technikerkonfig., Optionen...

**Benutzer ID :** 9999

**Benutzername :** Engineer

**Benutzer-PIN:** 001111

**Web Zugangscode :** \*\*\*\*\*

**Sprache :** English

**Zutrittskontrolle :**

**Kartennummer :** 0 Enter card number.

**Karte ungültig :**  Aktivieren um die Karte vorübergehend zu sperren.

**Verlängerte Zeit :**  Auswählen, um die Türöffnungszeit zu verlängern

**PIN-Bypass :**  Karte benötigt keine PIN and Türen, die zusätzl. eine PIN erfordern.

**Priorität :**  Karten mit Vorzug haben auch Zugang, wenn Türstrg n. verbunden ist.

**Begleitung :**  Karte kann Zutritt durch Türen mit Attrib. 'Begleitung' gewähren.

**Aufsicht :**  Aufsicht muss Türgruppe zuerst betreten, und als letztes verlassen.

OK Abbrechen

3. Bearbeiten Sie den **Benutzernamen** ‚Engineer‘, falls erforderlich.
4. Bearbeiten Sie die **User PIN (Benutzer-PIN)** für den Benutzer.



Die Mindestanzahl von Ziffern für jede PIN hängt von der Sicherheitseinstellung des Systems bzw. von dem im Menü **Zentralenkonfig > Systemoptionen > Optionen** gewählten Wert für die Option **Stellen PIN** ab.

5. Ändern Sie das **Web Passwort (Web-Passwort)** für den Zugriff über den Webbrowser (Buchstaben von A–Z, Zahlen von 0–9). Achten Sie bei der Eingabe des neuen Passworts auf die Groß- bzw. Kleinschreibung der Zeichen.



Die neue PIN und das Passwort können erst verwendet werden, nachdem die Konfigurationsdatei an die Zentrale gesendet wurde.

6. Klicken Sie auf **OK**.

### Zutrittskontrolle

Attribut	Beschreibung
Ausweisnummer	Eingabe Ausweisnr. Geben Sie 0 ein, wenn dieser Ausweis nicht zugewiesen werden soll.
Ung. Ausweis	Aktivieren, um den Ausweis vorübergehend zu sperren.
Verlängerte Türöffnungszeit	Verlängert die Türöffnungszeit, wenn der betreffende

Attribut	Beschreibung
	Ausweis vorgehalten wird.
PIN Bypass	Zutritt ohne Eingabe einer PIN an einer Tür mit PIN-Leser.
Priorität	<p>Karten (Ausweise) mit Vorzug werden lokal in den Tür-Controllern gespeichert und haben auch dann Zutritt, wenn die Türsteuerung aufgrund einer technischen Störung keine Verbindung zur Zentrale hat.</p> <p>Die maximale Anzahl von Benutzern mit Vorzugsrechten ist wie folgt:</p> <ul style="list-style-type: none"> <li>● SPC4xxx - Alle Benutzer</li> <li>● SPC5xxx - 512</li> <li>● SPC6xxx - 512</li> </ul>
Begleitung	<p>Die Begleitungsfunktion erfordert, dass privilegierte Ausweisinhaber andere Ausweisinhaber durch bestimmte Türen begleiten. Wird diese Funktion an einer Tür aktiviert, muss zuerst ein Ausweis mit „Begleitrecht“ vorgehalten werden, bevor andere Ausweisinhaber ohne dieses Recht die Tür öffnen können. Die Zeitspanne, innerhalb der Ausweisinhaber ihre Ausweise vorhalten können, nachdem ein Ausweis mit Begleitrecht vorgehalten wurde, kann für jede Tür separat eingestellt werden.</p>
Aufsicht	<p>Die Aufsichtsfunktion berechtigt einen Ausweisinhaber mit Aufsichtsprivileg zum ständigen Aufenthalt in einem Raum (bzw. innerhalb einer Türgruppe), wann immer sich andere Ausweisinhaber dort aufhalten.</p> <p>Die Aufsichtsperson muss den betreffenden Raum zuerst betreten. Andere Ausweisinhaber dürfen den Raum nur betreten, wenn sich eine Aufsichtsperson im Raum befindet. Der Ausweisinhaber mit Aufsichtsrechten darf den Raum erst wieder verlassen, wenn alle beaufsichtigten Personen den Raum verlassen haben.</p> <p>Kennzeichnet den Ausweisinhaber als Aufsichtsperson. Der Benutzer mit dem Attribut „Aufsicht“ muss eine Türgruppe, die einen Karteninhaber mit Aufsichtsrecht erfordert, als erster betreten und muss die betreffende Türgruppe als letzter verlassen.</p>

## 9 Systemoptionen ändern

### 9.1 Identifikation

Zentralenkonfig.



Systemoptionen

1. Wählen Sie die Registerkarte **Identifikation**.  
⇒ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

Zentralenkonfig. - Systemoptionen

Identifikation Standards Optionen Timer Uhrzeit Sprache SPC Pro/SPC Safe

### Systemidentifikation

Option	Wert	Beschreibung
Installations-ID	2	Numerische ID der Zentrale zur eindeutigen Identifikation.
Name der Inst.	Installation 2	Beschreibung der Installation
Installationsdatum	22.04.2009	
Name des Errichters	Daniel	Name des Errichters, der für den Service zuständig ist.
Tel. des Errichters	0176 5436789	Tel. des Errichters, der für den Service zuständig ist.
Zeige Errichter	<input checked="" type="checkbox"/>	Wenn aktiviert, werden die Errichterinformationen am Bedienteil angezeigt.
Sperrcode	<input checked="" type="checkbox"/>	Vor Werkseinst. muss Sperrcode eingegeben werden.
Techniker Sperr-Code	1111	4-stelliger Techniker-Sperrcode

Installations-ID	Geben Sie für jede Installation eine eindeutige Nummer ein (1–999999). Diese Nummer identifiziert die Installation.
Name der Inst	Geben Sie den Namen der Anlage ein. Ein Installationsname muss eingegeben werden, bevor die Installation auf dem System gespeichert wird. Die Installation kann am Bedienteil angezeigt werden.
Installationsdatum	Wählen Sie das Datum, an dem die Installation fertiggestellt wurde, aus dem Dropdown-Menü.
Name des Errichters	Geben Sie den Namen der Person ein, die das System installiert hat (zu Supportzwecken).
Tel Errichter	Geben Sie die Telefonnummer der Person ein, die das System installiert hat (zu Supportzwecken).
Zeige Errichter	Aktivieren Sie dieses Kontrollkästchen, um die Installationsdaten auf dem an der Zentrale angeschlossenen Bedienteil anzuzeigen (im Bereitschaftszustand).
Sperrcode	Aktivieren sie diese Kontrollkästchen, um die Eingabe des Techniker-Sperr-Codes zu verlangen, um die Zentrale auf Werkseinstellungen zurückzusetzen.
Techniker Sperrcode	Geben Sie einen vierstelligen Sperrcode ein.

## 9.2 Normen



Alle Alarmsysteme müssen den geltenden Sicherheitsnormen entsprechen. Jede Norm hat spezifische Sicherheitsanforderungen, die für den Markt bzw. das Land, in dem das Alarmsystem installiert wird, gelten.

Zentralenkonfig.



Systemoptionen

- Wählen Sie die Registerkarte **Standards**.  
⇒ Daraufhin erscheint das folgende Fenster.



In SPC PRO können die Einstellungen Region und Grade nicht bearbeitet werden.

Zentralenkonfig. - Systemoptionen

Identifikation Standards Optionen Timer Uhrzeit Sprache SPC Pro/SPC Safe SPC Manager

**Auswählen, um den Normen zu entsprechen.**

**Installationstyp :**

Privat  
 Kommerziell  
 Bankanwendungen

**Region :**

Auswählen, um den UK PD6662 Normen zu entsprechen.  
  Auswählen, um den irischen Normen zu entsprechen.  
  Auswählen, um den europäischen Normen zu entsprechen.  
  Auswählen, um den schwedischen SSF 1014:3 Normen zu entsprechen.  
  Auswählen, um den INCERT Normen zu entsprechen.  
  Auswählen, um den Schweizer Normen zu entsprechen  
  (\*) Auswählen, um den spanischen Normen zu entsprechen.  
  (\*) Auswählen, um den deutschen Normen zu entsprechen  
  (\*) Auswählen, um den französischen Normen zu entsprechen

**Sicherheitsgrad :**

VDS Klasse A ( )  
 VDS Klasse C ( )  
 Unbeschränkte Konfiguration

(\*) Wenn Sie diese regionale Norm auswählen, werden lokale bzw. nationale Anforderungen umgesetzt, die die Anforderungen der EN50131 erweitern

Installationstyp	Wählen Sie die Installationsart. Die verfügbaren Optionen sind: Privat, Kommerziell, Finanziell.
Region	Um die Region in Ihrer Zentrale zu ändern, empfehlen wir dringend, die Zentrale auf die Standardeinstellungen zurückzusetzen und im Start-Assistenten eine neue Region auszuwählen. Wählen Sie die Region, in der die Anlage installiert ist, und die regionalen Anforderungen, die sie erfüllt. Zur Auswahl stehen: UK, Irland, Schweden, Europa, Schweiz, Belgien (INCERT), Spanien und Deutschland (VdS).

Sicherheitsgrad	<p>Wählen Sie den Sicherheitsgrad, der für die Installation gilt.</p> <ul style="list-style-type: none"> <li>● Regionen Irland und Europa: <ul style="list-style-type: none"> <li>- EN50131 Grad 2</li> <li>- EN50131 Grad 3</li> <li>- Unbeschränkt</li> </ul> </li> <li>● Region UK: <ul style="list-style-type: none"> <li>- PD6662 (basiert auf EN50131 Grad 2)</li> <li>- PD6662 (basiert auf EN50131 Grad 3)</li> <li>- Unbeschränkt</li> </ul> </li> <li>● Region Schweden: <ul style="list-style-type: none"> <li>- SSF1014:3 Larmclass 1</li> <li>- SSF1014:3 Larmclass 2</li> <li>- Unbeschränkt</li> </ul> </li> <li>● Region Belgien: <ul style="list-style-type: none"> <li>- TO-14 (basiert auf EN50131 Grad 2)</li> <li>- TO-14 (basiert auf EN50131 Grad 3)</li> <li>- Unbeschränkt</li> </ul> </li> <li>● Region Schweiz: <ul style="list-style-type: none"> <li>- SES EN-CH-Grad 2</li> <li>- SES EN-CH-Grad 3</li> <li>- Unbeschränkt</li> </ul> </li> <li>● Region Spanien: <ul style="list-style-type: none"> <li>- EN50131 Grad 2</li> <li>- EN50131 Grad 3</li> </ul> </li> <li>● Region Deutschland: <ul style="list-style-type: none"> <li>- VdS Klasse A</li> <li>- VdS Klasse C</li> <li>- Unbeschränkt</li> </ul> </li> <li>● Frankreich <ul style="list-style-type: none"> <li>- NF&amp;A2P - Grad 2</li> <li>- NF&amp;A2P - Grad 3</li> <li>- Unbeschränkt</li> </ul> </li> </ul>
-----------------	---

### Sicherheitsgrad – Unbeschränkt

Die Sicherheitsgradeinstellung **Unbeschränkt** bedeutet, dass für die Installation keinerlei regional bedingte Sicherheitsbeschränkungen gelten. Die Einstellung „Unbeschränkt“ erlaubt es dem Techniker, die Installation durch Ändern der Sicherheitsrichtlinienoptionen und Konfigurieren zusätzlicher Optionen anzupassen, die nicht mit den ausgewählten regionalen Sicherheitsanforderungen übereinstimmen.

Konfigurationsoptionen für die Einstellung „Unbeschränkt“ werden im vorliegenden Dokument mit dem folgenden Symbol gekennzeichnet: 

Informationen zu Richtlinien für die Systemkonfiguration finden Sie unter Systemoptionen [[→ 225](#)].

## 9.2.1 Installationstyp

Der Installationstyp bestimmt die MG-Typen, die auf der Zentrale programmiert werden können, und die verfügbaren Funktionen.

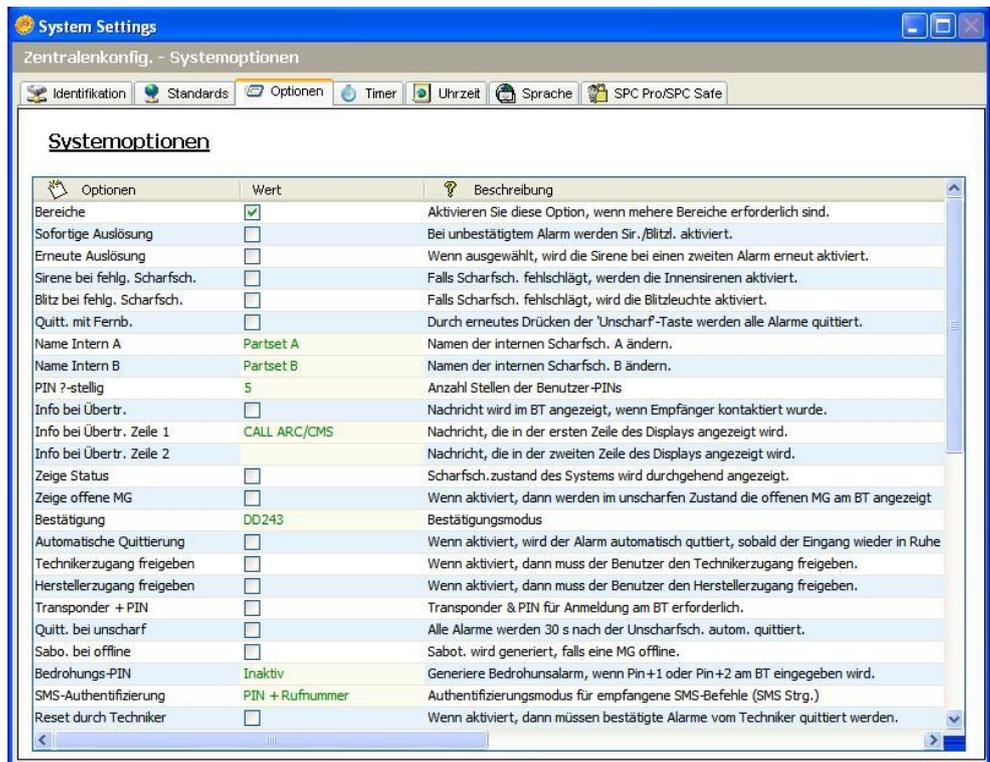
Sie können zwischen den folgenden Installationstypen wählen:

- **Privat:** Geeignet für Installationen in Wohnhäusern mit einem oder mehreren Bereichen und einer kleinen bis mittleren Anzahl von Einbruch-Meldergruppen. Für die Systemkonfiguration stehen entsprechende Eingangs-/Ausgangsfunktionen zur Verfügung.
- **Kommerziell:** Geeignet für Installationen in gewerblich genutzten Gebäuden mit verschiedenen Bereichen und einer großen Anzahl von Einbruch-Meldergruppen. Erweiterte Eingangs-/Ausgangsfunktionen wie „Kalender“ und „Automatische Scharfschaltung“ sind verfügbar.
- **Finanziell:** Geeignet für Banken und sonstige Finanzinstitute mit Tresor- und Geldautomatenumgebungen.

### 9.3 Optionen



1. Wählen Sie die Registerkarte **Optionen**.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



#### Systemoptionen



Die angezeigten Optionen variieren je nach Sicherheitsgrad des Systems.

Einschränkungen	Systemoptionen	Beschreibung
<b>Allgemeine Einstellungen</b>		
	Bereiche	Wählen Sie diese Option, um mehrere Bereich im System zu aktivieren.

Einschränkungen	Systemoptionen	Beschreibung
		<b>Hinweis:</b> Diese Option wird nur für private und kommerzielle Installationsarten angezeigt.
	Quittierung mit Code	Nur für Grad 3: Ein Benutzer, der keine Rechte zum Quittieren eines Alarms besitzt, kann den Alarm über diese Funktion trotzdem quittieren. Beim Versuch, einen Alarm zu quittieren, ist ein 6-stelliger Code erforderlich. Der Benutzer muss den Errichter anrufen, damit dieser einen Quittierungscode generiert, mit dem der Benutzer den Alarm quittieren kann.
	Sabo bei offline	Aktivieren Sie diese Option, damit ein Sabotagealarm generiert wird, falls eine Erweiterungs-MG offline geht.
	Quittierung mit Fernbedienung	Wenn aktiviert, können Alarme mit der Fernbedienung durch Drücken der Unscharfsch-Taste quittiert werden.
Nur Web und SPC Pro	LED Anzeige an Verifikationsmod.	Wenn aktiviert, wird die LED am Verifikationsmodul bei eingeschaltetem Mikrofon nicht aktiviert.
	Bericht im Konfigurationsmodus	Bei Aktivierung dieser Option meldet die Zentrale immer Alarmaktivierungen und Panikalarne.
	Ausgänge im Konf Modus	Wenn diese Option ausgewählt wird, werden folgende Ausgänge im Konfigurationsmodus nicht deaktiviert: <ul style="list-style-type: none"> <li>● Ausgänge der Zentrale</li> <li>● Ausgänge der Erweiterung</li> <li>● Anzeige-LEDs</li> <li>● Schlüsselschalter-LEDs</li> </ul>
	Warnung, wenn Bericht fehlgeschlagen	Wenn der Alarm ‚Warnung, wenn Bericht fehlgeschlagen‘ ausgelöst wird, werden die Außensirenen aktiviert.
	Bedrohungsalarm wiederholen	Wenn aktiviert, wird ein Bedrohungsalarm erneut ausgelöst
	Notrufalarm wiederholen	Wenn aktiviert, wird ein Notrufalarm erneut ausgelöst
	Überschreibe LEDs an Kartenleser	Wenn aktiviert, wird das LED-Verhalten der Ausweisleser von der Zentrale gesteuert.
	Akustik aus bei Audioverifik.	Wenn aktiviert, werden alle Innen- und Außensirenen (System und Bereich), die Bedienteilsummer und die Sprachausgaben auf dem Komfort-Bedienteil während einer Audioverifikation abgeschaltet.
	Watchdog Ausgang Mode	Aktiviert Ausgang 6 der SPC-Controllerplatine für Überwachungszwecke. Folgende Betriebsarten des Watchdog-Ausgangs können ausgewählt werden: <ul style="list-style-type: none"> <li>● Deaktiviert – Ausgang 6 ist als allgemeiner Universalausgang verfügbar.</li> <li>● Aktiviert – Ausgang 6 ist normalerweise AUS, wird jedoch eingeschaltet, wenn eine Watchdog-Störung vorliegt.</li> <li>● Pulsierend – Ausgang 6 PULSIERT in einem Intervall von 100 ms.</li> <li>● Aktivierung vertauscht – Ausgang 6 ist normalerweise EIN, wird jedoch ausgeschaltet, wenn eine Watchdog-Störung vorliegt.</li> </ul> Die folgenden Optionen kombinieren die Aktiviert-Option mit Hardware-Fehlerberichten, wenn der Hauptmikroprozessor ausfällt. Wenn ein derartiger Ausfall

Einschränkungen	Systemoptionen	Beschreibung
		<p>eintritt, wird ein SIA-Ereignis an ARC1 gesendet.</p> <p><b>Hinweis:</b> Der Empfänger muss so konfiguriert sein, dass er SIA und SIA Extended 1 oder 2 verwendet. CID und FF werden nicht von dieser Berichtsmethode unterstützt.</p> <ul style="list-style-type: none"> <li>● Aktiv + Auswertung (10 s) – Das Ausfallereignis wird 10 Sekunden nach Erkennung des Ausfalls an ARC1 gesendet. Diese Option muss verwendet werden, um mit VdS 2252 konform zu sein.</li> <li>● Aktiv + Auswertung (60 s) – Das Ausfallereignis wird 60 Sekunden nach Erkennung des Ausfalls an ARC1 gesendet.</li> </ul> <p>Das gemeldete SIA-Ereignis ist <b>HF</b> und Extended SIA meldet <b>Hardware-Störung</b>.</p> <p><b>Hinweis:</b> Hardware-Störungen werden nicht gemeldet, wenn der Techniker am System angemeldet ist.</p> <p>Weitere Information zu ARCs finden Sie unter Empfänger (Alarm Reporting Centres, ARCs) [→ 164].</p>
	SPCP355	Aktiviert die VdS-Stromversorgung. Für VdS-Installationen wird diese Option automatisch ausgewählt.
	Sirene bei fehlg Scharfsch.	Aktivieren Sie diese Option, um die Innensirenen zu aktivieren, falls das Scharfschalten des Systems fehlschlägt.
	Blitz bei fehlg Scharfsch.	Aktivieren Sie diese Option, um den Blitz zu aktivieren, falls das Scharfschalten des Systems fehlschlägt.
⬇	Verberge Bypass	Bei Aktivierung werden die Bypass-Meldungen nicht mehr auf dem Bedienteil angezeigt.
	Akku-Kapazität	Gesamtbatteriekapazität in Ah, nur für Bedienteile (3–100 Ah). Sie müssen diesen Wert und <b>Maximaler Strom</b> eingeben, um die verbleibende Batteriedauer auf dem Bedienteil für eventuelle Stromausfälle anzuzeigen. Dies wird unter „STATUS – AKKU – Akku Zeit“ angezeigt.
	Maximaler Strom	Die Gesamtstromaufnahme der Batterien, wenn die Stromversorgung ausfällt (30–20.000 mA). Sie müssen diesen Wert und <b>Akku Kapazität</b> eingeben, um die verbleibende Batteriedauer auf dem Bedienteil für eventuelle Stromausfälle anzuzeigen. Dies wird unter „STATUS – AKKU – Akku Zeit“ angezeigt.
<b>Intern scharf</b>		
	Name Intern A	Geben Sie einen neuen Namen für INTERNSCHARF A ein (z. B. Nachtmodus).
	Name Intern B	Geben Sie einen neuen Namen für INTERNSCHARF B ein (z. B. Nur 1. Stock).
<b>Alarm</b>		
	Sofortige Auslösung	Aktivieren Sie diese Option, um relevante Sirenen im Falle eines unbestätigten Alarms zu aktivieren. Wenn diese Option nicht aktiviert ist, werden die relevanten Sirenen nur bei einem bestätigten Alarm aktiviert oder wenn der Melder, der den unbestätigten Alarm ausgelöst hat, erneut aktiviert wird.
	Erneute Auslösung	Aktivieren Sie diese Option, um Sirenen erneut zu aktivieren, wenn eine zweite Meldergruppe auslöst (nach Ablauf der Aktivierungszeit). Wenn nicht aktiviert, wird die Sirene nur einmal aktiviert.
⬇	Kein Scharf bei	Wenn aktiviert, kann ein Bereich nicht geschärft werden, wenn ein Alarm in einem Bereich oder dem System

Einschränkungen	Systemoptionen	Beschreibung
Nur Web	Alarm	vorliegt. <b>Hinweis:</b> Nur verfügbar, wenn unter <b>Standards -&gt; Region</b> die Region „Schweiz“ oder der <b>Sicherheitsgrad</b> „Unbeschränkt“ ausgewählt ist.
	Quittierung bei unscharf	Aktivieren Sie diese Option, um Alarme nach 30 Sekunden im unscharfen Zustand automatisch zu quittieren. <b>Hinweis:</b> Um PD6662 zu erfüllen, muss diese Option deaktiviert werden.
Ⓣ	Antimask bei scharf	Wählen Sie den Meldungstyp für eine Erkennung von Antimask aus, wenn die Zentrale scharf geschaltet ist. Verfügbare Optionen sind: Inaktiv, Sabotage, Störung oder Alarm. Diese Option kann nur konfiguriert werden, wenn die Zentrale im Modus „Unbeschränkt“ ist. Im Modus Grad 2 oder Grad 3 entspricht der Meldungstyp den Standards für die ausgewählte Region: <ul style="list-style-type: none"> <li>● Irland – Alarm</li> <li>● Alle anderen Regionen – Alarm</li> </ul>
Ⓣ	Antimask bei Unscharf	Wählen Sie den Meldungstyp für eine Erkennung von Antimask aus, wenn die Zentrale unscharf geschaltet ist. Verfügbare Optionen sind: Inaktiv, Sabotage, Störung oder Alarm. Diese Option kann nur konfiguriert werden, wenn die Zentrale im Modus „Unbeschränkt“ ist. Im Modus Grad 2 oder Grad 3 entspricht der Meldungstyp den Standards für die ausgewählte Region: <ul style="list-style-type: none"> <li>● Irland – Deaktiviert</li> <li>● Alle anderen Regionen – Sabotage</li> </ul>
Ⓣ	EOL im Aus entschärfen	Wählen Sie den zu meldenden Ereignistyp aufgrund der Erkennung von EOL im Aus, wenn die Zentrale unscharf geschaltet ist. Verfügbare Optionen sind: Deaktiviert, Sabotage und Störung. Diese Option kann nur konfiguriert werden, wenn die Zentrale im Modus „Unbeschränkt“ ist. Im Modus Grad 2 oder Grad 3 entspricht der Meldungstyp den Standards für die ausgewählte Region: <ul style="list-style-type: none"> <li>● Deutschland VdS – Sabotage</li> <li>● Alle anderen Regionen – Störung</li> </ul>
Ⓣ	EOL im Aus schärfen	Wählen Sie den zu meldenden Ereignistyp aufgrund der Erkennung von EOL im Aus, wenn die Zentrale scharf geschaltet ist. Verfügbare Optionen sind: Deaktiviert, Sabotage und Störung. Diese Option kann nur konfiguriert werden, wenn die Zentrale im Modus „Unbeschränkt“ ist. Im Modus Grad 2 oder Grad 3 entspricht der Meldungstyp den Standards für die ausgewählte Region: <ul style="list-style-type: none"> <li>● Deutschland VDS – Sabotage</li> <li>● Alle anderen Regionen – Störung</li> </ul>
Ⓣ	MG instabil entschärfen	Wählen Sie den zu meldenden Ereignistyp aufgrund der Erkennung von Linie instabil, wenn die Zentrale unscharf geschaltet ist. Verfügbare Optionen sind: Deaktiviert, Sabotage und Störung. Eine Meldergruppe (Linie) ist instabil, wenn innerhalb von 10 Sekunden keine gültige Probe gewonnen werden kann. Diese Option kann nur konfiguriert werden, wenn die Zentrale im Modus „Unbeschränkt“ ist. Im Modus Grad 2

Einschränkungen	Systemoptionen	Beschreibung
		<p>oder Grad 3 entspricht der Meldungstyp den Standards für die ausgewählte Region:</p> <ul style="list-style-type: none"> <li>● Deutschland VDS – Sabotage</li> <li>● Alle anderen Regionen – Störung</li> </ul>
Ⓣ	MG instabil schärfen	<p>Wählen Sie den zu meldenden Ereignistyp aufgrund der Erkennung von Linie instabil, wenn die Zentrale scharf geschaltet ist. Verfügbare Optionen sind: Deaktiviert, Sabotage und Störung.</p> <p>Eine Meldergruppe (Linie) ist instabil, wenn innerhalb von 10 Sekunden keine gültige Probe gewonnen werden kann.</p> <p>Diese Option kann nur konfiguriert werden, wenn die Zentrale im Modus „Unbeschränkt“ ist. Im Modus Grad 2 oder Grad 3 entspricht der Meldungstyp den Standards für die ausgewählte Region:</p> <ul style="list-style-type: none"> <li>● Deutschland VDS – Sabotage</li> <li>● Alle anderen Regionen – Störung</li> </ul>
Ⓣ	EOL Spanne	Wenn aktiviert, werden die breiten EOL-Bänder verwendet.
	Hörbarer Verdachtsalarm	Wenn aktiviert, werden die FÜ-Verdachtsalarme akustisch und optisch am Bedienteil angezeigt. (nur im finanziellen Modus).
Pro	Endwiderstand (ENDWIDERSTAND)	<p>Wählen Sie die Endwiderstände, die entweder für alle Meldergruppen im System oder für neue Meldergruppen, die dem System hinzugefügt werden, gelten. Wählen Sie einen Wert, um die entsprechende Funktion zu aktivieren.</p> <p>Aktivieren Sie zur Anwendung einer neuen EOL-Einstellung für alle vorhandenen Meldergruppen das Kontrollkästchen ‚Endwiderstandswert aller Eingänge auf den Standardwert setzen‘. Wenn Sie den Wert für den Endwiderstand ändern, aber nicht dieses Kontrollkästchen aktivieren, gilt die neue Einstellung nur für Meldergruppen, die nach der Änderung des Werts hinzugefügt wurden.</p>
	Test KS bei manuel scharf	Wenn aktiviert, werden alle Körperschallmelder in den Bereichen, welche geschärft werden, vor der Scharfschaltung des Bereichs/Systems geprüft. (nur im finanziellen Modus).
Ⓣ	Automatische Quittierung	Aktivieren Sie diese Funktion, um Alarme auf dem System automatisch zu quittieren, d. h. wird die offene MG, die einen Alarm ausgelöst hat, geschlossen, ist eine manuelle Quittierung am Bedienteil/Browser nicht mehr erforderlich. Ist die Funktion nicht aktiviert, kann der Benutzer Alarme nicht durch Zurücksetzen des Eingangs, der den Alarm ausgelöst hat, quittieren.
Ⓣ	Erzwungene Schärfung mit Alarm	<p><b>Aktiv:</b> Wird eine nicht-verzögerte Meldergruppe aktiviert, während der Ausgangs-Timer abläuft, wird ein lokaler Alarm mit Sirenen ausgelöst.</p> <p><b>Deaktiviert:</b> Wird eine nicht-verzögerte Meldergruppe aktiviert, während der Ausgangs-Timer abläuft, wird kein Alarm ausgelöst.</p> <p><b>Hinweis:</b> Diese Option wird nur angezeigt, wenn der Grad <b>Unbeschränkte Konfiguration</b> ausgewählt wurde, da ihre Aktivierung nicht den Anforderungen der EN50131 entspricht. Wird unter der Menüoption <b>Einhaltung von Vorschriften</b> als <b>Region</b> Belgien oder Schweiz eingestellt, wird diese Option automatisch aktiviert, ist aber unter <b>Optionen</b> nicht sichtbar.</p>

Einschränkungen	Systemoptionen	Beschreibung
⏴	Alarm bei Eintrittsverzögerung	<p><b>Aktiv:</b> Wird eine nicht-verzögerte Meldergruppe aktiviert, während der Eingangs-Timer abläuft, wird ein lokaler Alarm mit Sirenen ausgelöst.</p> <p><b>Deaktiviert:</b> Wird eine nicht-verzögerte Meldergruppe aktiviert, während der Eingangs-Timer abläuft, wird kein Alarm ausgelöst.</p> <p><b>Hinweis:</b> Diese Option wird nur angezeigt, wenn der Grad <b>Unbeschränkte Konfiguration</b> ausgewählt wurde, da ihre Aktivierung nicht den Anforderungen der EN50131 entspricht. Wird unter der Menüoption <b>Einhaltung von Vorschriften</b> als <b>Region</b> die Schweiz ausgewählt, wird diese Option automatisch aktiviert, ist aber unter <b>Optionen</b> nicht sichtbar.</p>
<b>Bestätigung</b>		
⏴	Bestätigung	<p>Die Bestätigungsvariable legt fest, wann ein Alarm als bestätigter Alarm gilt.</p> <ul style="list-style-type: none"> <li>● <b>BS8243:</b> Stellt die Einhaltung der Anforderungen der britischen Polizei sicher (spezifische Anforderung für gewerbliche Installationen in GB). Die Anforderung sieht vor, dass ein Alarm nur als bestätigter Alarm gilt, wenn die folgenden Bedingungen erfüllt sind: Nachdem der erste MG-Alarm aktiviert wurde und bevor die Alarmbestätigungszeit abgelaufen ist, wird ein zweiter MG-Alarm aktiviert. Die Alarmbestätigungszeit muss zwischen 30 und 60 Sekunden lang sein. (Siehe Timer [→ 80])</li> </ul> <p>Wird innerhalb der Alarmbestätigungszeit kein zweiter Alarm aktiviert, wird der erste MG-Alarm gesperrt. Die BS8243-Bestätigungsoption wird automatisch gesetzt, wenn unter <b>Standards &gt; Region</b> die Region UK gewählt wird.</p> <ul style="list-style-type: none"> <li>● <b>Garda:</b> Stellt die Einhaltung der Richtlinien der irischen Garda für einen bestätigten Alarm sicher. Die Anforderung sieht vor, dass ein Alarm als bestätigter Alarm gilt, sobald ein zweiter MG-Alarm innerhalb des Alarmzeitraums im System aktiviert wurde. Die Garda-Bestätigungsoption wird automatisch gesetzt, wenn unter <b>Standards &gt; Region</b> die Region Irland gewählt wird.</li> <li>● <b>EN-50131-9</b> Stellt die Einhaltung der Anforderungen mit der EN-50131-9-Norm und der spanischen „Verordnung INT/316/2011 vom 1. Februar zur Bedienung von Alarmsystem für die private Sicherheit“ sicher. Diese Anforderung sieht vor, dass ein Alarm nur als bestätigter Alarm gilt, wenn die folgenden Bedingungen erfüllt sind:</li> </ul> <ul style="list-style-type: none"> <li>- 3 Aktivierungen einer Meldergruppe innerhalb von 30 Minuten (Standardwert), wobei zwei Aktivierungen vom selben Gerät stammen können, sofern die Aktivierungen von einem unterschiedlichen Typ sind, d. h. Alarm/Sabotage.</li> <li>- 1 Alarmaktivierung gefolgt von einer ATS[1]-Störung innerhalb von 30 Minuten (Standardwert).</li> <li>- ATS-Störung gefolgt von einer Sabotage oder einer Alarmbedingung innerhalb von 30 Minuten (Standardwert).</li> </ul>

Einschränkungen	Systemoptionen	Beschreibung
		<p>Wenn die Meldergruppe nach 30 Minuten wieder in den ursprünglichen physischen Zustand versetzt wird, werden die Alarme der Meldergruppe quittiert, wenn ein Benutzer der Ebene 2 diesen Alarm quittieren kann. In diesem Fall akzeptiert die Meldergruppe eine neue Alarmbedingung, die eine neue Aktivierung auslöst.</p> <p>Wenn die Meldergruppe nicht in den ursprünglichen Zustand versetzt wurde, wird die Meldergruppe gesperrt, sofern sie gesperrt werden darf.</p> <p>Wenn ein Alarm (ATS) nach einem Zeitraum von 30 Minuten (Standardwert) erneut ausgelöst wird, startet der 30-Minuten-Timer neu.</p> <p>Die EN50131-9-Bestätigungsoption wird automatisch gesetzt, wenn unter <b>Standards -&gt; Region</b> die Region „Spanien“ gewählt wird.</p> <ul style="list-style-type: none"> <li>● VDS</li> </ul> <p>Dies erzwingt die Einhaltung der VdS-Norm.</p>
<b>Bedienteil</b>		
!	Zeige Status (ZEIGE STATUS)	<p>Wenn aktiviert, wird der Schärfungszustand (Externscharf / Internscharf / Unscharf) des Systems dauerhaft in der unteren Zeile des Displays am Bedienteil angezeigt. Wenn nicht aktiviert, wird der Schärfungszustand nach 7 Sekunden ausgeblendet.</p>
	Zeige offene MG	<p>Wenn aktiviert, werden die offenen Meldergruppen im unscharfen Zustand am Bedienteil angezeigt.</p>
	Info bei Übertr	<p>Wenn aktiviert, wird für 30 Sekunden nach der Unscharfschaltung eine Nachricht angezeigt, wenn ein bestätigter Alarm übertragen wurde.</p>
	Info bei Übertr. Zeile 1	<p>Nachricht, die in der ersten Zeile des Displays angezeigt wird.</p>
	Info bei Übertr. Zeile 2	<p>Nachricht, die in der zweiten Zeile des Displays angezeigt wird.</p>
	Kamerastatus anzeigen	<p>Wenn aktiviert, werden nicht verbundene Kameras im unscharfen Zustand am Bedienteil angezeigt.</p>
	Sprache im Ruhezustand	<p>Wählen Sie die Sprache, die im Ruhezustand angezeigt werden soll.</p> <ul style="list-style-type: none"> <li>● Systemsprache: Die Sprache, in der Menüs und Texte auf den Bedienteilen, in der Webschnittstelle und im Logbuch angezeigt werden.</li> <li>● Zuletzt verwendet: Die zuletzt verwendete Sprache wird im Ruhezustand angezeigt.</li> </ul>
<b>PIN</b>		
	Pin ?-stellig	<p>Legen Sie die Anzahl der Stellen für Benutzer-PINs fest (max. 8 Stellen). Wird die Zahl der Stellen erhöht, wird bestehenden PINs eine entsprechende Anzahl von Nullen vorangestellt. Wird die Zahl der Stellen beispielsweise auf 8 eingestellt, wird aus der bestehenden Benutzer-PIN 2134 (4 Stellen) die PIN 00002134. Wird die Anzahl der PIN-Stellen verringert, werden die vorgestellten Stellen von bestehenden PINs entfernt. Wird also beispielsweise die Anzahl der Stellen auf 5 eingestellt, wird aus der bestehenden Benutzer-PIN 00002134 (8 Stellen) die PIN 02134.</p>

Einschränkungen	Systemoptionen	Beschreibung
		<p><b>Hinweis:</b> Diese Option kann nicht geändert werden, wenn ein SPC Manager-PIN-Stellen-Modus eingerichtet ist. Weitere Informationen finden Sie auf Seite [→ 87]</p> <p><b>Hinweis:</b> Zur Einhaltung der INCERT-Genehmigungen muss die Benutzer-PIN mehr als 4 Zeichen enthalten.</p>
	TP + PIN	Wenn aktiviert, werden Transponder und PIN benötigt.
	Bedrohungs-PIN	<p>Wählen Sie eine der folgenden Bedrohungs-PIN-Optionen, um die entsprechende Funktion auf dem System zu aktivieren.</p> <ul style="list-style-type: none"> <li>● PIN +1 (das System reserviert die PIN vor und nach der Benutzer-PIN als Bedrohungs-PIN)</li> <li>● PIN +2 (das System reserviert zwei PINs vor und nach der Benutzer-PIN als Bedrohungs-PINs)</li> </ul> <p>Die Bedrohungs-PIN muss für einzelne Benutzer aktiviert sein. Siehe Abschnitt Hinzufügen/Bearbeiten von Benutzern. [→ 51]</p>
	PIN-Richtlinien	<p>Klicken Sie auf die Schaltfläche <b>Bearbeiten</b>, um Optionen für die PIN-Nutzung auszuwählen.</p> <ul style="list-style-type: none"> <li>● Periodic changes required (Regelmäßige Änderungen erforderlich) – Erzwingt geplante Änderungen der Benutzer-PIN. Der Zeitraum wird im Feld <b>PIN Gültig</b> unter <b>Timer</b> definiert. Siehe Timer [→ 80].</li> <li>● Warnung, wenn Änderungen erforderlich – generiert einen Benutzerwarnung, wenn die Benutzer-PIN bald abläuft oder abgelaufen ist. Der Warnzeitraum wird im Feld <b>Pin Warnung</b> unter <b>Timer</b> definiert. Siehe Timer [→ 80].</li> <li>● User Selects the last digit (Benutzer wählt letzte Stelle) – ermöglicht es dem Benutzer, die letzte Stelle der PIN auszuwählen. Die vorhergehenden Stellen werden automatisch vom System generiert.</li> <li>● User selects the 2 digits (Benutzer wählt die letzten 2 Stellen) – Ermöglicht es dem Benutzer, die letzten zwei Stellen der PIN auszuwählen. Die vorhergehenden Stellen werden automatisch vom System generiert.</li> <li>● Limit Änderung – Beschränkt die Anzahl der möglichen Änderungen innerhalb eines gültigen PIN-Zeitraums. Dieser Wert wird im Feld <b>Limit PIN-Änderung</b> unter <b>Timer</b> definiert. Siehe Timer [→ 80]</li> <li>● Sichere PINs – Bei Aktivierung dieser Option wird die PIN automatisch von der Zentrale generiert.</li> </ul>
<b>Tür</b>		
	Karten zurücksetzen	Wenn aktiviert, werden alle Ausweise täglich um Mitternacht zurückgesetzt (Passback).
	Ignoriere Anlagen Kode	Bei Aktivierung ignoriert das Zugangssystem die Anlagencodes. Durch das Ignorieren des Anlagencodes fügen Sie nur die Ausweisnummer hinzu und erhöhen die Ausweisbenutzer im System von 100 auf 2.500.
	Ausweisformat	<p>Klicken Sie auf <b>Bearbeiten</b>, um die Ausweisformate auszuwählen, die in dieser Zentrale zugelassen werden sollen.</p> <p>Weitere Informationen zu derzeit unterstützten Ausweislesern und Ausweisformaten finden Sie im Anhang des SPC Installations- und Konfigurationshandbuch.</p> <p><b>Hinweis:</b> Die Auswahl von <b>Wiegand</b> aktiviert alle</p>

Einschränkungen	Systemoptionen	Beschreibung
		Wiegand-Ausweisformate.
Nur Web und SPC Pro	Türstatus bei scharf	Wählen Sie die erforderliche Benutzeridentifikation, um die Tür bei scharf geschaltetem Bereich zu öffnen. Verfügbare Optionen sind: <b>Standard, Karte und PIN, Karte oder PIN.</b>
Nur Web und SPC Pro	Türstatus bei unscharf	Wählen Sie die erforderliche Benutzeridentifikation, um die Tür bei unscharf geschaltetem Bereich zu öffnen. Verfügbare Optionen sind: <b>Standard, Karte und PIN, Karte oder PIN.</b>
<b>Techniker</b>		
Ⓣ	Reset durch Techniker	(Nur für Region „UK“): Wenn aktiviert, muss der Techniker bestätigte Alarme quittieren. Diese Option funktioniert in Kombination mit der Funktion „Bestätigung“.
	Techniker Austritt	Wenn aktiviert, kann der Techniker den Konfigurationsmodus verlassen, auch wenn noch Alarme aktiv sind.
Ⓣ	Technikerzugang freigeben	Aktivieren Sie diese Funktion, um sicherzustellen, dass der Techniker nur mit der Erlaubnis des Benutzers auf das System zugreifen kann. Wenn nicht aktiviert, ist die Menüoption <b>TECHNIKERZUGANG FREIGEBEN</b> nicht auf dem Bedienteil verfügbar. <b>Hinweis:</b> Nur verfügbar, wenn der Sicherheitsgrad ‚Unbeschränkt‘ ausgewählt ist. Für Grad 2 oder 3 ist die Benutzersteuerung für den Technikerzugang immer verfügbar.
Ⓣ	Herstellerezugang freigeben	Aktivieren Sie diese Funktion, um sicherzustellen, dass der Techniker nur mit der Erlaubnis des Benutzers auf das System zugreifen kann. Wenn nicht aktiviert, ist die Menüoption <b>HERSTELLERZUGANG FREIGEBEN</b> nicht auf dem Bedienteil verfügbar. <b>Hinweis:</b> Nur verfügbar, wenn der <b>Sicherheitsgrad</b> ‚Unbeschränkt‘ ausgewählt ist. Für Grad 2 oder 3 ist die Benutzersteuerung für den Technikerzugang immer verfügbar, wenn der Benutzer vom Typ ‚Manager‘ ist.
<b>SMS</b>		
	SMS-Authentifizierung	Folgende Optionen stehen zur Verfügung: <ul style="list-style-type: none"> <li>● Nur PIN: Anmeldung über eine gültige Benutzer-PIN. Siehe Seite [→ 51].</li> <li>● Nur Rufnummer: Anmeldung über die Telefonnummer (einschl. der dreistelligen Ländervorwahl), die für die Benutzer-SMS-Steuerung konfiguriert wurde. Die SMS-Steuerung zur Konfiguration durch den Benutzer steht nur zur Verfügung, wenn diese Option ausgewählt wurde.</li> <li>● PIN + Rufnummer</li> <li>● Nur SMS-PIN: Anmeldung über eine für den Benutzer konfigurierte, gültige PIN; dabei handelt es sich nicht um die Anmelde-PIN des Benutzers! Die SMS-Steuerung zur Konfiguration durch den Benutzer steht nur zur Verfügung, wenn diese Option ausgewählt wurde.</li> <li>● SMS-PIN + Rufnummer</li> </ul>
<b>Verfahrensweise</b>		

Einschränkungen	Systemoptionen	Beschreibung
Nur Web	Systemverhalten	Konfigurieren Sie die Technikeranmeldung und das Sabotagemeldeverhalten für das System.
Nur Web	Verhalten der Zeiten	Zeigen Sie das Verhalten der Zeiten an.
Nur Web und SPC Pro	Ausgangskonfiguration	Klicken Sie auf die Schaltfläche <b>Bearbeiten</b> , um Verriegelungs- und Auto-Scharfschaltungseinstellungen [→ 220] zu konfigurieren.
Nur Web Ⓣ	Systemalarme	Diese Programmieroption ermöglicht die Einschränkung der Benutzer- und Technikerrechte zum Quittieren, Abschalten und Sperren von Alarmen. Auch die Art und Weise, in der das System auf Alarme reagiert, kann programmiert werden.
Nur Web Ⓣ	Alarme von Meldergruppen	Wählen Sie, ob bestimmte Meldergruppen-Alarme vom Benutzer und vom Techniker quittiert, gesperrt oder abgeschaltet werden können.
Nur Web Ⓣ	Sabotage Meldergruppe	Wählen Sie, ob bestimmte Meldergruppen-Sabotagen vom Benutzer und vom Techniker quittiert, gesperrt oder abgeschaltet werden können.
Nur Web Ⓣ	Verhalten der Bedienteilanzeige	Wählen Sie die auf dem Bedienteil anzuzeigenden Meldungen für den scharfen und unscharfen Zustand aus.
Nur Web Ⓣ	Verhalten der LED Anzeigen am BT	Wählen Sie, welche LED auf den Bedienteilen für den scharfen und unscharfen Zustand angezeigt werden soll.
Nur Web Ⓣ	System General Policy (Allgemeine Systemrichtlinie)	Wählen Sie die folgenden Optionen, um die Fernsteuerung des Systems und die Alarm- und Sirenscharfschaltungen zu verwalten: - keine bestät. Alarme wenn internscharf - blockiere Fernrücksetzung - blockiere Fernabschaltung - blockiere Fernsperre - keine externe Sirene, wenn intern scharf - verzögerte Benachrichtigung wenn die Zutrittsverzögerung läuft - bestätigter Alarm bricht Verzögerung ab
Nur Web Ⓣ	Confirmed Alarms System Alerts (BEST.SYS.ALARM – Bestätige (System-)Alarme)	Wählen Sie aus, welche Systemalarmlisten einen bestätigten Alarm auslösen, wenn mindestens ein Alarm aktiv ist, und welcher Systemalarm bei der Zentrale den Wechsel in den Probestatus verursacht.

#### Siehe auch

- 📖 Hinzufügen/Bearbeiten von Benutzern [→ 51]
- 📖 Bereich hinzufügen/bearbeiten [→ 129]

## 9.4 Timer

Dieses Fenster bietet einen Überblick über vorhandene Standardzeiten einschließlich deren Beschreibung.



Diese Einstellungen, die je nach definiertem Sicherheitsgrad des Systems variieren, sollten nur von einem autorisierten Installationstechniker programmiert werden. Das Verändern von Einstellungen kann dazu führen, dass das SPC-System den geforderten Sicherheitsstandards nicht mehr entspricht. Beim Zurücksetzen des Systems auf Sicherheitsgrad EN 50131 Grad 2 oder EN 50131 Grad 3 werden sämtliche auf dieser Seite vorgenommenen Einstellungen überschrieben.

Zentralenkonfig.



Systemoptionen

1. Wählen Sie die Registerkarte **Timer**.  
⇒ Daraufhin erscheint das folgende Fenster.
2. Siehe die nachfolgende Tabelle für weitere Informationen.
3. Klicken Sie auf den Timer-Wert in der Spalte **Wert**.
4. Geben Sie den neuen Wert ein.

### System Timer

Timer	Wert	Einheit	Min.	Max.	Beschreibung
Innensirenen	15	Minuten	1	15	Dauer der Aktivierung der Innensirenen im Alarmfall
Außensirenen	15	Minuten	1	15	Dauer der Aktivierung der Außensirenen im Alarmfall
Verz. Außensirene	0	Sekunden	0	600	Verzögerung, bis die Außensirene nach einem Alarm aktiviert wird.
Blitzleuchte	15	Minuten	1	15	Dauer der Aktivierung des Ausgangs 'Blitzleuchte' im Alarmfall
Türglocke	2	Sekunden	1	10	Aktivierungsdauer Ausgang 'Türglocke'.
Doppelauslösung	10	Sekunden	1	99	Max. Zeit zwischen zwei Ausl. einer MG mit dem Attribut 'Doppelauslö...
Dauertest	14	Tage	1	99	Tage, die eine MG sich im Dauertest befindet, bis dieser autom. deak...
Verz. Netzstörung	0	Minuten	0	60	Minimale Dauer einer Netzstörung, bis eine Meldung generiert wird.
Verz. Übertragung	30	Sekunden	0	30	Verz.zeit nach einem Alarm, bis die Übertragung zum Empfänger gest...
BT Timeout	30	Sekunden	10	300	Wartezeit (in Sek.) auf eine Eingabe, bis das BT das akt. Menü verlässt.
Funk Scharfsch.verh.	0	Minuten	0	720	Zeit (in Min.) ohne FÜ-Meldung, nach der die Scharfsch. verhindert wird
Funküberwachung	720	Minuten	20	720	Zeit (in Min.) ohne FÜ-Meldung, nach der Melder als 'fehlt' gemeldet ...
Timeout Technikerfreig.	0	Minuten	0	999	Zeit (in Min.), nach der Technikerzugang automatisch wieder gesperr...
Scharfsch.quitt. Sirene	0	Sekunden	0	10	Sirene kurzzeitig zur Quittierung der externen Scharfschaltung aktivi...
Scharfsch.quitt. Blitzl...	0	Sekunden	0	10	Blitzleuchte kurzzeitig zur Quittierung der externen Scharfschaltung a...
Ext. Zeitabbruch	7	Sekunden	1	45	Zeit (in Sek.), nach der nach Schließen des Eingangs Scharfsch. erfolgt.
Verzögerung Technik	0	Sekunden	0	9999	Dauer (in Sek.), die eine Technik-MG verzögert ist.
Scharfsch. fehlg.	10	Sekunden	0	999	Zeit in Sek. für die 'Scharfsch. fehlgeschl.' am BT angez. wird (0 = bis...
Überwachungszeit	336	Stunden	1	9999	Zeit innerhalb der die MG mit 'Überwacht' Attribut aktiviert werden muss
Feuer-Voralarm	30	Sekunden	1	999	Zeitspanne (in Sek.), in der auf Bestätigung/Abbruch des Feueralarm...
Feuer-Erkennungzeit	120	Sekunden	1	999	Zeitspanne (in Sek.), in der auf Bestätigung/Abbruch des Feueralarm...

Klicken Sie auf den Wert des Timers um diesen zu bearbeiten... Jeder Timer hat einen min. und max. Wert, der beachtet werden muss...

### Timer

Die Funktionen werden in der nachstehenden Reihenfolge zugeordnet:

- 1<sup>st</sup> Zeile: Web/SPC Pro
- 2. Zeile: Bedienteil

Timer	Beschreibung	Rücksetzen
<b>Bedient. Summer</b>		
Innensirenen ZEIT INNENSIR	Dauer der Aktivierung der Innensirenen im Alarmfall (1 – 15 Minuten: 0 = niemals)	15 Min.

Timer	Beschreibung	Rücksetzen
Außensirenen ZEIT AUSSENSIR	Dauer der Aktivierung der Außensirenen im Alarmfall (1–15 Minuten: 0 = niemals)	15 Min.
Verzögerung Außensirene VERZ AUSSENSIR	Bewirkt eine verzögerte Aktivierung der Außensirene. (0–600 Sekunden)	0 Sek.
Türglocke ZEIT TÜRGLOCKE	Dauer, für die der Ausgang Türglocke aktiviert wird, wenn eine Meldergruppe mit dem Attribut Türglocke ausgelöst wird. (1–10 Sekunden)	2 Sek.
<b>Bestätigung</b>		
Confirm ZEIT BEST ALARM	<ul style="list-style-type: none"> <li>● <b>Hinweis:</b> Nur verfügbar, wenn der Sicherheitsgrad „Unbeschränkt“ und „DD243“ für die Bestätigungsvariable ausgewählt ist. (Siehe Systemoptionen [→ 71].)</li> </ul> Bezieht sich auf die Alarmbestätigungsfunktion: maximale Zeit zwischen den Auslösungen zweier unabhängiger Meldergruppen, die einen bestätigten Alarm generieren. (30–60 Minuten)	30 Min.
Bestätigter Überfall	Dieser Timer bezieht sich auf die Funktion für bestätigte Bedrohungen und ist als die maximale Zeit zwischen den Alarmen zweier nicht überlappender Meldergruppen definiert, die einen bestätigten Alarm generieren. (480–1200 Minuten)	480 min
Verzögerung Übertragung VERZ ÜBERTRAGUNG	Die Verzögerungszeit nach einem Alarm (0 - 30 Sek.), bis die Übertragung zum Empfänger gestartet wird. Dies dient insbesondere der Verringerung ungerechtfertigter Reaktionen seitens des Empfängers und der Polizei. Wird eine weitere Meldergruppe ausgelöst, wird die Übertragungsverzögerung ignoriert, und die Übertragung beginnt sofort. (0–30 Sekunden)	30 Sek.
Alarmabbruch ALARMABBRUCH	Zeit nach einem gemeldeten Alarm, in der eine Alarmabbruchmeldung gesendet werden kann. (0–999 Sekunden)	30 Sek.
<b>Einstellung</b>		
Scharfschalteberechtigung SCHARFSCH. BER.	Zeitraum, in dem die Scharfschalteberechtigung gültig ist. Geben Sie einen Wert zwischen 10 und 250 Sekunden ein.	20 Sek.
Extern Zeitabbruch EXT ZEITABBRUCH	Zeit (in Sek.), um welche die Scharfschaltung verzögert wird, nachdem eine Meldergruppe, für die das Attribut Extern Zeitabbruch gesetzt ist, geschlossen wird. (1–45 Sekunden)	7 Sek.
Scharfschquitt Sirene SCHARF QUITT SIR	Sirene wird zur Quittierung der externen Scharfschaltung kurzzeitig aktiviert. (1–10 Sekunden)	0 Sek.
Scharfschquitt Blitzleuchte SCHARF QU BLITZ	Blitzleuchte an der Außensirene wird zur Quittierung der externen Scharfschaltung kurzzeitig aktiviert. (1–10 Sekunden)	0 Sek.
Scharfsch fehlg. SCHARFSCH FEHLG	Zeit (in Sek), für die eine Meldung Scharfschaltung fehlgeschlagen am Bedienteil angezeigt wird (0 = bis gültige PIN eingegeben wird). (0 – 999 Sekunden)	10 Sek.
<b>Alarm</b>		
Doppelauslösung ZEIT DOPPELAUSL	Max. Zeit (in Sek.) zwischen 2 Auslösungen einer Meldergruppe mit dem Attribut Doppelauslösung, sodass ein Alarm generiert wird. (1–99 Sekunden)	10 Sek.
Dauertest TAGE DAUERTEST	Anzahl der Tage, die eine Meldergruppe im Dauertest verweilt, bis der Dauertest automatisch deaktiviert wird. (1–99 Tage)	14 Tage
Körperschallmelder Autotestzeit KSM AUTOTST	Der durchschnittliche Zeitraum zwischen automatischen Tests der Körperschallmelder (12–240 Stunden). <b>Hinweis:</b> Zur Aktivierung der automatischen Tests muss das Attribut <b>Automatischer Meldertest</b> für eine Körperschall-MG aktiviert sein.	168 Stunden.

Timer	Beschreibung	Rücksetzen
Dauer von KS Test KSM TESTZEIT	Maximale Zeit (in Sekunden), die ein Körperschallmelder benötigt um einen Alarm aufgrund des Körperschalltest-Ausgangs auszulösen. (3–120 Sekunden)	30 Sek.
Kein Zutritt erlaubt nach Alarm KEIN ZUTRITT ERLAUBT NACH ALARM	Dauer, für die der Zugang nach dem Alarm verweigert wird.	0 Min.
Blitzleuchte ZEIT BLITZL	Dauer, für die der Ausgang Blitzleuchte bei einem Alarm aktiviert wird. (1–15 Minuten: 0 = unendlich)	15 Min.
<b>ALARME</b>		
Verz Netzstörung VERZ STÖR NETZ	Die Verzögerungszeit nach einer erkannten Netzstörung, bis das System einen Alarm aktiviert. (0–60 Minuten)	0 min.
<b>Techniker</b>		
Technikerzugang ZUGANG TECHNIKER	Der Timer für den Technikerzugang läuft, sobald der Benutzer den Zugang aktiviert hat. (0–999 Minuten. 0 = keine Zeitbeschränkung für Systemzugang)	0 min.
Automatische Abmeldung des Technikers AUTO. ABMELDEN	Dauer der Inaktivität, nach der der Techniker automatisch abgemeldet wird	0 Min.
<b>Bedienteil</b>		
Bedienteil Timeout BEDIENT TIMEOUT	Die Zeitspanne in Sekunden, die das Bedienteil auf eine Eingabe wartet, bis es das aktuell angezeigte Menü verlässt. (10–300 Sekunden)	30 Sek.
Sprache Bedienteil EINSTELLEN DER SPRACHE	Die Zeitspanne in Sekunden, die das Bedienteil wartet, bevor es die Sprache auf Standardeinstellung wechselt. (0–9999 Sekunden; 0 = nie).	10 Sekunden
<b>Feuer</b>		
Feuer Voralarm FEUER VORALARM	Wartezeit in Sekunden, bis ein Feueralarm für MGs mit dem Attribut ‚Feuer Voralarm‘ gemeldet wird. (1–999 Sekunden) Siehe Meldergruppe bearbeiten [→ 127].	30 Sek.
Branderkennung BRANDERKENNUNG	Zusätzliche Wartezeit, bevor ein Feueralarm für MGs mit dem Attribut „Feuer Voralarm“ und „Feuer Erkundungszeit“ gemeldet wird. (1–999 Sekunden). Siehe Meldergruppe bearbeiten [→ 127].	120 Sek.
<b>PIN</b>		
Pin gültig PIN GÜLTIG	Zeitraum (in Tagen), in dem die PIN gültig ist (1–330)	30 Tage
Limit PIN-Änderung LIMIT PIN- ÄNDERUNG	Anzahl der Änderungen innerhalb eines gültigen Zeitraums (1–50)	5
PIN Warnung PIN WARNUNG	Zeitraum nach dem PIN-Ablauf, bis eine Warnung angezeigt wird. ( 1 - 14 )	5 Tage
<b>Allgemeine Einstellungen</b>		
Zeit Funk Ausgang FUNKAUSGANG	Die Dauer, für die der Funkausgang im System aktiv bleibt. (0 – 999 Sekunden)	0 Sek.
Zeit synch.Limit SYNCH-ZEIT LIMIT	Zeitraum, in dem kein Ereignis gemeldet wird. (0–999 Sek.) Zeitsynchronisierung findet nur statt, wenn die Systemzeit und Aktualisierungszeit außerhalb dieses Grenzwerts liegen.	0 s
Verb. abgelaufen VERB. ABGELAUFEN	Zeitüberschreitung für Ethernet-Verbindungsstörung (0 = Deaktiviert) (0–250)	0 Sek.

Timer	Beschreibung	Rücksetzen
Kamera Offline KAMERA OFFLINE	Zeit, nach der die Kamera offline geht (10–9999)	10 Sekunden
Verzögerung Technik TECHNIK VERZÖGERUNG	Zeit (in Sek), um die eine Technik-Meldergruppe verzögert ist, falls das entsprechende Attribut für die MG gesetzt ist. (0–9999 Sekunden)	0 Sek.
Überwacht ÜBERWACHT ⓘ	Dieses Attribut bezieht sich nur auf die Fernwartung. Zeitfenster, in dem die Meldergruppe mit gesetztem Attribut <b>Überwacht</b> geöffnet werden muss. (1–9999 Stunden)	336 Stunden (2 Wochen)
Stiller Bedrohungsalarm	Die Dauer (0–999) für die ein Bedrohungsalarm still bleibt und auf dem Bedienteil nicht wiederhergestellt werden kann.	0 Minuten
Bedrohung/ Panik still	Die Anzahl der Minuten (0–999), die ein Bedrohungs-/Panikalarm still bleibt und auf dem Bedienteil nicht wiederhergestellt werden kann.	0 Minuten



Die vorgegebenen Zeiten (Standardeinstellungen) sind von der Technikerkonfiguration abhängig. Die angegebenen Standardzeiten können daher zulässig sein oder nicht, je nach Konfiguration durch den zuständige Techniker.

## 9.5 Uhrzeit

In diesem Fenster können das Datum und die Uhrzeit des Systems eingestellt werden. Der Controller enthält eine batteriegepufferte Echtzeituhr (**Real-Time Clock, RTC**), die sicherstellt, dass Datum und Uhrzeit auch bei einem Ausfall der Stromversorgung im System erhalten bleiben.

Zentralenkonfig.



Systemoptionen

1. Klicken Sie auf die Registerkarte **Uhr** .  
⇒ Daraufhin erscheint das folgende Fenster:

## Datum/Uhrzeit

**Datum/Uhrzeit**

Uhrzeit :

Datum :

Autom. Umst. Sommer/Winterzeit

Zeit mit Netz synchr.

2. Wählen Sie **Uhrzeit** und **Datum** aus den Dropdown-Menüs aus.  
- ODER -  
Klicken Sie auf die Schaltfläche **PC Datum/Uhrzeit übernehmen**, um Datum und Uhrzeit vom angeschlossenen PC zu übernehmen.
3. Klicken Sie auf die Schaltfläche **An Zentrale senden**, um das Datum und die Uhrzeit an die Zentrale zu senden.
4. Konfigurieren Sie die folgenden Felder:

Automatische Umstellung Sommer/Winterzeit	Wenn aktiviert, schaltet das System automatisch zwischen Sommer- und Winterzeit um.
Zeit mit Netzspannung synchronisieren	Wenn aktiviert, synchronisiert sich die Echtzeituhr selbstständig mit der Sinuswelle im Stromnetz (Zeitsignal).



Die aktuelle gewählte Uhrzeit und das Datum werden am Bedienteil, in der Webschnittstelle und im Logbuch angezeigt.

## 9.6 Sprache

Zentralenkonfig.



Systemoptionen

1. Klicken Sie auf die Registerkarte **Sprache**.  
⇒ Das folgende Fenster wird angezeigt:

Sprachoptionen

Sprache

Deutsch

Wählen Sie die Sprache, die für das BT und das Webinterface verwendet wird.

2. Wählen Sie eine Sprache aus dem Dropdown-Menü.

⇒ Die Texte auf den Bedienteilen, in der Webschnittstelle und im Logbuch werden in der ausgewählten Sprache angezeigt.

Die in der Dropdown-Liste **Sprache** verfügbaren Sprachen sind von den im System definierten Sprachen abhängig. Wenn Sie eine Verbindung mit der Zentrale hergestellt und die Konfigurationsdatei heruntergeladen haben, werden alle Sprachen angezeigt. Wenn Sie die Konfigurationsdatei von der Zentrale heruntergeladen haben, werden in der Dropdown-Liste **Sprache** nur die im System verfügbaren Sprachen angezeigt.



Die Sprache, die von den Bedienteilen und dem Browser benutzt wird, wird von der individuell für jeden Benutzer konfigurierten Sprachauswahl bestimmt. Wenn z. B. Französisch als Systemsprache konfiguriert wurde, aber als individuelle Sprache des Benutzers Englisch definiert wurde, wird sowohl auf den Bedienteilen als auch im Browser Englisch benutzt, unabhängig von der eingestellten Systemsprache.

## 9.7 SPC Pro / SPC Safe

Kommunikation



SPC Pro / SPC Safe

### SPC Pro

1. Klicken Sie auf die Schaltfläche **SPC Pro / SPC Safe**.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

Aktivieren	Aktivieren, damit SPC Pro eine Verbindung mit der Zentrale herstellen kann.
Technikerzugang	Aktivieren, wenn der Technikerzugang freigegeben sein muss, damit SPC Pro eine Verbindung zur Zentrale herstellen kann.
Passwort	Geben Sie das Passwort für den SPC Pro-Zugang ein. Die Zentrale überprüft das Passwort jedes Mal, wenn SPC Pro eine Verbindung zur Zentrale herstellen will. Stimmt das Passwort in diesem Feld mit dem auf der Zentrale hinterlegten Passwort überein, wird

	die Verbindung zugelassen (Standard = )
IP aktivieren	Aktivieren, um über das Internet Protocol (IP) eine Verbindung mit der Zentrale herzustellen.
IP-Port	IP-Port eingeben, über den SPC Pro die Verbindung mit der Zentrale herzustellen.

### SPC Safe

Weitere Informationen über die Konfiguration von SPC Safe finden Sie im *SPCS410 Installations- und Konfigurationshandbuch*.

1. Klicken Sie auf die Schaltfläche **SPC Safe aktivieren**.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben. 15.2

Aktivieren	Aktivieren, damit Pro eine Verbindung mit der Zentrale herstellen kann.
Technikerzugang	Aktivieren, wenn der Technikerzugang freigegeben sein muss, damit Pro eine Verbindung zur Zentrale herstellen kann.
Passwort	Geben Sie das Passwort für den Pro-Zugang ein. Die Zentrale überprüft das Passwort jedes Mal, wenn Pro eine Verbindung zur Zentrale herstellen will. Stimmt das Passwort in diesem Feld mit dem auf der Zentrale hinterlegten Passwort überein, wird die Verbindung zugelassen (Standard = )
Installations-ID	Numerische ID der Installation eingeben (kann auch auf der Systemidentifikationsseite eingestellt werden).
Update aktivieren	Aktivieren, um zuzulassen, dass die Zentrale den Server kontaktiert, nachdem die Konfiguration geändert wurde.
Update Timer	Zeit in Minuten eingeben, innerhalb derer die Zentrale nach einer Änderung der Konfiguration den Server kontaktieren soll, um die Konfiguration zu aktualisieren (min.: 1, max.: 120).
IP aktivieren	Aktivieren, um über das Internet Protocol (IP) eine Verbindung mit der Zentrale herzustellen.
TCP/IP-Port	IP-Port eingeben, über den SPC Safe die Verbindung mit der Zentrale herstellt (= IP-Port der Zentrale).
Server-Adresse	Host-Name, URL oder IP-Adresse des SPC Safe-Servers eingeben (z.B. die IP-Adresse Ihres PCs).
Server TCP/IP-Port	TCP-Port des SPC-Servers eingeben (z. B. den IP-Port Ihres PCs).

## 9.8 SPC Manager

Im Einstellungsmodus von SPC Manager wird die Anzahl der Stellen für Benutzer-PINs und damit die Anzahl der verfügbaren PINs in einem globalen System festgelegt, das von SPC Manager gesteuert wird.

Mode41: 4-stellige PIN, max. 1.000 globale Anwender

Mode51: 5-stellige PIN, max. 10.000 globale Anwender

Modus61: 6-stelliger PIN, max. 100,000 Globale Anwender

Modus71: 7-stelliger PIN, max. 1000,000 Globale Anwender

Modus81: 8-stelliger PIN, max. 10.000.000 Globale Anwender

Wenn Sie eine SPC Manager-Betriebsart festlegen, werden den 4- oder 5-stelligen Benutzer-PINs zusätzliche Nullen vorangestellt, um die PIN für eine globale Nutzung anzupassen. Beispiel: Wenn **Betriebsart71: 7-Stellen PIN** ausgewählt

wird, werden den vorhanden 4-stelligen PINs 3 Nullen vorgestellt – 2222 wird dann zu 0002222.

Festlegen der SPC Manager-Betriebsart:

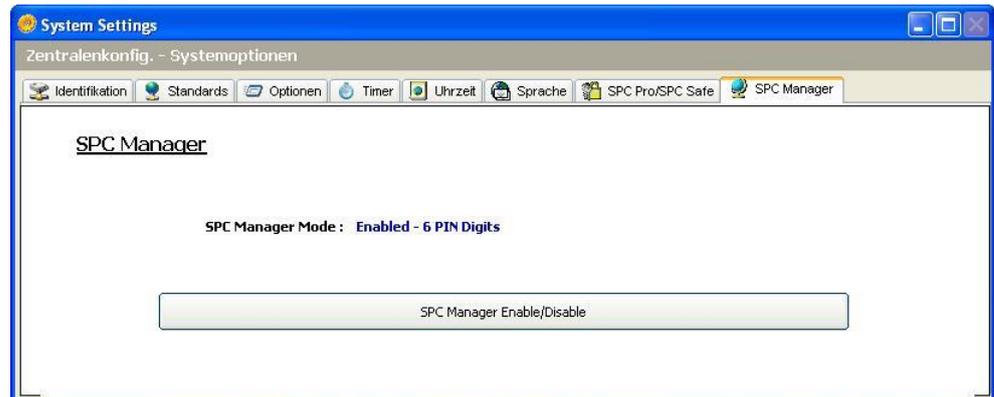
**Zentralenkonfig.**



Systemoptionen

1. Wählen Sie die Registerkarte **SPC Manager**.

⇒ Das folgende Fenster wird angezeigt:



2. Klicken Sie auf **SPC Manager Enable/Disable (SPC Manager Zu/ Abschalten)**.

3. Wählen Sie im angezeigten Dialog aus der Dropdown-Liste den Modus für den globalen Anwender von SPC Manager aus.

4. Klicken Sie auf **OK**.



#### **HINWEIS**

SPC Manager-Betriebsarten können nicht geändert werden, wenn globale Benutzer auf dem System vorhanden sind.

# 10 Ein-/Ausgänge der Zentrale konfigurieren

## 10.1 Ausgang bearbeiten

Zentralenkonfig.



Ein- & Ausgänge der  
Zentrale

1. Klicken Sie auf die Registerkarte **Eingänge**.

⇒ Daraufhin erscheint das folgende Fenster:

Zentralenkonfig. - Ein-/ Ausgänge der Zentrale

Eingänge | Ausgänge

Eingänge der Zentrale

Eing.	Endwiderstand	Analysed	Pulse Count	Gross Attack	MG	Beschreibung	Typ	Attribute	Bereich
1	Endw. 4K7/4K7		0	0	1	Front door	Einbruch verzög	✓	1 - 1
2	Endw. 4K7/4K7	✓	5	5	2	Sitting room	Einbruch	✓	1 - 1
3	Endw. 4K7/4K7	✓	5	5	3	Kitchen	Einbruch	✓	1 - 1
4	Endw. 4K7/4K7	✓	5	5	4	Upstairs front	Einbruch	✓	1 - 1
5	Endw. 4K7/4K7	✓	5	5	5	Upstairs rear	Einbruch	✓	1 - 1
6	Endw. 4K7/4K7		0	0	6	PIR Hallway	Einbruch	✓	1 - 1
7	Endw. 4K7/4K7		0	0	7	PIR Landing	Einbruch	✓	1 - 1
8	Endw. 4K7/4K7		0	0	8	Panic button	Überfall		1 - 1

Endwiderst. aller Eingänge ändern

2. Klicken Sie auf die Schaltfläche zum Ändern der Endwiderstandskonfiguration für alle Eingänge (Controller und Erweiterungen).



Achten sie darauf, dass die eingegebene Endwiderstandskonfiguration der tatsächlichen Konfiguration entspricht. Sollte dies nicht der Fall sein, kann es sein, dass Meldergruppen nicht einwandfrei funktionieren.

3. Klicken Sie auf einen Eingang in der Liste.

⇒ Daraufhin erscheint das folgende Fenster.

4. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

5. Klicken Sie auf **OK**.

Eingang der Erweiterung bearbeiten

## Eingang der Erweiterung bearbeiten 1

Eingangseinstellungen konfigurieren

**Eing.:** 1

**Endwiderstand:** Endw. 4K7/4K7

**Analysed:**

**Pulse Count:** 0

**Gross Attack:** 0

**MG:** 1

**Beschreibung:** Front door

**Typ:** S/U Eingang

**Bereich:** 1 - Reception

**Attribute**

<input type="checkbox"/>		Folgt. Verz.	<input type="checkbox"/>		Tastend
<input type="checkbox"/>		Nicht Intern A	<input type="checkbox"/>		Nur übertr.
<input type="checkbox"/>		Nicht Intern B	<input type="checkbox"/>		Ext. Zeitabtr.
<input type="checkbox"/>		24 Stunden	<input checked="" type="checkbox"/>		Ext. scharf erlaubt
<input type="checkbox"/>		Lokal	<input checked="" type="checkbox"/>		Unscharf erlaubt
<input type="checkbox"/>		Doppelausl.	<input type="checkbox"/>		Shunt
<input type="checkbox"/>		Türglocke	<input type="checkbox"/>		Übertragen
<input checked="" type="checkbox"/>		Sperrbar	<input type="checkbox"/>		Anzeigen am BT
<input type="checkbox"/>		Normal offen	<input type="checkbox"/>		Bedient. Summer
<input type="checkbox"/>		Still	<input type="checkbox"/>		Verzögert
<input type="checkbox"/>		Log	<input type="checkbox"/>		Übertr. nur bei scharf
<input type="checkbox"/>		Überwacht	<input type="checkbox"/>		Feuer Voralarm
<input type="checkbox"/>		Info vor Scharfsch.	<input type="checkbox"/>		Feuer Erkundungszeit
<input type="checkbox"/>		Automatischer	<input type="checkbox"/>		Unsch. lokal
<input checked="" type="checkbox"/>		Verz. Schärfung	<input checked="" type="checkbox"/>		Erzwungen Scharf

OK Abbrechen

Eingang	Diese Nummer wird als Referenz angezeigt und kann nicht programmiert werden.
Endwiderstand	Wählen Sie den Endwiderstand für den MG-Eingang (Werkseinstellung: 4K7).
Analysed	Wird angezeigt, wenn es sich bei dem Melder um einen Vibrationskontakt handelt.
Pulse count	Die in der Zentrale programmierte Pulszahl, bei der ein Alarm durch einen Vibrations-/Stoßmelder ausgelöst wird.
Gross Attack	Auf der Zentrale eingestellte Gross Attack, bei der ein Alarm von einem Vibrationskontakt ausgelöst wird.
Meldergruppe	Nummer der MG auf der Zentrale
Beschreibung	Geben Sie hier einen Beschreibungstext für den Eingang ein (max. 16 Zeichen). Dieser Text erscheint auch im Browser und im Bedienteil.
Typ	Der Typ der MG (siehe Seite [→ 278]).
Bereich	Nur wenn im Menü "Zentralenkonfig. > Systemoptionen > Optionen" die Option "(mehrere) Bereiche" aktiviert ist. Wählen Sie die Bereiche aus, denen diese Meldergruppe zugewiesen ist.
Attribute	Ein Symbol in diesem Feld zeigt an, dass Attribute für die MG programmiert wurden (siehe Seite [→ 91]).

### 10.1.1 MG-Einstellungen: Attribute

Jeder Meldergruppe der SPC kann ein Attribut zugewiesen werden, das die Eigenschaften dieser Meldergruppe bestimmt.  
Zuweisen eines Attributs zu einer Meldergruppe:



1. Klicken Sie auf die Registerkarte **Eingänge**.
  2. Klicken Sie auf einen Eingang in der Liste.
- ⇒ Daraufhin erscheint das folgende Fenster:



1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Attribut.
2. Klicken Sie auf **OK**.



Die auf dieser Seite angezeigten Attribute hängen vom ausgewählten Meldergruppen-Typ ab. Eine Liste der zuweisbaren Attribute finden Sie auf Seite [→ 284].

## 10.2 Bearbeiten eines Ausgangs

Zentralenkonfig.



Ein- & Ausgänge der  
Zentrale

1. Klicken Sie auf die Registerkarte **Ausgänge**.  
⇒ Daraufhin erscheint das folgende Fenster:

Ausgänge der Zentrale

Ausgang	Beschreibung	Typ	Zugewiesen als:	Typ	Invertieren	Log
1	Ext. Bell	<Systemausgang>	Systemausgang - [Außensirene]	Durchgängig		
2	Int. Bell	<Systemausgang>	Systemausgang - [Innensirene]	Durchgängig		
3	Strobe	<Systemausgang>	Systemausgang - [Blitzleuchte]	Durchgängig		
4	Fullset	<Systemausgang>	Systemausgang - [Extern scharf]	Durchgängig		
5	Alarm	<Systemausgang>	Systemausgang - [Einbruch]	Durchgängig		
6	Alarm Confirmed	<Systemausgang>	Systemausgang - [Einbruch best...]	Durchgängig		

Ausgang testen:  1  2  3  4  5  6

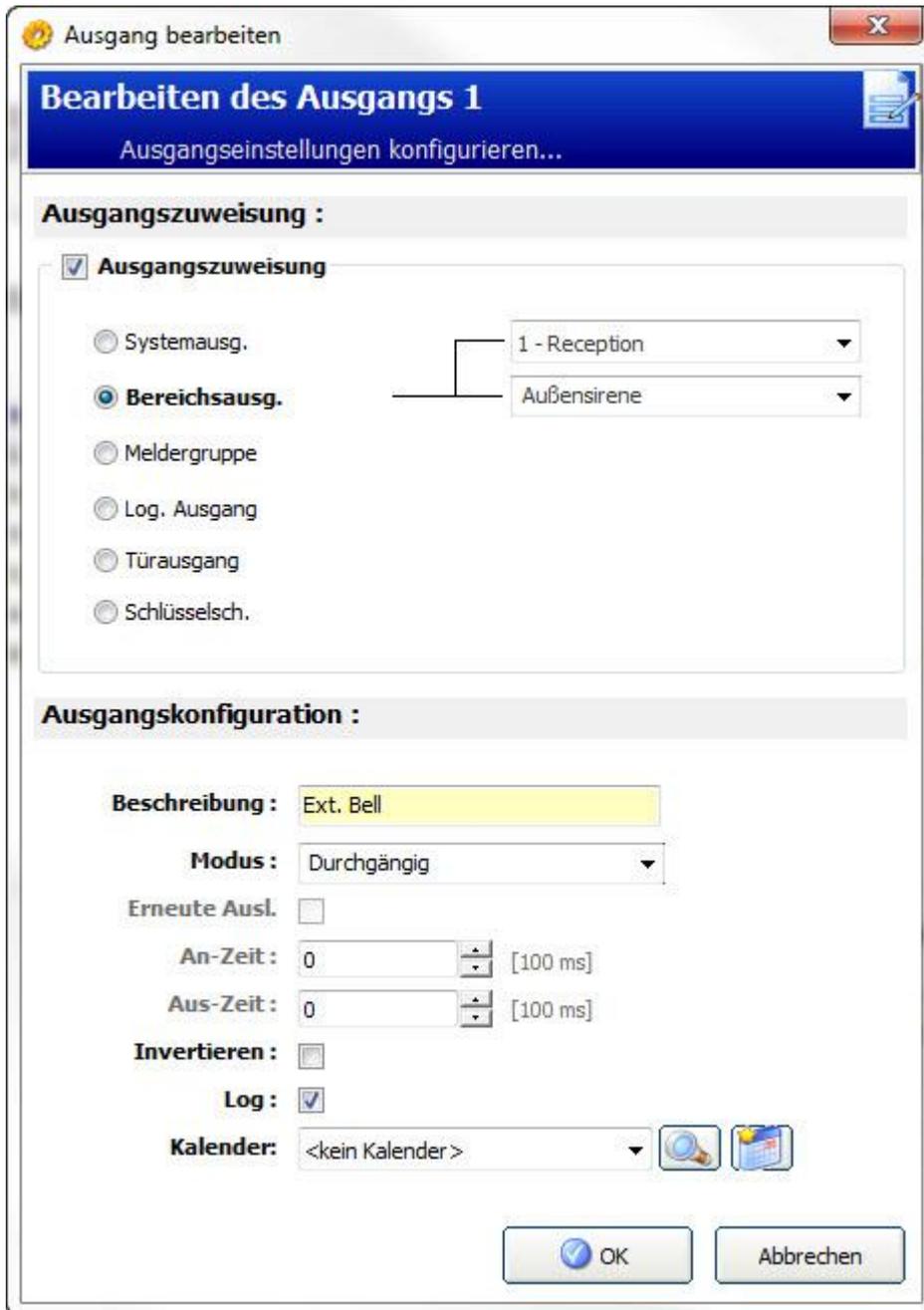
Ausgangsstatus aktualisieren

2. Klicken sie auf die Schaltfläche **Ausgangsstatus aktualisieren**.
3. Klicken Sie auf die Schaltfläche **Ausgang testen**, um zu prüfen, ob der jeweilige Ausgang korrekt angeschlossen ist (die Lampe leuchtet auf).



Die Funktion **Ausgang testen** steht nur im Konfigurationsmodus zur Verfügung.

4. Klicken Sie auf einen Ausgang in der Liste.  
⇒ Daraufhin erscheint das folgende Fenster.
5. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.
6. Klicken Sie auf **OK**.



Ausgangstyp	<ul style="list-style-type: none"> <li>● <b>Systemausgang:</b> Wählen Sie den Typ aus dem Dropdown-Menü. (Siehe Ausgangstypen und Ausgangsschnittstellen [→ 94].)</li> <li>● <b>Bereichsausgang:</b> Nur wenn im Menü <b>Zentralenkonfig &gt; Systemoptionen &gt; Optionen (mehrere) Bereiche</b> aktiviert ist. Wählen Sie einen Bereich und den Systemausgangstyp für diesen Bereich. (Siehe Ausgangstypen und Ausgangsschnittstellen [→ 94].)</li> <li>● <b>Meldergruppe:</b> Wählen Sie die Meldergruppe, die zugewiesen werden soll.</li> <li>● <b>Log Ausgang:</b> Wählen Sie den logischen Ausgang, der zugewiesen werden soll.</li> <li>● <b>Türausgang:</b> Wählen Sie die Türnummer und den Systemausgangstyp für die Tür. (Siehe Ausgangstypen und Ausgangsschnittstellen [→ 94].)</li> <li>● <b>Schlüsselsch.:</b> Wählen Sie die Erw-ID für den erforderlichen Schüsselschalter und die erforderliche Schlüsselstellung, die diesem Ausgang zugewiesen wird.</li> </ul>
Beschreibung	Geben Sie hier einen Beschreibungstext für den Ausgang ein (max. 16 Zeichen). Dieser Text erscheint auch im Browser und im Bedienteil.
Ausgangskonfiguration	<ul style="list-style-type: none"> <li>● <b>Modus:</b> Auswahl des Betriebsmodus. Durchgängig folgt dem Eingangstyp, Pulsierend schaltet an und aus, wenn der Ausgangstyp aktiv ist, Kurzzeitig</li> </ul>

	<p>erzeugt einen Puls, wenn der Ausgangstyp aktiviert wird.</p> <ul style="list-style-type: none"> <li>● <b>Erneute Ausl.:</b> Aktivieren Sie dieses Kontrollkästchen, um den kurzzeitigen Ausgang erneut auszulösen.</li> <li>● <b>AN-Zeit:</b> Geben Sie die AN-Zeit für kurzzeitige und pulsierende Ausgänge ein.</li> <li>● <b>AUS-Zeit:</b> Geben Sie die AUS-Zeit für kurzzeitige und pulsierende Ausgänge ein.</li> <li>● <b>Invertieren:</b> Aktivieren Sie dieses Kontrollkästchen, um den physischen Ausgang zu invertieren.</li> <li>● <b>Log:</b> Aktivieren Sie dieses Kontrollkästchen, um die Zustandsänderungen des Ausgangs im Logbuch zu erfassen.</li> <li>● <b>Kalender:</b> Wählen Sie bei Bedarf den gewünschten Kalender. Siehe Seite [→ 209].</li> </ul>
--	--

### Siehe auch

 Kalender [→ 209]

## 10.2.1 Ausgangstypen und Ausgangsschnittstellen

Jeder Ausgangstyp kann einem der 6 physischen Ausgangsschnittstellen am SPC-Controller oder einem Ausgang an einem der angeschlossenen Erweiterungsmodule zugewiesen werden. Ausgangstypen, die nicht physischen Ausgängen zugewiesen werden, dienen als Ereignisanzeiger im System und können protokolliert und/oder an entfernte Empfänger weitergeleitet werden, falls erforderlich.

Bei den Ausgangsschnittstellen an den Erweiterungsmodulen handelt es sich ausschließlich um einpolige Relaisausgänge (NO, COM, NC); daher kann es sein, dass die Ausgabegeräte zur Aktivierung eine externe Stromquelle benötigen, wenn sie mit Ausgängen an Erweiterungsmodulen verdrahtet sind.

Die Aktivierung eines bestimmten Ausgangstyps hängt vom Meldergruppentyp ab (siehe Seite [→ 278]) oder vom Alarmzustand, der die Aktivierung ausgelöst hat. Werden im System mehrere Bereiche definiert, werden die Ausgänge an der SPC in Systemausgänge und Bereichsausgänge gruppiert; die Systemausgänge werden aktiviert, um ein systemweites Ereignis (z. B. eine Störung der Netzstromversorgung) anzuzeigen, Bereichsausgänge zeigen Ereignisse an, die in einem oder mehreren der definierten Bereiche des Systems gemeldet wurden. Jeder Bereich verfügt über eine Anzahl eigener Bereichsausgänge; handelt es sich bei dem Bereich um einen gemeinsamen Bereich für mehrere andere Bereiche, zeigen seine Eingänge den Status aller Bereiche an, denen er als gemeinsamer Bereich zugewiesen ist, einschließlich seines eigenen Status. Beispiel: Ist Bereich 1 der gemeinsame Bereich für die Bereiche 2 und 3, und ist der Ausgang Bereich 2 Außensirene aktiv, ist auch der Ausgang Bereich 1 Außensirene aktiv.



Einige Ausgangstypen können nur systemweite Ereignisse anzeigen (keine bereichsbezogenen Ereignisse). Weitere Informationen entnehmen Sie bitte der folgenden Tabelle.

Ausgangstyp	Beschreibung
Außensirene	<p>Dieser Ausgangstyp dient der Aktivierung der Außensirene; er ist aktiv, wenn eine beliebige Außensirene des Bereichs aktiv ist. Dieser Ausgang wird standardmäßig dem ersten Ausgang an der Controller-Platine zugewiesen (EXT+, EXT-).</p> <p><b>Hinweis:</b> Ein Außensirenen-Ausgang wird automatisch aktiviert, sobald eine als Alarm-MG programmierte MG im Modus Extern Scharf oder Intern Scharf auslöst.</p>
Blitzleuchte	<p>Dieser Ausgangstyp dient der Aktivierung der Blitzleuchte; er ist aktiv, wenn eine beliebige Blitzleuchte des Bereichs aktiv ist. Dieser Ausgang wird standardmäßig dem Blitzleuchten-Relaisausgang (Ausgang 3) an der Controller-Platine zugewiesen (NO, COM, NC).</p>

	<b>Hinweis:</b> Ein Blitzleuchten-Ausgang wird automatisch aktiviert, sobald eine als Alarm-MG programmierte MG im Modus Extern Scharf oder Intern Scharf auslöst. Die Blitzleuchte wird bei Scharfsch. fehlgeschlagen aktiviert, falls Blitzleuchte für die Option Scharfsch. fehlgeschlagen in den Systemoptionen ausgewählt wurde.
Innensirene	Dieser Ausgangstyp dient der Aktivierung der Innensirene des Systems; er ist aktiv, wenn eine beliebige Innensirene des Bereichs aktiv ist. Dieser Ausgang wird standardmäßig dem zweiten Ausgang an der Controller-Platine zugewiesen (INT+, INT-). <b>Hinweis:</b> Ein Innensirenen-Ausgang wird automatisch aktiviert, sobald eine als Alarm-MG programmierte MG im Modus Extern Scharf oder Intern Scharf auslöst. Die Innensirene wird bei ‚Scharfsch. fehlgeschlagen‘ aktiviert, falls Sirene für die Option ‚Scharfsch. fehlgeschlagen‘ in den Systemoptionen ausgewählt wurde.
Alarm	Wird aktiviert, nachdem eine Alarm-MG im System oder ein im System angelegter Bereich ausgelöst hat.
Einbruch bestät.	Wird aktiviert, nachdem ein Alarm bestätigt wurde. Ein Alarm ist bestätigt, wenn zwei unabhängige Meldergruppen im System (oder innerhalb des gleichen Bereichs) innerhalb einer festgesetzten Zeitspanne auslösen.
Überfall*	Wird nach Auslösen von Überfallalarm-Meldergruppen in einem beliebigen Bereich aktiviert. Ein Überfallalarm-Ausgang wird auch generiert, wenn ein Bedrohungsalarm oder die Überfall-Option am Bedienteil aktiviert wird.
Bedrohung	Wird aktiviert, wenn eine als Bedrohungs-MG programmierte MG einen Alarm für einen beliebigen Bereich auslöst.
Feuer	Wird aktiviert, nachdem eine Feuer-MG im System (oder in einem beliebigen Bereich) ausgelöst hat.
Sabotage	Wird aktiviert, wenn ein Sabotagezustand in einem beliebigen Teil des Systems erkannt wurde. Wenn bei Systemen der Sicherheitsstufe 3 die Kommunikation mit einem XBUS-Gerät länger als 100 Sekunden unterbrochen ist, wird ein Sabotage-Alarm erstellt, und SIA- und CIR-Meldungen senden eine Sabotage.
Medizinischer Notfall	Wird aktiviert, wenn eine Medizin-MG aktiviert wurde.
Störung	Wird aktiviert, wenn eine technische Störung erkannt wurde.
Technik	Wird aktiviert, wenn eine Technik-MG auslöst.
Netzstörung*	Wird aktiviert, wenn die Netzstromversorgung ausfällt.
Batteriestörung*	Wird aktiviert, wenn ein Problem mit der Reservebatterie vorliegt. Fällt die Batteriespannung unter 11 V, wird der Ausgang aktiviert. Die Option ‚Quittieren‘ für diesen Fehler wird nur angeboten, wenn die Spannung wieder über 11,8 V steigt.
Intern scharf A	Wird aktiviert, wenn das System oder ein im System angelegter Bereich auf Intern Scharf A geschaltet wird.
Intern scharf B	Wird aktiviert, wenn das System oder ein im System angelegter Bereich auf Intern Scharf B geschaltet wird.
Extern Scharf	Wird aktiviert, wenn das System auf Extern Scharf geschaltet wird.
Schärfung fehlgeschlagen	Wird aktiviert, wenn das versuchte Scharfschalten des Systems oder eines im System angelegten Bereichs fehlschlägt; er wird zurückgesetzt, sobald der Alarm quittiert wurde.
Einbruch verzögert	Wird aktiviert, wenn eine auf Einbruch verzögert gesetzte MG aktiviert wurde, d. h., wenn eine Alarmverzögerung oder eine Schärfungsverzögerung läuft (System oder Bereich).
Ext Scharf bis Alarmverzögerung	Dieser Ausgang wird gemäß der Konfiguration für den statischen Ausgang des Systems aktiviert (siehe Konfiguration der Ausgänge für Systemverzögerung und automatische Scharfstellung [→ 220]). Der Ausgang kann verwendet werden, um verriegelte Sensoren als Rauch- oder Vibrationsmelder umzustellen.
Notausgang	Schaltet EIN, wenn Notausgang-Meldergruppen im System aktiviert werden.
Türglocke	Wird kurzzeitig eingeschaltet, wenn eine System-MG mit dem Attribut Türglocke ausgelöst wird.

Unscharf Quittierung	Dieser Ausgang wird kurzzeitig aktiviert (3 Sekunden), wenn ein Benutzer das System unscharf schaltet; kann verwendet werden, um Rauchmelder zurückzusetzen. Der Ausgang wird ebenfalls aktiviert, wenn die Meldergruppe wiederhergestellt wird. Beim Zurücksetzen eines verriegelten Rauchmelders mithilfe der Meldergruppe wird bei der ersten Eingabe des Codes nicht der Rauchausgang aktiviert, sondern die Sirenen stumm geschaltet; bei der nächsten Code-Eingabe wird der Rauchausgang vorübergehend aktiviert, falls die Feuer-Meldergruppe offen ist. Dieser Vorgang kann wiederholt werden, bis die Feuer-Meldergruppe geschlossen ist.
Gehtest*	Wird kurzzeitig aktiviert, wenn ein Gehtest läuft und eine Meldergruppe aktiviert wird. Der Ausgang kann zum Beispiel verwendet werden, um Funktionstests angeschlossener Melder durchzuführen (falls vorhanden).
Autom Scharfsch	Wird eingeschaltet, wenn die automatische Scharfschalt-Funktion im System aktiviert wurde.
Bedrohungs-PIN	Wird eingeschaltet, wenn ein Bedrohungs-PIN-Status aktiviert wurde (PIN + 1 wurde am Bedienteil eingegeben).
Melder abgedeckt	Wird eingeschaltet, wenn abgedeckte Bewegungsmelder im System erkannt werden. An der Bedienteil-LED wird ein Störausgang angezeigt. Dieser Ausgang bleibt so lange aktiviert, bis er von einem Benutzer der Ebene 2 quittiert wird. PIR-Maskierung wird standardmäßig protokolliert. Die Anzahl der Protokolleinträge beträgt zwischen Scharfschaltungszeiträumen nicht mehr als 8.
MG inaktiv	Wird eingeschaltet, wenn es im System gesperrte, deaktivierte Meldergruppen oder Meldergruppen, die im Gehtest-Modus laufen, gibt.
Übertragungsstörung	Wird eingeschaltet, wenn Störung bei der Übertragung von Daten zum Empfänger erkannt wird.
Man Down Test	Aktiviert eine Überfallfunkkomponente, die während eines Man-down Tests aktiviert wird.
Unscharf	Wird aktiviert, wenn das System auf Unscharf geschaltet wird.
Alarmabbruch	Wird aktiviert, wenn ein Alarmabbruch erfolgt, d. h. wenn nach einem bestätigten oder unbestätigten Alarm eine gültige Benutzer-ID über das Bedienteil eingegeben wird. Er wird zum Beispiel in Verbindung mit externen Wahlgeräten (SIA, CID, FF) verwendet.
Körperschallmelder-Test	Wird zur Aktivierung eines manuellen oder automatischen Tests einer Körperschall-MG verwendet. Körperschallmelder besitzen ein kleines Vibratorelement, das an der gleichen Wand wie der Sensor angebracht wird und mit einem Ausgang an der Zentrale oder einem ihrer Erweiterungsmodule angeschlossen wird. Während des Tests wartet die Zentrale bis zu 30 Sekunden, bis sich die MG öffnet. Öffnet sich die MG nicht, ist der Test fehlgeschlagen. Öffnet sie sich innerhalb von 30 Sekunden, wartet die Zentrale 10 Sekunden, bis sich die MG wieder schließt. Geschieht dies nicht, ist der Test fehlgeschlagen. Anschließend wartet die Zentrale weitere 2 Sekunden, bis das Ergebnis berichtet wird. Das Ergebnis des (manuellen oder automatischen) Tests wird im System-Logbuch gespeichert.
Lokale Alarmierung	Wird bei einem lokalen Einbruchalarm aktiviert.
Funk Ausgang	Wird aktiviert, wenn eine Transponder- oder FÜ-Taste gedrückt wird.
Modem 1 Störung Telefonleitung	Wird aktiviert, wenn eine Störung der Telefonleitung des primären Modems vorliegt.
Modem 1 Fehler	Wird aktiviert, wenn das primäre Modem ausfällt.
Modem 2 Leitungsunterbruch	Wird aktiviert, wenn eine Störung der Telefonleitung des sekundären Modems vorliegt.
Modem 2 Fehler	Wird aktiviert, wenn das sekundäre Modem ausfällt.
Batterie schwach	Wird aktiviert, wenn die Batterie schwach ist.
Status Eintritt	Wird aktiviert, wenn ein ‚Alles in Ordnung‘-Zutrittsvorgang implementiert und kein Alarm generiert wird, d. h. die ‚Alles in Ordnung‘-Taste wird innerhalb der konfigurierten Zeit gedrückt, nachdem die Benutzer-ID eingegeben wurde.
Status Warnung	Wird aktiviert, wenn ein ‚Alles in Ordnung‘-Zutrittsvorgang implementiert und ein stiller Alarm generiert wird, d. h. die ‚Alles in Ordnung‘-Taste wird nicht innerhalb der konfigurierten Zeit gedrückt, nachdem die Benutzer-ID eingegeben wurde.

Schärfungsbereit	Dieser Ausgang wird aktiviert, wenn ein Bereich zum Scharfschalten bereit ist.
Scharf-/Unscharf quittieren (SPC Pro — Scharf-/Unscharf. abgeschlossen)	Dieser Ausgang meldet den Scharfschaltungsstatus. Der Ausgang schaltet 3 Sekunden lang um, um zu signalisieren, dass das Scharfschalten fehlgeschlagen ist. Der Ausgang bleibt 3 Sekunden lang eingeschaltet, wenn das Scharfschalten erfolgreich war.
Schärfung abgeschlossen (SPC Pro — Scharf-/Unscharf. erfolgreich)	Dieser Ausgang bleibt 3 Sekunden lang aktiv, um zu signalisieren, dass das System extern scharf geschaltet wurde.
Blockschloss 1	Wird für normale Blockschloss-Geräte benutzt. Wenn alle Meldergruppen in einem Bereich geschlossen sind und keine Störungsmeldungen anstehen, wird der Ausgang „Blockschloss 1“ aktiviert. Ist die Sperre auf dem Blockschloss geschlossen, werden ein Scharf/Unscharf-Eingang aktiviert, der entsprechende Bereich scharf geschaltet und der Ausgang „Scharf-/Unscharf quittieren“ 3 Sekunden lang aktiviert, um anzuzeigen, dass die Scharfschaltung erfolgreich war. „Blockschloss 1“ wird nicht deaktiviert. Wird das Blockschloss entsperrt, deaktiviert das Blockschloss-Gerät den Scharf/Unscharf-Eingang und ändert den Zustand auf Unscharf (geschlossen); der Bereich wird unscharf geschaltet. Dann wird „Blockschloss 1“ deaktiviert.
Blockschloss 2	Genutzt für ein Blockschloss-Gerät vom Typ Bosch Blockschloss, Sigmalock Plus, E4.03. Wenn alle Meldergruppen in einem Bereich geschlossen sind und keine Störungsmeldungen anstehen, wird der Ausgang „Blockschloss 2“ aktiviert. Ist die Sperre auf dem Blockschloss geschlossen, werden ein Scharf/Unscharf-Eingang aktiviert, der entsprechende Bereich scharf geschaltet und der Ausgang „Scharf-/Unscharf quittieren“ 3 Sekunden lang aktiviert, um anzuzeigen, dass die Scharfschaltung erfolgreich war. Dann wird „Blockschloss 2“ deaktiviert. Wird das Blockschloss entsperrt, wird die Scharf/Unscharf-Eingang-Meldergruppe auf unscharf (geschlossen) geschaltet und der Bereich wird unscharf geschaltet. „Blockschloss 2“ wird aktiviert (wenn der Bereich schärfungsbereit ist)
Element sperren	Wird aktiviert, wenn das Sperrelement in der Stellung „gesperrt“ ist.
Element freigeben	Wird aktiviert, wenn das Sperrelement in der Stellung „freigegeben“ ist.
Code-Sabotage	Wird aktiviert, wenn im Bereich eine Code-Sabotage erkannt wird. Wird gelöscht, wenn der Zustand zurückgesetzt wird.
Problem	Wird aktiviert, wenn sich an irgendeiner MG ein Problemzustand ergibt.
Netzwerk-Verbindung	Wird aktiviert, wenn im Netzwerk eine Störung auftritt.
Netzwerk Störung	Wird aktiviert, wenn eine Störung in der EDV-Datenübertragung auftritt.
Glassbruch zurücksetzen	Dient dazu, die Stromversorgung für das Glasbruch-Schnittstellenmodul einzuschalten oder die Stromversorgung abzuschalten, um das Gerät zurückzusetzen. Der Ausgang wird zurückgesetzt, wenn ein Benutzer seinen Code eingibt, die Meldergruppe nicht geschlossen ist und die Sirenen deaktiviert sind.
Bestätigter Überfall	Wird zur PD6662-Einhaltung in den folgenden Szenarien aktiviert: <ul style="list-style-type: none"> <li>● zwei Aktivierungen von Bedrohungs-MGs, die mehr als zwei Minuten auseinander liegen</li> <li>● eine Aktivierung einer Bedrohungs-MG und eine Aktivierung einer Panik-MG, die mehr als zwei Minuten auseinander liegen</li> <li>● Wenn in dem zweiminütigen Zeitraum eine Bedrohungs- und Sabotage-MG oder eine Panik-MG und Sabotage-MG aktiviert werden</li> </ul>
Konfigurationsmodus	Wird aktiviert, wenn ein Techniker vor Ort ist und das System im Konfigurationsmodus ist.

*\*Diese Ausgangstypen können nur systemweite Ereignisse anzeigen (keine bereichsbezogenen Ereignisse).*

**Siehe auch**

- 📄 Konfiguration der Ausgänge für Systemverzögerung und automatische Scharfstellung [→ 220]

# 11 Konfigurieren von Erweiterungen, Bedienteilen und Türsteuerungen

## 11.1 Konfigurieren von Erweiterungen an einer SPC-Zentrale

<b>!</b>	<b>HINWEIS</b>
	<p>Es wird empfohlen, sich mit der Zentrale zu verbinden und die aktuelle Erweiterungskonfiguration heraufzuladen, bevor mit dem Konfigurieren von Erweiterungen an der Zentrale begonnen wird. Sie sollten nur Konfigurationseinstellungen an die Zentrale senden, ohne zuvor die vorhandene Konfiguration von der Anlage heraufgeladen zu haben, wenn Sie aktuelle und umfassende Kenntnisse über die derzeitige Konfiguration der Erweiterung an der Zentrale verfügen.</p>

Für das Hinzufügen und Bearbeiten von Erweiterungen gelten folgende Regeln:

- SPC Pro gestattet Ihnen NICHT, eine Konfigurationsdatei an die Zentrale zu senden, wenn die Anzahl der konfigurierten Erweiterungen nicht mit der Anzahl der an der Zentrale erkannten Erweiterungen übereinstimmt. Die Anzahl der an der Zentrale erkannten Erweiterungen wird im Konfigurationsfenster angezeigt (siehe Seite [→ 18]), wenn Sie sich mit der Zentrale verbinden.
- SPC Pro gestattet Ihnen NICHT, eine Konfigurationsdatei an die Zentrale zu senden, wenn der Typ der konfigurierten Erweiterungen nicht dem Typ der im System erkannten Erweiterungen entspricht. Wenn Sie beispielsweise 3 Bedienteile und 2 I/O-Erweiterungen in SPC Pro konfigurieren, können Sie diese Konfiguration nicht an eine Zentrale mit 3 I/O-Erweiterungen und 2 Bedienteilen senden.

Es gibt zwei Verfahren zum Konfigurieren von Erweiterungen an der Zentrale:

### Konfigurationsdatei vor dem Konfigurieren heraufladen (empfohlen)

Dies ist das empfohlene Verfahren zum Hinzufügen von Erweiterungen zur Zentrale. Zum Verbinden und Heraufladen der aktuellen Konfiguration Siehe Seite [→ 20].

SPC Pro zeigt Ihnen eine Kopie der aktuellen Konfiguration der Zentrale. Somit kennen Sie die Anzahl, den Typ und die Reihenfolge der über den X-BUS an die Zentrale angeschlossenen Erweiterungen. Siehe Seite [→ 99].

Sie können die Erweiterungen in der Liste nach Bedarf bearbeiten und dann Ihre Änderungen an die Zentrale senden.

### Konfigurationsdatei ohne vorherigen Upload an die Zentrale senden

1. Wenn Sie diese Methode verwenden wollen, müssen Sie die Anzahl und die Typen von an die Zentrale angeschlossenen Erweiterungen genau kennen. Führen Sie folgende Schritte aus, um Ihre Erweiterungskonfiguration an die Zentrale zu senden:
2. Beim ersten Anmelden an der Zentrale werden Anzahl und Typ der erkannten Erweiterungen im **Status der Zentrale** angezeigt – X-BUS-Übersichtsfenster. Siehe Seite [→ 36].
3. Notieren Sie sich Nummer, Typ und Reihenfolge der Erweiterungen am X-BUS.
4. Gehen Sie zu **Zentralenkonfiguration > Busteilnehmer > Erweiterungen**.

5. Fügen Sie die entsprechenden Nummern und Typen von Erweiterungen hinzu, damit sie denen im Fenster **Status** der Zentrale angezeigten Erweiterungen entsprechen – X-BUS.
6. Anschließend können Sie diese Erweiterungen nach Bedarf konfigurieren. Siehe Seite [→ 101].
7. Senden Sie Ihre Konfigurationsänderungen an die Zentrale.

## 11.2 Erweiterungen

### 11.2.1 Hinzufügen und Konfigurieren von Erweiterungen

Zentralenkonfig.



Busteilnehmer

1. Klicken Sie auf die Registerkarte **Erweiterung**.  
⇒ Daraufhin erscheint das folgende Fenster.

Konfigurierte Erweiterungen

Erw.	Typ	S/N	Beschreibung	Eingänge	Ausgänge
1	Erweiterung	114214801		8	2

2. Für jede Erweiterung werden die folgenden Informationen angezeigt.

Erweiterungen	Die Erweiterungsnummer in der Zentrale.
Typ	Der Typ der Erweiterung (Schlüsselschalter, E/A, Netzteil, Funkmodul usw.).
Seriennummer	Die Seriennummer der Erweiterung.
Beschreibung	Beschreibungstext für die Erweiterung.
Status	Der aktuelle Status der Erweiterung (online oder offline).
Eingänge	Die Anzahl der Eingänge an der Erweiterung.
Ausgänge	Die Anzahl der Ausgänge an der Erweiterung.

## Mögliche Aktionen

Neue Erw hinzufügen	Klicken Sie auf diese Schaltfläche, um eine Erweiterung zur Zentrale hinzuzufügen.
X-BUS-Zuweisung ansehen	
Einstellungen	Klicken Sie auf diese Schaltfläche, um den X-BUS an der Zentrale zu konfigurieren.
S/N der Busteilnehmer automatisch zuweisen	Klicken Sie auf diese Schaltfläche, um dem System zu ermöglichen, dass vorhandenen Erweiterungen in der Zentrale Seriennummern automatisch zugewiesen werden können.
IDs / S/N neu zuweisen	Klicken Sie auf diese Schaltfläche, um die an der Zentrale vorhandenen Erweiterungen neu zuzuweisen.

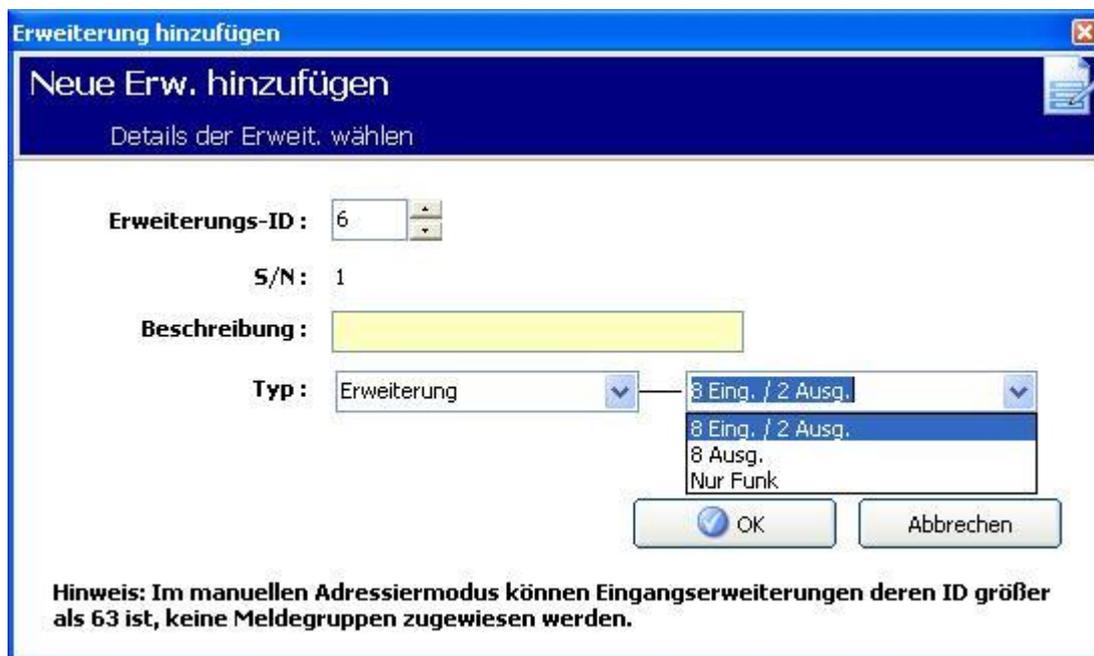
### Siehe auch

- 📖 X-BUS [→ 36]
- 📖 Bedienteil-Emulation aktivieren [→ 234]

## 11.2.1.1 Hinzufügen einer neuen Erweiterung

### Neue Erweiterung hinzufügen

1. Klicken Sie auf die Schaltfläche **Neue Erweiterung hinzufügen**.  
⇒ Daraufhin erscheint das folgende Fenster.



**Erweiterung hinzufügen**

**Neue Erw. hinzufügen**  
Details der Erweiter. wählen

Erweiterungs-ID: 6

S/N: 1

Beschreibung: [ ]

Typ: Erweiterung

8 Eing. / 2 Ausg.  
8 Eing. / 2 Ausg.  
8 Ausg.  
Nur Funk

OK Abbrechen

**Hinweis: Im manuellen Adressiermodus können Eingangserweiterungen deren ID größer als 63 ist, keine Meldegruppen zugewiesen werden.**

2. Konfigurieren Sie die Felder gemäß der Beschreibung in der nachfolgenden Tabelle.
3. Klicken Sie auf **OK**.

Erweiterungs-ID	Diese Nummer wird als Referenz angezeigt und kann nicht programmiert werden.
Seriennummer	Die Seriennummer einer Erweiterung ist in der Firmware festgelegt und kann

	nicht programmiert werden. Die in diesem Feld aufgeführte Nummer wird lediglich als Referenz verwendet, wenn eine neue Erweiterung hinzugefügt wird. Im Feld der Seriennummer in der Liste der Erweiterungen wird <Nicht zugewiesen> angezeigt, wenn diese Information noch nicht aus der Zentrale heraufgeladen wurde.
Beschreibung	Geben Sie hier einen Beschreibungstext für die Erweiterung ein (max. 16 Zeichen). Dieser Text erscheint auch im Browser und im Bedienteil.
Typ	Wählen Sie den Typ der Erweiterung. Wenn „Erweiterung“ ausgewählt ist, wählen Sie auch den Typ der Erweiterung aus.



Neue Erweiterungen können nur zur Zentrale hinzugefügt werden, wenn sie physisch an den X-BUS angeschlossen und der Konfigurationsdatei hinzugefügt wurden. Wenn eine Erweiterung vor Ort physisch an den X-BUS der Zentrale angeschlossen, aber noch nicht in der Datenbank konfiguriert wurde, können Sie sie mit folgenden Schritten über SPC Pro dem System hinzufügen:

### 11.2.1.2 Hinzufügen einer Erweiterung zur Konfigurationsdatenbank

1. Stellen Sie eine Verbindung mit der Zentrale her.
2. Überprüfen Sie den Übersichtsstatus von X-BUS. Siehe Seite [→ 36].
3. Neu verdrahtete Erweiterungen werden mit offenem Status angezeigt.
4. Klicken Sie auf das virtuelle Bedienteil. Siehe Seite [→ 234].
5. Rufen Sie den Konfigurationsmodus auf.
6. Wählen Sie KONFIGURATIONSMODUS > ERWEITERUNGEN > HINZUFÜGEN.  
⇒ Die Erweiterungen werden in diesem Menü aufgelistet.
7. Wählen **Hinzufügen**, um diese Erweiterungen der Datenbank hinzuzufügen.
8. Verlassen Sie das virtuelle Bedienteil.
9. Klicken Sie auf **Konfiguration der Zentrale anfordern**.
10. Öffnen Sie die Liste der Erweiterungen.  
⇒ Die neu hinzugefügten Erweiterungen werden angezeigt und können nach Bedarf konfiguriert werden.

### 11.2.2 Konfigurieren einer Erweiterung



Busteilnehmer

1. Klicken Sie auf eine Erweiterung in der Liste.  
⇒ Daraufhin erscheint das folgende Fenster.

**Busteilnehmer bearbeiten**  
Konfiguration dieses Busteilnehmers bearbeiten

Teilnehmer-ID : 1  
 Typ : Erweiterung [8 Eing. / 2 Ausg.]  
 S/N : 94289801  
 Beschreibung :   
 PSU Typ : SPCP355

Eingänge  Ausgänge  PSU

Eing.	Endwiderstand	Analyzed	Pulse Count	Gross Attack	MG	Beschreibung	Typ	Attribute	Bereich
1	Endw. 4K7/4K7				9	Seismic	Unbenutzt		1
2	Endw. 4K7/4K7				10		Unbenutzt		1
3	Endw. 4K7/4K7				11		Unbenutzt		1
4	Endw. 4K7/4K7				12		Unbenutzt		1
5	Endw. 4K7/4K7				13		Unbenutzt		1
6	Endw. 4K7/4K7				14		Unbenutzt		1
7	Endw. 4K7/4K7				15		Unbenutzt		1
8	Endw. 4K7/4K7				16		Unbenutzt		1

OK  Löschen  Abbrechen

2. Geben Sie für die Erweiterung die folgenden Informationen ein:

Beschreibung	Geben Sie für die Erweiterung einen neuen Namen ein, oder bearbeiten Sie einen vorhandenen Namen.
Lautstärken-Limit	<b>Nur Verifikationsmodul:</b> Lautstärke für das Verifikationsmodul und Satelliten (WAC 11. Einstellbereich ist min. 0 – max. 7 oder deaktiviert).
Zusatz-Lautsprecher/Mikrofon	<b>Nur Verifikationsmodul:</b> Diese Option sollte aktiviert sein, wenn an diese Erweiterung Satelliten angeschlossen werden, um Satellitenmikrofone mit Strom zu versorgen.

- Geben Sie **Eingabe-** und **Ausgabeinformationen** wie in den folgenden Abschnitten beschrieben ein.

### Eingänge

1. Klicken Sie auf einen Eingang in der Liste.  
⇒ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.
3. Klicken Sie auf **OK**.

Eingang der Erweiterung bearbeiten

## Eingang der Erweiterung bearbeiten 1

Eingangseinstellungen konfigurieren

**Eing. :** 1

**Endwiderstand :** Endw. 4K7/4K7

**Analyzed :**

**Pulse Count :** 0

**Gross Attack :** 0

**MG :** 1

**Beschreibung :** Front door

**Typ :** S/U Eingang

**Bereich :** 1 - Reception

**Attribute**

<input type="checkbox"/> Folgt. Verz. <input type="checkbox"/> Nicht Intern A <input type="checkbox"/> Nicht Intern B <input type="checkbox"/> 24 Stunden <input type="checkbox"/> Lokal <input type="checkbox"/> Doppelausl. <input type="checkbox"/> Türglocke <input checked="" type="checkbox"/> Sperrbar <input type="checkbox"/> Normal offen <input type="checkbox"/> Still <input type="checkbox"/> Log <input type="checkbox"/> Überwacht <input type="checkbox"/> Info vor Scharfsch. <input type="checkbox"/> Automatischer <input checked="" type="checkbox"/> Verz.Schärfung	<input type="checkbox"/> Tastend <input type="checkbox"/> Nur übertr. <input type="checkbox"/> Ext. Zeitabbr. <input checked="" type="checkbox"/> Ext. scharf erlaubt <input checked="" type="checkbox"/> Unscharf erlaubt <input type="checkbox"/> Shunt <input type="checkbox"/> Übertragen <input type="checkbox"/> Anzeigen am BT <input type="checkbox"/> Bedient. Summer <input type="checkbox"/> Verzögert <input type="checkbox"/> Übertr. nur bei scharf <input type="checkbox"/> Feuer Voralarm <input type="checkbox"/> Feuer Erkundungszeit <input type="checkbox"/> Unsch. lokal <input checked="" type="checkbox"/> Erzwungen Scharf
---	--

Eingang	Diese Nummer wird als Referenz angezeigt und kann nicht programmiert werden.
Endwiderstand	Wählen Sie den <b>Endwiderstand</b> (EOL) für den Meldergruppeneingang (Vorgabe: 4K7).
Analyzed	Zeigt an, ob es sich bei dem Melder um einen Vibrations-/Stoßsensor handelt.
Pulse count	Die in der Zentrale programmierte Pulszahl, bei der ein Alarm durch einen Vibrations-/Stoßmelder ausgelöst wird.
Gross Attack	Die in der Zentrale programmierte starke Erschütterung, bei der ein Alarm durch einen Vibration/Stoßmelder ausgelöst wird.
Meldergruppe	Nummer des Bereichs an der Zentrale.
Beschreibung	Geben Sie hier einen Beschreibungstext für den Eingang ein (max. 16 Zeichen). Dieser Text erscheint auch im Browser und im Bedienteil.
Typ	Der Typ der Meldergruppe. Siehe Seite [→ 278].
Bereich	Nur wenn im Menü <b>Zentralenkonfiguration &gt; Systemoptionen &gt; Optionen</b> (mehrere) <b>Bereiche</b> aktiviert sind. Die Bereiche, denen diese Meldergruppe zugewiesen wurde.



Ein Symbol in diesem Feld zeigt an, dass für diese Meldergruppe Attribute konfiguriert wurden. Siehe Seite [→ 281].

## Ausgänge

1. Klicken Sie im Fenster **Erweiterung bearbeiten** auf die Registerkarte **Ausgänge**.
2. Klicken Sie auf einen Ausgang in der Liste.  
⇒ Daraufhin erscheint das folgende Fenster.
3. Siehe die nachfolgende Tabelle für weitere Informationen.

### Ausgangstyp

- **Systemausgang:** Wählen Sie den Typ aus dem Dropdown-Menü. (Siehe Ausgangstypen und Ausgangsschnittstellen [→ 94].)
- **Bereichsausgang:** Nur wenn im Menü **Zentralenkonfig > Systemoptionen > Optionen (mehrere) Bereiche** aktiviert ist. Wählen Sie einen Bereich und den Systemausgangstyp für diesen Bereich. (Siehe Ausgangstypen und Ausgangsschnittstellen [→ 94].)
- **Meldergruppe:** Wählen Sie die Meldergruppe, die zugewiesen werden soll.
- **Log Ausgang:** Wählen Sie den logischen Ausgang, der zugewiesen werden soll.

	<ul style="list-style-type: none"> <li>● <b>Türausgang:</b> Wählen Sie die Türnummer und den Systemausgangstyp für die Tür. (Siehe Ausgangstypen und Ausgangsschnittstellen [→ 94].)</li> <li>● <b>Schlüsselsch.</b>: Wählen Sie die Erw-ID für den erforderlichen Schlüsselschalter und die erforderliche Schlüsselstellung, die diesem Ausgang zugewiesen wird.</li> </ul>
Beschreibung	Geben Sie hier einen Beschreibungstext für den Ausgang ein (max. 16 Zeichen). Dieser Text erscheint auch im Browser und im Bedienteil.
Ausgangskonfiguration	<ul style="list-style-type: none"> <li>● <b>Modus:</b> Auswahl des Betriebsmodus. Durchgängig folgt dem Eingangstyp, Pulsierend schaltet an und aus, wenn der Ausgangstyp aktiv ist, Kurzzeitig erzeugt einen Puls, wenn der Ausgangstyp aktiviert wird.</li> <li>● <b>Erneute Ausl.:</b> Aktivieren Sie dieses Kontrollkästchen, um den kurzzeitigen Ausgang erneut auszulösen.</li> <li>● <b>AN-Zeit:</b> Geben Sie die AN-Zeit für kurzzeitige und pulsierende Ausgänge ein.</li> <li>● <b>AUS-Zeit:</b> Geben Sie die AUS-Zeit für kurzzeitige und pulsierende Ausgänge ein.</li> <li>● <b>Invertieren:</b> Aktivieren Sie dieses Kontrollkästchen, um den physischen Ausgang zu invertieren.</li> <li>● <b>Log:</b> Aktivieren Sie dieses Kontrollkästchen, um die Zustandsänderungen des Ausgangs im Logbuch zu erfassen.</li> <li>● <b>Kalender:</b> Wählen Sie bei Bedarf den gewünschten Kalender. Siehe Seite [→ 209].</li> </ul>

### Ausführbare Aktionen

Ausgangsstatus aktualisieren	Klicken Sie auf diese Schaltfläche, um den Status der Ausgänge zu aktualisieren.
Ausgang testen	Klicken Sie auf eine dieser Schaltflächen, um zu testen, ob der Ausgang zurzeit angeschlossen ist (Leuchte geht an).



Die Funktion **Ausgang testen** steht nur im Konfigurationsmodus zur Verfügung.

#### Siehe auch

Kalender [→ 209]

### 11.2.2.1 Registerkarte PSU

Über die Registerkarte PSU können Sie die Ausgänge für das SPCP355 Smart PSU konfigurieren und testen.

**Hinweis:** Die Registerkarte wird nur angezeigt, wenn in der Dropdown-Liste PSU Type (PSU-Typ) die Option SPCP355 Smart PSU ausgewählt wurde.

Ausgang	Beschreibung	Typ	Zugewiesen als:	Modus	Invertieren	Log
1		----		Durchgängig		
2		----		Durchgängig		
3		----		Durchgängig		
4		----		Durchgängig		

Aktualisiere PSU Ausgänge

Ausgänge testen : ? ? ? ?  
1 2 3 4

Nur Primärbatterie

Ausgänge beobachten

- Beobachte Ausgang 1
- Beobachte Ausgang 2
- Beobachte Ausgang 3

OK    Löschen    Abbrechen

Die folgende Tabelle enthält die Felder auf der Registerkarte PSU:

Name	Beschreibung
Ausgang	Der nummerierte Ausgang. Klicken Sie auf eine Zeile, um das Fenster Edit PSU Output (PSU-Ausgang bearbeiten) zu öffnen. Über dieses Fenster können Sie jedem Ausgang ein bestimmtes Verhalten zuweisen. Weitere Informationen finden Sie unter Bearbeiten eines Ausganges [→ 92].
Beschreibung	Beschreibung für den Ausgang eingeben.
Typ ändern	Ggf. Ausgangstyp ändern.
Attribute	Dem Ausgang Attribute zuweisen.
Ausgänge testen	Ausgang testen.
Ausgänge beobachten	Wählen Sie aus, welche Ausgänge überwacht werden sollen.
Nur Primärbatterie	Aktivieren Sie dieses Kontrollkästchen, wenn keine sekundäre Batterie an das Netzteil angeschlossen ist.

### 11.2.3 Konfigurieren eines Anzeigemoduls

Es gibt zwei mögliche Konfigurationsmodi für die Anzeigenerweiterung:

- Betriebsart "Linked Mode"
- Flexible Mode

Zentralenkonfig.



Busteilnehmer

- Fügen Sie eine neue Anzeigenerweiterung hinzu oder klicken Sie auf ein vorhandenes Anzeigemodul.
- ⇒ Das nachstehende Dialogfeld für die **Linked Mode**-Konfiguration wird angezeigt.

**Busteilnehmer bearbeiten**  
Konfiguration dieses Busteilnehmers bearbeiten

Teilnehmer-ID : 4  
 Typ : Anzeigemodul [1 Eing. / 0 Ausg.]  
 S/N : 180373801  
 Beschreibung :

Eingang :

MG	Eingang	MG Text	Typ	Bereich
33	Erweiterung 4 - Eingan...		Unbenutzt	1 - Premises

Bedienteil :

LED immer an  Wählen Sie, ob die LEDs auch aktiv sein sollen, wenn die Tasten gesperrt sind.

**Funktionstasten**

Taste	Bereich
1	<input type="text" value="Keine"/>
2	<input type="text" value="Keine"/>
3	<input type="text" value="Keine"/>
4	<input type="text" value="Keine"/>

### Betriebsart "Linked Mode"

1. Geben Sie eine Beschreibung ein.
2. Legen sie fest, ob das Anzeigemodul nur nach Eingabe einer gültigen PIN an einem Bedienteil verwendet werden kann.
3. Wählen Sie die Bereiche, die mit den 4 Funktionstasten gesteuert werden sollen.
4. Eingang konfigurieren.

### Flexible Mode

1. Klicken Sie auf die Schaltfläche **Flexible Mode**.
2. Konfigurieren Sie die in der untenstehenden Tabelle beschriebenen Felder.
3. Eingang konfigurieren.

	<b>⚠️ WARNUNG</b>
	Ihr System erfüllt nicht die EN-Normen, wenn Sie eine Funktionstaste zur Scharfstellung des Systems ohne Eingabe einer gültigen PIN aktivieren.

Funktionstasten	
Bereich	Wählen Sie den Bereich, der mit der Funktionstaste gesteuert werden soll.
Funktion	Wählen Sie die Funktion, die mit dieser Taste in diesem Bereich ausgeführt werden soll.

Bereich	Wählen Sie einen Bereich, wenn das Anzeigemodul in einem gesicherten Bereich installiert ist.
<b>Optische Indikation</b>	
Anzeigemodul	Es gibt 8 Anzeigeelemente/LEDs auf der rechten und 8 Anzeigeelemente/LEDs auf der linken Seite.
Funktion	Die Funktion, die von dieser LED angezeigt wird.
Funktion Ein	Farbe und Status für jede LED festlegen, wenn die zugewiesene Funktion aktiviert ist.
Funktion aus	Farbe und Status für jede LED festlegen, wenn die zugewiesene Funktion deaktiviert ist.
Funktion ändern	Diese Schaltfläche anklicken, um die Funktion des betreffenden Anzeigeelements zu ändern. Die Funktion kann aktiviert werden oder für ein System, einen Bereich, eine Meldergruppe oder einen Schlüsselschalter verwendet werden.
<b>Akustische Indikationen</b>	
Alarm	Aktivieren, wenn Alarme akustisch gemeldet werden sollen.
Einbruch verzögert	Wählen, ob eine aktive Verzögerung akustisch hörbar sein soll.
Tastentöne	Aktivieren, wenn eine Tastenbetätigung akustisch quittiert werden soll.
<b>Deaktivierung</b>	
Kalender	Aktivieren, wenn die Aktivierung des Anzeigemoduls nur während der im Kalender eingestellten Zeit möglich sein soll.
Logischer Ausgang	Aktivieren, wenn das Anzeigemodul durch einen logischen Ausgang beschränkt werden soll.
Schlüsselsch.	Aktivieren, wenn das Anzeigemodul nur durch einen Schlüsselschalter aktiviert werden soll.
Bedienteil	Legen sie fest, ob das Anzeigemodul nur nach Eingabe einer gültigen PIN an einem Bedienteil verwendet werden kann. (siehe Warnhinweis oben)
Kartenleser	Aktivieren, wenn das Anzeigemodul nur aktiviert werden soll, wenn eine gültige Karte/Fernbedienung am integrierten Kartenleser vorgehalten wird.

## 11.2.4 Konfigurieren eines Schlüsselschalter-Erweiterungsmoduls

- Klicken Sie in der Liste der konfigurierten Erweiterungen auf den gewünschten Schlüsselschalter.
  - ⇒ Das folgende Dialogfeld wird angezeigt:

- Konfigurieren Sie die in der untenstehenden Tabelle beschriebenen Felder.

Beschreibung	Geben Sie einen Namen für die Schlüsselschalter-Erweiterung ein.
<b>Schlüsselloptionen</b>	
Ext Scharf bis Alarmverz	Schlüsselpos speichern, auch nachdem der Schlüssel abgezogen wurde.
Dauer d Speicherung	Dauer der Speicherung in Sekunden eingeben (0 - 9999, 0 = speichern, bis die selbe Pos erneut oder eine andere aktiviert wird).
<b>Bereiche</b>	
Adresse	Wählen Sie den Bereich aus, in dem das Bedienteil montiert ist.
<b>Optische Anzeigen</b>	
Anzeige/LED	Es gibt 1 Anzeigeelement/LED auf der rechten und 1 Anzeigeelement/LED auf der linken Seite.
Funktion	Die Funktion des jeweiligen Anzeigeelements / der jeweiligen LED.
Funktion Ein	Farbe und Status für jede LED festlegen, wenn die zugewiesene Funktion aktiviert ist.
Funktion aus	Farbe und Status für jede LED festlegen, wenn die zugewiesene Funktion deaktiviert ist.
Funktion ändern	Diese Schaltfläche anklicken, um die Funktion des betreffenden Anzeigeelements zu ändern. Die Funktion kann aktiviert werden oder für ein System, einen Bereich, eine Meldergruppe oder einen Schlüsselschalter verwendet werden.
<b>Deaktivierung</b>	
Kalender	Wählen Sie aus, ob die Aktivierung des Schlüsselschaltermoduls nur während der im Kalender eingestellten Zeit möglich sein soll.
Logischer	Aktivieren Sie diese Option, wenn das Schlüsselschaltermodul durch einen

Ausgang	logischen Ausgang beschränkt werden soll.
<b>Ausgang</b>	
Ausgang x	Konfigurieren Sie die Ausgänge für den Schlüsselschalter und geben Sie sie ein. Siehe Ausgänge [→ 104] für weitere Einzelheiten.
<b>Funktionen Schlüsselschalter</b>	
Stellungen: Mitte, Rechts und Links	Wählen Sie die <b>Funktion</b> , die bei dieser Schlüsselschalterstellung ausgeführt werden soll, sowie den betreffenden <b>Bereich</b> .



### ⚠️ WARNUNG

Ihr System erfüllt nicht die EN-Normen, wenn Sie eine Schlüsselschalterfunktion zur Scharfstellung des Systems ohne Eingabe einer gültigen PIN aktivieren.

## 11.2.5 Erweiterungen neu zuweisen

Zentralenkonfig.



Busteilnehmer

Die Reihenfolge, in der Erweiterungen auf dem X-BUS aufgelistet und gekennzeichnet sind, wird bei der ursprünglichen Installation oder bei einem Kaltstart der Zentrale festgelegt.

Eine Erweiterung einem anderen Ort auf dem X-BUS zuweisen:

1. Klicken Sie auf die Schaltfläche **Erweiterungen neu zuweisen** im Fenster **Konfigurierte Erweiterungen**.
2. Wählen Sie die Erweiterung, die Sie neu zuweisen möchten mit Hilfe der Pfeiltasten nach oben/unten auf der rechten Seite des Fensters.
3. Klicken Sie auf die Schaltfläche **Jetzt zuweisen**.
  - ⇒ Es erscheint eine Popup-Meldung, die darauf hinweist, dass die Erweiterung neu zugewiesen wird.
4. Klicken Sie auf **Ja**.
  - ⇒ Das Fenster mit der Liste der konfigurierten Erweiterungen wird angezeigt und enthält die neue Reihenfolge der Erweiterungen.

Mit dem neu Zuweisen von Erweiterungen haben Sie die Möglichkeit, Erweiterungs-IDS zu mischen und so umzustellen, dass sie der physischen Ergänzung oder dem Austausch einer Erweiterung entsprechen, d. h. der Errichter kann zwischen Erweiterungen mit den IDs 1 und 2 physisch eine I/O-Erweiterung anschließen. Die neue Erweiterung kann die sechste Erweiterung auf dem X-BUS sein, so dass eine ID-Reihenfolge von 1, 2, 6, 3, 4, 5 entsteht. Durch die Neuweisung der Erweiterungs-ID, um sie an die physische Reihenfolge der Erweiterungen an der Zentrale anzupassen, wird die tatsächliche Konfiguration auf dem aktuellen Stand gehalten. Dies hat folgenden Vorteil:

- Sie können beispielsweise Erweiterungen desselben Typs neu anordnen, um sie korrekt an die Programmierung der Zentrale anzupassen. Das bedeutet, dass die Konfiguration Ihrer dritten I/O-Erweiterung mitunter an die zweite I/O-Erweiterung an der Zentrale gesendet werden muss.
- Wenn Sie einen Kaltstart Ihres Systems durchführen, gehen die Konfigurationsdaten all Ihrer Erweiterungen nicht verloren und werden nicht

überschrieben, da die Nummerierung der Erweiterungen der physischen Reihenfolge der Erweiterungen entspricht.

## 11.2.6 Bearbeiten der X-Bus-Einstellungen

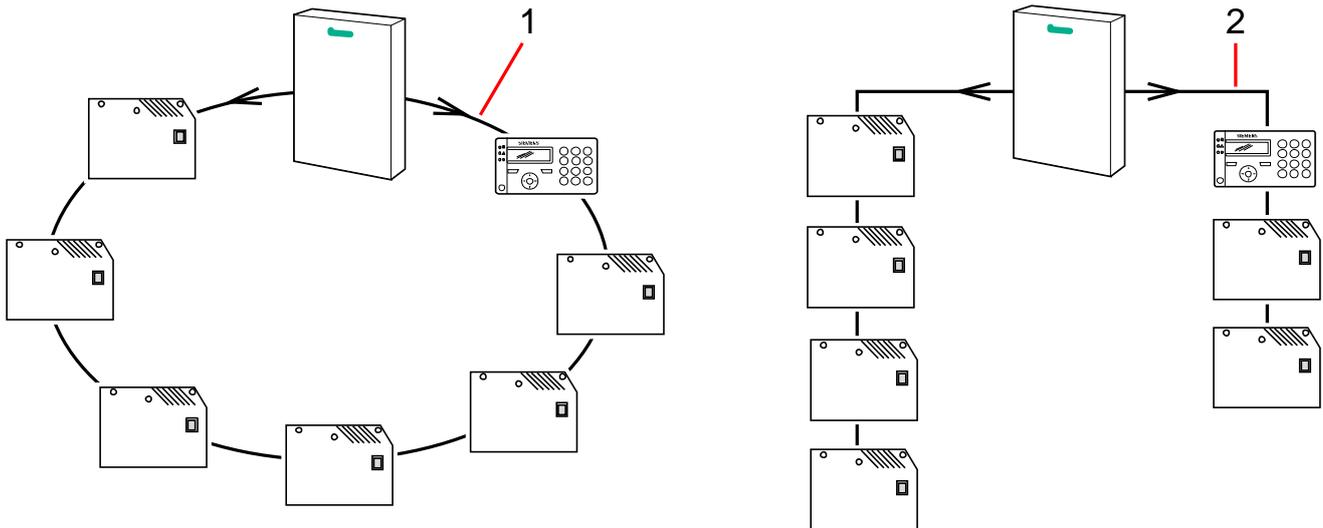
Zentralenkonfig.



Busteilnehmer

1. Klicken Sie auf die Schaltfläche **Einstellungen** im Fenster **Konfigurierte Erweiterungen**.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.
3. Klicken Sie auf **OK**.

Adressiermodus	Bestimmen Sie, ob die Erweiterung auf dem X-BUS manuell oder automatisch adressiert werden sollen.
X-BUS-Typ	Wählen Sie aus der Dropdown-Liste den Typ der X-BUS-Konfiguration (Stich oder Ring) aus. Wenn die Daten aus der Zentrale gelesen, geändert und anschließend wieder an die Zentrale zurückgesendet werden, bleibt die tatsächliche Konfiguration unverändert, sofern nicht ein Errichter vor Ort den X-BUS so neu verdrahtet hat, dass er der programmierten Konfiguration entspricht.
Erneute Übertr.	Wählen Sie die Anzahl von erneuten Kommunikationsversuchen auf dem X-BUS, wenn es elektrische Störungen am Installationsstandort gibt (1–99: Vorgabe ist 25).
Komm. Timeout	Wählen Sie die Anzahl von Sekunden, während der eine Störung vorliegen muss, bevor eine Kommunikationsstörung am X-BUS gemeldet wird.



1	RS485 Ringkonfiguration Die Kommunikation ist bei allen Erweiterungen bidirektional (nur bei SPC5000 / SPC6000).
2	RS485 Ringkonfiguration (Multidrop). Erweiterungen am Ende des Rings.



Man sollte unbedingt mit der physischen Konfiguration der Installation vertraut sein, bevor man diese Einstellung programmiert und an die Zentrale sendet. Die elektrischen Eigenschaften des können einige Anpassungen bei den Parametern für erneute Versuche und den Timeout des X-BUS erforderlich machen, damit die optimale Leistung erzielt wird.

## 11.3 Bedienteile

### 11.3.1 Ein Bedienteil hinzufügen

Zentralenkonfig.



Busteilnehmer

1. Klicken Sie auf das Register **Bedienteil**.
2. Klicken Sie auf die Schaltfläche **Neues Bedienteil hinzufügen**.  
⇒ Daraufhin erscheint das folgende Fenster:

**Neue Erw. hinzufügen**  
 Details der Erweiter. wählen

**Erweiterungs-ID :**

**S/N :** 3

**Beschreibung :**

**Typ :**

**Hinweis: Im manuellen Adressiermodus können Eingangserweiterungen deren ID größer als 63 ist, keine Meldegruppen zugewiesen werden.**

3. Konfigurieren Sie die folgenden Felder und klicken Sie auf **OK**.

Erweiterungs-ID	Diese Nummer wird als Referenz angezeigt und kann nicht programmiert werden.
S/N	Die Seriennummer einer Erweiterung ist in der Firmware festgelegt und kann nicht programmiert werden. Die in diesem Feld aufgeführte Nummer wird lediglich als Referenz verwendet, wenn eine neue Erweiterung hinzugefügt wird. Im Feld der Seriennummer in der Liste der Erweiterungen wird <Nicht zugewiesen> angezeigt, wenn diese Information noch nicht aus der Zentrale heraufgeladen wurde.
Beschreibung	Geben Sie hier einen Beschreibungstext für das Bedienteil ein (max. 16 Zeichen). Dieser Text erscheint auch im Browser und im Bedienteil.
Typ	Wählen Sie das Bedienteil aus.

### 11.3.2 Bearbeiten eines Standard-Bedienteils

Zentralenkonfig.



Busteilnehmer

1. Klicken Sie auf einen der ID-Parameter des Standard-Bedienteils.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

**Busteilnehmer bearbeiten**

Konfiguration dieses Busteilnehmers bearbeiten

**Teilnehmer-ID :** 1

**Typ :** Bedienteil [0 Eing. / 0 Ausg.]

**S/N :** 191640801

**Beschreibung :**

**Verzögerung extern**  If checked the exit timers are used across all areas.

Optische Indikation
  Akustische Indikation
  Sperren/Freigeben
  Bereiche

**Ort :**  Wählen Sie, ob das Bedienteil in einem gesicherten Bereich montiert ist.  
\* N.B. If secure area is set to 'NONE' exit entry will not operate on this keypad.

**Wählen Sie die Bereiche, die durch BT bedient werden dürfen. :**

1 [Bereich 1] - Premises  
 2 [Bereich 2] -

Beschreibung	Geben Sie einen eindeutigen Namen für das Bedienteil ein.
<b>Einstellungen der Funktionstasten (im Ruhezustand)</b>	
Überfall	Wählen Sie „Aktiv“, „Inaktiv“ oder „Aktiv Still“. Im Modus „Aktiv“ wird der Überfallalarm durch gleichzeitiges Drücken der beiden Softkeys aktiviert.
Verifikation	Wenn Sie einem Bedienteil eine Verifikationszone zuweisen, werden Audio- und Videoereignisse aktiviert, wenn durch das gleichzeitige Drücken von 2 Softkeys oder durch Eingabe eines Bedrohungscode ein Panikalarm ausgelöst wird.
<b>Optische Anzeigen</b>	
Hintergrundbeleuchtung	Wählen Sie, wann die Hintergrundbeleuchtung am Bedienteil aktiviert sein soll. Verfügbare Optionen sind: An bei Tastendruck; Immer an; Immer aus.
LED-Anzeigen	LEDs am Bedienteil aktivieren oder deaktivieren.
Systemstatus	Wählen Sie diese Option, wenn der Schärfsstatus im Bereitschaftszustand angezeigt werden soll.
<b>Akustische Indikationen</b>	

Summer	Summer am Bedienteil aktivieren oder deaktivieren.
Summer bei int.scharf	Summer während der Schärfungsverzögerung bei „Intern Scharf“ aktivieren oder deaktivieren.
Tastendruck	Wählen Sie diese Option, wenn eine Tastenbetätigung akustisch quittiert werden soll.
<b>Deaktivierung</b>	
Kalender	Wählen Sie, ob die Aktivierung des Bedienteils nur während der im Kalender eingestellten Zeit möglich sein soll. Siehe Kalender [→ 209].
Logischer Ausgang	Wählen Sie, ob das Bedienteil durch einen logischen Ausgang beschränkt werden soll.
Schlüsselsch.	Wählen Sie, ob das Bedienteil nur durch einen Schlüsselschalter aktiviert werden kann.
Zugang nur mit Transponder	Aktivieren Sie dieses Kontrollkästchen, um die Tasten am Bedienteil für die Dauer der Alarmverzögerung zu deaktivieren, wenn ein Transponder am Bedienteil konfiguriert ist.
<b>Bereiche</b>	
Ort	Wählen Sie, ob das Bedienteil in einem gesicherten Bereich montiert ist.
Bereiche	Wählen Sie die Bereiche, die über das BT gesteuert werden dürfen.
<b>Optionen</b>	
Verzögerung extern scharf	Wählen Sie diese Option, um eine verzögerte Scharfschaltung an allen Bedienteilen zu konfigurieren. Der Standort des Bedienteils wird dabei nicht berücksichtigt, und die Scharfschaltungsverzögerung gilt für alle Bereiche.

**HINWEIS**

Ein Bereich sollte nur dann einem Bedienteil zugewiesen werden, wenn das Bedienteil innerhalb des zugewiesenen Bereichs liegt. Wird ein Bereich zugewiesen, während der betreffende Bereich scharf und unscharf geschaltet ist, werden Alarmverzögerungen verwendet (falls konfiguriert). Weitere Funktionen in Bezug auf Eingangs-/Ausgangsrouten werden ebenfalls verfügbar. Wird kein Bereich zugewiesen, wird der Bereich sofort scharf- oder unscharfgeschaltet, und es stehen keine weiteren Eingangs-/Ausgangsfunktionen zur Verfügung.

**Siehe auch**

 Kalender [→ 209]

**11.3.3 Bearbeiten eines Komfort-Bedienteils**

Zentralenkonfig.



Busteilnehmer

1. Klicken Sie auf einen der ID-Parameter des Komfort-Bedienteils.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

**Erweiterung bearb.**

Einstellungen dieser Erweiterung konfigurieren

**Erweiterungs-ID :** 3  
**Typ :** Komfort Bedienteil [0 Eing. / 0 Ausg.]  
**S/N :** 103  
**Beschreibung :**

Funktionstasten
 Optische Indikation
 Akustische Indikation
 Sperren/Freige ◀ ▶

**Überfall**  ▼ Mit den beiden Softkeys

**Feuer**  Medizin. Notfall (mittels 2 Funktionstasten)

**Medizin. Notfall**  Medizinischer Notfall (mittels 2 Funktionstasten)

**Ext. Scharf**  Extern scharf erlaubt (Funktionstaste 2 zweimal Drücken)

**Intern A**  Intern A scharf erlaubt (Funktionstaste 3 zweimal Drücken)

**Intern B**  Intern B scharf erlaubt (Funktionstaste 4 zweimal Drücken)

Beschreibung	Geben Sie einen eindeutigen Namen für das Bedienteil ein.
<b>Einstellungen der Funktionstasten (im Ruhezustand)</b>	
Überfall	Wählen Sie „Aktiv“, „Inaktiv“ oder „Aktiv Still“. Im Modus „Aktiv“ wird der Überfallalarm durch gleichzeitiges Drücken der beiden Softkeys F1 und F2 aktiviert.
Feuer	Wenn aktiviert, kann der Feualarm durch gleichzeitiges Drücken der Softkeys F2 und F3 aktiviert werden.
Medizinischer Notfall	Wenn aktiviert, kann der medizinische Alarm durch gleichzeitiges Drücken der Softkeys F3 und F4 aktiviert werden.
Extern Scharf	Wenn aktiviert, kann die externe Scharfschaltung durch zweimaliges Drücken der F2-Taste aktiviert werden.
Intern scharf A	Wenn aktiviert, kann die interne Scharfschaltung A durch zweimaliges Drücken der F3-Taste aktiviert werden.
Intern scharf B	Wenn aktiviert, kann die interne Scharfschaltung B durch zweimaliges Drücken der F4-Taste aktiviert werden.

Verifikation	Wenn Sie einem Komfort-Bedienteil eine Verifikationszone zuweisen, werden Audio- und Videoereignisse aktiviert, wenn ein Medizin-, Panik- oder Feuersalarm ausgelöst wird oder wenn ein Benutzer einen Bedrohungscode eingibt.
<b>Optische Indikationen</b>	
Hintergrundbeleuchtung	Wählen Sie, wann die Hintergrundbeleuchtung am Bedienteil aktiviert sein soll. Verfügbare Optionen sind: An bei Tastendruck; Immer an; Immer aus.
Hintergrundbel. Intensität	Wählen Sie die Intensität der Hintergrundbeleuchtung. Einstellungsbereich: 1 (gering) - 8 (hoch).
LED-Anzeigen	LEDs am Bedienteil aktivieren oder deaktivieren.
Systemstatus	Aktivieren Sie diese Option, wenn der Systemstatus (SCHARF, INTERNSCHARF A usw.) im Bereitschaftszustand angezeigt werden soll. (LED)
Logo	Wählen Sie, ob das Logo im Ruhezustand angezeigt wird.
Analoge Uhr	Wählen Sie die Position der analogen Uhr aus, falls diese im Ruhezustand angezeigt wird. Verfügbare Optionen sind: Linksbündig, Mittig, Rechtsbündig, Deaktiviert.
Freigabe bei Feuer	Wählen Sie, ob die Funktionstasten für Überfall, Feuer und Medizinischen Notfall auf dem LCD-Display angezeigt werden sollen.
Direkte Scharfsch.	Wählen Sie, ob die Funktionstasten für Externe/Interne Scharfschaltung auf dem LCD-Display angezeigt werden sollen.
<b>Akustische Indikationen</b>	
Alarm	Wählen Sie die Lautstärke für Alarme oder schalten Sie den Ton aus.
Einbruch verzögert	Einstellbereich: 0 – 7 (max. Lautstärke)
Türglocke	Wählen Sie die Lautstärke der Verzögerungen oder schalten Sie den Ton aus.
Tastendruck	Einstellbereich: 0 – 7 (max. Lautstärke)
Sprachausgabe	Wählen Sie die Lautstärke für die Türglocke oder schalten Sie den Ton aus.
Summer bei int.scharf	Einstellbereich: 0 – 7 (max. Lautstärke)
<b>Deaktivierung</b>	
Kalender	Wählen Sie, ob die Aktivierung des Bedienteils nur während der im Kalender eingestellten Zeit möglich sein soll. Siehe Kalender.
Logischer Ausgang	Wählen Sie, ob das Bedienteil durch einen logischen Ausgang beschränkt werden soll.
Schlüsselsch.	Wählen Sie, ob das Bedienteil nur durch einen Schlüsselschalter aktiviert werden kann.
Zugang nur mit Transponder	Aktivieren Sie dieses Kontrollkästchen, um die Tasten am Bedienteil für die Dauer der Alarmverzögerung zu deaktivieren, wenn ein Transponder am Bedienteil konfiguriert ist.
<b>Bereiche</b>	
Ort	Wählen Sie, ob das Bedienteil in einem gesicherten Bereich montiert ist.
Bereiche	Wählen Sie die Bereiche, die über das BT gesteuert werden dürfen.
<b>Optionen</b>	
Verzögerung extern scharf	Wählen Sie diese Option, um eine verzögerte Scharfschaltung an allen Bedienteilen zu konfigurieren. Der Standort des Bedienteils wird dabei nicht berücksichtigt, und die

Scharfschaltungsverzögerung gilt für alle Bereiche.
---

**HINWEIS**

Ein Bereich sollte nur dann einem Bedienteil zugewiesen werden, wenn das Bedienteil innerhalb des zugewiesenen Bereichs liegt. Wird ein Bereich zugewiesen, während der betreffende Bereich scharf und unscharf geschaltet ist, werden Alarmverzögerungen verwendet (falls konfiguriert). Weitere Funktionen in Bezug auf Eingangs-/Ausgangsrouten werden ebenfalls verfügbar. Wird kein Bereich zugewiesen, wird der Bereich sofort scharf- oder unscharf geschaltet, und es stehen keine weiteren Eingangs-/Ausgangsfunktionen zur Verfügung.

## 11.4 Türmodule

Allgemeine Informationen zu Türsteuerungen finden Sie im Installations- und Konfigurationshandbuch der SPC42XX/43xx/52xx/53xx/62xx/63xx.

### 11.4.1 Eine Türsteuerung hinzufügen

Zentralenkonfig.



Busteilnehmer

1. Klicken Sie auf die Registerkarte **Türsteuerungen**.
2. Klicken Sie auf die Schaltfläche **Neue Türsteuerung hinz.**
3. Weitere Informationen finden Sie in der nachstehenden Tabelle.

**Neue Erw. hinzufügen**
✎

Details der Erweiter. wählen

---

**Erweiterungs-ID:**

**S/N:**

**Beschreibung:**

**Typ:**

**Hinweis:** Im manuellen Adressiermodus können Eingangserweiterungen deren ID größer als 63 ist, keine Meldegruppen zugewiesen werden.

Erweiterungs-ID	Diese Nummer wird als Referenz angezeigt und kann nicht programmiert werden.
S/N	Die Seriennummer einer Erweiterung ist in der Firmware festgelegt und kann nicht programmiert werden. Die in diesem Feld aufgeführte

	Nummer wird lediglich als Referenz verwendet, wenn eine neue Erweiterung hinzugefügt wird. Im Feld der Seriennummer in der Liste der Erweiterungen wird <Nicht zugewiesen> angezeigt, wenn diese Information noch nicht aus der Zentrale heraufgeladen wurde.
Beschreibung	Geben Sie hier einen Beschreibungstext für die Türsteuerung ein (max. 16 Zeichen). Dieser Text erscheint auch im Browser und im Bedienteil.
Typ	Wählen Sie eine Türsteuerung aus.

## 11.4.2 Türsteuerung bearbeiten

Zentralenkonfig.



Busteilnehmer

1. Klicken Sie auf eine Türsteuerung in der Liste.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.
3. Klicken Sie auf **OK**.

**Busteilnehmer bearbeiten**

Konfiguration dieses Busteilnehmers bearbeiten

**Teilnehmer-ID :** 6

**Typ :** Türsteuerung [4 Eing. / 2 Ausg.]

**S/N :** 5

**Beschreibung :**

**Türoptionen**

**Tür E/A 1 :** Tür 1

**Tür E/A 2 :** Ein-/Ausgänge

**Leser 1 :** Profil 1 [Fehler]

**Leser 2 :** Profil 1 [Fehler]



Zur Benennung und Identifikation:

Bei der Ringkonfiguration wird jede Erweiterung von der ersten (Erweiterung an 1A 1B am Controller) bis zur letzten (Erweiterung an 2A 2B am Controller) durchgehend mit aufeinanderfolgenden Nummern nummeriert.

Beispiel für SPC63xx: Erweiterungen, nummeriert von 1 bis 63, erhalten Meldergruppen (in 8er-Gruppen) mit aufeinanderfolgenden ID-Nummern von 1 bis 512 (die höchste MG-ID ist 512) zugewiesen. Daher können Erweiterungen, die mit einer Zahl >63 benannt oder identifiziert werden, keine Meldergruppen zugewiesen werden.

Erweiterungs-ID	An den Drehschaltern eingestellte ID der Türsteuerung
Typ	Typ der Türsteuerung
S/N	Seriennummer der Türsteuerung
Beschreibung	Beschreibung der Türsteuerung
Tür E/A 1	<ul style="list-style-type: none"> <li>● Wird eine Tür dem Tür E/A zugewiesen, entsprechende Türnummer auswählen. <b>Ein-/Ausgänge</b> wählen, wenn die beiden Ein- und Ausgänge konfigurierbar sind.</li> <li>● Wurde für den Tür E/A eine Türnummer ausgewählt, können die Türeinrichtungen durch Anklicken der Schaltfläche „Bearbeiten“ geändert werden. Dies entspricht dem Menüpfad <b>Einstellungen &gt; Türen</b>.</li> <li>● Wurde <b>MG / Optionen</b> ausgewählt, können die beiden MG und der Ausgang durch Anklicken der Schaltfläche „Bearbeiten“ konfiguriert werden.</li> </ul>
Tür E/A 2	
Profil 1	Für Leser mit einer grünen und einer roten LED.
Profil 2	Für VANDERBILT-Leser mit einer gelben LED (AR618X).
Profil 3	Profil 3 wird für HID-Leser verwendet, die nach dem Lesen einer Karte eine PIN mit einem vordefinierten Standortcode an die Zentrale senden (0).
Profil 4	Profil 4 wird für HID-Leser verwendet, die nach dem Lesen einer Karte eine PIN mit einem vordefinierten Standortcode an die Zentrale senden (255).
Profil 5	Wählen Sie diese Option für Sesam-Leser. Es empfiehlt sich, die Option Übergehen der Leserprofile auszuwählen, um Rückmeldung zum Schärfungsvorgang zu erhalten.

### Bearbeiten von Meldergruppen/Ausgängen eines Tür-E/As

1. Wählen Sie eine MG/einen Ausgang für den Tür E/A.
2. Klicken Sie auf die Schaltfläche **Bearbeiten**.
3. Die beiden Eingänge und der Ausgang, die zum E/A dieser Tür gehören, können als normale Ein- und Ausgänge konfiguriert werden. Siehe Seite [→ 147].
4. Um die Eingänge verwenden zu können, müssen sie eine MG-Nummer zugewiesen werden.

# 12 Funk

Die Funkmeldererkenkung (868 MHz) auf der SPC-Zentrale funktioniert über Funkempfängermodule, die bereits werksseitig im Bedienteil oder auf dem Controller installiert sein können oder durch ein Funkerweiterungsmodul im System integriert wurden.



1. Klicken Sie auf die Registerkarte **Liste**.
2. Weitere Informationen finden Sie in der nachstehenden Tabelle.

**Funkmelder**

Funkmelder	ID	Typ	MG	Funküberwachung
1	26661450	Magnetkontakt	30 - []	AN
2	59132927	Bewegungsmelder	32 - []	AN
3	26661470	Magnetkontakt	33 - [Test 1]	AN
4	26662209	Magnetkontakt	36 - [Test 2]	AN
5	26329994	Magnetkontakt	38 - [Test 3]	AN

Funkmelder	Die Nummer des im System angemeldeten Melders (1 = erster, 2 = zweiter usw.)
ID	Eine eindeutige ID für den Melder.
Typ	Typ des erkannten Funkmelders (Magnetkontakt, Vibration/Stoß usw.)
Meldergruppe	Die MG, in welcher der Melder angemeldet wurde.
Batterie	Der Status der Batterie im Melder (falls vorhanden).
Funküberwachung	Der Status der Überwachungsfunktion (OK = Überwachungssignal empfangen, Nicht Überwacht = keine Überwachungsfunktion).
Signal	Die Signalstärke, die vom Melder empfangen wurde (01=gering, 09=hoch). <b>Hinweis:</b> Ein Gerät mit einer Signalstärke unter 3 kann nicht eingelernt werden. Ein Gerät, dessen Signalstärke nach dem Einlernen unter den Wert 3 fällt, wird jedoch nicht abgemeldet.

## Ausführbare Aktionen

Funkmelder löschen	Klicken Sie auf diese Schaltfläche, um den markierten Funkmelder von der Zentrale zu entfernen. Bestätigen sie die Aktion.
Zeige Logbuch Funkmelder	Anklicken, um das Protokoll des Funksensors anzuzeigen. Siehe Seite [→ 122].

Nicht eingelernte Melder anzeigen	Anklicken, um die Liste der von der Zentrale erkannten, nicht eingelernten Melder anzuzeigen. Siehe Seite [→ 122].
-----------------------------------	--

## 12.1 Log - Funkmelder X

Anzeigen eines Ereignisprotokolls für einen Funkmelder:

1. Markieren Sie einen Funkmelder.
2. Klicken Sie auf die Schaltfläche **Zeige Logbuch Funkmelder** .
3. Weitere Informationen finden Sie in der nachstehenden Tabelle.

Datum/Uhrzeit	Datum und Uhrzeit des protokollierten Ereignisses.
Empfänger	Einbauort des Funkempfängers, d. h. Funkempfänger am Bedienteil, auf dem Controller oder im Funk-Erweiterungsmodul installiert.
Signal	Die Signalstärke, die vom Melder empfangen wurde (01=gering, 09=hoch).
Status	Der physische Status des Melders.
Batterie	Der Status der an den Melder angeschlossenen Batterie (OK, Störung).

## 12.2 Nicht eingelernte Funkmelder

Ansehen einer Liste aller Funkmelder, die in der Zentrale erkannt, aber noch nicht eingelernt wurden:

1. Klicken Sie auf die Schaltfläche **Nicht eingelernte Melder anzeigen**.
2. Weitere Informationen finden Sie in der nachstehenden Tabelle.

Funkmelder-ID	Die ID-Nummer, mit der dieser Melder eindeutig identifiziert wird. Diese Nummer ist erst zugänglich, wenn ein Signal vom Funkmelder der SPC-Zentrale empfangen wird.
Typ	Der Typ des erkannten Funkmelders (Magnetkontakt, Vibrations-/Stoßkontakt usw.).
Empfangen	Der Zeit- und Datumsstempel des letzten von diesem Melder empfangenen Signals.
Status	Der physische Status des Melders.
Empfänger	Der Ort des Funkempfängers, der das Signal von diesem Funkmelder erkannt hat.
Signal	Die Signalstärke, die vom Melder empfangen wurde (01=gering, 09=hoch). <b>Hinweis:</b> Wenn die Signalstärke geringer als 3 ist, wird der Funksensor nicht in der Liste <b>Nicht eingelernte Funkmelder</b> angezeigt.

## 12.3 Konfiguration Funk ändern

1. Klicken Sie auf die Registerkarte **Einstellungen**, um die Seite für Funkeinstellungen anzuzeigen.

2. Weitere Informationen finden Sie in der nachstehenden Tabelle.

Antenne	An das Funkmodul angeschlossenen Antennentyp (intern oder extern) aus dem Dropdown-Menü wählen. Der für das Funkmodul erforderliche Antennentyp hängt vom installierten Funkmodultyp ab.
Funküberwachung	Festlegen, ob ein Funkmelder, der als fehlend gemeldet wird, einen Sabotagealarm in der Zentrale auslöst. Ein Funkmelder wird als fehlend gemeldet, wenn die Dauer, in der kein Überwachungssignal vom betreffenden Melder empfangen wurde, die im Timer <b>Funkmelder fehlt</b> eingestellte Zeit überschreitet. Siehe Seite [→ 80].
Filter	Aktivieren, um schwache Funksignale zu filtern.
Erkennung Fremdfunk	Aktivieren, um einen Alarm zu generieren, wenn Fremdfunk erkannt wird.
FÜ Test Zeitplan	Wählen Sie, wie die SOS-Tasten auf einer Fernbedienung funktionieren sollen: <ul style="list-style-type: none"> <li>● Deaktivieren</li> <li>● Aktivieren</li> <li>● Aktiv (still)</li> <li>● Benutzer Medizin</li> <li>● Benutzer Bedrohung</li> <li>● Funk Ausgang</li> </ul>
FÜ-Test Zeitplan	Geben Sie eine maximale Dauer (in Tagen) zwischen zwei FÜ-Tests ein.
Funk Scharfsch.verhinderung	Geben Sie eine Zeitspanne in Minuten ein, nach der – wenn die Funküberwachungsmeldungen eines Melders nicht empfangen werden – die Scharfschaltung für den Bereich verhindert wird, in dem sich eine Funk-Meldergruppe befindet. Diese Einstellung gilt nur für die folgenden Einbruchmeldergruppen: <ul style="list-style-type: none"> <li>● Alarm</li> <li>● Einbruch verzögert</li> <li>● Endgültig scharf</li> <li>● Notruf</li> <li>● Überfall</li> <li>● Sabotage</li> <li>● Verschlussüberwachung</li> </ul>

	<ul style="list-style-type: none"> <li>● Körperschallmelder</li> <li>● Alles OK</li> <li>● Scharfschalteberechtigung</li> <li>● Sperrelement</li> </ul>
Geräteverlust	Geben Sie eine Zeitspanne in Minuten ein, nach der das Funkgerät (Melder oder FÜ) als fehlend gemeldet wird.

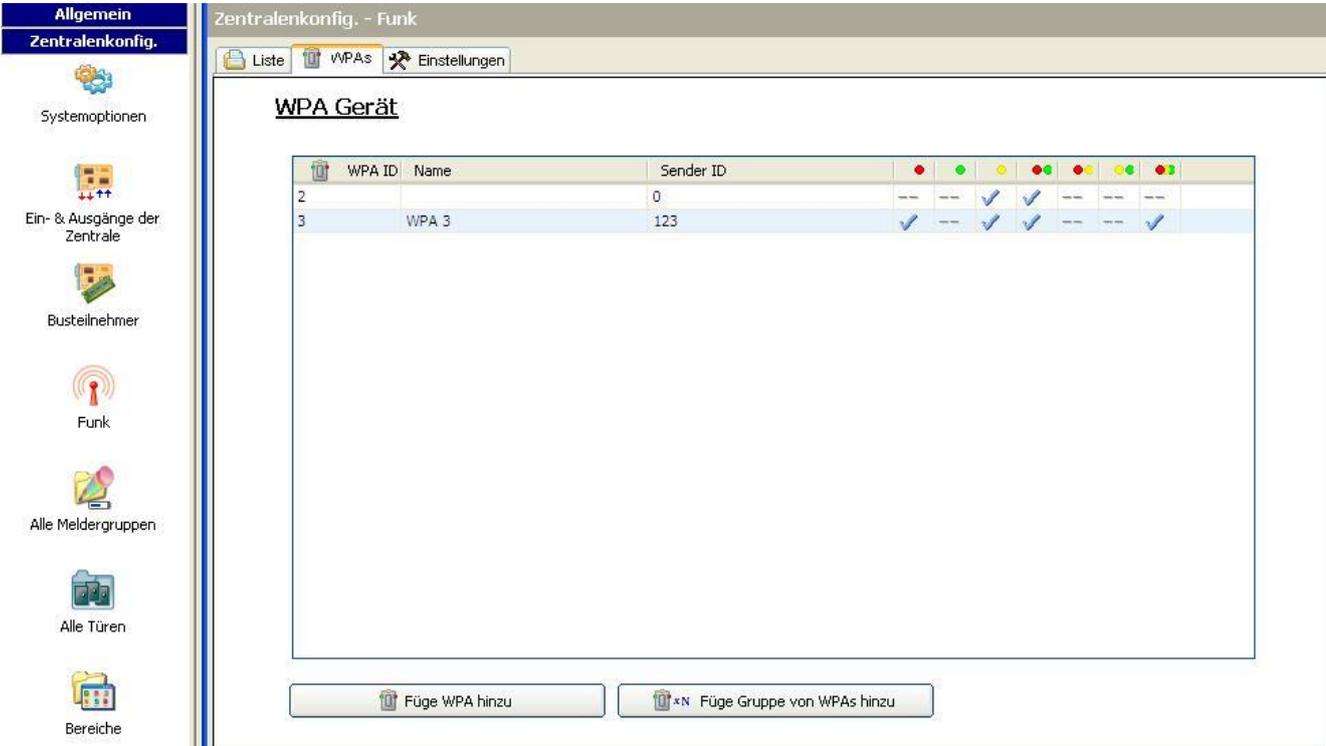
## 12.4 Konfigurieren eines FÜ

	<p><b>HINWEIS</b></p> <p>Die Seite für FÜ-Konfiguration und FÜ-Status wird nur angezeigt, wenn ein Funkmodul an die Zentrale oder an eines ihrer Erweiterungsmodule angeschlossen und die Zentrale für die angeschlossenen Modultypen zugelassen ist.</p>
---	---

Ein FÜ wird keinem Benutzer zugewiesen. Ein FÜ wird in der Regel von mehreren Leuten gemeinsam genutzt, z. B. von Wachleuten, die in verschiedenen Schichten arbeiten; alternativ können FÜs auch fest installiert werden, z. B. unter einer Tischplatte oder hinter einer Kasse.

Pro Zentrale sind maximal 128 FÜs erlaubt.

Wählen Sie für die Konfiguration eines FÜ mit SPC Pro die Optionen **Einstellungen** > **Funk** und anschließend die Registerkarte **WPAs**.



The screenshot shows the 'Zentralenkonfig. - Funk' window with the 'WPAs' tab selected. The 'WPA Gerät' table contains the following data:

WPA ID	Name	Sender ID							
2		0	---	---	✓	✓	---	---	---
3	WPA 3	123	✓	---	✓	✓	---	---	✓

At the bottom of the window, there are two buttons: 'Füge WPA hinzu' and 'Füge Gruppe von WPAs hinzu'.

Hier sind alle konfigurierten FÜs mit der entsprechenden ID aufgeführt. Eventuelle Tastenkombinationen für den FÜ werden auf dieser Seite ebenfalls angezeigt.

Klicken Sie auf **Füge WPA hinzu**, um einen FÜ hinzuzufügen und zu konfigurieren.

Klicken Sie auf **Füge Gruppe von WPAs hinzu**, um eine Gruppe von FÜs hinzuzufügen und zu konfigurieren.

## 12.4.1 Hinzufügen eines FÜ

Hinzufügen eines FÜ zum System:

- Klicken Sie auf der Hauptseite für FÜ-Geräte („WPA Gerät“) auf **Füge WPA hinzu**.
- ⇒ Die Seite zur Konfiguration eines neuen FÜ-Geräts wird angezeigt.

- Für die Konfiguration eines FÜ werden folgende Informationen verwendet:

Beschreibung/Name	Geben Sie eine eindeutige Beschreibung bzw. einen eindeutigen Namen für den FÜ ein.
Sender ID	Die Sender-ID ist auf das FÜ-Gehäuse gedruckt und kann hier manuell eingegeben werden. Sie können die ID auch per Fernzugriff abfragen, indem Sie eine beliebige Taste auf dem FÜ und anschließend auf <b>Lernen</b> klicken. Die Zentrale gibt automatisch die ID in dieses Feld ein, wenn momentan kein anderer FÜ dafür festgelegt ist.
Funküberwachung	Der Funküberfalltaster kann so konfiguriert werden, dass er ein regelmäßiges Überwachungssignal überträgt. Auf dem FÜ wird die Überwachung mithilfe eines Jumpers aktiviert. Die Überwachungsfunktion muss für den jeweiligen FÜ auch an der Zentrale aktiviert werden, damit die Überwachungsfunktion ordnungsgemäß

	<p>funktionieren kann. Falls die Zentrale kein Überwachungssignal empfängt, wird ein Alarm ausgelöst, der auf dem Bedienteil angezeigt und protokolliert wird.</p> <p>Wenn die Überwachungsfunktion nicht aktiviert ist, sendet das Funknotrufgerät alle 24 Stunden eine Überwachungsnachricht, um den Batteriestatus des Geräts an die Zentrale zu übermitteln. Der Sendezeitpunkt dieser Nachricht variiert nach dem Zufallsprinzip, um die Möglichkeit der Überschneidung mit den Sendungen anderer FÜs zu verringern.</p> <p>Aktivieren Sie das Kontrollkästchen <b>Überwachen</b>, wenn die Überwachung für den betreffenden FÜ aktiviert wurde.</p>
Test	<p>Aktivieren Sie das Kontrollkästchen <b>Test</b>, wenn regelmäßig ein FÜ-Test durchgeführt werden soll. Der Zeitrahmen für einen regelmäßigen Test wird auf der Seite Konfiguration Funk ändern konfiguriert.</p>
Zuweisen von Tasten	<p>Hier können Benutzer bestimmten Tastenkombinationen Funktionen zuweisen. Verfügbare Funktionen sind: Überfall, Notruf (Still), Bedrohung, Verdacht, WPA Medizin und Medizin. Es können mehrere Tastenkombinationen für die gleiche Funktion ausgewählt werden.</p> <p>Das oberhalb dargestellte Fenster zeigt die Standardeinstellungen für die Zentrale einer Installation in einer Bank:</p> <ul style="list-style-type: none"> <li>● Gelb – Verdacht</li> <li>● Rot + Grün – Überfall</li> </ul> <p>Für kommerzielle oder private Installationen ist die Standardeinstellung:</p> <ul style="list-style-type: none"> <li>● Rot + Grün – Panik</li> </ul> <p><b>Hinweis:</b> Wird einer Tastenkombination keine Funktion zugewiesen, ist es immer noch möglich, diese Kombination für einen Trigger zu verwenden. Siehe Trigger</p>

- Klicken Sie auf die Schaltfläche **Speichern**, um die Einstellungen zu speichern.

#### Siehe auch

 Konfiguration Funk ändern [→ 122]

# 13 Konfigurieren von Meldergruppen, Türen und Bereichen

## 13.1 Meldergruppe bearbeiten

Die Techniker- und Benutzeraktionen umfassen hier „Logbuch“, „Aus-/Einschalten“ und „Dauertest Ein/Aus“ für jede einzelne Meldergruppe im zulässigen Rahmen gemäß Sicherheitsgrad EN 50131 Grad 2 und EN 50131 Grad 3.

Zentralenkonfig.



Alle MG

1. Klicken Sie auf die Registerkarte **Liste**.

⇒ Daraufhin erscheint das folgende Fenster:

Zentralenkonfig. - Meldergruppen

Liste

Konfiguration der Meldergruppen

MG	Eingang	Beschreibung	Typ	Bereich	Attribute
1	✓ Zentrale - Eingang 1	Front door	Einbruch v...	1 - 1	
2	✓ Zentrale - Eingang 2	Sitting room	Einbruch	1 - 1	
3	✓ Zentrale - Eingang 3	Kitchen	Einbruch	1 - 1	
4	✓ Zentrale - Eingang 4	Upstairs front	Einbruch	1 - 1	
5	✓ Zentrale - Eingang 5	Upstairs rear	Einbruch	1 - 1	
6	✓ Zentrale - Eingang 6	PIR Hallway	Einbruch v...	1 - 1	
7	✓ Zentrale - Eingang 7	PIR Landing	Einbruch	1 - 1	
8	✓ Zentrale - Eingang 8	Panic button	Überfall	1 - 1	
9	✓ Erweiterung 1 - Eingan...		Einbruch	1 - 1	
10	✓ Erweiterung 1 - Eingan...		Einbruch	1 - 1	
11	✓ Erweiterung 1 - Eingan...		Einbruch	1 - 1	
12	✓ Erweiterung 1 - Eingan...		Einbruch	1 - 1	
13	✓ Erweiterung 1 - Eingan...		Einbruch	1 - 1	
14	✓ Erweiterung 1 - Eingan...		Einbruch	1 - 1	
15	✓ Erweiterung 1 - Eingan...		Einbruch	1 - 1	
16	✓ Erweiterung 1 - Eingan...		Einbruch	1 - 1	
17			Einbruch	1 - 1	
18			Einbruch	1 - 1	
19			Einbruch	1 - 1	
20			Einbruch	1 - 1	
21			Einbruch	1 - 1	

2. Wählen Sie eine MG aus der Liste.

⇒ Daraufhin erscheint das folgende Fenster.

3. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

4. Klicken Sie auf **OK**.

Konfiguration Meldergruppen

## Konfiguration Meldergruppen

MG konfigurieren...

**MG: 1**

**Beschreibung:** Front door

**Eingang:** Zentrale - Eingang 1

**Typ:** S/U Eingang

**Bereich:** 1 - Reception

**Kalender:** <kein Kalender>

**V-Zone:** --

**Attribute:**

<input type="checkbox"/>		Folgt. Verz.	<input type="checkbox"/>		Tastend
<input type="checkbox"/>		Nicht Intern A	<input type="checkbox"/>		Nur übertr.
<input type="checkbox"/>		Nicht Intern B	<input type="checkbox"/>		Ext. Zeitabbr.
<input type="checkbox"/>		24 Stunden	<input checked="" type="checkbox"/>		Ext. scharf erlaubt
<input type="checkbox"/>		Lokal	<input checked="" type="checkbox"/>		Unscharf erlaubt
<input type="checkbox"/>		Doppelausl.	<input type="checkbox"/>		Shunt
<input type="checkbox"/>		Türglocke	<input type="checkbox"/>		Übertragen
<input checked="" type="checkbox"/>		Sperrbar	<input type="checkbox"/>		Anzeigen am BT
<input type="checkbox"/>		Normal offen	<input type="checkbox"/>		Bedient. Summier
<input type="checkbox"/>		Still	<input type="checkbox"/>		Verzögert
<input type="checkbox"/>		Log	<input type="checkbox"/>		Übertr. nur bei scharf
<input type="checkbox"/>		Überwacht	<input type="checkbox"/>		Feuer Voralarm
<input type="checkbox"/>		Info vor Scharfsch.	<input type="checkbox"/>		Feuer Erkundungszeit
<input type="checkbox"/>		Automatischer	<input type="checkbox"/>		Unsch. lokal
<input checked="" type="checkbox"/>		Verz.Schärfung	<input checked="" type="checkbox"/>		Erzwungen Scharf

OK Abbrechen

Meldergruppe	Diese Nummer wird als Referenz angezeigt und kann nicht programmiert werden.
MG Text	Geben Sie einen Text ein (max. 16 Zeichen), der die MG eindeutig identifiziert.
Eingang	Der physische Eingang wird zu Referenzzwecken angezeigt und kann nicht konfiguriert werden.
Typ	Wählen Sie einen MG-Typ aus dem Dropdown-Menü (siehe Seite [→ 278]).
Bereich	Nur wenn (mehrere) <b>Bereiche</b> aktiviert sind. Wählen Sie aus dem Dropdown-Menü einen Bereich, dem die MG zugewiesen wird.
Kalender ⓘ	Wählen Sie ggf. den gewünschten Kalender (siehe Seite [→ 209]). Bei Sicherheitsgrad 2 / 3 kann ein Kalender nur MGs mit Typ "Abbruch Schärfungsverzögerung", "Technik", "Key Arm", "Shunt" und "X-Shunt". Bei

	Sicherheitsgrad "Unbeschränkt" kann eine Meldergruppe beliebigen Typs mit einem Kalender verbunden werden.
Attribute	Aktivieren Sie das relevante Kontrollkästchen für die MG. Es werden nur die Attribute angezeigt, die für den jeweiligen MG-Typ verfügbar sind (siehe MG-Attribute [→ 281]).

## 13.2 Bereich hinzufügen/bearbeiten

Zentralenkonfig.



Bereiche

▷ Nur wenn (mehrere) **Bereiche** aktiviert sind.

1. Klicken Sie auf die Registerkarte **Liste**.

⇒ Daraufhin erscheint das folgende Fenster:

Zentralenkonfig. - Bereiche/Bereichsgruppen

Liste Bereichsgruppen

### Bereichskonfiguration

Bereich	Typ	Text	Alarmv.	Scharf.V	Verb.	Calendar	Triggers
1	Standard ...	Premises	45	45			
2	Tres.		-	-			

Bereich hinz. Kurzkonfiguration Tresor/GAA Bereiche

2. Die Schaltfläche **Kurzkonfigurationsprogramm für Tresor-/GAA-Bereiche** [→ 145] bietet einen Shortcut zum Hinzufügen mehrerer Geldautomaten- und Tresorbereiche mit Standardkonfigurationseinstellungen.

3. Klicken Sie auf die Schaltfläche **Bereich hinz.**, um einen einzelnen Bereich hinzuzufügen oder klicken Sie auf einen Bereich aus der Liste, um ihn zu bearbeiten.

⇒ Daraufhin erscheint das folgende Fenster.

Bereichskonfiguration

## Bereich 2 Bearbeiten

Konfiguration des Bereichs

**Bereich :** 2

**Beschreibung :** Front Office

**Bereichsprofil :** Standard Bereich

**Alarmverz. :** 5 Sekunden

**Schärfungsverz. :** 5 Sekunden

**Austrittszeit inaktiv :**  Inaktiv

Intern Scharf Opt. Verknüpfte Ber S/US Ablaufplan Andere

### Optionen int. Scharfsch.

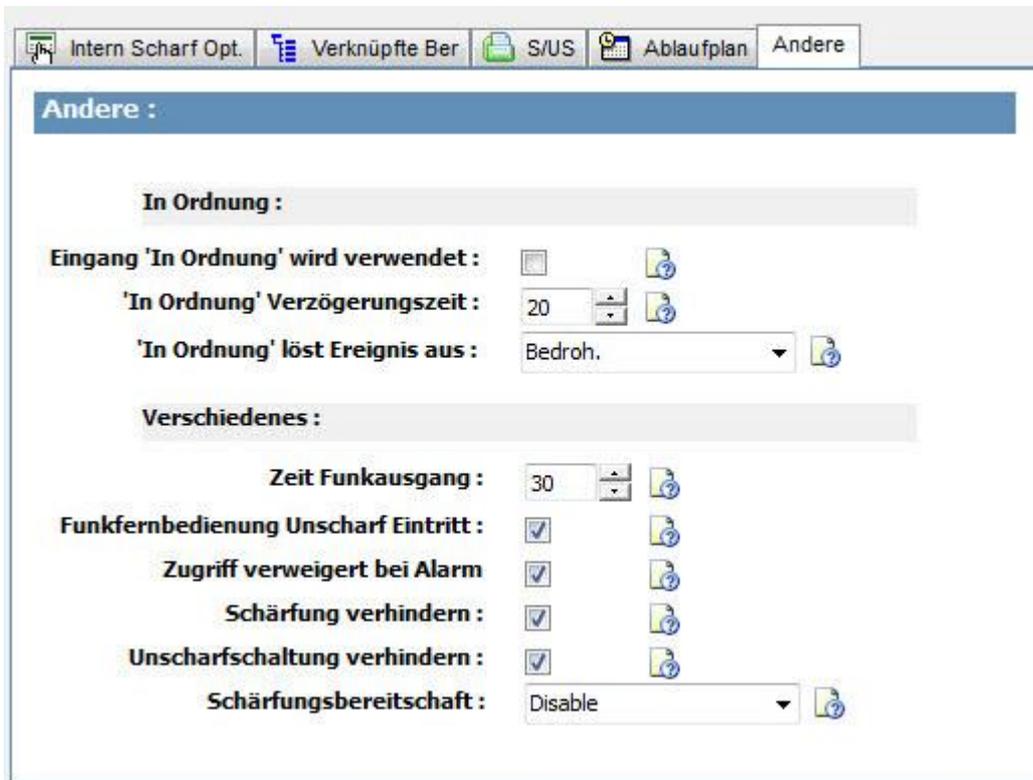
	Intern A	Intern B
Ermögliche Intern Scharf	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Intern verzögert	<input type="checkbox"/>	<input type="checkbox"/>
Folgt Verz. wird Einb. verz.	<input type="checkbox"/>	<input type="checkbox"/>
Einbruch verz.' wird 'Einbruch'	<input type="checkbox"/>	<input type="checkbox"/>
Lokal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Keine Sirene	<input type="checkbox"/>	<input type="checkbox"/>

Triggers

4. Geben Sie einen eindeutigen Namen für den Bereich ein.
5. Wählen Sie einen der folgenden Bereichstypen aus:
  - Standard – Für die meisten Bereiche geeignet.
  - GAA – Einstellungen und Standardkonfigurationen für Geldautomaten.
  - Tresor – Einstellungen und Standardkonfigurationen für Tresore.
  - Erweitert – Bietet sämtliche Bereichseinstellungen (Standard, GAA und Tresor).

- Konfigurieren Sie die Einstellungen für jeden Installationstyp wie in den folgenden Abschnitten beschrieben:

### 13.2.1 Einbruch verzögert

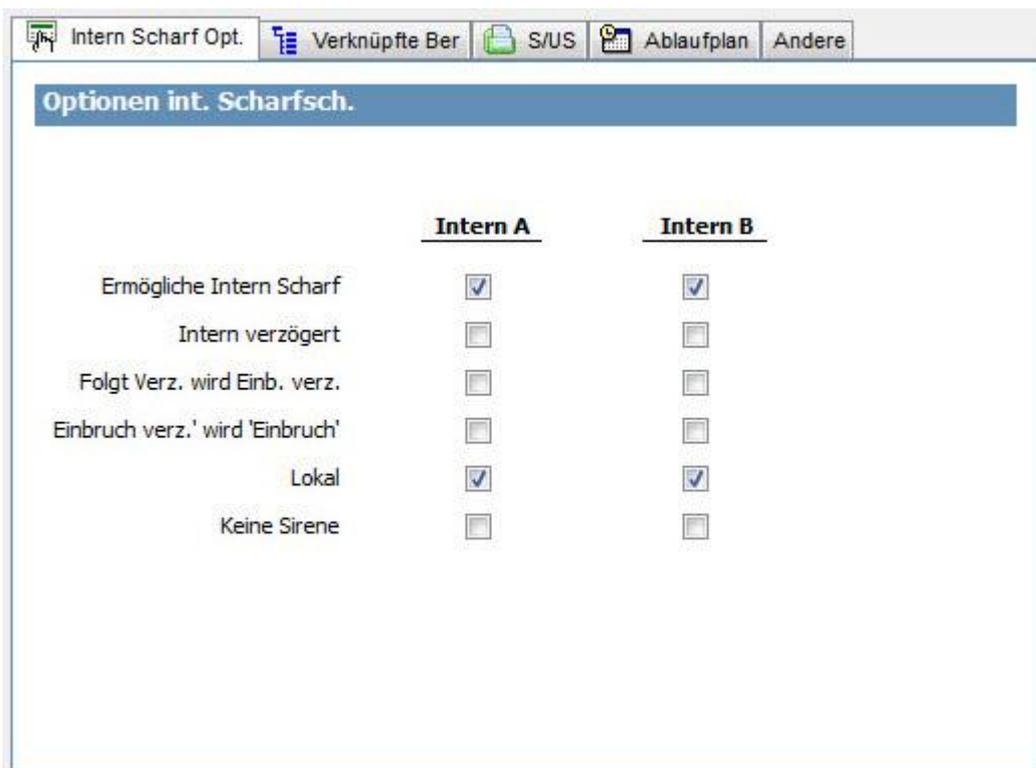


Konfigurieren Sie die folgenden Einstellungen für „Eintritt/Ausgang“:

Eintrittsverzögerung	Zeit (in Sekunden), die dem Benutzer zum Unscharfschalten des Alarms bleibt, nachdem eine verzögerte Meldergruppe eines scharf geschalteten Systems geöffnet wurde. Die Alarmverzögerung gilt für alle Meldergruppen mit Eintritt/Austritt in diesem Bereich (Werkseinstellung: 45 Sekunden).
Austrittsverzögerung	Die Zeit (in Sekunden), innerhalb der ein Benutzer einen überwachten Bereich verlassen muss, bevor die Scharfschaltung abgeschlossen ist. Sobald der Summer ertönt, um dem Benutzer anzuzeigen, dass das System scharf schaltet, nachdem die Verzögerungszeit abgelaufen ist, wird die verbleibende Zeit am Bedienteil bis Null rückwärts gezählt. Die Scharfschaltverzögerung gilt für alle Verzögerungsmeldergruppen in diesem Bereich (Werkseinstellung: 45 Sekunden).
Austrittsverzögerung deaktivieren	Wählen Sie diese Option, wenn keine Austrittsverzögerung erforderlich ist und die Einstellung MG „Endgültig scharf“ oder MG „Einbruch verz.“ mit Attribut „Ext. Zeitabbruch“ aktiviert wurde. Siehe Timer [→ 80].
Fernbedienung Unscharf Eintritt	Unscharfschalten mit der Fernbedienung ist nur möglich, wenn die Eintrittszeit läuft. Diese Option ist standardmäßig deaktiviert.
Zugang verweigert bei Alarm	Der Zutritt zum Bereich wird vorübergehend für den Zeitraum verweigert, der im Timer für die Aussperrung nach Alarm eingestellt wurde.
Schärfung verhindern	Wenn die Option aktiviert ist, verhindert das Bedienteil die Scharfschaltung.
Entschärfung verhindern	Wenn die Option aktiviert ist, verhindert das Bedienteil die Unscharfschaltung.
Scharfschalteberechtigung	Wird für die Konfiguration des Blockschlusses benutzt. Verfügbare

	<p>Optionen sind:</p> <ul style="list-style-type: none"> <li>● Deaktivieren</li> <li>● Scharf</li> <li>● Unscharf</li> <li>● Scharf- und unscharfschalten</li> </ul> <p>Wenn die Deaktiviert-Option ausgewählt ist (Standardeinstellung), schaltet das System scharf und unscharf ohne Änderung des Blockschlossvorgangs.</p> <p>Ist die Scharf-Option ausgewählt, ist ein Signal für „Scharfschalteberechtigung“ erforderlich, um diesen Bereich scharf zu schalten. Dieser Befehl kann von Bedienteilen oder einem MG-Eingang kommen (siehe Berechtigte Scharfschaltung des Blockschlusses). Der Benutzer kann das System vom Bedienteil aus nicht scharf schalten. Alle Bereiche, für die eine Scharfschalteberechtigung erforderlich ist, erscheinen auf dem Komfort-Bedienteil als gesperrt und werden beim Scharfschalten auf dem Standard-Bedienteil nicht angezeigt.</p> <p>Wenn die Unscharf-Option ausgewählt ist, kann der Benutzer den Bereich nicht von Bedienteilen aus unscharf schalten; er kann jedoch mit dem Bedienteil ein Scharfschalteberechtigungssignal generieren.</p> <p>Bei den Optionen Scharf und Unscharf kann der Benutzer zu keiner Zeit den Zustand eines Bereiches vom Bedienteil aus ändern.</p> <p>Es ist möglich, einen Timer für die Scharfschalteberechtigung zu konfigurieren. Siehe Timer [→ 80].</p>
--	--

## 13.2.2 Intern-scharf-Optionen



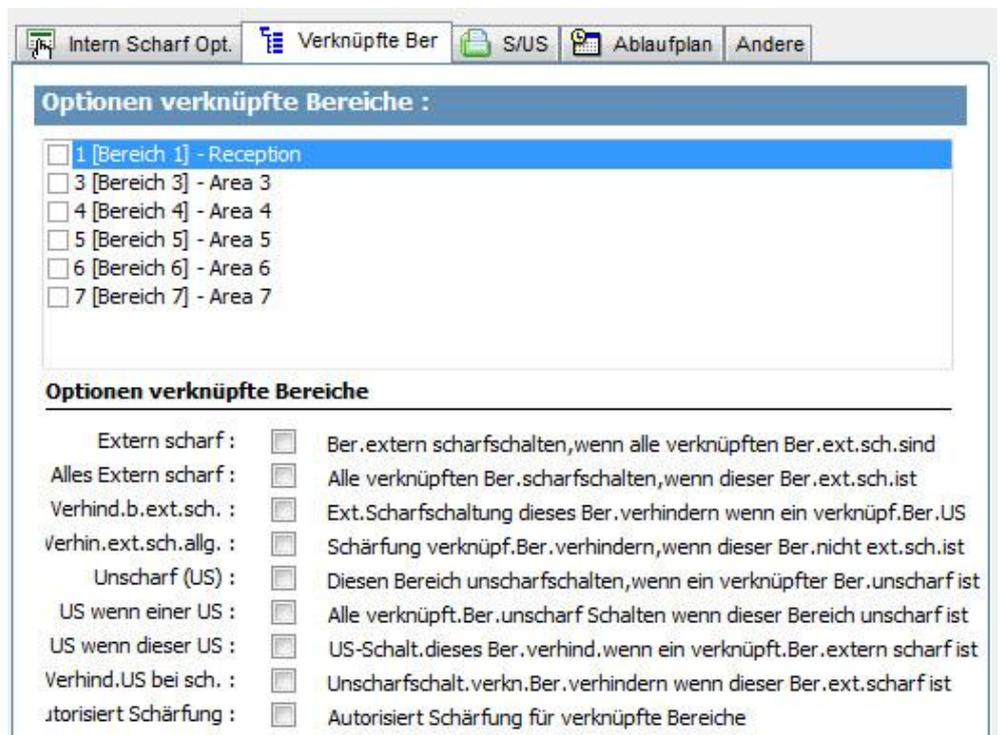
	<u>Intern A</u>	<u>Intern B</u>
Ermögliche Intern Scharf	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Intern verzögert	<input type="checkbox"/>	<input type="checkbox"/>
Folgt Verz. wird Einb. verz.	<input type="checkbox"/>	<input type="checkbox"/>
Einbruch verz.' wird 'Einbruch'	<input type="checkbox"/>	<input type="checkbox"/>
Lokal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Keine Sirene	<input type="checkbox"/>	<input type="checkbox"/>

Konfigurieren Sie bestimmte Meldergruppen für die Modi „Internscharf A“ und „Internscharf B“ wie im Folgenden beschrieben:

Intern scharf ermöglichen	Aktivieren Sie je nach Bedarf „Intern scharf“ für A und B.
Intern verzögert:	Kontrollkästchen Internscharf A oder B aktivieren, um die Scharfschaltungsverzögerung dem jeweiligen Modus

	zuzuweisen.
Folgt Verz wird Einb verz.:	Aktivieren Sie diese Kontrollkästchen, wenn sich Meldergruppen vom Typ „Folgt Verzögerung“ im Internscharf A- oder B-Modus wie Meldergruppen vom Typ „Einbruch verzögert“ verhalten sollen. Diese Funktion ist nützlich bei privaten Installationen, bei denen sich ein passiver Infrarotmelder (PIR-Melder) im Hausflur befindet. Wenn der Benutzer das System für die Nacht intern scharfstellt und sich in der Nacht im Haus bewegt, kann es sein, dass er unbeabsichtigt den PIR-Melder im Hausflur aktiviert und einen Alarm auslöst. Durch Einstellen der Option „Folgt Verz wird Einb verz.“, ertönt der Summer für die Dauer der Einbruchsverzögerung, nachdem der PIR-Melder ausgelöst wurde; so wird der Benutzer davor gewarnt, dass der Alarm aktiviert wird, wenn er keine Gegenmaßnahmen ergreift.
Einbruch verz wird Einbruch:	Aktivieren Sie dieses Kontrollkästchen, wenn sich Meldergruppen vom Typ „Einbruch verzögert“ im Internscharf A- oder B-Modus wie Meldergruppen vom Typ „Einbruch“ verhalten sollen. Diese Funktion ist nützlich bei privaten Installationen, wenn das System intern scharfgeschaltet wurde. Wenn der Benutzer das System für die Nacht intern scharfschaltet, möchte er möglicherweise, dass der Alarm sofort auslöst, wenn die Vorder- oder Hintertür während der Nacht geöffnet wird.
Lokal:	Aktivieren Sie dieses Kontrollkästchen, um das Melden von Alarmen im Internscharf-Modus auf lokale Meldungen zu beschränken (keine Fernmeldung).
Keine Sirenen	Wenn diese Option aktiviert wird, werden für Intern scharf A oder B keine Sirenen aktiviert.

### 13.2.3 Verbundene Bereiche



In diesem Abschnitt können Sie Bereiche für die Scharf- und Unscharfschaltung miteinander verbinden:

Extern Scharf	Bereich extern scharf schalten, wenn alle verbundenen Bereiche extern scharf sind.
Alle ext scharfsch.	Alle Bereiche extern scharf schalten, wenn dieser Bereich extern scharf ist.
Extern scharf verhindern	Für diesen Bereich eine externe Scharfschaltung verhindern, solange alle verbundenen Bereiche nicht extern scharf sind.
Alle extern scharf verhindern	Bei allen verbundenen Bereichen extern scharf verhindern, solange dieser Bereich nicht extern scharf ist.
Unscharf	Bereich unscharf schalten, wenn alle verbundenen Bereich unscharf geschaltet wird.
Alle unscharfsch.	Alle Bereiche unscharf schalten, wenn dieser Bereich unscharf ist.
Kein Unscharf	Ein Unscharfschalten dieses Bereichs verhindern, wenn ein verbundener Bereich extern scharf ist.
Kein Unscharf aller Bereiche	Die Unscharfschaltung aller verbundenen Bereiche wird verhindert, wenn ein Bereich extern scharf ist.
Scharfschaltung erlauben	Aktivierung der berechtigten Scharfschaltung für verbundene Bereiche. Siehe „Berechtigte Scharfschaltung des Blockschlusses“.
Verbundene Bereiche	Klicken Sie auf die Bereiche, die Sie mit diesem Bereich verbinden möchten.

## 13.2.4 Plan

Konfigurieren Sie Zeitpläne mithilfe der folgenden Einstellungen:

Kalender	Wählen Sie zur Zeitplansteuerung einen Kalender aus.
----------	--

Unscharf	Wählen Sie, ob der Bereich gemäß der im gewählten Kalender angegebenen Zeit automatisch unscharf gestellt werden soll.
Extern Scharf	Wählen Sie diese Option, um den Bereich für die Zeiten extern scharf zu schalten, die im ausgewählten Kalender festgelegt sind. Der Bereich wird ebenfalls scharfgeschaltet, wenn „Dauer Unscharf“ oder „Verzögerungsintervall“ abgelaufen ist (siehe Abschnitt Schärfen/Unschärfen [→ 135]). Wenn sich „Dauer Unscharf“ mit der festgelegten Zeit überschneidet, werden für diesen Bereich die Kalendereinstellungen angewendet.
Schließung nach Zeitplan	Wählen Sie diese Option, um den Bereich gemäß dem ausgewählten Kalender nach Zeitplan zu schließen. (Tresor-Bereich nur im Modus „Finanziell“)
Tresor-Zugang	Geben Sie die Anzahl der Minuten (0–120) ein, um diesen Timer nach Ablauf des Zeitintervalls für die Unscharfschaltung bei Schließung nach Zeitplan zu aktivieren. Wird der Bereich nicht unscharf geschaltet, nachdem der Timer abgelaufen ist, kann dieser Bereich nicht mehr unscharf geschaltet werden, bevor das nächste Zeitintervall für Unscharfschaltung bei Schließung nach Zeitplan beginnt. (Tresor-Bereich nur im Modus „Finanziell“)

### 13.2.5 Scharf-/Unscharfschalten



Folgende Parameter (mit Ausnahme des Verknüpfungs-/Verriegelungs-Parameters) sind nur in den nachstehend beschriebenen Fällen relevant:

- Ein Kalender ist ausgewählt (siehe Zeitplan [→ 134]), oder

- **Dauer Unscharf** ist aktiviert (und der zugewiesene Wert ist größer als Null), oder
- beide vorstehenden Bedingungen sind erfüllt.

Warnzeit (*)	Geben Sie die Anzahl der Minuten ein, während derer eine Warnung angezeigt wird, bevor automatisch scharf geschaltet wird. ( 0 - 30 ) Beachten Sie, dass die Zentrale entweder zur im Zeitplan definierten Zeit oder zu der Zeit scharf geschaltet wird, die im Parameter „Dauer Unscharf“ definiert wurde. Die erste Warnung wird zu dem hier konfigurierten Zeitpunkt vor der Zeit des Zeitplans angezeigt. Ab einer Minute vor Scharfschaltung werden weitere Warnungen angezeigt.
Abbruch durch Benutzer (*)	Mit dieser Funktion kann der Benutzer die automatische Scharfstellung abbrechen, indem er auf dem Bedienteil einen Code eingibt.
Verzögerung Benutzer (*)	Mit dieser Funktion kann der Benutzer die automatische Scharfstellung hinauszögern, indem er auf dem Bedienteil einen Code eingibt.
Schlüsselsch.	Bei dieser Funktion kann die automatische Scharfstellung mit einer Schlüsselschalter-Erweiterung hinausgezögert werden.
Verzögerungsintervall (*)	Geben Sie die Anzahl der Minuten ein, um die die automatische Scharfschaltung hinausgezögert werden soll. ( 1 - 300 )
Maximale Verzögerung (*)	Geben Sie die Anzahl der Male ein, um die die automatische Scharfschaltung verschoben werden kann. ( 0 – 99: 0 = unbegrenzt)
Verzögerte Unschärfung (*)	Geben Sie die Anzahl der Minuten ein, um die die automatische Unscharfschaltung hinausgezögert werden soll. ( 0 = keine Verzögerung)
Bereich verknüpfen	Wählen Sie eine Verknüpfungsgruppe aus, die Sie diesem Bereich zuweisen möchten. Bei einer Verknüpfung kann immer nur jeweils ein Bereich der Verknüpfungsgruppe unscharf geschaltet werden. Ein typischer Anwendungsbereich für diese Funktion sind GAA-Bereiche.
Dauer Unscharf (*)	Ist ein Bereich länger unscharf als hier eingestellt, wird er automatisch scharf geschaltet. (Bereich 0–120 min: 0 = nicht aktiv).
Doppelcode	Wenn diese Option aktiviert wurde, sind zwei PINs erforderlich, um einen Bereich mit dem Bedienteil scharf oder unscharf zu schalten. Beide PINs müssen Benutzern gehören, die das für den Vorgang (Scharf- oder Unscharfschalten) erforderliche Benutzerrecht besitzen. Wird der zweite PIN nicht innerhalb von 30 Sekunden oder falsch eingegeben, kann dieser Bereich nicht scharf oder unscharf geschaltet werden.

## Unterstützung für Überstunden

Ein gutes Beispiel für die Anwendung der Parameter für Scharf-/Unscharfschaltung ist eine Situation, in der in Räumen, für die ein automatisches Schärfen zu einer festgelegten Uhrzeit konfiguriert wurde, gelegentlich Überstunden anfallen und die automatische Scharfschaltung hinausgezögert werden muss.

Die Dauer der Verzögerung wird durch den Wert bestimmt, der im Parameter **Verzögerungsintervall** konfiguriert wurde. Mit dem Parameter **Maximale Verzögerung** wird festgelegt, wie oft das Scharfschalten verschoben werden kann. Für die Nutzung dieser Funktion benötigt der Benutzer den korrekten Wert unter **Verzögerung Benutzer**.

Die Scharfschaltung kann auf drei Arten verschoben werden:

1. Eingabe eines PINs über das Bedienteil.  
Das Standard-Bedienteil verfügt über die Menüoption VERZÖGERUNG. Die Verzögerungsfunktion kann mit den Tasten oben am Komfort-Bedienteil ausgeführt werden.
2. Mit einem Schlüsselschalter.  
Mit einer Rechtsdrehung des Schlüssels wird die Scharfschaltung des Systems um das voreingestellte Zeitintervall hinausgezögert, solange der Wert für die maximale Anzahl der Verzögerungsaktionen (**Maximale Verzögerung**) nicht überschritten wurde. Mit einer Linksdrehung des Schlüssels wird die Scharfschaltung um drei Minuten hinausgezögert (nicht konfigurierbar). Diese Funktion steht in unbegrenztem Maße zur Verfügung, unabhängig davon, wie oft die Schärfung verschoben wurde.
3. Mit einer Fernbedienung, FÜ oder einer Taste, die einen Trigger für **Auto Scharf Verz.** auslöst. (Siehe Seite 172)

## Vorübergehende Unscharfschaltung

Damit eine Anlage in einem im Kalender festgelegten Zeitraum vorübergehend unscharf geschaltet werden kann, müssen zuvor die folgenden drei Parameter konfiguriert werden:

1. **Kalender**  
Für den betreffenden Bereich muss ein Kalender konfiguriert und ausgewählt werden.
2. **Schließung nach Zeitplan**  
Damit dieser Bereich nur dann unscharf geschaltet werden kann, wenn dies laut konfiguriertem Kalender zulässig ist, muss diese Option aktiviert werden.
3. **Dauer Unscharf**  
Dieser Parameter muss auf einen Wert größer Null gesetzt werden, um eine Höchstdauer für die vorübergehende Unschärfung festzulegen.

Auf dem nachstehenden Bildschirm sind die geeigneten Einstellungen bereits konfiguriert:

Verknüpfte Ber S/AUS Ablaufplan Andere

### Optionen scharf/unscharf :

**Schärfen/Entschärfen :**

**Voralarmzeit :** \* 10

**Abbruch durch PIN :** \*

**Verzög.durch PIN :** \*

**Schlüsselschalter :** \* <Keine>

**Verzögerungszeit :** \* 60

**Anzahl Verz. :** \* 3

**US mit zwei Benutzer PIN :** -- Inaktiv

**Dauer Unscharf :** \* 0 Minutes

**Verz.Unscharf :** \* 10 Minutes

**Verriegelt :** Nicht verriegelt

**\* - Einstellungen beziehen sich auf Kalenderschärfung und Zeitrelevantes US-schalten**

---

Verknüpfte Ber S/AUS Ablaufplan Andere

### Ablaufplan (Kalender S/US) :

**Ablaufplan :** Vault

**Unscharf :**

**Extern Scharf :**

**Sperrzeit :**

**Tresorzugangszeit :** 0 Mins.

### 13.2.6 Alles in Ordnung

Bestätig. alles i.O.erforderlich	Wenn dieses Kästchen aktiviert ist, muss der Benutzer die Eingabe „alles in Ordnung“ bestätigen. Anderenfalls wird ein stiller Alarm ausgelöst. Weitere Einzelheiten zur Konfiguration eines MG-Eingangs „Alles in Ordnung“ siehe Meldergruppe bearbeiten [→ 127].
Bestätigungszeit für „alles in Ordnung“	Zeit in Sekunden bis ohne Bestätigung „alles in Ordnung“ ein stiller Alarm ausgelöst wird (Bereich 1–999 Sekunden)
Ereignis „Alles in Ordnung“	Wählen Sie den Ereignistyp aus, der übermittelt wird, wenn die Bestätigungszeit für „Alles in Ordnung“ abgelaufen ist. Die Optionen sind „Notruf (still)“, „Überfall“ und „Bedrohung“.

## 13.2.7 Übertragen

Intern Scharf Opt. Verknüpfte Ber SJS Ablaufplan Andere

**Ablaufplan (Kalender S/US) :**

Ablaufplan : -- <kein Kalender> [Suchen] [Kalender]

Unscharf :  [Suchen]

Extern Scharf :  [Suchen]

Sperrzeit :  [Suchen]

Tresorzugangszeit : 0 [Min.] [Suchen]

**Auswertung :**

	Aktiv	Timer	[Suchen]
Zu früh scharf :	<input type="checkbox"/>	0 [Suchen]	[Suchen]
Zu spät scharf :	<input type="checkbox"/>	0 [Suchen]	[Suchen]
Zu früh unscharf :	<input type="checkbox"/>	0 [Suchen]	[Suchen]
Zu spät unscharf :	<input type="checkbox"/>	0 [Suchen]	[Suchen]

Zentrale kann so konfiguriert werden, dass Scharf- Unscharfmeldungen ausserhalb der im Kalender geplanten Zeiten an die AES gesendet werden



Die Einstellungen für die Konfiguration von Meldungsübertragungen sind nur für Standard-Bereiche in kommerziellen Einrichtungen und Finanzinstituten anwendbar. Sie sind nur dann relevant, wenn ein Kalender ausgewählt wurde. (Siehe Abschnitt Zeitplan [→ 134])

Hier kann eingestellt werden, dass an das Kontrollzentrum oder an ausgewählte Mitarbeiter ein Bericht übertragen wird, falls die Zentrale außerhalb der im Kalender vorgegebenen Zeiten scharf oder unscharf geschaltet wird.

Zu früh scharf	Aktiviert die Übertragung eines Berichts, wenn die Anlage vor dem festgelegten Zeitpunkt und, bevor die Minuten im Timer-Feld verstrichen sind, manuell extern scharf geschaltet wird.
Zu spät scharf	Aktiviert die Übertragung eines Berichts, wenn die Anlage nach dem festgelegten Zeitpunkt und, nachdem die Minuten im Timer-Feld verstrichen sind, manuell extern scharf geschaltet wird.
Zu früh unscharf	Aktiviert die Übertragung eines Berichts, wenn die Anlage vor dem festgelegten Zeitpunkt und, bevor die Minuten im Timer-Feld verstrichen sind, manuell unscharf geschaltet wird.
Zu spät unscharf	Aktiviert die Übertragung eines Berichts, wenn die Anlage vor dem festgelegten Zeitpunkt und, bevor die Minuten im Timer-Feld verstrichen sind, manuell unscharf geschaltet wird.

Die Übertragung erfolgt per SMS oder über SIA und Contact-ID an eine Alarmempfangsstelle (Empfänger). Außerdem wird im Systemprotokoll ein Ereignis aufgezeichnet.

Übertragen werden nur Ereignisse, die für „Zu spät“ oder „Zu früh“ für den Bereich entsprechend konfiguriert wurden.

Die Übertragung von Ereignissen an eine Alarmempfangsstelle (ARC) oder per SMS muss zusätzlich aktiviert werden (nachfolgend beschrieben).

### Aktivieren der Übertragung von Meldungen zu ungewöhnlichem Scharf-/Unscharfschalten an einen Empfänger

Wählen Sie zur Konfiguration der Übertragung von Meldungen für eine Alarmempfangsstelle die Optionen **Kommunikation > ARC** aus. Daraufhin wird die Seite mit den Meldungsfiltern für die Alarmempfangsstelle angezeigt.

#### Kommunikation



**Filter Empfänger**  
Konfiguration des Empfängers

**Meldungsfilter**

<b>Alarmer</b>	<input checked="" type="checkbox"/> Alarm
<b>Rückst. Alarm</b>	<input checked="" type="checkbox"/> Rückstellung des Alarms
<b>Bestätigte Alarmer</b>	<input checked="" type="checkbox"/> Bestätigter Alarm
<b>Störungen/Sabo</b>	<input checked="" type="checkbox"/> Störung/Sabotage
<b>Rückst. Stör./Sabo</b>	<input checked="" type="checkbox"/> Rückstellung Störung/Sabotage
<b>Scharfsch.</b>	<input type="checkbox"/> Scharf-/Unscharfsch.
<b>Sperr./abschalt.</b>	<input type="checkbox"/> Sperrungen und Abschaltungen
<b>sonst. Meldungen</b>	<input type="checkbox"/> Sonstige Meldungen
<b>Türmeldungen</b>	<input type="checkbox"/> Meldungen der Zutrittskontrolle
<b>Alarm Abbruch</b>	<input type="checkbox"/> Alarmabbruch b. Eingabe gültiger PIN
<b>Früh/Spät</b>	<input checked="" type="checkbox"/> Scharf/Unscharf zu früh od. zu spät
<b>Netzwerk</b>	<input type="checkbox"/> Report von IP Netzwerkstörungen

**Bereiche**

- 1 - Reception
- 2 - Front Office
- 3 - Area 3
- 4 - Area 4
- 5 - Area 5
- 6 - Area 6
- 7 - Area 7

OK Abbrechen

Der Parameter **Scharf/Unscharf zu früh od. zu spät** ist aktiviert, um alle Scharf- bzw. Unscharfschaltungen außerhalb der im Zeitplan festgelegten Zeiten zu übertragen.

## Aktivierung der Übertragung von Meldungen zu ungewöhnlichem Scharf-/Unscharfschalten über SMS

Wählen Sie für die Technikerkonfiguration die Optionen **Allgemein** > **Benutzerkonfiguration**:

**Allgemein**



### SMS Konfiguration

Einstellen der SMS-Konfiguration für den Anwender

**SMS ID :** 5

**Benutzer :** 1: User 1

**SMS Nummer :**

**SMS-Meldungen :**

**Alarm :**

**Rückstellung Alarm :**

**Bestätigter Alarm :**

**Störungen/Sabo :**

**Rückst. Stör./Sabo :**

**Scharfsch. :**

**Früh/Spät :**

**Sperr./Abschalt. :**

**ungen der Zutrittskontrolle :**

**Andere :**

**SMS-Steuerung :**

FSET

USET

ASET

BSET

CLR

SSTA

LOG

ENGA

MANA

O

X

X Löschen

OK

Abbrechen

Aktivieren Sie Früh/Spät, um eine Scharf- oder Unscharfschaltung zu melden, die nicht dem Zeitplan entspricht.

## 13.2.8 Funk Ausgang



Andere :

**In Ordnung :**

- Eingang 'In Ordnung' wird verwendet :
- 'In Ordnung' Verzögerungszeit :
- 'In Ordnung' löst Ereignis aus :
- Funkfernbedienung Unscharf Eintritt :

**Funkausgang :**

Funkausgangszeit :

Zeit Funk Ausgang	Geben Sie die Zeit in Sekunden ein, während derer der Funkausgang aktiviert bleiben soll. Der Wert „0 Sekunden“ aktiviert und deaktiviert den Ausgang wechselweise.
-------------------	--



Informationen zu den anderen Optionen für Verschiedene finden Sie unter Einbruch verzögert [→ 131] für SPC Pro.

## 13.2.9 Bereich gesteuert

- Klicken Sie auf der Konfigurationsseite für Bereiche auf die Schaltfläche **Trigger**, um die Trigger für diesen Bereich zu konfigurieren.
- ⇒ Daraufhin wird die Seite für die Einstellung der Bereichstrigger angezeigt.



1. Klicken Sie auf einen Trigger, um die Bedingungen für diesen Trigger zu bearbeiten.
  2. Klicken Sie auf die Schaltfläche **Hinzufügen**, um einen neuen Trigger für den Bereich hinzuzufügen.
- ⇒ Daraufhin wird die Seite für die Aktions-Trigger für den Bereich angezeigt.



Wählen Sie einen Trigger aus und klicken Sie auf **Zuweisen**, um dem Bereich den Trigger zuzuweisen.

Mit den folgenden Schaltflächen können neue Trigger der Anlage hinzugefügt bzw. bestehende Trigger angezeigt oder bearbeitet werden:

	Hinzufügen eines neuen Triggers zur Liste.
	Trigger in der Liste anzeigen oder bearbeiten.

Konfigurieren Sie die Trigger für den Bereich mithilfe der folgenden Parameter:

Trigger	Wählen Sie einen Trigger aus der Dropdown-Liste aus.
Flanke	Der Trigger kann sowohl von der positiven als auch von der negativen Seite des Aktivierungssignals aus auslösen.
Aktion	<p>Diese Aktion wird ausgeführt, wenn der Trigger auslöst. Verfügbare Optionen sind:</p> <ul style="list-style-type: none"> <li>● Unscharf</li> <li>● Intern scharf A</li> <li>● Intern scharf B</li> <li>● Extern Scharf</li> <li>● Auto Scharf Verz. Diese Aktion verzögert die Scharfschaltung, wenn der Timer für „Auto Scharf“ läuft. Der Trigger fügt nur dann Zeit hinzu, wenn die maximale Anzahl der Verzögerungen nicht überschritten wurde. Jede Auslösung des Triggers verzögert die Scharfschaltung um das Zeitintervall, das unter der Option „Verzögerungsintervall“ (siehe Abschnitt Scharf-/Unscharfschalten [→ 135]) festgelegt wurde.</li> <li>● Alarme quittieren Hiermit werden alle Alarme in der konfigurierten MG gelöscht.</li> </ul>

**Hinweis:** Trigger können nicht von einem Bedienteil aus konfiguriert werden.

**Siehe auch**

 [Trigger \[→ 212\]](#)

## 13.2.10 Kurzkonfigurationsprogramm für Tresor-/GAA-Bereiche

Wenn Sie auf die Schaltfläche **Kurzkonfigurationsprogramm für Tresor/GAA Bereiche** klicken, wird die folgende Seite angezeigt:



Für Tresor- und GAA-Bereiche:

1. Geben Sie die Anzahl der zu konfigurierenden Tresor/GAA-Bereiche ein.
2. Aktivieren Sie das Kontrollkästchen **Verknüpfte Tresore/GAAs**, wenn alle Tresor- oder GAA-Bereiche verknüpft werden sollen.
3. Klicken Sie auf die Schaltfläche **Werkseinstellungen**, um die vorhandenen Standardeinstellungen zu bearbeiten, die für Tresor-/GAA-Bereiche konfiguriert wurden. (Weitere Informationen zur Konfiguration von Bereichen finden Sie unter Bereich hinzufügen/bearbeiten [→ 129].)
4. Klicken Sie auf **Erstelle Tresor/GAA Bereich jetzt**, um die angegebene Anzahl von Tresoren/GAAs zu erstellen.

### 13.3 Bereichsgruppe hinzufügen

Bereichsgruppen können zum Konfigurieren mehrerer Bereiche verwendet werden. So muss die Konfiguration nicht für jeden Bereich einzeln durchgeführt werden.

- ▷ Nur wenn die Option (mehrere) **Bereiche** aktiviert ist.

  1. Wählen Sie die Registerkarte **Bereichsgruppen**.
  2. Klicken Sie auf **Bereichsgruppe hinzufügen**.



1. Geben Sie einen Namen für die Gruppe ein.
2. Wählen Sie die Bereiche, die der Gruppe zugewiesen werden sollen.
3. Klicken Sie auf **OK**.
4. Klicken Sie auf **Neuen Bereich hinzufügen**, um einen neuen Bereich zu konfigurieren, der der Gruppe hinzugefügt werden kann.

	<p><b>HINWEIS</b></p> <p>Um Bereichsgruppen auf dem Komfort-Bedienteil zu verwenden, aktivieren Sie alle Bereiche auf der Registerkarte <b>Bereiche</b> in der <b>Zentrale</b> unter <b>Einstellungen &gt; Busteilnehmer &gt; Bedienteile &gt; Typ: Komfort-Bedienteil</b>.</p>
---	---

## 13.4 Tür bearbeiten

Zentralenkonfig.



Alle Türen

1. Klicken Sie auf die Registerkarte **Liste**.
2. Wählen Sie eine Tür aus der Liste.

**Türkonfiguration**  
 Konfiguration der Ein-/Ausgänge der Tür

**Tür-Eingänge:**

**Meldergruppe:** 37

**Beschreibung:** Door 1

**MG-Typ:** Einbruch verzögert

**MG-Attribute:** Bearbeiten

**Bereich:** 1 - Reception

**MK Endw.:** Endw. 4K7/4K7

**MK normal offen:**

**REX Endw.:** Keine

**REX normal offen:**

**Tür-Attribute:**

**Türgruppe:** Keine Gruppe

**Leserbereich betreten:** 1 - Reception

**Leserbereich verlassen:** 1 - Reception

Karte und Pin  
 Nur Pin (keine Karte)  
 PIN Code oder Karte  
 Pin zum Verlassen  
 Pin für scharf/unscharf  
 Freigabe bei Feuer  
 Begleitung  
 Hard Anti-Passback (\*)  
 Soft Anti-Passback (\*)

Türaufbruch ignorieren  
 Unscharf am Eintrittsleser  
 Unscharf am Austrittsleser  
 Ext. scharf am Eintrittsleser  
 Ext. scharf am Austrittsleser  
 Limit. Zugang verriegelter Türen (\*)  
 Einst. Präfix  
 Summer  
 Aufsicht (\*)

(\*) - Türe muss zu einer Türgruppe gehören

**Tür-Timer:**

Parameter	Wert	Einheit	Min	Max	Beschreibung
Zutritt gewährt	3	Sekunden	1	255	Dauer für die die Tür freigegeben bleibt, nachdem der Zutritt gewährt wurde.
Zutritt verweigert	3	Sekunden	1	255	Dauer für die die Türstrg. nach einem ungültigen Ereignis gesperrt ist.
Tür zu lange offen	10	Sekunden	1	255	Zeit in der Tür geschl. werden muss, um einen 'Tür zu lange offen' Alarm zu verm
Tür offen gelassen	10	Minuten	1	180	Zeit in der Tür geschl. werden muss, um einen 'Tür offen gelassen' Alarm zu verm
Verlängert	10	Sekunden	1	255	Freigabezeit für Benutzer mit dem Recht 'Verlängert'.
Begleitung	10	Sekunden	1	30	Dauer für 'begleiteten' Zugang nach Vorhalten einer Karte mit Recht 'Begleitung'

**Tür-Kalender:**

**Tür gesperrt:** <kein Kalender>

**Tür freigegeben:** <kein Kalender>

**Tür-Trigger:**

Türtrigger bearbeiten

OK
Abbrechen

3. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.
4. Klicken Sie auf **OK**.

### Tür-Eingänge

Jede Tür hat zwei Eingänge mit vordefinierten Funktionen. Diese beiden Eingänge, der Magnetkontakt und der REX-Taster, können konfiguriert werden.

Name	Beschreibung
Meldergruppe	Der Magnetkontakt-Eingang kann auch als Einbruchmelder verwendet werden. Wird der Magnetkontakt-Eingang für die Einbruchmeldefunktion verwendet, muss die MG-Nummer, welcher der Magnetkontakt-Eingang zugewiesen ist, ausgewählt werden. Wird der Magnetkontakt nur für die Zutrittskontrolle verwendet, muss die Option „NICHT ZUGEWIESEN“ ausgewählt werden.  Wird der Magnetkontakt einer Einbruch-Meldergruppe zugewiesen, kann er wie eine normale Meldergruppe

Name	Beschreibung
	konfiguriert werden, verfügt dann jedoch über einen eingeschränkten Funktionsumfang (z. B. können nicht alle Meldergruppentypen ausgewählt werden). Falls ein Bereich oder das System mit dem Ausweisleser scharfgeschaltet wird, muss der Magnetkontakt-Eingang einer MG-Nummer und dem Bereich oder dem System, der bzw. das scharf geschaltet werden sollen, zugewiesen werden.
Beschreibung (Nur Web und SPC Pro)	Beschreibung der MG, welcher der Magnetkontakt zugewiesen ist.
MG Typ (Nur Web und SPC Pro)	Typ der Meldergruppe, welcher der Magnetkontakt zugewiesen ist. (Es sind nicht alle Meldergruppentypen verfügbar.)
MG-Attribute (Nur Web und SPC Pro)	Die Attribute der Meldergruppe, welcher der Magnetkontakt zugewiesen ist, können modifiziert werden.
Bereich (Nur Web und SPC Pro)	Der Bereich, welcher die MG und der Ausweisleser zugewiesen sind. (Falls der Ausweisleser zum Scharfschalten/Unscharfschalten verwendet wird, ist dies der Bereich, der scharf/unscharf geschaltet wird.)
Magnetkontakt (Web) MK ENDWIDERSTAND (Bedienteile) MK Endw. (SPC Pro)	Der dem Magnetkontakt zugehörige Widerstand. Wählen Sie den verwendeten Widerstandswert bzw. die Widerstandskombination.
MK normal offen	Auswählen, ob der REX-Taster ein normal offener oder normal geschlossener Eingang ist.
Freigabe Tür (Web) REX ENDWIDERST (Bedienteile) MK Endw. (SPC Pro)	Der mit dem REX-Taster verwendete Widerstand. Wählen Sie den verwendeten Widerstandswert bzw. die Widerstandskombination.
REX-Taster normal offen	Auswählen, ob der REX-Taster ein normalerweise offener Eingang ist oder nicht.
No DRS (Kein REX) (Nur Web und SPC Pro)	Wählen Sie diese Option, um das REX zu ignorieren. Wenn für die Tür ein DC2 verwendet wird, MUSS diese Option ausgewählt werden. Wenn sie nicht ausgewählt wird, öffnet sich die Tür.
Leserposition (Eingang/Ausgang) (Nur Web und SPC Pro)	Wählen Sie die Position für die Leser am Ein- und Ausgang aus.
Leserformate (Web) READER INFO (LESER-INFO) (Bedienteile)	Zeigt das Format des letzten mit jedem konfigurierten Leser genutzten Ausweises an (nicht in SPC Pro verfügbar).



Den Meldergruppen kann jede beliebige freie Meldergruppennummer zugewiesen werden. Die Zuweisung ist jedoch nicht fest. Wenn einer Meldergruppe die Nummer ,9' zugewiesen wird, werden die Meldergruppe und ein Eingangserweiterungsmodul mit der Adresse 1 an den X-Bus angeschlossen (der die Meldergruppennummern 9–16 verwendet). Die zugewiesene MG der Zweitürsteuerungseinheit wird zur nächsten freien MG-Nummer verschoben. Die Konfiguration wird entsprechend angepasst.

## Tür-Attribute



Falls kein Attribut aktiviert ist, kann ein gültiger Ausweis verwendet werden.

Attribut	Beschreibung
Ungültig	Die Karte ist vorübergehend gesperrt.
Türgruppe	Wird verwendet, wenn einem Bereich mehrere Türen zugewiesen sind und/oder die Funktion „Anti-Passback“, „Aufsicht“ oder „Schleuse“ angewendet werden soll.
"Karte und PIN"	Für den Zutritt sind Karte und PIN erforderlich.
Nur Pin	PIN erforderlich. Eine Karte wird nicht akzeptiert.
PIN Code oder Karte/Badge	Für den Zutritt sind Karte und PIN erforderlich.
PIN für Austritt	Am Austrittsleser wird eine PIN benötigt. Eine Tür mit Ein- und Austrittsleser ist erforderlich.
PIN für scharf/unscharf	Zum Scharfschalten/Unscharfschalten des zugewiesenen Bereichs ist eine PIN erforderlich. Vor Eingabe der PIN muss die Karte vorgehalten werden.
Unscharf außen (Browser) Unscharf am Eintrittsleser (SPC Pro)	System/Bereich wird unscharf geschaltet, wenn eine Karte am Eintrittsleser vorgehalten wird.
Unscharf innen (Browser) Unscharf am Austrittsleser (SPC Pro)	System/Bereich wird unscharf geschaltet, wenn eine Karte am Austrittsleser vorgehalten wird.
Bypass Alarm	Der Zugriff wird gewährt, wenn ein Bereich scharf geschaltet ist und die Tür einen Alarm- oder Zutritts-MG-Typ aufweist.
Ext. scharf außen (Browser) Ext. scharf am Eintrittsleser (SPC Pro)	Zentrale/Bereich wird extern scharfgeschaltet, wenn eine Karte am Eintrittsleser 2x vorgehalten wird.
"Extern scharf innen" Ext. scharf am Austrittsleser (SPC Pro)	Zentrale/Bereich wird extern scharfgeschaltet, wenn eine Karte am Austrittsleser 2x vorgehalten wird.
Erzwungen Scharf	Falls der Benutzer über Rechte verfügt, können sie die Scharfschaltung des Eingangslesers erzwingen.
Freigabe bei Feuer	Das Türschloss öffnet sich, wenn ein Feueralarm im zugewiesenen Bereich erkannt wird.
Alle Notfälle	Feuer in einem beliebigen Bereich entsperrt die Tür.
Begleitung	Die Begleitungsfunktion erfordert, dass privilegierte Ausweisinhaber andere Ausweisinhaber durch bestimmte Türen begleiten. Wird diese Funktion einer Tür zugewiesen, muss zuerst eine Karte mit „Begleitrecht“ vorgehalten werden, bevor andere Karteninhaber ohne dieses Recht die Tür öffnen können. Die Zeitspanne, innerhalb der Ausweisinhaber ihre Ausweise vorhalten können, nachdem ein Ausweis mit Begleitrecht vorgehalten wurde, kann für jede Tür separat eingestellt werden.
Hard Anti-Passback*	Anti-Passback ist an der Tür umzusetzen. Alle Türen müssen mit Eintritts- und Austrittslesern versehen sein und müssen einer Türgruppe zugewiesen werden. In diesem Modus müssen Karteninhaber ihre

Attribut	Beschreibung
	Zugangskarte verwenden, um an einer festgelegten Türgruppe Ein- und Auslass zu erhalten. Wenn der Inhaber einer gültigen Karte einen Antipassback-Bereich unter Zuhilfenahme seiner Karte betritt und diesen wieder verlässt, ohne seine Karte zu benutzen, verstößt er damit gegen die Antipassback-Regeln. Wenn der Karteninhaber nun versucht, den gleichen Bereich über die betreffende Türgruppe wieder zu betreten, wird ein Hard Antipassback-Alarm ausgelöst, und der Zutritt zu dem Bereich wird verweigert.
Soft Anti-Passback*	Antipassback-Verletzungen werden lediglich im Zutrittslogbuch eingetragen. Alle Türen müssen mit Eintritts- und Austrittslesern versehen sein und müssen einer Türgruppe zugewiesen werden. In diesem Modus müssen Karteninhaber ihre Zugangskarte verwenden, um an einer festgelegten Türgruppe Ein- und Auslass zu erhalten. Wenn der Inhaber einer gültigen Karte einen Antipassback-Bereich unter Zuhilfenahme seiner Karte betritt und diesen wieder verlässt, ohne seine Karte zu benutzen, verstößt er damit gegen die Antipassback-Regeln. Wenn der Karteninhaber nun versucht, diesen Bereich über die betreffende Türgruppe wieder zu betreten, wird ein Soft-Antipassback-Alarm ausgelöst. Dem Karteninhaber wird jedoch Zutritt zu dem Bereich gewährt.
Aufsicht*	Die Aufsichtsfunktion erlaubt es Karteninhabern mit Aufsichtsrecht (der Aufsichtsperson), anderen Karteninhabern (beaufsichtigten Personen) Zutritt zu einem Raum zu gewähren. Die Aufsichtsperson muss den betreffenden Raum zuerst betreten. Beaufsichtigte Personen dürfen den Raum nur betreten, wenn sich die Aufsichtsperson im Raum befindet. Die Aufsichtsperson darf den Raum erst wieder verlassen, wenn alle beaufsichtigten Personen den Raum verlassen haben.
Türsummer	Bei Türalarmen ertönt ein auf der Türsteuerungsplatine angebrachter Summer.
Türaufbruch ignorieren	Ein Aufbrechen der Tür wird nicht verarbeitet.
Verriegelt* (Browser) Limit. Zugang verriegelter Türen (SPC Pro)	Es kann nur jeweils eine Tür eines Bereichs geöffnet werden. Dies erfordert eine Türgruppe.
Eingabe Präfix	Freigabe mit Präfix (A,B,* oder #) Taste für Scharfschaltung
* Dies erfordert eine Türgruppe.	

### "Tür-Timer"

Timer	min.	Max.	Beschreibung
Zutritt gewährt	1 s	255 s	Dauer, für die die Tür freigegeben bleibt, nachdem der Zutritt gewährt wurde.
Zutritt verwehrt	1 s	255 s	Dauer, für die die Türsteuerung nach einem ungültigen Ereignis gesperrt ist, und keine Eingabe akzeptiert.

Timer	min.	Max.	Beschreibung
Tür zu lange offen	1 s	255 s	Zeit, in der die Tür geschlossen werden muss, um einen „Tür zu lange offen“-Alarm zu vermeiden.
Tür offen gelassen	1 min	180 Min.	Zeit, in der die Tür geschlossen werden muss, um einen „Tür offen gelassen“-Alarm zu vermeiden.
Verlängert	1 s	255 s	Zusätzlich verfügbare Zeit, nachdem der Zutritt für eine Karte mit dem Attribut 'Verlängerte Türöffnungszeit' gewährt wurde.
Begleitung	1 s	30 s	Zeit, innerhalb der ein Benutzer ohne Begleitrecht Zutritt erhält, nachdem eine Karte mit Begleitrecht vorgehalten wurde.

## Tür-Kalender

Tür gesperrt	Wählen Sie einen Kalender, um die Tür während der konfigurierten Zeit zu sperren. Eine Karte/PIN wird während dieser Zeit nicht akzeptiert.
Tür gesperrt	Wählen Sie einen Kalender, um die Tür während der konfigurierten Zeit freizugeben. Die Tür ist während der konfigurierten Zeit freigegeben.

## Tür-Trigger

Trigger	Beschreibung
Trigger, die die Tür einmalig freigeben.	Wenn der zugewiesene Trigger aktiviert wird, wird die Tür für einen definierten Zeitraum freigegeben und anschließend wieder gesperrt.
Trigger, der die Tür sperrt	Wenn der zugewiesene Trigger aktiviert wird, wird die Tür gesperrt. Eine Karte/PIN wird nicht akzeptiert.
Trigger, der die Tür freigibt	Wenn der zugewiesene Trigger aktiviert wird, wird die Tür freigegeben. Eine Karte/PIN wird zum Öffnen der Tür nicht benötigt.
Trigger, der die Tür in den Normalzustand versetzt	Wenn der zugewiesene Trigger aktiviert wird, wird die Tür auf Normalbetrieb zurückgesetzt. Sperren/Freigaben der Tür sind damit aufgehoben. Zum Öffnen der Tür ist eine Karte/PIN erforderlich.

### 13.4.1 Schleusenfunktion

Die Schleusenfunktion verhindert, dass die übrigen Türen innerhalb einer Türverriegelungsgruppe geöffnet werden, solange eine Tür dieser Gruppe offen ist. Nachstehend sind einige Verwendungsbeispiele für diese Funktion aufgeführt:

- Bei Zugangskontrollsystemen mit zwei Türen, wie sie in Banken und anderen Gebäuden verwendet werden: Normalerweise wird der Zutritt mit einem Drucktaster oder einem Kartenleser gesteuert. Eine grüne und eine rote LED zeigen an, ob die Tür geöffnet werden kann oder nicht.

- In GAA-Technikbereichen zur Verknüpfung von GAA-Türen: Normalerweise sind, zusätzlich zur Tür, durch die man den Bereich betritt, alle GAA-Türen miteinander verknüpft.

Einrichten einer Verriegelungsgruppe:

1. Erstellen Sie eine Türgruppe. Siehe Bearbeiten einer Tür [→ 147].
2. Legen Sie das Attribut **Interlock** für die gewünschten Türen der Gruppe fest. Siehe Bearbeiten einer Tür [→ 147].
3. Konfigurieren Sie einen Türausgang für den Schleusenbetrieb. Dieser Ausgang wird für alle Türen der Verriegelungsgruppe aktiviert, sobald eine Tür dieser Gruppe offen ist, einschließlich der geöffneten Türe.  
An diesen Ausgang könnte z.B. eine rote LED oder Lampe angeschlossen werden, um anzuzeigen, dass diese Tür nicht geöffnet werden kann, und invertiert könnte eine grüne LED oder Lampe angeschlossen werden.

Konfigurieren eines Ausgangs für die Schleusenfunktion.

Zentralenkonfig.



Busteilnehmer

1. Klicken Sie auf eine Erweiterung in der Liste.
2. Klicken Sie auf die Registerkarte **Ausgangszuweisung**, um den Ausgang für diese Erweiterung zu konfigurieren.
3. Wählen Sie die Option **Türausgang**. Wählen Sie anschließend die gewünschte Tür und den Eintrag **Türe verriegelt** als Ausgangstyp aus den Dropdown-Menüs aus.

**Ausgang bearbeiten** 

**Bearbeiten des Ausgangs 1** 

Ausgangseinstellungen konfigurieren...

**Ausgangszuweisung :**

**Ausgangszuweisung**

Systemausg.  
 Bereichsausg.  
 Meldergruppe  
 Log. Ausgang  
 **Türausgang**  
 Schlüsselsch.

**Ausgangskonfiguration :**

**Beschreibung :**

**Modus :**  

Erneute Ausl.

**An-Zeit :**   [100 ms]

**Aus-Zeit :**   [100 ms]

**Invertieren :**

**Log :**

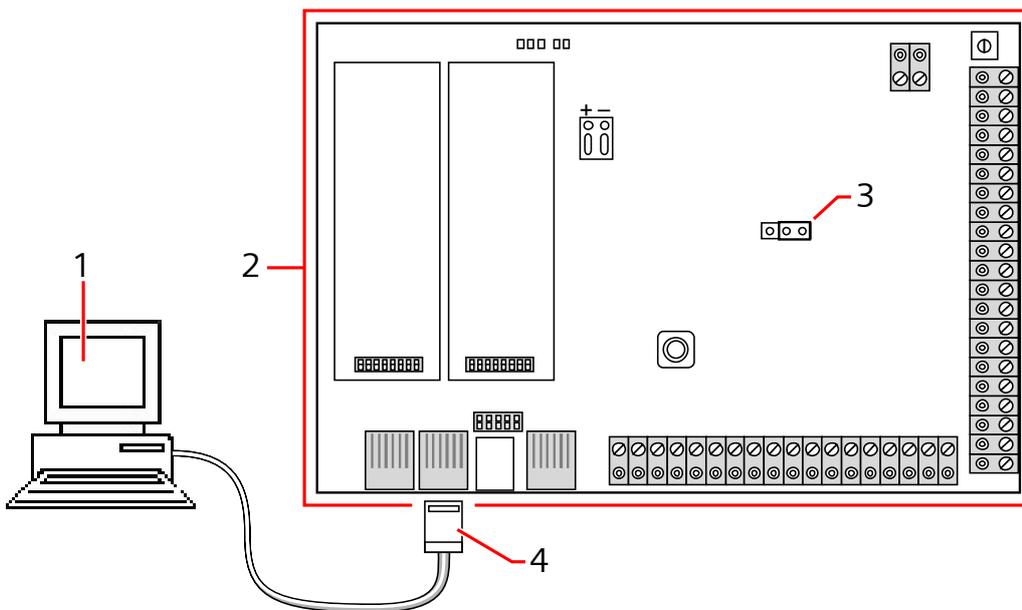
**Kalender :**    

# 14 Kommunikation konfigurieren

## 14.1 Serielle Schnittstellen

Der SPC-Controller verfügt über 2 serielle Ports (RS232) mit folgenden Funktionen:

- **X-10:** Der serielle Port 1 ist eine dedizierte Schnittstelle, die das X10-Protokoll unterstützt. Dieses Protokoll ermöglicht die Nutzung der im Gebäude vorhandenen Stromkabel zur Übertragung von Steuerdaten an X10-Geräte, sodass diese Geräte über den SPC-Controller aktiviert und überwacht werden können.
- **Ereignisprotokoll:** Der serielle Port 2 ermöglicht den Anschluss an eine serielle Schnittstelle an einem PC oder Drucker. Über diesen Anschluss kann ein Terminal-Programm so eingerichtet werden, dass es von der SPC-Zentrale ein Protokoll zu System- und Zugangsereignissen empfängt.
- **Systeminformationen:** Der serielle Port 2 bietet außerdem eine Schnittstelle über ein Terminal-Programm, das die Ausführung von Befehlen ermöglicht, mit denen bestimmte Systeminformationen von der Zentrale abgefragt werden können. Dieses Programm ist nur als Tool zum Beheben von Fehlern und Abfragen von Informationen erhältlich und sollte ausschließlich von erfahrenen Errichtern verwendet werden.



1	PC mit seriellem Port und Hyperterminal
2	SPC-Zentrale
3	JP9 <u>4000</u>
4	RS232

Konfigurieren der seriellen Anschlüsse:

**Kommunikation**



Ser.

Schnittstellen

- Klicken Sie auf die Registerkarte **Einstellungen**.

⇒ Daraufhin erscheint das folgende Fenster:

Die angezeigten Einstellungen hängen vom Verbindungstyp ab, für den die Schnittstellen verwendet werden. Die Einstellungen werden in den folgenden Abschnitten beschrieben:

## 14.2 Modems

Die SPC-Zentrale verfügt über zwei Onboard-Modemsteckplätze (primär und Backup), welche die Installation von PSTN- und/oder GSM-Geräten auf dem System ermöglichen.



Während der Ersteinrichtung des Systems über das Bedienteil nach einer Rücksetzung auf Werkseinstellung erkennt die Zentrale, ob ein primäres oder ein Backupmodem angeschlossen ist. Nach der Erkennung wird der Modemtyp angezeigt und das Modem bzw. die Modems wird/werden automatisch mit der Standardkonfiguration aktiviert. In dieser Phase sind keine weiteren Modemkonfigurationen erlaubt.

Konfigurieren der Modems:

**Hinweis:** Ein Modem muss installiert und vom System erkannt worden sein. (Siehe Abschnitt Installation von Einsteckmodulen)

### Kommunikation



- Aktivieren Sie das Kontrollkästchen **Aktiv** und konfigurieren Sie die Modems.

## Modemkonfiguration

## Modem 1 (Primär)

**Aktiv:**

**Modemtyp:** GSM

**Land:** Irland

**Anrufannahme:** 0-Niemals antworten

**Klingelanzahl:** 0

**Eingehende Anrufe:**  Nur antworten, wenn der Technikerzugang freigegeben ist

**Amtsholung:** Amtsholung

**Überwachung der Telefonl.:** Inaktiv

**Timer Überw. der Telefonl.:** 0 bis 999 Sekunden

**SMS aktivieren:**  Aktiv

**SMS-Servernummer:** 17409900 (nur PSTN)

**SIM-PIN:** (nur GSM)

**SMS-Test:** Test

**Routine-SMS-Intervall:** Inaktiv

**Routine-SMS #:**

GPRS-Einstellungen

## Modem 2 (Backup)

**Aktiv:**

**Modemtyp:** GSM

**Land:** Irland

**Anrufannahme:** 0-Niemals antworten

**Klingelanzahl:** 0

**Eingehende Anrufe:**  Nur antworten, wenn der Technikerzugang freigegeben ist

**Amtsholung:** Amtsholung

**Überwachung der Telefonl.:** Inaktiv

**Timer Überw. der Telefonl.:** 0 bis 999 Sekunden

**SMS aktivieren:**  Aktiv

**SMS-Servernummer:** (nur PSTN)

**SIM-PIN:** (nur GSM)

**SMS-Test:** Test

**Routine-SMS-Intervall:** Inaktiv

**Routine-SMS #:**

GPRS-Einstellungen



SMS-Erkennung und -Konfiguration sind erst verfügbar, nachdem die installierten Modems konfiguriert und aktiviert wurden.

## 14.2.1 SMS-Test

Wurde die SMS-Funktion für ein Modem aktiviert, kann ein Funktionstest durch Versenden einer Nachricht an eine gewünschte Empfängernummer durchgeführt werden.

1. Geben Sie die Mobiltelefonnummer (mit dreistelliger Ländervorwahl) in das Nummernfeld und eine kurze Textnachricht in das Nachrichtenfeld ein.
2. Klicken Sie auf **SMS versenden** und prüfen Sie, ob die Nachricht auf dem Mobiltelefon empfangen wird.



Der SMS-Test dient ausschließlich dem Zweck, die korrekte Funktionsweise der SMS-Funktion zu überprüfen. Verwenden Sie für den Funktionstest eine kurze Textnachricht mit alphabetischen Zeichen (A-Z).

Die SMS-Funktion verwendet ein Standardprotokoll, das auch in SMS-fähigen Telefonen verwendet wird. Bitte beachten Sie, dass nicht alle PSTN-Betreiber den SMS-Dienst über PSTN anbieten. Damit SMS über PSTN funktioniert, müssen folgende Kriterien erfüllt sein:

- Die Rufnummernanzeige muss am Telefonanschluss aktiviert sein.

- Es muss sich um einen Direktanschluss handeln – nicht um einen Anschluss über eine Telefonanlage oder sonstige Telekommunikationsanlagen.
- Bitte beachten Sie auch, dass die meisten Telekommunikationsdiensteanbieter nur SMS an ein im gleichen Land angemeldetes Telefon zulassen (aus abrechnungstechnischen Gründen).

## 14.2.2 SMS-Funktion

Der SPC-Controller unterstützt das Versenden von Textnachrichten (SMS) auf Systemen mit installierten Modems. Nachdem ein Modem installiert wurde, sind die folgenden Konfigurationen für die Nutzung des SMS-Dienstes erforderlich:

- SMS-fähiges Modem. Siehe Seite.
- SMS-Authentifizierung. Siehe Seite.
- Techniker-SMS-Steuerung. Siehe Seite.
- Benutzer-SMS-Steuerung. Siehe Seite.

Je nach Konfiguration sind folgende SMS-Funktionen verfügbar:

- Ereignismeldung. Siehe Seite.
- Fernsteuerung über SMS-Befehle (Benutzern können ausgewählte Befehle zugewiesen werden). Siehe Seite.

## 14.2.3 SMS-Systemoptionen

Sobald ein Modem installiert und die SMS-Funktion aktiviert wurde, muss die SMS-Authentifizierung zur Nutzung der SMS-Steuerung konfiguriert werden.

1. Wählen Sie **Konfiguration > System > Systemoptionen**.
2. Wählen Sie die gewünschte Option aus dem Dropdown-Menü **SMS-Authentifizierung**:
  - **Nur Pin**: Anmeldung über eine gültige Benutzer-PIN. Siehe Seite.
  - **Nur Rufnummer**: Anmeldung über die Telefonnummer (einschl. der dreistelligen Ländervorwahl), die für die Benutzer-SMS-Steuerung konfiguriert wurde. Nur wenn diese Option ausgewählt wurde, steht die SMS-Steuerung zur Konfiguration durch den Benutzer zur Verfügung.
  - **PIN + Rufnummer**
  - **NUR SMS PIN**: Anmeldung über eine für den Benutzer konfigurierte, gültige PIN; dabei handelt es sich nicht um die Anmelde-PIN des Benutzers! Siehe Seite. Nur wenn diese Option ausgewählt wurde, steht die SMS-Steuerung zur Konfiguration durch den Benutzer zur Verfügung.
  - **SMS-PIN + Rufnummer**

## 14.2.4 SMS-Befehle

Ist die SMS-Konfiguration abgeschlossen, können die SMS-Funktionen aktiviert werden. Befehle werden je nach SMS-Konfiguration über eine PIN oder eine Rufnummer an die Zentrale übertragen. Der Codetyp hängt von der Einstellung für die SMS-Authentifizierung ab. Weitere Informationen über die SMS-Authentifizierung finden Sie auf Seite [· 136].

Die nachfolgende Tabelle enthält alle verfügbaren SMS-Befehle. Die auf einen Befehl folgenden Aktionen und Reaktionen sind ebenfalls aufgeführt.

SMS-Befehle werden als Texte an die Telefonnummer der SIM-Karte im Controller gesendet.

Bei Befehlen, die eine PIN erfordern, besteht der Text aus der PIN gefolgt von einem Leerzeichen oder einem Punkt (wahlweise). Dabei steht \*\*\*\* für die PIN, und der anschließende Text ist der Befehl: \*\*\*\*.befehl oder \*\*\*\* befehl.

Beispiel: Der Befehl "HELP" (HILFE) = \*\*\*\* HELP oder \*\*\*\*.HELP.

BEFEHLE (**** = PIN)			
Mit PIN	Mit Rufnummer	Aktion	Reaktion
**** HELP ****.HELP	HELP	Alle verfügbaren Befehle werden angezeigt.	Alle verfügbaren Befehle
**** FSET (FULLSET) ****.FSET	FSET	Extern Scharfschaltung	Datum/Uhrzeit der Systemaktivierung. Falls zutreffend: Anzeige offener/erzwungen scharfer MGs
****ASET (PARTSET A) ****.ASET		Intern A Scharfsch via SMS zulassen	
**** BSET (PARTSET B) ****.BSET			
**** USET ****.USET	USET	Unscharfschaltung	System unscharf geschaltet
**** SSTA (STATUS) ****.SSTA	SSTA	Status anzeigen	Status des Systems und der zugehörigen Bereiche
**** XA1.ON ****.XA1.ON		In den Fällen, in denen das X10-Gerät als „A1“ konfiguriert ist, wird es eingeschaltet.	Status von „A1“
**** XA1.OFF ****.XA1.OFF		In den Fällen, in denen das X10-Gerät als „A1“ konfiguriert ist, wird es ausgeschaltet.	Status von „A1“
**** LOG ****.LOG		Letzte Meldungen werden angezeigt (bis zu 10)	Letzte Meldungen
**** ENG.ON ****.ENG.ON	ENG.ON	Technikerzugang freigeben	Technikerstatus
**** ENG.OFF ****.ENG.OFF	ENG.OFF	Technikerzugang sperren	Technikerstatus
**** MANA.ON ****.MANA.ON		Herstellerzugang freigeben	Herstellerstatus
**** MAN.OFF ****.MAN.OFF		Herstellerzugang sperren	Herstellerstatus
**** O5.ON ****.O5.ON		Wo der Ausgang als „O5“ konfiguriert ist, wird er eingeschaltet.	Status von „O5“
**** O5.OFF ****.O5.OFF		In den Fällen, in denen der Ausgang als „O5“ konfiguriert ist, wird er ausgeschaltet.	Status von „O5“



Der Ausgang verwendet für die SMS-Erkennung das Format ONNN; O steht für den Ausgang, NNN sind numerische Platzhalter, die nicht alle zwingend erforderlich sind. Beispiel: „O5“ für Ausgang 5.

Das X-10-Gerät verwendet für die SMS-Erkennung das Format: XYNN; X steht dabei für X-10, Y steht für die alphabetische ID, und NN sind die verfügbaren numerischen Platzhalter. Beispiel: XA1.

## 14.2.5 PSTN-Modem

Kommunikation



Modem-Konfiguration

1. Klicken Sie auf die Registerkarte **Einstellungen**.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

Modemkonfiguration

**Modem 1 (Primär)**

**Aktiv :**

**Modemtyp :** PSTN

**Land :** Deutschland

**Anrufannahme :** 1-Nach 'x' Ruftönen antworte

**Klingelanzahl :** 3

**Eingehende Anrufe :**  Nur antworten, wenn der Technikerzugang freigegeben ist

**Amtsholung :** Amtsholung

**Überwachung der Telefonl. :** Aktiv

**Timer Überw. der Telefonl. :** 300 0 bis 999 Sekunden

**SMS aktivieren :**  Aktiv

**SMS-Servernummer :** 9003266900 (nur PSTN)

**SIM-PIN :** (nur GSM)

**SMS-Test :** Test

**Routine-SMS-Intervall :** Inaktiv

**Routine-SMS # :**

### Modemkonfiguration

Land	Wählen Sie das Land, in dem die SPC installiert ist.
SIM-PIN	Nur für GSM. Geben Sie die PIN für die SIM-Karte im GSM-Modul ein.

Roaming zulassen	Wählen Sie diese Option um GSM-Roaming zu aktivieren. <b>Hinweis:</b> Bei Veränderung dieser Einstellung wird das Modem zurückgesetzt. <b>Hinweis:</b> Auf GSM-Modems der Version 3.08 oder höher unterstützt.
Eingehende Anrufe	Für die Anrufannahme-Funktion des Modems sind folgende Einstellungen möglich: <ul style="list-style-type: none"> <li>● Keine Anrufe annehmen: Das Modem nimmt grundsätzlich keine Anrufe an.</li> <li>● Nach x Ruftönen annehmen: Wählen Sie die Anzahl der Rufzeichen, nach welcher das Modem eingehende Anrufe annimmt.</li> <li>● Anrufe annehmen, nachdem ein Teilnehmer das Modem anruft, nach 1 Ruftönen auflegt und direkt danach das Modem erneut anruft. Das SPC-System nimmt den Anruf nun automatisch an.</li> <li>● Nur antworten, wenn der „Technikerzugang“ freigegeben ist</li> </ul>
Amtsholung	Nummer eingeben, die erforderlich ist, um eine Amtsleitung zu belegen (z. B. bei einem Anschluss über eine Telefonanlage).
Telefonleitungsüberwachung	<b>PSTN-Modem:</b> Aktivieren Sie diese Option, um die Spannung der an das Modem angeschlossenen Telefonleitung zu überwachen. <b>GSM-Modem:</b> Aktivieren Sie diese Option, um den Signalpegel des mit dem Modem verbundenen GSM-Masten zu überwachen. Mit der Option <b>Ext. scharf</b> wird diese Funktion nur aktiviert, wenn das System extern scharf ist. <b>Hinweis:</b> EN 50131-9-Bestätigungskonfiguration Für die ordnungsgemäße Funktion der EN50131-9-Bestätigung muss der Leitungstest aktiviert sein. (siehe Systemoptionen [→ 71])
Timer Überwachung	Wählen Sie die Dauer (in Sekunden), für welche die Leitungsspannung vom korrekten Wert abweichen kann, bevor die SPC eine Leitungstörung erkennt.
Störung Modem Zeit	Die Verzögerung für einen Systemalarm (0–9999 Sekunden). Standard: 60 Sekunden.
SMS aktivieren	Dieses Kästchen auswählen, um die die SMS-Funktion auf dem System zu aktivieren. <b>Hinweis:</b> Die SMS-Funktion verwendet ein Standardprotokoll, das auch in SMS-fähigen Telefonen verwendet wird. Bitte beachten Sie, dass nicht alle PSTN-Betreiber den SMS-Dienst über PSTN anbieten. Damit SMS über PSTN funktioniert, müssen folgende Kriterien erfüllt sein: Die Rufnummernanzeige muss am Telefonanschluss aktiviert sein. Es muss sich um einen Direktanschluss handeln – nicht um einen Anschluss über eine Telefonanlage oder sonstige Telekommunikationsanlagen. Bitte beachten Sie auch, dass die meisten Telekommunikationsdiensteanbieter nur SMS an ein im gleichen Land angemeldetes Telefon zulassen (aus abrechnungstechnischen Gründen). <b>Hinweis:</b> SMS über PSTN wird nicht mehr unterstützt. Diese Funktion wird im Produkt zur Wahrung der Rückwärtskompatibilität beibehalten.
SMS-Servernummer	Nur für PSTN. Auf dem Display wird automatisch die Standard-Landesvorwahl für SMS angezeigt, die im ausgewählten Land gilt. Geben Sie die passende Telefonnummer des SMS Service Providers ein, der an Ihrem Standort erreichbar ist.
Routine-SMS	Wählen Sie eine Zeiteinstellung für automatische SMS-Meldungen.
Routine-SMS-Nummer	Geben Sie eine SMS-Nummer für den Empfang automatischer SMS-Meldungen an.
ZEIT ROUTINERUF	Zeigt die Zeit des letzten SMS-Tests an.
GSM-Chip-Version	Zeigt die GSM-WISMO-Versionsnummer an. Steht keine Versionsnummer zur Verfügung, wird "----" angezeigt.
GPRS Access Point (APN)	Nur für GSM. Informationen zum Access Point müssen vom Service Provider bereitgestellt werden.
GPRS Access Point	Nur für GSM. Informationen zum Access Point müssen vom Service

Benutzername	Provider bereitgestellt werden.
GPRS Access Point Passwort	Nur für GSM. Informationen zum Access Point müssen vom Service Provider bereitgestellt werden.

Klicken Sie auf **SMS-Test**, um eine Test-SMS zum Testen der SMS-Funktion des Systems zu versenden.

Hinweis: Der SMS-Test dient ausschließlich dem Zweck, die korrekte Funktionsweise der SMS-Funktion zu überprüfen. Verwenden Sie für den Funktionstest eine kurze Textnachricht mit alphabetischen Zeichen (A-Z).



Der SMS-Test dient ausschließlich dem Zweck, die korrekte Funktionsweise der SMS-Funktion zu überprüfen. Verwenden Sie für den Funktionstest eine kurze Textnachricht mit alphabetischen Zeichen (A-Z).

Wird die SMS-Funktion über einen PSTN-Anschluss genutzt, muss die Telefonnummer des SMS-Diensteanbieters, der den Bereich abdeckt, in dem die SPC installiert wurde, eingegeben werden. Wenn die SMS-Funktion aktiviert ist verwendet das SPC-System diese Nummer dann automatisch, um den SMS-Server anzuwählen. Damit diese Funktion genutzt werden kann, MUSS die Rufnummernanzeige für den PSTN-Anschluss aktiviert sein. Jedes Land hat eigene SMS-Diensteanbieter mit eigenen Telefonnummern für den SMS-Dienst.



Diese Funktion kann nicht in allen Ländern genutzt werden. Bitte setzen Sie sich mit Ihrem Vertriebspartner vor Ort in Verbindung, um weiterführende Informationen zu erhalten (Unterstützung der Funktion, empfohlener Diensteanbieter).



Informationen zur Verfügbarkeit des Dienstes und die Nummern der SMS-Server erhalten Sie von den Diensteanbietern im jeweiligen Land. Einige SMS-Server haben möglicherweise zusätzliche technische Anforderungen, die erfüllt werden müssen, damit der SMS-Dienst ordnungsgemäß funktioniert. Genauere Informationen zu entsprechenden Anforderungen erfahren Sie von Ihrem lokalen SMS-Diensteanbieter.

## 14.2.6 GSM-Modem

Kommunikation



Modem-Konfiguration

- ▷ Ein GSM-Modem muss richtig installiert worden sein und fehlerfrei funktionieren.
- 1. Klicken Sie auf die Registerkarte **Einstellungen**.
- 2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

**Modem 2 (Backup)**

**Aktiv :**

**Modemtyp :** PSTN

**Land :** Deutschland

**Anrufannahme :** 1-Nach 'x' Ruftönen antworten

**Klingelanzahl :** 3

**Eingehende Anrufe :**  Nur antworten, wenn der Technikerzugang freigegeben ist

**Amtsholung :** Amtsholung

**Überwachung der Telefonl. :** Inaktiv

**Timer Überw. der Telefonl. :** 300 0 bis 999 Sekunden

**SMS aktivieren :**  Aktiv

**SMS-Servernummer :** 9003266900 (nur PSTN)

**SIM-PIN :** (nur GSM)

**SMS-Test :** Test

**Routine-SMS-Intervall :** 48 Stunden

**Routine-SMS # :** 0178656623

### Modemkonfiguration

Land	Wählen Sie das Land, in dem die SPC installiert ist.
SIM-PIN	Nur für GSM. Geben Sie die PIN für die SIM-Karte im GSM-Modul ein.
Roaming zulassen	Wählen Sie diese Option um GSM-Roaming zu aktivieren. <b>Hinweis:</b> Bei Veränderung dieser Einstellung wird das Modem zurückgesetzt. <b>Hinweis:</b> Auf GSM-Modems der Version 3.08 oder höher unterstützt.
Eingehende Anrufe	Für die Anrufannahme-Funktion des Modems sind folgende Einstellungen möglich: <ul style="list-style-type: none"> <li>● Keine Anrufe annehmen: Das Modem nimmt grundsätzlich keine Anrufe an.</li> <li>● Nach x Ruftönen annehmen: Wählen Sie die Anzahl der Rufzeichen, nach welcher das Modem eingehende Anrufe annimmt.</li> <li>● Anrufe annehmen, nachdem ein Teilnehmer das Modem anruft, nach 1 Ruftönen auflegt und direkt danach das Modem erneut anruft. Das SPC-System nimmt den Anruf nun automatisch an.</li> <li>● Nur antworten, wenn der „Technikerzugang“ freigegeben ist</li> </ul>
Amtsholung	Nummer eingeben, die erforderlich ist, um eine Amtsleitung zu belegen (z. B. bei einem Anschluss über eine Telefonanlage).
Telefonleitungsüberwachung	<b>PSTN-Modem:</b> Aktivieren Sie diese Option, um die Spannung der an das Modem angeschlossenen Telefonleitung zu überwachen. <b>GSM-Modem:</b> Aktivieren Sie diese Option, um den Signalpegel des mit dem Modem verbundenen GSM-Masten zu überwachen. Mit der Option <b>Ext. scharf</b> wird diese Funktion nur aktiviert, wenn das System extern scharf ist. <b>Hinweis:</b> EN 50131-9-Bestätigungskonfiguration

	Für die ordnungsgemäße Funktion der EN50131-9-Bestätigung muss der Leitungstest aktiviert sein. (siehe Systemoptionen [→ 71])
Timer Überwachung	Wählen Sie die Dauer (in Sekunden), für welche die Leitungsspannung vom korrekten Wert abweichen kann, bevor die SPC eine Leitungsstörung erkennt.
Störung Modem Zeit	Die Verzögerung für einen Systemalarm (0–9999 Sekunden). Standard: 60 Sekunden.
SMS aktivieren	Dieses Kästchen auswählen, um die die SMS-Funktion auf dem System zu aktivieren. <b>Hinweis:</b> Die SMS-Funktion verwendet ein Standardprotokoll, das auch in SMS-fähigen Telefonen verwendet wird. Bitte beachten Sie, dass nicht alle PSTN-Betreiber den SMS-Dienst über PSTN anbieten. Damit SMS über PSTN funktioniert, müssen folgende Kriterien erfüllt sein: Die Rufnummernanzeige muss am Telefonanschluss aktiviert sein. Es muss sich um einen Direktanschluss handeln – nicht um einen Anschluss über eine Telefonanlage oder sonstige Telekommunikationsanlagen. Bitte beachten Sie auch, dass die meisten Telekommunikationsdiensteanbieter nur SMS an ein im gleichen Land angemeldetes Telefon zulassen (aus abrechnungstechnischen Gründen). <b>Hinweis:</b> SMS über PSTN wird nicht mehr unterstützt. Diese Funktion wird im Produkt zur Wahrung der Rückwärtskompatibilität beibehalten.
SMS-Servernummer	Nur für PSTN. Auf dem Display wird automatisch die Standard-Landesvorwahl für SMS angezeigt, die im ausgewählten Land gilt. Geben Sie die passende Telefonnummer des SMS Service Providers ein, der an Ihrem Standort erreichbar ist.
Routine-SMS	Wählen Sie eine Zeiteinstellung für automatische SMS-Meldungen.
Routine-SMS-Nummer	Geben Sie eine SMS-Nummer für den Empfang automatischer SMS-Meldungen an.
ZEIT ROUTINERUF	Zeigt die Zeit des letzten SMS-Tests an.
GSM-Chip-Version	Zeigt die GSM-WISMO-Versionsnummer an. Steht keine Versionsnummer zur Verfügung, wird "---" angezeigt.
GPRS Access Point (APN)	Nur für GSM. Informationen zum Access Point müssen vom Service Provider bereitgestellt werden.
GPRS Access Point Benutzername	Nur für GSM. Informationen zum Access Point müssen vom Service Provider bereitgestellt werden.
GPRS Access Point Passwort	Nur für GSM. Informationen zum Access Point müssen vom Service Provider bereitgestellt werden.

Klicken Sie auf **SMS-Test**, um eine Test-SMS zum Testen der SMS-Funktion des Systems zu versenden.

Hinweis: Der SMS-Test dient ausschließlich dem Zweck, die korrekte Funktionsweise der SMS-Funktion zu überprüfen. Verwenden Sie für den Funktionstest eine kurze Textnachricht mit alphabetischen Zeichen (A-Z).



Der SMS-Test dient ausschließlich dem Zweck, die korrekte Funktionsweise der SMS-Funktion zu überprüfen. Verwenden Sie für den Funktionstest eine kurze Textnachricht mit alphabetischen Zeichen (A-Z).

## 14.3 Empfänger (Alarm Reporting Centres, ARCs)

Die SPC-Zentrale kann Informationen einer entfernten Empfangsstation mitteilen, wenn ein bestimmter Alarm in der Zentrale eintritt.

Die Empfänger müssen auf der Zentrale konfiguriert werden, damit die Kommunikation funktionieren kann.

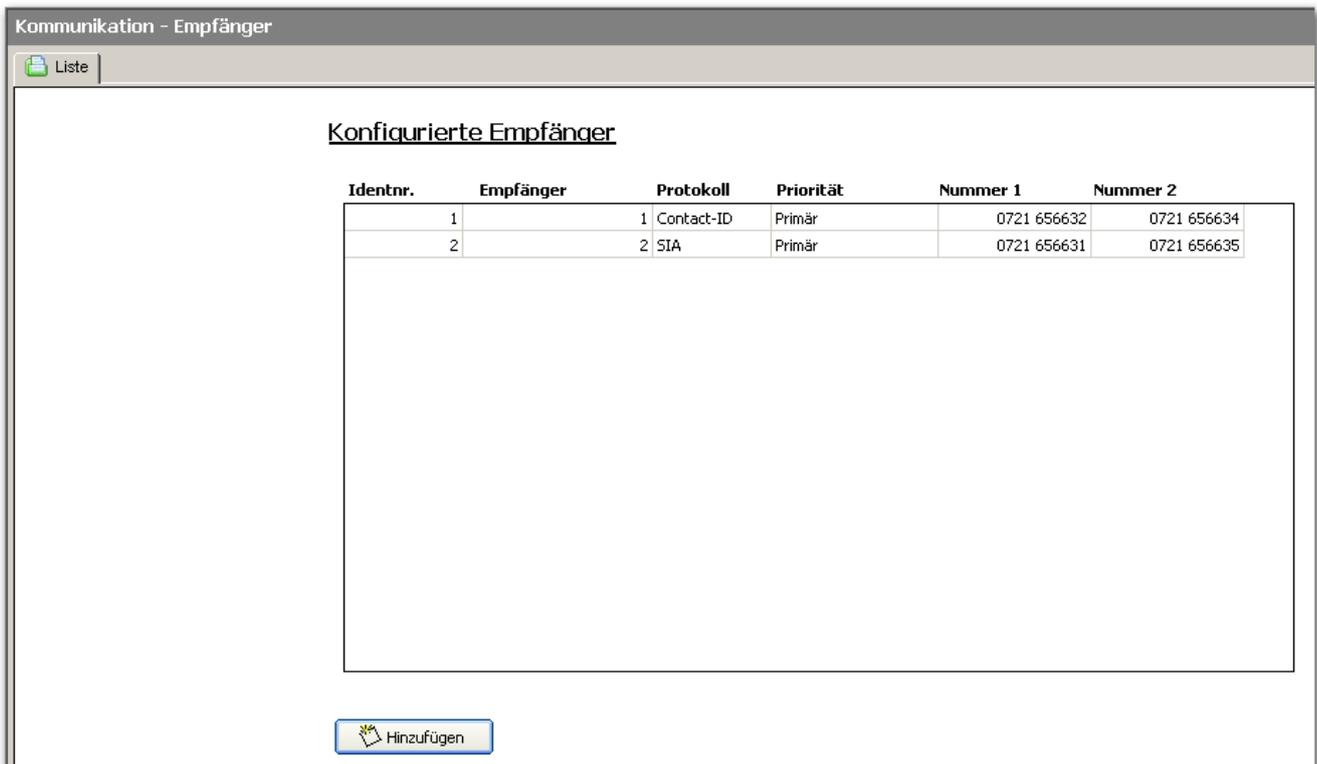
### 14.3.1 Hinzufügen/Bearbeiten von Empfängern mithilfe von SIA oder CID

**Kommunikation**



Empfänger

- ▷ Ein PSTN- oder GSM-Modem ist installiert und funktioniert ordnungsgemäß.
- 1. Klicken Sie auf die Registerkarte **Liste**.
  - ⇒ Daraufhin erscheint das folgende Fenster:



- 2. Klicken Sie auf **Hinzufügen** - ODER - Wählen Sie einen Empfänger aus der Liste.
  - ⇒ Daraufhin erscheint das folgende Fenster.
- 3. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

**Empfänger**

**Empfänger hinz./bearb.**  
Empfängerkonfiguration hinz./bearb.

**Beschreibung**  ID des Empfänger

**Identnr.**  Identnummer beim Empfänger

**Protokoll**  Verwendetes Übertragungsprotokoll

**Priorität**  Priorität des Empfängers

**Nummer 1**  Telefonnummer 1

**Nummer 2**  Telefonnummer 2

**Wählversuche**  Anzahl der Wählversuche zu einem Empfänger

**Länge Wählpause**  Wählpause (in Sek.) nach fehlg. Wählversuch

**Routine**  Intervall zwischen den autom. Übertragungstests

**Alle testen**  Aktivieren, wenn alle Modems getestet werden sollen.

Hinweis: Für Übertr.test muss der Empfänger in der Zentrale konfiguriert sein.

Beschreibung	Geben Sie eine Beschreibung für den Empfänger ein.
Identnr.	Identnummer eingeben. Diese Information sollte vom Empfänger zur Verfügung gestellt werden; sie dient der Identifizierung von Benutzern bei jedem Anruf / jeder Datenübertragung an den Empfänger. Für das Contact-ID-Konto sind maximal 6 Zeichen zulässig.
Protokoll	Das Kommunikationsprotokoll eingeben, das Sie verwenden möchten (SIA, SIA Extended, Contact ID, Fast Format). <b>Hinweis:</b> SPC unterstützt das Extended SIA-Protokoll. Das Protokoll unterstützt zusätzliche Textbeschreibungen der SIA-Ereignisse, die an den Empfänger übertragen werden.
Priorität	Wählen Sie die Priorität des Empfängers (primär oder Backup).
Nummer 1	Die erste Rufnummer, die für die Datenübertragung an den Empfänger gewählt werden soll. Das System wird stets versuchen, den Empfänger über diese Rufnummer zu erreichen, bevor es eine andere Rufnummer wählt.
Nummer 2	Die zweite Rufnummer, die zur Datenübertragung an den Empfänger gewählt werden soll. Das System versucht die Datenübertragung über diese Rufnummer nur dann, wenn unter der ersten Rufnummer keine Verbindung hergestellt werden konnte.
Wählversuche	Anzahl der Wählversuche des Systems zur Herstellung einer Verbindung zum Empfänger. (Standard = 8)
Verz Übertragung	Die Dauer der Wählpause (0–999, in Sek.), nach einem fehlgeschlagenen Wählversuch.

Länge Wählpause	Geben Sie die Dauer der Wählpause (in Sek.) nach einem fehlgeschlagenen Wählversuch ein. (0-999)
Routine	Die routinemäßige Verbindungstestfunktion wird durch Eingabe eines Zeitintervalls aktiviert. Die Einstellung führt einen automatischen Übertragungstest von Modem 1 zum primären Empfänger durch.
Alle testen	Aktivieren, wenn Sie auch von Modem 2 zum Backup-Empfänger einen automatischen Übertragungstest einrichten möchten.

1. Klicken Sie auf **Übertr Testmodem 1** oder **2**, um eine Testmeldung von Modem 1 oder Modem 2 an den primären Empfänger zu senden.
2. Klicken Sie auf **Empfänger Logbuch**, um eine Protokolldatei abzurufen. Ein Protokoll mit allen automatischen und manuellen Testmeldungen wird angezeigt.
3. Klicken Sie auf **OK**, um diese Informationen im System einzugeben.
  - ⇒ In der Liste **Konfigurierte Empfänger** werden die konfigurierten Empfängerkonten angezeigt.

### 14.3.2 Bearbeiten von Empfängerfiltern mithilfe von SIA oder CID

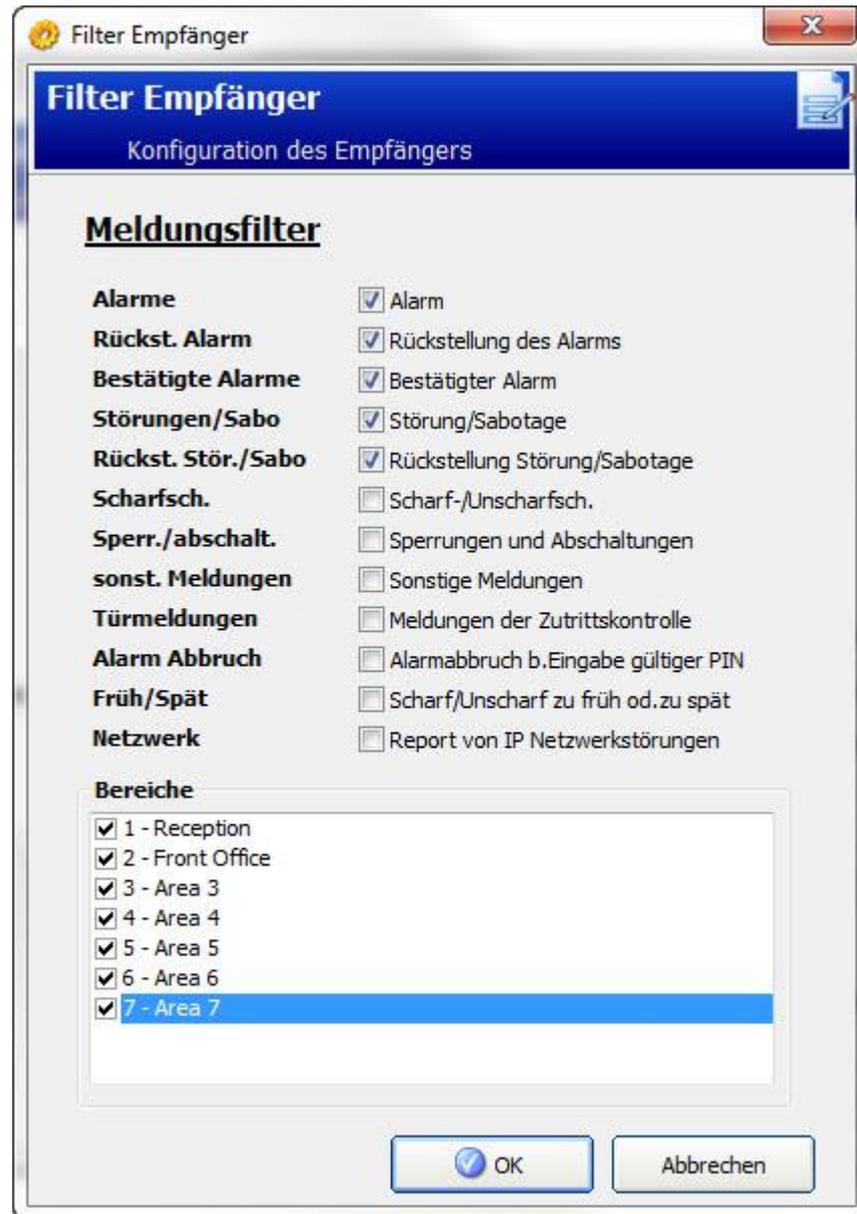
Konfigurieren der Ereignisse, die im SPC eine Datenübertragung zum Empfänger auslösen:

**Kommunikation**



Empfänger

- Klicken Sie auf die Schaltfläche **Filter** im Fenster **Empfänger hinz./bearb.**
  - ⇒ Daraufhin erscheint das folgende Fenster:



- Konfigurieren Sie die folgenden Felder und klicken Sie auf **OK**:

Aktivieren Sie ein beliebiges der folgenden Kontrollkästchen, wenn eine Datenübertragung an einen Empfänger initiiert werden soll, um ihn über ein bestimmtes Ereignis zu informieren.

Alarm	„Alarm“ ist aktiviert.
Rückstellung Alarm	Die Systemalarne werden quittiert.
Bestätigte Alarme	Von mehreren Meldegruppen bestätigte Alarme.
Alarmabbruch	„Alarm Abbruch“-Meldungen. Alarme werden nach der Eingabe eines gültigen Benutzercodes über das Bedienteil nach einem bestätigten oder unbestätigten Alarm abgebrochen.
Störungen/Sabo	Störungen und Sabotagen sind aktiv.
Rückstellung Störung/Sabo	Störungen und Sabotagealarme werden quittiert.
Einstellungen	Das System wird scharf und unscharf geschaltet.

Zu früh / Zu spät	Das System wird unplanmäßig scharf und unscharf geschaltet.
Sperrung/Abschaltung	Sperr- und Abschaltungsoperationen werden im System ausgeführt.
Meldungen der Zutrittskontrolle	Türmeldungen sind aktiviert. Nur möglich in Verbindung mit SIA-Protokoll.
Sonstige Meldungen	Alle anderen Meldungstypen werden im System erkannt.
Netzwerk	Report IP Netzwerk Polling Up/Down-Ereignisse werden gemeldet.
Bereiche	Wählen Sie die Bereiche aus, auf welche die obigen Meldungen angewendet werden sollen.



Wenn für jeden definierten Bereich ein separater Alarmempfänger hinzugefügt und programmiert wird, kann jeder der autonomen Bereiche seine Meldungen den jeweiligen Empfänger senden (Multi-Mandantensystem).

## 14.4 EDP-Einstellung

IP

Das System bietet die Möglichkeit, unter Verwendung des EDP-Protokolls (Enhanced Datagram Protocol) von Vanderbilt Informationen an den entfernten SPC-Kommunikationsserver zu senden. Durch richtiges Konfigurieren des EDP-Empfängers im System lässt er sich so programmieren, dass er automatisch Datenanrufe zum SPC-Kommunikationsserver an einem entfernten Standort macht, wenn Ereignisse wie Alarmaktivierungen, Sabotage, Scharf- oder Unscharfschaltung eintreten. Der Techniker kann das System so konfigurieren, dass die Datenübertragung an den Remote Server über folgende Verbindungsarten erfolgt:

- **PSTN** (PSTN-Modem erforderlich)
- **GSM** (GSM-Modem erforderlich)
- **Interne** (Ethernet-Schnittstelle)

Bei Verwendung des PSTN-Netzes ist darauf zu achten, dass das PSTN-Modem ordnungsgemäß installiert ist und korrekt funktioniert und dass eine funktionierende PSTN-Leitung an die Anschlüsse A, B am PSTN-Modem angeschlossen ist.

Bei Verwendung des GSM-Netzes ist darauf zu achten, dass das GSM-Modul ordnungsgemäß installiert ist und korrekt funktioniert. Eine IP-Verbindung kann über das Internet zu einem Server mit einer festen öffentlichen IP-Adresse hergestellt werden.

Wenn eine IP-Verbindung erforderlich ist, stellen Sie sicher, dass die Ethernet-Schnittstelle korrekt konfiguriert ist (siehe Seite [→ 236]) und dass der Internetzugang am Router aktiviert ist.

### 14.4.1 Hinzufügen eines EDP-Empfängers

Kommunikation



EDP-

Einrichtung

1. Klicken Sie auf die Registerkarte **Liste**.



Es können maximal 8 Empfänger zum SPC-System hinzugefügt werden.

2. Klicken Sie auf die Schaltfläche **Neuen Empfänger hinzufügen**.  
⇒ Daraufhin erscheint das folgende Fenster.
3. Weitere Informationen finden Sie in der nachstehenden Tabelle.

**Empfänger bearbeiten**

Einstellungen des EDP-Empfängers bearbeiten...

<b>Beschreibung</b>	<input type="text" value="receiver 1"/>	Beschreibung des Empfängers.
<b>Empfänger-ID</b>	<input type="text" value="12"/>	Numerische Identifikation vom EDP-Protokoll zur Identifikation des Empfängers
<b>Netzwerkadresse</b>	<input type="text" value="123.255.255.0"/>	IP-Adresse des Empfängers
<b>Telefonnummer 1</b>	<input type="text" value="01786533423"/>	Tel.nummer des Empfängers.
<b>Telefonnummer 2</b>	<input type="text" value="01786533435"/>	Tel.nummer des Empfängers.

**Erweitert**

**OK**

**Löschen**

**Abbrechen**

Beschreibung	Geben Sie eine Beschreibung des Empfängers ein.
Empfänger-ID	Geben Sie eine eindeutige Nummer ein, die vom EDP zur Identifizierung des Empfängers verwendet wird.
Netzwerkadresse	Geben Sie die IP-Adresse des Empfängers ein. Dies ist nur erforderlich, wenn die Verbindung zum EDP-Empfänger über die Ethernet-Schnittstelle erfolgt. Wird eines der Onboard-Modems verwendet, bleibt dieses Feld leer.
Telefonnummer	Geben Sie die erste Telefonnummer ein, die das Modem zum Aufbau der Verbindung mit dem Empfänger wählen soll.
Telefonnummer 2	Geben Sie eine zweite Telefonnummer ein, die das Modem wählen soll, falls die erste gewählte Nummer nicht zu einem erfolgreichen Verbindungsaufbau geführt hat.

#### Siehe auch

Bearbeiten der Einstellungen des EDP-Empfängers [→ 170]

## 14.4.2 Bearbeiten der Einstellungen des EDP-Empfängers

**Kommunikation**



EDP-  
Einrichtung

1. Wählen Sie einen Empfänger aus der Liste **Konfigurierte EDP-Empfänger** aus.  
⇒ Das folgende Fenster wird angezeigt:

EDP-Empfänger bearbeiten

**Empfänger bearbeiten**  
Einstellungen des EDP-Empfängers bearbeiten...

**Beschreibung**  Beschreibung des Empfängers.

**Empfänger-ID**  Numerische Identifikation vom EDP-Protokoll zur Identifikation des Empfängers

**Protokollversion**  Wähle EDP Protokollversion für diesen Empfänger

**VdS 2471 kompatibel**  EDP Empfänger muss VDS 2471 Norm erfüllen

2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.
3. Klicken Sie auf die Schaltfläche **Erweitert**, um andere erweiterte Einstellungen zu konfigurieren.  
⇒ Das folgende Fenster wird angezeigt:

EDP-Empfänger - erweiterte Einstellungen

### Erweiterte Empfängereinstellungen

**Sicherheit :**

**Steuerung freigegeben**  Eingehende Befehle von diesem Empfänger werden akzeptiert.

**Ändere Benutzercodes**  Änderung der Benutzercodes durch diesen Empfänger erlaubt

**Verschlüsselung aktiv**  Kommunikation von und zum Empfänger wird verschlüsselt.

**Schlüssel**  32 hexadezimale Zeichen

**Virtuelles BT**  Zugriff über virtuelles Bedienteil für diesen EDP Empfänger erlaubt

**Datenstrommodus** 1: Nach Ereignis  Datenstrommodus Live video

**Netzwerk :**

**Netzwerk aktiv**  Auswählen, wenn die Meldungen via IP versendet werden sollen.

**Netzwerk Protokoll** UDP/IP  Wähle Transportprotokolllayer über Ethernet

**Netzwerkadresse** 0 . 0 . 0 . 0  IP-Adresse des Empfängers (leer lassen, wenn nur Wählverbindung verw. wird).

**Netzwerk-Port** 0  UDP-Port des Empfängers

**Polling aktiv**  IP-Polling für diesen Empfänger aktivieren

**Zentrale ist Master**  Zentrale übernimmt Masterrolle des Pollings.

**Polling-Intervall**  Sekunden zwischen den einzelnen Polling-Nachrichten

**Vers. bis Übertragungsf.**  Anzahl der fehlenden Polling-Nachrichten, bis ein Netzwerkfehler gemeldet wird.

**Wählverbindung :**

**Wählverb. aktiv.**  Auswählen, wenn die Meldungen via Wählverbindung gesendet werden sollen.

**Anruf Typ** Ringschaltung  Wähle Anruftyp bei Verwendung von Wählleitungsverbindung

**Testintervall Wählverb.**  Zeit zwischen Tests der Wählverbindung, wenn Netzwerk in Ordnung ist.

**Testintervall Wählverb.**  Zeit zwischen Tests der Wählverbindung, wenn Netzwerk nicht in Ordnung ist

**Wählverb. b. Netzwerkf.**  Wählverb. wird getestet, wenn Netzwerkverb. gestört ist.

**Telefonnummer 1**  Rufnummer des Empfängers

**Telefonnummer 2**  Backup Rufnummer des Empfängers

**Ereignisse :**

**Primär-Empfänger**  Ausgewählt = Primär, Nicht ausgewählt = Backup

**Meldungen erneut vers.**  Auswählen, wenn fehlerhafte Übertragungen wiederholt werden sollen.

**Verifikation**  Wähle ob an diesen Empfänger Audio/Videoverifikation gesendet wird

**Meldungsfiler**  Konfiguration, welche Meldungen an diesen Empfänger gesendet werden sollen.

4. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

Beschreibung	Bearbeiten Sie den Namen des EDP-Empfängers. Es sind maximal 16 Zeichen zulässig.
Empfänger-ID	Bearbeiten Sie die ID des EDP-Empfängers. Der Bereich von 1 bis 999997 ist zulässig (999998 und 999999 sind für bestimmte Zwecke reserviert).
Protokollversion	Wählen Sie, welche Version des EDP-Protokolls für diesen EDP-Empfänger verwendet werden soll. Mögliche Optionen sind „Version 1“ oder „Version 2“. Version 2 wird empfohlen, wenn sie vom Empfänger unterstützt wird. Sie ist das sicherere Protokoll.
Zu VdS 2471 kompatibel	(nur für VdS-Norm) Bei Auswahl dieser Option erzwingt der EDP-Empfänger folgende Einstellungen für diesen Empfänger:

	<ul style="list-style-type: none"> <li>● Polling-Intervall von 8 s</li> <li>● Erzwungenes TCP-Protokoll</li> <li>● TCP-Versuche schlagen nach weniger als 10 s fehl (ca. 9 s)</li> <li>● EDP-Ereignisversuche werden unabhängig von der globalen Einstellung zur Anzahl der erneuten Übertragungsversuche in den EDP-Einstellungen auf 1 gesetzt.</li> <li>● FTC wird innerhalb von 20 Sekunden nach einem Netzwerkausfall generiert.</li> </ul>
--	--

<b>Sicherheit</b>	
Steuerung freigegeben	Aktivieren Sie dieses Kontrollkästchen, damit Befehle vom Server akzeptiert werden.
Benutzer-PINs ändern	Aktivieren Sie dieses Kontrollkästchen, damit Benutzer-PINs von einem dezentralen Standort aus geändert werden können. Diese Funktion ist nur verfügbar, wenn die die Steuerung auf dem Empfänger freigegeben ist.
Verschlüsselung aktiv	Aktivieren, um die Verschlüsselung von Daten, die vom und zum Empfänger gesendet werden, zu aktivieren.
Schlüssel für Verschlüsselung	Geben Sie einen hexadezimalen Schlüssel ein (max. 32 Ziffern), der zur Verschlüsselung der Daten verwendet werden soll. <b>Hinweis:</b> Der gleiche Schlüssel muss auch für den Empfänger verwendet werden.
Virtual Bedienteil	Diese Option aktiviert den Zugang zur Zentrale über ein virtuelles Bedienteil, d. h. ein PC-Softwaremodul, das wie ein SPC-Bedienteil aussieht und sich auch so verhält. Diese Software ist zusammen mit dem SPC-Com-Client erhältlich.
Live Übertragung/Streaming-Modus	Diese Option legt fest, wann ein Live-Streaming von Audio- und Videodaten verfügbar ist. Die möglichen Optionen sind „Niemals“, „Immer“ und „Nur nach Alarm“. Die Standardeinstellung ist „Nur nach Alarm“. <b>Hinweis:</b> Diese Einstellung hat offensichtlich Auswirkungen auf die Privatsphäre und sollte deshalb nur aktiviert werden, wenn angemessene lokale Gesetze und Richtlinien vorhanden sind und angewendet werden.
<b>Netzwerk</b> (Gilt nur für den Ethernet-Anschluss)	
Netzwerk aktiv	Aktivieren Sie dieses Kontrollkästchen, damit Ereignisse über das Netzwerk gemeldet werden können.
Netzwerkprotokoll	Wählen Sie den Typ des Netzwerkprotokolls für den Empfänger. Verfügbare Optionen sind „UDP“ und „TCP“. TCP wird empfohlen, wenn es vom Empfänger unterstützt wird.
Empfängeradresse	Geben Sie die IP-Adresse des Empfängers ein.
Netzwerk-Port	Geben Sie den IP-Port ein, den der EDP-Empfänger abhört.
Immer verbunden	Bei Aktivierung hält die Zentrale eine permanente Verbindung mit dem Empfänger aufrecht. Bei Deaktivierung verbindet sich die Zentrale nur nach einem Alarmereignis mit dem Empfänger.
Zentrale ist Master	Bei Aktivierung übernimmt die Zentrale die Masterrolle des Pollings. Dies gilt nur für UDP-Verbindungen.
Polling-Intervall	Geben Sie die Anzahl der Sekunden zwischen Abfragen ein.
Polling-Trigger	Geben Sie die Anzahl der fehlenden Polling-Nachrichten ein, ab der ein Netzwerkfehler gemeldet wird. Dies gilt nur für UDP-Verbindungen.
Erzeuge Netzwerkfehler	Wenn das Polling fehlschlägt, wird eine Netzwerkfehlermeldung generiert.
<b>Wählverb</b> (Gilt nur für GPRS-Modemverbindungen)	

Wählverbindung aktiv	Aktivieren, damit Ereignisse über eine Wählverbindung gemeldet werden können.
Übertragungsmodus	Wählen Sie den Übertragungsmodus für die aktivierte Wählverbindung aus. Wählen Sie GPRS.
GPRS Protokoll	Wählen Sie das Protokoll für die GPRS-Verbindung aus. Verfügbare Optionen sind „UDP“ und „TCP“. Dies gilt nur für den Übertragungsmodus „GPRS“.
GPRS-Adresse	Geben Sie die IP-Adresse des EDP-Empfängers für die GPRS-Verbindungen ein. Dies gilt nur für den Übertragungsmodus „GPRS“.
GPRS-Port	Geben Sie den UDP-Port ein, den der EDP-Empfänger abhört. Dies gilt nur für den Übertragungsmodus „GPRS“. Der Standard ist 50000.
GPRS Abbruch Zeitüberschreitung	Geben Sie die Zeit in Sekunden ein, nach der die GPRS-Verbindung getrennt wird. (0 = verbunden bleiben bis IP-Verbindung aufgebaut ist)
Autom.GPRS Verbind.	Aktivieren Sie dieses Kontrollkästchen, um bei einem IP-Netzwerkfehler eine GPRS-Verbindung mit dem Server aufzubauen.
Wählverbindung bei Netzwerkfehler	Aktivieren Sie dieses Kontrollkästchen, um Netzwerkfehler bei einem Test der Wählverbindung zu melden.
Testintervall Wählverb. 1*	Zeit zwischen Tests der Wählverbindung, wenn Netzwerkverb in Ordnung ist, eingeben (in Minuten).
Testintervall Wählverb. 2*	Zeit zwischen Tests der Wählverbindung, wenn Netzwerkverb. nicht in Ordnung ist, eingeben (in Minuten).
Network Address*	Geben Sie die IP-Adresse des Empfängers ein. Dies ist nur erforderlich, wenn die Verbindung zum EDP-Empfänger über die Ethernet-Schnittstelle erfolgt. Wird eines der Onboard-Modems verwendet, bleibt dieses Feld leer.
Telefonnummer*	Geben Sie die erste Telefonnummer ein, die das Modem zum Aufbau der Verbindung mit dem Empfänger wählen soll.
Telefonnummer 2*	Geben Sie eine zweite Telefonnummer ein, die das Modem wählen soll, falls die erste gewählte Nummer nicht zu einem erfolgreichen Verbindungsaufbau geführt hat.
<b>Ereignisse</b>	
Primär-Empfänger	Aktivieren Sie dieses Kontrollkästchen, um anzugeben, dass dies der Primärempfänger ist. Bei Deaktivierung ist dies der Backup-Empfänger.
Meldungen erneut vers	Aktivieren Sie dieses Kontrollkästchen, wenn nicht quitierte Meldungen erneut versendet werden sollen.
Verifikation	Aktivieren Sie dieses Kontrollkästchen, wenn Audio-/Videoverifikationsdaten an diesen Empfänger geschickt werden sollen.
Ereignisfilter	Schaltfläche anklicken, um die Filterereignisse zu bearbeiten, die einen EDP-Anruf auslösen. Weitere Informationen finden Sie unter Bearbeiten von Ereignisfiltereinstellungen [→ 175].



\* EDP-Wählverbindung über PSTN wird in dieser Version nicht unterstützt.

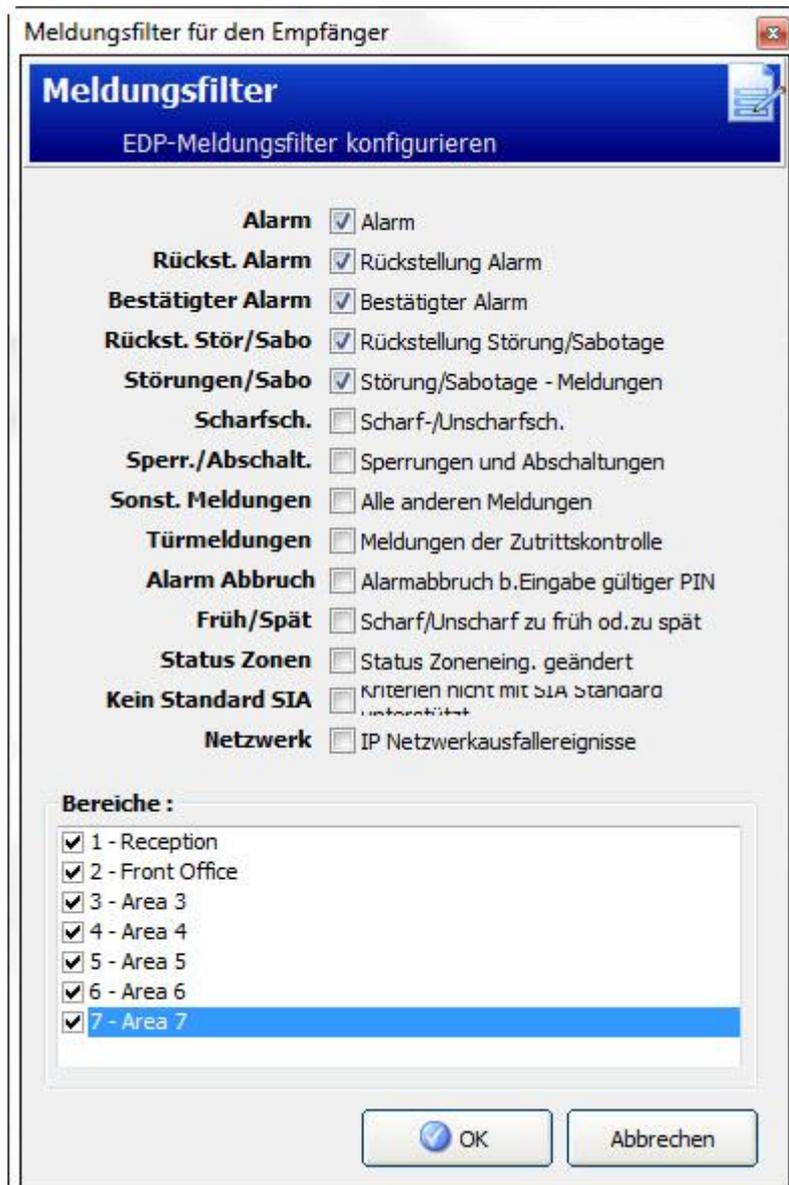
#### Siehe auch

Konfiguration von SMS [→ 60]

### 14.4.3 Meldungsfilter-Einstellungen bearbeiten



1. Klicken Sie auf die Schaltfläche **Erweitert**.
2. Klicken Sie auf die Schaltfläche **Filter**.  
⇒ Daraufhin erscheint das folgende Fenster.
3. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



Aktivieren Sie ein beliebiges der folgenden Kontrollkästchen, wenn eine Datenübertragung an einen EDP-Empfänger initiiert werden soll, um ihm ein bestimmtes Ereignis zu melden.

Alarm	„Alarm“ ist aktiviert.
Rückstellung Alarm	Die Systemalarme werden quittiert.
Bestätigte Alarmer	Von mehreren Meldegruppen bestätigte Alarmer.
Alarmabbruch	„Alarm Abbruch“-Meldungen. Alarmer werden nach der Eingabe eines gültigen Benutzercodes über das Bedienteil nach einem bestätigten oder unbestätigten Alarm abgebrochen.
Störungen/Sabo	Störungen und Sabotagen sind aktiv.
Rückstellung Störung/Sabo	Störungen und Sabotagealarmer werden quittiert.
MG Zustand	Die Eingabestatusänderungen aller MGs werden gemeldet.
Einstellungen	Das System wird scharf und unscharf geschaltet.
Zu früh / Zu spät	Das System wird unplanmäßig scharf und unscharf geschaltet.
Sperrung/Abschaltung	Sperr- und Abschaltungsoperationen werden im System ausgeführt.
Meldungen der Zutrittskontrolle	Türmeldungen sind aktiviert. Nur möglich in Verbindung mit SIA-Protokoll.
Sonstige Meldungen	Alle anderen Meldungstypen werden im System erkannt.
Andere (Nicht Standard)	Nicht unterstützte SIA-Codes werden mit SPC COM XT verwendet (einschließlich Kamera Online/Offline-Meldungen).
Netzwerk	Report IP Netzwerk Polling Up/Down-Ereignisse werden gemeldet.
Bereiche	Wählen Sie die Bereiche aus, auf welche die obigen Meldungen angewendet werden sollen.

#### 14.4.4 EDP-Einstellungen bearbeiten

Kommunikation



EDP-

Einrichtung

1. Klicken Sie auf die Registerkarte **Einstellungen**.  
⇒ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

Kommunikation - EDP

Liste Einstellungen

EDP-Einstellungen

<b>Aktivieren</b>	<input checked="" type="checkbox"/>	Auswählen, um EDP zu aktivieren.
<b>Geräte-ID</b>	<input type="text" value="1000"/>	Eindeutige ID der Zentrale
<b>UDP-Port</b>	<input type="text" value="50000"/>	UDP-Port auf dem IP-Pakete empfangen werden (Standard ist 50000)
<b>Limit Packetgröße</b>	<input type="text" value="1440"/>	Max.Packetgröße für Übertragung (Ab Werk 1440) [500-1440]
<b>Timeout erneute Übertr.</b>	<input type="text" value="10"/>	Dauer (in Sek.), bis eine nicht quittierte Meldung erneut übertragen wird.
<b>Anzahl erneute Übertr.</b>	<input type="text" value="10"/>	Max. Anzahl der erneuten Übertragungsversuche (5-199)
<b>Wählversuche</b>	<input type="text" value="10"/>	Max. Anzahl an fehlgeschlagenen Wählversuchen bis zur Modemsperre (1-199)
<b>Verz. Übertragung</b>	<input type="text" value="30"/>	Dauer der Wählpause (in Sek.) nach einem fehlgeschlagenen Wählversuch (1-199)
<b>Wählpause</b>	<input type="text" value="480"/>	Dauer (in Sek.) ohne Wählv., nachdem max. Anzahl fehlg. Wählvers. erreicht wurde

Optionen Ereignisspeicher :

- |                |                          |  |
|----------------|--------------------------|--|
| Status Komm.   | <input type="checkbox"/> |  |
| EDP Befehle    | <input type="checkbox"/> |  |
| A/V Ereigniss  | <input type="checkbox"/> |  |
| A/V Datenstrom | <input type="checkbox"/> |  |
| BT verwendet   | <input type="checkbox"/> |  |

Aktivieren	Aktivieren Sie dieses Kontrollkästchen, um EDP auf dem System zu aktivieren.
Geräte-ID	Geben Sie eine numerische ID ein, die vom EDP-Empfänger verwendet wird, um die Zentrale eindeutig zu identifizieren.
Zentralenport	Wählen Sie den IP-Port zum Empfang von IP-Paketen aus. Der Standard ist 50000.
Maximale Paketgröße	Geben Sie die maximale Anzahl an Bytes für die Übertragung eines EDP-Pakets an.
Timeout erneute Übertragung	Geben Sie die Dauer (in Sek) ein, bis eine nicht quittierte Meldung erneut übertragen wird.
Anzahl erneute Übertr.	Geben Sie die maximale Anzahl der vom System erlaubten wiederholten Übertragungsversuche für Meldungen ein.
Wählversuche	Geben Sie die maximale Anzahl fehlgeschlagener Wählversuche ein, die das System akzeptiert, bevor das Modem gesperrt wird (weitere Wählversuche werden unterdrückt). Die Dauer der Sperre wird in der Option „Modemsperre“ festgelegt.
Verz Übertragung	Geben Sie die Dauer (in Sek.) ein, für die das System wartet, bevor es nach einem fehlgeschlagenen Wählversuch erneut wählt.
Wählpause	Geben Sie die Dauer (in Sek.) ein, für die das System weitere Wählversuche aussetzt, wenn die max. Anzahl fehlgeschlagener Wählversuche erreicht wurde. Geben Sie „0“ ein, um Wählversuche nicht auszusetzen.

**Ereignisspeicherung**

Status Kommunikation	Speichert alle Änderungen der Verfügbarkeit der Kommunikationswege.
----------------------	---

EDP Befehle	Speichert alle ausgeführten EDP Befehle
A/V Ereignisse	Speichert Audio/Video-Verifikationsmeldungen, die an den Empfänger geschickt werden.
A/V Streaming	Speichert den Beginn einer Audio/Video-Live-Übertragung.
Benutzung Virtuelles BT	Speichert die Aktivierung eines virtuellen Bedienteils.

## 14.5 "Fernwartung"

Weitere Informationen finden Sie im Konfigurationshandbuch für die Fernwartung.

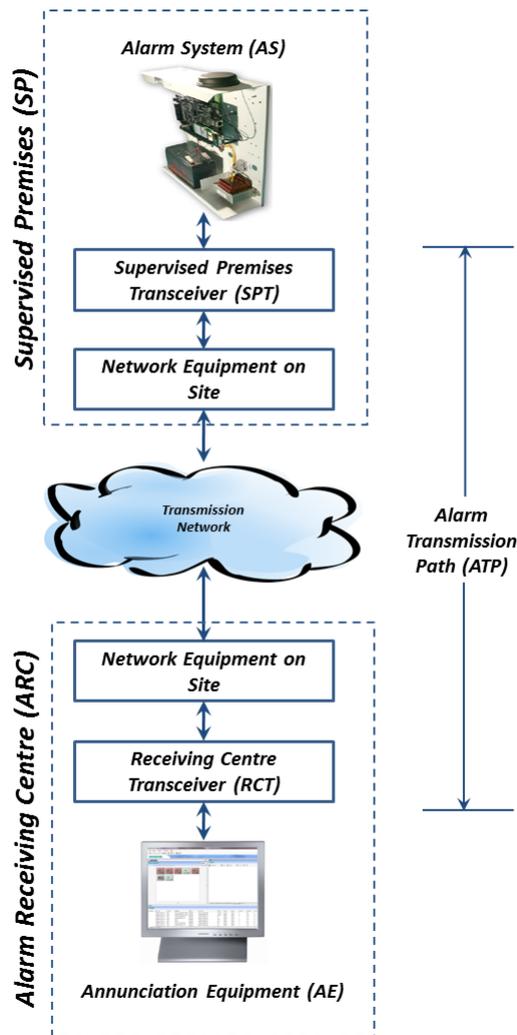
## 14.6 FlexC®

Das SPC Flexible Secure Communications Protocol (FlexC) ermöglicht die Kommunikation eines auf einem Internetprotokoll (IP) basierenden Alarmübertragungssystems (ATS) mit einem oder mehreren Pfaden. Ein ATS ist eine zuverlässige Kommunikationsverbindung zwischen einem Empfänger eines überwachten Gebäudes (SPT, z. B. auf der SPC-Zentrale integriertes Ethernet) und einem Empfänger einer Empfangszentrale (z. B. SPC Com XT oder der SPC Connect-Server ([www.spconnect.com](http://www.spconnect.com))). Eine FlexC-Empfangseinrichtung besteht auf einem primären Alarmübertragungspfad (ÜW) und bis zu neun Backup-Alarmübertragungspfaden (ÜWs). Sie ermöglicht:

- Zwei-Wege-Übertragungen von Daten zwischen dem SPT (z. B. die SPC-Zentrale über Ethernet) und der Empfangszentrale (z. B. der SPC Com XT-Server oder der SPC Connect-Server ([www.spconnect.com](http://www.spconnect.com))).
- Kommunikationsüberwachung eines kompletten ATS und einzelner ÜWs.

SPC-Einbruchszentralen unterstützen FlexC über IP mit einer der folgenden Schnittstellen:

- Ethernet
- GSM-Modem mit aktiviertem GPRS
- PSTN-Modem



#### Siehe auch

- 📄 Schnellstart-ÜW-Konfiguration für EN50136 ATS [→ 179]
- 📄 Konfigurieren von Ereignisprofilen [→ 193]
- 📄 Ereignis Ausnahmendefinition [→ 195]
- 📄 Konfigurieren von Steuerprofilen [→ 198]
- 📄 Konfigurieren eines EN50136-1-ATS oder kundenspezifischen ATS [→ 182]

### 14.6.1 Schnellstart-ÜW-Konfiguration für EN50136 ATS

FlexC bietet folgende Funktionen, mit denen Sie FlexC schnell einrichten und ausführen können:

- Schnellstart-Konfigurationsbildschirm für ein **Einzel-Weg-Übertragungssystem**, ein **Zwei-Wege-Übertragungssystem** und ein **Zwei-Wege-Übertragungssystem mit zwei Servern** gemäß EN50136.
- Vorgegebenes Ereignisprofil
- Vorgegebenes Steuerprofil (dies unterstützt keine Audio-Video-Verifizierung)
- Standardmäßiger/s **FlexC-Steuerungsbenutzername** (FlexC) und **Steuerungspasswort** (FlexC) für die Steuerung der Zentrale von der Empfangszentrale (SPC Com XT) aus.
- Automatische Verschlüsselung ohne Passwort

1. Öffnen Sie für eine schnelle Konfiguration einer FlexC-Verbindung zwischen einer Zentrale und einer Empfangszentrale (z. B. SPC Com XT) den Menüpfad **Kommunikation > FlexC > FlexC Empfangseinrichtung**.
2. Wählen Sie unter **EN50136 Übertragungssystem anf.** eine der folgenden Optionen, um den Bildschirm **ÜW Einstellungen** anzuzeigen:
  - **Ein Wege Ü.-System hinzufügen** – nur primäres ÜW
  - **Zwei Wege Ü.-System Hinzufügen** – primäre und Backup-ÜWs
  - **Zwei Wege 2 Server Ü.-System Hinzufügen** – primäre und Backup-ÜWs, primäre und Backup-Server

**Einstellungen FlexC ÜW**
?

weitere Einstellungsdetails zu neuen FlexC ÜW

---

**Zentralenident.**

**ATS Name :**  Name des Übertr.-Syst.

**Zentralen Ident-Nr.**  Die eindeutige Geräte ID der Zentrale(1-99999999, 0=Auto)

**Empfangszentrale**

**RCT ID:**  Die eindeutige ID der Empfangszentrale (z.B. SPC Com XT)(1-99999999)

**RCT URL oder IP Adresse:**  URL oder IP Adresse der Empfangszentrale

**RCT TCP Port:**  Der TCP Port der Empfangszentrale (der Port, auf dem die SPC Com XT lauscht)

**Sichern der Empfangszentr. Daten**

**RCT ID:**  Die eindeutige ID der Empfangszentrale (z.B. SPC Com XT)(1-99999999)

**RCT URL oder IP Adresse:**  URL oder IP Adresse der Empfangszentrale

**RCT TCP Port:**  Der TCP Port der Empfangszentrale (der Port, auf dem die SPC Com XT lauscht)

**Schnittstelle ÜW**

**EN50136 Übertr.-System Kat**  Auswahl der Kategorie der Übertragungssysteme gemäß EN50136-1:2012

**Hauptschnittstelle**  Schnittstelle des Hauptübertragungsweges

**Ersatzschnittstelle**  Schnittstelle des Ersatzübertragungsweges

1. Füllen Sie die Felder im Bildschirm **ÜW Einstellungen – EN50136 ATS** aus, die in der unteren Tabelle aufgeführt sind. Sie müssen mindestens das Feld **Empfangszentrale URL/ IP Adresse** ausfüllen, um speichern zu können. Wenn Sie keine **Geräte ID** eingeben, können Sie die Zentrale mithilfe der **Übertr.-Sys. Registrierung ID** in Betrieb nehmen, die automatisch bei der Speicherung erstellt wird. Der Bediener der Empfangszentrale muss diese **Übertr.-Sys. Registrierung ID** z. B. im SPC Com XT, eingeben.
2. Klicken Sie auf **Speichern**. Der Bildschirm **ATS Konfiguration** wird angezeigt und enthält die **Übertr.-Sys. Registrierung ID** und den konfigurierten primären ÜW oder die primären und Backup-ÜWs in der **Tabelle der Ereignisfolge**.
3. Klicken Sie im Bildschirm **ATS Konfiguration** auf **Speichern**, um die Standardeinstellungen anzunehmen (z. B. das **Vorgegebene Ereignisprofil**, das **Vorgegebene Steuerungsprofil** (einschließlich dem FlexC **Steuerungsbenutzername** und dem FlexC **Steuerungspasswort**) und die **Automatische Verschlüsselung** ohne Passwort). Informationen zur Änderung

der Einstellungen finden Sie unter Konfigurieren eines EN50136-1-ATS oder kundenspezifischen ATS [→ 182].

4. Klicken Sie auf **Zurück**. Das ATS wird in der Tabelle **Konfig. Übertragungssystem** angezeigt.
5. Klicken Sie auf die Schaltfläche **Registrierungs-ID aktualisieren**, um die Registrierungs-ID in der ATS-Tabelle anzuzeigen.

<b>Zentralen Kennung</b>	
ATS Name	Geben Sie den Namen des ATS ein. Wenn Sie keinen Wert eingeben, wird der ATS-Name standardmäßig auf ATS 1, ATS 2 usw. eingestellt.
Geräte ID	Die Nummer, welche die Zentrale eindeutig in der Empfangszentrale identifiziert. Geben Sie 0 ein, falls Sie keine Geräte-ID besitzen. In diesem Fall können Sie die Zentrale mithilfe der <b>Übertr.-Sys. Registrierung ID</b> in Betrieb nehmen. Für ein EN50136 ATS wird die <b>Übertr.-Sys. Registrierung ID</b> automatisch beim Klicken auf <b>Speichern</b> erstellt. Die Empfangszentrale kann die <b>Geräte-ID</b> an die Zentrale schicken, wenn sie verfügbar ist.
<b>RCT Identification &amp; Backup RCT Identification (Dual Path Dual Server Only)</b> (Identifikation der Empfangszentrale und Backup-Empfangszentrale (nur Zwei-Wege-Dualserver))	
Empfangszentr.ID	Geben Sie die <b>Empfangszentr.ID</b> ein, welche die Empfangszentrale (z. B. SPC Com XT) eindeutig in der Zentrale identifiziert. Diese muss mit der ID übereinstimmen, die auf dem SPC Com XT-Server im Configuration Manager im Feld <b>Server RCT ID</b> (Server-Empfangszentralen-ID) auf der Registerkarte <b>Serverdetails</b> eingegeben wurde. Weitere Informationen finden Sie im <i>Installations- und Konfigurationshandbuch des SPC Com XT</i> .
Empfangszentrale URL/ IP Adresse	Geben Sie die <b>Empfangszentrale URL/ IP Adresse</b> für den Serverstandort der Empfangszentrale (z. B. SPC Com XT-Server) ein.
EZ TCP Port	Geben Sie den TCP-Port für die Empfangszentrale (SPC Com XT) ein. Dies muss der gleiche Wert sein, der im Configuration Manager auf dem SPC Com XT-Server im Feld <b>Server FlexC-Port</b> eingegeben wurde.
<b>ÜW Schnittstelle</b>	
EN50136 ATS Kategorie	Wählen Sie die EN50136-ATS-Kategorie. Eine Beschreibung der Kategorien finden Sie unter Zeiten für Übertragungssystemkategorien [→ 289].
Primäre Schnittstelle	Wählen Sie die <b>Primäre Schnittstelle</b> zur Anwendung auf den primären Kommunikationspfad aus den folgenden aus: <ul style="list-style-type: none"> <li>● Ethernet</li> <li>● GPRS: Modem 1</li> <li>● GPRS: "Modem 2"</li> <li>● Wählverbindung Internet: Modem 1</li> <li>● Wählverbindung Internet: "Modem 2"</li> </ul>

Backup Schnittstelle	Wählen Sie für ein <b>Zwei-Wege-Übertragungssystem</b> eine der folgenden <b>Backup-Schnittstellen</b> , damit diese für die Backup-Kommunikation verwendet wird: <ul style="list-style-type: none"> <li>● Ethernet</li> <li>● GPRS: Modem 1</li> <li>● GPRS: "Modem 2"</li> <li>● Wählverbindung Internet: Modem 1</li> <li>● Wählverbindung Internet: "Modem 2"</li> </ul>
----------------------	--

## 14.6.2 Konfigurieren eines EN50136-1-ATS oder kundenspezifischen ATS

Ein ATS besteht aus einer Alarmzentrale, Netzwerkpfaden und einer Empfangszentrale (z. B. SPC Com XT). Es kombiniert einen oder mehrere Pfade zwischen einer SPC-Zentrale und einer Empfangszentrale. Sie können in ein ATS bis zu 10 ÜWs hinzufügen.

<b>!</b>	<b>HINWEIS</b>
	Für ein EN50136 ATS beginnt die Einrichtungssequenz mit der Konfiguration eines ÜW für ein ATS. Dadurch erhalten Sie eine Schnelleinrichtungsfunktion. Siehe Schnellstart-ÜW-Konfiguration für EN50136 ATS [→ 179].

1. Öffnen Sie zur Konfiguration eines ATS den Menüpfad **Kommunikation > FlexC > FlexC Empfangseinrichtung**.
2. Wählen Sie eine der folgenden Optionen:
  - **Ein Wege Ü.-System hinzufügen**
  - **Zwei Wege Ü.-System Hinzufügen**
  - **Zwei Wege 2 Server Ü.-System Hinzufügen**
  - **Angepasstes Übertragungssystem.**
1. Für ein EN50136 ATS müssen Sie zunächst die Einstellungen im Bildschirm **ÜW Einstellungen – EN50136** konfigurieren. Siehe Schnellstart-ÜW-Konfiguration für EN50136 ATS [→ 179].
2. Der Bildschirm **ATS Konfiguration** wird angezeigt. Ein EN50136-1 ATS zeigt einen primären oder primären und Backup-ÜW in der **Tabelle der Ereignisfolge** an.

**ATS Konfiguration**

Konfigurationsdetails für neue FlexC Alarm Ü.-Syst.

**ATS Name:**  Name des Über.-Systems

Seq.-Nr.	Name	Komm.- Schnittstelle	ÜW Gruppe	Status	Aktives Polling Timeout	Timeout

**ATS Profile**

**Ereignisprofil:**  Auswahl des Ereignisprofils, welches die Ereignisübertragung definiert

**Steuerungs-Profil:**  Auswahl des Steuerprofils, welches die Befehle definiert, die zulässig sind

**Störung ATS**

**Polling Timeout:**  Sekunden Timeout, wenn das Polling Paket nicht übertragen wurde. (0=Auto)

**ATS Ereignis Zeitübersch.**  Sekunden Zeit, die verstrichen nach der Auslösung und noch nicht übertragen

**Erzeuge Kom.-F.**  Auswahl, ob ein Kommunikationsfehler oder ein ÜW Timeout erzeugt wird

**Ereignis erneuern:**  Auswahl, was nach einem ÜW Timeout passiert

**Verzöger. Ereignis erneuern:**  Sekunden Verzögerung nach ÜW Timeout bevor die Übertragung erneut versucht wird

**Dauer Ereignis erneuern:**  Sekunden Zeitdauer, die ein Ereignis versucht wird zu übertragen bevor es gelöscht wird

1. Geben Sie einen **ATS-Namen** ein, um das ATS zu identifizieren. Wenn Sie keinen Wert eingeben, wird der ATS-Name standardmäßig auf ATS 1, ATS 2 usw. eingestellt.
2. Klicken Sie zum Hinzufügen eines primären und bis zu neun Backup-ÜWs auf **ÜW zur FlexCom (AE)** (siehe ÜW zur FlexCom (AE) [→ 184]). Oder klicken Sie auf **ÜW zu analogem Empfänger** (siehe ÜW zu analogem Empfänger [→ 189]).
3. Wählen Sie aus dem Dropdown-Menü ein **Ereignisprofil**. Informationen zur Anpassung, wie Ereignisse an ein ATS übertragen werden, finden Sie unter Konfigurieren von Ereignisprofilen [→ 193].
4. Wählen Sie ein **Steuerprofil** aus dem Dropdown-Menü. Informationen zur Anpassung des für einen Empfänger aktivierten Befehls zur Steuerung einer Zentrale finden Sie unter Konfigurieren von Steuerprofilen [→ 198].
5. Füllen Sie die Felder **ATS Störung** wie in der unten stehenden Tabelle aus.
6. Klicken Sie auf die Schaltfläche **Anpassen d. Installationsdetails**, um die Einstellungen abzuschließen und so die Zentrale für den Empfängerbediener zu identifizieren. Siehe Installationsdetails bearbeiten [→ 191].
7. Klicken Sie auf **Speichern** und **Zurück**, um zur Seite **ATS Konfiguration** zurückzukehren. Das neue ATS wird in der Tabelle **Konfig. Übertragungssystem** angezeigt.
8. Für mehrere ÜWs können Sie die Pfeilschaltflächen in der **Tabelle der Ereignisfolge** verwenden, um die Reihenfolge der ÜWs zu ändern.

Übertragungssys. Polling Timeout	Dieses Feld wird automatisch durch Hinzufügen der Werte aus der Spalte <b>Timeout des aktiven Polling</b> in der Tabelle der Ereignisfolge berechnet. Dies gilt für alle ÜWs in einem ATS. Sie können dieses Feld manuell überschreiben. Beispielsweise hat das Cat2 [Modem] ein <b>Timeout des aktiven Polling</b> von 24 Stunden 10 Minuten (87.000 Sekunden). Geben Sie für eine
----------------------------------	---

	kürzere Reaktionszeit einen kleineren Wert ein.
ATS Ereignis Timeout	Die Zeit nach einem Ereignis wurde erhöht und nicht erfolgreich übertragen, bevor das ATS aufgibt. Standard: 300 Sekunden.
Erzeuge Kommunikationsfehler	Wählen Sie, ob das System einen Kommunikationsfehler für eine ATS-Ereigniszeitüberschreitung erstellen soll.
Meldungen erneut vers	Wählen Sie diese Option, um Ereignisse nach der ATS-Zeitüberschreitung erneut in die Warteschlange zu setzen.
Wiedereinreichungsverzögerung des Ereignisses	Die Verzögerung nach einem Empfangseinrichtungstimeout, bevor das Ereignis erneut zu übertragen versucht wird. Standard: 300 Sekunden.
Dauer der Wiedereinreichung eines Ereignisses	Die Zeitspanne, in der ein Ereignis wieder zur Übertragung eingereiht wird, bevor es gelöscht wird. Standard: 86.400 Sekunden.

**Siehe auch**

 Zeiten für Übertragungssystemkategorien [→ 289]

**14.6.2.1 ÜW zur FlexCom (AE)**

Mithilfe der Option **ÜW zur FlexCom (AE)** können Sie einen ÜW zwischen der SPC-Zentrale und der Empfangszentrale (z. B. SPC Com XT) konfigurieren. Sie können bis zu 10 ÜWs für jedes ATS konfigurieren.

1. Klicken Sie auf die Schaltfläche **ÜW zur FlexCom (AE)**.

**Einstellungen FlexC ÜW**
?

weitere Einstellungsdetails zu neuen FlexC ÜW

---

**Zentralen Kennung**

**ÜW Abfolge Nummer:** 5 Abfolge des ÜW in der ATS Einstellung (1 ist Primäre, 2-10 Ausfallebene)

**Eindeutige ID ÜW:** 0 Die eindeutige ID des ÜW damit dieser vom Empfänger erkannt wird

**ÜW Name:** Backup ÜW 5 Name des ÜW

**SPT Konten Schlüssel:** 0 Nummer zur eindeutigen Festlegung Zentrale zum RCT

**ARC Erkennung**

**RCT ID:** 1 Die eindeutige ID des Empfängers(z.B: SPC Com XT)(1-99999999)

**URL oder IP-Adresse:** 0.0.0.0 URL oder IP-Adress des RCT

**RCT Port:** 52000 Der TCP Port des Empfängers (TCP Port den der Empfänger abhört)

**ÜW Schnittstelle**

**Kommun. Schnittstelle:** Ethernet Kommunikationsschnittstelle des ÜW

**ÜW Gruppe:** Cat 5 Wählen Sie bitte die ÜW Gruppe

**Erweitert**

**Erweiterte Einstellung:** Erweiterte ÜW Einstellung Erweitertes Einstellmenü nur für geübte Anwender

OK
Abbrechen

1. Füllen Sie die Felder wie in der unten stehenden Tabelle aus.
2. Klicken Sie gegebenenfalls auf **Erweiterte ATP Einstellungen**. Falls Sie die automatische Verschlüsselung verwenden, können Sie optional ein Passwort in das Feld **Verschlüsselungspasswort** eingeben. Siehe Konfigurieren der erweiterten ATP-Einstellungen [→ 186].
3. Klicken Sie auf **Speichern**.

	<p><b>⚠️ WARNUNG</b></p> <p>Es wird nicht empfohlen, die <b>Erweiterten ATP-Einstellungen</b> zu ändern. Änderungen dürfen nur von erfahrenen Benutzern vorgenommen werden.</p>
---	---

<b>Zentralen Kennung</b>	
ÜW Ablauffolge	Das Feld enthält die Sequenznummer des ÜW in der ATS-Konfiguration. Nummer 1 ist primär, die Nummern 2 bis 10 sind Backups.
ATP Unique ID	Wenn Sie einen ÜW speichern, weist ihm das System eine einzigartige ID zu. Dies ist die ID des ÜW, damit er von der Empfangszentrale erkannt werden kann.
Name des ÜW	Geben Sie einen Namen für den ÜW ein.
Geräte ID	Geben Sie eine Zahl ein, um die Zentrale eindeutig in der Empfangszentrale zu identifizieren.
<b>Empfänger Erkennung</b>	

Empfangszentr.ID	Geben Sie die Nummer ein, welche die Empfangszentrale (z. B. SPC Com XT) eindeutig in der Zentrale identifiziert. Diese muss mit der Nummer übereinstimmen, die auf dem SPC Com XT-Server im Configuration Manager im Feld <b>Server RCT ID</b> (Server-Empfangszentralen-ID) eingegeben wurde.
Empfangszentrale URL/ IP Adresse	Geben Sie die URL oder IP-Adresse der Empfangszentrale (z. B. SPC Com XT) ein.
EZ TCP Port	Geben Sie den TCP-Port ein, den die Empfangszentrale (z. B. SPC Com XT) überwacht. Der Standard ist 52000. Dieser Wert muss mit dem Wert in Feld <b>Server FlexC Port</b> im Server Configuration Manager-Tool übereinstimmen. Siehe <i>Installations- und Konfigurationshandbuch des SPC Com XT</i> .
<b>ÜW Schnittstelle</b>	
Kommunikationsschnittstelle	Wählen Sie aus der Dropdown-Liste die Schnittstelle, die der ÜW für die Kommunikation verwendet. <ul style="list-style-type: none"> <li>● Ethernet</li> <li>● GPRS: Modem 1</li> <li>● GPRS: Modem 2</li> <li>● Wählverbindung Internet: Modem 1</li> <li>● Wählverbindung Internet: Modem 2</li> </ul>
ÜW Kategorie	Wählen Sie die Kategorie, die auf diesen ÜW angewendet werden soll. Weitere Informationen zu den ÜW-Kategorien finden Sie unter ÜW Kategorie Zeiteinstellung [→ 290].
<b>Erweitert</b>	
Erweiterte ATP Einstellungen	Es wird nicht empfohlen, die erweiterten Einstellungen zu ändern. Änderungen dürfen nur von erfahrenen Benutzern vorgenommen werden.

### 14.6.2.1.1 Konfigurieren der erweiterten ATP-Einstellungen

	<b>⚠️ WARNUNG</b>
	Es wird nicht empfohlen, die Erweiterten ATP-Einstellungen zu ändern. Änderungen dürfen nur von erfahrenen Benutzern vorgenommen werden.

1. Klicken Sie auf die Schaltfläche **Erweiterte ATP Einstellungen**.

**ÜW Konfiguration-Erweiterte Konfiguration**  
 Erweiterte Konfigurationsdetails für neuen FlexC ÜW

**ÜW Verbindungen**

**Primärer ÜW:** Permanent: Verbunden bleiben Wähle die Verbindungsart wenn der ÜW der primäre, aktive Kommunikationsweg ist

**ÜW Backup:** Permanent: Verbunden bleiben Wähle die Verbindungsart wenn der ÜW der sekundäre, Backup Kommunikationsweg ist

**Routine**

**Modus Testanruf (Ruhender ÜW):** Routine abgeschaltet Modus zum Versenden von Testanrufen, wenn der ÜW ruht

**Modus Testanruf (Aktiver ÜW):** Routine abgeschaltet Modus zum Versenden von Testanrufen, wenn der ÜW aktiv ist

**Zeit der ersten Routine:** 00:00 Zeit d. ersten Routinerufes nach Reset o. ÜW Initialisierung

**Zufällig:**  Zufällige Zeit für erste Routine zw. 0-30 min

**Verschlüsselung (256bit AES mit CBC)**

**Schlüssel Update Modus:** Autom. Verschlüss. Auswahl wie die Schlüssel aktualisiert werden

**Errichter Passwort:**  Optionales Passwort zur Verstärkung der Sicherheit bei der ÜW Inbetriebnahme

**Rücksetzen:**  Rücksetzen des Schlüssels zum Vorgabewert beim Senden d. Konfig. zur Zentrale

**ÜW Profile**

**Ereignisprofil:** Über ATS Konfig. Auswahl des Ereignisprofils, welches festlegt was und wie übertragen wird

**Steuerungsprofil:** Über ATS Konfig. Auswahl des Steuerungsprofil, welches erlaubte Befehle festlegt

**ÜW Störung**

**ÜW Überwachungsstör.:**  Generiere Störung bei Ausfall der ÜW Überwachung oder Übertragungsfehler

**Ereignis Timeout:** 30s Zeitdauer die versucht wird das Ereignis zu übertragen

**Minimale Länge des Paketes**

**Poll Paket:** 0 Bytes Min. Länge eines Polling Paketes

**Ereignismeldung:** 0 Bytes

**andere Meldungen:** 0 Bytes Minimale Länge der Verbindungs- u. Schlüssel Update-Nachrichten

1. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben:
2. Klicken Sie auf **Speichern**.

<b>ÜW Verbindungen</b>	
Aktive ATP Verbindungen	Wählen Sie den ÜW-Verbindungstyp, wenn der ÜW als der primäre Kommunikationspfad betrieben wird. <ul style="list-style-type: none"> <li>● Permanent: Verbunden bleiben</li> <li>● Vorübergehend: Abbruch 1 Sekunde</li> <li>● Vorübergehend: Abbruch 20 Sekunden</li> <li>● Vorübergehend: Abbruch 80 Sekunden</li> <li>● Vorübergehend: Abbruch 3 Minuten</li> <li>● Vorübergehend: Abbruch 10 Minuten</li> <li>● Vorübergehend: Abbruch 30 Minuten</li> </ul>
Ruhende ATP Verbindungen	Wählen Sie den ÜW-Verbindungstyp, wenn der ÜW als ein Backup-Kommunikationspfad betrieben wird. <ul style="list-style-type: none"> <li>● Permanent: Verbunden bleiben</li> <li>● Vorübergehend: Abbruch 1 Sekunde</li> <li>● Vorübergehend: Abbruch 20 Sekunden</li> <li>● Vorübergehend: Abbruch 80 Sekunden</li> <li>● Vorübergehend: Abbruch 3 Minuten</li> <li>● Vorübergehend: Abbruch 10 Minuten</li> <li>● Vorübergehend: Abbruch 30 Minuten</li> </ul>

<b>Routine</b>	
Routine Modus (inaktiver ÜW)	<p>Wählen Sie den Modus für den Versand der Testanrufe, wenn der ÜW der inaktive ÜW ist.</p> <ul style="list-style-type: none"> <li>● Testanrufe abgeschaltet</li> <li>● Testanruf alle 10 Minuten</li> <li>● Testanruf jede Stunde</li> <li>● Testanruf alle 4 Stunden</li> <li>● Testanruf alle 24 Stunden</li> <li>● Testanruf alle 48 Stunden</li> <li>● Testanruf alle 7 Tage</li> <li>● Testanruf alle 30 Tage</li> </ul>
Routine Modus (Aktiver ÜW)	<p>Wählen Sie den Modus für den Versand der Testanrufe, wenn der ÜW der aktive ÜW ist.</p> <ul style="list-style-type: none"> <li>● Testanrufe abgeschaltet</li> <li>● Testanruf alle 10 Minuten</li> <li>● Testanruf jede Stunde</li> <li>● Testanruf alle 4 Stunden</li> <li>● Testanruf alle 24 Stunden</li> <li>● Testanruf alle 48 Stunden</li> <li>● Testanruf alle 7 Tage</li> <li>● Testanruf alle 30 Tage</li> </ul>
<b>Verschlüsselung (256 bit AES)</b>	
Schlüsselmodus	<p>Wählen Sie, wie die Verschlüsselung aktualisiert werden soll.</p> <ul style="list-style-type: none"> <li>● Automatische Verschlüsselung</li> <li>● Automatische Verschlüsselung mit Aktualisierungen</li> <li>● Fixe Verschlüsselung</li> </ul> <p>Hinweis: Die automatische Verschlüsselung nutzt den Standardschlüssel und aktualisiert ihn einmal. Die automatische Verschlüsselung mit Aktualisierungen ändert den Verschlüsselungsschlüssel alle 50.000 Nachrichten oder einmal pro Woche, je nachdem, welcher Fall eher eintritt.</p>
Verschlüsselungspasswort	<p>Optionales Passwort für eine erhöhte Sicherheit während der ersten Inbetriebnahme des ÜW. Das Passwort muss unabhängig im SPT oder in der Empfangszentrale eingegeben werden.</p>
Verschlüsselung zurücksetzen	<p>Setzt den Schlüssel für die Verschlüsselung und das Kennwort auf die Standardwerte zurück.</p>
<b>Verbindungswegprofile</b>	
Ereignisprofil	<p>Wählt das Ereignisprofil in dem festgelegt ist, wie und welche Ereignisse an dieses ATS übertragen werden.</p> <ul style="list-style-type: none"> <li>● Benutze ATS Einstellungen</li> <li>● Vorgegebenes Ereignisprofil</li> <li>● Alle Ereignisse</li> </ul>
Steuerprofil	<p>Auswahl des Steuerprofils, das die Befehle definiert, die in diesem ATS zulässig sind.</p> <ul style="list-style-type: none"> <li>● Benutze ATS Einstellungen</li> <li>● Vorgegebenes Steuerungsprofil</li> </ul>

	<ul style="list-style-type: none"> <li>● Custom Command Profile (Kd.spez. Steuerungsprofil)</li> </ul>
<b>ÜW Störung</b>	
Störung des Verbindungsweges (ATP)	Wählen Sie diese Option, um eine ÜW-Störung zu erzeugen, falls die ÜW-Überwachung fehlschlägt oder ein Ereignis nicht an den ÜW übertragen werden kann.
Timeout erneute Übertr.	Die Dauer, die der ÜW versucht, das Ereignis zu übermitteln, bis das Ereignis auf dem ÜW fehlschlägt und an den nächsten ÜW weitergeleitet wird. <ul style="list-style-type: none"> <li>● 30 Sekunden</li> <li>● 60 Sekunden</li> <li>● 90 Sekunden</li> <li>● 2 Minuten</li> <li>● 3 Minuten</li> <li>● 5 Minuten</li> <li>● 10 Minuten</li> </ul>
<b>Min. Nachrichtenlänge</b>	
Polling Nachricht	Minimallänge einer Polling-Nachricht. <ul style="list-style-type: none"> <li>● 0 Byte</li> <li>● 64 Byte</li> <li>● 128 Byte</li> <li>● 256 Byte</li> <li>● 512 Byte</li> </ul>
Ereignismeldung	Minimallänge eines Ereignisses und einer Testanrufnachricht. <ul style="list-style-type: none"> <li>● 0 Byte</li> <li>● 64 Byte</li> <li>● 128 Byte</li> <li>● 256 Byte</li> <li>● 512 Byte</li> </ul>
Sonstige Meldung	Minimallänge des Verbindungs- und Verschlüsselungsschlüssels und der Aktualisierungsmeldungen. <ul style="list-style-type: none"> <li>● 0 Byte</li> <li>● 64 Byte</li> <li>● 128 Byte</li> <li>● 256 Byte</li> <li>● 512 Byte</li> </ul>

### 14.6.2.2 ÜW zu analogem Empfänger

Falls eine Verbindung zwischen der SPC-Zentrale und der Empfangszentrale (z. B. SPC Com XT) unterbrochen wird, kann FlexC zu einer Backup-ÜW-Verbindung zwischen der SPC-Zentrale und einer analogen ARC wechseln. Sie können bis zu 10 ÜWs für jedes ATS konfigurieren.

1. Klicken Sie zur Konfiguration eines ÜW zwischen einer SPC-Zentrale und einer analogen ARC auf die Schaltfläche **ÜW zu analogem Empfänger**.
2. Füllen Sie die Felder wie in der unten stehenden Tabelle aus.
3. Klicken Sie auf **Speichern**.

<b>Zentralen Kennung</b>
--------------------------

ÜW Ablauffolge	Das Feld enthält die Sequenznummer des ÜW in der ATS-Konfiguration. Nummer 1 ist primär, die Nummern 2 bis 10 sind Backups.
ATP Unique ID	Diese ID identifiziert eindeutig den ÜW in der Empfangszentrale.
Name des ÜW	Geben Sie einen Namen für den ÜW ein.
Geräte ID	Geben Sie eine Zahl (1–999999) ein, um die Zentrale eindeutig in der Empfangszentrale zu identifizieren.
<b>ARC Verbindung</b>	
Nummer 1	Telefonnummer 1
Nummer 2	Telefonnummer 2
Modem Auswahl	Wählen Sie das zu verwendende Modem. <ul style="list-style-type: none"> <li>● Modem 1</li> <li>● Modem 2</li> </ul>
<b>Routine</b>	
Routine Modus (inaktiver ÜW)	Wählen Sie den Modus für den Versand der Testanrufe, wenn der ÜW im inaktiven Modus ist. Standard: 24 Stunden. <ul style="list-style-type: none"> <li>● Testanrufe deaktiviert</li> <li>● Testanruf alle 10 Minuten</li> <li>● Testanruf jede Stunde</li> <li>● Testanruf alle 24 Stunden</li> <li>● Testanruf alle 48 Stunden</li> <li>● Testanruf alle 7 Tage</li> <li>● Testanruf alle 30 Tage.</li> </ul>
Routine Modus (Aktiver ÜW)	Wählen Sie den Modus für den Versand der Testanrufe, wenn der ÜW ein aktiver ÜW ist. Standard: 24 Stunden. <ul style="list-style-type: none"> <li>● Testanrufe deaktiviert</li> <li>● Testanruf alle 10 Minuten</li> <li>● Testanruf jede Stunde</li> <li>● Testanruf alle 24 Stunden</li> <li>● Testanruf alle 48 Stunden</li> <li>● Testanruf alle 7 Tage</li> <li>● Testanruf alle 30 Tage.</li> </ul>
Zeit des ersten Testanrufes	Die Zeit des ersten Testanrufs nach dem Zurücksetzen oder nach der ATS-Initialisierung. <ul style="list-style-type: none"> <li>● Sofort Senden (Standard)</li> <li>● oder</li> <li>● Wählen Sie ein halbstündliches Intervall zwischen 00:00 und 23:30.</li> </ul>
<b>Ereignisprotokoll</b>	
Protokoll	Das verwendete Übertragungsprotokoll. <ul style="list-style-type: none"> <li>● SIA</li> <li>● SIA Extended 1</li> <li>● SIA Extended 2</li> <li>● Contact-ID</li> </ul>
Ereignisprofil	Wählt das Ereignisprofil in dem festgelegt ist, wie und welche Ereignisse an dieses ATS übertragen werden. <ul style="list-style-type: none"> <li>● Benutze ATS Einstellungen</li> <li>● Vorgegebenes Ereignisprofil</li> <li>● Vorgabe Portal Ereignis Profil</li> </ul>

	<ul style="list-style-type: none"> <li>● Alle Ereignisse</li> <li>● Kundenspezifisches Ereignisprofil</li> </ul>
<b>ÜW Störung</b>	
Störung des Verbindungsweges (ATP)	Wählen Sie diese Option, um eine ÜW-Störung zu erzeugen, falls die ÜW-Überwachung fehlschlägt oder ein Ereignis nicht an den ÜW übertragen werden kann.
Timeout erneute Übertr.	<p>Die Dauer, die der ÜW versucht, das Ereignis zu übermitteln, bis das Ereignis auf dem ÜW fehlschlägt und an den nächsten ÜW weitergeleitet wird. Standard: 2 Minuten</p> <ul style="list-style-type: none"> <li>● 30 Sekunden</li> <li>● 60 Sekunden</li> <li>● 90 Sekunden</li> <li>● 2 Minuten</li> <li>● 3 Minuten</li> <li>● 5 Minuten</li> <li>● 10 Minuten</li> </ul>

### 14.6.2.3 Installationsdetails bearbeiten

Die Installationsdetails werden an die Empfangszentrale weitergeleitet, um den Bediener bei der Identifizierung der Zentrale zu unterstützen.

1. Klicken Sie auf die Schaltfläche **Installation bearbeiten**.

1. Füllen Sie die Felder in der unteren Tabelle aus.

2. Klicken Sie auf **Speichern**.

ATS Installations-ID	Die ID der ATS-Installation (1–999999999).
Firmen-ID	Für zukünftige Verwendung.
Firmenname	Der Name des Unternehmens.
Adresse der ATS Installation	Die Adresse der ATS-Installation.
GPS Koordinaten	Die GPS-Koordinaten der Installation.
ATS Errichter Name	Der Name des Errichters des Übertragungssystems (ATS).
Telefonnr. des Errichter 1	Die Telefonnummer des Errichters des Übertragungssystems (ATS).
Telefonnr. des Errichter 2	Die Telefonnummer des Errichters des Übertragungssystems (ATS).
Hinweise	Zusätzliche Informationen für die Empfangszentrale.

### 14.6.3 Konfigurieren eines SPC-Connect-Übertragungssystems (ATS)

Die Funktion **SPC ConnectATS hinzufügen** stellt die Kommunikation zwischen der Zentrale (SPT) und dem **SPC Connect-Server** (Empfangszentrale, [www.spconnect.com](http://www.spconnect.com)) her. Mit der generierten SPC Connect ATS-Registrierungs-ID kann ein Zentralenbenutzer ein Benutzerkonto und eine Zentrale auf der SPC Connect-Website registrieren, um per Fernzugriff auf die Zentrale zuzugreifen.

1. Öffnen Sie zur Konfiguration eines SPC Connect ATS den Menüpfad **Kommunikation > FlexC > FlexC ATS**.
2. Klicken Sie im Fenster „ATS-Konfiguration“ auf **SPC Connect hinzufügen**, um einen Kommunikationspfad mit dem SPC Connect-Server zu öffnen.
  - ⇒ Der **Tabelle der Ereignisfolge** wird daraufhin ein SPC- Connect-Übertragungssystem mit den folgenden Attributen hinzugefügt:
    - SPC Connect ATS-Registrierungs-ID
    - Standard-ÜW über Ethernet. Weitere Informationen zu ÜW-Feldern finden Sie unter ÜW zur FlexCom (AE) [→ 184].
    - Standardmäßiges Ereignisprofil für SPC Connect
    - Standardmäßiges Befehlsprofil für SPC Connect
    - Die standardmäßige Empfangszentralen-URL lautet [www.spconnect.com](http://www.spconnect.com).
    - Der SPT-Kontocode für den ÜW wird aufgefüllt.
    - Notieren Sie sich die SPC Connect **ATS-Registrierungs-ID** und übergeben Sie sie dem Kunden zusammen mit dem *SPC Connect-Benutzerhandbuch*.

ID	ATS Name	RegistrierungsID	ATP Anzahl	Polling Timeout	ATS Ereignis Zeitüber.	Erzeuge FTC
1	ATS 1	-	4	360	300	Ja
2	DocTest	-	3	450	300	Ja
3	ATS 1	-	1	180	300	Ja
4	SPC Portal	-	1	86400	300	Nein
5	ATS 5	-	1	90	300	Ja
6	ATS 6	-	0	0	300	Ja
7	ATS 7	-	0	0	300	Ja
8	ATS 8	-	1	180	300	Ja
9	ATS 9	-	4	720	300	Ja
10	SPC Portal	-	1	86400	300	Nein

**SPC Connect aktivieren**  
SPC Connect Verbindung hinzufügen

**Neues EN50136-1 ATS**

EN50136-1:Einweg ATS Übertragungssystem (o. Backupweg)

EN50136-1 :Mehrwege ATS Übertrag.-system (m. Backupweg)

ATS, mit zwei Wegen und zwei Servern hinzufügen (EN50136-1:2012)

**neues kunden. ATS**

### 14.6.4 Konfigurieren von Ereignisprofilen

Das Ereignisprofil definiert, welche Ereignisse an ein ATS übermittelt werden, den Berichtstatus für ein Ereignis und die Ereignisausnahmen. Ereignisausnahmen ermöglichen Ihnen, Standardwerte für Ereignisse kundenspezifischen Werten neu zuzuordnen. Weitere Informationen finden Sie unter Ereignis Ausnahmendefinition [→ 195].

<b>!</b>	<p><b>HINWEIS</b></p> <p>Wählen Sie für eine schnelle Erstellung eines neuen Ereignisprofils die Optionen <b>Kommunikation &gt; FlexC &gt; Ereignisprofile</b>. Wählen Sie in der Tabelle <b>Ereignisprofile</b> ein Ereignisprofil, und klicken Sie auf die Schaltfläche „Bearbeiten“ (blauer Stift). Blättern Sie zum Ende des Bildschirms, und klicken Sie auf <b>Wiederholung</b>. Nun können Sie die erforderlichen Änderungen vornehmen.</p>
----------	--

1. Wählen Sie zur schrittweisen Konfiguration von FlexC-Ereignisprofilen die Optionen **Kommunikation > FlexC > Ereignisprofile**.
2. Klicken Sie auf **Hinzufügen**. Das Fenster **Ereignisprofile** wird angezeigt.

**Ereignis Profil Konfiguration**

Konfigurationsdetails für neue FlexC Ereignisprofile...

**Name:**  Name des Ereignisprofiles

**Ereignisfilter**

Filtergruppe	Berichtserei...	Ausnahmenzahl	Ausnahme hinzufügen
Bestätigte Alarme	<input checked="" type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Einbruchalarm	<input checked="" type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Einbruchalarm quittiert	<input checked="" type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Panik/Überfall/Bedrohung	<input checked="" type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Feuer Alarm Rückstellung	<input checked="" type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Medizin. Alarm und Rückstellung	<input checked="" type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Sabotage	<input checked="" type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Sabotage Rückstell.	<input checked="" type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Einstell.	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Stör.	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Störung Rückstell	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Netzwerk	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Routine	<input checked="" type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Techniker Zugriff System	<input checked="" type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
System Information	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Sperrung/Abschaltung	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
MG Gehetest	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
MG Zustandswechsel	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Kamera	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Tür Warnungen	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Tür Information	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme
Benutzer Info	<input type="checkbox"/>	0	Auswahl Ereignis als Ausnahme

**Ber.-filter**

[Bereich 1] - Area 1

1. Geben Sie einen **Namen** ein, um das Ereignisprofil zu identifizieren.
2. Wählen Sie die Ereignisfiltergruppen für die Meldung dieses Profils, indem Sie die Kontrollkästchen **Ereignisbericht** aktivieren.
3. Wählen Sie zur Verhinderung, dass bestimmte Ereignisse oder Adressen innerhalb eines Ereignisses gemeldet werden, die entsprechende Dropdown-Liste **Ereignis-Ausnahme hinzufügen**.
4. Klicken Sie auf **Hinzufügen**, um den Bildschirm **Ereignis Ausnahmendefinition** anzuzeigen. Weitere Informationen finden Sie unter Ereignis Ausnahmendefinition [→ 195].
5. Wählen Sie zur Anwendung eines Ereignisprofils auf einen Bereich diesen unter **Bereichsfilter** aus.
6. Klicken Sie auf **Speichern** und **Zurück**. Das neue Profil wird in der Tabelle **Ereignisprofile** angezeigt.



Sie können eine Liste aller Ereignisausnahmen für ein Ereignisprofil unter **Ereignis Ausnahmen** im Bildschirm **Ereignisprofile** anzeigen.

**HINWEIS**

Sie können ein **Vorgegebenes Ereignisprofil**, ein **Vorgabe Portal Ereignis Profil** oder ein Ereignisprofil nicht löschen, wenn es einem ATS zugewiesen ist. Wenn Sie versuchen, ein Ereignisprofil zu löschen, das in Gebrauch ist, erhalten Sie eine Fehlermeldung.

### 14.6.4.1 Ereignis Ausnahmendefinition

Ereignisausnahmen ermöglichen Ihnen die Änderung der folgenden Einstellungen für einen Bereich von Adressen in einem Ereignis:

- Ereignisbericht
- SIA-Code
- CID-Code
- Ereignisadresse (z. B. MG-ID, Bereich-IDs, Benutzer-IDs)

In der Filtergruppe **Einbruchalarme** können Sie beispielsweise eine Ereignis Ausnahme für einen Bereich von MG-IDs im Ereignis „Einbruchalarm“ (EA) wie folgt definieren:

- EA-Ereignisse für MG-ID 1–9 nicht melden
- SIA-Code von EA zu YZ nicht neu zuordnen
- CID von 130 / 1 bis 230 / 1 neu zuordnen
- MG-ID 1–9 zu MG-ID 101–109 neu zuordnen

### Definition Ereignis Ausnahme- Erweiterte Einstellungen

FlexC Ausnahmendef. für Ereignis Ausnahme

**Identifizierung**

**Name:** Ereignis Ausnahme 1 Name der Ereignis Ausnahme

**Ereignis ID:** 1000 Ereignis ID des Ereignisses im System

**Ereignis Beschreibung:** Einbruch Alarm [Alarm Meldegruppe] Beschreibung des Ereignis

**Ereignis Filter**

**Ereignisbericht:**  Auswahl wenn Ereignis normal gemeldet

**Ausnahme Filter ein:**  Auswahl zum Einschalten d. Filterausnahme

if ( 1 <= MG ID <= 9 )

dann Ereignis nicht melden

**Ereignisformat**

**SIA Code:** BA SIA code, der übermittelt wird zum Abbilden des Ereignisses

**Contact ID Ereignis Code/ Vermerk:** 130 / 1 Contact ID Ereignis Code/ Vermerk, der übermittelt wird zum Abbilden des Ereign.

**Ausnahme der Umleitung aktiv:**  zum Einschalten der Umleitungsausnahme

if ( 1 <= MG ID <= 9 )

dann leite SIA Ereignis um zu YZ

und leite Contact ID Ereignis Code/ Vermerk um zu 230 / 1

und leite Ereignisadresse um zu 101 - 109

1. Füllen Sie zur Konfiguration einer **Ereignis Ausnahmendefinition** die in der unteren Tabelle beschriebenen Felder aus.
2. Klicken Sie auf **Speichern**.
3. Klicken Sie auf **Zurück**, um zum Bildschirm **Ereignisprofile** zurückzukehren.
  - ⇒ Der Name jeder Ausnahme wird in der Tabelle **Ereignis Ausnahmen** im unteren Bereich des Bildschirms angezeigt. Die Tabelle enthält die Einstellungen für die Felder **Ereignisbericht**, **Ausnahme vom Filter**, **Ereigniskode (SIA/CID)** und **Ausnahme von der Umleitung** für das Ereignis.

Ereignis Ausnahme Name	Bericht Ereignis	Filter Ausnahme	Ereignis Code (SIA/ CID)	Umleitung Ausnahme
Ereign. ID 1000: Einbruch Alarm [Alarm Meldegruppe] Ereignis Ausnahme 1	Ja	Ereignis nicht melden [1-9]	BA/130	[1-9] - YZ/230[101-109]

1. Klicken Sie auf das Symbol **Bearbeiten**, um Änderungen vorzunehmen, oder klicken Sie auf das Symbol **Löschen**, um eine **Ereignis Ausnahme** zu löschen.
2. Aktivieren Sie zur Anwendung eines Ereignisprofils auf einen Bereich das entsprechende Bereichskontrollkästchen.
3. Klicken Sie auf **Speichern**, um das Ereignisprofil zu speichern.

4. Klicken Sie auf **Zurück**, um das Profil in der Tabelle **Ereignisprofile** anzuzeigen.

<b>Identifikation</b>	
Name	Geben Sie den Namen der Ereignisausnahme ein.
Ereignis ID	Die Ereignis-ID des Ereignisses im System. Sie dient nur zu Anzeigezwecken.
Ereignisbeschreibung	Die Beschreibung des Ereignisses. Sie dient nur zu Anzeigezwecken.
<b>Ereignisfilter</b>	
Ereignisbericht	Aktivieren Sie dieses Kontrollkästchen, um das Ereignis zu melden. Dadurch wird der für die Ereignisfiltergruppe festgelegte Berichtswert überschrieben. Falls die Filtergruppe <b>Einbruchalarme</b> beispielsweise gemeldet wird, können Sie das BA-Ereignis ausschließen oder diese Einstellung deaktivieren.
Ausnahme vom Filter zulassen	Aktivieren Sie dieses Kontrollkästchen, um einen Adressbereich, z. B. MG-IDs, von der Feldeinstellung <b>Ereignisbericht</b> auszuschließen.
wenn ( $0 \leq MG-ID \leq 9999$ ) dann Ereignisbericht/Ereignis nicht übertragen	Geben Sie einen Bereich von Adressen ein, um sie von der Einstellung <b>Ereignisbericht</b> auszuschließen. Wenn Sie beispielsweise den Ereignistyp „Einbruchalarm“ melden, können Sie wählen, die <i>MG-ID 1–9</i> nicht für dieses Ereignis zu melden.  Alternativ können Sie wählen, den Ereignistyp „Einbruchalarm“ nicht zu melden und die <i>MG-ID 1–9</i> für dieses Ereignis zu melden.
<b>Ereignisformat</b>	
SIA Ereigniskode	Der standardmäßige SIA-Ereigniskode, der zur Darstellung des Ereignisses übermittelt wird. Dieses Feld dient nur zu Anzeigezwecken.
Contact ID Ereignis Code/ Vermerk	Der standardmäßige Code/Vermerk für das Kontakt-ID-Ereignis, der zur Darstellung des Ereignisses übermittelt wird. Dieses Feld dient nur zu Anzeigezwecken.
Ausnahme von der Umleitung zulässig	Aktivieren Sie dieses Kontrollkästchen, um den standardmäßigen SIA, CID-Code / Vermerk und die Ereignisadresse den kundenspezifischen Werten hinzuzufügen (z. B. zur Neuordnung der <i>MG-IDs 1–9</i> zu den <i>MG-IDs 101–109</i> . Bei Aktivierung werden die unteren Felder angezeigt.
wenn ( $0 \leq MG-ID \leq 9999$ )	Geben Sie den Adressbereich ein, der für ein Ereignis neu zugeordnet werden soll. Wenn Sie beispielsweise die <i>MG-IDs 1–9</i> den <i>MG-IDs 101–109</i> neu zuordnen möchten, geben Sie <i>1</i> und <i>9</i> ein. Die Menge der Adressen im Bereich muss der Menge der im unteren Feld <b>Umleitung der Ereignisadresse zu</b> definierten Adressen entsprechen.
dann Umleitung von SIA Ereigniskode zu EA	Ordnen Sie den standardmäßigen SIA-Code dem kundenspezifischen SIA-Code neu zu.
und Umleitung von Contact ID Ereigniskode/ Vermerk zu	Ordnen Sie den standardmäßigen CID Ereignis Code / Vermerk einem kundenspezifischen CID Ereignis Code / Vermerk zu.
und Umleitung der Ereignisadresse zu	Geben Sie den neuen Bereich der Adressen ein. Wenn Sie beispielsweise die <i>MG-IDs 1–9</i> den <i>MG-IDs 101–109</i> neu zuordnen möchten, geben Sie <i>101 und 109</i> ein.

## 14.6.5 Konfigurieren von Steuerprofilen

Das Steuerprofil definiert die Befehle, die in einem ATS zulässig sind. Dieses Profil bestimmt, wie ein CMS eine Zentrale steuern kann. Das standardmäßige Steuerprofil unterstützt keine Videoverifikation.



### HINWEIS

Um schnell ein neues Steuerprofil zu erstellen, wählen Sie **Kommunikation > FlexC > Steuerprofil**. Wählen Sie in der Tabelle **Steuerprofil** ein Steuerprofil, und klicken Sie auf die Schaltfläche „Bearbeiten“ (blauer Stift), blättern Sie auf dem Bildschirm nach unten, und klicken Sie auf **Wiederholung**. Nun können Sie die erforderlichen Änderungen vornehmen.

- Wählen Sie **Kommunikation > FlexC > Steuerprofile**, um Schritt für Schritt ein Steuerprofil hinzuzufügen.

The screenshot shows the 'Communications - FlexC' window with three tabs: 'ATS Konfig', 'Ereignis Profile', and 'Befehls Profile'. The 'Befehls Profile' tab is active, displaying a table with the following data:

ID	Name des Befehls-Profiles	Befehle erlaubt	Befehle aufgezeichnet
1	Vorgabe Steuerungs Profil	49	40
2	Vorgegebene Befehle [SPC Connect]	75	40
3	Commandoprofil 3	49	40

Below the table is a button labeled 'Hinzufügen neues Befehlsprofil'.

- Klicken Sie auf **Hinzufügen**.

**Steuerungsprofil Konfiguration**  
Konfigurationsdetails für neues FlexC Profil...

Name: Commandoprofil 3 Name des Steuerungsprofils

**Befehlsprofil Authentifikation**

Authentifikation Modus: Befehls o Zentralenbenutzer Modus zum Bestätigen der Rechte des Benutzers des Befehlsprofils

Benutzername: FlexC Name des Benutzers des Befehlsprofils

Passwort: \*\*\*\*\* Passwort des Benutzers des Befehlsprofils

**Live Stream**

Live Stream Modus: Deaktiv Auswahl, wann Live Stream verfügbar ist

**Steuerungsfiler**

System Steuerungen	Steu. eingeschaltet	Steuerungslog
Zentralen Zusammenf. abfr.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Zeit und Datum stellen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Techniker freigeben	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Hersteller freigeben	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enter Full Engineer Mode	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Exit Full Engineer Mode	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Bereich Status abfragen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Status der Änderung des Bereichszustandes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modus des Bereiches (S/U) ändern	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Status der Zentralen Alarme abfrag.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Alarme bearbeiten	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sirene abstellen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MG Status abfragen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Meldegruppe steuern	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ereignisspeicher abfragen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ereignisse einer MG abfragen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Drahtlos Ereignisse abfragen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Status logischer Ausgang abfragen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Steuern logischer Ausgänge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Überprüfen d Benutzers in d. Zentr.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons: Löschen, Replicate, OK, Abbrechen

1. Geben Sie einen **Namen** ein, um das Steuerprofil zu identifizieren.
2. Wählen Sie aus dem Dropdown-Menü den **Modus der Authentifikation** (Steuerungsbenutzer oder Zentralenbenutzer, Nur Steuerungsbenutzer oder Jeder Benutzer auf Zentralenniveau).

<b>!</b>	<p><b>HINWEIS</b></p> <p>Der standardmäßige <b>Steuerungsbenutzername</b> stellt einen Out-of-the-box-Benutzer bereit, der schnell und einfach die Steuerung der Zentrale vom SPC Com XT ermöglicht. Er bietet eine Vielzahl von Befehlen. Der standardmäßige Steuerungsbenutzer kann beispielsweise alle Bereich scharf schalten und alle MGs steuern. Für eine strengere Steuerung, um z. B. nur bestimmte Bereiche scharfzustellen, können Sie ein kundenspezifisches Steuerprofil mit einem definierten Rechtesatz einrichten. Sie können ein <b>Vorgegebenes Steuerungsprofil</b>, ein <b>Vorgabe Portal Steuerungs Profil</b> oder ein Steuerprofil nicht löschen, wenn es einem ATS zugewiesen ist.</p>
----------	--

3. Geben Sie den Namen des Steuerungsbenutzers in das Feld **Steuerungsbenutzername** ein. Dieser muss mit dem Benutzernamen für die Authentifizierung auf dem SPC Com XT übereinstimmen.

4. Geben Sie das Passwort des Steuerprofils in das Feld **Steuerungspasswort** ein. Dieses muss mit der Benutzer-PIN oder dem Benutzerpasswort für die Authentifizierung auf dem SPC Com XT übereinstimmen.
5. Wählen Sie die Option **Live Übertragungs Modus** (Deaktiviert, Nur nach Alarm, Immer, System ist extern scharf), um die Datenschutzooptionen für das Streaming zu bestimmen. **Immer** erzeugt das höchste Datenvolumen.
6. Wählen Sie unter **Steuerungsfiler** die zu aktivierenden Befehle. Eine vollständige Liste der Befehl finden Sie unter FlexC-Steuerung [→ 287].
7. Wählen Sie die zu protokollierenden Befehle.
8. Klicken Sie auf **Speichern**.
9. Klicken Sie auf **Zurück**, um das Steuerprofil in der Tabelle **Steuerprofil** anzuzeigen.
10. Klicken Sie zur Änderung eines Steuerprofils neben einem Steuerprofil auf die Schaltfläche **Bearbeiten** (blauer Stift).

# 15 Kommunikationseinstellungen

## 15.1 Ethernet

IP



Wenn Sie die SPC Ethernet-Schnittstelle konfigurieren möchten, während sie mit einem vorhandenen Local Area Network (LAN) verbunden ist, setzen Sie sich bitte zuerst mit dem Netzwerkadministrator des LANs in Verbindung.

**Kommunikation**



Netzwerkeinstellungen

1. Wählen Sie die Registerkarte **Netzwerk**.
  - ⇒ Eine Ethernet-Verbindung mit dem Controller kann über eine Direktverbindung oder über eine LAN-Verbindung hergestellt werden. Siehe Seite [→ 271].
  - ⇒ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

Kommunikation - Netzwerkeinstellungen

Netzwerk Portal Dienste

### Netzwerkeinstellungen

<b>IP-Adresse</b>	<input type="text" value="192.168.1.100"/>	(x.x.x.x)
<b>IP-Netzwerk</b>	<input type="text" value="255.255.255.0"/>	(x.x.x.x)
<b>Gateway IP-Adresse</b>	<input type="text" value="0.0.0.0"/>	(x.x.x.x)
<b>DNS-Server</b>	<input type="text" value="0.0.0.0"/>	(x.x.x.x)
<b>DHCP aktiv</b>	<input type="checkbox"/>	Auswählen, um dynamische Adressen zu verwenden

IP-Adresse	Die IP-Adresse der Zentrale eingeben.
Netzmaske	Die Netzmaske (Subnet Mask) eingeben, welche den auf dem Local Area Network (LAN) implementierten Typ der Netzwerkadressstruktur definiert.
Gateway IP-Adresse	Die IP-Adresse des IP-Gateways eingeben (falls vorhanden). Hierbei handelt es sich um die Adresse, über die IP-Pakete an externe IP-Adressen im Internet geleitet werden.
DHCP aktivieren	Klicken Sie auf diese Schaltfläche, um die dynamische Adressenzuweisung in der Zentrale zu aktivieren.
DNS-Server	Die IP-Adresse des DNS-Servers eingeben.

## 15.2 Konfigurieren der Netzwerkdienste der Zentrale

### Kommunikation



#### Netzwerkeinstellungen

1. Wählen Sie die Registerkarte **Dienste**.  
⇒ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

### Netzwerkdienste

<b>HTTP aktiv</b>	<input checked="" type="checkbox"/>	Auswählen, um Web-Server zu aktivieren
<b>HTTP-Port</b>	<input type="text" value="443"/>	Port auf dem der Web-Server auf Verbindungen wartet
<b>TLS aktiv</b>	<input checked="" type="checkbox"/>	Auswählen, um die Kommunikation mit dem Web-Server zu verschlüsseln.
<b>Telnet aktiv</b>	<input type="checkbox"/>	Auswählen, um Telnet-Server zu aktivieren
<b>Telnet-Port</b>	<input type="text" value="23"/>	Port auf dem der Telnet-Server auf Verbindungen wartet
<b>SNMP aktiv</b>	<input type="checkbox"/>	Auswählen, um Simple Network Management Protocol zu aktivieren
<b>SNMP-Community</b>	<input type="text" value="public"/>	Community-ID für SNMP-Protokoll
<b>ENMP aktiv</b>	<input type="checkbox"/>	Auswählen zum Aktivieren des Erw. Netzwerk Management Protokolls
<b>ENMP-Port</b>	<input type="text" value="1287"/>	Port-Einstellungen für das ENMP-Protokoll
<b>ENMP-Passwort</b>	<input type="text"/>	Passwort für Konfigurationsänderungen via ENMP
<b>ENMP-Änderungen freigeg.</b>	<input checked="" type="checkbox"/>	Auswählen, um Änderungen der Netzwerkkonfig durch das ENMP-Protokoll zuzulassen

HTTP aktiv	Aktivieren, um den integrierten Webserver auf der Zentrale zu aktivieren.
HTTP-Port	Port-Nummer eingeben, die der Portalserver „abhört“. Als Standardwert ist hier 443 voreingestellt.
TLS aktiv	Aktivieren, um die Verschlüsselung auf dem integrierten Webserver zu aktivieren. Diese Funktion ist standardmäßig aktiviert. Ist TLS aktiviert, kann nur auf Webseiten zugegriffen werden, wenn der Präfix „https://“ vor der IP-Adresse eingegeben wird.
Telnet aktiv	Aktivieren, um den Telnet-Server zu aktivieren. (Standard: Aktiv) <b>Hinweis:</b> Die Verwendung von Telnet umfassende Kenntnisse kann die Controller-Konfiguration beschädigen. Daher sollte Telnet nur von erfahrenen Benutzern oder unter Anleitung eines erfahrenen Benutzers verwendet werden.
Telnet-Port	Die Nummer des Telnet-Ports eingeben.
SNMP aktiv	Aktivieren, um das Simple Network Management Protocol (SNMP) zu aktivieren. (Standard: Inaktiv)
SNMP-Community	Community-ID für das SNMP-Protokoll eingeben. (Standard: Öffentlich)
ENMP aktiv	Aktivieren, um das Enhanced Network Management Protocol (ENMP) zu aktivieren. (Standard: Inaktiv)
ENMP-Port	Geben Sie die ENMP-Portnummer ein (Standard: <b>1287</b> ).
ENMP-Passwort	Geben Sie das Kennwort für das ENMP-Protokoll ein.

---

ENMP-Änderungen freigegeben.	Aktivieren, um Änderungen der Netzwerkkonfiguration durch das ENMP-Protokoll zuzulassen.
------------------------------	--

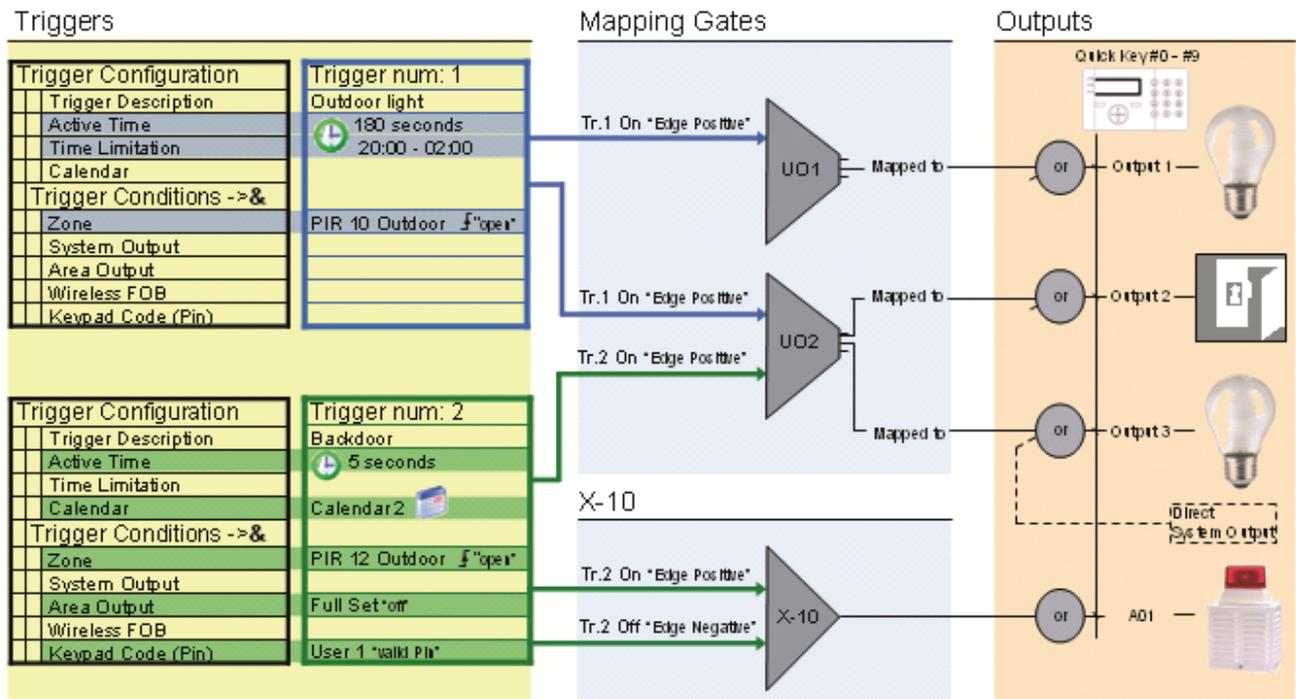
## 16 Konfigurieren der erweiterten Einstellungen

### 16.1 Cause & Effect

Cause & Effect bezeichnet eine Reihe von miteinander in Beziehung stehenden Leistungsmerkmalen und Funktionen, die die Auswertung eines logischen (oder virtuellen) Ausgangs als Funktion von Eingängen oder Bedingungen gemeinsam haben, die in bestimmten Fällen eine Wirkung hervorrufen können.

Die Cause & Effect-Funktionalität von SPC umfasst die Planung mit Kalendern, Triggern, Benutzerausgängen, physischen Ausgängen, Meldergruppen, Bereichen, Bedienteilen, X10 und Benutzerzugang. Den größten Teil der Funktionalität von Cause & Effect decken insbesondere Kalender und Trigger ab.

Funktion	Beschreibung
Kalender	Zeitplanerstellung. Dieser Bereich steuert den Benutzerzugang zur Zentrale und zu Bedienteilen und aktiviert Meldergruppen und physische Ausgänge. Er ist von entscheidender Bedeutung für die automatische Scharfschaltung von Bereichen und die Zeitsteuerung von Triggern.
Trigger	Zwischengeschaltete Ausgänge, die zum Gruppieren von logischen und zeitlichen Bedingungen verwendet werden. Können ihrerseits von X10-Ausgängen und benutzerdefinierten Ausgängen verwendet werden.
Logische Ausgänge	Virtuelle Ausgänge, die vom Benutzer für die logische Steuerung definiert werden. Können zum Ansteuern von echten Geräten auf physische Ausgänge gemappt werden.
X10-Ausgänge	Virtuelle Ausgänge, die für die Steuerung von X10-Geräten verwendet werden. Ein X10-Sender/Empfänger muss an den ersten seriellen Port der SPC-Zentrale angeschlossen sein.
Physische Ausgänge	Möglichkeit, externe Geräte anzusteuern.
Bedienteil-Tastenkombination	Möglichkeit, benutzerdefinierte Ausgänge und X10-Ausgänge anzusteuern.
SPC Pro	PC-Anwendung, die verwendet wird, um eine SPC-Zentrale von einem entfernten Standort oder lokal zu konfigurieren, zu überwachen und zu steuern. Möglichkeit die Zustände von X10-Ausgängen und benutzerdefinierten Ausgängen zu ändern.



### 16.1.1 Einen Cause & Effect hinzufügen

**Advanced**



Cause & Effect

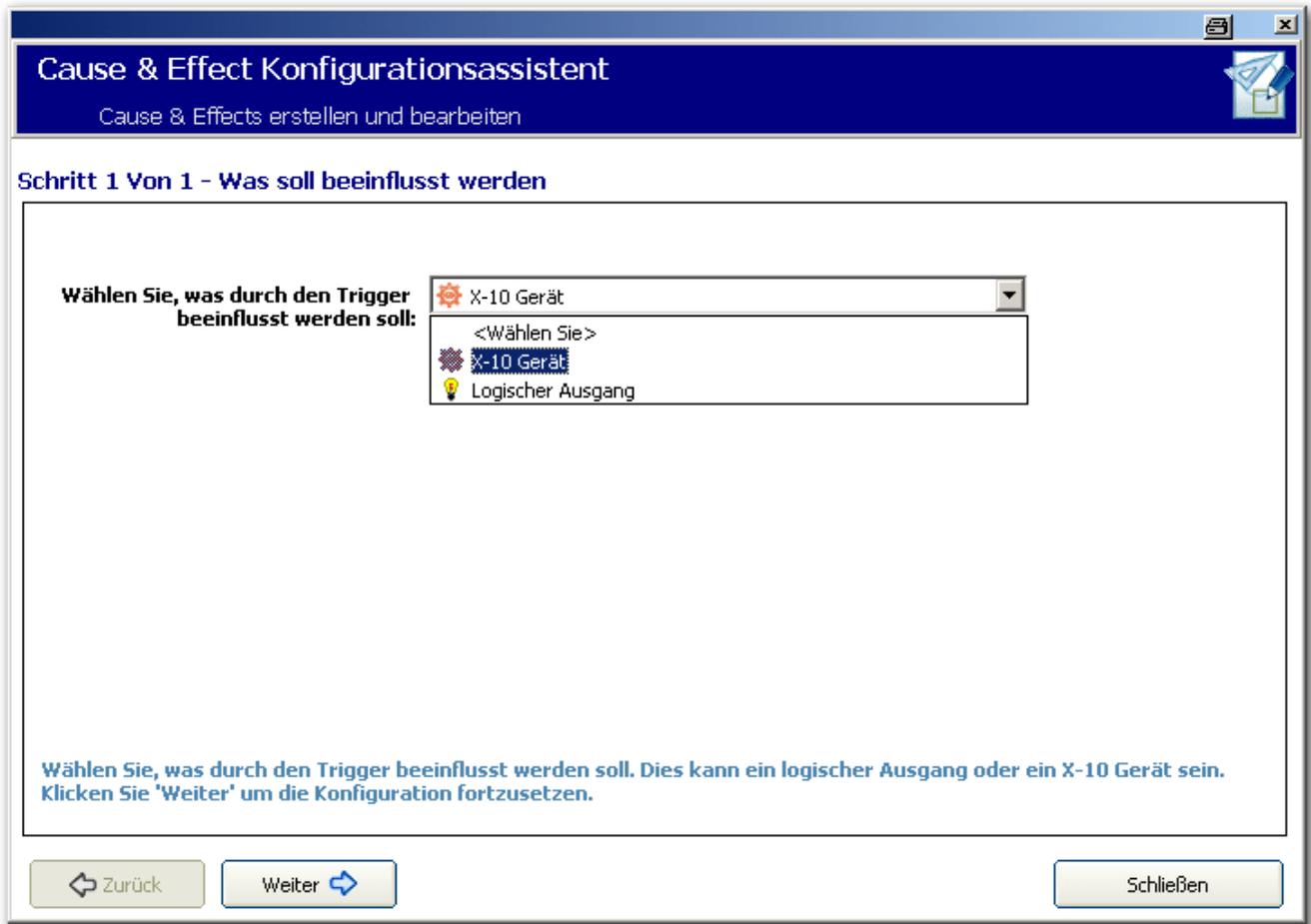
1. Klicken Sie auf das Register **Cause & Effect Liste**.  
⇒ Daraufhin erscheint das folgende Fenster:

Cause & Effect Auflistung

ID	Typ	Item	Beschreibung	# des Triggers
	X-10 Unit	Gerät A1		5
	X-10 Unit	Gerät D5		2

 Neues Cause & Effect hinzufügen

2. Klicken Sie auf die Schaltfläche **Neues Cause & Effect hinzufügen**.  
⇒ Daraufhin erscheint das folgende Fenster.
3. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



4. Wählen Sie den Gerätetyp.

Cause & Effect Konfigurationsassistent		
Schritt 1	Wählen Sie den Gerätetyp X10 oder Logischer Ausgang.	
	<b>X10 Gerät</b>	<b>Logischer Ausgang</b>
Schritt 2	Wählen Sie ein X-10 Gerät.	Wählen Sie einen logischen Ausgang aus der Liste.
Schritt 3	Geben Sie eine Beschreibung für das X10 Gerät ein. Weisen Sie eine Bedienteil-Kurzwahl zu (optional).	Geben Sie eine Beschreibung für den logischen Ausgang ein. Weisen Sie eine Bedienteil-Kurzwahl zu (optional).
Schritt 4	Trigger erstellen/zuweisen [→ 207].	Mappen Sie den logischen Ausgang auf den Erweiterungsausgang.
Schritt 5		Trigger erstellen/zuweisen [→ 207].

## 16.1.2 Trigger erstellen/zuweisen

**Advanced**



Cause & Effect

- ▷ Sie befinden sich im Cause & Effect Konfigurationsassistenten bei Schritt 4 (X10) oder Schritt 5 (logischer Ausgang) Trigger erstellen/zuweisen.

## Cause & Effect Konfigurationsassistent

Cause & Effects erstellen und bearbeiten

**Schritt 4 Von 4 - Trigger erstellen/zuweisen**

**Trigger AN**

AN-Trigger hinzufügen

Trigger löschen

Trigger	Flanke
2 - Trigger 2	Positiv
4 - Trigger 4	Negativ

**Trigger AUS**

AUS-Trigger hinzufügen

Trigger löschen

Trigger	Flanke
2 - Trigger 2	Positiv
4 - Trigger 4	Negativ

Trigger für das ausgewählte X-10 Gerät/log. Ausgang hinzufügen/löschen. Jeder Trigger besitzt eine/mehrere Bedingung(en), die diesen Trigger steuern. Klicken Sie auf einen Trigger um die Bedingung(en) anzuzeigen.

Zurück
Fertigstellen
Schließen

- Klicken Sie auf die Schaltfläche **AN-Trigger hinzufügen** oder die Schaltfläche **AUS-Trigger hinzufügen**.  
⇒ Daraufhin erscheint das folgende Fenster:

**Neuen AN-Trigger hinzufügen**

**Wähle Trigger :**

ID	Triggerbeschreibung
1	Test Trigger

**Flanke** Positiv

Zuweisen
Abbrechen



außerhalb der normalen wöchentlichen Zeitpläne.
---

### 16.2.1 Automatisches Scharf-/Unscharfschalten von Bereichen

Ein Kalender kann für das automatische Scharfschalten oder Unscharfschalten von Bereichen konfiguriert werden.

Für jeden Tag der Woche kann eine Konfiguration maximal 4 Scharfschalt- und 4 Unscharfschaltzeiten umfassen. Uhrzeiten werden im 24-Stunden-Format konfiguriert (hh:mm). Ist die Stundenangabe „24“, muss die Minutenangabe 00 sein – Mitternacht ist „24:00“. Es können Scharfsch-Zeiten ohne Unscharfsch-Zeit eingestellt werden und umgekehrt. Konfigurierte Zeiten schalten den zugewiesenen Bereich entweder scharf oder unscharf (vorausgesetzt alle Bedingungen sind erfüllt). Eingegebene Zeiten gelten nicht als Zeitdauer, sondern als Zeitpunkte, zu denen die betreffende Aktion (Scharfsch/Unscharfsch) ausgeführt wird. Wird der Controller hochgefahren oder zurückgesetzt, bleibt der zum jeweiligen Zeitpunkt eingestellte Scharfsch/Unscharfsch-Status erhalten, und nachfolgende Scharfsch/Unscharfsch-Zeiten werden gemäß Konfiguration umgesetzt.

### 16.2.2 Automatisches Scharf-/Unscharfschalten von anderen Funktionen der Zentrale

Funktionen der Zentrale wie Trigger, Aktivieren von Benutzern, Meldergruppen und physischen Ausgängen können automatisch mit den Statuskonfigurationen An/Aus, Wahr/Falsch, Aktiv/Inaktiv scharf oder unscharf geschaltet werden.

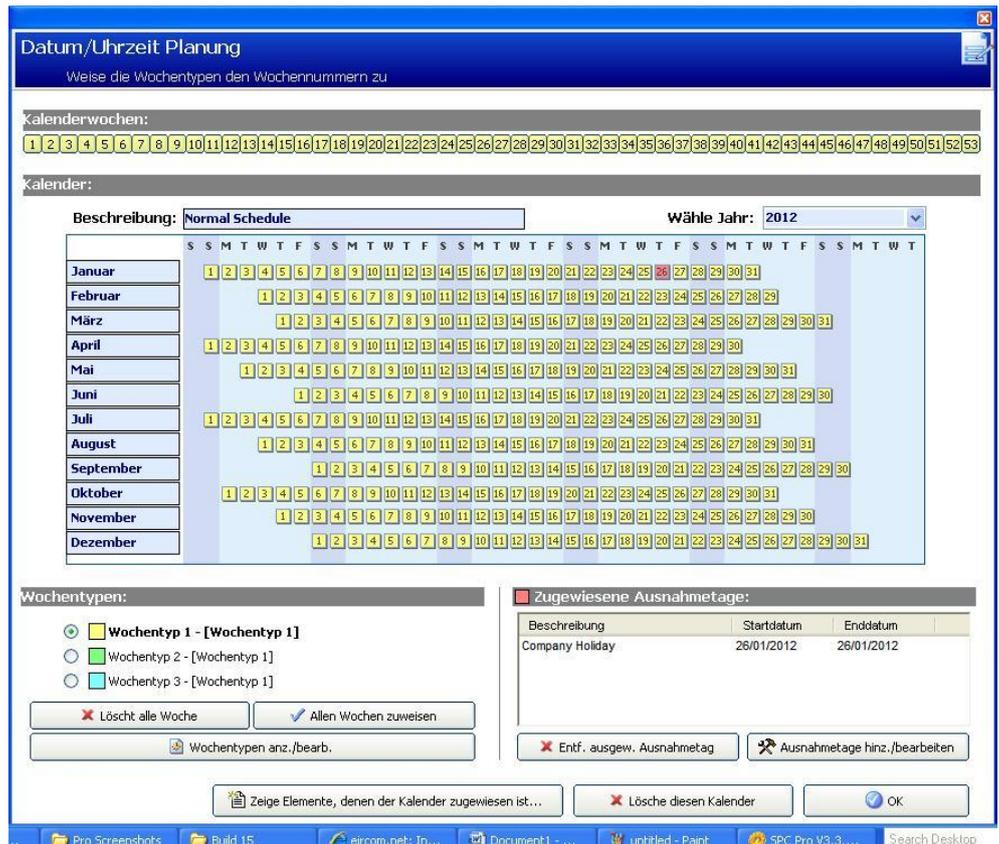
Die Statuswerte An/Aus, Wahr/Falsch, Aktiv/Inaktiv, und können einem Ausgang zugewiesen werden, der effektiv ein- oder ausgeschaltet wird und für jeden beliebigen Wochentag konfiguriert werden kann. Statuskonfigurationen umfassen maximal 4 Einschalt- und 4 Ausschaltzeiten. Uhrzeiten werden im 24-Stunden-Format konfiguriert (hh:mm). Ist die Stundenangabe 24, muss die Minutenabgabe 00 sein – Mitternacht ist 24:00. Jede Konfiguration besteht aus einem Einstellungs paar für einen Status: Ein/Aus, Wahr/Falsch, Aktiv/Inaktiv. Jede Einstellung ohne entsprechende Gegeneinstellung wird ignoriert.

### 16.2.3 Kalender hinzufügen/bearbeiten

Advanced

Kalender

1. Klicken Sie auf **Neuen Kalender hinzufügen**.  
⇒ Daraufhin erscheint das folgende Fenster:



2. Geben Sie eine **Beschreibung** für den Kalender ein (max. 16 Zeichen).
3. Wählen Sie ein **Jahr**.

### Wochentypen

Kalender werden konfiguriert, indem jeder Kalenderwoche ein optionaler Wochentyp zugewiesen wird. Für jeden Kalender können bis zu vier Wochentypen definiert werden. Es muss jedoch nicht allen Wochen ein Wochentyp zugewiesen werden (d. h. ein Wochentyp kann ‚leer‘ sein). Das System unterstützt eine max. Anzahl von 64 Kalenderkonfigurationen.

### Konfigurieren eines Wochentyps

1. Klicken Sie auf die Schaltfläche **Wochentypen anz./bearb.**  
⇒ Bis zu drei Wochentypen können konfiguriert werden.
2. Klicken Sie auf einen Wochentag, um den Konfigurationsdialog für Wochentypen zu öffnen.
3. Geben Sie die gewünschten Zeiten für Scharf-/Unscharfschalten oder für Trigger ein. Verwenden Sie die Zeit-Richtlinien für das automatische Scharf-/Unscharfschalten von Bereichen (siehe Seite [→ 210]) oder für das automatische Scharf-/Unscharfschalten von Funktionen der Zentrale (siehe Seite [→ 210]).
4. Klicken Sie auf **Speichern**.

1. **Zuweisen eines Wochentyps zu einem Kalender**
2. Klicken Sie oben im Kalender auf eine **Wochennummer**, oder klicken Sie im Kalender auf die gewünschte(n) Woche(n).

3. Klicken Sie im Bereich **Wochentypen** der geplanten Woche auf den gewünschten Wochentyp. Beispiel: Ein Wochentyp, der für die Weihnachtszeit konfiguriert ist, wird normalerweise Woche 51/52 zugewiesen.
4. Wenn Sie den Wochentyp einem gesamten Kalender zuweisen möchten, klicken Sie auf **Allen Wochen zuweisen**.

Klicken Sie auf **Zeige Elemente, denen der Kalender zugewiesen ist**, um die Elemente der Zentrale anzuzeigen, die diesen Kalender nutzen.

Klicken Sie auf **Löschen**, um den angezeigten Kalender zu löschen.



---

Globale mit SPC Manager erstellte Kalender können nicht gelöscht werden.

---

#### Siehe auch

-  Automatisches Scharf-/Unscharfschalten von Bereichen [→ 210]
-  Automatisches Scharf-/Unscharfschalten von anderen Funktionen der Zentrale [→ 210]

## 16.3 Trigger

Ein Trigger ist ein Systemstatus (z. B. MG-Schließen- / Zeit- / Systemereignis (Alarm) usw.), der als Cause & Effect-Eingang verwendet werden kann. Trigger können unter Verwendung der logischen Operanden und/oder logisch gemeinsam zugewiesen werden, um Benutzerausgänge zu erstellen. Das System unterstützt maximal 1024 Trigger im gesamten Cause & Effect-System.



Trigger

1. Klicken Sie auf die Schaltfläche **Neuen Trigger hinzufügen**.  
⇒ Daraufhin erscheint das folgende Fenster.

## Triggerkonfiguration

konfigurierte Bedienungen des Triggers

**Trigger-ID :** 1

**Triggerbeschreibung :**

**Aktivierungszeit :**  Anzahl der Sekunden, die der Trigger ausgelöst sein muss.

**Limit Zeit :**   bis

**Kalender :**

**Hinweis:** Der Trigger wird nur aktiviert, wenn alle Bedingungen zur gleichen Zeit erfüllt sind. Wenn ein Zeitlimit oder ein Kalender zugewiesen wird, wird die Aktivierung des Triggers weiter eingeschränkt, da er nur aktiviert wird, wenn alle Bedingungen innerhalb der Kalenderschaltzeit/Zeitlimit erfüllt sind.

Zugewiesene Triggerbedingungen	Triggerbedingungen
Meldergruppe 1 [Front door] - Offen	<input checked="" type="checkbox"/> Meldergruppe
Fernbedienung - Jeder Benutzer	<input type="checkbox"/> Systemausgang
Bedienteil-PIN - Benutzer 1 [Daniel]	<input type="checkbox"/> Bereichsausgang
	<input type="checkbox"/> Fernbedienung
	<input type="checkbox"/> Bedienteil-PIN
	<input type="checkbox"/> Tür
	<input type="checkbox"/> Log. Ausgang
	<input type="checkbox"/> Schlüsselschalter
	<input type="checkbox"/> Anzeigemodul

- Klicken Sie auf die Schaltfläche **Neuen Trigger hinzufügen**, um einen neuen Trigger für den Bereich hinzuzufügen.

## Triggerkonfiguration

konfigurierte Bedienungen des Triggers

Trigger-ID : 1

Triggerbeschreibung :

Aktivierungszeit :  Anzahl der Sekunden, die der Trigger ausgelöst sein muss.

Limit Zeit :  10:28 bis  11:23

Kalender :

**Hinweis:** Der Trigger wird nur aktiviert, wenn alle Bedingungen zur gleichen Zeit erfüllt sind. Wenn ein Zeitlimit oder ein Kalender zugewiesen wird, wird die Aktivierung des Triggers weiter eingeschränkt, da er nur aktiviert wird, wenn alle Bedingungen innerhalb der Kalenderschaltzeit/Zeitlimit erfüllt sind.

Zugewiesene Triggerbedingungen	Triggerbedingungen
Jede WPA [Funktion=Rot]	<input type="checkbox"/> Meldergruppe
Meldergruppe 1 [Front door] - Offen	<input type="checkbox"/> Systemausgang
	<input type="checkbox"/> Bereichsausgang
	<input type="checkbox"/> Fernbedienung
	<input type="checkbox"/> Bedienteil-PIN
	<input type="checkbox"/> Tür
	<input type="checkbox"/> Log. Ausgang
	<input type="checkbox"/> Schlüsselschalter
	<input type="checkbox"/> Anzeigemodul
	<input type="checkbox"/> WPA Funktion
	<input checked="" type="checkbox"/> Notruf Funk Fernbed.
	<input type="checkbox"/> Zeit

3. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

Trigger-ID	Das System hat eine Nummer für einen neuen Trigger erstellt. Trigger werden nur aktiv, wenn einer der beiden optionalen Schritte (Kalender-/Zeitbeschränkung) konfiguriert ist.
Triggerbeschreibung	Geben Sie eine Textbeschreibung für den Trigger ein.
Kalender	Wählen Sie bei Bedarf einen Kalender aus. Nach der Auswahl wird der Trigger nur während des ausgewählten Kalenderzeitraums aktiviert sein. Siehe Seite [→ 209].
Aktivierungszeit/Time r	Geben Sie die Zeit in Sekunden ein, für welche die Trigger-Bedingung erfüllt sein muss, damit der Trigger aktiviert wird.
Limit Zeit	Wählen Sie für die Aktivierung des Triggers einen Zeitraum zwischen 00:00 und 24:00. Die Startzeit ist eingeschlossen, die Endzeit ist nicht eingeschlossen. <b>Hinweis:</b> Dieser Parameter verzögert nur den Trigger-Übergang von AN nach AUS, der Übergang von AUS nach AN ist verzögerungsfrei.
Trigger-Bedingungen	Der Trigger ist AN, wenn folgende Bedingungen erfüllt sind (d. h. eine logische

	<p>UND-Operation findet statt):</p> <p><b>MG</b> – Der Trigger wird aktiviert, wenn die konfigurierte MG einen der folgenden Stati aufweist: offen, geschlossen, kurzgeschlossen oder getrennt.</p> <p><b>Tür</b> – Der Trigger wird aktiviert, wenn eine der folgenden Türoptionen konfiguriert ist: Zutritt gewährt, Zutritt verweigert, Austritt gewährt, Austritt verweigert, Tür zu lange offen, Tür offen gelassen, Tür aufgebrochen, Tür normal, Tür gesperrt, Tür freigegeben.</p> <p><b>System</b> – Der Trigger wird aktiviert, wenn der Systemausgang den konfigurierten Status aufweist (AN oder AUS). Mögliche Systemausgänge sind „Außensirene“, „Alarm“ usw.</p> <p><b>Bereich</b> - Der Trigger wird aktiviert, wenn der Bereichsausgang ein- oder ausgeschaltet ist. Mögliche Bereichsausgänge sind „Außensirene“, „Alarm“ usw.</p> <p><b>Funkfernbedienung</b> – Diese Bedingung kann für einen bestimmten Benutzer oder für alle Benutzer konfiguriert werden. Drückt der konfigurierte Benutzer (bzw. ein beliebiger Benutzer) bei dieser Konfiguration die „*-Taste an der Fernbedienung, führt dies zu einem unmittelbaren AUS/AN/AUS-Puls. Dies gilt nur für Fernbedienungen, die im System eingelernt wurden.</p> <p><b>Funkfernbedienung Überfall</b> – Diese Bedingung kann für einen bestimmten Benutzer oder für alle Benutzer konfiguriert werden. Drückt der konfigurierte Benutzer (bzw. ein beliebiger Benutzer) bei dieser Konfiguration die „*-Taste auf der Panik-Fernbedienung, führt dies zu einem unmittelbaren AUS/AN/AUS-Puls. Dies gilt nur für Situationen „Fernbedienung-Überfall“, die im System eingelernt wurden.</p> <p><b>Funküberfalltaster</b> – Der Trigger wird aktiviert, wenn eine Taste oder Tastenkombination gedrückt wird. Es ist möglich, eine Triggerbedingung allen FÜ oder nur einem bestimmten FÜ zuzuweisen. Wenn ein Trigger mit einer FÜ-Triggerbedingung definiert wird, kann er einem logischen Ausgang für verschiedene Zwecke (Scharfschalten eines Systems, Einschalten von Leuchten oder Öffnen einer Tür) zugewiesen werden.</p> <p><b>Bedienteil gültiger PIN</b> – Diese Bedingung kann für einen bestimmten Benutzer oder für alle Benutzer konfiguriert werden. Gibt der konfigurierte Benutzer (bzw. ein beliebiger Benutzer) bei dieser Konfiguration eine gültige PIN ein oder hält einen konfigurierten Transponder vor, führt dies zu einem unmittelbaren AUS/AN/AUS-Puls.</p> <p><b>Schlüsselschalter</b> – Der Trigger kann für eine bestimmte Schlüsselstellung am Schlüsselschalter konfiguriert werden.</p> <p><b>Zeittrigger</b> – Der Trigger wird zu einem bestimmten Zeitpunkt aktiviert, der in das dafür vorgesehene Feld im Format hh:mm eingegeben wurde.</p>
--	--

	<p><b>⚠️ WARNUNG</b></p> <p>Das System erfüllt nicht die EN-Normen, wenn Sie einen Trigger zur Scharfschaltung des Systems ohne die Eingabe eines gültigen PINs verwenden.</p>
---	--

## 16.4 Logische Ausgänge

Trigger werden in Verbindung mit logischen Ausgängen verwendet; dabei handelt es sich um virtuelle Ausgänge, die vom Benutzer definiert werden und einem physikalischen Ausgang zugewiesen werden können. Das System unterstützt eine max. Anzahl von 512 logischen Ausgängen.



Für einen kontinuierlichen Ausgang, bei Verwendung einer gültigen Benutzer-PIN als Trigger, müssen beide Stauseinstellungen die gleichen sein – entweder beide negativ oder beide positiv.

Advanced

Logische  
Ausgänge

Für jedes aufgelistete Gerät werden die folgenden Felder angezeigt:

- Ausgang
- Bedienteil
- Beschreibung
- Timer
- Trigger

1. Klicken Sie auf einen Ausgang in der Liste.

⇒ Daraufhin erscheint das folgende Fenster:

### Trigger des log. Ausgangs - Ausgang 1

Konfiguration der AN/AUS-Trigger des log. Ausgangs

**Logischer Ausgang # :** 1  An  Aus

**Beschreibung :**

**Zugewiesen zu :** Zeige Zuweisung zu Erw.

**BT Kurzwahl :**  ▼

**Timer (x 100ms) :**  ▲ ▼ 1/10 Sekunden

**Überwacht :**

#### Trigger an

Trigger	Flanke
1 - trig1	Positiv

AN-Trigger hinzufügen
Trigger löschen

**Hinweis: Wenn alle Bedingungen EINES Triggers erfüllt sind, dann wird der logische Ausgang aktiviert...**

#### Trigger aus

Trigger	Flanke

AUS-Trigger hinzufügen
Trigger löschen

**Hinweis: Wenn alle Bedingungen EINES Triggers erfüllt sind, dann wird der logische Ausgang deaktiviert...**

✖ Löschen
Zurücksetzen
✔ OK

2. Konfigurieren Sie die in der nachstehenden Tabelle beschriebenen Felder und klicken Sie auf **OK**.

Log Ausgang #	Diese Nummer wird als Referenz angezeigt und kann nicht programmiert werden.
Beschreibung	Geben Sie einen Namen für den Ausgang ein. Dieser ist wichtig, da auf der Benutzeroberfläche <b>Ausgänge</b> zum Ein- und Ausschalten von Ausgängen keine Ausgangsnummer, sondern nur der Name angezeigt wird.
Zugewiesen zu	Klicken Sie auf die Schaltfläche <b>Assign Now (Jetzt zuweisen)</b> , um eine Übersicht darüber zu erhalten, welchem Controller-/Erweiterungsausgang der Benutzerausgang zugewiesen ist. Klicken Sie zur Erstellung einer neuen Zentralen-/Erweiterungsmodulzuweisung auf einen Ausgang in der Liste und anschließend auf die Schaltfläche <b>Ausgewählten Ausgang als log Ausgang zuweisen</b> .
BT Kurzwahl	Eine Kurzwahl besteht aus einer ‚#‘ gefolgt von einer auf dem Bedienteil gedrückten Nummerntaste. Wird am Bedienteil eine konfigurierte Kurzwahl eingegeben, wird der Benutzer aufgefordert, den Ausgang ein- oder auszuschalten.

- Klicken Sie auf die Schaltfläche **Add ON Trigger (AN-Trigger hinzufügen)**, um die Trigger zum Ein- und Ausschalten des Ausgangs zu konfigurieren. In beiden Fällen muss eine positive oder negative Seite des Triggers definiert werden. Weitere Informationen zur Konfiguration von Triggern finden Sie im Abschnitt Trigger [→ 212].

Siehe auch

 Trigger [→ 212]

## 16.5 X10 Konfiguration – Einstellungen

Im X10-Einstellungsfenster können Sie die Funktionsweise von X10 auf der Zentrale konfigurieren.

**Advanced**



X-10



1. Aktivieren Sie das Kontrollkästchen **Aktiviert**, um den X10 in der Zentrale zu aktivieren.
2. Aktivieren Sie das Kontrollkästchen **Log**, um das Protokollieren aller X10-Ereignisse in der Zentrale zu aktivieren.
3. Klicken Sie auf eine Buchstaben-Registerkarte (A-P), um X10-Gerätetrigger zu konfigurieren.

⇒ Eine Liste der konfigurierbaren Gerätetrigger (1-16) wird für den gewählten Buchstaben angezeigt:

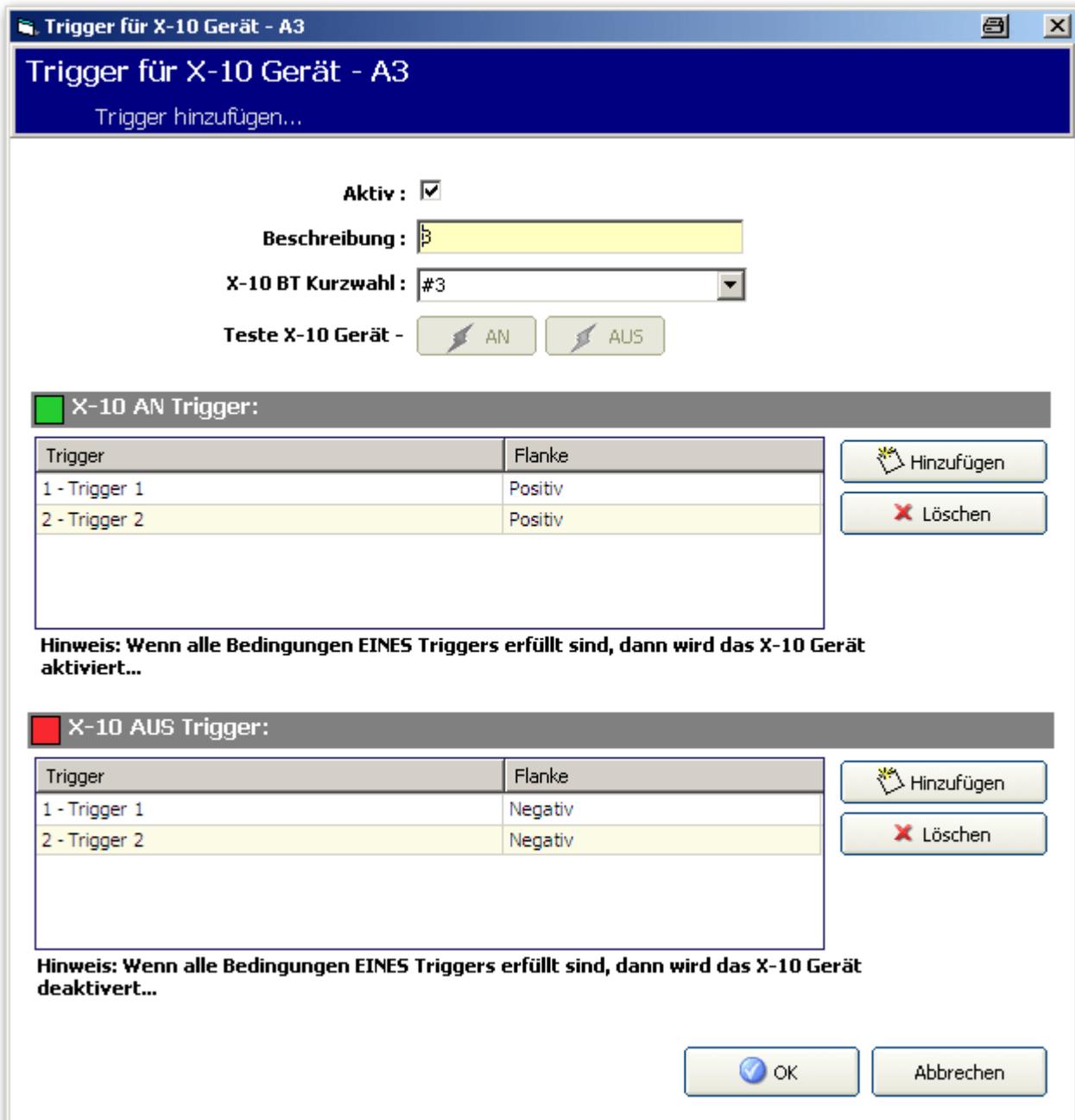
Einstellungen					
Trigger des X-10 Geräts [A]					
Gerät	Aktiv	Beschreibung	Trigger an	Trigger aus	BT Kurzwahl
1	Aktiv		3	2	#2
2	Aktiv		1	1	#1
3	Aktiv		2	2	#3
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					

Gerätenummer	Die Zahl (1-16), die dem Gerät zugewiesen wurde.
Aktiv	Dieses Feld zeigt an, ob das Gerät aktiv ist oder nicht.
Beschreibung	Dieses Feld enthält eine Beschreibung, die verwendet wird, um das Gerät einfacher zu identifizieren, z. B. „Licht unten“ (max. 16 Zeichen).
Trigger AN	Dieses Feld gibt an, ob ein Trigger programmiert wurde, um das X10-Gerät zu aktivieren (1, wenn ein Trigger programmiert ist - 2, wenn nicht).
Trigger AUS	Dieses Feld gibt an, ob ein Trigger programmiert wurde, um das X10-Gerät zu deaktivieren (1, wenn ein Trigger programmiert ist - 2, wenn nicht).
BT Kurzwahl	Dieses Feld zeigt an, ob die X10-Geräteaktivierung durch die Eingabe eines Codes auf dem Bedienteil möglich ist.

Bearbeiten eines X10-Geräts:

1. Klicken Sie auf einen Trigger in der Liste.

⇒ Daraufhin erscheint das folgende Fenster:



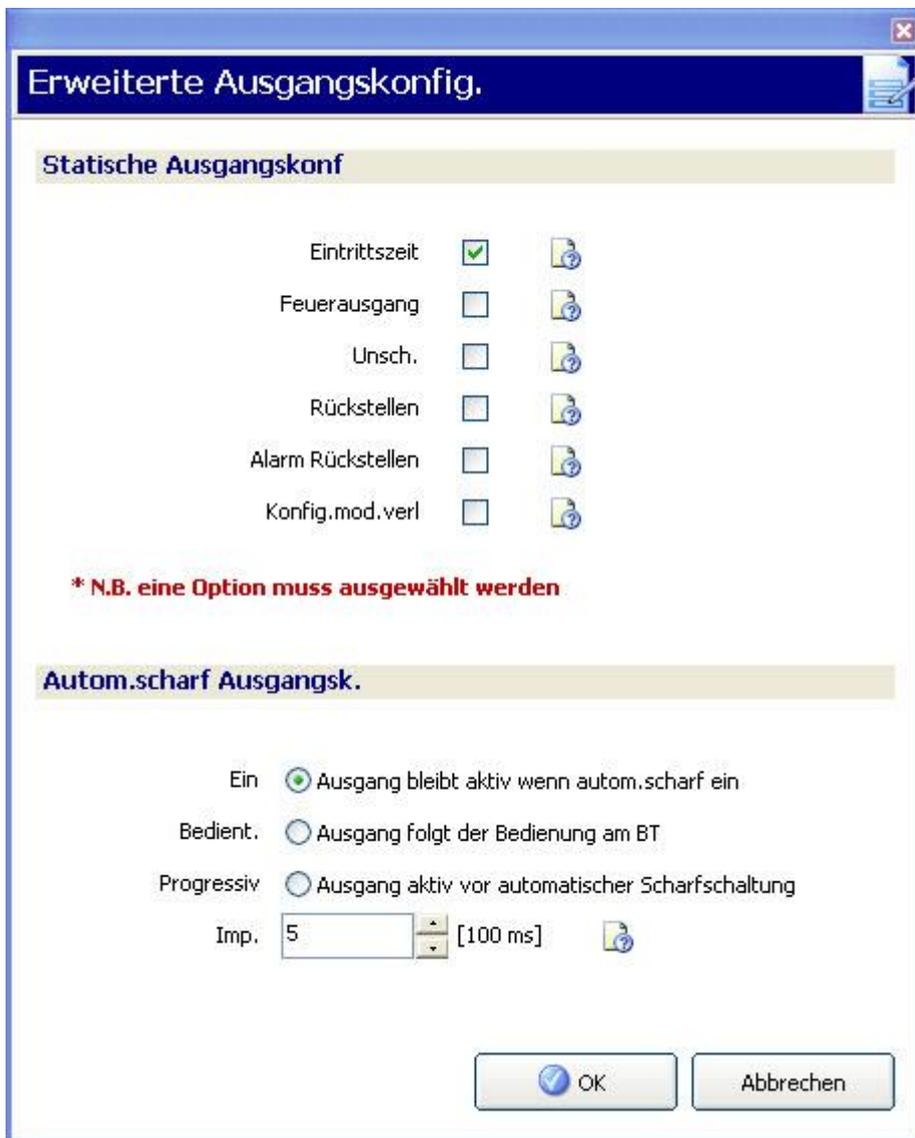
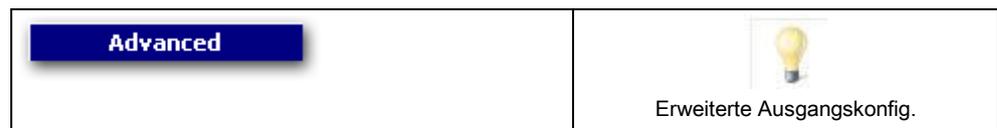
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben:
  3. Klicken Sie auf **Hinzufügen**.
  4. Klicken Sie im folgenden Fenster auf die Schaltfläche , um einen neuen Trigger zu erstellen, - ODER-  
Markieren Sie einen Trigger in der Liste und klicken Sie auf die Schaltfläche , um den gewählten Trigger zu bearbeiten.
- ⇒ Das Fenster **Triggerkonfiguration** wird geöffnet:

Aktiv	Aktivieren Sie dieses Kontrollkästchen, um X10 zu aktivieren.
Beschreibung	Geben Sie einen Text ein, um das X10-Gerät zu benennen (max. 10 Zeichen).
X10 Bedienteil	Wählen Sie eine PIN. Geben Sie diesen Code am Bedienteil ein, um das X10-

	Gerät zu aktivieren.
Testen Sie das X10-Gerät.	

Informationen zu weiteren Programmierschritten siehe Seite [→ 212].

## 16.6 Konfiguration der Ausgänge für Systemverzögerung und automatische Scharfstellung



- Wählen Sie die Bedingung für die Aktivierung des statischen Ausgangs aus:

Eintrittszeit.	Der Ausgang wird bei Ablauf der Schärfungsverzögerung aktiviert und bei Beginn der Eintrittszeit deaktiviert.
Notausgang	Der Ausgang wird aktiviert, wenn eine beliebige Feuerausgangs-MG aktiviert wird.
Unscharf	Der Ausgang wird aktiviert, wenn ein beliebiger Benutzer das System kurzzeitig unscharf schaltet.
Rückstellen	Der Ausgang wird aktiviert, wenn ein Alarm kurzzeitig rückgestellt wird.
Alarmrückstellen	Der Ausgang wird aktiviert, wenn beim Scharfschalten Glasbruchmelde- oder Brandmeldelinien offen sind, aber keine Alarm auslösen.
Techniker Austritt	Der Ausgang wird aktiviert, wenn ein Techniker kurzzeitig den Konfigurationsmodus verlässt.
Bedienteil gültiger Pin	Der Ausgang schaltet ein, wenn auf dem Bedienteil eine gültige Benutzer-PIN eingegeben wird und eine Feuer-MG aktiv ist.

- Wählen Sie das Ausgangsverhalten.

Ein	Der Ausgang bleibt aktiv, wenn die automatische Scharfschaltung aktiv ist.
Bedienteil	Der Ausgang folgt der Bedienung am Bedienteil.
Fortlaufend	Der Ausgang warnt fortlaufend vor der automatischen Scharfschaltung.
Puls Zeit	Wählen Sie die Zeitspanne aus, während der der Ausgang für automatische Scharfschaltung aktiv bleibt, wenn er gepulst wird.

## 16.7 Logo-Konfiguration



Logo-Konfiguration

Es besteht die Möglichkeit, ein individuelles Logo in die Bedienteile SPCK620/623 zu laden.

- Wählen Sie **Erweitert > Logo-Konfiguration**.
- ⇒ Der **Logo Manager** wird geöffnet.
- 1. Klicken Sie auf die Schaltfläche **Laden**.
- 2. Wählen Sie eine Datei in einem der folgenden Formate (max. Abmessungen: 18 x 45 Pixel).
  - Binäre RAW-Dateien, 1 Bit pro Pixel (\*.bin)
  - Monochromes Bitmap-Bild (\*.bmp)
  - Führen Sie eine der folgenden Schritte aus.

**HINWEIS**

Klicken Sie nach jeder Änderung, die Sie vornehmen, auf die Schaltfläche **Speichern**. Andernfalls werden Ihre Einstellungen nicht verwendet.

Vergrößern	Vergrößern des Logos von der 1-fachen auf die 4-fache Größe.
Speichern	Klicken Sie nach jeder Änderung, die Sie vornehmen, auf die Schaltfläche <b>Speichern</b> .
Schließen	Schließt den Logo-Manager.
Löschen	Löscht den Logo-Manager
Vorschau	Zeigt eine Vorschau des Logos auf dem Bedienteil.

## 16.8 Audio-Konfiguration

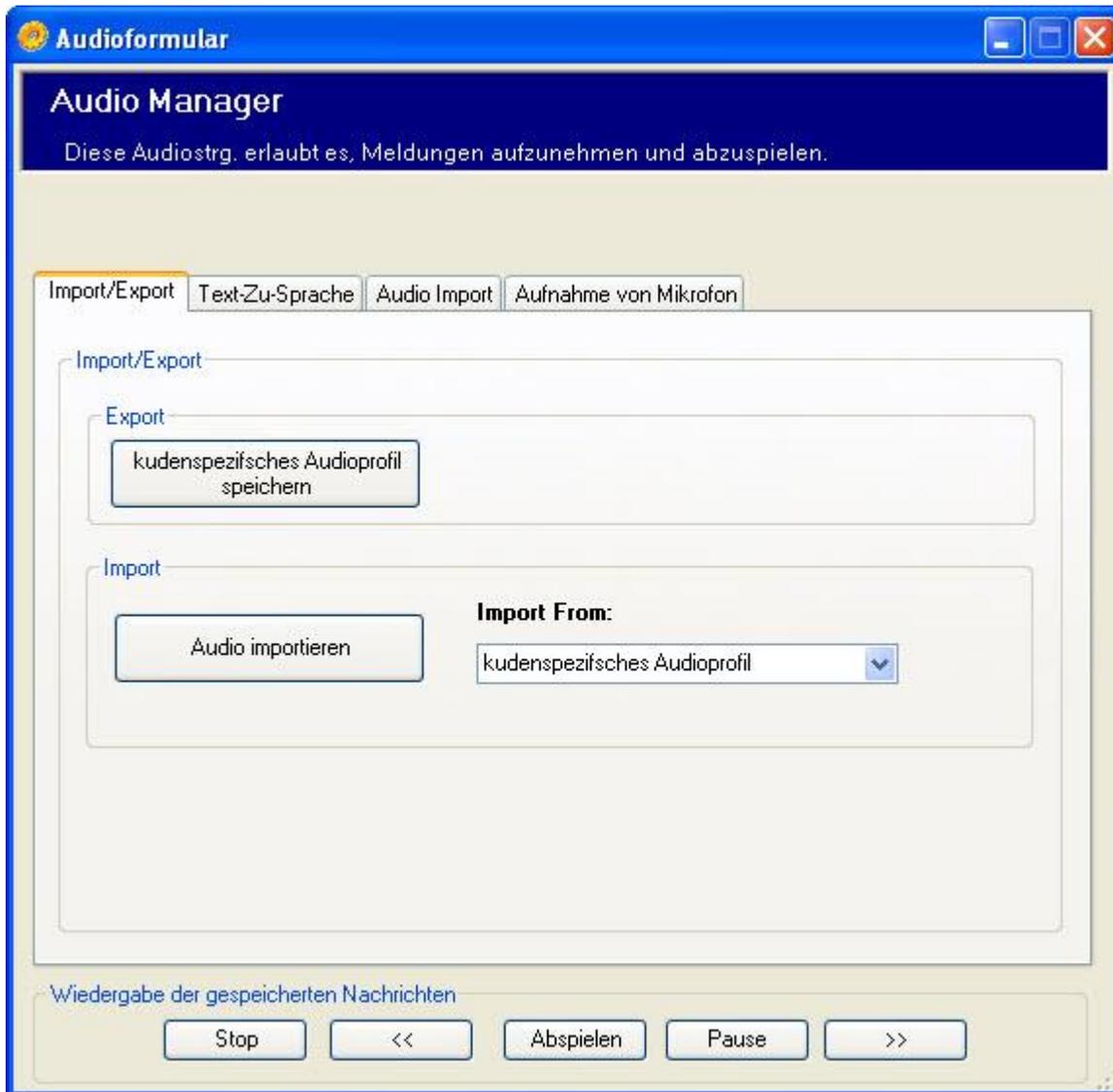
**Advanced**



Audio-Konfiguration

Mit dem Audio-Manager können Sie Sprachansagen für das Alarmsystem aufzeichnen und abspielen.

- Wählen Sie **Erweitert > Audio-Konfiguration**.
- ⇒ Der **Audio Manager** wird geöffnet.



### Allgemeine Funktionen

Die folgenden Funktionen stehen für alle Registerkarten im Audio Manager zur Verfügung.

Stopp	Das Abspielen gespeicherte Mitteilungen (Audioaufzeichnung) wird gestoppt.
<<	Die gespeicherten Mitteilungen (Audioaufzeichnungen) werden zurückgespult.
Wiedergabe	Die gespeicherten Mitteilungen (Audioaufzeichnungen) werden zurückgespult.
Pause	Die gespeicherten Mitteilungen (Audioaufzeichnungen) werden angehalten.
>>	Die gespeicherten Mitteilungen (Audioaufzeichnungen) werden vorgespult.
Audioaufzeichnung erstellen	Alle einzelnen Sprachansagen werden komprimiert und in einer herunterladbaren Datei gespeichert, die mit der SPC-Zentrale kompatibel ist. Die Sprachaufzeichnungen werden in der Datei „spc audio.bak“ im Ordner „C:\SPC Products\SPC Pro 2.0.0\Audio\Installations“ gespeichert.

### Import/Export

Benutzerspezifische	Wenn Sie das Standard-Audio-Profil ändern, können Sie es als
---------------------	--

Audio-Profil speichern	benutzerspezifisches Audio-Profil speichern. Das benutzerspezifische Audio-Profil wird standardmäßig im Ordner „C:\SPC Products\SPC Pro 2.0.0\Audio\My Audio Profiles“ gespeichert. Die Datei kann bei Bedarf jederzeit verwendet werden.
Audio importieren	Sie können das Standard-Audio-Profil oder das benutzerspezifische Audio-Profil, das Sie gespeichert haben, importieren.

## 17 Systemoptionen

1. Klicken Sie auf den Menüpunkt **Optionen > Systemoptionen**.
2. Konfigurieren Sie die folgenden Felder:

<b>Allgemein</b>	
Zeitstempel der Zentralenkonfiguration beim Verbinden überprüfen	Aktivieren Sie dieses Kontrollkästchen, um die Überprüfung des Zeit- und Datumsstempels beim Verbinden mit der Zentrale zu aktivieren. Siehe Seite [→ 23]. Diese Funktion ist standardmäßig aktiviert und dient als Sicherheit, indem sie Sie informiert, wenn es Abweichungen zwischen der Konfigurationsdatei auf dem PC und der Konfigurationsdatei in der Zentrale gibt. <b>Hinweis:</b> Wenn Sie diese Funktion deaktivieren, bemerken Sie nicht, ob es Unterschiede zwischen der Konfigurationsdatei auf Ihrem PC und der Konfigurationsdatei in der Zentrale gibt, wenn Sie sich verbinden.
Benutzerdefinierte Sprachauswahl auf unterstützen Zentralen zulassen	Aktivieren Sie dieses Kontrollkästchen, um hochgeladene benutzerdefinierte Sprachen zu verwenden. Siehe Hochladen von benutzerdefinierten Sprachen.
<b>Modemkonfiguration</b> Wenn Sie sich per Modem mit der Zentrale verbinden wollen, müssen Sie mitunter einige Initialisierungsparameter konfigurieren:	
Amtsholung	1. Geben Sie den Initialisierungsbefehl für das Modem ein.
Wählpause	1. Geben Sie den Zeitraum in Sekunden ein, wie lange das Modem warten soll, bevor es die Zentrale anruft (max. 60 Sek.).

## 18 Upgrade der Zentrale



### HINWEIS

Für das Upgrade der Firmware ist ein Herstellerzugang erforderlich. Ist die Option aktiviert, kann sowohl ein Upgrade der Controller-Firmware als auch der Firmware der Peripheriegeräte durchgeführt werden. Siehe Systemoptionen [→ 71].

### 18.1 Upgrade Zentralen-Firmware

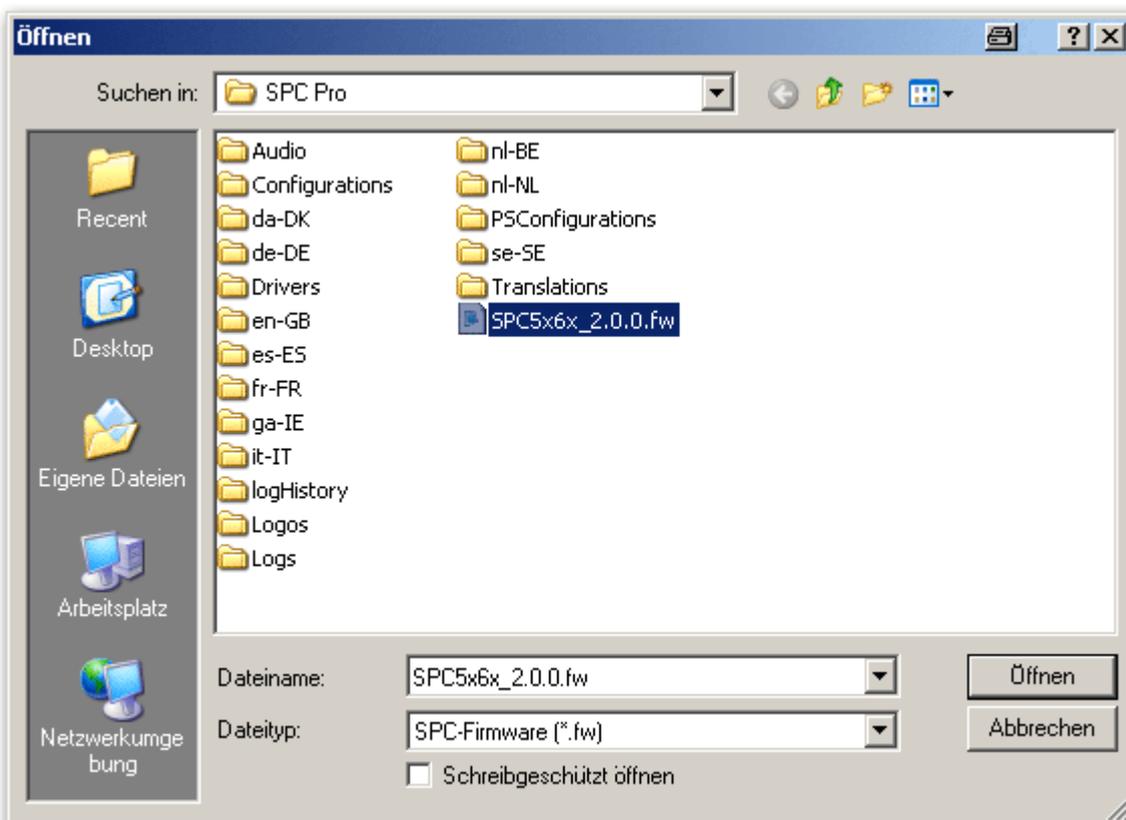
#### Voraussetzung:

- SPC Pro befindet sich im Konfigurationsmodus.
- Die korrekte Zentralen-Firmware-Datei (.fw) wurde in einem Verzeichnis auf Ihrer Festplatte gefunden.

Die Firmware der SPC-Zentrale upgraden

1. Klicken Sie auf das Menü **Erweitert**.
2. Wählen Sie **Firmware Upgrade (nur im Konfigurationsmodus)**.

⇒ Daraufhin erscheint das folgende Fenster:



3. Wählen Sie die erforderliche Firmware-Datei.
4. Klicken Sie auf **Öffnen**.

5. Überprüfen Sie die Werte der Felder.

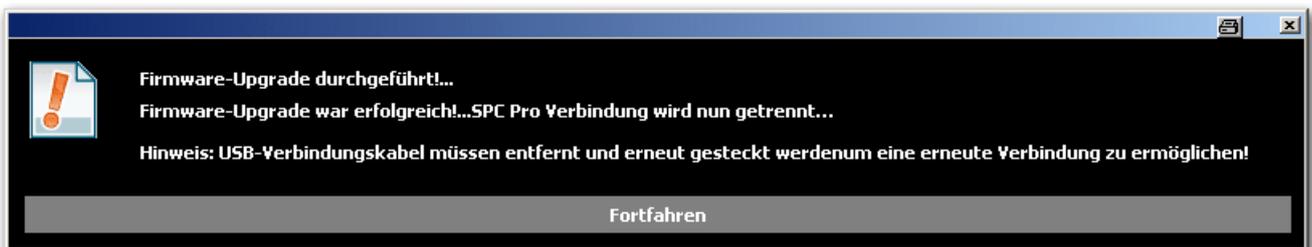
	<b>HINWEIS</b>
	Wenn der Upgrade-Vorgang einmal gestartet wurde, kann er nicht mehr abgebrochen werden. Es empfiehlt sich, die Firmware-Version vor dem Upgrade zweimal zu überprüfen.

6. Klicken Sie auf **Upgrade durchführen**.



Nachdem die Firmware gesendet wurde, wird die Zentrale neu gestartet. Die Verbindung zur Zentrale wird getrennt. Sie müssen sich nach dem Neustart erneut mit der Zentrale verbinden.

Wenn der Upgrade-Vorgang abgeschlossen ist, erscheint folgendes Fenster:



1. Klicken Sie auf **Fortfahren**, um die Verbindung zur Zentrale zu trennen.
  2. Stellen Sie die Verbindung wieder her, wenn die Firmware der Zentrale neu gestartet wurde (dies nimmt etwa 40 Sekunden in Anspruch).
- ⇒ Das Firmware-Upgrade ist abgeschlossen.

	<b>⚠️ WARNUNG</b>
	Wenn Sie die Zentralen-Firmware downgraden (d. h. eine ältere Version der Firmware installieren), behält das System standardmäßig alle aktuellen Konfigurationseinstellungen bei.

**WARNUNG!**

## 18.2 Upgrade der Peripherie-Firmware

**Voraussetzung:**

- Pro befindet sich im Konfigurationsmodus.
- Die korrekte Peripherie-Firmware-Datei (.pfw) wurde in einem Verzeichnis auf Ihrer Festplatte gefunden.

Upgrade der Firmware auf Peripheriegeräten:

1. Klicken Sie auf das Menü **Erweitert**.
2. Wählen Sie **Upgrade Peripherie-Firmware**.
  - ⇒ Daraufhin erscheint das folgende Fenster:

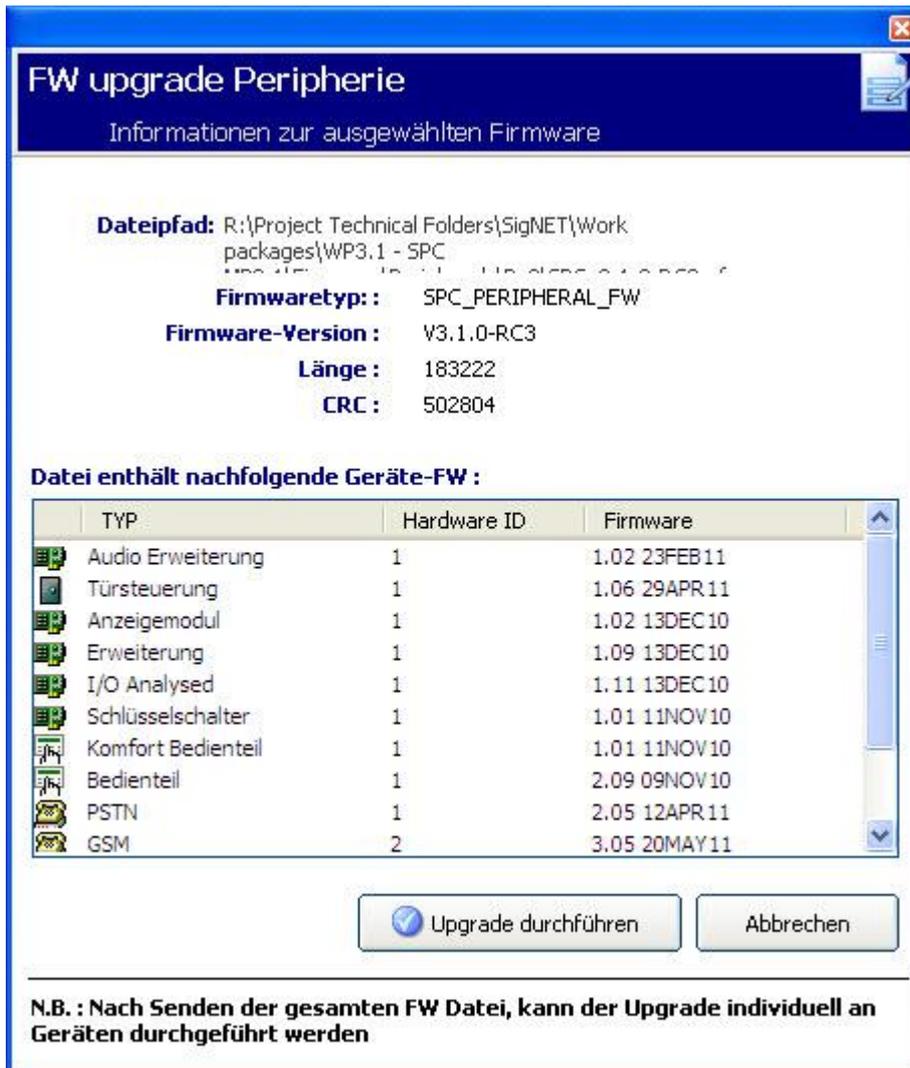
**System Geräte - Firmware Upgrade**  
Liste der vorh.EBUS und Modem Geräte an System...

**Liste der Systemgeräte :**

ID	TYP	S/N	Beschreibung	Hardware ID	Geräte Firmware	Verfügbare Firmware	Upgrade
3	Schlüsselschalter [1 Ausgang]	180426801		1	1.01 11NOV10	--	
4	Anzeigemodul [1 Eingang]	180373801		1	1.02 13DEC10	--	
7	Erweiterung [8 Eingang / 2 ...]	101647801		1	1.09 13DEC10	--	
8	Erweiterung	487907		1	1.09 13DEC10	--	
9	Erweiterung [8 Ausgang]	1101173801		1	1.09 13DEC10	--	
10	Audio Erweiterung [4 Einga...	1000802085		1	1.02 23FEB11	--	
11	Erweiterung [8 Ausgang]	101788801		1	1.09 13DEC10	--	
1	Bedienteil	191640801		1	2.09 09NOV10	--	
2	Komfort Bedienteil	183484801		1	1.01 11NOV10	--	
6	Türsteuerung [4 Eingang / ...]	5		1	1.06 29APR11	--	

Diese Option ermöglicht den Upgrade der X-Bus Gerätefirmware Zuerst muss die aktuelle Firmware Datei an die Zentrale gesendet werden danach können die Geräte für den Upgrade ausgewählt werden

- Klicken Sie auf **Sende neue FW Datei für Peripherie an Zentrale**.  
⇒ Daraufhin erscheint das folgende Fenster:



1. Klicken Sie auf **Upgrade durchführen**, um die Peripherie-Firmware-Datei an die Zentrale zu senden.
  - ⇒ Falls die .pfw-Dateiversion von der Controller-Version abweicht, wird eine Warnmeldung angezeigt.
 

Die Zentrale überprüft auch, ob die in der Peripheriegeräte-Datei enthaltene Firmware die jeweiligen Hardware-Versionen der installierten Peripheriegeräte unterstützt und lässt kein Upgrade für Geräte zu, die nicht unterstützt werden.
2. Die Peripherie-Firmware wird nur temporär im Dateisystem gespeichert. Wird eine neue Peripherie-Firmware hochgeladen, werden die aktuellen und neuen Versionen der Firmware für jedes Peripheriegerät und jedes Modem wie folgt angezeigt.
  - ⇒ Falls die Hauptversionsnummer der für ein Gerät verfügbaren Firmware von der Hauptversionsnummer der vorhandenen Firmware eines Geräts abweicht, wird ebenfalls eine Warnmeldung angezeigt.

**System Geräte - Firmware Upgrade**

Liste der vorh.EBUS und Modem Geräte an System...

**Liste der Systemgeräte :**

ID	TYP	S/N	Beschreibung	Hardware ID	Geräte Firmware	Verfügbare Firmware	Upgrade
3	Schlüsselschalter [1 Ausgang]	180426801		1	1.01 11NOV10	1.01 11NOV10	
4	Anzeigemodul [1 Eingang]	180373801		1	1.02 13DEC10	1.02 13DEC10	
7	Erweiterung [8 Eingang / 2 ...]	101647801		1	1.09 13DEC10	1.09 13DEC10	
8	Erweiterung	487907		1	1.09 13DEC10	1.09 13DEC10	
9	Erweiterung [8 Ausgang]	1101173801		1	1.09 13DEC10	1.09 13DEC10	
10	Audio Erweiterung [4 Einga...	1000802085		1	1.02 23FEB11	1.02 23FEB11	
11	Erweiterung [8 Ausgang]	101788801		1	1.09 13DEC10	1.09 13DEC10	
1	Bedienteil	191640801		1	2.09 09NOV10	2.09 09NOV10	
2	Komfort Bedienteil	183484801		1	1.01 11NOV10	1.01 11NOV10	
6	Türsteuerung [4 Eingang / ...]	5		1	1.06 29APR11	1.06 29APR11	

1. Wählen Sie nach dem Hochladen der Datei die Geräte aus, die ein Upgrade erhalten sollen, und klicken Sie auf **Upgrade ausgewählter Geräte**.

Falls die Firmware für ein Peripheriegerät in der .pfw-Datei älter ist als die auf dem Gerät vorhandene Firmware, wird die Schaltfläche **Downgrade des ausgewählten Geräts** angezeigt.

2. Wenn das Upgrade für das Gerät erfolgreich durchgeführt wurde, wechselt der Upgrade-Status zu „Bestanden“.

Das Upgrade der Peripheriegeräte-Firmware kann auch über den Browser oder den Fast Programmer erfolgen.

## 18.3 Aktualisieren der SPC-Lizenzen

Die Funktion **Lizenzoptionen** bietet einen Mechanismus, mit dem der Benutzer eine Funktion im SPC-System aktualisieren oder hinzufügen kann, wie z.B. für Migrationen, bei denen Peripheriegeräte, die nicht für SPC lizenziert sind, von einer SPC-Zentrale unterstützt werden sollen.

1. Stellen Sie online eine Verbindung mit der Zentrale her.
2. Klicken Sie auf das Menü **Erweitert**.
3. Wählen Sie die Option **Lizenzierungszentrale (nur im Konfigurationsmodus)**.

⇒ Das folgende Dialogfeld wird angezeigt:

4. Wenden Sie sich mit der gewünschten Funktion an den technischen Support und geben Sie den angezeigten Lizenzschlüssel an.

⇒ Bei Genehmigung Ihrer Anfrage wird ein neuer Lizenzschlüssel ausgestellt.

5. Geben Sie den neuen Schlüssel in das dafür vorgesehene Feld ein und klicken Sie auf die Schaltfläche **Schlüssel an Zentrale senden**.
  - ⇒ Bei erfolgreicher Änderung des Lizenzschlüssels wird das folgende Dialogfeld angezeigt:



## 18.4 Import benutzerdefinierter Sprachen für die SPC Pro-Bedienoberfläche

Sie können eine benutzerdefinierte Sprache für die SPC Pro-Bedienoberfläche importieren, die von der benutzerdefinierten Sprache völlig unabhängig ist, die auf der Zentrale für den Browser und die Bedienteile installiert ist. Sie können eine bestimmte Sprache für die Konfiguration mit SPC Pro und eine andere Sprache für die Zentrale.

Um die SPC Pro-Benutzersprache zu importieren:

1. Klicken Sie auf das Menü **Datei** in SPC Pro.
2. Wählen Sie im **Datei**-Menü die Option **SPC Pro-Sprachdatei importieren**.

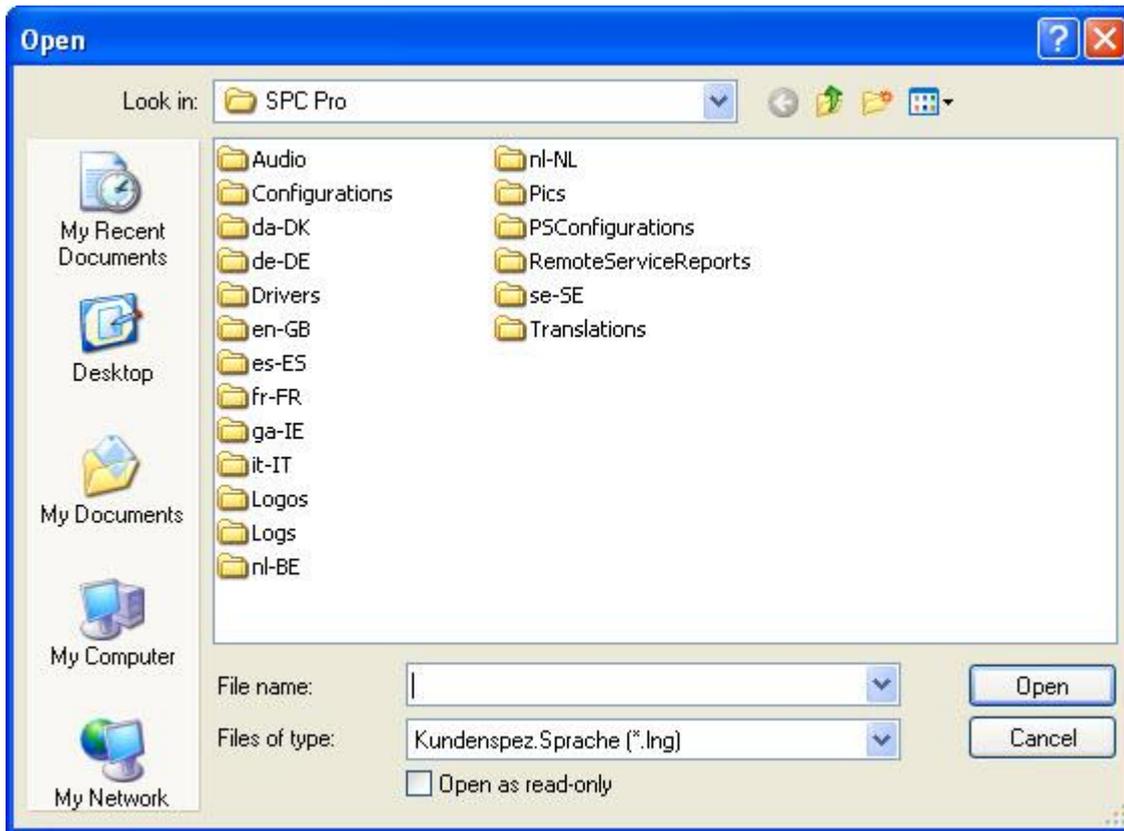


- Wählen Sie im Standort-Dialogfenster die gewünschte Sprachdatei aus und klicken Sie auf **Öffnen**.



### **HINWEIS**

SPC Pro-Sprachdateien haben die Dateierweiterung \*.msg.



Um die neue benutzerdefinierte Sprache zu verwenden:

1. Schließen Sie SPC Pro.
2. Rufen Sie die SPC Pro-Anwendung wieder auf.
3. Klicken Sie auf dem Anmeldebildschirm auf das Erdkugel-Symbol, das die die Benutzersprache anzeigt.

Anmelden

Passwort:

 Anmelden

© 2011, Siemens AG



Diese Sprache wird dann immer für die SPC Pro-Konfiguration verwendet, bis sie wieder ausdrücklich geändert wird.

## 19 Bedienteil-Emulation aktivieren

SPC Pro stellt Ihnen die Möglichkeit zur Verfügung, ein Bedienteil zu emulieren, wenn Sie mit der Zentrale verbunden sind.



Die Bedienteil-Emulation stellt ein virtuelles Bedienteil zur Verfügung, über das mithilfe der Standard-Bedienteiloberfläche auf Programmier- und Statusinformationen zugegriffen werden kann. Es ist nicht direkt mit einem physischen Bedienteil im System verknüpft und hat daher auch nicht die Attribute eines physischen Bedienteils.



- Klicken Sie auf das Symbol  in der Symbolleiste.
  - ⇒ Das Bedienteil wird am Bildschirm angezeigt und stellt Ihnen folgende Funktionalität zur Verfügung.

### Systeminformationen

Das Display des Bedienteils wird in Echtzeit aktualisiert, um immer genau die Informationen anzuzeigen, die auf einem echten Bedienteil angezeigt werden, das mit der Zentrale verbunden ist (d. h. Zeit, Datum, von der Zentrale erkannte Alarme usw.).

### Zugang zur Programmierung

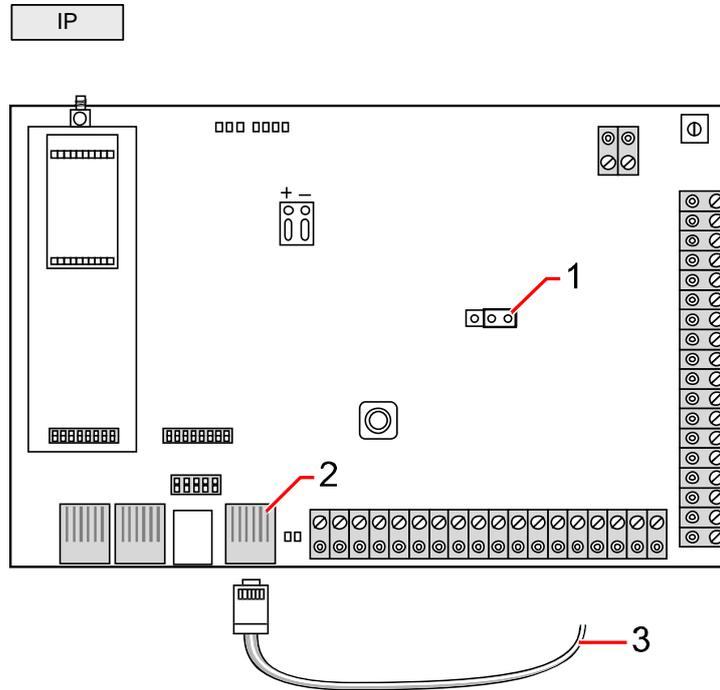
- Geben Sie die Techniker-PIN ein, indem Sie auf die Zifferntasten klicken. (Weitere Informationen zu Techniker-PINS finden Sie im Installations- und Konfigurationshandbuch.)
  - ⇒ Das Display wird bei Eingabe der Ziffern jeweils aktualisiert.
  - ⇒ Alle Programmieroptionen des Bedienteils werden wie im Installations- und Konfigurationshandbuch der betreffenden SPC beschrieben angezeigt.



1	Statusinformationen der Zentrale in Echtzeit
2	Klicken Sie auf die Schaltflächen, um die Programmiercodes einzugeben.
3	Klicken Sie, um die Bedienteil-Emulation zu verlassen.
4	Klicken Sie auf die Navigationsschaltflächen, um sich durch die Programmiermenüs zu bewegen.

## 20 Mit der Zentrale verbinden

### 20.1 Ethernet-Schnittstelle



Verbinden

1	JP9 <del>SPC4xxx</del>
2	Ethernet-Port
3	Zum Ethernet-Port am PC



Wird die SPC Ethernet-Schnittstelle an ein vorhandenes **Local Area Network** (LAN) angeschlossen, setzen Sie sich bitte mit dem Netzwerkadministrator des LANs in Verbindung, bevor Sie die Verbindung zur Zentrale herstellen. Standard-IP-Adresse: 192.168.1.100

#### Kabel anschließen

- Verbinden Sie die Ethernet-Schnittstelle am PC über ein Ethernet-Kabel mit dem Ethernet-Port an der Controller-Platine  
– ODER –  
Bei einer Direktverbindung von einem PC muss ein Kreuzkabel verwendet werden. Siehe Seite [→ 271].  
⇒ Die LEDs rechts von der Ethernet-Schnittstelle zeigen die erfolgreiche Herstellung einer Datenverbindung (rechte LED leuchtet) und Ethernet-Datenverkehr (linke LED blinkt) an.

#### IP-Adresse des SPC-Controllers bestimmen

1. Technikermodus aufrufen (siehe Techniker-PINs).

2. Blättern Sie mit den Pfeiltasten nach oben/unten zur Option KOMMUNIKATION und drücken Sie auf AUSWAHL.
3. Blättern Sie zu ETHERNET PORT und drücken Sie auf AUSWAHL.
4. Blättern Sie zu IP ADRESSE und drücken Sie auf AUSWAHL.

### SPC Pro

1. Starten Sie SPC Pro.
2. Wählen Sie eine Installation aus.
3. Klicken Sie auf die Schaltfläche **Konfigurieren**.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Mit Zentrale verbinden**.  
⇒ Daraufhin erscheint das folgende Fenster:



5. Wählen sie die Option **IP-Verbindung** .  
⇒ Die IP-Adresse wird angezeigt.
6. Falls die IP-Adresse geändert werden muss: Installationsdaten bearbeiten und die korrekte IP-Adresse im Feld IP-Adresse eingeben. Siehe Seite.
7. Klicken Sie auf **Verbinden**.  
⇒ Die Verbindung ist hergestellt.

## 20.2 USB-Anschluss

Der USB-Anschluss der SPC-Zentrale kann mit einem Standard-USB-Kabel, Typ A zu Typ B, an einen PC angeschlossen werden.

Eine USB-Verbindung von der SPC-Zentrale zum PC herstellen:

1. Kopieren Sie die Batch-Datei SPC\_USB.bat auf Ihren PC.
2. Führen Sie die Datei aus.
3. Schließen Sie das USB Kabel von der SPC-Zentrale an den USB-Anschluss Ihres PC an.

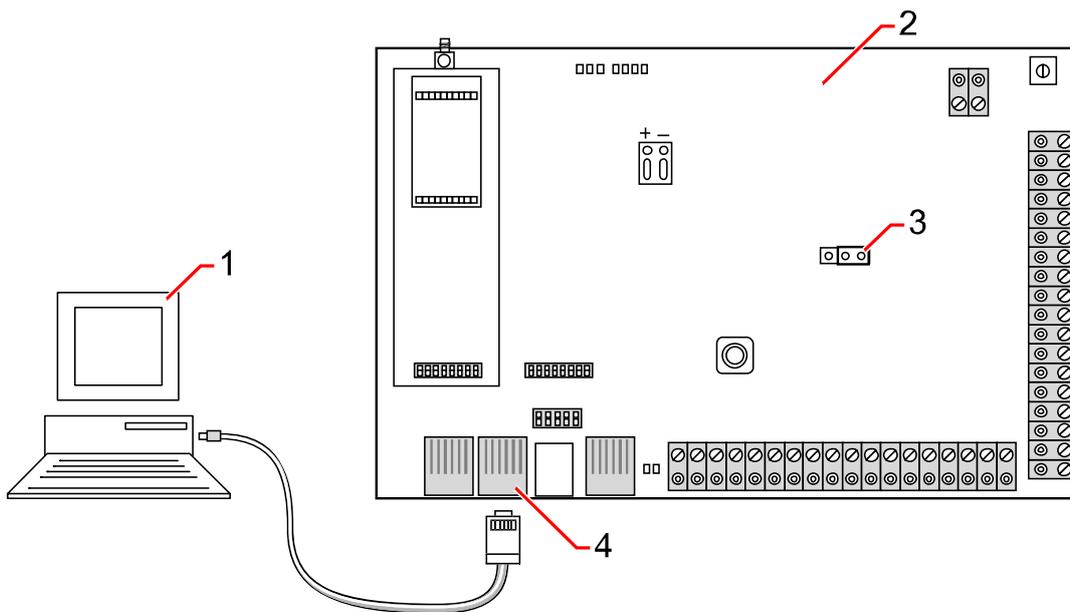
4. Starten Sie das Programm SPC Pro.
5. Wählen Sie eine Installation.
6. Klicken Sie auf die Schaltfläche **Konfigurieren**.
7. Klicken Sie in der Symbolleiste auf die Schaltfläche **Mit Zentrale verbinden**.  
⇒ Daraufhin erscheint das folgende Fenster:



8. Wählen Sie die Option **Direkt-USB**.
9. Stellen Sie sicher, dass im Dropdown-Menü der korrekte serielle Port für die Netzwerkverbindung gewählt ist.
10. Klicken Sie auf **Verbinden**.  
⇒ Die Verbindung ist hergestellt.

## 20.3 Serielle Schnittstelle

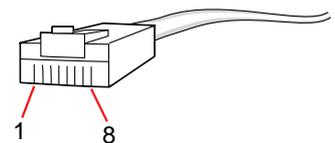
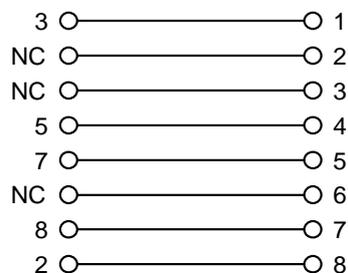
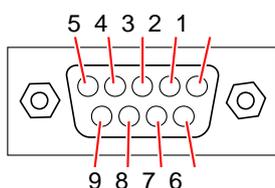
Der serielle Anschluss (RS232) der SPC-Zentrale kann verwendet werden, um Zugang zu SPC Pro zu erhalten. Hierzu muss das unten aufgeführte serielle Kabel verwendet werden, und das System muss entsprechend konfiguriert werden. Wenn das serielle Kabel angeschlossen ist und der serielle Anschluss entsprechend konfiguriert wurde, können Sie eine Direktverbindung von der Zentrale zu SPC Pro herstellen.



1	PC mit seriellem Anschluss, auf dem Hyperterminal läuft
2	SPC-Zentrale
3	JP9 
4	RS232

Eine serielle Verbindung von der SPC-Zentrale zum PC herstellen:

1. Verbinden Sie den seriellen Anschluss DB9 am PC mit der Rj45-Schnittstelle an der SPC, die die Beschriftung RS232 trägt.
2. Verwenden Sie folgende Kabelkonfiguration:



Der serielle Port 2 teilt sich einen Kommunikationskanal mit dem Backup-Modem. Wenn ein Backup-Modem installiert ist, muss es entfernt werden, damit die serielle Kommunikation über diese Schnittstelle möglich ist. Der serielle Port 2 ist auch als Klemmenblock verfügbar (TX, RX, GND).

Konfigurieren des seriellen Anschlusses über das Bedienteil

1. Rufen Sie über ein an die SPC-Zentrale angeschlossenes Bedienteil den Programmiermodus auf.
2. Gehen Sie in den Konfigurationsmodus.
3. Wählen Sie KOMMUNIKATION.
4. Gehen Sie zu SERIELLE ANSCHLÜSSE und drücken Sie auf Auswahl.
5. Wählen Sie den seriellen Anschluss, den Sie verbinden wollen (Anschluss 1 oder 2).

6. Wählen Sie im Menü TYP die Option DRUCKER, um das Logbuch der SPC aufzurufen, oder TERMINAL, um Systeminformationen aufzurufen.
7. Wählen Sie im Menü BAUDRATE 115200.
8. Wählen Sie im Menü DATENBITS 8 DATENBITS.
9. Wählen Sie im Menü STOPBITS 1 STOPBIT.
10. Wählen Sie im Menü PARITÄT die Option KEINE PARITÄT.
11. Wählen Sie im Menü FLUSSTEUERUNG die Option RTS/CTS-STEUERUNG.

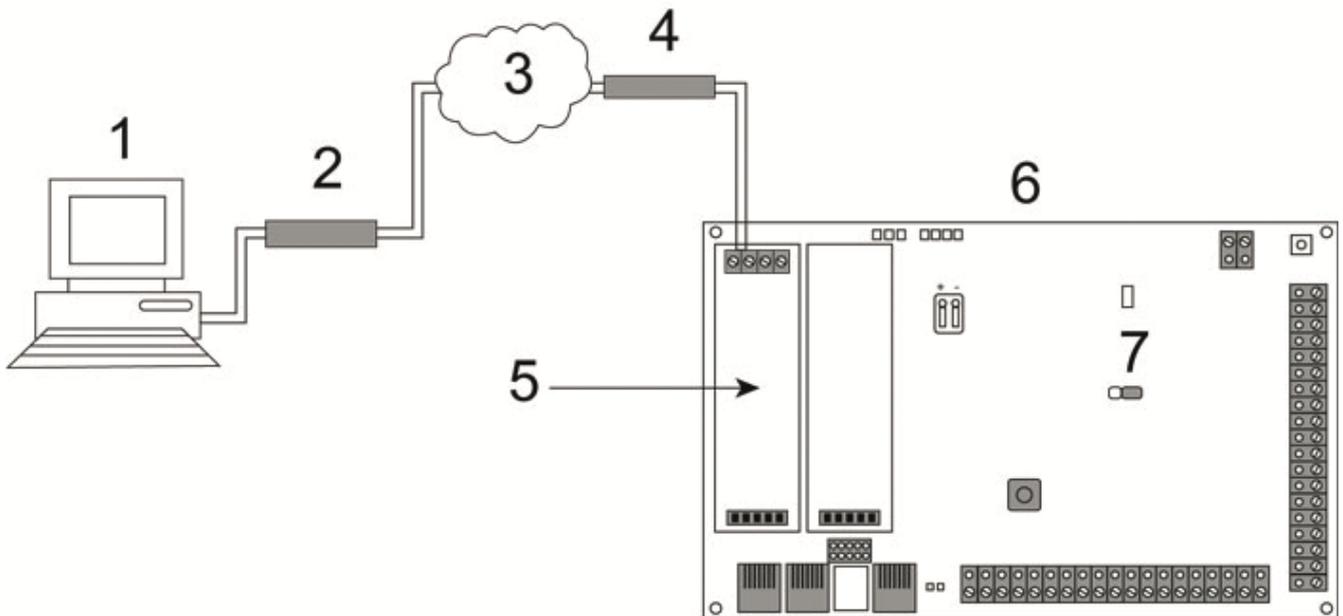
Konfigurieren des seriellen Anschlusses über SPC Pro

1. Starten Sie SPC Pro.
2. Wählen Sie eine Installation.
3. Klicken Sie auf die Schaltfläche **Konfigurieren**.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Mit Zentrale verbinden**.  
⇒ Daraufhin erscheint das folgende Fenster:



5. Wählen Sie die Option **Direkt-seriell (RS232)**.  
⇒ Es es wird das Com-Port-Menü angezeigt, in dem die auf Ihrem PC konfigurierten COM-Ports aufgeführt sind.
6. Wählen Sie den COM-Port, an den das serielle Kabel angeschlossen ist.
7. Klicken Sie auf **Verbinden**.  
⇒ Die Verbindung ist hergestellt.

## 20.4 PSTN-Modem



PSTN-Verbindung

1	Remote-PC mit Browser
2	PSTN-Modem
3	PSTN-Netz
4	Telefonleitung
5	PSTN-Modem
6	SPC-Controller
7	JP9 

Auf die SPC-Zentrale kann per Fernverbindung über eine Telefonleitung zugegriffen werden.

Voraussetzungen:

- An die Zentrale muss eine Telefonleitung angeschlossen sein.
- Auf der entfernten Seite der Verbindung benötigt der Benutzer ein PSTN-Modem auf einem PC mit Zugang zu einer PSTN-Leitung.

### Das Modem in der SPC über das Bedienteil konfigurieren

▷ In der Zentrale ist ein Wählmodem installiert. Weitere Einzelheiten finden Sie im Installations- und Konfigurationshandbuch der SPC.

1. Schließen Sie die Telefonleitung an die Schraubklemmen A und B am Anschluss auf der Oberseite des Modems an.
2. Rufen Sie den Konfigurationsmodus auf.
3. Blättern Sie zu KOMMUNIKATION und drücken Sie auf AUSWAHL.
4. Blättern Sie zu MODEMS und drücken Sie AUSWAHL.
5. Wählen Sie PRIMÄR oder BACKUP und drücken Sie AUSWAHL.

⇒ Parameter und sonstige Details, falls vorhanden, werden wie in der folgenden Tabelle dargestellt zum Bearbeiten angezeigt.

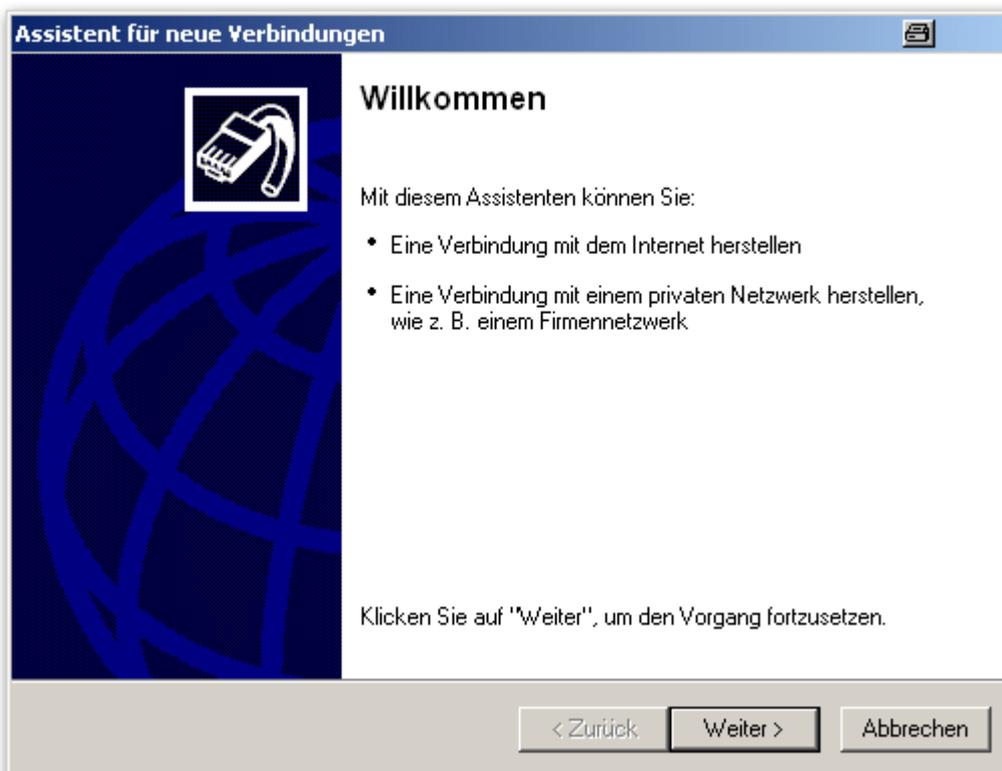
- Herstellen einer Wählverbindung auf dem entfernten PC unter Verwendung der Rufnummer der Leitung, die an das Wählmodem in der SPC angeschlossen ist.

Modem aktiv	Stellen Sie <b>Modem aktiv</b> ein.
Typ	Zeigt den Modemtyp an (Wählmodem, PSTN).
Ländercode	Wählen Sie die betreffende Ländervorwahl aus (Irland, UK, Spanien usw.).
Anrufannahme	Wählen Sie die Anzahl von Ruftönen. Hiermit geben Sie an, das Modem ein bestimmte Anzahl von Ruftönen abwarten soll, bevor es einen eingehenden Ruf annimmt.
Modem Rings	Die Anzahl von Ruftönen, die möglich sind, bevor ein eingehender Ruf angenommen wird (max. 8 Ruftöne).

### Unter Windows XP

- Gehen Sie zu **Systemsteuerung > Netzwerkverbindungen > Neue Verbindung erstellen**.

⇒ Daraufhin erscheint das folgende Fenster:



- Wählen Sie im Fenster **Netzwerkverbindungstyp** die Option „Mit dem Internet verbinden“.
- Wählen Sie im Fenster **Vorbereitung** die Option „Verbindung manuell einrichten“.
- Wählen Sie im Fenster **Internetverbindung** die Option „Über Wählmodem verbinden“.
- Geben Sie im Fenster **Verbindungsname** den Verbindungsnamen ein, z. B. „SPC-Fernverbindung“.
- Geben Sie im Fenster **Zu wählende Rufnummer** die Rufnummer des Anschlusses an, der mit dem Modem verbunden ist.

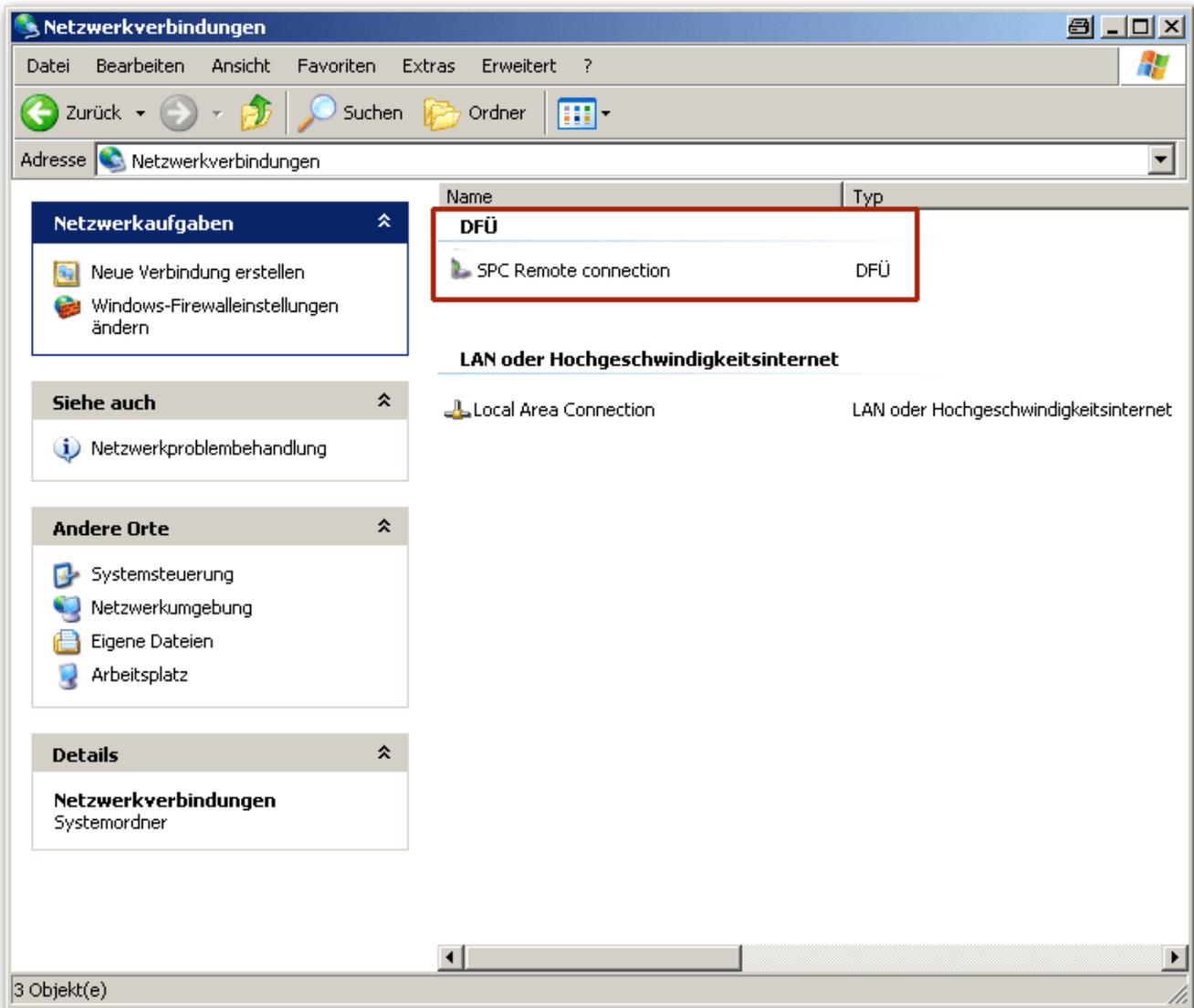
7. Geben Sie im Fenster für die Verfügbarkeit der Verbindung an, ob dieser Verbindung allen Benutzern zur Verfügung stehen soll.

Machen Sie im Fenster zum Internet-Konto folgende Angaben:

1. Benutzername: SPC
2. Passwort: password
3. Passwort bestätigen: password
  - ⇒ Es wird ein Fenster mit dem Titel „Assistent für neue Verbindung“ angezeigt.
4. Klicken Sie auf die Schaltfläche **Fertigstellen**, um die Wählverbindung zu Ihrem PC zu speichern.

### Eine Wählverbindung aktivieren

- Klicken Sie auf das Symbol in der Systemsteuerung.
  - ⇒ Daraufhin erscheint das folgende Fenster:



Der PC macht dann einen Datenanruf zu dem Anschluss des Wählnetzes, der an das Wählmodem angeschlossen ist.

Das PSTN-Modem beantwortet den eingehenden Ruf nach der angegebenen Anzahl von Ruftönen und baut eine IP-Verbindung zum Computer am entfernten Standort auf.

Dem entfernten PC wird vom SPC-System automatisch eine IP-Adresse zugewiesen.

1. Klicken Sie mit der rechten Maustaste auf das Symbol **Wählverbindung**, um die IP-Adresse einzusehen.
2. Klicken Sie auf die Registerkarte **Details**.
  - ⇒ Die IP-Adresse wird als Server-IP-Adresse angezeigt. Diese IP-Adresse, die in SPC Pro im Fenster zum Verbindungstyp angegeben werden muss. Siehe Seite [→ 27].



Einzelheiten zum Verbinden mit der Zentrale von einem entfernten Standort über ein GSM-Modem siehe Anhang.

## 21 Verwenden des Fast Programmer

### 21.1 Installieren des Fast Programmer auf einem PC

#### Für Windows XP

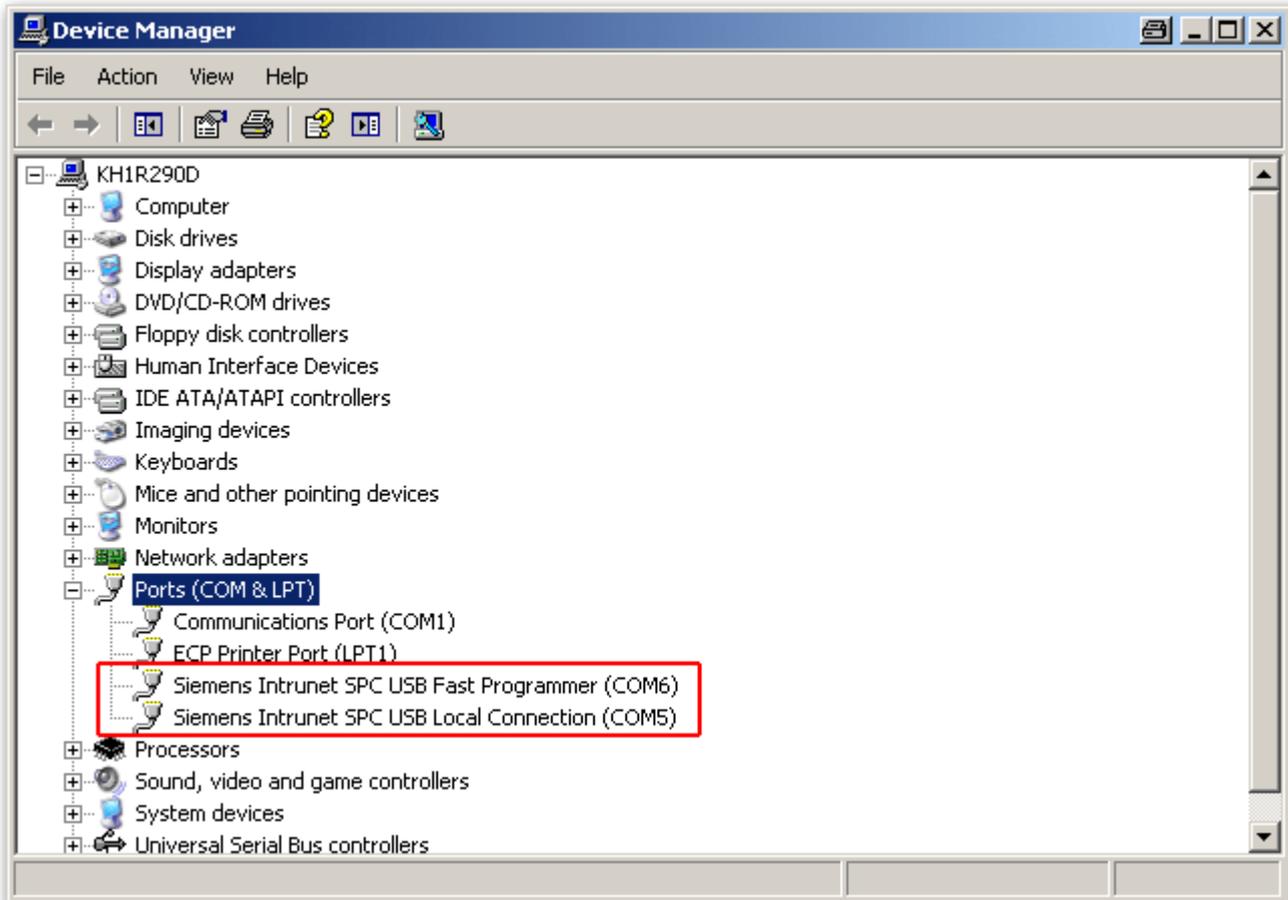
- ▷ SPC Pro muss auf dem PC mit Windows XP installiert sein.
- 1. Schließen Sie den Fast Programmer an eine USB-Schnittstelle des PC an.
  - ⇒ Der Assistent **Neue Hardware gefunden** wird angezeigt.
- 2. Klicken Sie auf **Weiter**.
- 3. Klicken Sie auf **Installation fortsetzen**.
  - ⇒ Am Ende des Installationsprozesses zeigt ein Bestätigungsfenster an, dass die Installation abgeschlossen ist.
- 4. Klicken Sie auf **Fertig stellen**.

#### Für Windows 7

- ▷ Sie verfügen über Administratorrechte.
- ▷ SPC Pro muss auf dem PC mit Windows 7 installiert sein.
- Schließen Sie den Fast Programmer an eine USB-Schnittstelle des PC an.
  - ⇒ Die Treiber werden automatisch installiert

#### Ansicht SPC Fast Programmer

- Wählen Sie im Windows-Menü **Start > Systemsteuerung > System > Geräte manager**.
- ⇒ Der Treiber für den Fast Programmer ist im Ports (COM & LPT)-Verzeichnis als **SPC USB Fast Programmer (COM X)** (X = COM-Port-Nummer) aufgeführt.



## 21.2 Mit dem Fast Programmer verbinden



Sie können sich nicht mit dem Fast Programmer verbinden, wenn Sie sich im Konfigurationsmodus befinden.

Wenn der Fast Programmer erfolgreich auf Ihrem PC installiert wurde, starten Sie SPC Pro.

- Klicken Sie auf der Hauptseite der Installation auf die Schaltfläche **Fast Programmer**.  
⇒ Daraufhin erscheint das folgende Fenster.



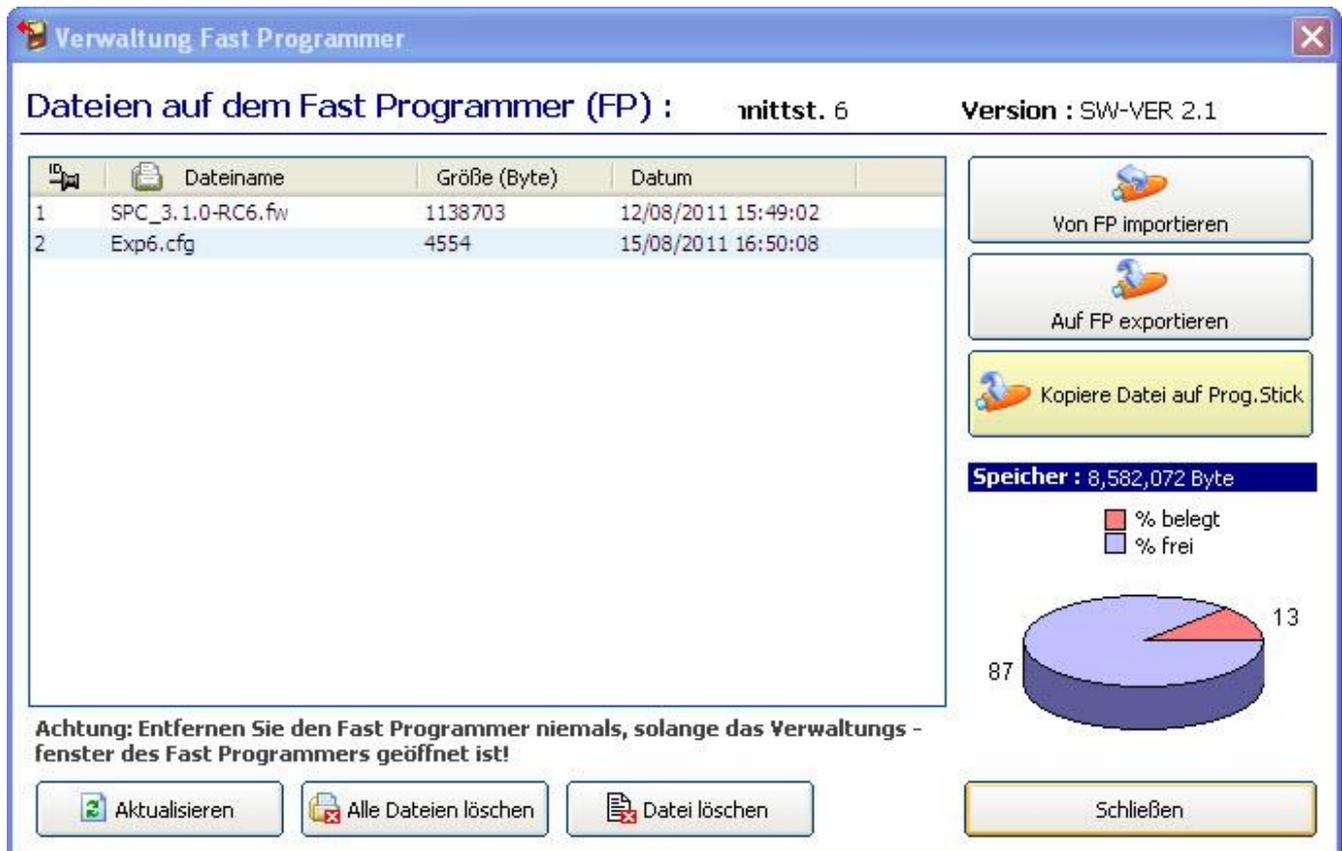
Das Fenster zeigt den seriellen Anschluss an, an dem der Fast Programmer erkannt wurde.



Wenn SPC Pro den Fast Programmer nicht erkennt, erscheint eine Pop-up-Meldung.

Installieren Sie den Fast Programmer erneut und stellen Sie sicher, dass er unter den COM-Ports im Gerätemanager angezeigt wird.

- Klicken Sie auf **Verbinden**.  
⇒ Daraufhin erscheint das folgende Fenster.



In diesem Fenster sind Dateien aufgelistet, die im Gerät gefunden wurden, sowie der verbleibende Speicherplatz zum Speichern weiterer Konfigurationen.



#### **HINWEIS**

Trennen Sie den Fast Programmer **NICHT**, solange das Fenster **Fast Programmer Manager** geöffnet ist. Hierdurch können Daten beschädigt werden, die im Fast Programmer gespeichert sind.

Es können folgende Aktionen ausgeführt werden:

- Importieren von Konfigurationsdateien aus dem Fast Programmer [→ 248]
- Exportieren von Konfigurationsdateien zum Fast Programmer [→ 249]
- Kopieren von Firmware- und Sprachdateien auf den Fast Programmer [→ 250]

## 21.3 Importieren von Konfigurationsdateien aus dem Fast Programmer

Eine Konfigurationsdatei vom SPC Fast Programmer importieren

1. Klicken Sie auf die Datei, die Sie benötigen.
2. Klicken Sie auf die Schaltfläche **Von FP importieren**.  
⇒ Daraufhin erscheint das folgende Fenster.



3. Klicken Sie auf **Ja**.  
⇒ Daraufhin erscheint das folgende Fenster:



Nach dem Laden der Konfigurationsdatei wird folgendes Fenster angezeigt:

Auflistung der Installationen

### Installationsdetails

Details für diese Installation eingeben...

SPC Pro ID :  Muss eindeutige ID sein (1-9999999)

Installationsname:

Installationsadresse:

Zentralentyp:

Zentralenversion :

\*Region :

\*Grade :

Gruppe:

IP-Adresse:  IP-Port:

Telefonnummer 1:

Telefonnummer 2:

Passwort :



Im Fenster mit den Installationsdetails werden grundlegende Konfigurationsdaten der geladenen Datei angezeigt. Wenn Sie bereits eine Installation in SPC Pro mit der selben Installations-ID haben, werden Sie aufgefordert, die ID zu ändern, bevor Sie fortfahren.

- Klicken Sie auf **OK**, um die Datei zu importieren.



Es wird nachdrücklich empfohlen, die Konfigurationsdetails einer vom Fast Programmier importierten Datei zu überprüfen, BEVOR diese Konfiguration an die Zentrale gesendet wird.

## 21.4 Exportieren von Konfigurationsdateien zum Fast Programmier

Ihre Konfigurationseinstellungen im Fast Programmier speichern

1. Klicken Sie auf die Schaltfläche **Auf FP exportieren**.

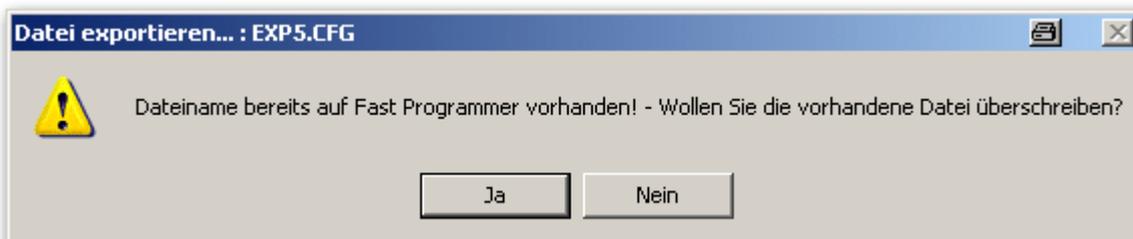
⇒ Daraufhin erscheint das folgende Fenster:



2. Wählen Sie die Installation, die Sie exportieren wollen, aus dem Dropdown-Menü **Installation auswählen**.
  - ⇒ Es wird eine Liste aller derzeit in SPC Pro verfügbaren Installationskonfigurationen angezeigt.
3. Geben Sie den Namen der Konfigurationsdatei im Feld **Dateiname auf FP** an (zulässige Zeichen sind 'a-z' und die Ziffern '0-9').
  - ⇒ Dieser Name wird auf der Datei erscheinen, wenn Sie sie vom Fast Programmer importieren.



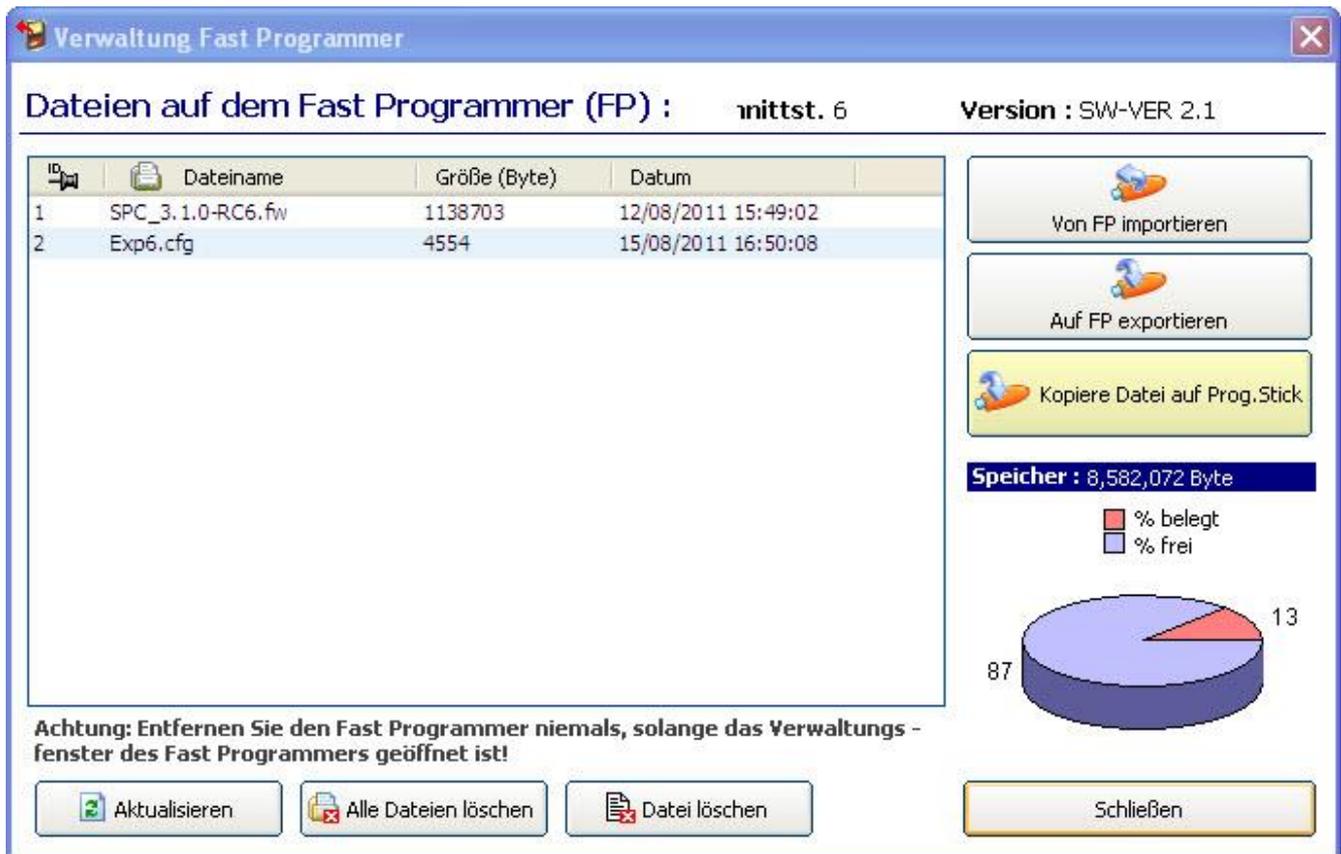
Geben Sie einen eindeutigen Namen für die Installation ein. Wenn im Fast Programmer bereits eine Konfigurationsdatei mit demselben Namen existiert, wird eine Warnmeldung angezeigt, die Sie auffordert, die Konfiguration umzubenennen.



## 21.5 Kopieren von Firmware- und Sprachdateien auf den Fast Programmer

Controller- und Peripherie-Firmware-Dateien sowie kundenspezifische Sprachdateien können auf den Fast Programmer kopiert werden, um ein Upgrade auf der Zentrale über ein Bedienteil oder den SPC-Browser durchzuführen.

<b>!</b>	<b>HINWEIS</b>
	Die letzte Firmware-Version ist eventuell nicht mit älteren Fast Programmer-Modellen kompatibel. In diesem Fall müssen Sie zunächst ein Upgrade von Fast Programmer durchführen, um neue Firmware-Versionen kopieren zu können.



Datei auf den Programmer kopieren.

1. Klicken Sie im Dialog „Fast Programmer Manager“ auf **Kopiere Datei auf Prog.Stick**.
  2. Wählen Sie im folgenden Dialogfeld die gewünschte Firmware- oder Sprachdatei aus.
- ⇒ Die Informationen zur ausgewählten Firmware werden wie folgt dargestellt.



- Klicken Sie auf die Schaltfläche **Jetzt kopieren**.

⇒ Die Datei wird im Dialogfeld „Fast Programmer Manager“ angezeigt.

Das Upgrade für Firmware und kundenspezifische Sprachen erfolgt auf der Zentrale über das Bedienfeld oder den SPC-Browser. Weitere Informationen finden Sie im *SPC-Installations- und Konfigurationshandbuch*.

## 22 Audio/Video-Verifikation

Einrichten der Audio/Video-Verifikation im SPC-System:

1. Installieren und konfigurieren Sie die Verifikationsmodule.
2. Installieren und konfigurieren Sie die Videokamera(s).
3. Installieren und konfigurieren Sie die Audioausrüstung.
4. Konfigurieren Sie die Verifikationszone(n).
5. Testen Sie die Audiowiedergabe der Verifikationszone(n).
6. Weisen Sie die Verifikationszone(n) den physischen Zonen zu.
7. Konfigurieren Sie die Verifikationseinstellungen.
8. Zeigen Sie die Bilder der Verifikationszonen im Webbrowser oder in SPC Pro an.

	<b>HINWEIS</b>
	Bedienteile und Zutrittskontrollen könnten je nach Dateigröße während der Übertragung der Audiodatei an die Zentrale für einige Minuten deaktiviert sein.

### 22.1 Konfigurieren von Video

#### Überblick

Kameras werden für die Videoverifikation verwendet. Die SPC-Zentrale unterstützt maximal vier Kameras. Es werden nur IP-Kameras unterstützt, und die Zentrale muss über einen Ethernet-Port verfügen.

	<b>HINWEIS</b>
	Kameras dürfen nicht übergreifend mit anderen CCTV-Anwendungen genutzt werden.

Kameras können nur mit dem Webbrowser oder SPC Pro konfiguriert werden. Die Konfiguration über das Bedienteil wird nicht unterstützt. SPC Pro ist für die Konfiguration einfacher zu nutzen und wird empfohlen.

Die Zentrale unterstützt zwei Kameraauflösungen:

- 320X240  
Diese Einstellung wird empfohlen, wenn Sie die Bilder in einem Browser anzeigen möchten.
- 640X480 (mit einigen Einschränkungen).

Die folgenden Kameras werden zusätzlich zu anderen generischen Kameras unterstützt:

- Vanderbilt CCIC1410 (1/4" VGA, IP-Farbkamera)
- Vanderbilt CFMC1315 (1/3" 1.3 MP, IP-Domkamera, Innenverwendung)

Für den direkten Zugriff auf die Konfigurationsdetails der oben angegebenen Kameras steht eine standardmäßige Befehlszeichenfolge zur Verfügung. Für andere generische IP-Kameras muss die Befehlszeichenfolge manuell eingegeben werden.

## Hinzufügen von Kameras

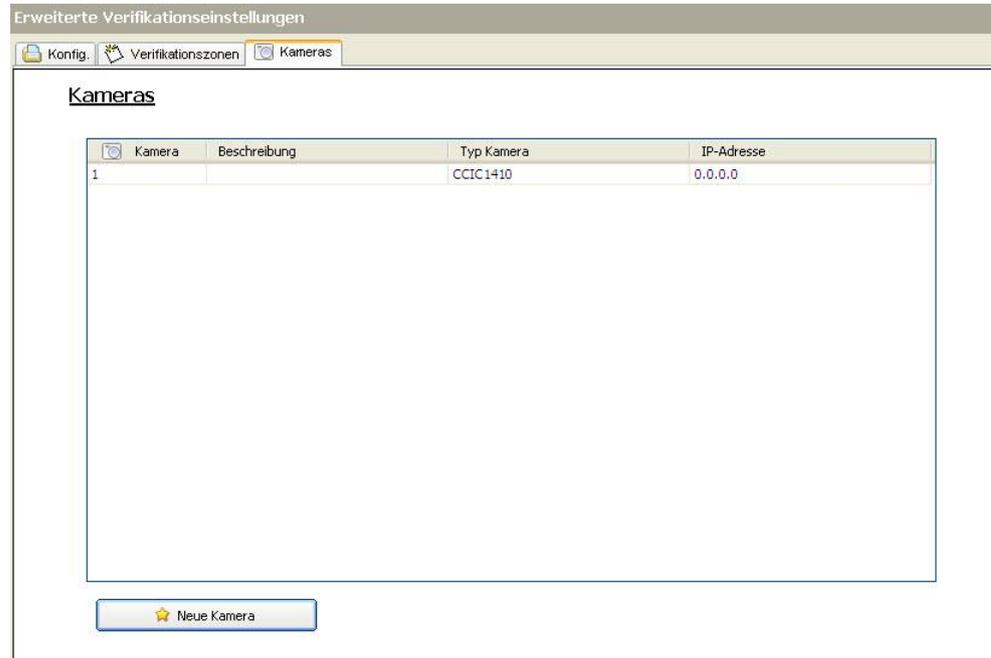
Advanced



Verifikation

1. Klicken Sie auf die Registerkarte **Kameras**.

⇒ Eine Liste der zuvor konfigurierten Kameras wird angezeigt.



2. Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Kamera hinzuzufügen.

3. Klicken Sie auf eine vorhandene Kamera, um deren Konfiguration zu bearbeiten.

4. Konfigurieren Sie die Kamera. (Siehe Konfigurieren einer Kamera [→ 255])

### 22.1.1 Lese Kameraeinstellungen

Nach Klick auf **Lese Kameraeinstellungen** stellt SPC Pro eine Verbindung zur Kamera her, um deren Einstellungen zu lesen.



SPC Pro verwendet die IP-Adresse und den TCP-Port, der im Bereich „Allg. Einstellung“ angezeigt wird. Falls die Authentifikation aktiviert ist, werden auch der konfigurierte Benutzername und das dazugehörige Passwort verwendet.

Dieser Vorgang führt in den folgenden Fällen zu einem Timeout oder schlägt fehl:

- Die Kamera ist ausgeschaltet.
- Die Kamera ist nicht angeschlossen.
- Die IP-Adresse oder der Port ist falsch.
- Der Benutzername oder das Passwort ist falsch.

## 22.1.2 Konfigurieren einer Kamera

Das Dialogfeld **IP-Kamera hinzufügen** wird angezeigt:

- wenn im Hauptfenster **Kameras** auf die Schaltfläche **Kamera hinzufügen** geklickt wird, um manuell eine neue Kamera hinzuzufügen.
- wenn im Hauptfenster **Kameras** zur Bearbeitung auf eine Kamera geklickt wird  
Konfigurieren Sie die folgenden Einstellungen:

Allgemeine Einstellungen	
Kamera ID	Die vom System generierte Kamera-ID.
Beschreibung	Geben Sie einen eindeutigen Namen zur Beschreibung der Kamera ein.
Typ	Wählen Sie einen der folgenden Kameratypen aus: <ul style="list-style-type: none"><li>• Allgemein</li><li>• Vanderbilt CCIC1410</li><li>• Vanderbilt CFMC1315</li></ul>
Kamera IP	Geben Sie die IP-Adresse der Kamera ein.
Kamera Port	Geben Sie den TCP-Port ein, über den die Kamera sendet. Standard = 80.
Befehlszeile	Geben Sie die Befehlszeichenfolge ein, die an den HTTP-Server der Kamera gesendet werden soll, um Bilder abzurufen. Diese Zeichenfolge muss den Benutzernamen und das Passwort für die Kamera enthalten. Schlagen Sie in der Kameradokumentation für die jeweils erforderliche Zeichenfolge des ausgewählten Kameratyps nach. SPC Pro kann diese Einstellung automatisch konfigurieren, falls die Kamera über ein LAN angeschlossen ist. Die standardmäßige Befehlszeichenfolge für eine Vanderbilt CCIC1410- oder CFMC1315-Kamera ohne Passwort ist „/cgi-bin/stilljpeg“. Für nicht generische Kamera deaktiviert.
Vor-Alarm-Bilder	Geben Sie die Anzahl der aufzuzeichnenden Vor-Alarm-Bilder ein (0–16). Standard = 8.
Vor-Alarm-Intervall	Geben Sie das Zeitintervall (in Sek.) zwischen Vor-Alarm-Bildern ein (1–10). Der Standard ist 1 Sekunde.
Nach-Alarm-Bilder	Geben Sie die Anzahl der aufzuzeichnenden Nach-Alarm-Bilder ein (0–16). Standard = 8.
Nach-Alarm-Intervall	Geben Sie das Zeitintervall (in Sek.) zwischen Nach-Alarm-Bildern ein (1–10). Der Standard ist 1 Sekunde.
Kameraeinstellungen (nur für die Vanderbilt-Kameras CCIC1410 und CFMC1315)	
Authentifizierung	Aktivieren Sie dieses Kontrollkästchen, falls für die Kamera eine Authentifikation angefordert werden soll.
Benutzername	Geben Sie einen Anmeldebenutzernamen für die Kameraauthentifikation ein.
Passwort	Geben Sie ein Anmeldepasswort für die Kameraauthentifikation ein.
Auflösung	Wählen Sie eine jpg-Bildauflösung für die Kamera aus. (320 × 240 oder 640 × 680) <b>Hinweis:</b> Die Einstellung „320 × 240“ wird empfohlen, wenn Sie Bilder in einem Browser anzeigen möchten.



Kameraeinstellungen können von einem Techniker geändert und dezentral aktualisiert werden.

In diesem Dialogfeld sind die folgenden Funktionen verfügbar.

Schaltfläche	Wann deaktiviert?	Funktion
Lese Kameraeinstellungen	Für generische Kamera immer deaktiviert.	Aktiviert die Kommunikation zwischen SPC Pro und der Kamera, um deren Einstellungen zu lesen.
Erweiterte Kameraeinstellungen	Für generische Kamera immer deaktiviert. Für andere Kameratypen nur aktiviert, nachdem auf die Schaltfläche <b>Lese Kameraeinstellungen</b> geklickt wurde und die Einstellungen erfolgreich gelesen wurden.	Stellt für die Konfiguration eine direkte Browserverbindung zu einer Kamera her.
Momentaufzeichnung Kamera	Niemals.	Versucht, eine Momentaufzeichnung von der Kamera zu erhalten, um die Funktionalität zu testen.
Einstellungen an Kamera schicken	Für generische Kamera immer deaktiviert.	Schickt die Konfigurationseinstellungen an die Kamera.

Klicken Sie auf die Schaltfläche **Speichern**, um die Einstellungen in der Konfigurationsdatei zu speichern.

Klicken Sie auf die Schaltfläche **Entfernen**, um die aktuelle Kamerakonfiguration aus der Konfigurationsdatei zu entfernen.

Klicken Sie auf die Schaltfläche **Abbrechen**, um die Konfiguration abubrechen und zu den vorherigen Einstellungen zurück zu kehren.

## 22.2 Konfigurieren von Verifikationszonen

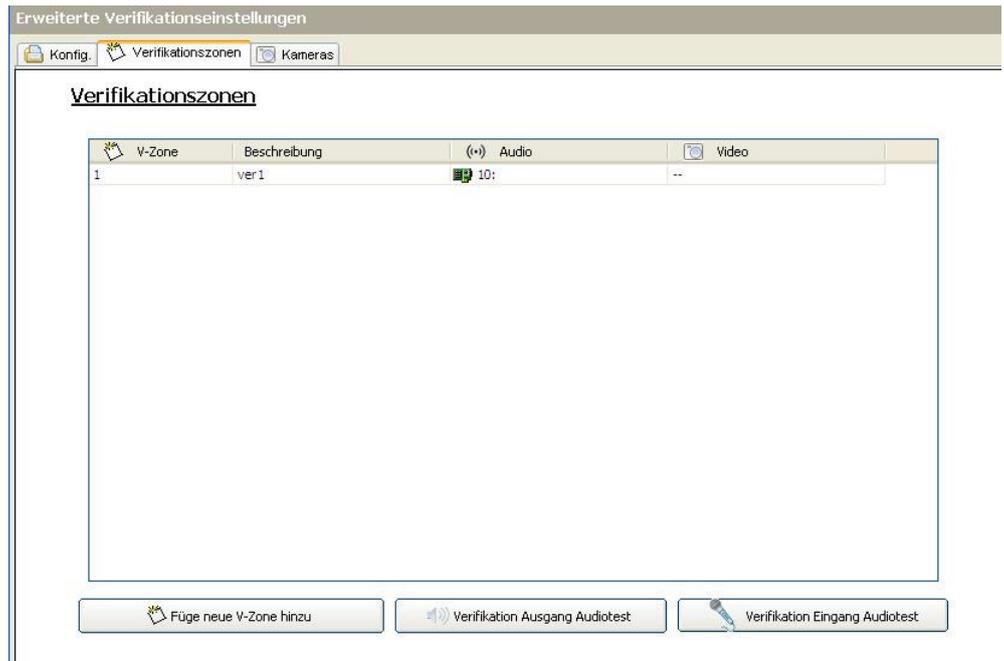
Einrichten einer Verifikationszone:



Verifikation

1. Klicken Sie auf die Registerkarte **Verifikation**.

⇒ Eine Liste der vorhandenen Verifikationszonen wird angezeigt.



2. Klicken Sie auf die Schaltfläche **Neue Verifikationszone hinzufügen**.

⇒ Das folgende Dialogfeld wird angezeigt.



3. Geben Sie zur **Beschreibung** der Zone einen Namen ein.
4. Wählen Sie **Verifikationsmodul** aus der Dropdown-Liste aus.
5. Wählen Sie ein **Video** aus der Dropdown-Liste aus.
6. Klicken Sie auf **Speichern**.
7. Weisen Sie diese Verifikationszone einer real vorhandenen Meldergruppe im SPC-System zu. (Siehe Meldergruppe bearbeiten [→ 127].)



Der Audioeingang und -ausgang der Verifikationszone kann nur von einem Techniker in SPC Pro getestet werden.

**Siehe auch**

📄 Meldergruppe bearbeiten [→ 127]

**22.2.1 Testen des Audiosignals**

Der Audioeingang und -ausgang der Verifikationszonen kann nur von einem Techniker in SPC Pro getestet werden.



Zur Durchführung dieser Tests müssen an den PC, auf dem SPC Pro ausgeführt wird, ein Headset oder Lautsprecher und ein Mikrofon angeschlossen sein. Stellen Sie sicher, dass die Lautsprecher nicht stumm geschaltet sind.

**22.2.1.1 Testen der Audiowiedergabe**

1. Klicken Sie auf der Registerkarte „Verifikations Zonen“ auf die Schaltfläche **Audiotest Verifikationsausgang**.

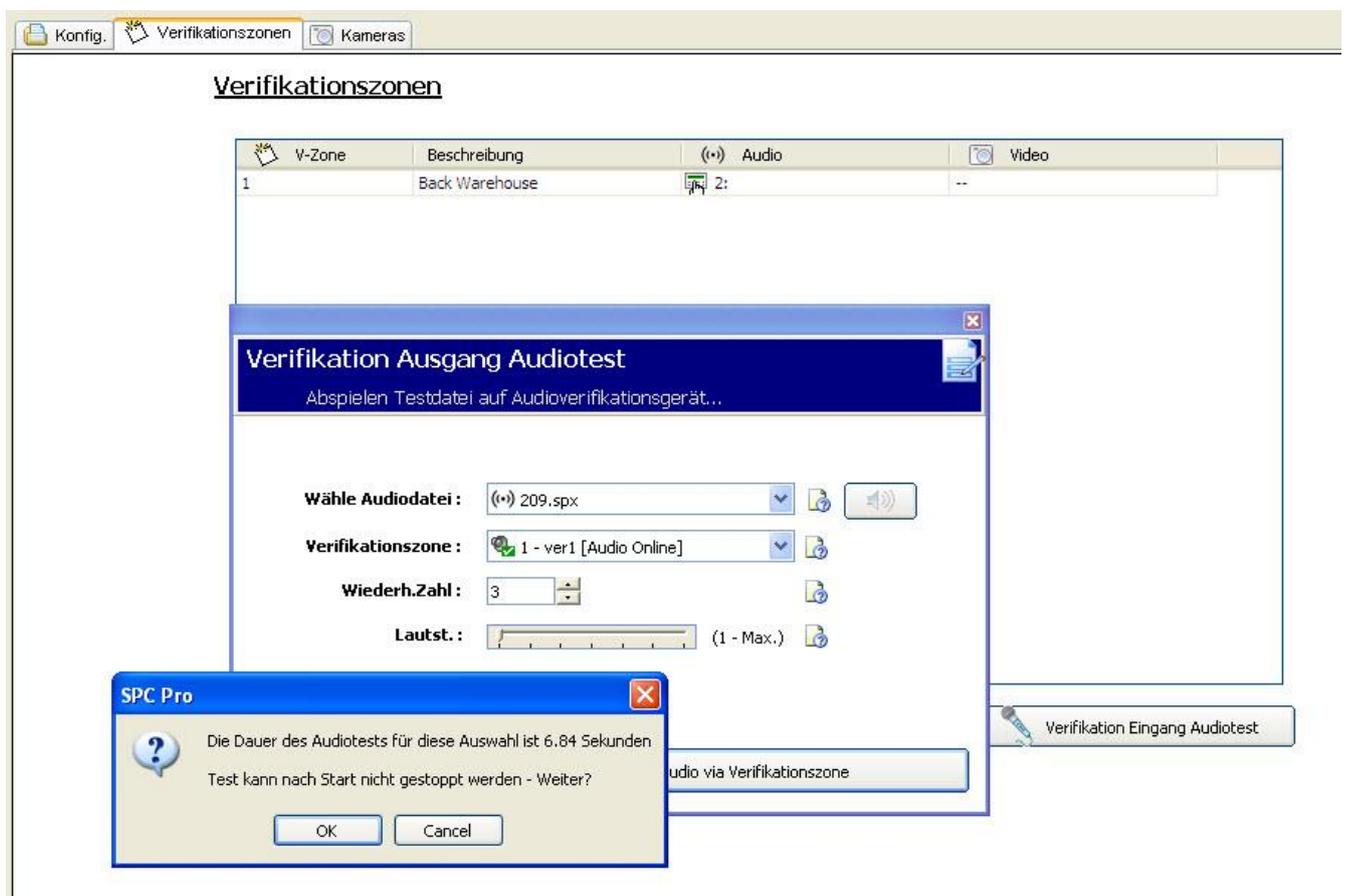
⇒ Das folgende Dialogfeld wird angezeigt.



2. Wählen Sie eine **Audiodatei**, die an die Zentrale geschickt werden soll. Die aufgelisteten Audiodateien enthalten Sprachnachrichten, die in SPC Pro installiert sind. Diese Dateien sind Speex-verschlüsselt.
3. Wählen Sie eine zu testende **Verifikationszone** aus. Nur Zonen, die online sind und über ein konfiguriertes Audiogerät verfügen, können getestet werden.
4. Legen Sie bei **Wiederholungsanzahl** die Anzahl fest, für welche die Audiodatei wiederholt werden soll, um längere Tests zu ermöglichen. Die Maximalanzahl beträgt 100.
5. Legen Sie die **Wiedergabelautstärke** für das Audiogerät fest. Standard = 7. Diese Einstellung legt das maximale Limit für die Lautstärke des Geräts fest, um es zu schützen.

6. Klicken Sie auf die Schaltfläche **Audio über Verifikationszone wiedergeben**, um die Datei wiederzugeben.
  - ⇒ Die folgende Meldung wird angezeigt.
  - ⇒ SPC Pro berechnet, wie lange die Wiedergabe der Audioprobe dauert (17,1 Sek. im folgenden Beispiel), indem die Dauer pro Probe mit der Wiederholungsanzahl multipliziert und jeweils 1 Sekunde zwischen den Wiederholungen einberechnet wird. Diese Dauer beinhaltet nicht die Zeit, die benötigt wird, um die Audiodatei in die Zentrale hochzuladen.

	<p><b>⚠ WARNUNG</b></p> <p>Bedienteile und Zutrittskontrollen könnten je nach Dateigröße während der Übertragung einer Audiodatei an die Zentrale für einige Minuten deaktiviert sein.</p>
---	--

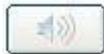


Das folgende Dialogfeld wird während der Wiedergabe angezeigt.



### Wiedergeben der Audiodatei auf dem PC

- Klicken Sie auf die Lautsprecherschaltfläche neben dem Feld **Audiodatei auswählen**.



Die Audiodatei wird auf dem PC wiedergegeben. Das ist hilfreich, um diese Wiedergabe mit der Wiedergabe in der Zentrale zu vergleichen.

#### 22.2.1.2 Testen der Audioaufzeichnung

1. Klicken Sie auf die Schaltfläche **Audiotest Verifikationseingang**.  
⇒ Das folgende Dialogfeld wird angezeigt.



2. Wählen Sie eine zu testende **Verifikationszone** aus. Nur Zonen, die online sind und über ein konfiguriertes Audiogerät verfügen, können getestet werden.
3. Wählen Sie die **Aufzeichnungsdauer** aus. Die Auswahl kann im Bereich von 1–30 Sekunden erfolgen.
  - ⇒ Eine Fortschrittsanzeige zeigt die vergangene Aufzeichnungszeit an.
  - ⇒ Das aufgenommene Audiosignal wird dann auf den PC heruntergeladen. Dies wird von einer weiteren Fortschrittsanzeige angezeigt.



4. Klicken Sie auf die Schaltfläche **Aufgezeichnetes Audiosignal wiedergeben**, die jetzt aktiviert ist.
  - ⇒ Das aufgenommene Audiosignal wird auf dem PC wiedergegeben.

## 22.3 Konfigurieren der Verifikationseinstellungen

**Hinweis:** Die folgenden Einstellungen gelten für alle Verifikationszonen [→ 256].

Advanced



1. Klicken Sie auf die Registerkarte **Einstellungen**.
  - ⇒ Das folgende Fenster wird angezeigt.



2. Konfigurieren Sie die folgenden Einstellungen.

Vor-Alarm Aufzeichnung	Geben Sie eine erforderliche Dauer für die Vor-Alarm-Aufzeichnung in Sekunden (0–120) ein. Standard = 10.
Nach-Alarm Aufzeichnung	Geben Sie eine erforderliche Dauer für die Nach-Alarm-Aufzeichnung in Sekunden (0–120) ein. Standard = 30.

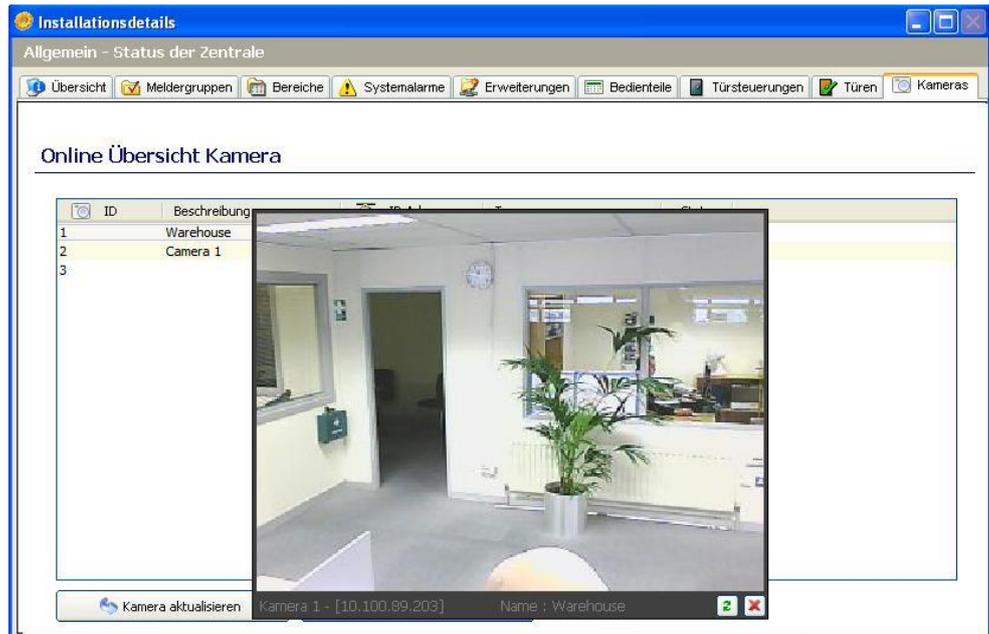
## 22.4 Anzeigen von Videobildern

Videobilder der konfigurierten Kamera können in SPC Pro angezeigt werden. Im Gegensatz zum Webbrowser, der die Bilder aller konfigurierten Kameras gleichzeitig anzeigen kann, wird in SPC Pro jeweils nur das Bild einer Kamera angezeigt.

Anzeigen eines Kamerabildes:



1. Klicken Sie auf die Registerkarte **Kameras**.
  - ⇒ Das Dialogfeld **Übersicht Kameras online** wird angezeigt.
2. Wählen Sie eine Kamera aus der Liste der konfigurierten Kamera aus.
  - ⇒ Das Bild dieser Kamera wird angezeigt.



3. Klicken Sie auf **Aktualisieren**, um das Bild manuell zu aktualisieren.



Zur Anzeige von Bildern der anderen Kameras müssen Sie das aktuelle Bild abbrechen und im Dialogfeld **Übersicht Kameras online** eine neue Kamera auswählen.

**Hinweis:** SPC Pro kann Bilder mit einer Auflösung von 320 × 240 und 640 × 480 anzeigen.

## 23 Körperschallmelder

Vibrationssensoren, auch Körperschallmelder genannt, werden verwendet, um ein versuchtes Eindringen durch mechanische Mittel wie Bohren oder das Durchstoßen von Wänden und Tresoren zu verhindern.

Körperschallmelder werden nur unterstützt, wenn der Installationstyp der Zentrale ‚finanziell‘ ist.

Es gibt mehrere Möglichkeiten, um Körperschallmelder zu testen. Der einfachste Weg einen Körperschallmelder zu testen ist, an eine Wand und einen Tresor zu schlagen und zu überprüfen, ob die Meldergruppe bei einem Gehstest geöffnet wird. Diese Testmethode ist mit allen Körperschallmeldertypen möglich.

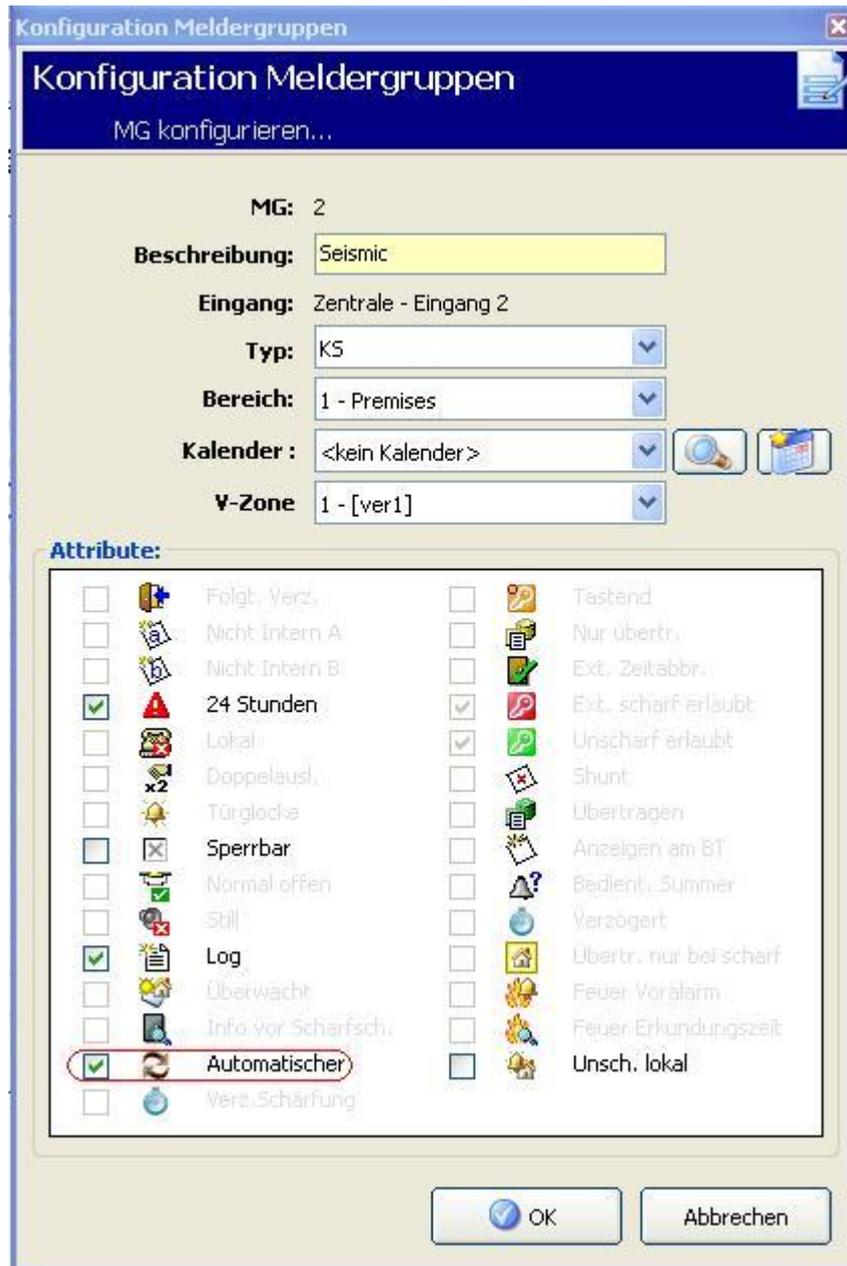
Wenn der Körperschallmelder mit einem Testsender ausgestattet ist, sind folgende Testmöglichkeiten verfügbar:

- Manuelles Testen, das am Bedienteil oder in SPC Pro (keine Browserunterstützung) initiiert wird;
- Automatisches Testen in regelmäßigen Intervallen oder wenn die Zentrale über das Bedienteil geschärft wird.

Die Testsender ist ein Hochfrequenzvibratorelement, das in geringem Abstand zum Körperschallmelder auf der gleichen Wand angebracht ist. Der Testsender ist mit einem Ausgang der Zentrale oder einem Erweiterungsmodul verbunden.

### Konfigurieren der Körperschallmelder in der Zentrale

1. Konfigurieren Sie eine Körperschall-MG. Körperschallmelder müssen einer MG zugewiesen sein. (Siehe Meldergruppe bearbeiten [→ 127].)
2. Legen Sie die Attribute für die Meldergruppe wie dargestellt fest.



3. Aktivieren Sie das automatische Testen des Melders mit dem Attribut **Automatischer Meldertest**.
4. Wählen Sie einen Kalender aus, um die Körperschall-MG zu steuern, falls erforderlich.
5. Weisen Sie einer Verifikationszone diese Zone zu, wenn eine Audio/Video-Verifikation erforderlich ist.
6. Konfigurieren Sie Timer, um festzulegen, wie oft die Körperschallmelder getestet werden sollen (Standard: 7 Tage) sowie die Dauer der Tests. (Das Attribut Automatischer Sensor Test muss eingestellt sein.) (Siehe Timer [→ 80].)

Zentralenkonfig. - Systemoptionen

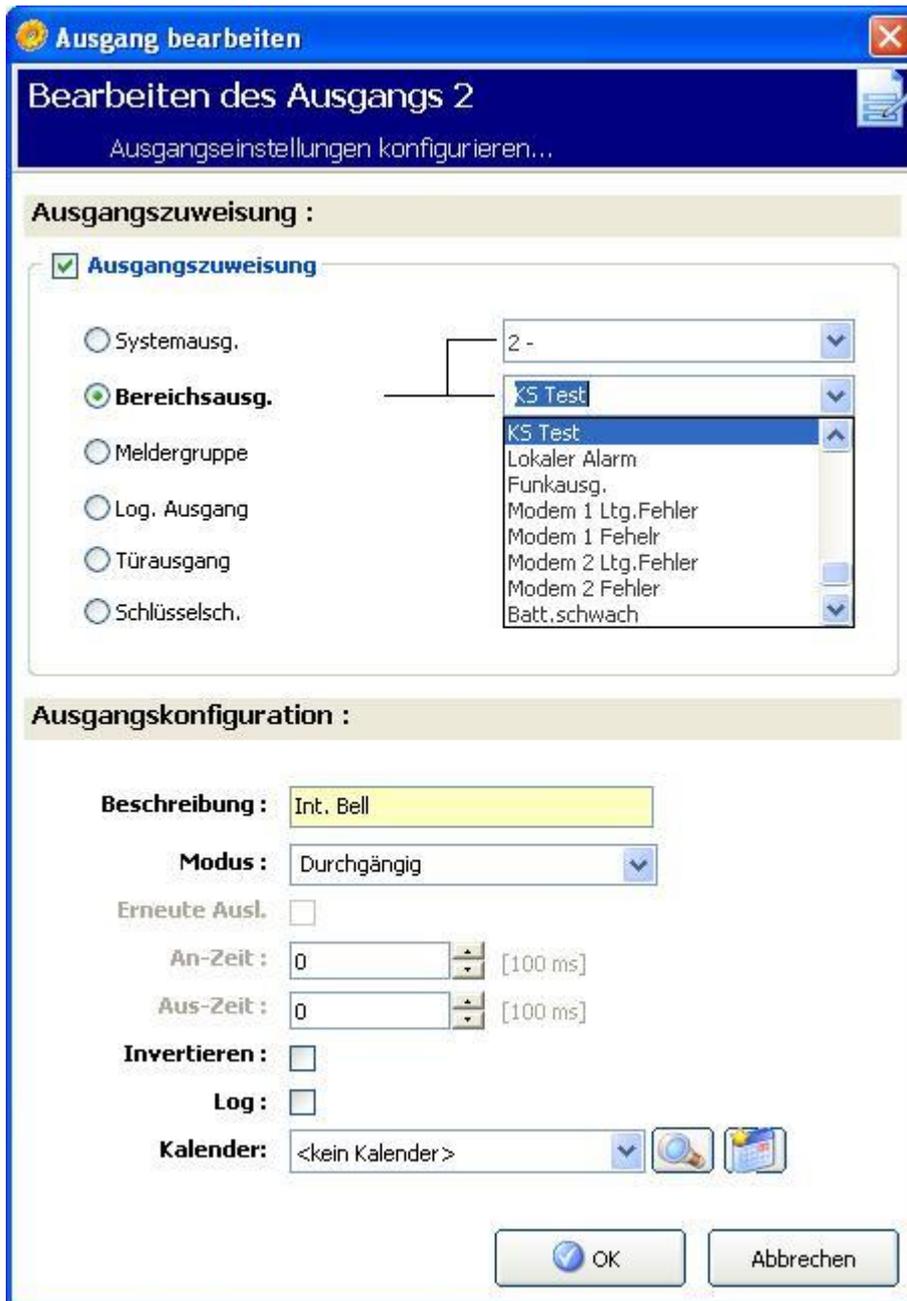
Identifikation Standards Optionen **Timer** Uhrzeit Sprache SPC Pro/SPC Safe

### System Timer

Timer	Wert	Einheit	Min.	Max.	Beschreibung
Doppelauslösung	10	Sekunden	1	99	Max. Zeit zwischen zwei Ausl. einer MG mit dem Attribut 'Doppelauslösung'
Dauertest	14	Tage	1	99	Tage, die eine MG sich im Dauertest befindet, bis dieser autom. deaktiviert
Verz. Netzstörung	0	Minuten	0	720	Minimale Dauer einer Netzstörung, bis eine Meldung generiert wird.
Verz. Übertragung	30	Sekunden	0	30	Verz.zeit nach einem Alarm, bis die Übertragung zum Empfänger gestartet
BT Timeout	30	Sekunden	10	300	Wartezeit (in Sek.) auf eine Eingabe, bis das BT das akt. Menü verlässt.
Timeout Technikerfreig.	0	Minuten	0	999	Zeit (in Min.), nach der Technikerzugang automatisch wieder gesperrt wird
Scharfsch. quitt. Sirene	0	Sekunden	0	10	Sirene kurzzeitig zur Quittierung der externen Scharfschaltung aktivieren
Scharfsch. quitt. Blitzleuchte	0	Sekunden	0	10	Blitzleuchte kurzzeitig zur Quittierung der externen Scharfschaltung aktiviert
Ext. Zeitabbruch	7	Sekunden	1	45	Zeit (in Sek.), nach der nach Schließen des Eingangs Scharfsch. erfolgt.
Verzögerung Technik	0	Sekunden	0	9999	Dauer (in Sek.), die eine Technik-MG verzögert ist.
Scharfsch. fehlg.	10	Sekunden	0	999	Zeit in Sek. für die 'Scharfsch. fehlgeschl.' am BT angez. wird (0 = bis PIN)
Überwachungszeit	336	Stunden	1	9999	Zeit innerhalb der die MG mit 'Überwacht' Attribut aktiviert werden muss
Feuer-Voralarm	30	Sekunden	1	999	Zeitspanne (in Sek.), in der auf Bestätigung/Abbruch des Feueralarms ge
Feuer Erkundungszeit	120	Sekunden	1	999	Zeitspanne (in Sek.), in der auf Bestätigung/Abbruch des Feueralarms wa
Zeitspanne Bedientellsprache	10	Sekunden	0	9999	Dauer bis Bedientellsprache bei Ruhezustand auf voreingestellte Sprache
Autom.Körperschallmeld.test	168	Stunden	12	240	Durchschnittliche Dauer für automatischen Körperschallmeldertest
Alarm Abbruch	30	Sekunden	0	999	Max. Zeit in der nach einer Alarmübertragung die Meldung Alarmabbruch
Max. Dauer KS-Meldertest	30	Sekunden	3	120	Max. Zeit bis ein bestätigter Alarm durch die Alarmabbruchmeldung quitti
Zeit Funkausgang	0	Sekunden	0	999	Aktivierungszeit von Funkausgang im System
Limit für Zeitsynchronisation	0	Sekunden	0	999	Wenn System- und Lindatezeit ausserhalb Limit wird Zeit synchronisiert

Klicken Sie auf den Wert des Timers um diesen zu bearbeiten... Jeder Timer hat einen min. und max. Wert, der beachtet werden muss...

7. Konfigurieren Sie einen Ausgang zum Testen einer Körperschall-MG. (Siehe Ausgangstypen und Ausgangsschnittstellen [→ 94])  
 Wenn die Zentrale so konfiguriert ist, dass Bereiche verwendet werden (zumeist in finanziellen Umgebungen), kann der Ausgang entweder dem System oder einem Bereich zugewiesen werden. Der Ausgang sollte nur dem System zugewiesen werden, wenn die Zentrale keine Bereiche verwendet.



**Siehe auch**

- 📖 Timer [→ 80]
- 📖 Konfigurieren einer Erweiterung [→ 101]
- 📖 Ausgangstypen und Ausgangsschnittstellen [→ 94]
- 📖 Meldergruppe bearbeiten [→ 127]

## 23.1 Testen der Körperschallmelder

Körperschall-MGs müssen konfiguriert werden, damit sowohl manuelle als auch automatische Tests verfügbar sind. Die Ergebnisse des (manuellen oder automatischen) Tests werden im System-Logbuch gespeichert.

Während des Tests werden eine oder mehrere Körperschall-MGs getestet. Beim Test einer MG werden alle anderen MGs im gleichen Bereich kurzzeitig deaktiviert, da pro Bereich nur ein einzelner Körperschalltestausgang vorhanden ist.

## 23.1.1 Vorgang des manuellen und automatischen Tests

Ein manueller oder automatischer Test wird wie folgt ausgeführt:

1. Die Zentrale aktiviert den Körperschalltestausgang für die entsprechenden Bereiche, in denen die Körperschall-MGs getestet werden sollen.
2. Die Zentrale wartet anschließend, bis sich alle getesteten Körperschall-MGs öffnen und verifiziert anschließend, dass alle Körperschallmelder in diesem Bereich im unter **Dauer von KS Test** festgelegten Zeitraum den gleichen Alarmstatus annehmen. MGs, die sich nicht im maximalen Zeitraum geöffnet haben, haben den Test nicht bestanden.
3. Wenn alle Körperschallmeldergruppen im Bereich offen sind oder die maximale Dauer des KS-Tests erreicht wurde (was immer zuerst eintritt), gibt die Zentrale den Ausgang für den KS-Test für diesen Bereich frei.
4. Die Zentrale wartet anschließend für einen festgelegten Zeitraum, damit sich alle Körperschallmelder im Bereich schließen. MGs, die sich nicht schließen, haben den Test nicht bestanden.
5. Anschließend wartet die Zentrale für einen weiteren festgelegten Zeitraum, bevor das Testergebnis gemeldet wird. Das Ergebnis des (manuellen oder automatischen) Tests wird im System-Logbuch gespeichert.

Der Körperschallausgang ist normal hoch und nimmt während der Tests ab (d. h. wenn er aktiv ist). Falls dieses Signal für einen bestimmten Melder nicht geeignet ist, kann der Ausgang als invertiert konfiguriert werden.

## 23.1.2 Automatisches Testen der Melder

Körperschallmelder werden entweder regelmäßig oder nach der Scharfschaltung des Systems mithilfe des Bedienteils getestet.

### Regelmäßige automatische Tests

Periodische automatisch Tests werden für alle Körperschallmeldergruppen durchgeführt, für die Tests aktiviert sind.

Automatische Tests finden zufällig im konfigurierten Testzeitraum statt und werden unabhängig für jeden Bereich ausgeführt.

Alle Körpermeldergruppen im gleichen Bereich (für die automatische Tests aktiviert sind) werden gleichzeitig getestet.

Die Konfigurationsoption **Körperschallmelder Autotestzeit** im Menü Timer [→ 80] bestimmt die durchschnittliche Testdauer für automatische Tests der Körperschallmelder. Der Standardwert ist 168 Stunden (7 Tage). Der einstellbare Wert muss zwischen 12 und 240 Stunden liegen.

Der Testzeitpunkt wird nach dem Zufallsprinzip innerhalb des festgelegten Toleranzbereichs (+/- 15 %) gewählt. Wenn ein Test beispielsweise alle 24 Stunden geplant ist, kann er zwischen der Stunde 20,4 und der Stunde 27,6 nach dem letzten Test durchgeführt werden.

Ein automatischer Test der Körperschallmelder wird nach einem Neustart ausgeführt. Wenn die Zentrale vor dem Neustart im Konfigurationsmodus war, wird der Test nur durchgeführt, wenn die Zentrale nach dem Neustart nicht im Konfigurationsmodus ist.

Wenn ein Test der Körperschallmelder fehlschlägt, wird ein Störungsereignis (SIA-Code „BT“) gemeldet. Außerdem wird ein entsprechendes Quittierungsereignis ausgegeben (SIA-Code „BJ“).

### Automatischer Test zur Scharfschaltung

Die Option **Test KS bei manuell scharf** kann im Menü Systemoptionen [→ 71] konfiguriert werden. Bei Aktivierung werden alle Körperschallmeldergruppen in allen Bereichen, die scharf geschaltet werden sollen, vor der eigentlichen Scharfschaltungssequenz getestet. Die gilt nur für den Bedienteilbetrieb.

Während des Tests wird die Meldung „KSM TEST“ auf dem Bedienteil angezeigt. Wenn der Körperschallmeldertest erfolgreich war, wird die Scharfschaltung normal fortgesetzt.

Wenn alle Bereiche, eine Bereichsgruppe oder ein einzelner Bereich scharf geschaltet werden soll(en) und der Körperschallmeldertest fehlschlägt, wird die Meldung „KSM FEHLER“ angezeigt. Durch Klicken auf **Best** wird eine Liste der fehlgeschlagenen MGs angezeigt, durch die mithilfe der Pfeiltasten geblättert werden kann.

Abhängig von den Einstellungen **Sperren** für die fehlgeschlagenen Körperschall-MGs und Ihrem Benutzerprofil kann Folgendes eintreten:

- Falls alle Körperschall-MGs, die den Test nicht bestanden haben, das Attribut **Sperren** aufweisen und Ihr Benutzerprofil mit dem Recht **Sperren** konfiguriert ist:
  1. Klicken Sie für die fehlgeschlagenen MGs auf **Best**.
    - ⇒ Die Meldung „ALLE ERZQ.SCHARF?“ wird angezeigt.
  2. Klicken Sie erneut auf **Best**, um alle Körperschall-MGs zu sperren, die den Test nicht bestanden haben. (Kehren Sie alternativ zum vorherigen Menü zurück.)
    - ⇒ Die Scharfschaltung wird normal fortgesetzt.
- Falls einige Körperschall-MGs, die den Test nicht bestanden haben, nicht das Attribut **Sperren** aufweisen und Ihr Benutzerprofil nicht mit dem Recht **Sperren** konfiguriert ist:
- Klicken Sie auf **Best**.
  - ⇒ Die Meldung „SCHARFSCH FEHLG“ wird angezeigt und keine Bereiche werden scharfgeschaltet.

Es gibt keinen automatischen Test für Körperschall-MGs für Bereiche, die aus einem beliebigen Grund automatisch scharf geschaltet werden (z. B. Bereiche, die durch einen Kalender oder Trigger aktiviert werden). Außerdem gibt es keinen automatischen Test für Körperschall-MGs, wenn das System mit SPC Com, SPC Pro oder dem Browser scharfgeschaltet wird. Es gibt jedoch einen automatischen Test für Körperschall-MGs, wenn ein virtuelles Bedienteil mit SPC Com oder SPC Pro verwendet wird.

Es wird kein Ereignis gemeldet, wenn der Test vor der Scharfschaltung fehlschlägt. Der Timer des regelmäßigen automatischen Systemtests startet neu, nachdem ein Test nach der Scharfschaltung durchgeführt wurde.

### 23.1.3 Manueller Meldertest

#### Allgemein



Status

Manuelles Testen der Melder:

1. Wählen Sie im Dialogfeld **Allgemeiner Status** die Registerkarte **Meldergruppen** aus.
2. Wählen Sie eine Körperschall-MG aus der Liste aus.
3. Klicken Sie auf die Schaltfläche **Körperschallmelder-Test**. (Nur möglich, wenn eine Körperschall-MG gewählt wurde.)

Allgemein - Status der Zentrale

Übersicht Meldergruppen Bereiche Systemalarme Erweiterungen Bedienteile Türsteuerungen Türen Kameras

### Online Übersicht Meldergruppen

Autom. Aktualisieren der Statusanzeige

MG	Beschreibung	Bereich	MG-Typ	Phys....	Status
1	Front door	1 - Premises	Einbruch	Geschlossen	OK
2	Seismic	1 - Premises	KS	Geschlossen	OK
3	Kitchen	1 - Premises	Einbruch	Geschlossen	OK
4	Upstairs front	1 - Premises	Einbruch	Geschlossen	OK
9	Door 1	1 - Premises	Einbruch verzögert	Geschlossen	OK
10	Door 2	1 - Premises	Einbruch verzögert	Geschlossen	OK

MG aktualisieren LOG Alarme quittieren Sperren Abschalten Dauertest

KS Test Filter MG: Alle MG

Wenn der Test erfolgreich ist oder fehlschlägt, wird eine ähnliche Meldung wie die folgende angezeigt:



Testergebnisse werden im Logbuch mit den folgenden Details gespeichert:

- Ergebnis (OK oder FEHLER)
- Benutzer-ID (z. B. 513)
- MG-Nummer und -Name

Als Ergebnis des Tests wird kein Ereignis gemeldet.

## 24 Anhang

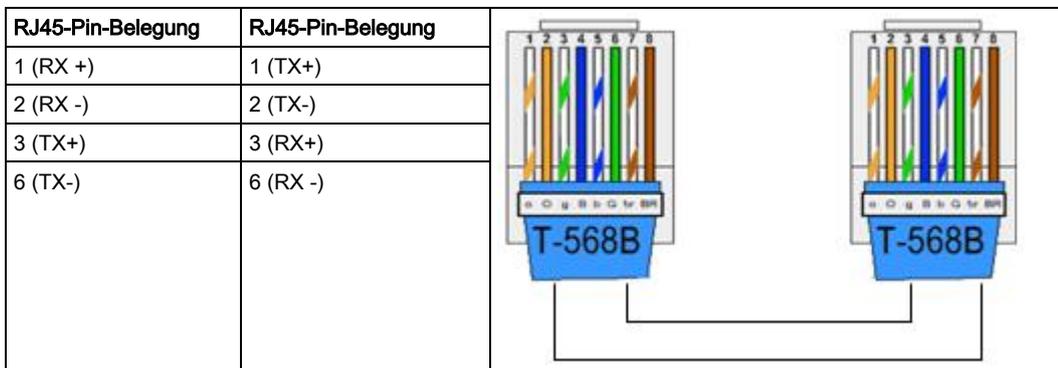
### 24.1 Netzwerk-Kabelverbindungen

IP

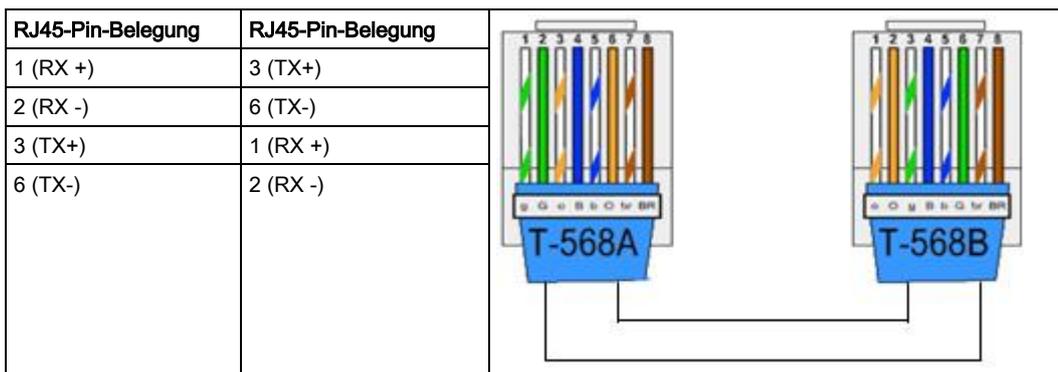
An die SPC-Zentrale kann direkt über die Ethernet-Schnittstelle oder über eine LAN-Verbindung ein PC angeschlossen werden. In der nachstehenden Tabelle sind die beiden möglichen Konfigurationen aufgeführt.

- Ist die SPC über einen Hub an ein bestehendes Netzwerk angeschlossen, schließen Sie ein gerades Kabel vom Hub zur SPC und ein anderes vom Hub zum PC an.
- Ist die Zentrale nicht an ein Netzwerk angeschlossen (d. h. die Ethernet-Schnittstelle wird nicht benutzt), sollte ein gerades Kabel zwischen der SPC-Zentrale und dem PC angeschlossen werden.

Verwenden Sie das gerade Kabel, um den SPC-Controller über einen Hub an den PC anzuschließen.



Verwenden Sie das Kreuzkabel, um den SPC-Controller direkt an einen PC anzuschließen.



### 24.2 Alarmempfangsstelle (Empfänger)

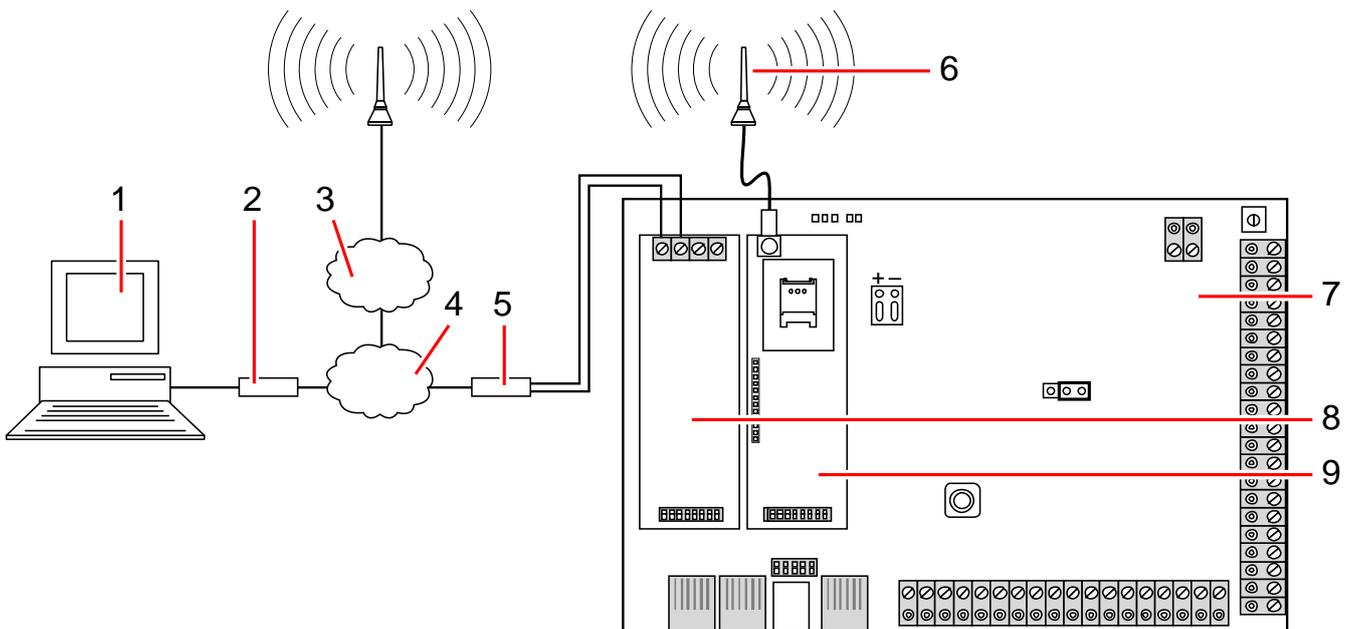
Die SPC-Zentrale kann Informationen einer entfernten Empfangsstation mitteilen, wenn ein bestimmter Alarm in der Zentrale eintritt. Einen Überblick über die Alarmempfangsstelle finden Sie auf Seite [→ 271]. Der Techniker kann das System so konfigurieren, dass es Anrufe an eine Alarmempfangsstation (Empfänger) über das Festnetz (PSTN) oder das GSM-Netz macht. Stellen Sie sicher, dass das PSTN- oder GSM-Modem korrekt installiert ist und funktioniert, bevor Sie im System einen Empfänger konfigurieren.



Stellen Sie sicher, dass beim Auswechseln oder Installieren von Modulen im SPC-System die Anschlüsse von Wechselstromversorgung und Batterie getrennt sind. Stellen Sie sicher, dass bei der Handhabung von Anschlüssen, Drähten, Klemmen und Platinen alle erforderlichen Antistatikmaßnahmen getroffen werden.

Stellen Sie sicher, dass beim Auswechseln oder Installieren von Modulen im SPC-System die Anschlüsse von Wechselstromversorgung und Batterie getrennt sind. Stellen Sie sicher, dass bei der Handhabung von Anschlüssen, Drähten, Klemmen und Platinen alle erforderlichen Antistatikmaßnahmen getroffen werden.

### Installation von Einsteckmodulen



1	Alarmempfangsstelle (Empfänger)
2	PSTN-Modem
3	GSM-Netz
4	PSTN-Netz
5	Telefonleitung
6	Externe Antenne
7	SPC-Zentrale
8	PSTN-Modem
9	GSM-Modem

## 24.3 EDP-Protokoll (Enhanced Datagram Protocol)

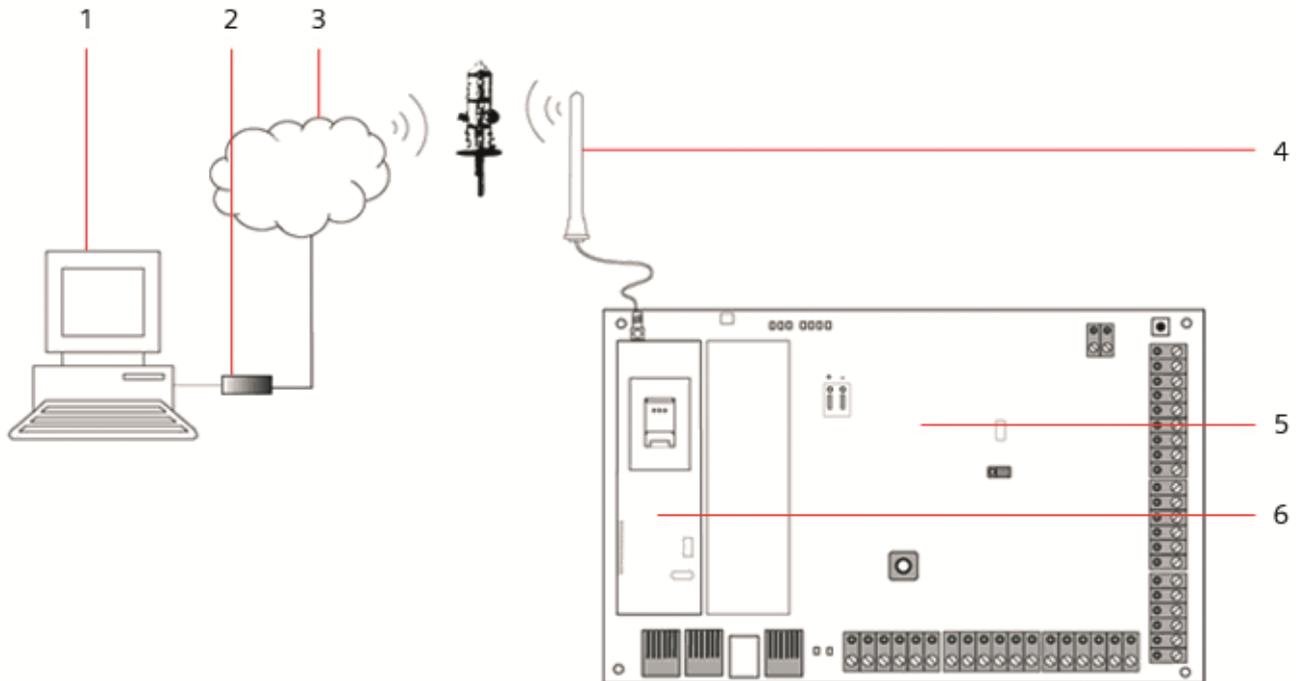
IP

Das System bietet die Möglichkeit, unter Verwendung des EDP-Protokolls (**E**n

### hanced **D**atagram **P**rotocol) von Vanderbilt Informationen an den entfernten SPC-Kommunikationsserver zu senden. Durch richtiges Konfigurieren des EDP-Empfängers im System lässt er sich so programmieren, dass er automatisch Datenanrufe zum SPC-Kommunikationsserver an einem entfernten Standort macht, wenn Ereignisse wie Alarmaktivierungen, Sabotage, Scharf- oder



## 24.4 Herstellen einer Fernverbindung zur Zentrale über GSM



1	PC mit SPC Pro
2	PSTN/GSM-Modem
3	PSTN/GSM-Netz
4	Externe Antenne
5	SPC-Zentrale
6	GSM-Modem

Auf die SPC-Zentrale kann per Fernverbindung über das GSM-Netz zugegriffen werden. In der Zentrale muss wie oben dargestellt ein GSM-Modul (mit SIM-Karte) installiert sein, um den Fernzugriff auf die SPC zu ermöglichen. Am entfernten Standort der Verbindung muss im PC des Benutzers ein Wählmodem oder ein GSM-Modem installiert sein, das mit einem PC verbunden ist, auf dem SPC Pro installiert ist. Falls ein PSTN-Modem installiert ist, muss es mit einem aktiven PSTN-Anschluss verbunden sein.

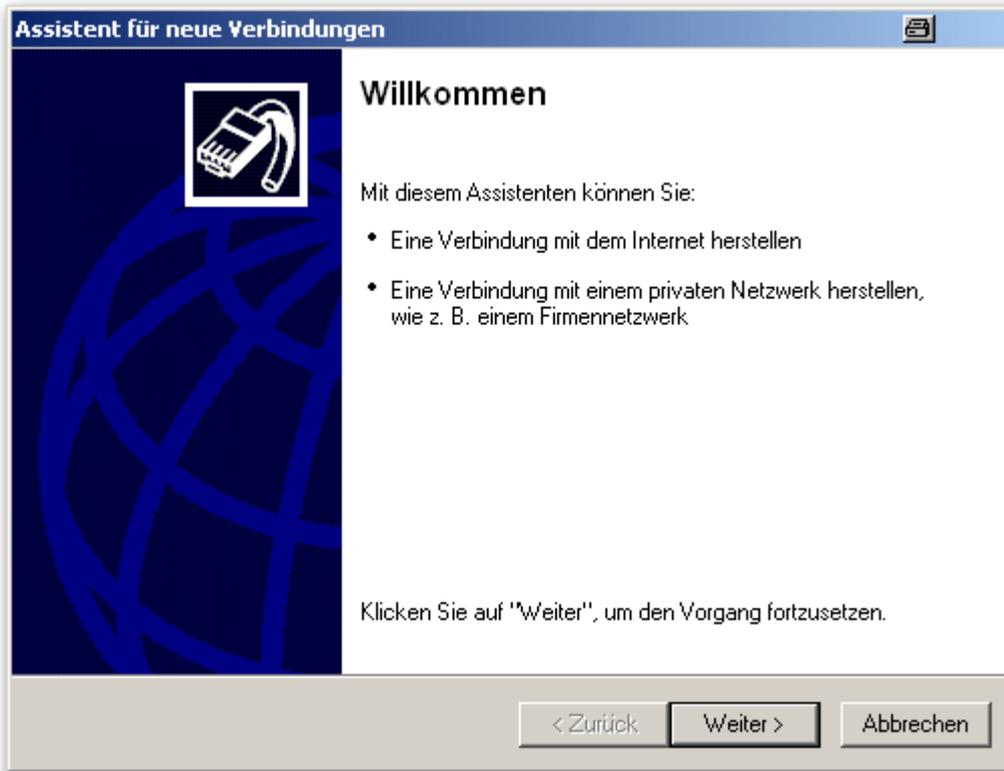
### Das Modem in der SPC-Zentrale konfigurieren

Installieren Sie ein GSM-Modem in der SPC-Zentrale und überprüfen Sie, ob es korrekt funktioniert. (Einzelheiten hierzu finden Sie in den technischen Informationen zum SPC). Rufen Sie über ein an die SPC angeschlossenes Bedienteil den Konfigurationsmodus auf und konfigurieren Sie das Modem (Primär oder Backup), das eingehende Anrufe annehmen soll.

- Modem aktiv – Auf Modem aktiv einstellen.
- Typ – Zeigt den Modemtyp an (GSM).
- Ländervorwahl – Wählen Sie die betreffende Ländervorwahl aus (Irland, UK, Spanien usw.)
- Anrufannahme – Wählen Sie die Anzahl von Ruftönen. Hiermit geben Sie an, das Modem eine bestimmte Anzahl von Ruftönen abwarten soll, bevor es einen eingehenden Ruf annimmt.
- Modemrufzeichen – Wählen Sie die Anzahl von Ruftönen, die möglich sind, bevor ein eingehender Ruf angenommen wird (max. 8 Ruftöne).

## Unter Windows XP

1. Öffnen Sie den Assistenten für neue Verbindungen, indem Sie **Systemsteuerung > Netzwerkverbindungen > Neue Verbindung erstellen** (im Fenster Netzwerkaufgaben).



2. Wählen Sie im Fenster Netzwerkverbindungstyp **Mit dem Internet verbinden**.
3. Wählen Sie im Fenster Vorbereitung **Verbindung manuell einrichten**.
4. Wählen Sie im Fenster Internetverbindung **Über Wählmodem verbinden**.
5. Geben Sie im Fenster „Verbindungsname“ den Verbindungsnamen ein, z. B. „SPC-Fernverbindung“.
6. Geben Sie im Fenster Zu wählende Rufnummer die Rufnummer des Anschlusses an, der mit dem SPCModem verbunden ist.
7. Geben Sie im Fenster für die Verfügbarkeit der Verbindung an, ob dieser Verbindung allen Benutzern zur Verfügung stehen soll.

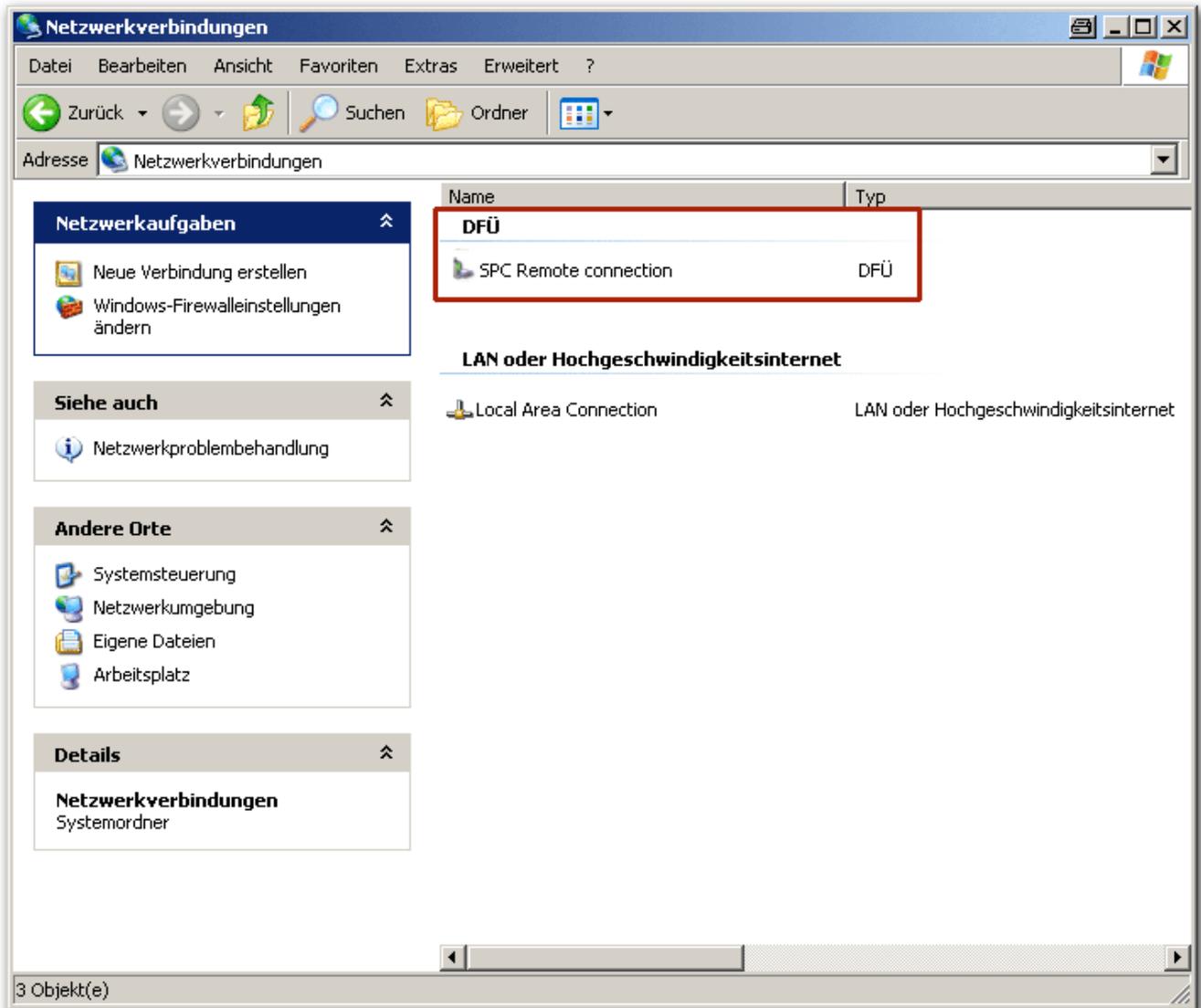
8. Machen Sie im Fenster zum Internet-Konto folgende Angaben:

- Benutzername: SPC
- Passwort: password
- Passwort bestätigen: password
- ⇒ Es wird das Fenster **Assistent für neue Verbindung** fertiggestellt wird angezeigt.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**, um die Wählverbindung zu Ihrem PC zu speichern.

So aktivieren Sie diese Wählverbindung:

- Klicken Sie auf das Symbol **Systemsteuerung > Netzwerkverbindungen**.
  - ⇒ Der PC macht dann einen Datenanruf zu dem Anschluss des Wählnetzes, der an das SPC-Wählmodem angeschlossen ist.



- ⇒ Das SPCPSTN-Modul beantwortet den eingehenden Ruf nach der angegebenen Anzahl von Ruftönen und baut eine IP-Verbindung zum Computer am entfernten Standort auf.
- ⇒ Dem entfernten PC wird vom SPC-System automatisch eine IP-Adresse zugewiesen.

Diese IP-Adresse aufrufen:

1. Klicken Sie mit der rechten Maustaste auf das Wählsymbol.
  2. Klicken Sie auf die Registerkarte **Details**.
- ⇒ Die IP-Adresse wird als Server-IP-Adresse angezeigt. Diese IP-Adresse, die in SPC Pro im Fenster zum Verbindungstyp angegeben werden muss. Siehe Seite [→ 27].



Es empfiehlt sich, die Baudrate des Modem im PC auf 9600 bps einzustellen.

## 24.5 Meldergruppentypen

Die Meldergruppentypen im SPC-System können sowohl mit dem Browser als auch mit dem Bedienteil programmiert werden. In der nachstehenden Tabelle werden die im SPC-System verfügbaren Meldergruppentypen kurz beschrieben. Jeder Meldergruppentyp aktiviert seinen eigenen eindeutigen Ausgangstyp (ein interner Merker oder Indikator), der protokolliert oder, falls erforderlich, zur Aktivierung eines spezifischen Geräts einem physischen Ausgang zugewiesen werden kann.

MG Typ	Verarbeitungskategorie	Beschreibung
EINBRUCH	Eindringling	Dieser Meldergruppentyp ist als Standard voreingestellt und wird für Standardinstallationen am häufigsten verwendet. Die Aktivierung eines Sabotage-, Offen- oder Leitungsunterbrechungsmelders löst in jedem Modus (mit Ausnahme von Unscharf) ohne Verzögerung einen vollen Alarm aus. Im Unscharf-Modus werden Sabotage-Ereignisse protokolliert und es wird die Warnmeldung SABOTAGE MELDERGRUPPE generiert und ein lokaler Alarm ausgelöst. In den Modi Intern scharf A, Intern scharf B und Extern scharf werden alle Aktivitäten aufgezeichnet.
EINBRUCH VERZÖGERT	Eindringling	Dieser Meldergruppentyp sollte allen Meldergruppen entlang einer Route für das Betreten/Verlassen eines Bereichs (z. B. einem Haupteingang oder einem anderen Zugangsbereich des Gebäudes oder der Räumlichkeiten) zugewiesen werden. Dieser MG-Typ stellt eine Scharfschaltungsverzögerung für das Betreten bzw. Verlassen des Bereichs zur Verfügung. Der Zugangs-Timer steuert diese Verzögerung. Bei Extern-Scharfschaltung des Systems aktiviert dieser Meldergruppentyp eine Scharfschaltungsverzögerung, die ausreichend Zeit zum Verlassen eines Bereichs gewährt. Der Ausgangs-Timer steuert diese Verzögerung. Im Modus Intern scharf A ist dieser Meldergruppentyp nicht aktiv.
ABBRUCH SCHARFSCHALTUNG SVERZÖGERUNG	Eindringling	Dieser Meldergruppentyp wird zusammen mit einem Taster an der Route zum Ausgang eingesetzt und löst den Abbruch der Scharfschaltungsverzögerung aus. Das bedeutet, er gewährt eine unbegrenzte Scharfschaltungsverzögerungszeit; das System kann erst dann scharf schalten, wenn der Taster gedrückt wird.
FEUER	Bedrohung	Meldergruppen für Feueralarm sind 24-Stunden-MGs zur Brandverhütung. Sie sprechen unabhängig vom Betriebsmodus der Zentrale an. Wenn eine Feueralarm-MG öffnet, wird ein voller Alarm generiert und der Ausgangstyp FEUERALARME wird aktiviert. Ist das Attribut „Nur Übertragen“ gesetzt, wird diese Aktivierung nur an die Zentrale übertragen, ein voller Alarm wird nicht generiert.
NOTAUSGANG	Bedrohung	Dies ist eine besondere Art von 24-Stunden-MG für den Einsatz mit Notausgängen, die immer geschlossen bleiben sollten. Im Unscharf-Modus löst die Aktivierung dieser Meldergruppe den Ausgang für Notausgang aus; es werden Warnmeldungen erzeugt.
TELEFONLEITUNG	Störung	Eingang zur Überwachung der Telemetrieleitung. Er wird normalerweise in Verbindung mit einem Telefonleitungs-Überwachungsausgang eines externen digitalen Wählgeräts oder eines Kommunikationssystems mit Direktverbindung verwendet. Bei Aktivierung wird bei Unscharf ein lokaler Alarm und in allen anderen Modi ein voller Alarm generiert.
ÜBERFALLALARME	Bedrohung	Dieser Meldergruppentyp ist rund um die Uhr aktiv und wird über eine Überfalltaste ausgelöst. Wenn eine Überfall-Meldergruppe ausgelöst wird, sendet sie ein Überfall-Ereignis, unabhängig vom Schärfungszustand der Zentrale. Alle Auslösungen werden protokolliert und übertragen, wenn das Log-Attribut aktiv ist. Ist das STILL-Attribut aktiviert, wird ein stiller Alarm ausgelöst (die Aktivierung wird an die Alarmempfangszentrale übertragen), andernfalls wird ein voller Alarm generiert.
BEDROHUNGSALARME	Bedrohung	Dieser Meldergruppentyp ist rund um die Uhr aktiv und wird über eine Taste ausgelöst. Wenn eine Bedrohungs-Meldergruppe ausgelöst wird, sendet sie ein Bedrohungsereignis, unabhängig vom Schärfungszustand

		der Zentrale. Das STILL-Attribut ist standardmäßig eingestellt. Deshalb ist der Alarm still. Bei Deaktivierung des Attributs, wird ein voller Alarm generiert. Alle Auslösungen werden protokolliert und übertragen, wenn das Log-Attribut aktiv ist.
SABOTAGE	Sabotage	Wird dieser Melder im unscharfen Zustand geöffnet, wird ein lokaler Alarm generiert. Eine Außensirene wird nicht aktiviert. Bei Extern scharf wird ein voller Alarm generiert. Ist das System für Sicherheitsgrad 3 konfiguriert, kann der Alarm nur mit einer Techniker-PIN quittiert werden.
TECHNIK	Eindringling	Die Technik-Meldergruppe steuert einen dezidierten Technik-MG-Ausgang an. Ändert eine Technik-MG ihren Zustand, wird der Technik-MG-Ausgang geschaltet. Das bedeutet: <ul style="list-style-type: none"> <li>● Wenn die Technik-MG öffnet, wird der Technik-MG-Ausgang ausgelöst.</li> <li>● Wenn die Technik-MG schließt, wird der Technik-MG-Ausgang deaktiviert.</li> </ul> <p>Wurden mehrere Technik-Meldergruppen zugewiesen, bleibt der Technik-MG-Ausgang aktiv, bis alle Technik-MGs geschlossen sind.</p>
MEDIZINISCHER NOTFALL	Bedrohung	Dieser Meldergruppentyp wird in Verbindung mit medizinischen Notfallschaltern verwendet, die verkabelt sind oder mit Funkübertragung arbeiten. <p>Unabhängig vom Modus tritt bei einer Aktivierung Folgendes ein:</p> <ul style="list-style-type: none"> <li>● Der Ausgang für das digitale Wählgerät für Medizinischen Notfall wird ausgelöst (es sei denn, das Attribut Lokal ist aktiviert)</li> <li>● Der Summer in der Zentrale ertönt (es sei denn, das Attribut Lokal ist aktiviert)</li> <li>● Die Meldung „Medizinischer Notfall“ wird angezeigt</li> </ul>
SCHARF/UNSCHARF EINGANG	Eindringling	Dieser Meldergruppentyp wird normalerweise in Verbindung mit einem Verriegelungsmechanismus mit Schlüssel verwendet. Eine Meldergruppe Scharf/Unscharf Eingang schaltet System/Bereich/gemeinsame Bereiche SCHARF, wenn sie ÖFFNET, und UNSCHARF, wenn sie SCHLIESST. <ul style="list-style-type: none"> <li>● Ist die Meldergruppe mit dem Typ Scharf/Unscharf Eingang in einem System ohne Bereiche zugewiesen, schaltet die Betätigung des Verriegelungsmechanismus das System SCHARF/UNSCHARF.</li> <li>● Ist die Meldergruppe mit dem Typ Scharf/Unscharf Eingang einem Bereich zugewiesen, schaltet die Betätigung des Verriegelungsmechanismus den Bereich SCHARF/UNSCHARF.</li> <li>● Ist die Meldergruppe mit dem Typ Scharf/Unscharf Eingang einem gemeinsamen Bereich zugewiesen, schaltet die Betätigung des Verriegelungsmechanismus alle Bereiche dieses gemeinsamen Bereichs SCHARF/UNSCHARF.</li> <li>● Ist das Attribut „Tastend“ gesetzt, wird der Schärfungszustand von System/Bereich/gemeinsamen Bereichen bei jeder Öffnung des Verriegelungsmechanismus umgeschaltet. (d. h. einmal Öffnen schaltet das System SCHARF, Schließen und erneutes Öffnen schaltet UNSCHARF)</li> <li>● Ist das Attribut „Extern scharf erlaubt“ aktiviert, wird bei Aktivierung der Meldergruppe das System nur extern scharf geschaltet.</li> <li>● Ist das Attribut „Unscharf erlaubt“ aktiviert, wird bei Aktivierung der Meldergruppe nur das System unscharf geschaltet.</li> </ul> <p>Bei Scharf/Unscharf Eingang wird das System/der Bereich erzwungen scharf geschaltet. Alle offenen Meldergruppen bzw. Störungsbedingungen werden automatisch gesperrt.</p> <p><b>Hinweis: Ihr System erfüllt nicht die EN-Normen, wenn Sie diesen Meldergruppentyp zur Scharfstellung des Systems ohne Eingabe einer gültigen PIN an einem externen Gerät aktivieren.</b></p>
SHUNT	Eindringling	Dieser Meldergruppentyp steht nur in der Betriebsart Kommerziell zur Verfügung. Der Meldergruppentyp Shunt-Alarm kann zwar auch im Betriebsmodus Privat gesetzt werden, bleibt dort jedoch wirkungslos. <p>Wenn dieser MG-Typ öffnet, werden alle Meldergruppen gesperrt, bei denen das Shunt-Attribut gesetzt ist. Dies geschieht sowohl bei SCHARF</p>

		als auch bei UNSCHARF. Sobald die Shunt-MG geschlossen wird, werden die Meldergruppen mit aktivem Shunt-Attribut wieder entsperrt.
X-SHUNT	Eindringling	Dieser Meldergruppentyp steht nur in der Betriebsart Kommerziell zur Verfügung. Eine Meldergruppe, die als X-Shunt-MG programmiert ist, sperrt die unmittelbar nachfolgende Meldergruppe im System, immer wenn sie geöffnet wird. Dies geschieht sowohl bei SCHARF als auch bei UNSCHARF. Sobald die X-Shunt-MG geschlossen wird, wird die nachfolgende Meldergruppe wieder entsperrt.
MELDERSTÖRUNG	Störung	Meldestörzonen sind 24-Stunden-Zonen, die auf ein Meldegerät wie z. B. PIR angewendet werden. Der Störzonentyp aktiviert den Störausgang. Bei Scharfschaltung des Systems wird ein Störausgang ausgelöst. Sowohl die Bedienteil-LED als auch der Summer werden bei einer Unscharfschaltung aktiviert.
RIEGELKONTAKT	Eindringling	Nur im Modus „Kommerziell“ verfügbar. Zur Überwachung einer Türverriegelung verwendet. System kann so programmiert werden, dass eine Scharfschaltung nur bei verriegelter Tür erfolgt.
KÖRPERSCHALLM.	Eindringling	Nur verfügbar, wenn die Zentrale im Modus „Finanziell“ betrieben wird. Vibrationsensoren, auch Körperschallmelder genannt, werden verwendet, um ein versuchtes Eindringen durch mechanische Mittel wie Bohren oder das Durchstoßen von Wänden und Tresoren zu verhindern.
ALLES IN ORDNUNG	Eindringling	Dieser Meldergruppentyp ermöglicht die Implementierung einer speziellen Zugangsprozedur mithilfe eines Benutzercodes und der Eingabe „Alles in Ordnung“. Ein stiller Alarm wird ausgelöst, wenn nicht die Taste „Alles in Ordnung“ innerhalb des konfigurierten Zeitraums nach der Eingabe des Benutzercodes gedrückt wird. (Siehe Bereiche [→ 129] für Einzelheiten zur Konfiguration „Alles in Ordnung“.) „Alles in Ordnung“ verwendet zwei Ausgänge (Eingangstatus [grüne LED] und Warnungsstatus [rote LED]), um den Eingangstatus mithilfe des LEDs auf dem Bedienteil anzuzeigen.
UNBENUTZT	Eindringling	Hiermit kann eine Meldergruppe abgeschaltet werden, auch wenn nicht an allen Meldergruppen EOL-Widerstände angebracht sind. Jegliche Auslösung an dieser Meldergruppe wird ignoriert.
BEDROHUNGSSTÖRUNG	Störung	Bedrohungsstörzonen sind 24-Stunden-Zonen, die auf ein Bedrohungsausgabegerät wie z. B. FÜ angewendet werden. Der Störzonentyp aktiviert den Störausgang. Bei Scharfschaltung des Systems wird ein Störausgang ausgelöst. Sowohl die Bedienteil-LED als auch der Summer werden bei einer Unscharfschaltung aktiviert. Dieser Meldergruppentyp überträgt SIA-, HT (Holdup Trouble)- und HJ (Holdup Trouble Restore)-Meldungen. Für CID wird ein Sensor-Alarmereignis (380) erstellt.
WARNSTÖRUNG	Störung	Warnstörzonen sind 24-Stunden-Zonen, die auf ein Warnausgabegerät wie z. B. eine Innen- oder Außensirene angewendet werden. Der Störzonentyp aktiviert den Störausgang. Bei Scharfschaltung des Systems wird ein Störausgang ausgelöst. Sowohl die Bedienteil-LED als auch der Summer werden bei einer Unscharfschaltung aktiviert. Dieser Meldergruppentyp überträgt SIA-, YA (Bell Fault)- und HY (Bell Restore)-Meldungen. Für CID wird ein Sensor-Alarmereignis (380) erstellt. <b>Hinweis:</b> Bei einem System der Sicherheitsstufe 2 wird im Falle eines Kabelfehlers eine Störung und kein Alarm generiert.
SCHÄRFUNGSBEREITSCHAFT.	Eindringling	Gilt für Blockschlossbetrieb. Dieser Meldergruppentyp wird verwendet, um ein Schärfungsberechtigungssignal an die Zentrale zu senden, mit dem angezeigt wird, dass das Blockschloss schärfungsbereit ist. Die Scharfschaltungsoption muss für das Schärfungsbereitschaft-Attribut für den Bereich ausgewählt werden.
SPERRELEMENT	Eindringling	Bei der Verwendung eines Sperrelements (Schraube) mit einem

		Blockschloss, signalisiert dieser Meldergruppentyp der Zentrale die Position des Sperrelements (gesperrt oder freigegeben). Diese Schraube sperrt die Tür im scharf geschalteten Zustand. Dieses Signal wird während des Scharfschaltvorgangs geprüft. Wenn die Information zur Sperrung nicht empfangen wird, schlägt die Scharfschaltung fehl.
GLASBRUCH	Eindringling	<p>Die Meldergruppe ist mit einer Glasbruch-Schnittstelle vom Typ RI S 10 D-RS-LED mit GB2001 Glasbruchmeldern verbunden.</p> <ul style="list-style-type: none"> <li>● Dieser Meldergruppentyp steht auf Zentralen und Erweiterungen zur Verfügung. Er ist nicht als Funk- oder Türmeldergruppentyp verfügbar, wenn DC2 als Tür konfiguriert ist.</li> <li>● Der Meldergruppentyp meldet auf die selbe Art und Weise wie eine Alarmmeldergruppe über SIA und Contact-ID.</li> <li>● Die Rechte zum Quittieren/Sperren/Abschalten von Glasbruch-Meldungen sind gleich einer Alarmmeldergruppe.</li> <li>● Power-up-Bedingung - Da die Stromversorgung über die Zentrale erfolgt, werden alle Zustandsänderungen 10 Sekunden nach ihrem Eintreten ignoriert, damit das Gerät zur Ruhe kommen kann.</li> <li>● Rücksetz-Bedingung - Während der ersten 3 Sekunden nach dem Rücksetzen eines Geräts werden Signale von der Glasbruch-Schnittstelle ignoriert.</li> <li>● Verlassen des Technikermodus - Beim Verlassen des Technikermodus ist es möglich, dass der Glasbruch-Ausgang umschaltet. In diesem Fall werden die Signale von diesem Melder 3 Sekunden lang ignoriert.</li> </ul>

## 24.6 MG-Attribute

In SPC wird mit den MG-Attributen festgelegt, wie die programmierten Meldergruppentypen funktionieren.

MG-Attribut	Beschreibung
Folgt Verzögerung	<p>Wenn für eine Meldergruppe das Attribut „Folgt Verzögerung“ aktiviert ist, wird beim Öffnen dieser Meldergruppe kein Alarm generiert, wenn der Eingangs- oder Ausgangstimer läuft. Bei Extern scharf geschaltetem System ist das Attribut „Folgt Verzögerung“ nicht aktiv; bei Öffnung der Meldergruppe wird ein voller Alarm ausgelöst. Das Attribut „Folgt Verzögerung“ wird meistens für PIR-Melder verwendet, die in der Nähe einer verzögerten Meldergruppe angebracht sind. Es gestattet dem Benutzer, sich innerhalb des Zugangsbereichs frei zu bewegen, während der Timer für Zutritt bzw. für Verlassen läuft.</p> <p>Das Attribut „Folgt Verzögerung“ ist nur für Alarm-MG-Typen gültig. Alle angeschlossenen Geräte (Sirenen - Innen und Außen, Summer, Blitzleuchte) sind aktiv.</p> <p><b>HINWEIS:</b> Eine Alarm-Meldergruppe mit dem Attribut „Folgt Verzögerung“ kann im Intern-scharf-Modus automatisch in eine verzögerte Meldergruppe umgewandelt werden, wenn die Option „Folgt Verz. wird Einb. verzögert“ aktiviert ist.</p>
"Nicht bei Intern A"	<p>Wenn für eine Meldergruppe das Attribut „Nicht bei Intern A“ aktiviert ist, wird beim Öffnen dieser Meldergruppe kein Alarm generiert, solange sich die Zentrale im Intern-scharf-A-Modus befindet. Das Attribut „Nicht bei Intern A“ ist nur für Meldergruppen vom Typ Alarmverzögerung und Einbruch verzögert gültig.</p> <p>Ein VOLLER Alarm wird generiert, wenn eine Meldergruppe mit aktiviertem Attribut „Nicht bei Intern A“ geöffnet wird, während das System EXTERN SCHARF oder INTERN SCHARF B geschaltet ist (Innen- und Außensirene, Blitzleuchte).</p>
"Nicht bei Intern B"	<p>Wenn für eine Meldergruppe das Attribut „Nicht bei Intern B“ aktiviert ist, wird beim Öffnen dieser Meldergruppe kein Alarm generiert, solange sich die</p>

	<p>Zentrale im Intern-scharf-B-Modus befindet. Das Attribut „Nicht bei Intern B“ ist nur für Alarm-Meldergruppen und verzögerte Meldergruppen gültig.</p> <p>Ein VOLLER Alarm wird generiert, wenn eine Meldergruppe mit aktiviertem Attribut „Nicht bei Intern B“ geöffnet wird, während das System EXTERN SCHARF oder INTERN SCHARF A geschaltet ist (Innen- und Außensirene, Blitzleuchte).</p>
24 Stunden	<p>Wird für eine Meldergruppe das Attribut „24 Stunden“ aktiviert, ist diese Meldergruppe immer aktiv und löst einen vollen Alarm aus, wenn sie geöffnet wird, unabhängig vom Betriebsmodus. Dieses Attribut kann nur den EINBRUCH-Meldergruppen zugewiesen werden. Ein VOLLER Alarm wird bei UNSCHARF, SCHARF und INTERN SCHARF generiert.</p> <p><b>HINWEIS:</b> Das Attribut „24 Stunden“ hat Vorrang vor allen anderen Attributeinstellungen für eine bestimmte Einbruchs-Meldergruppe.</p>
Lokal	<p>Wenn das Attribut „Lokal“ gesetzt ist, wird bei einem Alarm, der durch Öffnen einer Meldergruppe generiert wird, keine externe Meldung des Ereignisses gesendet. Das Attribut „Lokal“ kann bei Einbruch-, verzögerten, Feueralarm-, Notausgang- und Medizin-Meldergruppen aktiviert werden.</p>
Unscharf Lokal	<p>Wenn dieses Attribut gesetzt ist, wird der Alarm durch die Aktivierung der Meldergruppe, wenn der Bereich extern scharf oder intern scharf geschaltet wird, normal übertragen. Wenn der Bereich jedoch unscharf geschaltet wird, wird nur ein lokaler Alarm ausgelöst (z. B. Bedienteil-Summer, LED blinkt und MG wird angezeigt). Dieses Attribut kann nur den Einbruchs-, Feuer- und Körperschall-Meldergruppen zugewiesen werden.</p>
Doppelauslösung	<p>Dieses Attribut wird für problematische Melder verwendet. (Bestimmte Melder können willkürlich Aktivierungssignale generieren, die dann unbeabsichtigt Systemalarme auslösen).</p> <p>Ein Alarm wird ausgelöst, wenn eine Meldergruppe mit Doppelauslösung während des Doppelauslösungszeitraums zweimal aktiviert wird. Die Doppelauslösungszeit wird in Sekunden konfiguriert (siehe Seite [→ 80]). Zwei Öffnungen innerhalb dieses Zeitraums lösen einen Alarm aus. Bei Scharfschaltung des Systems werden alle offenen Doppelauslösungs-Meldergruppen protokolliert.</p>
Türglocke	<p>Wenn für eine Meldergruppe das Attribut „Türglocke“ gesetzt wird, werden jedes Mal, wenn die Meldergruppe bei unscharf geschaltetem System geöffnet wird, die internen Summer eine kurze Zeit lang ausgelöst (ca. 2 Sekunden).</p> <p>Das Attribut „Türglocke“ kann bei Einbruchsmeldergruppen, verzögerten Meldergruppen und Technik-Meldergruppen aktiviert werden.</p>
Sperren	<p>Wenn das Attribut „Sperrung“ aktiviert ist, kann der Benutzer die betreffende Meldergruppe sperren. Die Sperre deaktiviert die Störung bzw. die MG nur für ein Scharfschaltungsintervall.</p>
Normal offen	<p>Wenn das Attribut „Normal offen“ aktiviert ist, geht das System davon aus, dass ein angeschlossener Melder/Sensor als Gerät mit Schließkontakt funktioniert. (Das heißt, dass ein Sensor als aktiviert gilt, wenn die Kontakte im Gerät geschlossen werden).</p>
Still	<p>Ist das Attribut „Still“ aktiviert, wird der Alarm weder optisch noch akustisch angezeigt. Die Alarmauslösung wird an die Alarmempfangsstation gesendet. Bei unscharfem System wird auf dem Display eine Warnmeldung angezeigt.</p>
Log (Protokoll)	<p>Wird dieses Attribut aktiviert, werden alle Zustandsänderungen der Meldergruppe protokolliert.</p>
Info vor Scharfsch.	<p>Wenn gesetzt, wird für eine ausgelöste verzögerte Meldergruppe vor der Scharfschaltung eine Information angezeigt. Die Scharfschaltung wird dadurch nicht verhindert (nur im Komfort Bedienteil).</p>
Überwacht	<p>Dieses Attribut bezieht sich nur auf die Fernwartung*. Wird dieses Attribut für eine Meldergruppe aktiviert, muss die Meldergruppe zu Fernwartungszwecken innerhalb des voreingestellten Überwachungszeitraums öffnen.</p>
Endwiderstand	<p>Das Attribut „Endwiderstand“ (EOL) stellt im System eine Reihe von Verdrahtungskonfigurationen für Eingangs-Meldergruppen zur Verfügung.</p>

Analysed	Das Attribut „Analysed“ muss bei Meldergruppen aktiviert werden, die mit einem Vibrationsmelder verdrahtet sind. Die Werte für Impulszähler und starke Erschütterung sollten für jeden Vibrationsmelder im System in Übereinstimmung mit den Ergebnissen einer einfachen Kalibrierung des Geräts programmiert werden.
Pulse Count	Impulszähler-Triggerstufe für Vibrationsmelder mit dem Attribut „Analysed“.
Gross Attack	Erschütterungs-Triggerstufe für Vibrationsmelder mit dem Attribut „Analysed“.
Extern Zeitabbruch	Das Attribut „Extern Zeitabbruch“ kann nur verzögerten Meldergruppen zugewiesen werden. Mit diesem Attribut kann die Standardprozedur für den Ablauf der Scharfschaltverzögerung beim Schließen außer Kraft gesetzt werden, solange das System Extern scharf geschaltet ist. Wenn alle anderen Eingangs-/Ausgangs-Routen in den Räumlichkeiten geschlossen sind, schalten Sie das System Extern scharf und schließen die letzte verzögerte Meldergruppe. Sobald die Tür geschlossen ist, läuft die endgültige Scharfschaltverzögerung für die Schärfung des Systems ab.
Shunt	Eine Meldergruppe, bei der das Attribut „Shunt“ aktiviert ist, wird gesperrt, sobald eine Shunt-Meldergruppe geöffnet wird. Mit diesem Attribut können Meldergruppen gruppenweise gesperrt werden, wenn der Shunt-Meldergruppentyp geöffnet wird.
Nur übertragen	Dieses Attribut bezieht sich nur auf Feueralarm-Meldergruppen. Ist dieses Attribut aktiviert, wird bei der Auslösung der Feueralarm-Meldergruppe nur diese Auslösung an die Zentrale gemeldet. Vor Ort wird kein Alarm generiert.
Tastend	Dieses Attribut bezieht sich nur auf Meldergruppen vom Typ „Scharf/Unscharf Eingang“. Ist dieses Attribut aktiviert, wird der Scharfschaltungszustand des Gebäudes nur beim Öffnen umgeschaltet.
Extern scharf erlaubt	Dieses Attribut bezieht sich nur auf Meldergruppen vom Typ „Scharf/Unscharf Eingang“. Ist dieses Attribut aktiviert, wird bei Aktivierung der Meldergruppe das System/der Bereich extern scharf geschaltet. Wenden Sie dieses Attribut an, wenn gewünscht wird, dass der Benutzer das System nur von einer Meldergruppe des Typs „Scharf/Unscharf“ EXTERN SCHARF schalten kann.
Unscharf erlaubt	Dieses Attribut bezieht sich nur auf Meldergruppen vom Typ „Scharf/Unscharf Eingang“. Ist dieses Attribut aktiviert, wird bei Aktivierung der Meldergruppe das System/der Bereich unscharf geschaltet. Wenden Sie dieses Attribut an, wenn gewünscht wird, dass der Benutzer das System nur von einer Meldergruppe des Typs „Scharf/Unscharf“ UNSCHARF schalten kann.
Technik-Meldergruppe übertragen	Mit diesem Attribut wird ermöglicht, dass eine Meldergruppe unabhängig vom Scharfschaltungszustand an die ARC einen Alarm überträgt, in den Formaten FF CID, SIA und SIA erweitert. Werden Bereiche ausgewählt, wird der Alarm nur an die ARC übertragen, der der betreffende Bereich zugewiesen wurde. Es handelt sich hier um einen unbekanntem Alarm (UA), bei dem die Meldergruppennummer und – wenn SIA erweitert ausgewählt wurde – Text mit übertragen werden. Außerdem wird an den Endbenutzer und an den Techniker eine SMS gesendet, vorausgesetzt, dies wurde bei der Auswahl des Filters für unbestätigten Alarm eingestellt.
Technik-Meldergruppe Display	Ermöglicht es dem Techniker, eine sich öffnende Meldergruppen auf dem System-Bedienteil anzuzeigen. Außerdem sollte die Alarm-LED aufleuchten. Sind Bereiche ausgewählt, wird der Alarm nur an das Bedienteil übertragen, das dem Bereich zugewiesen wurde, zu dem die Meldergruppe gehört. Der Alarm kann nur auf dem Bedienteil angezeigt werden, wenn der Bereich unscharf ist und nicht bei Intern scharf A, Intern scharf B oder Extern scharf.
Technik-Meldergruppe hörbar	Damit kann eine ausgelöste Meldergruppe den Summer aktivieren. Die Funktionsweise ist dieselbe wie beim Attribut „Technik-Meldergruppe Display“ in den verschiedenen Schärfungszuständen und in Systemen mit Bereichen.
Technik-Meldergruppe Verzögerung	Damit kann der Meldergruppe eine programmierbare Verzögerung zugewiesen werden. Die Verzögerung kann zwischen 0 und 9999 gewählt werden und ist für alle Technik-Meldergruppen wirksam. Die Verzögerung funktioniert genauso wie beim Netzstrom-Timer: Wird die Meldergruppe innerhalb der Verzögerungszeit geschlossen, wird an die ARC kein Alarm übertragen, an den Benutzer wird keine SMS gesendet und der Technik-Ausgang wird nicht ausgelöst. <b>HINWEIS:</b> Der Technik-Ausgang wird nicht ausgelöst, bis die

	Verzögerungszeit abgelaufen ist.
Übertragung nur bei Aktiviert	Öffnungen werden nur im scharf geschalteten Modus gemeldet.
Feuer Voralarm	Bei Aktivierung und Feueralarm wird ein „Feuer Voralarm“-Timer gestartet und Innensirenen sowie Summer werden aktiviert. (Siehe Timer [→ 80].) Wenn der Alarm nicht innerhalb des Zeitraums quittiert wird, wird der Feueralarm bestätigt, die Innen- und Außensirenen werden ausgelöst und eine Meldung wird an den Empfänger geschickt.
Feuer Erkundungszeit	Bei Aktivierung wird ein „Feuer Erkundungszeit“-Timer aktiviert, der dem „Feuer Voralarm“-Timer zusätzliche Zeit zuweist, bis für die MG ein Feueralarm gemeldet wird. Siehe Timer [→ 80].
Körperschalltest/Automatischer Meldertest	Ein Körperschall-Meldergruppentyp kann manuell oder automatisch getestet werden. Dieses Attribut ermöglicht die Aktivierung des automatischen Tests. Siehe Abschnitt Timer [→ 80] für weitere Einzelheiten zur Konfiguration des Timers, der bestimmt, wie oft die Zentrale die Körperschall-MGs mit diesem Attribut testet. Der Standardwert für den Timer ist 7 Tage.
Verzögert	Das Attribut für eine verzögerte Scharfschaltung wird für „Schärfung mit Schlüssel“-MGs verwendet, um die Scharfschaltung eines Bereichs zu verzögern. Die Verzögerung folgt der Scharfschaltungsverzögerung für den Bereich, auf den sich die Schärfung mit Schlüssel bezieht.
Verifikation	Wählen Sie die konfigurierte Verifikationszone aus, um dieser den Trigger „Audio/Video Verifikation“ zuzuweisen.
Erzwungen scharf	Bei Aktivierung kann das Scharf/Unscharf-Eingangsgesetz das System scharf schalten und somit alle offenen Meldergruppen sperren.

## 24.7 Anwendbare Attribute nach Meldergruppentypen

Die nachstehende Tabelle fasst zusammen, welche Attribute dem jeweiligen Meldergruppentyp zugewiesen werden können:

Zone Type																										
	Alarm	Entry/Exit	Exit Term	Fire	Fire Exit	Line	Panic	Holdup	Tamper	Tech	Medical	Keyarm	Unused	Shunt	X-Shunt	Detector Fault	Lock Supervision	Seismic **	All Okay	Hold-up Fault	Warning Fault	Setting Authorisation	Lock Element	Glass Break		
Access	v																								v	
Exclude A	v	v																							v	v
Exclude B	v	v																							v	v
24 Hour	v																	v							v	
Local	v	v		v	v						v						v				v	v			v	v
Unset Local	v			v														v							v	
Double Knock	v																								v	
Chime	v	v									v												v		v	
Inhibit	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v	v		v	v	
Normal Open	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v	v	v	v	v	
Silent	v						v	v																	v	
Log	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v	v	v	v	v	
Shunt	v	v			v																				v	
Frequent *	v	v	v							v	v			v	v										v	
Analyzed	v	v			v																					
Pulse Count	v	v			v																					
Gross attack	v	v			v																					
Calendar	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v	v	v	v	v	
Verification	v	v		v	v		v	v		v	v							v							v	
Exit Open		v																								
Seismic Test																		v								
Timed												v														
Report Only				v																						
Open Only													v										v			
Final Exit		v																							v	
Fullset enable												v														
Unset enable												v														
Shunt	v	v			v																				v	
Report (Tech)											v															
Display(Tech)											v															
Audible (Tech)											v															
Delay (Tech)											v															
Report When Set											v															
Fire Pre-alarm				v	v																					
Fire Recognition				v	v																					
Force set												v														

 Nur im Modus „Kommerziell“ verfügbar.

\* Nur mit Fernwartung.

\*\* Nur im Modus „Finanziell“ verfügbar

## 24.8 FlexC-Glossar

Abkürzung	EN50136-1 Beschreibung	FlexC Beispiel
-----------	------------------------	----------------

AE	<b>Empfangseinrichtung</b> Die im Empfänger befindliche Ausrüstung, die den Alarmzustand sichert und anzeigt, oder der geänderte Alarmzustand der AS als Antwort auf den Empfang eingehende Alarmer vor dem Senden einer Quittierung. Die Empfangseinrichtung (AE) ist nicht Bestandteil des Übertragungssystems (ATS).	SPC Com XT-Client
ARC	<b>Alarmempfangscenter</b> Durchgehend besetztes Zentrum, an das Informationen zum Zustand eines oder mehrerer AS gemeldet werden.	SPC Com XT wäre in einem Empfänger installiert.
AS	<b>Alarmsystem</b> Die elektrische Einrichtung, die auf die manuelle oder automatische Erfassung einer Gefahrensituation reagiert. Das Alarmsystem (AS) ist nicht Bestandteil des Übertragungssystems (ATS).	SPC-Zentrale
ATE	<b>Alarmübertragungsequipment</b> Ein Sammelbegriff zur Beschreibung von SPT, MCT (Überwachungszentrumsempfänger) und des Empfängers.	-
ÜW	<b>Alarmübertragungsweg</b> Die Route einer Alarmmeldung, die zwischen einem einzelnen AS und seiner zugehörigen Empfangseinrichtung (AE) übermittelt wird. Der Alarmübertragungsweg beginnt an der Schnittstelle zwischen dem AS und dem SPT und endet an der Schnittstelle zwischen dem Empfänger und der AE. Für Benachrichtigungs- und Überwachungszwecke kann ebenfalls die umgekehrte Richtung verwendet werden.	Ein definierter Pfad zwischen der SPC-Zentrale und dem SPC Com XT. Beispielsweise wäre ein System mit Ethernet als primärer Pfad und GPRS als Backup-Pfad zwei separate ÜWs eines ATS.
ATS	<b>Alarmübertragungssystem</b> Die Übertragungseinrichtung und das Netzwerk, die zur Übertragung von Informationen über den Status eines oder mehrerer ASs in einer überwachten Liegenschaft an eine oder mehrere Empfangseinrichtungen eines oder mehrerer ARCs verwendet werden. Ein ATS kann aus mehr als einem ÜW bestehen.	Ein System, das einen oder mehrere Pfad zwischen der SPC-Zentrale und dem SPC Com XT kombiniert.
RCT	<b>Empfänger/Empfangszentrale</b> Die Übertragungseinrichtung am ARC einschließlich der Schnittstelle zu einem oder mehreren AEs und der Schnittstelle zu einem oder mehreren Übertragungsnetzwerken als Teil	SPC Com XT-Server

	von einem oder mehreren ÜWs. In einigen Systemen kann dieser Empfänger Änderungen des Status eines AS anzeigen und Protokolldateien speichern. Dies kann erforderlich sein, um die ATS-Verfügbarkeit im Falle eines AE-Ausfalls zu erhöhen.	
SPT	<b>Überwachte Übertragungseinrichtung der Zentrale</b> Die Übertragungseinrichtung an überwachten Liegenschaften einschließlich der Schnittstelle zu einem AS und der Schnittstelle zu einem oder mehreren Übertragungsnetzwerken als Teil von einem oder mehreren ÜWs.	Integriert in die SPC-Zentrale mithilfe von Ethernet, GPRS und PPP over PSTN.

FlexC verwendet außerdem die folgenden Abkürzungen.

Abkürzung	Beschreibung
ASP	<b>Analoges Sicherheitsprotokoll</b> Das analoge Sicherheitsprotokoll wird traditionell zur Übertragung von Alarmen über Telefonnetzwerke verwendet, z. B. SIA, Kontakt-ID.

## 24.9 FlexC-Steuerung

Die folgende Tabelle enthält die Befehle, die Sie für ein Steuerprofil aktivieren können. Das Steuerprofil, das Sie einem ATS zuweisen können, definiert, wie Sie eine Zentrale von einem SPC Com XT steuern.

Steuerungsfiler	Befehle
Systemsteuerungen	Anfordern der Zentralen Zusammenfassung
	Einstellung der Systemzeit und Datum
	Technikerzugang freigegeben
	Herstellerzugang freigegeben
Einbruchsteuerungen	Anfordern des Bereichsstatus
	Anfordern des Zustandes S/ U des Bereiches
	Ändern des Zustandes S/ U des Bereiches
	Status der Zentralenalarme abfragen
	Auszuführende Aktionen auf Alarmlmeldungen
	Sirene abschalten
	Anfordern MG Status
	Steuern einer Meldegruppe
	Anfordern System Logbuch
	Anfordern des Logbuch einer Meldegruppe
Anfordern des Funklogbuchs	
Ausgangsbefehle	Anfordern des Status der logischen Ausgänge
	Steuern der logischen Ausgänge
Benutzersteuerung	Prüfe Benutzer in der Zentrale

	Anfordern einer Benutzer Konfiguration
	Neuer Benutzer
	Bearbeiten eines Benutzers
	Löschen eines Benutzers
	Anfordern eines Benutzerprofils
	Hinzufügen eines Anwenderprofils
	Bearbeiten eines Benutzerprofils
	Löschen eines Benutzerprofils
	Ändern der Benutzereigenen PIN
Kalender Kommandos	Lese Kalender Konfiguration
	Neuer Kalender
	Kalender bearbeiten
	Kalenderwoche bearbeiten
	Löschen des Kalender
	Neuer Ausnahmetag des Kalenders
	Bearbeiten eines Ausnahmetages eines Kalenders
	Löschen eines Ausnahmetages des Kalenders
Kommunikationsbefehle	Anfordern des Ethernet Status
	Anfordern des Modems Status
	Anfordern des Logbuches eines Modems
	Anfordern des Logbuch eines Alarm Empfängers (ARC)
FlexC-Steuerung	Anfordern des Status eines FlexC Übertr.-sys. (ATS)
	Anfordern des Netzwerk Logbuches eines FlexC ATS
	Anfordern des Ereignis Logbuches eines FlexC ATS
	Anfordern des Logbuches eines FlexC ÜW
	Anfordern des Netzwerk Logbuches eines FlexC ÜW
	Export einer FlexC Ü.-System Konfigurationsdatei
	Import einer FlexC Ü.-System Konfigurationsdatei
	Löschen eines FlexC Übertragungssystems
	Löschen eines FlexC ÜW
	Löschen eines FlexC Ereignisprofils
	Löschen eines FlexC Steuerungsprofils
	Aufforderung zu einem Routineruf für einen ÜW
Zutrittskontrollsteuerung	Anfordern der Konfiguration für eine Tür
	Lese Status einer Tür
	Steuern einer Tür
	Anfordern Zutrittslogbuch
Verifizierungsbefehle	Lese Kamerabild
	Anfordern des Status einer Verifikationszone
	Anfordern der Daten einer Verifikationszone
	Daten werden zur Verifikationsmeldegruppe gesendet
Virtuelle Bedienteilsteuerungen	Bedienteil
Datei-Operationen	Upgrade der Zentralenfirmware
	Upgrade der Firmware der Peripherie
	Eine Konfigurationsdatei hochladen
	Eine Konfigurationsdatei herunterladen
	Sichern der Zentralen Konfiguration

	Rücksetzen der Zentrale
Legacy Steuerungen	Anfordern der Zentralen Information
	Anfordern des Zentralen Status
	Anfordern des Headers der Konfigurationsdatei
	Anfordern der Sprachkonfiguration
	Anfordern der Intruder Konfiguration
	Anfordern Status XBus Geräte
	Anfordern der Bereichskonfiguration

## 24.10 Zeiten für Übertragungssystemkategorien

Diese Tabelle enthält Beschreibungen der EN50136 ATS-Kategoriezeiten gemäß der Norm und Beschreibungen, wie die FlexC-Implementierung diese Norm erfüllt.

		EN50136 ATS Kategorie Zeitanforderungen				FlexC Implementierung der Zeitanforderungen der Kategorie des Übertragungssystems			
ATS- Katego- rie	Vorgeg- ebene Schnitts- stelle	Timeo- ut erneut Übertr- .	Primär Polling Timeo- ut	Backup ÜW Polling Timeout (Primär OK)	Backup ÜW Polling Timeout (Primäre r down)	Timeo- ut erneut Übertr- .	Primär Polling Timeo- ut	Backup ÜW Polling Timeout (Primär OK)	Backup ÜW Polling Timeout (Primäre r down)
SP1	Cat1 [Ethernet]	8 min	32 Tage	-	-	2 min	30 Tage	-	-
SP2	Cat2 [Ethernet]	2 min	25 h	-	-	2 min	24 h	-	-
SP3	Cat3 [Ethernet]	60 s	30 min	-	-	60 s	30 min	-	-
SP4	Cat4 [Ethernet]	60 s	3 min	-	-	60 s	3 min	-	-
SP5	Cat5 [Ethernet]	30 s	90 s	-	-	30 s	90 s	-	-
SP6	Cat6 [Ethernet]	30 s	20 s	-	-	30 s	20 s	-	-
DP1	Cat2 [Ethernet] Cat2 [Modem ]	2 min	25 h	50 h	25 h	2 min	24 h	24 h 30 min	24 h 10 min
DP2	Cat3 [Ethernet] Cat3 [Modem ]	60 s	30 min	25 h	30 min	60 s	30 min	24 h 30 min	30 min
DP3	Cat4 [Ethernet]	60 s	3 min	25 h	3 min	60 s	3 min	24 h 30 min	3 min

	et] Cat4 [Modem ]								
DP4	Cat5 [Ethernet] Cat5 [Modem ]	30 s	90 s	5 h	90 s	30 s	90 s	4 h 10 min	90 s

## 24.11 ÜW Kategorie Zeiteinstellung

Die folgende Tabelle enthält die Einstellungen, die auf Ereigniszeitüberschreitungen, Polling-Intervalle (aktiv und inaktiv) sowie Polling-Zeitüberschreitungen (aktiv und inaktiv) für jede ÜW-Kategorie angewendet werden. Für das Ethernet sind Polling-Intervall und Wiederholungsintervall identisch. Zur Reduzierung der Kosten für GPRS-Anrufe unterscheiden sich das Intervall und das Wiederholungsintervall für GPRS-Pfade. Beispielsweise ruft Cat3 [Modem] alle 25 Minuten ab und anschließend alle 60 s für 5 Minuten, bis nach 30 Minuten eine Zeitüberschreitung eintritt. Eine visuelle Übersicht der konfigurierten Polling-Intervalle finden Sie unter **Stats > FlexC > Netzwerk Anmeldung**.



Wenn ein ÜW eingeschaltet und aktiv ist und anschließend ausfällt, bleiben die Polling-Raten für zwei weitere Polling-Zyklen aktiv, bis auf die Polling-Intervalle **ATP down** (ÜW ausgefallen) gewechselt wird.

<i>Übertragungsweg-Kategorien</i>		Polling wenn der Übertragungsweg aktiv ist			Polling wenn der Übertragungsweg inaktiv ist			Polling wenn der Übertragungsweg unterbrochen ist	
ÜW Kategorie	Ereignis Timeout	Polling-Intervall I	Wiederholungsintervall II	Polling Timeout	Polling-Intervall I	Wiederholungsintervall II	Polling Timeout	Polling Intervall	Zeitüberschreitung
Cat6 [Ethernet]	30 s	8 s	30 s	20 s	8 s	30 s	20 s	30 s	30 s
Cat5 [Ethernet]	30 s	10 s	30 s	90 s	10 s	30 s	90 s	30 s	30 s
Cat4 [Ethernet]	60 s	30 s	30 s	3 min	30 s	30 s	3 min	30 s	30 s
Cat3 [Ethernet]	60 s	60 s	60 s	30 min	60 s	60 s	30 min	60 s	30 s
Cat2A [Ethernet]	2 min	2 min	2 min	4 h	2 min	2 min	4 h	2 min	30 s
Cat2 [Ethernet]	2 min	2 min	2 min	24 h	2 min	2 min	24 h	2 min	30 s
Cat1 [Ethernet]	2 min	2 min	2 min	30 Tage	2 min	2 min	30 Tage	2 min	30 s
<i>Modem ATP Kategorien</i>									
Cat5	30 s	10 s	30 s	90 s	4 h	2 min	4 h	10 mi	90 s

[Modem]							10 min	n	
Cat4A [Modem]	60 s	60 s	60 s	3 min	4 h	2 min	4 h 10 min	30 mi n	90 s
Cat4 [Modem]	60 s	60 s	60 s	3 min	24 h	2 min	24 h 30 min	1 h	90 s
Cat3 [Modem]	60 s	25 min	60 s	30 min	24 h	2 min	24 h 30 min	4 h	90 s
Cat2A [Modem]	2 min	4 h	2 min	4 h 10 min	24 h	2 min	24 h 30 min	4 h	90 s
Cat2 [Modem]	2 min	24 h	2 min	24 h 10 min	24 h	2 min	24 h 30 min	24 h	90 s
Cat1 [Modem]	2 min	24 h	10 min	25 h	30 Tage	10 min	30 Tage 1 h	7 Tag e	90 s

Herausgegeben von  
Vanderbilt

Clonshaugh Business and Technology Park  
Clonshaugh  
Dublin  
D17 KV84  
[www.service.vanderbiltindustries.com](http://www.service.vanderbiltindustries.com)

© Vanderbilt, 2015  
Liefermöglichkeiten und technische Änderungen vorbehalten.