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

Installations- und Konfigurationshandbuch

3.6

A6V10271081
01.05.2016

Vanderbilt

Urheberrecht

Technische Spezifikationen und Verfügbarkeit können ohne vorherige Ankündigung geändert werden.

Ausgabe: 01.05.2016

Dokument-ID: A6V10271081

Inhalt

1 Bedeutung der Symbole

Im vorliegenden Dokument werden verschiedene Symbole verwendet:

Symbol	Beschreibung
SPC4xxx	Nicht verfügbar für SPC42xx, SPC43xx.
IP	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 Sicherheit

2.1 Zielgruppe

Die Anweisungen in dieser Dokumentation richten sich an folgende Zielgruppen:

Zielgruppe	Qualifikation	Aktivität	Gerätezustand
Installationspersonal	Technische Ausbildung für Gebäude- oder Elektroinstallationen.	Montiert und installiert die Hardwarekomponenten vor Ort.	Einzelne Komponenten, die montiert und installiert werden müssen.
Inbetriebnahmepersonal	Adäquate technische Schulung in Bezug auf die Aufgaben und Produkte, Geräte oder Systeme, die in Betrieb genommen werden sollen	Inbetriebnahme des Geräts oder Systems, das vor Ort bereits montiert ist	Neue, fertig montierte und installierte Geräte oder modifizierte Geräte.

2.2 Allgemeine Sicherheitshinweise

⚠ WARNUNG

Lesen Sie vor der Installation und Verwendung dieses Geräts die Sicherheitshinweise. Dieses Gerät darf nur an Stromquellen angeschlossen werden, die der Norm EN60950-1, Kapitel 2.5 („begrenzte Stromquelle“) entsprechen.

2.2.1 Allgemeine Informationen

- Bewahren Sie dieses Dokument für zukünftige Zwecke auf.
- Geben Sie dieses Dokument immer zusammen mit dem Produkt weiter.
- Beachten Sie bitte alle zusätzlichen länderspezifischen Sicherheitsnormen oder -vorschriften hinsichtlich Projektplanung, Betrieb und Entsorgung des Produkts.

Haftungsanspruch

- Schließen Sie das Gerät nicht an das 230-V-Stromnetz an, falls es beschädigt ist oder Teile fehlen.
- Nehmen Sie nur solche Änderungen oder Modifikationen am Gerät vor, die in diesem Handbuch ausdrücklich erwähnt werden und vom Hersteller genehmigt sind.
- Verwenden Sie ausschließlich vom Hersteller zugelassene Ersatz- und Zubehörteile.

2.2.2 Transport

Transportschäden

- Bewahren Sie das Verpackungsmaterial für einen zukünftigen Transport auf.

- Setzen Sie das Gerät keinen mechanischen Erschütterungen oder Stößen aus.

2.2.3 Konfiguration

Funkstörungen im Umfeld anderer Geräte / EMV

- Beachten Sie beim Umgang mit Modulen, bei denen es zu elektrostatischen Entladungen kommen kann, bitte die ESD-Richtlinien.

Schäden aufgrund eines ungeeigneten Montageortes

- Beachten Sie die vom Hersteller empfohlenen Umgebungsbedingungen. Siehe Technische Daten.
- Betreiben Sie das Gerät nicht in der Nähe starker elektromagnetischer Strahlung.

Stromschlaggefahr aufgrund eines unzulässigen Anschlusses

- Schließen Sie das Gerät nur an Stromquellen mit der vorgeschriebenen Spannung an. Angaben zur Versorgungsspannung finden Sie auf dem Typenschild.
- Stellen Sie sicher, dass das Gerät ständig an der Stromversorgung angeschlossen ist und eine leicht zugängliche Trennvorrichtung vorhanden ist.
- Stellen Sie sicher, dass der Stromkreis, an den das Gerät angeschlossen ist, mit einer 16-A-Sicherung (max.) abgesichert ist. Schließen Sie keine Geräte aus anderen Systemen an diese Sicherung an.
- Dieses Gerät ist für den Betrieb an Stromversorgungen mit TN-System ausgelegt. Schließen Sie das Gerät nicht an eine andere Stromversorgung an.
- Die elektrische Erdung muss den jeweils geltenden Sicherheitsnormen und -vorschriften entsprechen.
- Primäre Versorgungskabel und sekundäre Kabel sind so zu verlegen, dass sie nicht parallel verlaufen, sich kreuzen oder im Gehäuse gegenseitig berühren.
- Telefonkabel sind von anderen Kabeln separiert in die Einheit zu führen.

Gefahr von Kabelschäden durch Belastung!

- Stellen Sie sicher, dass alle abgehenden Kabel und Drähte ausreichend zugentlastet sind.

2.2.4 Betrieb

Gefahrensituation aufgrund eines Fehlalarms

- Achten Sie darauf, vor dem Testen des Systems alle maßgeblichen Beteiligten und Hilfe leistenden Behörden zu verständigen.
- Um Panik zu vermeiden, sollten vor dem Testen von Alarmvorrichtungen stets alle Anwesenden informiert werden.

2.2.5 Service und Wartung

Gefahr von Elektroschocks bei der Wartung

- Die Wartung muss von geschulten Fachleuten durchgeführt werden.
- Trennen Sie vor der Durchführung von Wartungsarbeiten stets das Netzkabel sowie sonstige Kabel von der Stromversorgung ab.

Gefahr von Elektroschocks beim Reinigen des Geräts

- Verwenden Sie keine Flüssigreiniger oder Sprays, die Alkohol, Spiritus oder Ammoniak enthalten.

2.3 Bedeutung der schriftlichen Warnhinweise

Signalwort	Art des Risikos
GEFAHR	Gefahr einer schweren oder sogar tödlichen Verletzung.
WARNUNG	Mögliche Gefahr einer schweren oder sogar tödlichen Verletzung.
VORSICHT	Gefahr einer leichten Verletzung oder eines Sachschadens
WICHTIG	Gefahr von Fehlfunktionen

2.4 Bedeutung der Gefahrensymbole

	⚠ WARNUNG
	Warnung vor einem Gefahrenbereich

	⚠ WARNUNG
	Warnung vor gefährlicher elektrischer Spannung

3 Richtlinien und Normen

3.1 EU-Richtlinien

Dieses Produkt erfüllt die Anforderungen der EU-Richtlinien 2004/108/EG „Elektromagnetische Verträglichkeit“, 2006/95/EG „Niederspannungsrichtlinie“ und 1999/5/EG „Funkanlagen und Telekommunikationsendeinrichtungen“. Die EU-Konformitätserklärung ist für alle verantwortlichen Vertretungen verfügbar unter http://pcd.vanderbiltindustries.com/doc/SPC

Europäische Richtlinie 2004/108/EG „Elektromagnetische Verträglichkeit“

Die Einhaltung der EU-Richtlinie 2004/108/EG wurde in Tests gemäß folgender Normen nachgewiesen:

EMV-Emission	EN 55022 Klasse B
EMV-Verträglichkeit	EN 50130-4

Europäische Richtlinie 2006/95/EG “Niederspannungsrichtlinie”

Die Einhaltung der EU-Richtlinie 2006/95/EG wurde in Tests gemäß folgender Norm nachgewiesen:

Sicherheit	EN 60950-1

3.1.1 Überblick über EN50131-Konformität

Dieser Abschnitt vermittelt einen Überblick darüber, wie weit SPC die EN-Norm 50131 erfüllt.

Adresse der Zertifizierungsstelle
VDS (VDS A / C / EN / SES Approval) AG Köln HRB 28788 Sitz der Gesellschaft: Amsterdamer Str. 174, 50735 Köln Geschäftsführer: Robert Reinermann JörgWilms-Vahrenhorst (Stv.)

SPC-Produkte wurden aufgeführt geprüft nach EN50131-3: 2009 und alle relevanten RTC-Spezifikationen.

Produkttyp	Norm
● SPC6350.320 ● SPC6330.320 ● SPC5350.320 ● SPC5330.320 ● SPCP355.300 ● SPCP333.300 ● SPCE652.100 ● SPCK420.100 ● SPCK421.100 ● SPCE452.100 ● SPCE110.100 ● SPCE120.100 ● SPCA210.100 ● SPCK620.100	EN50131 Grad 3

● SPCK623.100 ● SPCN110.000 ● SPCN310.000	
● SPC5320.320 ● SPC4320.320 ● SPCP332.300	EN50131 Grad 2

Angaben in Bezug auf die Einhaltung der Anforderungen der EN50131 sind in den folgenden Abschnitten des vorliegenden Dokuments enthalten.

EN50131-Anforderung	SPC Installations- und Konfigurationshandbuch
Betriebstemperatur und Luftfeuchtigkeit	SPC4000 – Technische Daten [→ 33] SPC5000 – Technische Daten [→ 35] SPC6000 – Technische Daten [→ 37]
Gewicht und Abmessungen	SPC4000 – Technische Daten [→ 33] SPC5000 – Technische Daten [→ 35] SPC6000 – Technische Daten [→ 37]
Befestigung	Montage der Systemkomponenten [→ 42]
Installations-, Inbetriebnahme- und Wartungsanleitung einschließlich Anschlussidentifizierung	Montage der Systemkomponenten [→ 42] Controller-Hardware [→ 67]
Verbindungsarten (siehe 8.8);	SPC4000 – Technische Daten [→ 33] SPC5000 – Technische Daten [→ 35] SPC6000 – Technische Daten [→ 37] Verdrahtung der X-Bus-Schnittstelle [→ 74]
Möglichkeiten zum Scharfschalten und Unscharfschalten (siehe 11.7.1 bis 11.7.3 und Tabellen 23 bis 26);	Benutzerprogrammierung über das Bedienteil Bereiche – Scharf-/Unscharfschalten [→ 263] Konfigurieren eines Schlüsselschalter-Erweiterungsmoduls [→ 222] Konfigurieren einer Fernbedienung [→ 112] Trigger [→ 277]
Zu wartende Teile	SPC4000 – Technische Daten [→ 33] SPC5000 – Technische Daten [→ 35] SPC6000 – Technische Daten [→ 37]
Energieversorgunganforderungen bei Systemen ohne integrierte Energieversorgung	Siehe Installationsanleitung für SPCP33x und SPCP43x PSU-Erweiterungsmodule.
Bei integrierter Energieversorgung, erforderliche Angaben nach EN 50131-6:2008, Teil 6	SPC4000 – Technische Daten [→ 33] SPC5000 – Technische Daten [→ 35] SPC6000 – Technische Daten [→ 37]
Maximale Anzahl der verschiedenen Transponder und Erweiterungsmodule.	Verdrahtung der X-Bus-Schnittstelle [→ 74] SPC4000 – Technische Daten [→ 33] SPC5000 – Technische Daten [→ 35] SPC6000 – Technische Daten [→ 37]
Stromaufnahme des CIE und der einzelnen Transponder und Erweiterungsmodule mit und ohne Alarmbedingung.	Siehe relevante Installationsanleitung.
Maximaler Nennstrom der einzelnen	SPC4000 – Technische Daten [→ 33]

EN50131-Anforderung	SPC Installations- und Konfigurationshandbuch
elektrischen Ausgänge	SPC5000 – Technische Daten [→ 35] SPC6000 – Technische Daten [→ 37]
Programmierbare Funktionen	Technikerprogrammierung über das Bedienteil [→ 115] Technikerprogrammierung über den Browser [→ 170]
Wie der Zugriff auf Anzeigen für Benutzer der Ebene 1 verwehrt wird, wenn Benutzer der Ebenen 2, 3 oder 4 nicht länger auf die Informationen zugreifen (siehe 8.5.1).	Benutzeroberfläche des Bedienteils [→ 94] Einstellungen des Standard-Bedienteils [→ 127] Einstellungen des Komfort-Bedienteils [→ 128] Konfigurieren eines Anzeigemoduls [→ 221]
Maskieren/Reduzieren von Bereichssignalen/-meldungen, die als „Fehlerereignis“ oder „Maskiererereignis“ verarbeitet werden (siehe 8.4.1, 8.5.1 und Tabelle 11);	Systemoptionen [→ 239] Verdrahtung Linieneingänge [→ 86] SIA-Codes [→ 365] PIR-Maskierung wird immer als Meldergruppen-Maskiererereignis gemeldet (SIA – ZM). Zusätzlich kann die Anti-Maskierfunktion (Anti-Mask) je nach Konfiguration einen Alarm auslösen, Sabotage oder eine Störung melden oder keine weiteren Aktionen initiieren. Aktuelle Standardeinstellungen bei zusätzlichem PIR: **Irland**: Unscharf – keine Scharf – Alarm **UK, Europa, Schweden, Schweiz, Belgien**: Unscharf – Sabotage Scharf – Alarm
Priorisierung der Verarbeitung und Anzeige von Signalen und Meldungen (siehe 8.4.1.2, 8.5.3);	Anzeige des Standard-Bedienteils [→ 96] Anzeige des Komfort-Bedienteils [→ 100]
Minimale Anzahl von Abweichungen bei PIN-Codes, logischen Schlüsseln, biometrischen Schlüsseln und/oder mechanischen Schlüsseln für jeden Benutzer (siehe 8.3);	Benutzer-PIN-Kombinationen [→ 371]
Methode zur Zeitbegrenzung interner WD für Level-3-Zugang ohne Level-2-Autorisierung (siehe 8.3.1);	Nicht unterstützt – Der Techniker kann nur mit Erlaubnis auf das System zugreifen.
Anzahl von und Informationen zu nicht zulässigen PIN-Codes (siehe 8.3.2.2.1);	Automatische Sperren [→ 372]
Informationen zu den verwendeten biometrischen Autorisierungsmethoden (siehe 8.3.2.2.3);	Nicht zutreffend
Zur Bestimmung der Anzahl der Kombinationen von PIN-Codes, logischen Schlüsseln, biometrischen Schlüsseln und/oder mechanischen Schlüsseln verwendete Methode (siehe 11.6);	Benutzer-PIN-Kombinationen [→ 371]
Anzahl der ungültigen Code-Eingaben bis zur Sperrung der Benutzerschnittstelle (siehe 8.3.2.4);	Zugangs-PINs [→ 372]
Informationen zu Möglichkeiten der temporären Autorisierung des	Benutzermenüs – Zugriff gewähren

EN50131-Anforderung	SPC Installations- und Konfigurationshandbuch
Benutzerzugangs (siehe 8.3.2);	
Bei automatischer Scharfstellung zu voreingestellten Zeiten: Informationen zur Anzeige der Voreinstellungen und automatisches Außerkraftsetzen der Vermeidung der Scharfstellung (siehe 8.3.3, 8.3.3.1);	Bereiche – Scharf-/Unscharfschalten [→ 263]
Informationen zu Bedingungen für die Scharfschaltung (siehe 8.3.3.4);	Das System scharf und unscharf schalten Konfiguration des Standard-Bedienteils [→ 127] Konfiguration des Komfort-Bedienteils [→ 128] Ausgänge [→ 212] Meldergruppentypen [→ 375]
Ausgangssignalbenachrichtung oder Meldungen (siehe 8.6);	Ausgänge [→ 212] Bereiche – Scharf-/Unscharfschalten [→ 263] Benutzerrechte [→ 200]
Sonstige Ausgangskonfigurationen zum Anschluss von I&HAS-Komponenten (siehe 8.2);	Ausgänge [→ 212] Meldergruppentypen [→ 375] Test [→ 154] Benutzeroberfläche des Bedienteils [→ 94]
Kriterien für das automatische Entfernen des „Dauertest“-Attributs (siehe 8.3.9);	Timer [→ 248]
Anzahl der Ereignisse, die zur automatischen Sperre führen	Automatische Sperren [→ 372]
Für Transponder vom Typ A oder Typ B (siehe 8.7) und portabel oder beweglich (siehe 11.14);	Alle Geräte sind fest verdrahtet und werden über Systemnetzteile mit Strom versorgt. Siehe relevante technische Daten zu Netzteilen.
Komponentendaten für Festspeicherkomponenten (siehe Tabelle 30, Schritt 6);	Weitere Informationen über die Bedienteile SPCK420/421 und SPCK620/623 finden Sie in der Anwenderdokumentation.
Lebensdauer der Speicherbatterie (siehe 8.10.1);	N/V In Festspeichern gespeichert.
Optionale Funktionen (siehe 4.1);	Technikerprogrammierung über das Bedienteil Technikerprogrammierung über den Browser [→ 170]
Zusatzfunktionen (siehe 4.2, 8.1.8);	Sicherheitsgrad – Unbeschränkt Richtlinien – Systemoptionen [→ 239]
Erforderliche Zugangslevel für den Zugriff auf die Zusatzfunktionen;	Benutzerkonfiguration (Bedienteil) [→ 161] Benutzerkonfiguration (Browser) [→ 196]
Informationen zu programmierbaren Vorrichtungen, die bei Einbruch- und Überfallmeldeanlagen zu einer Nichteinhaltung der Anforderungen der EN 50131-1:2006, 8.3.13 oder zu einem geringeren Sicherheitsgrad führen; mit Anleitung zum Entfernen der Konformitätskennzeichnung (siehe 4.2 und 8.3.10).	Sicherheitsgrad – Unbeschränkt Richtlinien – Systemoptionen [→ 239] EN50131-Konformität [→ 19]

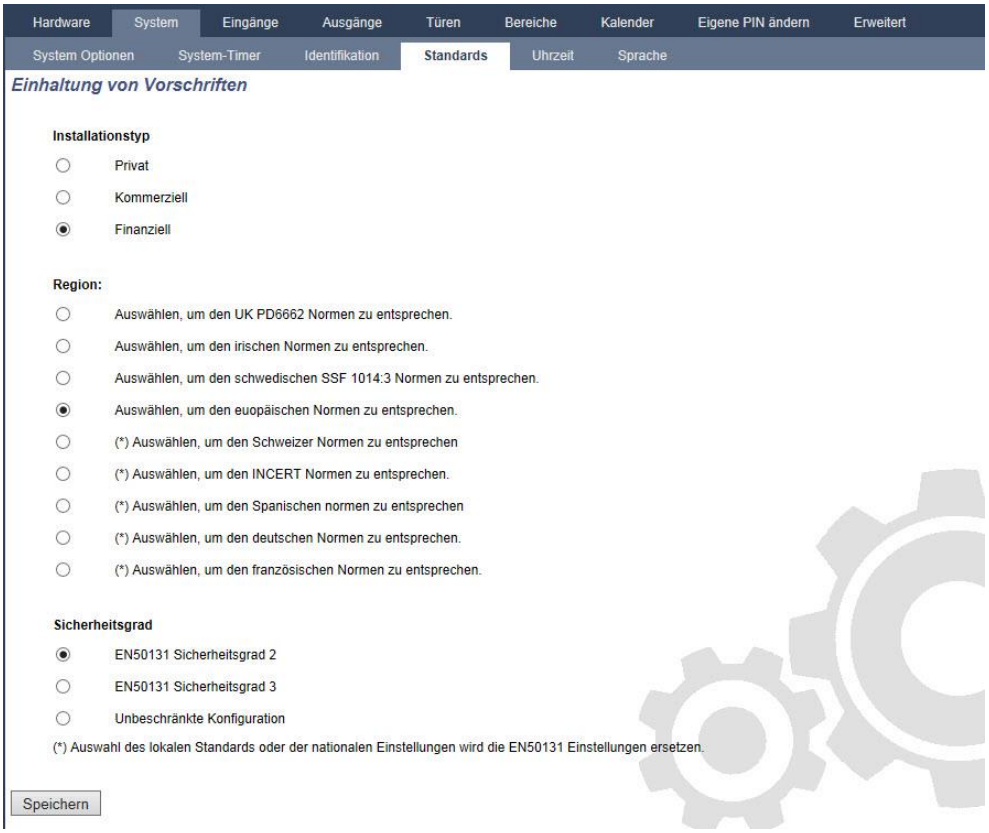
SPC Produkte nach EN50131-6 aufgeführt wurden getestet, und alle relevanten RTC-Spezifikationen.

Produkttyp	Norm
● SPC6350.320 ● SPC6330.320 ● SPC5350.320 ● SPC5330.320 ● SPCP355.300 ● SPCP333.300 ● SPCP355.300 ● SPCE652.100 ● SPCK420.100 ● SPCK421.100 ● SPCE452.100 ● SPCE110.100 ● SPCE120.100 ● SPCA210.100 ● SPCK620.100 ● SPCK623.100 ● SPCN110.000 ● SPCN310.000	EN50131-6
● SPC5320.320 ● SPC4320.320 ● SPCP332.300	EN50131-6

3.1.2 Einhaltung der Zulassungsanforderungen gemäß EN50131

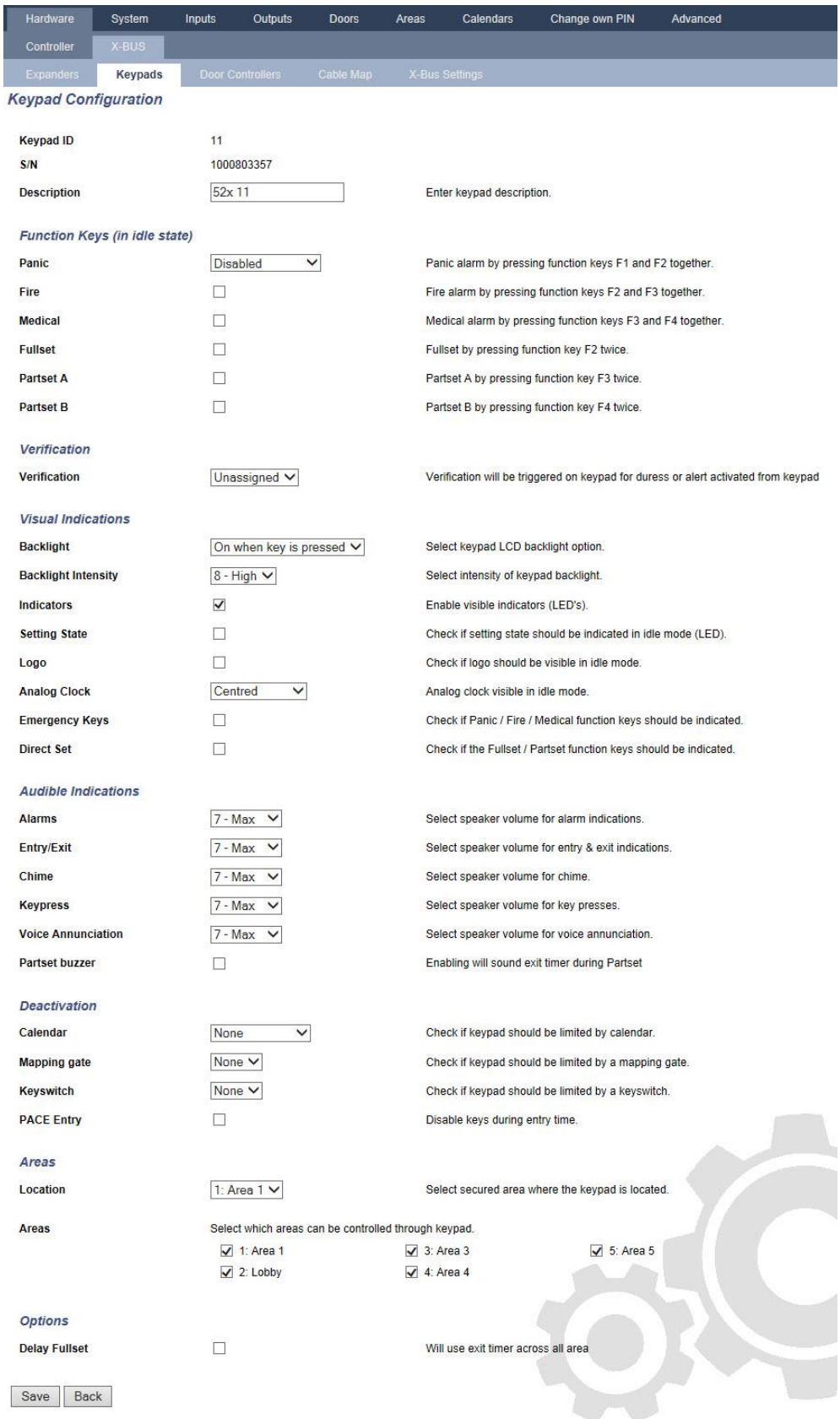
Softwarevoraussetzungen

Es ist nicht möglich, die Region oder den Grad in SPC Pro zu ändern. Es ist nur möglich, diese Einstellungen im Browser oder am Bedienteil zu ändern.



- Wählen Sie auf der Einstellungsseite **Standards** unter **Region** die Option **Europa**, um die EN50131-Anforderungen zu implementieren.
- Wählen Sie die Option **Grad 2** oder **Grad 3**, um den Grad der EN50131-Konformität zu implementieren.
- Die **Funkeinstellungen Funk Scharfsch.verhinderung** und **Funküberwachung** müssen auf einen anderen Wert als 0 eingestellt sein.
- Wählen Sie in den Einstellungen **Uhr** die Option **Synchronisierungszeit mit Netz**, um das Netz als Uhr-Master zu verwenden.

- Wählen Sie in den Konfigurationseinstellungen des **Bedienteils** für **Optische Indikation** NICHT das Attribut **Schärfungszustand**.



Hardwarevoraussetzungen

- Der rückwärtige Sabotageschalter (SPCY130) muss für Zentralen und Stromversorgungen zur Konformität mit EN50131 Grad 3 montiert werden.

- Mit EN50131 Grad 3 konforme Komponenten dürfen nur in Systemen montiert werden, die mit EN50131 Grad 3 konform sind.
- Mit EN50131 Grad 2 oder Grad 3 konforme Komponenten dürfen in Systemen montiert werden, die mit EN50131 Grad 2 konform sind.
- Es ist nicht möglich, ein Drahtlosgerät mit einer Signalstärke von weniger als 3 anzumelden.
- Als Verhältnis werden 20 Transmitter für 1 Empfänger empfohlen.
- Für Glasbruch-Funktionen muss eine Glasbruch-Schnittstelle verwendet werden, die die Euronorm erfüllt.
- Um EN50131-3:2009 zu erfüllen, darf das System weder mit der SPCE120 (Anzeigemodul-Erweiterung) noch mit der SPCE110 (Schlüselschalter-Erweiterung) scharf oder unscharf geschaltet werden.

	HINWEIS
	Das SPCN110 PSTN-Modul und das SPCN130 GSM/GPRS-Modul werden mit Zentralen gemäß EN50131 Grad 2 und Grad 3 getestet und können mit diesen zulässigen Zentralen verwendet werden.

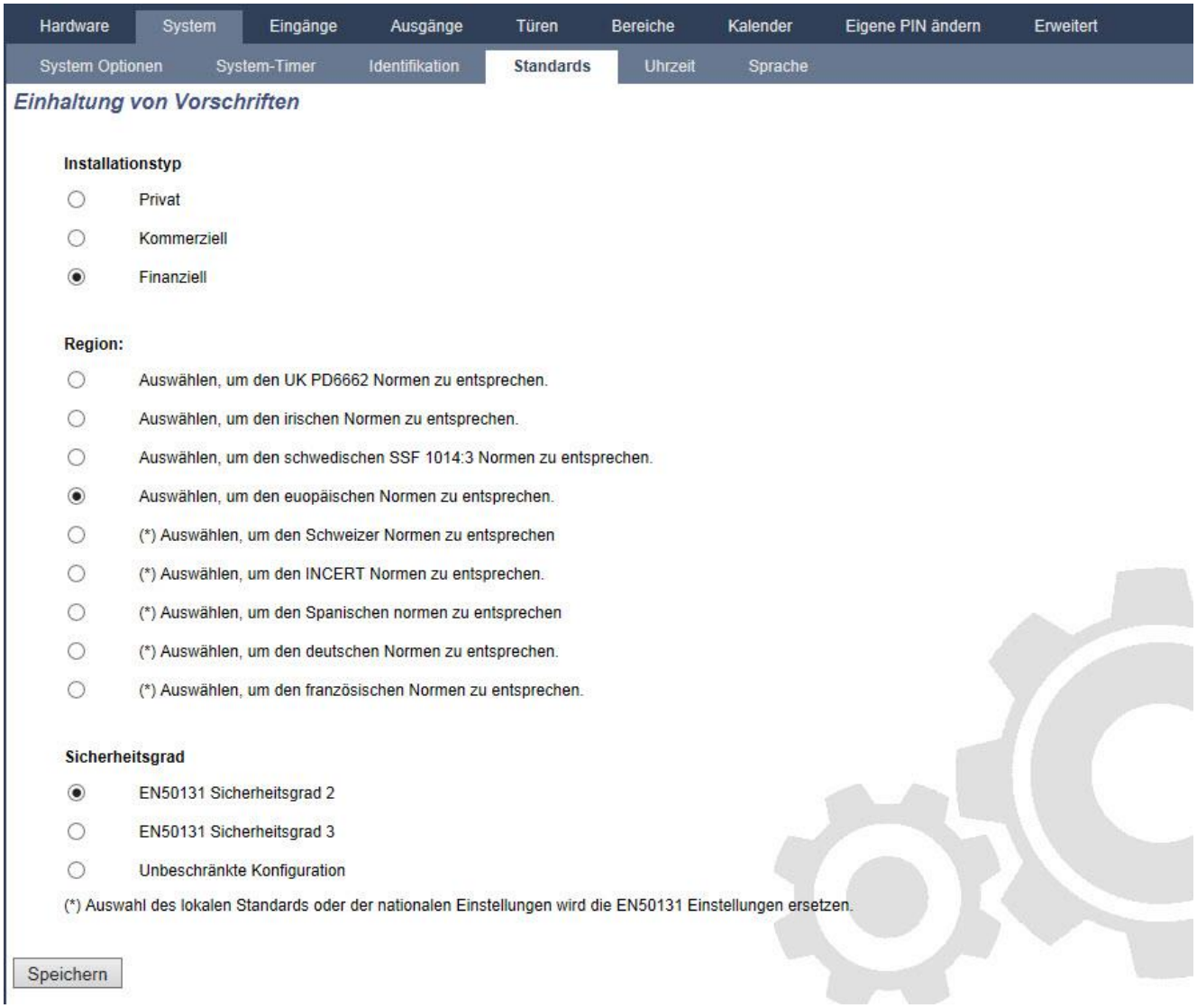
3.1.3 Einhaltung der EN 50136-1: 2012 und EN 50136-2: 2014

Die aufgelisteten SPC-Produkte wurden gemäß EN 50136-1: 2012 und EN 50136-2: 2014

3.1.4 Konformität mit INCERT-Zulassungen

Softwarevoraussetzungen

Die Auswahl von „Belgien (*)“ unter **Region** implementiert die lokalen und nationalen Anforderungen, die die EN50131-Anforderungen übersteigen.



Durch die Auswahl von **Grad 2** oder **Grad 3** wird die EN50131-Konformität mit zusätzlichen INCERT-Anforderungen ausgewählt:

- Nur ein Techniker kann eine Sabotage quittieren. Bei INCERT gilt dies für alle Grade.
  Das ist normalerweise nur eine Anforderung für EN50131 Grad 3.
- Eine Sabotage in einer gesperrten/isolierten MG muss einem Empfänger gemeldet werden und wird dem Benutzer angezeigt.
  Bei INCERT werden Sabotagen für isolierte MGs verarbeitet. Bei allen anderen Normvariationen werden die Sabotagen in isolierten MGs ignoriert.
- Benutzer-PINs müssen mit mehr als 4 Stellen definiert werden.

Hardwarevoraussetzungen

- Die minimale Akkukapazität für SPC42xx/43xx/52xx/53xx/63xx beträgt 10 Ah/12 V. Wird ein Akku mit 10 Ah verwendet, wird der Akku zur linken Gehäuseseite geneigt, und die untere Lasche wird so gebogen, dass sie den Akku hält.
- Den Jumper (J12) auf der Batterieauswahl für die zu verwendende 17/10 Ah-Batterie anbringen und für die 7 Ah-Batterie entfernen.
- Die Strommenge am Zusatzausgang bei Verwendung einer 10-Ah-Batterie für SPC42xx/SPC52xx beträgt:

KOMM	KEINE	PSTN	GSM	PSTN+GSM

Standby-Zeit				
12 Std.	568 mA	543 mA	438 mA	413 mA
24 Std.	214 mA	189 mA	84 mA	59 mA
30 Std.	143 mA	118 mA	13 mA	n.r.
60 Std.	2 mA	n.r.	n.r.	n.r.

- Die Strommenge am Zusatzausgang bei Verwendung eines 10-Ah-Akkus für SPC43xx/SPC53xx/SPC63xx beträgt:

KOMM Standby-Zeit	KEINE	PSTN	GSM	PSTN+GSM
12 Std.	538 mA	513 mA	408 mA	383 mA
24 Std.	184 mA	159 mA	54 mA	29 mA
30 Std.	113 mA	88 mA	n.r.	n.r.
60 Std.	n.r.	n.r.	n.r.	n.r.

3.1.5 Richtlinien zur Einhaltung von PD 6662:2010

Dieser Anhang enthält alle Kriterien für die Installation, Inbetriebnahme und Wartung des SPC-Systems gemäß der Norm PD 6662:2010.

3.1.5.1 Produktumfang

Der Umfang dieses Dokuments gilt für die folgenden Komponenten des SPC-Systems:

SPC4320.320-L1-Grad 2-Controller
SPC5320.320-L1-Grad 2-Controller
SPC5330.320-L1-Grad 3-Controller
SPC5350.320-L1 Grad 3 Controller
SPC6330.320-L1 Grade 3 Controller
SPC6350.320-L1 Grad 3 Controller
SPCK420/421.100-LCD-Bedienteil
SPCE452.100-Erweiterungsmodul, 8 Relaisausgänge
SPCE652.100-Erweiterungsmodul, 8 Eingänge/2 Ausgänge
SPCP332.300 Smart-Netzteil mit E/A-Erweiterungsmodul
SPCP355.300 Strom-versorgungseinheit mit erweiterungsmodul, 8 Eingänge/2 Ausgänge
SPCP333.300 Smart-Netzteil mit E/A-Erweiterungsmodul
SPCN110.000 PSTN-Modul
SPCN310.000 GSM-Modul

3.1.5.2 Normenübersicht

Richtlinien für die Implementierung der Norm PD 6662:2010 für ein SPC System werden gemäß den folgenden relevanten Normen bereitgestellt:

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

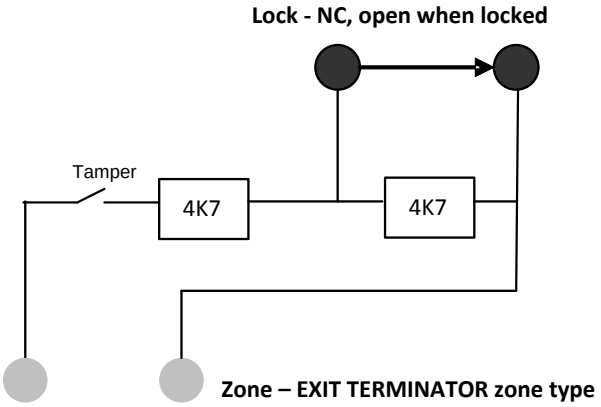
3.1.5.3 Methoden zur Scharf- und Unscharfschaltung

3.1.5.3.1 Methoden zur Scharfschaltung (BS 8243:2010 – Klausel 6.3)

Der Abschluss/die Beendigung der externen Scharfschaltung wird mithilfe folgender Methoden erreicht:

a) Shunt-Schloss, an der endgültigen Ausgangstür angebracht

Ein Shunt-Schloss muss von einem Techniker wie folgt montiert werden:



Für SPC muss der Meldergruppentyp ABBRUCH SCHARFSCHALTUNGSVERZÖGERUNG konfiguriert werden.

Weitere Informationen finden Sie im folgenden Abschnitt dieses Handbuchs:

Meldergruppentypen [➙ 375]

b) Druckknopfschalter, außerhalb des überwachten Geländes angebracht

Schließen Sie den Druckknopf wie folgt an einen SPC-Meldergruppeneingang an:

Für SPC muss der Meldergruppentyp ABBRUCH SCHARFSCHALTUNGSVERZÖGERUNG konfiguriert werden.

Weitere Informationen finden Sie im folgenden Abschnitt dieses Handbuchs:

Meldergruppentypen [➙ 375]

c) Schutzschalter (d. h. Türkontakt), an der endgültigen Ausgangstür des scharf geschalteten Geländes oder Bereichs

Schließen Sie den Schalter wie folgt an das SPC-System an:

Der Kontakt wird an der endgültigen Ausgangstür angebracht und mit einer EINBRUCH VERZÖGERT-Meldergruppe mit ‚Ext. Zeitabbr.'-Attribut verbunden.

Weitere Informationen finden Sie im folgenden Abschnitt dieses Handbuchs:

Meldergruppentypen [➙ 375]
MG-Attribute [➙ 378]

Ein Fehlbetriebssignal kann mit Hilfe einer Alarmabbruchsfunktion ausgegeben werden. Diese Funktion ist standardmäßig aktiviert.

Weitere Informationen finden Sie im folgenden Abschnitt dieses Handbuchs:

OPTIONEN [➙ 116] (Bedienteil)

Optionen [→ 239] (Browser)

d) Digitaler Schlüssel

Nicht unterstützt von SPC.

e) In Verbindung mit einem Empfänger

Diese Einstellungsmethode wird unter Verwendung eines SPC COM XT oder einer Empfängersoftware eines Drittherstellers, die EDP-Befehle verwendet, unterstützt.

3.1.5.3.2 Methoden zur Unscharfschaltung (BS 8243:2010 – Klausel 6.4)

Die Methoden zur Unscharfschaltung werden wie folgt eingehalten:

6.4.1 Für alle Methoden zur Unscharfschaltung im SPC-System gibt es ein akustisches Signal, das dem Benutzer die erfolgreiche Unscharfschaltung des Systems angibt. Dabei handelt sich um eine Pieptonsequenz vom CIE.

6.4.2 Verhinderung des Zutritts zum überwachten Gebäude, bevor das Einbruchalarmsystem (IAS) unscharf geschaltet wurde:

a) Ein Entriegeln der ersten Eingangstür verursacht die Unscharfschaltung des IAS;

Konformität durch SPC, wenn S/U EINGANG-Meldergruppe nur mit dem UNSCHARF-Attribut verwendet wird. Dieser Meldergruppentyp darf nicht für die Scharfschaltung verwendet werden.

b) Die Unscharfschaltung des IAS durch den Benutzer vor dem Zutritt zum überwachten Gebäude verursacht und erlaubt die Entriegelung der ersten Eingangstür.

Konformität durch SPC und Unscharfschaltung mithilfe eines Ausweises am Eintrittsleser mit der UNSCHARF-Option, oder durch Eingabe eines Drittherstellerzutrittssystems in einer EINGANG-Meldergruppe mit UNSCHARF-Attribut.

6.4.3 Verhinderung des Zutritts zum überwachten Gebäude, bevor alle Mittel zur Einbruchalarmbestätigung deaktiviert wurden:

a) Eine Entriegelung der ersten Eingangstür verursacht, dass alle Bestätigungsmittel deaktiviert werden.

Betrieb nicht durch SPC erlaubt.

b) Die Deaktivierung aller Mittel zur Bestätigung durch den Benutzer vor dem Zutritt zum überwachten Gebäude verursacht und erlaubt die Entriegelung der ersten Eingangstür.

Betrieb nicht durch SPC erlaubt.

6.4.4 Das Öffnen der ersten Eingangstür deaktiviert alle Mittel zur Einbruchalarmbestätigung.

Betrieb nicht durch SPC erlaubt.

6.4.5 Abschluss der Unscharfschaltung mithilfe eines digitalen Schlüssels

a) Benutzung eines digitalen Schlüssels vor dem Zutritt zum überwachten Gebäude (z. B. über Funk)

SPC erfüllt diese Klausel, wenn der Installateur einen TRANSPONDER-Leser (z. B. SPCK421) außen am Gebäude installiert.

b) Benutzung eines digitalen Schlüssels nach dem Zutritt zum überwachten Gebäude von einem Standort aus, der so nahe wie praktisch möglich an der ersten Eingangstür liegt.

Diese Funktion wird durch die Nutzung eines TRANSPONDER-Lesers (z. B. SPCK421) nahe der Eingangstür des Gebäudes ermöglicht.

Weitere Informationen finden Sie in den folgenden Abschnitten dieses Handbuchs:

- Meldergruppentypen [→ 375]
- MG-Attribute [→ 378]

⚠ WARNUNG

Sie müssen darauf achten, dass durch das Zulassen dieser Methode zur Unscharfschaltung die Polizei nicht gerufen wird, wenn ein Einbrecher die erste Eingangstür aufbrechen kann. Dabei ist das weitere Vordringen des Einbrechers in das Gebäude unwichtig.

Diese Methode zur Unscharfschaltung des Einbruchalarmsystems könnte für Ihren Versicherer nicht akzeptabel sein.

6.4.6 Unscharfschaltung in Verbindung mit einem Empfänger (ARC)

Konformität durch SPC mithilfe der ARC-Software eines Drittanbieters Eine Kennzeichnung außerhalb des Gebäudes muss durch Mittel wie einen zeitgesteuerten Summer/Blitz usw. vorhanden sein, die bei der Unscharfschaltung des Systems für einen definierten Zeitraum (z. B. 30 Sekunden) aktiv ist.

Weitere Informationen finden Sie in den folgenden Abschnitten dieses Handbuchs:

Timer [→ 119]

3.1.5.4 Konfigurationsanforderungen zur Einhaltung der Norm PD 6662:2010

Empfehlungen für die Aufzeichnung von ferngemeldeten Alarmbedingungen (BS 8243:2010 – Anhang G.1 und G.2)

Alarmbedingungen können zur Analyse gemäß Anhang G kategorisiert werden, wenn das SPC-System so konfiguriert wird, dass die Zutrittsverzögerung weniger als 30 Sekunden beträgt und die Wählgerätverzögerung auf 30 Sekunden eingestellt ist.

Weitere Informationen finden Sie in den folgenden Abschnitten dieses Handbuchs:

BEREICHE [→ 122]

Bereich hinzufügen/bearbeiten [→ 257]

Timer [→ 119]

Anforderungen für Systeme mit dedizierten Alarmpfaden (BS EN 50136-1-2, 1998)

Das SPC-System muss so konfiguriert werden, dass ein automatisierter Übertragungstest zum Empfänger erfolgt.

Das SPC-System muss mit einem ‚Übertragungsstörung'-Ausgang konfiguriert werden.

Weitere Informationen finden Sie im folgenden Abschnitt dieses Handbuchs:

Hinzufügen/Bearbeiten eines Empfängers [→ 316]

Anforderungen für Ausrüstungsteile in Systemen mit digitalen Kommunikationsgeräten unter Verwendung von PSTN (BS EN 50136-2-2, 1998)

Störausgang

Das SPC-System muss mit einem ‚Übertragungsstörung'-Ausgang konfiguriert werden.

Weitere Informationen finden Sie in den folgenden Abschnitten dieses Handbuchs:

AUSGÄNGE [→ 144] (Bedienteil)

Ein-/Ausgänge der Zentrale konfigurieren [→ 210] (Browser)

Hinzufügen/Bearbeiten eines Empfängers [→ 316]

Erneute Übertragungsversuche

Die Konfiguration von erneuten Übertragungsversuchen (Wählversuche) wird in diesem Handbuch beschrieben:

Hinzufügen/Bearbeiten eines Empfängers [→ 316]

EDP-Einstellungen bearbeiten [→ 325]

Ein Minimum von 1 und ein Maximum von 12 erneuten Übertragungen sind zulässig.

Einbruch und Bedrohung – Systemaufbau (DD CLC TS 50131-7, 2008)

Scharf- und Unscharfschaltungen

Das SPC-System kann so konfiguriert werden, dass die Scharfschaltung durch ‚Ext. Zeitabbruch' abgeschlossen werden.

Es ist möglich, das SPC-System so zu konfigurieren, dass bei Scharfschaltung ein Warngerät aktiviert wird.

Weitere Informationen finden Sie in den folgenden Abschnitten dieses Handbuchs:

Timer [→ 119]

MG-Attribute [→ 378]

AUSGÄNGE [→ 144] (Bedienteil)

Bearbeiten eines Ausgangs [→ 211] (Browser)

Einbruchs- und Bedrohungsalarm (BS8243:2010-Bezeichnung der Bedrohungsalarmsignale für aufeinander folgende Bestätigung)

Das SPC-System kann so konfiguriert werden, dass die folgenden Szenarien einen bestätigten Bedrohungsalarm (HV für SIA und 129 für CID) melden, wenn sie mehr als zwei Minuten von einer Bedrohungs-MGs oder einem Bedrohungsgerät (HD) ausgelöst werden:

- zwei Aktivierungen der Bedrohungs-MG
- eine Aktivierung der Bedrohungs-MG und eine Aktivierung der Panik-MG

Wird in dem zweiminütigen Zeitraum eine Bedrohungs-, Sabotage- oder Panikmeldergruppe aktiviert, wird ebenfalls ein bestätigter Bedrohungsalarm verschickt.

Eine bestätigte Bedrohung erfordert keine Wiederherstellung durch einen Techniker, auch wenn die Technikerwiederherstellung aktiviert ist. Ein Ereignis einer bestätigten Bedrohung wird im Systemprotokoll festgehalten.

Kommunikationssicherheit für Fernsupport und Fernsystemüberprüfungen (DD 263:2010)

Stellen Sie bitte sicher, dass SPC Pro innerhalb der Bestimmungen von DD 263:2010 genutzt wird.

3.1.5.5 Zusätzliche Inbetriebnahmeanforderungen zur Einhaltung der Norm PD 6662:2010

Im Systemaufbauangebot anzugebende Informationen und Montagedokument (BS 8243:2010 – Anhang F)

- Während der Installation, Konfiguration und Inbetriebnahme eines SPC-Systems muss der Monteur folgende Richtlinien gemäß dem oben genannten Anhang beachten:
- Es wird empfohlen, dass duale Pfade für die Signalisierung verwendet werden, die im SPC-System durch GFM, PSTN und Ethernet-Optionen unterstützt werden.
- Das SPC-System muss so installiert und konfiguriert werden, dass eine effektive Bestätigungseinrichtung entsteht. Ausnahmen dahingehend müssen im Montagedokument aufgeführt werden.
- Kombinationen und Sequenzen, die zu einem bestätigten Alarm beitragen, müssen dem Endanwender eindeutig mitgeteilt werden.
- Die Einbruchsbestätigungsdauer muss dem Endanwender eindeutig mitgeteilt werden.
- Methoden zur Scharf- und Unscharfschaltung müssen dem Endanwender, wie in diesem Dokument beschrieben, eindeutig erläutert werden.
- Stellen Sie sicher, dass dem Endanwender im Falle eines Schlossausfalls schriftliche Vereinbarungen zur Verfügung stehen.

Es wird empfohlen, dass die beiliegende PD 6662:2010-Kennzeichnung in einer angemessenen Position im Inneren des SPC-Gehäuses neben dem Produkttypenschild angebracht wird.

3.1.5.6 Zusätzliche Informationen

Netzwerkübertragungsanforderungen – Leistung, Verfügbarkeit und Sicherheitsstufen (BS EN 50136-1-2, 1998 und BS EN 50136-1-5, 2008)

Das SPC-System wurde gemäß EN 50136-1-1 getestet und genehmigt.

SPC-Stufen werden wie folgt klassifiziert:

Übertragungsdauer	DS als Max.
Übertragungsdauer, max. Werte	M0 - M4
Meldedauer	T3 als Max.
Verfügbarkeit	Weitere Informationen finden Sie im folgenden Abschnitt dieses Handbuchs: ATS-Stufen und Dämpfungsspezifikationen

	[→ 383]
Signalsicherheitsstufen	Gemäß EN 50136-1-1 getestet und als ‚S0' klassifiziert.

3.1.6 Konformität mit VdS-Genehmigungen

Diese Installationsanleitung umfasst die erforderlichen Produktinstallationsinformationen für die VdS Zulassungen.

Vanderbilt

VdS Zertifikatsnummer

G 112104, G112124, G112128.

VdS EN Zertifikate

EN-ST000142, EN-ST000143, EN-ST000055, EN-ST000056, EN-ST000057, EN-ST000058, EN-ST000061, EN-ST000062.

Siemens

VdS Zertifikatsnummer

G116035.

VdS EN Zertifikate

EN-ST000225, EN-ST000226, EN-ST000227, EN-ST000228, EN-ST000229, EN-ST000230, EN-ST000231, EN-ST000232.

Dieser Abschnitt beschreibt die Konformität dieses Systems mit den VdS-Genehmigungen.

Software

Zur Scharfschaltung des Systems gemäß der VdS-Genehmigung müssen Sie wie folgt vorgehen:

1. Melden Sie sich über den Browser an der Zentrale an.
2. Wählen Sie den Konfigurationsmodus aus.
3. Wählen Sie im Menü die Einstellungen aus.
4. Wählen Sie Standards aus.
5. Wählen Sie Deutschland aus der Regionsliste aus.
6. Wählen Sie den durch Ihren Installationstyp erforderlichen VdS-Grad aus.

- Fernabschaltungen – Es ist nicht möglich, die aktiven Störungen mithilfe des Browsers oder SPC Pro auszuschalten. Die Abschaltung kann nur über die Bedienteile erfolgen.
- Fernverbindungen – Es ist nicht möglich, zur Verbindung mit einem scharf geschalteten System den Browser oder SPC Pro zu verwenden.
- Bestätigte Alarme – Ein intern scharf geschaltetes System kann keinen bestätigen Alarm erzeugen.
- Hardware-Störauswertung – In den **Optionen** müssen Sie **Aktiv + Auswertung (10 s)** aus dem Dropdown-Menü des **Watchdog Ausgang Mode** wählen.

  Hinweis: Hardware-Störungen werden nicht gemeldet, wenn der Techniker am System angemeldet ist.

Hardware

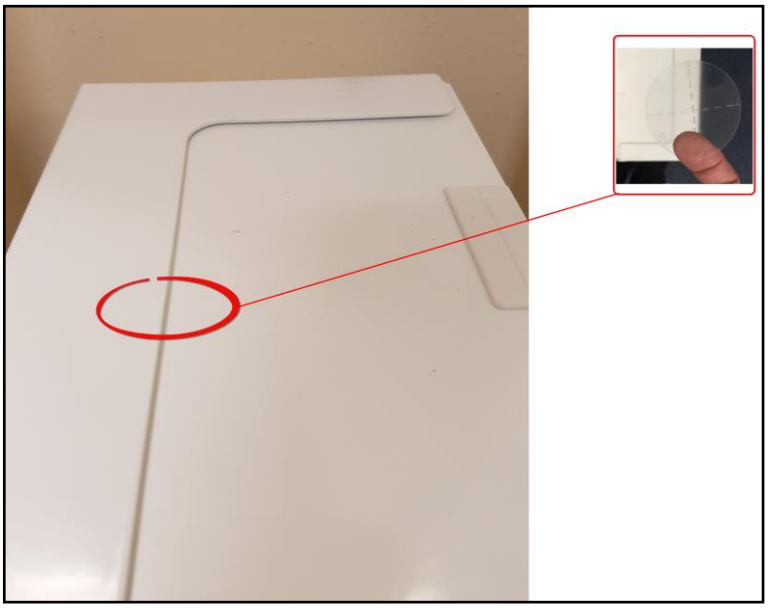
Zur Einhaltung der VdS-Genehmigung ist Folgendes erforderlich:

- Ein G5-Gehäuse mit vorderem Sabotageschutz implementiert als minimale Anforderung
- Bedienteile zeigen nicht die Statusinformationen an, wenn das System scharf geschaltet ist.
- Nachstehend die Anzahl der unterstützten Meldergruppen:
  - 512 Meldergruppen in Ringkonfiguration

  - 128 Meldergruppen pro X-Bus in Multidrop-Konfiguration (Stichleitung)
- Die folgenden Endwiderstandskombinationen entsprechen nicht den VdS-Normen:
  - 1k, 470 Ohm
  - 1k, 1k, 6k6 Ohm

3.1.7 Konformität mit NF und A2P Genehmigungen

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



Um den NF & Installationsbestimmungen gerecht zu werden, muss das Gehäuse nach der Installation mit dem mitgelieferten Siegel verplombt werden.

SPC aufgeführten Produkte wurden getestet nach NF324 - H58, mit Bezug auf die RTC 50131-6 und 50131-3 RTC und aktuellen EN-Zertifizierungen finden Einhaltung EN50131 Zulassungen.

Produkttyp	Konfiguration	Norm	Logo
SPC6350.320 + SPCP355.300 (Cert. XXXXXXXXXX)	60 Std, nicht überwacht	NF Grad 3, Klasse 1	
SPC5350.320 + SPCP355.300 (Cert. XXXXXXXXXX)	60 Std, nicht überwacht		
SPC6350.320 (Cert. XXXXXXXXXX)	60 Std, nicht überwacht		
SPC5350.320 (Cert. XXXXXXXXXX)	60 Std, nicht überwacht		
SPC6330.320 + SPCP333.300 (Zert. 1232200003)	60 Std., nicht überwacht	NF-Grad 3, Klasse 1	
SPC5330.320 + SPCP333.300 (Zert. 1232200003)	60 Std., nicht überwacht		
SPC6330.320 (Zert. 1232200003)	30 Std., überwacht		
SPC5330.320 (Zert. 1232200003)	30 Std., überwacht		
SPC5320.320 (Zert. 1222200003)	36 Std., nicht überwacht	NF-Grad 2, Klasse 1	
SPC4320.320 (Zert. 1222200003)	36 Std., nicht überwacht		
SPCN110.000 SPCN310.000 SPCK420.100 SPCK620.100 SPCK623.100 SPCE652.100 SPCE452.100 SPCE110.100 SPCE120.100		NF-Grad 2 und 3, Klasse 1	

4 Technische Daten

4.1 SPC4000

Programmierbare Bereiche	4
Max. Anzahl von Benutzer-PINs	100
Fernbedienungen	Bis zu 32
Funk-Panikalarm	Bis zu 128
Ereignisspeicher	1.000 Einbruchsereignisse, 1.000 Zutrittsereignisse
Anzahl integrierte Meldergruppen	8
Max. Anzahl von fest verdrahteten Meldergruppen	32
Max. Anzahl von Funk-Meldergruppen	32 (ohne verdrahtete Meldergruppen)
Max. Anzahl von Intrunet-Funkmeldern pro Funkempfänger (empfohlen)	20
EOL-Widerstand	2 Endw. 4k7 (Standard), andere Widerstandskombinationen sind konfigurierbar
Anzahl Relais onboard	1 Blitzleuchte (30 V DC / 1 A ohmscher Schaltstrom)
Anzahl Open-Collector-Ausgänge onboard	2 Innen-/Außensirenen, 3 frei programmierbar (jeweils max. 400 mA ohmscher Schaltstrom über Hilfsausgang)
Firmware	V3.x
Anzahl Türen	Max. 4 Eingangstüren und 2 Eingangs-/Ausgangstüren
Anzahl Kartenleser	Max. 4
Funkmodul	● SPC4221: integrierter SiWay-Funkempfänger (868 MHz) ● SPC4320.220: optional (SPCW111), ● SPC4320.320: Optional (SPCW110)
Verifikation	4 Verifikationszonen mit max. 4 IP-Kameras und 4 Audiogeräten
Video	Bis zu 16 Vor- / 16 Nachereignisaufnahmen (JPEG, Auflösung 320 × 240, max. 1 Bild/Sek.)
Audio	Bis zu 60 Sek. Vor- / 60 Sek. Nachereignisaudioaufnahme
Feldbus 1)	X-BUS über RS485 (307 kBit/s)
Anzahl lokale Geräte 2)	Max. 11 (4 Bedienteile, 2 Türerweiterungen, 5 Eingangs-/Ausgangserweiterungen)
Anschließbare lokale Geräte	● Bedienteile: SPCK42x, SPCK62x ● Türerweiterungen: SPCA210, SPCP43x ● Erweiterungen mit E/A: SPCE65x, SPCE45x, SPCP33x, SPCE110, SPCE120, SPCV32x
Schnittstellen	● 1 X-BUS (1 Stichleitung) ● 1 RS232 ● 1 USB (PC-Anschluss) ● 1 SPC Fast Programmer ● SPC43xx: Zusätzlich 1 Ethernet (RJ45)
Sabotagekontakt	Feder-Sabotageschalter vorn, 2 Hilfssabotageeingänge
Versorgungsspannung	Typ A (nach EN50131-1)
Netzspannung	230 V AC, +10 % / -15 %, 50 Hz
Hauptsicherung	250 mA T (austauschbares Teil am Netzanschlussblock)
Stromaufnahme	SPC42xx: Max. 160 mA bei 230 V AC

	SPC43xx: Max. 200 mA bei 230 V AC
Betriebsstrom	SPC42xx-Controller: Max. Max. 160 mA bei 12 V DC SPC43xx-Zentrale: Max. 200 mA bei 12 V DC
Ruhestrom	SPC42xx-Controller: Max. 140 mA bei 12 V DC (165 mA bei PSTN, 270 mA bei GSM, 295 mA bei PSTN und GSM) SPC43xx-Zentrale: Max. 170 mA bei 12 V DC (195 mA mit PSTN, 300 mA mit GSM, 325 mA mit PSTN und GSM)
Ausgangsspannung	13–14 V DC unter Normalbedingungen (Netzspannung vorhanden und Batterie voll aufgeladen), min. 10,5 V DC bei Betrieb über Sekundärgerät (bevor das System zum Tiefentladungsschutz abschaltet)
Unterspannungsauslösung	7,5 V DC
Überspannungsschutz	15,7 V DC
Spitze-Spitze-Welligkeit	Max. 5 % der Ausgangsspannung
Hilfsstromversorgung (Nennwert)	Max. 750 mA bei 12 V DC
Batterietyp	SPC422x/4320: YUASA NP7-12FR (7 Ah), Batterie nicht im Lieferumfang enthalten
Batterieladung	SPC422x/4320: Max. 72 h bis 80 % der Batteriekapazität
Batterieschutz	Intensität auf 1 A begrenzt (geschützt durch Sicherung), Tiefentladungsschutz bei 10,5 V DC +/- 3 %
Software-Update	Vor-Ort- und Fern-Upgrade für Controller, Peripheriegeräte und GSM/PTSN-Modems.
Kalibrierung	Keine Kalibrierungsprüfungen erforderlich (werksseitig kalibriert)
Zu wartende Teile	Keine zu wartenden Teile
Betriebstemperatur	-10 ~ +50 °C
Rel. Luftfeuchtigkeit	Max. 90 % (nicht kondensierend)
Farbe	RAL 9003 (Signalweiß)
Gewicht	SPC422x/4320: 4.500 kg
Abmessungen (B × H × T)	SPC422x/4320: 264 × 357 × 81 mm
Gehäuse	SPC4320.320: Kleines Metallgehäuse (1,2 mm, Baustahl) SPC422x.220: Kleines Gehäuse mit Metallunterteil (1,2 mm, Baustahl) und Kunststoffdeckel
Aufnahmekapazität des Gehäuses	SPC422x/4320: 1 zusätzliches Erweiterungsmodul (150 mm × 82 mm)
IP-Klasse	30
ATS	2
ÜW	4
Ereignisprofile	5
Ereignisausnahmen	10
Steuerprofile	5

1) Max. 400 m zwischen Geräten / Kabel vom Typ IYSTY 2 × 2 × Ø 0,6 mm (min.), UTP cat5 (Massivdrahtleiter) oder Belden 9829.

2) Anstelle einer Bedienteil- oder Türerweiterung können mehrere E/A-Erweiterungen adressiert werden, aber die Anzahl der programmierbaren Ein-/Ausgänge darf die angegebenen Systemgrenzen nicht überschreiten.

4.2 SPC5000

Programmierbare Bereiche	16
Max. Anzahl von Benutzer-PINs	500
Fernbedienungen	Bis zu 120
Funk-Panikalarm	Bis zu 128
Ereignisspeicher	10.000 Einbruchsereignisse, 10.000 Zutrittsereignisse
Anzahl integrierte Meldergruppen	● SPC5320\5330 – 8 ● SPC5350 – 16
Max. Anzahl von fest verdrahteten Meldergruppen	128
Max. Anzahl von Funk-Meldergruppen	120 (ohne verdrahtete Meldergruppen)
Max. Anzahl von Intrunet Funkmeldern pro Funkempfänger (empfohlen)	20
EOL-Widerstand	2 Endw. 4k7 (Standard), andere Widerstandskombinationen sind konfigurierbar
Relaisausgänge	● SPC5320\5330 – 1 Blitzleuchte (30 V DC/1 A ohmscher Schaltstrom) ● SPC5350 – 4 (einpolige Umschaltung, 30 V DC/max. 1 A ohmscher Schaltstrom)
Elektronische Ausgänge	● SPC5320\5330 – 5 Ausgänge: – 2 interne/externe Sirenen – 3 programmierbar. Maximal 400 mA ohmscher Schaltstrom pro Ausgang, Versorgung über Hilfsausgang. ● SPC5350 – 8 Ausgänge. Maximal 400 mA ohmscher Schaltstrom pro Ausgang – 5 Standard-Leistungsausgänge – 3 überwachte Ausgänge
Firmware	V3.x
Anzahl Türen	Max. 16 Eingangstüren und 8 Eingangs-/Ausgangstüren
Anzahl Kartenleser	Max. 16
Funkmodul	Optional (SPCW110)
Verifikation	16 Verifikationszonen mit max. 4 IP-Kameras und 16 Audiogeräten
Video	Bis zu 16 Vor- / 16 Nachereignisaufnahmen (JPEG, Auflösung 320 × 240, max. 1 Bild/Sek.)
Audio	Bis zu 60 Sek. Vor- / 60 Sek. Nachereignisaudioaufnahme
Feldbus 1)	X-BUS über RS485 (307 kBit/s)
Anzahl lokale Geräte 2)	Max. 48 (16 Bedienteile, 8 Türerweiterungen, 16 Eingangs-/Ausgangserweiterungen)
Anschließbare lokale Geräte	● Bedienteile: SPCK42x, SPCK62x ● Türerweiterungen: SPCA210, SPCP43x ● Erweiterungen mit E/A: SPCE65x, SPCE45x, SPCP33x, SPCP35x, SPCE110, SPCE120, SPCV32x
Schnittstellen	● 2 X-BUS (2 Stichleitungen oder 1 Schleife),

	● 2 RS232 ● 1 USB (PC-Anschluss), ● 1 SPC Fast Programmer, ● SPC53xx: Zusätzlich 1 Ethernet (RJ45)
Sabotagekontakt	● SPC5320/5330: Feder-Sabotageschalter vorn, 2 Hilfssabotageeingänge ● SPC5350: Sabotageschalter auf der Frontplatte und rückwärtig
Versorgungsspannung	Typ A (nach EN50131-1)
Netzspannung	230 V AC, +10 % / -15 %, 50 Hz
Hauptsicherung	● SPC5320/5330: 250 mA T (austauschbares Teil am Netzanschlussblock) ● SPC5350: 800 mA T (austauschbares Teil am Netzanschlussblock)
Stromaufnahme	● SPC5320/5330: Max. 200 mA bei 230 V AC ● SPC5350: Max. 500 mA bei 230 V AC
Betriebsstrom	● SPC5320/5330: Zentrale: Max. 200 mA bei 12 V DC ● SPC5350: Max. 210 mA bei 12 V DC
Ruhestrom	SPC53xx-Controller: Max. 170 mA bei 12 V DC (195 mA mit PSTN, 300 mA mit GSM, 325 mA mit PSTN und GSM)
Ausgangsspannung	13–14 V DC unter Normalbedingungen (Netzspannung vorhanden und Batterie voll aufgeladen), min. 10,5 V DC bei Betrieb über Sekundärgerät (bevor das System zum Tiefentladungsschutz abschaltet)
Unterspannungsauslösung	11 V DC
Überspannungsschutz	● SPC5320/5330: 15,7 V DC ● SPC5350: 15 V DC Nennspannung
Spitze-Spitze-Welligkeit	Max. 5 % der Ausgangsspannung
Hilfsstromversorgung (Nennwert)	● SPC5320/5330: Max. 750 mA bei 12 V DC ● SPC5350: Max. 2200 mA bei 12 V DC (8 Ausgänge mit separaten Sicherungen, 300 mA pro Ausgang)
Batterietyp	● SPC5320: YUASA NP7-12FR (7 Ah), ● SPC5330: YUASA NP17-12FR (17 Ah) ● SPC5350: YUASA NP24-12 (12 V 24 Ah), Alarmcom AB1227-O (12 V 27 Ah) ● SPC5350: FIAMM FGV22703 (12V 27Ah) Batterie nicht im Lieferumfang enthalten
Batterieladung	● SPC5320: Max. 72 Std., ● SPC5330/5350: Max. 24 h bis 80 % der Batteriekapazität
Batterieschutz	● SPC5320/5330: Intensität auf 1 A begrenzt (geschützt durch Sicherung), Tiefentladungsschutz bei 10,5 V DC +/- 3 % ● SPC5350: Stromstärke begrenzt auf 2 A (geschützt durch rücksetzbare PTC-Sicherung), Tiefentladungsschutz bei 10,5 V DC.
Software-Update	Vor-Ort- und Fern-Upgrade für Controller, Peripheriegeräte und GSM/PTSN-Modems.
Kalibrierung	Keine Kalibrierungsprüfungen erforderlich (werksseitig kalibriert)
Zu wartende Teile	● SPC5320/5330: Keine zu wartenden Teile

	● SPC5350: 8 Glassicherungen (400 mA AT) für Ausgänge mit 12 V DC
Betriebstemperatur	-10 ~ +50 °C
Rel. Luftfeuchtigkeit	Max. 90 % (nicht kondensierend)
Farbe	RAL 9003 (Signalweiß)
Gewicht	● SPC5320: 4.500 kg ● SPC5330: 6.400 kg ● SPC5350: 18.600 kg
Abmessungen (B × H × T)	● SPC5320: 264 × 357 × 81 mm ● SPC5330: 326 × 415 × 114 mm ● SPC5350: 498 × 664 × 157 mm
Gehäuse	● SPC5320: kleines Metallgehäuse (1,2 mm, Baustahl) ● SPC5330: aufklappbares Metallgehäuse (1,2 mm, Baustahl) ● SPC5350: Metallgehäuse (1,5 mm, Baustahl)
Aufnahmekapazität des Gehäuses	● SPC5320: 1 zusätzliches Erweiterungsmodul, ● SPC5330: 4 zusätzliche Erweiterungsmodule (150 mm × 82 mm) ● SPC5350: 4 zusätzliche Erweiterungsmodule (150 mm × 82 mm)
IP / IK Klasse	30 / 06
ATS	5
ÜW	15
Ereignisprofile	10
Ereignisausnahmen	50
Steuerprofile	8

1) Max. 400 m zwischen Geräten / Kabel vom Typ IYSTY 2 × 2 × Ø 0,6 mm (min.), UTP cat5 (Massivdrahtleiter) oder Belden 9829.

2) Anstelle einer Bedienteil- oder Türerweiterung können mehrere E/A-Erweiterungen adressiert werden, aber die Anzahl der programmierbaren Ein-/Ausgänge darf die angegebenen Systemgrenzen nicht überschreiten.

4.3 SPC6000

Programmierbare Bereiche	60
Max. Anzahl von Benutzer-PINs	2.500
Fernbedienungen	Bis zu 120
Funk-Panikalarm	Bis zu 128
Ereignisspeicher	10.000 Einbruchsereignisse, 10.000 Zutrittsereignisse
Anzahl integrierte Meldergruppen	● SPC6320\6330 – 8 ● SPC6350 – 16
Max. Anzahl von fest verdrahteten Meldergruppen	512
Max. Anzahl von Funk-Meldergruppen	120 (ohne verdrahtete Meldergruppen)
Max. Anzahl von Intrunet-Funkmeldern pro Funkempfänger (empfohlen)	20

EOL-Widerstand	2 Endw. 4k7 (Standard), andere Widerstandskombinationen sind konfigurierbar
Relaisausgänge	● SPC6320\6330 – 1 Blitzleuchte (30 V DC/1 A ohmscher Schaltstrom) ● SPC6350 – 4 (einpolige Umschaltung, 30 V DC/max. 1 A ohmscher Schaltstrom)
Elektronische Ausgänge	● SP6320\6330 – 5 Ausgänge: – 2 interne/externe Sirenen – 3 programmierbar. Maximal 400 mA ohmscher Schaltstrom pro Ausgang, Versorgung über Hilfsausgang. ● SPC6350 — 8 Ausgänge. Maximal 400 mA ohmscher Schaltstrom pro Ausgang – 5 Standard-Leistungsausgänge – 3 überwachte Ausgänge
Firmware	V3.x
Anzahl Türen	Max. 64 Eingangstüren oder 32 Ein-/Ausgangstüren
Anzahl Kartenleser	Max. 64
Funkmodul	Optional (SPCW110)
Verifikation	32 Verifikationszonen mit max. 4 IP-Kameras und 32 Audiogeräten
Video	Bis zu 16 Vor- / 16 Nachereignisaufnahmen (JPEG, Auflösung 320 × 240, max. 1 Bild/Sek.)
Audio	Bis zu 60 Sek. Vor- / 60 Sek. Nachereignisaudioaufnahme
Feldbus 1)	X-BUS über RS485 (307 kBit/s)
Anzahl lokale Geräte 2)	Max. 128 (32 Bedienteile, 32 Türerweiterungen, 64 Eingangs-/Ausgangserweiterungen)
Anschließbare lokale Geräte	● Bedienteile: SPCK42x, SPCK62x ● Türerweiterungen: SPCA210, SPCP43x ● Erweiterungen mit E/A: SPCE65x, SPCE45x, SPCP33x, SPCP35x, SPCE110, SPCE120, SPCV32x
Schnittstellen	● 2 X-BUS (2 Stichleitungen oder 1 Schleife), ● 2 RS232 ● 1 USB (PC-Anschluss), ● 1 SPC Fast Programmer, ● SPC63xx: Zusätzlich 1 Ethernet (RJ45)
Sabotagekontakt	● SPC6330: Feder-Sabotageschalter vorn, 2 Hilfssabotageeingänge ● SPC6350: Sabotageschalter auf der Frontplatte und rückwärtig
Versorgungsspannung	Typ A (nach EN50131-1)
Netzspannung	230 V AC, +10 %/-15 %, 50 Hz
Hauptsicherung	● SPC6330: 250 mA T (austauschbares Teil am Netzanschlussblock) ● SPC6350: 800 mA T (austauschbares Teil am Netzanschlussblock)
Stromaufnahme	● SPC6330: Max. 200 mA bei 230 V AC ● SPC6350: Max. 500 mA bei 230 V AC
Betriebsstrom	● SPC6330: Max. 200 mA bei 12 V DC ● SPC6350: Max. 210 mA bei 12 V DC
Ruhestrom	SPC63xx-Controller: Max. 170 mA bei 12 V DC (195 mA mit

	PSTN, 300 mA mit GSM, 325 mA mit PSTN und GSM)
Ausgangsspannung	● SPC6330: 13–14 V DC unter Normalbedingungen (Netzspannung vorhanden und Batterie voll aufgeladen), min. 9,5 V DC bei Betrieb über Sekundärgerät (bevor das System zum Tiefentladungsschutz abschaltet) ● SPC6350: 13–14 V DC unter Normalbedingungen (Netzspannung vorhanden und Batterie voll aufgeladen), min. 9,5 V DC bei Betrieb über Sekundärgerät (bevor das System zum Tiefentladungsschutz abschaltet)
Unterspannungsauslösung	11 V DC
Überspannungsschutz	● SPC6330: 15,7 V DC ● SPC6350: 15 V DC Nennspannung
Spitze-Spitze-Welligkeit	Max. 5 % der Ausgangsspannung
Hilfsstromversorgung (Nennwert)	● SPC6330: Max. 750 mA bei 12 V DC ● SPC6350: Max. 2200 mA bei 12 V DC (8 Ausgänge mit separaten Sicherungen, 300 mA pro Ausgang)
Batterietyp	● SPC6330: YUASA NP17-12FR (17 Ah) ● SPC6350: YUASA NP24-12 (12 V 24 Ah), Alarmcom AB1227-O (12 V 27 Ah) ● SPC6350: FIAMM FGV22703 (12V 27Ah) Batterie nicht im Lieferumfang enthalten
Batterieladung	SPC63xx: Max. 24 h bis 80 % der Batteriekapazität
Batterieschutz	● SPC6330: Intensität auf 1 A begrenzt (geschützt durch Sicherung), Tiefentladungsschutz bei 10,5 V DC +/- 3 % ● SPC6350: Stromstärke begrenzt auf 2 A (geschützt durch rücksetzbare PTC-Sicherung), Tiefentladungsschutz bei 10,5 V DC, Anzeige für niedrige Spannung bei 11 V DC
Software-Update	Vor-Ort- und Fern-Upgrade für Controller, Peripheriegeräte und GSM/PTSN-Modems.
Kalibrierung	Keine Kalibrierungsprüfungen erforderlich (werksseitig kalibriert)
Zu wartende Teile	● SPC6330: Keine zu wartenden Teile ● SPC6350: 8 Glassicherungen (400 mA AT) für Ausgänge mit 12 V DC
Betriebstemperatur	-10 ~ +50 °C
Rel. Luftfeuchtigkeit	Max. 90 % (nicht kondensierend)
Farbe	RAL 9003 (Signalweiß)
Gewicht	● SPC6330: 6.400 kg ● SPC6350: 18.600 kg
Abmessungen (B × H × T)	● SPC6330: 326 × 415 × 114 mm ● SPC6350: 498 × 664 × 157 mm
Gehäuse	● SPC6330: aufklappbares Metallgehäuse (1,2 mm, Baustahl) ● SPC6350: Metallgehäuse (1,5 mm, Baustahl)
Aufnahmekapazität des Gehäuses	● SPC6330: 4 zusätzliche Erweiterungsmodule (150 mm × 82 mm) ● SPC6350: 6 zusätzliche Erweiterungsmodule (150 × 82 mm) oder 1 zusätzlicher Controller + 4 Erweiterungen

IP / IK Klasse	30 / 06
ATS	10
ÜW	30
Ereignisprofile	20
Ereignisausnahmen	100
Steuerprofile	10

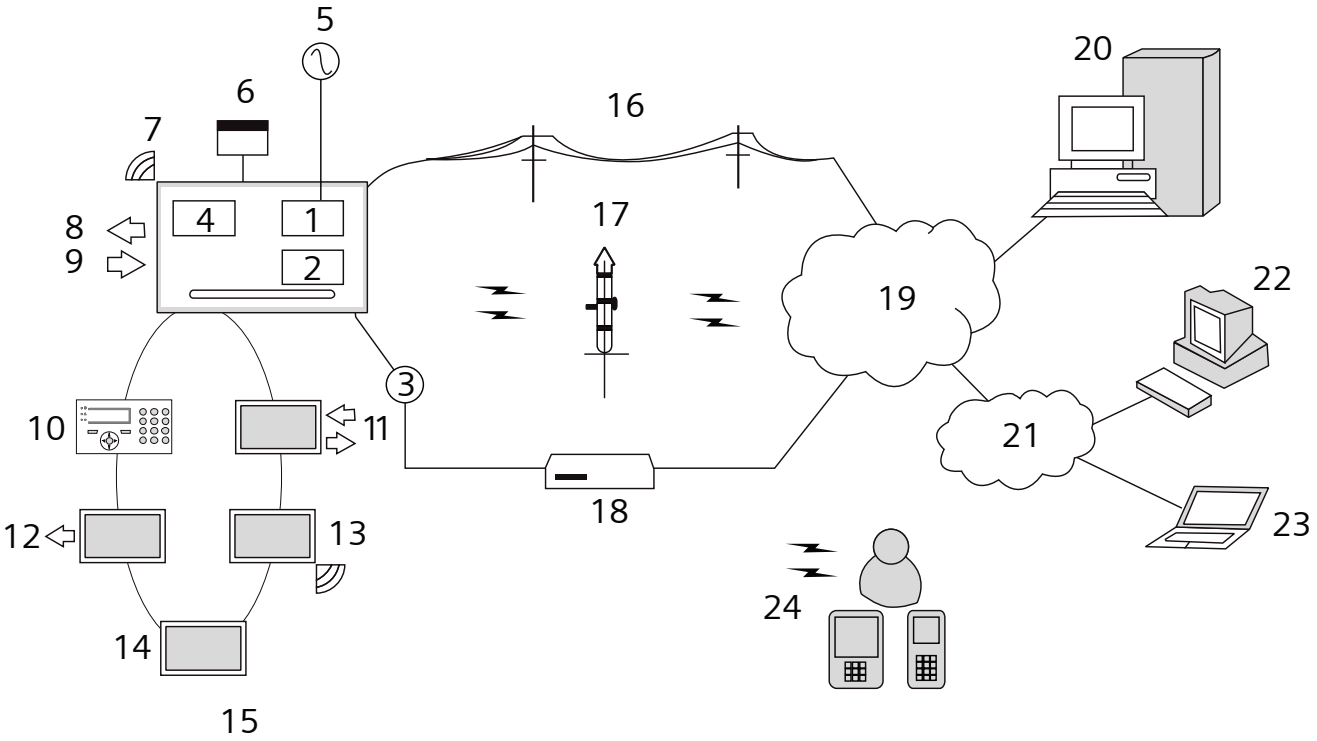
1) Max. 400 m zwischen Geräten / Kabel vom Typ IYSTY 2 × 2 × Ø 0,6 mm (min.), UTP cat5 (Massivdrahtleiter) oder Belden 9829.

2) Anstelle einer Bedienteil- oder Türerweiterung können mehrere E/A-Erweiterungen adressiert werden, aber die Anzahl der programmierbaren Ein-/Ausgänge darf die angegebenen Systemgrenzen nicht überschreiten.

5 Einführung

Der Controller der SPC-Produktreihe ist ein echter Hybrid-Controller mit 8 integrierten verdrahteten Meldergruppen, die mit Einbruchsensoren verbunden sind.

Der flexible Aufbau des Controllers ermöglicht es, die funktionalen Komponenten (PSTN/GSM/RF) zu kombinieren und so die Möglichkeiten des Systems zu erweitern. Dieser Ansatz ermöglicht dem Errichter eine effiziente Installation mit geringem Verdrahtungsaufwand.



Überblick

1	PSTN	13	Funk-Erweiterungsmodul
2	GSM	14	NETZTEIL
3	Ethernet	15	Durchschleifbare Konfiguration
4	Funkempfänger	16	PSTN-Netz
5	Netzstrom	17	GSM-Netz
6	Batterie 12 V	18	Breitband-Router
7	RF	19	Netzwerk
8	Verdrahtete Ausgänge (6)	20	Zentrale
9	Verdrahtete Eingänge (8)	21	LAN/WLAN
10	Bedienteile	22	Kundendienst
11	E/A-Erweiterung	23	Remote-Benutzer
12	Ausgangserweiterung	24	Mobile Schnittstellen

6 Montage der Systemkomponenten

6.1 Montage eines G2-Gehäuses

Im Lieferumfang für das SPC G2-Gehäuse ist ein Metall- oder Kunststoffdeckel enthalten. Die Abdeckung ist mit zwei Befestigungsschrauben am oberen und unteren Ende des Oberteils am Unterteil befestigt.

Entfernen Sie zum Öffnen des Gehäuses die beiden Schrauben mit einem geeigneten Schraubendreher, und heben Sie die Abdeckung vom Unterteil ab.

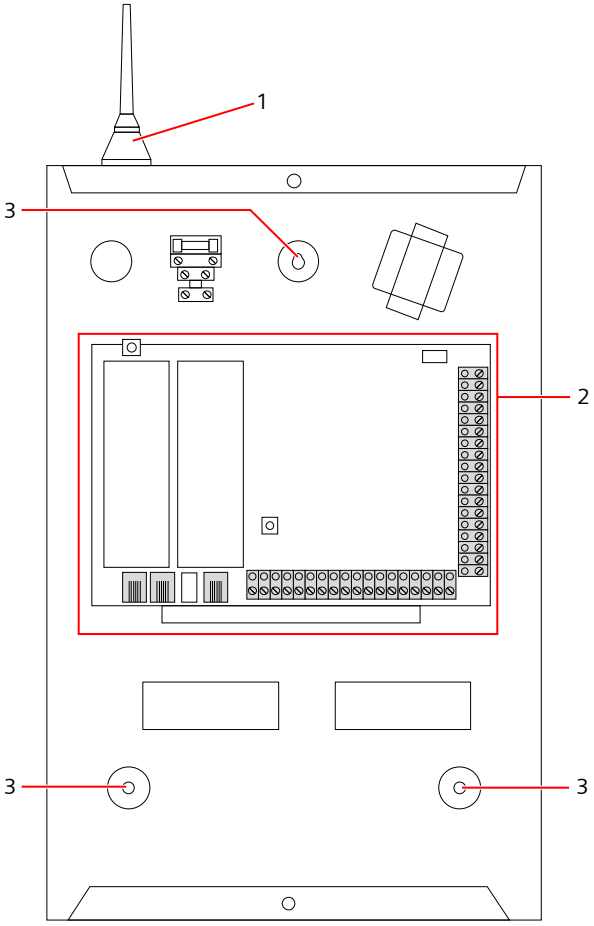
Das G2-Gehäuse enthält die Controller-Platine (PCB - **P**rinted **C**ircuit **B**oard), die auf vier Montagezapfen sitzt. Direkt unter der Controller-Platine kann optional ein Eingabe/Ausgabe-Modul eingebaut sein. Unter dem Controller kann eine Batterie mit einer max. Kapazität von 7 Ah angebracht werden.

Bei Gehäusen mit Metalldeckel muss eine optionale externe Antenne angebracht werden, wenn Funkverbindungen genutzt werden sollen. Wird die Einheit mit einer Antenne versehen, muss diese in der Firmware aktiviert werden.

Das SPC G2-Gehäuse besitzt 3 Bohrungen zur Befestigung der Einheit an der Wand.

Entfernen Sie zum Befestigen der Einheit an der Wand die Abdeckung, und suchen Sie nach der Bohrung für die erste Befestigungsschraube am oberen Ende des Gehäuses. Markieren Sie die Position der Bohrung an der gewünschten Stelle an der Wand, und bohren Sie das erste Befestigungsloch. Schrauben Sie die Einheit an der Wand fest, und markieren Sie die Lage der beiden unteren Bohrungen. Achten sie dabei auf die korrekte vertikale Ausrichtung der Einheit.

Für die Montage des Gehäuses werden Schrauben mit einem 4-5 mm langen Schaft, einem Mindest-Kopfdurchmesser von 8 mm und einer Mindestlänge von 40 mm empfohlen. Je nach Wandkonstruktion können zusätzliche Erweiterungsstecker oder -befestigungen verwendet werden.



Standardgehäuse

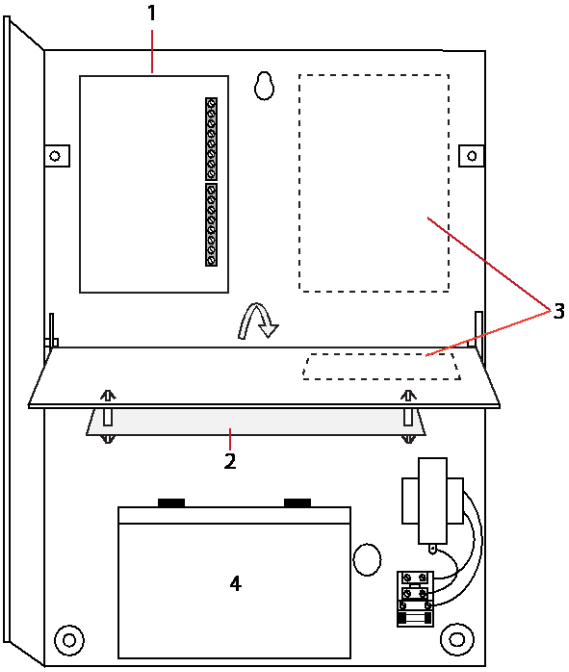
1	Funkantenne
2	SPC-Controller
3	Bohrungen für die Wandmontage

6.2 Montage eines GS-Gehäuses

Im Lieferumfang für das SPC G3-Gehäuse ist ein Metalldeckel enthalten. Die Abdeckung ist mit Scharnieren am unteren Ende des Gehäuses befestigt und mit einer Schraube auf der rechten Seite gesichert.

Zum Öffnen des Gehäuses die Schraube mit einem geeigneten Schraubendreher lösen, und die vordere Abdeckung aufklappen.

Das G3-Gehäuse enthält die auf einer klappbaren Montagehalterung angebrachte Controller-Platine (Leiterplatte). Erweiterungsmodule und Netzteile können auf der Unterseite der klappbaren Montagehalterung und auch an der Gehäuserückwand unter der Montagehalterung angebracht werden.



1 Erweiterungsmodule/Netzteil

2 Controller

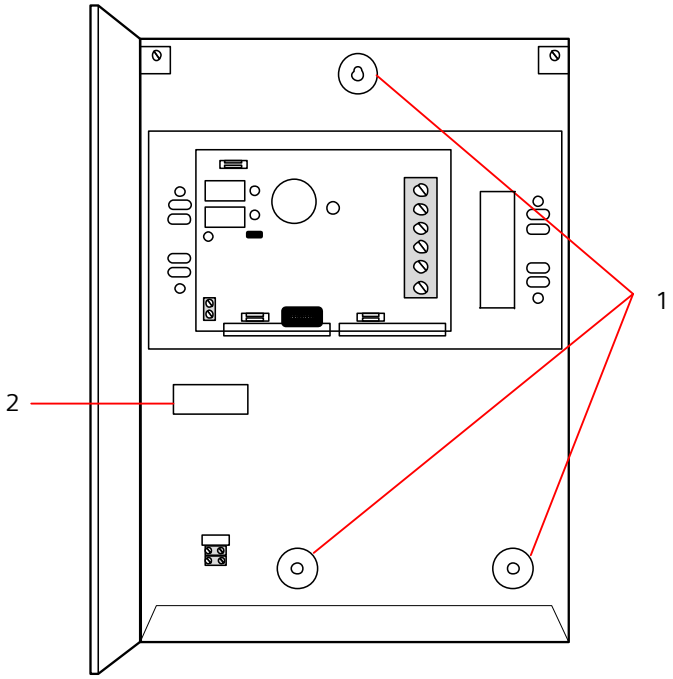
3 Erweiterungsmodule/Netzteil

4 Batterie

Bei Gehäusen mit Metalldeckel muss eine optionale externe Antenne angebracht werden, wenn Funkverbindungen genutzt werden sollen. Wird die Einheit mit einer Antenne versehen, muss diese in der Firmware aktiviert werden.

Das SPC G3-Gehäuse besitzt 3 Bohrungen zur Befestigung der Einheit an der Wand (siehe Pos. 1 unten).

Für die Montage des Gehäuses werden Schrauben mit einem 4-5 mm langen Schaft, einem Mindest-Kopfdurchmesser von 8 mm und einer Mindestlänge von 40 mm empfohlen. Je nach Wandkonstruktion können zusätzliche Erweiterungsstecker oder -befestigungen verwendet werden.



Befestigung des Gehäuses an der Wand:

1. Öffnen Sie die Abdeckung und suchen Sie die Bohrung für die erste Befestigungsschraube am oberen Ende des Gehäuses.
2. Markieren Sie die Position der Bohrung an der gewünschten Stelle an der Wand, und bohren Sie das erste Befestigungsloch.
3. Schrauben Sie die Einheit an der Wand fest, und markieren Sie die Lage der beiden unteren Bohrungen. Achten sie dabei auf die korrekte vertikale Ausrichtung der Einheit.

Anforderungen an den rückwärtigen Sabotagekontakt

Möglicherweise muss ein rückwärtiger Sabotagekontakt installiert werden, um eine Zulassung gemäß örtlicher Vorschriften zu erhalten.

Der rückwärtige Sabotagekontakt ist bei SPC-Zentralen in Gehäusen der Sicherheitsstufe 3 im Lieferumfang enthalten oder als optionales Zubehör mit Befestigungsmaterial erhältlich (SPCY130). 3G-Zentralen mit EN50131 (SPCxx3x.x20) werden standardmäßig mit einem rückwärtigen Sabotagekontakt-Satz geliefert.

6.2.1 Anbringen eines rückwärtigen Sabotageschalter-Satzes

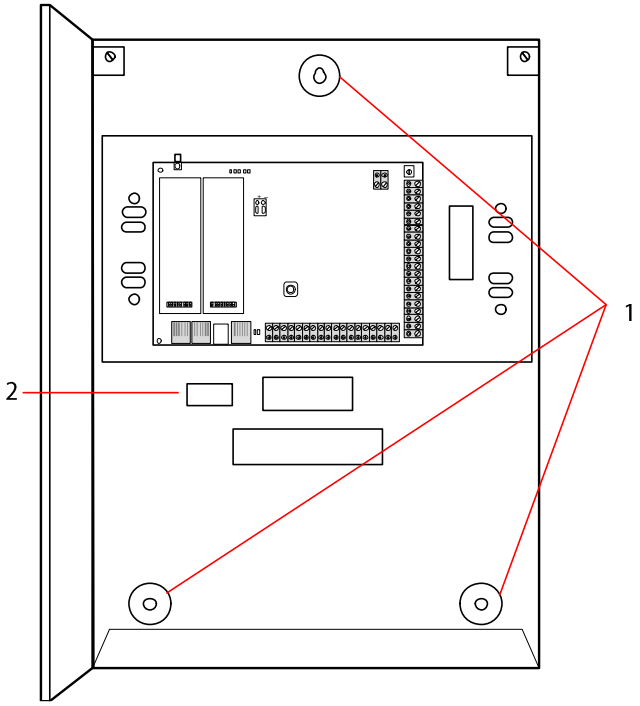
Der Satz für den rückwärtigen Sabotageschalter bietet die Möglichkeit, SPC-Zentralen und Stromversorgungen mit einem Sabotagekontakt sowohl an der Vorder- als auch der Rückseite auszustatten.

Der Satz für rückwärtigen Sabotageschutz umfasst folgende Teile:

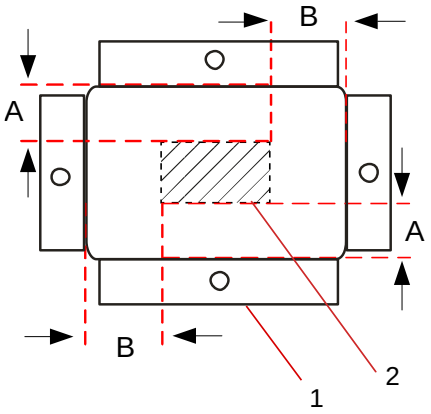
- Sabotagekontakt
- Drähte für den Anschluss des rückwärtigen Sabotagekontakts an die Controller-Platine
- Wandplatte

Montage der Wandplatte

1. Befestigen Sie die SPC mit allen 3 Halterungen an geeigneter Stelle an der Wand (siehe Element 1 unten).



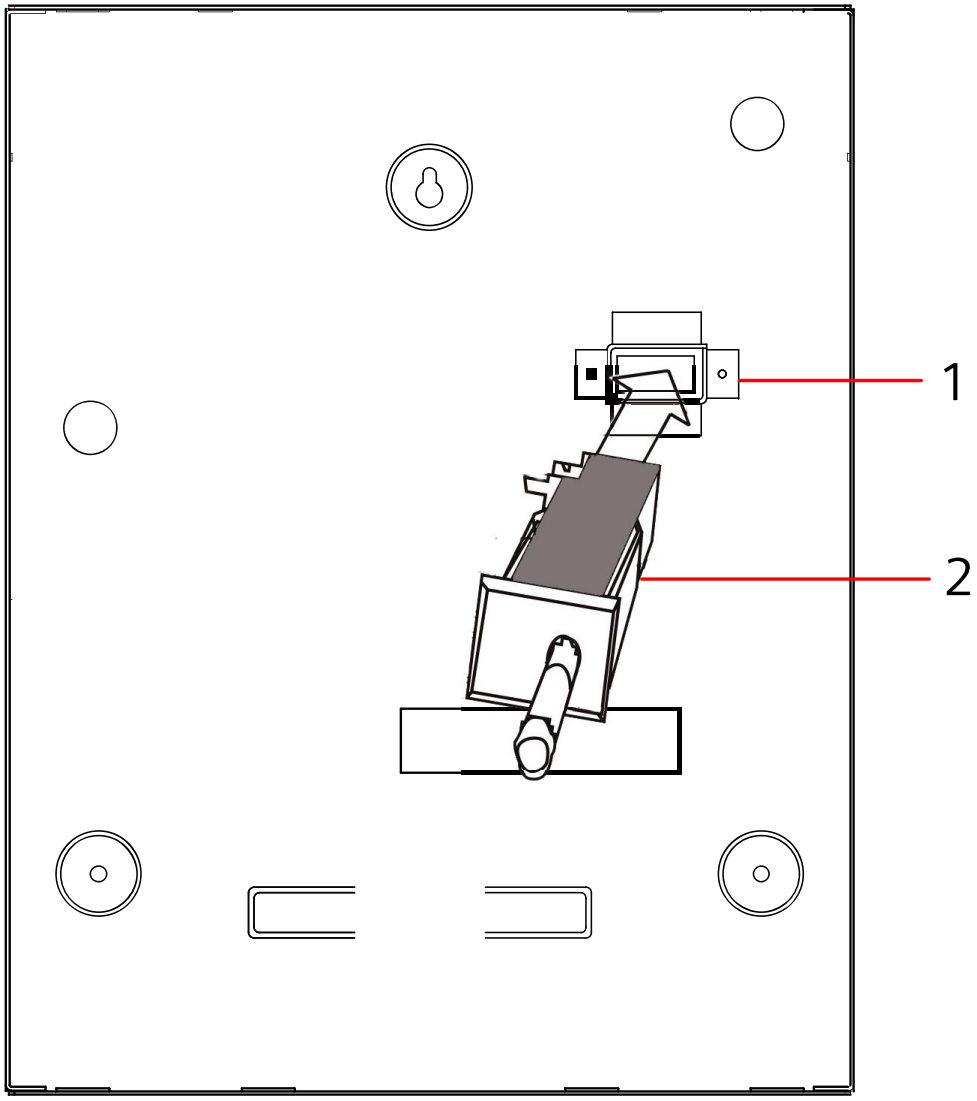
2. Ziehen Sie eine Linie um das Innere des hinteren Sabotageschalter-Ausschnitts (siehe Element 2 oben), um einen Bezugspunkt für die Anbringung der Wandplatte zu erhalten. Entfernen Sie das Gehäuse von der Wand.
3. Halten Sie die Wandplatte (siehe Element 1 unten) an die Wand, und zentrieren Sie die Platte exakt um das zuvor angezeichnete Rechteck (siehe Element 2 unten).



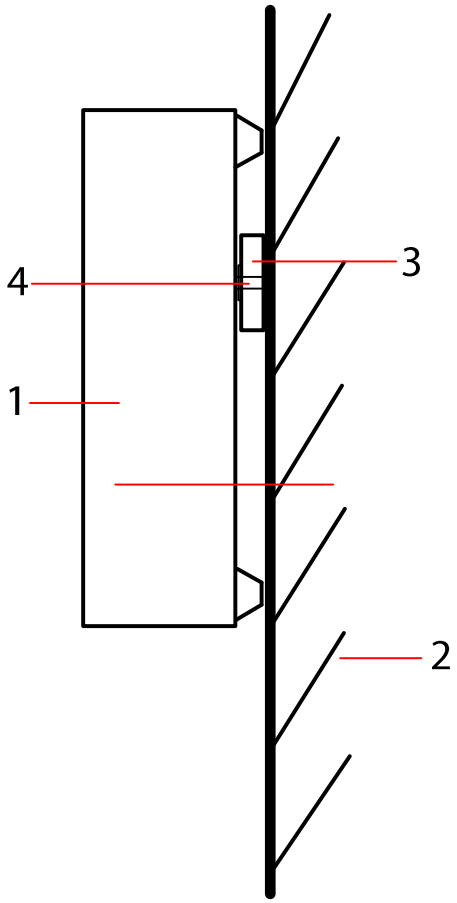
4. Stellen Sie sicher, dass alle 4 Haltebleche flach auf der Wand aufliegen.
5. Markieren Sie die 4 Befestigungsbohrungen der Wandplatte an der Wand.
6. Bohren Sie Löcher, und verwenden Sie für die Wand geeignete Befestigungsschrauben (max. 4 mm).
7. Befestigen Sie die Wandplatte an der Wand.

Anbringen des rückwärtigen Sabotagekontakts

1. Setzen Sie den Sabotagekontakt (siehe Element 2 unten) in die Rückseite des Gehäuses ein, so dass der Stift nach außen zeigt (siehe Element 1 unten).



2. Setzen Sie das Gehäuse wieder auf die Wand. Verwenden Sie hierzu die drei zuvor entfernten Halterungen (siehe Element 2 unten). Stellen Sie sicher, dass das Gehäuse rundum ohne Zwischenraum auf der Wandplatte aufliegt.



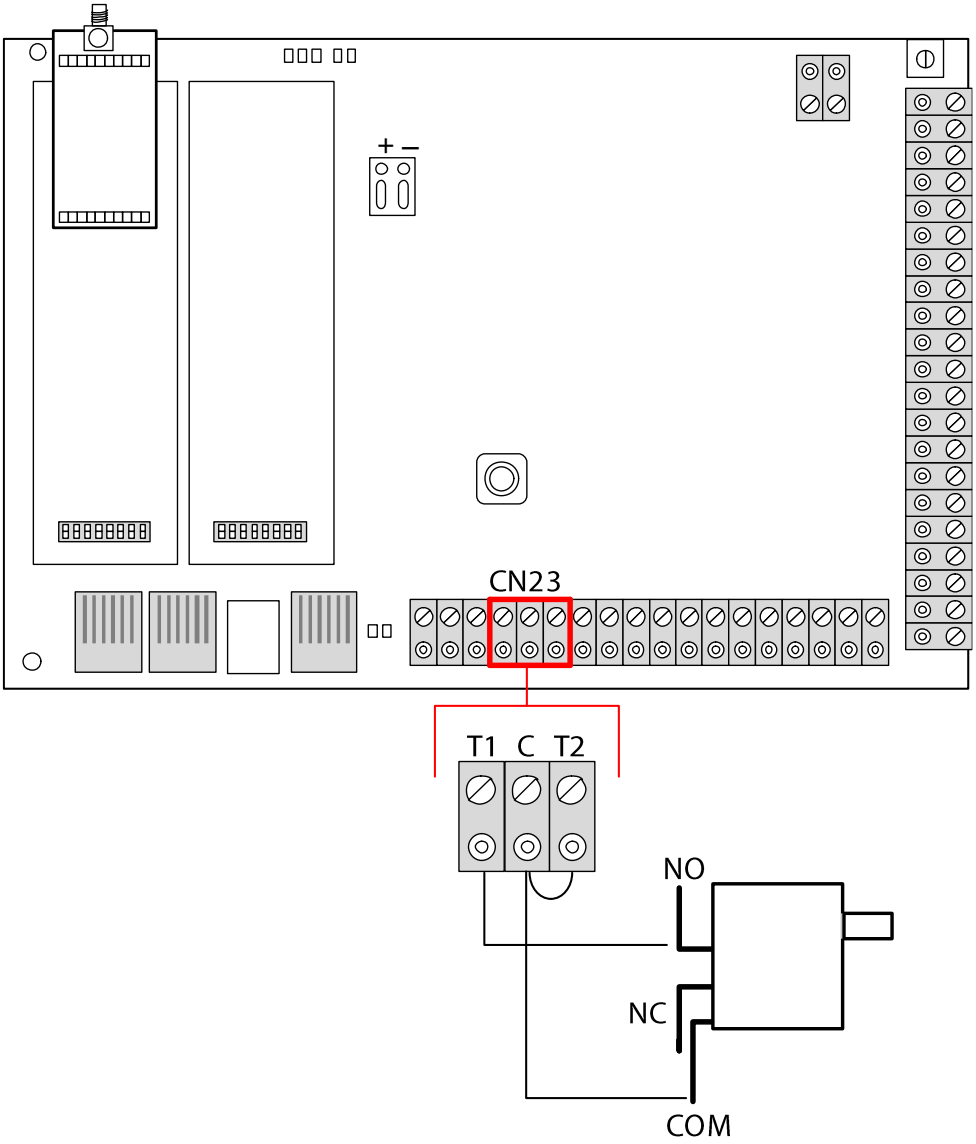
1 Gehäuse
2 Wand
3 Wandplatte
4 Sabotageschalter

	⚠ WARNUNG
	Falls die Wandplatte nicht korrekt ausgerichtet ist, sitzt das Gehäuse nicht richtig auf seinen Halterungen.

Anschließen des rückwärtigen Sabotageschalters an die Zentrale

Alle Controller-Platinen besitzen freie Eingänge, die als Sabotageeingänge konfiguriert sind. Sie sind für die Verbindung mit dem Sabotageschalter vorgesehen und bedürfen keiner Programmierung.

Der Sabotageschalter wird vom System als ‚Aux Tamper 1' erkannt.



1. Verbinden Sie den Schließer (NO) am Sabotagekontakt mit dem Anschluss T1 auf der Controller-Platine.
2. Verbinden Sie den gemeinsamen Kontakt COM am Sabotagekontakt mit dem Anschluss C auf der Controller-Platine. Stellen Sie sicher, dass Jumper T2 nicht entfernt wird.
3. Sobald der Sabotagekontakt verdrahtet ist, kann der Controller auf normale Weise in Betrieb genommen werden.

6.2.2 EN 50131-konforme Batterieinstallation

Um die EN50131-Anforderungen zu erfüllen, muss die Batterie so im Gehäuse gehalten werden, dass sie sich nicht bewegen kann. Dies wird erreicht, indem Sie die Laschen hinten im aufklappbaren Gehäuse so nach außen biegen, dass die Batterie festgehalten wird.

Wird eine Batterie mit 7 Ah verwendet, wird die Batterie zur linken Gehäuseseite geneigt, und die untere Lasche wird so gebogen, dass sie die Batterie hält.

Wird eine Batterie mit 17 Ah verwendet, wird die Batterie zur rechten Gehäuseseite geneigt, und die mittlere Lasche wird so gebogen, dass sie die Batterie hält.

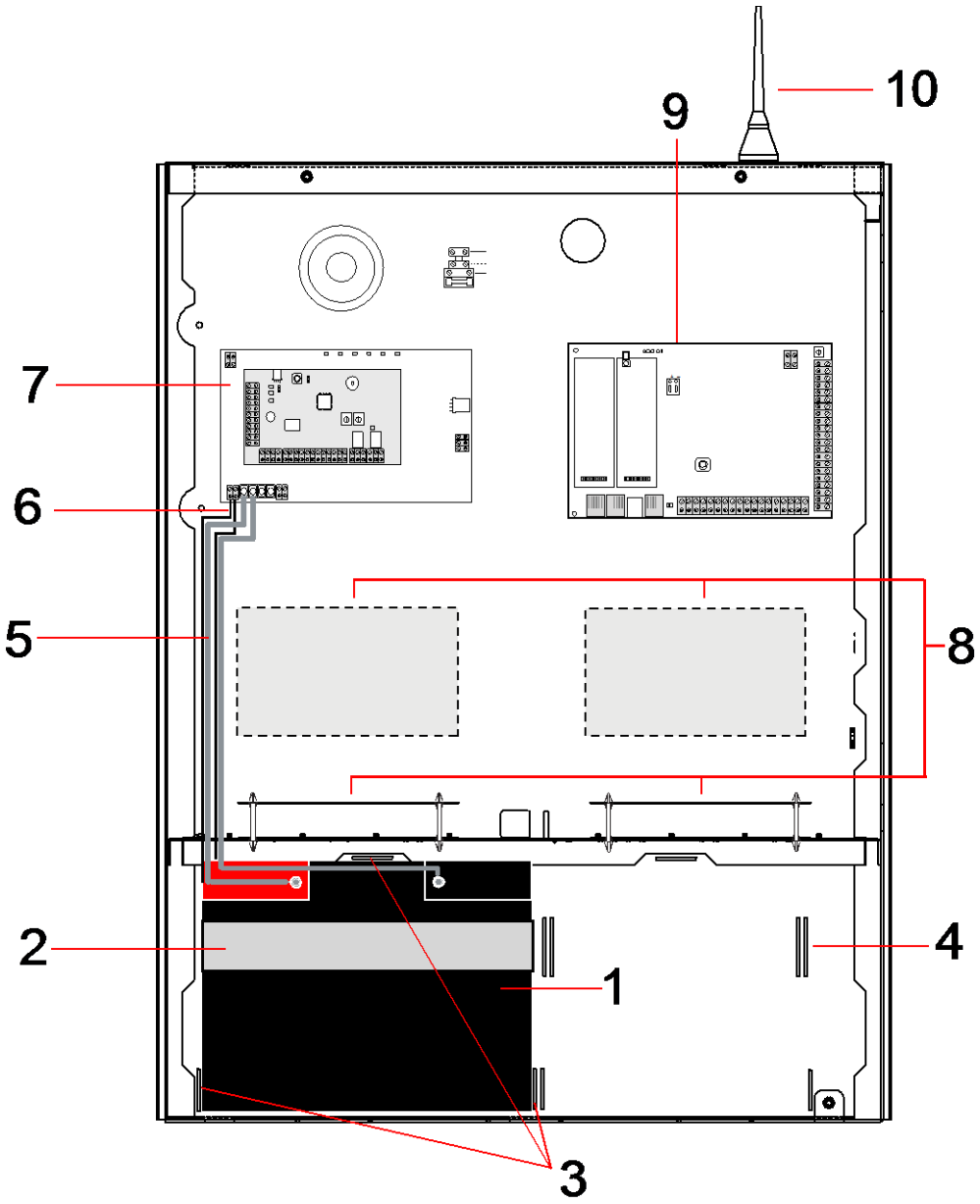
Die Batterie-Haltelaschen sind vorsichtig zu biegen, damit die Batterie nicht beschädigt wird. Sollte die Batterie Anzeichen von Beschädigung aufweisen oder sollte Batterieflüssigkeit auslaufen, ist die Batterie gemäß der jeweils geltenden Vorschriften zu entsorgen, und eine neue Batterie ist einzusetzen.

6.3 Montage eines G5-Gehäuses

Das SPC G5-Gehäuse besteht aus einem Metallunterteil und einem Oberteil. Die Abdeckung ist mit zwei Befestigungsschrauben am oberen und unteren Ende des Oberteils am Unterteil befestigt.

Entfernen Sie zum Öffnen des Gehäuses alle Schrauben mit einem geeigneten Schraubendreher, und heben Sie die Abdeckung vom Unterteil ab.

Das G5-Gehäuse enthält die Controller-Platine (PCB - **P**rinted **C**ircuit **B**oard) sowie das SPC355 Smart-Netzteil, die beide auf vier Montagezapfen befestigt sind. Oben auf dem Netzteil ist ein Erweiterungsmodul mit 8 Ein-/2 Ausgängen befestigt. Vier weitere Zapfen sind im Lieferumfang enthalten. Mit ihnen kann im G5-Gehäuse das Erweiterungsmodul mit 8 Ein-/2 Ausgängen unterhalb der Netzteilplatine eingebaut werden. Zusätzliche Erweiterungen können, wie gezeigt, im Gehäuse eingebaut werden.



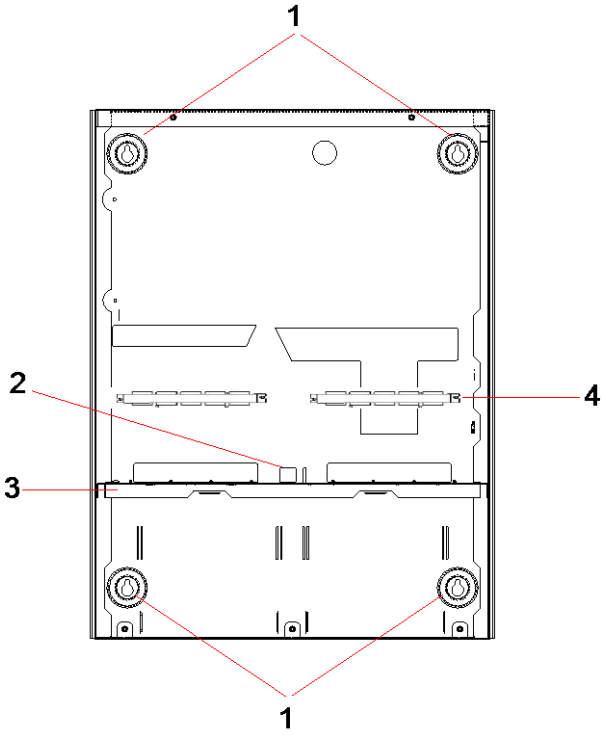
Nummer	Beschreibung	Nummer	Beschreibung
1	Batterie	6	Batterietemperatur-Kabel
2	Befestigungsband für Batterie	7	Netzteil
3	Befestigungslaschen	8	Einbauorte für optionale Erweiterungen
4	Ösen für Haltebänder	9	Controller
5	Batteriekabel	10	Antenne

Im Batteriefach unten im Gehäuse können zwei Batterien mit einer maximalen Kapazität von 27 Ah untergebracht werden.

Bei Metallgehäusen muss außen eine optionale Antenne angebracht werden, wenn Funkverbindungen genutzt werden sollen. Das Gehäuse besitzt an der Oberseite an drei Stellen Ausbrechlöcher, in denen die Antenne angebracht

werden kann. Wird die Einheit mit einer Antenne versehen, muss diese in der Firmware aktiviert werden.

Das SPC G5-Gehäuse besitzt 4 Bohrungen zur Befestigung der Einheit an der Wand.



Nummer	Beschreibung
1	Eckbefestigungen
2	Sabotageschalter-Ausschnitt
3	Trennwand zum Batteriefach
4	Ausschnitt für Telekommunikationsanschlussbuchse

6.3.1 Sabotageschutz

Der Sabotageschalter und die Klammer für den hinteren Sabotagekontakt werden am Gehäuse angebracht. Der Schalter allein dient zum Sabotageschutz der Vorderabdeckung, kann aber auch mit der hinteren Sabotagekontakt-Klammer zusammen zum Sabotageschutz für Vorder- und Rückseite eingesetzt werden. Je nach den lokal geltenden Vorschriften ist Sabotageschutz für Vorder- oder Rückseite erforderlich.

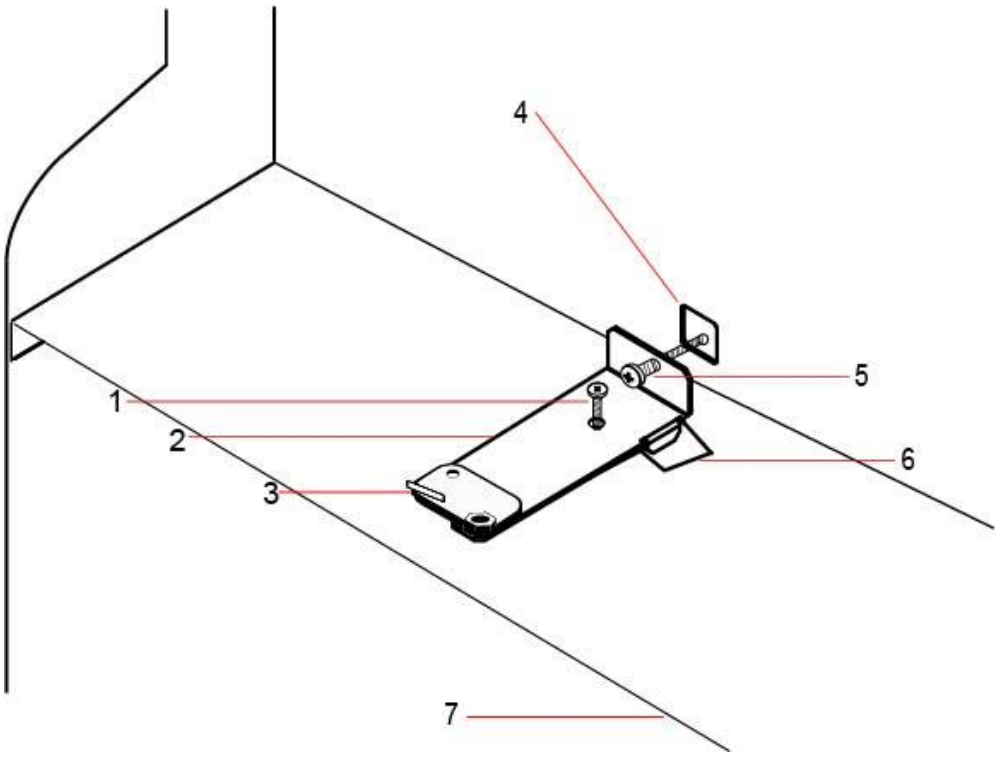
Die Sabotageschutzklammer wird mit einer Befestigungsschraube fixiert. Vergessen Sie nicht, diese Schraube zu lösen, bevor Sie das System für rückwärtigen Sabotageschutz einrichten. Wird nur der vordere Sabotageschutz benutzt, darf diese Schraube nicht gelöst werden.

6.3.2 Montage des Gehäuses mit Sabotageschutz

Gehen Sie bei der Montage wie folgt vor:

1. Markieren Sie mithilfe der im Lieferumfang enthaltenen Montageschablone die Positionen der 4 Bohrlöcher für die Befestigung des Gehäuses an der Wand.

2. Bohren Sie die Löcher, und bringen Sie passende Schrauben an (siehe beiliegende Schablone). Die Schrauben müssen 1,5 cm aus der Wand herausragen.
3. Das G5-Gehäuse ist nur für vorderen Sabotageschutz vorkonfiguriert. Um das Gehäuse für vorderen und rückwärtigen Sabotageschutz vorzubereiten, müssen Sie die Befestigungsschraube für den vorderen Sabotageschutz lösen und entfernen (siehe Element 1).
   ⇨ Die Sabotageschutzklammer schwingt ganz nach rechts im Ausrichtungsschlitz (Element 6).
4. Bringen Sie das G5-Gehäuse in der richtigen Position an der Wand an, und ziehen Sie die 4 Befestigungsschrauben fest. Stellen Sie sicher, dass das Gehäuse nicht von der Wand absteht.
5. Bewegen Sie die Sabotageschutzklammer ganz nach links im Ausrichtungsschlitz, und drehen Sie die Schraube für den rückwärtigen Sabotageschutz (Element 5) fest in die Wand. Die Sabotageschutzklammer sollte im rechten Winkel zur Gehäuserückwand ausgerichtet sein.
6. Bringen Sie den Deckel auf dem Gehäuse an, um den Anschluss des Sabotagekontakts zu überprüfen. Öffnen Sie den Deckel ca. 1 mm, um den Sabotagekontakt auszulösen

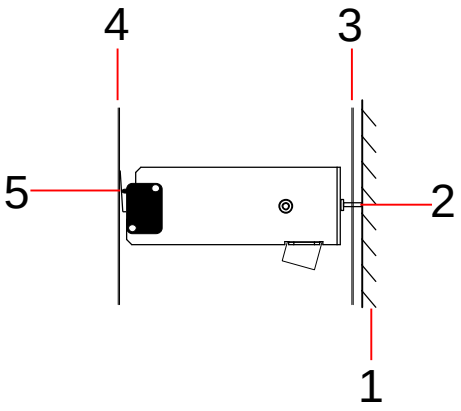


Nummer	Beschreibung	Nummer	Beschreibung
1	Befestigungsschraube für vorderen Sabotageschutz	5	Schraube für rückwärtigen Sabotageschutz
2	Sabotageschutzklammer	6	Ausrichtungsschlitz
3	Sabotagekontakt	7	Trennwand zum Batteriefach
4	Ausschnitt für rückwärtigen Sabotageschutz		

	WARNUNG
	Wenn die Schraube für den rückwärtigen Sabotageschutz nicht fest in der Wand befestigt ist, ist der gesamte Sabotageschutz gefährdet. Wird das Gehäuse von der Wand abgebaut oder verrückt, muss noch einmal überprüft werden, ob der rückwärtige Sabotageschutz funktioniert. Gegebenenfalls muss er neu justiert werden.

6.3.2.1 Funktion des Sabotagekontakts

Sabotagekontakt - Normalstellung



1 Wand

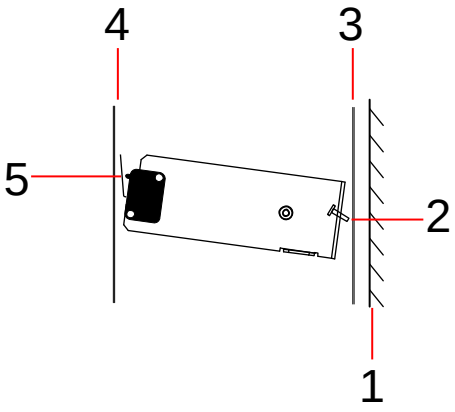
2 Schraube für rückwärtigen Sabotageschutz

3 Gehäuserückwand

4 Gehäusedeckel

5 Kontakt des Sabotageschalters geschlossen

Sabotagekontakt – verschoben



1 Wand

2 Schraube für rückwärtigen Sabotageschutz

3 Gehäuserückwand

4 Gehäusedeckel

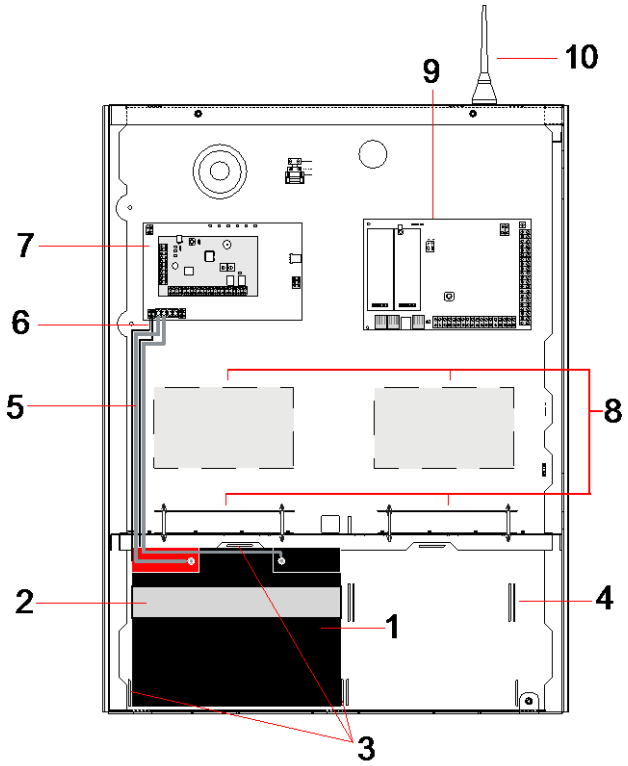
5 Sabotageschalter-Kontakt unterbrochen

Wird das Gehäuse von der Wand abgenommen oder verrückt, steckt die Schraube der Sabotageschutzklammer nicht mehr fest in der Wand und die Klammer dreht sich. Daraufhin dreht sich der Sabotageschalter vom Deckel weg und der Kontakt wird unterbrochen.

	⚠ WARNUNG
	Wenn die Schraube für die Sabotageschutzklammer nicht fest in der Wand befestigt ist, ist der Sabotageschutz gefährdet.

6.3.3 Einsetzen der Batterien

	HINWEIS
	Wird das G5-Gehäuse mit zwei Batterien bestückt, sollten beide Batterien den gleichen Amperestundenwert aufweisen.



1	Batterie	6	Batterietemperatur-Kabel
2	Halteband	7	Netzteil
3	Batterie-Befestigungslaschen	8	Einbauorte für optionale Erweiterungen
4	Ösen für Haltebänder	9	Controller
5	Batteriekabel	10	Antenne

Gehen Sie zum Einbau der Batterien wie folgt vor:

1. Setzen Sie die Batterien in das Batteriefach ein.
2. Drücken Sie die Metalllaschen auf der Oberseite und zu beiden Seiten der Batterien nach innen auf die Batterien.
3. Befestigen Sie jede Batterie mit einem Halteband am Gehäuse. Stellen Sie dabei sicher, dass das Band durch die dafür vorgesehenen Ösen auf der Batteriefachrückseite und um die Batterie herum geführt wird. Die beiden Enden müssen sich auf der Vorderseite der Batterie befinden.
4. Ziehen Sie das Band straff, und schließen Sie den Klettverschluss. Das Halteband muss straff um die Batterie herum gespannt sein.
5. Schließen Sie jeweils ein Ende der Batteriekabel und den „+“- und „-“-Pol der Batterie und das andere Ende an die entsprechenden „+“- und „-“-Eingänge des Netzteils an.

⚠ VORSICHT

Beim Einbau der Batterie muss immer zuerst das Pluskabel (+) an die Batterie angeschlossen werden, und dann erst das Minuskabel (-). Beim Ausbau der Batterie muss zuerst das Minuskabel (-) und dann das Pluskabel (+) abgezogen werden.

6. Schließen Sie die freien Enden der Kabel für die Temperaturüberwachung an die Netzteileingänge für die Batterietemperaturüberwachung an.

6.4 Montage des Bedienteils

Siehe hierzu die entsprechende Montageanleitung.

6.5 Montage einer Erweiterung

Siehe hierzu die entsprechende Montageanleitung.

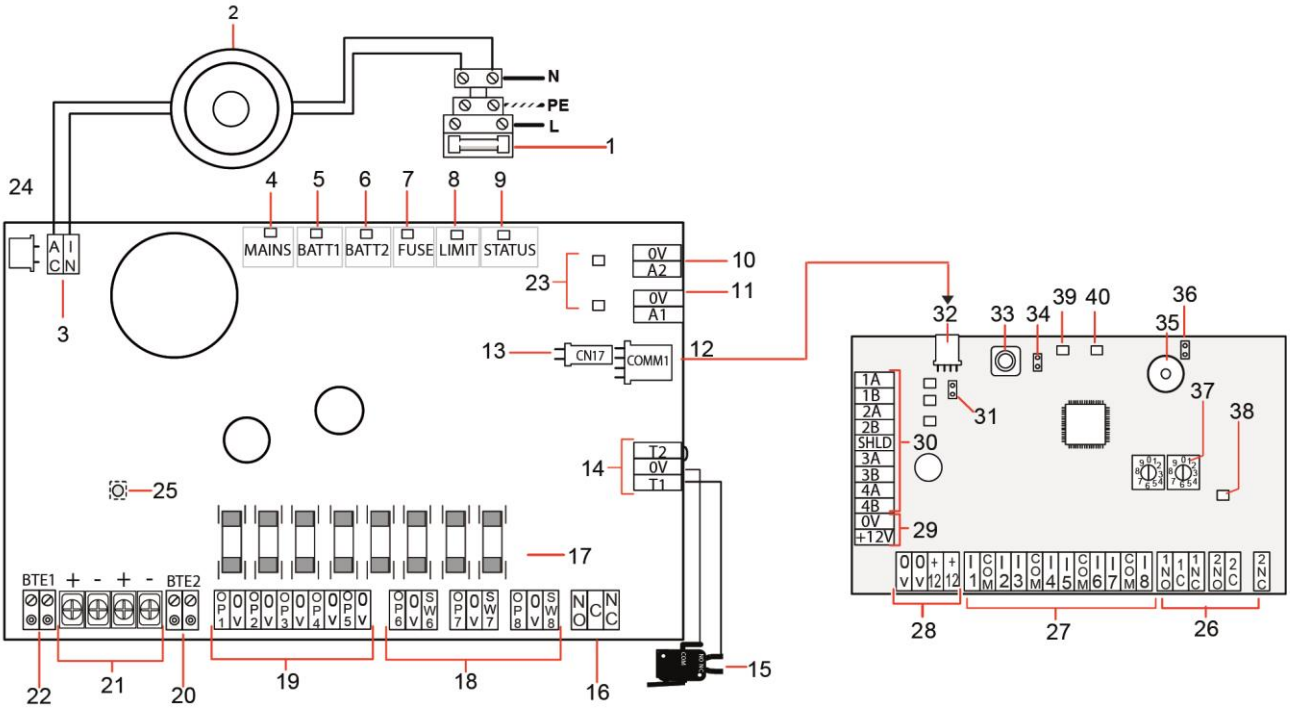
7 Smart-Netzteil

In diesem Abschnitt werden die Komponenten und die Verdrahtung des intelligenten Netzteils beschrieben.

7.1 SPCP355 Smart-Netzteil

Das SPC355 Smart-Netzteil ist eine Kombination aus einem Netzteil und einer Erweiterung für 8 Ein-/2 Ausgänge, die in einem G5-Gehäuse montiert sind. Das Netzteil ist mit 2 Backup-Batterien mit jeweils 24 Ah bzw. 27 Ah ausgestattet und besitzt acht Leistungs- und vier logische Ausgänge

Die Erweiterung überwacht das Netzteil auf Überstrom, Sicherungsausfall, Wechselspannung, Kommunikation und Batterieausgangsspannung. Die Erweiterung wird vom Netzteil über ein Anschlusskabel mit Strom und Daten versorgt. Sie ist außerdem über den SPX X-BUS mit dem SPC-Controller verbunden.



Nummer	Beschreibung
SPCP355 Smart-Netzteil	
1	Netzstromeingang und Sicherungsblock
2	Eingangstransformator
3	**AC IN** – Wechselstromanschluss
4	NETZ – Netz-LED
5	BATT1 – LED für Ladezustand Batterie 1
6	BATT2 – LED für Ladezustand Batterie 2
7	SICH – LED für Sicherungsausfall
8	LIMIT – LED für Strombegrenzung
9	STATUS – Status-LED
10	A2 – Stromversorgungsausgang 14,5 V

Nummer	Beschreibung
	● Kein Backup durch Batterie ● Geschützt durch rücksetzbare PTC-Sicherung mit 300 mA Nennstrom (Element 23 in obiger Abbildung)
11	A1 – Verbindung zum Stromversorgungseingang (+/-) auf SPC5350/6350
12	COMM1 – 4-polige Erweiterungsschnittstelle. Verbindung zu Element 32, Strom- und Datenverbindung, in obiger Abbildung, über ein Durchgangskabel.
13	Referenztakt – Verbindung zu Referenztakt auf SPC5350/6350
14	T1, T2 – Sabotageschalter-Eingänge. Verbinden Sie diese Eingänge mit dem vorderen/rückwärtigen Sabotageschalter Weitere Informationen finden Sie im Abschnitt Montage des Gehäuses mit Sabotageschutz [→ 52].
15	Vorderer/rückwärtiger Sabotageschalter. Weitere Informationen finden Sie im Abschnitt Montage des Gehäuses mit Sabotageschutz [→ 52].
16	NO/NC – Konfigurierbarer logischer Relaisausgang (NO/NC). Weitere Informationen finden Sie im Abschnitt Verdrahtung der Ausgänge [→ 64].
17	Glassicherungen – T-Sicherungen (400 mA) für Ausgänge 1–8
18	A 6–8 und SW 6–8 – Kombinierte Strom- (A) und logische Ausgänge (SW) Standard-Stromausgänge für 12 V DC, kombiniert mit konfigurierbaren logischen Open-Drain-Ausgängen (überwachte/nicht überwachte 4k7-Abschlusswiderstände).
19	A 1–5 – Standard-Stromausgänge für 12 V Weitere Informationen enthält der nachstehende Warnhinweis.
20	BTE2 – Eingang für Temperaturüberwachung Batterie 2
21	BATT1 und BATT2 – Anschlüsse für Batterie 1 und 2
22	BTE1 – Eingang für Temperaturüberwachung Batterie 1
23	PTC-Sicherungen – Sicherungen mit Nennstrom 300 mA. Schützen die Ausgänge A1 und A2. Weitere Informationen finden Sie im Abschnitt Wiederherstellung des Systems [→ 66].
24	PTC-Sicherung – Sicherung mit Nennstrom 5 A. Schützt den Wechselstrom-Eingang (Element 3 in oben stehender Abbildung) Weitere Informationen finden Sie im Abschnitt Wiederherstellung des Systems [→ 66].
25	Kickstart-Schalter für Netzteil – Weitere Informationen finden Sie im Abschnitt Wiederherstellung des Systems [→ 66].
Erweiterungsmodule	
26	NO/NC – Logische Relais-Ausgänge. Auf dem Erweiterungsmodul stehen zwei konfigurierbare logische Ausgänge (NO/NC) zur Verfügung. Weitere Informationen finden Sie im Abschnitt Verdrahtung der Eingänge [→ 63]
27	I 1-8 – Eingänge. Das Erweiterungsmodul verfügt über 8 Linieneingänge, die im SPC-System als Einbruchalarmlinien konfiguriert werden können. Weitere Informationen finden Sie im Abschnitt Verdrahtung der Eingänge [→ 63]
28	Hilfsausgangsspannung (12 V) – Nicht verwenden. Die Stromversorgung der Erweiterung erfolgt über COMM1 auf dem SPCP355 Smart-Netzteil.
29	X-BUS Stromeingang – Nicht verwenden. Die Stromversorgung der Erweiterung erfolgt über COMM1 auf dem SPCP355 Smart-Netzteil.

Nummer	Beschreibung
30	X-BUS-Schnittstelle – Der Kommunikationsbus verbindet die Erweiterungsmodule mit dem SPC-System.
31	Abschlussbrücke – Diese Brücke ist standardmäßig immer gesteckt. Weitere Informationen finden Sie im Abschnitt Verdrahtung der X-BUS-Schnittstelle [→ 62].
32	4-polige Netzteil-Schnittstelle – Verbindung zu COMM1 auf SPCP355 Smart-Netzteil (Element 12 auf oben stehender Abbildung), Strom- und Datenverbindung, über ein Durchgangskabel.
33	Vorderer Sabotageschalter – Nicht verwendet. Bei dieser Installation ist nur der vordere/rückwärtige Sabotagekontakt erforderlich, angeschlossen an T1 und T2 auf dem SPCP355 Smart-Netzteil.
34	JP1 – Der Bypass für den vorderen Sabotagekontakt muss gesteckt sein.
35	Summer – Aktiviert zur Lokalisierung der Erweiterung. Weitere Informationen finden Sie im X-BUS-Menü "LOKALISIEREN" [→ 126].
36	JP6 – Bypass für rückwärtigen Sabotagekontakt. Muss gesteckt sein.
37	Schalter für manuelle Adressierung – Ermöglichen die manuelle Einstellung der Erweiterungs-ID.
38	Status LED für X-BUS – Zeigt den X-BUS-Status wie folgt an, wenn das System im Konfigurationsmodus ist: ● Blinkt langsam (alle 1,5 Sekunden) – Kommunikationsstatus des X-BUS ist in Ordnung. ● Blinkt schnell (alle 0,2 Sekunden) – Zeigt einen der folgenden Sachverhalte an: – Bei Stichleitungskonfigurationen das letzte Erweiterungsmodul in der Leitung. – Ein Problem in der Datenübertragung zwischen zwei Erweiterungen. Wenn zwei nebeneinander liegende Erweiterungen schnell blinken, besteht das Problem zwischen diesen beiden Erweiterungen.
39	LED — nicht verwendet.
40	Netzteil Status LED.

⚠ WARNUNG

Der kombinierte maximale Laststrom, der an allen 12 V-DC-Ausgängen (A 1–8) und COMM1 entnommen werden kann, sollte 2,4 A nicht übersteigen. Jeder einzelne Ausgang für sich und Ausgang A2 sollte 300 mA nicht übersteigen. Ist der Strombedarf des Verbrauchers höher als 300 mA, empfiehlt es sich, die Ausgänge parallel zu schalten.

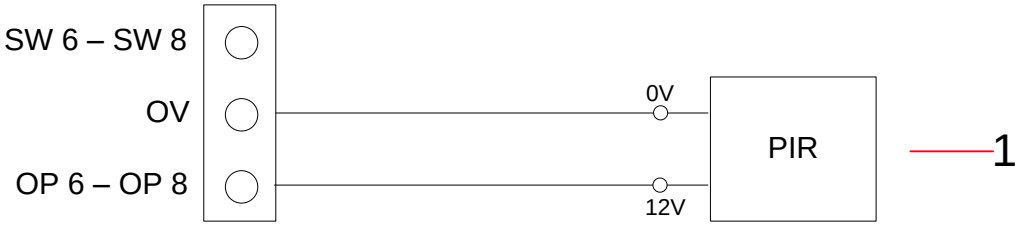
Hinzufügen zusätzlicher Erweiterungen

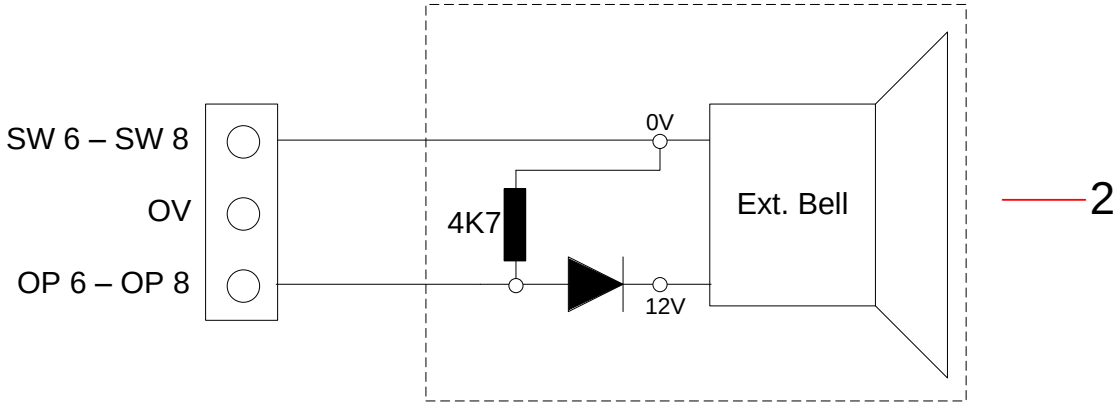
Wenn Sie zusätzliche Erweiterungsmodule in das G5-Gehäuse einbauen, müssen Sie sicherstellen, dass die vorderen und rückwärtigen Sabotagekontakte deaktiviert sind. Hierzu müssen die passenden Brücken gesteckt werden. Bei einem G5-Gehäuse wird der vordere und rückwärtige Sabotageschalter vom Gehäuse selbst und vom SPCP355 Smart-Netzteil gehandhabt.

7.1.1 Überwachte Ausgänge

Das SPCP355 Smart-Netzteil unterstützt drei logische Open-Drain-Ausgänge, die zur Sabotageerkennung überwacht werden können. Die Ausgangssabotageerkennung wird durch Konfiguration aktiviert. Zur Aktivierung der Ausgangssabotageerkennung wird parallel zum Lastgerät, wie z. B. einer

Außensirene, ein 4k7-Abschlusswiderstand geschaltet. Außerdem wird eine Stromdiode (z. B. 1N4001 o.Ä.) benötigt, sofern diese nicht bereits im externen Gerät vorhanden ist.



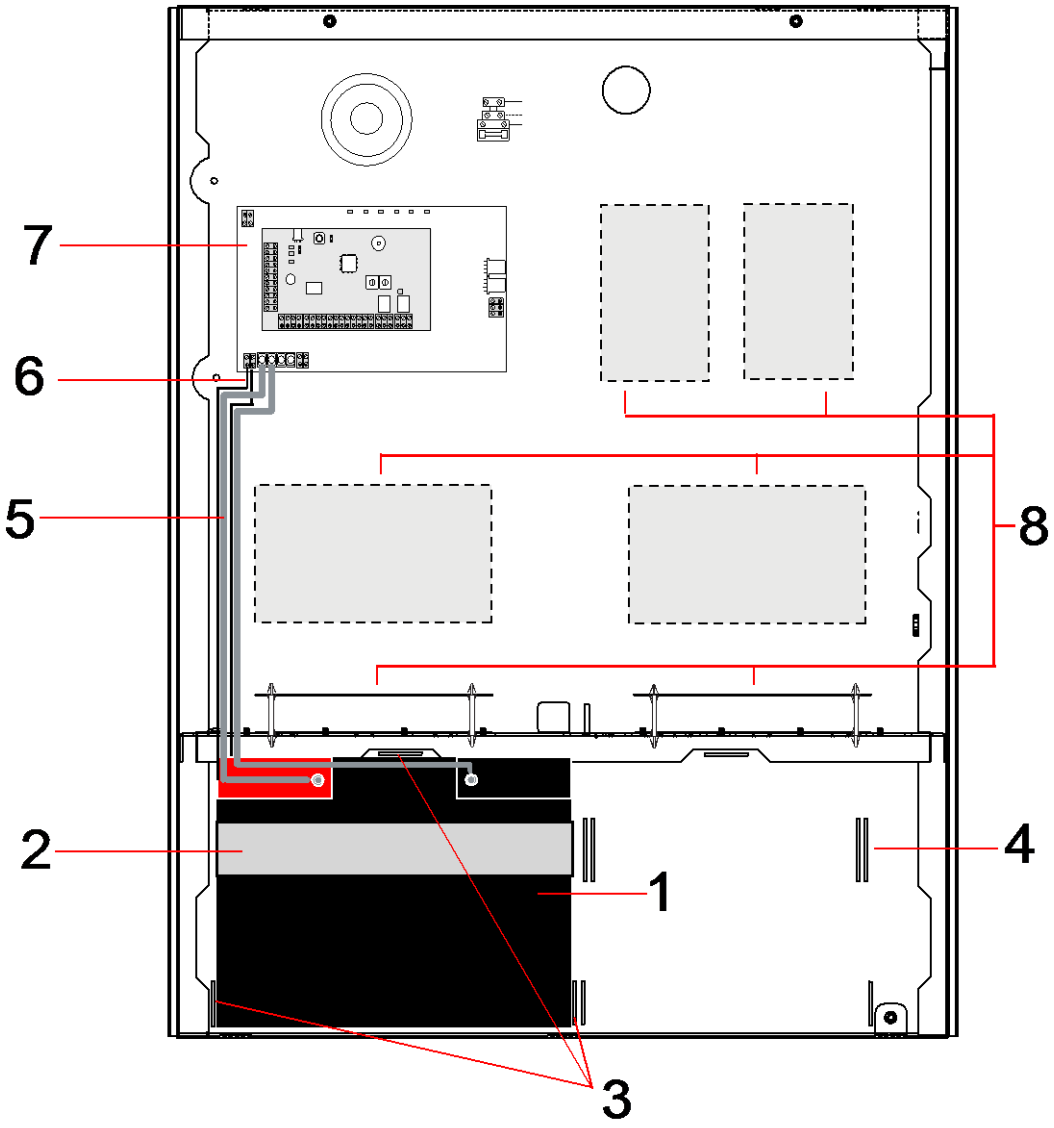


Nummer	Beschreibung
1	Standard-Stromausgang (12 V)
2	Konfigurierbarer, überwachter, geschalteter logischer Ausgang (12 V DC).

7.1.2 Batterien

7.1.2.1 Batterieinstallation

In diesem Abschnitt wird die Installation der Batterien für SPCP355 Smart-Netzteil und G5-Gehäuse beschrieben.



Nummer	Beschreibung
1	Batterie
2	Befestigungsband für Batterie
3	Befestigungsbohrungen
4	Ösen für Haltebänder
5	Batteriekabel
6	Batterietemperatur-Kabel
7	Netzteil\Erweiterung
8	Einbauorte für zusätzliche Erweiterungsmodule.

Es wird empfohlen, zwei Batterien zu verwenden. Die beiden Batterien müssen die gleiche Bauart und Kapazität haben.

1. Setzen Sie die Batterien im Batteriefach ein.

2. Befestigen Sie jede Batterie mit den mitgelieferten Bändern. Dabei muss das Band durch die Ösen hinter der Batterie und um die Batterie herum geführt werden.
3. Verbinden Sie die beiden Enden des Bands vor der Batterie miteinander. Das Band muss straff sitzen.
4. Schließen Sie mit den entsprechenden Kabeln die Batterien in folgender Reihenfolge an das SPCP355 Smart-Netzteil an:
   - Zuerst die Plusleitung (rot) mit dem Pluspol verbinden.
   - Dann die Minusleitung (schwarz) anschließen.

⚠ GEFAHR

Beim Abziehen der Batteriekabel immer zuerst die Minusleitung (schwarz) und dann erst die Plusleitung (rot) lösen.

7.1.2.2 Testen der Batteriespannung

Das SPCP355 Smart-Netzteil führt mit jeder Batterie einen Belastungstest durch. Hierbei wird zwischen die Batteriepole ein Arbeitswiderstand geschaltet und die resultierende Spannung gemessen. Dieser Batterietest wird in Abständen von fünf Sekunden ausgeführt.

7.1.2.3 Tiefentladungsschutz

Falls die Netzstromversorgung des SPCP355 Smart-Netzteils für einen längeren Zeitraum ausfällt, übernehmen die beiden Batterien für einen begrenzten Zeitraum die Stromversorgung für die 12-V-Gleichstromausgänge des Netzteils. Am Ende entladen sich die Batterien. Um die Tiefentladung einer Batterie unter den Punkt zu verhindern, an dem die Batterie unwiederbringlich beschädigt wird, trennt das SPCP355 Smart-Netzteil die Batterie ab, wenn die gemessene Spannung 10,5 V DC unterschreitet. Die Batterie kann wieder aufgeladen werden, sobald die Netzstromversorgung wiederhergestellt ist.

7.1.2.4 Batterie-Standby-Zeiten

Informationen zum Batterie-Standby finden Sie im Abschnitt Berechnung der erforderlichen Batterieleistung [➞ 361].

7.1.3 Verdrahtung der X-BUS-Schnittstelle

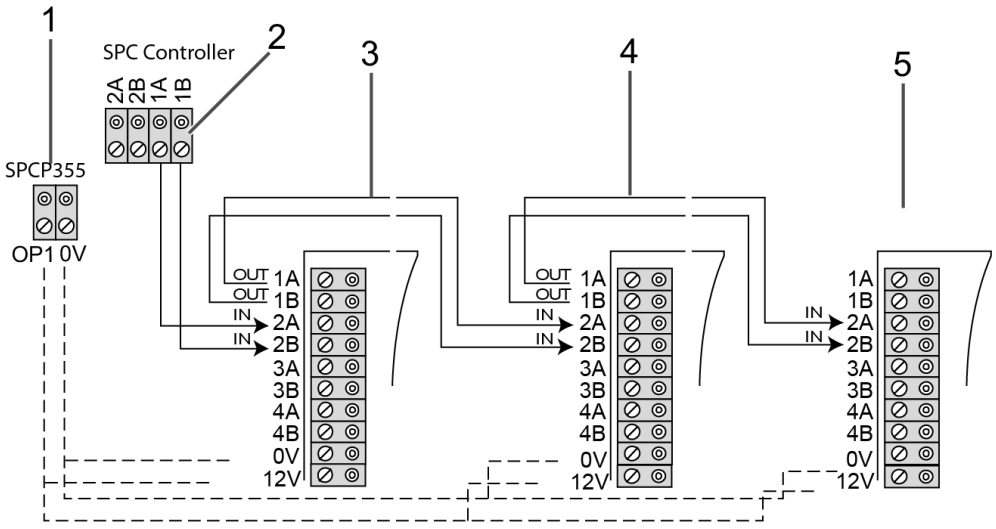
Die X-BUS-Schnittstelle verbindet Erweiterungsmodule und Bedienteile mit dem SPC-Controller. Der X-BUS kann je nach Anforderungen an die Anlage auf unterschiedliche Weise verdrahtet werden.

In der nachstehenden Tabelle sind die empfohlenen Kabeltypen und -längen aufgeführt:

Maximale Kabellänge = (Anzahl der Erweiterungsmodule und Bedienteile im System) × (maximale Entfernung für den jeweiligen Kabeltyp).

Kabeltyp	Länge
CQR-Standardalarmkabel	200 m
UTP cat5-Massivdrahtleiter	400 m
Belden 9829	400 m
IYSTY 2 × 2 ×0,6 (min)	400 m

Das folgende Diagramm zeigt ein Beispiel für die Verdrahtung des X-BUS:



Nummer	Beschreibung
1	Ausgänge des SPCP355 Smart-Netzteils
2	SPC-Zentrale
3	Eingang/Ausgang-Erweiterung für SPCP355
4	Nächste Erweiterung
5	Nächste Erweiterung

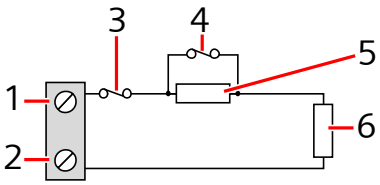
7.1.3.1 Verdrahtung der Eingänge

Das Erweiterungsmodul besitzt 8 Meldergruppeneingänge onboard, die folgendermaßen konfiguriert werden können:

- Kein Endwiderstand
- Einzelner Endwiderstand
- Dualer Endwiderstand
- Anti-Masking-PIR-Konfiguration

Standard-Konfiguration

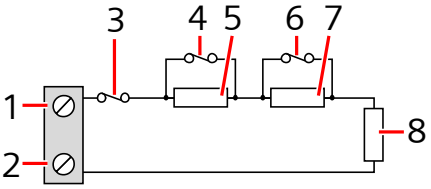
Das folgende Diagramm zeigt eine Standardkonfiguration mit Doppel-Endwiderstand 4K7:



Nummer	Beschreibung
1	Eingang 1
2	COM
3	Sabotage
4	Alarm
5	4K7
6	EOL 4K7

Anti-Masking-PIR-Konfiguration

Das nachstehende Diagramm zeigt die Anti-Masking-PIR-Konfiguration:



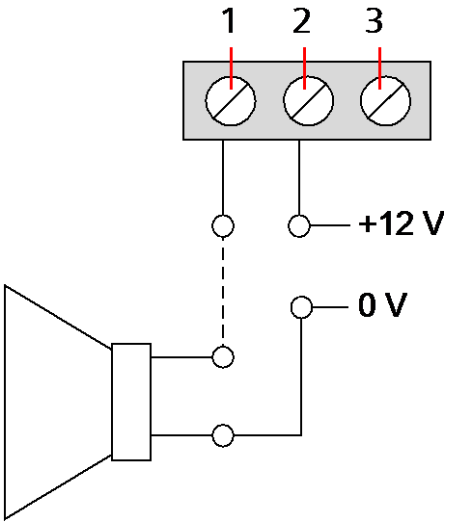
Nummer	Beschreibung
1	Eingang 2
2	COM
3	Sabotage
4	Alarm
5	4K7
6	Melderstörung
7	2K2
8	EOL 4K7

7.1.3.2 Verdrahtung der Ausgänge

Die logischen Relaisausgänge des Erweiterungsmoduls und des Netzteils können beliebigen SPC-Systemausgängen zugewiesen werden. Diese Relaisausgänge können bei 1 A eine Nennspannung von 30 V DC schalten (nicht-induktive Last).

Wenn das Relais aktiviert wird, wird die gemeinsame Klemme (COM) von einem Ruhekontakt (NC) auf einen Schließkontakt (NO) umgeschaltet.

Folgende Abbildung zeigt die Verdrahtung eines Active-High-Ausgangs.



Nummer	Beschreibung
1	Arbeitskontakt (NO)
2	Gemeinsame Anschlussklemme (COM)
3	Ruhekontakt (NC)

7.1.4 LEDs für Netzteil-Statusanzeige

In der folgenden Tabelle ist zusammengefasst, welche Statusinformationen mit den LEDs angezeigt werden:

LED	NETZ	BATT 1 & 2	SICH	LIMIT	STATUS
FARBE	Grün	Grün	Rot	Rot	Grün
Bedingung					
Normal	Ein	Ein	Aus	Aus	Ein
Netz OK, Batterie wird geladen	Ein	Blinkt			Ein
Netz ausgefallen, Batterie OK	Aus	Ein			Ein
Netz OK, Batterie defekt oder nicht vorhanden	Ein	Aus			Ein
Netz OK, Batterie defekt, nicht vorhanden oder im Modus Tiefentladungsschutz	Alle LEDs aus.				
Sicherungsausfall			Ein		Ein
Gesamtlaststrom überschritten				Ein	Ein
Störung an PSU-Umschalter	Aus				Blinkt

7.1.5 Wiederherstellung des Systems

Ausfall von Netz und Batterie

Fallen sowohl die Netz- als auch die Batterie-Stromversorgung aus, kann mit dem Kickstart-Schalter des Netzteils (Element 25 in SPCP355 Smart-Netzteil [→ 57]) das System neu gestartet werden, sobald zumindest die Batterie-Stromversorgung wiederhergestellt ist. Führen Sie für einen Kickstart des Systems folgende Schritte aus:

▷ Netz-Stromversorgung ist ausgefallen

▷ Batterie-Stromversorgung ist ausgefallen

▷ Neue Batterien stehen zur Verfügung

1. Schließen Sie die Batteriekabel an.
2. Drücken Sie den Kickstart-Knopf auf dem Netzteil und halten Sie ihn gedrückt.
   ⇨ Alle LEDs blinken.
3. Halten Sie den Kickstart-Knopf auf dem Netzteil so lange gedrückt, bis die LEDs erlöschen.
4. Lassen Sie den Kickstart-Knopf auf dem Netzteil los.

Zurücksetzen der PTC-Sicherung

Zum Zurücksetzen der PTC-Sicherungen müssen Sie die Netz- und Batterie-Stromversorgung von Hand unterbrechen und wiederherstellen.

8 Controller-Hardware

In diesem Abschnitt wird die Hardware der Zentrale beschrieben.

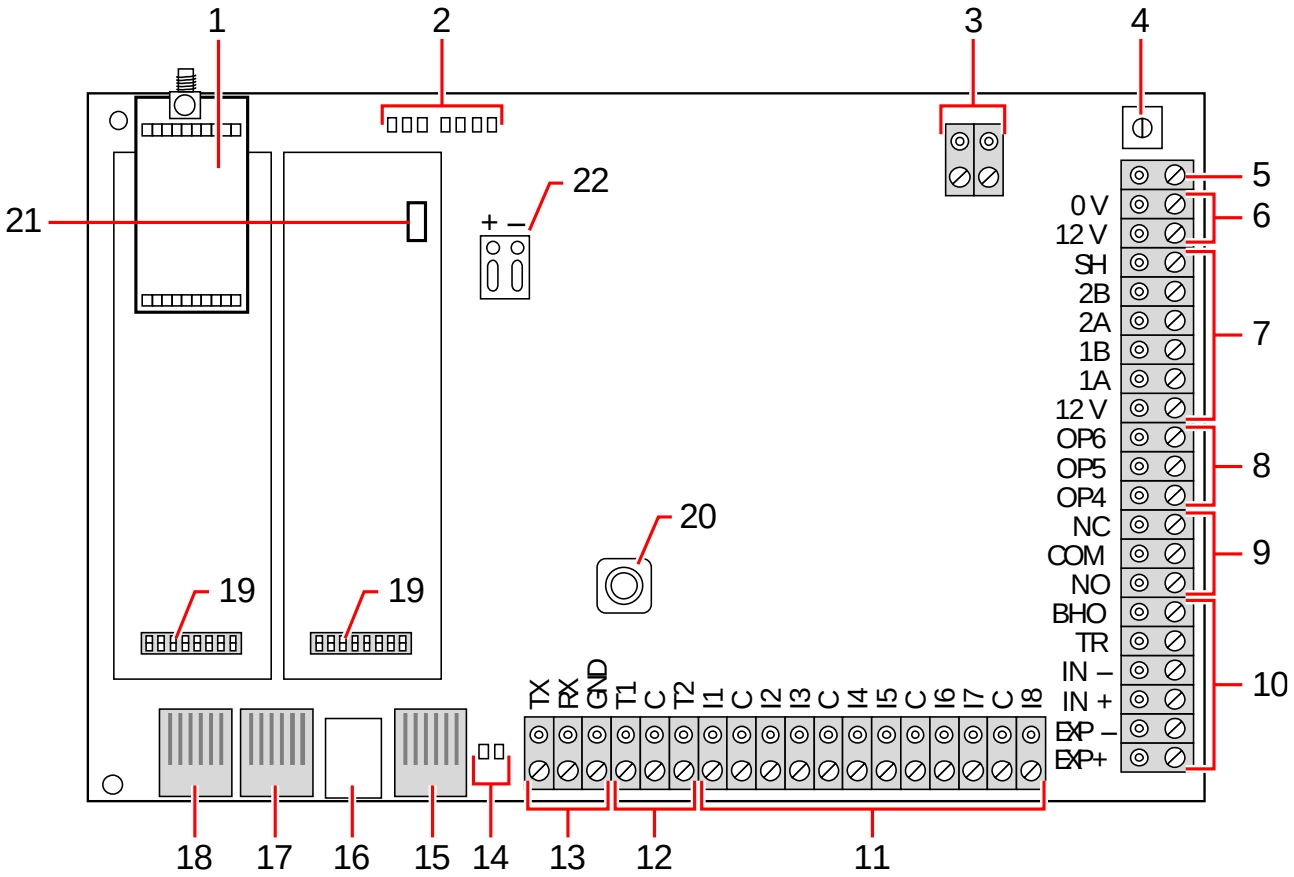
Siehe auch

- Stromversorgung der Erweiterungsmodule über die Hilfsstromversorgungsanschlüsse [→ 360]
- Verdrahtung der X-BUS-Schnittstelle [→ 74]
- Verdrahten eines internen Tongenerators [→ 90]
- Verdrahtung Linieneingänge [→ 86]
- LEDs für Controller-Status [→ 359]
- LEDs für Controller-Status [→ 359]
- Stromversorgung der Erweiterungsmodule über die Hilfsstromversorgungsanschlüsse [→ 360]
- Verdrahtung der X-BUS-Schnittstelle [→ 74]
- Verdrahten eines internen Tongenerators [→ 90]
- Verdrahtung Linieneingänge [→ 86]

8.1 Hardware der Zentralen 42xx\43xx\53xx\63xx

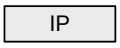
In diesem Abschnitt wird die Zentrale für die Modelle SPC42xx, 43xx, 53xx und 63xx beschrieben. Die Modelle SPC5350 und SPC6350 werden im Kapitel Hardware der Zentralen SPC5350 und 6350 [→ 69] beschrieben.

Die SPC-Zentrale bietet 8 integrierte verdrahtete Meldergruppen und optionale drahtlose Meldergruppen.



1	Optionales Funkmodul	Die Controller-Platine kann werksseitig mit einem Funkmodul für den Einsatz mit Funksensoren (868 MHz) ausgerüstet sein.

2	SPC Status-LEDs	Diese 7 LEDs zeigen den Status verschiedener Systemparameter gemäß der Beschreibung auf Seite [→ 359] an.
3	Netzstromeingang	Netzeingang: Die Netzeingangsspannung wird über einen Transformator im SPC-Gehäuse auf diesen zweipoligen Anschluss angelegt. Der Erdleiter des Netzkabels wird an einem Anschlusspunkt am Metallgehäuse befestigt. Referenztakt*: Auf diesen 2-poligen Anschluss kann auch ein Referenztaktsignal angewendet werden, um eine genaue Systemzeit einzuhalten.
4	Reset-Taste	● Zurücksetzen des Controllers: – Drücken Sie die Taste einmal. ● Zum Zurücksetzen der programmierten Einstellungen auf die Standardwerte und Neustarten des Controllers: – Halten Sie die Taste gedrückt, bis die Frage erscheint, ob eine Zurücksetzung auf die Werkseinstellungen gewünscht ist. – Wählen Sie JA aus, um die Werkseinstellungen wiederherzustellen. **Warnung**: Beim Zurücksetzen der Zentrale auf die Werkseinstellungen werden alle Konfigurationsdateien einschließlich der auf der Zentrale gespeicherten Sicherungskopien gelöscht. Alle Abschaltungen und Sperren werden ebenso gelöscht. Wir empfehlen, auf einem PC eine Sicherungskopie der Konfigurationsdaten anzulegen, bevor Sie die Zentrale auf die Werkseinstellungen zurücksetzen. **Hinweis**: Diese Funktion steht nicht zur Verfügung, wenn die Technikersperre aktiviert ist.
5	Erdungsanschlussklemme	Diese Klemme ist nicht erforderlich und sollte nicht belegt werden.
6	Zusatzausgang (12 V)	Der SPC-Controller verfügt über einen zusätzlichen 12-V-Gleichstromausgang, der verwendet werden kann, um Erweiterungsmodule und Vorrichtungen wie Riegel, Sirenen usw. mit Strom zu versorgen. Siehe Seite [→ 360]. Der Höchstnennstrom beträgt 750 mA. **Bitte beachten**: Die Stromaufnahme ist abhängig von der Zeitspanne, für welche die Funktion bei Batteriebetrieb aufrechterhalten werden soll.
7	X-BUS-Schnittstelle	Dies ist der SPC-Kommunikationsbus, mit dem Erweiterungsmodule im System untereinander verbunden werden. Siehe Seite [→ 74]. SPC4000 besitzt nur 1 X-BUS-Schnittstelle.
8	Integrierte Ausgänge	Die Ausgänge OP4, OP5 und OP6 sind ohmsche Open Collector 12-V-Ausgänge, die sich einen Nennstrom von 400 mA mit dem 12-V-Ausgang teilen. Sind die Ausgänge nicht an die 12-V-Versorgung des Controllers angeschlossen, sondern werden über eine externe Stromquelle versorgt, muss der Nullleiter der Stromquelle an den Nullleiter des Controllers angeschlossen werden. Die Spannung der externen Stromquelle darf in diesem Fall 12 V nicht überschreiten.
9	Relaisausgang	Der SPC-Controller verfügt über ein einpoliges 1-A-Umschaltrelais, das zur Ansteuerung des Blitzleuchtenausgangs an der Außensirene verwendet werden kann.
10	Außensirene / Innensirene	Die Ausgänge für die Innen- und Außensirene (INT+, INT-, EXT+, EXT-) sind ohmsche Ausgänge mit 400 mA Nennstrom. Die BHO (**B**ell **H**old **O**ff)-, **TR** (**T**amper **R**eturn)- und EXT-Ausgänge dienen dem Anschluss einer Außensirene an den Controller. Die Klemmen INT+ und INT- dienen dem Anschluss interner Vorrichtungen wie etwa einer Innensirene. Siehe Seite [→ 90].
11	MG-Eingänge	Der Controller verfügt über 8 integrierte Meldergruppen-Eingänge, die mit Hilfe verschiedener Überwachungskonfigurationen überwacht werden können. Die Konfigurationen können bei der Systemprogrammierung eingegeben werden. Die Standardkonfiguration ist **D**ual **E**nd **o**f **L**ine (DEOL) mit einer Widerstandskombination von 4K7. Siehe Seite [→ 86].
12	Sabotagekontakt-Anschlüsse	Der Controller verfügt über 2 zusätzliche Sabotageeingänge, die mit zusätzlichen Sabotage-Erkennungsvorrichtungen verbunden werden können, wenn ein erhöhter Sabotageschutz gewünscht ist. Diese Anschlüsse sollten kurzgeschlossen werden, wenn sie nicht verwendet

		werden.
13	Anschlussklemme - Serieller Port 2 	Der Anschlussklemmenblock für den seriellen Port 2 (TX, RX, GND) kann verwendet werden, um ein externes Modem oder ein PC-Terminal-Programm anzuschließen. Der serielle Port 2 teilt sich einen Kommunikationskanal mit dem Backup-Modem. Achten Sie darauf, dass keine Vorrichtungen an diesen seriellen Port angeschlossen werden, wenn ein Backup-Modem installiert ist.
14	 LEDs für die Ethernet-Verbindung	Die 2 Ethernet-LEDs zeigen den Status der Ethernet-Verbindung an. Die linke LED zeigt Datenaktivität am Ethernet-Port an; die rechte LED zeigt, an, dass die Ethernet-Verbindung aktiv ist.
15	 Ethernet-Schnittstelle	Die Ethernet-Schnittstelle ermöglicht den Anschluss eines PCs an den Controller, mit dem das System programmiert werden kann.
16	USB-Anschluss	Der USB-Anschluss dient zur Herstellung einer Verbindung für die Browser-Programmierung oder zu einem Terminal-Programm.
17	Serieller Port 2 	Dieser RS232 serielle Port kann verwendet werden, um ein externes Modem oder ein PC-Terminal-Programm anzuschließen. Der serielle Port 2 teilt sich einen Kommunikationskanal mit dem Backup-Modem. Achten Sie darauf, dass keine Vorrichtungen an diesen seriellen Port angeschlossen werden, wenn ein Backup-Modem installiert ist.
18	Serielle Schnittstelle 1	Dieser RS232 serielle Port kann verwendet werden, um ein Gerät mit X10-Protokoll anzuschließen.
19	Optionale Einsteckmodule	Ein Primärmodul (linker Steckplatz) und eine Backup-Modul (rechter Steckplatz) können an den Controller angeschlossen werden. Bei diesen Modulen kann es sich um GSM- oder PSTN-Modems handeln, die eine erweiterte Kommunikation ermöglichen. Das Backup-Modem sollte nicht angeschlossen werden, falls ein externes Modem oder ein sonstiges Gerät an den seriellen Port 2 angeschlossen ist.
20	Sabotageschalter an der Frontplatte	Der eingebaute Sabotageschalter an der Frontplatte (Schalter/Schalter) schützt das Gehäuse vor Manipulation. **Hinweis**:Der vordere Sabotageschutz wird im G5-Gehäuse nicht verwendet.
21	Batterieauswahl	J12: Jumper für 17-Ah-Batterie anbringen und für 7-Ah-Batterie entfernen. Bitte beachten: Diese Auswahl ist nur auf der Controller-Leiterplatine der Änderungsversion 2.3 verfügbar. (Gilt nicht für SPC5350- und SPC5360-Zentralen)
22	Hilfsversorgungsspannung	12-V-Eingang der Batterie oder des Netzteils**.

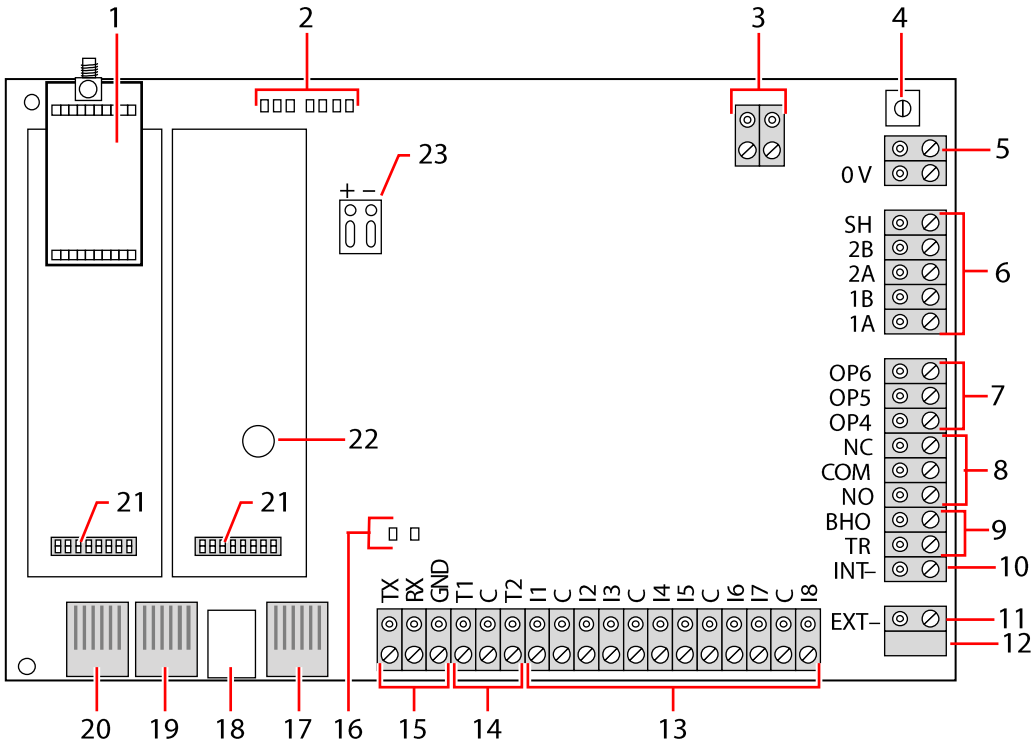
* Standardeinrichtung für SPC5350- und SPC5360-Zentralen

** Netzteil gilt nur für SPC5350- und SPC5360-Zentralen

8.2 Hardware der Zentralen SPC5350 und 6350

In diesem Kapitel werden die Modelle SPC5350 und SPC6350 beschrieben.

Die von Werk aus eingestellte XBUS Adresse(ID01) der Erweiterung auf dem Netzteil im G5 Gehäuse, darf nicht verändert werden.



1	Optionales Funkmodul	Die Controller-Platine kann werksseitig mit einem Funkmodul für den Einsatz mit Funksensoren (868 MHz) ausgerüstet sein.
2	SPC Status-LEDs	Diese 7 LEDs zeigen den Status verschiedener Systemparameter gemäß der Beschreibung auf Seite [→ 359].
3	Referenztakt	Auf diesen 2-poligen Anschluss kann auch ein Referenztaktsignal angewendet werden, um eine genaue Systemzeit einzuhalten. Verbindung zu Referenztakt CN17 auf SPCP355 Smart-Netzteil.
4	Reset-Taste	● Zurücksetzen des Controllers: – Drücken Sie die Taste einmal. ● Zum Zurücksetzen der programmierten Einstellungen auf die Standardwerte und Neustarten des Controllers: – Halten Sie die Taste gedrückt, bis die Frage erscheint, ob eine Zurücksetzung auf die Werkseinstellungen gewünscht ist. – Wählen Sie JA aus, um die Werkseinstellungen wiederherzustellen. **Warnung**: Beim Zurücksetzen der Zentrale auf die Werkseinstellungen werden alle Konfigurationsdateien einschließlich der auf der Zentrale gespeicherten Sicherungskopien gelöscht. Alle Abschaltungen und Sperren werden ebenso gelöscht. Wir empfehlen, auf einem PC eine Sicherungskopie der Konfigurationsdaten anzulegen, bevor Sie die Zentrale auf die Werkseinstellungen zurücksetzen. **Hinweis**: Diese Funktion steht nicht zur Verfügung, wenn die Technikersperre aktiviert ist.
5	Erdungsanschlussklemme	Diese Klemme ist nicht erforderlich und sollte nicht belegt werden.

6	X-BUS-Schnittstelle	Dies ist der SPC-Kommunikationsbus, mit dem Erweiterungsmodule im System untereinander verbunden werden. Siehe Seite [→ 74]. Terminal 1B und 1A müssen mit Terminal 2A bzw. 2B auf der SPCP355-E/A-Erweiterung verbunden werden. Terminal 2A und 2B müssen mit Terminal 2A bzw. 2B auf der nächsten Erweiterung auf dem X-BUS verbunden werden.
7	Integrierte Ausgänge	Die Ausgänge OP4, OP5 und OP6 sind ohmsche Open Collector 12-V-Ausgänge, mit einem Nennstrom von 300 mA. Der OP4-Lastausgang muss an das SPCP355 Smart-Netzteil angeschlossen werden.
8	Relaisausgang	Der SPC-Controller verfügt über ein einpoliges 1-A-Umschaltrelais, das zur Ansteuerung des Blitzleuchtenausgangs an der Außensirene verwendet werden kann.
9	Sirene zurückhalten (BHO) und Sabotagealarm zurück (TR)	BHO (**B**ell **H**old **O**ff) und **TR** (**T**amper **R**eturn) sowie der EXT-Ausgang werden zum Anschluss einer Außensirene an die Zentrale verwendet. Siehe Seite [→ 90].
10	Innensirene (-)	Das Terminal INT- wird zum Anschluss interner Geräte wie etwa einem internen Tongenerator benutzt. Die Stromversorgung für den internen Tongenerator muss an das SPCP355 Smart-Netzteil angeschlossen werden.
11	Außensirene (-)	Das Terminal EXT- wird zum Anschluss externer Geräte wie etwa einer Außensirene benutzt. Die Stromversorgung für den internen Tongenerator muss an das SPCP355 Smart-Netzteil angeschlossen werden.
12	Nicht verwenden.	Nicht verwenden.
13	MG-Eingänge	Der Controller verfügt über 8 integrierte Meldergruppen-Eingänge, die mit Hilfe verschiedener Überwachungskonfigurationen überwacht werden können. Die Konfigurationen können bei der Systemprogrammierung eingegeben werden. Die Standardkonfiguration ist **D**ual **E**nd **o**f **L**ine (DEOL) mit einer Widerstandskombination von 4K7. Siehe Seite [→ 86].
14	Sabotagekontakt-Anschlüsse	Der Controller verfügt über 2 zusätzliche Sabotageeingänge, die mit zusätzlichen Sabotage-Erkennungsvorrichtungen verbunden werden können, wenn ein erhöhter Sabotageschutz gewünscht ist. Diese Anschlüsse sollten kurzgeschlossen werden, wenn sie nicht verwendet werden.
15	Anschlussklemme - Serieller Port 2	Der Anschlussklemmenblock für den seriellen Port 2 (TX, RX, GND) kann verwendet werden, um ein externes Modem oder ein PC-Terminal-Programm anzuschließen. Der serielle Port 2 teilt sich einen Kommunikationskanal mit dem Backup-Modem. Achten Sie darauf, dass keine Vorrichtungen an diesen seriellen Port angeschlossen werden, wenn ein Backup-Modem installiert ist.
16	LEDs für die Ethernet-Verbindung	Die 2 Ethernet-LEDs zeigen den Status der Ethernet-Verbindung an. Die linke LED zeigt Datenaktivität am Ethernet-Port an; die rechte LED zeigt, an, dass die Ethernet-Verbindung aktiv ist.
17	Ethernet-Schnittstelle	Die Ethernet-Schnittstelle ermöglicht den Anschluss eines PCs an den Controller, mit dem das System programmiert werden kann.
18	USB-Anschluss	Der USB-Anschluss dient zur Herstellung einer Verbindung für die Browser-Programmierung oder zu einem Terminal-Programm.
19	Serieller Port 2	Dieser RS232 serielle Port kann verwendet werden, um ein externes Modem oder ein PC-Terminal-Programm anzuschließen. Der serielle Port 2 teilt sich einen Kommunikationskanal mit dem Backup-Modem. Achten Sie darauf, dass keine Vorrichtungen an diesen seriellen Port angeschlossen werden, wenn ein Backup-Modem installiert ist.
20	Serielle Schnittstelle 1	Dieser RS232 serielle Port kann verwendet werden, um ein Gerät mit X10-Protokoll anzuschließen.

21	Optionale Einsteckmodule	Ein Primärmodul (linker Steckplatz) und eine Backup-Modul (rechter Steckplatz) können an den Controller angeschlossen werden. Bei diesen Modulen kann es sich um GSM- oder PSTN-Modems handeln, die eine erweiterte Kommunikation ermöglichen. Das Backup-Modem sollte nicht angeschlossen werden, falls ein externes Modem oder ein sonstiges Gerät an den seriellen Port 2 angeschlossen ist.
22	Batterie für Echtzeituhr	Batterie für Echtzeituhr (RTC)
23	Hilfsversorgungsspannung	12-V-Eingang von A1 auf dem SPCP355 Smart-Netzteil

Siehe auch

Stromversorgung der Erweiterungsmodule über die Hilfsstromversorgungsanschlüsse [→ 360]

9 Türerweiterung

Die Zweitür-Erweiterung ist eine Steuereinheit für bis zu zwei Türen und zwei Ausweisleser. Die Konfiguration des Betriebsmodus erfolgt über die E/As der beiden angeschlossenen Türen. Die Funktionen der beiden Eingänge und des Ausgangs der Türsteuereinheit werden über die Tür-E/As gesteuert. Einer Tür-E/A-Einheit kann eine bestimmte Türnummer zugewiesen werden, über welche den Ein- und Ausgänge vordefinierte Funktionen zugewiesen werden. Wird keinem der Tür-E/As eine Nummer zugewiesen (Option „Meldergruppen“ ist ausgewählt), können die Eingänge und Ausgänge der Türsteuereinheit wie Ein- und Ausgänge innerhalb der Zentrale verwendet werden. Dann stehen an der Zweitürsteuereinheit keine Zugangskontrollfunktionen zur Verfügung.

Wird nur den E/As der ersten Tür der Zweitürsteuereinheit eine Türnummer zugewiesen, wird der erste Leser als Eingangsleser für diese Tür verwendet. Ist ein zweiter Leser vorhanden, wird dieser als Ausgangsleser für die konfigurierte Tür verwendet. Zwei Eingänge und ein Ausgang besitzen vordefinierte Funktionen, und zwei Eingänge und ein Ausgang können vom Benutzer konfiguriert werden. Zusätzlich kann der Eingang des Türzustandssensors der ersten Tür als Einbruch-MG verwendet werden, jedoch mit eingeschränkter Funktionalität.

Wird jeder der beiden Tür-E/As eine Türnummer zugewiesen, werden die beiden Türen unabhängig voneinander behandelt. Der erste Ausweisleser wird als Eingangsleser für die erste Tür verwendet, der zweite Ausweisleser wird als Eingangsleser für die zweite Tür verwendet. Alle Eingänge und Ausgänge haben vordefinierte Funktionen. Die Türzustandssensor-Eingänge der beiden Türen können zusätzlich als Einbruch-MG verwendet werden, jedoch nur mit eingeschränkter Funktionalität.

Weitere Informationen zu derzeit unterstützten Ausweislesern und Ausweisformaten finden Sie im Anhang [→ 383].

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

10 Verdrahtung des Systems

10.1 Verdrahtung der X-BUS-Schnittstelle

Die X-BUS-Schnittstelle stellt die Anschlüsse von Erweiterungsmodulen an den Controller bereit. Der X-BUS kann je nach Anforderungen der Installation in unterschiedlichen Konfigurationen verkabelt werden. Die Baudrate der X-BUS-Schnittstelle beträgt 307 kBit/s.

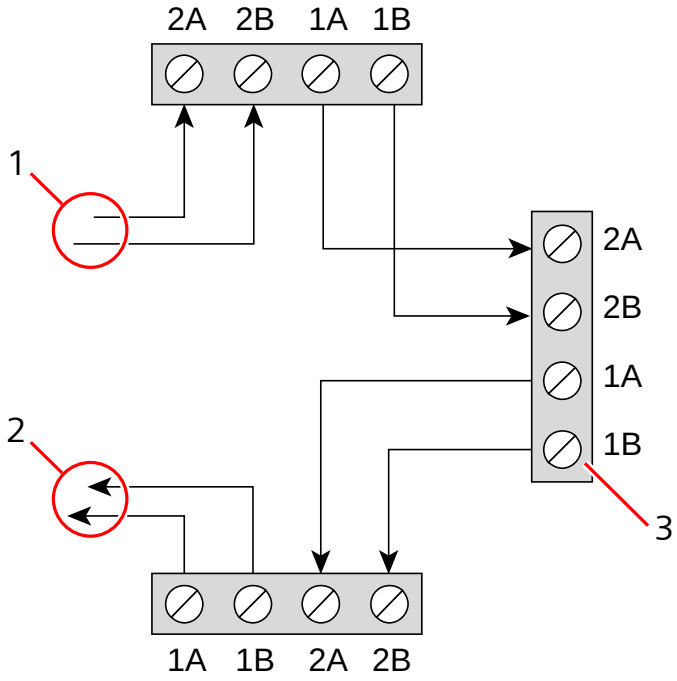
	*HINWEIS*
	Der X-BUS ist ein Bus vom Typ RS-485 mit einer Baudrate von 307 kBit/s. Die vollständige Leistung wird nur in der Stichleitungs- [→ 75] und durchschleifbaren [→ 76] Anschlusskonfiguration unterstützt (beste Signalqualität aufgrund der Verkettungsanordnung isolierter Bereiche mit 1 Sender / 1 Empfänger und ausgeglichenen Abschlusswiderständen an jedem Ende). Die Leistung in der Stern- [→ 77] oder Multidrop [→ 77]-Anschlusskonfiguration ist aufgrund von suboptimalen Bedingungen der RS-485-Busspezifikation begrenzt (reduzierte Signalqualität aufgrund von mehreren parallel geschalteten Sendern / Empfängern mit unausgeglichenen Abschlusswiderständen).

	*HINWEIS*
	Es wird dringendst empfohlen, die Stichleitungs- [→ 75] oder durchschleifbare [→ 76] Konfiguration zu verwenden.

Die untere Tabelle zeigt die maximalen Abstände zwischen Controller/Erweiterung oder Erweiterung/Erweiterung für alle Kabeltypen in der durchschleifbaren und Stichleitungskonfiguration.

Kabeltyp	Länge
CQR-Standardalarmkabel	200 m
UTP-Kategorie: 5 (Massivdrahtleiter)	400 m
Belden 9829	400 m
IYSTY 2 × 2 × 0,6 (min)	400 m

Jedes Gerät hat 4 Klemmen (1A, 1B, 2A, 2B) für den Anschluss von Erweiterungsmodulen über das X-BUS-Kabel. Der Controller initiiert beim Einschalten einen Erkennungsprozess, bei dem die Anzahl der an das System angeschlossenen Erweiterungsmodule und die Anschlusstopologie erkannt werden.



Verkabelung von Erweiterungsmodulen

1	Vorangegangene Erweiterung
2	Nächste Erweiterung
3	SPC-Controller

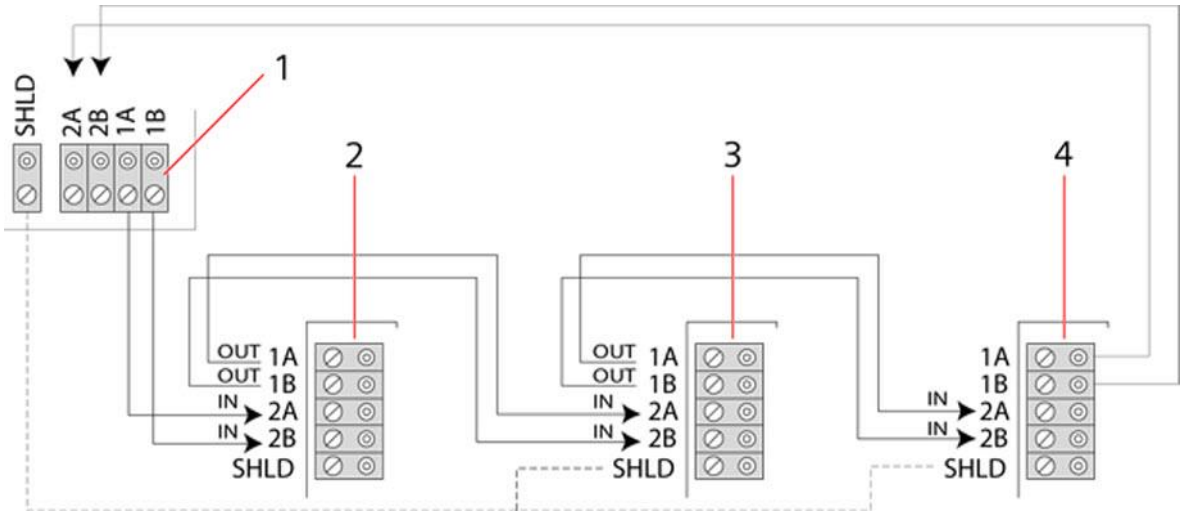
Die meisten Erweiterungen sind mit den zusätzlichen Klemmen 3A/3B und 4A/4B für die Verkabelung von Abzweig-Erweiterungsmodulen ausgestattet. Siehe Seite [→ 84] für weitere Anleitungen zur Verkabelung von Abzweig-Erweiterungsmodulen.

10.1.1 Durchschleifbare Konfiguration

	HINWEIS
	~~4000~~ Der SPC42xx/43xx unterstützt nicht die durchschleifbare Konfiguration (nur 1 X-BUS-Anschluss).

	HINWEIS
	Alle Erweiterungen/Bedienteile werden standardmäßig mit einem Abschluss-Jumper angebracht. In der durchschleifbaren Konfiguration ist es absolut erforderlich, diese Jumper zu montieren.

Die durchschleifbare Verkabelung (oder Ringverkabelung) bietet ein Höchstmaß an Sicherheit durch die Bereitstellung einer fehlertoleranten Kommunikation auf dem X-BUS. Sämtliche Bedienteile und Erweiterungsmodule werden überwacht, und im Falle eines X-BUS-Fehlers oder -Bruchs funktioniert das System weiterhin und alle Melder werden weiterhin überwacht. Dies wird durch den Anschluss von 1A, 1B am Controller an 2A, 2B am ersten Bedienteil oder Erweiterungsmodul erreicht. Die weitere Verkabelung geschieht über den Anschluss von 1A, 1B an 2A, 2B am nächsten Erweiterungsmodul und so weiter bis zum letzten Bedienteil oder Erweiterungsmodul. Der letzte Anschluss ist 1A, 1B des letzten Erweiterungsmoduls an 2A, 2B des Controllers. Siehe die Verdrahtungsoptionen in der nachfolgenden Abbildung.



1	Controller
2-4	Erweiterungen

10.1.2 Stichleitungskonfiguration

	HINWEIS
	SPC52xx/53xx/63xx unterstützt 2 Stichleitungen (2 X-BUS-Anschlüsse). SPC42xx/43xx unterstützt 1 Stichleitung (1 X-BUS-Anschluss).

	HINWEIS
	Alle Erweiterungen/Bedienteile werden standardmäßig mit einem Abschluss-Jumper angebracht. In der Stichleitungskonfiguration ist es absolut erforderlich, diese Jumper zu montieren.

Die Verdrahtung per Stichleitungskonfiguration (oder Ringkonfiguration) bietet eine hohe Fehlertoleranz und kann bei bestimmten Installationen komfortabler sein. Im Falle eines X-BUS-Fehlers oder -Bruchs werden alle Erweiterungsmodule und Melder bis zum Fehlerpunkt weiterhin überwacht.

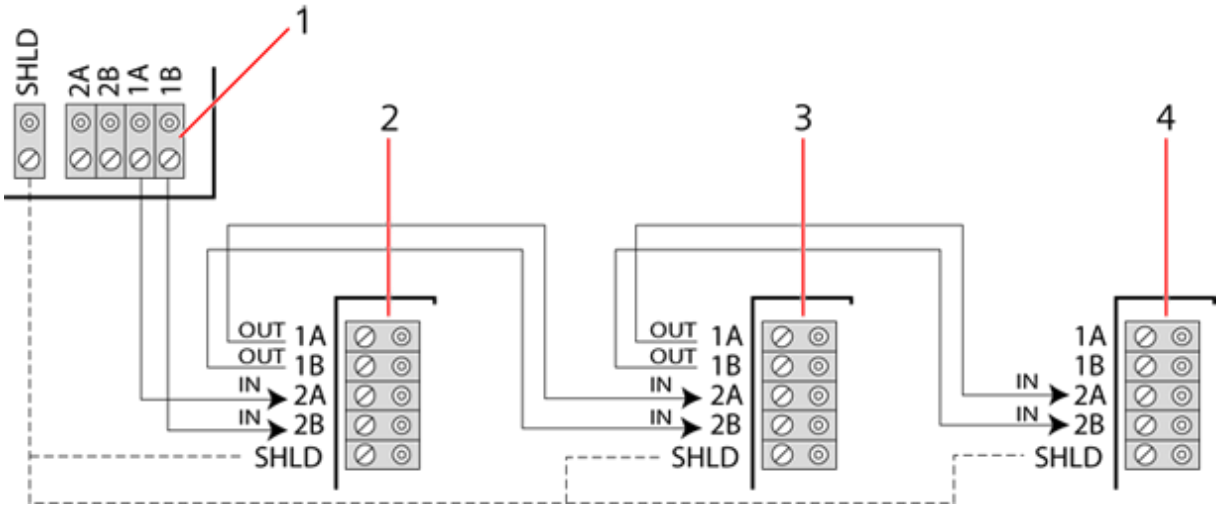
Bei dieser Konfiguration unterstützt der SPC-Controller eine Gruppe von Erweiterungsmodulen über einen einzelnen X-BUS-Port (1A/1B oder 2A/2B). Siehe die Verdrahtungsoptionen in der nachfolgenden Abbildung. Bei einer

Stichleitungskonfiguration hat das letzte Erweiterungsmodul keine Rückleitung zum Controller und ist im Konfigurationsmodus an der schnell blinkenden LED zu erkennen (blinkt etwa alle 0,2 Sekunden).

Im Automatikmodus beginnt die Nummerierung der Erweiterungsmodule mit dem Erweiterungsmodul, das dem Controller am nächsten ist, und endet mit dem Erweiterungsmodul, das am weitesten vom Controller entfernt angeschlossen ist. Werden zum Beispiel 6 Erweiterungsmodule in Stichleitungskonfiguration angeschlossen, ist das nächstgelegene Erweiterungsmodul am X-BUS-Anschluss Erweiterungsmodul 1, das zweitnächste ist Erweiterungsmodul 2 usw., und die Reihe endet mit dem Erweiterungsmodul, das am weitesten vom Controller entfernt angeschlossen ist (Erweiterungsmodul 6).

Alle Erweiterungsmodule/Bedienteile sind standardmäßig mit Abschlussjumpern versehen, was einen Abschluss an allen Geräten ermöglicht. Dies ist bei der Stichleitungskonfiguration absolut erforderlich, da der Jumper als Abschlusswiderstand fungiert und Echos in der Leitung unterdrückt.

Innerhalb der Ringkonfiguration werden alle Erweiterungsmodule/Bedienteile standardmäßig mit einem Jumper versehen, der eine Terminierung am Gerät ermöglicht.



Stichleitungskonfiguration

1	Controller
2-4	Erweiterungen

10.1.3 Stern- und Multidrop-Konfiguration

	HINWEIS
	Lesen Sie vor Beginn der Installation die Abschnitte Verdrahtungsbeispiele [→ 82] und Abschirmung [→ 83].

Die Stern- und Multidrop-Verkabelungsmethoden ermöglichen die Übernahme von vorhandenen Verkabelungen mit vieradrigen Kabeln in kleinen Gebäuden (typischerweise Heimbereiche) mit geringem elektrischen Rauschen. Diese Verkabelungsmethoden sind auf die folgenden Spezifikationen beschränkt:

	SPC42xx/SPC43xx	SPC52xx/SPC53xx/SPC63xx
Max.	8	16 (8 pro X-BUS-Anschluss)

Erweiterungen/Bedienteile		
Gesamtkabellänge	200 m	200 m

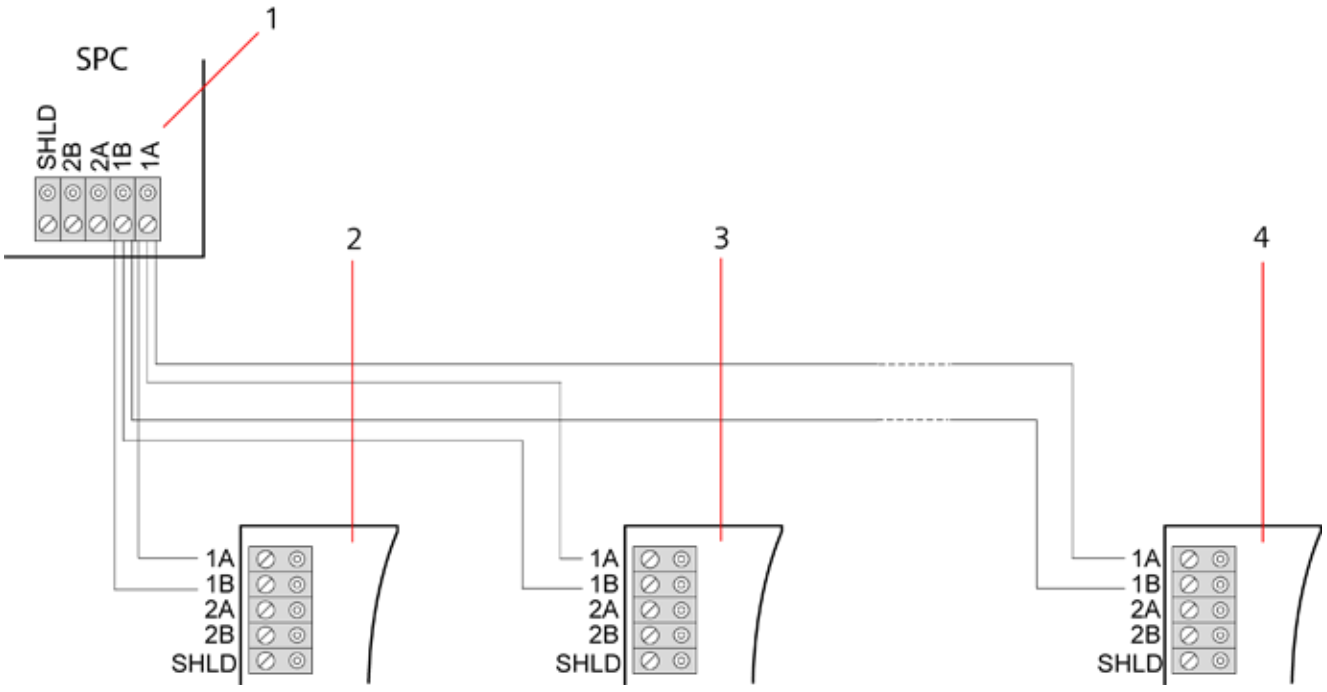
	HINWEIS
	Die Leistung in der Stern- oder Multidrop-Anschlusskonfiguration ist aufgrund von suboptimalen Bedingungen der RS-485-Busspezifikation begrenzt (reduzierte Signalqualität aufgrund von mehreren parallel geschalteten Sendern / Empfängern mit unausgeglichenen Abschlusswiderständen).

Sternkonfiguration

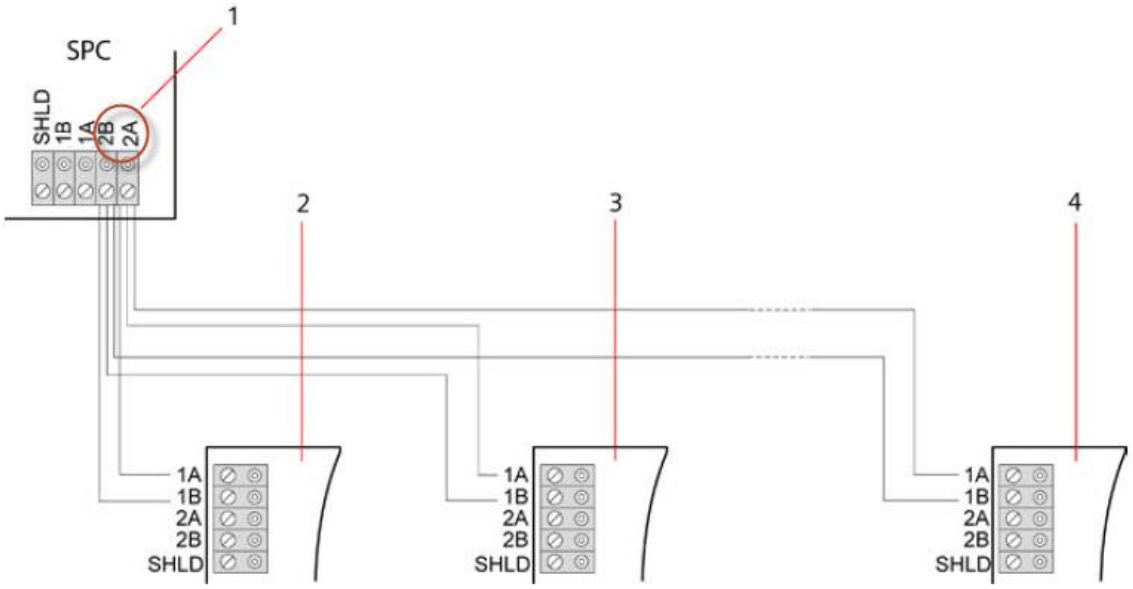
	HINWEIS
	Alle Erweiterungen/Bedienteile werden standardmäßig mit einem Abschluss-Jumper angebracht. In der Sternkonfiguration ist es absolut erforderlich, diese Jumper zu **entfernen**.

Eine Sternkonfiguration wird hergestellt, indem mehrere Erweiterungsmodule mit einer Rückleitung zum gleichen X-BUS-Anschluss auf dem SPC-Controller versehen werden. Je nach Controllertyp können 2 Anschlüsse (1A/1B, 2A/2B) vorhanden sein. Jedoch darf nur ein Anschluss (1A/1B) pro Bedienteil oder Erweiterungsmodul verwendet werden.

Im Falle eines X-BUS-Bruchs wird dieser einzelne abgetrennt, und alle anderen Erweiterungsmodule und Melder werden weiterhin überwacht. Ein Kurzschluss im Kabel führt zur Deaktivierung aller Erweiterungsmodule.



Sternkonfiguration



Sternkonfiguration 2

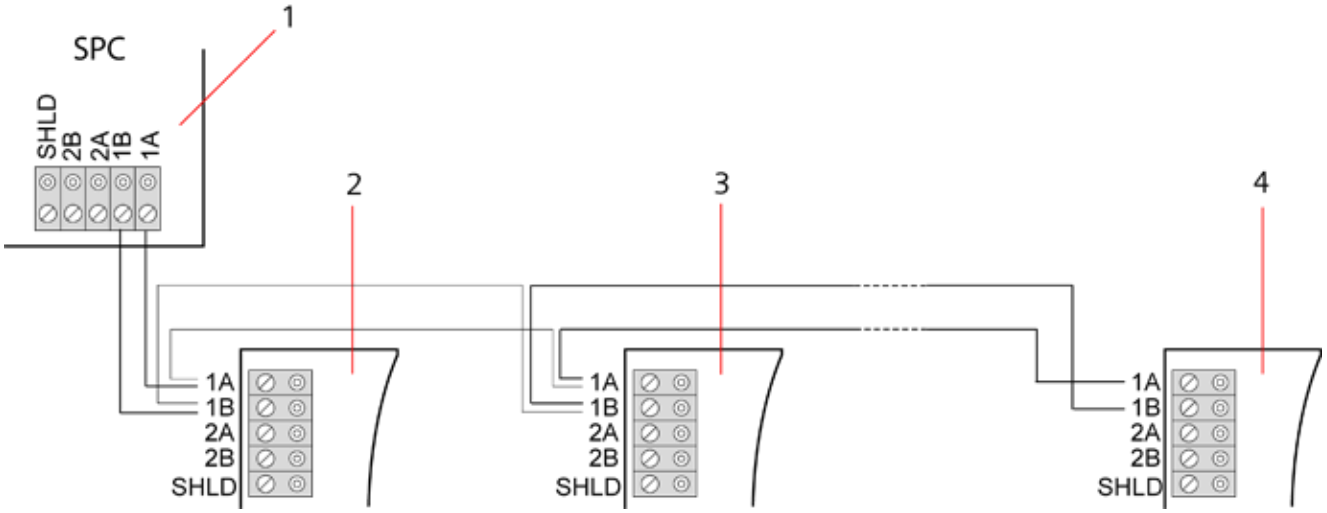
1	SPC-Controller
2-4	Erweiterungen

Multidrop-Konfiguration

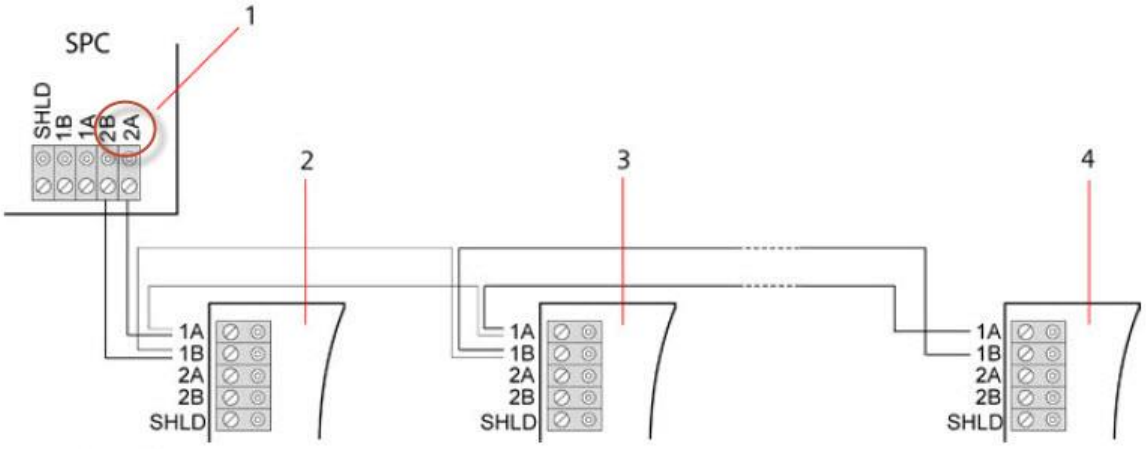
	HINWEIS
	Alle Erweiterungen/Bedienteile werden standardmäßig mit einem Abschluss-Jumper angebracht. In der Multidrop-Konfiguration ist es absolut erforderlich, diese Jumper zu **entfernen**.

Die Multidrop-Konfiguration unterscheidet sich dadurch, dass jedes Erweiterungsmodul bei der Verdrahtung zum nächsten Erweiterungsmodul den gleichen Übertragungskanal verwendet, wobei alle Erweiterungsmodule den gleichen Eingangskanal verwenden. Siehe die Multidrop-Konfiguration in der zweiten Abbildung.

Im Falle eines X-BUS-Bruchs werden alle Erweiterungsmodule und Melder bis zum Fehlerpunkt weiterhin überwacht. Ein Kurzschluss im Kabel führt zur Deaktivierung aller Erweiterungsmodule.



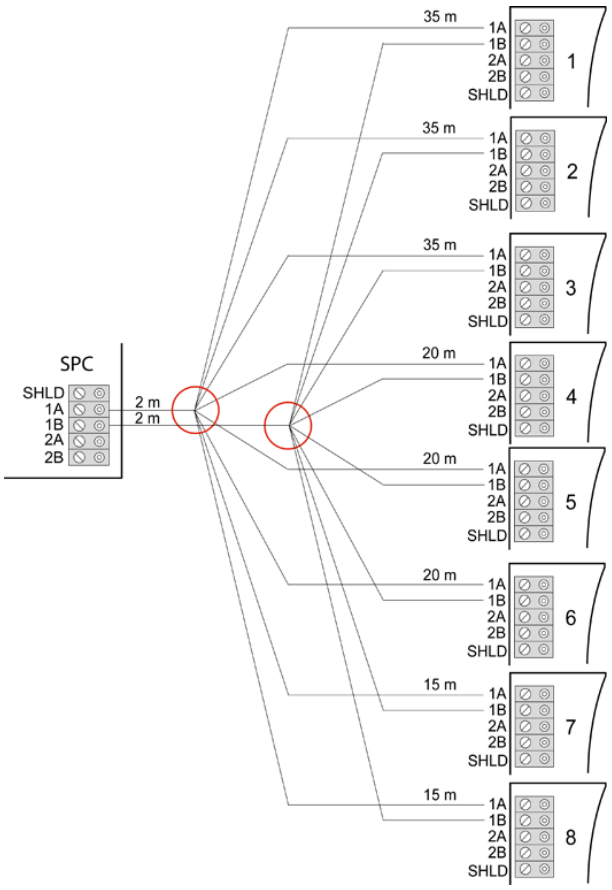
Multidrop-Konfiguration



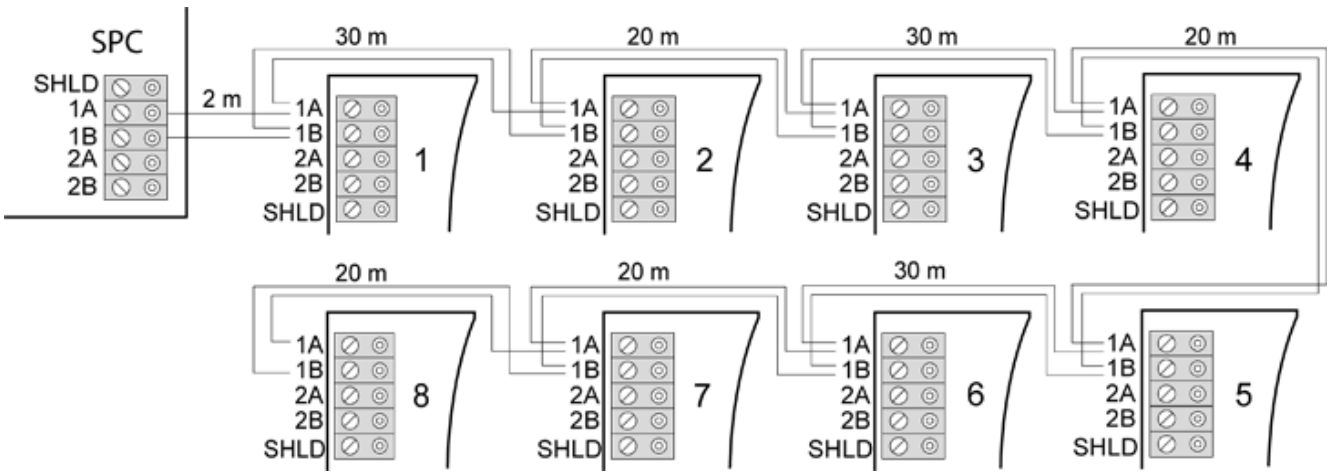
Multidrop-Konfiguration 2

1	SPC-Controller
2-4	Erweiterungen

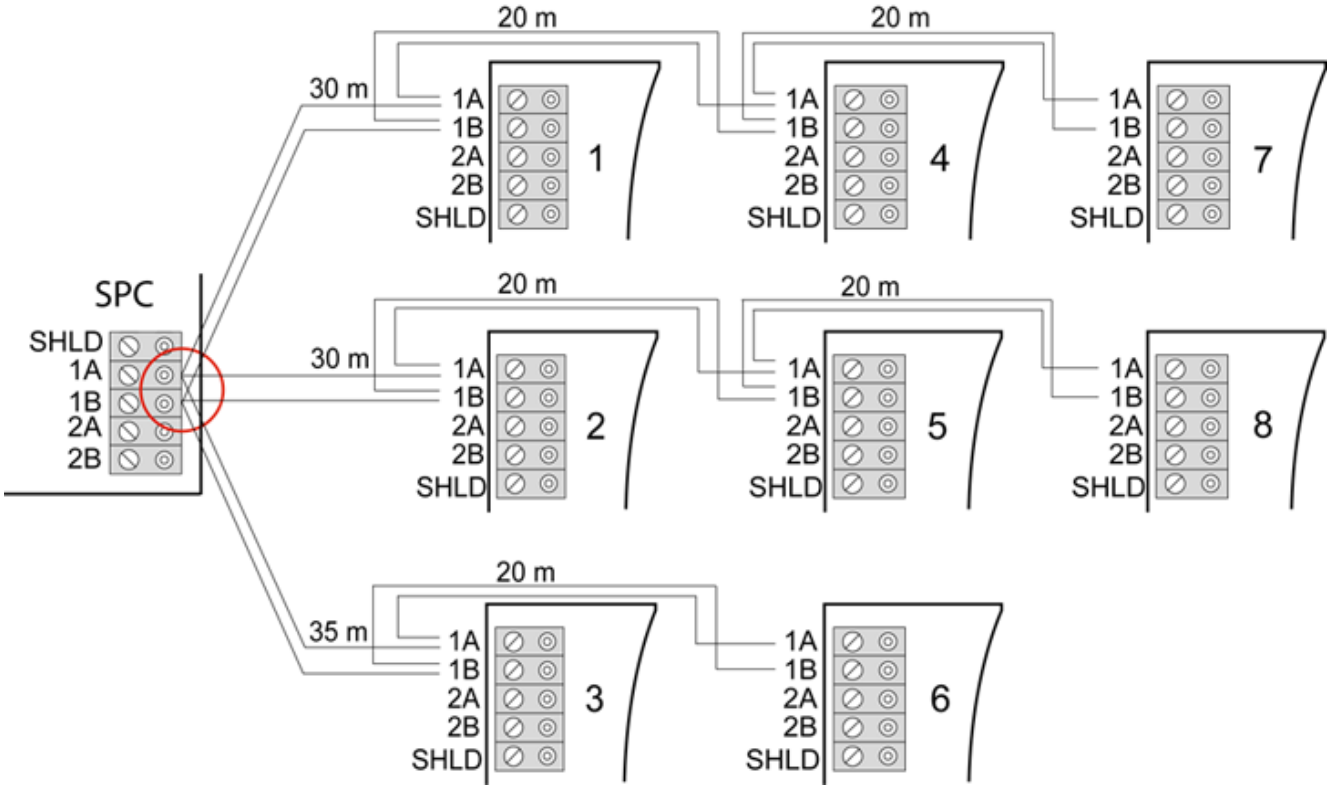
10.1.3.1 Beispiele für einen korrekten Anschluss



Sternverkabelung



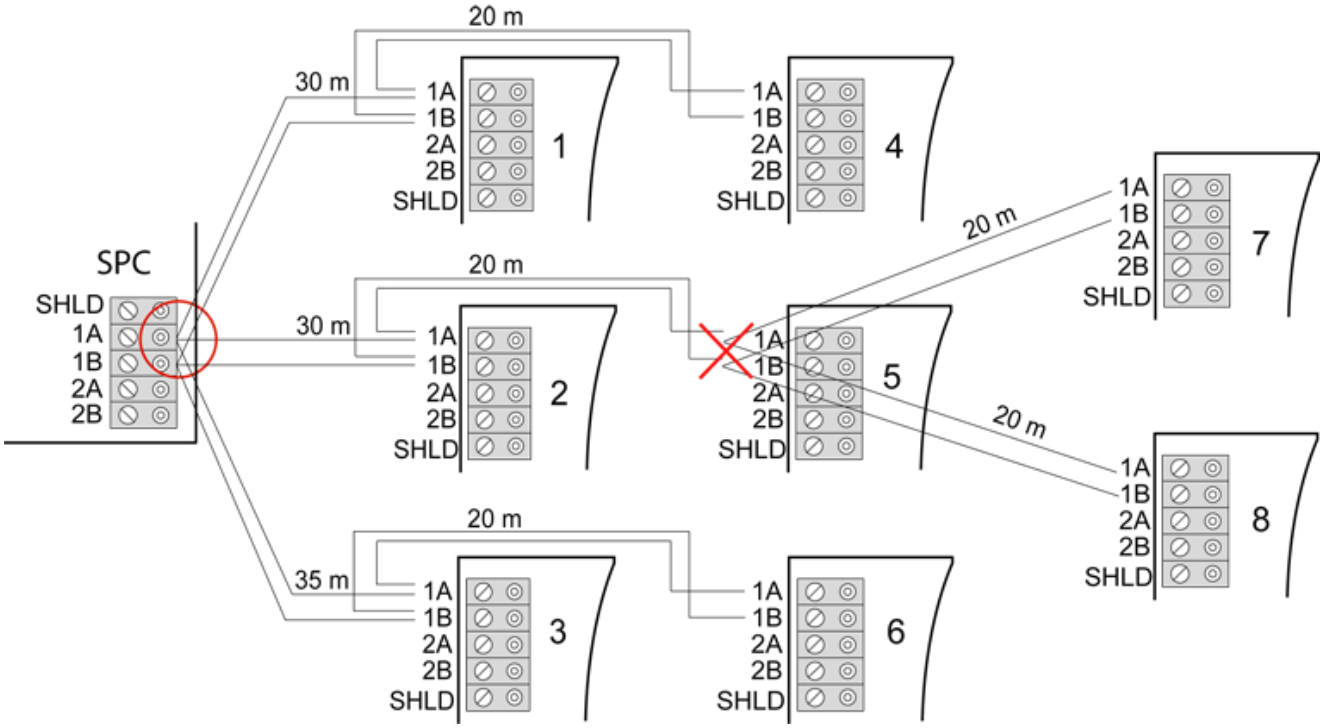
Multidrop-Verkabelung



Gemischte Verkabelung

10.1.3.2 Beispiele für einen falschen Anschluss

	HINWEIS
	Eine Mischung aus Stern- und Multidrop-Konfiguration ist nur zulässig, wenn sich der Sternpunkt am X-BUS-Anschluss des Controllers befindet. In diesem Fall müssen alle Erweiterungsmodule/Bedienteile in einer Multidrop-Konfiguration ohne weitere Sternpunkte angeschlossen werden.



Nicht zulässige Verkabelungen mit einem zweiten Sternpunkt

	HINWEIS
	Falls die Mischung aus Stern- und Multidrop-Konfiguration nicht ordnungsgemäß verkabelt ist, kann die reduzierte Signalqualität zu einer langsamen Reaktionszeit der angeschlossenen Geräte (z. B. Bedienteilbetrieb) oder sogar zum Verbindungsverlust zu den Geräten führen. Kommt es zu einer solchen Situation, ist eine durchschleifbare ODER Sternkonfiguration dringendst zu empfehlen.

10.1.4 Abschirmung

Die geschirmten Klemmen (SHLD) sollten nur für geschirmte Kabeltypen verwendet werden (z. B. Belden 9829). Falls eine Abschirmung erforderlich ist (z. B. an Standorten mit starken elektrischen Interferenzen): Verbinden Sie den Kabelschirm mit den SHLD-Anschlussklemmen am Controller und allen angeschlossenen Erweiterungsmodulen. Falls der Schirm mit der Erde verbunden werden muss, muss ein Kabel von der SHLD-Klemme am Controller mit dem Erdungsbolzen am Gehäuse verbunden werden. Die SHLD-Anschlussklemme darf NICHT über eines der Erweiterungsmodule geerdet werden.

	HINWEIS
	Für Stern- und Multidrop-Konfigurationen Aufgrund der unvorteilhaften elektrischen Eigenschaften abgeschirmter Kabel (hohe Kapazitäten) wird es nicht empfohlen, diese in Stern- und Multidrop-Konfigurationen zu verwenden. Wenn jedoch eine Abschirmung notwendig ist (d. h. an Standorten mit starken elektrischen Interferenzen), muss eine neue Verkabelung mit ordnungsgemäßer durchschleifbarer oder Stichleitungskonfiguration und den passenden Kabeln erfolgen.

10.1.5 Leitungsplan

Die Markierungs- und Nummerierungsordnung für Erweiterungsmodule und Bedienteile unterscheidet sich je nach Adressierung der Erweiterungsmodule (automatisch oder manuell). Informationen zur manuellen und automatischen Konfiguration finden Sie auf page [➙ 123].

Bei Systemen mit manueller Nummerierung haben Erweiterungsmodule und Bedienteile eine separate Nummerierungsfolge, die vom Techniker manuell festgelegt wird. Das heißt, Erweiterungsmodule werden mit 01, 02, 03 usw. wie gewünscht nummeriert. Bedienteile können ebenfalls unter Verwendung der gleichen Zahlen wie gewünscht nummeriert werden.

Bei der manuellen Konfiguration weist das System jedem Erweiterungsmodul automatisch Linien zu. Aus diesem Grund sollten Geräte ohne Linien wie Erweiterungsmodule mit 8 Ausgängen zuletzt adressiert werden.

Bei Systemen mit automatischer Adressierung gehören Erweiterungsmodule und Bedienteile in dieselbe Nummerierungsgruppe; die Zuweisung erfolgt durch den Controller. Das heißt, Erweiterungsmodule und Bedienteile werden in der Reihenfolge, in der sie erkannt werden, gemeinsam nummeriert und zwar nach ihrer Anordnung in Bezug zum Controller mit 01, 02, 03 usw.

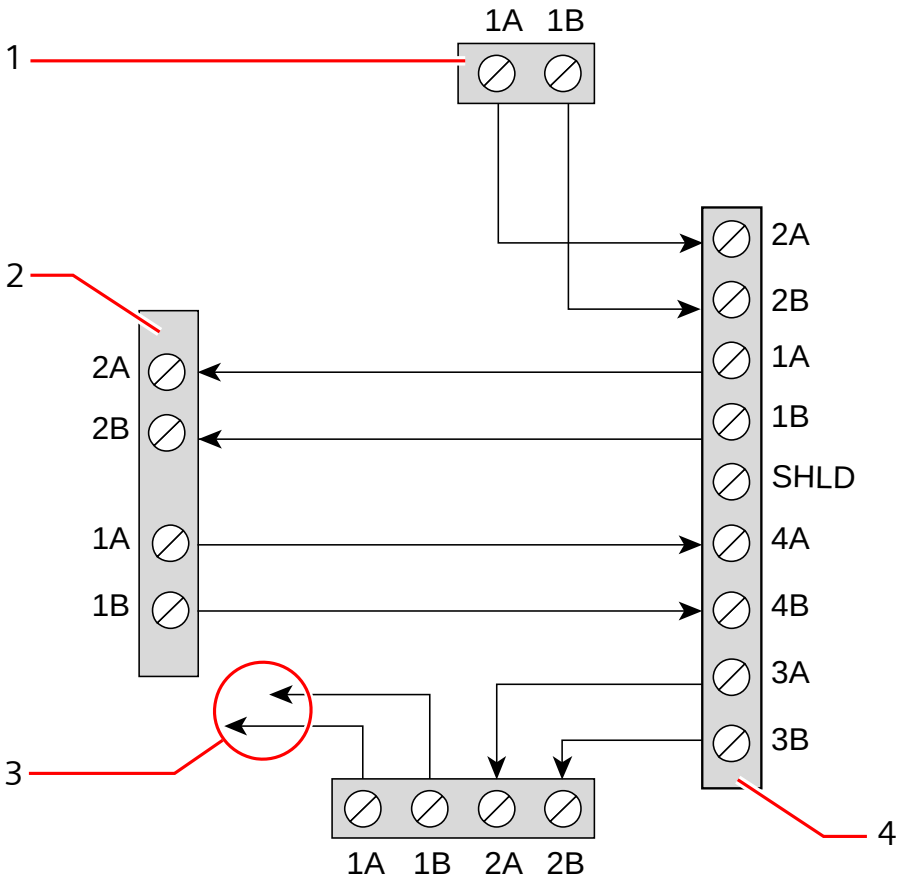
10.2 Verkabelung von Abzweig-Erweiterungsmodulen

Die Verkabelung der X-BUS-Schnittstelle mit den 8 Anschlussklemmen 1A/1B bis 4A/4B ermöglicht den Anschluss eines zusätzlichen Abzweig-Erweiterungsmoduls.

Wird der Abzweig nicht verwendet, werden die Anschlussklemmen 1A/1B für den Anschluss des nächsten Erweiterungsmoduls/Bedienteils verwendet. Die Anschlussklemmen 3A/3B und 4A/4B werden dann nicht verwendet..

Die folgenden Module bieten die Möglichkeit zum Anschluss von Abzweig-Erweiterungsmodulen (zusätzliche Klemmen 3A/B und 4A/B):

- Erweiterungsmodul mit 8 Eingängen / 2 Ausgängen
- Erweiterungsmodul mit 8 Ausgängen
- PSU-Erweiterungsmodul
- Funk-Erweiterungsmodul
- 2-Türen-Erweiterungsmodul



Verkabelung von Abzweig-Erweiterungsmodulen

1	Vorangegangene Erweiterung
2	Mit Abzweig verbundenes Erweiterungsmodul
3	Nächste Erweiterung
4	Erweiterungsmodul mit Abzweig

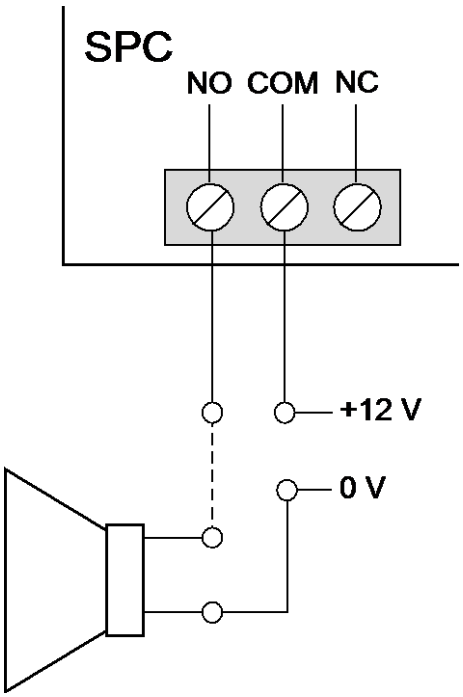
10.3 Verdrahtung der Systemmasse

Die Nullleiter der Smart PSUs (Stromversorgungseinheiten), Bedienteile und Erweiterungsmodule müssen mit dem Nullleiter des SPC-Controllers (Betriebserde) verbunden werden.

10.4 Verdrahtung des Relaisausgangs

Der SPC-Controller verfügt über ein integriertes einpoliges 1-A-Umschaltrelais, das jedem beliebigen SPC-Systemausgang zugewiesen werden kann. Dieser Relaisausgang kann eine Nennspannung von 30 V DC schalten (nicht induktive Last).

Wenn das Relais aktiviert wird, wird die gemeinsame Anschlussklemme (COM) von einem Ruhekontakt (NC für **N**ormally **C**losed) auf einen Arbeitskontakt (NO für **N**ormally **O**pen) umgeschaltet.



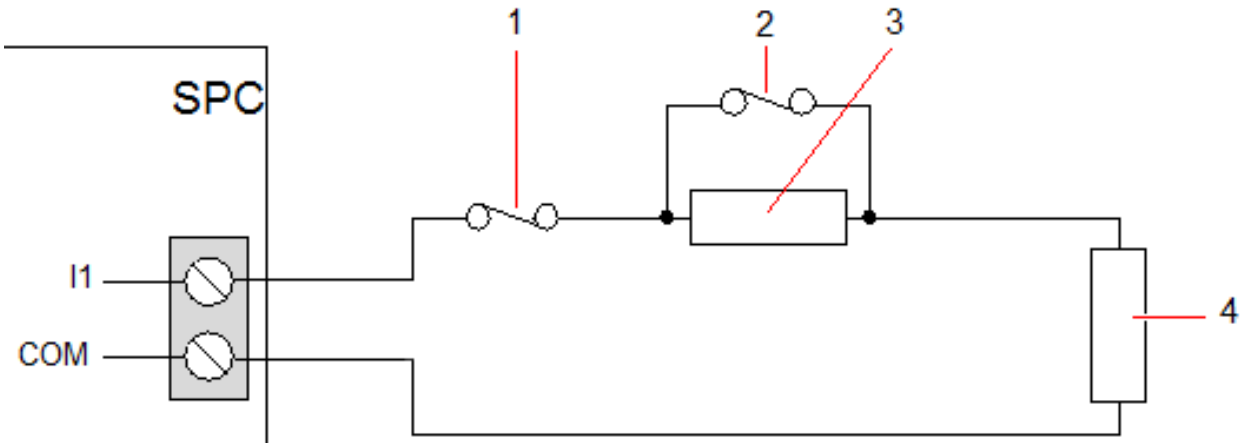
Standard-Verkabelung

NO	Arbeitskontakt (NO)
COM	Gemeinsame Anschlussklemme (COM)
NC	Ruhekontakt (NC)

10.5 Verdrahtung Linieneingänge

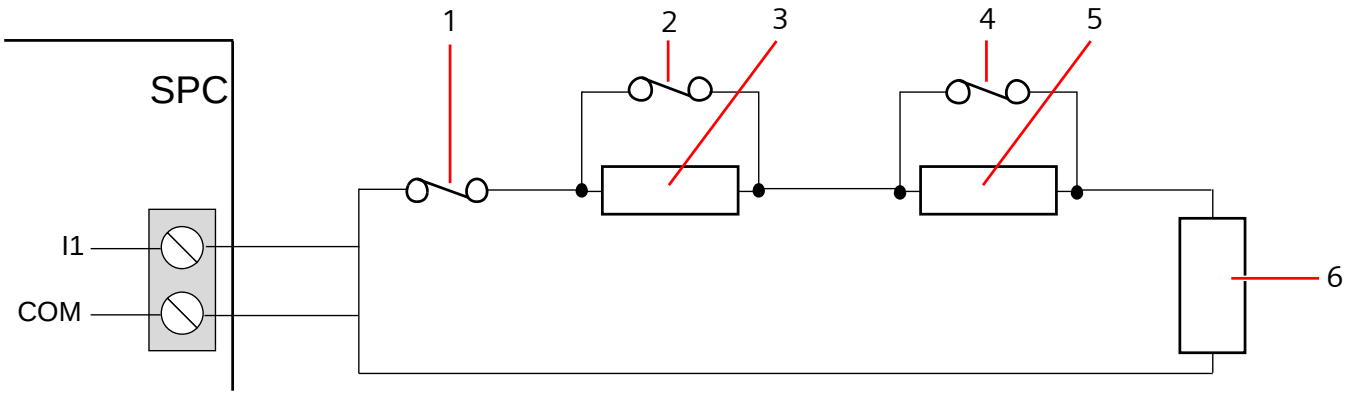
Der SPC-Controller verfügt über 8 integrierte Meldergruppen-Eingänge. Diese Eingänge werden standardmäßig über Endwiderstände überwacht. Beim Verdrahten der Eingänge kann der Installateur nach Belieben eine der folgenden Konfigurationen wählen:

- Kein Endwiderstand (NEOL – No End of Line)
- Einzelner Endwiderstand (SEOL – Single End of Line)
- DEOL (Dual End of Line)
- Anti-Masking-PIR-Konfiguration



Standardkonfiguration (DEOL 4K7)

1	Sabotage
2	Alarm
3	EOL 4K7
4	EOL 4K7



Anti-Masking-PIR-Konfiguration

1	Sabotage
2	Alarm
3	EOL 4K7
4	Störung
5	EOL 2K2
6	EOL 4K7

Die folgende Tabelle enthält die Widerstandsbereiche für jede einzelne Konfiguration:

Einzelne Endwiderstände

Endwiderstandstyp	Ruhestrom			Alarm		
	Min	Nom	Max	Min	Nom	Max
KEINE	0 Ω (-100%)	150 Ω	300 Ω (+100%)	300 Ω (+100%)	n.r.	Unbegrenzt
SINGLE_1K	700 Ω	1 kΩ	1,3 kΩ	23 kΩ	n.r.	Unbegrenzt

	(-30%)		(+30%)			
SINGLE_1K5	1,1 kΩ (-27%)	1,5 kΩ	2,1 kΩ (+40%)	23 kΩ	n.r.	Unbegrenzt
SINGLE_2K2	1,6 kΩ (-28%)	2,2 kΩ	2,9 kΩ (+32%)	23 kΩ	n.r.	Unbegrenzt
SINGLE_4K7	3,1 kΩ (-22%)	4,7 kΩ	6,3 kΩ (+24%)	23 kΩ	n.r.	Unbegrenzt
SINGLE_10K	7 kΩ (-30%)	10 kΩ	13 kΩ (+30%)	23 kΩ	n.r.	Unbegrenzt
SINGLE_12K	8,5 kΩ (-30%)	12 kΩ	15,5 kΩ (+30%)	23 kΩ	n.r.	Unbegrenzt

Doppelendwiderstände mit PIR-Maskierung und Störung

Endwiderstandstyp	Ruhestrom			Alarm		
	Min	Nom	Max	Min	Nom	Max
Mask_1K_1K_6K8 (1K / 1K / 6K8)	700 Ω (-30%)	1 kΩ	1,3 kΩ (+30%)	1,5 kΩ (-25%)	2 kΩ	2,5 kΩ (+25%)
Mask_1K_1K_2K2 (1K / 1K / 2K2)	700 Ω (-30%)	1 kΩ	1,3 kΩ (+30%)	1,5 kΩ (-25%)	2 kΩ	2,6 kΩ (+30%)
Mask_4K7_4K7_2K2 (4K7 / 4K7 / 2K2)	3,9 kΩ (-18%)	4,7 kΩ	5,6 kΩ (+20%)	8,4 kΩ (-11%)	9,4 kΩ	10,3 kΩ (+10%)

Endwiderstandstyp	Störung			Maskierung		
	Min	Nom	Max	Min	Nom	Max
Mask_1K_1K_6K8	2700 Ω (-69%)	8,8 kΩ	12,6 kΩ (+20%)	-	-	-
Mask_1K_1K_2K2	2,8k (-13%)	3,2k	3,6k (+13%)	3,8k (-10%)	4,2k	4,8k (+15)
Mask_4K7_4K7_2K2	6k (-14%)	6,9k	7,8k (+14%)	10,8k (-7%)	11,6k	12,6k (+9%)

Doppel-Endwiderstände

Endwiderstandstyp	Ruhestrom			Alarm		
	Min	Nom	Max	Min	Nom	Max
DUAL_1K0_470	400 Ω (-20%)	470 Ω	700 kΩ (+40%)	1,1 kΩ (-27%)	1,5 kΩ	2 kΩ (+34%)
DUAL_1K0_1K0	700 Ω (-30%)	1 kΩ	1,3 kΩ (+30%)	1,5 kΩ (-25%)	2 kΩ	2,6 kΩ (+30%)
DUAL_1k0_2k2	1,6 kΩ (-28%)	2,2 kΩ	2,9 kΩ (+32%)	2,3 kΩ (-29%)	3,2 kΩ	4,2 kΩ (+32%)
DUAL_1k5_2k2	1,6 kΩ (-28%)	2,2 kΩ	2,9 kΩ (+32%)	2,7 kΩ (-28%)	3,7 kΩ	4,8 kΩ (+30%)
DUAL_2K2_2K2	1,6 kΩ (-28%)	2,2 kΩ	2,9 kΩ (+32%)	3,4 kΩ (-23%)	4,4 kΩ	5,6 kΩ (+28%)
DUAL_2k2_4k7	4,1 kΩ (-13%)	4,7 kΩ	5,4 kΩ (+15%)	6 kΩ (-14%)	6,9 kΩ	7,9 kΩ (+15%)
DUAL_2K7_8K2	7,2 kΩ (-13%)	8,2 kΩ	9,2 kΩ (+13%)	9,9 kΩ (-10%)	10,9 kΩ	11,9 kΩ (+10%)
DUAL_3K0_3K0	2,1 kΩ	3,0 kΩ	3,9 kΩ	4,5 kΩ	6 kΩ	7,5 kΩ

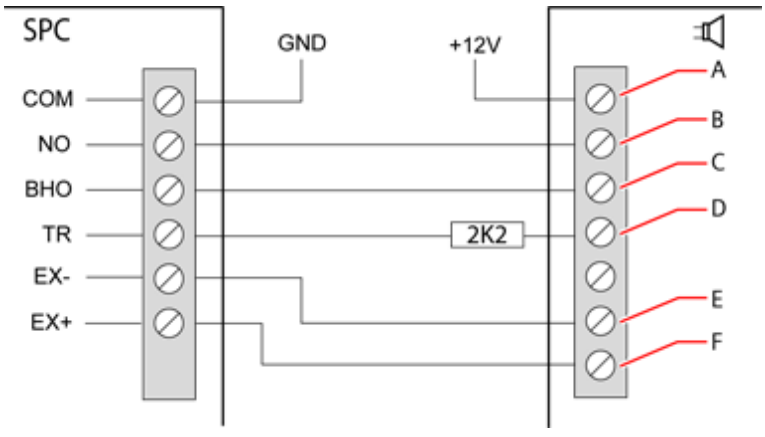
	(-30%)		(+30%)	(-25%)		(+25%)
DUAL_3K3_3K3	2,3 kΩ (-26%)	3,3 kΩ	4,3 kΩ (+31%)	4,9 kΩ (-26%)	6,6 kΩ	8,3 kΩ (+26%)
DUAL_3K9_8K2	7,0 kΩ (-15%)	8,2 kΩ	9,5 kΩ (+16%)	10,5 kΩ (-14%)	12,1 kΩ	13,8 kΩ (+15%)
DUAL_4K7_2K2	1,6 kΩ (-28%)	2,2 KΩ	2,9 kΩ (+32%)	5 kΩ (-28%)	6,9 kΩ	8,8 kΩ (+28%)
DUAL_4K7_4K7	3,3 kΩ (-30%)	4,7 kΩ	6,1 kΩ (+30%)	7 kΩ (-26%)	9,4 kΩ	11,9 kΩ (+27%)
DUAL_5K6_5K6	4,0 kΩ (-26%)	5,6 kΩ	7,2 kΩ (+29%)	8,3 kΩ (-26%)	11,2 kΩ	14,1 kΩ (+26%)
DUAL_6K8_4K7	3,3 kΩ (-30%)	4,7 kΩ	6,1 kΩ (+30%)	8,1 kΩ (-30%)	11,5 kΩ	14,9 kΩ (+30%)
DUAL_2k2_10K	9,2 kΩ (-8%)	10 kΩ	10,8 kΩ (+8%)	11,3 kΩ (-8%)	12,2 kΩ	13,2 kΩ (+9%)
DUAL_10k_10k	7,5 kΩ (-25%)	10 kΩ	12,5 kΩ (+25%)	17 kΩ (-15%)	20 kΩ	23 kΩ (+15%)

Bei allen Endwiderstandstypen wird ein Widerstand unter 300 Ω als Kurzschluss angesehen. Wenn der Widerstand nicht innerhalb der angegebenen Grenzwerte liegt, wird dies als Verbindungsunterbrechung angesehen.

10.6 Verkabelung einer externen SAB-Sirene

Beim Anschluss einer Außensirene an die SPC-Controller-Platine wird der Relaisausgang mit dem Blitzleuchteneingang mit **B**ell **H**old **O**ff (BHO) und **T**amper **R**eturn (TR) und den jeweiligen Eingängen an der Außensirenenschnittstelle verbunden.

Auf der Controller-Platine ist zwischen den BHO- und TR-Anschlussklemmen ein Widerstand (2K2) vorinstalliert. Beim Verdrahten einer Außensirene wird dieser Widerstand in Serie von der TR-Anschlussklemme am Controller zur TR-Anschlussklemme an der Außensirenenschnittstelle angeschlossen.



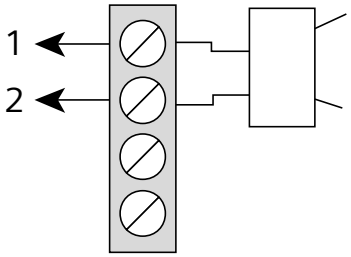
Verdrahtung einer Außensirene

A	Blitzleuchte +
B	Blitzleuchte –
C	Halten aus
D	Sabotagealarm zurück

E	Sirene –
F	Sirene +

10.7 Verdrahten eines internen Tongenerators

Verbinden Sie zum Verdrahten eines internen Tongenerators am SPC-Controller die Anschlussklemmen IN+ und IN– direkt mit dem 12-V-Tongeneratoreingang.



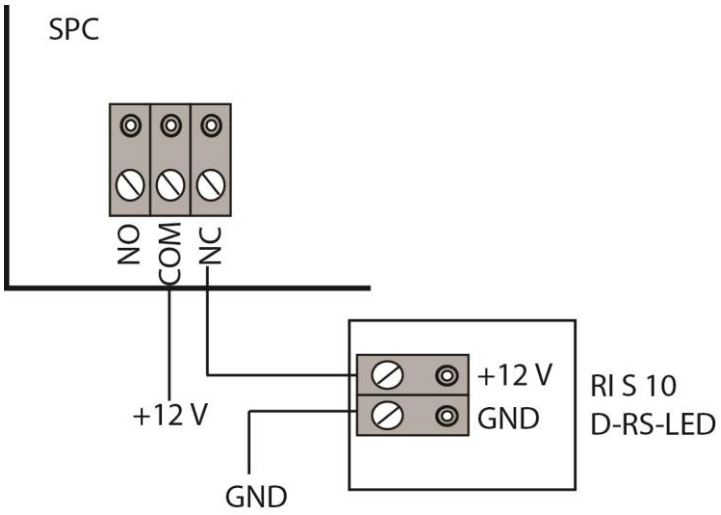
Verdrahtung eines internen Tongenerators (12 V)

IN–	IN- (SPC-Controller)
IN+	IN+ (SPC-Controller)

10.8 Verdrahtung von Glasbruchmeldern

SPC unterstützt die Glasbruch-Schnittstelle vom Typ RI S 10 D-RS-LED in Verbindung mit GB2001 Glassbruchmeldern.

Das nachstehende Diagramm zeigt, wie die Glasbruch-Schnittstelle zur Stromversorgung mit der SPC-Zentrale oder einer 8-E/2-A-Erweiterung verdrahtet wird:



Informationen zur Verdrahtung der Glasbruch-Schnittstelle mit einer Meldergruppe finden Sie in der Dokumentation für das jeweilige Produkt.

Informationen zur Verdrahtung der Glasbruchmelder mit der Glasbruch-Schnittstelle finden Sie in der Dokumentation für das jeweilige Produkt.

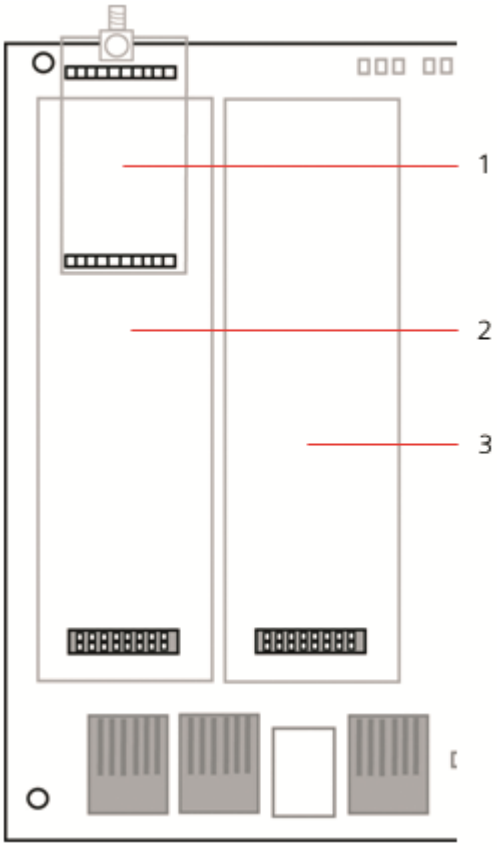
10.9 Installation von Einsteckmodulen

Zur Erweiterung des Funktionsumfangs können zwei Modems (PSTN oder GSM) an die Controller-Platine angeschlossen werden. Die nachfolgende Abbildung zeigt die beiden verfügbaren Modem-Steckplätze: den primären Steckplatz (links) und den Backup-Steckplatz (rechts).

Sind beide Modem-Steckplätze vorhanden, sollte das Einsteckmodul am primären Steckplatz angeschlossen werden; das System versucht stets, PSTN- oder GSM-Anrufe über ein Modem am primären Steckplatz durchzuführen, bevor es versucht, über den Backup-Steckplatz anzurufen.

⚠ WARNUNG

Die Modems sind nicht „plug and play“, d. h. sie müssen eigens konfiguriert werden und dürfen nicht bei eingeschalteter Stromversorgung angeschlossen werden. Sie müssen sich an der Zentrale im Konfigurationsmodus anmelden und dann die Controller-Platine abschalten. Erst dann dürfen Modems installiert, entfernt oder von einer Position auf eine andere umgesetzt werden. Schließen Sie nach dem Einbau des Modems das System wieder an die Stromversorgung an, und melden Sie sich wieder im Konfigurationsmodus an der Zentrale an. Führen Sie die Konfiguration aus und speichern Sie sie ab. Die Nichtbeachtung dieser Anweisungen verursacht einen CRC-Fehler.



Einsteckmodule

1	Funkempfänger-Steckplatz
2	Primärer Modem-Steckplatz
3	Backup-Modem-Steckplatz

Hinweise zur Installation finden Sie in der zugehörigen Installationsanleitung.

11 Einschalten des SPC-Controllers

Der SPC-Controller hat zwei Stromquellen: die Netzstromversorgung und die eingebaute Reservebatterie. Der Anschluss an das Stromnetz sollte von einem qualifizierten Elektriker durchgeführt werden. Die Netzstromversorgung sollte über eine Leitung erfolgen, die getrennt werden kann. Auf Seite [→ 373] finden Sie vollständige Angaben zu Leitergrößen, Sicherungsnennströmen usw.

Das SPC sollte primär über das Stromnetz versorgt werden, dann erst über die interne Reservebatterie. Zur Einhaltung der EN-Anforderungen muss eine Batterie mit geeigneter Leistung/Kapazität verwendet werden.

11.1 Einschalten über die Batterie

Es wird empfohlen, das beim Einschalten eines Systems allein über die Batterie diese vollständig geladen ist (> 13 V). Das System schaltet sich nicht ein, wenn eine Batterie mit weniger als 12 V Ladung verwendet wird und kein Stromkabel angeschlossen ist.

	*HINWEIS*
	Die Batterie versorgt das System so lange mit Strom, bis das Tiefentladungsniveau (10,5 V bis 10,8 V) erreicht wird. Die Dauer, wie lange das System von der Batterie versorgt wird, hängt von externen Lasten und von der Ah-Nennladung der Batterie ab.

12 Benutzeroberfläche des Bedienteils

Folgende Bedienteil-Modelle stehen zur Verfügung:

- SPCK420/421 – Wird in diesem Handbuch durchgehend als LCD-Bedienteil bezeichnet.
- SPCK620/623 – Wird in diesem Handbuch durchgehend als Komfort-Bedienteil bezeichnet.

12.1 SPCK420/421

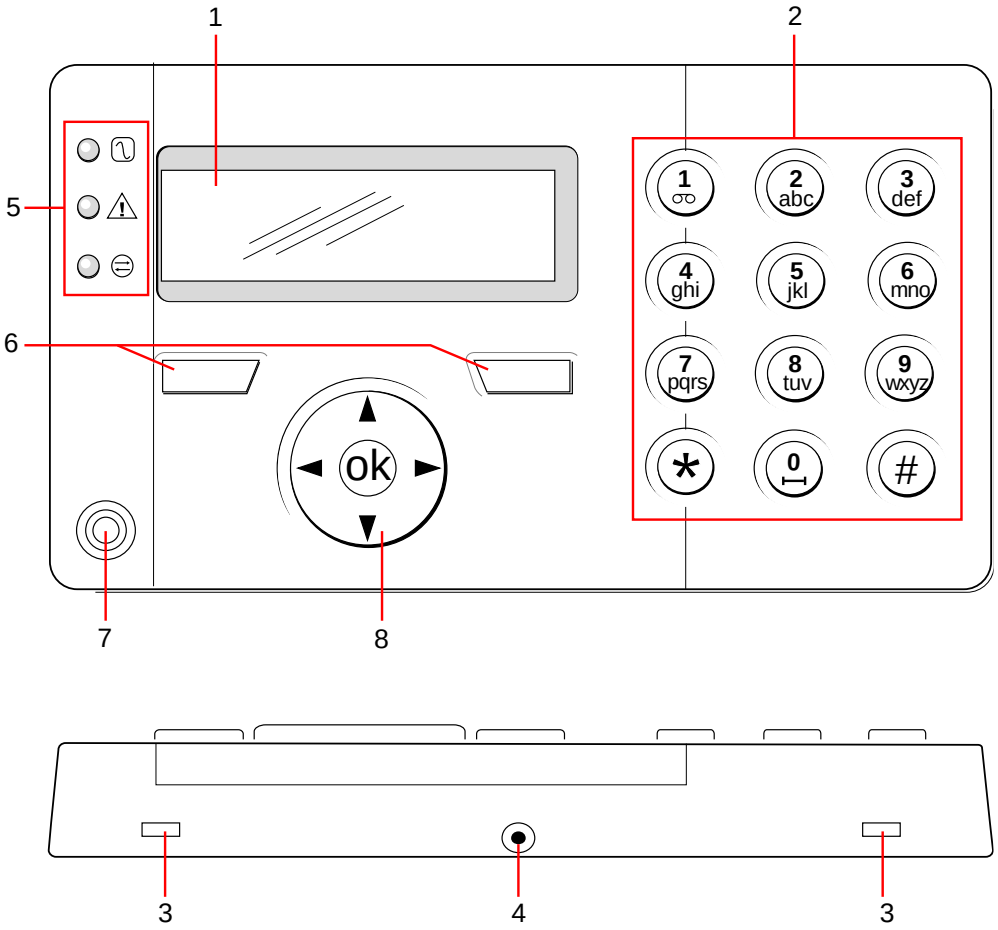
12.1.1 Einführung

Beim LCD-Bedienteil handelt es sich um eine wandmontierte Benutzeroberfläche, mit deren Hilfe

- **Techniker** das System über die Techniker-Programmiermenüs (kennwortgeschützt) programmieren und scharf oder unscharf schalten können. Benutzer können das System hiermit im täglichen Betrieb steuern.
- **Benutzer** auf Benutzer-Programmiermenüs (kennwortgeschützt) zugreifen und Betriebseinstellungen am System vornehmen können (scharf/unscharf schalten). (Weitere Informationen zur Benutzerprogrammierung finden Sie in der SPCK420/421-Bedienungsanleitung.)

Das LCD-Bedienteil verfügt über einen integrierten Sabotageschalter an der Frontplatte und ein zweizeiliges Display mit 16 Zeichen pro Zeile. Es verfügt über eine benutzerfreundliche Navigationstaste zum einfacheren Auffinden der gewünschten Programmieroptionen sowie zwei kontextsensitive Softkeys (links und rechts) zum Auswählen der gewünschten Menü- oder Programmeinstellungen. 3 LEDs auf dem Bedienteil zeigen den Status der Wechselstromversorgung, der Alarme und der Kommunikationsfunktionen an.

Das LCD-Bedienteil kann werksseitig mit einem Portable ACE (PACE) Proxy-Leser versehen werden (siehe Seite [➙ 371]).

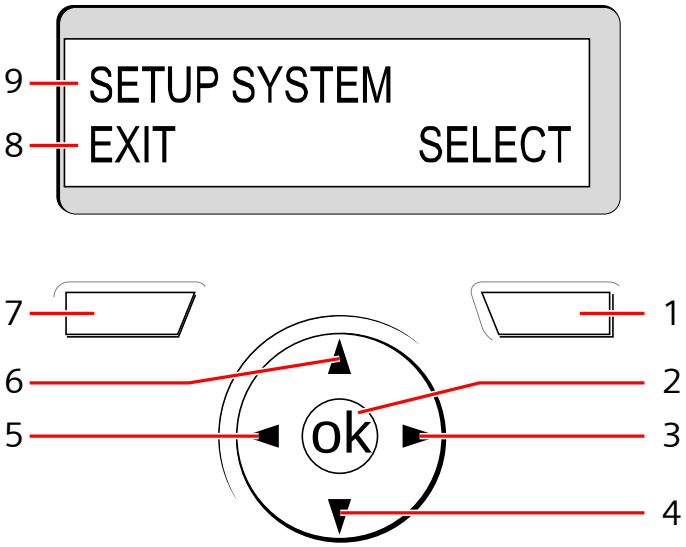


LCD-Bedienteil

1	Display (LCD)	Das Display des Bedienteils (2 Zeilen à 16 Zeichen) zeigt Alarm- und Warnmeldungen an und dient als Benutzeroberfläche beim Programmieren des Systems (nur Techniker-Programmierung). Anzeigekontrast und Hintergrundbeleuchtung des Displays lassen sich einstellen.
2	Alphanumerische Tasten	Die alphanumerischen Tasten ermöglichen die Eingabe von Text und Zahlen bei der Programmierung. Buchstaben werden gewählt, indem die Tasten entsprechend häufig gedrückt werden. Drücken Sie die Taste #, um zwischen Groß- und Kleinschreibung zu wechseln. Um eine Zahl einzugeben, muss die jeweilige Taste 2 Sekunden lang gedrückt werden.
3	Hebellaschen	Über die Hebellaschen erfolgt der Zugriff auf die Montageclips auf der Rückseite des Bedienteils. Diese Clips können vom Benutzer aus dem Vorderteil ausgehakt werden. Hierzu einen 5-mm-Schraubendreher in die Aussparung stecken und leichten Druck ausüben.
4	Rückwandbefestigungsschraube	Diese Schraube hält die Frontplatte und die Rückwand des Bedienteils zusammen. Sie muss gelöst werden, um das Bedienteil zu öffnen.
5	LED-Statusanzeigen	Die LED-Statusanzeigen liefern Informationen über den aktuellen Systemzustand; siehe hierzu die nachfolgende Tabelle.
6	Softkeys	Beim linken und rechten Softkey handelt es sich um kontextsensitive Tasten zur Navigation innerhalb von Menüs und bei der Programmierung.
7	Proxy-Empfangsbereich	Falls das Bedienteil werksseitig mit einem Proxy-Empfänger ausgerüstet wurde (siehe Seite [➙ 371]), können Benutzer das System SCHARF/UNSCHARF schalten, indem sie den portablen Transponder in etwa 1 cm Entfernung vor diesen Bereich halten.
8	Multifunktionale Navigationstaste	Die multifunktionale Navigationstaste bildet zusammen mit dem Display die Benutzeroberfläche zum Programmieren des Systems.

LED		Status
Netzstrom (grün)		Zeigt den Status der Stromversorgung an (Strom/kein Strom). BLINKT: Fehler der Netzstromversorgung KONSTANT: Netzstromversorgung in Ordnung
Systemalarm (gelb)	⚠	Weist auf einen Systemalarm hin BLINKT: Systemalarm erkannt. Display zeigt Ort und Art des Alarms an. Wenn das System SCHARF geschaltet ist, wird KEIN Systemalarm angezeigt. AUS: Kein Alarm erkannt. Wenn ein Bedienteil mehreren Bereichen zugewiesen ist, zeigt die LED keinen Alarmzustand an, wenn einer dieser Bereiche SCHARF geschaltet ist.
X-BUS-Status (rot)		Zeigt im Konfigurationsmodus den Status der X-BUS-Kommunikation an. Blinkt regelmäßig (ca. alle 1,5 Sekunden): Zeigt an, dass der Kommunikationsstatus OK ist. Blinkt schnell (ca. alle 0,25 Sekunden): Zeigt an, dass das Bedienteil das letzte Erweiterungsmodul innerhalb der X-BUS ist. Wenn das Bedienteil zum ersten Mal installiert wird und der Strom eingeschaltet wird, bevor die Verbindung zur X-BUS-Schnittstelle des Controllers hergestellt wurde, bleibt die LED im Zustand EIN.

12.1.2 Bedienung der Benutzeroberfläche des LCD-Bedienteils



Display des Bedienteils

1	RECHTER SOFTKEY	Diese Taste dient zur Auswahl der Option auf der rechten Seite der unteren Displayzeile. Mögliche Werte sind: → AUSWAHL zum Auswählen der in der oberen Zeile angezeigten Option → BEST(ÄTIGE) zum Eingeben der in der oberen Zeile angezeigten Daten → WEITER zur Anzeige des nächsten Alarms nach dem in der oberen Zeile angezeigten Alarm → LÖSCHEN zum Löschen des in der oberen Zeile angezeigten Alarms → SPEICHERN zum Speichern einer Einstellung
2	OK	Die OK-Taste dient als AUSWAHL-Taste für die in der oberen Zeile des Displays angezeigte Menüoption und auch als BESTÄTIGEN/SPEICHERN-Taste für in der oberen Zeile angezeigte Daten.
3	▶	Im Programmiermodus kann sich der Benutzer mit der rechten Pfeiltaste in Menüs einen Schritt weiter bewegen – ebenso wie durch Drücken der AUSWAHL-Option (rechter Softkey).

		Im Dateneingabemodus dient die Taste dazu, den Cursor um jeweils eine Position weiter nach rechts zu bewegen.
4	▽	Im Programmiermodus gelangt der Benutzer mit der „Nach unten“-Pfeiltaste zur nächsten Programmieroption innerhalb der gleichen Menüebene. Wird sie gedrückt gehalten, blättert der Cursor durch alle Programmieroptionen, die innerhalb der aktuellen Menüebene zur Verfügung stehen. Im alphanumerischen Modus dient die Taste zum Wechseln von Großschreibung zu Kleinschreibung. Werden Alarmmeldungen angezeigt, gelangt der Benutzer mit der „Nach unten“-Pfeiltaste zur nächsten Alarmmeldung in der Reihenfolge ihrer Priorität. (Weitere Informationen finden Sie im Abschnitt über die Priorisierung angezeigter Meldungen.)
5	◁	Im Programmiermodus gelangt der Benutzer mit der linken Pfeiltaste zur vorherigen Menüebene. Durch Drücken der Taste auf der obersten Menüebene verlässt der Benutzer den Programmiermodus. Im Dateneingabemodus dient die Taste dazu, den Cursor um jeweils eine Position weiter nach links zu bewegen.
6	△	Im Programmiermodus wird mit der „Nach oben“-Pfeiltaste der Cursor zur vorherigen Programmieroption innerhalb der gleichen Menüebene bewegt. Wird sie gedrückt gehalten, blättert der Cursor durch alle Programmieroptionen, die innerhalb der aktuellen Menüebene zur Verfügung stehen. Im alphanumerischen Modus dient die Taste zum Wechseln von Kleinschreibung zu Großschreibung.
7	LINKER SOFTKEY	Diese Taste dient zur Auswahl der Option auf der linken Seite der unteren Displayzeile. Mögliche Werte sind: → BEENDEN zum Beenden des Programmierens → ZURÜCK um zum vorigen Menü zurückzukehren
8	UNTERE DISPLAYZEILE	Im Bereitschaftszustand ist diese Zeile leer. Im Programmiermodus zeigt diese Zeile die verfügbaren Optionen an. Die Optionen werden entweder rechts- oder linksbündig angezeigt und können mit dem jeweiligen Softkey ausgewählt werden.
9	OBERE DISPLAYZEILE	Im Bereitschaftszustand werden hier Uhrzeit und Datum angezeigt. Im Programmiermodus erscheint in dieser Zeile eine der folgenden Anzeigen: → Die zur Auswahl stehende Programmieroption → Die aktuelle Einstellung der gewählten Funktion → Die Art des aktuellen Alarms während eines Alarmzustands. (Siehe Priorisierung angezeigter Meldungen im Folgenden.)

Zuweisung von Prioritäten zu angezeigten Meldungen

Fehlermeldungen und Alarme werden in der folgenden Reihenfolge auf dem Bedienteil angezeigt:

- Meldergruppe
  - Alarm
  - Sabotage
  - Problem
- Meldergruppenalarme
  - Schärfung fehlgeschlagen
  - Eingabe-Timeout
  - Code-Sabotage
- Systemalarme
  - Netz
  - Batterie
  - Stör Netzteil
  - Stör Aux
  - Sicherung Außensirene

  - Sicherung Innensirene
  - Sabotage Sirene
  - Sabotage Deckelkontakt
  - Zentrale Sabotage 1
  - Zentrale Sabotage 2
  - Fremdfunk
  - Modem 1 Störung
  - Modem 1 Telefonleitung
  - Modem 2 Störung
  - Modem 2 Telefonleitung
  - Übertragungsfehler
  - Bedrohungspin
  - XBUS Leitungsbr
  - XBUS Kommunikationsfehler
  - XBUS Stör Netz
  - XBUS Störung Batterie
  - XBUS Störung Stromversorgung
  - XBUS Stör Sich
  - XBUS Störung Sabotage
  - XBUS Störung Antenne
  - XBUS Fremdfunk
  - XBUS Überfall
  - XBUS Feuer
  - XBUS Med Notfall
  - XBUS Verbindung Stromversorgung
  - XBUS Ausgang Sabotage
  - XBUS Niedrige Spannung
  - Technikerquittierung erforderlich
  - Autom Scharfsch
- Systeminformationen
  - Meldergruppen im Dauertest
  - Offene Eingänge
  - Bereichsstatus
  - Batterie schwach (Sensor)
  - Sensor Störung Kommunikation
  - FÜ Batterie schwach
  - FÜ Störung Kommunikation
  - FÜ Test überfällig
  - Kamera Offline
  - Fernbedienung Batterie schwach
  - XBUS Überstrom
  - Name des Errichters
  - Tel des Errichters
  - Techniker freigegeben
  - Hersteller freigegeben
  - Neu starten
  - Hardware Störung
  - Überstrom Ausgang
  - Akku schwach

- Netzwerkverbindung
- Systemname

12.1.3 Dateneingabe auf dem LCD-Bedienteil

Die Eingabe von Daten und die Navigation innerhalb der Menüs auf dem LCD-Bedienteil erfolgt über die Programmierschnittstelle. Im Folgenden wird die Verwendung der Schnittstelle für die verschiedenen Aktionsarten beschrieben.

Eingabe numerischer Werte

Im numerischen Eingabemodus können nur die Zahlen 0 - 9 eingegeben werden.

- Mit der linken und rechten Pfeiltaste kann der Cursor um jeweils ein Zeichen nach links bzw. rechts bewegt werden.
- Drücken Sie die Menütaste ZURÜCK, um die Funktion zu verlassen, ohne Ihre Eingaben zu speichern.
- Drücken Sie BESTätigen oder OK, um Ihre Eingaben zu speichern.

Eingabe von Text

Im Texteingabemodus können sowohl Buchstaben (A–Z) als auch Zahlen (0–9) eingegeben werden.

- Drücken Sie zur Eingabe eines Buchstaben die entsprechende Taste so oft, bis der gewünschte Buchstabe erscheint.
- Drücken Sie zur Eingabe sprachspezifischer Sonderzeichen (ä, ö, ü...) Taste 1 so oft, bis das gewünschte Zeichen erscheint.
- Zur Eingabe von Leerzeichen und sonstigen Sonderzeichen (+, -./[ ]…) drücken Sie Taste 0 so oft, bis das gewünschte Zeichen erscheint.
- Um eine Zahl einzugeben, muss die jeweilige Taste 2 Sekunden lang gedrückt gehalten und dann losgelassen werden.
- Mit der linken und rechten Pfeiltaste kann der Cursor um jeweils ein Zeichen nach links bzw. rechts bewegt werden.
- Drücken Sie ZURÜCK, um die Funktion zu verlassen, ohne Ihre Eingaben zu speichern.
- Drücken Sie BESTätigen oder OK, um Ihre Eingaben zu speichern.
- Drücken Sie zum Wechseln zwischen Groß- und Kleinschreibung die Nach oben/Nach unten-Pfeiltasten, wenn der Cursor das gewünschte Zeichen markiert.
- Drücken Sie die „Raute“-Taste (#), um zwischen Groß- und Kleinschreibung für alle nachfolgenden Zeichen zu wechseln.
- Drücken Sie die „Stern“-Taste (*) zum Löschen von Zeichen links vom Cursor.

Auswahl einer Programmieroption

Im Navigationsmodus kann der Techniker/Benutzer verschiedene vordefinierte Programmieroptionen aus einer Liste wählen.

- Drücken sie die Nach oben/Nach unten-Pfeiltasten, um sich innerhalb der Liste der zur Auswahl stehenden Optionen zu bewegen.
- Drücken Sie ZURÜCK, um die Funktion zu verlassen, ohne Ihre Eingaben zu speichern.
- Drücken Sie SPEICHERN oder OK, um die gewählte Option zu speichern.

12.2 SPCK620/623

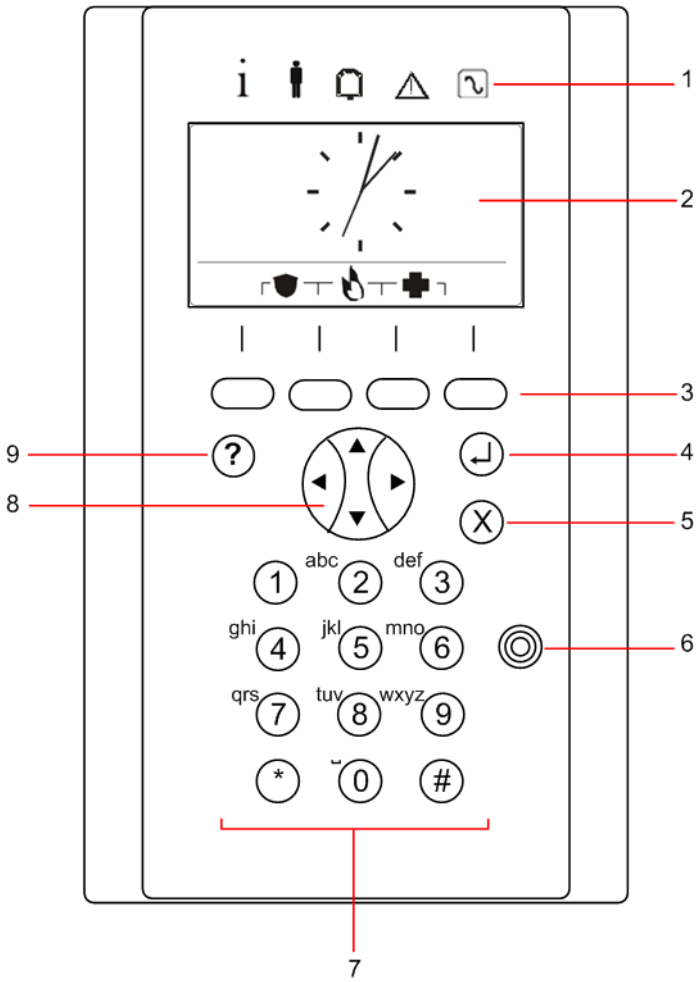
12.2.1 Einführung

Beim Komfort-Bedienteil handelt es sich um eine wandmontierte Benutzeroberfläche, mit deren Hilfe

- Techniker das System über die Techniker-Programmiermenüs (kennwortgeschützt) programmieren und scharf oder unscharf schalten können. Benutzer können das System hiermit im täglichen Betrieb steuern.
- Benutzer auf Benutzer-Programmiermenüs (kennwortgeschützt) zugreifen und Betriebseinstellungen am System vornehmen können (scharf/unscharf schalten). (Weitere Informationen zur Benutzerprogrammierung finden Sie in der SPC620/623 Bedienungsanleitung.)

Das SPCK620 verfügt über Softkeys und ein großes grafisches Display (LCD) für eine einfache Bedienung. Der Funktionsumfang kann mit einem Schlüsselschalter-Erweiterungsmodul SPCE110 oder einem Anzeige-Erweiterungsmodul SPCE120 erweitert werden.

Das SPCK623 verfügt über einen Proxy-Ausweisleser (125 kHz EM 4102) für einen einfachen Benutzerzugang, Softkeys, ein großes LCD-Display und unterstützt Sprachansage. Der Funktionsumfang kann mit einem Schlüsselschalter-Erweiterungsmodul SPCE110 oder einem Anzeige-Erweiterungsmodul SPCE120 erweitert werden.



1	LED-Statusanzeigen	Die LED-Statusanzeigen liefern Informationen über den aktuellen Systemzustand; siehe hierzu die nachfolgende Tabelle.
2	Display (LCD)	Das Display des Bedienteils zeigt Alarm- und Warnmeldungen an und dient als Benutzeroberfläche beim Programmieren des Systems (nur Techniker-Programmierung).

		(Weitere Informationen finden Sie im Abschnitt zur Priorisierung angezeigter Meldungen.) Für das Display können Bedingungen konfiguriert werden, unter denen die Hintergrundbeleuchtung eingeschaltet wird.
3	Softkeys	Kontextsensitive Tasten zur Navigation innerhalb von Menüs und bei der Programmierung
4	Eingabetaste	Bestätigen einer Anzeige oder Eingabe
5	Menütaste Zurück	● Zurückgehen im Menü Zurücksetzen von Summer, Sirene und Alarmen im Speicher
6	Proxy-Empfangsbereich	Nur SPCK 623: Wenn das Bedienteil mit einem Proxy-Empfänger ausgestattet ist, müssen Benutzer den portablen Transponder innerhalb von 1 cm Entfernung zu diesem Bereich halten.
7	Alphanumerische Tasten	Die alphanumerischen Tasten ermöglichen die Eingabe von Text und Zahlen bei der Programmierung. Buchstaben werden gewählt, indem die Tasten entsprechend häufig gedrückt werden. Drücken Sie die Taste #, um zwischen Groß- und Kleinschreibung zu wechseln. Um eine Zahl einzugeben, muss die jeweilige Taste 2 Sekunden lang gedrückt werden.
8	Multifunktionale Navigationstaste	Navigation innerhalb von Menüs und Durchblättern der Alarmmeldungen. (Siehe „Priorisierung angezeigter Meldungen“ im Folgenden)
9	Taste Informationen	Anzeigen von Informationen

Zuweisung von Prioritäten zu angezeigten Meldungen

Fehlermeldungen und Alarme werden in der folgenden Reihenfolge auf dem Bedienteil angezeigt:

- Meldergruppe
  - Alarm
  - Sabotage
  - Problem
- Meldergruppenalarme
  - Schärfung fehlgeschlagen
  - Eingabe-Timeout
  - Code-Sabotage
- Systemalarme
  - Netz
  - Batterie
  - Stör Netzteil
  - Stör Aux
  - Sicherung Außensirene
  - Sicherung Innensirene
  - Sabotage Sirene
  - Sabotage Deckelkontakt
  - Zentrale Sabotage 1
  - Zentrale Sabotage 2
  - Fremdfunk
  - Modem 1 Störung

  - Modem 1 Telefonleitung
  - Modem 2 Störung
  - Modem 2 Telefonleitung
  - Übertragungsfehler
  - Bedrohungspin
  - XBUS Leitungsbr
  - XBUS Kommunikationsfehler
  - XBUS Stör Netz
  - XBUS Störung Batterie
  - XBUS Störung Stromversorgung
  - XBUS Stör Sich
  - XBUS Störung Sabotage
  - XBUS Störung Antenne
  - XBUS Fremdfunk
  - XBUS Überfall
  - XBUS Feuer
  - XBUS Med Notfall
  - XBUS Verbindung Stromversorgung
  - XBUS Ausgang Sabotage
  - XBUS Niedrige Spannung
  - Technikerquittierung erforderlich
  - Autom Scharfsch
- Systeminformationen
  - Meldergruppen im Dauertest
  - Offene Eingänge
  - Bereichsstatus
  - Batterie schwach (Sensor)
  - Sensor Störung Kommunikation
  - FÜ Batterie schwach
  - FÜ Störung Kommunikation
  - FÜ Test überfällig
  - Kamera Offline
  - Fernbedienung Batterie schwach
  - XBUS Überstrom
  - Name des Errichters
  - Tel des Errichters
  - Techniker freigegeben
  - Hersteller freigegeben
  - Neu starten
  - Hardware Störung
  - Überstrom Ausgang
  - Akku schwach
  - Netzwerkverbindung
  - Systemname

12.2.2 Beschreibung der LEDs

Beschreibung	Symbol	Farbe	Betriebsstatus	Beschreibung
Information	i	Blau	Ein	Das System oder der Bereich kann nicht scharfgeschaltet werden. Erzwungene Scharfschaltung ist möglich (Fehler oder offene MGs können gesperrt werden).
			Blinkt	Das System oder der Bereich kann nicht scharfgeschaltet werden, erzwungene Scharfschaltung ist nicht möglich (Fehler oder offene MGs können nicht unterdrückt werden).
			Aus	Das System oder der Bereich kann scharfgeschaltet werden.
		Orange	Blinkt	Techniker ist vor Ort.
Benutzer		Grün	Ein	Der zugewiesene Bereich ist unscharfgeschaltet.
			Blinkt	Der zugewiesene Bereich intern scharfgeschaltet (A/B).
			Aus	Der zugewiesene Bereich ist extern scharfgeschaltet.
Alarm		Rot	Ein	Alarm
			Blinkt	-
			Aus	Kein Alarm
Alarm		Orange	Ein	-
			Blinkt	Problem
			Aus	Keine Probleme
Netz		Grün	Ein	System in Ordnung
			Blinkt	Störung Netzstromversorgung
			Aus	Keine Verbindung zum Bus

	HINWEIS
	Die LED-Anzeigen für Information, Bereichsstatus, Alarm und Störung werden im Bereitschaftszustand des Bedienteils deaktiviert. Ein gültige Benutzer-PIN muss eingegeben werden. Sie kann konfiguriert werden, wenn die Stromanzeige im Bereitschaftszustand leuchtet.

12.2.3 Beschreibung des Anzeigemodus

Es gibt zwei Anzeigemodi (automatisch):

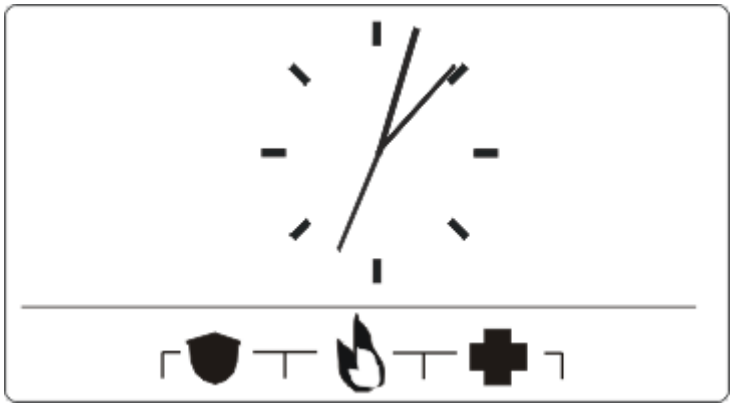
- Mehrbereichsansicht: Der Benutzer hat Zugriff auf mehrere Bereiche. Die Anzeige der Bereiche erfolgt über Bereichsgruppen. Wurden keine Bereichsgruppen angelegt, wird nur die allgemeine Gruppe „Alle meine Bereiche“ angezeigt.

- Einzelbereichsansicht: Der Benutzer besitzt nur Rechte für einen Bereich. In der Einzelbereichsansicht wird nur der Bereich, der direkt kontrolliert werden kann, in großer Schrift angezeigt.

	HINWEIS
	Die Rechte eines Benutzers können über die Benutzereinstellungen oder die Einstellungen des Bedienteils, an dem sich der Benutzer anmeldet, beschränkt werden. Nur wenn der Benutzer und das Bedienteil, an dem er sich anmeldet, die Rechte für einen bestimmten Bereich besitzen, wird dieser auch angezeigt. Besitzt der Benutzer Rechte für mehrere Bereiche, das Bedienteil jedoch nur Rechte für einen Bereich, steht auch dem Benutzer nur die Einzelbereichsansicht zur Verfügung.

12.2.4 Funktionstasten im Bereitschaftszustand

Notfalltasten

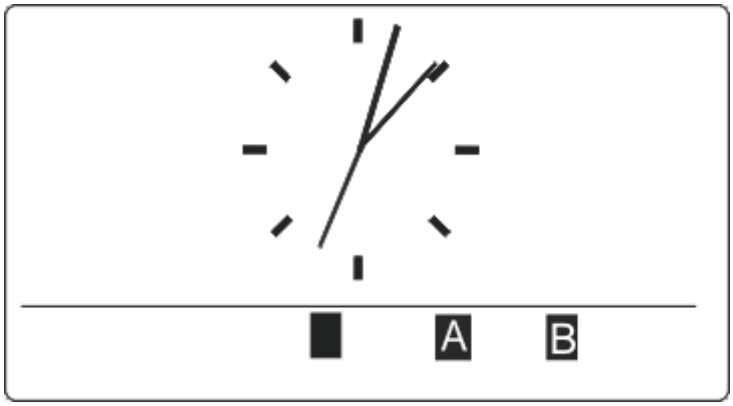


Je nach Konfiguration werden Notfalltasten angezeigt. Das gleichzeitige Drücken der Tasten aktiviert einen Alarm bzw. Notruf.

	Überfallalarm
	Feueralarm
	Medizinischer Notfall

Der aktivierte Prozess hängt von der jeweiligen Systemkonfiguration ab. Einzelheiten erfahren Sie von Ihrem Errichter.

Direkteinstellungen



Je nach Konfiguration wird die Direkteinstellungsoption angezeigt. In diesem Fall ist für den Bereich, der dem Bedienteil zugewiesen ist, eine erzwungene Scharfschaltung / interne Scharfschaltung ohne PIN möglich.

13 Software-Supporttools

Für die Fernverwaltung einer SPC-Zentrale stehen folgende PC-basierte Software-Tools zur Verfügung:

- **SPC Manager**
  Mit diesem Tool können zugriffsbasierte Funktionen des SPC-Systems aus der Ferne erstellt, gesteuert und geändert werden.
- **SPC Safe**
  Mit diesem Tool kann ein SPC-System automatisch aus der Ferne verwaltet werden.
- **SPC Fernwartung**
  Mit diesem Tool kann ein SPC-System aus der Ferne überwacht und gewartet werden.

14 Systemstart

!	⚠ VORSICHT
	DasSPC-System muss von einem autorisierten Installationstechniker errichtet werden.

1. Verdrahten Sie das Bedienteil mit der X-BUS-Schnittstelle am Controller.
2. Rufen Sie den Techniker-Programmiermodus durch Eingabe der Techniker-PIN (Werkseinstellung: 1111) auf. Weitere Informationen finden Sie unter Techniker-PINs [→ 107].

14.1 Technikermodi

Das SPC-System verfügt über zwei Programmiermodi für autorisierte Installationstechniker: Konfigurationsmodus und Wartungsmodus. Im Browser ist eine Abmeldung nur im Wartungsmodus zulässig.

Konfigurationsmodus

i	Sämtliche Alarme, Störungen und Sabotagemeldungen müssen abgeschaltet oder gelöscht werden, bevor der Konfigurationsmodus verlassen werden kann.

Im Konfigurationsmodus stehen umfangreiche Programmierfunktionen zur Verfügung. Allerdings werden beim Programmieren im Konfigurationsmodus alle Alarmeinstellungen, Berichte und im System programmierte Ausgänge deaktiviert. Eine vollständige Übersicht über die Menüoptionen im Konfigurationsmodus finden Sie auf Seite [→ 115].

Wartungsmodus

Im Wartungsmodus stehen weniger Programmierfunktionen zur Verfügung; im System programmierte Ausgänge werden jedoch nicht beeinträchtigt. Eine vollständige Übersicht über die Menüoptionen im Wartungsmodus finden Sie auf Seite [→ 114].

14.1.1 Techniker-PIN/Code

Die standardmäßige Techniker-PIN beim Start ist 1111.

Wenn die Installation nach dem Start von Grade 2 auf Grade 3 geändert wurde, erhalten alle PINs eine vorangestellte 0. Die standardmäßige Techniker-PIN lautet dann 01111.

Wird die Zahl der Stellen einer PIN erhöht (siehe Systemoptionen [→ 239]), wird bestehenden PINs eine entsprechende Anzahl von Nullen vorgestellt (zum Beispiel: 001111 für eine 6-stellige PIN).

!	*HINWEIS*
	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.

14.2 Programmiertools

Bedienteil

Das Bedienteil gewährleistet einen schnellen Zugriff auf Menüs und Programmieroptionen direkt vor Ort. Der autorisierte Installationstechniker muss die anfänglichen Standardkonfigurationen über das Bedienteil einstellen. Auch die Programmierung der Proxy-Ausweis-/Geräte-Leser und die Benutzerzuweisung muss über das Bedienteil erfolgen.

SPC Pro

SPC Pro ist eine Softwareanwendung, mit der sich SPC-Systeme online und offline konfigurieren lassen. Das SPC Pro-Programmiertool bietet zusätzliche Kommunikations- und X10-Funktionen, die auf dem Bedienteil nicht zur Verfügung stehen. Mit SPC Pro können außerdem Firmware-Upgrades durchgeführt werden.

SPC Pro unterstützt Verbindungen über USB, serielle Anschlüsse, Ethernet und PSTN/GSM-Modems mit einem SPC-Controller.

14.2.1 Fast Programmer

Beim SPC Fast Programmer handelt es sich um einen externen Speicherstick, mit dem der Techniker Konfigurationsdateien schnell und bequem hoch- und herunterladen kann. Der Fast Programmer kann in Verbindung mit allen vorgenannten Programmiertools verwendet werden. Weitere Informationen finden Sie auf Seite [→ 336].

Der Fast Programmer kann Firmware-Upgrades ausführen.

14.3 Konfigurierung der Starteinstellungen

Die folgenden Starteinstellungen können später bei der Konfiguration der Systemfunktionen geändert werden.

Beim Start der Zentrale wird die Versionsnummer des SPC-Systems auf dem Bedienteil angezeigt.

Voraussetzung:

▷ Drücken Sie die Reset-Taste auf der Leiterplatine für mindestens 6 Sekunden, um die Startkonfiguration zu initialisieren.

1. Drücken Sie eine Taste auf dem Bedienteil.
   - Drücken Sie nach jeder Einstellung auf WEITER, um zur nächsten Einstellung zu gelangen.
2. Wählen Sie eine SPRACHE für den Konfigurationsassistenten aus.
3. Wählen Sie die passende REGION aus.
   - EUROPA, SCHWEDEN, SCHWEIZ, BELGIEN, SPANIEN, UK, IRLAND, ITALIEN, KANADA, USA
4. Wählen Sie die ART der Installation:
   - PRIVAT: Geeignet für den Einsatz zu Hause (Privathäuser und -wohnungen).
   - KOMMERZIELL: Bietet zusätzliche MG-Typen und gewerbliche Standard-MG-Beschreibungen für die ersten acht MGs.

- FINANZSEKTOR: Speziell für Banken und sonstige Finanzinstitute; umfasst Funktionen wie automatische Scharfschaltung, Schließung nach Zeitplan, Verknüpfung von Bereichen und Zonen mit Körperschallmelder.

Weitere Informationen zu Standard-MG-Beschreibungen finden Sie auf Standardeinstellungen für die Modi „Privat“, „Kommerziell“ und „Finanziell“ [→ 363].

5. Wählen Sie den Sicherheitsgrad Ihrer Anlage aus.
6. SPRACHE Zeigen Sie die verfügbaren Standardsprachen an. Die folgenden Sprachen sind für die jeweilige Region verfügbar:
   - IRLAND/UK – Englisch, Französisch, Deutsch
   - EUROPA/SCHWEIZ/SPANIEN/FRANKREICH/DEUTSCHLAND – Englisch, Französisch, Deutsch, Italienisch, Spanisch
   - BELGIEN – Englisch, Niederländisch, Flämisch, Französisch, Deutsch
   - SCHWEDEN – Englisch, Schwedisch, Dänisch, Französisch, Deutsch

!	*HINWEIS*
	Wenn das System zurückgesetzt und die REGION beim Start geändert wird, stehen für die neue REGION nur die auf dem System verfügbaren Sprachen der vorherigen REGION zur Verfügung.

7. Wählen Sie die Sprachen aus, die in Ihrer Anlage zur Verfügung stehen sollen. Ausgewählten Sprachen wird ein Sternchen (*) vorangestellt. Mit der Rautetaste (#) wählen Sie eine Sprache aus und entfernen die Markierung.
   ⇨ Sprachen, die nicht markiert sind, werden aus dem System gelöscht und stehen nicht mehr zur Verfügung, wenn Sie das System auf die Standardeinstellungen zurücksetzen.
   ⇨ Informationen zum Hinzufügen von Sprachen finden Sie in den jeweiligen Abschnitten ‚Upgrade von Sprachen‘ für das Bedienteil, den Browser und SPC Pro.
8. Geben Sie das DATUM und die UHRZEIT ein.
   ⇨ Das System durchsucht den X-BUS nach Modems.
9. Aktivieren Sie SPC CONNECT, damit die Zentrale mit https://www.spcconnect.com kommunizieren kann, sobald die IP-Adresse der Zentrale konfiguriert wurde.
10. Aktivieren Sie DHCP, um der Zentrale automatisch eine verfügbare Netzwerk-IP-Adresse zuzuweisen. Wenn Sie SPC CONNECT und DHCP aktiviert haben, wird nun ein SPC CONNECT ATS zur Zentrale hinzugefügt, um die Verbindung mit https://www.spcconnect.com herzustellen.
11. Für Zentralen mit aktiviertem DHCP wird die automatisch zugewiesene IP-Adresse im Menü „IP-ADRESSE“ angezeigt. Falls DHCP nicht aktiviert ist, wird die standardmäßige IP-Adresse angezeigt. Fahren Sie mit AUSWAHL fort. Im Techniker-Programmiermodus müssen Sie unter KOMMUNIKATION die statische IP-Adresse für die Zentrale manuell eingeben.
12. Wählen Sie den X-BUS-Adressiermodus aus:
   - MANUELL: für die häufigsten Installationstypen empfohlen, besonders bei einer Vorkonfiguration

- AUTO: wird nur für sehr kleine Anlagen empfohlen.

13. Wählen Sie die Installationstopologie: DURCHSCHLEIFBAR (Ring) oder STICHLEITUNG

    ⇨ Das System sucht nach der Anzahl der Bedienteile, Erweiterungsmodule, Türsteuerungen und verfügbaren Linieneingängen.

14. Betätigen Sie WEITER, um alle X-BUS-Geräte zu suchen.

    ⇨ Der PROGRAMMIERMODUS wird angezeigt.
    ⇨ Die Starteinstellungen sind abgeschlossen.

15. Überprüfen Sie die Alarme im Menü SYSTEMSTATUS > ALARME
    Anderenfalls können Sie den Konfigurationsmodus nicht verlassen.

16. Konfigurieren Sie das System über das Bedienteil, SPC Pro oder den Webbrowser.

Siehe auch

Standardeinstellungen für die Modi „Privat“, „Kommerziell“ und „Finanziell“ [→ 363]

14.4 Anlegen von Systembenutzern

Das SPC-System erlaubt standardmäßig nur Technikerzugriff auf das System. Der Techniker muss Benutzer anlegen, damit Mitarbeiter vor Ort das System bei Bedarf scharfschalten, unscharfschalten und damit grundlegende Aktionen ausführen können. Benutzer können nur eingeschränkte Funktionen der Zentrale nutzen, indem sie bestimmten Profilen zugeordnet werden.

Das System lässt alle Benutzer-PINs innerhalb des vorgegebenen PIN-Bereichs zu, d. h. wird eine PIN aus vier Ziffern verwendet, sind alle Benutzer-PINs zwischen 0000 und 9999 zulässig.

Weitere Informationen finden Sie im Abschnitt Hinzufügen von Benutzern:

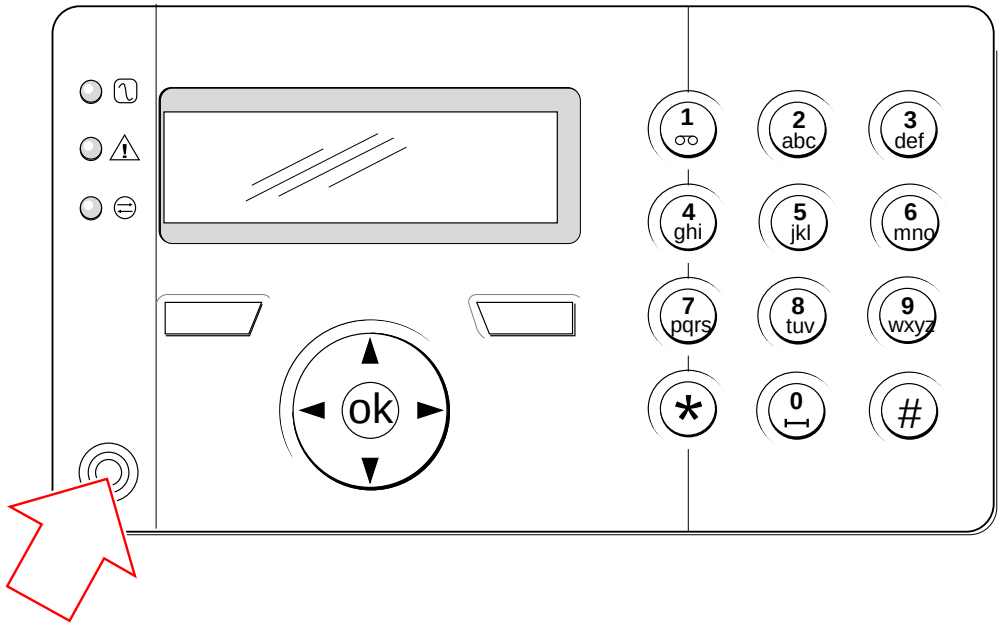
Der Herstellerzugriff auf das System (d. h. er kann Firmware-Upgrades der Zentrale zulassen) ist als Benutzerrecht für ein Benutzerprofil konfiguriert. Wenn ein Benutzer Firmware-Upgrades ermöglichen möchte, muss er über das korrekte Profil für diese Aktivität verfügen.

Siehe auch

Techniker-PIN/Code [→ 107]

14.5 Programmierung des Transponders

Das SPC-Bedienteil kann für den Betrieb mit einem Proxy-Karten-/Geräteleser konfiguriert werden. Benutzer, deren Profile entsprechend konfiguriert wurden, können das System berührungslos scharfschalten oder unscharfschalten und auch programmieren, je nach Benutzerlevel. Wurde ein Proxy-Gerät auf dem Bedienteil programmiert, kann der Benutzer das System scharfschalten oder unscharfschalten oder auf die Benutzerprogrammierung zugreifen, indem er das Proxy-Gerät in 1 cm Entfernung vor den Empfangsbereich am Bedienteil hält.



Empfangsbereich am Bedienteil

Programmieren des Transponders am Bedienteil:

1. Techniker-Programmier-PIN eingeben. (Als Standard-Pin ist 1111 vorgegeben. (Siehe Techniker-PINs [➙ 107].)
2. Blättern Sie zum Menüpunkt BENUTZER.
3. Drücken Sie auf AUSWAHL.
4. Wählen Sie BEARBEITEN und anschließend BENUTZER1 aus der Liste.
5. Blättern Sie zu TRANSPONDER und drücken Sie auf AUSWAHL.
6. Schalten Sie die TRANSPONDER-Funktion AKTIV bzw. INAKTIV.
   ⇨ In der oberen Zeile des Bedienteils blinkt TP VORHALTEN.
7. Halten Sie den Transponder (TP) im Abstand von 1 cm vor den Empfangsbereich des Bedienteils.

⇨ Das Bedienteil zeigt an, dass das Gerät angemeldet wurde (Anzeige: TP KONFIGURIERT).

Deaktivieren eines Transponders im System:

1. Techniker-Programmier-PIN eingeben. (Als Standard-Pin ist 1111 vorgegeben. (Siehe Techniker-PINs [➙ 107].)
2. Blättern Sie zum Menüpunkt BENUTZER.
3. Drücken Sie auf AUSWAHL.
4. Wählen Sie BEARBEITEN und anschließend BENUTZER1 aus der Liste.
5. Blättern Sie zu TRANSPONDER und drücken Sie auf AUSWAHL.
6. Wählen Sie INAKTIV.

⇨ Auf dem Bedienteil wird AKTUALISIERT angezeigt.

14.6 Konfiguration von Funk-Fernbedienungen

Ist auf dem Bedienteil oder dem Controller ein 868-MHz-Funkempfängermodul installiert, kann über das Bedienteil eine Fernbedienung programmiert werden.

Programmieren der Fernbedienung im System:

1. Geben Sie die Techniker-Programmier-PIN ein (Standard-PIN ist 1111). (Siehe Techniker-PINs [→ 107].)
2. Verwenden Sie die Pfeiltasten nach oben/unten, um bis zur Option BENUTZER zu blättern.
3. Drücken Sie auf AUSWAHL.
4. Wählen Sie die Option BEARBEITEN und drücken Sie auf AUSWAHL.
5. Blättern Sie zum gewünschten Benutzer und drücken Sie auf AUSWAHL.
6. Blättern Sie zur Option FERNBEDIENUNG und drücken Sie auf AUSWAHL.
7. Wählen Sie die Einstellung AKTIV und drücken Sie auf AUSWAHL.
   ⇨ In der oberen Zeile des Bedienteils blinkt die Meldung FERNB BETÄTIGEN.
8. Begeben Sie sich mit der Fernbedienung in eine Entfernung von max. 8 Metern vom Bedienteil und drücken Sie eine der Tasten auf der Fernbedienung.

⇨ Die Meldung FERNB EINGELERNT auf dem Display zeigt an, dass das Gerät angemeldet.

Deaktivierung der Fernbedienung im System:

1. Geben Sie die Techniker-Programmier-PIN ein (Standard-PIN ist 1111). (Siehe Techniker-PINs [→ 107].)
2. Verwenden Sie die Pfeiltasten nach oben/unten, um bis zur Option BENUTZER zu blättern.
3. Wählen Sie die Option BEARBEITEN und drücken Sie auf AUSWAHL.
4. Blättern Sie zum gewünschten Benutzer und drücken Sie auf AUSWAHL.
5. Blättern Sie zur Option FERNBEDIENUNG und drücken Sie auf AUSWAHL.
6. Wählen Sie INAKTIV und drücken Sie SPEICHERN.

Wird kein 868-MHz-Funkempfänger im System erkannt, wird die Option FERNBEDIENUNG nicht im Menü des Bedienteils angezeigt.

Anzahl der Fernbedienungen pro Benutzer: Pro Benutzer kann nur eine Fernbedienung programmiert werden. Um Fernbedienungen unter Benutzern zu Tauschen, führen Sie bei neuen Geräten den Programmierprozess nochmals durch. Vorhandene Fernbedienungen stehen zur Verwendung durch unterschiedliche Benutzer zur Verfügung.

14.6.1 Quittieren von Alarmen mithilfe der Fernbedienung

Alarme im SPC-System werden in der Regel über die Option QUITTIEREN am Bedienteil bestätigt bzw. quittiert. Alarme können aber auch mit der Fernbedienung quittiert werden.

Wird auf dem Bedienteil ein aktiver Alarm angezeigt, während das System UNSCHARF ist, kann der Alarm durch Drücken der UNSCHARF-Taste auf der Fernbedienung für 5 Sekunden, nachdem das System unscharfgeschaltet wurde, quittiert bzw. zurückgesetzt werden.

Zum Aktivieren dieser Funktion muss die Systemoption QUITT MIT FERNB. aktiviert sein:

1. Melden Sie sich mit der Techniker-PIN am Bedienteil an.
2. Blättern Sie zu KONFIG. MODUS > OPTIONEN.
3. Drücken Sie auf AUSWAHL.
4. Blättern Sie zu QUITT MIT FERNB und drücken Sie auf AUSWAHL.
5. Wählen Sie die Einstellung AKTIV und drücken Sie SPEICHERN.

15 Programmieren über das Bedienteil im Wartungsmodus

Im nachstehenden Abschnitt werden die Programmieroptionen im Wartungsmodus unter Verwendung des LCD-Bedienteils beschrieben.

Die nachstehend beschriebenen Menüoptionen stehen nur im Techniker-Programmiermodus zur Verfügung:

1. Geben Sie eine gültige Techniker-PIN ein (Standard-PIN ist 1111. Weitere Informationen finden Sie unter Techniker-PINs [→ 107]).
2. Blättern Sie mit den Pfeiltasten nach oben/unten zur gewünschten Programmieroption.
3. Eine Programmieroption kann auch über die Nummerntasten am Bedienteil aufgerufen werden; hierzu müssen Sie die Techniker-Programmier-PIN plus die in der nachfolgenden Grafik aufgeführte Nummer eingeben.

⇨ Bei Änderung einer Programmieroption erscheint im Display des Bedienteils sofort die Meldung AKTUALISIERT.

1	SCHÄRFUNG	Unscharfschalten Scharfschalten oder intern scharfschalten des Systems. Siehe Seite
2	MELD SPERREN	Zeigt eine Liste der gesperrten Meldergruppen im System an. Siehe Seite
3	MELDERGRUPPE ABSCHALTEN	Ermöglicht es dem Techniker, Meldergruppen auf dem System auszuschalten. Siehe Seite [→ 159]
4	LOGBUCH	Zeigt eine Liste der letzten Systemereignisse an. Siehe Seite [→ 159]
5	ZUTRITTS LOGBUCH	Zeigt eine Liste der letzten Zugriffe auf das System an. Siehe Seite
6	ALARMPROTOKOLLIERUNG	Zeigt eine Liste der letzten Alarme an.
7	TECHN PIN ÄNDERN	Hier kann der Techniker die Techniker-PIN ändern. Siehe Seite [→ 160]
8	BENUTZER	Hier kann der Techniker Benutzer hinzufügen, bearbeiten oder löschen. Siehe Seite [→ 161]
9	SMS	Mit dieser Funktion kann der Benutzer SMS-Details für Benutzer hinzufügen, bearbeiten oder löschen. Siehe SMS [→ 165]

Siehe auch

- TEST [→ 154]
- TÜRSTEUERUNG [→ 168]
- Technikerprogrammierung über das Bedienteil [→ 115]
- SYS IDENTIFIK [→ 168]
- DATUM/UHRZEIT [→ 168]
- SMS [→ 165]

16 Technikerprogrammierung über das Bedienteil

Im nachstehenden Abschnitt werden die Programmieroptionen im Konfigurationsmodus unter Verwendung des LCD-Bedienteils beschrieben.

Die nachstehend beschriebenen Menüoptionen stehen nur im Konfigurationsmodus zur Verfügung:

1. Geben Sie eine gültige Techniker-PIN ein (Standard-PIN ist 1111. Weitere Informationen finden Sie unter Techniker-PINs [→ 107]).
2. Drücken Sie auf AUSWAHL, um KONFIG. MODUS zu wählen.
3. Blättern Sie mit den Pfeiltasten nach oben/unten zur gewünschten Programmieroption.
4. Eine Schnellzugriffsfunktion steht ebenfalls zur Verfügung. Drücken Sie #, um einen Parameter auszuwählen (z. B. ein Meldergruppen-Attribut). Der ausgewählte Parameter wird mit einem * markiert (z. B. *Sperren).

⇨ Nach Abschluss des Programmiervorgangs erscheint im Display des Bedienteils sofort die Meldung AKTUALISIERT.

16.1 SYSTEM STATUS

Die Systemstatus-Funktion zeigt alle Störungen im System an.

Anzeigen der Störungen:

1. Blättern Sie zum Menüpunkt SYSTEM STATUS.
2. Drücken Sie auf AUSWAHL.

⇨ Der Status der folgenden Elemente wird angezeigt.

⇨ Klicken Sie auf ein Element, um weitere Informationen anzuzeigen.

OFFENE MG	Zeigt alle offenen Meldergruppen an.
ALARME	Zeigt aktuelle Alarme des Systems an.
DAUERTEST	Zeigt alle Meldergruppen an, die sich im Dauertest befinden.
ABSCHALTUNGEN	Zeigt ausgeschaltete Meldergruppen an.
SCHARFSCH FEHLG	Zeigt alle Bereiche an, für die die Scharfstellung fehlgeschlagen ist. Wählen Sie einen Bereich, um Informationen zum Fehlschlagen der Scharfstellung anzuzeigen.
BATTERIE	Zeigt die verbleibende Laufzeit, Spannung und Stromstärke der Batterie an. Damit die verbleibende Akkulaufzeit auf dem Bedienteil bei einem eventuellen Stromausfall angezeigt wird, müssen unter OPTIONEN die Werte für **Akku Kapazität** und **Maximaler Strom** eingegeben werden. Dies wird unter „STATUS – AKKU – Akku Zeit“ angezeigt. Dieses Menü zeigt außerdem an, ob eine Akkustörung vorliegt.
AUSG.	Zeigt Spannung und Stromstärke der Hilfsstromversorgung an.

	HINWEIS
	Benutzer können den KONFIG MODUS nicht verlassen, solange Störungen bestehen. Die erste Störung wird am Bedienteil angezeigt, sobald der Benutzer versucht, den Technikermodus zu verlassen. Sie können alle Störungsmeldungen im Menü SYSTEM STATUS unter ALARME und OFFENE MG anzeigen und abschalten.

16.2 OPTIONEN

1. Blättern Sie zu OPTIONEN und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten Programmieroption:

⇨ Die im Menü OPTIONEN angezeigten Programmieroptionen unterscheiden sich je nach Sicherheitsgrad des Systems (siehe rechte Spalte).

	⚠ **WARNUNG**
	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.

Variable	Beschreibung	Rücksetzen
SICHERHEITSGRAD	Legt den Sicherheitsgrad der SPC-Installation fest. ● Regionen Irland und Europa: – EN50131 Grad 2 – EN50131 Grad 3 – Unbeschränkt ● Region UK: – PD6662 (basiert auf EN50131 Grad 2) – PD6662 (basiert auf EN50131 Grad 3) – Unbeschränkt ● Region Schweden: – SSF1014:3 Larmclass 1 – SSF1014:3 Larmclass 2 – Unbeschränkt ● Region Belgien: – TO-14 (basiert auf EN50131 Grad 2) – TO-14 (basiert auf EN50131 Grade 3) – Unbeschränkt ● Region Schweiz: – SWISSI Kat. 1 – SWISSI Kat. 2 – Unbeschränkt ● Region Spanien – EN50131 Grad 2 – EN50131 Grad 3 ● Region Deutschland – VdS Klasse A	Grad: 2 Land: n.r.

Variable	Beschreibung	Rücksetzen
	– VdS Klasse C – Unbeschränkt ● Frankreich – NFtyp2 – NFtyp3 – Unbeschränkt	
REGION	Legt die spezifischen regionalen Anforderungen fest, welche die Anlage erfüllt. Verfügbare Optionen sind: UK, IRLAND, EUROPA, SCHWEDEN, SCHWEIZ, BELGIEN, DEUTSCHLAND und FRANKREICH	
INSTALLATIONSTYP	Legt fest, ob SPC in einem gewerblichen (Geschäftsräume usw.) oder einem privaten Objekt (Wohnung, Wohnhaus usw.) installiert wird. Wählen Sie zwischen KOMMERZIELL (siehe Seite [→ 346]), PRIVAT (siehe Seite [→ 345]) oder FINANZSEKTOR.	Privat

Weitere Informationen zu den nachfolgend aufgeführten OPTIONEN finden Sie im Abschnitt Systemoptionen [→ 239].

INTERNSCHARF A	UMBENENNEN VERZÖGERT F VERZ ZU VERZ VERZ ZU EINBRUCH LOKAL
INTERNSCHARF B	UMBENENNEN VERZÖGERT F VERZ ZU VERZ VERZ ZU EINBRUCH LOKAL
INFO BEI ÜBERTR	INFO ANZEIGEN (AKTIV/INAKTIV)
BESTÄTIGUNG	VDS DD243: GARDA EN50131-9
BEST.ZONEN	ANZ. MG auswählen.
AUTO QUITTIERUNG	AKTIV/INAKTIV
QUITT MIT FERNB	AKTIV/INAKTIV
BEDROHUNGSPIN	DEAKTIVIERT PIN +1 PIN +2
WIEDERH.SIRENE	AKTIV/INAKTIV
SOFORTIGE AUSL	AKTIV/INAKTIV
SIR SCHÄFEHLG	AKTIV/INAKTIV
BLITZ SCHÄFEHLG	AKTIV/INAKTIV
ERZW MIT ALARM	AKTIV/INAKTIV Nut verfügbar im Modus UNBESCHRÄNKT, da die Einstellungen nicht den Anforderungen der EN50131 entsprechen.
SPRACHE	SYSTEMSPRACHE SPRACHE IN RUHE
PIN ?-STELLIG	4 STELLEN

	5 STELLEN 6 STELLEN 7 STELLEN 8 STELLEN
QUITT MIT CODE	AKTIV/INAKTIV
WEB ZUGRIFF	AKTIV/INAKTIV Erlaubt/beschränkt den Zugriff auf den Webbrowser.
OFFENE MG	AKTIV/INAKTIV
TECHNIKER FREIG	AKTIV/INAKTIV
HERSTELLER FREIG. *	AKTIV/INAKTIV
ZEIGE STATUS	AKTIV/INAKTIV
ENDWIDERSTAND	KEINE ENDW. 1K ENDW. 1K5 ENDW. 2K2 ENDW. 4K7 ENDW. 10K ENDW. 12K 2 ENDW. 1K / 470R 2 ENDW. 1K / 1K 2 ENDW. 2K2 / 1K0 2 ENDW. 2K2 / 1K5 2 ENDW. 2K2 / 2K2 2 ENDW. 2K2 / 4K7 2 ENDW. 2K7 / 8K2 2 ENDW. 2K2/ 10K 2 ENDW. 3K0 / 3K0 2 ENDW. 3K3 / 3K3 2 ENDW. 3K9 / 8K2 2 ENDW. 4K7 / 2K2 2 ENDW. 4K7 / 4K7 2 ENDW. 5K6 / 5K6 2 ENDW. 6K8 / 4K7 2 ENDW. 10K / 10K MASK_1K_1K_6K8 MASK_1K_1K_2K2 MASK_4K7_4K7_2K2
SMS AUTH MODUS	NUR PIN NUR RUFNUMMER PIN + RUFNUMMER NUR SMS PIN SMS PIN + RUFNUMMER
TP + PIN	AKTIV/INAKTIV
QUITT BEI UNSCH	AKTIV/INAKTIV **Hinweis**:Um PD6662 zu erfüllen, muss diese Option deaktiviert werden.
TECHNIKERRESET	AKTIV/INAKTIV
SABO BEI OFFLINE	AKTIV/INAKTIV
SPERRCODE	AKTIV/INAKTIV Wenn aktiviert, kann die Anlage nicht über die gelbe Taste an der Zentrale zurückgesetzt werden, solange keine Techniker-PIN am Bedienteil eingegeben wird.
SICHERE PINS	AKTIV/INAKTIV
UHR EINSTELLUNG	AUTO WINTERZEIT ZEIT SYNCH. NETZ

VERDACHT HÖRBAR	AKTIV/INAKTIV
ZEIGE KAMERAS	AKTIV/INAKTIV
KS TEST B.SCHARF	AKTIV/INAKTIV
VERBOTEN SCHARF	AKTIV/INAKTIV
ANTIMASK SCHARF	DEAKTIVIERT SABOTAGE STÖRUNG EINBRUCH
ANTIMASK UNSCH.	DEAKTIVIERT SABOTAGE STÖRUNG EINBRUCH
BEDROHUNGSALARM WIEDERHOLEN	AKTIV/INAKTIV
NOTRUF MEHRFACH	AKTIV/INAKTIV
VERIFIKAT.STILL	AKTIV/INAKTIV
KONFIG.BEENDET	AKTIV/INAKTIV

* Nicht verfügbar für SPC42xx, SPC43xx.

16.3 TIMER

1. Blättern Sie zu TIMER und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten Programmieroption:

Timer

Die Funktionen werden in der nachstehenden Reihenfolge zugeordnet:

- 1st Zeile: Web/SPC Pro
- 2· Zeile: Bedienteil

Timer	Beschreibung	Rücksetzen
Bedient. Summer		
Innensirenen ZEIT INNENSIR	Dauer der Aktivierung der Innensirenen im Alarmfall (1 – 15 Minuten: 0 = niemals)	15 Min.
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.
Bestätigung		
Confirm ZEIT BEST ALARM	• **Hinweis**: Nur verfügbar, wenn der Sicherheitsgrad „Unbeschränkt“ und „DD243“ für die Bestätigungsvariable ausgewählt ist. (Siehe Systemoptionen [→ 239].) Bezieht sich auf die Alarmbestätigungsfunktion: maximale Zeit zwischen den Auslösungen zweier unabhängiger Meldergruppen, die einen bestätigten Alarm generieren. (30–	30 Min.

Timer	Beschreibung	Rücksetzen
	60 Minuten)	
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 Alarmabbruchsmeldung gesendet werden kann. (0–999 Sekunden)	30 Sek.
Einstellung		
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.
Alarm		
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). **Hinweis**: Zur Aktivierung der automatischen Tests muss das Attribut **Automatischer Meldertest** für eine Körperschall-MG aktiviert sein.	168 Stunden.
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.
ALARME		
Verz Netzstörung VERZ STÖR NETZ	Die Verzögerungszeit nach einer erkannten Netzstörung, bis das System einen Alarm aktiviert. (0–60 Minuten)	0 min.
Techniker		

Timer	Beschreibung	Rücksetzen
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.
Bedienteil		
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
Feuer		
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 [→ 256].	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 [→ 256].	120 Sek.
PIN		
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
Allgemeine Einstellungen		
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.
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 **Überwacht** 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.

16.4 BEREICHE

1. Blättern Sie zu BEREICHE und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten Programmieroption:

HINZUFÜGEN	In den Modi „Privat“ und „Kommerziell“ ist standardmäßig der Bereichstyp „Standard“ eingestellt. Im Modus „Finanziell“ können die Bereichstypen STANDARD, ATM, TRESOR oder ERWEITERT ausgewählt werden. Geben Sie den Namen des Bereichs und die gewünschte Verzögerungszeit ein.
BEARBEITEN	Bearbeiten Sie die folgenden Einstellungen: ● BESCHREIBUNG ● EINBRUCH VERZ – ALARMVERZ – SCHÄRFUNGSVERZ – KEINE VERZÖGER. – EING.FERNB.AKTIV ● INTERNSCHARF A/B – AKTIV/INAKTIV – VERZÖGERT – F VERZ ZU VERZ – VERZ ZU EINBRUCH – LOKAL – KEINE SIRENEN ● VERKNÜPFTE BER. – BER – EXT SCHARF – SCHARFSCH ALLE – KEIN SCHARF – ALLE EXTERN SCHARF VERHINDERN – UNSCHARF – UNSCH ALLE – KEIN UNSCHARF – KEIN UNSCH. ALLE ● ZEITPLAN – KALENDER – AUTO SCHARF/UNSCHARF – ZEIT GESPERRT – TRESOR ZUGANG ● ÜBERTRAGEN – ZU FRÜH SCHARF – ZU SPÄT SCHARF – ZU FRÜH UNSCHARF

	– ZU SPÄT UNSCHARF ● SCHARF/UNSCHARF – VORWARNZEIT – BENUTZER ABBR. – BENUTZER VERZ. – SCHLÜSSELSCHALT – VERZ. INTERVAL – VERZ. LIMITE – UNSCHARF VERZ. – DAUER UNSCHARF – INTERLOCK – DOPPELCODE ● FUNKAUSGANG
LÖSCHEN	Wählen Sie den Bereich, den Sie löschen möchten, aus.

Weitere Informationen zu diesen Optionen finden Sie unter Bereich hinzufügen/bearbeiten [→ 257].

16.5 BEREICHSGRUPPEN

1. Blättern Sie zu BEREICHSGRUPPEN, und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten Programmieroption:

HINZUFÜGEN	Geben Sie den Namen der Bereichsgruppe ein.
BEARBEITEN	GRUPPEN NAME – Benennen Sie die Gruppe wie gewünscht um. BEREICHE – Blättern Sie zu einem Bereich und wählen Sie ihn aus. Wählen Sie, wie erforderlich, AKTIV oder INAKTIV, um ihn zur Gruppe hinzuzufügen oder aus der Gruppe zu entfernen. Ein Sternchen (*) zeigt an, dass ein Bereich zur Gruppe gehört
LÖSCHEN	Wählen Sie den Bereich, den Sie löschen möchten, aus.

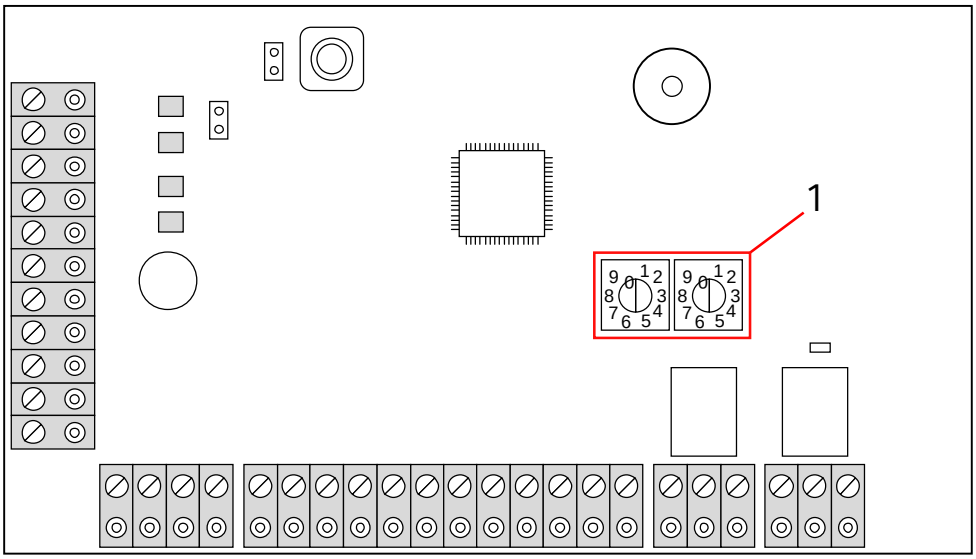
16.6 X-BUS-

1. Blättern Sie zu XBUS und drücken Sie AUSWAHL.
2. Blättern Sie wie nachfolgend dargestellt zu den gewünschten Programmieroptionen.

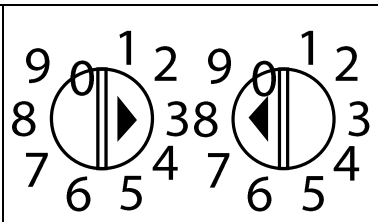
16.6.1 X-BUS-Adressierung

Mit den im vorliegenden Abschnitt beschriebenen Schritten können Erweiterungsmodule, Bedienteile und Meldergruppen konfiguriert, erkannt und überwacht werden. Über dieses Menü kann ebenfalls auf X-BUS-Einstellungen wie Typ, Übertragungszeiten und erneute Übertragungen zugegriffen werden.

Die nachfolgende Abbildung zeigt zwei Drehschalter mit Pfeilsymbolen, die jeweils auf eine Ziffer zeigen, die zusammengenommen als ID dienen (hier 3 und 8). Der rechte Schalter stellt die Einerstelle ein und der linke Schalter die Zehnerstelle. Das Erweiterungsmodul hat in diesem Fall die ID '38'.



Drehschalter

1	 Über diese Drehschalter ist die Geräte-ID '38' eingestellt.

Bei Systemen mit automatischer Nummerierung gehören Erweiterungsmodule und Bedienteile in dieselbe Nummerierungsfolge. Erweiterungsmodule und Bedienteile werden vom Controller in der Reihenfolge, in der sie erkannt werden, d. h. nach ihrer für den Controller relevanten Anordnung automatisch mit 01, 02, 03 usw. nummeriert. Bei dieser Konfiguration werden jedem Eingangserweiterungsmodul Meldergruppen zugewiesen.

Das SPC41xx unterstützt keine automatisch adressierten Erweiterungsmodule.

16.6.2 XBUS AKTUALISIE.

Das Dienstprogramm X-BUS aktualisieren führt eine Erkennung des momentanen X-BUS-Status aus und zeigt die aktuelle X-BUS-Konfiguration an.

So aktualisieren Sie den X-BUS-Status:

1. Blättern Sie zu XBUS AKTUALISIE.
2. Drücken Sie auf AUSWAHL.
   ⇨ Die Anzahl der angeschlossenen Bedienteile wird angezeigt.
3. Drücken Sie nach jeder Anzeige auf den rechten Bedienteil-Softkey, um Erweiterungen, Meldergruppen und Offline-Elemente anzuzeigen.
4. Drücken Sie zum Schließen der Anzeige erneut diese Taste.

Aktualisieren führt keine Änderungen im System durch; es ist jedoch hilfreich bei der Erkennung von Systemstörungen, wie z. B. lockeren Anschlüssen oder inaktiven Erweiterungsmodulen, bevor die Option **Neu Konfigurieren** ausgeführt wird.

16.6.3 NEU KONFIGURIEREN

	HINWEIS
	Eine Neukonfiguration ist nur für verdrahtete Meldergruppen an einem Erweiterungsmodul möglich. Funk-MGs an einem Erweiterungsmodul und Controller-MGs können nach einer Neukonfiguration nicht mehr online gebracht werden. Um Controller-MGs online zu bringen, darf den betreffenden MGs nicht der MG-Typ ‚Unbenutzt' zugewiesen werden; verwenden Sie das Menü Meldergruppen am Bedienteil oder im Webbrowser, um den MG-Typ zu ändern.

Verfügt das System über unterschiedliche Erweiterungsmodultypen (mit und ohne Drehschalter), kann das System ausschließlich automatisch neu konfiguriert werden. Besitzen sämtliche Erweiterungsmodule eines Systems Drehschalter, kann das System dennoch automatisch neu konfiguriert werden. Das System ignoriert in diesem Fall die Drehschalter und adressiert alle Erweiterungsmodule im System automatisch.

Es empfiehlt sich, vor dem Ausführen von **Neu Konfigurieren** das System mit **Aktualisieren** aufzufrischen.

Neukonfigurieren von Bedienteilen / Erweiterungsmodulen:

1. Blättern Sie zum Menüpunkt NEU KONFIGURIEREN.
2. Drücken Sie auf AUSWAHL.
   ⇨ Die Anzahl der angeschlossenen Bedienteile wird angezeigt.
3. Drücken Sie auf WEITER.
   ⇨ Die Anzahl der angeschlossenen Erweiterungsmodule wird angezeigt.
4. Drücken Sie auf WEITER.
   ⇨ Die Anzahl der angeschlossenen Meldergruppen wird angezeigt.
5. Drücken Sie ZURÜCK, um das Menü zu verlassen.

16.6.4 BEDIENTEILE/ERWEITERUNGSMODULE/TÜRSTEUER

UNGEN

	HINWEIS
	Vor dem Hinzufügen von Türsteuerungen müssen Sie ein Upgrade der Firmware auf Version 1.1 durchführen. Bei früheren Firmware-Versionen werden die Türsteuerungen von der Alarmzentrale als normale E/A-Erweiterungen erkannt, und die Türen müssen manuell hinzugefügt werden.

16.6.4.1 "LOKALISIEREN"

Gehen Sie wie folgt vor, um ein Bedienteil/eine Erweiterung/eine Türsteuerung zu lokalisieren:

1. Blättern Sie zu BEDIENTEILE, ERWEITERUNGEN oder TÜRSTEUERUNGEN und drücken Sie auf AUSWAHL.
2. Blättern Sie zu LOKALISIEREN und drücken Sie auf AUSWAHL.
3. Blättern Sie zum Bedienteil/zur Erweiterung/zur Türsteuerung, das/die lokalisiert werden soll, und drücken Sie auf AUSWAHL.
   ⇨ Das ausgewählte Gerät gibt einen Signalton ('Piepton') ab, und die LED blinkt, damit der Techniker es finden (lokalisieren) kann.
4. Drücken Sie ZURÜCK, um das Menü zu verlassen.

⇨ Verwenden Sie zum Lokalisieren von Bedienteilen die gleichen Menüpfade und wählen Sie „Bedienteile“ anstelle von „Erweiterungen“.

16.6.4.2 "STATUS INFO"

Gehen Sie wie folgt vor, um einen Überblick über die an das System angeschlossenen Bedienteile/Erweiterungen/Türsteuerungen zu erhalten:

1. Blättern Sie zu BEDIENTEILE, ERWEITERUNGEN oder TÜRSTEUERUNGEN und drücken Sie auf AUSWAHL.
2. Blättern Sie zu STATUS INFO und drücken Sie auf AUSWAHL.
3. Blättern Sie zur gewünschten Status-Programmieroption.
4. Drücken Sie auf AUSWAHL.
   ⇨ Eine Liste der erkannten Bedienteile/Erweiterungen wird angezeigt.
5. Blättern Sie innerhalb der Liste und drücken Sie auf AUSWAHL, um das gewünschte Gerät auszuwählen.
   ⇨ Parameter und sonstige Details, falls vorhanden, werden wie in der folgenden Tabelle dargestellt zum Bearbeiten angezeigt.
6. Drücken Sie ZURÜCK, um das Menü zu verlassen.

STATUS	Online oder offline
S/N	Seriennummer (zum Verfolgen und Identifizieren)
VER	Firmware-Version
STROM/SPANN	Parameter der Stromversorgung: Echtzeit-Messwerte für Spannung und

UNG	Stromstärke
INFO ADRESSE	Der Adressiermodus und die Adresse von Bedienteil\Erweiterungsmodul\Türsteuereinheit.
SICHERUNG	Der Status der Netzteilsicherung auf der Erweiterung\Türsteuereinheit
Netzteil	Netzteiltyp und -status. (nur Netzteilerweiterungen) Blättern Sie, um die Spannungs- und Stromlast auf die Ausgänge und den Batteriestatus anzuzeigen. Die Option MODE LINK steht ebenfalls zur Verfügung. Sie zeigt an, wie der Jumper für die Einstellung der gewünschten Ampere-Stunden auf der Zentrale gesteckt werden muss. Es stehen 7 Ah und 17 Ah zur Auswahl. (Dieser Jumper ist bei den Modellen SPC5350 und SPC6350 nicht vorhanden) Bei den Modellen SPC5350 und 6350 wird in diesem Menü der Status der Batterie und der Sicherungen an den Ausgängen angezeigt.
BATTERIE	Batteriespannung: Anzeige der aktuellen Batteriespannung (nur Netzteilerweiterungen)
EINGANGSSTATUS	Status der einzelnen Meldergruppen-Eingänge in Verbindung mit einer Erweiterung: C: Geschlossen, O: Offen; D: Getrennt; S: Kurzgeschlossen (nur Erweiterungen mit Eingängen)

16.6.4.3 BEDIENTEILE BEARBEITEN

Zum Bearbeiten der Bedienteile:

1. Blättern Sie zu BEDIENTEILE > BEARBEITEN.
2. Drücken Sie auf AUSWAHL.
3. Blättern Sie zu dem Gerät, das Sie bearbeiten möchten, und drücken Sie auf AUSWAHL.
   ⇨ Die Konfigurationseinstellungen für das Standard-Bedienteil und das Komfort-Bedienteil werden in den folgenden Abschnitten beschrieben.
4. Drücken Sie ZURÜCK, um das Menü zu verlassen.

Einstellungen des LCD-Bedienteils

Nehmen Sie die folgenden Einstellungen für das Bedienteil vor.

Beschreibung	Geben Sie einen eindeutigen Namen für das Bedienteil ein.
Einstellungen der Funktionstasten (im Ruhezustand)	
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 Bedrohungscodes ein Panikalarm ausgelöst wird.
Optische Anzeigen	
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 Schärfungsstatus im Bereitschaftszustand angezeigt werden soll.
Akustische Indikationen	
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.
Deaktivierung	

Kalender	Wählen Sie, ob die Aktivierung des Bedienteils nur während der im Kalender eingestellten Zeit möglich sein soll. Siehe Kalender [→ 273].
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.
Bereiche	
Ort	Wählen Sie, ob das Bedienteil in einem gesicherten Bereich montiert ist.
Bereiche	Wählen Sie die Bereiche, die über das BT gesteuert werden dürfen.
Optionen	
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.

Einstellungen Komfort-Bedienteil

Nehmen Sie die folgenden Einstellungen für das Komfort-Bedienteil vor.

Beschreibung	Geben Sie einen eindeutigen Namen für das Bedienteil ein.
Einstellungen der Funktionstasten (im Ruhezustand)	
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 Feueralarm 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 Feueralarm ausgelöst wird oder wenn ein Benutzer einen Bedrohungscode eingibt.
Optische Indikationen	
Hintergrundbeleucht	Wählen Sie, wann die Hintergrundbeleuchtung am Bedienteil

ung	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.
Akustische Indikationen	
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)
Deaktivierung	
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.
Bereiche	
Ort	Wählen Sie, ob das Bedienteil in einem gesicherten Bereich montiert ist.
Bereiche	Wählen Sie die Bereiche, die über das BT gesteuert werden dürfen.
Optionen	
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.

16.6.4.4 ERWEITERUNGEN BEARBEITEN

Zum Bearbeiten der Erweiterungen:

1. Blättern Sie zu ERWEITERUNGEN > BEARBEITEN.
2. Drücken Sie auf AUSWAHL.
3. Blättern Sie zu dem Gerät, das Sie bearbeiten möchten, und drücken Sie auf AUSWAHL.
   ⇨ Parameter und sonstige Details, falls zutreffend, werden zum Bearbeiten angezeigt:
4. Drücken Sie ZURÜCK, um das Menü zu verlassen.

Zur Benennung und Identifizierung erhalten Erweiterungen Meldergruppen zugewiesen (in 8er-Gruppen) mit aufeinanderfolgenden ID-Nummern von 1 bis 512. (Die höchste Meldergruppen-ID ist somit 512.) Daher können Erweiterungen, die mit einer Zahl >63 benannt oder identifiziert werden, keine Meldergruppen zugewiesen werden.

16.6.4.4.1 Bearbeiten von E/A-Erweiterungen

In der nachstehenden Tabelle werden die Optionen aufgeführt, die für E/A-Erweiterungen zur Verfügung stehen:

Funktion	Beschreibung
Beschreibung	Bearbeiten der Erweiterungsbeschreibung

16.6.4.4.2 Bearbeiten von Audio-Erweiterungen

In der nachstehenden Tabelle werden die Optionen aufgeführt, die im Menü **Bearbeiten** für Audio-Erweiterungen zur Verfügung stehen:

Name	Beschreibung
BESCHREIBUNG	Eingabe oder Bearbeitung der Beschreibung der Audio-Erweiterung
EINGANG	Auswahl des Meldergruppen-Eingangs.
LAUTST. LIMIT	Auswahl des Lautstärken-Limits

16.6.4.4.3 Bearbeiten von Funk-Erweiterungen

In der nachstehenden Tabelle werden die Optionen aufgeführt, die für Funk-Erweiterungen zur Verfügung stehen:

Funktion	Beschreibung
Beschreibung	Bearbeiten der Erweiterungsbeschreibung

16.6.4.4.4 Bearbeiten von analysierten E/A-Erweiterungen

In der nachstehenden Tabelle werden die Optionen aufgeführt, die für IOA-Erweiterungen zur Verfügung stehen:

Name	Beschreibung
Beschreibung	Bearbeiten der Erweiterungsbeschreibung

16.6.4.4.5 Bearbeiten von Anzeigemodul-Erweiterungen

In der nachstehenden Tabelle werden die Optionen aufgeführt, die für Anzeigemodul-Erweiterungen zur Verfügung stehen:

Name	Beschreibung
BESCHREIBUNG	Eingabe oder Bearbeitung der Erweiterungsbeschreibung
ORT	Auswahl des Orts für die Erweiterung aus einer Liste mit verfügbaren Bereichen
FUNKTIONSTASTEN	Mit dieser Funktion können Sie bestimmten Tasten Funktionen für bestimmte Bereiche zuweisen. Wählen Sie einen Bereich aus, und weisen Sie diesem Bereich eine der nachstehenden Optionen zu: ● Keine ● Unscharf ● Intern scharf A ● Intern scharf B ● Extern Scharf ● Taster Unscharf/ext scharf ● Taster Unscharf/intern scharf A ● Taster Unscharf/intern scharf B Funktionstasten ● Alles in Ordnung ● Scharfschalteberechtigung
OPTISCHE INDIKATIONEN (nur Flexible Mode)	Mit dieser Funktion können Sie jeder LED auf dem Anzeigemodul ein bestimmtes Verhalten zuweisen. Für jede LED stehen folgende Optionen zur Verfügung: ● FUNKTION – Folgende Optionen sind verfügbar: – SCHLÜSSELSCHALT – Auswahl eines Schlüsselschalters und der Schlüsselstellung – INAKTIV – Zum Deaktivieren der LED – SYS. – Auswahl des Alarmtyps, der die LED auslöst

Name	Beschreibung
	– BEREICH – Auswahl des Bereichs, der die LED auslöst – MG – Auswahl der Meldergruppe, die die LED auslöst – TÜR – Auswahl der Tür und der Türoption, die die LED auslöst ● AN – FARBE – Festlegung der Farbe bei Aktivierung ● AN – BLINKEN – Festlegung des LED-Verhaltens bei Auslösung Verfügbar sind folgende Optionen: – Permanent – leuchtet ununterbrochen – Schnell\Mittel\Langsam Blinken – Verändern der Blinkgeschwindigkeit. ● AUS – FARBE – Festlegung der Farbe bei Deaktivierung der LED ● AUS – BLINKEN – Festlegung des LED-Verhaltens im inaktiven Zustand Verfügbar sind folgende Optionen: – Permanent – leuchtet ununterbrochen – Schnell\Mittel\Langsam Blinken – Verändern der Blinkgeschwindigkeit.
LED IMMER AN	Aktivieren Sie diese Option, wenn LED-Anzeigen bei Deaktivierung der Tasten aktiv bleiben.
AKUSTISCHE IND (nur Flexible Mode)	Auswahl der akustischen Anzeigen für Alarme, Einbruch verzögert und Tastenbetätigung
DEAKTIVIERUNG (nur Flexible Mode)	Wählen Sie eine oder mehrere der nachstehenden Deaktivierungsoptionen aus: ● Kalender – Wählen Sie aus den zur Verfügung stehenden Optionen einen Kalender aus. ● Schlüsselschalter – Wählen Sie aus den zur Verfügung stehenden Optionen einen Schlüsselschalter aus. ● Bedienteil – Wählen Sie aus den zur Verfügung stehenden Optionen ein Bedienteil aus. ● Kartenleser – Aktivieren oder deaktivieren Sie die Deaktivierung mit einem Bedienteil.
MODUS	Wählen Sie Linked oder Flexible. Im Linked Mode stehen im Menü „Erweiterung bearbeiten“ nur eine reduzierte Anzahl von Optionen zur Verfügung.
EINGANG	Wählen Sie die Meldergruppe aus

16.6.4.4.6 Bearbeiten von Schlüsselschalter-Erweiterungen

In der nachstehenden Tabelle werden die Optionen aufgeführt, die für Schlüsselschalter-Erweiterungen zur Verfügung stehen:

Name	Beschreibung
BESCHREIBUNG	Eingabe oder Bearbeitung der Erweiterungsbeschreibung
ORT	Wählen Sie einen Ort für die Erweiterung aus einer Liste mit definierten Bereichen aus.
EXTS BIS AVERZ	Aktivieren oder desaktivieren Sie „Extern scharf bis Alarmverzögerung“ an der Schlüsselstellung.
OPTISCHE INDIKATIONEN	Mit dieser Funktion können Sie jeder LED auf der Schlüsselschalter-Erweiterung ein bestimmtes Verhalten

Name	Beschreibung
(nur Flexible Mode)	zuweisen. Für jede LED stehen folgende Optionen zur Verfügung: ● FUNKTION – Folgende Optionen sind verfügbar: – SCHLÜSSELSCHALT – Auswahl eines Schlüsselschalters und der Schlüsselstellung. – INAKTIV – Zum Deaktivieren der LED – SYS. – Auswahl des Alarmtyps, der die LED auslöst – BEREICH – Auswahl des Bereichs, der die LED auslöst – MG – Auswahl der Meldergruppe, die die LED auslöst – TÜR – Auswahl der Tür und der Türoption, die die LED auslöst ● AN – FARBE – Festlegung der Farbe bei Aktivierung ● AN - BLINKEN - Festlegung des LED-Verhaltens bei Auslösung. Verfügbar sind folgende Optionen: – Permanent – leuchtet ununterbrochen – Schnell\Mittel\Langsam Blinken – Verändern der Blinkgeschwindigkeit. ● AUS – FARBE – Festlegung der Farbe bei Deaktivierung der LED ● AUS – BLINKEN – Festlegung des LED-Verhaltens im inaktiven Zustand Verfügbar sind folgende Optionen: – Permanent – leuchtet ununterbrochen ● Schnell\Mittel\Langsam Blinken – Verändern der Blinkgeschwindigkeit.
DEAKTIVIERUNG (nur Flexible Mode)	Wählen Sie aus den verfügbaren Optionen eine Deaktivierungsmethode aus: ● Kalender – Wählen Sie einen Kalender aus.
SCHLÜSSELSTELLUNGEN	Mit dieser Funktion können Sie bestimmten Schlüsselstellungen ein Verhalten für bestimmte Bereiche zuweisen. Wählen Sie einen Bereich für die Schlüsselstellung aus, und weisen Sie diesem Bereich eine der nachstehenden Optionen zu: ● Keine ● Unscharf ● Intern scharf A ● Intern scharf B ● Extern Scharf ● Taster Unscharf/ext scharf ● Taster Unscharf/intern scharf A ● Taster Unscharf/intern scharf B Funktionstasten ● Alles in Ordnung ● Scharfschalteberechtigung

16.6.4.5 TÜRSTEUERUNGEN BEARBEITEN

Weitere Informationen zu Türsteuerungen finden Sie auf Seite [→ 73].

1. Blättern Sie zu TÜRSTEUERUNGEN > BEARBEITEN.
2. Drücken Sie auf AUSWAHL.

3. Blättern Sie zu dem Gerät, das Sie bearbeiten möchten, und drücken Sie auf AUSWAHL.

⇨ Parameter und sonstige Details, falls vorhanden, werden wie in der folgenden Tabelle dargestellt zum Bearbeiten angezeigt.

BESCHREIBUNG	Name der Türsteuerung
TÜREN	Konfiguration von Tür-E/A 1 und Tür-E/A 2.
LESER	Konfiguration von Leserprofilen

Bearbeiten eines TÜR-E/A:

1. Blättern Sie zum Menüpunkt TÜREN.
2. Drücken Sie auf AUSWAHL.
3. Blättern Sie zum TÜR-E/A, den Sie bearbeiten möchten, und drücken Sie auf AUSWAHL.

⇨ Parameter und sonstige Details, falls vorhanden, werden wie in der folgenden Tabelle dargestellt zum Bearbeiten angezeigt.

MELDERGRUPPEN	Es werden keine Zugangsfunktionen umgesetzt. Die Ein- und Ausgänge können normal verwendet werden.
TÜR 1 - TÜR 64	Die ausgewählte Türnummer wird dem TÜR E/A zugewiesen.

Falls die Option „MG“ für einen TÜR-E/A ausgewählt wird, müssen die beiden Eingänge dieses Tür-E/A konfiguriert werden:

Bearbeiten der beiden Meldergruppen eines TÜR-E/A:

1. Blättern Sie zum TÜR-E/A, den Sie bearbeiten möchten, und drücken Sie auf AUSWAHL

   ⇨ Die Option „MG“ ist markiert.
2. Drücken Sie auf AUSWAHL.
3. Wählen Sie die MG aus, die bearbeitet werden soll (EINGANG MK oder EINGANG REX).
4. Drücken Sie auf AUSWAHL.

⇨ Parameter und sonstige Details, falls vorhanden, werden wie in der folgenden Tabelle dargestellt zum Bearbeiten angezeigt.

NICHT ZUGEWIESEN	Diese Meldergruppe ist nicht zugewiesen und kann nicht verwendet werden.
MG 1 – MG 512	Die MG, die bearbeitet wird, wird dieser MG-Nummer zugewiesen. Wird die MG einer bestimmten MG-Nummer zugewiesen, kann sie wie eine normale MG konfiguriert werden.

Die Meldergruppen können jeder freien MG-Nummer zugewiesen werden. Die Zuweisung ist jedoch nicht fest. Wurde die MG der MG-Nummer 9 zugewiesen und wird ein Eingangserweiterungsmodul mit der Adresse 1 an den X-Bus angeschlossen (der die MG-Nummern 9–16 verwendet), wird die zugewiesene MG der Zweitürsteuerungseinheit zur nächsten freien MG-Nummer verschoben. Die Konfiguration wird entsprechend angepasst.

Bearbeiten eines LESERPROFILS:

1. Blättern Sie zu LESER.
2. Drücken Sie auf AUSWAHL.
3. Blättern Sie zu dem LESER, das Sie bearbeiten möchten, und drücken Sie auf AUSWAHL.

⇨ Wählen Sie eines der folgenden Profile für den Leser:

1	Für Leser mit einer grünen und einer roten LED.
2	Für VANDERBILT-Leser mit einer gelben LED (AR618X).
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).
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).
5	Wählen Sie diese Option für Sesam-Leser. Damit die VdS-Normen eingehalten werden, müssen Sie die Option **Überschreibe LEDs an Kartenleser** auswählen, um Rückmeldung zum Schärfungsvorgang zu erhalten.

Siehe auch

Türerweiterung [→ 73]

16.6.5 ADRESSIERMODUS

Die X-BUS-Adressierung kann auf eine der folgenden beiden Arten konfiguriert werden:

Automatische Adressierung

Die automatische Adressierung kann mit einer Kombination aus Erweiterungsmodulen mit Drehschalter und solchen ohne Drehschalter durchgeführt werden. Bei der automatischen Adressierung annulliert der Controller ggf. vorhandene Drehschalter und weist Erweiterungen und Bedienteilen im System automatisch IDs in sequenzieller Folge zu.

Manuelle Adressierung

Bei der manuellen Adressierung kann die ID jedes einzelnen Erweiterungsmoduls/Bedienteils in einem System manuell festgelegt werden. Alle Geräte sollten dort installiert werden, wo sie erforderlich sind. Dann werden die jeweiligen IDs manuell über die Drehschalter eingestellt. Die Meldergruppen zur ID können mithilfe der folgenden Formel berechnet werden: (ID-Wert × 8) + 1) = erste Meldergruppennummer und die nächsten 7 aufeinanderfolgenden Meldergruppen. Beispiel: ((ID2 × 8) +1) = 17 Meldergruppe 17 wird Eingang 1 für ID2 zugewiesen. Jedem Eingang ist die nächste darauffolgende Meldergruppe zugewiesen, in diesem Fall bis zu Meldergruppe 24. Hinweis: ID-Beschränkung für Meldergruppenzuweisung SPC 4000: Erweiterungs-ID 1–3 SPC 5000: Erweiterungs-ID 1–15 SPC 6000: Erweiterungs-ID 1–63.

ID	Zone	ID	Zone	ID	Zones	ID	Zones	ID	Zones
1	9-16	14	113-120	27	217-224	40	321-328	53	425-432
2	17-24	15	121-128	28	225-232	41	329-336	54	433-440
3	25-32	16	129-136	29	233-240	42	337-344	55	441-448
4	33-40	17	137-144	30	241-248	43	345-352	56	449-456
5	41-48	18	145-152	31	249-256	44	353-360	57	457-464
6	49-56	19	153-160	32	257-264	45	361-368	58	465-472
7	57-64	20	161-168	33	265-272	46	369-376	59	473-480

8	65-72	21	169-176	34	273-280	47	377-384	60	481-488
9	73-80	22	177-184	35	281-288	48	385-392	61	489-496
10	81-88	23	185-192	36	289-296	49	393-400	62	497-504
11	89-96	24	193-200	37	297-304	50	401-408	63	505-512

Werden zwei Geräte vom gleichen Typ (z. B. Erweiterungen) auf die gleiche ID gesetzt, geben beide Erweiterungen ein Tonsignal aus, und eine blinkende LED weist auf einen Konflikt hin. Setzen Sie die Schalter zurück, und das System liest neu ein.

Werden beide Drehschalter an einem Gerät auf Null gestellt (0, 0), wird die gesamte Konfiguration zur automatischen Adressierungskonfiguration.

Auswahl des ADRESSIERMODUS:

1. Blättern Sie zum Menüpunkt ADRESSIERMODUS.
2. Klicken Sie auf AUSWAHL.
3. Wählen Sie den gewünschten Adressiermodus: AUTOMATISCH oder MANUELL.
4. Klicken Sie auf AUSWAHL, um die Einstellungen zu übernehmen.

16.6.6 XBUS TYP

Programmieren des X-BUS-Typs am Bedienteil:

1. Blättern Sie zu XBUS TYP.
2. Drücken Sie auf AUSWAHL.
3. Blättern Sie, um die gewünschte Konfiguration auszuwählen:
   - RING
   - STICH
4. Drücken Sie auf AUSWAHL, um die Einstellungen zu übernehmen.

16.6.7 ERNEUTE ÜBERTR

Programmieren der Anzahl der erneuten Daten-Übertragungsversuche des Systems über die X-BUS-Schnittstelle, bevor ein Kommunikationsfehler ausgegeben wird:

1. Blättern Sie zum Menüpunkt ERNEUTE ÜBERTR.
2. Drücken Sie auf AUSWAHL.
3. Geben Sie die gewünschte Anzahl der erneuten Datenübertragungsversuche des Systems ein.
4. Drücken Sie auf AUSWAHL, um die Einstellungen zu übernehmen.

16.6.8 KOMM TIMER

Einstellen der Dauer, bis ein Kommunikationsfehler aufgezeichnet wird:

1. Blättern Sie zum Menüpunkt KOMM TIMER.

2. Drücken Sie auf AUSWAHL.
3. Die gewünschte Zeiteinstellung eingeben.
4. Drücken Sie BESTÄTIGEN, um die Einstellungen zu übernehmen.

16.7 FUNK

1. Blättern Sie zu FUNK und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten Programmieroption:

SENSOREN	Es kann erforderlich sein, den im System eingelernten Meldertyp zu ändern, falls der Meldertyp beim Einlernprozess nicht korrekt erkannt wurde. Wurden keine Funkmelder eingelernt, wird am Bedienteil KEINE MELD AKTIV angezeigt. Für Sensoren sind folgende Optionen verfügbar: ● HINZUFÜGEN Siehe SENSOREN HINZUFÜGEN [→ 137] ● BEARBEITEN (MG-Zuweisung ändern) Siehe SENSOREN BEARBEITEN (MG-ZUWEISUNG) [→ 138] ● LÖSCHEN Wählen Sie das Gerät oder den Melder, das/der gelöscht werden soll.
FÜ	Einen FÜ (Funküberfalltaster) hinzufügen, bearbeiten oder löschen. ● HINZUFÜGEN Siehe FÜ HINZUFÜGEN [→ 138] ● BEARBEITEN Siehe FÜ BEARBEITEN [→ 139] ● LÖSCHEN Wählen Sie den FÜ, den Sie löschen möchten, aus.
EXTERNE ANTENNE	Externe Antenne aktivieren oder deaktivieren.
FUNKÜBERWACHUNG	Sabotage-Überwachung aktivieren oder deaktivieren.
FILTER SCHW SIG	Signal „Filter schwach“ aktivieren oder deaktivieren (Funksignalstärken 0 und 1).
ERK FREMDFUNK	Fremdfunkerkennung aktivieren oder deaktivieren.
ÜBERFALL FERNB	Überfall-Fernbedienung aktivieren oder deaktivieren oder den stillen Modus für die Überfall-Fernbedienung aktivieren.
FÜ TEST ZEITPLAN	Geben Sie eine maximale Dauer (in Tagen) zwischen zwei FÜ-Tests ein. Der maximale Wert ist 365 Tage.
SCHARF ÜBERSCHRE	Geben Sie eine Zeitspanne in Minuten ein, nach der – wenn innerhalb der eingestellten Zeitspanne die Funküberwachungsmeldungen eines Melders oder einer FÜ nicht empfangen werden – die Scharfschaltung einer Meldergruppe verhindert wird. Der maximale Wert ist 720 Minuten.
GERÄTEVERLUST	Geben Sie eine Zeitspanne in Minuten an, nach der die Funkkomponente als fehlend gemeldet wird, wenn sie sich nicht innerhalb dieser Zeitspanne gemeldet hat. (Mindestens 20 Minuten, maximal 720 Minuten.)

16.7.1 SENSOREN HINZUFÜGEN

Hinzufügen einer Sensorkomponente:

1. Blättern Sie zu HINZUFÜGEN und drücken Sie auf AUSWAHL.
   ⇨ Die Aufforderung EINLERNEN ALARM wird angezeigt.
2. Drücken Sie auf AUSWAHL.
   ⇨ In der oberen Zeile des Displays blinkt der Text AKTIVES GERÄT.
3. Aktivieren Sie die Funkkomponente 3 bis 5 Mal hintereinander, damit der Empfänger am Bedienteil das Funksignal des Geräts empfangen kann.
   ⇨ Im Display wird durch die blinkende Meldung FUNKM GEFUNDEN angezeigt, dass die Komponente erkannt wurde. Der Geräte-TYP und die Geräte-ID werden abwechselnd angezeigt.
4. Drücken Sie auf EINLERNEN.

⇨ Eine Aufforderung zur Auswahl des Meldergruppen-Typs wird angezeigt.

1. Drücken Sie auf AUSWAHL.
2. Blättern Sie zum gewünschten Meldergruppen-Typ und drücken Sie auf AUSWAHL.

Wenn Sie eine Komponente über EINLERNEN SABO hinzufügen möchten, blättern Sie in Schritt 2 zu dieser Option. Der Einlernprozess ist exakt gleich – bis auf die Aufforderung, vor dem Meldergruppentyp noch einen Bereichstyp auszuwählen.

16.7.2 SENSOREN BEARBEITEN (MG-ZUWEISUNG)

Es kann erforderlich sein, die MG-Zuweisung eines im System eingelernten Melders zu ändern.

Ändern der MG-Zuweisung eines Funkmelders:

1. Blättern Sie zu BEARBEITEN und drücken Sie auf AUSWAHL.
2. Blättern Sie zum Melder, der geändert werden soll, und drücken Sie auf AUSWAHL.
3. Blättern Sie zu MG.
4. Blättern Sie zur entsprechenden MG-Nummer (nur freie MG-Nummern werden angezeigt).
5. Drücken Sie auf AUSWAHL.

16.7.3 FÜ HINZUFÜGEN

!	*HINWEIS*
	Sie können einen Funküberfalltaster (FÜ) nur konfigurieren oder seinen Status auf dem Bedienteil überprüfen, wenn ein Funkmodul an die Zentrale oder an eines ihrer Erweiterungsmodule angeschlossen wurde, und wenn die Zentrale für die angeschlossenen Modultypen zugelassen ist.

Ein FÜ wird keinem Benutzer zugewiesen. Ein FÜ wird in der Regel von mehren 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.

Konfigurieren eines FÜ mit dem Bedienteil:

1. Wählen Sie FUNK und dann FÜ.
2. Wählen Sie HINZUFÜGEN, um einen FÜ hinzuzufügen.
3. Wählen Sie MANUELL und geben Sie manuell eine FÜ ID ein.
   Die ID kann auch automatisch durch die Zentrale eingegeben werden; wählen Sie hierzu die Option LERNE FÜ. Damit die Zentrale den FÜ erkennen kann, muss eine der Tasten des FÜ gedrückt sein, während die Meldung AKTIVIERE FÜ angezeigt wird. Die Zentrale akzeptiert keine FÜ, wenn ihre ID ein Duplikat einer aktuell konfigurierten FÜ ist.
4. Verlassen Sie das Menü HINZUFÜGEN und wählen Sie das Menü BEARBEITEN zum Konfigurieren des FÜ.

16.7.4 FÜ BEARBEITEN

Konfigurieren eines FÜ mit dem Bedienteil:

1. Wählen Sie FUNK und dann FÜ.
2. Wählen Sie BEARBEITEN, um einen FÜ zu konfigurieren.

BESCHREIBUNG	Geben Sie einen eindeutigen Namen für den FÜ ein.
FUNK ID	Geben Sie die FÜ ID ein. Die Zentrale akzeptiert keine FÜ, wenn ihre ID ein Duplikat einer aktuell konfigurierten FÜ ist.
TASTEN ZUWEISEN	Hier können Benutzer bestimmten Tastenkombinationen Funktionen zuweisen. Verfügbare Funktionen sind: Überfall, Notruf (Still), Bedrohung, Verdacht, WPA Medizin, Medizin. Für die gleiche Funktion können mehrere Tastenkombinationen ausgewählt werden. Beispiel: ● Gelb – Verdacht● ● Rot + Grün – Überfall ● Für kommerzielle oder private Installationen ist die Standardeinstellung: Rot + Grün – Panik **Hinweis**: Wird einer Tastenkombination keine Funktion zugewiesen, ist es immer noch möglich, diese Kombination für einen Trigger zu verwenden. Siehe Trigger [→ 277]
FUNKÜBERWACHUNG	Der Funküberfalltaster kann so konfiguriert werden, dass er ein regelmäßiges Überwachungssignal überträgt. Wird Funküberwachung auf dem FÜ aktiviert (mit dem Jumper), sendet der FÜ etwa alle 7,5 Sekunden ein Überwachungssignal. Die Zeit zwischen den Sendungen wird randomisiert, um die Möglichkeit der Überschneidung mit den Sendungen anderer FÜs zu verringern. Die Überwachungsfunktion muss für den jeweiligen FÜ auch an der Zentrale aktiviert werden, damit die Überwachungsfunktion ordnungsgemäß funktionieren kann. Falls die Zentrale kein Überwachungssignal empfängt, wird ein Alarm ausgelöst, der auf dem Bedienteil angezeigt und protokolliert wird. 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. Wählen Sie AKTVIEREN, wenn Überwachung für den betreffenden FÜ aktiviert wurde.

TEST	Aktiviert den Test eines FÜ-Signals.

Siehe auch

Trigger [➙ 277]
FÜ Timer konfigurieren [➙ 137]
Testen einer FÜ vom Bedienteil aus [➙ 157]

16.8 MELDERGRUPPEN

1. Blättern Sie zu MELDERGRUPPEN und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten MELDERGRUPPE (MG 1-x).
3. Blättern Sie zur gewünschten Programmieroption:

BESCHREIBUNG	Dient der Identifizierung der Meldergruppe. Geben Sie einen eindeutigen und beschreibenden Namen ein.
MG TYP	Legt den Meldergruppentyp fest. Siehe Seite [➙ 375].
ATTRIBUTE	Legt die Attribute der Meldergruppe fest. Siehe Seite [➙ 378].
BIS BEREICH	Legt fest, welche MG welchem Bereich zugeordnet wird. Diese Menüoption wird nur angezeigt, wenn mehrere Bereiche im System definiert wurden. Durch die Auswahl dieser Funktion können Benutzer ein MG-Sets einrichten, die einem bestimmten Bereich innerhalb des Gebäudes zugeordnet werden.

Anzahl und Typ der in den Bedienteil-Menüs für einen bestimmten Bereich angezeigten Attribute unterscheiden sich je nach gewähltem Meldergruppentyp. Siehe Seite.

16.9 TÜREN

16.9.1 TÜREN

1. Blättern Sie zu TÜREN und drücken Sie auf AUSWAHL.
2. Blättern Sie zur Tür, die programmiert werden soll, und drücken Sie auf AUSWAHL.
3. Parameter und sonstige Details, falls zutreffend, werden wie folgt zum Bearbeiten angezeigt:
   - Beschreibung
   - Tür-Eingänge
   - Türgruppe
   - Tür-Attribute
   - Tür-Timer
   - Leserinformationen (Nur Anzeige – Format des letzten mit dem konfigurierten Leser genutzten Ausweises)

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 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)	Zeigt das Format des letzten mit jedem konfigurierten Leser genutzten Ausweises an (nicht in SPC Pro verfügbar).

Name	Beschreibung
(Bedienteile)	

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.

Türgruppen

Die verschiedenen Türen können Türgruppen zugewiesen werden. Dies ist erforderlich, wenn eine der folgenden Funktionen aktiviert ist:

- Aufsicht
- Soft Anti-Passback
- Hard Anti-Passback
- Schleusenfunktion

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	Zentrale/Bereich wird extern scharfgeschaltet, wenn eine Karte am Eintrittsleser 2x vorgehalten wird.

Attribut	Beschreibung
Pro)	
"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 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.

Attribut	Beschreibung
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.
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.

16.10 AUSGÄNGE

Jeder Meldergruppentyp im SPC-System hat einen zugewiesenen Ausgangstyp (interner Merker oder Indikator). Wird ein Meldergruppentyp aktiviert, d. h. eine Tür oder ein Fenster wird geöffnet, Rauch wird gemeldet, ein Alarm wird gemeldet usw., wird der entsprechende Ausgang aktiviert.

1. Blättern Sie zu AUSGÄNGE und drücken Sie auf AUSWAHL.
2. Blättern Sie zu CONTROLLER oder ERWEITERUNG und drücken Sie auf AUSWAHL.
3. Blättern Sie zur Erweiterung bzw. zum Ausgang, die bzw. der programmiert werden soll, und drücken Sie auf AUSWAHL.

   ⇨ Werden die Ausgangsaktivierungen (d. h. aktiviert, aufgezeichnete Elemente / deaktiviert, Elemente) im System-Logbuch protokolliert, stehen

die in der nachfolgenden Tabelle beschriebenen Programmieroptionen zur Verfügung.

NAMEN	Dient der Identifizierung des Ausgangs. Geben Sie einen eindeutigen und beschreibenden Namen ein.
"AUSGANGS TYP"	Legt den Ausgangstyp fest; siehe hierzu die Tabelle auf page [→ 145] (Beschreibung der Ausgangstypen).
AUSGANGS MODUS	Legt die Ausgangsart fest: durchgängig, kurzzeitig, pulsierend.
POLARITÄT	Legt fest, ob der Ausgang bei positiver oder negativer Polarität aktiviert wird.
LOG	Legt fest, ob das System-Logbuch aktiviert oder deaktiviert wird.

Eine Beschreibung des Ausgangstests finden Sie auf Seite [→ 156].

16.10.1 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 [→ 375]) 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	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-). **Hinweis**: Ein Außensirenen-Ausgang wird automatisch aktiviert, sobald eine als Alarm-MG programmierte MG im Modus Extern Scharf oder Intern Scharf auslöst.
Blitzleuchte	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).

	Hinweis: 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-). **Hinweis**: 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 [→ 216]). 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-Meldegruppe 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: ● zwei Aktivierungen von Bedrohungs-MGs, die mehr als zwei Minuten auseinander liegen ● eine Aktivierung einer Bedrohungs-MG und eine Aktivierung einer Panik-MG, die mehr als zwei Minuten auseinander liegen ● Wenn in dem zweiminütigen Zeitraum eine Bedrohungs- und Sabotage-MG oder eine Panik-MG und Sabotage-MG aktiviert werden
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 [→ 216]

16.11 KOMMUNIKATION

1. Blättern Sie zu KOMMUNIKATION und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten Programmieroption.

16.11.1 SER SCHNITTST

Über die seriellen Anschlüsse können ältere PCs oder sonstige Peripheriegeräte wie etwa Drucker mit dem System verbunden werden.

1. Blättern Sie zu SER SCHNITTST.
2. Drücken Sie auf AUSWAHL.
3. Blättern Sie zum seriellen Anschluss, der programmiert werden soll.
4. Wählen Sie die gewünschte Programmieroption (siehe nachfolgende Tabelle):
5. Drücken Sie ZURÜCK, um das Menü zu verlassen.

TYP	Legt fest, ob es sich um ein TERMINAL (Systeminformation) oder einen DRUCKER (SPC-Logbuch) handelt.
"BAUDRATE"	Bestimmt die Übertragungsgeschwindigkeit für die Kommunikation zwischen der Zentrale und dem jeweiligen Peripheriegerät. Bitte beachten Sie, dass an beiden Geräten die gleiche Baudrate eingestellt werden muss.
DATEN BITS	Bestimmt die Größe der Datenpakete, die zwischen der Zentrale und dem jeweiligen Peripheriegerät übertragen werden. Bitte beachten Sie, dass an beiden Geräten der gleiche Datenbits-Wert eingestellt werden muss.
STOP BITS	Legt die Anzahl der Stopbits am Ende des Datenpakets fest. Bitte beachten Sie, dass an beiden Geräten der gleiche Stopbits-Wert eingestellt werden muss.
PARITÄT	Legt die Parität (ungerade/gerade) der Datenpakete fest. Bitte beachten Sie, dass an beiden Geräten die gleiche Parität eingestellt werden muss.
FLUSSSTRG	Legt fest, ob die Daten von der Hardware (RTS, CTS) oder der Software (Keine) gesteuert werden. Bitte beachten Sie, dass an beiden Geräten die gleiche Flusssteuerung eingestellt werden muss.

16.11.2 NETZWERK

Programmieren der Netzwerkverbindung:

1. Blättern Sie zu NETZWERK.
2. Drücken Sie auf AUSWAHL.
   ⇨ Die Option IP ADRESSE wird angezeigt: XXX.XXX.XXX.XXX (bei Einzelziffern sind führende Nullen erforderlich, z. B. 001.001...). z. B., 001
3. Drücken Sie auf AUSWAHL und geben Sie die gewünschte IP-Adresse ein.
   ⇨ Wird die Taste BESTÄTIGEN gedrückt, gibt das System zwei Signaltöne aus und zeigt anschließend die Meldung AKTUALISIERT an, wenn die IP-Adresse gültig ist. Wird die IP-Adresse manuell zugewiesen, muss es sich um eine innerhalb des mit der Zentrale verbundenen LAN oder VLAN eindeutige Adresse handeln. Bei Verwenden der DHCP-Option wird kein Wert eingegeben.
4. Blättern Sie zum Menüpunkt IP NETZMASKE.
5. Drücken Sie auf AUSWAHL und geben Sie die IP NETZMASKE im Format XXX.XXX.XXX.XXX ein. (bei Einzelziffern sind führende Nullen erforderlich.

Wird die Taste BESTÄTIGEN gedrückt, gibt das System zwei Signaltöne aus und zeigt anschließend die Meldung AKTUALISIERT an, wenn die IP-Adresse gültig ist.

6. Blättern Sie zu GATEWAY. Beachten Sie, dass für einen Zugang außerhalb des Netzwerks (Verwendung mit dem Portal) der Gateway programmiert werden muss.
7. Drücken Sie auf AUSWAHL und geben Sie das GATEWAY im Format XXX.XXX.XXX.XXX ein. (bei Einzelziffern sind führende Nullen erforderlich. Wird die Taste BESTÄTIGEN gedrückt, gibt das System zwei Signaltöne aus und zeigt anschließend die Meldung AKTUALISIERT an, wenn der GATEWAY gültig ist.
8. Blättern Sie DHCP. DHCP ist aktiviert, wenn das LAN über einen DHCP-Server zum Zuweisen der IP-Adresse verfügt. Die IP-Adresse muss manuell aktiviert werden. Beachten Sie, dass der Gateway programmiert werden muss, wenn die Zentrale einen Zugang außerhalb des Netzwerks (für Portal-Dienste) benötigt.
9. Drücken Sie auf AUSWAHL und geben Sie das GATEWAY im Format XXX.XXX.XXX.XXX ein. (bei Einzelziffern sind führende Nullen erforderlich. z. B., 001)
   ⇨ Wird die Taste BESTÄTIGEN gedrückt, gibt das System zwei Signaltöne aus und zeigt anschließend die Meldung AKTUALISIERT an, wenn der GATEWAY gültig ist.
   ⇨ Die DHCP-Option wird angezeigt.
10. Wählen Sie DHCP AKTIV oder DHCP INAKTIV als bevorzugte Option.
11. Drücken Sie auf AUSWAHL.

16.11.3 MODEMS

Das SPC-System unterstützt SPC-Intell-Modems zur Kommunikation mit analogen Anschlüssen und mobile Netzwerkschnittstellen für erweiterte Kommunikation und Konnektivität. Das SPC-System muss entsprechend konfiguriert werden.

16.11.3.1 Überwachung der Netzwerkverbindung

Das SPC Alarmsystem sendet ein Polling zu der SPC COM XT, welche mit einer Pollingbestätigung (ACK) antwortet.
Beim Empfang einer Pollingbestätigung (ACK) durch die SPC COM XT, wird das SPC System den Übertragungsstatus auf „OK“ ändern und paralell die Pollingintervallzeit (gemäß dem Alarmübertragungspfad, kurz „ATP“) zurückstellen.

Wenn das SPC Alarmsystem innerhalb des vorgesehenen Zeitintervalls (gemäß dem Alarmübertragungspfad, kurz „ATP“) keine Pollingbestätigung (ACK) erhält, wird der Übertragungsstatus auf“ Fehler“ gesetzt.

SPC unterstützt die folgendenen Übertragungswege:

- Ethernetverbindung
- GSM Modem mit aktiver GPRS Verbindung
- PSTN (analoger Telefonanschluss)

!	*HINWEIS*
	Achten Sie darauf, dass alle Stromquellen (Netz und Batterie) getrennt sind, bevor Sie eine neue PIN- oder SIM-Karte einlegen, da die Karte sonst nicht aktiviert wird.

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

16.11.3.2 Konfigurieren eines GSM- oder PSTN-Modems:

1. Blättern Sie zu MODEMS und drücken Sie AUSWAHL.
2. Wählen Sie den gewünschten Modem-Steckplatz (PRIMÄR oder BACKUP) und drücken Sie auf AUSWAHL.
   ⇨ Die Option MODEM AKT wird angezeigt.
3. AKTIVIEREN oder DEAKTIVIEREN Sie das Modem je nach Bedarf.
4. Blättern Sie zu MODEMSTATUS, TYP, FIRMWARE VERSION und SIGNALSTÄRKE, und drücken Sie auf AUSWAHL, um Informationen zum Modem anzuzeigen.
5. Konfigurieren Sie über das entsprechende Menü die folgenden Modemeinstellungen. Drücken Sie nach jeder Auswahl ENTER.

Menüoption	Beschreibung
LÄNDERVORWAHL	Wählen Sie aus der Liste ein Land aus.
GSM PIN	(nur GSM-Modem) Geben Sie für die SIM-Karte eine GSM-PIN ein.
ANRUFANNAHME	Wählen Sie den Verarbeitungsmodus des Modems für eingehende Anrufe aus: NIE ANTWORTEN oder IMMER ANTWORTEN
TECH. ANTWORT ACC	Wählen Sie AKTIVIEREN, um nur bei freigegebenem Technikerzugang zu antworten.
SMS KONFIG	Wählen Sie SMS AKTIVIEREN, um SMS für dieses Modem zu aktivieren. (Nur für PSTN.) Falls erforderlich, wählen Sie SMS-Server, und geben Sie die passende Telefonnummer des SMS-Service-Providers ein, der an Ihrem Standort erreichbar ist. Auf dem Display wird automatisch die Standard-Landesvorwahl für SMS angezeigt, die im ausgewählten Land gilt. Um SMS manuell zu testen, wählen Sie SMS TEST, und geben Sie die SMS-NUMMER ein. Um SMS automatisch in bestimmten Zeiträumen zu testen, wählen Sie

Menüoption	Beschreibung
	ROUTINEINTERVALL, wählen Sie anschließend ein TEST INTERVALL und geben Sie die SMS-NUMMER ein.
AMTSHOLUNG	(Nur PSTN-Modem) Geben Sie eine Vorwahl ein, die vor der SMS-Nummer angegeben werden soll (falls erforderlich).
TL ÜBERWACHUNG	**Für PSTN**: Aktivieren Sie diese Option, um die Spannung der an das Modem angeschlossenen Telefonleitung zu überwachen. **GSM-Modem**: Aktivieren Sie diese Funktion, um den Signalpegel des mit dem Modem verbundenen GSM-Masten zu überwachen. Wählen Sie einen Überwachungsmodus (IMMER AKTIV, EXT. SCHARF, DEAKTIVIERT). Mit der Option KEIN SCHAR wird diese Funktion nur aktiviert, wenn das System extern scharf ist. Geben Sie die Zeit in Sekunden für das ÜBERWACHUNGSINTERVALL ein (0–9999 Sek.) **Hinweis**: EN 50131-9-Bestätigungskonfiguration Für die ordnungsgemäße Funktion der EN50131-9-Bestätigung muss der Leitungstest aktiviert sein. (siehe Systemoptionen)

Nur GSM-Modem. Wenn SMS aktiviert ist und drei Mal hintereinander die falsche PIN für die SIM-Karte eingegeben wird, wird die SIM-Karte gesperrt. Falls dies der Fall sein sollte, wird empfohlen, die SIM-Karte zu entnehmen und mit einem Mobiltelefon zu entsperren. Wird die SIM-Karte am GSM-Modul gewechselt oder wird eine SIM-Karte in Verbindung mit einer PIN verwendet, wird empfohlen, die PIN einzuprogrammieren, bevor die Karte in den SIM-Kartenhalter gesteckt wird, um sicherzustellen, dass keine falschen PINs an die Karte gesendet werden. Bevor die SIM-Karte in den SIM-Kartenhalter gesteckt wird, sind sämtliche Stromquellen abzuschalten bzw. zu trennen (Stromnetz und Batterie).

16.11.4 EMPFÄNGER

16.11.4.1 HINZUFÜGEN

Programmieren der Empfänger-Einstellungen:

1. Blättern Sie zu EMPFÄNGER > HINZUFÜGEN.
2. Drücken Sie auf AUSWAHL.
3. Wählen Sie die gewünschte Programmieroption (siehe nachfolgende Tabelle):
4. Nach Abschluss des Programmierens, wird die Option, einen Übertragungstest durchzuführen, am Bedienteil angezeigt.

IDENTNUMMER	Diese Information sollte vom Empfänger zur Verfügung gestellt werden; sie dient der Identifizierung von Benutzern bei jedem Anruf / jeder Datenübertragung an den Empfänger.
EMPFÄNGER NAME	Beschreibung des Empfängers
PROTOKOLL	Das zu verwendende Kommunikationsprotokoll (SIA, Contact ID, Fast Format)
1 TEL NUMMER	Die erste Rufnummer, die zur Datenübertragung an den Empfänger gewählt

	werden soll.
2 TEL NUMMER	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.
PRIORITÄT	Das Modem (Primär oder Backup), das für die Kommunikation mit dem Empfänger verwendet werden soll.

16.11.4.2 BEARBEITEN

Zum Bearbeiten der Einstellungen für Empfänger:

1. Blättern Sie zu EMPFÄNGER > BEARBEITEN.
2. Drücken Sie auf AUSWAHL.
3. Wählen Sie die gewünschte Programmieroption (siehe nachfolgende Tabelle):
4. Nach Abschluss des Programmierens, wird die Option, einen Übertragungstest durchzuführen, am Bedienteil angezeigt.

IDENTNUMMER	Diese Information sollte vom Empfänger zur Verfügung gestellt werden; sie dient der Identifizierung von Benutzern bei jedem Anruf / jeder Datenübertragung an den Empfänger.
EMPFÄNGER NAME	Beschreibung des Empfängers
PROTOKOLL	Das zu verwendende Kommunikationsprotokoll (SIA, Contact ID, Fast Format)
1 TEL NUMMER	Die erste Rufnummer, die zur Datenübertragung an den Empfänger gewählt werden soll.
2 TEL NUMMER	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.
LÄNGE WÄHLPAUSE	Geben Sie die Dauer der Wählpause (in Sek.) nach einem fehlgeschlagenen Wählversuch ein. (0–999)
BER ZUWEISEN	Weisen Sie die Bereiche zu, für die dem Empfänger Ereignisse gemeldet werden sollen.
ÜBERTRAGENE MELD	Definieren Sie die Ereignisarten, die dem Empfänger gemeldet werden sollen.
PRIORITÄT	Das Modem (Primär oder Backup), das für die Kommunikation mit dem Empfänger verwendet werden soll.
AUTOMATIC TEST	Definiert einen Zeitplan für die Überprüfung der Verbindung zum Empfänger. Es können Zeitintervalle zwischen den Werten "stündlich" und "alle 30 Tage" konfiguriert werden.

16.11.4.3 LÖSCHEN

Mit dieser Option können Sie einen Empfänger löschen, der im System konfiguriert ist.

16.11.4.4 ÜBERTRAGUNGSTEST

Mit dieser Option können Sie die Verbindung zum Empfänger überprüfen.
Führen Sie folgende Schritte für einen Übertragungstest aus:

1. Wählen Sie ÜBERTRAGUNGSTEST.
2. Wählen Sie den Empfängernamen aus.
3. Klicken Sie auf AUSWAHL.
4. Wählen Sie das Modem aus, mit dem der Übertragungstest durchgeführt werden soll.

⇨ Der Test wird ausgeführt.

16.11.5 FERNWARTUNG

1. Blättern Sie zu FERNWARTUNG > FERNWART AKT
2. Drücken Sie auf AUSWAHL.
3. Schalten Sie zwischen AKTIV und INAKTIV um.
4. Wählen Sie die gewünschte Programmieroption (siehe nachfolgende Tabelle):

ID	Fernwartungs-ID. Muss mit der ID von SPC Pro übereinstimmen (1 - 999999).
PASSWORT	Kennwort für Fernwartung. Muss mit dem Kennwort in SPC Pro übereinstimmen.
KONFIG EING VERB	Einstellungen der eingehenden Verbindungen. Sie können IP EING AKTIV aktivieren, um eingehende IP-Verbindungen vom Fernwartungsserver zu akzeptieren. Wenn nicht aktiviert, werden nur Modemverbindungen akzeptiert. Geben Sie den EING TCP/IP PORT ein, auf dem die Zentrale auf eingehende IP -Verbindungen des Fernwartungsservers wartet.
KONFIG AUSG VERB	Einstellungen der ausgehenden Verbindungen. Wählen Sie, auf welchem Wege ausgehende Verbindungen zum Fernwartungsserver aufgebaut werden (INAKTIV, VIA MODEM oder VIA IP).

16.12 TEST

1. Blättern Sie zu TEST und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten Programmieroption.

16.12.1 SIGNALGEBERTEST

Durchführen eines Signalgebertests:

1. Blättern Sie zu TEST > SIGNALGEBERTEST.
2. Drücken Sie auf AUSWAHL.

⇨ Wurde SIGNALGEBERTEST ausgewählt, stehen folgende Optionen zur Auswahl: AUSSENSIRENEN, BLITZLEUCHTE, INNENSIRENEN und SUMMER. Bei der Auswahl der einzelnen Optionen gibt jedes der gewählten Geräte zur Überprüfung der ordnungsgemäßen Funktionsweise ein Signal aus.

16.12.2 GEHTEST

Ein Gehtest stellt sicher, dass die Melder im SPC-System ordnungsgemäß funktionieren.

Durchführen eines Gehtests:

1. Blättern Sie zu TEST > GEHTEST.
2. Drücken Sie auf AUSWAHL.
3. Im Display wird die Anzahl der zu testenden MGs im System angezeigt: TO TEST XX (wobei XX die Anzahl der gültigen Gehtest-MGs ist). Lokalisieren Sie den Melder in der ersten MG und aktivieren Sie ihn (Tür oder Fenster öffnen).
   ⇨ Der Bedienteil-Summer ertönt kontinuierlich für etwa zwei Sekunden, um anzuzeigen, dass die Aktivierung der MG erkannt wurde. Die Anzahl der noch zu testenden MGs (Anzeige am Bedienteil) verringert sich.
4. Fahren Sie mit den verbleibenden Meldergruppen im System fort, bis alle MGs getestet wurden. Wird die Aktivierung einer MG vom System nicht erkannt, prüfen Sie die Verdrahtung des Melders und/oder tauschen Sie den Melder ggf. aus.

	HINWEIS
	Alle Meldergruppen können in einen Gehtest aufgenommen werden.

16.12.3 EINGANGSTEST

Die Option „Eingangstest“ zeigt Informationen zum Status aller Meldergruppen innerhalb des Systems an.

Anzeigen der MG-Statusinformationen:

1. Blättern Sie zu TEST > EINGANGSTEST.
2. Klicken Sie auf AUSWAHL.
3. Blättern Sie zur gewünschten MG und drücken Sie AUSWAHL.
   ⇨ Der Status der MG und der zugehörige Widerstandswert werden angezeigt.
4. Drücken Sie WEITER, um die MG zu lokalisieren (z.B. CONTROLLER 1 = erste MG am Controller).

⇨ Weitere Statusinformationen können Sie der nachfolgenden Tabelle entnehmen (gilt für Zweifach-Endwiderstände).

MG-Status	Abkürzung
UNBEKANNT	UK
GESCHLOSSEN	ZU
OFFEN	OF
KUZRZSCHLUSS	KS
UNTERBRECHUNG	DI
PULSE	PU
GROSS	GR
ABGEDECKT	AM
STÖRUNG	FA
FREMDSPANNUNG	DC

AUSSERHALB D. GR	OB
MELDERGRUPPEN INSTABIL SCHÄRFEN	MG INSTABIL ENTSCHÄRFEN

Alle MGs im System können über einen Überwachungstest auf ihre ordnungsgemäße Funktion hin überwacht werden.

Durchführen eines Überwachungstests:

1. Blättern Sie zu EINGANGSTEST.
2. Klicken Sie auf AUSWAHL.
3. Blättern Sie zur gewünschten MG und drücken Sie AUSWAHL oder geben Sie die MG-Nummer direkt ein.
   ⇨ Befindet sich die Meldergruppe nahe beim Bedienteil, können Sie die Veränderung der Bedienteil-Anzeige verfolgen. Der MG-Status und der Widerstandswert werden oben rechts angezeigt.
4. Verändern Sie den Status des Melders; öffnen Sie, z. B., bei einem Türkontakt die Tür.

⇨ Der Bedienteil-Summer ertönt, und der Status des Melders wechselt von ZU (Geschlossen) nach OF (Offen). Der angezeigte Widerstandswert ändert sich auf einen Wert, der vom jeweiligen Endwiderstandsschema abhängt.

Es wird empfohlen, die Funktionsweise aller MGs im System zu prüfen, nachdem das System vollständig errichtet wurde. Wählen Sie WEITER (unten rechts) am Bedienteil, um die jeweils nächste Meldergruppe zu lokalisieren. Die MG-Statuswerte KS oder DI zeigen an, dass die Meldergruppe kurzgeschlossen oder unterbrochen ist.

16.12.4 AUSGANGSTEST

Durchführen eines Ausgangstests:

1. Blättern Sie zum Menüpunkt AUSGANGSTEST.
2. Drücken Sie auf AUSWAHL.
3. Wählen Sie CONTROLLER oder ERWEITERUNG.
4. Blättern Sie zum Testen der Controller-Ausgänge zum gewünschten Ausgang und drücken Sie auf AUSWAHL. Wählen Sie zum Testen der Erweiterungsausgänge die jeweilige Erweiterung und anschließend den Ausgang.
   ⇨ Das Bedienteil-Display zeigt den aktuellen Status des Ausgangs in der oberen Zeile an.
5. Schalten Sie den Ausgangsstatus zwischen EIN/AUS um.
6. Prüfen Sie, ob das an den gewählten Ausgang angeschlossene Gerät seinen Status entsprechend ändert.

16.12.5 DAUERTEST

Ein Dauertest biete die Möglichkeit, ausgewählte Meldergruppen einem Langzeittest zu unterziehen. Meldergruppen, die sich im Dauertest befinden, geben keine Alarme aus; stattdessen werden alle Ereignisse im Logbuch aufgezeichnet. Die ausgewählten Meldergruppen bleiben so lange im Dauertest, bis der Dauertest-Timer gemäß Standardeinstellung abgelaufen ist (14 Tage).

Durchführen eines Dauertests:

1. Blättern Sie zu DAUERTEST und drücken Sie auf AUSWAHL.
2. Wählen Sie die gewünschte Option: DAUERT AKTIV oder DAUTERT ABBR.
3. Blättern Sie zur gewünschten MG und drücken Sie AUSWAHL.

⇨ Eine Meldung, welche die Aktivierung des Dauertests für die ausgewählte Meldergruppe bestätigt, wird angezeigt.

	HINWEIS
	Alle Meldergruppen können in einen Dauertest aufgenommen werden.

16.12.6 KONFIG FÜR TEST

Die Testkonfiguration betrifft die Aktivierung/Deaktivierung von Tonsignalen, die zur Bestätigung der Funktionen bei einem Gehtest dienen.

So ändern Sie die Testkonfiguration:

1. Blättern Sie zum Menüpunkt KONFIG FÜR TEST.
2. Drücken Sie auf AUSWAHL.
3. Blättern Sie zu einer der folgenden Optionen: ALLE, INNENSIRENE, AUSSENSIRENE, BEDIENTEIL
4. Drücken Sie SPEICHERN.
5. Drücken Sie ZURÜCK, um das Menü zu verlassen.

16.12.7 OPTISCHE INDIKATOREN

Mit diesem Test werden alle Bildpunkte (Pixel) auf dem LCD-Bedienteil und alle Bildpunkte und LED-Anzeigen auf dem Komfort-Bedienteil, Anzeigemodul und dem Schlüsselschalter überprüft.

Zur Überprüfung eines Bedienteils:

1. Blättern Sie zu OPTISCHE IND.
2. Drücken Sie auf AUSWAHL.
3. Drücken Sie AKTIVIEREN.

Auf dem LCD-Bedienteil werden zwei Zeilen mit ständig wechselnden Zeichen angezeigt.

Auf dem Komfort-Bedienteil leuchten alle LED-Anzeigen auf, und auf dem Bildschirm werden alle Bildpunkte angezeigt.

1. Drücken Sie ZURÜCK, um den Test zu beenden.
2. Drücken Sie ZURÜCK, um das Menü zu verlassen.

16.12.8 FÜ-TEST

	HINWEIS
	Dieser Test kann nur von einem Techniker oder Benutzer durchgeführt werden, dem ein „FÜ Test“-Recht zugewiesen wurde. Siehe Benutzerrechte.

Testen des FÜ über das Bedienteil:

1. Blättern Sie zu FÜ TEST und drücken Sie auf AUSWAHL.
2. Wenn die Aufforderung AKTIVIERE FÜ angezeigt wird, die drei Tasten des FÜ gleichzeitig drücken.

⇨ Ist der Test erfolgreich, wird die Meldung FÜ *n* OK angezeigt, wobei n die Nummer des getesteten FÜ ist.

1. Den Test falls erforderlich wiederholen.
2. ZURÜCK oder X drücken, um den Test zu beenden.

16.12.9 KÖRPERSCHALLMELDER-TEST

Durchführen eines Körperschallmelder-Tests:

1. Blättern Sie zu TEST > KSM TEST.
2. Drücken Sie auf AUSWAHL.
3. Wählen Sie TEST ALLE BER. oder wählen Sie einen bestimmten Bereich für den Test aus.
4. Falls Sie einen bestimmten Bereich für den Test auswählen, können Sie entweder TEST ALLE MG oder eine bestimmte zu testende Körperschall-MG auswählen.
   ⇨ Während des Tests wird die Meldung „KSM TEST“ auf dem Bedienteil angezeigt.
   ⇨ Wenn der Test fehlschlägt, wird die Meldung „KSM FEHLER“ angezeigt. Durch Drücken der „i“- oder ANZEIGE-Taste wird eine Liste der fehlgeschlagenen MGs angezeigt, die durchgeblättert werden kann.
   ⇨ Ist der Test erfolgreich, wird „TEST OK“ angezeigt.

Siehe auch Testen der Körperschallmelder [→ 351].

16.13 KONFIG OPTIONEN

1. Blättern Sie zu KONFIG OPTIONEN und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten Programmieroption:

SYSTEM SOFTWARE	Anzeigen der aktuellen Softwareversion.
RÜCKSETZEN	Zurücksetzen von Benutzern oder des Systems auf die Werkseinstellungen.
KONFIG SICHERN	Sichern einer Konfiguration.
KONFIG WIEDERHER	Wiederherstellen einer Konfiguration.
FAST PROGRAMMER	• DATEN VON SPC: Übertragen von Daten von der Zentrale zum Fast Programmer. Um zu verhindern, dass Konfigurationsdateien überschrieben werden, erhalten Sie eine Bestätigungsaufforderung, wenn der neue Konfigurationsdateiname der gleiche ist wie der Name einer bereits im Fast Programmer vorhandenen Datei. • DATEN ZU SPC: Übertragen von Daten vom Fast Programmer zur Zentrale. • DATEIEN LÖSCHEN: • FIRMWARE UPGRADE: Hinweis: Wenn Sie die Firmware downgraden (d. h. eine ältere Version der Firmware installieren), behält das System

	standardmäßig alle aktuellen Konfigurationseinstellungen bei. Außerdem muss bei einem Downgrade der Firmware unbedingt auch ein Downgrade der Firmware auf den zugehörigen Peripheriegeräten durchgeführt werden, sonst können Meldergruppen als getrennt/ausgeschaltet, offen oder geschlossen angezeigt werden. ● UPGRADE PERIPHERIE-FIRMWARE: ● SPRACH-UPGRADE:
SPC PRO/SPC SAFE	Programmieren der folgenden SPC-Pro-Optionen: ● ZUGRIFF AKT: Legt fest, ob SPC Pro aktiviert oder deaktiviert wird. ● ZUGANG TECHNIKER: Legt fest, ob der Technikerzugang aktiviert oder deaktiviert wird. ● PASSWORT: Bearbeiten des bestehenden Passworts. ● IP AKTIV: Aktivieren Sie diese Option, um eine Verbindung zum System via IP herzustellen. ● IP PORT: Wählen Sie diese Option, über welchen IP-Port SPC Pro/SDK Verbindungen herstellt.
"SYSTEM NEUSTART"	Für den Neustart des Systems.
LIZENZ	Geben Sie eine Lizenznummer ein, um den SPC-Lizenzschlüssel zu ändern. Das System protokolliert oder meldet keine Lizenzänderung.

16.14 MELDERGRUPPE ABSCHALTEN

Meldergruppen, Systemalarme oder Alarme von X-BUS-Geräten können manuell am Bedienteil abgeschaltet werden. Durch Abschalten einer Meldergruppe wird diese solange deaktiviert, bis sie wieder vom Benutzer eingeschaltet wird.

Abschalten von Meldergruppen, Systemalarmen oder Alarmen von X-BUS-Geräten:

1. Blättern Sie zu MELD ABSCHALTEN und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten Option aus der folgenden Tabelle und drücken Sie auf AUSWAHL.

MG	Wählen Sie die gewünschte Meldergruppen aus und ändern Sie die Einstellung von NICHT ABGESCHALT auf ABGESCHALTET.
SYS	Abschalten eines Systemalarms.
XBUS	Abschalten des Alarms von ERWEITERUNGEN oder BEDIENTEILEN: ● XBUSSTÖR KOMM ● XBUS STÖRUNG SICHERUNG (nur Erweiterungen) ● X-BUS SABO
ZEIGE ABGES MELD	Anzeigen einer Liste der abgeschalteten MGs, Systemalarme oder Alarme von X-BUS-Geräten:

16.15 LOGBUCH

Kürzlich im System aufgetretene Ereignisse werden in der Option LOGBUCH angezeigt. Ereignisse blinken im Sekundentakt.

1. Blättern Sie zu LOGBUCH und drücken Sie auf AUSWAHL.
2. Um ein Ereignis an einem bestimmten Datum anzuzeigen, geben Sie über die Zifferntasten das gewünschte Datum ein.

⇨ Die neuesten Ereignisse werden in der unteren Zeile des Displays angezeigt. Alle früheren Ereignisse werden jeweils eine Sekunde lang angezeigt.

16.16 ZUTRITTS LOGBUCH

Zutritt zu Meldergruppen wird im System in der Option ZUTRITTS LOGBUCH angezeigt.

1. Blättern Sie zu ZUTRITTS LOGBUCH und drücken Sie auf AUSWAHL.
2. Wählen Sie eine Tür im System, für die Zutrittsereignisse angezeigt werden sollen.
   ⇨ Die jüngsten Zutrittsereignisse werden mit Datum und Zeit angezeigt.
3. Blättern Sie durch die Zutrittsereignisse oder geben Sie ein Datum ein und drücken Sie BEST, um nach einem bestimmten Zutrittsereignis zu suchen.

16.17 ALARMPROTOKOLLIERUNG

Das ALARMPROTOKOLL zeigt eine Liste der Alarmereignisse an.

- Wählen Sie **Log > Logbuch > Alarm Log**.

In diesem Logbuch werden folgende Type angezeigt:

- Meldegruppen
  - Alarm
  - Überfall
- Systemereignisse
  - Best Alarm
  - Bedrohungs-PIN
  - XBUS Überfall
  - Bedrohungspin
  - RPA PANIC

16.18 TECHNIKER-PIN ÄNDERN

Ändern der Techniker-PIN:

1. Blättern Sie zu TECHN PIN ÄNDERN, und drücken Sie auf AUSWAHL.
   ⇨ Eine zufällig generierte PIN wird angezeigt.
2. Geben Sie eine neue PIN ein, falls erforderlich. Überschreiben Sie dazu die angezeigte PIN, und drücken Sie ENTER.
   ⇨ 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. Das System akzeptiert keine PIN mit weniger Stellen, als eingestellt sind.
3. Bestätigen Sie die neue PIN, drücken Sie SPEICHERN.
4. Drücken Sie ZURÜCK, um zur vorherigen Anzeige zurückzukehren und die PIN zu ergänzen.

⇨ Sollte das Display während des Prozesses abschalten (Timeout), bleibt die bisherige PIN gültig.

16.19 BENUTZER

Nur Benutzer, für die das betreffende Recht aktiviert ist, können Benutzer hinzufügen, bearbeiten oder löschen:

16.19.1 HINZUFÜGEN

Hinzufügen von Benutzern zum System:

1. Blättern Sie zum Menüpunkt BENUTZER > HINZUFÜGEN.
   ⇨ Wählen Sie eine Benutzer-ID aus den auf dem System verfügbaren IDs aus und drücken Sie auf AUSWAHL.
2. Drücken Sie auf ENTER, um den angezeigten Standardnamen zu verwenden oder geben Sie einen anwenderspezifischen Benutzernamen ein und drücken Sie auf ENTER.
3. Blättern Sie zum gewünschten Benutzerprofiltyp und drücken Sie auf ENTER.
   ⇨ Das System generiert eine Standard-PIN für jeden neuen Benutzer.
4. Drücken Sie auf ENTER, um die Standard-PIN zu übernehmen, oder geben Sie eine neue Benutzer-PIN ein und drücken Sie auf ENTER.

Das Bedienteil bestätigt, dass ein neuer Benutzer angelegt wurde.

16.19.2 BEARBEITEN

Bearbeiten von Benutzern im System:

1. Blättern Sie zu BENUTZER > BEARBEITEN.
2. Drücken Sie auf AUSWAHL.
3. Bearbeiten Sie die gewünschte Benutzereinstellung (siehe nachfolgende Tabelle):

NAME ÄNDERN	Den aktuellen Benutzernamen bearbeiten.
BENUTZERPROFIL	Wählen Sie das passende Profil für diesen Benutzer aus.
BEDROHUNGSPIN	Aktivieren oder deaktivieren Sie eine Bedrohungs-PIN für diesen Benutzer.
LIMIT DATUM	Aktivieren Sie diese Funktion, um sicherzustellen, dass der Benutzer nur während eines bestimmten Zeitraums auf das System zugreifen kann. Geben Sie ein Datum VON und BIS und drücken Sie BEST.
TRANSPONDER	TP-Option aktivieren oder deaktivieren.
FERNBEDIENUNG	Zugang via Fernbedienung aktivieren oder deaktivieren (Funk-Bedienteil, Fernbedienung).
MAN-DOWN (MDT)	Aktiviert den Man-Down-Test.
ZUTRITTSKONTR	Falls dem Benutzer kein Ausweis zugewiesen wurde: ● Ausweis hinzufügen ● KARTE EINLERNEN Falls dem Benutzer ein Ausweis zugewiesen wurde: ● KARTE BEARBEITEN – KARTENNUMMER – KARTENATTRIBUTE (siehe Zutrittskontrolle) ● KARTE ZURÜCKSETZEN ● KARTE LÖSCHEN
SPRACHE	Wählen Sie eine Sprache für diesen Benutzer aus, die auf im System angezeigt

	wird.

16.19.2.1 ZUTRITTSKONTR

Jedem Benutzer der Zentrale kann jeweils eine Zutrittskarte zugewiesen werden.
Konfigurieren der Zutrittskontrolle für einen Benutzer:

1. Blättern Sie zu BENUTZER > BEARBEITEN.
2. Drücken Sie auf AUSWAHL.
3. Wählen Sie den Benutzer, der konfiguriert werden soll, und drücken Sie auf AUSWAHL.
4. Blättern Sie zu ZUTRITTSKONTR und drücken Sie auf AUSWAHL.

Die folgenden Abschnitte beschreiben die Programmierschritte, die innerhalb der Option "Zugangskontrolle" des ausgewählten Benutzers zur Verfügung stehen.

16.19.2.1.1 KARTE HINZUFÜGEN manuell

Wenn das Ausweisformat oder die Ausweisnummer bekannt ist, kann der Ausweis manuell angelegt werden.
Die Anlagennummer des Ausweise ist für das Anwenderprofil konfiguriert, das diesem Benutzer zugeordnet ist.

1. Blättern Sie zum Menüpunkt AUSWEIS HINZUFÜG.
2. Drücken Sie auf AUSWAHL.

⇨ Ein leerer Ausweis wurde hinzugefügt und kann nun bearbeitet werden.

16.19.2.1.2 KARTE EINLERNEN

	HINWEIS
	Nur Karten mit einem unterstützten Kartenformat können eingelernt werden.

Wenn die Kartennummer oder das Kartenformat nicht bekannt ist, können die Karte gelesen und die Karteninformationen eingelernt werden.

1. Blättern Sie zum Menüpunkt KARTE EINLERNEN.
2. Drücken Sie auf AUSWAHL.
3. Wählen Sie die Tür, an der die Karte vorgehalten wird.
4. Drücken Sie auf AUSWAHL.

	HINWEIS
	Die neue Karte kann an jedem Eintritts- oder Austrittsleser der gewählten Tür vorgehalten werden.

5. Halten Sie die Karte an einem Kartenleser der gewählten Tür vor.

⇨ Die Informationen der neuen Karte sind nun eingelernt.

16.19.2.1.3 KARTE BEARBEITEN

Wurde eine Karte bereits einem Benutzer zugewiesen, kann sie am Bedienteil bearbeitet werden:

1. Blättern Sie zu KARTE BEARBEITEN.
2. Drücken Sie auf AUSWAHL.
3. Bearbeiten Sie die gewünschte Benutzereinstellung (siehe nachfolgende Tabelle):
4. Drücken Sie ZURÜCK, um das Menü zu verlassen.

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: ● SPC4xxx - Alle Benutzer ● SPC5xxx - 512 ● SPC6xxx - 512
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.

16.19.2.1.4 KARTE LÖSCHEN

Wird eine Karte nicht mehr gebraucht, kann sie am Bedienteil gelöscht werden.

1. Blättern Sie zum Menüpunkt KARTE LÖSCHEN.
2. Drücken Sie auf AUSWAHL.

16.19.2.1.5 KARTE ZURÜCKSETZ

Ist die Hard Anti-Passback (HAPB)-Funktion in einem Raum aktiviert, und ein Benutzer verlässt den Raum, ohne den Austrittsleser zu verwenden, darf er diesen Raum nicht mehr betreten. Die Karte des Benutzers kann zurückgesetzt werden, damit er seine Karte einmalig ohne Passback-Prüfung vorhalten kann.

Zurücksetzen der Karte am Bedienteil:

1. Blättern Sie zum Menüpunkt KARTE ZURÜCKSETZ.
2. Drücken Sie auf AUSWAHL.

16.19.3 LÖSCHEN

Löschen von Benutzern im System:

1. Blättern Sie zum Menüpunkt BENUTZER > LÖSCHEN.
2. Drücken Sie auf AUSWAHL.
   ⇨ Eine Eingabeaufforderung wird angezeigt, in der Sie den Löschbefehl bestätigen müssen.
3. Drücken Sie JA, um den Benutzer zu löschen.

16.20 ANWENDERPROFILE

Siehe auch

Hinzufügen/Bearbeiten von Profilen [→ 200]

16.20.1 HINZUFÜGEN

Hinzufügen von Benutzerprofilen zum System:

Die Person, die das Benutzerprofil anlegt, muss ein Benutzerprofil vom Typ „Manager“ besitzen.

1. Blättern Sie zu ANWENDERPROFILE > Hinzufügen .
   ⇨ Die Option NEUER NAME wird angezeigt. Drücken Sie auf AUSWAHL.
2. Geben Sie einen benutzerdefinierten Namen für das Benutzerprofil ein und drücken Sie auf BESTÄTIGEN.
   ⇨ Das Bedienteil bestätigt, dass ein neues Benutzerprofil angelegt wurde.

16.20.2 BEARBEITEN

Bearbeiten von Benutzerprofilen im System:

1. Blättern Sie zu ANWENDERPROFILE > Bearbeiten.
2. Drücken Sie auf AUSWAHL.
3. Bearbeiten Sie die gewünschte Benutzerprofileinstellung (siehe nachfolgende Tabelle):

NAME ÄNDERN	Ändern Sie bei Bedarf den Profilnamen.
"BEREICHE ÄNDERN"	Wählen Sie die Bereiche aus, die für dieses Profil relevant sind.
KALENDER	Wählen Sie einen konfigurierten Kalender oder die Option KEINE aus.
RIGHT	Aktivieren oder Deaktivieren Sie Systemfunktionen für dieses Profil. Siehe Benutzerrechte [→ 200].
TÜR	Wählen Sie den Zugangstyp aus, der in diesem Profil für die konfigurierten Türen zur Verfügung stehen soll. Optionen are KEINE, KEINE BESCHRÄNKUNGEN oder KALENDER.
ANLAGENNUMMER	Geben Sie für alle Karten mit diesem Profil eine Anlagennummer ein.

16.20.3 LÖSCHEN

Löschen von Benutzerprofilen im System:

1. Blättern Sie zu ANWENDERPROFILE > Löschen.
2. Blättern Sie durch die Anwenderprofile bis zum gewünschten Profil.
3. Drücken Sie auf AUSWAHL
   ⇨ Sie werden dazu aufgefordert, den Löschvorgang zu bestätigen.
4. Drücken Sie auf AUSWAHL, um das Anwenderprofil zu löschen.

16.21 SMS

Das SPC-System unterstützt die Übertragung von SMS-Alarmen von der Zentrale an den Techniker und an ausgewählte Mobiltelefone (SMS-Meldungen). Außerdem können Benutzer das SPC-System auch aus der Ferne via SMS steuern (SMS-Steuerung). Diese beiden Funktionen arbeiten Hand in Hand, da sie ermöglichen, dass ein Benutzer auf eine SMS-Meldung reagieren kann, ohne dass er persönlich vor Ort am überwachten Objekt sein muss.

Maximal können 32 (SPC4xxx), 50 (SPC5xxx) oder 100 (SPC6xxx) SMS-IDs für jede Zentrale konfiguriert werden. Für die Aktivierung der SMS-Kommunikation sind ein SMS-fähiges Modem sowie ein geeignetes System und eine Benutzerkonfiguration erforderlich.

Je nach dem ausgewählten Modus für die SMS-AUTHENTIFIZIERUNG (siehe Menü OPTIONEN [→ 116]) kann die SMS-Benutzerauthentifizierung so konfiguriert werden, dass verschiedene Kombinationen aus Benutzer-PIN und Anrufer-PIN oder SMS PIN und Anrufer-PIN verwendet werden.

Die SMS-Meldung kann über ein PSTN-Modem laufen, sofern der PSTN-Anbieter SMS über PSTN unterstützt. Für die SMS-Steuerung ist jedoch ein GSM-Modem in der Zentrale erforderlich. Ein GSM-Modem unterstützt beide Funktionen – SMS-Meldung und SMS-Steuerung.

SMS-Steuerung

Die SMS-Steuerung kann so eingestellt werden, dass ein Remote-Benutzer folgende Funktionen der Zentrale per SMS steuern kann:

- Scharfschalten/Unscharfschalten
- Techniker aktivieren/deaktivieren
- Herstellerzugang aktivieren/deaktivieren
- Logischer Ausgang ein/aus

SMS-Meldungen

Die SMS-Funktion kann so eingestellt werden, dass verschiedene Ereignisse im System per SMS gemeldet werden:

- Alarmmeldungen
- Bestätigter Alarm
- Störungen und Sabotage
- Scharfschalten und Unscharfschalten
- Sperrungen und Abschaltungen
- Alle anderen Meldungen

16.21.1 HINZUFÜGEN

▷ Ein Modem ist installiert und vom System erkannt.

▷ Die Funktion **SMS-Authentifizierung** wird unter OPTIONEN [→ 116] aktiviert.

1. Blättern Sie zu SMS -> Hinzufügen und drücken Sie auf AUSWAHL.
2. Wählen Sie einen Benutzer aus, für den ein SMS-Vorgang hinzugefügt werden soll.
3. Geben Sie für diesen Benutzer eine SMS-Nummer ein und drücken Sie BEST.
4. Geben Sie für diesen Benutzer eine SMS-PIN ein und drücken Sie BEST.

⇨ Das Bedienteil zeigt an, dass die SMS-Einstellungen aktualisiert wurden.

16.21.2 BEARBEITEN

▷ Ein Modem ist installiert und vom System erkannt.

▷ Die Funktion **SMS-Authentifizierung** wird unter OPTIONEN [→ 116] aktiviert.

1. Blättern Sie zu SMS -> Bearbeiten und drücken Sie auf AUSWAHL.
2. Wählen Sie die Techniker- oder Benutzer-SMS-ID aus, die bearbeitet werden soll.

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). **Hinweis:** 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 [→ 205]

!	*HINWEIS*
	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 **C**alling **L**ine **I**dentity (CLI) am gewählten Anschluss aktiviert ist, damit Verbindungen zum SMS-Netz möglich sind. Setzen Sie sich für weitere Einzelheiten mit dem Telefonanlagenadministrator in Verbindung.

16.21.3 LÖSCHEN

1. Blättern Sie zu SMS -> Löschen.
2. Blättern Sie zur gewünschten SMS ID.
3. Drücken Sie auf AUSWAHL.

⇨ The Bedienteil zeigt an, dass die SMS-Information aktualisiert wurde.

16.22 X-10

Ab Version 3.4 befindet sich X-10 im Wartungszustand. Diese Funktion wird im Produkt zur Wahrung der Rückwärtskompatibilität beibehalten.

X10 ist eine Technologie, mit der sich Komponenten wie Leuchten oder andere Geräte vom System steuern lassen. Außerdem können Systemereignisse verwendet werden, um Ausgänge von X10-Geräten anzusteuern. Der SPC-Controller verfügt über eine dedizierte serielle Schnittstelle (serieller Port 1) für den direkten Anschluss standardmäßiger X10-Geräte.

1. Blättern Sie zu X-10, und drücken Sie AUSWAHL.
2. Blättern Sie zur gewünschten Programmieroption:

X-10 AKTIVIEREN	X-10-Funktionen im System aktivieren oder deaktivieren.
GERÄTE	X-10-Geräte hinzufügen, bearbeiten, löschen oder testen.
EINTRAGEN IN LOG	X-10-Protokollfunktion aktivieren oder deaktivieren.

16.23 DATUM/UHRZEIT

Das Datum und die Uhrzeit können manuell im System eingegeben werden. Die Datums- und Uhrzeitangabe wird am Bedienteil und im Browser angezeigt und wird bei zeitbezogenen Programmierfunktionen verwendet.

1. Blättern Sie zu DATUM/UHRZEIT und drücken Sie auf AUSWAHL.
   ⇨ Das Datum wird in der oberen Zeile des Displays angezeigt.
2. Über die Zifferntasten können Sie ein neues Datum eingeben bzw. das angezeigte Datum korrigieren. Mit der linken und rechten Pfeiltaste kann der Cursor nach links und rechts bewegt werden.
3. Drücken Sie BEST, um das neue Datum zu übernehmen.
   ⇨ Wird versucht, einen ungültigen Datumswert zu speichern, wird die Meldung UNGÜLTIGER WERT für 1 Sekunde angezeigt, und der Benutzer wird aufgefordert, ein gültiges Datum einzugeben.
4. Über die Zifferntasten können Sie eine neue Uhrzeit eingeben bzw. die angezeigte Uhrzeit korrigieren. Mit der linken und rechten Pfeiltaste kann der Cursor nach links und rechts bewegt werden.
5. Drücken Sie BEST, um die neue Uhrzeit zu übernehmen.
   ⇨ Wird versucht, einen ungültigen Wert für die Uhrzeit zu speichern, wird die Meldung UNGÜLTIGER WERT für 1 Sekunde angezeigt, und der Benutzer wird aufgefordert, eine gültige Uhrzeit einzugeben.

16.24 SYS IDENTIFIK

Diese Einstellung ermöglicht es dem Techniker, Systeminformationen und Techniker-Kontaktdaten einzugeben.

1. Blättern Sie zu SYS IDENTIFIK und drücken Sie auf AUSWAHL.
2. Blättern Sie zur gewünschten Programmieroption:

SYSTEMNAME	Dient der Identifizierung des Systems. Geben Sie einen eindeutigen und beschreibenden Namen ein.
INST ID	Dient der Identifizierung des Systems, wenn es an einen Empfänger (ARC) angebunden wird (max. 10 Ziffern).
NAME ERRICHTER	Kotaktdaten des Technikers
TEL ERRICHTER	Kotaktdaten des Technikers
DISP. ERRICHTER	Einstellung zur Anzeige der Errichter-Angaben im Bereitschaftszustand.

Die im Rahmen dieser Menüoptionen eingegebenen Kontaktdaten des Errichters sollten bei Abschluss der Installation auch auf dem ausklappbaren Schild am Bedienteil eingetragen werden.

16.25 TÜRSTEUERUNG

Über diese Option können Sie alle Türen im System steuern.

1. Blättern Sie zu TÜRSTEUERUNG und drücken Sie auf AUSWAHL.
2. Wählen Sie die Tür, die gesteuert werden soll, und drücken Sie auf AUSWAHL.

3. Wählen Sie einen Türstatus aus der nachfolgenden Liste und drücken Sie auf AUSWAHL.

NORMAL	Die Tür befindet sich im normalen Betriebsmodus. Zum Öffnen der Tür ist eine Karte mit den entsprechenden Zutrittsrechten erforderlich.
KURZZEITIG	Die Tür wird nur für ein vorbestimmtes Zeitintervall für den Zutritt freigegeben.
GESPERRT	Die Tür ist abgesperrt. Die Tür bleibt geschlossen, selbst wenn eine Karte mit den entsprechenden Zutrittsrechten vorgehalten wird.
FREIGEGEBEN	Die Tür ist freigegeben.

16.26 SPC CONNECT

Fügen Sie ein SPC-Connect-Übertragungssystem hinzu, um eine Verbindung zwischen einer Zentrale und der SPC Connect-Website „https://www.spcconnect.com“ einzurichten. Dadurch kann sich ein Zentralenbenutzer registrieren und über die SPC Connect-Website per Fernzugriff auf seine Zentrale zugreifen. Wenn SPC Connect während der Startassistentsequenz nicht aktiviert ist, können Sie dieses Menü verwenden, um ein SPC Connect ATS hinzuzufügen. Wenn SPC Connect während des Starts aktiviert ist, zeigt dieses Menü die Registrierungs-ID für die Zentrale an.

HINZUFÜGEN	Wenn SPC CONNECT im Startassistenten deaktiviert wurde, wird das Menü „HINZUFÜGEN“ angezeigt. Wählen Sie HINZUFÜGEN, um ein SPC Connect ATS zu erstellen. Dadurch kann sich ein Zentralenbenutzer registrieren und über die SPC Connect-Website „https://www.spcconnect.com“ per Fernzugriff auf seine Zentrale zugreifen.
REGISTRIERUNGS-ID	Wenn SPC CONNECT im Startassistenten aktiviert wurde, wird die Registrierungs-ID der Zentrale angezeigt. Stellen Sie diese Information einem Endbenutzer bereit, damit er seine Zentrale für einen Fernzugriff darauf mit der SPC Connect-Website „https://www.spcconnect.com“ registrieren kann.
FIRMEN-ID	Für zukünftige Verwendung.
LÖSCHEN	Wählen Sie zur Entfernung eines SPC Connect ATS von einer Zentrale die Option LÖSCHEN.

17 Technikerprogrammierung über den Browser

Der Zugriff auf die Techniker-Programmieroptionen der SPC-Zentrale erfolgt über einen beliebigen Standard-Webbrowser auf einem PC; der Zugriff ist kennwortgeschützt.

Rufen Sie den Techniker-Programmiermodus durch Eingabe der Techniker-PIN (1111) auf. Weitere Informationen finden Sie unter Techniker-PINs [→ 107].

Der Webserver bietet Zugang zu sämtlichen Programmieroptionen, die zum Installieren und Konfigurieren des SPC-Systems verwendet werden.

Diese Programmieroption sollte ausschließlich autorisierten Einrichtern des SPC-Systems vorbehalten bleiben.

Die Techniker-Programmierfunktionen von SPC sind in folgende Kategorien unterteilt:

Wartungsfunktionen

Diese Funktionen können programmiert werden, ohne dass das Alarmsystem deaktiviert werden muss; der Zugriff darauf ist unmittelbar nach der Anmeldung im Technikermodus möglich.

Konfigurationsfunktionen

Diese Funktionen erfordern, dass das Alarmsystem deaktiviert wird, bevor programmiert werden kann; der Zugriff erfolgt über das Konfigurationsmenü.

!	*HINWEIS*
	Ist die Option „Konfig.mod.verlassen“ unter „Systemoptionen“ aktiviert, darf der Techniker den Konfigurationsmodus bei aktiven Alarmen verlassen, muss aber alle im Bedienteil oder im Browser aufgelisteten Alarme quittieren, bevor er vom Konfigurationsmodus in den Wartungsmodus wechselt.

Der Zugriff auf den Webserver auf dem SPC-Controller erfolgt entweder via Ethernet oder USB-Schnittstelle.

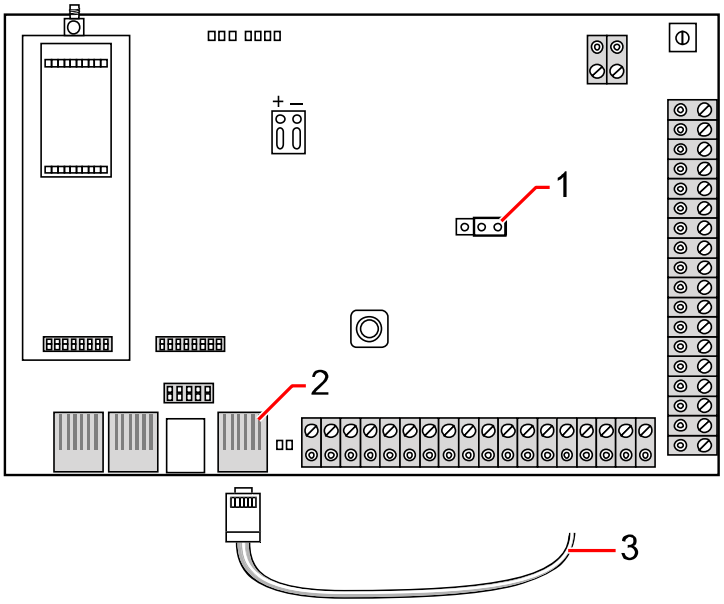
Denken Sie beim Programmieren mit einer Browserschnittstelle daran, Ihre Änderungen durch Klicken auf **Speichern** zu übernehmen.
Klicken Sie auf **Aktualisieren**, um die aktuellen Programmierwerte auf einer Webseite anzuzeigen.

17.1 Systeminformationen

Klicken Sie auf das Symbol **?**, um das Hilfemenü anzuzeigen. Es enthält aktuelle Informationen über die Zentrale und die Funktionen, für die im Augenblick auf dem System eine gültige Lizenz besteht.

17.2 Ethernet-Schnittstelle

IP



Verbinden

1	JP9 ~~SPC4xxx~~
2	Ethernet-Port
3	Zum Ethernet-Port am PC

Wird die SPC Ethernet-Schnittstelle an ein vorhandenes **L**ocal **A**rea **N**etwork (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 [➔ 359].

  ⇨ 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 [➔ 107]).
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.

17.3 Mit der Zentrale über USB verbinden

Wird die Zentrale bei angeschlossenem USB-Kabel zurückgesetzt, muss das Kabel herausgezogen und wieder eingesteckt werden.

Der USB-Anschluss am Controller kann mit einem Standard-USB-Kabel, Typ A oder Typ B, an einen PC angeschlossen werden. Zum Herstellen einer USB-Verbindung vom Controller zum PC müssen Treiber installiert werden:

▷ Auf Ihrem PC muss SPC Pro installiert sein.

▷ Sie benötigen ein USB-Kabel, um den PC und die Zentrale miteinander zu verbinden.

1. Schließen Sie das USB-Kabel am Controller an und verbinden Sie es mit einem USB-Anschluss am PC.
   ⇨ Der Assistent **Neue Hardware gefunden** wird angezeigt.
2. Drücken Sie auf **Weiter**.
   ⇨ Windows XP erkennt einen generischen USB-Hub.
3. Klicken Sie auf Fertig stellen.
   ⇨ Windows XP erkennt das SPC – Advanced Security System am COM-Port N (N ist die Nummer des COM-Ports, der dem Gerät zugewiesen ist).
4. Notieren Sie sich, welcher COM-Port dem Gerät zugeordnet ist; Sie benötigen diese Angabe im weiteren Verlauf.
   ⇨ Der Assistent **Neue Hardware gefunden** wird noch einmal angezeigt.
5. Wählen Sie **Software automatisch installieren**.
6. Falls der Assistent für die Installation der Windows XP-Treiber Sie dazu auffordert, aus einer Liste die beste Entsprechung auszuwählen, wählen Sie die folgende Option:
   ⇨ **Vanderbilt Intrunet SPC lokale USB Verbindung**
7. Klicken Sie auf **Next** (Weiter).
   ⇨ Ein Dialogfeld mit Hinweisen zur Windows-Zertifizierung wird angezeigt. Vanderbilt hält es für zulässig, mit dem Installationsprozess fortzufahren. Setzen Sie sich für weitere Nachfragen bitte mit Ihrem Netzwerkadministrator oder einem Vanderbilt-Techniker in Verbindung.
8. Klicken Sie auf **Installation fortsetzen**.
   ⇨ Der Installationsvorgang endet.
9. Klicken Sie auf Fertig stellen.

⇨ Der Treiber ist installiert.

Konfigurieren der Verbindung unter Windows XP

Einrichten der neuen Verbindung auf dem Computer:

1. Klicken Sie auf die Startoption.
2. Wählen Sie **Verbinden mit > Alle Verbindungen anzeigen > Neue Verbindung erstellen**.
3. Wählen Sie im Assistenten für neue Verbindungen die Option **Eine erweiterte Verbindung einrichten**.

4. Wählen Sie in den erweiterten Verbindungsoptionen die Option **Verbindung direkt mit einem anderen Computer herstellen**.
5. Wählen Sie die Rolle **Gast** für diesen Computer aus.
6. Geben Sie einen Namen für die Verbindung ein.
7. Wählen Sie einen serielle Schnittstelle für die Verbindung aus. Dieser Port sollte der COM-Port sein, den das USB-Gerät verwendet.
8. Wählen Sie, ob die Verbindung für alle Benutzer oder nur für Sie selbst verfügbar sein soll.
9. Klicken Sie im letzten Dialog des Assistenten auf **Fertig stellen**.
10. Der PC verlangt einen Benutzernamen und ein Passwort für die USB-Verbindung. Geben Sie folgende Daten ein:
    - Benutzername: SPC
    - Passwort: password (Standard)
11. Klicken Sie auf **Verbinden**.
    ⇨ Der PC initiiert einen Datenverbindung zum Controller. Nachdem die Verbindung hergestellt wurde, wird ein Verbindungssymbol in der Taskleiste am unteren Rand des PC-Bildschirms angezeigt.
12. Klicken Sie das Verbindungssymbol mit der rechten Maustaste an und wählen Sie **Status**.
    ⇨ Im anschließend angezeigten Statusfenster wird eine IP-Adresse aufgeführt.
13. Geben Sie diese Adresse in die Adressleiste eines Internetbrowsers ein; verwenden Sie dabei das **H**yper **T**ext **T**ransfer **P**rotocol **S**ecure (z. B. https://192.168.5.1).
14. Melden Sie sich mit Ihrer Benutzer-PIN an der SPC-Browseranwendung an.

Ändern Sie sofort Ihre Standard-PIN, und notieren Sie sich die neue PIN. Eine vergessene Techniker-PIN kann nur durch Rücksetzen des Systems auf die Werkseinstellungen zurückgesetzt werden. Dadurch wird auch die Systemkonfiguration zurückgesetzt. Die Konfiguration kann jedoch über eine Sicherungskopie (Backup) wiederhergestellt werden.

Windows 7

▷ Führen Sie alle unter USB-Verbindung unter Windows 7 für SPC Pro beschriebenen Aktionen durch.

▷ Sie müssen lokale Administratorrechte besitzen, um diese Aufgabe ausführen zu können.

1. Öffnen Sie unter Windows 7 die Systemsteuerung.
2. Wählen Sie **Telefon und Modem** aus.
   ⇨ Das Fenster **Telefon und Modem** wird geöffnet.
3. Wählen Sie die Registerkarte **Modems**, und klicken Sie auf **Hinzufügen**.
   ⇨ Das Fenster **Hardware-Assistent – Neues Modem installieren** wird geöffnet.
4. Klicken Sie zweimal auf **Weiter**.
   ⇨ Der **Hardware-Assistent** zeigt eine Liste mit Modems an.

5. Wählen Sie **Kommunikationskabel zwischen zwei Computern**.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie den unter USB-Verbindung unter Windows 7 für SPC Pro zugewiesenen COM-Port aus.
8. Klicken Sie auf **Weiter**, dann auf **Fertig stellen**.
9. Kehren Sie zur Registerkarte **Modems** im Fenster **Telefon und Modem** zurück.
10. Wählen Sie das neue Modem aus, und klicken Sie auf **Eigenschaften**.
    ⇨ Das Fenster **Kommunikationskabel zwischen zwei Computern – Eigenschaften** wird geöffnet.
11. Klicken Sie auf der Registerkarte **Allgemein** auf **Einstellungen ändern**, um die Eigenschaften zu bearbeiten.
12. Wählen Sie die Registerkarte **Modem**.
13. Ändern Sie den Wert unter **Maximale Übertragungsrate** auf **115200**, und klicken Sie auf **OK**.
14. Öffnen Sie in der **Systemsteuerung** das **Netzwerk- und Freigabecenter**.
15. Klicken Sie auf **Adaptereinstellungen ändern**. Falls die Liste mit verfügbaren Anschlüssen ein neues Modem enthält, fahren Sie mit Schritt 23 fort. Falls das Modem *nicht* vorhanden ist, führen Sie die folgenden Schritte aus.
16. Klicken Sie im **Netzwerk- und Freigabecenter** auf **Neue Verbindung oder neues Netzwerk einrichten**.
17. Wählen Sie **Wählverbindung einrichten**, und klicken Sie auf **Weiter**.
18. Geben Sie in die Felder **Telefonnummer**, **Benutzername** und **Kennwort** die entsprechenden Daten ein, und geben Sie im Feld **Verbindungsname** eine Bezeichnung ein.
19. Klicken Sie auf **Verbinden**.
    ⇨ Windows 7 erstellt die Verbindung.
20. Überspringen Sie den Vorgang **Internetverbindung wird getestet**.
21. Klicken Sie auf **Schließen**.
22. Klicken Sie in **Netzwerk- und Freigabecenter** auf **Adaptereinstellungen ändern**.
23. Doppelklicken Sie auf das neue Modem.
    ⇨ Das Fenster *Verbindungsname* **verbinden** wird geöffnet. *Verbindungsname* steht für den Namen, den Sie für das Modem definiert haben.
24. Klicken Sie auf **Eigenschaften**.
25. Vergewissern Sie sich, dass das Feld **Verbinden über** die richtigen Angaben enthält, wie z. B. Kommunikationskabel zwischen zwei Computern (COM3).
26. Öffnen Sie Ihren Browser, und geben Sie die IP-Adresse der Zentrale ein. Verwenden Sie https als Verbindungsprotokoll.
27. Klicken Sie auf Installation fortsetzen, wenn der Browser eine Seite mit einer Fehlermeldung wegen eines falschen Zertifikats anzeigt.
28. Melden Sie sich an der Zentrale an.

17.4 Im Browser anmelden

Melden Sie sich im Browser an:

1. Öffnen Sie den Browser auf dem PC, sobald eine Ethernet- oder USB-Verbindung hergestellt und die IP-Adresse des Controllers ermittelt wurde.
2. Geben Sie die IP-Adresse in das Adressfeld ein; verwenden Sie dabei das **H**yper **T**ext **T**ransfer **P**rotocol **S**ecure (z. B. https:// 192.168.1.100). Siehe hierzu die nachfolgende Tabelle.
   ⇨ Ein Fenster mit einer Sicherheitsmeldung wird angezeigt.
3. Klicken Sie auf **Laden dieser Website fortsetzen** .
   ⇨ Der Anmeldebildschirm wird angezeigt.

4. Geben Sie folgende Daten ein:
   - **Benutzer ID**: Benutzer- oder Technikername
   - **Passwort**: Benutzer- oder Techniker-PIN
5. Wählen Sie eine Sprache, in der die Browser-Bildschirme angezeigt werden sollen. Die Standard-Sprachen-Einstellung „Auto“ lädt automatisch die Sprache, die dieser Benutzer-ID zugewiesen ist.
6. Klicken Sie auf **Anmelden**.

Standardeinstellungen für WEBserver-Adressen:

Verbindung	IP-Adresse Webserver
Ethernet	192.168.1.100 (Werkseinstellung)
RS232	192.168.2.1 (feste IP)
Backup-Modem / RS232	192.168.3.1 (feste IP)
Primär-Modem	192.168.4.1 (feste IP)
USB	192.168.5.1 (feste IP)

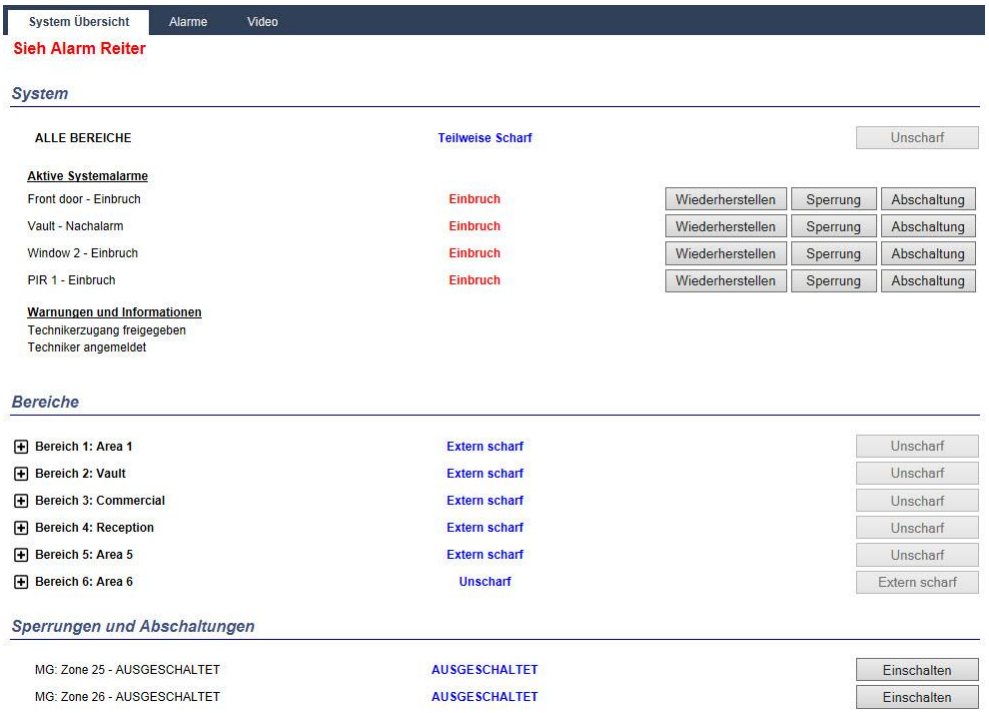
17.5 SPC Startseite

Die SPC-Startseite enthält die Registerkarten **System Übersicht**, **Alarme** und **Video**.

17.5.1 System-Übersicht

Die Registerkarte **System Übersicht** ist in die folgenden Abschnitte unterteilt:

- **System**: Zeigt den Status aller Bereiche, aktive Systemalarme und Warnungen sowie Informationen für das System an.
- **Bereiche**: Zeigt den Status jedes im System definierten Bereichs mit bis zu 20 Alarmereignissen an. Sie können einen Bereich scharf und unscharf stellen, und der Bereichsstatus wird hier angezeigt.
- **Sperrungen und Abschaltungen**: Listet alle abgeschalteten MGs auf und ermöglicht Ihnen das Einschalten oder Umgehen vor der Scharfschaltung.



!	*HINWEIS*
	Falls im System Alarme vorhanden sind, wird die Meldung **Siehe Alarm Reiter** angezeigt.

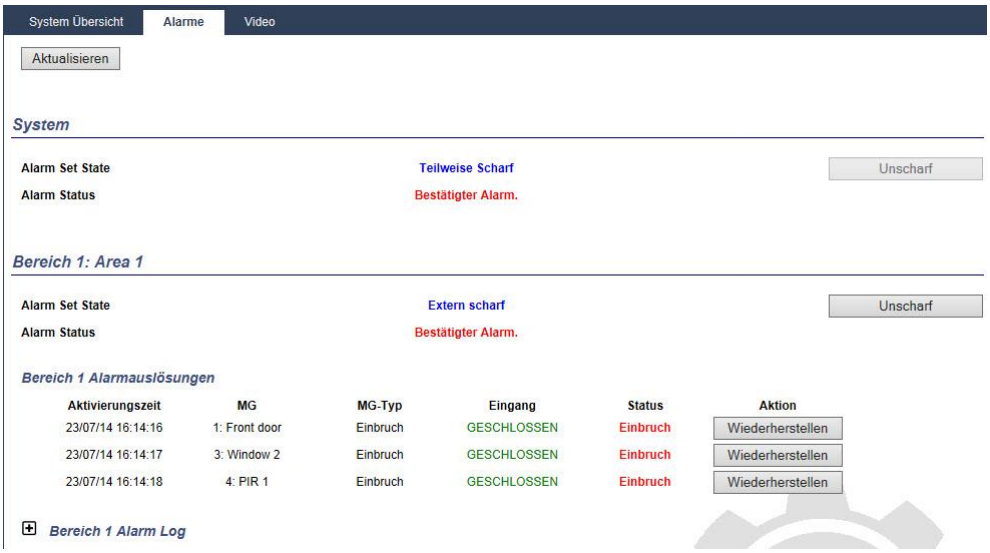
17.5.2 Alarmübersicht

Die Registerkarte **Alarme** enthält die folgenden Systeminformationen:

- **Alarm Set State** (Schärfungszustand bei Alarm) – Zeigt an, ob das System teilweise oder vollständig scharf geschaltet war, als der Alarm ausgelöst wurde.
- **Alarm Status** – Zeigt der Typ des Alarms an (Alarm, bestätigter Alarm usw.)
- **Sirenen Aktiv** – Zeigt an, ob der Alarm die Sirenen aktiviert hat. Klicken Sie auf die Schaltfläche **Sirenen abschalten**, um sie zu deaktivieren.

Für jeden Bereich wird **Alarm Set State**, **Alarm Status**, **Alarmauslösungen** und **Alarm Log** angezeigt. **Alarmauslösungen** zeigt eine Liste der MGs am

Alarmzustand geordnet nach ihrer Aktivierung. Klicken Sie zum Löschen auf die Schaltfläche **Wiederherstellen**. **Alarm Log** zeigt bis zu 20 Ereignisse.



17.5.3 Anzeigen des Videos

Die Registerkarte **Video** zeigt die Bilder von bis zu 4 IP-Kameras.

- Wählen Sie im Konfigurationsmodus, Wartungsmodus oder Benutzermodus die Optionen **SPC Startseite > Video**.

  ⇨ Alle konfigurierten und betriebsbereiten Kamera (bis zu 4 Stück) werden auf der Seite **Videokameras** angezeigt. Im folgenden Beispiel sind nur zwei Kameras verfügbar.

Die Bilder werden automatisch gemäß der Intervalleinstellungen der Kamera aktualisiert. (Siehe Konfigurieren von Video [→ 280])

Klicken Sie auf die Schaltfläche **Refresh aus**, um das aktuelle Bild auf dem Bildschirm zu belassen und die Aktualisierung zu unterbrechen. Klicken Sie auf die Schaltfläche **Refresh ein**, um die Aktualisierung der Bilder in der Zentrale fortzusetzen.

Hinweis: Stellen Sie sicher, dass für die Kameras eine Auflösung von 320 × 240 ausgewählt ist. Anderenfalls werden die Bilder nicht ordnungsgemäß im Browser angezeigt. Die höhere Auflösung von 640 × 480 kann für SPC Pro und SPC Com verwendet werden.

Meldung einer Videostörung

Eine Meldung der Videostörung wird über dem Kamerabild angezeigt. Die folgende Tabelle enthält die möglichen Meldungen:

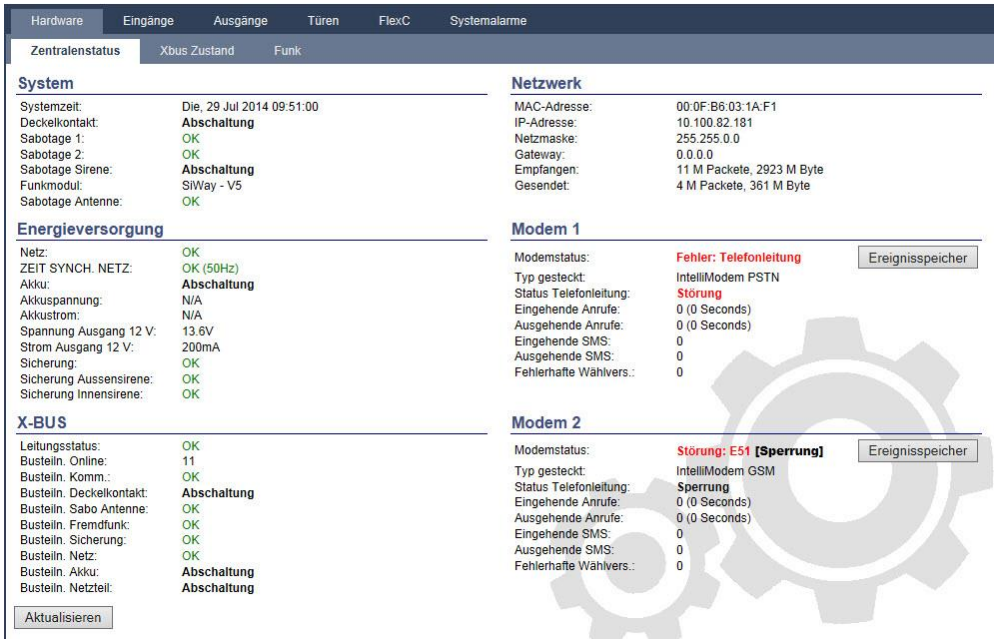
Nachricht	Beschreibung
OK	Die Kamera verhält sich normal.
Komm. Timeout	Die Kameraverbindung hat eine Zeitüberschreitung verursacht.
Socket Ungültig	Interner Socket-Umgangsfehler
Bild zu klein	Das empfangene Bild ist zu klein.
Buffer zu klein	Das empfangene Bild ist zu groß. Verringern Sie die Auslösung in der Kamerakonfiguration.
Format incorrect (Falsches Format)	Es wurde ein ungültiges Format empfangen.
Abbrechen	Die TCP-Verbindung wurde getrennt.
Intern	Die Alarmzentrale besitzt zu wenig Arbeitsspeicher, um die Abfrage abzuschließen.
Fehlerhafte Abfrage	Es wurde eine fehlerhaft formulierte Abfrage an die Kamera gesendet. Prüfen Sie die Konfigurationseinstellungen Ihrer Kamera.
Clientfehler	Die Kamera hat einen Clientfehler zurückgegeben. Prüfen Sie die Konfigurationseinstellungen Ihrer Kamera.
Authorization error (Autorisierungsfehler)	Das Benutzername oder das Kennwort ist falsch.
Unbekannt	Es wurde ein unbekannter Fehler zurückgegeben. Bei der Kamera könnte es sich um ein nicht unterstütztes Modell handeln.

17.6 Status der Zentrale

17.6.1 Status

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

1. Wählen Sie **Status > Hardware > Zentralenstatus**.
2. Siehe die nachfolgende Tabelle für weitere Informationen.



Ausführbare Aktionen

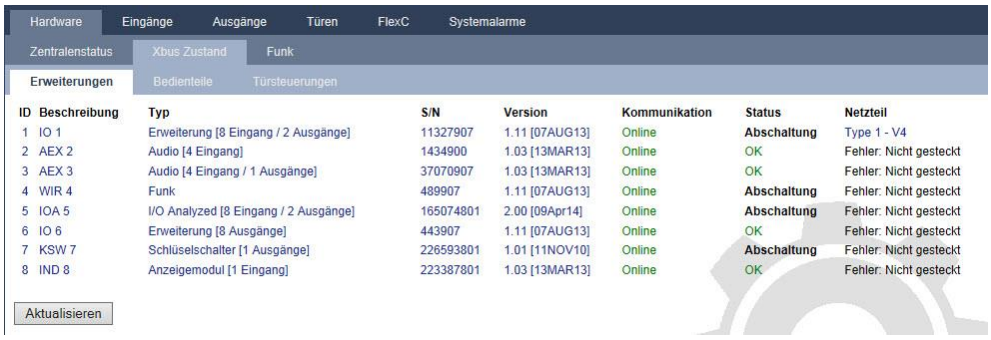
Die nachstehenden Aktionen können nur dann ausgeführt werden, wenn eine Verbindung aufgebaut wurde.

Alle Alarme quittieren (Pro)	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.

17.6.2 X-Bus-Status

1. Wählen Sie **Status > Hardware > X-Shunt**.

   ⇨ Das folgende Fenster mit dem Status der verschiedenen X-BUS-Geräte wird angezeigt. Alle erkannten Erweiterungen werden als Standard aufgelistet.



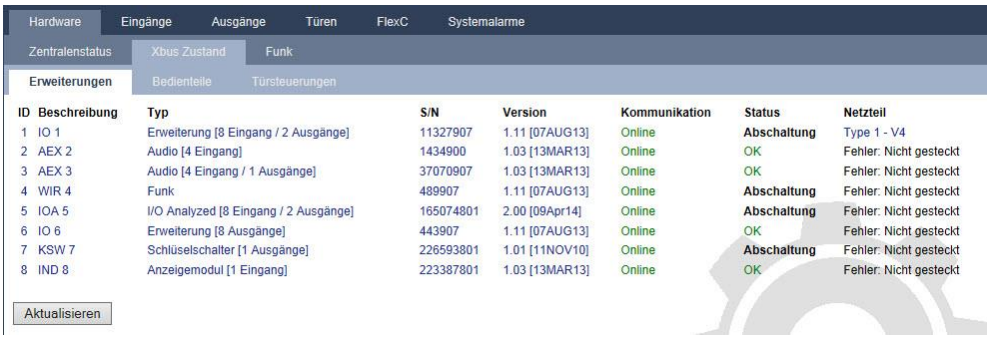
2. Wählen Sie eine der folgenden Registerkarten.
   - Erweiterungen (Programmieren von Erweiterungen siehe Seite [→ 219]).
   - Bedienteile (Programmieren von Bedienteilen siehe Seite [→ 224]).

- Türsteuerungen (Programmieren von Türsteuerungen siehe Seite [→ 230]).

3. Klicken Sie auf einen der Parameter des Bedienteils/der Erweiterung/der Türsteuerung (ID, Beschreibung, Typ, Seriennummer), um weitere Statusinformationen anzuzeigen.

17.6.2.1 Status Erweiterung

1. Wählen Sie **Status > Hardware > X-Shunt**.
2. Wählen Sie die Registerkarte **Erweiterungen**.
   ⇨ Eine Liste mit erkannten Erweiterungen und den entsprechenden Netzteilen wird angezeigt.



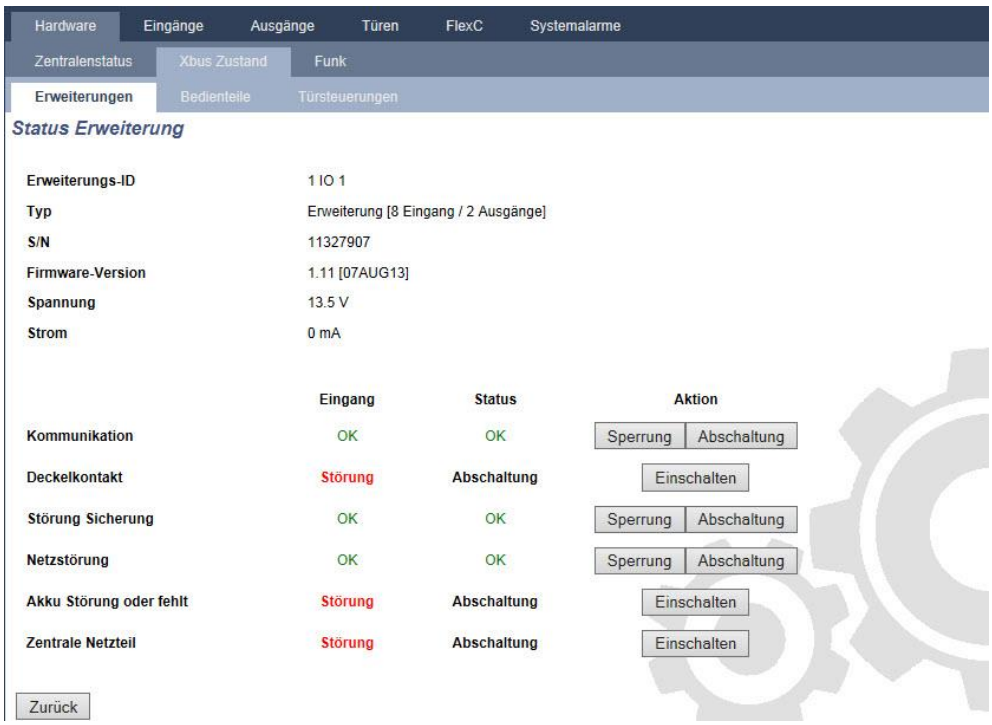
Erweiterungs-ID	Mit dieser ID wird die Erweiterung eindeutig gekennzeichnet.
Beschreibung	Beschreibungstext für die Erweiterung. Dieser Text erscheint auch im Browser und im Bedienteil.
Typ	Der Typ der erkannten Erweiterung (I/O, Netzteil, Bedienteil usw.).
S/N	Die Seriennummer der Erweiterung.
Version	Die Firmware-Version der Erweiterung.
Komm.	Der Status der Erweiterung (online oder offline).
Status	Der Status der Erweiterung (OK, Störung, OF Tür Sabotage).
Netzteil	Der Netzteiltyp der Erweiterung, falls zutreffend. Klicken Sie auf das Netzteil (NT), um den Status anzuzeigen.

Ausführbare Aktionen

Aktualisieren	Klicken Sie auf die Schaltfläche, um den Status des X-BUS zu aktualisieren.

Anzeigen weiterer Statusinformationen:

- Klicken Sie auf einen der Parameter der Erweiterung (ID, Beschreibung, Typ, Seriennummer), um weitere Statusinformationen anzuzeigen.



Name	Beschreibung
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.
Störung Netz Zentrale	Der physische und der programmierte Status der Netzstromversorgung für den Controller.
Batteriestörung	Der physische und der programmierte Status der Batterie.
Busteiln. Fremdfunk	Der physische und der programmierte Status des Netzteils.
OP Sabo.	Der physische und der programmierte Status der Sabotage-Ausgänge auf dem Netzteil.
Niedrige Spannung	Statusanzeige für niedrige Batteriespannung

Ausführbare Aktionen

Name	Beschreibung
Alarme quittieren	Klicken Sie auf die Schaltfläche, um alle Alarme 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. 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

Name	Beschreibung
	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.

Siehe auch

Netzteilstatus [→ 182]

17.6.2.2 Netzteilstatus

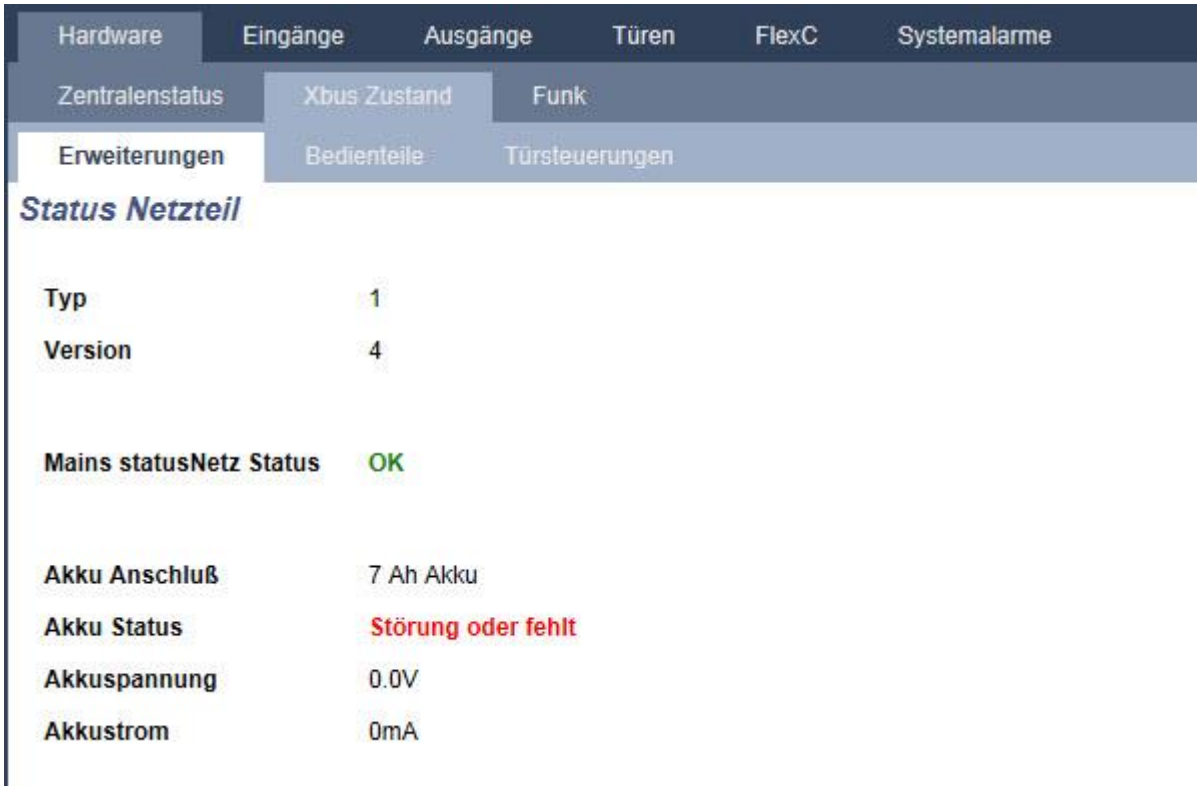
Das Fenster **Status Netzteil** zeigt Informationen über den aktuellen Status des Netzteils und seine Ausgänge sowie den jeweiligen Status verbundener Batterien an.

Die folgenden Netzteiltypen werden unterstützt:

- SPCP332/333 Smart-Netzteil
- SPCP355 Smart-Netzteil

Status SPCP332/333 Smart-Netzteil

Die folgende Abbildung zeigt den Smart-Netzteilstatus an:

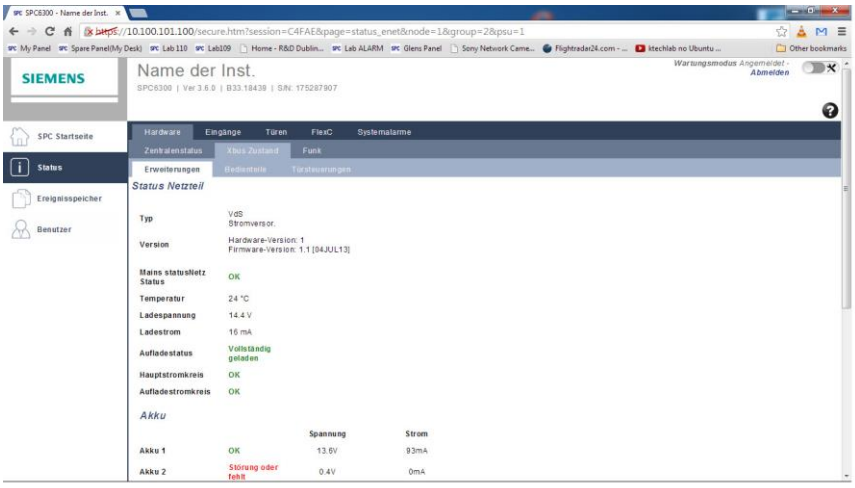


Name	Beschreibung
Typ	Der Typ des Netzteils.
Version	Die Version des Netzteils.
Netz-Status	Zeigt den Zustand der Netzverbindung an. Mögliche Werte sind: Störung oder OK

Name	Beschreibung
Batterie Link	Zeigt den Typ der angeschlossenen Batterie an.
Batteriezustand	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 Status des SPCP355 Smart-Netzteils an:



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.

Name	Beschreibung
Hauptstromkreis	Zeigt den Zustand des Hauptstromkreises an, der bei verbundenem Netzstrom für die Stromversorgung zuständig ist.
Aufladestromkreis	Zeigt den Status des Aufladestromkreises an, der bei korrekter Netzstromversorgung 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.

17.6.2.3 Status Bedienteil

1. Wählen Sie **Status > Hardware > X-Shunt**.
2. Wählen Sie die Registerkarte **Bedienteile**.
   ⇨ Eine Liste mit den erkannten Türsteuerungen wird angezeigt.

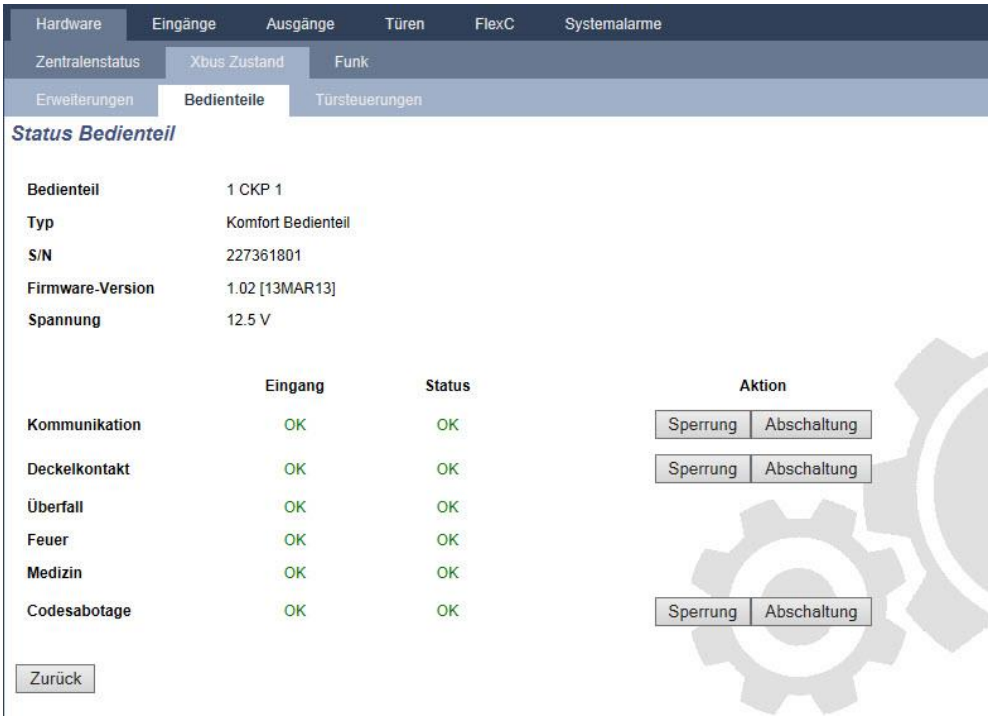
Name	Beschreibung
Erweiterungs-ID	Mit dieser ID wird das Bedienteil eindeutig gekennzeichnet.
Beschreibung	Beschreibungstext für das Bedienteil (max. 16 Zeichen).
Typ	Der Typ der erkannten Erweiterung (= Bedienteil).
S/N	Die Seriennummer des Bedienteils.
Version	Die Firmware-Version des Bedienteils.
Komm.	Der Status des Bedienteils (online oder offline).
Status	Der Status des Bedienteils (OK, Störung).

Ausführbare Aktionen

Aktualisieren	Klicken Sie auf die Aktualisierungsschaltfläche, um die Liste mit den erkannten Bedienteilen und den jeweiligen Status zu aktualisieren.

Anzeigen weiterer Statusinformationen:

- Klicken Sie auf einen der Parameter des Bedienteils (ID, Beschreibung, Typ, Seriennummer), um weitere Statusinformationen anzuzeigen.



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.
TRANSPONDER	Betrifft nur Bedienteile, in denen ein Transpondersignalempfänger installiert ist.
Überfall	Anzeige des Überfall-Alarmstatus am Bedienteil.
Feuer	Anzeige des Feuer-Alarmstatus am Bedienteil.
Medizinischer Notfall	Anzeige des Alarmstatus zu einem medizinischen Notfall am Bedienteil.
Code-Sabotage	Status Bedienteil-PIN Sabotage-Alarm

Ausführbare Aktionen

Alarme quittieren	Klicken Sie auf die Schaltfläche, um alle Alarme 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. 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.

17.6.2.4 Türen aktual.

1. Wählen Sie **Status > Hardware > X-Shunt**.
2. Wählen Sie die Registerkarte **Türsteuerungen**.
   ⇨ Eine Liste der erkannten Türsteuerungen wird angezeigt.

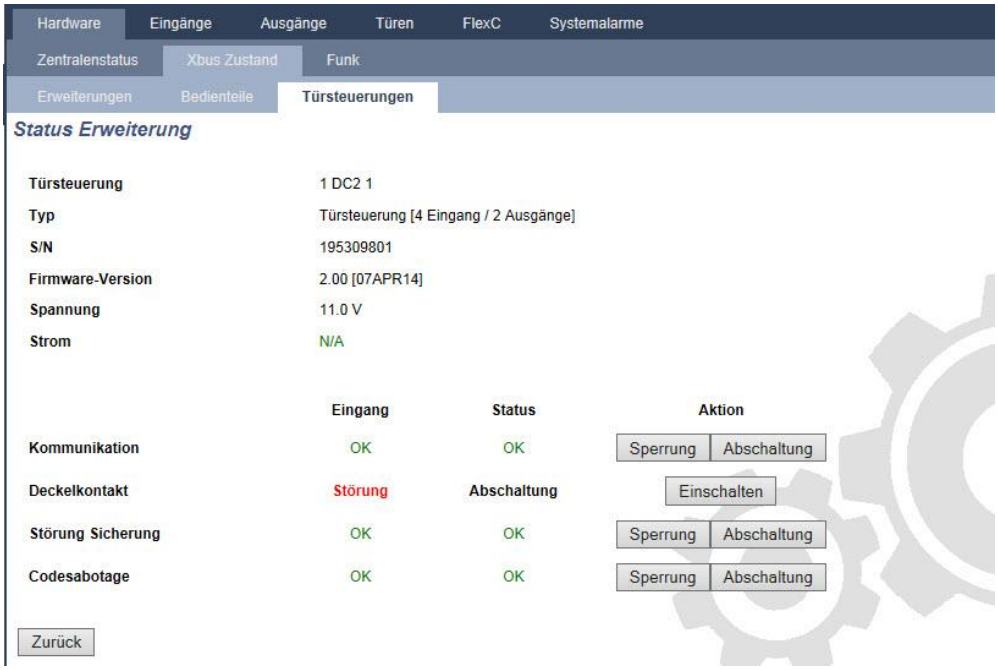
Erweiterungs-ID	Mit dieser ID wird die Türsteuerung eindeutig gekennzeichnet.
Beschreibung	Beschreibungstext für die Türsteuerung (max. 16 Zeichen).
Typ	Der Typ der erkannten Türsteuerung (= Türsteuerung).
S/N	Die Seriennummer der Türsteuerung
Version	Die Firmware-Version der Türsteuerung.
Komm.	Der 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.

Anzeigen weiterer Statusinformationen:

- Klicken Sie auf einen der Parameter der Türsteuerung (ID, Beschreibung, Typ, Seriennummer), um weitere Statusinformationen anzuzeigen.



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.
Code-Sabotage	Status des Benutzer-PIN. Nach mehreren fehlgeschlagenen Versuchen wird ein Alarm ausgelöst.

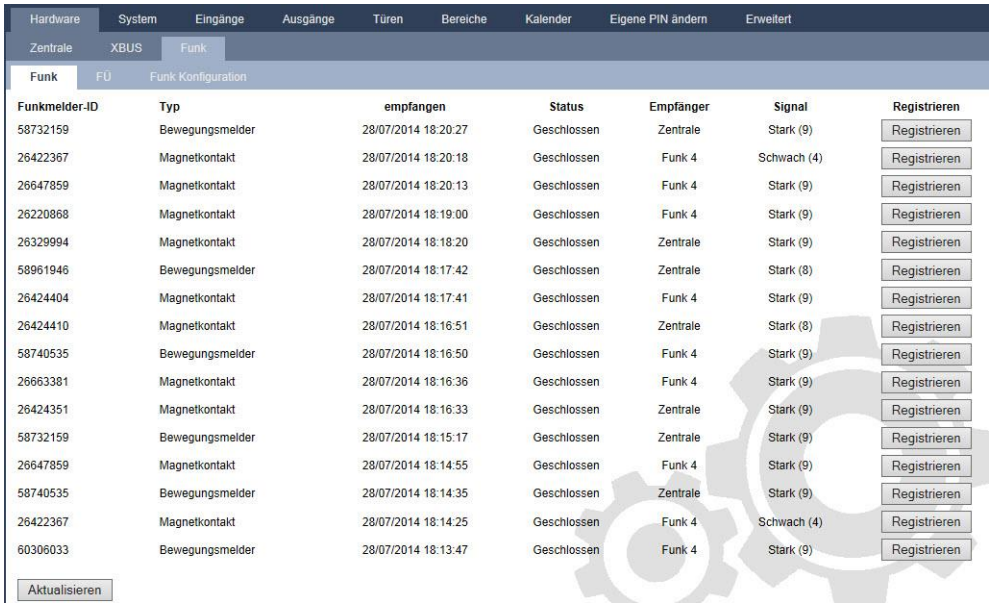
Ausführbare Aktionen

Alarme quittieren	Klicken Sie auf die Schaltfläche, um alle Alarme 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. 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.

17.6.3 Funk

Die Funkmeldererkennung (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. Wählen Sie **Konfiguration > Hardware > Funk > Funk**.
2. Weitere Informationen finden Sie in der nachstehenden Tabelle.



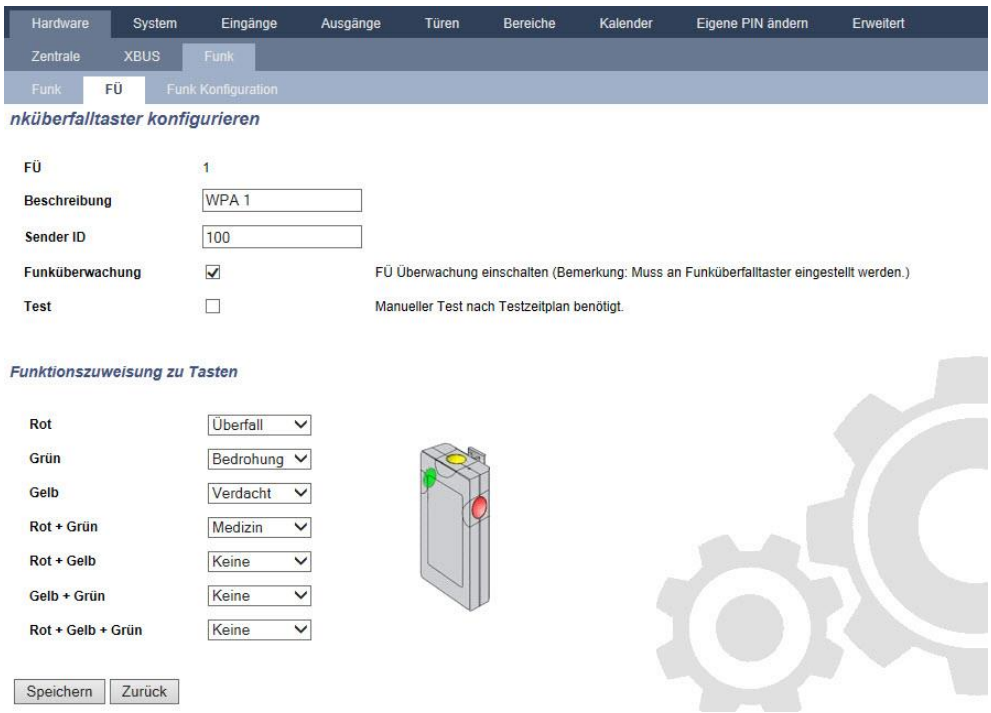
Funkmelder-ID	Typ	empfangen	Status	Empfänger	Signal	Registrieren
58732159	Bewegungsmelder	28/07/2014 18:20:27	Geschlossen	Zentrale	Stark (9)	Registrieren
26422367	Magnetkontakt	28/07/2014 18:20:18	Geschlossen	Funk 4	Schwach (4)	Registrieren
26647859	Magnetkontakt	28/07/2014 18:20:13	Geschlossen	Funk 4	Stark (9)	Registrieren
26220868	Magnetkontakt	28/07/2014 18:19:00	Geschlossen	Funk 4	Stark (9)	Registrieren
26329994	Magnetkontakt	28/07/2014 18:18:20	Geschlossen	Zentrale	Stark (9)	Registrieren
58961946	Bewegungsmelder	28/07/2014 18:17:42	Geschlossen	Zentrale	Stark (8)	Registrieren
26424404	Magnetkontakt	28/07/2014 18:17:41	Geschlossen	Funk 4	Stark (9)	Registrieren
26424410	Magnetkontakt	28/07/2014 18:16:51	Geschlossen	Zentrale	Stark (8)	Registrieren
58740535	Bewegungsmelder	28/07/2014 18:16:50	Geschlossen	Funk 4	Stark (9)	Registrieren
26663381	Magnetkontakt	28/07/2014 18:16:36	Geschlossen	Funk 4	Stark (9)	Registrieren
26424351	Magnetkontakt	28/07/2014 18:16:33	Geschlossen	Zentrale	Stark (9)	Registrieren
58732159	Bewegungsmelder	28/07/2014 18:15:17	Geschlossen	Zentrale	Stark (9)	Registrieren
26647859	Magnetkontakt	28/07/2014 18:14:55	Geschlossen	Funk 4	Stark (9)	Registrieren
58740535	Bewegungsmelder	28/07/2014 18:14:35	Geschlossen	Zentrale	Stark (9)	Registrieren
26422367	Magnetkontakt	28/07/2014 18:14:25	Geschlossen	Funk 4	Schwach (4)	Registrieren
60306033	Bewegungsmelder	28/07/2014 18:13:47	Geschlossen	Funk 4	Stark (9)	Registrieren

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). **Hinweis:** 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

Log (Protokoll)	Anklicken, um das Protokoll des Funksensors anzuzeigen. Siehe Seite [→ 188].
Einlernen	Klicken Sie auf diese Option, um die Liste mit abgemeldeten Funkgeräten zu öffnen.

1. Wählen Sie **Status > Hardware > Funk > WPA**.
2. Die Identität jedes eingelernten FÜ und der Status werden angezeigt.



17.6.3.1 Log - Funkmelder X

Anzeigen eines Ereignisprotokolls für einen Funkmelder:

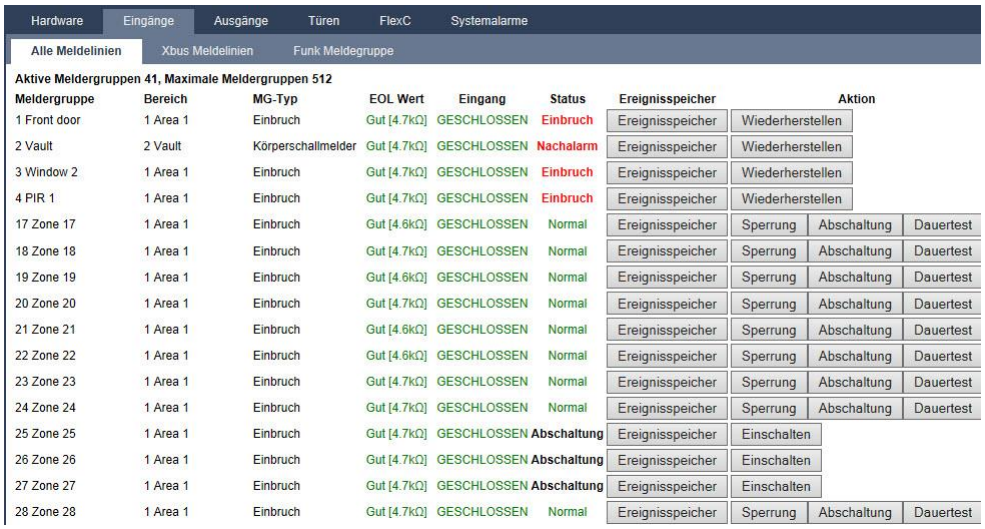
1. Klicken Sie auf die Schaltfläche **Log**.
2. Weitere Informationen finden Sie in der nachstehenden Tabelle.
3. Erstellen Sie eine Textdatei des Logs durch Klicken auf **Textdatei** .

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).

17.6.4 Meldegruppen

Informationen zur Konfiguration finden Sie auf Seite [→ 256].

1. Wählen Sie zur Anzeige aller Meldergruppe die Optionen **Status > Eingänge > Alle Meldelinien**. Wählen Sie zur Anzeige der MGs mit X-Bus die Registerkarte **X-Bus Zones** (MGs mit X-Bus) oder wählen Sie zur Anzeige der Funkmeldergruppen die Registerkarte **Funk Meldegruppe**.
2. Siehe die nachfolgende Tabelle für weitere Informationen.



Autom Aktualisieren der Statusanzeige Pro	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	Zeit den EOL-Wert für den Widerstandsbereich des Meldergruppenzustands an. Mögliche Werte sind: ● Gut – Nomineller Wert +/- 25 % des definierten Bereichs ● OK – Nomineller Wert +/- 50 % des definierten Bereichs ● Schwach – Nomineller Wert +/- 75 % des definierten Bereichs ● Ungenügend — jeder andere Wert ● Laut – zeigt ein Problem bei der Signalerkennung an. Das Kabel könnte sich in der Nähe eines Hauptkabels oder einer anderen Interferenzquelle befinden. Diese Spalte ist nur im Techniker-Modus sichtbar. Weitere Informationen zu nominellen Widerstandswerten und deren definierte Bereiche finden Sie unter Verdrahtung Linieneingänge [→ 86].
Eingang	Der erkannte Eingabestatus dieser MG (Unbekannt, Offen, Geschlossen, Leitungsbruch, Kurzschluss, Impuls, Erschütterung, Abgedeckt, Störung, Ausserhalb d. Gr, Meldergruppen instabil schärfen, Fremdspannung, Laut). Fremdspannung ist ein Eingabe-Sabotagealarm. Bei einem Fremdspannungsaustausch wird eine regelmäßige Überprüfung ausgeführt, um sicherzustellen, dass keine externen Spannungen an diesen Schaltkreis angelegt werden. Instabil: Ein instabiler Zustand tritt ein, wenn der Widerstandswert der Linieneingänge über einen definierten Probenzeitraum instabil ist. Laut: Ein lauter Zustand tritt ein, wenn während eines definierten Messintervalls eine externe Interferenz in den Eingangsschaltkreis induziert wird. Im Aus: Ein Im-Aus-Zustand tritt ein, wenn der Widerstandswert am Meldergruppeneingang nicht innerhalb der akzeptierten Toleranzen der aktuellen EOL-Werte liegt.

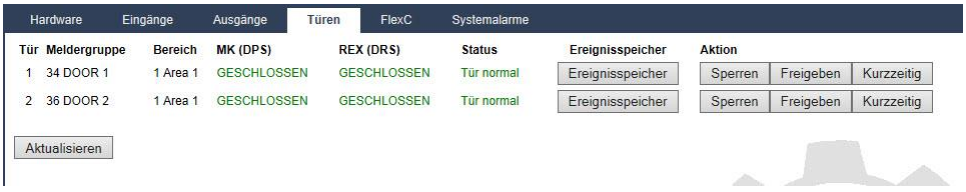
Status	Der programmierte Status einer MG. Der Statuswert Normal bedeutet, dass die MG für den normalen Betrieb programmiert ist. Nachstehend finden Sie eine vollständige Liste der möglichen Werte: Abschaltung, Dauertest, Sperrung, Sabotage, Alarm, Notausgang, Warnung Fehler, Bedrohung Fehler, Störung, 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.

Ausführbare Aktionen

Aktualisieren	Aktualisiert die für die Zentrale angezeigten Statusinformationen.
Log (Protokoll)	Klicken Sie auf die Schaltfläche „Log“, um ein Protokoll des Eingangsstatus dieser MG anzuzeigen..
Sperren (!)	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.
Quittieren	Klicken Sie auf diese Schaltfläche, um den Alarmzustand der Zentrale zu quittieren.
Abschalten	Meldergruppe. 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 Pro	Klicken Sie auf diese Schaltfläche, um den ausgewählten Körperschallmelder zu testen. Weitere Informationen über Körperschallmelder finden Sie unter Körperschallmelder [→ 350].
Geschl Eingänge nicht anzeigen	Klicken Sie auf diese Schaltfläche, um alle geschlossenen Eingänge zu verbergen.
Filter-MG Pro	Wählen Sie einen Meldergruppen -Typ aus dem Dropdown-Menü. Es wird nur die Übersicht für den gewählten Meldergruppen-Typ angezeigt.

17.6.5 Türen

1. Wählen Sie **Status > Türmeldungen**.
2. Siehe die nachfolgende Tabelle für weitere Informationen.



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) Pro	Status des REX Tasters.

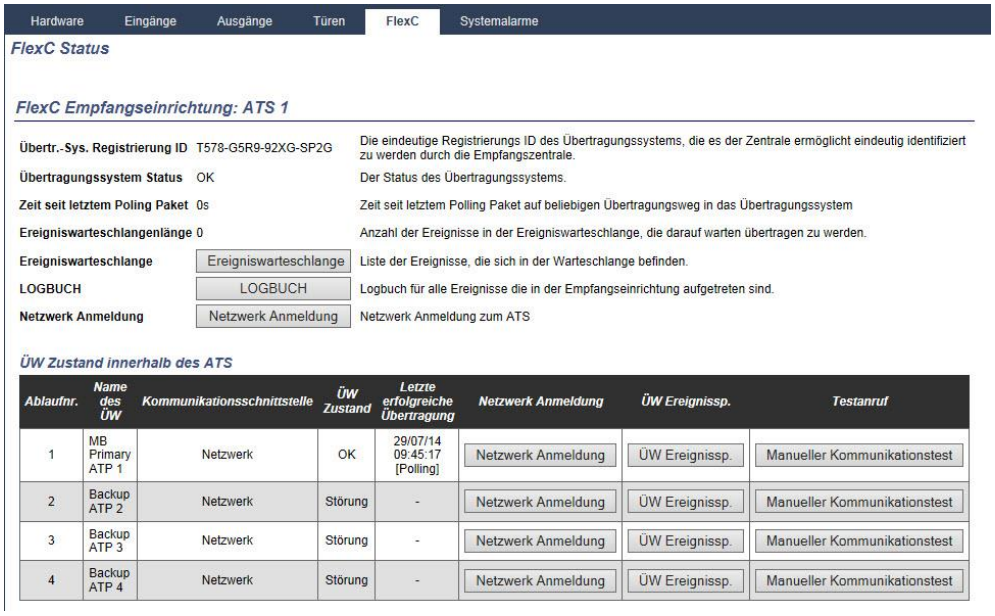
Ausführbare Aktionen

Aktualisieren	Aktualisiert die Tür-Übersicht.
Log (Protokoll)	Zeigt ein Ereignisprotokoll der gewählten Tür an.
Sperren	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.

17.6.6 FlexC Status

Dieser Bildschirm zeigt den Status jedes im System konfigurierten ATS an.

1. Wählen Sie zur Anzeige des Status eines ATS die Optionen **Status > FlexC**.
2. In der unteren Tabelle werden die Statuskriterien beschrieben, die für jedes ATS verfügbar sind.

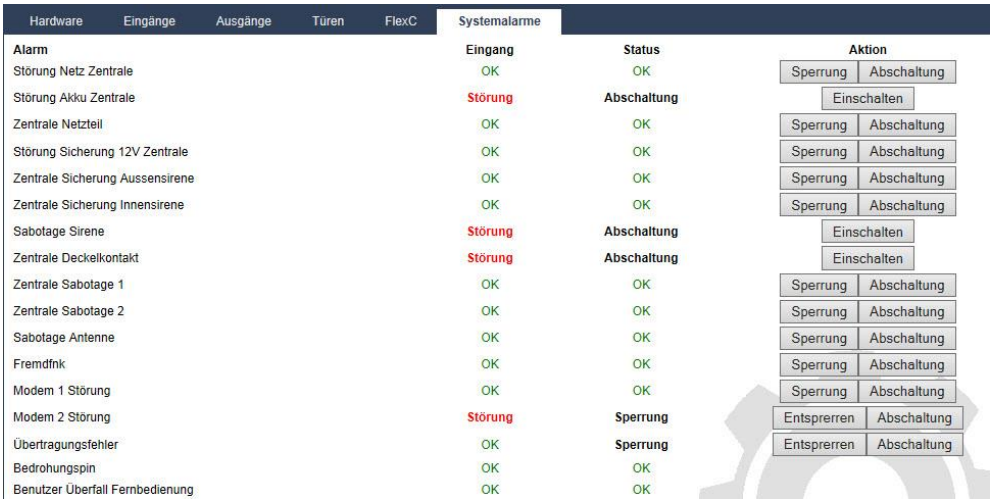


Übertr.-Sys. Registrierung ID	Die eindeutige Registrierungs-ID des Übertragungssystems, die es der Zentrale ermöglicht, durch die Empfangszentrale eindeutig identifiziert zu werden.
Übertragungssystem Status	Der Status des ATS, z. B. „Wird initialisiert“.
Time since last poll (Zeit seit letztem Polling)	Zeit seit letztem Polling-Paket auf einem beliebigen Übertragungsweg in das Übertragungssystem.
Ereigniswarteschlangenlänge	Anzahl der Ereignisse in der Ereigniswarteschlage, die auf ihre Übertragung werden.
Ereigniswarteschlangenlänge	Anzahl der Ereignisse in der Ereigniswarteschlage, die auf ihre Übertragung werden.

Ereigniswarteschlange	Liste der Ereignisse, die sich in der Ereigniswarteschlange befinden. Die Tabelle enthält Folgendes: ● Ereignisfolge-Nummer ● Ereignis Zeitstempel ● Ereignisbeschreibung ● Zusätzliche Ereignisinformation ● Start Zeitstempel ● Berichtsdauer
Ereignisprotokoll	Der Ereignisprotokollverlauf für alle Ereignisse, die im ATS aufgetreten sind. Die Tabelle enthält die gleichen Felder wie die obige Ereigniswarteschlange und zusätzlich das folgende Feld: ● Ereignisfolge-Nummer ● Ereignis Zeitstempel ● Ereignisbeschreibung ● Zusätzliche Ereignisinformation ● "Ergebnis" ● Berichteter ÜW ● Start Zeitstempel ● FlexC Beispiel ● Berichtsdauer
Netzwerk Anmeldung	Netzwerkanmeldung für das ATS mit dem konfigurierten Polling-Intervall.
Status of ATPs within ATS (Status der ÜWs im ATS)	Diese Tabelle enthält jedes ÜW im ATS. Die Tabelle zeigt für jedes ÜW die Sequenznummer, den Namen, die Kommunikationsschnittstelle, den Status, die letzte erfolgreiche Übertragung, die Netzwerkanmeldung, das Protokoll und die Schaltfläche „Testanruf“ an. **Netzwerk Anmeldung**: Klicken Sie auf diese Schaltfläche, um die Netzwerkanmeldung anzuzeigen. **ÜW Ereignissp.**: Zeigt eine Liste der Polling-Übertragungen. Klicken Sie auf die Schaltfläche **Aktualisieren**, um das Protokoll zu aktualisieren. Klicken Sie auf die Schaltfläche **Letzte Zuletzt**, um die Anzeigereihenfolge zu ändern. Standardmäßig wird das neueste Ereignis zuerst angezeigt. Schaltfläche **Manueller Kommunikationstest**: Klicken Sie auf diese Schaltfläche, um einen Testanruf zu erzwingen. Das Ereignis wird der Ereigniswarteschlange hinzugefügt.

17.6.7 Systemalarme

1. Wählen Sie **Status > Systemalarme** .
2. Siehe die nachfolgende Tabelle für weitere Informationen.



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

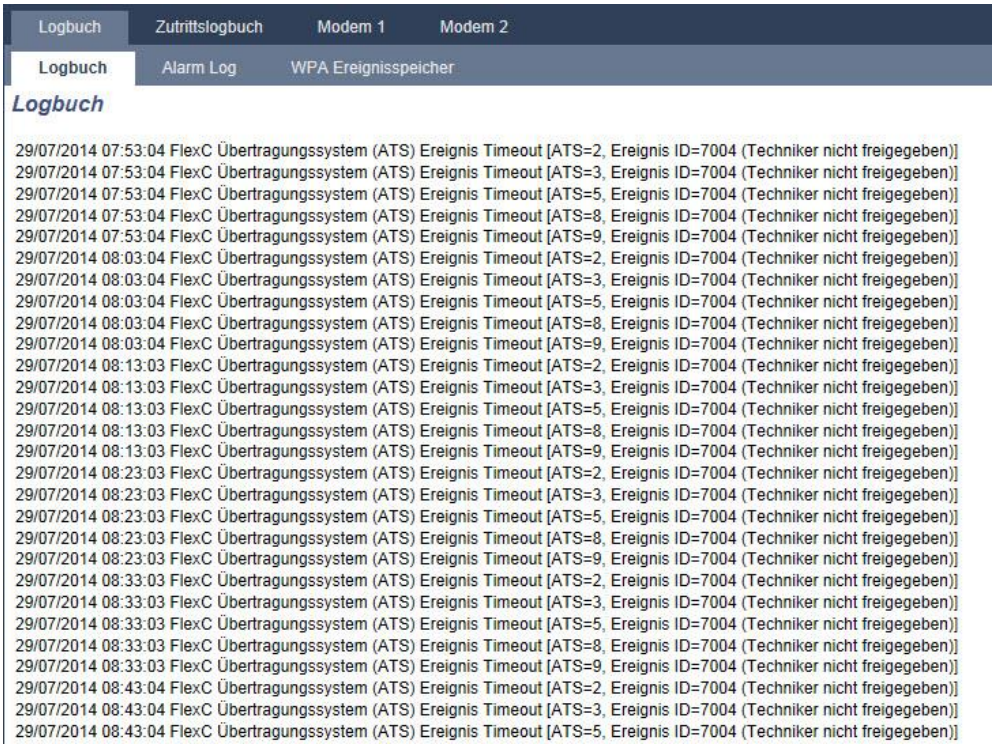
Aktualisieren	Klicken Sie auf diese Schaltfläche, um den Status der Systemalarme zu aktualisieren.
Quittieren	Klicken Sie auf diese Schaltfläche, um einen Alarm auf der Zentrale wiederherzustellen.
Sperren ⓘ	Klicken Sie auf diese Schaltfläche, um eine Störungsbedingung zu sperren. Durch das Sperren werden 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.

17.7 Logbücher

17.7.1 Logbuch System

Dieses Logbuch enthält alle Systemereignisse des SPC-Systems.

1. Wählen Sie **Logbuch > Logbuch > Logbuch Zentrale**.
2. Erstellen Sie eine Textdatei des Logs durch Klicken auf **Textdatei** .
3. Die Protokollierung der Statusänderungen einzelner Meldergruppen wird aktiviert durch Setzen des Log-Attributs für die Meldergruppe auf der Konfigurationsseite für MG-Attribute.



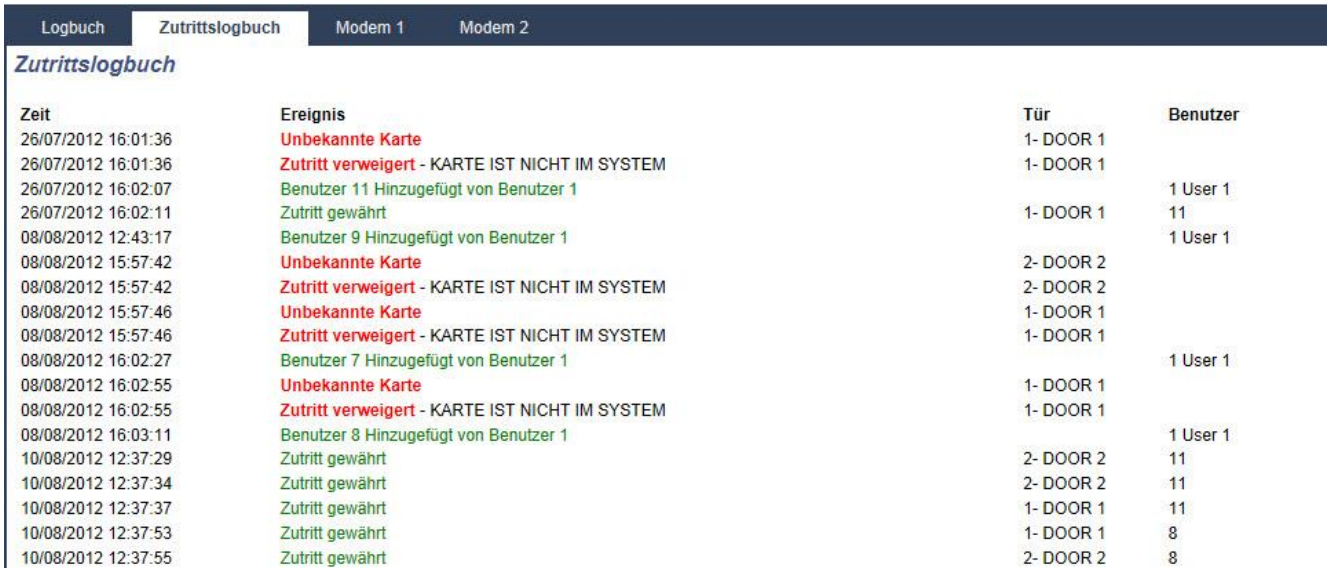
Um zu vermeiden, dass mehrere Ereignisse aus der gleichen Quelle das Log füllen, lässt das SPC -System gemäß der geltenden Normen die Protokollierung von maximal 3 Aktivierungen der gleichen Meldergruppe innerhalb eines Alarmzeitraums zu.

17.7.2 Logbuch der Zutrittskontrollfunktion

Das Protokoll informiert über alle Zutrittsereignisse des SPC-Systems.

- Wählen Sie **Log > Zutrittslogbuch**.

⇨ Daraufhin erscheint das folgende Fenster:



Zeit	Ereignis	Tür	Benutzer
26/07/2012 16:01:36	Unbekannte Karte	1- DOOR 1	
26/07/2012 16:01:36	Zutritt verweigert - KARTE IST NICHT IM SYSTEM	1- DOOR 1	
26/07/2012 16:02:07	Benutzer 11 Hinzugefügt von Benutzer 1		1 User 1
26/07/2012 16:02:11	Zutritt gewährt	1- DOOR 1	11
08/08/2012 12:43:17	Benutzer 9 Hinzugefügt von Benutzer 1		1 User 1
08/08/2012 15:57:42	Unbekannte Karte	2- DOOR 2	
08/08/2012 15:57:42	Zutritt verweigert - KARTE IST NICHT IM SYSTEM	2- DOOR 2	
08/08/2012 15:57:46	Unbekannte Karte	1- DOOR 1	
08/08/2012 15:57:46	Zutritt verweigert - KARTE IST NICHT IM SYSTEM	1- DOOR 1	
08/08/2012 16:02:27	Benutzer 7 Hinzugefügt von Benutzer 1		1 User 1
08/08/2012 16:02:55	Unbekannte Karte	1- DOOR 1	
08/08/2012 16:02:55	Zutritt verweigert - KARTE IST NICHT IM SYSTEM	1- DOOR 1	
08/08/2012 16:03:11	Benutzer 8 Hinzugefügt von Benutzer 1		1 User 1
10/08/2012 12:37:29	Zutritt gewährt	2- DOOR 2	11
10/08/2012 12:37:34	Zutritt gewährt	2- DOOR 2	11
10/08/2012 12:37:37	Zutritt gewährt	1- DOOR 1	11
10/08/2012 12:37:53	Zutritt gewährt	1- DOOR 1	8
10/08/2012 12:37:55	Zutritt gewährt	2- DOOR 2	8

- Erstellen Sie eine Textdatei des Logs, indem Sie auf die Schaltfläche **Textdatei** klicken.

17.7.3 WPA Ereignisspeicher

Dieses Logbuch enthält alle FÜ-Ereignisse des Systems.

- Wählen Sie **Logbuch > Logbuch > WPA Ereignisspeicher**.
  - ⇨ Daraufhin erscheint das folgende Fenster:

17.7.4 ALARMPROTOKOLLIERUNG

Das ALARMPROTOKOLL zeigt eine Liste der Alarmereignisse an.

- Wählen Sie **Log > Logbuch > Alarm Log**.

In diesem Logbuch werden folgende Type angezeigt:

- Meldegruppen
  - Alarm
  - Überfall
- Systemereignisse
  - Best Alarm
  - Bedrohungs-PIN
  - XBUS Überfall
  - Bedrohungspin
  - RPA PANIC

17.8 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

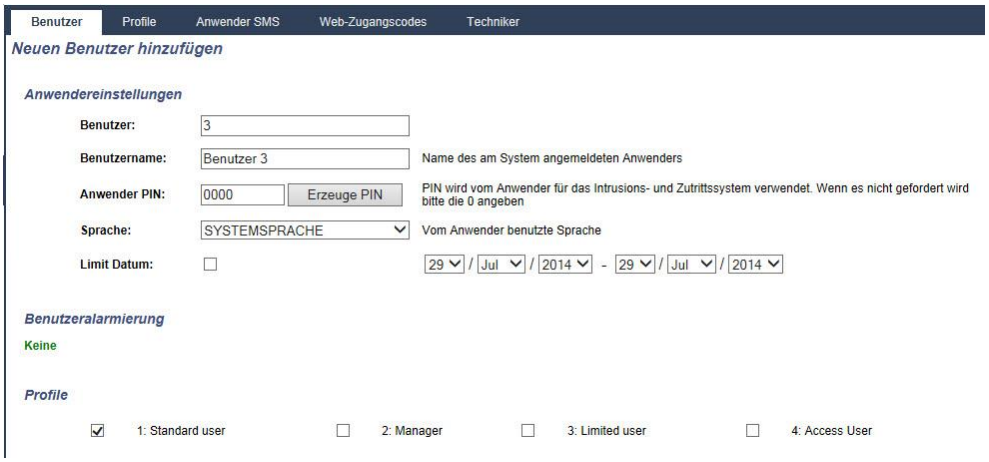
⚠ WARNUNG

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 [→ 199]). Prüfen Sie nach dem Firmware-Upgrade sämtliche Benutzerkonfigurationseinstellungen.
- Die Standard-Techniker-ID wird von 513 in 9999 geändert.

17.8.1 Hinzufügen/Bearbeiten von Benutzern

1. Wählen Sie **Benutzer > Benutzer > Benutzer hinzufügen**.
   ⇨ Eine Liste mit den konfigurierten Benutzern wird angezeigt.

2. Klicken Sie auf **Benutzer hinzufügen** oder klicken Sie neben einem Benutzer auf **Bearbeiten**.
   ⇨ Das folgende Fenster wird angezeigt.



3. Geben Sie unter **Benutzer** eine ID ein, die derzeit nicht verwendet wird. Sollten Sie eine ID eingeben, die bereits verwendet wird, wird die Meldung „ID nicht verfügbar“ angezeigt.

4. Geben Sie einen **Benutzernamen** ein (max. 16 Zeichen, mit Groß- und Kleinschreibung).
5. Klicken Sie zur automatischen Erstellung einer **Anwender-PIN** für einen neuen Benutzer auf die Schaltfläche **Erzeuge PIN**. Ändern Sie die PIN, falls erforderlich. Geben Sie 0 ein, wenn keine PIN erforderlich ist.
   ⇨ **Hinweis**: Zur Einhaltung der INCERT-Genehmigungen muss die Benutzer-PIN mehr als 4 Zeichen enthalten.
6. Sie können den Systemzugriff für diesen Benutzer auch durch Aktivieren des Kontrollkästchens **Limit Datum** und Eingabe eines Anfangs- und Enddatums in den Datumsfeldern begrenzen.
   ⇨ **Benutzer Alarme** zeigt den Status der Benutzer-PIN an. So wird z. B. angezeigt, in wie vielen Tage die PIN ungültig wird, falls in den PIN-Richtlinien des Systems die Option Regelmäßige Änderungen aktiviert ist.
7. Wählen Sie das passende Profil [→ 199] für diesen Benutzer aus.
8. Wählen Sie für diesen Benutzer, falls erforderlich, die Option **Bedrohungspin ermöglichen**. Die für Bedrohungs-PINs zugewiesene Anzahl an PINs (PIN +1 oder PIN+2) wird in System Optionen [→ 239] festgelegt.

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.

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: ● SPC4xxx - Alle Benutzer ● SPC5xxx - 512 ● SPC6xxx - 512
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

Attribut	Beschreibung
	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.

17.8.1.1 Unbekannte Geräte

Wenn ein unbekanntes Gerät, wie z. B. eine Fernbedienung, ein Transponder oder ein Ausweis, eingescannt wurde, aber keinem Benutzer zugewiesen ist, wird im betreffenden Abschnitt der Benutzerseite eine Schaltfläche angezeigt.

- Schaltfläche **Funkfernbedienung - Unbekannte Fernbedienung** oder, wenn das Gerät dem Benutzer zugewiesen ist, die Schaltfläche **Fernbedienung löschen**
- Schaltfläche **Transponder - Unbekannter Transponder** oder, wenn das Gerät dem Benutzer zugewiesen ist, die Schaltfläche **Transponder löschen**
- Zutrittskontrolle — Schaltfläche Unbekannte Karte

Um dem Benutzer eine Fernbedienung, einen Transponder oder einen Ausweis zuzuweisen:

1. Klicken Sie auf die **Unbekannt**-Schaltfläche für das jeweilige Gerät. Auf der Benutzerseite wird eine Liste mit unbekannten Geräten angezeigt.
2. Klicken Sie auf **Hinzufügen**, um das Gerät dem Benutzer zuzuweisen.

Hinweis: Um einem Benutzer eine Karte zuzuweisen, muss im zugeordneten Benutzerprofil die richtige Anlagennummer eingetragen sein.

Um die Zuweisung einer Fernbedienung oder eines Transponders zu einem Benutzer rückgängig zu machen:

1. Klicken Sie auf die Schaltfläche **Löschen**.
   Die Zuweisung des Geräts zum Benutzer wird aufgehoben und das Gerät wird aus dem System gelöscht.
2. Um das Gerät wieder hinzuzufügen, müssen Sie es erneut einscannen.

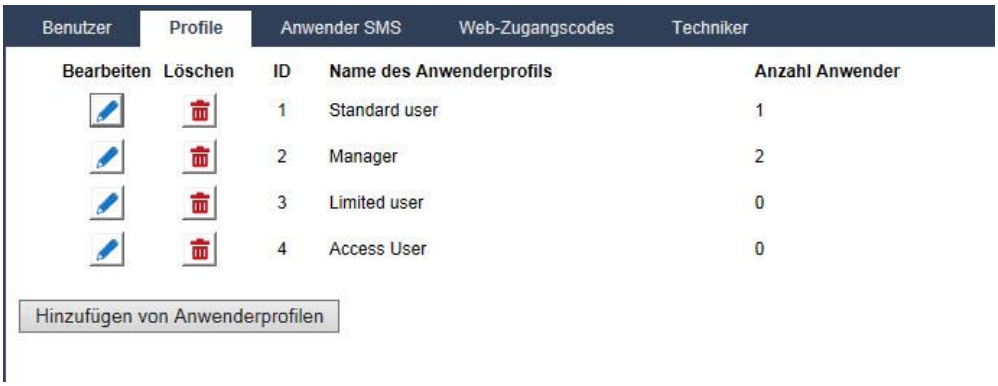
Um die Zuweisung eines Ausweises zu einem Benutzer aufzuheben:

1. Stellen Sie die Ausweisnummer auf Null (0) um.
2. Klicken Sie auf **Speichern**.
   Die Zuweisung des Ausweises zum Benutzer wird aufgehoben und der Ausweis wird aus dem System gelöscht.
3. Um den Ausweis wieder hinzuzufügen, müssen Sie ihn erneut einscannen.

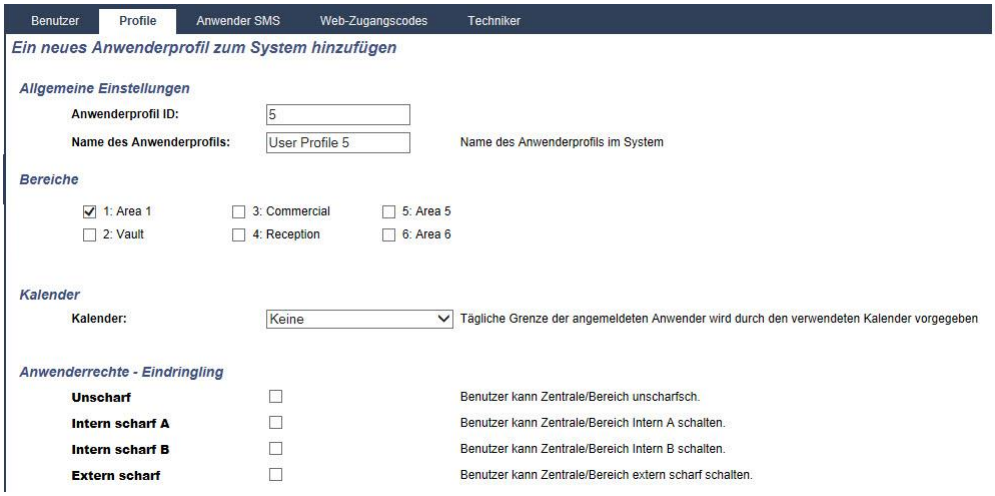
17.8.2 Hinzufügen/Bearbeiten von Profilen

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

1. Wählen Sie **Benutzer** > **Profile**.
   ⇨ Eine Liste mit konfigurierten Profilen und der Anzahl der einem Profil zugewiesenen Benutzer wird angezeigt.



2. Wählen Sie **Hinzufügen von Anwenderprofilen** oder klicken Sie für das erforderliche Profil auf **Bearbeiten**.
   Das folgende Fenster wird mit den wie folgt kategorisierten Konfigurationsoptionen angezeigt:
   - Allgemeine Einstellungen
   - Benutzer-/Systemrechte
   - Zutrittskontrolle



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
Anwenderrechte – Eindringling		
Extern Scharf	Limited Standard Manager	Im EXT SCHARF-Betrieb schaltet das Alarmsystem extern scharf und gewährleistet den umfassenden 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 OptionINTERNSCHARF 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	Die Option UNSCHARF deaktiviert den Alarm. Diese

Recht	Standard-Anwenderprofiltyp	Beschreibung
	Standard Manager	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 [→ 263]
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 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.
Anwenderrechte – System		
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 [→ 159] 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 [→ 168] 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	Hier können Benutzer ihre Benutzer-PINs ändern

Recht	Standard-Anwenderprofiltyp	Beschreibung
	Manager	[→ 160]. **Hinweis**: 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 Bedienteilsummers, 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 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.
Anwenderrechte – Steuerung		
Ausgänge	Standard Manager	Der Anwender kann konfigurierte Ausgänge ein-/ausschalten (logische Ausgänge). Siehe Bearbeiten eines Ausgangs [→ 211].
X-10	Standard Manager Zutrittskontrolle	Der Anwender kann konfigurierte X-10-Geräte ein- und ausschalten. **Hinweis:** 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.
Anwenderrechte – Test		
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.
Anwenderrechte – Service-Techniker		
Gibt dem Anwender Managerrechte		Anwender können andere Anwender im System ohne Einschränkung von Anwenderrechten erstellen und bearbeiten.

Recht	Standard-Anwenderprofiltyp	Beschreibung
Ändern von Anwenderprofilen		Anwender kann Anwenderprofile im System erstellen und ändern.
Gibt Kalenderrechte		Anwender kann Kalender konfigurieren.
Ändern der Türeinstellungen		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 [→ 383].
2. Wählen Sie die **Zutrittsberechtigungen** dieses Profils für die im System konfigurierten Türen. Verfügbare Optionen sind:
   - Kein Zutritt
   - 24 Stunden
   - Kalender (sofern konfiguriert)

Benutzer

Eine Liste mit den Benutzern, die diesem Profil zugeordnet sind, wird angezeigt. Klicken Sie auf einen Benutzer, um die entsprechenden Benutzerinformationen anzuzeigen oder zu bearbeiten.

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 [→ 200]
- Bereich hinzufügen/bearbeiten [→ 257]

17.8.3 Konfiguration von SMS

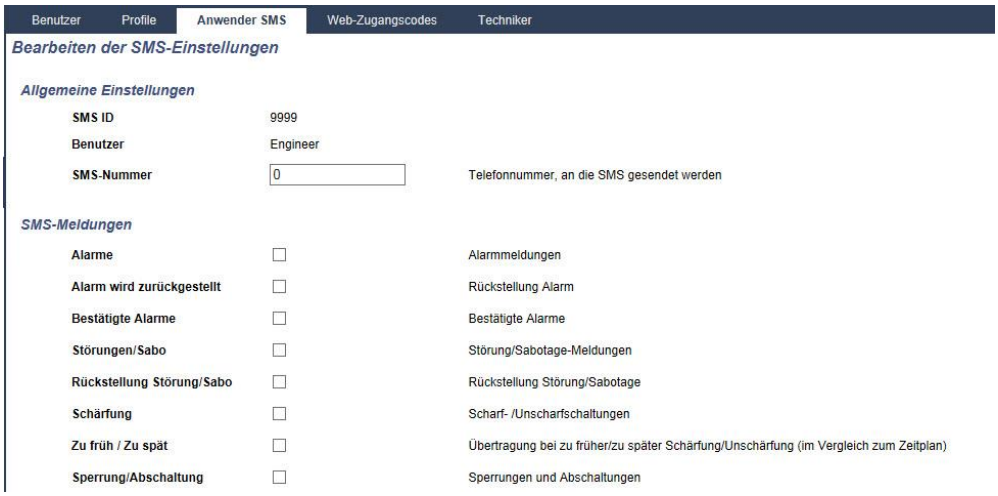
Das SPC-System unterstützt das Versenden von Textnachrichten (SMS) auf Systemen mit installierten Modems.

▷ Ein Modem ist installiert und vom System erkannt.

▷ Die Funktion **SMS-Authentifizierung** ist aktiviert. Siehe Seite [→ 239].

1. Wählen Sie **Benutzer > Anwender SMS**.
   ⇨ Die SMS ID des Technikers sowie eine Liste mit SMS IDs und den entsprechenden SMS-Informationen werden angezeigt.

2. Klicken Sie auf die Schaltfläche **Test**, um eine SMS-Nummer zu testen.
3. Klicken Sie auf **Hinzufügen**, um eine neue SMS ID hinzuzufügen oder klicken Sie neben einer SMS ID auf **Bearbeiten**.



4. 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). **Hinweis:** 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 [→ 205]

!	*HINWEIS*
	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 **C**alling **L**ine **I**dentity (CLI) am gewählten Anschluss aktiviert ist, damit Verbindungen zum SMS-Netz möglich sind. Setzen Sie sich für weitere Einzelheiten mit dem Telefonanlagenadministrator in Verbindung.

17.8.4 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 ● Bei einem System mit nur einem Bereich werden das System und der Modus ausgegeben, wenn der Modus der Scharfschaltungsstatus des Systems ist. ● Bei einem System mit mehreren Bereichen wird der Status jedes Bereichs ausgegeben.
**** XA1.AN (X10)		In den Fällen, in denen das X10-Gerät als „A1“	Status von „A1“

****.XA1.AN		konfiguriert ist, wird es eingeschaltet.	
**** 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: ● Ausgang O5 aktiv. ● Ausgang „Heizung“ aktiv (wobei „Heizung“ der Name des Ausgangs ist).
**** 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 [→ 239]	System scharf.
****.BSET (INTERN SCHARF B)		Intern B Scharfsch via SMS zulassen Es kann auch der individuelle Name eingegeben werden, der im Feld INTERNSCHARF umbenennen des Optionsfensters definiert wurde. Siehe Optionen [→ 239] Beispiel: ****.ASET NIGHT	System scharf.
****.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)

17.8.5 Löschen von Web-Zugangscodes

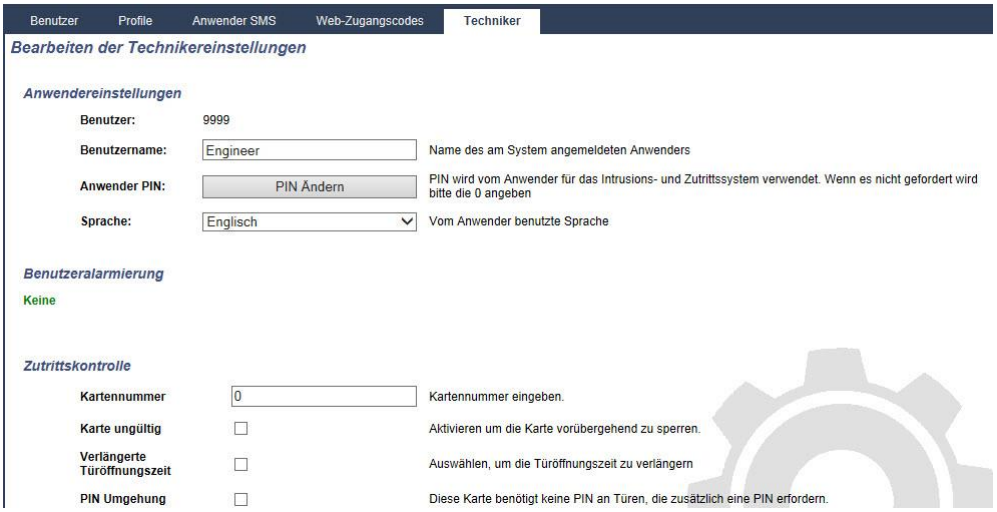
In diesem Fenster werden sämtliche Benutzer- und Techniker-Passwörter aufgelistet, die für den Zugriff über den Webbrowser erstellt wurden.

1. Wählen Sie **Benutzer > Web-Zugangscodes**.

2. Klicken Sie neben einem Benutzer oder Techniker auf die Schaltfläche **Löschen**, um das Passwort zu löschen.

17.8.6 Konfiguration der Technikereinstellungen

1. Wählen Sie **Benutzer > Techniker**.



2. Ändern Sie den **Benutzernamen** ‚Engineer', falls erforderlich.
3. Klicken Sie auf PIN Ändern [➞ 209], um die Techniker-PIN zu ändern.
   ⇨ **Hinweis**: Zur Einhaltung der INCERT-Genehmigungen muss die Benutzer-PIN mehr als 4 Zeichen enthalten.
4. Wählen Sie die **Sprache**, die vom Techniker benutzt wird. (Die Option wird nur angezeigt, wenn mehrere Sprachen verfügbar sind – siehe Upgrade von Sprachen [➞ 333])

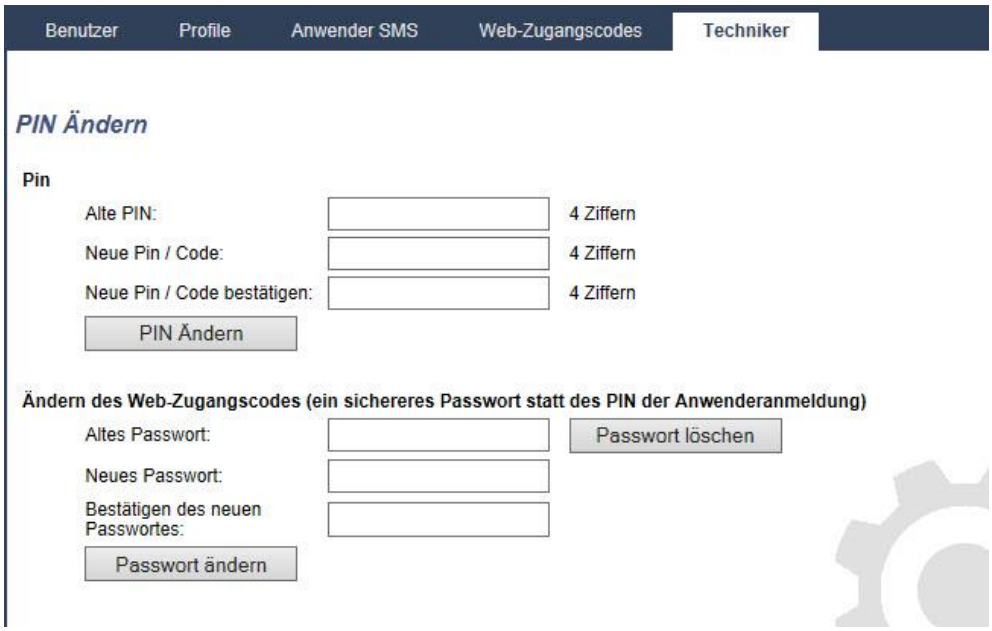
Zutrittskontrolle

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: ● SPC4xxx - Alle Benutzer ● SPC5xxx - 512 ● SPC6xxx - 512
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

Attribut	Beschreibung
	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.

17.8.6.1 Ändern von Techniker-PIN und Web-Zugangscode

In diesem Fenster können Sie die PIN ändern, die für den Zugriff auf die Zentrale verwendet wird. Weiterhin können Sie das Passwort für den Zugriff über den Webbrowser ändern (nur auf Techniker-Level).



- Ändern der PIN:

Alte PIN	Geben Sie die vorhandene Techniker-PIN ein. (Nur Ziffern)
Neue PIN/Code	Geben Sie die neue Techniker-PIN ein. (Nur Ziffern)
Neue PIN/Code bestätigen	Geben Sie die neue Techniker-PIN nochmals ein.

1. Klicken Sie auf **PIN Ändern**, um die neue PIN zu aktivieren.

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.

2. Ändern Sie den Web-Zugangscode in ein sichereres Kennwort für den Zugriff über den Webbrowser.

Neues Passwort	Geben Sie den neuen Web-Zugangscode ein (Buchstaben von A–Z, Ziffern

	von 0-9).
Neues Passwort bestätigen	Geben Sie den neuen Web-Zugangscode nochmals ein.

- Klicken Sie auf die Schaltfläche **Passwort ändern**, um das neue Passwort zu aktivieren.

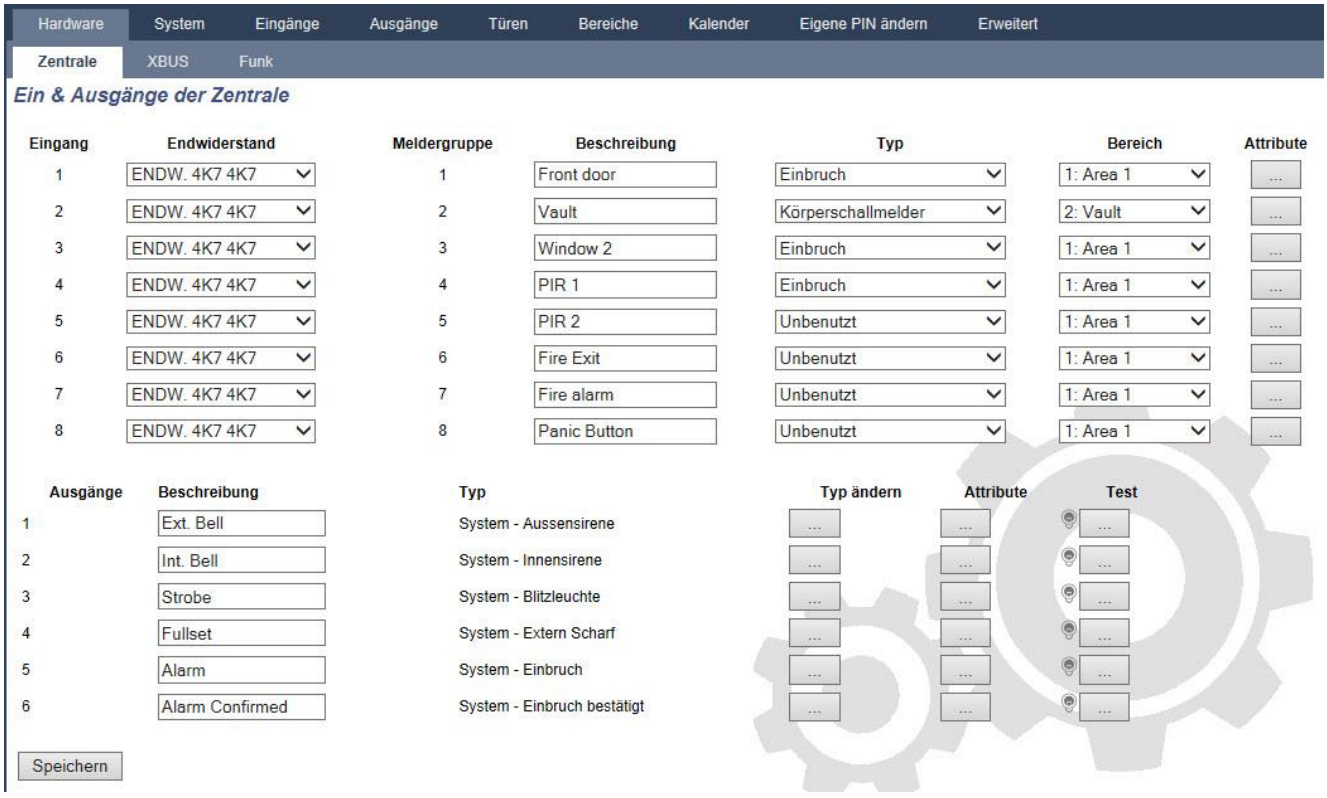
Achten Sie bei der Eingabe des neuen Passworts auf die Groß- bzw. Kleinschreibung der Zeichen.

17.9 Konfiguration

17.9.1 Ein-/Ausgänge der Zentrale konfigurieren

17.9.1.1 Ausgang bearbeiten

1. Wählen Sie **Konfiguration > Hardware > Controller**.
   ⇨ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



Eingang	Diese Nummer wird als Referenz angezeigt und kann nicht programmiert werden.
Endwiderstand	Wählen Sie den Endwiderstand für den MG-Eingang (Werkseinstellung: 4K7).
Analyzed (Pro)	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

Pro	Vibrations-/Stoßmelder ausgelöst wird.
Gross Attack Pro	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 [➞ 375]).
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 [➞ 211]).

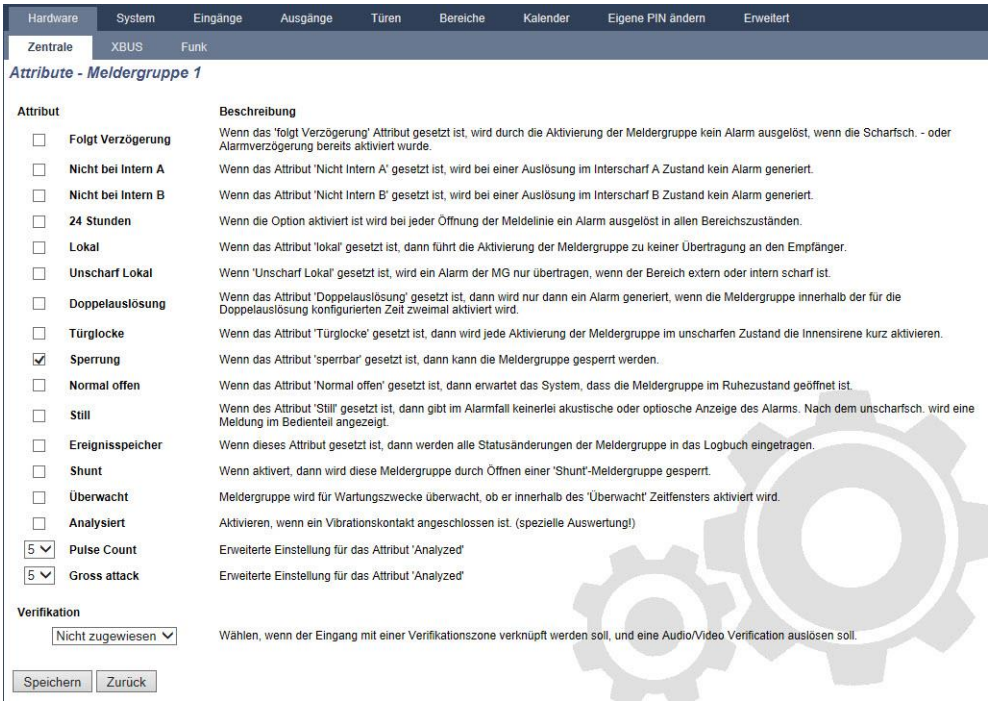
17.9.1.1.1 MG-Einstellungen: Attribute

Jeder Meldergruppe der SPC kann ein Attribut zugewiesen werden, das die Eigenschaften dieser Meldergruppe bestimmt.

Zuweisen eines Attributs zu einer Meldergruppe:

1. Wählen Sie **Konfiguration > Hardware > Controller > Attribute**.

   ⇨ Daraufhin erscheint das folgende Fenster:



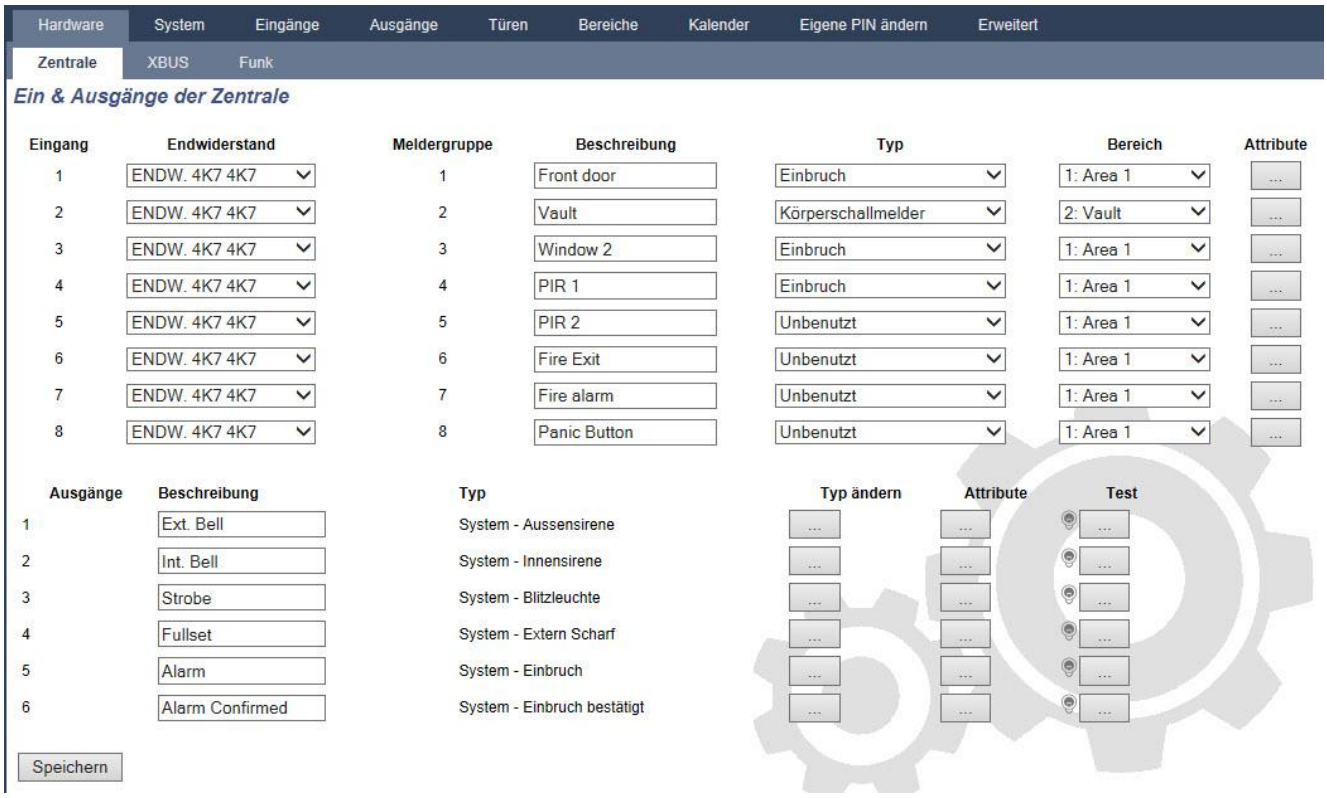
2. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Attribut.

Die auf dieser Seite angezeigten Attribute hängen vom ausgewählten Meldergruppen-Typ ab. Eine Liste der zuweisbaren Attribute finden Sie auf Seite [➞ 381].

17.9.1.2 Bearbeiten eines Ausgangs

1. Wählen Sie **Konfiguration > Hardware > Controller**.

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



Ausgangstyp	● **Systemausgang**: Wählen Sie den Typ aus dem Dropdown-Menü. (Siehe Ausgangstypen und Ausgangsschnittstellen [→ 213].) ● **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 [→ 213].) ● **Meldergruppe**: Wählen Sie die Meldergruppe, die zugewiesen werden soll. ● **Log Ausgang**: Wählen Sie den logischen Ausgang, der zugewiesen werden soll. ● **Türausgang**: Wählen Sie die Türnummer und den Systemausgangstyp für die Tür. (Siehe Ausgangstypen und Ausgangsschnittstellen [→ 213].) ● **Schlüsselsch.**: Wählen Sie die Erw-ID für den erforderlichen Schlüsselschalter und die erforderliche Schlüsselstellung, die diesem Ausgang zugewiesen wird.
Beschreibung	Geben Sie hier einen Beschreibungstext für den Ausgang ein (max. 16 Zeichen). Dieser Text erscheint auch im Browser und im Bedienteil.
Ausgangskonfiguration	● **Modus**: 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. ● **Erneute Ausl.**: Aktivieren Sie dieses Kontrollkästchen, um den kurzzeitigen Ausgang erneut auszulösen. ● **AN-Zeit**: Geben Sie die AN-Zeit für kurzzeitige und pulsierende Ausgänge ein. ● **AUS-Zeit**: Geben Sie die AUS-Zeit für kurzzeitige und pulsierende Ausgänge ein. ● **Invertieren**: Aktivieren Sie dieses Kontrollkästchen, um den physischen Ausgang zu invertieren. ● **Log**: Aktivieren Sie dieses Kontrollkästchen, um die Zustandsänderungen des Ausgangs im Logbuch zu erfassen. ● **Kalender:** Wählen Sie bei Bedarf den gewünschten Kalender. Siehe Seite [→ 273].

Siehe auch

Kalender [→ 273]

17.9.1.2.1 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 [→ 375]) 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	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-). **Hinweis**: Ein Außensirenen-Ausgang wird automatisch aktiviert, sobald eine als Alarm-MG programmierte MG im Modus Extern Scharf oder Intern Scharf auslöst.
Blitzleuchte	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). **Hinweis**: 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-). **Hinweis**: 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 [→ 216]). 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-Meldegruppe 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: ● zwei Aktivierungen von Bedrohungs-MGs, die mehr als zwei Minuten auseinander liegen ● eine Aktivierung einer Bedrohungs-MG und eine Aktivierung einer Panik-MG, die mehr als zwei Minuten auseinander liegen ● Wenn in dem zweiminütigen Zeitraum eine Bedrohungs- und Sabotage-MG oder eine Panik-MG und Sabotage-MG aktiviert werden
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).*

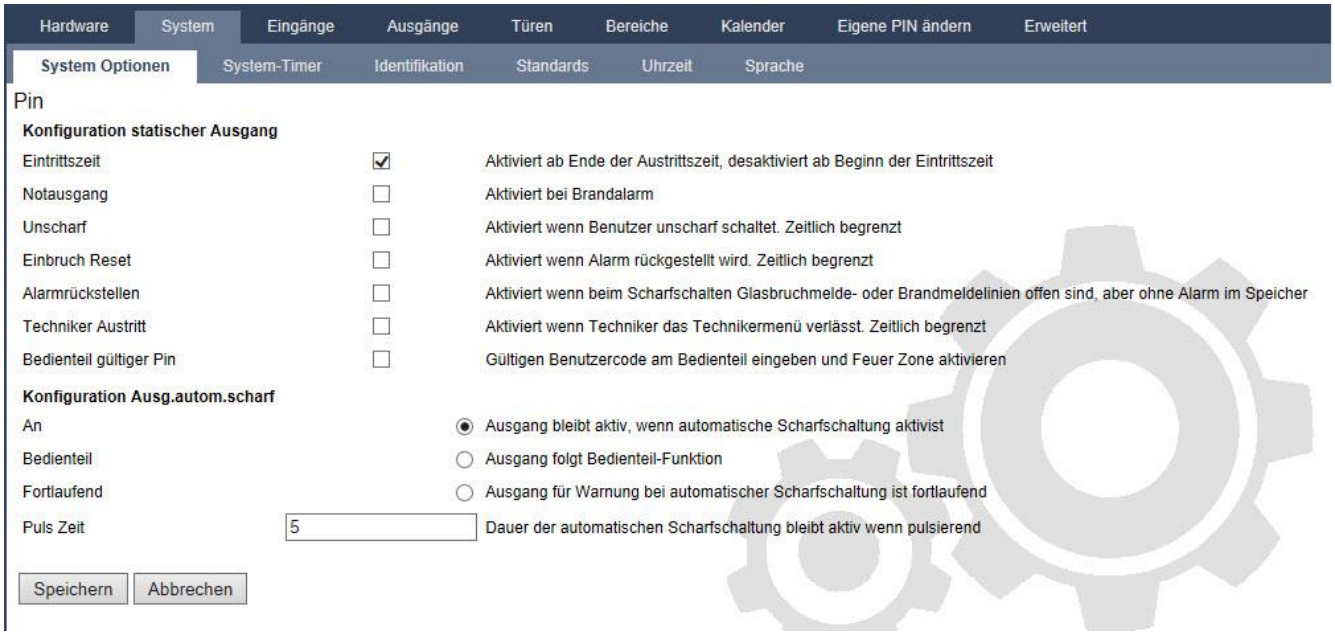
Siehe auch

Konfiguration der Ausgänge für Systemverzögerung und automatische Scharfstellung [→ 216]

17.9.1.3 Konfiguration der Ausgänge für Systemverzögerung und automatische Scharfstellung

- Klicken Sie unter **Richtlinie** auf **Bearbeiten** und unter **Systemoptionen** auf die Option **Konfiguration Ausgang**.

⇨ Der folgende Bildschirm wird angezeigt:



- 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.

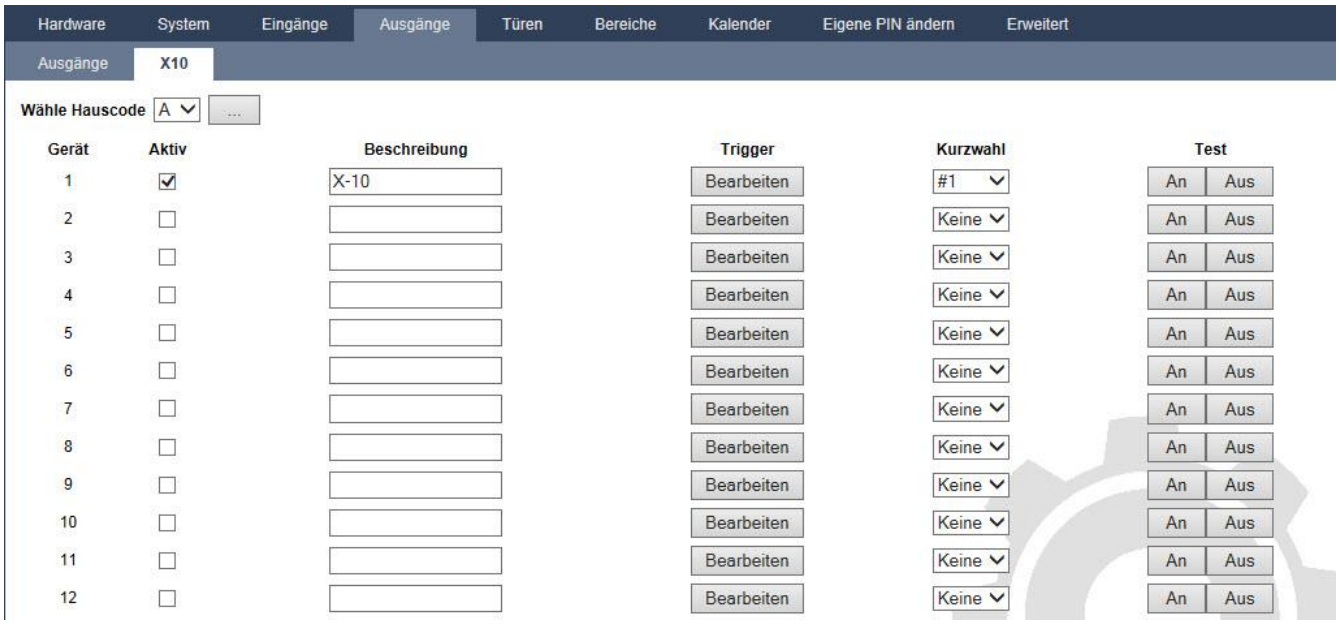
Ein	Der Ausgang bleibt aktiv, wenn die automatische Scharfschaltung aktiv ist.
Bedienteil	Der Ausgang folgt der Bedienung am Bedienteil.
Fortlaufend	Der Ausgang warnt fortlaufend vor der automatischen Scharfschaltung.
Puls Zeit	Wählen Sie die Zeitspanne aus, während der der Ausgang für automatische Scharfschaltung aktiv bleibt, wenn er gepulst wird.

17.9.1.4 X10 Konfiguration - Einstellungen

Im X10-Einstellungsfenster können Sie die Funktionsweise von X10 auf der Zentrale konfigurieren.

1. Wählen Sie **Konfiguration > Ausgänge > X10**.
   ⇨ Daraufhin erscheint das folgende Fenster:

2. Aktivieren Sie das Kontrollkästchen **Aktivieren**, um den X10 in der Zentrale zu aktivieren.
3. Aktivieren Sie das Kontrollkästchen **Log**, um das Protokollieren aller X10-Ereignisse in der Zentrale zu aktivieren.
4. Klicken Sie auf **Speichern**.
5. 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:



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).
Kurzwahl	Dieses Feld zeigt an, ob die X10-Geräteaktivierung durch die Eingabe eines Codes auf dem Bedienteil möglich ist.

Bearbeiten eines X-10-Geräts

1. Klicken Sie auf **Bearbeiten**.
   ⇨ Daraufhin erscheint das folgende Fenster:

2. Informationen zu weiteren Programmierschritten siehe Seite [→ 277].

17.9.2 X-BUS-

17.9.2.1 Erweiterungen

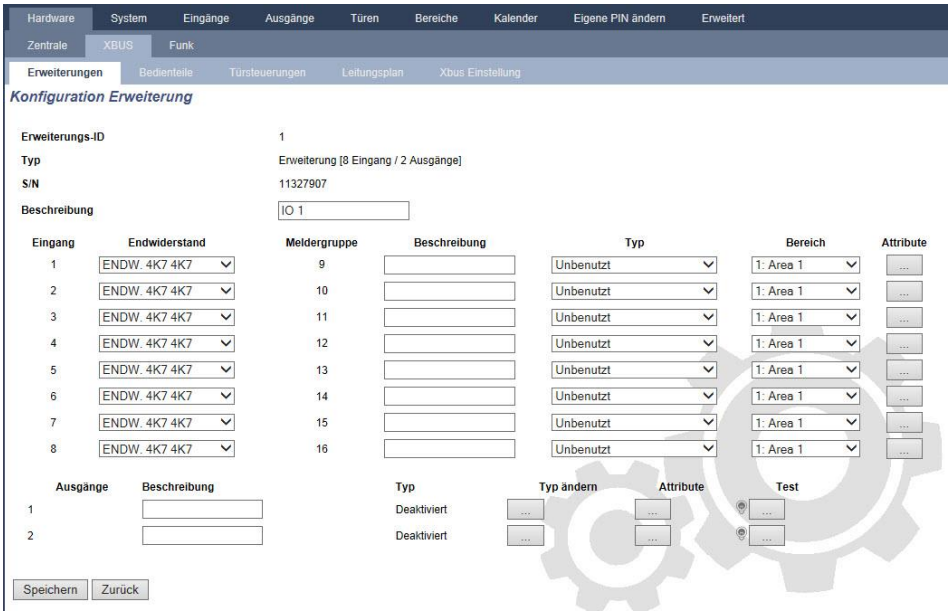
1. Wählen Sie **Konfiguration > Hardware > X-Bus > Erweiterungen**.
   ⇨ Daraufhin erscheint das folgende Fenster:

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.

2. Klicken Sie auf einen der Parameter der Erweiterung, um das Fenster **Konfiguration Erweiterung** anzuzeigen.



- Konfigurieren Sie die folgenden Felder:

Beschreibung	Zur Anzeige auf Geräte-LEDs.
Lautstärken-Limit	**Nur Verifikationsmodul**: Lautstärke für das Verifikationsmodul und Satelliten (WAC 11). Sie sind alle parallel geschaltet. Beachten Sie, dass der Lautsprecher an WAC 11 über ein Potenziometer für die Feinregulierung der Lautstärke verfügt. Der Regelbereich ist 0 (Min.) – 7 (Max.) bzw. deaktiviert.
Zusatz-Lautsprecher/Mikrofon	**Nur Verifikationsmodul**:Diese Option sollte aktiviert sein, wenn an dieses Modul Satelliten (WAC 11) angeschlossen sind. **Hinweis**: Wird diese Option aktiviert, werden die Satelliten-Mikrofone mit Strom versorgt. Die Satellitenlautsprecher sind unabhängig von dieser Einstellung immer aktiviert.
Endwiderstand	Wählen Sie den korrekten Endwiderstand (Werkseinstellung: DEOL 4K7). Diese Einstellung muss der tatsächlichen Verdrahtung des Eingangs am Controller oder Erweiterungsmodul entsprechen. Siehe Seite [→ 74].
(MG-) Beschreibung	Beschreibung für eine zugewiesene Meldergruppe eingeben.
(MG-) Typ	Meldergruppentyp wählen. Siehe Seite [→ 378].
Bereich	Bereich wählen.
Attribute	Attribute nach Wunsch zuweisen. Siehe Seite [→ 375].
Ausgänge/Netzteilausgänge (NUR für SPCP355 Smart-Netzteil angezeigt)	
Ausgang	Der nummerierte Ausgang. Der Wert in Klammern entspricht dem physischen Ausgang auf der Netzteilplatine.
Beschreibung	Beschreibung für den Ausgang eingeben.
Typ ändern	Ggf. Ausgangstyp ändern.
Attribute	Dem Ausgang Attribute zuweisen.
Test	Ausgang testen.
Beobachte Ausgang	Wählen Sie aus, welche Ausgänge überwacht werden sollen. **Hinweis**: Der Parallelwiderstand, die Diode und die erforderliche Last müssen angewendet werden, bevor diese Option aktiviert wird. Das SPCP355 muss vor Beginn der Überwachung eine Kalibrierung durchführen. Weitere Informationen finden Sie unter Überwachte Ausgänge [→ 59]
Nur Primärbatterie	Aktivieren Sie dieses Kontrollkästchen, wenn keine sekundäre Batterie an das Netzteil angeschlossen ist.

Wenn Erweiterungen hinzugefügt oder entfernt werden:

- Klicken Sie auf **Neu Konfigurieren**, um Änderungen zu übernehmen.

Siehe auch

- Verdrahtung des Systems [→ 74]
- MG-Attribute [→ 378]
- Meldergruppentypen [→ 375]

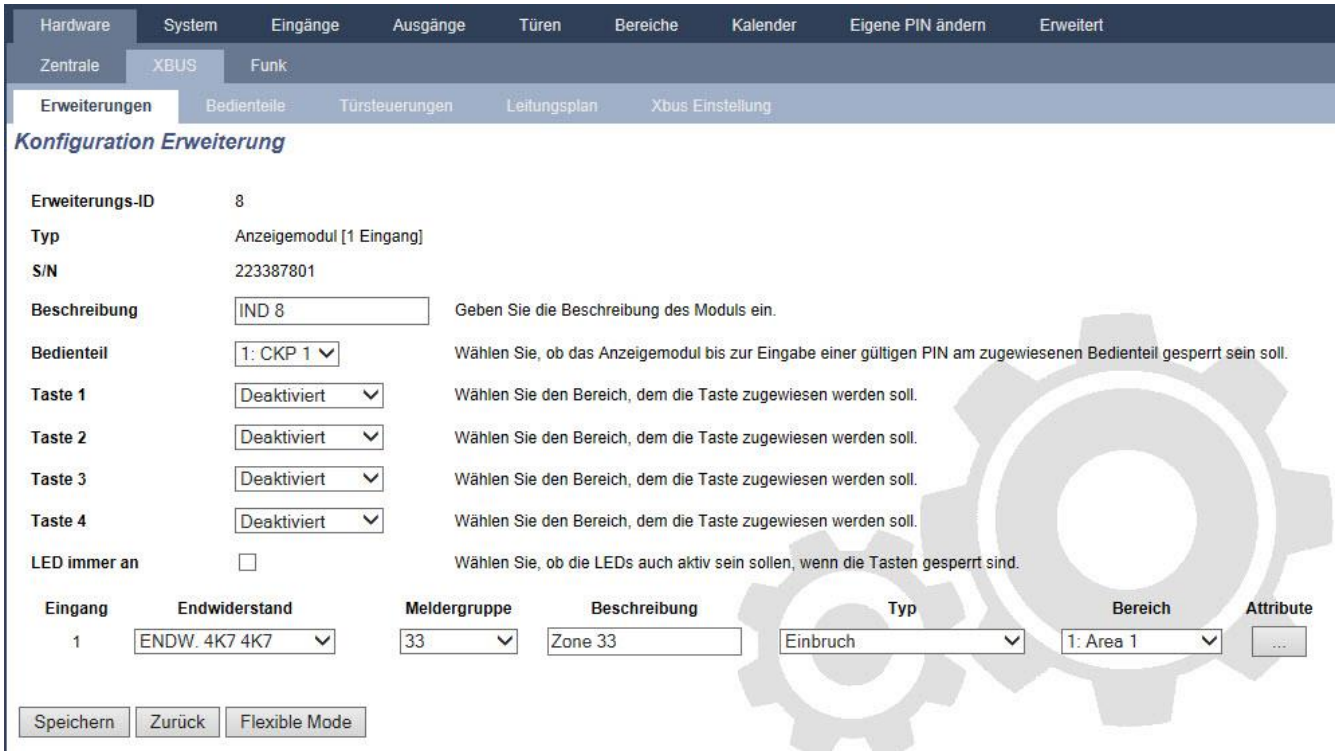
17.9.2.1.1 Konfigurieren eines Anzeigemoduls

Es gibt zwei mögliche Konfigurationsmodi für die Anzeigeerweiterung:

- Betriebsart "Linked Mode"
- Flexible Mode

1. Wählen Sie **Konfiguration > Hardware > X-Bus > Erweiterungen**.
2. Klicken Sie auf einen der ID-Parameter des Anzeigemoduls.

⇨ Das nachstehende Fenster für die **Linked Mode**-Konfiguration wird angezeigt.



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.

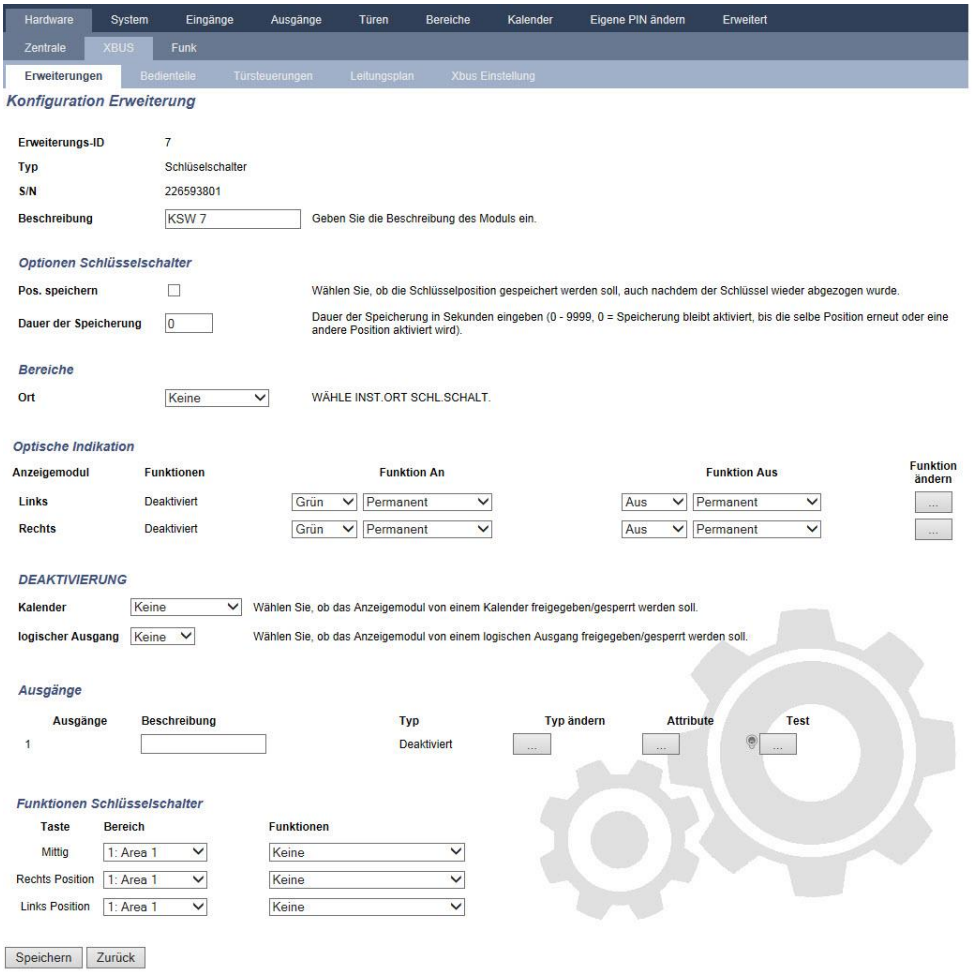
⚠ WARNUNG

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.
Optische Indikation	
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.
Akustische Indikationen	
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.
Deaktivierung	
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.

17.9.2.1.2 Konfigurieren eines Schlüsselschalter-Erweiterungsmoduls

1. Wählen Sie **Einstellungen > X-Bus > Erweiterungen**.
2. Klicken Sie auf einen der ID-Parameter des Schlüsselschalters.
   ⇨ Das folgende Dialogfeld wird angezeigt.



- Konfigurieren Sie die in der untenstehenden Tabelle beschriebenen Felder.

Beschreibung	Geben Sie einen Namen für die Schlüsselschalter-Erweiterung ein.
Schlüsseloptionen	
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).
Bereiche	
Adresse	Wählen Sie den Bereich aus, in dem das Bedienteil montiert ist.
Optische Anzeigen	
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.
Deaktivierung	
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.
Ausgang	
Ausgang *x*	Konfigurieren Sie die Ausgänge für den Schlüsselschalter und geben Sie sie ein. Siehe Ausgänge [→ 212] für weitere Einzelheiten.
Funktionen Schlüsselschalter	
Stellungen: Mitte, Rechts und Links	Wählen Sie die **Funktion**, die bei dieser Schlüsselschalterstellung ausgeführt werden soll, sowie den betreffenden **Bereich**.

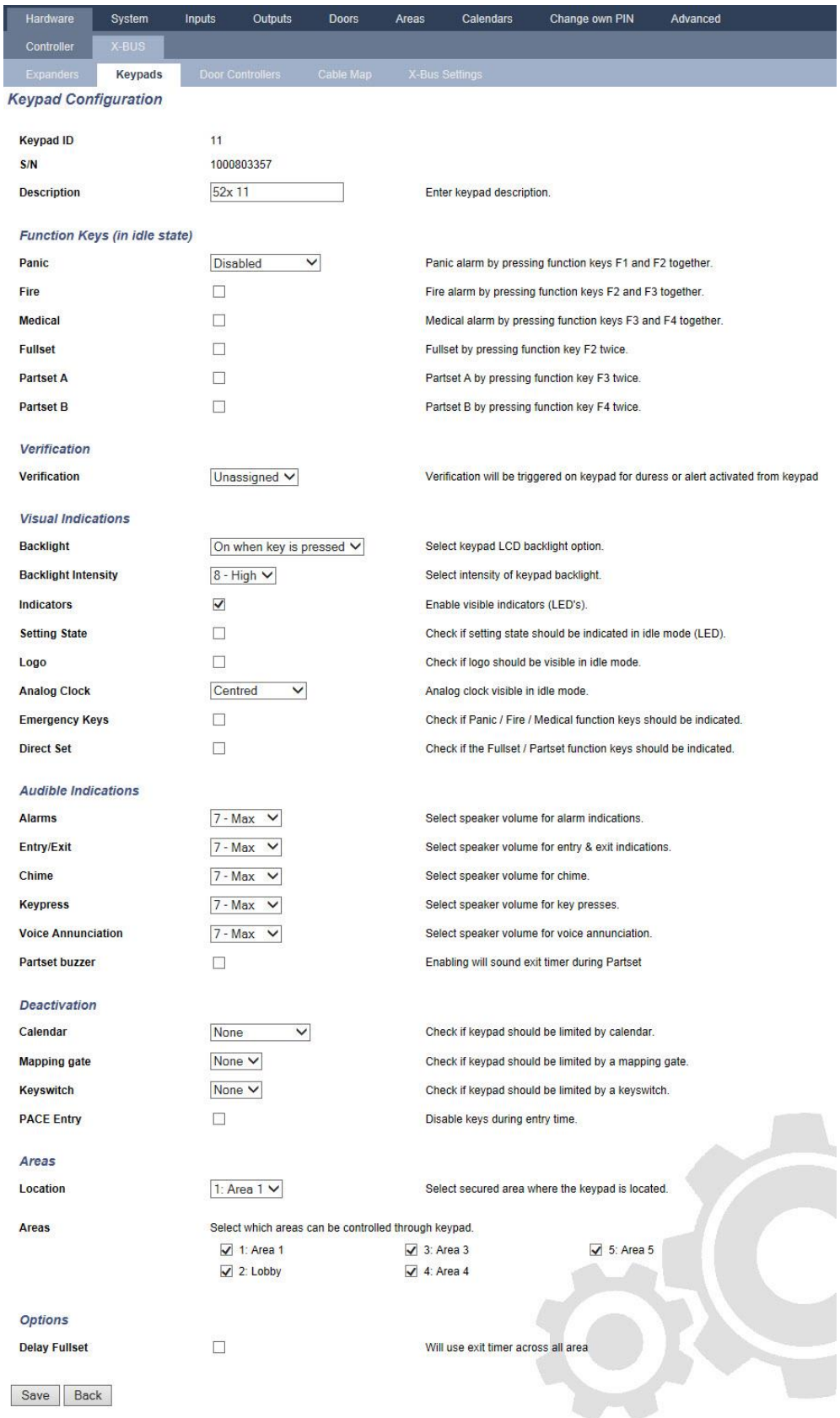
⚠ WARNUNG

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

17.9.2.2 Bedienteile

17.9.2.2.1 Bearbeiten eines Standard-Bedienteils

1. Wählen Sie **Konfiguration > Hardware > X-Bus > Bedienteile**.
2. Klicken Sie auf einen der ID-Parameter des Standard-Bedienteils.
3. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



Beschreibung	Geben Sie einen eindeutigen Namen für das Bedienteil ein.
Einstellungen der Funktionstasten (im Ruhezustand)	

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 Bedrohungscodes ein Panikalarm ausgelöst wird.
Optische Anzeigen	
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 Schärfungsstatus im Bereitschaftszustand angezeigt werden soll.
Akustische Indikationen	
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.
Deaktivierung	
Kalender	Wählen Sie, ob die Aktivierung des Bedienteils nur während der im Kalender eingestellten Zeit möglich sein soll. Siehe Kalender [→ 273].
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.
Bereiche	
Ort	Wählen Sie, ob das Bedienteil in einem gesicherten Bereich montiert ist.
Bereiche	Wählen Sie die Bereiche, die über das BT gesteuert werden dürfen.
Optionen	
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 [→ 273]

17.9.2.2.2 Bearbeiten eines Komfort-Bedienteils

1. Wählen Sie **Konfiguration > Hardware > X-Bus > Bedienteile**.

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

Hardware | System | Eingänge | Ausgänge | Türen | Bereiche | Kalender | Eigene PIN ändern | Erweitert

Zentrale | XBUS | Funk

Erweiterungen | Bedienteile | Türsteuerungen | Leitungsplan | Xbus Einstellung

Konfiguration Bedienteil

Bedienteil-ID	1	
S/N	227361801	
Beschreibung	CKP 1	Beschreibung des Bedienteils eingeben

Einstellungen der Funktionstasten (im Ruhezustand)

Überfall	Deaktiviert	Überfallalarm auslösen durch gleichzeitiges Drücken der Funktiontasten 1 & 2.
Feuer	☐	Feueralarm auslösen durch gleichzeitiges Drücken der Funktiontasten 2 & 3.
Medizin	☐	Medizinischen Notfall auslösen durch gleichzeitiges Drücken der Funktiontasten 3 & 4.
Extern scharf	☐	Externe Scharfsch. durch zweimaliges Drücken der Funktionstaste 2
Intern scharf A	☐	Intern A Scharfsch. durch zweimaliges Drücken der Funktionstaste 3
Intern scharf B	☐	Intern B Scharfsch. durch zweimaliges Drücken der Funktionstaste 4

Verifikation

Verifikation	Nicht zugewiesen	Verifikation am Bedienteil wird angestoßen für Bedrohungen oder Störungen, die am Bedienteil aktiviert wurden

Optische Indikation

Hintergrundbel.	An bei Tastendruck	Wählen Sie die Option für die LCD-Hintergrundbeleuchtung
Intensität der Hintergrundbel.	8 - Stark	Wählen Sie die Intensität der Hintergrundbeleuchtung.
LED-Anzeigen	☑	Sollen die LEDs des Bedienteils im Ruhezustand aktiv sein.
Schärfungszustand	☐	Wählen Sie, ob der Schärfungszustand im Ruhezustand des Bedienteils angezeigt werden soll (LED).
Logo	☐	Wählen, ob das Logo im Ruhezustand angezeigt wird.
Analoge Uhr	Mittig	Analoge Uhr im Ruhezustand
Notfall	☐	Wählen Sie, ob die Funktionstasten für Überfall/Feuer/Med. Notfall im Ruhezustand des Bedienteils angezeigt werden sollen.
Direkte Scharfsch.	☐	Wählen Sie, ob die Funktionstasten für Ext./Intern scharf im Ruhezustand des Bedienteils angezeigt werden sollen.

Akustische Indikation

Alarme	6	Wählen Sie die Lautstärke für Alarme.
Verzögerung	6	Wählen Sie die Lautstärke der Verzögerungen.
Türglocke	6	Wählen Sie die Lautstärke der Türglocke.
Tastentöne	2	Wählen Sie die Lautstärke der Tastentöne.
Sprachausgabe	Deaktiviert	Wählen Sie die Lautstärke der Sprachausgabe.
Summer bei int.scharf	☐	Aktivierung der akustischen Austrittsverzögerung bei Intern scharf

DEAKTIVIERUNG

Kalender	Keine	Wählen Sie, ob das Bedienteil von einem Kalender gesperrt/freigegeben werden soll.
logischer Ausgang	Keine	Wählen Sie, ob das Bedienteil von einem logischen Ausgang gesperrt/freigegeben werden soll.
Schlüselschalter	Keine	Wählen Sie, ob das Bedienteil von einem Schlüsselschalter gesperrt/freigegeben werden soll.
Eintritt nur mit Transponder	☐	Tasten während der Alarmverz. sperren

Bereiche

Ort	1: Area 1	Wählen Sie, ob das Bedienteil in einem gesichteren Bereich montiert ist.

Bereiche — Wählen Sie die Bereiche, die durch das Bedienteil bedient werden dürfen.

☑ 1: Area 1	☑ 3: Commercial	☑ 5: Area 5
☑ 2: Vault	☑ 4: Reception	☑ 6: Area 6

Optionen

Verzögerung extern scharf	☐	Verzögerung extern scharf für alle Bereiche

Speichern | Zurück

Beschreibung	Geben Sie einen eindeutigen Namen für das Bedienteil ein.
Einstellungen der Funktionstasten (im Ruhezustand)	
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 Feueralarm 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 Feueralarm ausgelöst wird oder wenn ein Benutzer einen Bedrohungscode eingibt.
Optische Indikationen	
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.
Akustische Indikationen	
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)

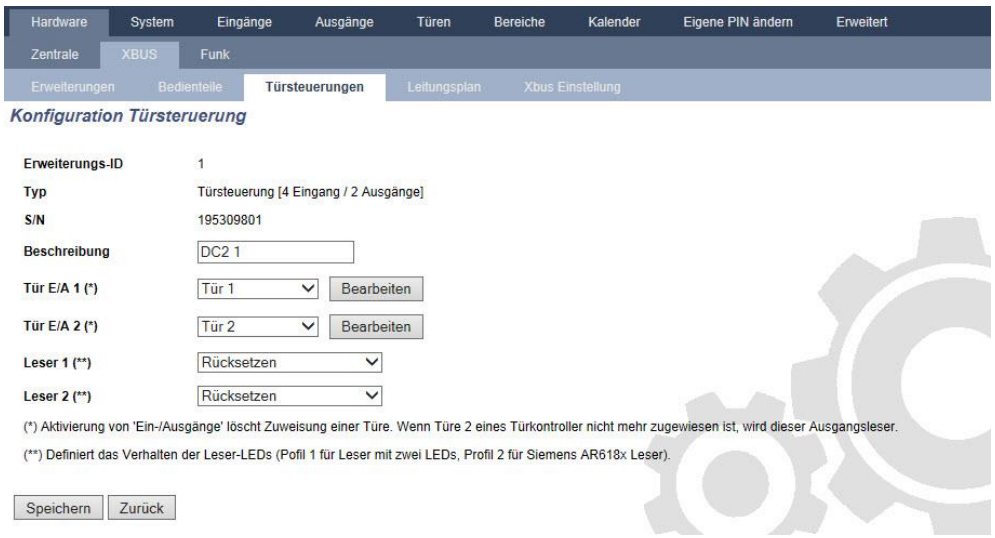
Deaktivierung	
Kalender	Wählen Sie, ob die Aktivierung des Bedienteils nur während der im Kalender eingestellten Zeit möglich sein soll. Siehe Kalender.
Logischer Ausgang	Wählen Sie, ob das Bedienteil durch einen logischen Ausgang beschränkt werden soll.
Schlüsselsch.	Wählen Sie, ob das Bedienteil nur 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.
Bereiche	
Ort	Wählen Sie, ob das Bedienteil in einem gesicherten Bereich montiert ist.
Bereiche	Wählen Sie die Bereiche, die über das BT gesteuert werden dürfen.
Optionen	
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.

17.9.2.3 Türsteuerungen

17.9.2.3.1 Türsteuerung bearbeiten

1. Wählen Sie **Konfiguration > Hardware > X-Bus > Türsteuerungen**.
2. Klicken Sie auf eine der blau markierten Angaben (z. B. die Seriennummer).
3. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



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 Tür E/A 2	● Wird eine Tür dem Tür E/A zugewiesen, entsprechende Türnummer auswählen. **Ein-/Ausgänge** wählen, wenn die beiden Ein- und Ausgänge konfigurierbar sind. ● Wurde für den Tür E/A eine Türnummer ausgewählt, können die Türeinstellungen durch Anklicken der Schaltfläche „Bearbeiten“ geändert werden. Dies entspricht dem Menüpfad **Einstellungen > Türen**. ● Wurde **MG / Optionen** ausgewählt, können die beiden MG und der Ausgang durch Anklicken der Schaltfläche „Bearbeiten“ konfiguriert werden.
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 [→ 266].
4. Um die Eingänge verwenden zu können, müssen sie eine MG-Nummer zugewiesen werden.

17.9.2.4 Leitungsplan

Anzeigen einer Liste der Erweiterungen/Bedienteile in der Reihenfolge, in der sie im SPC-System konfiguriert sind:

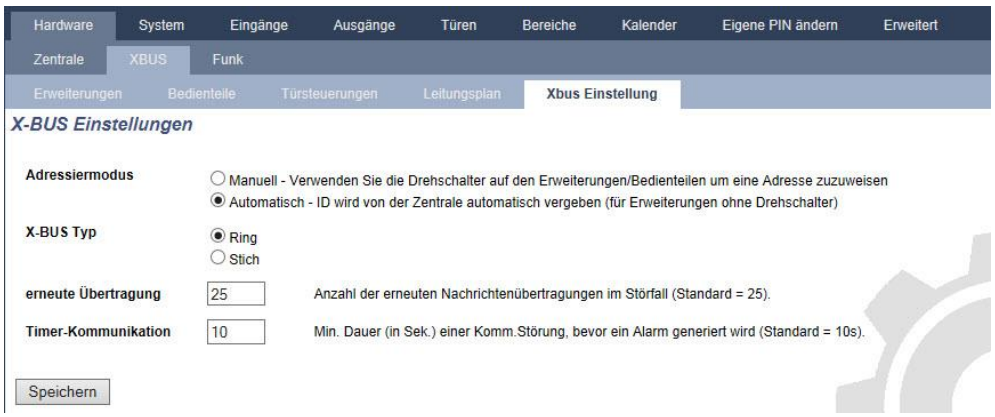
- Wählen Sie **Konfiguration > Hardware > X-Bus > Leitungsplan**.
  ⇨ Daraufhin erscheint das folgende Fenster:

Weitere Informationen zu X-BUS-Schnittstellen finden Sie auf Seite [→ 74].

17.9.2.5 Einstellungen

Konfigurieren von X-BUS-Verbindungen:

1. Wählen Sie **Konfiguration > Hardware > X-Bus > Xbus Meldelinien**.
   ⇨ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

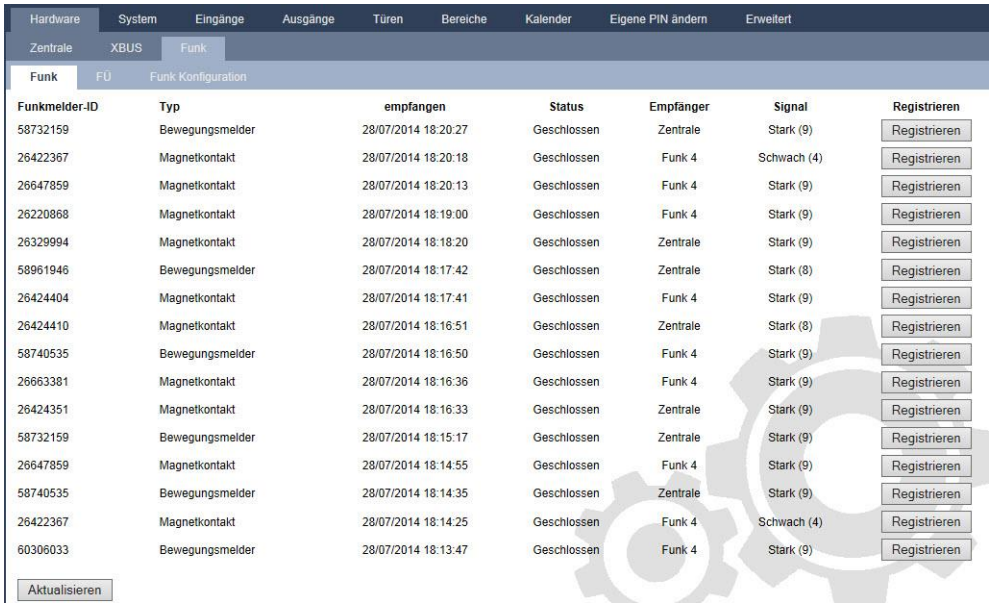


Adressiermodus	Bestimmen Sie, ob die Erweiterungen/Bedienteile im X-BUS manuell oder automatisch adressiert werden sollen.
X-BUS-Typ	Wählen Sie zwischen durchschleifbarer und Stichleitungskonfiguration.
Erneute Übertr.	Anzahl der erneuten Daten-Übertragungsversuche des Systems über die X-BUS-Schnittstelle, bevor ein Kommunikationsfehler ausgegeben wird. (1 – 99: Standard = 25).
Timer-Kommunikation	Zeitspanne, die verstreicht, bis ein Kommunikationsfehler aufgezeichnet wird.

17.9.3 Funk

Die Funkmeldererkennung (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. Wählen Sie **Konfiguration > Hardware > Funk > Funk**.
2. Weitere Informationen finden Sie in der nachstehenden Tabelle.



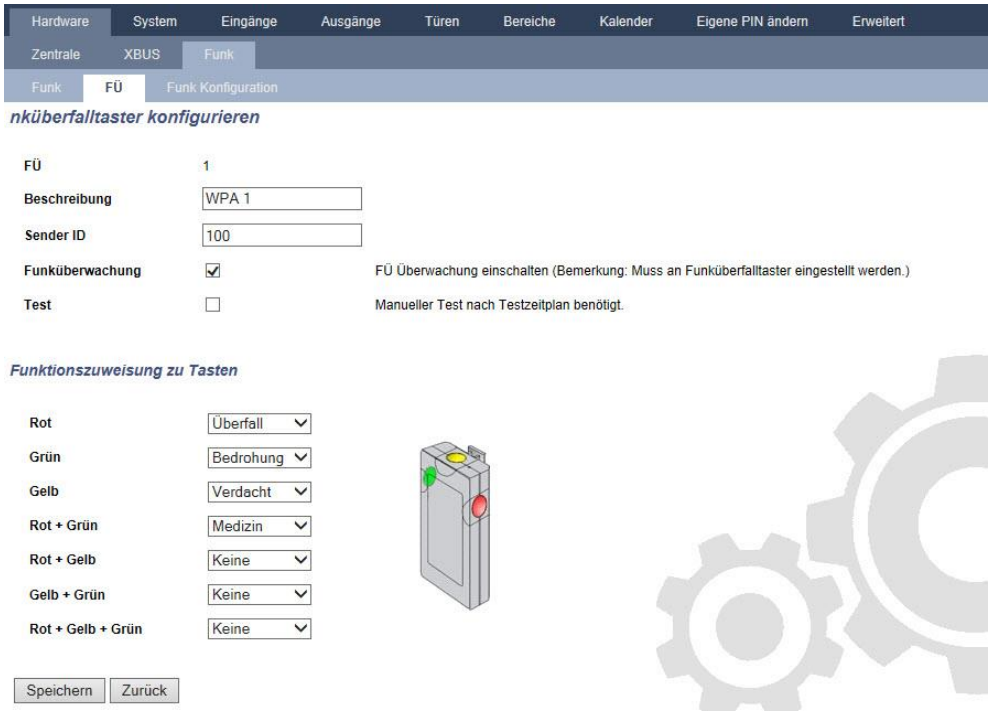
Funkmelder	Die Nummer des im System angemeldeten Melders (1 = erster, 2 = zweiter usw.)
ID	Eine eindeutige ID für den Melder.
Typ	Typ des erkannten Funkmelders (Magnetkontakt, Vibration/Stoß usw.)

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). **Hinweis:** 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

Log (Protokoll)	Anklicken, um das Protokoll des Funksensors anzuzeigen. Siehe Seite [→ 234].
Einlernen	Klicken Sie auf diese Option, um die Liste mit abgemeldeten Funkgeräten zu öffnen.

1. Wählen Sie **Status > Hardware > Funk > WPA**.
2. Die Identität jedes eingelernten FÜ und der Status werden angezeigt.



17.9.3.1 Log - Funkmelder X

Anzeigen eines Ereignisprotokolls für einen Funkmelder:

1. Klicken Sie auf die Schaltfläche **Log**.
2. Weitere Informationen finden Sie in der nachstehenden Tabelle.
3. Erstellen Sie eine Textdatei des Logs durch Klicken auf **Textdatei** .

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).

17.9.3.2 Konfigurieren eines FÜ

	HINWEIS
	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.

Ein FÜ wird keinem Benutzer zugewiesen. Ein FÜ wird in der Regel von mehren 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.

Konfigurieren eines FÜ über den Browser:

- Wählen Sie den Konfigurationsmodus und die Optionen **Konfiguration > Hardware > Funk > FÜ**.

Auf dieser Seite können folgende Elemente überprüft bzw. konfiguriert werden:

- **Batteriezustand**

  Die Zentrale empfängt vom FÜ mit jedem Datensatz eine Meldung zum Batteriezustand. Der Batteriezustand ist entweder „Ok“ oder „Niedrig“.

  Die Überwachung des Batteriezustands ist nur bei einem FÜ mit einer Contoller-Leiterplatine der Änderungsversion E-PC138612 oder höher möglich.

- **Funküberwachung**

  Die Funküberwachung kann einen der folgenden Zustände annehmen:

  – Störung
  Die Zentrale hat in dem Zeitraum, der auf der Seite für die Funkeinstellungen konfiguriert wurde, keine Überwachungsmeldung vom FÜ erhalten.

  – Deaktiviert
  Die Überwachung ist nicht konfiguriert.

  – Ok
  Die Überwachungsmeldungen werden normal übertragen.

- **Status**
  Der Teststatus kann einen der folgenden Zustände annehmen:
  – Überfällig
  Der FÜ wurde in dem Zeitraum, der auf der Seite für die Funkeinstellungen konfiguriert wurde, nicht getestet.
  – Deaktiviert
  Die Überwachung ist nicht konfiguriert.
  – OK
  Der FÜ-Test ist in Ordnung.

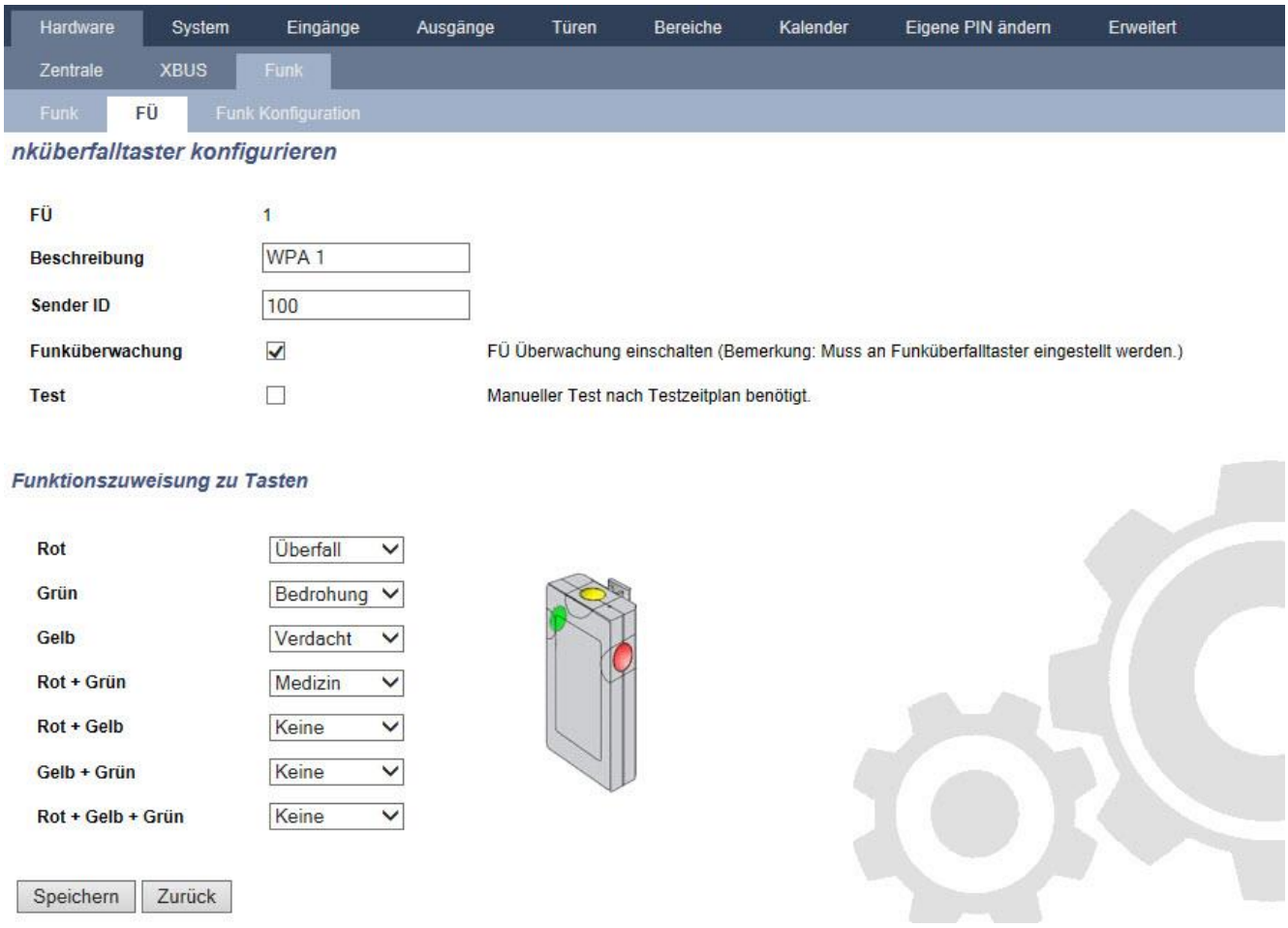
1. Klicken Sie auf **Bearbeiten**, um die FÜ-Konfiguration zu bearbeiten.
2. Klicken Sie auf **Löschen**, um einen FÜ aus dem System zu entfernen.

17.9.3.2.1 Hinzufügen eines FÜ

Hinzufügen eines FÜ zum System:

- Klicken Sie auf der Hauptseite für die Konfiguration und den Status von FÜ auf **Hinzufügen**.

⇨ Die Seite zur Konfiguration eines neuen FÜ 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 **Lernen** 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 funktionieren kann. Falls die Zentrale kein Überwachungssignal empfängt, wird ein Alarm ausgelöst, der auf dem Bedienteil angezeigt und protokolliert wird. 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. Aktivieren Sie das Kontrollkästchen **Überwachen**, wenn die Überwachung für den betreffenden FÜ aktiviert wurde.
Test	Aktivieren Sie das Kontrollkästchen **Test**, wenn regelmäßig ein FÜ-Test durchgeführt werden soll. Der Zeitrahmen für einen regelmäßigen Test wird auf der Seite Konfiguration Funk ändern [→ 237] konfiguriert.
Zuweisen von Tasten	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. Das oberhalb dargestellte Fenster zeigt die Standardeinstellungen für die Zentrale einer Installation in einer Bank: ● Gelb – Verdacht ● Rot + Grün – Überfall Für kommerzielle oder private Installationen ist die Standardeinstellung: ● Rot + Grün – Panik **Hinweis**: Wird einer Tastenkombination keine Funktion zugewiesen, ist es immer noch möglich, diese Kombination für einen Trigger zu verwenden. Siehe Trigger [→ 277]

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

Siehe auch

- Konfiguration Funk ändern [→ 237]
- Konfiguration Funk ändern [→ 237]
- Trigger [→ 277]

17.9.3.2.2 Bearbeiten eines FÜ

Klicken Sie auf der Hauptseite für die Konfiguration und den Status von FÜ auf **Bearbeiten**.

Die Seite für das **Bearbeiten** ähnelt der Seite für das **Hinzufügen** eines FÜ mit dem Unterschied, dass keine Anmeldetaste für das automatische Einfügen der FÜ-ID vorhanden ist.

17.9.3.3 Konfiguration Funk ändern

1. Wählen Sie **Konfiguration > Hardware > Funk > Funkeinstellungen**.

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 erforderlich 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 **Funkmelder fehlt** eingestellte Zeit überschreitet. Siehe Seite [→ 248].
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: ● Deaktivieren ● Aktivieren ● Aktiv (still) ● Benutzer Medizin ● Benutzer Bedrohung ● Funk Ausgang
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: ● Alarm ● Einbruch verzögert ● Endgültig scharf ● Notruf ● Überfall ● Sabotage ● Verschlussüberwachung ● Körperschallmelder ● Alles OK ● Scharfschalteberechtigung

	• Sperrelement
Geräteverlust	Geben Sie eine Zeitspanne in Minuten ein, nach der das Funkgerät (Melder oder FÜ) als fehlend gemeldet wird.

17.9.4 Systemoptionen ändern

17.9.4.1 Optionen

1. Wählen Sie **Konfiguration > System > Systemoptionen**.
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
Allgemeine Einstellungen		
	Bereiche	Wählen Sie diese Option, um mehrere Bereich im System zu aktivieren. **Hinweis**: 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 Panikalarme.
	Ausgänge im Konf Modus	Wenn diese Option ausgewählt wird, werden folgende Ausgänge im Konfigurationsmodus nicht deaktiviert: • Ausgänge der Zentrale • Ausgänge der Erweiterung • Anzeige-LEDs • Schlüsselschalter-LEDs
	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

Einschränkungen	Systemoptionen	Beschreibung
	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: ● Deaktiviert – Ausgang 6 ist als allgemeiner Universalausgang verfügbar. ● Aktiviert – Ausgang 6 ist normalerweise AUS, wird jedoch eingeschaltet, wenn eine Watchdog-Störung vorliegt. ● Pulsierend – Ausgang 6 PULSIERT in einem Intervall von 100 ms. ● Aktivierung vertauscht – Ausgang 6 ist normalerweise EIN, wird jedoch ausgeschaltet, wenn eine Watchdog-Störung vorliegt. Die folgenden Optionen kombinieren die Aktiviert-Option mit Hardware-Fehlerberichten, wenn der Hauptmikroprozessor ausfällt. Wenn ein derartiger Ausfall eintritt, wird ein SIA-Ereignis an ARC1 gesendet. **Hinweis:** 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. ● 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. ● Aktiv + Auswertung (60 s) – Das Ausfallereignis wird 60 Sekunden nach Erkennung des Ausfalls an ARC1 gesendet. Das gemeldete SIA-Ereignis ist **HF** und Extended SIA meldet **Hardware-Störung**. **Hinweis**: Hardware-Störungen werden nicht gemeldet, wenn der Techniker am System angemeldet ist. Weitere Information zu ARCs finden Sie unter Empfänger (Alarm Reporting Centres, ARCs) [→ 316].
	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 **Maximaler Strom** eingeben, um die verbleibende Batteriedauer auf dem Bedienteil für eventuelle Stromausfälle anzuzeigen. Dies wird unter „STATUS – AKKU – Akku Zeit“ angezeigt.

Einschränkungen	Systemoptionen	Beschreibung
	Maximaler Strom	Die Gesamtstromaufnahme der Batterien, wenn die Stromversorgung ausfälle (30–20.000 mA). Sie müssen diesen Wert und **Akku Kapazität** eingeben, um die verbleibende Batteriedauer auf dem Bedienteil für eventuelle Stromausfälle anzuzeigen. Dies wird unter „STATUS – AKKU – Akku Zeit“ angezeigt.
Intern scharf		
	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).
Alarm		
	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.
Nur Web	Kein Scharf bei Alarm	Wenn aktiviert, kann ein Bereich nicht geschärft werden, wenn ein Alarm in einem Bereich oder dem System vorliegt. **Hinweis**: Nur verfügbar, wenn unter **Standards -> Region** die Region „Schweiz“ oder der **Sicherheitsgrad** „Unbeschränkt“ ausgewählt ist.
	Quittierung bei unscharf	Aktivieren Sie diese Option, um Alarme nach 30 Sekunden im unscharfen Zustand automatisch zu quittieren. **Hinweis:** 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: • Irland − Alarm • Alle anderen Regionen – Alarm
	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: • Irland − Deaktiviert • Alle anderen Regionen – Sabotage
	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,

Einschränkungen	Systemoptionen	Beschreibung
		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: ● Deutschland VdS – Sabotage ● Alle anderen Regionen – Störung
⏻	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: ● Deutschland VDS – Sabotage ● Alle anderen Regionen – Störung
⏻	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 oder Grad 3 entspricht der Meldungstyp den Standards für die ausgewählte Region: ● Deutschland VDS – Sabotage ● Alle anderen Regionen – Störung
⏻	MG instabil schärfen	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. 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 oder Grad 3 entspricht der Meldungstyp den Standards für die ausgewählte Region: ● Deutschland VDS – Sabotage ● Alle anderen Regionen – Störung
⏻	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)	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. 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

Einschränkungen	Systemoptionen	Beschreibung
		für Meldergruppen, die nach der Änderung des Werts hinzugefügt wurden.
	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	**Aktiv:** Wird eine nicht-verzögerte Meldergruppe aktiviert, während der Ausgangs-Timer abläuft, wird ein lokaler Alarm mit Sirenen ausgelöst. **Deaktiviert:** Wird eine nicht-verzögerte Meldergruppe aktiviert, während der Ausgangs-Timer abläuft, wird kein Alarm ausgelöst. **Hinweis**: Diese Option wird nur angezeigt, wenn der Grad **Unbeschränkte Konfiguration** ausgewählt wurde, da ihre Aktivierung nicht den Anforderungen der EN50131 entspricht. Wird unter der Menüoption **Einhaltung von Vorschriften** als **Region** Belgien oder Schweiz eingestellt, wird diese Option automatisch aktiviert, ist aber unter **Optionen** nicht sichtbar.
⏻	Alarm bei Eintrittsverzögerung	**Aktiv:** Wird eine nicht-verzögerte Meldergruppe aktiviert, während der Eingangs-Timer abläuft, wird ein lokaler Alarm mit Sirenen ausgelöst. **Deaktiviert:** Wird eine nicht-verzögerte Meldergruppe aktiviert, während der Eingangs-Timer abläuft, wird kein Alarm ausgelöst. **Hinweis**: Diese Option wird nur angezeigt, wenn der Grad **Unbeschränkte Konfiguration** ausgewählt wurde, da ihre Aktivierung nicht den Anforderungen der EN50131 entspricht. Wird unter der Menüoption **Einhaltung von Vorschriften** als **Region** die Schweiz ausgewählt, wird diese Option automatisch aktiviert, ist aber unter **Optionen** nicht sichtbar.
Bestätigung		
⏻	Bestätigung	Die Bestätigungsvariable legt fest, wann ein Alarm als bestätigter Alarm gilt. ● BS8243: 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. (SieheTimer [→ 248]) Wird innerhalb der Alarmbestätigungszeit kein zweiter Alarm aktiviert, wird der erste MG-Alarm gesperrt. Die BS8243-Bestätigungsoption wird automatisch gesetzt, wenn unter **Standards > Region** die Region UK gewählt wird. ● Garda: Stellt die Einhaltung der Richtlinien der irischen

Einschränkungen	Systemoptionen	Beschreibung
		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 **Standards > Region** die Region Irland gewählt wird. ● EN-50131-9 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: - 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. - 1 Alarmaktivierung gefolgt von einer ATS[1]-Störung innerhalb von 30 Minuten (Standardwert). - ATS-Störung gefolgt von einer Sabotage oder einer Alarmbedingung innerhalb von 30 Minuten (Standardwert). 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. Wenn die Meldergruppe nicht in den ursprünglichen Zustand versetzt wurde, wird die Meldergruppe gesperrt, sofern sie gesperrt werden darf. Wenn ein Alarm (ATS) nach einem Zeitraum von 30 Minuten (Standardwert) erneut ausgelöst wird, startet der 30-Minuten-Timer neu. Die EN50131-9-Bestätigungsoption wird automatisch gesetzt, wenn unter **Standards -> Region** die Region „Spanien“ gewählt wird. ● VDS Dies erzwingt die Einhaltung der VdS-Norm.
Bedienteil		
ⓘ	Zeige Status (ZEIGE STATUS)	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.
	Zeige offene MG	Wenn aktiviert, werden die offenen Meldergruppen im unscharfen Zustand am Bedienteil angezeigt.
	Info bei Übertr	Wenn aktiviert, wird für 30 Sekunden nach der Unscharfschaltung eine Nachricht angezeigt, wenn ein bestätigter Alarm übertragen wurde.
	Info bei Übertr. Zeile 1	Nachricht, die in der ersten Zeile des Displays angezeigt wird.

Einschränkungen	Systemoptionen	Beschreibung
	Info bei Übertr. Zeile 2	Nachricht, die in der zweiten Zeile des Displays angezeigt wird.
	Kamerastatus anzeigen	Wenn aktiviert, werden nicht verbundene Kameras im unscharfen Zustand am Bedienteil angezeigt.
	Sprache im Ruhezustand	Wählen Sie die Sprache, die im Ruhezustand angezeigt werden soll. ● Systemsprache: Die Sprache, in der Menüs und Texte auf den Bedienteilen, in der Webschnittstelle und im Logbuch angezeigt werden. ● Zuletzt verwendet: Die zuletzt verwendete Sprache wird im Ruhezustand angezeigt.
PIN		
	Pin ?-stellig	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. **Hinweis**: Diese Option kann nicht geändert werden, wenn ein SPC Manager-PIN-Stellen-Modus eingerichtet ist. Weitere Informationen finden Sie auf Seite [→ 328] **Hinweis**: Zur Einhaltung der INCERT-Genehmigungen muss die Benutzer-PIN mehr als 4 Zeichen enthalten.
	TP + PIN	Wenn aktiviert, werden Transponder und PIN benötigt.
	Bedrohungs-PIN	Wählen Sie eine der folgenden Bedrohungs-PIN-Optionen, um die entsprechende Funktion auf dem System zu aktivieren. ● PIN +1 (das System reserviert die PIN vor und nach der Benutzer-PIN als Bedrohungs-PIN) ● PIN +2 (das System reserviert zwei PINs vor und nach der Benutzer-PIN als Bedrohungs-PINs) Die Bedrohungs-PIN muss für einzelne Benutzer aktiviert sein. Siehe Abschnitt Hinzufügen/Bearbeiten von Benutzern.
	PIN-Richtlinien	Klicken Sie auf die Schaltfläche **Bearbeiten**, um Optionen für die PIN-Nutzung auszuwählen. ● Periodic changes required (Regelmäßige Änderungen erforderlich) – Erzwingt geplante Änderungen der Benutzer-PIN. Der Zeitraum wird im Feld **PIN Gültig** unter **Timer** definiert. Siehe Timer [→ 248]. ● Warnung, wenn Änderungen erforderlich – generiert einen Benutzerwarnung, wenn die Benutzer-PIN bald abläuft oder abgelaufen ist. Der Warnzeitraum wird im Feld **Pin Warnung** unter **Timer** definiert. Siehe Timer [→ 248]. ● 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. ● User selects the 2 digits (Benutzer wählt die letzten 2 Stellen) – Ermöglicht es dem Benutzer, die letzten

Einschränkungen	Systemoptionen	Beschreibung
		zwei Stellen der PIN auszuwählen. Die vorhergehenden Stellen werden automatisch vom System generiert. ● Limit Änderung – Beschränkt die Anzahl der möglichen Änderungen innerhalb eines gültigen PIN-Zeitraums. Dieser Wert wird im Feld **Limit PIN-Änderung** unter **Timer** definiert. Siehe Timer [→ 248] ● Sichere PINs – Bei Aktivierung dieser Option wird die PIN automatisch von der Zentrale generiert.
Tür		
	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	Klicken Sie auf **Bearbeiten**, um die Ausweisformate auszuwählen, die in dieser Zentrale zugelassen werden sollen. Weitere Informationen zu derzeit unterstützten Ausweislesern und Ausweisformaten finden Sie im Anhang des SPC Installations- und Konfigurationshandbuch. **Hinweis:** Die Auswahl von **Wiegand** aktiviert alle 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: **Standard**, **Karte und PIN**, **Karte oder PIN**.
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: **Standard**, **Karte und PIN**, **Karte oder PIN**.
Techniker		
⏻	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 TECHNIKERZUGANG FREIGEBEN nicht auf dem Bedienteil verfügbar. **Hinweis**: Nur verfügbar, wenn der Sicherheitsgrad ‚Unbeschränkt‘ ausgewählt ist. Für Grad 2 oder 3 ist die Benutzersteuerung für den Technikerzugang immer verfügbar.
⏻	Herstellerzugang 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 HERSTELLERZUGANG FREIGEBEN nicht auf dem Bedienteil verfügbar.

Einschränkungen	Systemoptionen	Beschreibung
		Hinweis: Nur verfügbar, wenn der **Sicherheitsgrad** ‚Unbeschränkt' ausgewählt ist. Für Grad 2 oder 3 ist die Benutzersteuerung für den Technikerzugang immer verfügbar, wenn der Benutzer vom Typ ‚Manager' ist.
SMS		
	SMS-Authentifizierung	Folgende Optionen stehen zur Verfügung: ● 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. Die SMS-Steuerung zur Konfiguration durch den Benutzer steht nur zur Verfügung, wenn diese Option ausgewählt wurde. ● 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! Die SMS-Steuerung zur Konfiguration durch den Benutzer steht nur zur Verfügung, wenn diese Option ausgewählt wurde. ● SMS-PIN + Rufnummer
Verfahrensweise		
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 **Bearbeiten**, um Verriegelungs- und Auto-Scharfschaltungseinstellungen [→ 216] 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 Sirenenscharfschaltungen zu verwalten: - keine bestät. Alarme wenn internscharf - blockiere Fernrücksetzung - blockiere Fernabschaltung - blockiere Fernsperre - keine externe Sirene, wenn intern scharf

Einschränkungen	Systemoptionen	Beschreibung
		- 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 Systemalarme einen bestätigten Alarm auslösen, wenn mindestens ein Alarm aktiv ist, und welcher Systemalarm bei der Zentrale den Wechsel in den Probestatus verursacht.
Bedrohungsdaten		
Nur Web	Bedrohungspasswort 1	Bedrohungspasswort 1
Nur Web	Bedrohungspasswort 2	Bedrohungspasswort 2
Nur Web	Telefonnummer 1	Telefonnummer 1
Nur Web	Telefonnummer 2	Telefonnummer 2

Siehe auch

Bereich hinzufügen/bearbeiten [→ 257]

17.9.4.2 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.

1. Wählen Sie **Konfiguration > System > System Timers** (System-Timer).
   ⇨ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

Timer

Die Funktionen werden in der nachstehenden Reihenfolge zugeordnet:

- 1st Zeile: Web/SPC Pro

- 2. Zeile: Bedienteil

Timer	Beschreibung	Rücksetzen
Bedient. Summer		
Innensirenen ZEIT INNENSIR	Dauer der Aktivierung der Innensirenen im Alarmfall (1 – 15 Minuten: 0 = niemals)	15 Min.
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.
Bestätigung		
Confirm ZEIT BEST ALARM	• **Hinweis**: Nur verfügbar, wenn der Sicherheitsgrad „Unbeschränkt“ und „DD243“ für die Bestätigungsvariable ausgewählt ist. (Siehe Systemoptionen [→ 239].) 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 Alarmabbruchsmeldung gesendet werden kann. (0–999 Sekunden)	30 Sek.
Einstellung		
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.
Alarm		
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–	14 Tage

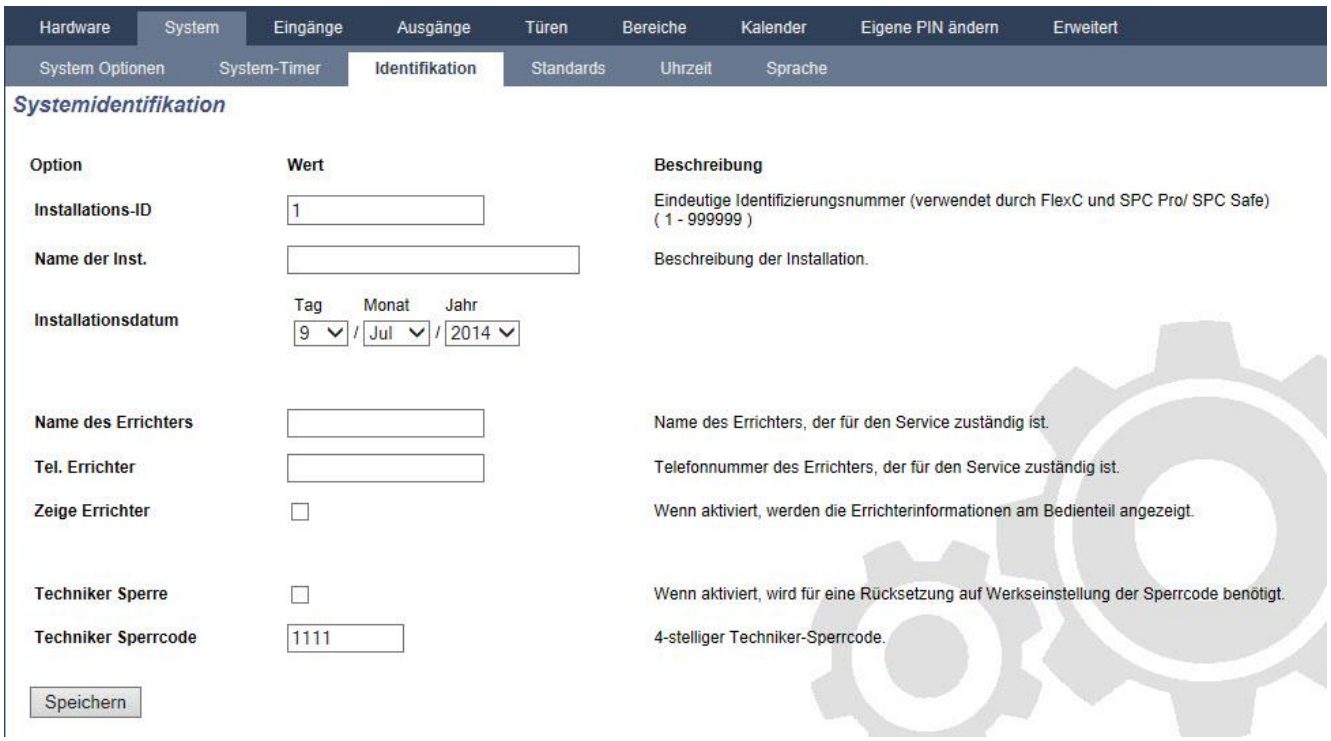
Timer	Beschreibung	Rücksetzen
	99 Tage)	
Körperschallmelder Autotestzeit KSM AUTOTST	Der durchschnittliche Zeitraum zwischen automatischen Tests der Körperschallmelder (12–240 Stunden). **Hinweis**: Zur Aktivierung der automatischen Tests muss das Attribut **Automatischer Meldertest** für eine Körperschall-MG aktiviert sein.	168 Stunden.
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.
ALARME		
Verz Netzstörung VERZ STÖR NETZ	Die Verzögerungszeit nach einer erkannten Netzstörung, bis das System einen Alarm aktiviert. (0–60 Minuten)	0 min.
Techniker		
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.
Bedienteil		
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
Feuer		
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 [→ 256].	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 [→ 256].	120 Sek.
PIN		
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
Allgemeine Einstellungen		
Zeit Funk Ausgang FUNKAUSGANG	Die Dauer, für die der Funkausgang im System aktiv bleibt. (0 – 999 Sekunden)	0 Sek.

Timer	Beschreibung	Rücksetzen
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.
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 **Überwacht** 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.

17.9.4.3 Identifikation

1. Wählen Sie **Konfiguration > System > Identifikation**.
   ⇨ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

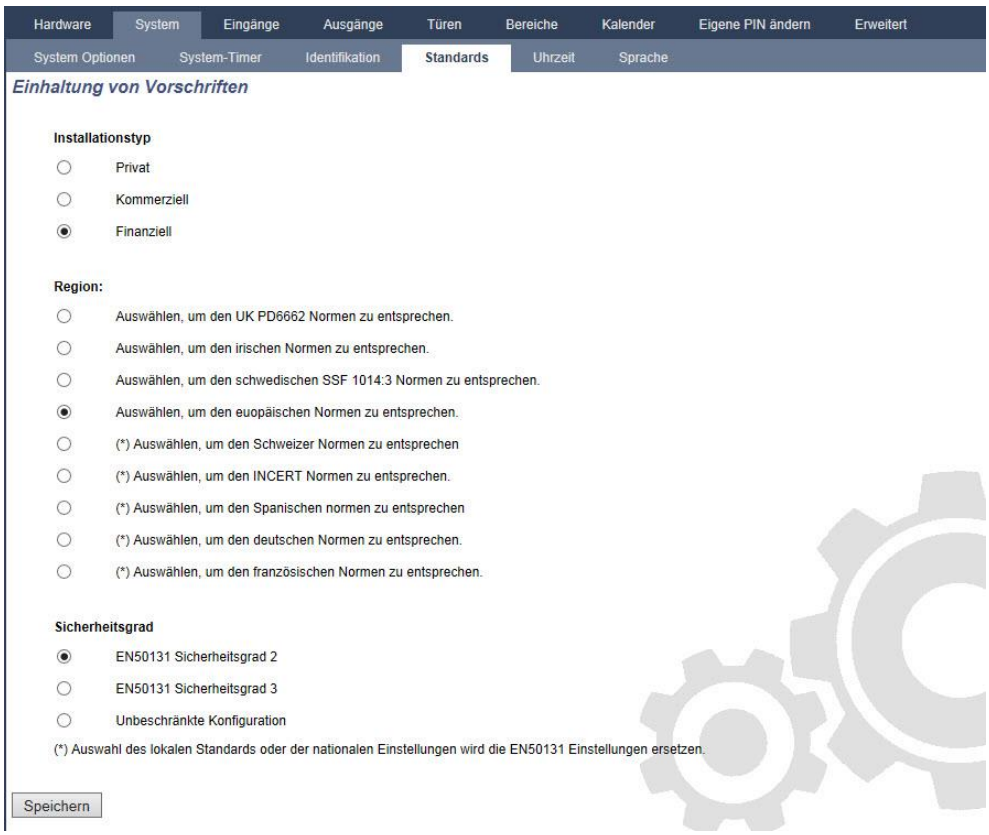


Installations-ID	Geben Sie für jede Installation eine eindeutige Nummer ein (1–999999). Diese Nummer identifiziert die Installation.
Name der Inst	Geben Sie den Namen der Anlage ein. Ein Installationsname muss eingegeben werden, bevor die Installation auf dem System gespeichert wird. Die Installation 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.

17.9.4.4 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.

1. Wählen Sie **Konfiguration > System > Standards**.
   ⇨ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



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	Wählen Sie den Sicherheitsgrad, der für die Installation gilt. ● Regionen Irland und Europa: – EN50131 Grad 2 – EN50131 Grad 3 – Unbeschränkt ● Region UK: – PD6662 (basiert auf EN50131 Grad 2) – PD6662 (basiert auf EN50131 Grad 3) – Unbeschränkt ● Region Schweden: – SSF1014:3 Larmclass 1 – SSF1014:3 Larmclass 2 – Unbeschränkt ● Region Belgien: – TO-14 (basiert auf EN50131 Grad 2) – TO-14 (basiert auf EN50131 Grad 3) – Unbeschränkt ● Region Schweiz: – SES EN-CH-Grad 2 – SES EN-CH-Grad 3 – Unbeschränkt

	● Region Spanien: – EN50131 Grad 2 – EN50131 Grad 3 ● Region Deutschland: – VdS Klasse A – VdS Klasse C – Unbeschränkt ● Frankreich – NF&A2P - Grad 2 – NF&A2P - Grad 3 – Unbeschränkt

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.

17.9.4.5 Uhrzeit

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

1. Wählen Sie **Konfiguration > System > Uhrzeit**.
   ⇨ Daraufhin erscheint das folgende Fenster.

2. Wählen Sie **Uhrzeit** und **Datum** aus den Dropdown-Menüs.

3. 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.

17.9.4.6 Sprache

- Wählen Sie **Konfiguration > System > Sprache**.
  - ⇨ Das folgende Fenster wird angezeigt:

- Wählen Sie für die Option **Sprache** eine Sprache aus dem Dropdown-Menü.
- ⇨ Diese Option bestimmt die Systemsprache, in der Menüs und Texte auf den Bedienteilen, in der Webschnittstelle und im Logbuch angezeigt werden.
- Wählen Sie für die Option **Sprache in Ruhezustand** entweder „Verwende Systemsprache“ oder „Zuletzt verwendete“.
- ⇨ Die Option „Sprache in Ruhezustand“ bestimmt, welche Sprache auf dem Bedienteil angezeigt wird, wenn die Zentrale im Ruhezustand ist. Wenn „Zuletzt verwendete“ ausgewählt ist, wird die Sprache angezeigt, die bei der letzten Benutzeranmeldung ausgewählt war.

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.

Siehe auch

Sprache [➞ 255]
OPTIONEN [➞ 116]

17.9.5 Konfigurieren von Meldergruppen, Türen und Bereichen

17.9.5.1 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.

1. Wählen Sie **Konfiguration >Eingänge > Alle Meldergruppen**.
   ⇨ Daraufhin erscheint das folgende Fenster.

Sie können **Konfiguration > Eingänge > Xbus Meldelinien** wählen, um nur verkabeltes MGs zu konfigurieren, oder **Konfiguration > Eingänge > Funk Meldegruppe**, um nur Funk-MGs zu konfigurieren.

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

Meldergruppe	Diese Nummer wird als Referenz angezeigt und kann nicht programmiert werden.
Beschreibung	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 [→ 375]).
Bereich	Nur wenn (mehrere) **Bereiche** aktiviert sind. Wählen Sie aus dem Dropdown-Menü einen Bereich, dem die MG zugewiesen wird.
Kalender Pro !	Wählen Sie ggf. den gewünschten Kalender (siehe Seite [→ 273]). 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 [→ 378]).

17.9.5.2 Bereich hinzufügen/bearbeiten

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

1. Wählen Sie **Konfiguration >Bereiche > Bereiche**.
   ⇨ Daraufhin erscheint das folgende Fenster:

2. Klicken Sie auf **Bearbeiten**, um einen bestehenden Bereich zu bearbeiten.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Bereich hinzuzufügen. Bei den Installationstypen *Privat* oder *Kommerziell* wird ein Bereich automatisch hinzugefügt und das Fenster Bereichseinstellungen bearbeiten wird angezeigt. Beachten Sie bitte, dass der Bereichstyp für den neuen Bereich automatisch auf Standard gesetzt wird.
   Beim Installationstyp *Finanziell* wird das folgende Fenster angezeigt, und der Bereich muss manuell hinzugefügt werden.

4. Geben Sie einen Namen für den neuen Bereich ein, und 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).
5. Klicken Sie auf die Schaltfläche **Hinzufügen**, um den Bereich hinzuzufügen.

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

17.9.5.2.1 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 [→ 248].
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 Blockschlosses benutzt. Verfügbare Optionen sind: ● Deaktivieren ● Scharf ● Unscharf ● Scharf- und unscharfschalten Wenn die Deaktiviert-Option ausgewählt ist (Standardeinstellung), schaltet das System scharf und unscharf ohne Änderung des Blockschlossvorgangs. 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 Blockschlosses). 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. 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. Bei den Optionen Scharf und Unscharf kann der Benutzer zu keiner Zeit den Zustand eines Bereiches vom Bedienteil aus ändern. Es ist möglich, einen Timer für die Scharfschalteberechtigung zu konfigurieren. Siehe Timer [→ 248].

17.9.5.2.2 Intern-scharf-Optionen

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.

17.9.5.2.3 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 Blockschlosses“.
Verbundene Bereiche	Klicken Sie auf die Bereiche, die Sie mit diesem Bereich verbinden möchten.

17.9.5.2.4 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 angegeben 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 [➙ 263]). 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“)

17.9.5.2.5 Übertragen

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 [➙ 260])

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.

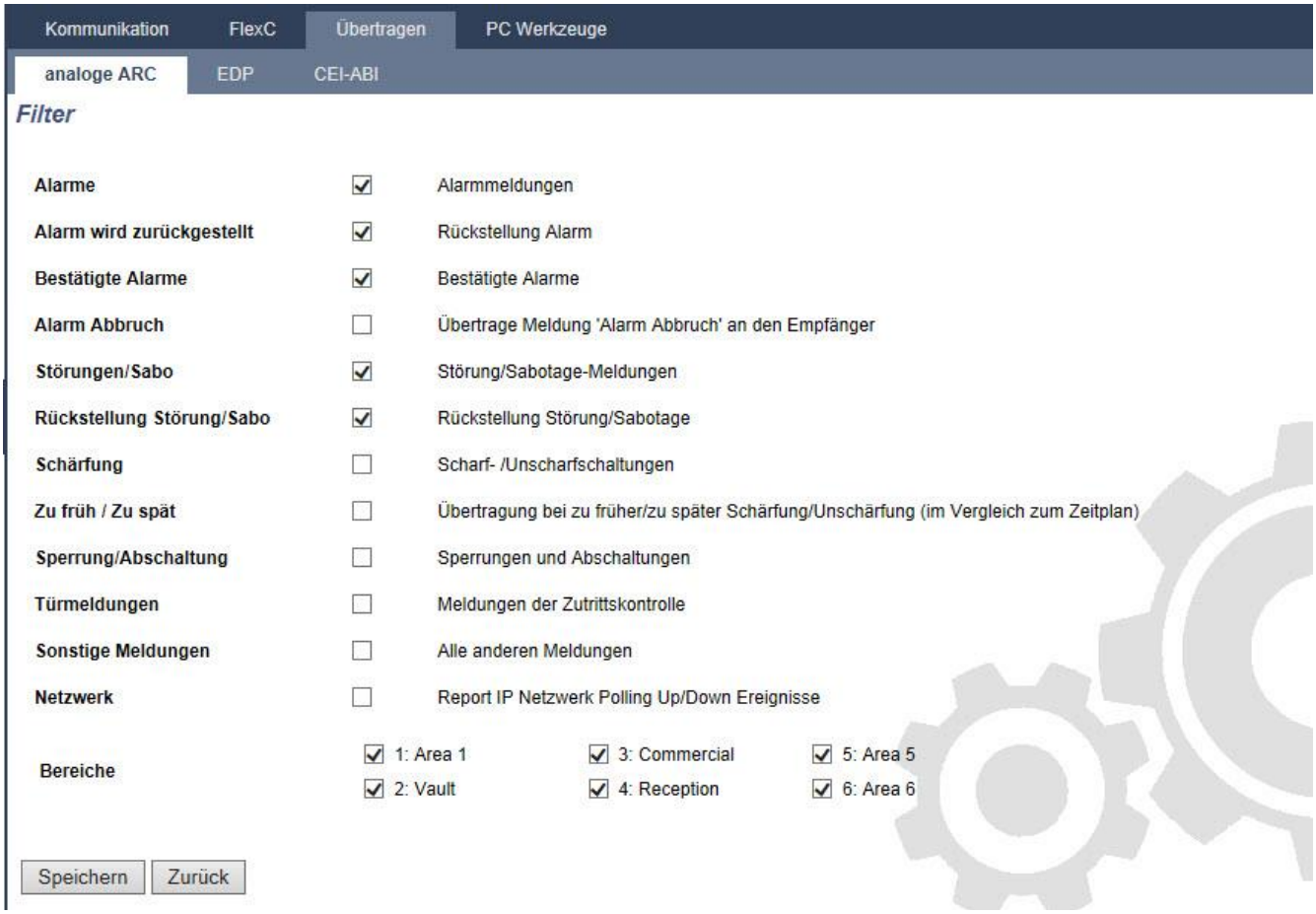
Die Übertragung erfolgt per SMS oder über SIA und Contact-ID an eine Alarmempfangsstelle (Empfänger). Außerdem wird im Systemprotokoll ein Ereignis aufgezeichnet.

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 zum Konfigurieren eines Ereignisbericht für einen Empfänger, der über SIA oder CID kommuniziert, die Optionen **Kommunikation > Reporting (Meldung) > Analoge ARC > Bearbeiten > Filter**. Daraufhin wird die Seite mit den Meldungsfiltern für eine Alarmempfangsstelle (ARC) angezeigt.

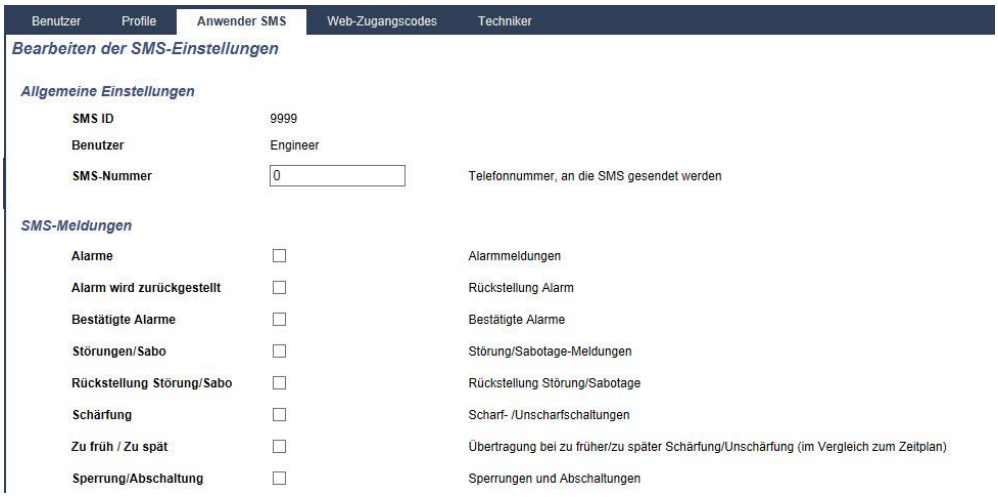


Der Parameter **Früh/Spät** ist aktiviert, um alle Scharf- bzw. Unscharfschaltungen außerhalb der im Zeitplan festgelegten Zeiten zu melden.

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

Die Übertragung per SMS kann auf den Konfigurationsseiten für Techniker und auch Benutzer konfiguriert werden.

Wählen Sie im Konfigurationsmodus die Optionen **Benutzer > Anwender SMS > Techniker SMS > Bearbeiten**:



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

17.9.5.2.6 Scharf-/Unscharfschalten

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

- Ein Kalender ist ausgewählt (siehe Zeitplan [→ 260]), 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:

17.9.5.2.7 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 [→ 256].
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“.

17.9.5.2.8 Funk Ausgang

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 [→ 258] für SPC Pro.

17.9.5.2.9 Fluchtweg

Fluchtweg	Wählen Sie die Türen, die geöffnet werden, wenn es in diesem Bereich brennt. Diese Option wird im privaten Modus nicht angezeigt.

17.9.5.2.10 Bereich gesteuert

Der Abschnitt zu Triggern wird nur angezeigt, wenn zuvor Trigger definiert wurden. (Siehe Abschnitt über Trigger)

Klicken Sie auf die Schaltfläche **Bearbeiten**, um einen neuen Trigger für den Bereich hinzuzufügen oder Bedingungen für den Trigger zu bearbeiten oder zu löschen. Die folgende Seite wird angezeigt:

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	Diese Aktion wird ausgeführt, wenn der Trigger auslöst. Verfügbare Optionen sind: ● Unscharf ● Intern scharf A ● Intern scharf B ● Extern Scharf ● 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 [→ 263]) festgelegt wurde. ● Alarme quittieren Hiermit werden alle Alarme in der konfigurierten MG gelöscht.

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

Siehe auch

Trigger [→ 277]

17.9.5.3 Tür bearbeiten

1. Wählen Sie **Konfiguration > Türen**.
   ⇨ Eine Liste mit konfigurierten Türen wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Bearbeiten**.
3. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

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 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)	Zeigt das Format des letzten mit jedem konfigurierten Leser genutzten Ausweises an (nicht in SPC Pro verfügbar).

Name	Beschreibung
(Bedienteile)	

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.

Attribut	Beschreibung
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 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

Attribut	Beschreibung
	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.
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.

17.9.5.3.1 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:

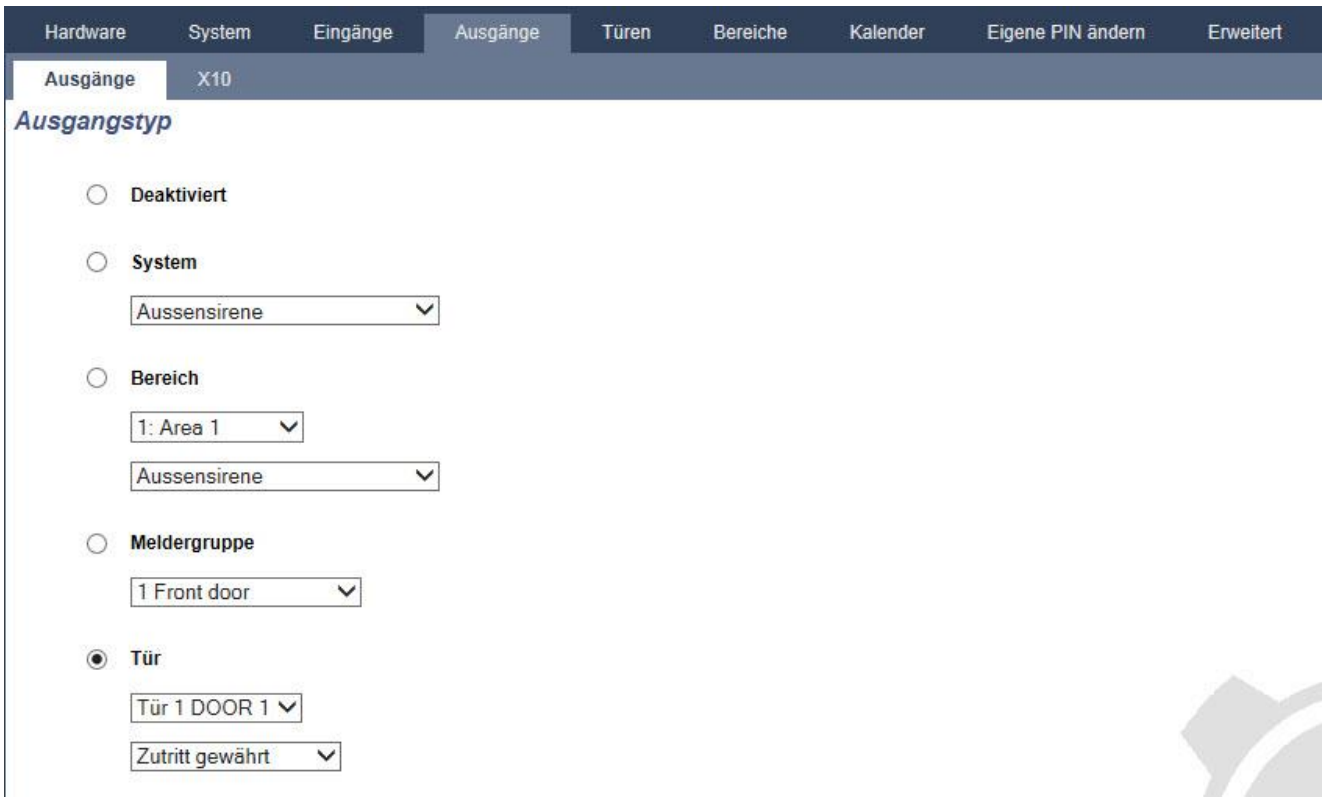
- Bei Zugangskontrollsystemen mit zwei Türen, wie sie in Banken und anderen Gebäuden verwendet werden: Normalerweise wird der Zutritt mit einem Drucktaster oder einem Kartenleser gesteuert. Eine grüne und eine rote LED zeigen an, ob die Tür geöffnet werden kann oder nicht.
- In GAA-Technikbereichen zur 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 [→ 266].
2. Legen Sie das Attribut **Interlock** für die gewünschten Türen der Gruppe fest. Siehe Bearbeiten einer Tür [→ 266].
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.

1. Wählen Sie im Konfigurationsmodus die Optionen **Konfiguration > Hardware > X-Bus > Erweiterungen**.
2. Klicken Sie auf der Seite **Konfiguration Erweiterung** auf die Schaltfläche **Typ ändern** des gewünschten Ausgangs.
3. Wählen Sie den Ausgangstyp **Tür**.
4. Wählen Sie die gewünschte Tür und als Ausgangstyp **Schleuse**.

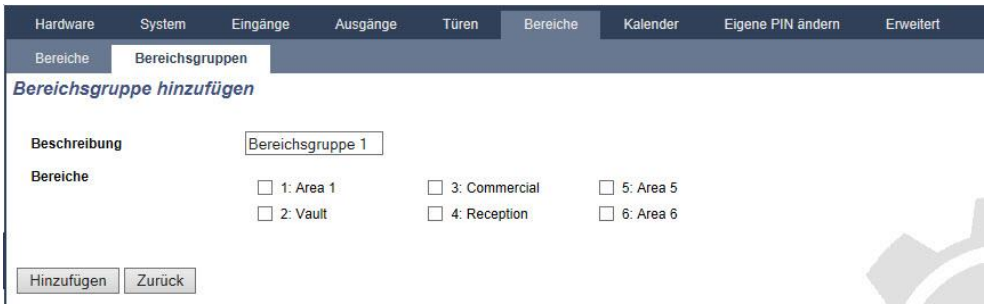


17.9.5.4 Bereichsgruppe hinzufügen

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.

- Wählen Sie **Einstellungen > Bereiche > Bereichsgruppen**.



1. Klicken Sie auf die Schaltfläche **Hinzufügen**.
2. Geben Sie einen Namen für die Gruppe ein.
3. Wählen Sie die Bereiche, die der Gruppe zugewiesen werden sollen.
4. Klicken Sie auf **Hinzufügen**.

	HINWEIS
	Um Bereichsgruppen auf dem Komfort-Bedienteil zu verwenden, aktivieren Sie alle Bereiche im Feld **Bereiche** unter **Konfiguration > Hardware > X-BUS > Bedienteile > Typ: Komfort-Bedienteil**.

17.9.6 Kalender

Kalender werden verwendet, um die zeitbasierte Steuerung für mehrere Funktionen der Zentrale wie folgt zu planen:

- Automatisches Scharf-/Unscharfschalten von Bereichen
- Automatisches Scharf-/Unscharfschalten anderer Funktionen der Zentrale wie Trigger, Aktivieren von Benutzern, Meldergruppen, physischen Ausgängen usw.

Jeder Zeitplan eines Kalenders kann zu jederzeit ‚aktiv' sein, wenn die Zeitbedingungen erfüllt werden.

Jeder Woche eines Kalenderjahres wird eine Ordnungsnummer zugewiesen. Je nach Verteilung der Wochentage innerhalb eines Monats kann es in einem Jahr 52 oder 53 Wochen geben. Die SPC-Kalenderimplementierung entspricht der internationalen Norm ISO 8601.

Konfiguration von Kalendern

- Wählen Sie **Konfiguration > Kalender**.
  - ⇨ Eine Liste mit den konfigurierten Kalendern wird angezeigt:

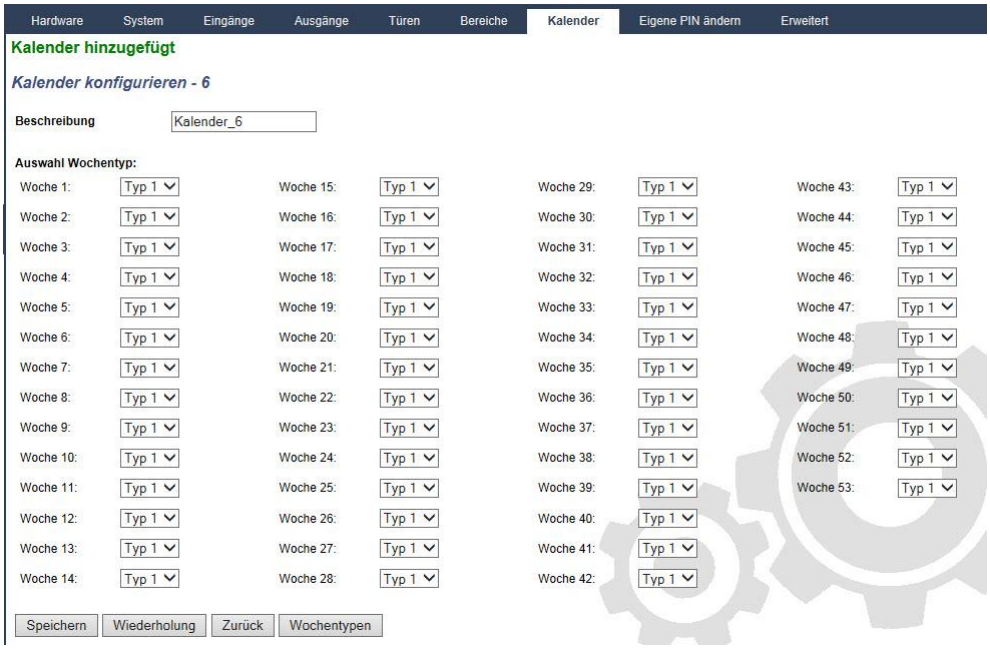
Ausführbare Aktionen

Hinzufügen	Fügen Sie einen neuen Kalender hinzu.
Ausnahmen	Konfigurieren Sie Zeitpläne für besondere Umstände außerhalb der normalen wöchentlichen Zeitpläne.
Bearbeiten/Ansehen	Bearbeiten Sie den ausgewählten Kalender, oder zeigen Sie ihn an.
Löschen	Löschen Sie den ausgewählten Kalender. Der Kalender kann nicht gelöscht werden, wenn er momentan einem SPC-Konfigurationselement zugeordnet ist, z. B. Meldergruppe, Bereich, Benutzerprofil, Ausgang, Trigger, Tür oder X-Bus-Komponente. Es wird eine Meldung angezeigt, die das zugewiesene Element angibt.

Globale Kalender, welche über die SPC Manager Software erstellt wurden, können lokal nicht bearbeitet oder gelöscht werden. (siehe Beispiel Abbildung 3)

17.9.6.1 Kalender hinzufügen/bearbeiten

- Wählen Sie **Konfiguration > Kalender > Hinzufügen**.
  - ⇨ Daraufhin erscheint das folgende Fenster:



- Geben Sie eine **Beschreibung** für den Kalender ein (max. 16 Zeichen).

Kopieren eines Kalenders

Klicken Sie zur Erstellung einer Kopie des Kalenders auf die Schaltfläche **Replicate** (Kopieren).

Ein neuer Kalender mit der gleichen Konfiguration wie der Originalkalender wird erstellt. Sie können für den neuen Kalender eine neue Beschreibung angeben und die Kalenderkonfiguration nach Bedarf bearbeiten.

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 **Wochentypen**.
2. 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 [→ 276]) oder für das

automatische Scharf-/Unscharfschalten von Funktionen der Zentrale (siehe Seite [→ 276]).

⇨ Bis zu drei Wochentypen können konfiguriert werden.

3. Klicken Sie auf **Speichern** und anschließend auf **Zurück**.
4. Wählen Sie aus dem Dropdown-Menü den gewünschten Wochentyp für jede der erforderlichen geplanten Wochen im Kalender aus.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Zurück**.

Siehe auch

- Automatisches Scharf-/Unscharfschalten von Bereichen [→ 276]
- Automatisches Scharf-/Unscharfschalten von anderen Funktionen der Zentrale [→ 276]

17.9.6.1.1 Ausnahmen

Mit Ausnahmen oder Ausnahmetagen werden automatische Zeitpläne für besondere Umstände außerhalb der normalen wöchentlichen Zeitpläne im Kalender konfiguriert. Für Ausnahmen wird ein Start- und Enddatum festgelegt (Tag/Monat/Jahr) sowie bis zu vier An-/Aus-Zeiträume für verschiedene Funktionen der Zentrale wie das automatische Scharf-/Unscharfschalten von Bereichen oder das Ein-/Ausschalten von Ausgängen. Es können bis zu 64 Ausnahmen im System konfiguriert werden.

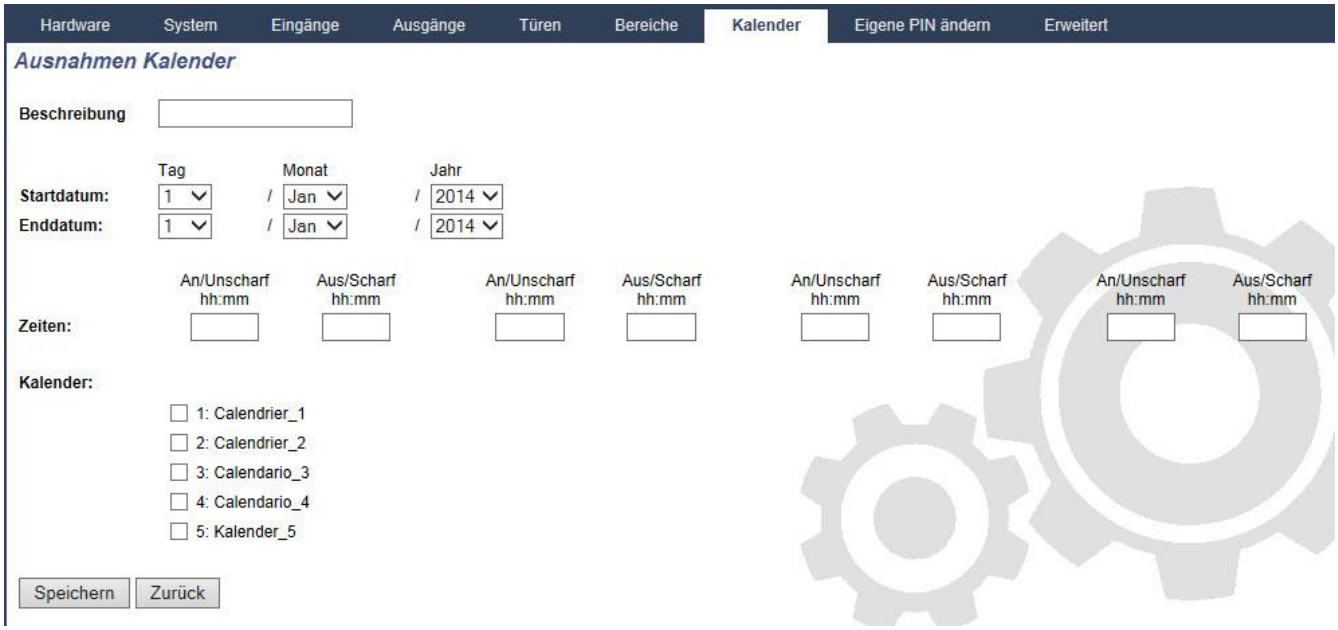
Ausnahmen sind allgemeine Einheiten, die einem oder mehreren Kalendern zugewiesen werden können. Wird eine Ausnahme einem Kalender zugewiesen, überschreiben die Ausnahmeeinstellungen alle anderen Kalenderkonfigurationen für das betreffende Start- und Enddatum (jeweils einschließlich dieser beiden Daten).

Konfiguration von Ausnahmetagen

1. Wählen Sie **Konfiguration > Kalender > Ausnahmen > Hinzufügen**.

   ⇨ Daraufhin erscheint das folgende Fenster.

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



Beschreibung	Geben Sie einen Namen für die Ausnahme ein (max. 16 Zeichen).
Startdatum/Enddatum	Wählen Sie das Start- und Enddatum.
On Time (An-Zeit) / Off Time (Aus-Zeit)	Wählen Sie die gewünschten Zeiten für das Scharf-/Unscharfschalten oder für Trigger. Verwenden Sie die Zeit-Richtlinien für das automatische Scharf-/Unscharfschalten von Bereichen (siehe Seite [➞ 276]) oder für das automatische Scharf-/Unscharfschalten von Funktionen der Zentrale (siehe Seite [➞ 276]).
Kalender zugewiesen zu	Wählen Sie den/die gewünschten Kalender.

!	*HINWEIS*
	Globale Ausnahmetage, die aus der Ferne mit dem SPC Manager-Tool erstellt wurden, können lokal nicht bearbeitet oder gelöscht werden.

17.9.6.2 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.

17.9.6.3 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 Einstellungspaar für einen Status: Ein/Aus, Wahr/Falsch, Aktiv/Inaktiv. Jede Einstellung ohne entsprechende Gegeneinstellung wird ignoriert.

17.9.7 Eigene PIN ändern

Informationen zur Änderung einer PIN finden Sie unter Ändern von Techniker-PIN und Web-Zugangscode [→ 209].

17.9.8 Konfigurieren der erweiterten Einstellungen

17.9.8.1 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.

1. Wählen Sie **Konfiguration > Erweitert > Trigger**.
   ⇨ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

Trigger	Das System hat eine Nummer für einen neuen Trigger erstellt. Trigger werden nur aktiv, wenn einer der beiden optionalen Schritte (Kalender-/Zeitbeschränkung) konfiguriert ist.
Beschreibung	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 [→ 273].

Aktivierungszeit/Timer	Geben Sie die Zeit in Sekunden ein, für welche die Trigger-Bedingung erfüllt sein muss, damit der Trigger aktiviert wird.
Limit Uhrzeit	Wählen Sie für die Aktivierung des Triggers einen Zeitraum zwischen 00:00 und 24:00. Die Startzeit ist eingeschlossen, die Endzeit ist nicht eingeschlossen. **Hinweis**: 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 UND-Operation findet statt): **MG** – Der Trigger wird aktiviert, wenn die konfigurierte MG einen der folgenden Stati aufweist: offen, geschlossen, kurzgeschlossen oder getrennt. **Tür** – 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. **System** – Der Trigger wird aktiviert, wenn der Systemausgang den konfigurierten Status aufweist (AN oder AUS). Mögliche Systemausgänge sind „Außensirene“, „Alarm“ usw. **Bereich** - Der Trigger wird aktiviert, wenn der Bereichsausgang ein- oder ausgeschaltet ist. Mögliche Bereichsausgänge sind „Außensirene“, „Alarm“ usw. **Funkfernbedienung** – 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. **Funkfernbedienung Überfall** – 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. **Funküberfalltaster** – 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, Einschalter von Leuchten oder Öffnen einer Tür) zugewiesen werden. **Bedienteil gültiger PIN** – 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. **Schlüsselschalter** – Der Trigger kann für eine bestimmte Schlüsselstellung am Schlüsselschalter konfiguriert werden. **Zeittrigger** – Der Trigger wird zu einem bestimmten Zeitpunkt aktiviert, der in das dafür vorgesehene Feld im Format hh:mm eingegeben wurde.

	⚠ **WARNUNG**
	Das System erfüllt nicht die EN-Normen, wenn Sie einen Trigger zur Scharfschaltung des Systems ohne die Eingabe eines gültigen PINs verwenden.

17.9.8.2 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 Statuseinstellungen die gleichen sein – entweder beide negativ oder beide positiv.

1. Wählen Sie **Konfiguration > Erweitert > Logischer Ausgänge**.
   ⇨ Daraufhin erscheint das folgende Fenster.

2. Geben Sie einen Namen für den Ausgang unter **Beschreibung** ein. Dieser ist wichtig, da auf der Benutzerseite **Ausgänge** zum Ein- und Ausschalten von Ausgängen keine Ausgangsnummer, sondern nur der Name angezeigt wird.
3. Aktivieren Sie das Kontrollkästchen **Geschützt**, damit Benutzer, auch wenn sie das Recht dazu haben, diesen Ausgang nicht ein- und ausschalten können. Ein geschützter Ausgang wird auf der Benutzerseite **Ausgänge** nicht angezeigt.
4. Wählen Sie die gewünschte **Kurzwahl**.
   Eine Kurzwahl besteht aus einer ‚#' gefolgt von einer auf dem Bedienteil gedrückten Nummerntaste. Wird eine konfigurierte Kurzwahl am Bedienteil eingegeben, wird der Benutzer aufgefordert, den Ausgang ein- oder auszuschalten.

Mit einer einzigen Kurzwahl können viele Ausgänge aktiviert werden, sowohl X-10 als auch logische Ausgänge.

5. Fügen Sie einen **Timer** für den Ausgang hinzu. Die verwendete Einheit ist 1/10 Sekunden.
6. Klicken Sie auf die Schaltfläche **Trigger**, 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 [→ 277].
7. Wählen Sie **Hinzufügen**, um einen neuen Ausgang hinzuzufügen. Oder klicken Sie auf **Speichern**, um die Einstellungen für einen vorhandenen Ausgang zu speichern.

Siehe auch

Trigger [→ 277]

17.9.8.3 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.

!	*HINWEIS*
	Bedienteile und Zutrittskontrollen könnten je nach Dateigröße während der Übertragung der Audiodatei an die Zentrale für einige Minuten deaktiviert sein.

17.9.8.3.1 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.

i	*HINWEIS*
	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).

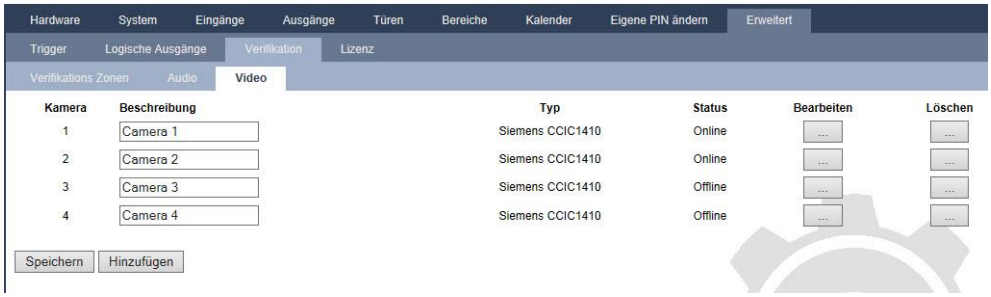
Die folgenden Kameras werden zusätzlich zu anderen generischen Kameras unterstützt:

- 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 angegeben Kameras steht eine standardmäßige Befehlszeichenfolge zur Verfügung. Für andere generische IP-Kameras muss die Befehlszeichenfolge manuell eingegeben werden.

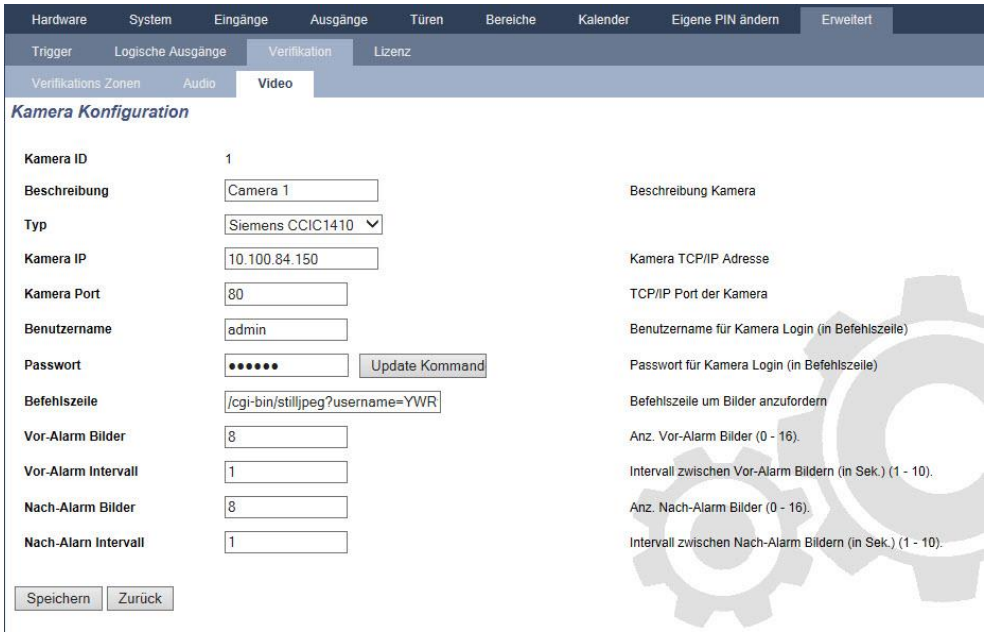
Hinzufügen einer Kamera

1. Wählen Sie **Konfiguration > Erweitert > Video**.
   ⇨ Eine Liste der zuvor konfigurierten Kameras wird zusammen mit dem jeweiligen Online- oder Offline-Status angezeigt. Eine Kamera ist online, wenn in den vorangegangenen 10 Sekunden ein Bild von der Kamera empfangen wurde.



2. Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Kamera hinzufügen. Oder klicken Sie auf die Schaltfläche **Bearbeiten**, um eine vorhandene Kamera zu bearbeiten.

   ⇨ Das folgende Fenster wird angezeigt.



3. Konfigurieren Sie die Kamera mit den folgenden Parametern:

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: ● Allgemein ● Vanderbilt CCIC1410 ● Vanderbilt CFMC1315
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. **Hinweis:** Die CCIC1410-Kamera kann nur über Port 80 verwendet werden.
Benutzername	Nur für die Kameras Vanderbilt CCIC1410 und CFMC1315. Geben Sie einen Anmeldebenutzernamen für die Kamera ein, die der nachfolgenden Befehlszeichenfolge hinzugefügt werden soll, wenn die Schaltfläche **Update Kommandozeile** bestätigt wird.
Passwort	Nur für die Kameras Vanderbilt CCIC1410 und CFMC1315. Geben Sie ein Anmeldepasswort für die Kamera ein, die der nachfolgenden Befehlszeichenfolge hinzugefügt werden soll, wenn

	die Schaltfläche **Update Kommandozeile** bestätigt wird.
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 eine Vanderbilt CCIC1410- oder CFMC1315-Kamera über ein LAN angeschlossen ist. Die standardmäßige Befehlszeichenfolgen für eine Vanderbilt CCIC1410- oder CFMC1315-Kamera ohne Passwort ist „/cgi-bin/stilljpeg“.
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.

17.9.8.3.2 Konfigurieren von Verifikationszonen

Einrichten einer Verifikationszone:

1. Wählen Sie **Konfiguration > Erweitert > Verifikation > Verifikations Zonen**.
   ⇨ Eine Liste der vorhandenen Verifikationszonen wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Geben Sie zur **Beschreibung** der Zone einen Namen ein.
4. Wählen Sie **Verifikationsmodul** aus der Dropdown-Liste.
5. Wählen Sie ein **Video** aus der Dropdown-Liste.
6. Klicken Sie auf **Speichern**.
7. Weisen Sie diese Verifikationszone einer real vorhandenen Meldergruppe im SPC-System zu. (Siehe Meldergruppe bearbeiten [→ 256].)

Der Audioeingang und -ausgang der Verifikationszone kann nur von einem Techniker in SPC Pro getestet werden.

Siehe auch

- Meldergruppe bearbeiten [→ 256]

17.9.8.3.3 Konfigurieren der Verifikationseinstellungen

Hinweis: Die folgenden Einstellungen gelten für alle Verifikationszonen [→ 282].

1. Wählen Sie **Konfiguration > Erweitert > Verifikation > Audio**.
   ⇨ 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.

17.9.8.3.4 Anzeigen von Videobildern

Videobilder der konfigurierten Kameras können im Webbrowser im Konfigurations- oder Wartungsmodus angezeigt werden. Diese Funktion ist auch für Benutzer verfügbar, denen in ihrem Profil das Recht zur Videoanzeige zugewiesen wurde. (Siehe Einstellen von Benutzerrechten [→ 196].) Zur Nutzung dieser Funktion muss auch das Recht für den Webzugriff zugewiesen sein.

Das Recht zur Anzeige von Videos kann auch über das Bedienteil und in SPC Pro (Einstellung „Video im Browser“) zugewiesen werden.

Wählen Sie zur Anzeige von Bildern die Optionen **SPC Startseite > Video**. Siehe Anzeigen des Videos [→ 177].

Siehe auch

- Hinzufügen/Bearbeiten von Benutzern [→ 196]
- Konfigurieren von Video [→ 280]

17.9.8.4 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 lizensiert sind, von einer SPC-Zentrale unterstützt werden sollen.

1. Wählen Sie **Konfiguration > Erweitert > Lizenz**.

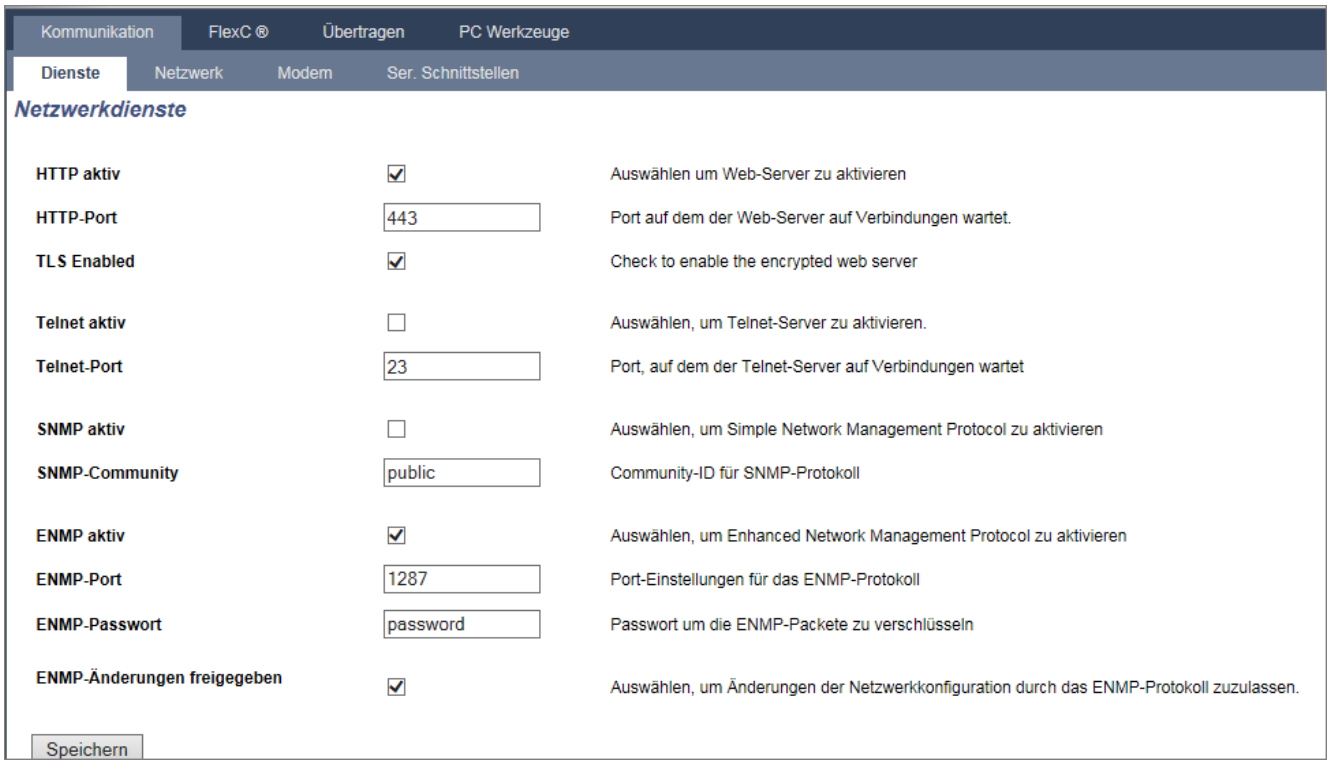
2. Wenden Sie sich mit der gewünschten Funktion an den technischen Support und geben Sie den angezeigten Lizenzschlüssel an.
   ⇨ Bei Genehmigung Ihrer Anfrage wird ein neuer Lizenzschlüssel ausgestellt.
3. Geben Sie den neuen Schüssel in das dafür vorgesehene Feld ein.

17.10 Kommunikation konfigurieren

17.10.1 Kommunikationseinstellungen

17.10.1.1 Konfigurieren der Netzwerkdienste der Zentrale

1. Wählen Sie **Kommunikation > Kommunikation > Dienste**.
   ⇨ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



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) **Hinweis**: 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: **1287**).
ENMP-Passwort	Geben Sie das Kennwort für das ENMP-Protokoll ein.
ENMP-Änderungen freigegeben	Aktivieren, um Änderungen der Netzwerkkonfiguration durch das ENMP-Protokoll zuzulassen.

17.10.1.2 Ethernet

IP

Der Ethernet-Port am Controller kann sowohl über die Browser als auch über die Bedienteilschnittstelle konfiguriert werden. Eine Ethernet-Verbindung mit dem SPC-Controller kann über eine Direktverbindung oder über eine LAN-Verbindung hergestellt werden.

1. Wählen Sie **Kommunikation > Kommunikation > Ethernet**.
   ⇨ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

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.

17.10.1.3 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 [➙ 91])

1. Wählen Sie **Kommunikation > Kommunikation > Modems**.
2. Klicken Sie auf **Aktivieren** und **Konfigurieren**.

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

17.10.1.3.1 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).

17.10.1.3.2 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.

17.10.1.3.3 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 [→ 110].
- **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**

17.10.1.3.4 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 ****.05.ON		Wo der Ausgang als „O5“ konfiguriert ist, wird er	Status von „O5“

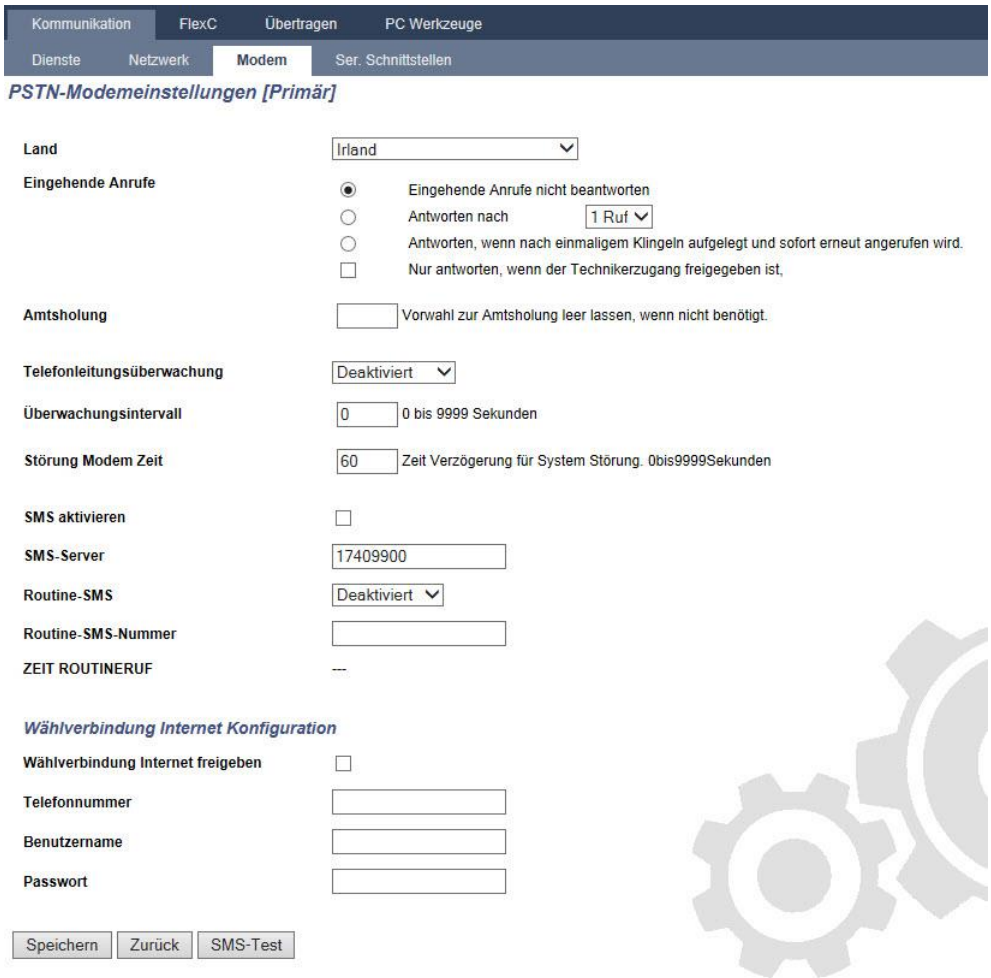
		eingeschaltet.	
**** O5.OFF ****.05.OFF		In den Fällen, in denen der Ausgang als „O5“ konfiguriert ist, wird er ausgeschaltet.	Status von „O5“

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.

17.10.1.3.5 PSTN-Modem

1. Wählen Sie **Kommunikation > Kommunikation > Modems > Konfigurieren**.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



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.

	Hinweis: Bei Veränderung dieser Einstellung wird das Modem zurückgesetzt. **Hinweis:** Auf GSM-Modems der Version 3.08 oder höher unterstützt.
Eingehende Anrufe	Für die Anrufannahme-Funktion des Modems sind folgende Einstellungen möglich: ● Keine Anrufe annehmen: Das Modem nimmt grundsätzlich keine Anrufe an. ● Nach x Ruftönen annehmen: Wählen Sie die Anzahl der Rufzeichen, nach welcher das Modem eingehende Anrufe annimmt. ● Anrufe annehmen, nachdem ein Teilnehmer das Modem anruft, nach 1 Rufton auflegt und direkt danach das Modem erneut anruft. Das SPC-System nimmt den Anruf nun automatisch an. ● Nur antworten, wenn der „Technikerzugang“ freigegeben ist
Amtsholung	Nummer eingeben, die erforderlich ist, um eine Amtsleitung zu belegen (z. B. bei einem Anschluss über eine Telefonanlage).
Telefonleitungsüberwachung	**PSTN-Modem:** Aktivieren Sie diese Option, um die Spannung der an das Modem angeschlossenen Telefonleitung zu überwachen. **GSM-Modem**: Aktivieren Sie diese Option, um den Signalpegel des mit dem Modem verbundenen GSM-Masten zu überwachen. Mit der Option **Ext. scharf** wird diese Funktion nur aktiviert, wenn das System extern scharf ist. **Hinweis**: EN 50131-9-Bestätigungskonfiguration Für die ordnungsgemäße Funktion der EN50131-9-Bestätigung muss der Leitungstest aktiviert sein. (siehe Systemoptionen [→ 239])
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. **Hinweis:** 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). **Hinweis**: 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).

Wird die SMS-Funktion über einen PSTN-Anschluss genutzt, muss die Telefonnummer des SMS-Dienstanbieters, 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-Dienstanbieter mit eigenen Telefonnummern für den SMS-Dienst.

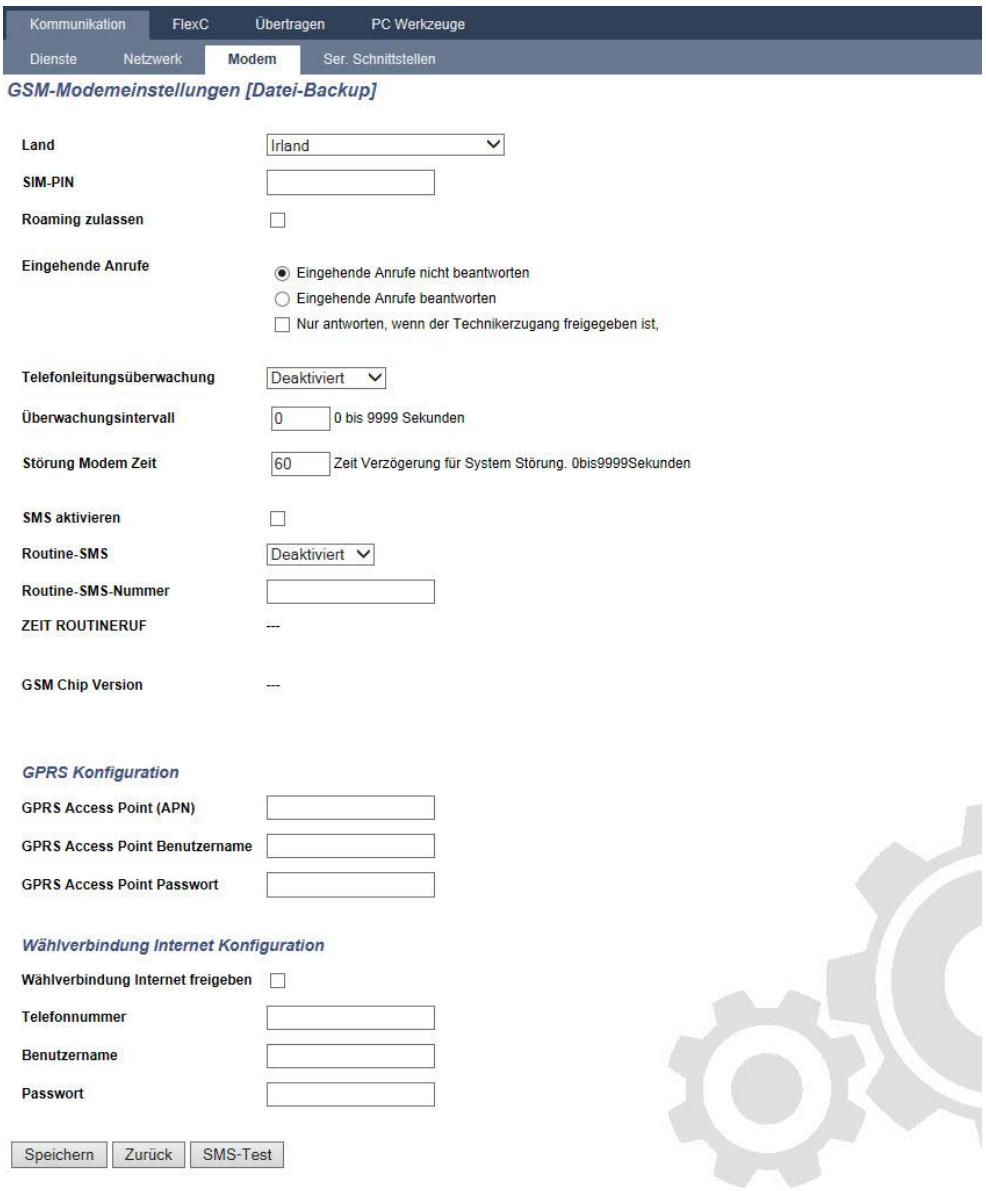
Diese Funktion kann nicht in allen Ländern genutzt werden. Bitte setzen Sie sich mit Ihrem Vertriebspartner vor Ort in Verbindung, um weiterführende Informationen zu erhalten (Unterstützung der Funktion, empfohlener Dienstanbieter).

Informationen zur Verfügbarkeit des Dienstes und die Nummern der SMS-Server erhalten Sie von den Dienstanbietern 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-Dienstanbieter.

17.10.1.3.6 GSM-Modem

▷ Ein GSM-Modem muss richtig installiert worden sein und fehlerfrei funktionieren.

1. Wählen Sie **Kommunikation > Kommunikation > Modems > Konfigurieren**.
   ⇨ Daraufhin erscheint das folgende Fenster:



2. Konfigurieren Sie die folgenden Felder:

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. **Hinweis**: Bei Veränderung dieser Einstellung wird das Modem zurückgesetzt. **Hinweis:** Auf GSM-Modems der Version 3.08 oder höher unterstützt.
Eingehende Anrufe	Für die Anrufannahme-Funktion des Modems sind folgende Einstellungen möglich: ● Keine Anrufe annehmen: Das Modem nimmt grundsätzlich keine Anrufe an. ● Nach x Ruftönen annehmen: Wählen Sie die Anzahl der Rufzeichen, nach welcher das Modem eingehende Anrufe annimmt. ● Anrufe annehmen, nachdem ein Teilnehmer das Modem anruft, nach 1 Rufton auflegt und direkt danach das Modem erneut anruft. Das SPC-System nimmt den Anruf nun automatisch an.

	● Nur antworten, wenn der „Technikerzugang“ freigegeben ist
Amtsholung	Nummer eingeben, die erforderlich ist, um eine Amtsleitung zu belegen (z. B. bei einem Anschluss über eine Telefonanlage).
Telefonleitungsüberwachung	**PSTN-Modem:** Aktivieren Sie diese Option, um die Spannung der an das Modem angeschlossenen Telefonleitung zu überwachen. **GSM-Modem**: Aktivieren Sie diese Option, um den Signalpegel des mit dem Modem verbundenen GSM-Masten zu überwachen. Mit der Option **Ext. scharf** wird diese Funktion nur aktiviert, wenn das System extern scharf ist. **Hinweis**: EN 50131-9-Bestätigungskonfiguration Für die ordnungsgemäße Funktion der EN50131-9-Bestätigung muss der Leitungstest aktiviert sein. (siehe Systemoptionen [→ 239])
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. **Hinweis:** 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). **Hinweis**: 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.

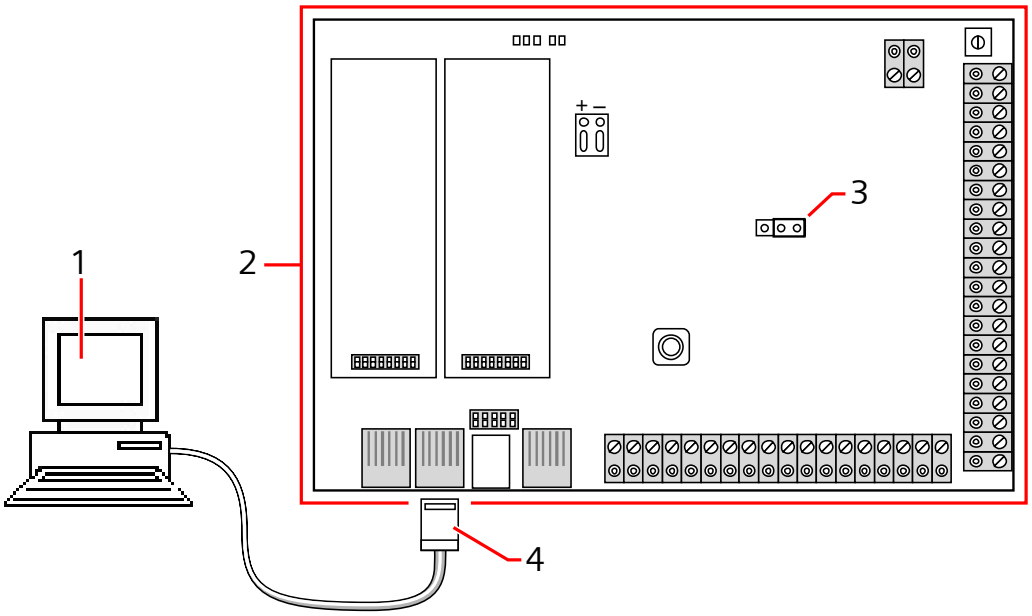
Hinweis: Der SMS-Test dient ausschließlich dem Zweck, die korrekte Funktionsweise der SMS-Funktion zu überprüfen. Verwenden Sie für den Funktionstest eine kurze Textnachricht mit alphabetischen Zeichen (A-Z).

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).

17.10.1.4 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 4000
4	RS232

Konfigurieren der seriellen Anschlüsse:

- Wählen Sie **Kommunikation > Kommunikation > Ser. Schnittstellen**.
  - ⇨ 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:

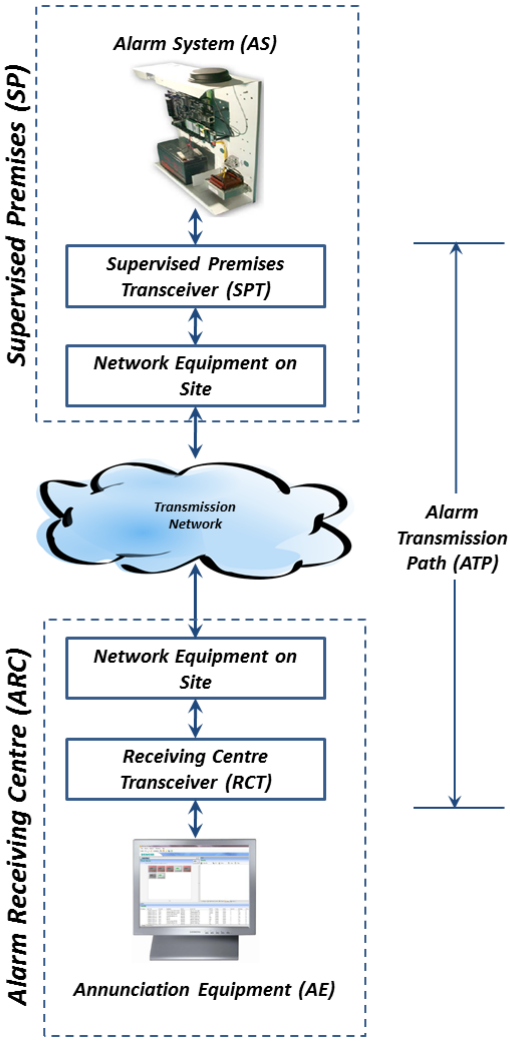
17.10.2 FlexC®

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.spcconnect.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.spcconnect.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 [→ 296]
- Konfigurieren von Ereignisprofilen [→ 310]
- Ereignis Ausnahmendefinition [→ 312]
- Konfigurieren von Steuerprofilen [→ 314]
- FlexC Status [→ 191]
- Konfigurieren eines EN50136-1-ATS oder kundenspezifischen ATS [→ 299]

17.10.2.1 Betriebsarten

Das System nutzt die Speichervermittlungsmethode beim Übertragen von Ereignissen.

Das SPC Alarmsystem sendet ein Ereignis zu der SPC COM XT und erwartet eine Übermittlungsbestätigung von der SPC COM XT um die Übermittlung als erfolgreich zu bestätigen. Die SPC COM XT wird nur dann eine Übermittlungsbestätigung senden, wenn das Ereignis erfolgreich in die SQL Datenbank geschrieben worden ist. Die SPC COM XT wird dann das Ereignis zum SPC COM XT Client und zur Sur-Gard Schnittstelle weiterleiten.

17.10.2.2 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 Steuerungsprofil (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

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 [→ 299].

4. Klicken Sie auf **Zurück**. Das ATS wird in der Tabelle **Konfig. Übertragungssystem** angezeigt.

Zentralen Kennung	
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 **Übertr.-Sys. Registrierung ID** in Betrieb nehmen. Für ein EN50136 ATS wird die **Übertr.-Sys. Registrierung ID** automatisch beim Klicken auf **Speichern** erstellt. Die Empfangszentrale kann die **Geräte-ID** an die Zentrale schicken, wenn sie verfügbar ist.
RCT Identification & Backup RCT Identification (Dual Path Dual Server Only) (Identifikation der Empfangszentrale und Backup-Empfangszentrale (nur Zwei-Wege-Dualserver))	
Empfangszentr.ID	Geben Sie die **Empfangszentr.ID** 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 **Server RCT ID** (Server-Empfangszentralen-ID) auf der Registerkarte **Serverdetails** eingegeben wurde. Weitere Informationen finden Sie im *Installations- und Konfigurationshandbuch des SPC Com XT*.
Empfangszentrale URL/ IP Adresse	Geben Sie die **Empfangszentrale URL/ IP Adresse** 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 **Server FlexC-Port** eingegeben wurde.
ÜW Schnittstelle	
EN50136 ATS Kategorie	Wählen Sie die EN50136-ATS-Kategorie (SP1-SP6, DP1-DP4). Eine Beschreibung der Kategorien finden Sie unter Zeiten für Übertragungssystemkategorien [→ 391].
Primäre Schnittstelle	Wählen Sie die **Primäre Schnittstelle** zur Anwendung auf den primären Kommunikationspfad aus den folgenden aus: ● Ethernet ● GPRS: Modem 1 ● GPRS: "Modem 2" ● Wählverbindung Internet: Modem 1 ● Wählverbindung Internet: "Modem 2"
Backup Schnittstelle	Wählen Sie für ein **Zwei-Wege-Übertragungssystem** eine der folgenden **Backup-Schnittstellen**, damit diese für die Backup-Kommunikation verwendet wird:

	• Ethernet • GPRS: Modem 1 • GPRS: "Modem 2" • Wählverbindung Internet: Modem 1 • Wählverbindung Internet: "Modem 2"

17.10.2.3 Konfigurieren eines EN50136-1-ATS oder kundenspezifischen ATS

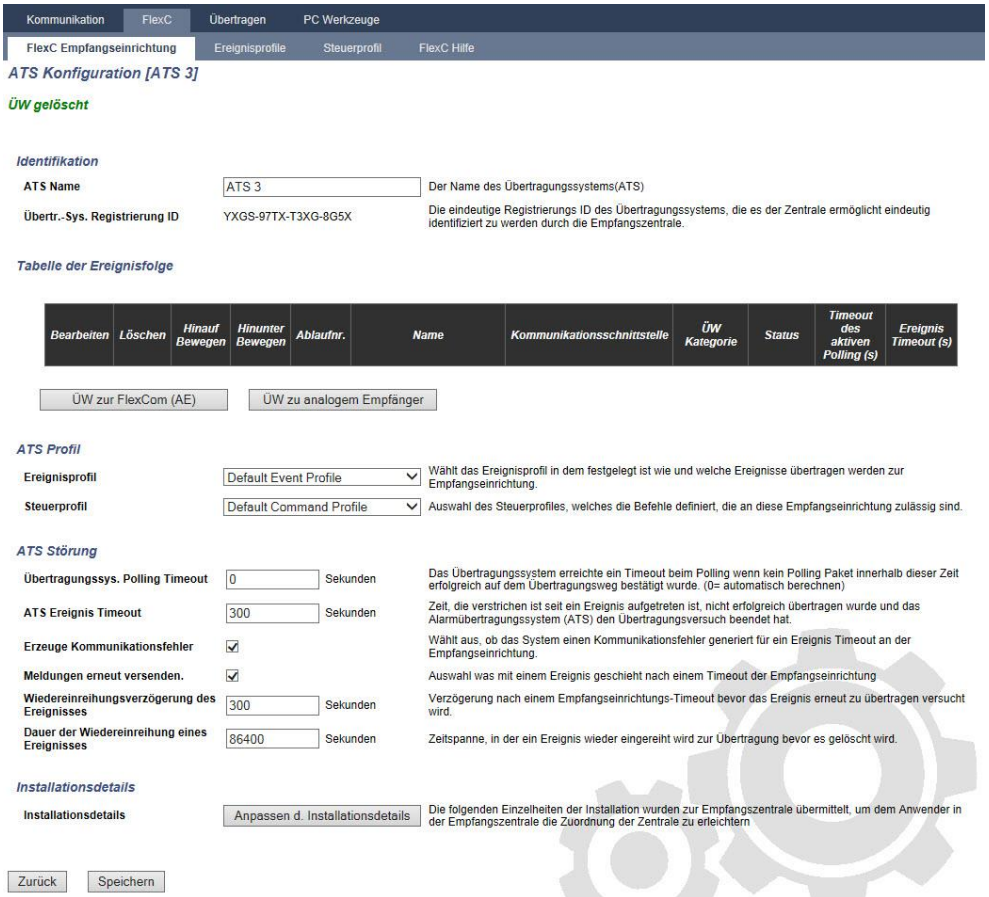
Ein ATS besteht aus einer Alarmzentrale, Netzwerkpfaden und einer Empfangszentrale (z. B. SPC Com XT). Es kombiniert einen oder mehrere Pfade zwischen einer SPC-Zentrale und einer Empfangszentrale. Sie können in ein ATS bis zu 10 ÜWs hinzufügen.

!	*HINWEIS*
	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 [→ 296].

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 [→ 296].
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.



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) [➙ 301]). Oder klicken Sie auf **ÜW zu analogem Empfänger** (siehe ÜW zu analogem Empfänger [➙ 306]).
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 [➙ 310].
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 [➙ 314].
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 [➙ 307].
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.

!	*HINWEIS*
	Die **Übertr.-Sys. Registrierung ID wird automatisch für ein ATS erstellt.** Sie identifiziert eindeutig die Empfangszentrale für den ÜW. Falls Sie die **Geräte ID** nicht kennen, können Sie die Zentrale mithilfe dieser **Übertr.-Sys. Registrierung ID** in Betrieb nehmen. Der CMS-Bediener muss außerdem diese **Übertr.-Sys. Registrierung ID** in der Empfangszentrale (z. B. SPC Com XT) eingeben. Siehe *Installations- und Konfigurationshandbuch des SPC Com XT*).

Übertragungssys. Polling Timeout	Dieses Feld wird automatisch durch Hinzufügen der Werte aus der Spalte **Timeout des aktiven Polling** 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 **Timeout des aktiven Polling** 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.
Wiedereinreihungsverzögerung des Ereignisses	Die Verzögerung nach einem Empfangseinrichtungstimeout, bevor das Ereignis erneut zu übertragen versucht wird. Standard: 300 Sekunden.
Dauer der Wiedereinreihung eines Ereignisses	Die Zeitspanne, in der ein Ereignis wieder zur Übertragung eingereiht wird, bevor es gelöscht wird. Standard: 86.400 Sekunden.

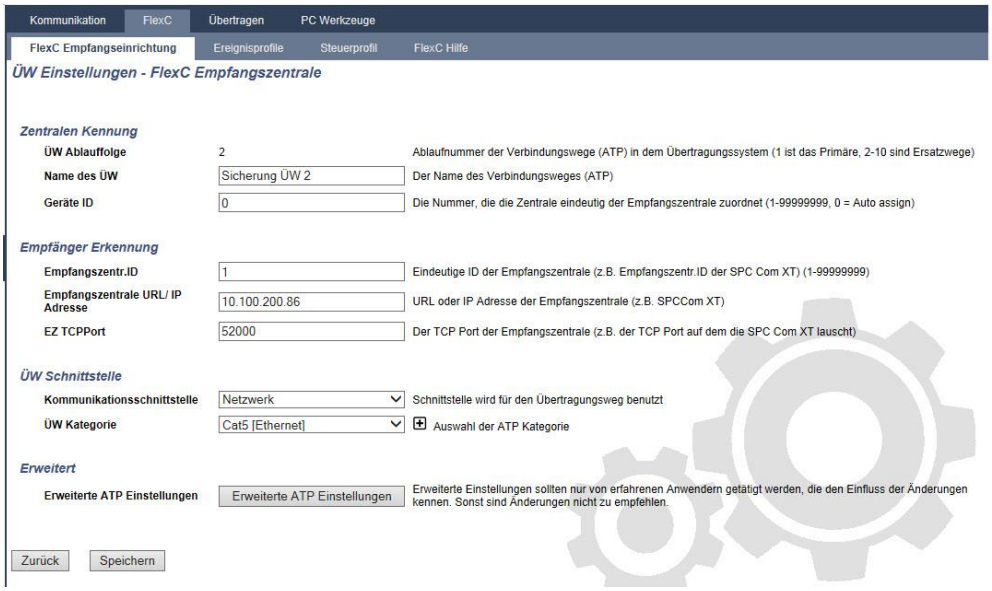
Siehe auch

Zeiten für Übertragungssystemkategorien [→ 391]

17.10.2.2.1 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)**.



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 [→ 303].
3. Klicken Sie auf **Speichern**.

⚠ WARNUNG

Es wird nicht empfohlen, die **Erweiterten ATP-Einstellungen** zu ändern. Änderungen dürfen nur von erfahrenen Benutzern vorgenommen werden.

Zentralen Kennung	
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.
Empfänger Erkennung	
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 **Server RCT ID** (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 **Server FlexC Port** im Server Configuration Manager-Tool

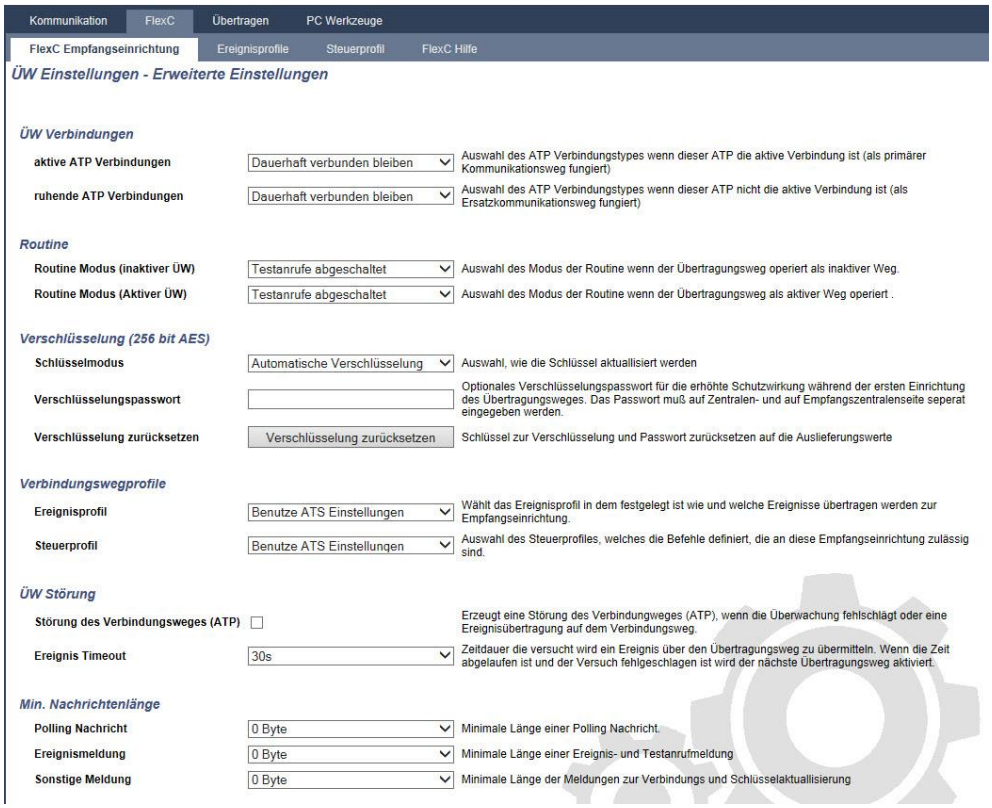
	übereinstimmen. Siehe *Installations- und Konfigurationshandbuch des SPC Com XT*.
ÜW Schnittstelle	
Kommunikationsschnittstelle	Wählen Sie aus der Dropdown-Liste die Schnittstelle, die der ÜW für die Kommunikation verwendet. ● Ethernet ● GPRS: Modem 1 ● GPRS: Modem 2 ● Wählverbindung Internet: Modem 1 ● Wählverbindung Internet: Modem 2
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 [→ 392].
Erweitert	
Erweiterte ATP Einstellungen	Es wird nicht empfohlen, die erweiterten Einstellungen zu ändern. Änderungen dürfen nur von erfahrenen Benutzern vorgenommen werden.

17.10.2.2.1.1 Konfigurieren der erweiterten ATP-Einstellungen

⚠ WARNUNG

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**.



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

2. Klicken Sie auf **Speichern**.

ÜW Verbindungen	
Aktive ATP Verbindungen	Wählen Sie den ÜW-Verbindungstyp, wenn der ÜW als der primäre Kommunikationspfad betrieben wird. ● Permanent: Verbunden bleiben ● Vorübergehend: Abbruch 1 Sekunde ● Vorübergehend: Abbruch 20 Sekunden ● Vorübergehend: Abbruch 80 Sekunden ● Vorübergehend: Abbruch 3 Minuten ● Vorübergehend: Abbruch 10 Minuten ● Vorübergehend: Abbruch 30 Minuten
Ruhende ATP Verbindungen	Wählen Sie den ÜW-Verbindungstyp, wenn der ÜW als ein Backup-Kommunikationspfad betrieben wird. ● Permanent: Verbunden bleiben ● Vorübergehend: Abbruch 1 Sekunde ● Vorübergehend: Abbruch 20 Sekunden ● Vorübergehend: Abbruch 80 Sekunden ● Vorübergehend: Abbruch 3 Minuten ● Vorübergehend: Abbruch 10 Minuten ● Vorübergehend: Abbruch 30 Minuten
Routine	
Routine Modus (inaktiver ÜW)	Wählen Sie den Modus für den Versand der Testanrufe, wenn der ÜW der inaktive ÜW ist. ● Testanrufe abgeschaltet ● Testanruf alle 10 Minuten ● Testanruf jede Stunde ● Testanruf alle 4 Stunden ● Testanruf alle 24 Stunden ● Testanruf alle 48 Stunden ● Testanruf alle 7 Tage ● Testanruf alle 30 Tage
Routine Modus (Aktiver ÜW)	Wählen Sie den Modus für den Versand der Testanrufe, wenn der ÜW der aktive ÜW ist. ● Testanrufe abgeschaltet ● Testanruf alle 10 Minuten ● Testanruf jede Stunde ● Testanruf alle 4 Stunden ● Testanruf alle 24 Stunden ● Testanruf alle 48 Stunden ● Testanruf alle 7 Tage Testanruf alle 30 Tage
Verschlüsselung (256 bit AES)	
Schlüsselmodus	Wählen Sie, wie die Verschlüsselung aktualisiert werden soll. ● Automatische Verschlüsselung ● Automatische Verschlüsselung mit Aktualisierungen ● Fixe Verschlüsselung 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.
Verschlüsselungspasswort	Optionales Passwort für eine erhöhte Sicherheit während der ersten Inbetriebnahme des ÜW. Das Passwort muss unabhängig im SPT oder in der Empfangszentrale eingegeben werden.
Verschlüsselung zurücksetzen	Setzt den Schlüssel für die Verschlüsselung und das Kennwort auf die Standardwerte zurück.
Verbindungswegprofile	
Ereignisprofil	Wählt das Ereignisprofil in dem festgelegt ist, wie und welche Ereignisse an dieses ATS übertragen werden. ● Benutze ATS Einstellungen ● Vorgegebenes Ereignisprofil ● Alle Ereignisse
Steuerprofil	Auswahl des Steuerprofils, das die Befehle definiert, die in diesem ATS zulässig sind. ● Benutze ATS Einstellungen ● Vorgegebenes Steuerungsprofil ● Custom Command Profile (Kd.spez. Steuerungsprofil)
ÜW Störung	
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. ● 30 Sekunden ● 60 Sekunden ● 90 Sekunden ● 2 Minuten ● 3 Minuten ● 5 Minuten ● 10 Minuten
Min. Nachrichtenlänge	
Polling Nachricht	Minimallänge einer Polling-Nachricht. ● 0 Byte ● 64 Byte ● 128 Byte ● 256 Byte ● 512 Byte
Ereignismeldung	Minimallänge eines Ereignisses und einer Testanrufnachricht. ● 0 Byte ● 64 Byte ● 128 Byte ● 256 Byte

	• 512 Byte
Sonstige Meldung	Minimallänge des Verbindungs- und Verschlüsselungsschlüssels und der Aktualisierungsmeldungen. • 0 Byte • 64 Byte • 128 Byte • 256 Byte • 512 Byte

17.10.2.2.2 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**.

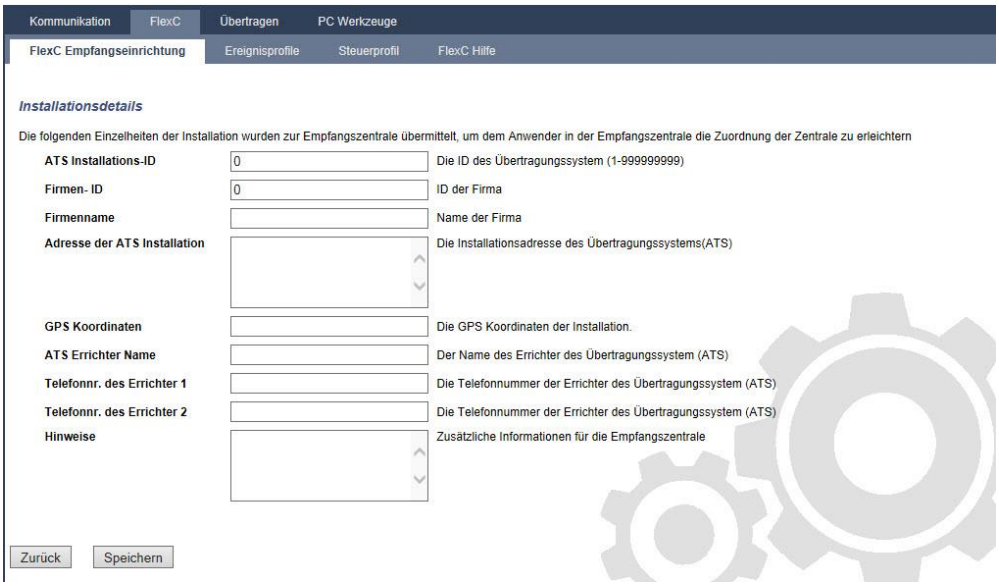
Zentralen Kennung	
ÜW Ablauffolge	Das Feld enthält die Sequenznummer des ÜW in der ATS-Konfiguration. Nummer 1 ist primär, die Nummern 2 bis 10 sind Backups.
ATP Unique ID	Diese ID identifiziert eindeutig den ÜW in der Empfangszentrale.
Name des ÜW	Geben Sie einen Namen für den ÜW ein.
Geräte ID	Geben Sie eine Zahl (1–999999) ein, um die Zentrale eindeutig in der Empfangszentrale zu identifizieren.
ARC Verbindung	
Nummer 1	Telefonnummer 1
Nummer 2	Telefonnummer 2
Modem Auswahl	Wählen Sie das zu verwendende Modem. • Modem 1 • Modem 2
Routine	
Routine Modus (inaktiver ÜW)	Wählen Sie den Modus für den Versand der Testanrufe, wenn der ÜW im inaktiven Modus ist. Standard: 24 Stunden. • Testanrufe deaktiviert • Testanruf alle 10 Minuten • Testanruf jede Stunde • Testanruf alle 24 Stunden • Testanruf alle 48 Stunden • Testanruf alle 7 Tage • Testanruf alle 30 Tage.
Routine Modus (Aktiver ÜW)	Wählen Sie den Modus für den Versand der Testanrufe, wenn der ÜW ein aktiver ÜW ist. Standard: 24 Stunden. • Testanrufe deaktiviert • Testanruf alle 10 Minuten • Testanruf jede Stunde

	● Testanruf alle 24 Stunden ● Testanruf alle 48 Stunden ● Testanruf alle 7 Tage ● Testanruf alle 30 Tage.
Zeit des ersten Testanrufes	Die Zeit des ersten Testanrufs nach dem Zurücksetzen oder nach der ATS-Initialisierung. ● Sofort Senden (Standard) ● oder ● Wählen Sie ein halbstündliches Intervall zwischen 00:00 und 23:30.
Ereignisprotokoll	
Protokoll	Das verwendete Übertragungsprotokoll. ● SIA ● SIA Extended 1 ● SIA Extended 2 ● Contact-ID
Ereignisprofil	Wählt das Ereignisprofil in dem festgelegt ist, wie und welche Ereignisse an dieses ATS übertragen werden. ● Benutze ATS Einstellungen ● Vorgegebenes Ereignisprofil ● Vorgabe Portal Ereignis Profil ● Alle Ereignisse ● Kundenspezifisches Ereignisprofil
ÜW Störung	
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. Standard: 2 Minuten ● 30 Sekunden ● 60 Sekunden ● 90 Sekunden ● 2 Minuten ● 3 Minuten ● 5 Minuten ● 10 Minuten

17.10.2.2.3 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.

17.10.2.4 Konfigurieren eines SPC-Connect-Übertragungssytems (ATS)

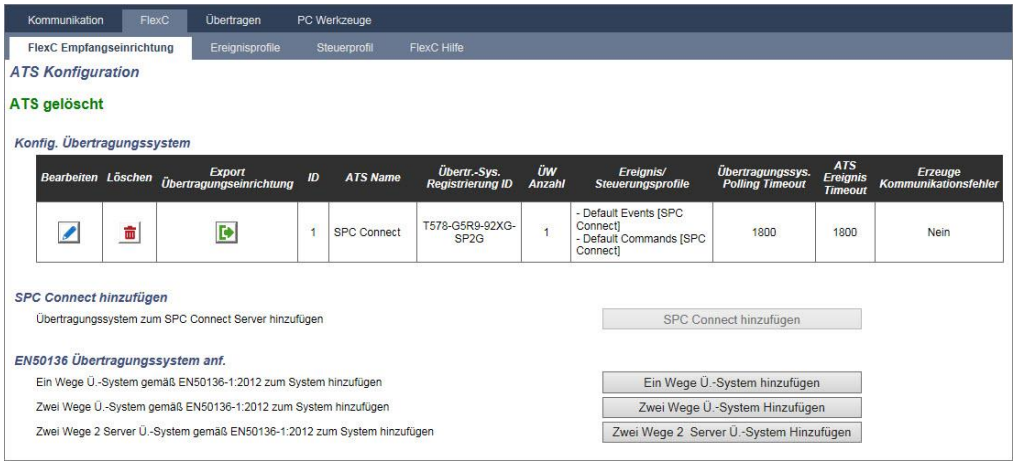
Die Funktion **SPC Connect**ATS **hinzufügen** stellt die Kommunikation zwischen der Zentrale (SPT) und dem **SPC Connect**-Server (Empfangszentrale, www.spcconnect.com) her. Mit der generierten SPC Connect ATS-Registrierungs-ID kann ein Zentralenbenutzer ein Benutzerkonto und eine Zentrale auf der SPC 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) [→ 301].
- Standardmäßiges Ereignisprofil für SPC Connect

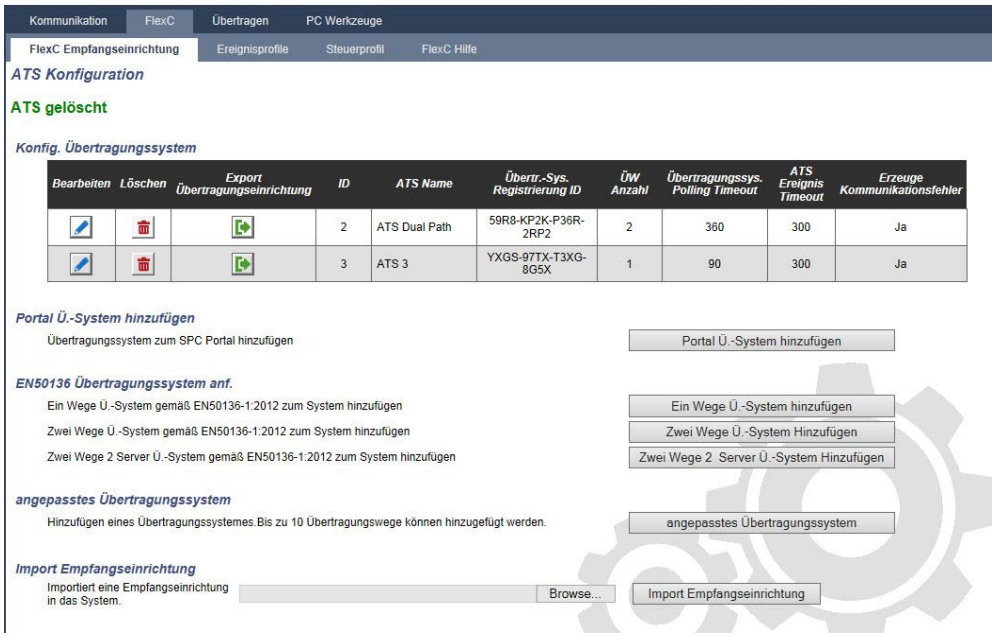
- Standardmäßiges Befehlsprofil für SPC Connect
- Die standardmäßige Empfangszentralen-URL lautet www.spcconnect.com.
- Der SPT-Kontocode für den ÜW wird aufgefüllt.
- Notieren Sie sich die SPC Connect **ATS-Registrierungs-ID** und übergeben Sie sie dem Kunden zusammen mit dem *SPC Connect-Benutzerhandbuch*.



17.10.2.5 Exportieren und Importieren eines ATS

ATS-Dateien tragen die Erweiterung „.cxml“. Sie müssen das ATS im SPC-Browser erstellen und es exportieren, bevor Sie es in ein System importieren können.

1. Öffnen Sie zum Exportieren eines ATS den Menüpfad **Kommunikation > FlexC > FlexC Empfangseinrichtung**.
2. Suchen Sie in der Tabelle **Konfig. Übertragungssystem** das zu exportierende ATS, und klicken Sie auf die Schaltfläche **Export Übertragungseinrichtung** (grüner Pfeil).



3. Speichern Sie die Datei mit den Standarddateinamen **export_flexc.cxml** oder benennen Sie sie um.
4. Sie können die Datei im Notepad öffnen.

5. Öffnen Sie zum Importieren eines ATS in das System den Menüpfad **Kommunikation > FlexC > FlexC Empfangseinrichtung**.
6. Blättern Sie zu **Import Empfangseinrichtung**.
7. Klicken Sie auf die Schaltfläche **Durchsuchen**, und wählen Sie ein zu importierendes ATS (Dateierweiterung „.cxml“).
8. Klicken Sie auf **Import Empfangseinrichtung**.

⇨ Das ATS wird in der Tabelle **Konfig. Übertragungssystem** mit der verfügbaren ID angezeigt.

!	Wenn Sie ein ATS exportieren, ändert sich die Geräte ID in 0. Dadurch wird verhindert, dass ein ATS exportiert und importiert wird und anschließend ein vorhandenes ATS repliziert wird.

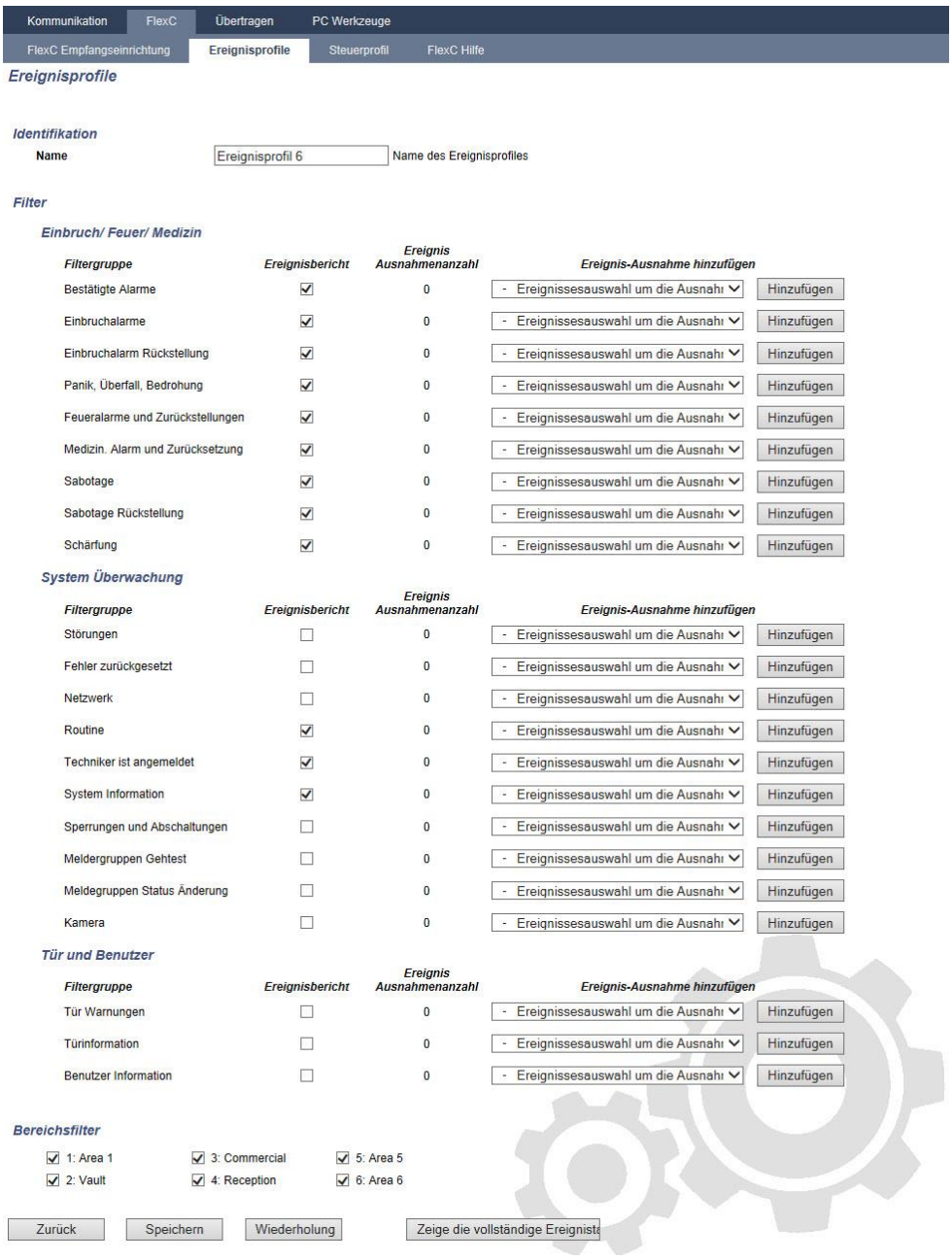
17.10.2.6 Konfigurieren von Ereignisprofilen

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 [→ 312].

!	*HINWEIS*
	Wählen Sie zur Anzeige der Liste aller Ereignisse die Optionen **Kommunikation > FlexC > Ereignisprofile.** Klicken Sie für ein Ereignisprofil auf **Bearbeiten** (blauer Stift). Blättern Sie zum Ende des Bildschirms, und klicken Sie auf **Zeige die vollständige Ereignistabelle**.

!	*HINWEIS*
	Wählen Sie für eine schnelle Erstellung eines neuen Ereignisprofils die Optionen **Kommunikation > FlexC > Ereignisprofile**. Wählen Sie in der Tabelle **Ereignisprofile** ein Ereignisprofil, und klicken Sie auf die Schaltfläche „Bearbeiten“ (blauer Stift). Blättern Sie zum Ende des Bildschirms, und klicken Sie auf **Wiederholung**. Nun können Sie die erforderlichen Änderungen vornehmen.

1. Wählen Sie zur schrittweisen Konfiguration von FlexC-Ereignisprofilen die Optionen **Kommunikation > FlexC > Ereignisprofile**.
2. Klicken Sie auf **Hinzufügen**. Das Fenster **Ereignisprofile** wird angezeigt.



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 [→ 312].
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.

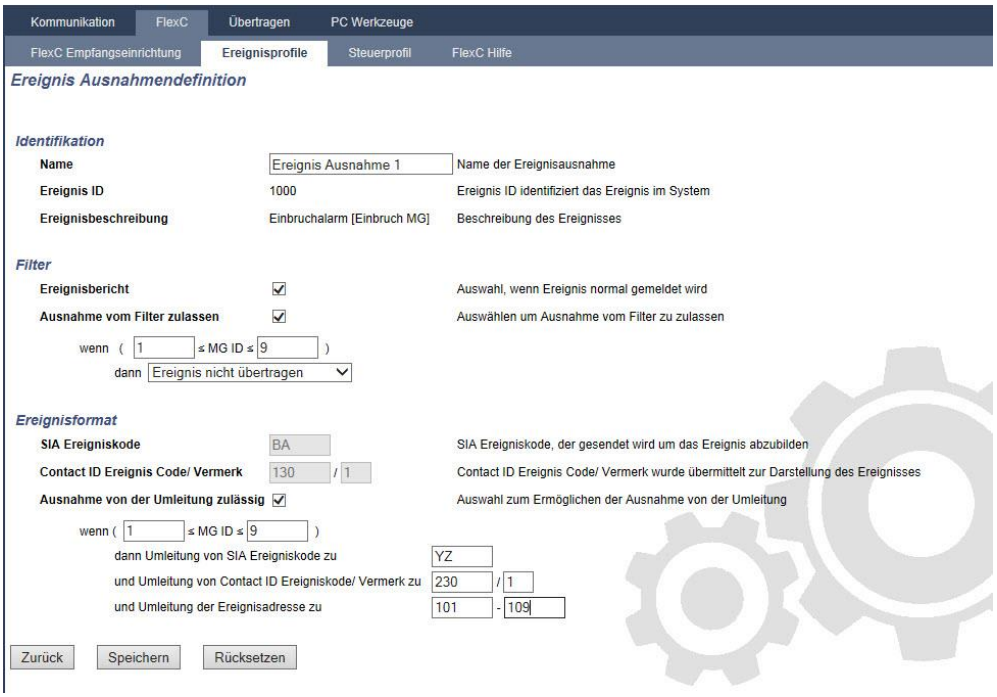
17.10.2.5.1 Ereignis Ausnahmendefinition

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)

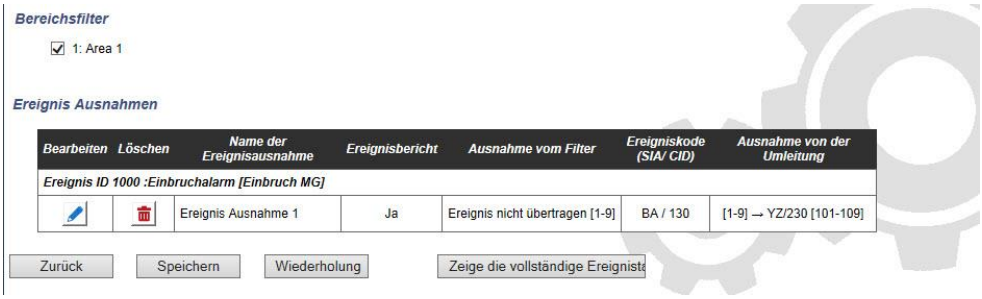
In der Filtergruppe **Einbruchalarme** können Sie beispielsweise eine Ereignisausnahme für einen Bereich von MG-IDs im Ereignis „Einbruchalarm“ (EA) wie folgt definieren:

- 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



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.



1. Klicken Sie auf das Symbol **Bearbeiten**, um Änderungen vorzunehmen, oder klicken Sie auf das Symbol **Löschen**, um eine **Ereignisausnahme** 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.

Identifikation	
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.
Ereignisfilter	
Ereignisbericht	Aktivieren Sie dieses Kontrollkästchen, um das Ereignis zu melden. Dadurch wird der für die Ereignisfiltergruppe festgelegte Berichtswert überschrieben. Falls die Filtergruppe **Einbruchalarme** 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 **Ereignisbericht** auszuschließen.
wenn (0 ≤ *MG-ID* ≤ 9999) dann Ereignisbericht/Ereignis nicht übertragen	Geben Sie einen Bereich von Adressen ein, um sie von der Einstellung **Ereignisbericht** auszuschließen. Wenn Sie beispielsweise den Ereignistyp „Einbruchsalarm“ melden, können Sie wählen, die *MG-ID 1–9* nicht für dieses Ereignis zu melden. Alternativ können Sie wählen, den Ereignistyp „Einbruchsalarm“ nicht zu melden und die *MG-ID 1–9* für dieses Ereignis zu melden.
Ereignisformat	
SIA Ereigniskode	Der standardmäßige SIA-Ereigniscode, 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

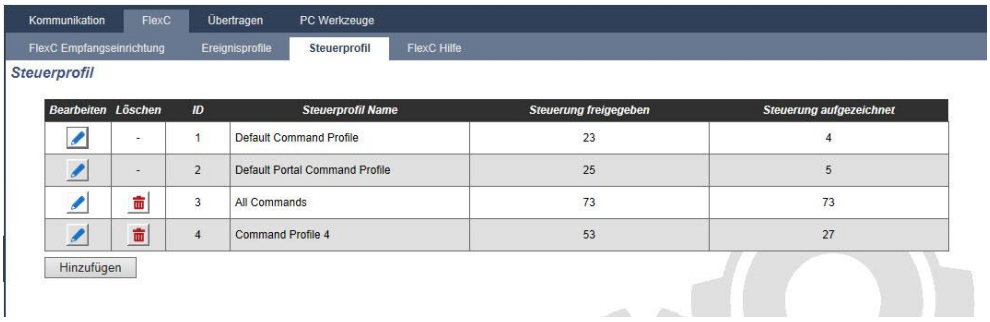
	die Ereignisadresse den kundenspezifischen Werten hinzuzufügen (z. B. zur Neuzuordnung der *MG-IDs 1–9* zu den *MG-IDs 101–109*. Bei Aktivierung werden die unteren Felder angezeigt.
wenn (0 ≤ *MG-ID* ≤ 9999)	Geben Sie den Adressbereich ein, der für ein Ereignis neu zugeordnet werden soll. Wenn Sie beispielsweise die *MG-IDs 1–9* den *MG-IDs 101–109* neu zuordnen möchten, geben Sie *1* und *9* ein. Die Menge der Adressen im Bereich muss der Menge der im unteren Feld **Umleitung der Ereignisadresse zu** 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 *MG-IDs 1–9* den *MG-IDs 101–109* neu zuordnen möchten, geben Sie *101 und 109* ein.

17.10.2.7 Konfigurieren von Steuerprofilen

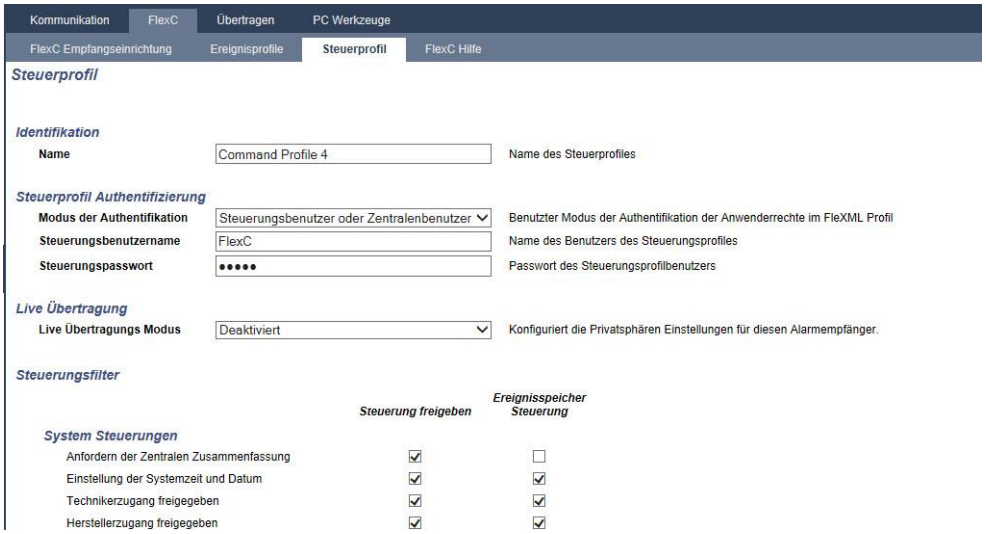
Das Steuerprofil definiert die Befehle, die in einem ATS zulässig sind. Dieses Profil bestimmt, wie ein CMS eine Zentrale steuern kann. Das standardmäßige Steuerprofil unterstützt keine Videoverifikation.

!	*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.



- Klicken Sie auf **Hinzufügen**.



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).

!	*HINWEIS*
	Der standardmäßige **Steuerungsbenutzername** 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 **Vorgegebenes Steuerungsprofil**, ein **Vorgabe Portal Steuerungs Profil** oder ein Steuerprofil nicht löschen, wenn es einem ATS zugewiesen ist.

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 Datenschutzoptionen für das Streaming zu bestimmen. **Immer** erzeugt das höchste Datenvolumen.
6. Wählen Sie unter **Steuerungsfilter** die zu aktivierenden Befehle. Eine vollständige Liste der Befehl finden Sie unter FlexC-Steuerung [→ 389].
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).

17.10.3 Übertragen

17.10.3.1 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.

17.10.3.1.1 Hinzufügen/Bearbeiten von Empfängern mithilfe von SIA oder CID

▷ Ein PSTN- oder GSM-Modem ist installiert und funktioniert ordnungsgemäß.

1. Wählen Sie **Kommunikation > Übertragen > Analoge ARC**.
   ⇨ Daraufhin erscheint das folgende Fenster:

2. Klicken Sie auf die Schaltfläche **Modem1/2**, um entweder von Modem 1 oder Modem 2 einen Übertragungstest an den Empfänger durchzuführen.
3. Klicken Sie auf **Logbuch**, um eine Protokolldatei abzurufen. Ein Fenster mit den Protokollen aller automatischen und manuellen Übertragungstests wird angezeigt.
4. Um einen Empfänger hinzuzufügen oder zu bearbeiten, klicken Sie auf **Hinzufügen** – ODER –
   auf **Bearbeiten**.
   ⇨ Daraufhin erscheint das folgende Fenster.
5. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

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). **Hinweis**: 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.

- Klicken Sie auf **Hinzufügen**, um diese Informationen im System einzugeben.

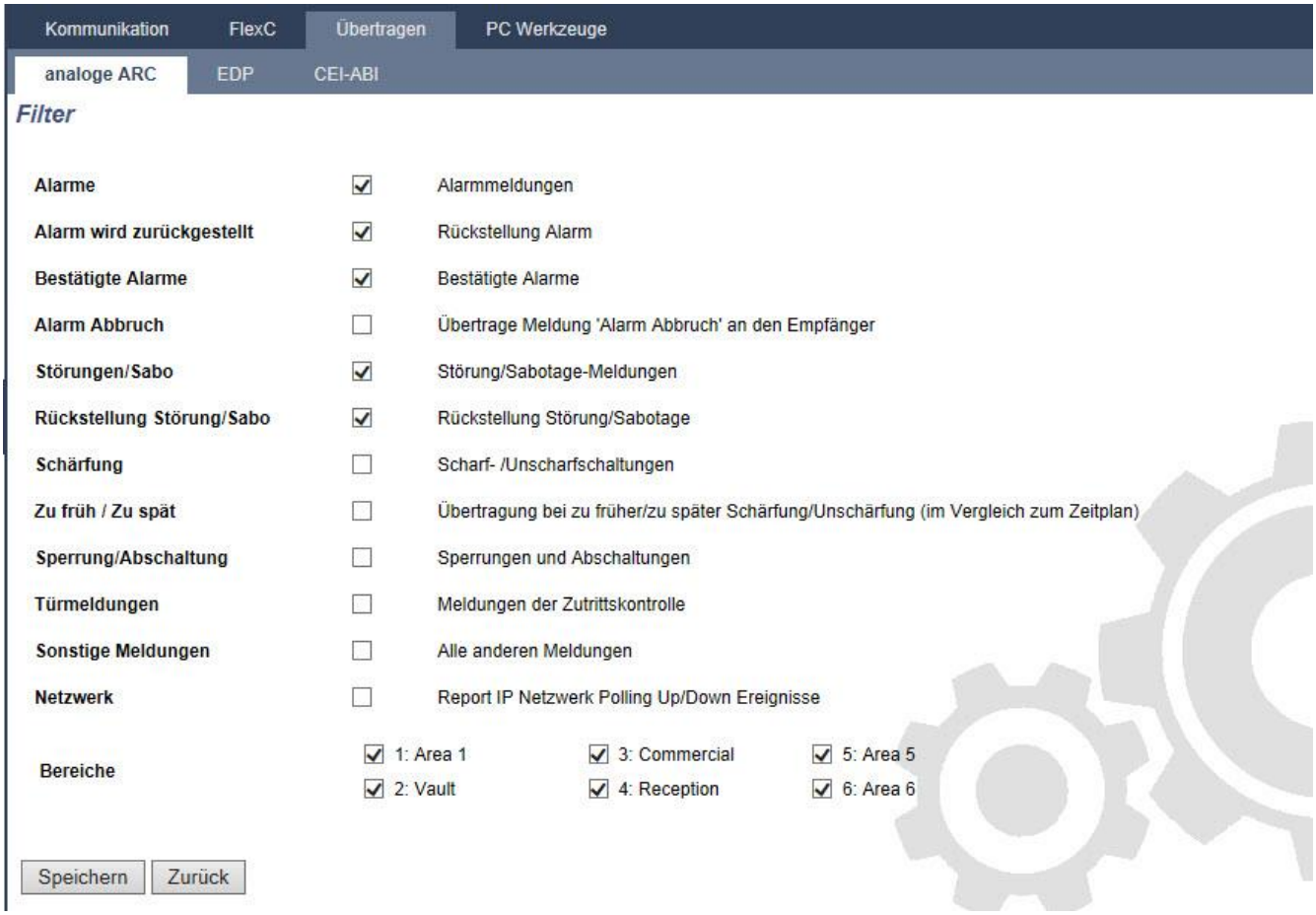
⇨ Im Browser wird eine Liste der konfigurierten Empfänger-Konten angezeigt mit der Identnummer, der Beschreibung, dem Protokoll, dem Status der Wählverbindungen und der Uhrzeit und dem Datum der letzten Verbindung zum Empfänger.

17.10.3.1.2 Bearbeiten von Empfängerfiltern mithilfe von SIA oder CID

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

1. Wählen Sie **Kommunikation > Übertragen > analoge ARC > Bearbeiten > Filter**.

   ⇨ Daraufhin erscheint das folgende Fenster:



2. Konfigurieren Sie die folgenden Felder:

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 Systemalarme 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).

17.10.3.1.3 Bearbeiten eines Empfängerfilters mithilfe von Fast Format

So konfigurieren Sie die Ereignisse auf dem SPC, die einen Anruf an den Empfänger auslösen, wenn **Fast Format** das ausgewählte ist:

- Wählen Sie **Kommunikation > Übertragen > Analoge ARC > Bearbeiten > Filter**.

1. Eine Liste der acht Kanäle wird zusammen mit den Alarmbedingungen angezeigt, die für jeden Kanal programmiert werden können. Wählen Sie die Alarmbedingungen für jeden Kanal nach Bedarf. Die jeweilige Beschreibung finden Sie unter Ausgangstypen und Ausgangsschnittstellen [→ 213].
2. Wählen Sie aus dem Dropdown-Menü **Umfang** den Eintrag **System** oder einen bestimmten Bereich, um Ihre ausgewählten Einstellungen anzuwenden.
3. Klicken Sie auf die Schaltfläche **Test** neben dem ersten Kanal, um die Alarmaktivierung zu testen.
   ⇨ Das Glühbirnensymbol leuchtet auf.
4. Warten Sie etwa fünf Sekunden, und klicken Sie anschließend erneut auf die Schaltfläche **Test** für den gleichen Kanal. Dadurch wird eine Kanalwiederherstellung an den Empfänger geschickt, und das Glühlampensymbol wird deaktiviert.
5. Fahren Sie mit dem Test der anderen Kanäle fort.

17.10.3.2 EDP-Einstellung

IP

Das System bietet die Möglichkeit, unter Verwendung des EDP-Protokolls (**E**nhanced **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 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)

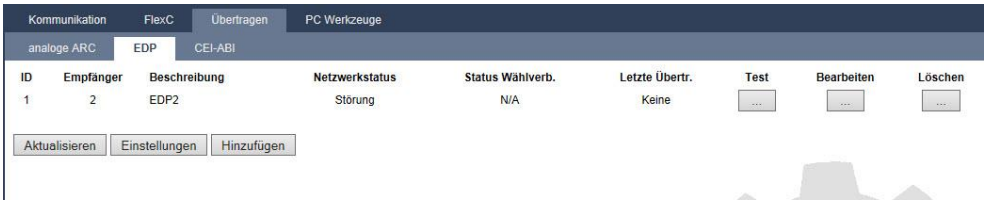
Bei Verwendung des PSTN-Netzes ist darauf zu achten, dass das PSTN-Modem ordnungsgemäß installiert ist und korrekt funktioniert und dass eine funktionierende PSTN-Leitung an die Anschlüsse A, B am PSTN-Modem angeschlossen ist.

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 [→ 170]) und dass der Internetzugang am Router aktiviert ist.

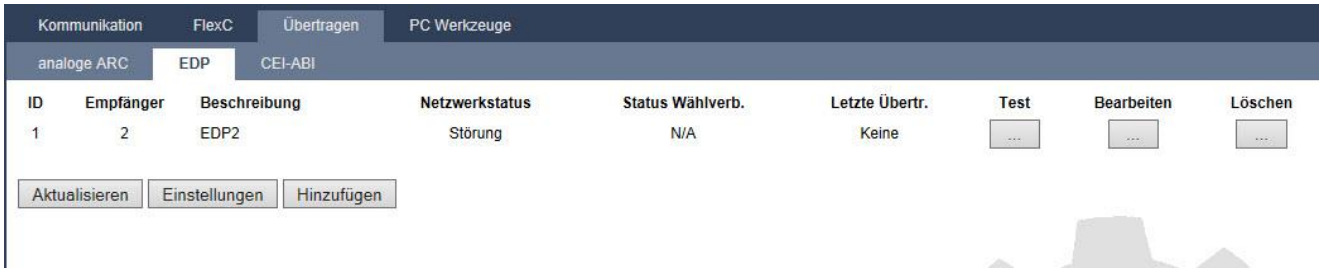
17.10.3.2.1 Hinzufügen eines EDP-Empfängers

1. Wählen Sie **Kommunikation > Übertragen > EDP**.
   ⇨ Daraufhin erscheint das folgende Fenster:



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

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
   ⇨ Daraufhin erscheint das folgende Fenster.



3. Weitere Informationen finden Sie in der nachstehenden Tabelle.

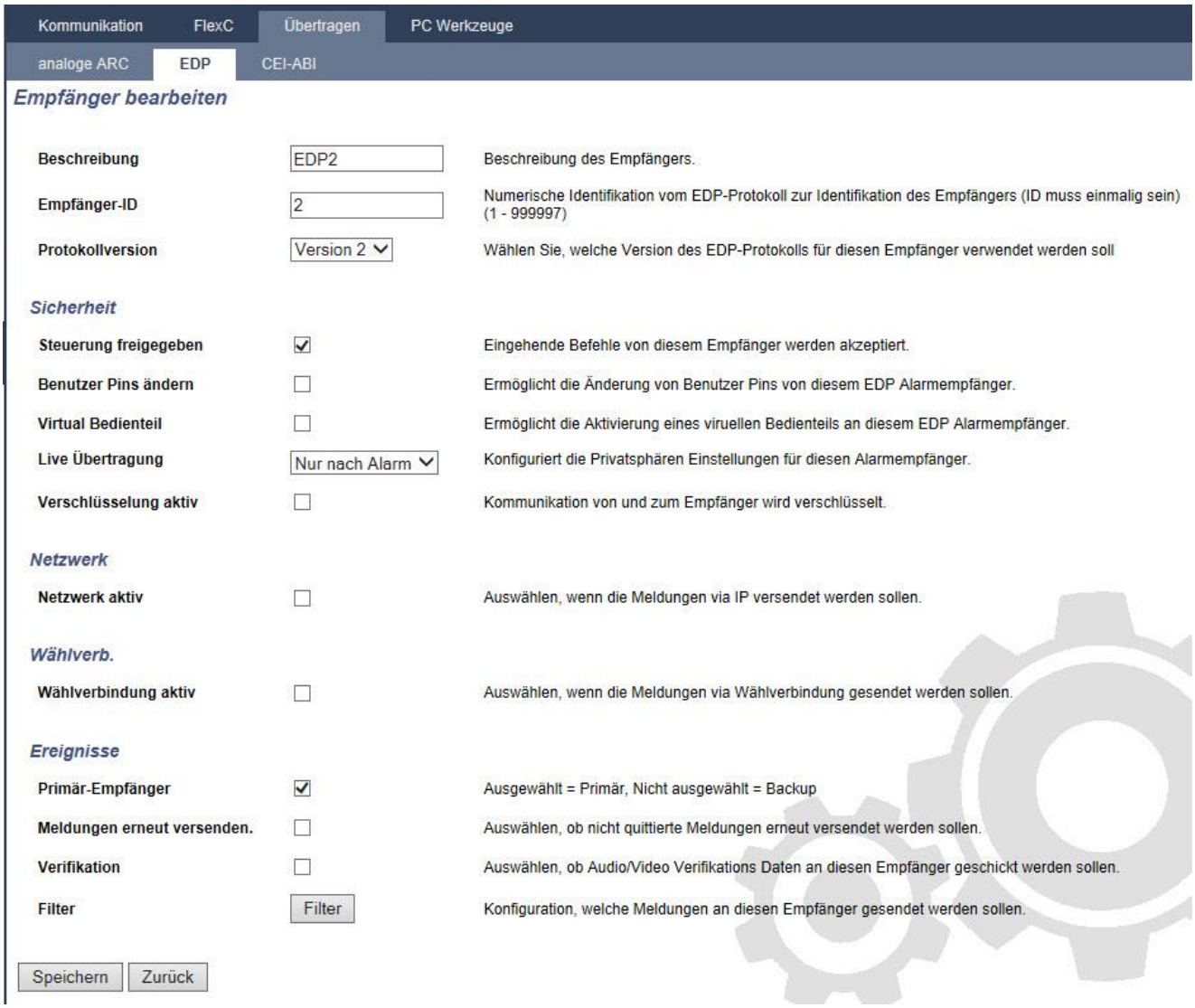
Beschreibung	Geben Sie eine Beschreibung des Empfängers ein.
Empfänger-ID	Geben Sie eine eindeutige Nummer ein, die vom EDP zur Identifizierung des Empfängers verwendet wird.

Siehe auch

Bearbeiten der Einstellungen des EDP-Empfängers [→ 321]

17.10.3.2.2 Bearbeiten der Einstellungen des EDP-Empfängers

1. Wählen Sie **Kommunikation > Übertragen > EDP > Bearbeiten**.
   ⇨ Daraufhin erscheint das folgende Fenster.
2. 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: ● Polling-Intervall von 8 s

	● Erzwungenes TCP-Protokoll ● TCP-Versuche schlagen nach weniger als 10 s fehl (ca. 9 s) ● EDP-Ereignisversuche werden unabhängig von der globalen Einstellung zur Anzahl der erneuten Übertragungsversuche in den EDP-Einstellungen auf 1 gesetzt. ● FTC wird innerhalb von 20 Sekunden nach einem Netzwerkausfall generiert.

Sicherheit	
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. **Hinweis**: 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“. **Hinweis**: 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.
Netzwerk (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.
Wählverb (Gilt nur für GPRS-Modemverbindungen)	
Wählverbindung	Aktivieren, damit Ereignisse über eine Wählverbindung gemeldet

aktiv	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.
Ereignisse	
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 quittierte 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 [→ 324].

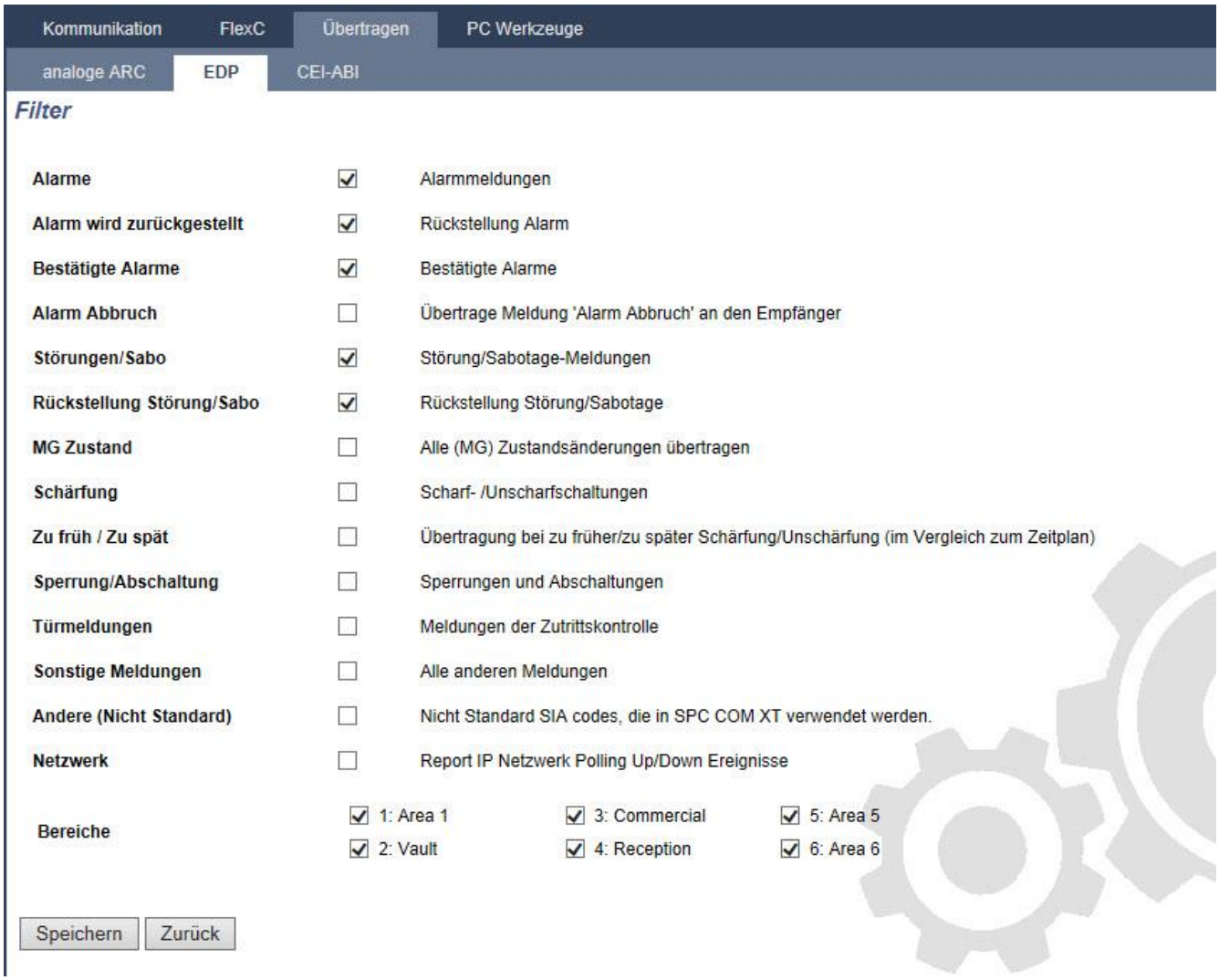
* EDP-Wählverbindung über PSTN wird in dieser Version nicht unterstützt.

Siehe auch

- Konfiguration von SMS [→ 203]

17.10.3.2.3 Meldungsfilter-Einstellungen bearbeiten

1. Wählen Sie **Kommunikation > Übertragen > EDP > Bearbeiten > Filter**.
   ⇨ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



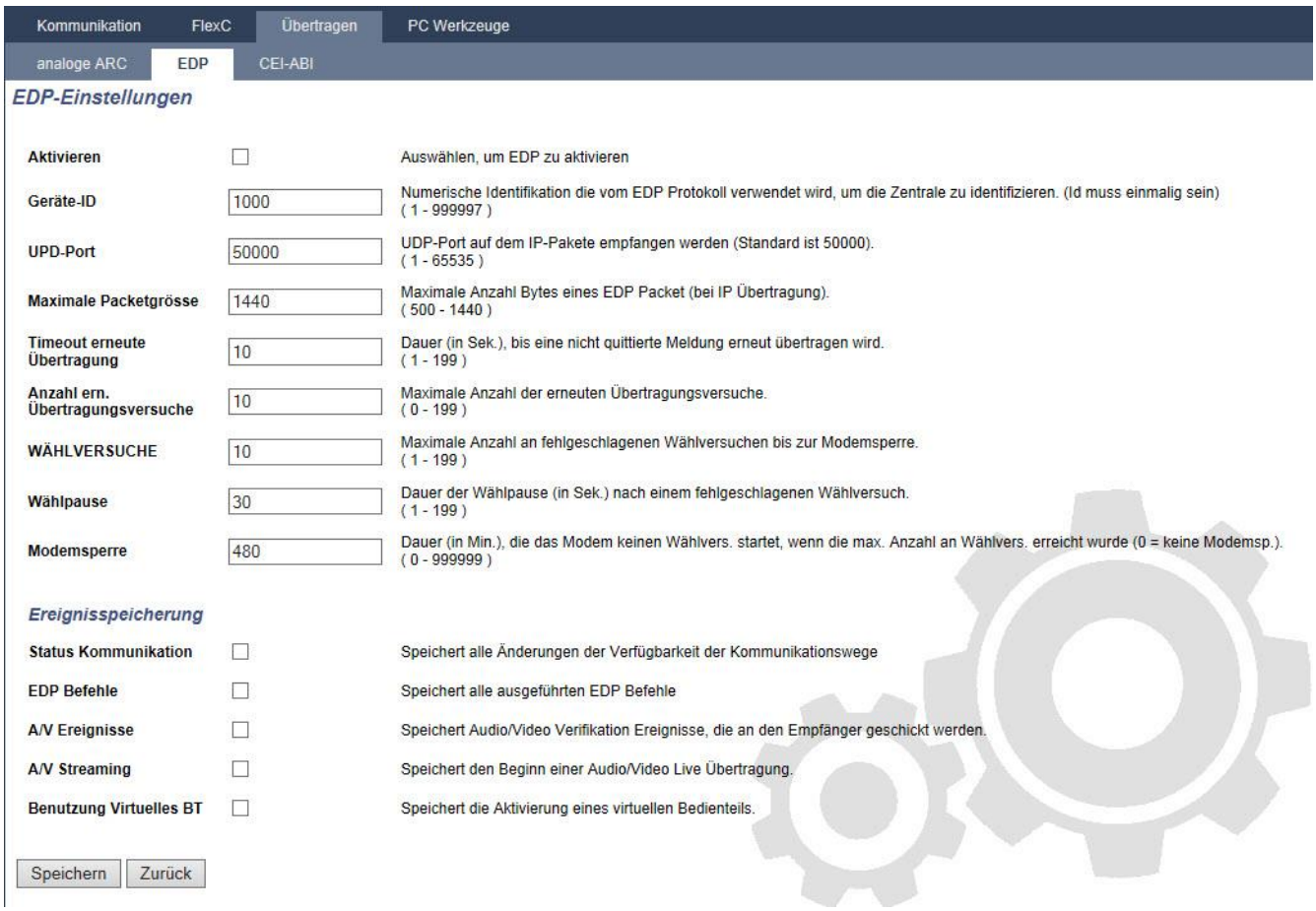
Aktivieren Sie ein beliebiges der folgenden Kontrollkästchen, wenn eine Datenübertragung an einen EDP-Empfänger initiiert werden soll, um ihm ein bestimmtes Ereignis zu melden.

Alarm	„Alarm“ ist aktiviert.
Rückstellung Alarm	Die Systemalarme werden quittiert.
Bestätigte 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.
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.

17.10.3.2.4 EDP-Einstellungen bearbeiten

1. Wählen Sie **Kommunikation > Übertragen > EDP > Einstellungen**.
   ⇨ Daraufhin erscheint das folgende Fenster.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.



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.

17.10.4 PC Werkzeuge

17.10.4.1 SPC Pro / SPC Safe

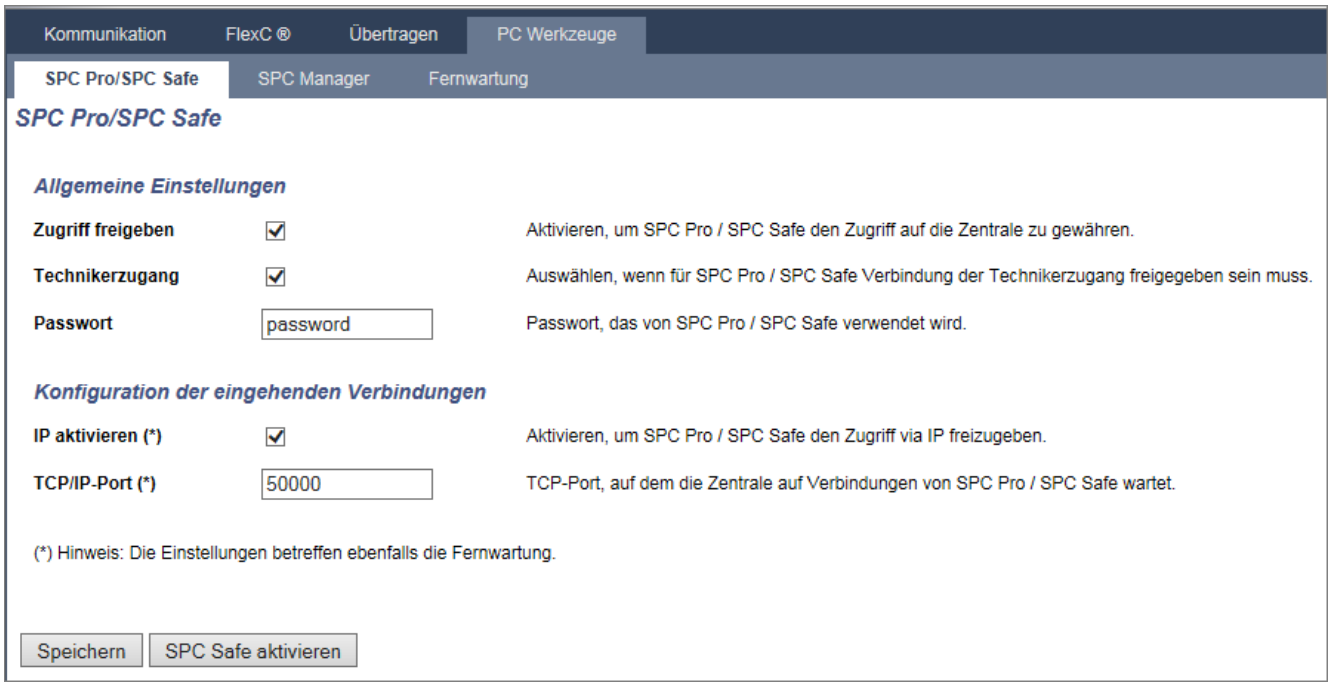
1. Wählen Sie **Kommunikation > PC Werkzeuge > SPC Pro/SPC Safe**.
2. Konfigurieren Sie die Felder wie in der unten stehenden Tabelle beschrieben.

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.



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).

17.10.4.2 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:

1. Wählen Sie **Kommunikation > PC Werkzeuge > SPC Manager**.

2. Wählen Sie aus der Dropdown-Liste den Modus für den globalen Benutzer von SPC Manager aus.
3. Klicken Sie auf **Speichern**.
   ⇨ Dieser Modus kann nicht gespeichert werden, wenn zwischen der lokal vorhandenen Benutzer-PIN und einer anderen Benutzer-PIN auf dem globalen System ein Konflikt besteht. Der Fehler ‚Ungültige PIN' wird angezeigt.
4. Klicken Sie neben der zu löschenden PIN auf die entsprechende Schaltfläche, und speichern Sie den Modus, oder ändern Sie die PIN in eine zufällig generierte neue PIN, und speichern Sie anschließend den neuen Modus.

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

17.10.4.3 "Fernwartung"

Weitere Informationen finden Sie im Konfigurationshandbuch für die Fernwartung.

17.10.4.3.1 Fernwartungsbericht

Ein Fernwartungsbericht kann direkt von SPC Pro in der Zentrale abgerufen werden.

▷ SPC Pro muss mit der Zentrale verbunden und online sein.

▷ Die Option **Fernwartung** muss aktiviert sein.

1. Klicken Sie auf das Menü **Erweitert**.
2. Wählen Sie die Menüoption **Get Service Report from Panel** (Dienstbericht von Zentrale abrufen).

Weitere Informationen zur Fernwartung finden Sie im SPC-Fernwartungshandbuch.

17.11 Dateioperationen

Vorgänge an Dateien und Konfigurationen der Zentrale durchführen:

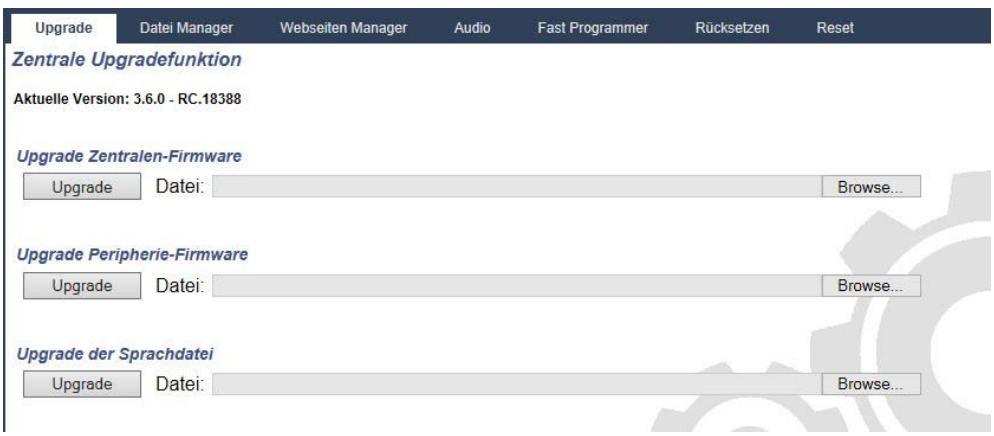
- Wählen Sie **Datei**.
  ⇨ Folgende Registerkarten werden angezeigt:

Upgrade	Optionen zum Aktualisieren des Controllers, der Peripherie-Firmware und der Sprachen der Zentrale. Siehe Datei-Upgrade-Operationen [→ 329].
Datei Manager	Optionen zur Verwaltung der Systemkonfigurationsdatei und zum Up- und Download von Benutzerdaten von und zur Zentrale. Siehe Datei Manager-Operationen [→ 335].
Audio	Laden Sie eine Audiodatei auf SPC hoch. Die Datei muss im SPC Pro Audio Manager erstellt werden. Klicken Sie auf **Durchsuchen** und anschließend auf **Hochladen**, um die Audiodatei zu SPC hinzuzufügen. Klicken Sie nach dem Hochladen auf die Schaltfläche **Test**, um die Audiodatei zu prüfen.
Fast Programmer	Dateioperationen mit dem Fast Programmer Siehe Verwenden des Fast Programmer [→ 336].
Default (Standard)	Setzt das SPC-System auf die Werkseinstellungen zurück. **HINWEIS! Beim Zurücksetzen auf Werkseinstellungen von der Webseite aus, wird die IP-Adresse beibehalten, um die Verbindung zur Webschnittstelle zu ermöglichen.**
Reset (Zurücksetzen)	Startet die Zentrale neu.
Richtlinientext	Auf dieser Registerkarte wird die Konfiguration für Ihre SPC-Produkteinstellungen basierend auf der Auswahl für **Region**, **Sicherheitsgrad** und **Type** zusammengefasst.

17.11.1 Datei-Upgrade-Operationen

Upgrade der Firmware und der Sprachen des Systems durchführen:

- Wählen Sie **Datei > Upgrade**.
  ⇨ Die folgende Seite wird angezeigt:



Siehe auch

- Optionen [→ 239]
- Verwenden des Fast Programmer [→ 336]

17.11.1.1 Upgrade der Firmware

	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 [→ 239].

Die Firmware für SPC ist in zwei separaten Dateien enthalten:

- Zentralen-Firmware-Datei
  Enthält ausschließlich die Firmware für die Controller-CPUs. Die Datei besitzt die Dateierweiterung *.fw.
- Peripherie-Firmware-Datei
  Enthält die Firmware für die X-BUS-Knoten sowie für die PSTN- und GSM-Modems. Die Datei besitzt die Dateierweiterung *.pfw.

Das Upgrade der beiden Dateien erfolgt separat.

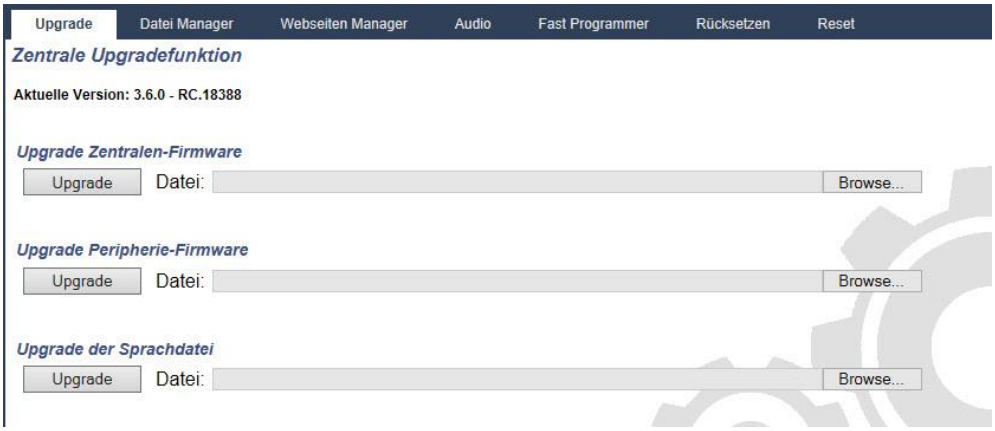
	HINWEIS
	Vor dem Upgrade sämtlicher Peripherie-Firmware wird ein Upgrade der Controller-Firmware empfohlen.

Hinweis: Firmware kann auch über das Bedienteil, SPC Pro und den Fast Programmer aktualisiert werden.

Zentralen-Firmware

Upgrade der Controller-Firmware durchführen:

1. Wählen Sie auf der Seite **Datei** die Option **Zentrale „Upgrade"-Funktion**.
   ⇨ Die folgende Seite wird angezeigt:



2. Wählen Sie die Firmware-Datei, für die ein Upgrade durchgeführt werden soll. Klicken Sie dazu neben der entsprechenden Option auf **Browse**

(Durchsuchen), wählen Sie die Firmware-Datei aus, und klicken Sie anschließend auf die entsprechende Schaltfläche **Upgrade**.

⇨ Ein Bestätigungsfenster wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Bestätigen**, um das Upgrade auf die neue Version der Controller-Firmware zu bestätigen.

⇨ Nachdem das Upgrade der Controller-Firmware abgeschlossen wurde, zeigt das System die Meldung an, dass das System zurückgesetzt wird. Sie müssen sich erneut im System anmelden, um fortzufahren.

⚠ WARNUNG

Wenn Sie die Controller-Firmware downgraden (d. h. eine ältere Version der Firmware installieren), behält das System standardmäßig alle aktuellen Konfigurationseinstellungen bei. Außerdem muss bei einem Downgrade der Firmware unbedingt auch ein Downgrade der Firmware auf den zugehörigen Peripheriegeräten durchgeführt werden, sonst können Meldergruppen als getrennt/ausgeschaltet, offen oder geschlossen angezeigt werden.

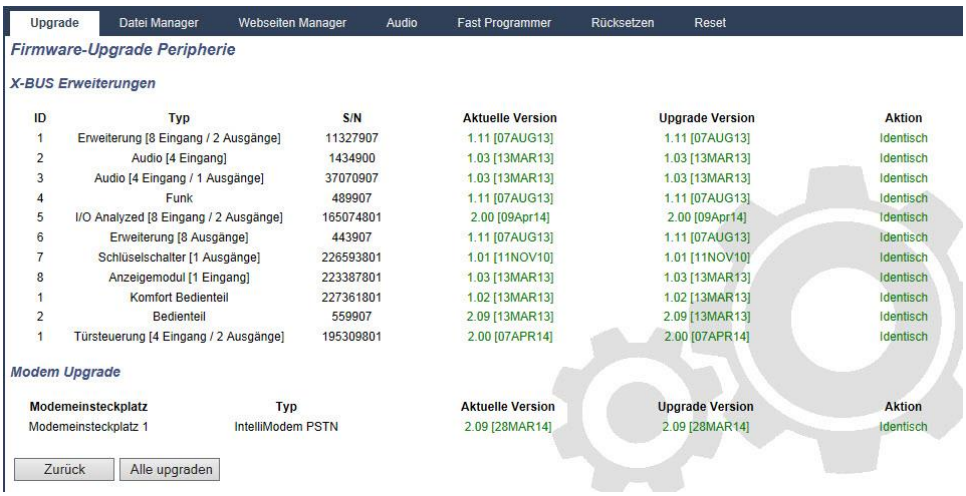
⚠ WARNUNG

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 [→ 199]). Prüfen Sie nach dem Firmware-Upgrade sämtliche Benutzerkonfigurationseinstellungen.
- Die Standard-Techniker-ID wird von 513 in 9999 geändert.

Upgrade Peripherie-Firmware

Das Upgrade der Peripherie-Firmware erfolgt nach demselben Verfahren wie das Upgrade der Controller-Firmware.

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:



- Klicken Sie neben den Peripheriegeräten, die ein Upgrade erfordern, auf die Schaltfläche **Upgrade**, oder klicken Sie auf **Alle upgraden**, um ein Upgrade für alle Peripheriegeräte durchzuführen.

⇨ Falls die Firmware für ein Peripheriegerät in der .pfw-Datei älter ist als die auf dem Gerät vorhandene Firmware, wird die Schaltfläche **Downgrade** angezeigt.

Währen des Upgrades überprüft das Bedienteil, ob die in der Peripheriegeräte-Datei enthaltene Firmware die jeweiligen Hardware-Versionen der installierten Peripheriegeräte unterstützt und lässt kein Update für Geräte zu, die nicht unterstützt werden.

Falls die .pfw-Dateiversion von der Controller-Version abweicht, wird eine Warnmeldung angezeigt.

Falls die Hauptversionsnummer der für ein Gerät verfügbaren Firmware von der Hauptversionsnummer der vorhandenen Firmware eines Geräts abweicht, wird ebenfalls eine Warnmeldung angezeigt.

Das Upgrade der Peripheriegeräte-Firmware kann auch über SPC Pro oder den Fast Programmer [→ 336] erfolgen.

Upgrade der Firmware des SPCP355 Smart-Netzteils

Für ein ordnungsgemäßes Upgrade des SPCP355 Smart-Netzteils müssen Sie Folgendes beachten:

Die Firmware des SPCP355 Smart-Netzteils kann nur über den Browser aktualisiert werden. Ein Upgrade mit SPC Pro ist nicht möglich.

- Die Netzstromversorgung muss eingeschaltet sein.

Der Upgrade-Vorgang kann bis zu 2 Minuten dauern. Führen Sie währenddessen keine Aktionen mit dem Browser aus. Das System darf erst dann ausgeschaltet oder neu gestartet werden, wenn der Vorgang abgeschlossen ist. Nach Abschluss des Vorgangs wird eine Meldung angezeigt.

Siehe auch

Hinzufügen/Bearbeiten von Profilen [→ 199]

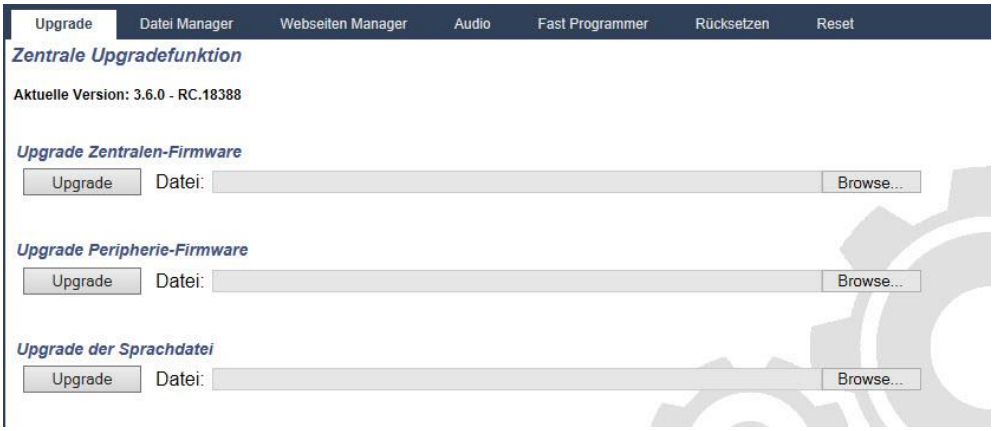
17.11.1.2 Upgrade von Sprachen

Eine individuelle Sprachendatei (*.clng) kann in die Zentrale hochgeladen werden. Diese Datei bezieht sich ausschließlich auf die Bedienteil-Firmware und steht nicht für SPC Pro oder SPC Safe zur Verfügung.

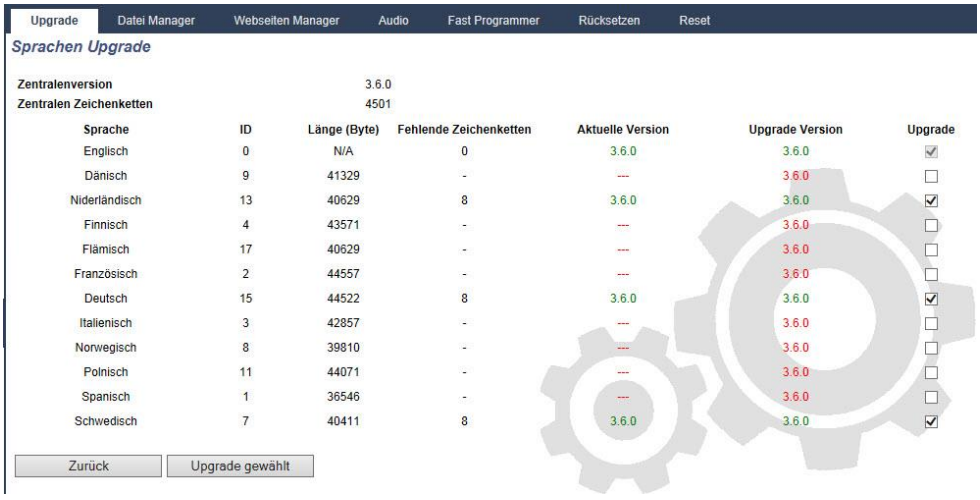
!	*HINWEIS*
	Das Bedienteil muss für die Verwendung kundenspezifischer und weiterer Sprachen lizenziert sein.

Upgrade der Sprachen des Systems durchführen:

1. Wählen Sie **Datei >Upgrade**.
   ⇨ Die Seite **Zentrale Upgradefunktion** wird angezeigt:



2. Wählen Sie die Sprachdatei, für die ein Upgrade durchgeführt werden soll. Klicken Sie dazu neben der Option **Upgrade der Sprachdatei** auf **Durchsuchen**, wählen Sie die erforderliche Sprachdatei, und klicken Sie anschließend auf die entsprechende Schaltfläche **Upgrade**.
   ⇨ Es wird eine Liste der Sprachen angezeigt, die in dieser Datei verfügbar sind.



3. Aktivieren Sie das Kontrollkästchen neben der zu installierenden Sprache.

Es können maximal 4 Sprachen installiert werden.

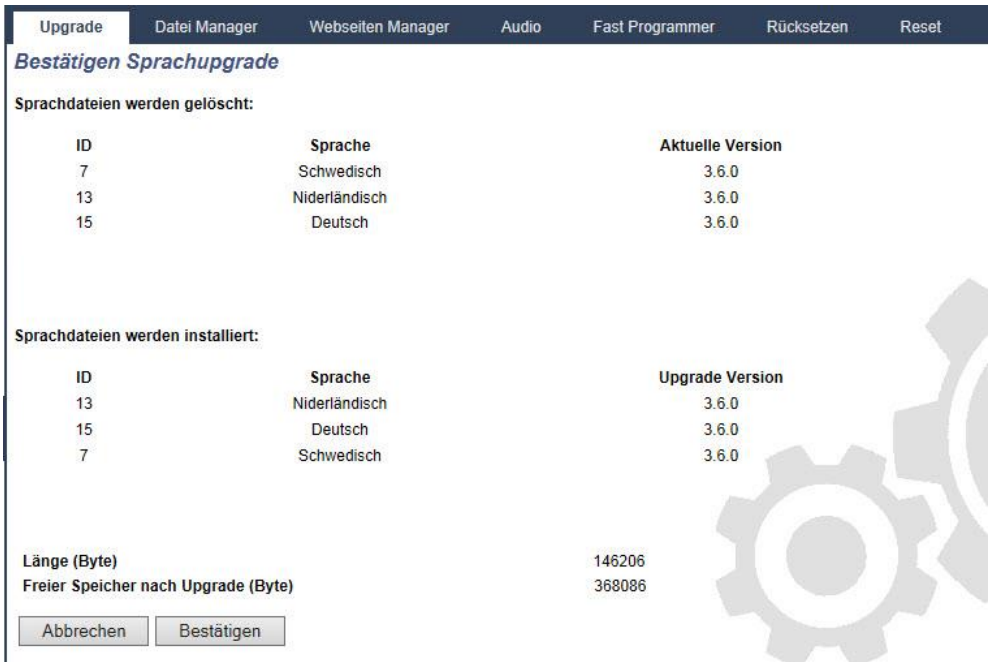
4. Klicken Sie auf **Upgrade gewählt**.
   ⇨ Das Fenster **Bestätigen Sprachupgrade** wird angezeigt und enthält alle Sprachen, die installiert werden.
5. Klicken Sie auf **Bestätigen**.

Es wird eine Meldung angezeigt, ob die Aktualisierung der Sprache erfolgreich war oder fehlgeschlagen ist.

Sprachen löschen

Löschen der Sprachen aus der Sprachdatei:

1. Wählen Sie die Sprachdatei, für die ein Upgrade durchgeführt werden soll. Klicken Sie dazu neben der Option **Upgrade der Sprachdatei** auf **Browse** (Durchsuchen), wählen Sie die erforderliche Sprachdatei, und klicken Sie anschließend auf die entsprechende Schaltfläche **Upgrade**.
   ⇨ Es wird eine Liste der Sprachen angezeigt, die in dieser Datei verfügbar sind.
2. Deaktivieren Sie die Kontrollkästchen neben den Sprachen, die gelöscht werden sollen.
3. Klicken Sie auf **Upgrade gewählt**.
   ⇨ Das Fenster **Bestätigen Sprachupgrade** wird angezeigt. Beim Löschen einer Sprache werden von der Zentrale zunächst alle Sprachen gelöscht und anschließend die erforderlichen Sprachen erneut installiert. Im folgenden Beispiel wird Flämisch gelöscht.



4. Klicken Sie auf **Bestätigen**, um die zu löschenden Sprachen zu bestätigen.

Sprachdateien können auch über den Fast Programmer [→ 336] importiert werden.

Weitere Informationen zur Auswahl von „System“- und „Ruhezustand“-Sprachen für die Zentrale im Browser finden Sie unter Sprache [→ 255].

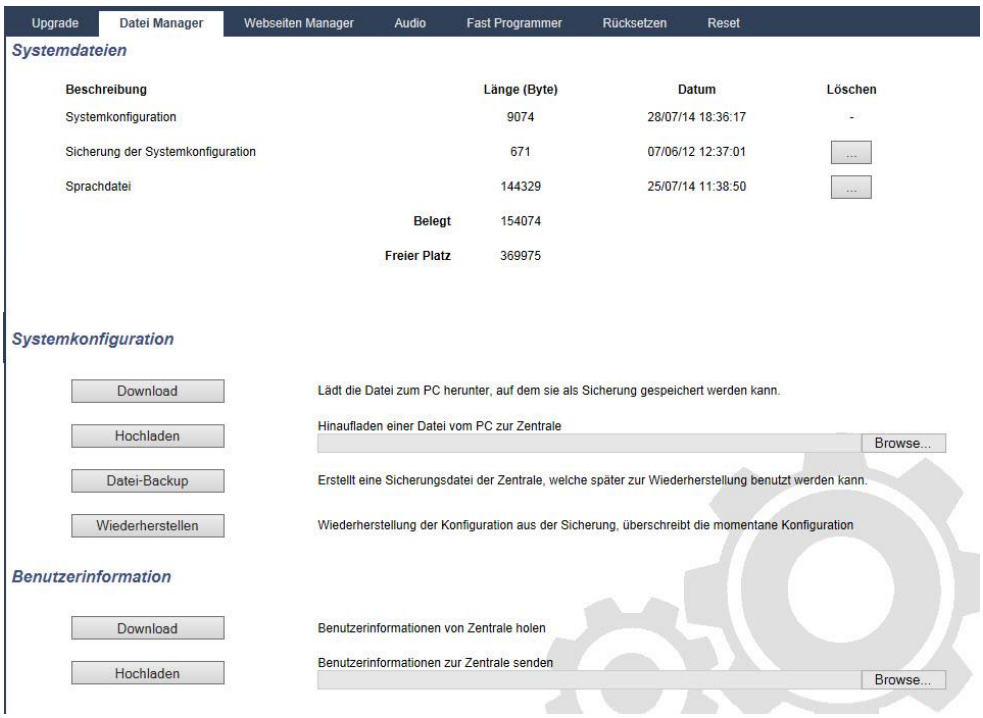
Weitere Informationen zur Auswahl von „System“- und „Ruhezustand“-Sprachen für die Zentrale auf dem Bedienteil finden Sie unter OPTIONEN [➙ 116].

Siehe auch

Sprache [➙ 255]

17.11.2 Datei Manager-Operationen

- Wählen Sie **Datei > Datei Manager**.
  - ⇨ Ein Bildschirm zeigt die Details der Systemkonfiguration, Sprache und Ablaufverfolgungsdateien an.



Systemkonfiguration

Zur Verwaltung der Systemkonfigurationsdatei stehen folgende Optionen zur Verfügung:

Download	Herunterladen einer Konfigurationsdatei vom Controller **Hinweis**: Falls nach dem Anklicken der Download-Schaltfläche eine Fehlermeldung erscheint, wie folgt vorgehen: 1. Wähle Sie im Menü „Tools“ (Werkzeuge) die Option **Internetoptionen**. 2. Wählen Sie die Registerkarte **Erweitert**. 3. Aktivieren Sie das Kontrollkästchen **Keine verschlüsselten Seiten auf Laufwerk speichern**. 4. Klicken Sie auf **Übernehmen**. 5. Klicken Sie auf **OK**. 6. Klicken Sie nochmals auf **Download**. Beim Herunterladen von Konfigurationsdateien, werden die Konfigurationseinstellungen in einer **.cfg**-Datei gespeichert. Diese Datei kann dann auf andere Controller hochgeladen werden, um zeitraubende Programmierprozesse zu vermeiden.
Upload	Hochladen einer Konfigurationsdatei auf den Controller
Datei-Backup	Sicherung der aktuellen Konfiguration auf den Flash-Speicher
Quittieren	Wiederherstellung einer Sicherungskopie der aktuellen Konfiguration aus dem Flash-Speicher

Benutzerinformation

Zur Verwaltung der Benutzerinformationen stehen folgende Optionen zur Verfügung:

Download	Klicken Sie auf die Schaltfläche, um die Benutzerinformationen von der Zentrale **herunterzuladen**. In einem Dialogfeld werden Sie nach dem Speicherort für die Datei **users.csv** gefragt.
Upload	Klicken Sie auf die Schaltfläche **Durchsuchen**, um die Benutzerinformationen auf die Zentrale **hochzuladen**. Dabei muss es sich um eine CSV-Datei handeln.

17.12 Verwenden des Fast Programmer

Beim SPC Fast Programmer handelt es sich um einen externen Speicherstick, mit dem der Techniker Konfigurationsdateien schnell und bequem hoch- und herunterladen kann. Der Fast Programmer hat zwei sich gegenüberliegende Stecker:

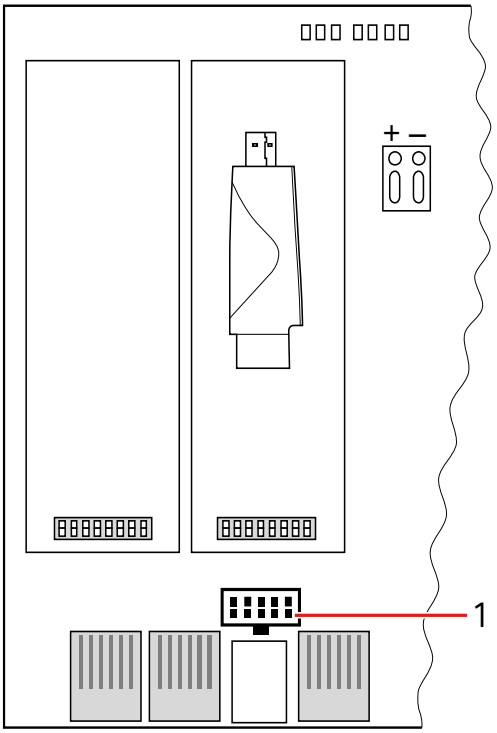
SPC-Controller-Schnittstelle

Dieser 10-polige serielle Stecker befindet sich oben am Fast Programmer und kann direkt in die Fast Programmer-Buchse auf der Controller-Platine eingesteckt werden. Wenn er angeschlossen ist, kann der Techniker über den Browser und über Programmiertools des Bedienteils direkt Dateien vom Fast Programmer hoch- oder herunterladen.

PC USB-Stecker

Dieser USB-Stecker befindet sich an der unteren Seite des Fast Programmer und kann direkt in eine USB-Buchse am PC eingesteckt werden. Konfigurationsdateien und andere Dateien können nur über das SPC Pro-Programmiertool zwischen dem Computer und dem Fast Programmer kopiert werden.

17.12.1 Anschließen des Fast Programmer an den Controller



Fast Programmer-Buchse

1	Fast Programmer-Buchse

So schließen Sie den SPC Fast Programmer an den Controller an:

1. Öffnen Sie das SPC-Controller-Gehäuse und stellen Sie fest, wo sich die Fast Programmer-Buchse befindet.
   HINWEIS! Schalten Sie die Stromversorgung des Controllers nicht ab..
2. Richten Sie den Fast Programmer mit dem 10-poligen seriellen Stecker nach unten über der Fast Programmer-Buchse auf der SPC-Controller-Platine aus.
3. Achten sie darauf, dass die Stifte des Steckers korrekt über den Löchern der Buchse ausgerichtet sind, und drücken sie den Stecker vorsichtig bis zum Anschlag in die Buchse.

⇨ Die LED am Fast Programmer beginnt sofort zu blinken, wenn auf die darin enthaltenen Daten zugegriffen wird.
VORSICHT! Entfernen Sie den Fast Programmer nicht, solange die LED blinkt..

⇨ Der Fast Programmer ist nun an den Controller angeschlossen.

Zum Entfernen des Fast Programmers das Gerät vorsichtig aus der Fast Programmer-Buchse ziehen.

17.12.2 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 > Gerätemanager**.

⇨ Der Treiber für den Fast Programmer ist im Ports (COM & LPT)-Verzeichnis als SPC **USB Fast Programmer (COM X)** (X = COM-Port-Nummer) aufgeführt.

17.12.3 Dateioperationen mit dem Fast Programmer

Controller- und Peripherie-Firmware-Upgrades und der Import kundenspezifischer Sprachen können über den Fast Programmer und SPC Pro erfolgen.

17.12.3.1 Zugreifen auf den Fast Programmer über das Bedienteil

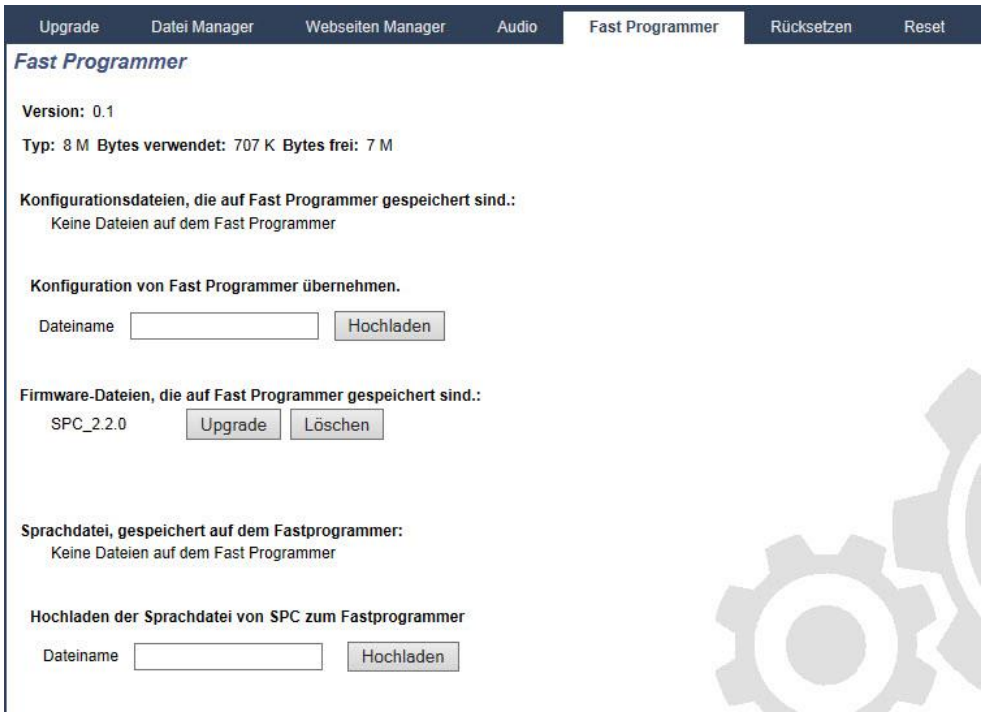
1. Rufen Sie den Konfigurationsmodus auf, und blättern Sie zu KONFIG OPTIONEN > FAST PROGRAMMER.
2. Drücken Sie auf AUSWAHL.
3. Blättern Sie zur gewünschten Option und wählen Sie diese aus:

DATEN VON SPC	Die gewünschte Datei aus der Liste wählen.
DATEN ZU SPC	Die gewünschte Datei aus der Liste wählen.
DATEIEN LÖSCHEN	Die gewünschte Datei aus der Liste wählen.
FIRMWARE UPGRADE	Die Zentrale sucht nach einer gültigen Controller-Firmware. Sobald sie die Firmware-Datei gefunden hat, kann der Benutzer diese auswählen und die Zentrale aktualisieren.
UPGRADE PERIPHERIE-FIRMWARE	Die Zentrale sucht nach einer gültigen Peripherie-Firmware. Sobald sie die Firmware-Datei gefunden hat, kann der Benutzer diese auswählen und die Zentrale aktualisieren.
SPRACHUPGRADE	Eine Liste der auf dem Fast Programmer verfügbaren Sprachdateien wird angezeigt. Wählen Sie die gewünschte Sprache aus und drücken Sie auf AUSWAHL, um die Datei zu importieren.

17.12.3.2 Zugreifen auf den Fast Programmer über den Browser

1. Wechseln Sie in der Browser-Programmierung in den Konfigurationsmodus, und wählen Sie die Programmierseite **Datei**.
2. Klicken Sie auf **Fast Programmer**.

⇨ Die Optionen für das Hochladen und Herunterladen von Dateien werden angezeigt.



Herunterladen von Konfigurationsdateien auf die Zentrale

Eine Liste der auf dem Fast Programmer gespeicherten Konfigurationsdateien und die Optionen zum Herunterladen oder Löschen der Dateien werden angezeigt.

Hochladen von Konfigurationsdateien auf den Fast Programmer

Beim Hochladen von Dateien vom SPC auf den Fast Programmer werden Sie aufgefordert, die bestehende Datei auf dem Programmer zu löschen, bevor die neue Datei gespeichert werden kann.

Geben Sie zum Hochladen einer Konfigurationsdatei vom Fast Programmer auf die SPC den Dateinamen in das Feld „Dateiname“ ein und klicken Sie auf **Upload**.

Vollständige Informationen zur Verwendung des Fast Programmer mit SPC Pro finden Sie im *SPC Pro-Konfigurationshandbuch*.

Upgrade der Firmware

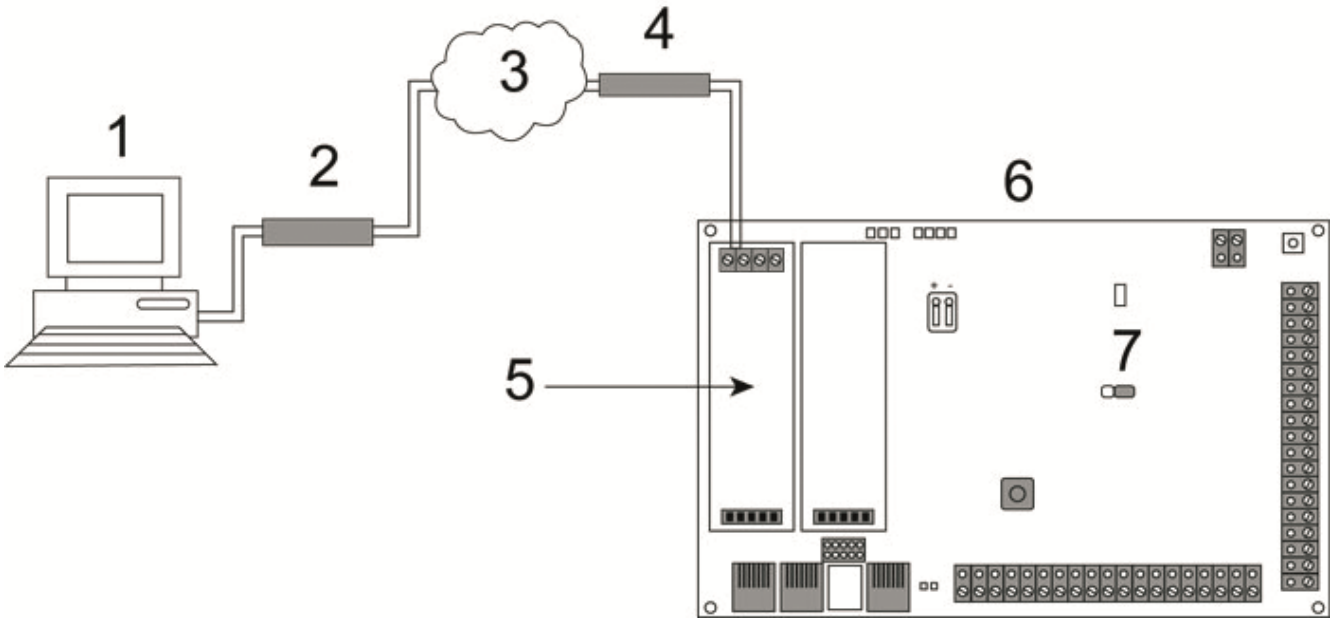
!	*HINWEIS*
	Für Firmware-Operationen ist Herstellerzugang erforderlich.

Eine Liste der auf dem Fast Programmer gespeicherten Firmware-Dateien wird angezeigt.

Klicken Sie für ein Firmware-Upgrade auf die Schaltfläche **Upgrade** neben der betreffenden Firmware-Datei.

18 Fernzugriff auf den Webserver

18.1 PSTN-Verbindung



PSTN-Verbindung

1	Remote-PC mit Browser
2	PSTN-Modem
3	PSTN-Netz
4	Telefonleitung
5	PSTN-Modem
6	SPC-Controller
7	JP9 ~~SPC4xxx~~

Auf den Webserver auf dem Controller kann per Fernzugriff über eine PSTN-Telefonverbindung zugegriffen werden. Für den Fernzugriff auf den Controller müssen ein PSTN-Modul und eine PSTN-Leitung wie oben dargestellt an den Controller angeschlossen sein.

Auf der entfernten Seite der Verbindung benötigt der Benutzer ein PSTN-Modem auf einem PC mit Zugang zu einer PSTN-Leitung.

Herstellen der Fernzugriffsverbindung zur Zentrale:

1. Installieren Sie ein PSTN-Modem auf dem Controller (siehe die entsprechende Installationsanleitung).
2. Schließen Sie die Telefonleitung an die Schraubklemmen A und B am Anschluss auf der Oberseite des Modems an.
3. Rufen Sie die Techniker-Programmierung am Bedienteil auf und konfigurieren Sie das Modem (primär oder Backup) so, dass es eingehende Anrufe annimmt.
4. Blättern Sie am Bedienteil zu **Konfigurationsmodus > Komm. > Modems**
5. Wählen Sie die folgenden Einstellungen:
   - **Modem aktiv:** Auf aktiv setzen.

- **Typ:** Zeigt den Modemtyp an (PSTN)
- **Ländercode:** Wählen Sie die betreffende Ländervorwahl aus (Irland, UK, Europa).
- **Anrufannahme:** Wählen Sie die Option „Klingelanzahl“; hier wird dem Modem die Zahl der Ruftöne vorgegeben, die es abwartet, bis es einen eingehenden Anruf annimmt.
- **Modem Rings:** Wählen Sie die Anzahl der Ruftöne, nach welcher das Modem eingehende Anrufe annimmt (max. 8).

6. Richten Sie eine Wählverbindung auf dem Remote-PC ein; verwenden Sie hierbei die Telefonnummer des Anschlusses, mit dem das PSTN-Modul am Controller verbunden ist. Im Folgenden finden Sie eine Anleitung zum Einrichten einer Wählverbindung unter Windows XP:

Unter Windows XP:

1. Rufen Sie den Assistenten zum Einrichten einer neuen Verbindung auf; wählen Sie hierzu den Pfad **Systemsteuerung > Netzwerkverbindungen > Neue Verbindung erstellen** (im Fenster "Netzwerkaufgaben").
2. Wählen Sie im Fenster **Netzwerkverbindungstyp** die Option **Mit dem Internet verbinden**.
3. Wählen Sie im Fenster **Vorbereitung** die Option **Verbindung manuell einrichten**.
4. Wählen Sie im Fenster **Internetverbindung** die Option **Über Wählmodem verbinden**.
5. Geben Sie im Fenster **Verbindungsname** einen Namen für die Verbindung ein, z.B. „SPC-Fernverbindung“.
6. Geben Sie im Fenster **Zu wählende Rufnummer** die Rufnummer des Anschlusses an, der mit dem Modem verbunden ist.
7. Legen Sie im Fenster **Verfügbarkeit der Verbindung** fest, ob die eingerichtete Verbindung allen Benutzer zur Verfügung stehen soll.
8. Geben Sie im Fenster **Internetkontoinformationen** die folgenden Angaben ein:
   - Benutzername: SPC
   - Passwort: passwrod (Standard)
   - Passwort bestätigen: password

   ⇨ Das Fenster **Fertigstellen des Assistenten** wird angezeigt.
9. Klicken Sie auf **Fertig stellen**, um die Wählverbindung auf dem PC zu speichern.

Das werkseitig eingestellte Standardpasswort sollte geändert und notiert werden, da Vanderbilt

das neue Password nicht abrufen kann. Bei Verlust des Passworts, muss das System auf Werkseinstellungen zurückgesetzt werden, wobei alle Konfigurationsparameter und Einstellungen verloren gehen. Die Konfigurationen und Einstellungen können jedoch über eine Sicherungskopie (Backup) wiederhergestellt werden.

So aktivieren Sie diese Wählverbindung:

- Klicken Sie auf das Verbindungssymbol im Fenster **Systemsteuerung > Netzwerkverbindungen**.

- ⇨ Der PC führt dann einen Datenanruf an diePSTN -Leitung durch, die an das SPC PSTN-Modul angeschlossen ist.
- ⇨ Das SPC PSTN-Modul nimmt den eingehenden Datenanruf nach der eingestellten Anzahl von Ruftönen an und stellt eine IP-Verbindung zum Remote Computer her.
- ⇨ Das SPC-System weist dem Remote Computer automatisch eine IP-Adresse zu.

Bei einigen Windows-Betriebssystemen wird ein Dialogfeld mit Hinweisen zur Windows-Zertifizierung angezeigt. Vanderbilt

hält es jetzt für zulässig, mit dem Installationsprozess fortzufahren. Sollten weitere Abfragen erscheinen, setzen Sie sich bitte mit Ihrem Netzwerkadministrator oder einem Vanderbilt

-Techniker in Verbindung.

Diese IP-Adresse aufrufen:

1. Klicken Sie mit der rechten Maustaste auf das Verbindungssymbol.
2. Klicken Sie auf die Registerkarte **Details**.

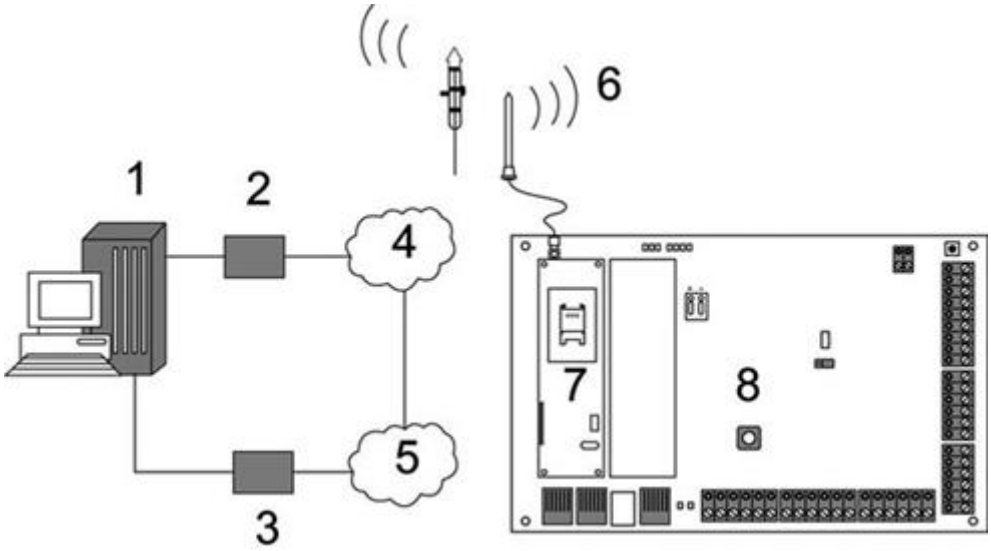
⇨ Die IP-Adresse wird als Server-IP-Adresse angezeigt.

1. Geben Sie diese IP-Adresse in die Adressleiste des Browsers ein und drücken Sie die Eingabetaste.
2. Wenn das Verbindungssymbol in der Taskleiste des PC-Bildschirms angezeigt wird, rufen Sie den Browser auf und geben Sie die IP-Adresse der SPC ein.

⇨ Im Browser wird die Anmeldeseite angezeigt.

Zum Einrichten einer Wählverbindung auf einem anderen Betriebssystem finden Sie die entsprechenden Anleitungen in der Hilfe des jeweiligen Betriebssystems.

18.2 GSM-Verbindung



GSM-Verbindung

1	Remote-PC mit Browser

2	GSM-Modem
3	PSTN-Modem
4	GSM-Netz
5	PSTN-Netz
6	Externe Antenne
7	GSM-Modem
8	SPC-Controller

Auf den Webserver auf dem Controller kann per Fernzugriff über ein 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. Die Datenoption der SIM-Karte muss aktiviert sein, und die Datennummer muss verwendet werden.

Auf der entfernten Seite der Verbindung benötigt der Benutzer ein PSTN- oder GSM-Modem auf einem PC mit Browser. Falls ein PSTN-Modem installiert ist, muss es mit einem aktiven PSTN-Anschluss verbunden sein.

Herstellen der Fernzugriffsverbindung zur Zentrale:

1. Installieren Sie ein GSM-Modem auf dem Controller (siehe die entsprechende Installationsanleitung).
2. Rufen Sie die Techniker-Programmierung (Konfigurationsmodus) am Bedienteil auf und konfigurieren Sie das Modem (primär oder Backup) so, dass es eingehende Anrufe annimmt.
3. Blättern Sie am Bedienteil zum folgenden Menü: KONFIG MODUS > KOMMUNIKATION > MODEMS und nehmen Sie die folgenden Einstellungen vor:

Modem aktiv	Auf „Modem aktiviert“ setzen.
Typ	Zeigt den Modemtyp an (GSM)
Ländercode	Wählen Sie den zutreffenden Ländercode.
Anrufannahme	Wählen Sie die Option „Klingelanzahl; hier wird dem Modem die Zahl der Rufzeichen vorgegeben, die es abwartet, bis es einen eingehenden Anruf annimmt.
Modem Rings	Wählen Sie die Anzahl der Rufzeichen, nach welcher das Modem eingehende Anrufe annimmt (max. 8).

Unter Windows XP:

1. Rufen Sie den Assistenten zum Einrichten einer neuen Verbindung auf; wählen Sie hierzu den Pfad **Systemsteuerung > Netzwerkverbindungen > Neue Verbindung erstellen** (im Fenster "Netzwerkaufgaben").
2. Wählen Sie im Fenster **Netzwerkverbindungstyp** die Option **Mit dem Internet verbinden**.
3. Wählen Sie im Fenster **Vorbereitung** die Option **Verbindung manuell einrichten**.
4. Wählen Sie im Fenster **Internetverbindung** die Option **Über Wählmodem verbinden**.
5. Geben Sie im Fenster **Verbindungsname** einen Namen für die Verbindung ein, z.B. „SPC-Fernverbindung“.
6. Geben Sie im Fenster **Zu wählende Rufnummer** die Rufnummer des Anschlusses an, der mit dem Modem verbunden ist.

7. Legen Sie im Fenster **Verfügbarkeit der Verbindung** fest, ob die eingerichtete Verbindung allen Benutzer zur Verfügung stehen soll.
8. Geben Sie im Fenster **Internetkontoinformationen** die folgenden Angaben ein:
   - Benutzername: SPC
   - Passwort: password (Standard)
   - Passwort bestätigen: password

   ⇨ Das Fenster **Fertigstellen des Assistenten** wird angezeigt.
9. Klicken Sie auf **Fertig stellen**, um die Wählverbindung auf dem PC zu speichern.

Das werkseitig eingestellte Standardpasswort sollte geändert und notiert werden, da Vanderbilt

das neue Password nicht abrufen kann. Bei Verlust des Passworts, muss das System auf Werkseinstellungen zurückgesetzt werden, wobei alle Konfigurationsparameter und Einstellungen verloren gehen. Die Konfigurationen und Einstellungen können jedoch über eine Sicherungskopie (Backup) wiederhergestellt werden.

So aktivieren Sie diese Wählverbindung:

- Klicken Sie auf das Verbindungssymbol im Fenster **Systemsteuerung > Netzwerkverbindungen**.

  ⇨ Der PC führt dann einen Datenanruf an diePSTN -Leitung durch, die an das SPC PSTN-Modul angeschlossen ist.
  ⇨ Das SPC PSTN-Modul nimmt den eingehenden Datenanruf nach der eingestellten Anzahl von Ruftönen an und stellt eine IP-Verbindung zum Remote Computer her.
  ⇨ Das SPC-System weist dem Remote Computer automatisch eine IP-Adresse zu.

Bei einigen Windows-Betriebssystemen wird ein Dialogfeld mit Hinweisen zur Windows-Zertifizierung angezeigt. Vanderbilt

hält es jetzt für zulässig, mit dem Installationsprozess fortzufahren. Sollten weitere Abfragen erscheinen, setzen Sie sich bitte mit Ihrem Netzwerkadministrator oder einem Vanderbilt

-Techniker in Verbindung.

Diese IP-Adresse aufrufen:

1. Klicken Sie mit der rechten Maustaste auf das Verbindungssymbol.
2. Klicken Sie auf die Registerkarte **Details**.

⇨ Die IP-Adresse wird als Server-IP-Adresse angezeigt.

1. Geben Sie diese IP-Adresse in die Adressleiste des Browsers ein und drücken Sie die Eingabetaste.
2. Wenn das Verbindungssymbol in der Taskleiste des PC-Bildschirms angezeigt wird, rufen Sie den Browser auf und geben Sie die IP-Adresse der SPC ein.

⇨ Im Browser wird die Anmeldeseite angezeigt.

Zum Einrichten einer Wählverbindung auf einem anderen Betriebssystem finden Sie die entsprechenden Anleitungen in der Hilfe des jeweiligen Betriebssystems.

19 Einbruchalarm-Funktion

Das SPC-System kann in drei unterschiedlichen Einbruchalarm-Modi betrieben werden, im Modus **Finanziell**, im Modus **Kommerziell** oder im Modus **Privat**, wobei alle Modi mehrere Bereiche unterstützen.

Jeder Bereich kann wiederum vier unterschiedliche Alarmmodi unterstützen. Die Modi „Kommerziell“ und „Finanziell“ umfassen mehr programmierbare Alarmtypen als der Modus „Privat“. Die Standardeinstellungen für Meldergruppennamen und -typen für jeden Modus finden Sie auf Seite [→ 363].

19.1 Finanzieller Modus

Der Modus „Finanziell“ ist für Banken und Finanzdienstleister geeignet, die über bestimmte gesicherte Bereiche wie Tresore und Geldautomaten verfügen.

Jeder im System eingerichtete Bereich unterstützt die nachfolgend aufgeführten Alarmmodi.

Alarmmodus	Beschreibung
UNSCHARF	Der Bereich ist deaktiviert, nur Einbruch-MG mit dem Attribut „24 Stunden“ lösen einen Alarm aus.
INTERNSCHARF A	Dieser Modus bietet Schutz für einen bestimmten Bereich des Gebäudes, während man sich im Ein- und 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.
INTERNSCHARF B	Durch die Option INTERNSCHARF 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.
EXT. SCHARF	Der Bereich ist extern scharfgeschaltet. Das Öffnen von Meldergruppen startet die Alarmverzögerung. Wird der Alarm nicht unscharf geschaltet, bevor die Alarmverzögerung abläuft, wird der Alarm ausgelöst.

19.2 Betriebsmodus „Kommerziell

Der kommerzielle Modus ist geeignet für Installationen in gewerblich genutzten Gebäuden mit verschiedenen Bereichen und einer großen Anzahl von Einbruch-MGs. Jeder im System eingerichtete Bereich unterstützt die nachfolgend aufgeführten Alarmmodi.

Alarmmodus	Beschreibung
UNSCHARF	Der Bereich ist deaktiviert, nur Einbruch-MG mit dem Attribut „24 Stunden“ lösen einen Alarm aus.
INTERNSCHARF A	Dieser Modus bietet Schutz für einen bestimmten Bereich des Gebäudes, während man sich im Ein- und 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.
INTERNSCHARF B	Durch die Option INTERNSCHARF 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

Alarmmodus	Beschreibung
	Scharfschaltungsverzögerung in diesem Modus verwendet werden, indem der Parameter Intern scharf B verzögert aktiviert wird.
EXT. SCHARF	Der Bereich ist extern scharfgeschaltet. Das Öffnen von Meldergruppen startet die Alarmverzögerung. Wird der Alarm nicht unscharf geschaltet, bevor die Alarmverzögerung abläuft, wird der Alarm ausgelöst.

19.3 Betriebsmodus „Privat

Der private Modus ist geeignet für Installationen in Wohnhäusern mit einem oder mehreren Bereichen und einer kleinen bis mittleren Anzahl von Einbruch-MGs. Jeder im System eingerichtete Bereich unterstützt die nachfolgend aufgeführten Alarmmodi.

Alarmmodus	Beschreibung
UNSCHARF	Der Bereich ist deaktiviert, nur Einbruch-MG mit dem Attribut „24 Stunden“ lösen einen Alarm aus.
INTERNSCHARF A	DIeser Modus bietet Schutz für einen bestimmten Bereich des Gebäudes, während man sich im Ein- und Ausgangsbereich frei bewegen kann (z. B. an der Eingangstür und im Hausflur). Meldergruppen, die als NICHT BEI INTERN A klassifiziert wurden, bleiben in diesem Modus ungeschützt. In diesem Modus sind keine Scharfschaltungsverzögerungen verfügbar, die Überwachung beginnt sofort mit der Auswahl dieses Modus.
INTERNSCHARF B	Durch die Option INTERNSCHARF 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.
EXT. SCHARF	Der Bereich ist extern scharfgeschaltet. Das Öffnen von Meldergruppen startet die Alarmverzögerung. Wird der Alarm nicht unscharf geschaltet, bevor die Alarmverzögerung abläuft, wird der Alarm ausgelöst.

19.4 Volle und lokale Alarme

Die vom SPC-System generierten Alarmtypen können sich je nach Meldergruppentyp, der die Aktivierung des Alarms ausgelöst hat, unterscheiden. Der größte Teil aller Alarme erfordert die sichtbare (Blitzleuchte) und hörbare (Sirene) Anzeige eines Einbruchs in die überwachte Anlage bzw. in das überwachte Gebäude.

Standardmäßig sind die ersten drei Ausgänge am SPC-Controller für den Anschluss von Außensirene, Innensirene und externer Blitzleuchte vorgesehen. Bei Aktivierung bieten diese drei Ausgänge zusammen eine ausreichende Warnung vor einer Alarmbedingung für Personen innerhalb oder in der unmittelbaren Umgebung des Gebäudes bzw. der Anlage, in das bzw. in die eingebrochen wurde.

Volle und lokale Alarme auf der SPC aktivieren die folgenden physischen Ausgänge:

- Zentralenausgang 1: Außensirene
- Zentralenausgang 2: Innensirene
- Zentralenausgang 3: Blitzleuchte

Einzelheiten zur Verdrahtung der Sirenen und der Blitzleuchte finden Sie auf Seite [→ 74].

Eine **Voller Alarm**-Aktivierung meldet den Alarm an den Empfänger (Notruf- & Serviceleitstelle, NSL), sofern wenigstens ein Empfänger auf dem System konfiguriert wurde.

Einer **Lokaler Alarm**-Aktivierung folgt keine Meldung an einen Empfängern, selbst dann nicht, wenn wenigstens ein Empfänger konfiguriert wurde.

Eine **Stiller Alarm**-Aktivierung aktiviert die Ausgänge 1-3 nicht (keine sichtbare oder hörbare Anzeige des Alarms). Das Alarmereignis wird an den Empfänger gemeldet. Stille Alarme werden nur generiert, wenn Einbruch-MG mit dem Attribut „Still“ beim der Systemkonfiguration eingerichtet wurden.

20 Systembeispiele und -szenarien

20.1 Empfehlungen für die Einrichtung eines gemeinsamen Bereichs

Die Konfigurierung gemeinsamer Bereiche ist eine bequeme Möglichkeit, um innerhalb einer einzigen Anlage mehrere Bereiche einzurichten. Ein Benutzer, der einem gemeinsamen Bereich zugewiesen ist, kann ALLE Bereiche innerhalb dieses gemeinsamen Bereichs SCHARF schalten (einschließlich der Bereiche, die ihm nicht zugewiesen wurden). Die Benutzer können jedoch nur diejenigen Bereiche UNSCHARF schalten, die ihnen zugewiesen wurden.

Gemeinsame Bereiche sollten nur dann verwendet werden, wenn im primären Zugangsbereich nur ein einziges Bedienteil installiert ist, das von allen Benutzern innerhalb des Gebäudes benutzt wird (in einem System mit mehreren Bedienteilen in verschiedenen Bereichen ist die Einrichtung eines gemeinsamen Bereichs nicht zu empfehlen).

Szenario: 2 Abteilungen eines Unternehmens (Buchhaltung und Vertrieb) teilen sich einen gemeinsamen Zugangsbereich (Haupteingang).

In diesem Fall sollten im System 3 Bereiche eingerichtet werden (Gemeinsamer Bereich, Buchhaltung und Vertrieb). Dem gemeinsamen Bereich muss auch der Hauptzugangsbereich (Haupteingang) zugeorndet sein. Weisen Sie die Meldergruppen in der Buchhaltung dem Bereich 2 zu und die Meldergruppen im Vertrieb dem Bereich 3. Installieren Sie ein Bedienteil am Haupteingang und ordnen Sie es allen 3 Bereichen zu. Definieren Sie (mindestens) 2 Benutzer im System, einen pro Abteilung, und weisen Sie die Benutzer ihren jeweiligen Bereichen und dem gemeinsamen Bereich zu.

Bedienung: System scharfschalten

Der Leiter der Buchhaltung verlässt das Büro um 17 Uhr. Wenn er auf dem Bedienteil seine PIN eingibt, werden unter der Option EXTERN SCHARF die folgenden 3 Untermenüs angezeigt:

- ALLE BEREICHE: Schaltet alle dem gemeinsamen Bereich zugeordneten Bereiche (Gemeinsamer Bereich, Buchhaltung und Vertrieb) scharf sowie alle zusätzlichen Bereiche, die dem Leiter der Buchhaltung zugewiesen sind (in diesem Fall sind keine weiteren Bereiche eingerichtet). Der Timer für die Scharfschaltungsverzögerung am Haupteingang fordert den Benutzer auf, das Gebäude zu verlassen.
- GEMEINS. BEREICH: Schaltet alle dem gemeinsamen Bereich zugeordneten Bereiche (Gemeinsamer Bereich, Buchhaltung und Vertrieb) scharf und aktiviert die Scharfschaltungsverzögerung für den Haupteingang.
- BUCHHALTUNG: Schaltet nur den Bereich Buchhaltung scharf, der Bereich Vertrieb bleibt unscharf. Der Zutritt am Haupteingang ist weiterhin gestattet.

Wenn der letzte Vertriebsmitarbeiter das Gebäude verlässt, schließt er/sie alle Türen und Fenster in BEREICH 3 und gibt am Bedienteil seine/ihre PIN ein. Unter der Option EXTERN SCHARF werden die folgenden 3 Untermenüs angezeigt:

- ALLE BEREICHE: Schaltet alle dem gemeinsamen Bereich zugeordneten Bereiche (Gemeinsamer Bereich, Buchhaltung und Vertrieb) scharf sowie alle zusätzlichen Bereiche, die dem Vertriebsarbeiter zugewiesen sind; in diesem Fall sind keine weiteren Bereiche eingerichtet. Der Timer für die Scharfschaltungsverzögerung am Haupteingang fordert den Benutzer auf, das Gebäude zu verlassen.
- GEMEINS. BEREICH: Schaltet alle dem gemeinsamen Bereich zugeordneten Bereiche (Gemeinsamer Bereich, Buchhaltung und Vertrieb) scharf und aktiviert die Scharfschaltungsverzögerung für den Haupteingang.

- VERTRIEB: Schaltet ALLE dem gemeinsamen Bereich zugeordneten Bereiche (Gemeinsamer Bereich, Buchhaltung und Vertrieb) scharf, da im System keine sonstigen unscharfen Unterbereiche vorhanden sind.

Bedienung: System unscharfschalten

Wenn der Leiter der Buchhaltung am Morgen kommt, um das Gebäude aufzuschließen, und seine PIN eingibt, werden unter der Option UNSCHARF die folgenden 3 Untermenüs angezeigt:

- ALLE BEREICHE: Schaltet alle dem Mitarbeiter der Buchhaltung zugeordneten Bereiche (Gemeinsamer Bereich, Buchhaltung) unscharf und deaktiviert alle zusätzlichen Bereiche, die dem Mitarbeiter der Buchhaltung zugewiesen sind. In diesem Fall sind keine weiteren Bereiche eingerichtet. HINWEIS: Der Mitarbeiter der Buchhaltung kann den Bereich Vertrieb nicht UNSCHARF schalten.
- GEMEINS. BEREICH: Schaltet NUR den gemeinsamen Bereich (Empfang) unscharf. Mit dieser Option kann nur der Empfangsbereich unscharf geschaltet werden, während die Buchhaltung und der Vertrieb scharfgeschaltet bleiben.
- BUCHHALTUNG: Schaltet den Bereich Buchhaltung und den gemeinsamen Bereich (Empfang) unscharf. In diesem Fall bleibt der Bereich Vertrieb scharfgeschaltet. Der Zutritt am Haupteingang ist weiterhin gestattet.

Verwendung von gemeinsamen Bereichen:

- Meldergruppe Scharf/Unscharf Eingang

Ist die Route für das Betreten/Verlassen des gemeinsamen Bereichs als Meldergruppe Scharf/Unscharf Eingang programmiert, werden alle Bereiche, die zum gemeinsamen Bereich gehören, SCHARF geschaltet, sobald diese Meldergruppe aktiviert wird. Wird die Meldergruppe Scharf/Unscharf Eingang deaktiviert, werden alle Bereiche des gemeinsamen Bereichs UNSCHARF geschaltet.

- Mehrere Bedienteile

Sind Bereiche, die dem gemeinsamen Bereich zugeordnet sind, mit eigenen Bedienteilen für Eingangs-/Ausgangskontrolle ausgestattet, muss darauf geachtet werden, dass die Scharfschaltverzögerungszeiten, die diesen Bereichen zugeordnet werden, ausreichend lang sind, damit der Benutzer den Ausgang des gemeinsamen Bereichs erreichen kann, bevor das System scharfgeschaltet wird. Dies gilt insbesondere für den Fall, dass der scharfgeschaltete Bereich der letzte noch unscharfe Bereich im System ist und somit die Scharfschaltung des gesamten gemeinsamen Bereichs auslöst.

Es empfiehlt sich, gemeinsame Bereiche in Anlagen einzusetzen, die nur mit einem Bedienteil am gemeinsamen Eingang, d. h. dem Haupteingang zum gesamten Gebäude, ausgestattet sind.

21 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 Gehtest geöffnet wird. Diese Testmethode ist mit allen Körperschallmeldertypen möglich.

Wenn der Körperschallmelder mit einem Testsender ausgestattet ist, sind folgende Testmöglichkeiten verfügbar:

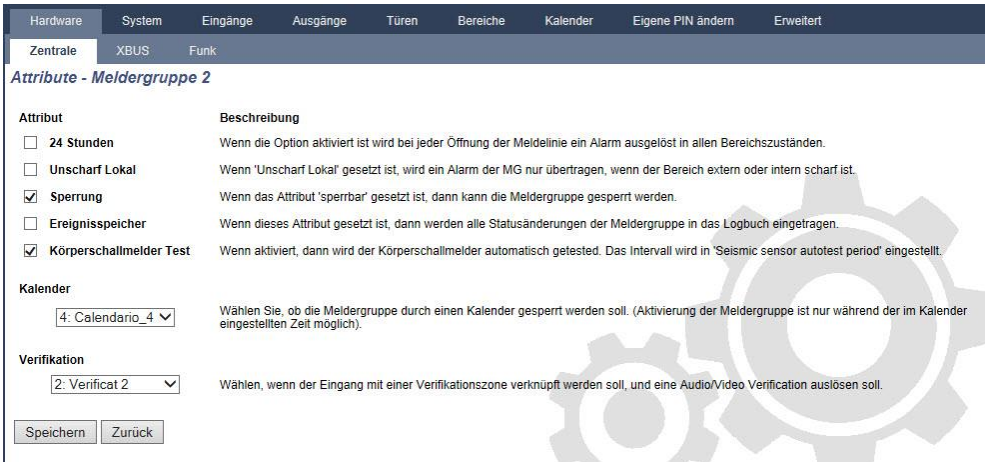
- Manuelles Testen, das am Bedienteil oder in SPC Pro (keine Browserunterstützung) initiiert wird;
- Automatisches Testen in regelmäßigen Intervallen oder wenn die Zentrale über das Bedienteil geschärft wird.

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

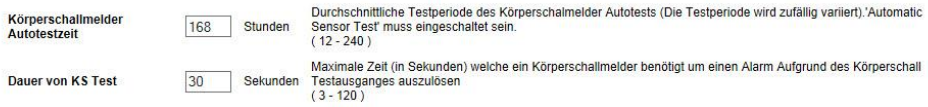
1. Konfigurieren Sie eine Körperschall-MG. Körperschallmelder müssen einer MG zugewiesen sein. (Siehe Meldergruppe bearbeiten [→ 256].)

2. Legen Sie die Attribute der Meldergruppe fest.



3. Aktivieren Sie das automatische Testen des Melders mit dem Attribut **Automatischer Sensor Test**.
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 [→ 248].)



7. Konfigurieren Sie einen Ausgang zum Testen einer Körperschall-MG. (Siehe Ausgangstypen und Ausgangsschnittstellen [→ 213])
   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.

Verwenden des Bedienteils

1. Wählen Sie **KONFIGURATIONSMODUS > Meldergruppen > (MG wählen) > MG-Typ > KSM**.
2. Wählen Sie **KONFIGURATIONSMODUS > MELDERGRUPPEN > (MG wählen) > ATTRIBUTE > AUTOMATISCHER SENSOR TEST**.

Siehe auch

- Timer [→ 248]
- Ausgangstypen und Ausgangsschnittstellen [→ 213]
- Meldergruppe bearbeiten [→ 256]

21.1 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.

21.1.1 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.

21.1.2 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 [→ 248] 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 [→ 239] 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.

21.1.3 Manueller Meldertest

Wählen Sie zum manuellen Testen der Melder auf dem Bedienteil im Menü TEST die Optionen TEST > KSM TEST aus.

Ein manueller Test der Körperschall-MGs mit dem Bedienteil kann vom Techniker im Konfigurationsmodus und ebenfalls von einem Benutzer des Typs „Manager“ oder „Standard“ ausgeführt werden.

- Ein Techniker kann mit einem Bedienteil alle Melder in allen Bereichen testen, die im System konfiguriert sind.
- Ein Benutzer kann nur die Melder in den Bereichen testen, die ihm und dem Bedienteil, das er verwendet, zugewiesen sind.

Wählen Sie zur Durchführung eines Tests der Körperschallmelder im Technikermodus die Optionen KONFIGURATIONSMODUS ⇒ TEST ⇒ KSM TEST.

Wählen Sie zur Durchführung eines Tests der Körperschallmelder im Benutzermodus die Optionen MENÜ ⇒ TEST ⇒ KSM TEST.

Hinweis: Die folgenden Anweisungen beziehen sich sowohl auf den Techniker- als auch den Benutzermodus. Beachten Sie jedoch, dass einem Benutzer nur ein Teil der Optionen zur Verfügung stehen könnte.

Die folgenden Optionen sind im Menü KSM TEST verfügbar:

- TEST ALLE BER.
  Testet Körperschall-MGs in allen verfügbaren Bereich, wenn mehr als ein Bereich Körperschall-MGs enthält.
- *NAME BEREICH*
  Die Namen der Bereiche, die Körperschall-MGs enthalten, werden einzeln aufgelistet. Wenn ein bestimmter Bereich ausgewählte wird, stehen folgende Optionen zur Verfügung:

- TEST ALLE MG
  Testet alle Körperschall-MGs in diesem Bereich, wenn mehr als eine Körperschall-MG vorhanden ist.
- *NAME MG*
  Die Namen aller Körperschall-MGs werden aufgelistet und können für individuelle Tests ausgewählt werden.

Während des Tests wird die Meldung „KSM TEST“ auf dem Bedienteil angezeigt.

Wenn der Test fehlschlägt, wird die Meldung „KSM FEHLER“ angezeigt. Durch Drücken der „i“- oder ANZEIGE-Taste wird eine Liste der fehlgeschlagenen MGs angezeigt, die durchgeblättert werden kann.

Ist der Test erfolgreich, wird „TEST OK“ angezeigt.

Ergebnisse werden im Logbuch mit den folgenden Details gespeichert:

- Benutzer, der den Test initiiert hat
- Ergebnis (OK oder FEHLER)
- Bereichs- und MG-Nummer/-Name.

Bei manuellen Tests werden keine Ereignisse gemeldet.

22 Funktion des Blockschlosses

Die Blockschlossbetätigung und die Scharfschalteberechtigung eines Blockschlosses werden durch die SPC Zutrittskontrolle unterstützt.

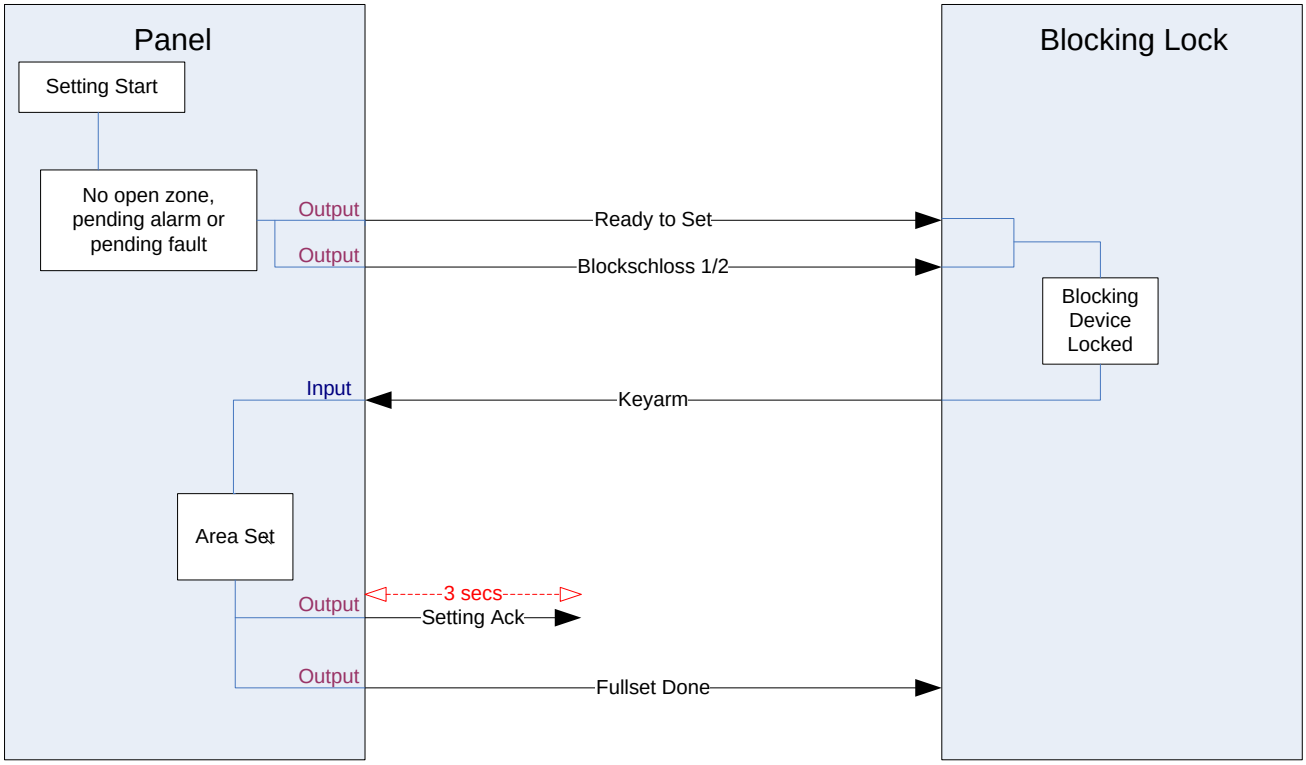
22.1 Blockschloss

Ein Blockschloss ist eine mechanische Sperre, die neben einem normalen Schloss an einer Tür angebracht wird und zur Scharf- und Unscharfschaltung eines Einbruchmeldesystems verwendet wird. SPC unterstützt normale Blockschlossvorrichtungen (Blockschloss 1) sowie das Bosch Blockschloss Sigmalock Plus und E4.03 (Blockschloss 2).

Je nach Blockschloss ist ein Signal erforderlich, um das Sperren und Entsperren des Schlosses zu aktivieren, d. h. das Blockschloss kann nur gesperrt und das System nur scharf geschaltet werden, wenn die Zentrale das Signal "Schärfungsbereit" sendet. Dies wird mithilfe eines Magnetschalters gesteuert.

Ein Blockschloss funktioniert wie folgt:

1. Wenn keine offene Meldergruppe vorhanden ist, kein Alarm und keine Störung in einem Bereich aussteht, kann der Bereich scharf geschaltet werden und die Zentrale sendet das Signal Schärfungsbereit.
2. Wenn das Blockschloss daraufhin gesperrt wird, wird der Ausgang für Blockschloss 1/2 aktiviert.
3. Gemäß der Änderung im Eingangstyp Scharf/Unscharf-Eingang wird der entsprechende Bereich scharf geschaltet.
4. Der Ausgang zur (Un-)Scharfschaltungsquittierung wird für 3 Sekunden aktiviert, um eine erfolgreiche Scharfschaltung des Bereichs zu signalisieren. Der Ausgang Blockschloss 1 wird deaktiviert, wenn das System scharf geschaltet wird. Blockschloss 2 bleibt aktiviert, wenn das System scharf geschaltet wird.
5. Bei Entsperrung des Blockschlosses wird der Scharf/Unscharf-Eingang in den unscharfen Zustand (geschlossen) geschaltet.
6. Gemäß der Änderung des Eingangstyps Scharf/Unscharf Eingang wird der Bereich unscharf geschaltet. Blockschloss 1 wird deaktiviert, Blockschloss 2 jedoch aktiviert, wenn der Bereich schärfungsbereit ist.



Die Konfigurationsanforderungen für ein Blockschloss sind wie folgt:

- Ausgänge:
  - Schärfungsbereit
  - Scharf-/Unscharf quittieren
  - Schärfung abgeschlossen
  - Blockschloss 1/2
- Eingänge
  - "Scharf/Unscharf Eingang"

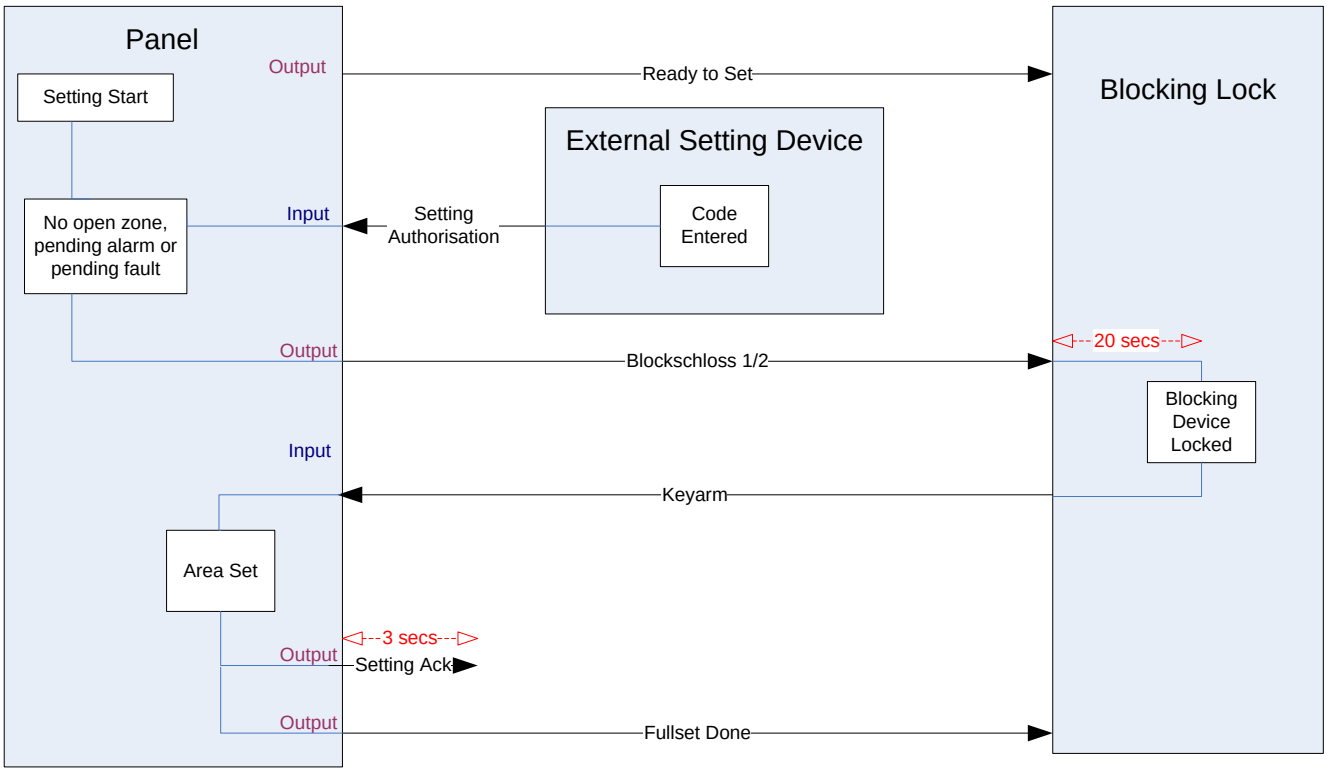
22.2 Berechtigte Scharfschaltung des Blockschlosses

Die Funktion der "Scharfschalteberechtigung" erweitert den Scharf- und Unscharfschaltungsvorgang für ein Blockschloss durch eine zweite Sicherheitsstufe. Bevor das System scharf oder unscharf geschaltet werden kann, muss ein Code in eine externe Scharfschaltungsvorrichtung wie einen Ausweis- oder PIN-Leser mit einem separaten Controller eingegeben werden. Dieser Controller kann über Eingänge und Ausgänge mit allen Arten von Einbruchmeldesystem verbunden werden.

Der Betrieb läuft wie folgt:

1. Die Zentrale signalisiert der externen Scharfschaltungsvorrichtung, wenn die Scharfschaltung über den Ausgang "Schärfungsbereit" möglich ist.
2. Bei Eingabe des Codes werden der Eingang zur Scharfschalteberechtigung sowie Blockschloss 1/2 aktiviert.
3. Das Blockschloss öffnet einen Zentraleneingang (Scharf/Unscharf Eingang), der den Scharfschaltungsvorgang der Zentrale initiiert.
4. Die externe (Un-)Scharfschaltungsvorrichtung wartet bis zu 8 Sekunden auf das Signal vom Ausgang "Schärfung abgeschlossen" von der Zentrale.

5. Wenn dieses Signal nicht empfangen wird, schlägt die Scharfschaltung fehl und die externe Scharfschaltungsvorrichtung schaltet das System wieder unscharf.



Die Konfigurationsanforderungen für eine berechtigte Scharfschaltung sind wie folgt:

- Bereichsattribute:
  - Scharfschalteberechtigung
    Scharf
    Scharf und Unscharf (für VdS erforderlich)
    Unscharf
- Ausgänge:
  - Schärfungsbereit
  - Scharf-/Unscharf quittieren
  - Schärfung abgeschlossen
- Eingänge
  - "Scharf/Unscharf Eingang"

22.3 Sperrelement

Für die Einhaltung der VdS-Bestimmungen ist es zwingend notwendig, das Eindringen in einen scharf geschalteten Bereich zu verhindern. Dies erfolgt, indem ein Sperrelement verwendet wird, das am Türrahmen befestigt ist. Das Sperrelement besteht aus einer kleinen Kunststoffschraube, welche die Tür in einem scharfen Zustand sperrt. Die Position der Schraube wird durch die Ausgänge **Sperrelement – schließt** und **Sperrelement – öffnet** signalisiert. Dieses Signal wird während des Scharfschaltungsvorgangs geprüft. Wenn die Information "gesperrt" nicht empfangen wird, schlägt die Scharfschaltung fehl.

Wenn sich ein Sperrelement in einem Bereich befindet, wird der Ausgangs-Timer auf ein Minimum von 4 Sekunden beschränkt, so dass das Sperrelement aktiviert werden kann. Wenn der Scharfschaltungsverzögerung 4 Sekunden erreicht, wird

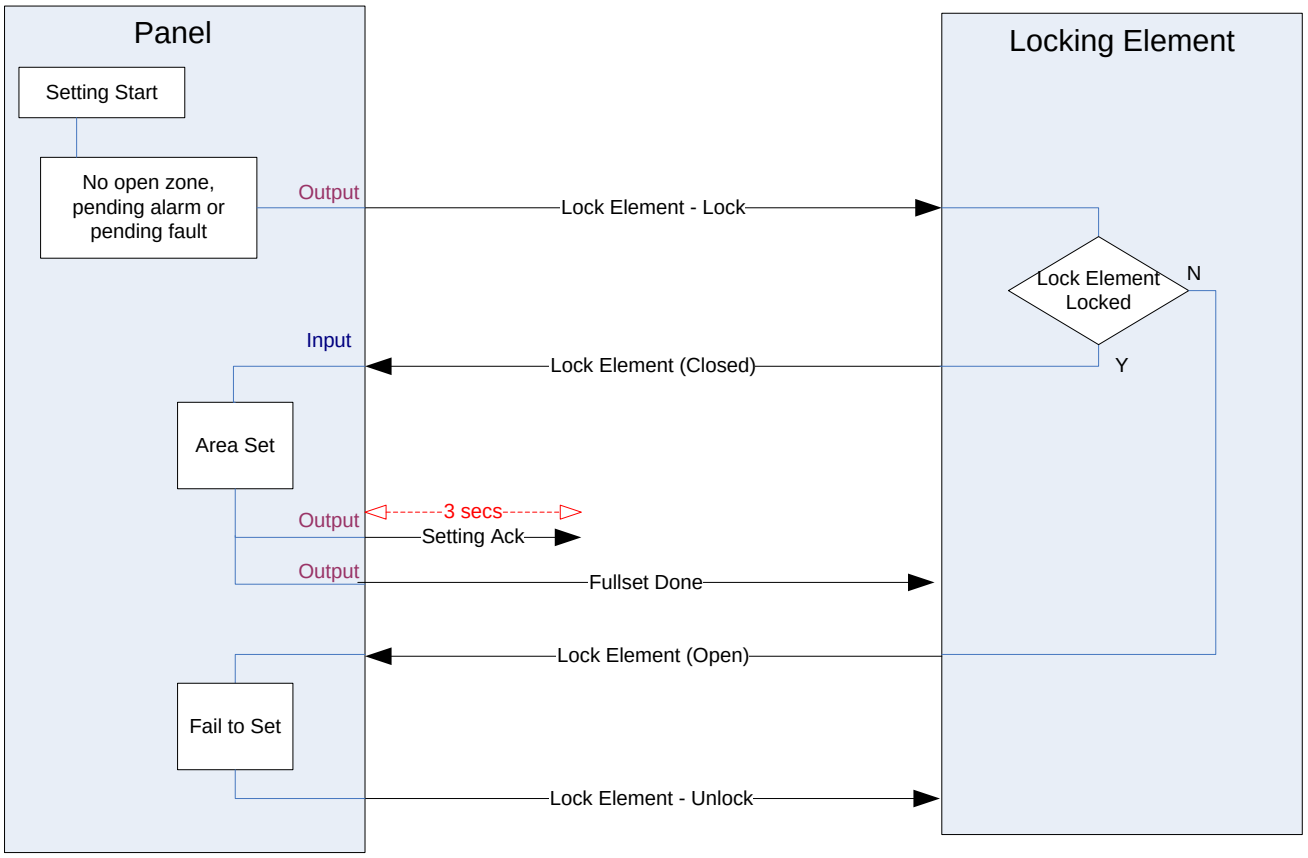
das Sperrelement für 3 Sekunden aktiviert. Wenn die Scharfschaltungsverzögerung abgelaufen ist, muss sich der Sperrelementeingang im geschlossenen Zustand befinden. Daraufhin wird das System scharf geschaltet.

Wenn ein Sperrelement während eines Scharfschaltungszeitraums geöffnet wird, wird es wie eine Alarmmeldergruppe behandelt.

Wenn ein Sperrelement während eines Unscharfschaltungsvorgangs geschlossen wird, wird es als sabotiert angesehen und ein Sabotagealarm für die Meldergruppe ausgelöst.

Wenn das Sperrelement nach dem Entsperrungssignal zur Vorrichtung nicht geöffnet wird, wird eine Störungswarnung für die Meldergruppe generiert, um eine mechanische Störung zu melden.

Wenn sich der Eingang des Sperrelements (wenn konfiguriert) beim Ablauf des Ausgangs-Timers nicht im geschlossenen Zustand befindet, wird das System nicht scharf geschaltet und das Signal "Scharfschaltung fehlgeschlagen" wird gesendet. Der Ausgang Sperrelement öffnet wird aktiviert.



Die Konfigurationsanforderungen für das Sperrelement lauten wie folgt:

- Ausgänge:
  - Sperrelement schließt
  - Sperrelement öffnet
- Eingänge
  - Sperrelement

23 Anhang

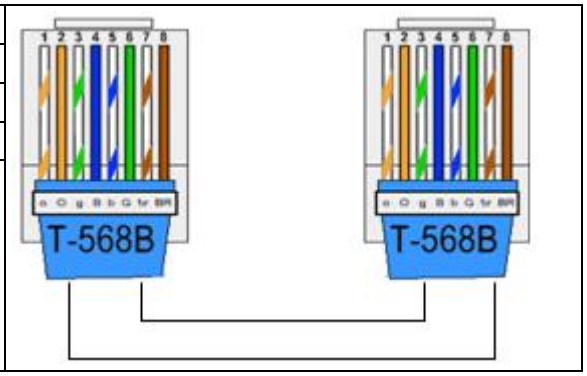
23.1 Netzwerk-Kabelverbindungen

IP

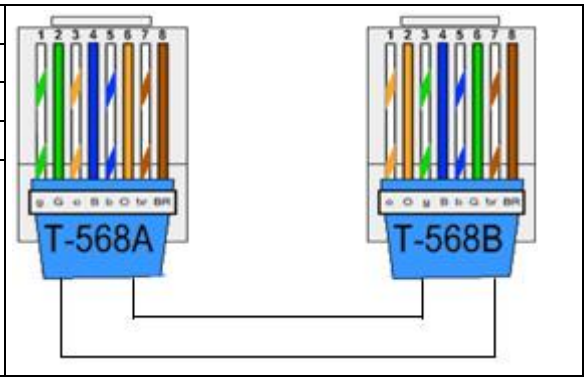
An die SPC-Zentrale kann direkt über die Ethernet-Schnittstelle oder über eine LAN-Verbindung ein PC angeschlossen werden. In der nachstehenden Tabelle sind die beiden möglichen Konfigurationen aufgeführt.

- 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.

RJ45-Pin-Belegung	RJ45-Pin-Belegung	
1 (RX +)	1 (TX+)	
2 (RX -)	2 (TX-)	
3 (TX+)	3 (RX+)	
6 (TX-)	6 (RX -)	

Verwenden Sie das Kreuzkabel, um den SPC-Controller direkt an einen PC anzuschließen.

RJ45-Pin-Belegung	RJ45-Pin-Belegung	
1 (RX +)	3 (TX+)	
2 (RX -)	6 (TX-)	
3 (TX+)	1 (RX +)	
6 (TX-)	2 (RX -)	

23.2 LEDs für Controller-Status

LED	Funktion
LED 1	Funkdaten BLINKT: Datenempfang über das Funkmodul AUS: kein Datenempfang über Funk
LED 2	Batteriezustand EIN: Batteriespannung ist unter das Tiefentladungsniveau (10,9 V) gefallen

	AUS: Zustand OK
LED 3	Stromversorgung EIN: Netzausfall AUS: Stromversorgung OK
LED 4	X-BUS-Status EIN: X-BUS als Ring konfiguriert AUS: X-BUS als Stichleitung konfiguriert BLINKT: hat EOL-Erweiterungsmodule oder Kabelbruch entdeckt
LED 5	Systemstörung EIN: auf der Platine wurde ein Hardwarefehler entdeckt AUS: kein Hardwarefehler entdeckt
LED 6	Schreiben in Flash-Speicher EIN: System schreibt in Flash-Speicher AUS: System schreibt nicht in Flash-Speicher
LED 7	Heartbeat BLINKT: System arbeitet fehlerfrei

EIN	AUS	BLINKT

23.3 Stromversorgung der Erweiterungsmodule über die Hilfsstromversorgungsanschlüsse

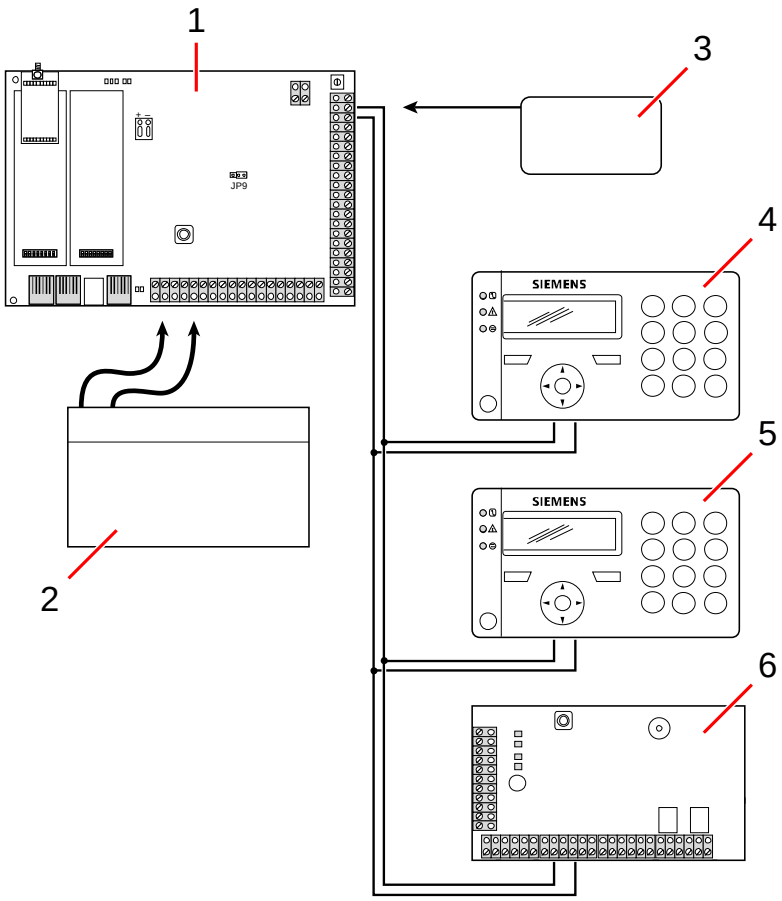
Um zu bestimmen, wie viele Erweiterungsmodule/Bedienteile problemlos an diese 12-VDC-Hilfsstromversorgungsanschlüsse angeschlossen werden können, müssen die Höchststromverbrauchswerte aller gewünschten Erweiterungsmodule/Bedienteile aufaddiert werden. Die Hilfsausgangsspannung darf 12 V DC nicht überschreiten.

Informationen zum spezifischen Hilfsstrom und die entsprechende Installationsanleitung bzw. das Datenblatt zur Stromaufnahme der Module, Bedienteile und Erweiterungsmodule finden Sie im Abschnitt .

Stromaufnahme (mA) Erweiterungsmodul 1 + Stromaufnahme (mA) Erweiterungsmodul 2 +... < Hilfsstrom

Wenn die elektronischen oder Relaisausgänge bereits externe Geräte mit Spannung versorgen, muss die Spannung zu diesen Geräten von der 12 V-DC-Hilfsspannungsversorgung abgezogen werden, um die verfügbare Spannung von den Hilfsstromversorgungsanschlüssen (0 V 12 V) zu bestimmen.

Überschreitet der Gesamt-Höchststromverbrauch der Erweiterungen den Hilfsstrom, sollte ein Netzteil-Erweiterungsmodul verwendet werden, um die Stromversorgung aller Geräte zu gewährleisten.



Stromversorgung der Erweiterungsmodule über die Hilfsstromversorgungsanschlüsse

1	SPC-Controller
2	Batterie
3	Hilfsstromversorgungsanschlüsse (12 V)
4	Bedienteil
5	Bedienteil
6	E/A-Erweiterungsmodul

23.4 Berechnung der erforderlichen Batterieleistung

Es ist wichtig, dass eine angemessene Standby-Stromversorgung zur Verfügung steht, um alle Geräte bei einem Ausfall der Netzversorgung mit Strom zu versorgen. Um eine ausreichende Stromversorgung zu gewährleisten, müssen immer die richtige Backup-Batterie und das richtige Netzteil angeschlossen werden.

In der unten stehenden Tabelle sind Näherungswerte für den maximalen Laststrom aufgeführt, der jedem Akkutyp über die angegebenen Standby-Zeiten entnommen werden kann.

Bei diesen Näherungswerten wird vorausgesetzt, dass der Stromverbrauch der SPC-Controller-Platine bei seinem Maximalwert liegt (alle verdrahteten Eingänge sind mit den jeweiligen Endwiderständen versehen) und die von der Batterie bereitgestellte Ausgangsleistung 85% ihrer maximalen Kapazität beträgt.

0,85 x Batteriekapazität (Ah)	-	(Icont + Ibell)	=	Imax
Zeit (Stunden)				

Batteriegröße = Kapazität in Ah, abhängig vom SPC-Gehäuse

Zeit = Sicherungsdauer in Stunden, abhängig vom Sicherheitsgrad

Icont = Ruhestrom (in A) der SPC-Zentrale

Ibell = Ruhestrom (in A) der angeschlossenen Außen- und Innensirenen

Imax = Höchststrom, der an den Hilfsstromanschlüssen abgenommen werden kann

Strommenge am Zusatzausgang bei Verwendung einer 7-Ah-Batterie (SPC422x/522x)

KOMM Standby-Zeit	KEINE	PSTN	GSM	PSTN+GSM
12 Std.	356 mA	331 mA	226 mA	201 mA
30 Std.	58 mA	33 mA	n.r.	n.r.

Strommenge am Zusatzausgang bei Verwendung eine 17-Ah-Batterie (SPC523x)

KOMM Standby-Zeit	KEINE	PSTN	GSM	PSTN+GSM
12 Std.	750 mA	750 mA	750 mA	750 mA
30 Std.	342 mA	317 mA	212 mA	187 mA

Strommenge am Zusatzausgang bei Verwendung einer 7-Ah-Batterie (SPC432x/532x)

KOMM Standby-Zeit	KEINE	PSTN	GSM	PSTN+GSM
12 Std.	326 mA	301 mA	196 mA	171 mA
30 Std.	28 mA	n.r.	n.r.	n.r.

Strommenge am Zusatzausgang bei Verwendung einer 17-Ah-Batterie (SPC533x/633x)

KOMM Standby-Zeit	KEINE mA	PSTN mA	GSM mA	PSTN+GSM mA
12 Std.	750	750	750	750
30 Std.	312	287	182	157

Strommenge am Zusatzausgang bei Verwendung einer 17-Ah-Batterie (SPC535x/635x)

KOMM Standby-Zeit	KEINE mA	PSTN mA	GSM mA	PSTN+GSM mA
12 Std.	1650	1625	1610	1585
24 Std.	650	625	610	585
30 Std.	450	425	410	385
60 Std.	50	25	10	n.r.

Strommenge am Zusatzausgang bei Verwendung einer 24-Ah-Batterie (SPC535x/635x)

KOMM Standby-Zeit	KEINE mA	PSTN mA	GSM mA	PSTN+GSM mA
12 Std.	2205	2180	2165	2140
24 Std.	1650	1625	1610	1585
30 Std.	1250	1225	1210	1185
60 Std.	450	425	410	385

Strommenge am Zusatzausgang bei Verwendung einer 27-Ah-Batterie (SPC535x/635x)

KOMM Standby-Zeit	KEINE mA	PSTN mA	GSM mA	PSTN+GSM mA
12 Std.	1900	1875	1860	1835
24 Std.	775	750	735	710
30 Std.	550	525	510	485
60 Std.	100	75	60	35

Strommenge am Zusatzausgang bei Verwendung einer 27-Ah-Batterie (SPC535x/635x)

KOMM Standby-Zeit	KEINE mA	PSTN mA	GSM mA	PSTN+GSM mA
12 Std.	2205	2180	2165	2140
24 Std.	1900	1875	1860	1835
30 Std.	1450	1425	1410	1385
60 Std.	550	525	510	485

Die Angabe „nicht relevant (n.r.)“ bedeutet, dass die gewählte Batterie nicht die Kapazität besitzt, um auch nur die Mindestlast der SPC-Zentrale über die angegebene Standby-Zeit zu decken. Siehe Seite [→ 361] für Angaben zur Höchstlast von Geräten und Modulen.

Es dürfen nur geschlossene, ventilgeregelte Batterien verwendet werden.

Um die EN-Anforderungen zu erfüllen, muss der Versorgungsstrom über die erforderliche Standby-Zeit von der Batterie bereitgestellt werden.

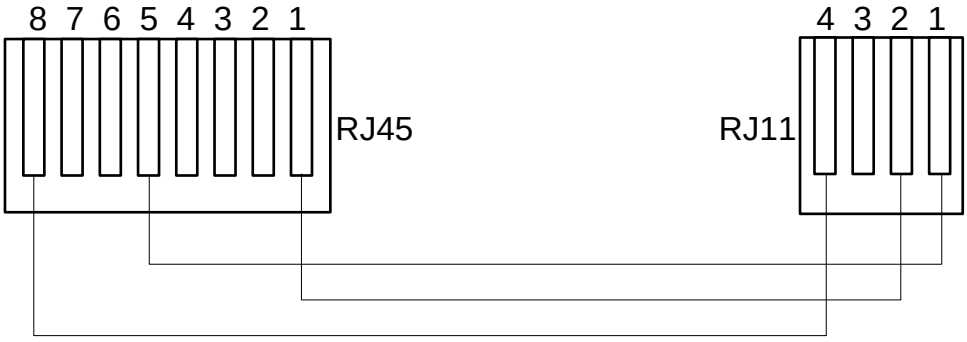
23.5 Standardeinstellungen für die Modi „Privat“, „Kommerziell“ und „Finanziell“

In der nachstehenden Tabelle sind für den jeweiligen Betriebsmodus die Standard-Einstellungen bzw. -benennungen (Meldergruppenname und -typ) in der Zentrale angegeben. All Meldergruppen auf angeschlossenen Erweiterungsmodulen

werden als nicht benutzt eingestuft, solange sie nicht ausdrücklich vom Installationstechniker konfiguriert werden.

Funktion	Modus Privat	Modus Kommerziell	Finanzieller Modus
Meldergruppennamen			
Zentrale - Meldergruppe 1	Haupteingang	Haupteingang	Haupteingang
Zentrale - Meldergruppe 2	Wohnzimmer	Fenster 1	Fenster 1
Zentrale - Meldergruppe 3	Küche	Fenster 2	Fenster 2
Zentrale - Meldergruppe 4	Obergeschoss Vorderfront	PIR 1	PIR 1
Zentrale - Meldergruppe 5	Obergeschoss Rückfront	PIR 2	PIR 2
Zentrale - Meldergruppe 6	PIR Flur	Notausgang	Notausgang
Zentrale - Meldergruppe 7	PIR Treppenabsatz	Feueralarm	Feueralarm
Zentrale - Meldergruppe 8	Überfalltaste	Überfalltaste	Überfalltaste
Meldergruppentypen			
Zentrale - Meldergruppe 1	EINBRUCH VERZÖGERT	EINBRUCH VERZÖGERT	EINBRUCH VERZÖGERT
Zentrale - Meldergruppe 2	EINBRUCH	EINBRUCH	EINBRUCH
Zentrale - Meldergruppe 3	EINBRUCH	EINBRUCH	EINBRUCH
Zentrale - Meldergruppe 4	EINBRUCH	EINBRUCH	EINBRUCH
Zentrale - Meldergruppe 5	EINBRUCH	EINBRUCH	EINBRUCH
Zentrale - Meldergruppe 6	EINBRUCH	NOTAUSGANG	EINBRUCH
Zentrale - Meldergruppe 7	EINBRUCH	FEUER	EINBRUCH
Zentrale - Meldergruppe 8	ÜBERFALL	ÜBERFALL	EINBRUCH

23.6 Verdrahtung der X10-Schnittstelle



Verdrahtung des X10-Anschlusses an die Zentrale

PIN	RJ45	RJ11
TX	8	4
Masse	5	1
RX	1	2

23.7 SIA-Codes

BESCHREIBUNG	CODE
AC RESTORAL	AR
AC TROUBLE	AT
BURGLARY ALARM	BA
BURGLARY BYPASS	BB
BURGLARY CANCEL	BC
SWINGER TROUBLE	BD
SWINGER TROUBLE RESTORE	BE
BURGLARY TROUBLE RESTORE	BJ
BURGLARY RESTORAL	BR
BURGLARY TROUBLE	BT
BURGLARY UNBYPASS	BU
BURGLARY VERIFIED	BV
BURGLARY TEST	BX
CLOSING DELINQUENT	CD
FORCED CLOSING	CF
CLOSE AREA	CG
FAIL TO CLOSE	CI
EARLY TO CLOSE	CK
CLOSING REPORT	ZU
AUTOMATIC CLOSING	CP
REMOTE CLOSING	CQ
CLOSING KEYSWITCH	CS

BESCHREIBUNG	CODE
LATE TO OPEN	CT
ACCESS CLOSED	DC
ACCESS DENIED	DD
DOOR FORCED	DF
ACCESS GRANTED	DG
ACCESS DENIED PASSBACK	DI
DOOR LEFT OPEN	DN
ACCESS OPEN	DO
DOOR RESTORAL	DR
REQUEST TO EXIT	DX
EXIT ALARM	EA
EXPANSION TAMPER RESTORE	EJ
EXPANSION MISSING	EM
EXPANSION MISSING RESTORE	EN
EXPANSION RESTORAL	ER
EXPANSION DEVICE TAMPER	ES
EXPANSION TROUBLE	ET
FIRE ALARM	FA
FIRE BYPASS	FB
FIRE CANCEL	FC
FIRE TROUBLE RESTORE	FJ
FIRE RESTORAL	FR
FIRE TROUBLE	FT
FIRE UNBYPASS	FU
HOLDUP ALARM	HA
HOLDUP BYPASS	HB
HOLDUP TROUBLE RESTORE	HJ
HOLDUP RESTORAL	HR
HOLDUP TROUBLE	HT
HOLDUP UNBYPASS	HU
BESTÄTIGTER ÜBERFALL	HV
USER CODE TAMPER ¦WEB or ¦XBUS	JA
TIME CHANGED	JT
LOCAL PROGRAMMING	LB
MODEM RESTORAL ¦ 1 or 2	LR
MODEM TROUBLE ¦ 1 or 2	LT
LOCAL PROGRAMMING ENDED	LX
MEDICAL ALARM	MA
MEDICAL BYPASS	MB
MEDICAL TROUBLE RESTORE	MJ
MEDICAL RESTORAL	MR

BESCHREIBUNG	CODE
MEDICAL TROUBLE	MT
MEDICAL UNBYPASS	MU
PERIMETER ARMED	NL
NETWORK LINK IP RESTORE	NR
NETWORK LINK GPRS RESTORE	NR
NETWORK LINK IP FAIL	NT
NETWORK LINK GPRS FAIL	NT
AUTOMATIC OPENING	OA
OPEN AREA	OG
EARLY OPEN	OK
OPENING REPORT	OF
OPENING KEYSWITCH	OS
LATE TO CLOSE	OT
REMOTE OPENING	OQ
DISARM FROM ALARM	OR
ÜBERFALLALARM	PA
PANIC BYPASS	PB
PANIC TROUBLE RESTORE	PJ
PANIC RESTORAL	PR
PANIC TROUBLE	PT
PANIC UNBYPASS	PU
RELAY CLOSE	RC
REMOTE RESET	RN
RELAY OPEN	RO
AUTOMATIC TEST	RP
POWERUP	RR
REMOTE PROGRAM SUCCESS	RS
DATA LOST	RT
MANUAL TEST	RX
SABOTAGE	TA
TAMPER BYPASS	TB
TAMPER RESTORAL	TR
TAMPER UNBYPASS	TU
TEST CALL	TX
UNTYPED ALARM	UA
UNTYPED BYPASS	UB
UNTYPED TROUBLE RESTORE	UJ
UNTYPED RESTORAL	UR
UNTYPED TROUBLE	UT
UNTYPED UNBYPASS	UU
BELL FAULT	YA

BESCHREIBUNG	CODE
RF JAM RESTORAL	XH
RF TAMPER RESTORAL	XJ
LESER GESPERRT	RL
LESER ENTSPERRT	RG
BEDIENTEIL ENTSPERRT	KG
RF JAM FAULT	XQ
RF TAMPER	XS
COMMUNICATION FAIL	YC
CHECKSUM FAULT	YF
BELL RESTORED	YH
COMMUNICATION RESTORAL	YK
AKKU MISSING	YM
PSU TROUBLE	YP
PSU RESTORAL	YQ
AKKU RESTORAL	YR
COMMUNICATION TROUBLE	YS
AKKU TROUBLE	YT
WATCHDOG RESET	YW
SERVICE REQUIRED	YX
SERVICE COMPLETED	YZ
SPEZIELLE SIA-EREIGNISSE	
BEDROHUNGSPIN	HA
USER DURESS RESTORE	HR
ENET PANIC ALARM	PA
ENET PANIC RESTORAL	PR
USER PANIC ALARM	PA
ENET FIRE ALARM	FA
ENET FIRE RESTORAL	FR
ENET MEDICAL ALARM	MA
ENET MEDICAL RESTORAL	MR
MDT PANIC	PA
MDT TILT	MA
MDT BELT CLIP	HA
MDT PANIC RESTORE	PR
MDT TILT RESTORE	MR
MDT BELT CLIP RESTORE	HR
RPA PANIC	PA
RPA PANIC RESTORE	PR
RPA HOLDUP	HA
RPA HOLDUP RESTORE	HR
BENUTZER-PIN ÄNDERN	JV

BESCHREIBUNG	CODE
PIN GELÖSCHT	
NICHT STANDARDMÄSSIGE SIA-CODES FÜR MG-ZUSTANDSMELDUNG	
MG OFFEN	ZO
MG GESCHLOSSEN	ZC
MG KURZGES.	ZX
MG LEITUNGSBRUCH	ZD
MG ABGEDECKT	ZM
MG GEHTEST	TP
WALKTEST START	ZK
GEHTEST BEENDET	TC
MG BATTERIE SCHWACH	XT
ZONE LOW BATTERY RESTORAL	XR
ANDERE NICHT STANDARDMÄSSIGE CODES	
KAMERA ONLINE	CU
KAMERA OFFLINE	CV
ALARM GESCHLOSSEN	SD
ALARM NEU ÖFFNEN	SO
XBUS ALARM GESCHLOSSEN	NB
XBUS ALARM NEU AUFRUFEN	NO
UNBEK. AUSWEIS	AU
BENUTZERZUGANG	JP
BEUTZERZUGANG BEENDET	ZG
NIEDRIGE SPANNUNG	XD
LOW VOLTAGE RESTORAL	XG
DEEP CHARGE	XK
"BT BLOCKIERT"	WW

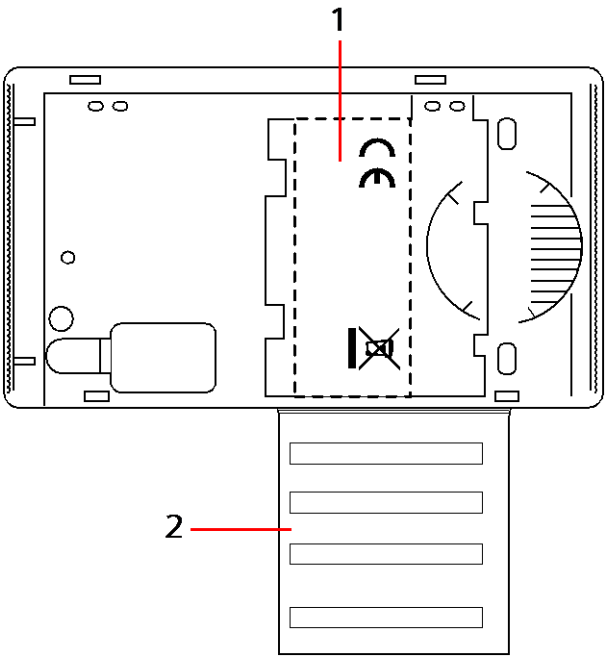
23.8 CID-Codes

CODE	CID-EREIGNIS	BESCHREIBUNG
100	MEDIZINISCHER NOTFALL	Medizinischer oder Überfallalarm und Quittierung.
110	FEUER	
120	ÜBERFALL	
121	BEDROHUNG	
129	BESTÄTIGTER ÜBERFALL	Weitere Informationen finden Sie unter Konfigurationsanforderungen zur Einhaltung der Norm PD 6662:2010 [→ 27].
130	EINBRUCH	
134	EINBRUCH VERZÖGERT	
137	SABOTAGE	Fehlerhafte Sabotage am Deckelkontakt und Zusatzgerät sowie Quittierung.

139	VERIFIED	Bestätigter Alarm.
144	MELDER SABOTAGE	MG-Sabotage fehlerhaft und Quittierung.
150	NON BURGLARY	
300	SYSTEM TROUBLE	Störung Netzteil und Quittierung.
301	AC LOSS	Störung Hauptnetzteil und Quittierung.
302	AKKU SCHWACH	
305	RESET	System zurücksetzen.
311	STÖRUNG AKKU	Störung Netzteilakku und Quittierung.
312	NETZTEIL ÜBERSTROM	Störung Netzteilsicherung intern, extern und Behelf und Quittierung.
320	SUMMER	Sabotage Sirene fehlerhaft und Quittierung.
330	PROBLEM SYSTEMPERIPHERIE	Störung Netzteil und Quittierung.
333	STÖRUNG ERW	Störung Kommunikation X-Bus-Kabel und Knoten und Quittierung.
338	AKKU ERW	Störung X-Bus-Knoten Akku und Quittierung.
341	SABOTAGE ERW	Sabotage X-Bus und Funkantenne Alarm und Quittierung.
342	AC ERW	Störung X-Bus-Knoten Strom und Quittierung.
344	FREMDFNK	Störung Fremdfunk und Quittierung.
351	TELCO 1	Störung Primärmodem und Rücksetzung.
352	TELCO 2	Störung Sekundärmodem und Rücksetzung.
376	HOLDUP TROUBLE	
380	PROBLEM MELDER	
401	ÖFFNENSCHLIESSEN	Unscharf, Nach-Alarm und extern scharf.
406	ALARMABBRUCH	Alarm aufheben.
451	FRÜH ÖFFNENSCHLIESSEN	
452	SPÄT ÖFFNENSCHLIESSEN	
453	FAIL TO OPEN	Zu spät unscharf.
454	FAIL TO CLOSE	Zu spät scharf.
456	EVENT PARTSET	Internscharf A/B.
461	CODETAMPER	Benutzercode Sabotage.
466	SERVICE	Technikermodus aktiviert und deaktiviert.
570	BYPASS	MG gesperrt und entsperrt; MG isoliert und unisoliert.
601	MANUAL TEST	Manueller Modemtest.
602	AUTO TEST	Automatischer Modemtest.
607	GEHTEST	
613	MG GEHTEST	
614	FEUER MG GEHTEST	
615	ÜBERFALL MG GEHTEST	
625	TIME RESET	Zeit setzen.

23.9 Übersicht über die Bedienteiltypen

Bedienteiltyp	Modellnr.	Grundlegende Funktionen	Proximity-Erkennung	Audio
Standard-Bedienteil	SPCK420	✓	-	-
Bedienteil mit TP	SPCK421	✓	✓	-
Komfort-Bedienteil	SPCK620	✓		-
Komfort-Bedienteil mit Audio/CR	SPCK623	✓	✓	✓



Bedienteiletikett SPCK420/421

1	Etikett im Inneren des Bedienteils
2	Abziehetikett für Errichterangaben. Nach Abschluss der Installation alle relevanten Angaben eintragen.

23.10 Benutzer-PIN-Kombinationen

Das System unterstützt PINs mit 4, 5, 6, 7 und 8 Stellen für jeden Benutzer (Benutzer- und Techniker-PINs). Die maximale Anzahl an logischen Kombinationen/Variationen für jede PIN-Ziffer kann der nachfolgenden Tabelle entnommen werden.

Anzahl der Stellen	Anzahl der Variationen	Letzte gültige Benutzer-PINs
4	10.000	9999
5	100.000	99999
6	1.000.000	999999
7	10.000.000	9999999
8	100.000.000	99999999

Die maximale Anzahl der logischen Kombinationen/Variationen ergibt sich aus:

10 Anzahl der Stellen = Anzahl der Variationen (schließlich Benutzer- und Techniker-PIN)

Hinweis: Zur Einhaltung der INCERT-Genehmigungen muss die Benutzer-PIN mehr als 4 Zeichen enthalten.

Die standardmäßige Techniker-PIN lautet 1111. Weitere Informationen finden Sie unter Techniker-PINs [→ 107].

23.11 Bedrohungs-PINs

Die letzte Benutzer-PIN in einer PIN-Zuweisung mit einer bestimmten Anzahl an PIN-Stellen kann nicht als Bedrohungs-PIN konfiguriert werden. Für die Konfiguration einer Bedrohungs-PIN mit ‚PIN +1' oder ‚PIN +2' müssen nach einer bestimmten PIN entweder 1 oder 2 zusätzliche PINs verfügbar sein. Beispiel: Bei einer Zuweisung von 4-stelligen PINs stehen insgesamt 10.000 (0–9999) PINs zur Verfügung. Wenn in diesem Fall die Bedrohungs-PIN-Konfiguration ‚PIN +1' verwendet wird, lautet die letztmögliche Bedrohungs-PIN 9998. Wenn ‚PIN +2' verwendet wird, lautet die letztmögliche Bedrohungs-PIN 9997.

Wenn die Funktion Bedrohungs-PIN aktiviert ist, sind aufeinanderfolgende Benutzer-PINs (z. B. 2906, 2907) nicht zulässig, da das Eingeben dieser PIN über das Bedienteil einen Bedrohungsalarm auslösen würde.

Wenn das System in den System Optionen [→ 239] für PIN +2 oder PIN +2 konfiguriert ist und bestimmte Benutzer für eine Bedrohungs-PIN aktiviert sind, (siehe Benutzer [→ 195]), **darf** es nur geändert werden, wenn alle Benutzer gelöscht und Benutzer-PINs neu zugewiesen sind.

23.12 Automatische Sperren

Im System können in den nachstehend beschriebenen Fällen automatische Sperren konfiguriert werden.

23.12.1 Meldegruppen

Wenn „UK" und „Kommerziell" ausgewählt sind (siehe Normen [→ 252]), funktioniert das System DD243-konform. In diesem Fall sperrt das System Meldergruppen unter folgenden Bedingungen:

- Eine verzögerte Meldergruppe löst kein Alarmsignal an die Zentrale aus und kann nicht Teil eines bestätigen Alarms sein. Sie wird gesperrt, wie in DD243 gefordert.
- Wenn eine einzige Meldergruppe ausgelöst wird und innerhalb des Bestätigungszeitraums (Standardeinstellung 30 Minuten) keine weitere Meldergruppe ausgelöst wird, aber die erste MG immer noch ausgelöst ist, dann wird die erste Meldergruppe automatisch gesperrt, und von dieser Meldergruppe werden während der Scharfschaltung keine weiteren Alarme ausgelöst.

23.12.2 Zugangs-PINs

Für Systeme der Sicherheitsstufe 2: Nach 10 erfolglosen Versuchen mit der falschen PIN wird das Bedienteil oder der Browser 90 Sek. lang deaktiviert, nach weiteren 10 Versuchen mit der falschen PIN wird das Bedienteil oder der Browser noch einmal 90 Sek. lang deaktiviert. Sobald eine richtige PIN eingegeben wird, wird der Zähler auf Null zurückgesetzt; dann können weitere 10 Versuche unternommen werden, bevor das Bedienteil deaktiviert wird.

Für Systeme der Sicherheitsstufe 3: Nach 10 erfolglosen Versuchen mit der falschen PIN wird das Bedienteil oder der Browser 90 Sek. lang deaktiviert, nach

weiteren 10 Versuchen mit der falschen PIN wird das Bedienteil oder der Browser noch einmal 90 Sek. lang deaktiviert. Sobald eine richtige PIN eingegeben wird, wird der Zähler auf Null zurückgesetzt; dann können weitere 10 Versuche unternommen werden, bevor das Bedienteil deaktiviert wird.

23.12.3 Technikerzugang

Ein Techniker kann nur auf das System zugreifen, wenn dies von einem Benutzer des Typs „Manager“ (siehe Attribut „Techniker“ unter Benutzerrechte) zugelassen wurde. Der Zugriff ist nur für einen bestimmten Zeitraum zulässig (siehe „Technikerzugriff“ unter Timer [→ 248]).

23.12.4 Benutzerabmeldung vom Bedienteil

Wenn für einen bestimmten Zeitraum keine Tasten auf dem Bedienteil gedrückt werden (siehe „Bedienteil Timeout“ unter Timer [→ 119]), wird der Benutzer automatisch abgemeldet.

23.13 Verdrahtung des Netzkabels an die Zentrale

Voraussetzungen:

Die Elektroinstallation des Gebäudes muss mit einer leicht zugänglichen, homologierten Trennvorrichtung ausgestattet sein. Dieser Trennschalter muss beide Phasen gleichzeitig trennen. Zulässig sind Schalter, Sicherungsautomaten o. Ä.

- Das Trennungsbauteil muss einen Mindestabstand von 3 mm zwischen den Kontakten aufweisen.
- Die Netzkabel müssen einen Leiterquerschnitt von mindestens 1,5 mm² aufweisen.
- Es dürfen nur Sicherungsautomaten mit einem Höchstnennstrom von 16 A eingesetzt werden.

Das Netzkabel wird mit einem Kabelbinder so an der V-förmigen Einbuchtung der Grundplatte befestigt, dass sich diese zwischen Kabel und Binder befindet. Es ist darauf zu achten, dass der Kabelbinder an der Zusatzisolierung des Netzkabels, d. h. an der äußeren PVC-Kabelhülle, befestigt wird. Der Kabelbinder muss so fest angezogen werden, dass sich das Kabel, auch wenn man daran zieht, innerhalb des Kabelbinders nicht bewegt.

Der Schutzleiter ist so am Klemmenblock anzubringen, dass der Schutzleiter das letzte abgeschlossene Kabel am Block ist, auf das Zugkräfte wirken, falls das Netzkabel aus seiner Befestigung rutschen sollte.

Das Netzkabel muss homologiert sein und die Kennzeichnung HO5 VV-F oder HO5 VVH2-F2 aufweisen.

Der Plastik-Kabelbinder muss bezüglich der Entflammbarkeit die Anforderungen der Klasse V-1 erfüllen.

23.14 Wartungs-Controller

Das System sollte in Übereinstimmung mit dem geltenden Wartungsplan gewartet werden. Die einzigen austauschbaren Teile im Controller sind die Hauptsicherungen, die Standby-Batterie und die Zeit/Datum-Batterie (auf Platine).

Es wird empfohlen, dass während einer Wartung Folgendes überprüft wird:

- Das Logbuch, um zu prüfen, dass seit der letzten Wartung keine Tests der Standby-Batterie fehlgeschlagen sind. Falls die Tests fehlgeschlagen sind, sollte die Standby-Batterie ausgetauscht werden.
- Die Standby-Batterie sollte gemäß dem Wartungsplan ausgetauscht werden, um sicherzustellen, dass sie ausreichend Kapazität hat, um das System

während der festgelegten Dauer mit Strom zu versorgen. Die Batterie muss auf Deformierungen des Gehäuses und Anzeichen eines Auslaufens geprüft werden. Falls einer dieser Schäden vorliegt, muss die Batterie sofort ausgetauscht werden.

	*HINWEIS*
	Die neue Batterie muss die gleiche oder eine höhere Kapazität aufweisen (bis zur maximal möglichen Kapazität für das System).

- Wenn die Hauptsicherung durchbrennt, muss das System auf die Ursache geprüft werden. Die Sicherung muss durch eine baugleiche Sicherung ersetzt werden. Die Stromstärke kann dem Systemetikett auf der Rückseite des Schaltschrankes entnommen werden.
- Die Zeit/Datum-Batterie auf der Platine wird nur verwendet, wenn das System ohne Strom ist. Bei dieser Verwendung hält die Batterie etwa 5 Jahre. Die Batterie sollte einmal jährlich auf Schäden geprüft werden. Außerdem sollte das System einmal jährlich abgeschaltet werden, um sicherzustellen, dass das Datum und die Uhrzeit erhalten bleiben. Wenn das System das Datum und die Uhrzeit nicht beibehält, muss die Batterie durch eine neue Lithiumzelle vom Typ CR1216 ersetzt werden.
- Alle elektrischen Anschlüsse müssen überprüft werden, um sicherzustellen, dass die Isolierung intakt ist, kein Kurzschlussrisiko besteht und sie nicht leicht abgetrennt werden können.
- Es wird empfohlen, die Veröffentlichungshinweise für Firmware-Updates auf zusätzliche Updates zu überprüfen, die die Sicherheit des Systems verbessern könnten.
- Überprüfen, dass alle Befestigungen intakt sind. Beschädigte Befestigungen müssen durch baugleiche Teile ersetzt werden.

23.15 Wartung der Smart PSU

Das System sollte in Übereinstimmung mit dem geltenden Wartungsplan gewartet werden. Die einzigen austauschbaren Teile der Smart PSU sind die Hauptsicherung und die Standby-Batterie.

Es wird empfohlen, dass während einer Wartung Folgendes überprüft wird:

- Das Controller-Logbuch, um zu prüfen, dass seit der letzten Wartung keine Tests der Standby-Batterie fehlgeschlagen sind. Falls die Tests fehlgeschlagen sind, sollte die Standby-Batterie ausgetauscht werden.
- Die Standby-Batterie sollte gemäß dem Wartungsplan ausgetauscht werden, um sicherzustellen, dass sie ausreichend Kapazität hat, um das System während der festgelegten Dauer mit Strom zu versorgen. Die Batterie muss auf Deformierungen des Gehäuses und Anzeichen eines Auslaufens geprüft werden. Falls einer dieser Schäden vorliegt, muss die Batterie sofort ausgetauscht werden.

	*HINWEIS*
	Die neue Batterie muss die gleiche oder eine höhere Kapazität aufweisen (bis zur maximal möglichen Kapazität für das System).

- Den Zustand LEDs auf der Steuerplatine des Netzteils prüfen. Siehe Smart PSU-Dokument für Einzelheiten zu den LEDs.
- Wenn die Hauptsicherung durchbrennt, muss das System auf die Ursache geprüft werden. Die Sicherung muss durch eine baugleiche Sicherung ersetzt

werden. Die Stromstärke kann dem Systemetikett auf der Rückseite des Schaltschrankes entnommen werden.

- Alle elektrischen Anschlüsse müssen überprüft werden, um sicherzustellen, dass die Isolierung intakt ist, kein Kurzschlussrisiko besteht und sie nicht leicht abgetrennt werden können.
- Es wird empfohlen, die Veröffentlichungshinweise für Firmware-Updates auf zusätzliche Updates zu überprüfen, die die Sicherheit des Systems verbessern könnten.
- Überprüfen, dass alle Befestigungen intakt sind. Beschädigte Befestigungen müssen durch baugleiche Teile ersetzt werden.

23.16 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 SCHARFSCHALTUNGSVERZÖGERUNG	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 FEUERALARM 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.
ÜBERFALLALARM	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.
BEDROHUNGSALARM	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: ● Wenn die Technik-MG öffnet, wird der Technik-MG-Ausgang ausgelöst. ● Wenn die Technik-MG schließt, wird der Technik-MG-Ausgang deaktiviert. Wurden mehrere Technik-Meldergruppen zugewiesen, bleibt der Technik-MG-Ausgang aktiv, bis alle Technik-MGs geschlossen sind.
MEDIZINISCHER NOTFALL	Bedrohung	Dieser Meldergruppentyp wird in Verbindung mit medizinischen Notfallschaltern verwendet, die verkabelt sind oder mit Funkübertragung arbeiten. Unabhängig vom Modus tritt bei einer Aktivierung Folgendes ein: ● Der Ausgang für das digitale Wählgerät für Medizinischen Notfall wird ausgelöst (es sei denn, das Attribut Lokal ist aktiviert) ● Der Summer in der Zentrale ertönt (es sei denn, das Attribut Lokal ist aktiviert) ● Die Meldung „Medizinischer Notfall“ wird angezeigt
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. ● Ist die Meldergruppe mit dem Typ Scharf/Unscharf Eingang in einem System ohne Bereiche zugewiesen, schaltet die Betätigung des Verriegelungsmechanismus das System SCHARF/UNSCHARF. ● Ist die Meldergruppe mit dem Typ Scharf/Unscharf Eingang einem Bereich zugewiesen, schaltet die Betätigung des Verriegelungsmechanismus den Bereich SCHARF/UNSCHARF. ● 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. ● 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) ● Ist das Attribut „Extern scharf erlaubt“ aktiviert, wird bei Aktivierung der Meldergruppe das System nur extern scharf geschaltet.

		● Ist das Attribut „Unscharf erlaubt“ aktiviert, wird bei Aktivierung der Meldergruppe nur das System unscharf geschaltet. Bei Scharf/Unscharf Eingang wird das System/der Bereich erzwungen scharf geschaltet. Alle offenen Meldergruppen bzw. Störungsbedingungen werden automatisch gesperrt. **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.**
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. Wenn dieser MG-Typ öffnet, werden alle Meldergruppen gesperrt, bei denen das Shunt-Attribut gesetzt ist. Dies geschieht sowohl bei SCHARF 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. Vibrationssensoren, 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 [→ 257] für Einzelheiten zur Konfiguration „Alles in Ordnung“.) „Alles in Ordnung“ verwendet zwei Ausgänge (Eingangsstatus [grüne LED] und Warnungsstatus [rote LED]), um den Eingangsstatus 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. **Hinweis**: 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 geschaltenen Zustand. Dieses Signal wird während des Scharfschaltungsvorgangs geprüft. Wenn die Information zur Sperrung nicht empfangen wird, schlägt die Scharfschaltung fehl.
GLASBRUCH	Eindringling	Die Meldergruppe ist mit einer Glasbruch-Schnittstelle vom Typ RI S 10 D-RS-LED mit GB2001 Glassbruchmeldern verbunden. ● Dieser Meldergruppentyp steht auf Zentralen und Erweiterungen zur Verfügung. Er ist nicht als Funk- oder Türmeldergruppentyp verfügbar, wenn DC2 als Tür konfiguriert ist. ● Der Meldergruppentyp meldet auf die selbe Art und Weise wie eine Alarmmeldergruppe über SIA und Contact-ID. ● Die Rechte zum Quittieren/Sperren/Abschalten von Glasbruch-Meldungen sind gleich einer Alarmmeldergruppe. ● 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. ● Rücksetz-Bedingung - Während der ersten 3 Sekunden nach dem Rücksetzen eines Geräts werden Signale von der Glasbruch-Schnittstelle ignoriert. ● 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.

23.17 MG-Attribute

In SPC wird mit den MG-Attributen festgelegt, wie die programmierten Meldergruppentypen funktionieren.

MG-Attribut	Beschreibung
Folgt Verzögerung	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. Das Attribut „Folgt Verzögerung“ ist nur für Alarm-MG-Typen gültig. Alle angeschlossenen Geräte (Sirenen - Innen und Außen, Summer, Blitzleuchte) sind aktiv. **HINWEIS**: 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.
"Nicht bei Intern A"	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. 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).
"Nicht bei Intern B"	Wenn für eine Meldergruppe das Attribut „Nicht bei Intern B“ aktiviert ist, wird beim Öffnen dieser Meldergruppe kein Alarm generiert, solange sich die Zentrale im Intern-scharf-B-Modus befindet. Das Attribut „Nicht bei Intern B“ ist nur für Alarm-Meldergruppen und verzögerte Meldergruppen gültig. 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).
24 Stunden	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. **HINWEIS**: Das Attribut „24 Stunden“ hat Vorrang vor allen anderen Attributeinstellungen für eine bestimmte Einbruchs-Meldergruppe.
Lokal	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.
Unscharf Lokal	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.
Doppelauslösung	Dieses Attribut wird für problematische Melder verwendet. (Bestimmte Melder können willkürlich Aktivierungssignale generieren, die dann unbeabsichtigt Systemalarme auslösen). Ein Alarm wird ausgelöst, wenn eine Meldergruppe mit Doppelauslösung während des Doppelauslösungszeitraums zweimal aktiviert wird. Die Doppelauslösungszeit wird in Sekunden konfiguriert (siehe Seite [➙ 248]). Zwei Öffnungen innerhalb dieses Zeitraums lösen einen Alarm aus. Bei Scharfschaltung des Systems werden alle offenen Doppelauslösungs-Meldergruppen protokolliert.
Türglocke	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). Das Attribut „Türglocke“ kann bei Einbruchsmeldergruppen, verzögerten Meldergruppen und Technik-Meldergruppen aktiviert werden.
Sperren	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.
Normal offen	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).
Still	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.

Log (Protokoll)	Wird dieses Attribut aktiviert, werden alle Zustandsänderungen der Meldergruppe protokolliert.
Info vor Scharfsch.	Wenn gesetzt, wird für eine ausgelöste verzögerte Meldergruppe vor der Scharfschaltung eine Information angezeigt. Die Scharfschaltung wird dadurch nicht verhindert (nur im Komfort Bedienteil).
Überwacht	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.
Endwiderstand	Das Attribut „Endwiderstand“ (EOL) stellt im System eine Reihe von Verdrahtungskonfigurationen für Eingangs-Meldegruppen zur Verfügung.
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 Scharfschaltungsverzögerung 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 unbekannten 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. **HINWEIS**: 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 [→ 248].) 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 [→ 248].
Körperschalltest/Automatischer Meldertest	Ein Körperschall-Meldergruppentyp kann manuell oder automatisch getestet werden. Dieses Attribut ermöglicht die Aktivierung des automatischen Tests. Siehe Abschnitt Timer [→ 248] 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-Eingangsgerät das System scharf schalten und somit alle offenen Meldergruppen sperren.

23.18 Anwendbare Attribute nach Meldergruppentypen

Die nachstehende Tabelle fasst zusammen, welche Attribute dem jeweiligen Meldergruppentyp zugewiesen werden können:

			⊛		⊛	⊛		⊛				⊛		⊛	⊛	⊛	⊛		⊛						
Zone Type / **Attribute**	Alarm	Entry/Exit	Exit Term	Fire	Fire Exit	Line	Panic	Holdup	Tamper	Tech	Medical	Keyarm	Unused	Shunt	X-Shunt	Detector Fault	Lock Supervision	Seismic **	All Okay	Hold-up Fault	Warning Fault	Setting Authorisation	Lock Element	Glass Break
Access	v																							v
Exclude A	v	v																					v	v
Exclude B	v	v																					v	v
24 Hour	v																	v						v
Local	v	v		v	v						v					v				v	v		v	v
Unset Local	v			v														v						v
Double Knock	v																							v
Chime	v	v								v												v		v
Inhibit	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v		v	v
Normal Open	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v		v	v	v	v	v	v
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
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
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*

23.19 ATS-Stufen und Dämpfungsspezifikationen

ATS (Alarm Transmission System)-Stufen

In der folgenden Tabelle werden die ATS-Stufen beschrieben, die für die Zentrale bei folgenden Kommunikationsmethoden erforderlich sind:

- GSM an Empfänger (ARC)
- PSTN an Empfänger (ARC)
- Ethernet an SPC-Kommunikationsempfänger-Software
- GPRS an SPC-Kommunikationsempfänger-Software

	GSM ARC	PSTN ARC	Ethernet	GPRS
ATS-Stufe	ATS 2	ATS 2	ATS 6	ATS 5

Dämpfung von PSTN-Verbindungen

Bei einem PSTN-Wählgerät wird für den Anschluss des Modems an die Telefonleitung ein internes CW1308-Telefonkabel oder ähnliches empfohlen. Die Kabellänge sollte zwischen 0,5 und 100 m betragen.

Dämpfung von Ethernet-Verbindungen

Für Ethernet-Verbindungen wird die Verwendung eines Cat-5-Kabels mit einer Länge von 0,5 bis 100 m empfohlen.

Dämpfung von GSM-Verbindungen

Die Feldstärke eines GSM-Signals muss mindestens -95 dB betragen. Liegt die Stärke unter diesem Wert, gibt das Modem einen Empfangsfehler (schwaches Signal) an die Zentrale weiter. Dieser Fehler wird wie andere Systemfehler behandelt.

Überwachung und Watchdog-Funktion für PSTN (SPCN110) und GSM (SPCN310)

Ein Schnittstellenfehler zwischen PSTN-Modem und der Zentrale wird nach 30 Sekunden erkannt. Anschließend tritt ein ATS-Fehler ein.

Ein Schnittstellenfehler zwischen GSM-Modem und der Zentrale wird nach 30 Sekunden erkannt. Anschließend tritt ein ATS-Fehler ein.

23.20 Unterstützte Ausweisleser und Ausweisformate

Auf dem SPC-System werden die folgenden Ausweisleser und -formate unterstützt:

Leser	Ausweisformat
HD500-EM PR500-EM SP500-EM PM500-EM	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
AR6181-RX AR6182-RX	IB41-EM IB42-EM

Leser	Ausweisformat
	IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
HD500-Cotag PR500-Cotag SP500-Cotag PM500-Cotag HF500-Cotag	IB928 IB911 IB968 IB961 IB958M
PP500-Cotag	IB928 IB911 IB968 IB961 IB958M
PP500-EM	IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
AR6181-MX AR6182-MX	ABP5100-BL Mifare Classic 1K ABR5100-PR Mifare Classic 4K
iClass R10 iClass R15 iClass R30 iClass R40 iClassRK40	ABP5100-BL 32-Bit-Format, nur MiFare
MultiClass RP40 MultiClass RP15 MultiClass RPK40	ABP5100-BL 32-Bit-Format, nur MiFare IB41-EM IB42-EM IB44-EM IB45-EM ABR5100-BL ABR5100-TG ABR5100-PR
HID Prox Pro	26 Bit Wiegand EPX 36 Bit Wiegand

Anlagennummern und Einschränkungen

Leserformat	Anlagennummer verfügbar	Einschränkungen
EM4102	Nein	Max. Ausweisnummer 9999999999
COTAG	Nein	Max. Kartennummer 9999999999
Wiegand 26 Bit	Ja	Max. Anlagennummer 255 Max. Ausweisnummer 65535
Wiegand 36 Bit	Ja	Max. Anlagennummer 32767

Leserformat	Anlagennummer verfügbar	Einschränkungen
		Max. Ausweisnummer 524287
"HID Corporate 1000"	Ja	Max. Anlagennummer 4095 Max. Ausweisnummer 1048575
HID 37	Nein	Max. Ausweisnummer 34359738370
HID 37f	Ja	Max. Anlagennummer 65535 Max. Ausweisnummer 5242875
HID 37BCD	Nein	Max. Ausweisnummer 99999999
HID ICLASS Mifare	Nein	Max. Ausweisnummer 4294967295
HID Iclass DESFire	Nein	Verschlüsselte Ausweisnummer Max. Ausweisnummer 72 x 10^{16}. Dieser Ausweis muss in der Zentrale eingelernt werden.
AR618 Wie BCD 52 BIT	Nein	Max. Ausweisnummer 4294967295
AR618 Clock/ Data 80	Nein	Max. Ausweisnummer 9999999999999

23.21 SPC-Unterstützung für E-Bus-Geräte

Der SPC-E-Bus-Gateway (SPCG310) ist eine X-Bus-Erweiterung, die die Kommunikation zwischen einem SPC-Controller und Sintony E-Bus-Geräten ermöglicht. Die Sintony E-BUS-Adressierung erlaubt die Duplizierung der Adressen für E-Bus-Geräte über verschiedene E-BUS-Abschnitte hinweg. X-Bus-Geräte erfordern eindeutige Adressen. Für die Lösung dieses Konflikts könnte eine Neuadressierung der E-BUS-Peripherie erforderlich sein. Weitere Informationen finden Sie im Abschnitt ADRESSIERMODUS [→ 135].

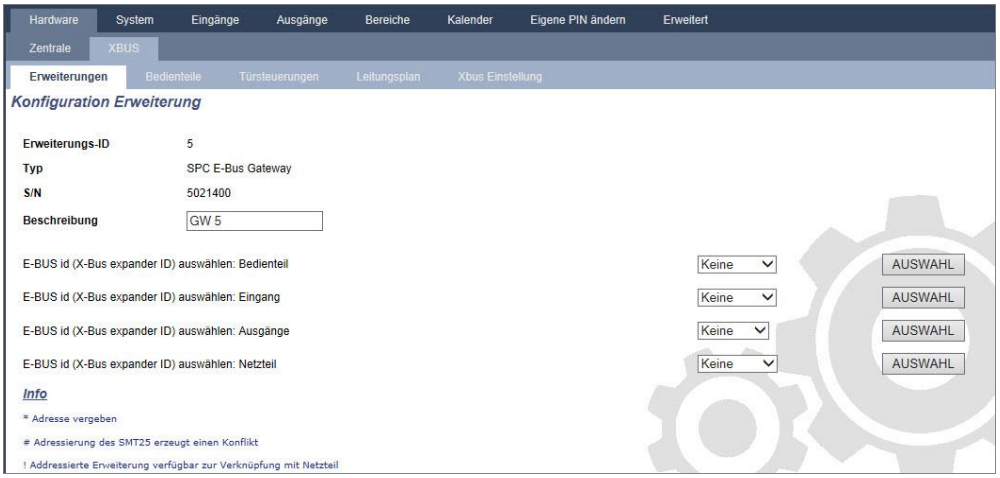
!	*HINWEIS*
	Vanderbilt empfiehlt, vor der Konfiguration der E-Bus-Geräte das Dokument **Sintony-Systemmigration** zu lesen.

23.21.1 Konfigurieren und Adressieren von E-Bus-Geräten

Sie können die folgenden E-Bus-Geräte konfigurieren und adressieren, um mit dem SPC-Controller zu kommunizieren:

- Sintony-Bedienteile
- Sintony-Eingangstransponder
- Sintony-Ausgangstransponder
- Sintony-Netzteile: SAP 8, SAP 14, SAP 20 und SAP 25

1. Öffnen Sie im Browser **Einstellungen – X-BUS – Erweiterungen**.
   ⇨ Die Liste **Konfigurierte Erweiterungen** wird angezeigt.
2. Wählen Sie ein **SPC-E-Bus-Gateway**.
3. Geben Sie auf dem Bildschirm **Konfiguration Erweiterung** eine **Beschreibung** für das **SPC-E-Bus-Gateway** ein. Weitere Informationen zur Konfiguration von Erweiterungen finden Sie unter Erweiterungen [→ 219].



4. Wählen Sie zur Adressierung eines E-Bus-Geräts eine ID aus dem entsprechenden Dropdown-Menü, die in der unteren Tabelle beschrieben ist. In Gebrauch befindliche IDs sind mit einem Sternchen (*) gekennzeichnet. Diese IDs können Sie nicht wählen.
5. Klicken Sie auf die Schaltfläche **Auswahl**.
   ⇨ `Adressierung erfolgt... Neukonfiguration des X-Bus wird erforderlich sein` wird im oberen Bereich des Bildschirms angezeigt.
   ⇨ Das SPC-E-Bus-Gateway piept wiederholt.
6. Halten Sie die Adressierungstaste je nach E-Bus-Gerät und wie in Spalte **Adresse** der unteren Tabelle beschrieben gedrückt.
   ⇨ Das SPC-E-Bus-Gateway piept anhaltend, um anzuzeigen, dass die ID nun dem E-Bus-Gerät zugewiesen ist.
7. Öffnen Sie **Einstellungen – X-BUS – Erweiterungen**.
8. Klicken Sie auf die Schaltfläche **Neu Konfigurieren**.
   ⇨ `Neukonfiguration abgeschlossen` wird im oberen Bereich des Bildschirms angezeigt. E-Bus-Eingänge und -Ausgänge werden in der Liste **Konfigurierte Erweiterungen angezeigt.** Wenn ein Eingangstransponder ein zugewiesenes Netzteil besitzt, wird in der Spalte **Netzteil** der Netzteiltyp angezeigt. Bedienteile werden in der Liste **Konfigurierte Bedienteile** angezeigt.
9. Weitere Informationen zum Abschluss der Schritte zur manuellen Adressierung, um die Netzteilgeräte SAP 8, SAP 14 und SAP 20 der Liste **Konfigurierte Erweiterungen** hinzuzufügen, finden Sie unter Adressieren von Transpondern für SAP 8, SAP 14 und SAP 20 [→ 387].
10. Bei Adressierungskonflikten des X-BUS wird die Warnung `Ungültige oder doppelte Erweiterungs-ID` angezeigt. Wiederholen Sie die obigen Adressierungsschritte, bis kein Adressierungskonflikt mehr vorliegt.

E-Bus-Gerät: Dropdown-Menü	Beschreibung	ID-Format	Adressierung
Bedienteil	IDs, die Sintony-Bedienteilen zugeordnet werden	E-BUS-ID (X-BUS-ID)	Halten Sie die Tasten 1 und 3 gleichzeitig gedrückt, bis das SPC-E-Bus-Gateway anhaltend piept.
Eingang	IDs, die Sintony-Eingangstranspondern	E-BUS-ID (X-BUS-ID)	Drücken Sie die Adressierungstaste

	zugeordnet werden		5 Sekunden lang; beim Loslassen ertönt ein anhaltender Piepton.
Ausgang	IDs, die Sintony-Ausgangstranspondern zugeordnet werden	E-BUS-ID (X-BUS-ID)	Drücken Sie die Adressierungstaste 5 Sekunden lang; beim Loslassen ertönt im SPC-E-Bus-Gateway ein anhaltender Piepton.
NETZTEIL	IDs, die den Sintony-Netzteilen SAP 8, SAP 14, SAP 20 und SAP 25 zugeordnet werden	E-BUS-ID (X-BUS-ID des zugehörigen Transponders)	Drücken Sie die Adressierungstaste, bis im SPC-E-Bus-Gateway ein anhaltender Piepton ertönt.

Siehe auch

ADRESSIERMODUS [→ 135]

23.21.1.1 Adressieren von Transpondern für SAP 8, SAP 14 und SAP 20

Nach der Zuweisung einer Netzteil-ID zum SAP 8, SAP 14 oder SAP 20 (siehe Konfigurieren und Adressieren von E-Bus-Geräten [→ 385]) müssen Sie dem Netzteil einen Eingangstransponder zuweisen. Dies simuliert die Kommunikation mit dem SPC-Controller über eine Erweiterung.

1. Wählen Sie in der Liste **Konfigurierte Erweiterungen** den Eintrag **SPC-E-Bus-Gateway**.
   ⇨ Der Bildschirm **Konfiguration Erweiterung** wird angezeigt.
2. In der Dropdown-Liste wird die neu zugewiesene Netzteil-ID angezeigt.
   ⇨ Vor der Netzteil-ID, die Sie dem Gerät zugewiesen haben steht ein Ausrufezeichen (!). Dies zeigt an, dass ein Eingangstransponder verfügbar ist, der dem Netzteil zugewiesen werden kann.
3. Notieren Sie sich die Nummer in Klammern neben der Netzteil-ID. Diese Nummer ist die ID, die Sie dem Eingangstransponder zuweisen müssen. Beispiel: Wenn die Netzteil-ID **ID 14 (27)** lautet, müssen Sie manuell einen Transponder mit der **ID 27** aus der Dropdown-Liste **Eingang** wählen.
4. Wählen Sie aus der Dropdown-Liste **Eingang** die Transponder-ID, die in Klammern neben der Netzteil-ID angegeben war.
5. Klicken Sie auf die Schaltfläche **Auswahl**.
6. Öffnen Sie **Einstellungen – X-BUS – Erweiterungen**.
7. Klicken Sie auf **Neu Konfigurieren**.

⇨ Das Netzteil wird in der Liste **Konfigurierte Erweiterungen** angezeigt.

23.21.1.2 Adressieren von Transpondern für das Netzteil SAP 25

Das Netzteil SAP 25 von Sintony besitzt zwei interne Transponder. Jeder Transponder erfordert eine ID. Diese beiden IDs werden automatisch zugewiesen, wenn Sie die unter Konfigurieren und Adressieren von E-Bus-Geräten [→ 385] beschriebenen Adressierungsschritte abschließen. Die Formel `2n - 1` gilt, wobei

n der Wert der Netzteil-ID ist. Beispiel: Wenn Sie einem SAP 25 die ID 10 zuweisen, erhalten die Transponder jeweils die X-BUS-ID 19 bzw. 20.

!	*HINWEIS*
	In der Dropdown-Liste der Netzteile steht vor der SAP 25-ID eine Raute (#), um anzuzeigen, dass die automatische Adressierung von Transpondern mit vorhandenen Eingangstranspondern in Konflikt stehen wird. Zur Lösung dieses Konflikts müssen Sie eines der betroffenen Geräte neu adressieren.

23.22 FlexC-Glossar

Abkürzung	EN50136-1 Beschreibung	FlexC Beispiel
AE	**Empfangseinrichtung** Die im Empfänger befindliche Ausrüstung, die den Alarmzustand sichert und anzeigt, oder der geänderte Alarmzustand der AS als Antwort auf den Empfang eingehende Alarme vor dem Senden einer Quittierung. Die Empfangseinrichtung (AE) ist nicht Bestandteil des Übertragungssystems (ATS).	SPC Com XT-Client
ARC	**Alarmempfangscenter** Durchgehend besetztes Zentrum, an das Informationen zum Zustand eines oder mehrerer AS gemeldet werden.	SPC Com XT wäre in einem Empfänger installiert.
AS	**Alarmsystem** 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	**Alarmübertragungsequipment** Ein Sammelbegriff zur Beschreibung von SPT, MCT (Überwachungszentrumsempfänger) und des Empfängers.	-
ÜW	**Alarmübertragungsweg** 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. Beispielweise wäre ein System mit Ethernet als primärer Pfad und GPRS als Backup-Pfad zwei separate ÜWs eines ATS.
ATS	**Alarmübertragungssystem**	Ein System, das einen oder mehrere Pfad zwischen der

	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.	SPC-Zentrale und dem SPC Com XT kombiniert.
RCT	**Empfänger/Empfangszentrale** Die Übertragungseinrichtung am ARC einschließlich der Schnittstelle zu einem oder mehreren AEs und der Schnittstelle zu einem oder mehreren Übertragungsnetzwerken als Teil 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 eins AE-Ausfalls zu erhöhen.	SPC Com XT-Server
SPT	**Überwachte Übertragungseinrichtung der Zentrale** 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	**Analoges Sicherheitsprotokoll** Das analoge Sicherheitsprotokoll wird traditionell zur Übertragung von Alarmen über Telefonnetzwerke verwendet, z. B. SIA, Kontakt-ID.

23.23 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.

Steuerungsfilter	Befehle
Systemsteuerungen	Anfordern der Zentralen Zusammenfassung
	Einstellung der Systemzeit und Datum
	Technikerzugang freigegeben
	Herstellerzugang freigegeben

Einbruchssteuerungen	Anfordern des Bereichsstatus
	Anfordern des Zustandes S/ U des Bereiches
	Ändern des Zustandes S/ U des Bereiches
	Status der Zentralenalarme abfragen
	Auszuführende Aktionen auf Alarmmeldungen
	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 Benutzerprofiles
	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 Übertragungssystemes
	Löschen eines FlexC ÜW
	Löschen eines FlexC Ereignisprofiles
	Löschen eines FlexC Steuerungsprofiles
	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

23.24 Zeiten für Übertragungssystemkategorien

Diese Tabelle enthält Beschreibungen der EN50136 ATS-Kategoriezeiten (SP1-SP6, DP1-DP4) 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-Kategorie	Vorgegebene Schnittstelle	Timeout erneute Übertr.	Primär Polling Timeout	Backup ÜW Polling Timout (Primärer OK)	Backup ÜW Polling Timout (Primärer down)	Timeout erneute Übertr.	Primär Polling Timeout	Backup ÜW Polling Timout (Primärer OK)	Backup ÜW Polling Timout (Primärer 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] Cat4 [Modem]	60 s	3 min	25 h	3 min	60 s	3 min	24 h 30 min	3 min
DP4	Cat5 [Ethernet] Cat5 [Modem]	30 s	90 s	5 h	90 s	30 s	90 s	4 h 10 min	90 s

23.25 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 Pollling-Intervalle **ATP down** (ÜW ausgefallen) gewechselt wird.

Übertragungsweg-Kategorien		Polling wenn der Übertragungsweg aktiv ist			Polling wenn der Übertragungsweg inaktiv ist			Polling wenn der Übertragungsweg unterbrochen ist	
ÜW Kategorie	**Ereignis Timeout**	**Polling-Intervall**	**Wiederholungs Intervall**	**Polling Timeout**	**Polling-Intervall**	**Wiederholungs Intervall**	**Polling Timeout**	**Polling Intervall**	**Zeitüberschreitung**
Cat6	30 s	8 s	30 s	20 s	8 s	30 s	20 s	30 s	30 s

[Ethernet]									
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
Modem ATP Kategorien									
Cat5 [Modem]	30 s	10 s	30 s	90 s	4 h	2 min	4 h 10 min	10 min	90 s
Cat4A [Modem]	60 s	60 s	60 s	3 min	4 h	2 min	4 h 10 min	30 min	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 Tage	90 s

Herausgegeben von
Vanderbilt

Clonshaugh Business and Technology Park
Clonshaugh
Dublin
D17 KV84
www.service.vanderbiltindustries.com

Dokument-ID A6V10271081
Ausgabe 01.05.2016