Control Panel

B5512/B4512/B3512 (B5512E/B4512E/B3512E)

de Program Entry Guide

Inhaltsverzeichnis

1	**Fernparametrier-Software**	**16**
2	**Zentralenspezifische Informationen**	**17**
2.1	Zentrale – Symbolleiste und Symbole	17
2.2	Verbindung mit der Zentrale herstellen	18
2.2.1	Verbinden über: Cloud	18
2.2.2	Verbinden über: Mobilfunk	19
2.2.3	Verbinden über: Rückruf per Mobilfunk	20
2.2.4	Verbinden über: USB	22
2.2.5	Verbinden über: Netzwerk	23
2.2.6	Verbinden über: IP-Direktverbindung	24
2.3	Verbindung mit der Zentrale trennen	26
2.3.1	Fehlerhafte Terminierung	26
2.4	Online-Vorgänge	26
2.4.1	Zentrale und RPS synchronisieren	26
2.4.2	Vergleichen	27
2.4.3	Suchen und ersetzen	28
2.4.4	Sicherheit	29
2.4.5	Send/Receive (Senden/Empfangen)	31
2.4.6	Hintergrundspeicher anzeigen	32
2.4.7	Get history (Hintergrundspeicher abrufen)	32
2.4.8	Diagnose	32
2.4.9	Datum/Uhrzeit der Zentrale aktualisieren	33
2.4.10	Kontohinweise	33
2.4.11	Firmware-Aktualisierung	34
2.5	Online-Diagnose – System	36
2.5.1	Panel diagnostics (Zentralendiagnose)	36
2.5.2	Integrierte IP-Adresse – Diagnose	36
2.5.3	Steckplatinendiagnose	37
2.6	Parametrierhinweise	39
3	**Konformitätseinstellungen**	**40**
3.1	SIA CP-01–Verifizierung	40
3.2	ULC-Konformität	40
3.2.1	Konformität mit CAN/ULC-S304	40
3.2.2	CAN/ULC-S559 – erforderliche Parametrierung	41
3.2.3	CAN/ULC-S559 – empfohlene Parametrierung	46
3.3	Überwachungskonfiguration	50
3.4	Europäische Anwendung	51
4	**Panel Wide Parameters (Zentralenübergreifende Parameter)**	**53**
4.1	Telefon und Telefonparameter	53
4.1.1	Telefon-Zieladresse 1 (bis 4)	53
4.1.2	Format für Telefon-Zieladresse 1 (bis 4)	53
4.1.3	DTMF Dialing (DTMF-Wählverfahren)	54
4.1.4	Phone Supervision Time (Telefonüberwachungsdauer)	54
4.1.5	Alarm on fail (Alarm bei Fehler)	54
4.1.6	Buzz on Fail (Störungston bei Fehler)	55
4.1.7	Expand Test Report (Prüfprotokoll erweitern)	55
4.1.8	PSTN-Kompatibilität	55
4.2	Integriertes Ethernet (IP)-Übertragungsgerät	56

4.2.1	IPv6-Modus	56
4.2.2	IPv6 DHCP	57
4.2.3	IPv4 DHCP/AutoIP Enable (IPv4 DHCP/AutoIP aktivieren)	57
4.2.4	IPv4-Adresse	57
4.2.5	IPv4-Subnetzmaske	57
4.2.6	IPv4-Standard-Gateway	58
4.2.7	IPv4 DNS Server IP Address (IPv4-DNS-Server-IP-Adresse)	58
4.2.8	IPv6-DNS-Server-IP-Adresse	58
4.2.9	UPnP (Universal Plug & Play) aktivieren	59
4.2.10	ARP-Cache-Timeout (Sekunden)	59
4.2.11	Hostname des Moduls	59
4.2.12	TCP/UDP Port Number (TCP/UDP-Portnummer)	60
4.2.13	TCP Keep Alive Time (TCP Keep-Alive-Zeit)	60
4.2.14	IPv4-Testadresse	60
4.2.15	IPv6-Testadresse	61
4.2.16	IP-Adresse des alternativen IPv4-DNS-Servers	61
4.2.17	IP-Adresse des alternativen IPv6-DNS-Servers	61
4.3	Mobilfunk-Steckplatine	62
4.3.1	Eingehende SMS	62
4.3.2	Session Keep Alive Period (minutes) (Dauer des Sitzungs-Keep-Alive in Minuten)	62
4.3.3	Inaktivitäts-Timeout (Minuten)	62
4.3.4	Reporting Delay for Low Signal Strength (sec.) (Reportverzögerung bei geringer Signalstärke in Sek.)	63
4.3.5	Reporting Delay for No Towers (sec.) (Reportverzögerung bei fehlenden Funkmasten in Sek.)	63
4.3.6	Reportverzögerung bei nur einem Funkmast	64
4.3.7	Outgoing SMS Length (Länge ausgehender SMS)	64
4.3.8	Name des Netzwerkzugriffspunkts (APN)	65
4.3.9	Network Access Point User Name (Benutzername des Netzwerkzugriffspunkts)	65
4.3.10	Passwort des Netzwerkzugriffspunkts	66
4.3.11	SIM-PIN	66
4.4	Cloud Remote Connect	66
4.4.1	Cloud Remote Connect (Ethernet)	66
4.4.2	Cloud Remote Connect (Cellular) [Cloud Remote Connect (Mobilfunk)]	67
4.5	IP-Kameras	67
4.5.1	Camera name (first language) [Kameraname (erste Sprache)]	67
4.5.2	Camera name (second language) [Kameraname (zweite Sprache)]	67
4.5.3	URL oder IP-Adresse	67
4.6	Verbundene Kameras von Bosch	68
4.6.1	RCP+ port # (RCP+-Port #)	68
4.6.2	Service-Passwort	68
4.6.3	Supervision period (sec.) (Überwachungszeitraum in Sek.)	69
4.7	Live (Video)	69
4.7.1	Port # (Portnummer)	69
4.7.2	Use HTTPS? (HTTPS verwenden?)	70
4.7.3	Benutzername	70
4.7.4	Passwort	70
4.8	Protokollübersicht	71
4.9	Report Routing (Protokoll-Routing)	73

4.9.1	Feuerprotokolle	78
4.9.2	Gasprotokolle	78
4.9.3	Einbruchprotokolle	79
4.9.4	Personennotfall-Protokolle	80
4.9.5	Benutzerprotokolle	80
4.9.6	Prüfprotokolle	81
4.9.7	Diagnoseprotokolle	82
4.9.8	Ausgangsprotokolle	83
4.9.9	Autofunktionsprotokolle	83
4.9.10	RPS-Protokolle	84
4.9.11	Melderprotokolle	84
4.9.12	Benutzeränderungsprotokolle	85
4.10	Übertragungsgerät – Übersicht	86
4.10.1	Primary Destination Device (Primäres Zielgerät)	88
4.10.2	Ersatzzielgeräte	88
4.10.3	RG Same Network Receiver (RG, selber Netzwerkempfänger)	89
4.10.4	Zeitsynchronisation	90
4.11	Enhanced Communication (Erweiterte Kommunikation)	90
4.11.1	Reporting Format (Protokollformat)	90
4.11.2	Empfänger	91
4.11.3	Netzwerkadresse	91
4.11.4	Portnummer	92
4.11.5	Receiver Supervision Time (Empfängerüberwachungsdauer)	92
4.11.6	Poll Rate (sec.) (Pollingrate in Sek.)	94
4.11.7	ACK Wait Time (sec.) (ACK-Wartezeit in Sek.)	95
4.11.8	Retry Count (Anzahl der Wiederholungsversuche)	96
4.11.9	Größe des AES-Schlüssels	96
4.11.10	AES-Verschlüsselungsschlüssel	97
4.12	SDI2 RPS/Enhanced Communication (SDI2 RPS/Erweiterte Kommunikation)	97
4.12.1	Enable Enhanced Communication? (Erweiterte Kommunikation aktivieren?)	97
4.12.2	Answer RPS Over Network? (RPS über Netzwerk antworten?)	97
4.12.3	RPS-Adressenverifizierung	98
4.12.4	RPS-Netzwerkadresse	98
4.12.5	RPS-Portnummer	98
4.13	Überwachung der Stromversorgung	99
4.13.1	Netzstromausfallzeit	99
4.13.2	Resend AC Fail (Netzstromfehler erneut senden)	99
4.13.3	AC Fail Display (Anzeige Netzstromfehler)	99
4.13.4	Netzstromfehler-/Netzstromwiederherstellungsprotokoll	99
4.13.5	AC Tag Along (Netzstromprotokoll angehängt)	99
4.13.6	AC / Battery Buzz (Netzstrom-/Batterie-Störungston)	100
4.13.7	Batteriefehler-/Batteriewiederherstellungsprotokoll	100
4.14	RPS-Parameter	100
4.14.1	RPS-Zugangscode	100
4.14.2	Belegte Protokollkapazität in %	101
4.14.3	Contact RPS if Log % Full (RPS bei belegter Protokollkapazität in % kontaktieren)	101
4.14.4	RPS Call Back (RPS-Rückruf)	102
4.14.5	RPS Line Monitor (RPS-Leitungsüberwachung)	102
4.14.6	Answer Armed (Antwort scharf)	102

4.14.7	Answer Disarmed (Antwort unscharf)	103
4.14.8	RPS-Telefonnummer	104
4.14.9	Geschwindigkeit des RPS-Modems	104
4.15	Sonstiges	104
4.15.1	Bedrohungstyp	104
4.15.2	Abbruchsprotokoll	105
4.15.3	Call for Service Text - First Language (Text Überprüfungsaufruf – erste Sprache)	106
4.15.4	Call for Service Text - Second Language (Text Überprüfungsaufruf – zweite Sprache)	106
4.15.5	On Site Authorization for Firmware Update (Vor-Ort-Autorisierung für Firmware-Aktualisierung)	106
4.15.6	Systemsabotagereaktion	107
4.15.7	Enclosure Tamper Enable (Gehäusesabotagekontakt aktivieren)	107
4.15.8	Feuer- und Gas-Zusammenfassung beibehalten	108
4.15.9	Typ des Feuerüberwachungsereignisses	108
4.15.10	Feuer und Gas – Signalton	108
4.15.11	Early Ambush Time (Zeit für zweimalige Authentifizierung)	109
4.15.12	Second Ambush Code (Code für zweimalige Authentifizierung)	109
4.15.13	Alarmabbruchzeit	109
4.15.14	Benutzercodelänge	110
4.15.15	Anzahl der Mehrfachauslösungsumgehungen	111
4.15.16	Remote Warning (Remote-Warnung)	111
4.15.17	Crystal Time Adjust (Quarzzeit anpassen)	112
4.15.18	Part On Output (Ausgang Außenhautüberwachung)	112
4.15.19	Early Area Armed Output (Ausgang frühe Bereichsscharfschaltung)	112
4.15.20	Sommerzeit	112
4.15.21	Date Format (Datumsformat)	113
4.15.22	Date Delimiter (Datumstrennzeichen)	113
4.15.23	Zeitformat	113
4.15.24	Zeitzone	114
4.15.25	Custom Text Format (Format Benutzerdefinierter Text)	116
4.16	Personal Notification Destinations (Persönliche Benachrichtigungsziele)	116
4.16.1	Beschreibung	116
4.16.2	SMS-Zielrufnummer/E-Mail-Adresse	116
4.16.3	User Language (Benutzersprache)	117
4.16.4	Methode	117
4.17	Personal Notification Reports (Persönliche Benachrichtigungen)	118
4.18	Persönliche Benachrichtigung – Routing-Versuche	118
4.19	Konfiguration des E-Mail-Servers	119
4.19.1	Email Server Name/Address (Name/Adresse des E-Mail-Servers)	119
4.19.2	Email Server Port Number (Portnummer des E-Mail-Servers)	120
4.19.3	Email Server Authentication/Encryption (Authentifizierung/Verschlüsselung des E-Mail-Servers)	121
4.19.4	Authentication User Name (Authentifizierungs-Benutzername)	121
4.19.5	Authentication Password (Authentifizierungs-Passwort)	122
5	**Area Wide Parameters (Bereichsübergreifende Parameter)**	**123**
5.1	Bereichs-/Signalparameter, Optionen für Öffnen/Schließen	123
5.1.1	Area Name Text (first language) [Text Bereichsname (erste Sprache)]	123
5.1.2	Area Name Text (Second Language) [Text Bereichsname (zweite Sprache)]	123
5.1.3	Area On (Bereich an)	124

5.1.4	Kontonummer	124
5.1.5	Force Arm/Bypass Max (Zwangsläufiges Scharfschalten/Abschalten)	125
5.1.6	Delay Restorals (Wiederherstellungen bei Verzögerung)	125
5.1.7	Exit Tone (Scharfschaltungston)	126
5.1.8	Scharfschalteverzögerungszeit	126
5.1.9	Auto Watch (Automatische Überwachung)	126
5.1.10	Neustartzeit	127
5.1.11	Duress Enable (Bedrohungsalarm aktivieren)	128
5.1.12	Bereichstyp	129
5.1.13	Zwei-Mann-Regel?	131
5.1.14	Zweimalige Authentifizierung?	132
5.1.15	Feuer und Gas – Zeit	132
5.1.16	Fire Pattern (Brandmuster)	133
5.1.17	Burg Time (Einbruchalarmzeit)	133
5.1.18	Burg Pattern (Muster für Einbruchalarm)	134
5.1.19	Gas Pattern (Gasmuster)	134
5.1.20	Single Ring (Ein Alarmsignal)	134
5.1.21	Zutrittssignaltest	135
5.1.22	Account O/C (Konto öffnen/schließen)	136
5.1.23	Area O/C (Bereich öffnen/schließen)	136
5.1.24	Disable O/C in Window (Öffnen/Schließen in Fenster deaktivieren)	137
5.1.25	Auto Close (Automatische Scharfschaltung)	137
5.1.26	Fehler beim Öffnen	137
5.1.27	Fehler beim Schließen	138
5.1.28	Latest Close Time (Letzte Schließzeit)	138
5.1.29	Restricted O/C (Eingeschränkt öffnen/schließen)	138
5.1.30	Part On O/C (Außenhautüberwachung öffnen/schließen)	139
5.1.31	Exit Delay Restart (Neustart der Scharfschalteverzögerung)	139
5.1.32	All On - No Exit (Vollscharfschaltung – Kein Austritt)	140
5.1.33	Warnung Scharfschalteverzögerungszeit	141
5.1.34	Warnung Eintrittsverzögerung	141
5.1.35	Area Re-Arm Time (Zeit zum erneuten Scharfschalten des Bereichs)	141
5.2	Area Arming Text (Text Bereichsscharfschaltung)	142
5.2.1	Area name text (Text Bereichsname)	142
5.2.2	Account is On text (Text für Konto aktiv)	142
5.2.3	Area # is On text (Text für Bereichsnr. aktiv)	142
5.2.4	Area # is not Ready text (Text für Bereichsnr. nicht bereit)	143
5.2.5	Area Nr. is Off text (Text für Bereichsnr. ist ausgeschaltet)	143
6	**Bedienteile**	**144**
6.1	Bedienteilzuweisungen	144
6.1.1	Keypad Name (first language) [Name des Bedienteils (erste Sprache)]	144
6.1.2	Keypad Name (second language) [Name des Bedienteils (zweite Sprache)]	144
6.1.3	Keypad Type (Bedienteiltyp)	144
6.1.4	Area Assignment (Bereichszuordnung)	145
6.1.5	Bedienteilsprache	145
6.1.6	Scope (Bereich)	145
6.1.7	Areas in Scope (Bereiche im Umfang)	146
6.1.8	Passcode Follows Scope? (Zugangscode entspricht Anwendungsbereich?)	146
6.1.9	Enter Key Output (Ausgang Eingabetaste)	147

6.1.10	Passcode Enter Function (Zugangscode-Eingabefunktion)	147
6.1.11	Dual Authentication (Zweifache Authentifizierung)	148
6.1.12	Dual Authentication Duration (Dauer der zweifachen Authentifizierung)	149
6.1.13	Trouble Tone (Störungston)	149
6.1.14	Entry Tone (Eingangston)	149
6.1.15	Exit Tone (Scharfschaltungston)	150
6.1.16	Arm Area Warning Tone (Warnton Bereichsscharfschaltung)	150
6.1.17	Idle Scroll Lock (Bildlauf gesperrt, wenn inaktiv)	150
6.1.18	Function Lock (Funktionssperre)	150
6.1.19	Abort Display (Abbruch anzeigen)	151
6.1.20	Cancel Display (Abgebrochen anzeigen)	151
6.1.21	Nightlight Enable (Nachtlicht aktivieren)	151
6.1.22	Nightlight Brightness (Nachtlichthelligkeit)	152
6.1.23	Silence Keypress Tone (Tastenton stummschalten)	152
6.1.24	Show Date and Time (Datum und Uhrzeit anzeigen)	152
6.1.25	Keypad Volume (Bedienteillautstärke)	152
6.1.26	Keypad Brightness (Bedienteilhelligkeit)	152
6.1.27	Disable Presence Sensor (Anwesenheitsmelder deaktivieren)	153
6.1.28	Disable Token Reader (Codierschlüssel-Leser deaktivieren)	153
6.1.29	Enable Tamper Switch (Sabotagekontakt aktivieren)	153
6.1.30	Feature Button Option (Option Funktionsschaltfläche)	153
6.1.31	Überwachung	154
6.1.32	Passcode [Esc] Option (Option „Zugangscode [Esc]”)	154
6.2	Global Keypad Settings (Globale Bedienteileinstellungen)	155
6.2.1	A-key Response (Funktion A-Taste)	155
6.2.2	A-key Custom Function (Benutzerdefinierte Funktion A-Taste)	155
6.2.3	B-key Response (Funktion B-Taste)	156
6.2.4	Benutzerdefinierte Funktion B-Taste	156
6.2.5	Funktion C-Taste	156
6.2.6	Benutzerdefinierte Funktion C-Taste	157
6.2.7	Manueller stiller Alarm hörbar bei Kommunikationsstörung	157
6.2.8	Kartentyp	157
6.2.9	Optionen für Übertragungsstörung	158
6.3	Globaler Funk-Handsender	158
6.3.1	Funk-Handsender Funktion A benutzerdefinierte Funktion	158
6.3.2	Funk-Handsender Funktion B benutzerdefinierte Funktion	158
6.3.3	Notrufoptionen für Funk-Handsender	159
7	**Benutzerdefinierte Funktionen**	**160**
7.1	Text der benutzerdefinierten Funktion (erste Sprache)	160
7.2	Text der benutzerdefinierten Funktion (zweite Sprache)	160
7.3	Funktionen	160
8	**Kontextmenü**	**162**
8.1	Funktion	162
8.2	Set/Clear all (Alle festlegen/löschen)	163
8.3	Adresse Nr.	163
9	**Ausgangsparameter**	**164**
9.1	Bereichsübergreifende Ausgänge	165
9.1.1	Alarm-Signalgeber	165
9.1.2	Feueralarm	166

9.1.3	Reset Sensors (Melder zurücksetzen)	166
9.1.4	Fehler beim Schließen/Außenhautüberwachung scharfgeschaltet	167
9.1.5	Zwangsläufig scharfgeschaltet	167
9.1.6	Überwachungsmodus	167
9.1.7	Bereich scharfgeschaltet	168
9.1.8	Bereich unscharfgeschaltet	168
9.1.9	Störung im Bereich	168
9.1.10	Bedrohungsausgang	169
9.1.11	Fehler bei Außenhautüberwachung	169
9.1.12	Stiller Alarm	169
9.1.13	Gasalarm	170
9.2	Zentralenübergreifende Ausgänge	170
9.2.1	Netzstörung	170
9.2.2	Batteriestörung	170
9.2.3	Telefon Fehler	170
9.2.4	Kommunikationsfehler	171
9.2.5	Belegte Protokollkapazität in %	171
9.2.6	Zusammenfassung Feuer	171
9.2.7	Zusammenfassung Alarm	172
9.2.8	Zusammenfassung Feuerstörung	172
9.2.9	Zusammenfassung Feuer-Errichterbedienung	173
9.2.10	Zusammenfassung Störung	173
9.2.11	Zusammenfassung Einbruch-Errichterbedienung	173
9.2.12	Ausgang für Zusammenfassung Gas	174
9.2.13	Errichterbedienungsausgang für Zusammenfassung Gas	174
9.2.14	Störungsausgang für Zusammenfassung Gas	175
9.3	Ausgangskonfiguration	175
9.3.1	Output Source (Ausgangsquelle)	175
9.3.2	Ausgangstext (erste Sprache)	175
9.3.3	Ausgangstext (zweite Sprache)	176
9.3.4	Für Benutzer ausblenden	176
10	**Benutzerkonfiguration**	**177**
10.1	Benutzerzuweisungen (Zugangscodes)	177
10.1.1	Benutzername	177
10.1.2	Zugangscode	177
10.1.3	Fernzugriff	177
10.1.4	Benutzergruppe	178
10.1.5	Bereichsberechtigungen	178
10.1.6	Standortcode	178
10.1.7	Kartendaten	179
10.1.8	Inovonics Funk-Handsender RFID (B820)	179
10.1.9	RFID des RADION Funk-Handsenders (B810)	180
10.1.10	Überwacht	180
10.1.11	Benutzersprache	180
10.2	Benutzergruppen	180
10.2.1	Name der Benutzergruppe	180
10.3	Benutzerfunktionen (Bedienteil)	181
10.3.1	Verzögerte Vollscharfschaltung	181
10.3.2	Unverzögerte Vollscharfschaltung	181

10.3.3	Unverzögerte Außenhautüberwachung	181
10.3.4	Verzögerte Außenhautüberwachung	182
10.3.5	Überwachungsmodus	182
10.3.6	View Area Status (Bereichsstatus anzeigen)	182
10.3.7	Aktuelle Ereignisse anzeigen/löschen	183
10.3.8	View Point Status (Melderstatus anzeigen)	183
10.3.9	Revision (alle Melder für Nicht-Feueralarme und Einbruchalarme)	183
10.3.10	Revision für alle Feuermelder	184
10.3.11	Protokoll senden (Prüfung/Status)	185
10.3.12	Bedienteilhelligkeit/Lautstärke/Tastenton einstellen	185
10.3.13	Datum und Uhrzeit einstellen/anzeigen	185
10.3.14	Zugangscodes ändern	186
10.3.15	Benutzer hinzufügen/bearbeiten	186
10.3.16	Benutzer löschen	186
10.3.17	Extend Close (Schließen verlängern)	187
10.3.18	Ereignisprotokoll anzeigen	187
10.3.19	Benutzerbefehl 7	187
10.3.20	Benutzerbefehl 9	188
10.3.21	Bypass a Point (Einen Melder übergehen)	188
10.3.22	Unbypass a Point (Einen Melder einschalten)	188
10.3.23	Melder zurücksetzen	189
10.3.24	Ausgang ändern	189
10.3.25	Fernparametrierung	189
10.3.26	Gehe zu Bereich	190
10.3.27	Typ und Version des Anzeigetableaus	190
10.3.28	Wartungs-Funktionstest für alle Melder	190
10.3.29	Change Skeds (Zeitgesteuerte Ereignisse ändern)	191
10.3.30	Revision für alle unsichtbaren Melder für Einbruchalarme	191
10.3.31	Stummschalten-Funktion	191
10.3.32	Benutzerdefinierte Funktion	192
10.3.33	Bedienteilparametrierung	192
10.4	Benutzerrechte	193
10.4.1	Name der Benutzerrechte (erste Sprache)	193
10.4.2	Name der Benutzerrechte (zweite Sprache)	193
10.4.3	Auswahl unscharfschalten	193
10.4.4	Verzögerte Vollscharfschaltung	194
10.4.5	Unverzögerte Vollscharfschaltung	194
10.4.6	Unverzögerte Außenhautüberwachung	194
10.4.7	Verzögerte Außenhautüberwachung	195
10.4.8	Überwachungsmodus	195
10.4.9	View Area Status (Bereichsstatus anzeigen)	196
10.4.10	View Event Memory (Aktuelle Ereignisse anzeigen)	196
10.4.11	View Point Status (Melderstatus anzeigen)	196
10.4.12	Revision (alle Melder für Nicht-Feueralarme und Einbruchalarme)	197
10.4.13	Revision für alle Feuermelder	197
10.4.14	Revision für alle unsichtbaren Melder für Einbruchalarme	198
10.4.15	Wartungs-Funktionstest für alle Melder	198
10.4.16	Protokoll senden (Prüfung/Status)	199
10.4.17	Bedienteilanzeige ändern	199

10.4.18	Datum und Uhrzeit ändern	199
10.4.19	Zugangscodes ändern	200
10.4.20	Zugangscodes/Karte/Ebene des Benutzers hinzufügen	200
10.4.21	Zugangscode/Karte/Ebene des Benutzers löschen	200
10.4.22	Extend Close (Schließen verlängern)	201
10.4.23	Ereignisprotokoll anzeigen	201
10.4.24	Benutzerbefehl 7	201
10.4.25	Benutzerbefehl 9	201
10.4.26	Bypass a Point (Einen Melder übergehen)	202
10.4.27	Unbypass a Point (Einen Melder einschalten)	202
10.4.28	Melder zurücksetzen	202
10.4.29	Ausgänge ändern	202
10.4.30	Fernparametrierung	203
10.4.31	Go to Area (Gehe zu Bereich)	203
10.4.32	Typ und Version des Anzeigetableaus	204
10.4.33	Change Skeds (Zeitgesteuerte Ereignisse ändern)	204
10.4.34	Benutzerdefinierte Funktion	204
10.4.35	Erzwungenes Scharfschalten	205
10.4.36	Sendebereich öffnen/schließen	205
10.4.37	Eingeschränkt öffnen/schließen	205
10.4.38	Außenhautüberwachung öffnen/schließen	206
10.4.39	Bedrohung senden	206
10.4.40	Scharfschaltung durch Zugangscode	206
10.4.41	Scharfschaltung durch Zugangscode aufheben	207
10.4.42	Sicherheitsstufe	207
10.4.43	Unscharfschaltungsstufe	208
10.4.44	Funktionsebene	209
10.4.45	Funk-Handsender scharfschalten	209
10.4.46	Funk-Handsender unscharfschalten	210
10.4.47	Firmware-Aktualisierung	210
10.4.48	Stummschalten-Funktion	210
11	**Melder-**	**211**
11.1	Melderzuweisungen	211
11.1.1	Quelle	211
11.1.2	Text (erste Sprache)	211
11.1.3	Text (zweite Sprache)	211
11.1.4	Profil (Index)	212
11.1.5	Beschreibung des Profils (Index)	212
11.1.6	Bereich	212
11.1.7	Entprellen	212
11.1.8	Ausgang	213
11.1.9	RADION RFID (B810)	213
11.1.10	RADION-Gerätetyp	214
11.1.11	Inovonics RFID (B820)	215
11.2	Melderabhängigkeit-Parameter	216
11.2.1	Melderabhängigkeit-Schaltuhr	216
11.3	Melderprofile	216
11.3.1	Melderprofiltext (Erste Sprache)	216
11.3.2	Melderprofiltext (Zweite Sprache)	217

11.3.3	Melderart/Reaktion/Stromkreisbauweise	217
11.3.4	Melderart	218
11.3.5	Übersicht über Melderreaktionen	222
11.3.6	Melderreaktion	223
11.3.7	Stromkreisbauweise	237
11.3.8	Eingangsverzögerung	238
11.3.9	Eingangston aus	238
11.3.10	Stilles Zutrittssignal	238
11.3.11	Sabotagereaktion	239
11.3.12	Klingelzeichen bis Zurücksetzung	239
11.3.13	Hörbar nach 2 Fehlern	239
11.3.14	Unsichtbarer Melder	240
11.3.15	Summeralarm bei Fehler	240
11.3.16	Überwachungsmelder	241
11.3.17	Ausgangsreaktionstyp	241
11.3.18	Als Gerät anzeigen	241
11.3.19	Lokal, wenn unscharfgeschaltet	242
11.3.20	Lokal, wenn scharfgeschaltet	242
11.3.21	Wiederherstellungen deaktivieren	243
11.3.22	Zwangsläufige Scharfschaltung wiederherstellbar	243
11.3.23	Übergehung wiederherstellbar	243
11.3.24	Übergehen möglich	244
11.3.25	Swinger-Übergehung	244
11.3.26	Übergehungsprotokoll beim Auftreten	244
11.3.27	Übergehungsprotokoll verzögern	245
11.3.28	Melderabhängigkeit	245
11.3.29	Alarmbestätigung	246
11.3.30	Rücksetzbar	247
11.3.31	Alarmabbruch	247
11.3.32	Überwachungsdauer des Funkmelders	247
11.3.33	Benutzerdefinierte Funktion	248
11.3.34	Überwachungsverzögerung	248
11.3.35	Verzögerte Antwort, unscharf	249
11.3.36	Verzögerte Antwort, scharf	249
11.3.37	Normalzustand	250
11.4	Melderprofilbeschreibungen	250
11.4.1	24 Stunden	250
11.4.2	Außenhautüberwachung	250
11.4.3	Innenbereich	251
11.4.4	Wegmelder Innenbereich	252
11.4.5	Schlüsselschalter	253
11.4.6	Schlüsseltaster	253
11.4.7	Öffnen-/Schließen-Melder	253
11.4.8	Feuermelder	254
11.4.9	AUX-AC-Überwachung	254
11.4.10	Gasmelder	254
11.4.11	Benutzerdefinierte Funktion	254
12	**Zeitpläne**	**255**
12.1	Fenster öffnen/schließen	255

12.1.1	Öffnen-Fenster-Timeline	255
12.1.2	Tabelle für Öffnen-/Schließen-Fenster	256
12.1.3	Sonntag bis Samstag	258
12.1.4	Frühes Öffnen – Beginn	258
12.1.5	Fenster öffnen - Start	259
12.1.6	Fenster öffnen – Stopp	259
12.1.7	Frühes Schließen – Beginn	260
12.1.8	Fenster schließen - Start	261
12.1.9	Fenster schließen - Stopp	261
12.1.10	Außer an Feiertagen	262
12.1.11	Feiertags-Nr.	262
12.1.12	Bereich Nr.	263
12.2	Benutzergruppen-Fenster	263
12.2.1	Benutzergruppe	263
12.2.2	Sonntag bis Samstag	263
12.2.3	Gruppenaktivierungszeit	264
12.2.4	Gruppendeaktivierungszeit	264
12.2.5	Außer an Feiertagen	265
12.2.6	Feiertags-Nr.	265
12.3	Zeitgesteuerte Ereignisse	265
12.3.1	Zeitgesteuerte Ereignisse Name Text	265
12.3.2	Zeitgesteuertes Ereignis – Namenstext (zweite Sprache)	266
12.3.3	Zeitbearbeitung	266
12.3.4	Funktion	266
12.3.5	Zeit	267
12.3.6	Datum	267
12.3.7	Sonntag bis Samstag	268
12.3.8	Außer an Feiertagen	268
12.3.9	Feiertags-Nr.	268
12.4	Feiertagsindexe	269
12.4.1	Zeitplan	269
12.5	Funktion „Zeitgesteuertes Ereignis“ – Beschreibungen	269
12.5.1	All On Delay (Verzögerte Vollscharfschaltung)	269
12.5.2	All On Instant (Unverzögerte Vollscharfschaltung)	269
12.5.3	Verzögerte Außenhautüberwachung	269
12.5.4	Unverzögerte Außenhautüberwachung	269
12.5.5	Unscharfschalten	270
12.5.6	Extend Close (Schließen verlängern)	270
12.5.7	Bypass a Point (Einen Melder übergehen)	270
12.5.8	Unbypass a Point (Einen Melder einschalten)	270
12.5.9	Unbypass All Points (Alle Melder einschalten)	270
12.5.10	Reset Sensors (Melder zurücksetzen)	270
12.5.11	Ausgang einschalten	270
12.5.12	Ausgang ausschalten	271
12.5.13	Ausgang umschalten	271
12.5.14	Monostabiler Ausgang	271
12.5.15	Alle Ausgänge zurücksetzen	271
12.5.16	Verzögerung	271
12.5.17	RPS antworten	271

12.5.18	RPS kontaktieren	271
12.5.19	RPS kontaktieren – Benutzerport	272
12.5.20	Send Status Report (Zustandsmeldungen senden)	272
12.5.21	Send Test Report (Prüfprotokolle senden)	272
12.5.22	Prüfprotokoll bei nicht-normalem Zustand senden	274
12.5.23	Go to Area (Gehe zu Bereich)	274
12.5.24	Überwachung einschalten	274
12.5.25	Überwachung ausschalten	274
12.5.26	Datum und Uhrzeit anzeigen	274
12.5.27	Überwachungston ausgeben	274
12.5.28	Bedienteillautstärke festlegen	275
12.5.29	Bedienteilhelligkeit festlegen	275
12.5.30	Störung stummschalten	275
12.5.31	Alarm stummschalten	275
12.5.32	Benutzerdefinierte Funktion ausführen	275
13	**Automatisierung/Remote-App**	**276**
13.1	Automatisierungsgerät	276
13.2	Status-Rate	276
13.3	Automatischer Zugangscode	276
13.4	Modus 1 – Automatisierung Ethernet-Port-Nummer	277
13.5	Remote-App	277
13.6	Remote-App-Zugangscode	277
14	**SDI2-Module**	**278**
14.1	B208-Octo-Eingang	278
14.1.1	Gehäusesabotage	278
14.2	B308-Octo-Ausgang	278
14.2.1	Modul-Gehäusesabotagekontakt	278
14.3	(B42x) IP-Übertragungsgerät	279
14.3.1	Modul-Gehäusesabotagekontakt	279
14.3.2	IPv6-Modus	279
14.3.3	IPv6 DHCP	279
14.3.4	IPv4 DHCP/AutoIP Enable (IPv4 DHCP/AutoIP aktivieren)	280
14.3.5	IPv4-Adresse	280
14.3.6	IPv4-Subnetzmaske	280
14.3.7	IPv4-Standard-Gateway	281
14.3.8	IPv4 DNS Server IP Address (IPv4-DNS-Server-IP-Adresse)	281
14.3.9	IPv6-DNS-Server-IP-Adresse	281
14.3.10	UPnP (Universal Plug & Play) aktivieren	281
14.3.11	HTTP-Portnummer	282
14.3.12	ARP-Cache-Timeout (Sek.)	282
14.3.13	Zugriff über Webbrowser/USB	282
14.3.14	Passwort für Zugriff über Webbrowser/USB	282
14.3.15	Firmware-Upgrade aktivieren	282
14.3.16	Hostname des Moduls	283
14.3.17	Modulbeschreibung	283
14.3.18	TCP/UDP Port Number (TCP/UDP-Portnummer)	283
14.3.19	TCP Keep-Alive-Zeit	283
14.3.20	IPv4-Testadresse	283
14.3.21	IPv6-Testadresse	283

14.3.22	Sicherheit bei Webzugriff und Automatisierung	284
14.3.23	IP-Adresse des alternativen IPv4-DNS-Servers	284
14.3.24	IP-Adresse des alternativen IPv6-DNS-Servers	284
14.4	B450 Mobilfunk	285
14.4.1	Eingehende SMS	285
14.4.2	Dauer des Sitzungs-Keep-Alive (Min.)	285
14.4.3	Inaktivitäts-Timeout (Min.)	285
14.4.4	Reporting Delay for Low Signal Strength (sec.) (Reportverzögerung bei geringer Signalstärke in Sek.)	286
14.4.5	Reportverzögerung bei nur einem Funkmast (s)	286
14.4.6	Reporting Delay for No Towers (sec.) (Reportverzögerung bei fehlenden Funkmasten in Sek.)	286
14.4.7	Outgoing SMS Length (Länge ausgehender SMS)	287
14.4.8	SIM-PIN	287
14.4.9	Name des Netzwerkzugriffspunkts (APN)	287
14.4.10	Network Access Point User Name (Benutzername des Netzwerkzugriffspunkts)	288
14.4.11	Passwort des Netzwerkzugriffspunkts	288
14.5	B520 zusätzliches Netzteil	289
14.5.1	Modul aktivieren	289
14.5.2	Modul-Gehäusesabotagekontakt	289
14.5.3	Ein oder zwei Batterien	289
14.6	Funkempfänger	290
14.6.1	Typ des Funkmoduls	290
14.6.2	Modul-Gehäusesabotagekontakt	290
14.6.3	Systemüberwachungsdauer (Repeater)	291
14.6.4	Signalton bei schwacher Batterie	291
14.6.5	Störungserkennung aktivieren	291
14.7	Wireless Repeater (Funkrepeater)	291
14.7.1	Modul-Gehäusesabotagekontakt	292
14.7.2	RADION RFID (B810)	292
14.7.3	Inovonics RFID (B820)	292
15	**Einstellungen des Hardwareschalters**	**293**
15.1	Bedienteil-Adresse	293
15.2	Schaltereinstellungen für das B208-Modul mit acht Eingängen	294
15.3	Schaltereinstellungen für B308-Modul mit acht Ausgängen	295
15.4	Schaltereinstellungen für das B426-Ethernet-Übertragungsmodul	295
15.5	Schaltereinstellungen für B450-Mobilfunkmodul	295
15.6	Schaltereinstellungen für B520-Netzteil	296
15.7	Schaltereinstellungen für B810 RADION-Funkempfänger	296
15.8	Schaltereinstellungen des B820 Inovonics-Funkempfängers	296
16	**Konfigurieren für den Mobilfunkdienst**	**297**
17	**Formate von IP-Adresse und Domainname**	**300**

1 Fernparametrier-Software

Remote Programming Software (RPS) ist ein Dienstprogramm zur Kontoverwaltung und Parametrierung der Zentrale für Microsoft Windows-Betriebssysteme. Die Bediener können RPS für bestimmte Zentralen zur Fernparametrierung, Speicherung von Konten, Fernbedienung und für Diagnosen verwenden.

2 Zentralenspezifische Informationen

2.1 Zentrale – Symbolleiste und Symbole

Beim Öffnen von RPS befinden sich diese Symbole auf der Funktionsleiste.

Symbol	Name	Beschreibung
	Neu	Erstellen Sie ein neues Zentralenkonto.
	Anzeigen	Rufen Sie Kontoeinrichtungsdetails für die gewählte Zentrale auf.
	Löschen	Löschen Sie das ausgewählte Zentralenkonto.
	Öffnen	Öffnen Sie das ausgewählte Zentralenkonto.
	Filtern	Filtern Sie Daten in der sichtbaren Listenansicht.
	Ansicht löschen	Löschen Sie Inhalte der Ansicht.

Beim Öffnen eines Zentralenkontos befinden sich diese Symbole auf der Funktionsleiste. Einige der Symbole werden nur angezeigt, wenn RPS mit der Zentrale verbunden ist.

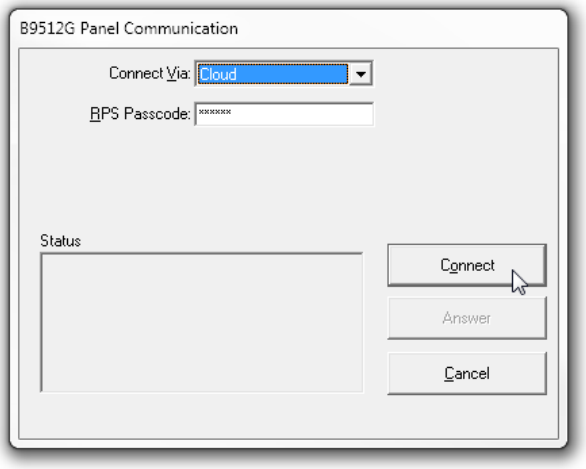
Symbol	Name	Beschreibung
	Vergleichen, Seite 27	Vergleichen Sie zwei Zentralenkonten des gleichen Zentralentyps miteinander.
	Suchen und ersetzen, Seite 28	Suchen Sie im aktuellen Fenster nach einem Parameterwert. Setzen Sie einen neuen Wert ein.
	Sicherheit, Seite 29	Ändern Sie die Sicherheitsstufen der Zentrale.
	Send/Receive (Senden/Empfangen), Seite 31	Senden Sie Daten an die Zentrale, oder empfangen Sie Daten von ihr.
	Hintergrundspeicher anzeigen, Seite 32	Zeigen Sie den letzten Verlauf der Zentralenereignisse an.
	Get history (Hintergrundspeicher abrufen), Seite 32	Rufen Sie ein aktualisiertes Ereignisprotokoll von der Zentrale ab.
	Diagnose, Seite 32	Öffnen Sie das Fenster „Diagnose“.

Symbol	Name	Beschreibung
	Verbindung mit der Zentrale herstellen, Seite 18	Öffnen Sie das Dialogfeld „Panel Communication“ (Anlagenverbindung).
	Kontohinweise, Seite 33	Öffnen Sie das Fenster „Account Notes“ (Kontohinweise). Tippen und speichern Sie Hinweise.
	Firmware-Aktualisierung, Seite 34	Öffnen Sie den Firmware Update-Assistenten. Aktualisieren Sie die Firmware in der Zentrale oder den Modulen.

2.2 Verbindung mit der Zentrale herstellen

Zum Öffnen des Fensters „Panel Communication“ (Anlagenverbindung) klicken Sie im Menü „Operations“ (Betrieb) oder auf der Funktionsleiste auf **„Verbinden“** . Wählen Sie über das Fenster „Panel Communication“ (Anlagenverbindung) eine Verbindungsmethode aus.

2.2.1 Verbinden über: Cloud

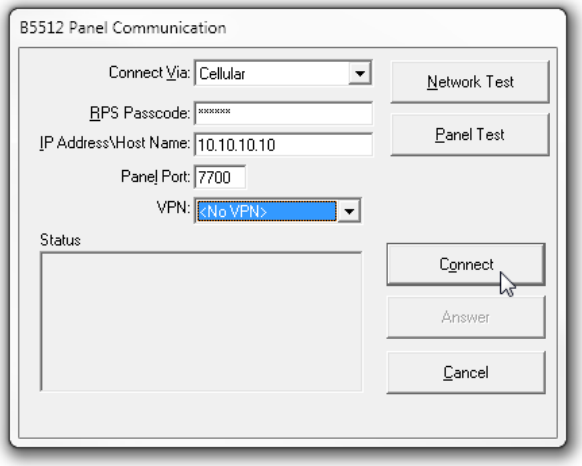


Feld/Schaltfläche	Beschreibung
Verbinden über [**Cloud**]	Wählen Sie die Verbindungsmethode, mit der RPS eine Verbindung mit der Zentrale herstellt.
RPS-Zugangscode	RPS zeigt Sternchen (*) für den Zugangscode aus dem Parameter „ZENTRALENÜBERGREIFENDE PARAMETER“ > „RPS-Parameter“ > „RPS-Zugangscode“ an. Wenn Sie einen anderen RPS-Zugangscode für diese Verbindung eingeben, wird dieser von RPS nicht gespeichert.
Status	Dieses Feld zeigt den Status des Verbindungsprozesses an.
Verbinden	Mit einem Klick auf diese Schaltfläche stellen Sie eine Verbindung mit der Zentrale her.

Feld/Schaltfläche	Beschreibung
Verbinden	Diese Schaltfläche „Verbinden“ ist für die Methode „Cloudverbindung“ nicht aktiv.
Abbrechen	Klicken Sie auf „Abbrechen“, um das Fenster „Panel Communication“ (Anlagenverbindung) zu schließen. Wenn Sie zum Starten des Verbindungsprozesses auf „Verbinden“ geklickt haben, wird die Schaltfläche „Abbrechen“ zur Schaltfläche „Abbrechen“. Klicken Sie auf „Abbrechen“, um den Verbindungsprozess zu beenden.

2.2.2 Verbinden über: Mobilfunk

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

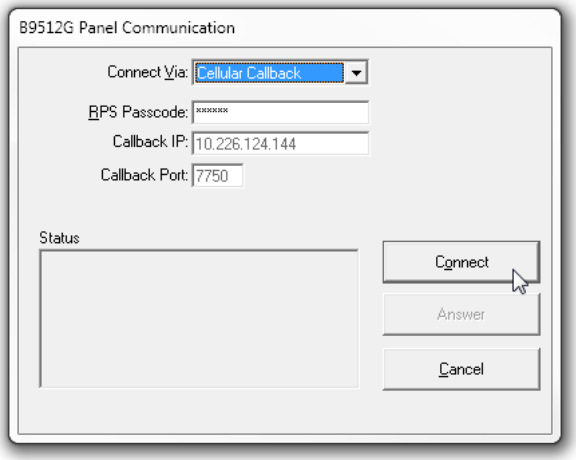


Feld/Schaltfläche	Beschreibung
Verbinden über [**Mobilfunk**]	Wählen Sie die Verbindungsmethode, mit der RPS eine Verbindung mit der Zentrale herstellt.
RPS-Zugangscode	RPS zeigt Sternchen (*) für den Zugangscode aus dem Parameter „ZENTRALENÜBERGREIFENDE PARAMETER“ > „RPS-Parameter“ > „RPS-Zugangscode“ an. Wenn Sie einen anderen RPS-Zugangscode für diese Verbindung eingeben, wird dieser von RPS nicht gespeichert.
IP-Adresse\Hostname	In diesem Feld wird die IP-Adresse oder der Hostname aus der Ansicht der Zentralendaten angezeigt, IP-Adresse > HostName-Parameter.

Feld/Schaltfläche	Beschreibung
Port Zentrale	In diesem Feld wird die Portnummer aus der Ansicht der Zentralendaten angezeigt, Feld „Port Zentrale“.
VPN	Wählen Sie aus im Fenster „Config“ (Konfiguration) (Menü)/„System“/ „Anschlussmöglichkeiten“/„VPN“ konfigurierten virtuellen privaten Netzwerken (Virtual Private Networks, VPN).
Status	In diesem Feld wird der Status des Verbindungsprozesses, einer Netzwerkprüfung oder Zentralenprüfung angezeigt.
Netzwerkprüfung	Klicken Sie auf diese Schaltfläche, um eine Netzwerkprüfung zu starten. RPS sendet einen Ping an die Netzwerkschnittstelle der Zentrale. Wenn die Zentrale den Ping hört, sendet sie eine Antwort an RPS. Im Feld „Status“ wird das Ergebnis der Netzwerkprüfung angezeigt.
Zentralenprüfung	Klicken Sie auf diese Schaltfläche, um eine Zentralenprüfung zu starten. RPS sendet einen Ping an die Netzwerkschnittstelle der Zentrale. Wenn die Zentrale den Ping hört, sendet sie eine Antwort an RPS. Im Feld „Status“ wird das Ergebnis der Prüfung angezeigt.
Verbinden	Mit einem Klick auf diese Schaltfläche stellen Sie eine Verbindung mit der Zentrale her.
Verbinden	Klicken Sie auf „Verbinden“, um eine von der Zentrale initiierte Verbindung abzuschließen.
Abbrechen	Klicken Sie auf „Abbrechen“, um das Fenster „Panel Communication“ (Anlagenverbindung) zu schließen. Wenn Sie zum Starten des Verbindungsprozesses auf „Verbinden“ geklickt haben, wird die Schaltfläche „Abbrechen“ zur Schaltfläche „Abbrechen“. Klicken Sie auf „Abbrechen“, um den Verbindungsprozess zu beenden.

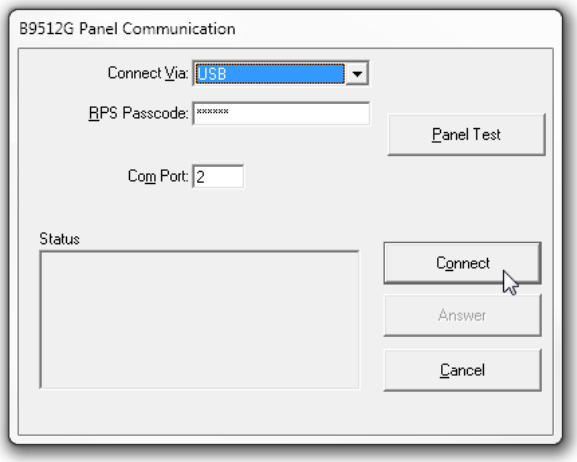
2.2.3 Verbinden über: Rückruf per Mobilfunk

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.



Feld/Schaltfläche	Beschreibung
Verbinden über [**Rückruf per Mobilfunk**]	Wählen Sie die Verbindungsmethode, mit der RPS eine Verbindung mit der Zentrale herstellt.
RPS-Zugangscode	RPS zeigt Sternchen (*) für den Zugangscode aus dem Parameter „ZENTRALENÜBERGREIFENDE PARAMETER“ > „RPS-Parameter“ > „RPS-Zugangscode“ an. Wenn Sie einen anderen RPS-Zugangscode für diese Verbindung eingeben, wird dieser von RPS nicht gespeichert.
Rückruf-IP	Dieses Feld ist schreibgeschützt. Zeigt die IP-Adresse an, über die die Zentrale eine Verbindung mit RPS herstellt.
Rückruf-Port	Dieses Feld ist schreibgeschützt. Hier wird die IP-Adresse angegeben, über die die Zentrale eine Verbindung mit RPS herstellt.
Verbinden	Mit einem Klick auf diese Schaltfläche stellen Sie eine Verbindung mit der Zentrale her.
Verbinden	Klicken Sie auf „Verbinden“, um eine von der Zentrale initiierte Verbindung abzuschließen.
Abbrechen	Klicken Sie auf „Abbrechen“, um das Fenster „Panel Communication“ (Anlagenverbindung) zu schließen. Wenn Sie zum Starten des Verbindungsprozesses auf „Verbinden“ geklickt haben, wird die Schaltfläche „Abbrechen“ zur Schaltfläche „Abbrechen“. Klicken Sie auf „Abbrechen“, um den Verbindungsprozess zu beenden.

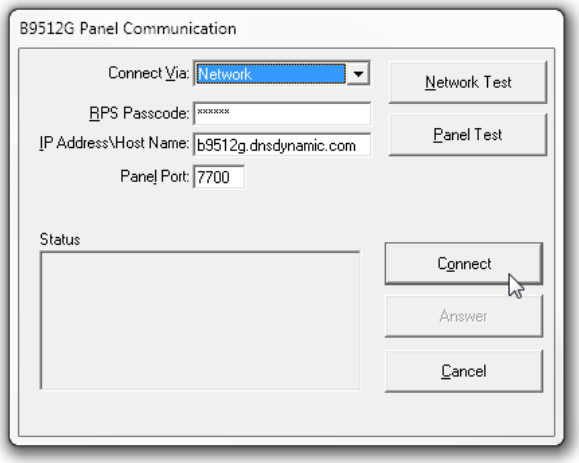
2.2.4 Verbinden über: USB



Feld/Schaltfläche	Beschreibung
Verbinden über [**USB**]	Wählen Sie die Verbindungsmethode, mit der RPS eine Verbindung mit der Zentrale herstellt.
RPS-Zugangscode	RPS zeigt Sternchen (*) für den Zugangscode aus dem Parameter „ZENTRALENÜBERGREIFENDE PARAMETER“ > „RPS-Parameter“ > „RPS-Zugangscode“ an. Wenn Sie einen anderen RPS-Zugangscode für diese Verbindung eingeben, wird dieser von RPS nicht gespeichert.
Zentralenprüfung	RPS führt eine Zentralenprüfung durch, indem ein Ping an die Zentrale gesendet wird. Diese Prüfung bestätigt, dass die Verbindung zwischen der Zentrale und RPS korrekt konfiguriert ist. Im Feld „Status“ wird das Ergebnis der Zentralenprüfung angezeigt.
COM-Schnittstelle	Wenn Sie die Zentrale mit dem RPS-Computer über ein USB-Kabel vor der Wahl der USB-Verbindungsmethode verbunden haben, wird in diesem Feld die COM-Schnittstelle für die USB-Verbindung angezeigt.
Verbinden	Mit einem Klick auf diese Schaltfläche stellen Sie eine Verbindung mit der Zentrale her.
Verbinden	Durch Klicken der Schaltfläche „Verbinden“ schließen Sie eine von der Zentrale initiierte Verbindung ab.

Feld/Schaltfläche	Beschreibung
Abbrechen (USB)	Klicken Sie auf „Abbrechen“, um das Fenster „Panel Communication“ (Anlagenverbindung) zu schließen. Wenn Sie zum Starten des Verbindungsprozesses auf „Verbinden“ geklickt haben, wird die Schaltfläche „Abbrechen“ zur Schaltfläche „Abbrechen“. Klicken Sie auf „Abbrechen“, um den Verbindungsprozess zu beenden.

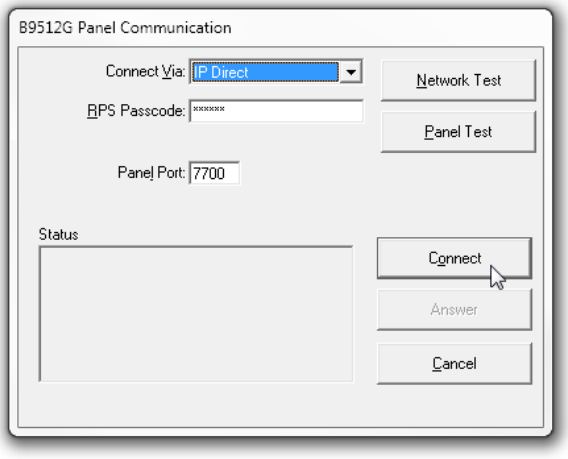
2.2.5 Verbinden über: Netzwerk



Feld/Schaltfläche	Beschreibung
Verbinden über [**Netzwerk**]	Wählen Sie die Verbindungsmethode, mit der RPS eine Verbindung mit der Zentrale herstellt.
RPS-Zugangscode	RPS zeigt Sternchen (*) für den Zugangscode aus dem Parameter „ZENTRALENÜBERGREIFENDE PARAMETER“ > „RPS-Parameter“ > „RPS-Zugangscode“ an. Wenn Sie einen anderen RPS-Zugangscode für diese Verbindung eingeben, wird dieser von RPS nicht gespeichert.
IP-Adresse/Hostname	In diesem Feld wird die IP-Adresse oder der Hostname aus der Ansicht der Zentralendaten angezeigt, IP-Adresse > HostName-Parameter.
Port Zentrale	In diesem Feld wird die Portnummer aus der Ansicht der Zentralendaten angezeigt, Feld „Port Zentrale“.
Status	In diesem Feld wird der Status des Verbindungsprozesses, einer Netzwerkprüfung oder Zentralenprüfung angezeigt.

Feld/Schaltfläche	Beschreibung
Netzwerkprüfung	Klicken Sie auf diese Schaltfläche, um eine Netzwerkprüfung zu starten. RPS sendet einen Ping an die Netzwerkschnittstelle der Zentrale. Wenn die Zentrale den Ping hört, sendet sie eine Antwort an RPS. Im Feld „Status“ wird das Ergebnis der Netzwerkprüfung angezeigt.
Zentralenprüfung	Klicken Sie auf diese Schaltfläche, um eine Zentralenprüfung zu starten. RPS sendet einen Ping an die Netzwerkschnittstelle der Zentrale. Wenn die Zentrale den Ping hört, sendet sie eine Antwort an RPS. Im Feld „Status“ wird das Ergebnis der Prüfung angezeigt.
Verbinden	Mit einem Klick auf diese Schaltfläche stellen Sie eine Verbindung mit der Zentrale her.
Verbinden	Durch Klicken der Schaltfläche „Verbinden“ schließen Sie eine von der Zentrale initiierte Verbindung ab.
Abbrechen	Klicken Sie auf „Abbrechen“, um das Fenster „Panel Communication“ (Anlagenverbindung) zu schließen. Wenn Sie zum Starten des Verbindungsprozesses auf „Verbinden“ geklickt haben, wird die Schaltfläche „Abbrechen“ zur Schaltfläche „Abbrechen“. Klicken Sie auf „Abbrechen“, um den Verbindungsprozess zu beenden.

2.2.6 Verbinden über: IP-Direktverbindung



Feld/Schaltfläche	Beschreibung
Verbinden über: [**IP-Direktverbindung**]	Wählen Sie die Verbindungsmethode, mit der RPS eine Verbindung mit der Zentrale herstellt.
RPS-Zugangscode	RPS zeigt Sternchen (*) für den Zugangscode aus dem Parameter „ZENTRALENÜBERGREIFENDE PARAMETER“ > „RPS-Parameter“ > „RPS-Zugangscode“ an. Wenn Sie einen anderen RPS-Zugangscode für diese Verbindung eingeben, wird dieser von RPS nicht gespeichert.
Port Zentrale	In diesem Feld wird die Portnummer aus der Ansicht der Zentralendaten angezeigt, Feld „Port Zentrale“.
Status	In diesem Feld wird der Status des Verbindungsprozesses, einer Netzwerkprüfung oder Zentralenprüfung angezeigt.
Netzwerkprüfung	Klicken Sie auf diese Schaltfläche, um eine Netzwerkprüfung zu starten. RPS sendet einen Ping an die Netzwerkschnittstelle der Zentrale. Wenn die Zentrale den Ping hört, sendet sie eine Antwort an RPS. Im Feld „Status“ wird das Ergebnis der Netzwerkprüfung angezeigt.
Zentralenprüfung	Klicken Sie auf diese Schaltfläche, um eine Zentralenprüfung zu starten. RPS sendet einen Ping an die Netzwerkschnittstelle der Zentrale. Wenn die Zentrale den Ping hört, sendet sie eine Antwort an RPS. Im Feld „Status“ wird das Ergebnis der Prüfung angezeigt.
Verbinden	Mit einem Klick auf diese Schaltfläche stellen Sie eine Verbindung mit der Zentrale her.
Verbinden	Durch Klicken der Schaltfläche „Verbinden“ schließen Sie eine von der Zentrale initiierte Verbindung ab.
Abbrechen	Klicken Sie auf „Abbrechen“, um das Fenster „Panel Communication“ (Anlagenverbindung) zu schließen. Wenn Sie zum Starten des Verbindungsprozesses auf „Verbinden“ geklickt haben, wird die Schaltfläche

Feld/Schaltfläche	Beschreibung
	„Abbrechen“ zur Schaltfläche „Abbrechen“. Klicken Sie auf „Abbrechen“, um den Verbindungsprozess zu beenden.

2.3 Verbindung mit der Zentrale trennen

Gehen Sie folgendermaßen vor, um die Verbindung zwischen RPS und einer Zentrale zu trennen:

1. Klicken Sie auf der Funktionsleiste auf „Trennen“.
2. Wählen Sie „Zentrale zurücksetzen“, um die Zentrale nach dem Trennen der Verbindung zurückzusetzen.
3. Klicken Sie zum Trennen der Verbindung auf „OK“.

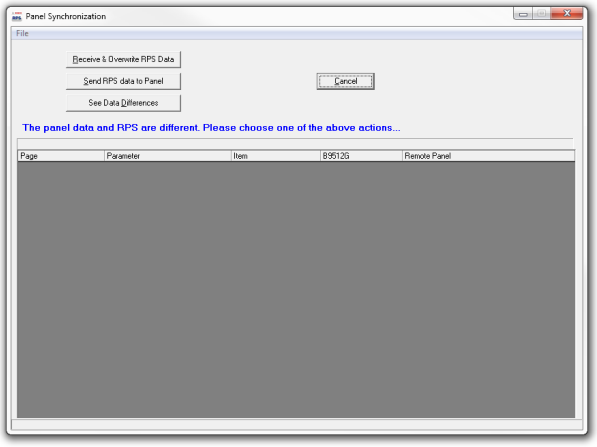
2.3.1 Fehlerhafte Terminierung

Wenn die Verbindung zwischen RPS und der Zentrale ausfällt, zeigt RPS eine Fehlermeldung an. Klicken Sie auf „OK“, um die Fehlermeldung zu löschen und fortzufahren. Überprüfen Sie die Parametrierung nach einer fehlerhaften Terminierung in der Zentrale auf beschädigte Daten. Siehe *Zentrale und RPS synchronisieren, Seite 26*.

2.4 Online-Vorgänge

2.4.1 Zentrale und RPS synchronisieren

Wenn RPS eine Verbindung zur Zentrale herstellt, vergleicht es die Daten in der Zentrale mit den Daten im RPS-Konto. Bei Unterschieden zwischen den Daten wird das Fenster „Zentralensynchronisation“ geöffnet.



Schaltfläche	Beschreibung
Receive and Overwrite RPS Data (RPS-Daten empfangen und überschreiben)	Klicken Sie auf diese Schaltfläche, um die Zentralenparameterdaten zu empfangen und die Parameterdaten im RPS-Konto zu überschreiben.
Send RPS Data to Panel (RPS-Daten an Zentrale senden)	Klicken Sie auf diese Schaltfläche, um die RPS-Parameterdaten an die Zentrale zu senden. Die Zentralendaten werden von den RPS-Daten überschrieben.

Schaltfläche	Beschreibung
See Data Differences (Datenunterschiede ansehen)	Klicken Sie auf diese Schaltfläche, um die Unterschiede zwischen den RPS-Zentralenparameterdaten (RPS-Konto) und den Zentralenparameterdaten anzuzeigen. Nachdem Sie die Unterschiede gesehen haben, können Sie die Zentralendaten empfangen und die RPS-Daten überschreiben, die RPS-Daten senden und die Daten in der Zentrale überschreiben oder abbrechen und keine Änderungen vornehmen.
Abbrechen	Klicken Sie auf diese Schaltfläche, um das Fenster „Zentralensynchronisation“ ohne Synchronisieren zu schließen.

2.4.2 Vergleichen

Sie können Zentralenkontoparameter nur zwischen Zentralen des gleichen Typs vergleichen. Beispiel: B5512 mit B5512

Klicken Sie auf der Symbolleiste auf das Symbol „Vergleichen“ , um die Inhalte zweier Zentralentypen miteinander zu vergleichen.
Das Fenster „Ziel auswählen“ wird geöffnet und listet Zentralenkonten desselben Typs in RPS auf. Wählen Sie die Zentrale aus, die Sie mit der gerade geöffneten Zentrale vergleichen möchten. Sie können mit dieser Funktion auch Vorlagen vergleichen.

Feld/Schaltfläche	Beschreibung
Zielinformationen	– Name: der Name des Zentralenkontos, wie er im Fenster „Panel Data-View“ (Zentralendaten – Anzeigen) angezeigt wird – Beschreibung: – die Beschreibung des Zentralenkontos, wie sie im Fenster „Panel Data-View“ (Zentralendaten – Anzeigen) angezeigt wird – Typ: erkennt, ob es sich beim gelisteten Konto um eine Zentrale oder eine Vorlage handelt
Öffnen	Klicken Sie auf diese Schaltfläche, um das Fenster „Vergleichen“ zu öffnen.
Abbrechen	Klicken Sie auf diese Schaltfläche, um dieses Fenster zu schließen und keine Vergleichssitzung zu starten.

Klicken Sie im Fenster „Select Target“ (Ziel auswählen) auf die Schaltfläche „Öffnen“, um eine Vergleichssitzung starten. Das Fenster „Vergleichen“ wird geöffnet.

Abbildung 2.1:

Feld/Schaltfläche	Beschreibung
Datei	Das Menü „Datei“ enthält eine Druckoption, mit der Sie die Ergebnisse einer abgeschlossenen Vergleichssitzung speichern oder drucken. Klicken Sie auf Datei > Drucken. Im daraufhin geöffneten Fenster „Compare Panels Report“ (Zentralenvergleichsprotokoll) erscheint eine Druckvorschau. Führen Sie in diesem Fenster eine Suche durch, speichern Sie das Dokument als Datei, oder passen Sie die Druckereinstellungen an.
Quelle/Ziel	– Quelle. Dieses schreibgeschützte Feld bezeichnet das Quellkonto, mit dem das Zielkonto verglichen wird. – Ziel. Im schreibgeschützten Feld steht das Zielkonto, mit dem das Quellkonto verglichen wird.
Begin Compare (Vergleich beginnen)	Klicken Sie auf diese Schaltfläche, um den Vergleich des Zielkontos mit dem Quellkonto zu starten.
Cancel Compare (Vergleich abbrechen)	Klicken Sie auf diese Schaltfläche, um eine bereits gestartete Vergleichssitzung abzubrechen. Vor Beginn und nach Abschluss einer Vergleichssitzung ist diese Schaltfläche inaktiv (grau).
Abgeschlossen	Klicken Sie auf diese Schaltfläche, um das Fenster „Vergleichen“ zu schließen, wenn Sie den Kontenvergleich abgeschlossen haben.
Ergebnisbereich	Wenn RPS Unterschiede zwischen dem Quellkonto und dem Zielkonto findet, werden die Ergebnisse der Vergleichssitzung in diesem Fenster angezeigt. Dieses Fenster bleibt leer, wenn RPS keine Unterschiede findet.

2.4.3 Suchen und ersetzen

RPS bietet die Möglichkeit, bestimmte Daten innerhalb einer Zentrale, einer Gruppe oder der gesamten Datenbank zu suchen und zu ersetzen.

Zum Suchen und/oder Ändern bestimmter Informationen in einer Zentrale, Gruppe oder Datenbank klicken Sie im Fenster „Zentralenansicht“auf der Symbolleiste auf das Symbol „Find/Replace“ (Suchen/Ersetzen) . Das Fenster „Find/Replace“ (Suchen/Ersetzen) wird geöffnet.

Feld/Schaltfläche	Beschreibung
Suchen nach	Geben Sie das Wort, den Ausdruck oder den Wert ein, den Sie suchen.
Replace with (Ersetzen durch)	Geben Sie das Wort, den Ausdruck oder Wert ein, um den im Feld „Suchen nach“ eingegeben Eintrag zu ersetzen.
Match case (Groß-/Kleinschreibung beachten)	Durch Markieren dieses Felds wird bei der Suche die Groß-/Kleinschreibung beachtet.
Suchen	Mit einem Klick auf diese Schaltfläche starten Sie die Suche.
Ersetzen	Mit dieser Schaltfläche ersetzen Sie ein Element, wenn eine Übereinstimmung gefunden wurde.
Abbrechen	Klicken Sie auf diese Schaltfläche, um das Fenster zu schließen.

Mit der Funktion „Find/Replace“ (Suchen/Ersetzen) kann nicht global gesucht oder ersetzt werden. Wenn Sie z. B. einen „Ja“-Eintrag finden und ihn durch einen „Nein“-Eintrag ersetzen möchten, ändert die Funktion „Find/Replace“ (Suchen/Ersetzen) ein Feld nach dem anderen. Die Einstellungen für einige Parameter können nicht unabhängig von anderen Parametern vorgenommen werden. Die Funktion „Suchen/Ersetzen“ wird keine Änderungen an diesen Parametern vornehmen.

2.4.4 Sicherheit

Standardeinstellung: 5
Auswahl: 0 bis 15
Mit dieser Funktion wird der Zugriff auf bestimmte Parameter beschränkt.
Die Sicherheitsstufen sind von 0 bis 15 durchnummeriert. „0“ steht dabei für die niedrigste Sicherheitsstufe (keine Berechtigung), während der Wert „15“ die höchste Sicherheitsstufe (vollständiger Zugriff auf alle Parameter) darstellt.
Jedem Parameter sind Sicherheitsstufen zugewiesen. Wenn eine Sicherheitsstufe einem Parameter zugewiesen ist, können nur Bediener mit mindestens der Sicherheitsstufe des Parameters den Paramater ansehen oder bearbeiten.

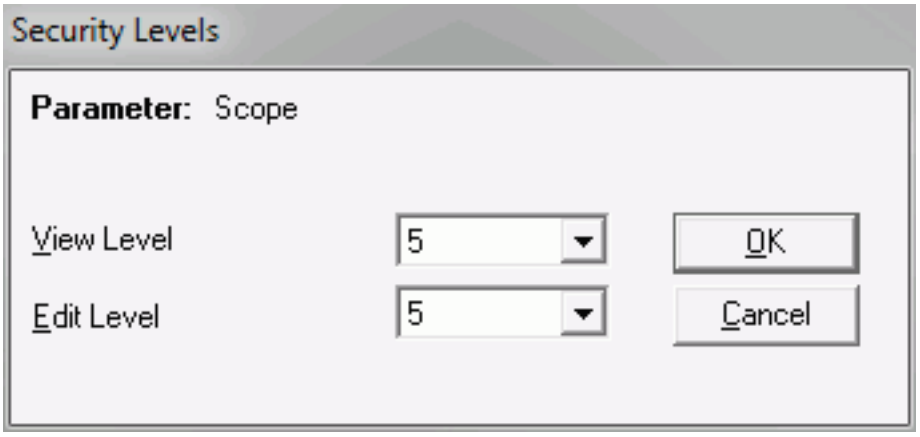
Beispiel
Unternehmen A hat die Sicherheitsstufe für die Benutzerzuordnungen (Zugangscodes) folgendermaßen festgelegt:
Anzeigestufe = 10
Bearbeitungsstufe = 14

Joe hat die Sicherheitsstufe 15. Wenn er diese Zentrale in RPS öffnet, sieht er die Zugangscodes aller Benutzer (ANSICHT), die im Parameter Benutzerzuordnungen > Zugangscodes aufgelistet sind, weil seine Sicherheitsstufe über der Sicherheitsstufe 10 liegt. Joe kann ebenfalls den Zugangscode eines Benutzers ändern (BEARBEITEN), weil er mindestens die Sicherheitsstufe 14 hat.
Robert hat die Sicherheitsstufe 5. Er kann keine Zugangscodes von Benutzern BEARBEITEN, da hierfür die Sicherheitsstufe 10 erforderlich ist. Auch sind die Zugangscodes der Benutzer für Robert nicht sichtbar, da seine Sicherheitsstufe unterhalb der Sicherheitsstufe 10 (Mindestvoraussetzung für ANSICHT) liegt.

Klicken Sie auf der Symbolleiste auf das Symbol „Sicherheit“ , oder klicken Sie auf Bearbeiten > Sicherheit, um die erforderliche Mindestsicherheitsstufe für den Zugriff auf Parameter für diese Zentrale und alle anderen Zentralen dieses Typs festzulegen. Die Sicherheitsfunktion wird aktiviert und bereitet alle RPS-Parameter darauf vor, Änderungen der Sicherheitsstufen zu erlauben.

Gehen Sie folgendermaßen vor, um die Sicherheitsstufe für einen bestimmten Parameter zu ändern:

1. Suchen Sie den Parameter mithilfe des Menübaums „RPS“.
2. Klicken Sie einmal auf eine beliebige Zelle innerhalb der Zeile des gewünschten Parameters.
3. Drücken Sie [F5]. Das Dialogfeld „Security Levels “ (Security Levels) wird geöffnet.



1. Klicken Sie auf die Pfeile, und wählen Sie in den Dropdown-Tabellen die für diesen Parameter gewünschten Sicherheitsstufen aus.
2. Klicken Sie zum Schluss auf die Schaltfläche „OK“.

Zum Speichern der neuen Sicherheitseinstellungen und Deaktivieren der Sicherheitsfunktion verfahren Sie wie folgt:
Klicken Sie auf der Symbolleiste auf das Symbol „Sicherheit“. RPS speichert die neuen Einstellungen auf dem aktuellen Computer im Ordner „PegDef“ in der Datei „.peg.Security“.

Hinweis!
Aktualisierte Sicherheitsstufeneinstellungen gelten NUR für die aktuelle Arbeitsstation. Auf dieser Arbeitsstation gespeicherte Sicherheitsstufen haben keinen Einfluss auf andere Arbeitsstationen. Zum Anwenden dieser Einstellungen auf alle Arbeitsstationen kopieren Sie den Ordner „PegDef“ mit den neuen Sicherheitsstufen und importieren Sie es auf allen Arbeitsstationen in den Ordner „RPS“.

2.4.5 Send/Receive (Senden/Empfangen)

Mit dieser Funktion werden Daten an die Zentrale gesendet oder von ihr empfangen.

Wenn Sie auf das Symbol „Send/Receive“ (Senden/Empfangen) klicken, wird das Fenster „Zentralensynchronisation“ geöffnet.
Sind die Daten in RPS und der Zentrale synchronisiert (matfch), wird das Fenster „Zentralensynchronisation“ nicht geöffnet.

Schaltfläche	Beschreibung
Receive Panel Data (Zentralendaten empfangen)	Zum Empfangen der Zentralendaten – entweder um die Unterschiede zwischen dem Programm der Zentrale und dem Programm von RPS anzusehen oder das Programm von RPS durch das Programm der Zentrale zu ersetzen – klicken Sie auf „Receive Panel Data“ (Zentralendaten empfangen) und dann auf „OK“. Nach dem Empfangen wird das Fenster „Panel Update“ (Zentralenaktualisierung) geöffnet. Siehe Fenster „Panel Update“ (Zentralenaktualisierung).
Send only updated RPS data to panel (Nur aktualisierte RPS-Daten an die Zentrale senden)	Wählen Sie diese Option, wenn Sie die Zentrale zum ersten Mal kontaktieren und die Parametrierungsinformationen senden möchten, oder wenn Sie Änderungen am Programm durchgeführt haben und diese Änderungen auch in der Zentrale übernommen werden sollen. Klicken Sie dann auf „OK“. **WICHTIGE**: Bei einigen Control Panels ist die Möglichkeit, Daten an die Zentrale zu senden, aufgrund von Programmeinträgen eingeschränkt.
Send all RPS data to panel (Alle RPS-Daten an Zentrale senden)	Wählen Sie diese Option, wenn Sie alle RPS-Daten (einschließlich unveränderter Daten) an die Zentrale senden möchten. **WICHTIG**: Diese Option steht auch im bedienungsfreien Modus zur Verfügung.
No update (Keine Aktualisierung)	Wenn Sie weder RPS noch die Zentrale aktualisieren möchten, klicken Sie auf „No Update“ (Keine Aktualisierung) und dann auf „OK“. Dieses Fenster wird dann geschlossen, und Sie können andere Online-Vorgänge starten. **WICHTIG**: Wenn Sie auf einigen Control Panels „No Update“ (Keine Aktualisierung) auswählen, wird ein zusätzliches Fenster „Abort Synchronization“ (Synchronisierung abbrechen) mit dem Hinweis angezeigt, dass die Diagnose

Schaltfläche	Beschreibung
	möglicherweise nicht genau ist. Führen Sie „Receive“ (Empfangen) aus, und speichern Sie anschließend alle Änderungen, oder führen Sie vor der Diagnose „Send“ (Absenden) aus.
Enable exclusive mode (Exklusivmodus aktivieren)	Mit dem „Exclusive Mode“ (Exklusivmodus) wird die Übertragung großer Datenmengen beschleunigt. Verwenden Sie diesen Modus für langsamere Verbindungen. **Warnung**: Dieser Modus versetzt die Zentrale in einen ähnlichen Bedienmodus wie nach Aktivierung des Stand-by-Schalters der Zentrale.
Critical differences (Kritische Unterschiede)	Diese Liste erleichtert das Erkennen von Änderungen an allen Konfigurationsleistungsmerkmalen, die sich auf das erneute Verbinden mit RPS, das Senden von Protokollen an einen Bedienteilempfänger oder das Erteilen des Benutzerzugriffs auf die Räume auswirken können. Weitere Informationen entnehmen Sie der unten stehenden Unterschiedstabelle.
OK	Klicken Sie auf diese Schaltfläche, um die Auswahl bzw. den Eintrag zu übernehmen, und schließen Sie das Fenster.
Abbrechen	Über diese Schaltfläche schließen Sie dieses Fenster ohne die Übernahme einer Auswahl oder eines Eintrags.

2.4.6 Hintergrundspeicher anzeigen

2.4.7 Get history (Hintergrundspeicher abrufen)

2.4.8 Diagnose

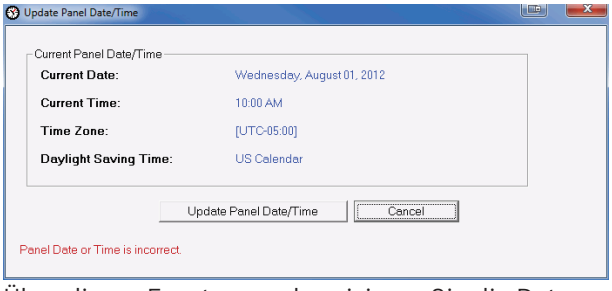
Klicken Sie auf das Symbol „Diagnose“ , um Diagnoseinformationen anzuzeigen und einige Zentraleneinstellungen zu ändern. Der Bildschirm „Diagnose“ wird mit dem aktiven Bildschirm „Zentrale“ geöffnet.
Der Menübaum auf der linken Seite des Fensters führt die verfügbaren Diagnosebildschirme auf. Im Menübaum rot dargestellte Module weisen Störungen auf. Klicken Sie auf den Modulnamen, schauen Sie sich den entsprechenden Modulbildschirm an, und führen Sie die für die Behebung der Störung erforderlichen Schritte aus. Diese Bildschirme enthalten Informationen zum Betriebszustand der Zentrale. Verwenden Sie die Bildschirme für die Diagnose von Problemen im Feld oder für das Überprüfen des Betriebszustands neu installierter Geräte usw.
HINWEIS: Das Fenster „Diagnose“ enthält möglicherweise unterschiedliche Zentralenversionen.

Datum und Uhrzeit aktualisieren

Wenn Sie im Bildschirm „Zentralendiagnose“ auf die Schaltfläche „Datum/Uhrzeit“ klicken, wird das Fenster „Update Panel Date/Time“ (Datum/Uhrzeit der Zentrale aktualisieren) geöffnet. Über dieses Fenster synchronisieren Sie die Datums- und Uhrzeiteinstellungen der Zentrale mit den RPS-Computereinstellungen. Siehe *Datum/Uhrzeit der Zentrale aktualisieren, Seite 33*, um weitere Informationen zu erhalten.

2.4.9 Datum/Uhrzeit der Zentrale aktualisieren

Wenn Sie im Bildschirm „Panel Diagnostics“ (Zentralendiagnose) auf die Schaltfläche „Datum/Uhrzeit“ klicken, wird das Fenster „Update Panel Date/Time“ (Datum/Uhrzeit der Zentrale aktualisieren) geöffnet.



Über dieses Fenster synchronisieren Sie die Datums- und Uhrzeiteinstellungen der Zentrale mit den RPS-Computereinstellungen.

RPS fragt das aktuelle Datum und die aktuelle Uhrzeit von der Zentrale ab. Außerdem fragt es den Beginn der Sommerzeit sowie die Zeitzonenwerte von der Zentrale ab und berechnet Datum und Uhrzeit neu. RPS sendet das neue Datum und die neue Uhrzeit an die Zentrale. Die aktualisierte Uhrzeit wird im 24-Stunden-Format angezeigt. Die Uhrzeit wird in Stunden und Minuten ohne Berücksichtigung von Sekunden angezeigt.

Eine von drei verschiedenen Statusmeldungen (roter Text am unteren Ende des Dialogfelds) wird eingeblendet.

- Datum und Uhrzeit der Zentrale können nicht aktualisiert werden, wenn RPS und Zentralenkonfiguration nicht synchronisiert sind.
- Datum oder Uhrzeit der Zentrale ist nicht korrekt.
- Datum und Uhrzeit der Zentrale sind korrekt.

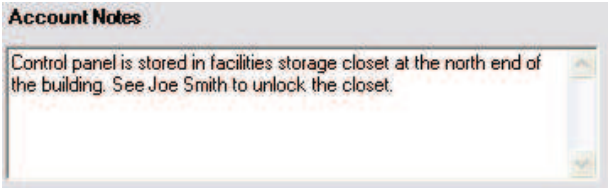
Hinweis!

Wenn die automatische Aktualisierung aktiviert ist, wird möglicherweise verhindert, dass Sie Datum und Uhrzeit der Zentrale einstellen.

2.4.10 Kontohinweise

Klicken Sie auf der Symbolleiste auf das Symbol „Account Notes“ (Kontohinweise) , um Kontohinweise, Warnungen, Erinnerungen oder andere Hinweise für andere Benutzer zu hinterlassen.

Wenn das Fenster „Account Notes“ (Kontohinweise) geöffnet wird, geben Sie eine Nachricht ein und klicken dann auf „OK“.



2.4.11 Firmware-Aktualisierung

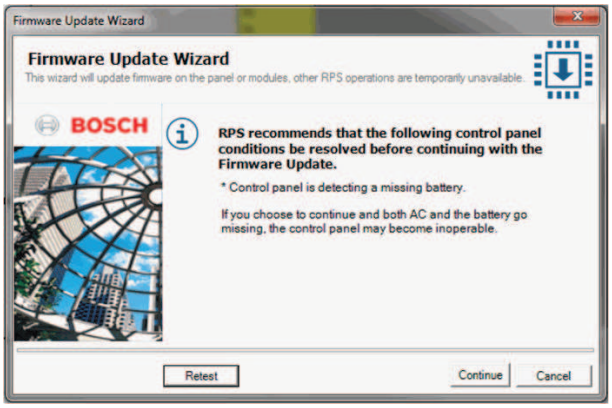
Mit dem RPS-Firmware-Update-Assistenten aktualisieren Sie die Zentralenfirmware per Fernzugriff.

1. Klicken Sie im Fenster „Penal View“ (Zentralenansicht) auf der Symbolleiste auf das Symbol „Verbinden“, um eine Verbindung mit der Zentrale herzustellen. Das Dialogfeld „Panel Communication“ (Anlagenverbindung) wird geöffnet. Füllen Sie die Felder aus, und klicken Sie im Dialogfeld dann auf die Schaltfläche „Verbinden“.
2. Klicken Sie auf das Symbol „Firmware Update Wizard“ (Firmware Update-Assistent) .
3. Der Firmware-Assistent wird im Begrüßungsbildschirm geöffnet. Klicken Sie auf „Fortfahren“.

Hinweis!
Findet der Firmware Update-Assistent in der Datenbank keine Firmware-Aktualisierungsdatei, werden in der Systemkonfiguration Anweisungen für den Zugriff auf die Registerkarte „Firmware-Dateien“ angezeigt, um Firmware-Aktualisierungsdateien zu importieren. Anschließend werden Sie aufgefordert, den Assistenten zu schließen.
Weitere Informationen zur Verwendung der Registerkarte „Firmware Files“ (Firmware-Dateien) finden Sie in der allgemeinen Hilfe unter .

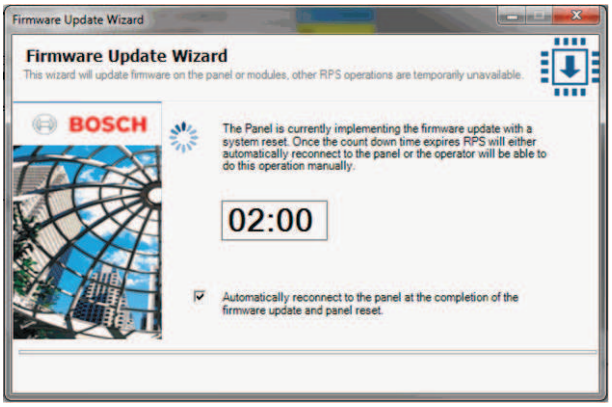
4. Der Bildschirm „Available Firmware “(Verfügbare Firmware) erscheint. Die aufgeführte Firmware enthält die aktuellen und neueren Firmware-Dateien für die Zentrale, mit der RPS verbunden ist. Firmware-Dateien, die älter als die in der verbundenen Zentrale verwendete Firmware sind, werden nur aufgeführt, wenn eine Installation der älteren Firmware möglich ist.
   Wählen Sie in der Liste der verfügbaren Dateien die Firmware-Aktualisierungsdatei, und klicken Sie auf „Fortfahren“.
5. Der Assistent führt eine Reihe von Überprüfungen durch:
   Netzstatus: Wenn ein Stromausfallereignis erkannt wird, beschreibt der Assistent mögliche Gefahren beim Fortsetzen des Vorgangs. Sie haben die Möglichkeit, die Überprüfung nochmals durchzuführen, den Vorgang abzubrechen oder fortzufahren.
   Batteriestatus: Wenn eine Batterie fehlt, beschreibt der Assistent mögliche Gefahren beim Fortsetzen des Vorgangs. Sie haben die Möglichkeit, die Überprüfung nochmals durchzuführen, den Vorgang abzubrechen oder fortzufahren.
   Bereichsstatus: Wenn scharfgeschaltete Bereiche erkannt werden, fordert Sie der Assistent dazu auf, alle Bereiche unscharfzuschalten. Sie können eine erneute Prüfung durchführen oder den Assistenten abbrechen.
   Version der Firmware-Aktualisierungsdatei. Wenn die gewählte Firmware-Version älter als die Version der Zentralen-Firmware ist, brechen Sie entweder ab oder fahren mit der älteren Version fort.

Hinweis!
Wenn RPS während der Überprüfungen beendet wird, erscheint der Warnhinweis „Could not update firmware” (Firmware konnte nicht aktualisiert werden). Schließen Sie den Assistenten, und starten Sie den Firmware- Aktualisierungsvorgang erneut.
Bei anderen Fehlermeldungen: Schließen Sie den Assistenten, beheben Sie das Problem, und starten Sie den Firmware-Aktualisierungsvorgang erneut.



6. Nachdem Sie eine Firmware-Datei ausgewählt und auf „Fortfahren“ geklickt haben, bietet der Assistent die Option, nach der Firmware-Aktualisierung automatisch eine erneute Verbindung mit der Zentrale herzustellen.
7. Nach den Überprüfungen wird die Aktualisierung fortgeführt und ein Bildschirm mit wichtigen Hinweisen angezeigt. Markieren Sie das Bestätigungskästchen, und klicken Sie auf „Fortfahren“.

8. Falls eine Autorisierung für Firmware-Aktualisierungen vor Ort erforderlich ist (siehe *On Site Authorization for Firmware Update (Vor-Ort-Autorisierung für Firmware-Aktualisierung), Seite 106*), wird ein Bildschirm mit dem Hinweis geöffnet, dass RPS auf die lokale Firmware-Autorisierung wartet. Wenn eine Vor-Ort-Autorisierung nicht erforderlich ist (oder bereits gewährt wurde), erscheint die Meldung „Sending the firmware” (Firmware wird gesendet) unter Angabe des Vorgangsfortschritts.
9. Nachdem der Assistent die Aktualisierung beendet hat, wird der Bildschirm „Zurücksetzen des Systems“ angezeigt. Markieren Sie das Kontrollkästchen „Automatically Reconnect“ (Automatische Wiederherstellung der Verbindung), und klicken Sie auf „Fortfahren“.



10. Nach Ablaufen des Zeitschalters öffnet RPS automatisch das Verbindungsdialogfeld und stellt die Verbindung erneut her. Im Fenster „Zentrale“ erkennen Sie auf der Titelleiste, ob die Zentrale die richtige Firmware ausführt. Die Firmware-Version steht direkt hinter der Überschrift „Panel View“ (Zentralenansicht).

2.5 Online-Diagnose – System

2.5.1 Panel diagnostics (Zentralendiagnose)

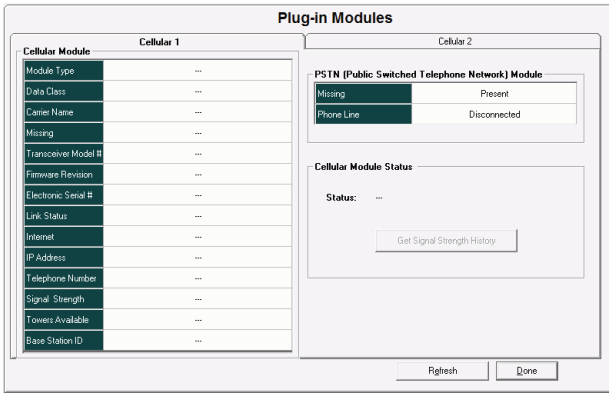
2.5.2 Integrierte IP-Adresse – Diagnose

Im Fenster „On-board IP“ (Integrierte IP-Adresse) wird der Status des Übertragungsgeräts für die integrierte IP-Adresse der Zentrale angezeigt.

Feld	Beschreibung
Link Status (Verbindungsstatus)	Informiert über den Status der Ethernet-Verbindung („OK“/„Fehler“)
Hostname (Hostname)	Gibt den Hostnamen des Übertragungsgeräts für die integrierte IP-Adresse an.
MAC-48 Address (MAC-48-Adresse)	Zeigt die ab Werk eingestellte MAC-48-Adresse an, mit der die Zentrale im Netzwerk eindeutig identifiziert wird.
DNS Status (DNS-Status)	„Fehler“ wird angezeigt, wenn die Zentrale den Hostnamen nicht in eine IP-Adresse (Fehler beim Durchführen eines DNS-Lookup) konvertieren kann.
IP-Adresse	Zeigt die von DHCP zugewiesene IP-Adresse an. Ist DHCP deaktiviert, wird die eingegebene IP-Adresse angezeigt.
LAN Status (LAN-Status)	Dieses Feld informiert über den Verbindungsstatus („OK“/„Fehler“) im lokalen Netzwerk (LAN). „OK“ bedeutet, dass die Zentrale das Gateway anpingen kann.
WAN Status (WAN-Status)	In diesem Feld wird der Verbindungsstatus („OK”/„Fehler”) im Wide Area Network (WAN) angezeigt. „OK“ bedeutet, dass die Zentrale die eingegebene IPv4- oder IPv6-Testadresse anpingen kann ...

Feld	Beschreibung
UPnP	Wenn das lokale IP-Netzwerk einen WAN-IP-Verbindungsdienst enthält, gibt diese Zeile den Status „OK“/„Fehler“ einer Verbindung zwischen einem externen und einem internen Gerät an. Wird eine Fehler erkannt, bedeutet dies, dass das lokale IP-Netzwerk keinen WAN-IP-Verbindungsdienst unterstützt oder die Nummer des konfigurierten lokalen Ports von einem anderen Gerät verwendet wird.

2.5.3 Steckplatinendiagnose



Zeilen des Telefon-Moduls

Zeile	Beschreibung
Fehlt	In dieser Zeile steht der Status der Telefon-Steckplatine. – Fehlt (kein Modul eingesteckt, aber Modul wird erwartet) – Vorhanden (Ein erwartetes oder nicht erwartetes gültiges Modul ist eingesteckt.) – Ungültig (Ein Modul ist eingesetzt, wird aber nicht erkannt, ist defekt, oder es liegt ein falscher Modultyp vor.) – ---- (Kein Modul ist eingesetzt, und es wird kein Modul erwartet.)
Telefonleitung	Diese Zeile enthält den Status des öffentlichen Telefonanschlusses. – Verbunden/OK (Die Telefonleitung wird überwacht und ist einsatzbereit.) – Getrennt/Fehler (Die Telefonleitung wird überwacht, ist aber nicht betriebsbereit.) – ---- (Die Telefonleitung wird nicht überwacht, oder ein Telefon-Modul ist nicht eingesteckt.)

Zeilen des Mobilfunkmoduls

Zeile	Beschreibung
Modultyp	In dieser Zeile steht der Typ des verwendeten Mobilfunkmoduls.

Zeile	Beschreibung	
Datenklasse	Diese Zeile informiert über die Datenklasse der aktuellen Verbindung.	
	B440	1xRTT, 3G
	B441	1xRTT
	B442	GPRS
	B443	GPRS, EDGE, WCDMA oder HSPA
	B444	4G LTE
	B444 A/V (AT&T/Verizon)	4G LTE (V) 4G LTE/3G HSPA+ (A)
	Unbekannt	Das Modem gibt einen unbekannten Wert zurück.
	Hinweis: Dieses Diagnosefeld ist nur für Zentralen der B-Series v2. 03 oder höher verfügbar. Bei allen anderen Zentralen werden Striche angezeigt.	
Name des Anbieters	In dieser Zeile wird der Name des Mobilfunkanbieters aufgeführt. B440/B441: zeigt „HOME“ oder „ROAMING“ an B442/443/444: gibt den Namen des Anbieters (bis zu 16 Zeichen lang) an	
Fehlt	In dieser Zeile steht der Status der Mobilfunk-Steckplatine. – Fehlt (kein Modul eingesteckt, aber Modul wird erwartet) – Vorhanden (Ein erwartetes oder nicht erwartetes gültiges Modul ist eingesteckt.) – Ungültig (Ein Modul ist eingesetzt, wird aber nicht erkannt, ist defekt, oder es liegt ein falscher Modultyp vor.) – ---- (Kein Modul ist eingesetzt, und es wird kein Modul erwartet.)	
Transceiver-Modellnummer	Diese Zeile enthält die Transceiver-Modellnummer. Wenn das Mobilfunkmodul ausfällt oder keine Modellnummer erkannt wurde, erscheint „Failed“ (Fehler).	
Firmware Verision	Hier wird die Nummer der aktuellen Firmware-Version angezeigt.	
Elektronische Seriennummer	Diese Zeile enthält die ID-Nummer des Mobilfunkmoduls.	
Verbindungsstatus	In diesem Feld steht der Status der Verbindung zum Mobilfunknetz.	
Internet	Dieses Feld gibt den Internet-Verbindungsstatus an.	
IP-Adresse	In diesem Feld steht die aktuelle IP-Adresse.	

Zeile	Beschreibung
Telefon	In dieser Zeile steht die Telefonnummer. Wenn das Mobilfunkmodul nicht aktiviert wurde, wird die Telefonnummer im Format „000000 + vier Ziffern“ angezeigt. Hinweis: Die B444 A-Version (AT&T) zeigt die Zielrufnummer nicht an. Mobilfunkrückruf wird nicht unterstützt.
Signalstärke	Diese Zeile informiert über den Status der Signalstärke.
Verfügbare Funkmasten	Diese Zeile nennt die Anzahl der für die Kommunikation zur Verfügung stehenden Funkmasten.
Basisstations-ID	In dieser Zeile wird die Identifikationsnummer der Basisstation angegeben.

Signalstärkeverlauf abrufen

Klicken Sie auf diese Schaltfläche, um ein Protokoll mit dem Verlauf der Signalstärke des mit dem Funkmast verbundenen Mobilfunkmoduls zu erstellen. Das Protokoll wird direkt unter „C:\RPS\Logs“ gespeichert.

Die Datei wird als .csv-Datei gespeichert, deren Name den Zeitstempel enthält. (Beispiel: 09-28-20121.39PM.csv)

Die Protokolldatei gibt die durchschnittliche Signalstärke für jedes 15-Minuten-Intervall der vergangenen 48 Stunden an.

	A	B	C
1	Date/Time	Strength Level	Signal
2	9/26/2012 13:39	12	Very Good 0
3	9/26/2012 13:54	14	Very Good 2
4	9/26/2012 14:09	10	Good 2
5	9/26/2012 14:24	14	Very Good 2
6	9/26/2012 14:39	14	Very Good 2
7	9/26/2012 14:54	12	Very Good 0
8	9/26/2012 15:09	14	Very Good 2
9	9/26/2012 15:24	14	Very Good 2
10	9/26/2012 15:39	14	Very Good 2
11	9/26/2012 15:54	14	Very Good 2
12	9/26/2012 16:09	14	Very Good 2
13	9/26/2012 16:24	14	Very Good 2
14	9/26/2012 16:39	14	Very Good 2
15	9/26/2012 16:54	14	Very Good 2

Die Signalstärke wird in Form der folgenden Kategorien angegeben: Kein Signal, Schlecht, Minimal, Gut oder Sehr gut.

Strength Level	Signal
0	No Signal
1	Bad 0
2	Bad 1
3	Bad 2
4	Marginal 0
5	Marginal 1
6	Marginal 2
7	Marginal 2
8	Good 0
9	Good 1
10	Good 2
11	Good 3
12	Very Good 0
13	Very Good 1
14	Very Good 2
15	Very Good 3

2.6 Parametrierhinweise

Hinweis!

Führen Sie nach der Systeminstallation oder der Parametrierung der Zentrale einen umfassenden Systemtest durch.

Prüfen Sie die Zentrale, alle Geräte und die Datenübertragung (gesendete Protokolle an das Bedienteil und persönliche Benachrichtigungen).

3 Konformitätseinstellungen

3.1 SIA CP-01–Verifizierung

Standardeinstellung: Nein

Auswahl:

– Ja: RPS untersucht die Einstellungen der Zentralenkontoparameter auf Konformität mit SIA CP-01.

– Nein: RPS führt keine Konformitätsprüfung für Parameter durch.

RPS überprüft die folgenden Parameter auf Konformität mit SIA CP-01:

Bedrohungstyp, Seite 104

Alarm-Signalgeber, Seite 165

Scharfschalteverzögerungszeit, Seite 126

Burg Time (Einbruchalarmzeit), Seite 133

Warnung Scharfschalteverzögerungszeit, Seite 141

Warnung Eintrittsverzögerung, Seite 141

Eingangsverzögerung, Seite 238

Benutzercodelänge, Seite 110

Remote Warning (Remote-Warnung), Seite 111

Anzahl der Mehrfachauslösungsumgehungen, Seite 111

Abbruchsprotokoll, Seite 105

Zwei-Mann-Regel?, Seite 131?

Zweimalige Authentifizierung?, Seite 132?

Unverzögerte Vollscharfschaltung, Seite 194

Unverzögerte Außenhautüberwachung, Seite 194

Passcode Enter Function (Zugangscode-Eingabefunktion), Seite 147

Melde-Adresse des Menüs „RPS“

Compliance Verification > SIA CP-01 Verification (Konformitätsbestätigung > SIA CP-01-Verifizierung)

3.2 ULC-Konformität

Standardeinstellung: Nein

Auswahl:

– Ja: Zentralenbetrieb für Konformität mit UL Kanada (ULC) anpassen

– Nein: Zentralenbetrieb nicht für Konformität mit UL Kanada (ULC) anpassen

Wird dieser Parameter auf „Ja“ gesetzt, ignoriert die Zentrale beim Systemstart Dateneingänge aller Melder mindestens 120 Sekunden lang.

Beim Start der Sensorverarbeitung meldet die Zentrale ein einmaliges Ereignis, bevor Melderereignisse protokolliert werden. Darüber hinaus werden durch die Stromversorgung ausgelöste Ereignisse nur dann gemeldet, wenn die Störung nicht innerhalb der Verzögerungszeit von 120 Sekunden behoben werden kann.

Melde-Adresse des Menüs „RPS“

Compliance Settings > ULC Compliance (Konformitätseinstellungen > ULC-Konformität)

3.2.1 Konformität mit CAN/ULC-S304

CAN/ULC-S304 – SIGNALEMPFANGSZENTRUM UND GEBÄUDEEINBRUCHALARMZENTRALEN

Diese Norm deckt Konstruktions- und Leistungsanforderungen für Auswerteeinheiten und Zubehör für Einbruchmeldeanlagen ab. Eingeschlossen sind Auswerteeinheiten für geschützte Räume und Zubehör für lokale Verbindungen oder Verbindungen mit dem

Signalempfangszentrum sowie Alarmempfangsgeräte für das Alarmempfangszentrum (einschließlich Aufzeichnungsgeräten). Diese Geräte sind für den Einsatz in Räumen, Safes und Schließfächern vorgesehen.

Anforderungen zur Zentralenparametrierung
Zur Gewährleistung von Konformität mit CAN/ULC-S304 ist das Setzen des Parameters „ULC Compliance“ (ULC-Konformität) auf „Ja“ die entscheidende Zentralenparametrierungsanforderung.

3.2.2 CAN/ULC-S559 – erforderliche Parametrierung

CAN/ULC S559 – Grundausstattung für Brandsignalempfangszentren und -systeme
CAN/ULC-S559 enthält die Anforderungen an Brandsignalempfangszentren und -systeme, einschließlich Übertragungs- und Empfangsgeräten, proprietären Geräten für das Brandsignalempfangszentrum sowie Zubehör für die Auswerteeinheit. Systeme des Brandsignalempfangszentrums enthalten eine Einheit für geschützte Gebäude und Empfänger für gewöhnliche (nicht gefährliche) Innen- und Außenbereiche. Parametriermethoden sowie Prüf-, Service- und andere Software, die für die Verwendung von Geräten für Brandsignalempfangszentren und -systeme vorgesehen ist, sind in der Auswertung der Geräte enthalten. Signalempfangseinheiten, die in Brandsignalempfangszentren, Satellitenzentren, Signalverarbeitungszentren und Überbrückungszentren Anwendung finden, sind ebenfalls von den Anforderungen dieser Norm abgedeckt.

COMPLIANCE SETTINGS > UL Canada Compliance (KONFORMITÄTSEINSTELLUNGEN > UL Kanada-Konformität)
Setzen Sie den Parameter „COMPLIANCE SETTINGS > UL Canada Compliance“ (KONFORMITÄTSEINSTELLUNGEN > ULC Kanada-Konformität) auf „Ja“.

PANEL WIDE PARAMETERS > Report Routing (ZENTRALENÜBERGREIFENDE PARAMETER > Protokoll-Routing)
Spalte „Zielgruppe 4“:
- Setzen Sie „Feuerprotokolle“, „Gas Reports“ (Gasprotokolle), „Einbruchprotokolle“, „Personal Emergency Reports“ (Personennotfall-Protokolle), „Benutzerprotokolle“ und „Prüfprotokolle“ auf „Nein“.
- Setzen Sie „Output Reports“ (Ausgangsprotokolle), „Autofunktionsprotokolle“, „Melderprotokolle“ „Benutzeränderungsprotokolle“ und „Zutrittsprotokolle“ auf „Nein“.
- Stellen Sie sicher, dass der Menüeintrag „Diagnoseprotokolle“ auf „Benutzerdefiniert“ eingestellt ist. Im Folgenden werden die benutzerdefinierten Einstellungen konfiguriert.

PANEL WIDE PARAMETERS > Report Routing > Fire Reports > Fire Cancel (ZENTRALENÜBERGREIFENDE PARAMETER > Protokoll-Routing > Feuerprotokolle > Feuer Abbrechen)
Setzen Sie den Parameter „PANEL WIDE PARAMETERS > Report Routing > Fire Reports > Fire Cancel“ (ZENTRALENÜBERGREIFENDE PARAMETER > Protokoll-Routing > Feuerprotokolle > Feuer Abbrechen) für jede Zielgruppe (1 bis 4) auf „Nein“.

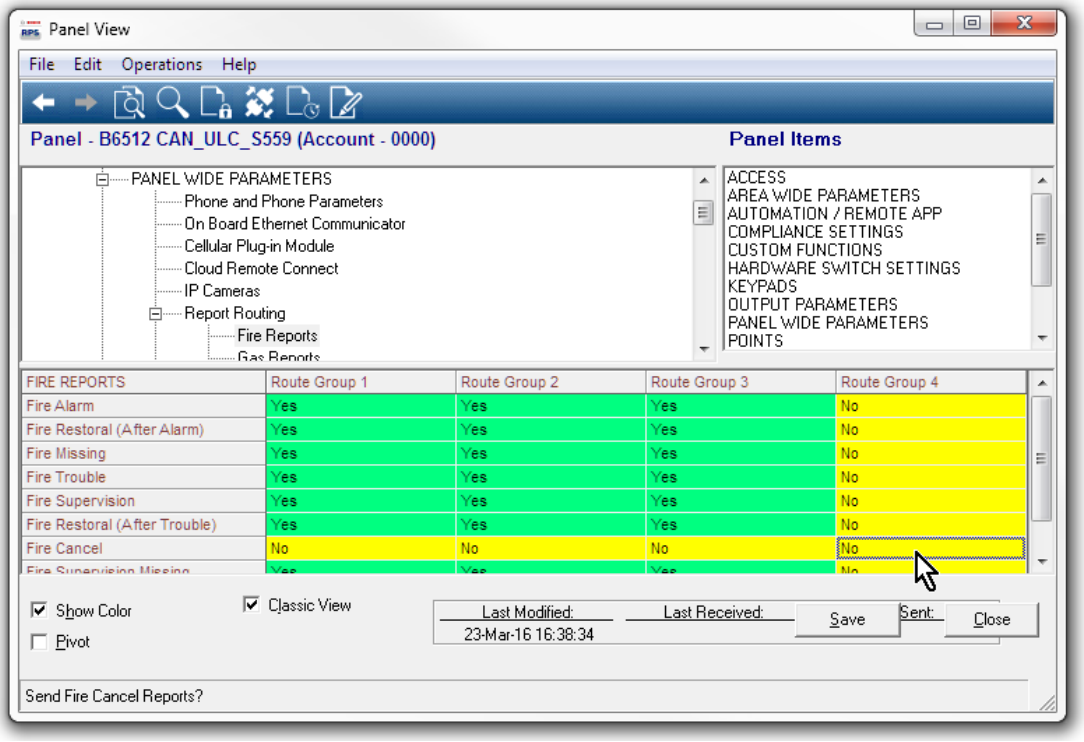


Abbildung 3.1: Feuer Abbrechen

PANEL WIDE PARAMETERS > Report Routing > Diagnostic Reports (ZENTRALENÜBERGREIFENDE PARAMETER > Protokoll-Routing > Diagnoseprotokolle)
Setzen Sie in der Spalte „Zielgruppe 4“ „SDI2 Device Failure“ (Fehler des SDI2-Geräts) auf „Ja“. Setzen Sie die übrigen Protokolle auf „Nein“.

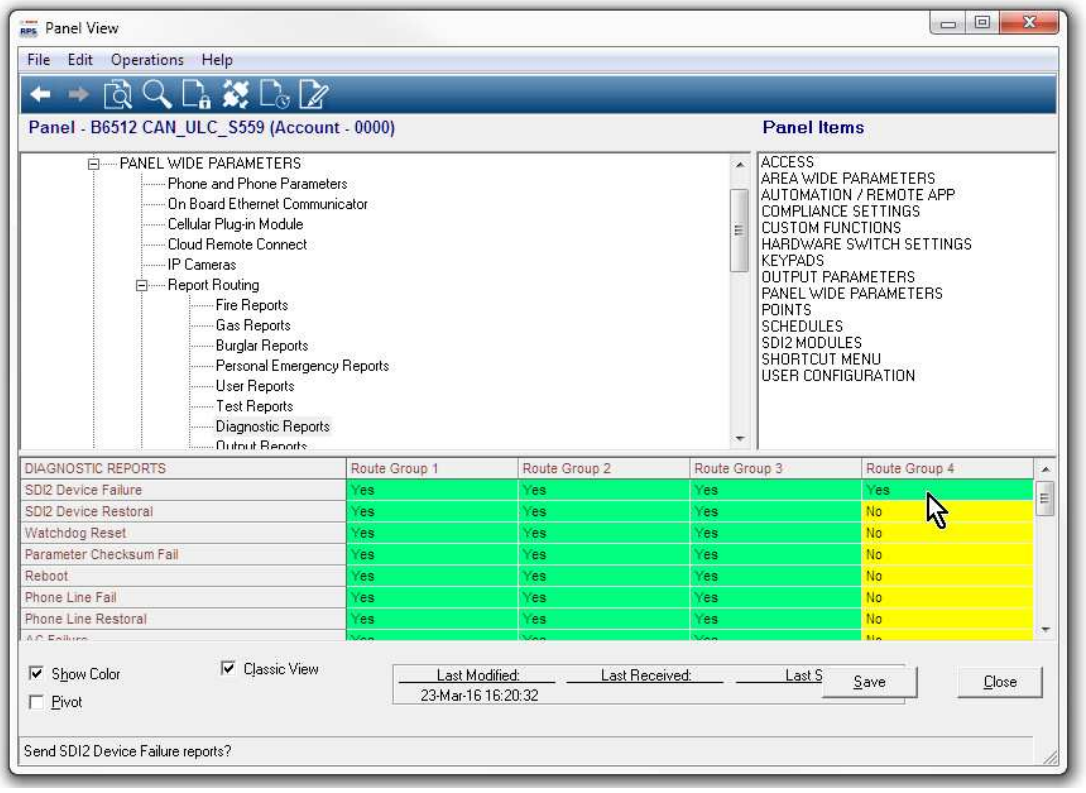


Abbildung 3.2: SDI2 Device Failure (Fehler des SDI2-Geräts)

PANEL WIDE PARAMETERS > Communicator > Primary Destination Device [ZENTRALENÜBERGREIFENDE PARAMETER > Übertragungsgerät > Primäres Zielgerät)
FStellen Sie in der Spalte „Zielgruppe 4“ für den aktuell verwendeten Gerätetyp „Primary Destination Device“ (Primäres Zielgerät) auf „Adresse 4“ ein (z. B. „integrierte IP-Adresse, Adresse 4”), wenn die Zentrale Protokolle über das integrierte Ethernet sendet.

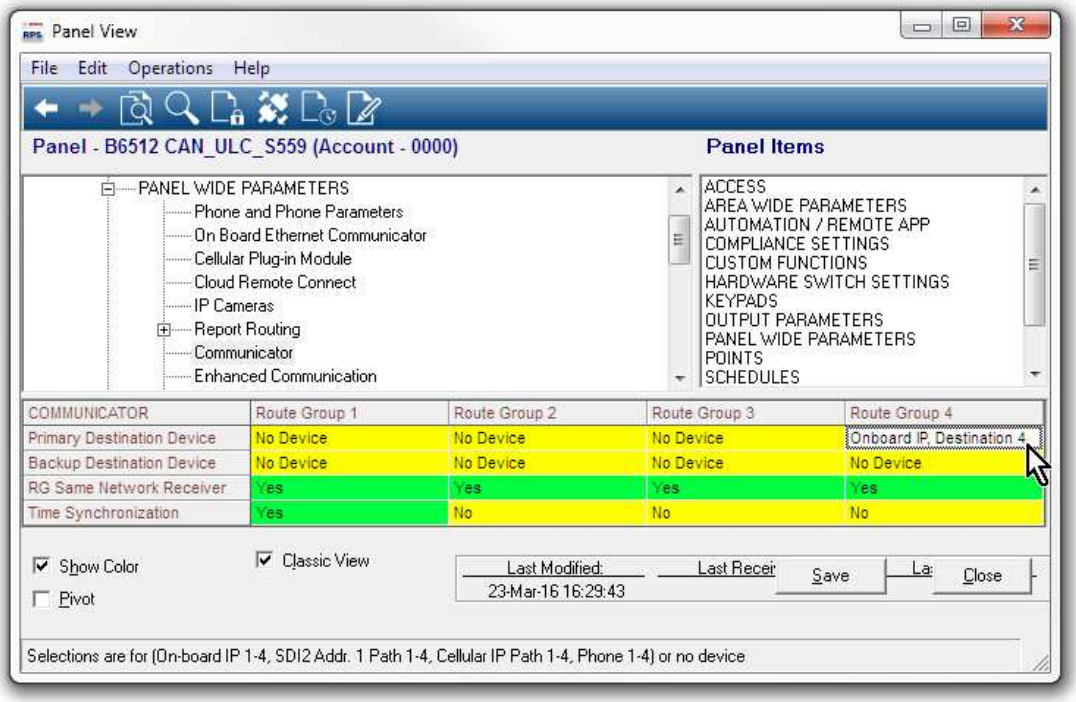


Abbildung 3.3: Primary Destination Device (Primäres Zielgerät)

PANEL WIDE PARAMETERS > Enhanced Communication > Destination 4 (ZENTRALENÜBERGREIFENDE PARAMETER > Erweiterte Kommunikation > Adresse 4)
Stellen Sie in der Spalte „Adresse 4" die Netzwerkadresse auf „0.1.1.1“ ein (diese Adresse stellt bewusst keine echte Adresse im Netzwerk dar). Stellen Sie die Pollingrate auf „0“ und die ACK-Wartezeit (Sek.) auf „5“.

POINTS > Point Profiles (Point Indexes) [MELDER > Melderprofile (Melderindexe)]
Konfigurieren Sie die Melderprofile 1, 4 und 6 wie nachfolgend beschrieben.
Parameter sind der Reihe nach zu konfigurieren.

Melderprofil 1
Setzen Sie „Alarm Abort” (Alarmabbruch) auf „Nein“.
Stellen Sie „Point Profile Text (First Language)“ [Melderprofiltext (Erste Sprache)] auf „Fire Panel Trouble“ (Störung Brandmeldezentrale) ein.
Setzen Sie „Point Type/Response/Circuit Style > Point Type” (Melderart/Reaktion/Stromkreisbauweise > Melderart) auf „Feuermelder“.
Setzen Sie „Point Type/Response/Circuit Style > Circuit Style” (Melderart/Reaktion/Stromkreisbauweise > Stromkreisbauweise) auf „Einzel-EOL (1 KΩ)“ oder „Einzel-EOL (2 KΩ)“.
Wählen Sie für „Response“ (Reaktion) den Wert „3“.

Melderprofil 4
Setzen Sie „Point Profile Text (First Language)“ (Melderprofiltext (Erste Sprache)) auf „Fire Panel Alarm“ (Brandmeldezentrale Alarm).
Setzen Sie „Point Type/Response/Circuit Style > Point Type” (Melderart/Reaktion/Stromkreisbauweise > Melderart) auf „Feuermelder“.

Setzen Sie „Point Type/Response/Circuit Style > Circuit Style” (Melderart/Reaktion/ Stromkreisbauweise > Stromkreisbauweise) auf „Einzel-EOL (1 KΩ)“, „Einzel-EOL (2 KΩ)“ oder „Doppel-EOL“.
Wenn Sie „Point Type/Response/Circuit Style > Circuit Style” (Melderart/Reaktion/ Stromkreisbauweise > Stromkreisbauweise) auf „Einzel-EOL (1 KΩ)“ oder„Einzel-EOL (2 KΩ)“ festlegen, setzen Sie „Response“ (Reaktion) auf „1“.
Falls Sie „Point Type/Response/Circuit Style > Circuit Style” (Melderart/Reaktion/ Stromkreisbauweise > Stromkreisbauweise) auf „Doppel-EOL“ setzen, legen Sie für „Response“ (Reaktion) den Wert „0“ fest.

Melderprofil 6

Setzen Sie „Point Profile Text (First Language)“ [Melderprofiltext (Erste Sprache)] auf „Fire Panel Supervisory“ (Brandmeldezentrale Errichterbedienung).
Setzen Sie „Point Type/Response/Circuit Style > Point Type” (Melderart/Reaktion/ Stromkreisbauweise > Melderart) auf „Feuermelder“.
Setzen Sie „Point Type/Response/Circuit Style > Circuit Style” (Melderart/Reaktion/ Stromkreisbauweise > Stromkreisbauweise) auf „Einzel-EOL (1 KΩ)“, „Einzel-EOL (2 KΩ)“ oder „Doppel-EOL“.
Wenn Sie für Melderart/„Response“ (Reaktion)/Stromkreisbauweise > Stromkreisbauweise „Einzel-EOL (1 KΩ)“ oder„Einzel-EOL (2 KΩ)“ festlegen, setzen Sie „Response“ (Reaktion) auf „9“.
Wenn Sie Melderart/„Response“ (Reaktion)/Stromkreisbauweise > Stromkreisbauweise auf „Doppel-EOL“ setzen, legen Sie für „Response“ (Reaktion) den Wert „2“ fest.

Abbildung 3.4: Melderprofile

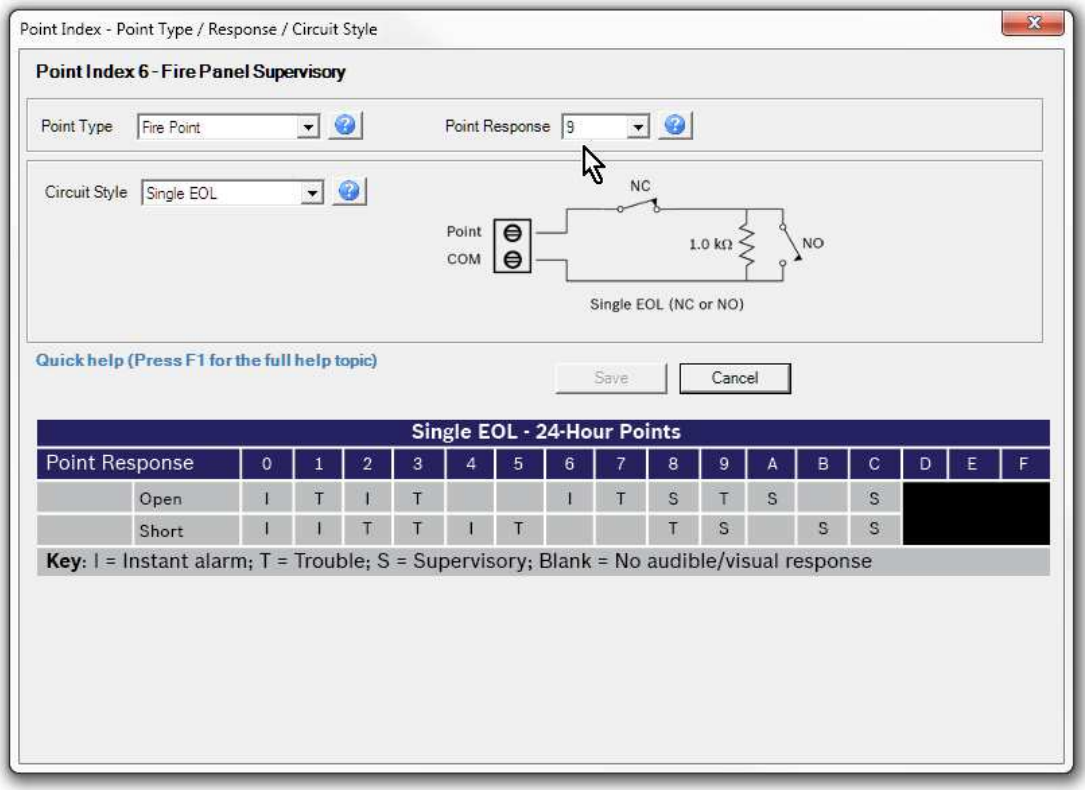


Abbildung 3.5: Melderart, Reaktion und Stromkreisbauweise

POINTS > Point Assignments (MELDER > Melderzuweisungen)

Legen Sie die Parameter „POINTS > Point Assignments, Text and Profile" (MELDER > Melderzuweisungen, Text und Profil) für die integrierten Melder 1, 2 und 3 wie folgt fest:

Melder 1

Setzen Sie „Point Assignments > Text" (Melderzuweisungen > Text) auf „Fire Panel Alarm" (Alarm Brandmeldezentrale).
Setzen Sie „Point Assignments > Profile" (Melderzuweisungen > Profil) auf „4 – Fire Panel Alarm" (4 – Brandmeldezentrale Alarm).

Melder 2

Setzen Sie „Point Assignments > Text" (Melderzuweisungen > Text) auf „Fire Panel Trouble" (Störung Brandmeldezentrale).
Setzen Sie „Point Assignments > Profile" (Melderzuweisungen > Profil) auf „1 – Fire Panel Trouble" (1 – Brandmeldezentrale Störung).

Melder 3

Stellen Sie „Point Assignments > Text" (Melderzuweisungen > Text) auf „Fire Panel Supervisory" (Brandmeldezentrale Errichterbedienung) ein.
Setzen Sie „Point Assignments > Profile" (Melderzuweisungen > Profil) auf „6 – Fire Panel Supervisory" (Brandmeldezentrale Errichterbedienung).

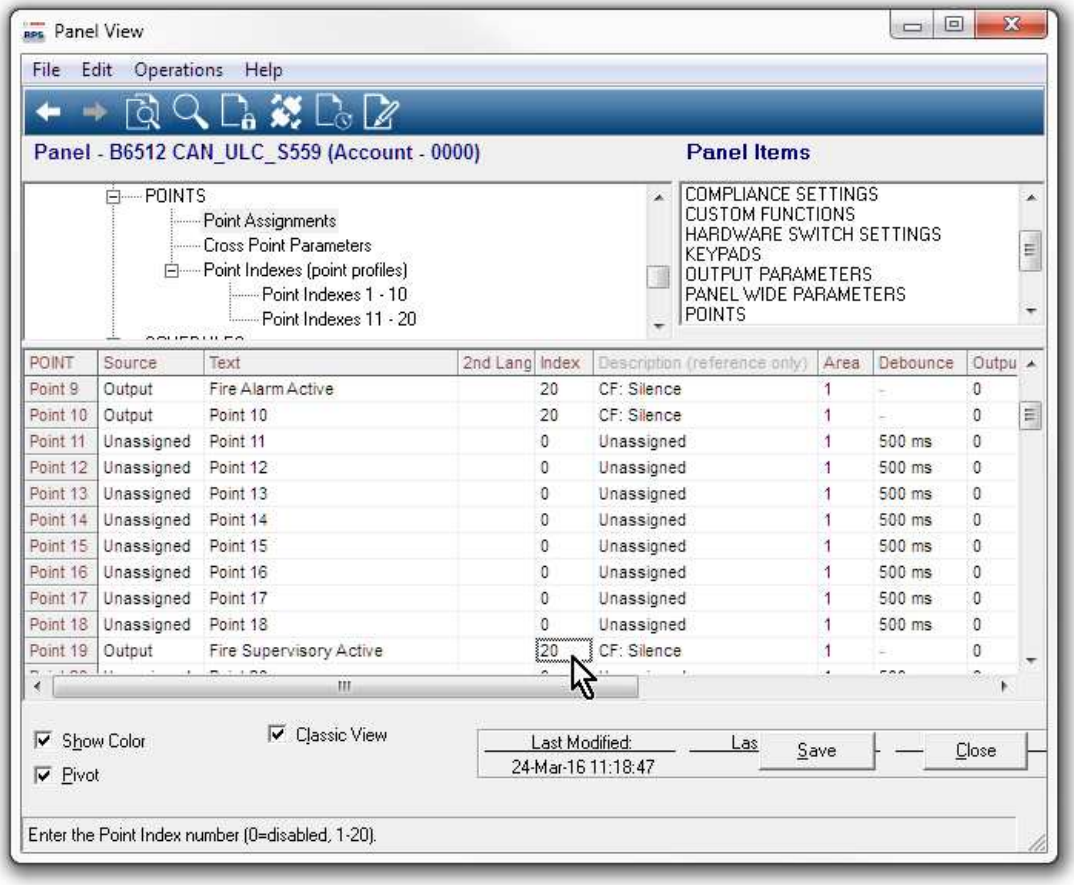


Abbildung 3.6: Fire Panel Supervisory (Brandmeldezentrale Errichterbedienung)

3.2.3 CAN/ULC-S559 – empfohlene Parametrierung

Feueralarm-, Zentralenalarm-, Störungs- und Errichterbedienungsereignisse über Zentrale stummschalten

Wenn Zentralen wie nachfolgend beschrieben konfiguriert werden, werden mit der Zentrale verbundene Bedienteile bei Feuer-, Störungs- und Errichterbedienungsereignissen automatisch stummgeschaltet.

Hinweis!

Automatische Stummschaltung ist für B3512-Zentralen nicht verfügbar

Automatisches Stummschalten von Feueralarm-, Zentralenalarm-, Störungs- und Errichterbedienungsereignissen steht für B3512-Zentralen nicht zur Verfügung. Diese Ereignisse müssen von Benutzern am Bedienteil stummgeschaltet werden.

BENUTZERDEFINIERTE FUNKTIONEN > Benutzerdefinierte Funktion 128

Stellen Sie „Benutzerdefinierte Funktion 128 > Benutzerdefinierte Funktion” auf „Stummschalten“.

Stellen Sie „Benutzerdefinierte Funktion 128 > Funktion 1” auf „Trouble Silence“ (Störung Stummschalten) (setzen Sie Parameter 1 auf „Bereich 1”).

Stellen Sie „Benutzerdefinierte Funktion 128 > Funktion 2” auf „Alarm Silence“ (Alarm Stummschalten) (setzen Sie Parameter 1 auf „Bereich 1”).

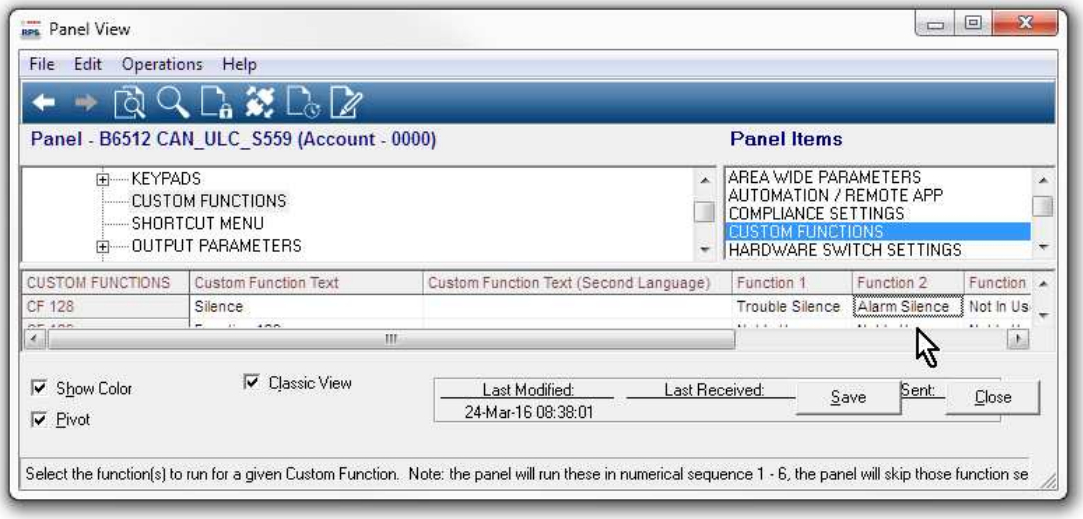


Abbildung 3.7: Benutzerdefinierte Funktion 128

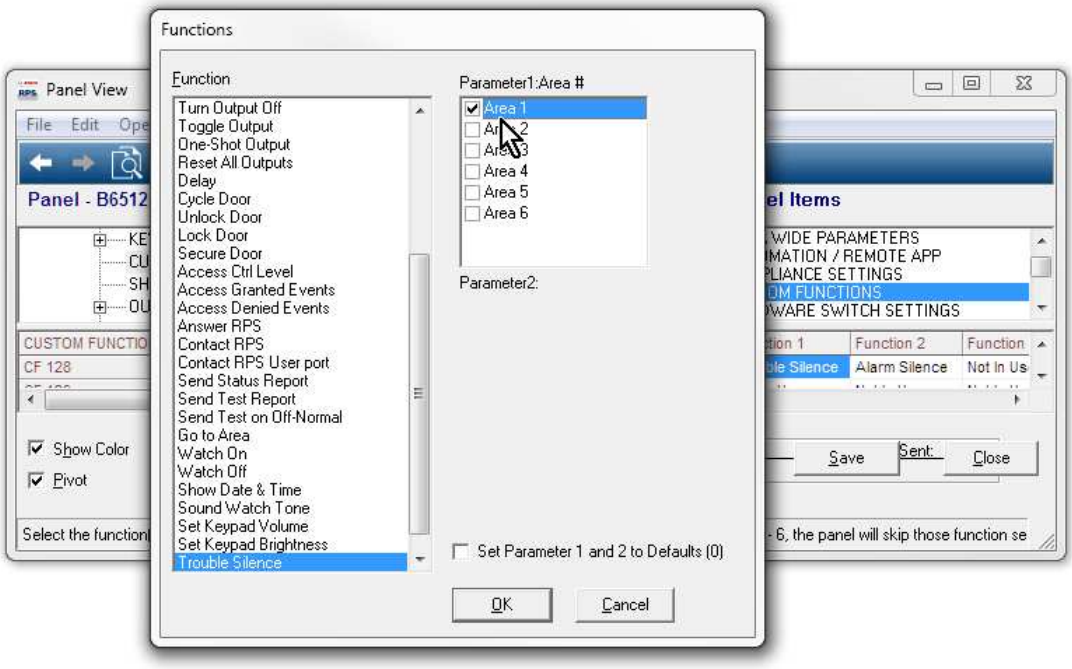


Abbildung 3.8: Auswahl für Bereich 1

OUTPUT PARAMETERS > Panel Wide Outputs (AUSGANGSPARAMETER > Zentralenübergreifende Ausgänge)

Für virtuelle Ausgänge:

Stellen Sie „Panel Wide Outputs > Summary Fire" (Zentralenübergreifende Ausgänge > Zusammenfassung Feuer) auf den Wert „9" ein.

Setzen Sie „Panel Wide Outputs > Summary Fire Trouble" (Zentralenübergreifende Ausgänge > Zusammenfassung Feuerstörung) auf „10".

Setzen Sie „Panel Wide Outputs > Summary Supervisory" (Zentralenübergreifende Ausgänge > Zusammenfassung Feuer-Errichterbedienung) auf „19".

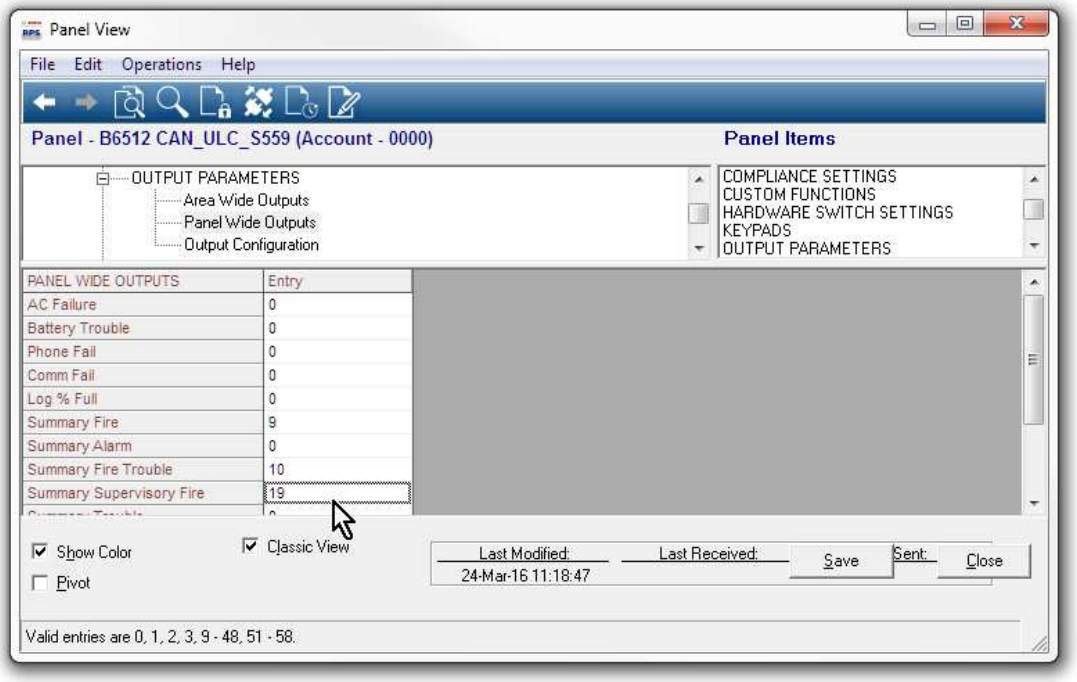


Abbildung 3.9: Zentralenübergreifende Ausgänge

POINTS > Point Profiles (Point Indexes) [MELDER > Melderprofile (Melderindexe)]

Konfigurieren Sie Melderprofil 20 wie unten beschrieben.

Parameter sind der Reihe nach zu konfigurieren.

Melderprofil 20

Stellen Sie „Point Profile Text (First Language)“ [Melderprofiltext (Erste Sprache)] auf „CF: Stummschalten“.

Setzen Sie „Point Type/Response/Circuit Style > Point Type” (Melderart/Reaktion/Stromkreisbauweise > Melderart) auf „Benutzerdefinierte Funktion“.

Belassen Sie „Point Type/Response/Circuit Style > Circuit Style” (Melderart/Reaktion/Stromkreisbauweise > Stromkreisbauweise) auf der Standardeinstellung „Einzel-EOL (1 KΩ)“.

Belassen Sie „Point Type/Response/Circuit Style > Response” (Melderart/Reaktion/Stromkreisbauweise > Reaktion) auf der Standardeinstellung „7“.

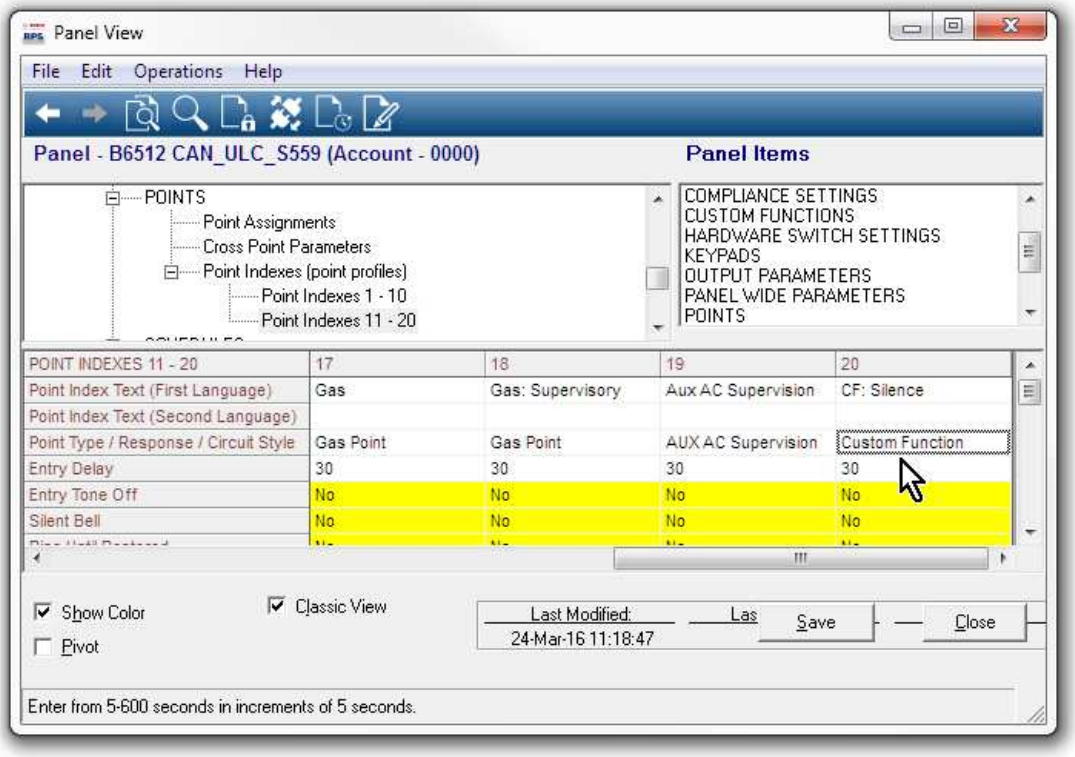


Abbildung 3.10: Melderprofil 20

POINTS > Point Assignments (MELDER > Melderzuweisungen)

Legen Sie die Parameter „POINTS > Point Assignments" (MELDER > Melderzuweisungen), „Source" (Quelle), „Text" und „Profil" für die Melder 9, 10 und 19 wie folgt fest:

Melder 9

Setzen Sie „Point Assignments > Source" (Melderzuordnungen > Quelle) auf „Ausgang".
Setzen Sie „Point Assignments > Text" (Melderzuweisungen > Text) auf „Fire Alarm Active" (Feueralarm aktiv).
Stellen Sie „Point Assignments > Profile" (Melderzuweisungen > Profil) auf „20 – CF: Stummschalten".

Melder 10

Setzen Sie „Point Assignments > Source" (Melderzuordnungen > Quelle) auf „Ausgang".
Setzen Sie „Point Assignments > Text" (Melderzuweisungen > Text) auf „Fire Panel Active" (Feuerstörung aktiv).
Stellen Sie „Point Assignments > Profile" (Melderzuweisungen > Profil) auf „20 – CF: Stummschalten".

Melder 19

Setzen Sie „Point Assignments > Source" (Melderzuordnungen > Quelle) auf „Ausgang".
Setzen Sie „Point Assignments > Text" (Melderzuweisungen > Text) auf „Fire Supervisory Active" (Feuer–Errichterbedienung aktiv).
Stellen Sie „Point Assignments > Profile" (Melderzuweisungen > Profil) auf „20 – CF: Stummschalten".

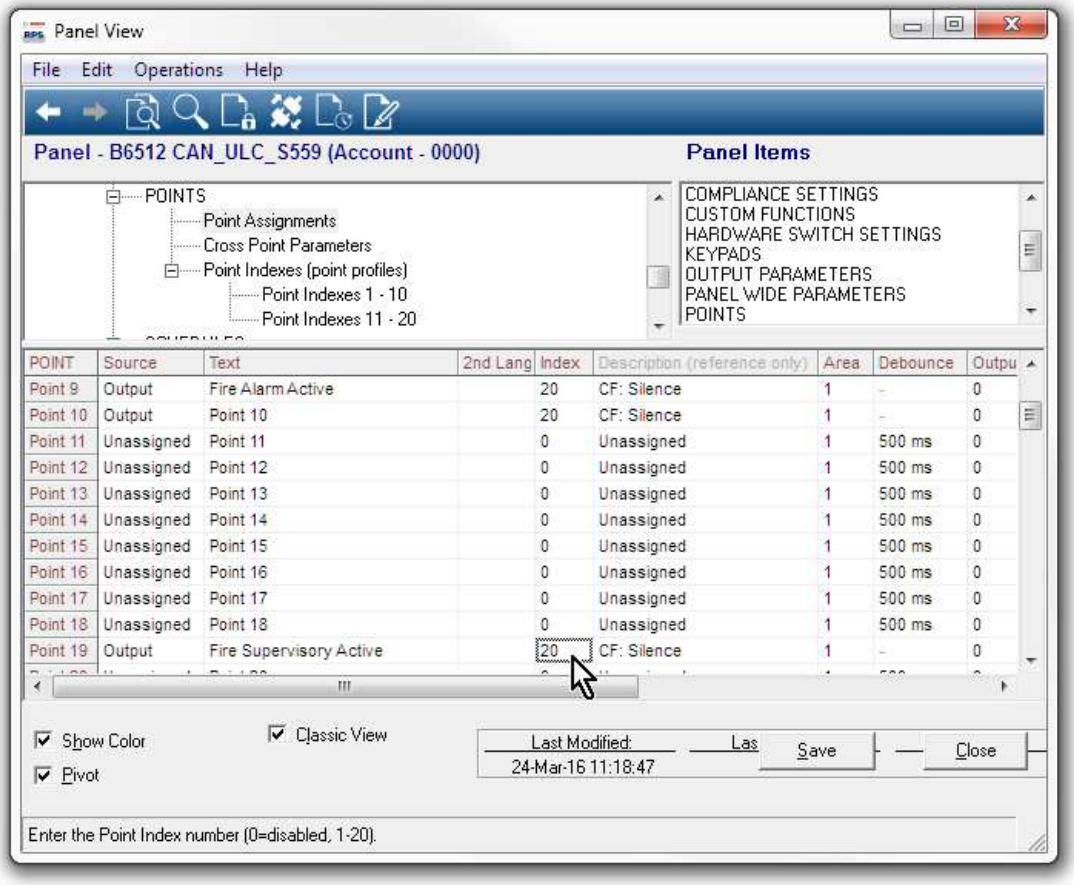


Abbildung 3.11: Melderzuweisungen

3.3 Überwachungskonfiguration

Daten für die Überwachung optimieren:

Montageart	Einbruchüberwachung im Gewerbebetrieb (UL1610)	Einbruchüberwachung im Gewerbebetrieb (ULC S304)	High Supervision (Hohe Überwachung)	Stündlich	Medium Security or Household Fire (Mittlere Sicherheit oder Privathaushalte)	Daily Supervision (Tägliche Überwachung)
Required Supervision Interval (Erforderliches Überwachungsintervall)	200 Sek	180 Sek	300 Sek	1 Stunde	4 Stunden	25 Stunden

Montageart	Einbruchüberwachung im Gewerbebetrieb (UL1610)	Einbruchüberwachung im Gewerbebetrieb (ULC S304)	High Supervision (Hohe Überwachung)	Stündlich	Medium Security or Household Fire (Mittlere Sicherheit oder Privathaushalte)	Daily Supervision (Tägliche Überwachung)
Empfohlener Serviceplan	Erweitert	Erweitert	High Supervision (Hohe Überwachung)	Standard	Standard	Ersatz
Zentralenparametrierung						
Receiver Supervision Time (Empfängerüberwachungsdauer)	200 Sek	Benutzerdefiniert	300 Sek	1 Stunde – NFPA	4 Stunden – Mittlere Sicherheit	25 Stunden
Pollingrate – Zentrale (Sek.)	k. A.	89 Sek	k. A.	k. A.	k. A.	k. A.
Panel ACK Wait (sec) (Bestätigungswartezeit Zentrale in Sek.)	k. A.	15	k. A.	k. A.	k. A.	k. A.
Panel Retry Count (Anzahl der Wiederholungsversuche Zentrale)	k. A.	5	k. A.	k. A.	k. A.	k. A.

3.4 Europäische Anwendung

Standardeinstellung: Nein

Auswahl:

Ja – Anwendung auf dem europäischen Markt. Das SIA DC-09 Übertragungsformat kann eingesetzt werden.

Nein – keine Anwendung auf dem europäischen Markt. Das SIA DC-09 Übertragungsformat kann nicht eingesetzt werden.

Hinweis!
SIA DC-09 wurde nicht durch UL für die Verwendung untersucht und sind für außereuropäische Anwendungen nicht verfügbar. Sie dürfen das SIA DC-09 Übertragungsformat nicht für UL- oder ULC-Anwendungen auswählen.

Ort im RPS-Menü
Konformitätseinstellungen > Europäische Anwendung

4 Panel Wide Parameters (Zentralenübergreifende Parameter)

4.1 Telefon und Telefonparameter

4.1.1 Telefon-Zieladresse 1 (bis 4)

Standardeinstellung: Leer

Auswahl:

- Leer: Die Zentrale wählt keine Telefonnummer.
- 0-9: Die Zentrale wählt diese Zeichen.
- C: Die Zentrale pausiert 2 Sekunden, wenn sie ein „C“ in der Wählsequenz erkennt.
- D: Die Zentrale wählt, wenn sie einen Wählton erkennt oder die 7 Sekunden lange Wähltonerkennungsdauer abgelaufen ist. Zum Verlängern der Wähltonerkennungsdauer fügen Sie am Beginn der Wählsequenz ein „D“ ein.
- #, *: Die Zentrale wählt diese Zeichen so, als würden sie auf einem Telefontastenfeld gedrückt.

Geben Sie die von der Zentrale verwendete Wählsequenz (Telefonnummer) ein, um Protokolle an den Bedienteilempfänger zu senden.

Das Leerlassen dieses Parameters führt nicht zum Deaktivieren der Telefon-Zieladresse. Um zu verhindern, dass die Telefon-Zieladresse verwendet wird, weisen Sie sie keinem Primär- oder Ersatzzielgerät zu. Weitere Informationen finden Sie unter *Übertragungsgerät – Übersicht, Seite 86*.

Telefon-Zieladressen für Anklopfen konfigurieren

Das Wählen einer Anklopfsequenz mit einer Telefonleitung ohne Anklopfen hindert die Zentrale daran, Protokolle an den Bedienteilempfänger zu senden. Wenn ein Kunde den Anklopfdienst ohne Benachrichtigung seines Sicherheitsunternehmens beendet, kann die Zentrale keine Protokolle über das Ersatzzielgerät senden.

Wenn Sie eine Telefon-Zieladresse mit einer Telefonnummer konfigurieren, die eine Sequenz zum Abbruch des Anklopfens enthält, wählen Sie diese Telefon-Zieladresse als das *Primary Destination Device (Primäres Zielgerät), Seite 88* für eine Zielgruppe. Konfigurieren Sie eine andere Telefon-Zieladresse ohne die Anklopf-Abbruchsequenz, und wählen Sie sie als *Ersatzzielgeräte, Seite 88* für die Zielgruppe.

Melde-Adresse des Menüs „RPS“

Panel Wide Parameters > Phone and Phone Parameters > Phone Destination 1 to 4 (Zentralenübergreifende Parameter > Telefon und Telefonparameter > Telefon-Zieladresse 1 bis 4)

4.1.2 Format für Telefon-Zieladresse 1 (bis 4)

Standardeinstellung: Modem4

Auswahl:

- Modem4: Die Zentrale sendet erweiterte Modem4-Protokolle an den Leitstellenempfänger. Erweiterte Informationen enthalten Meldertext, Ausgangstext und Benutzernamen.
- Contact-ID: Die Zentrale sendet Contact-ID-Protokolle. Verwenden Sie dieses Format, wenn der Leitstellenempfänger das Modem4-Format nicht unterstützt.

Melde-Adresse des Menüs „RPS“

Panel Wide Parameters > Phone and Phone Parameters > Phone Destination (1 to 4) Format [Zentralenübergreifende Parameter > Telefon und Telefonparameter > Telefon (1 bis 4)-Zielformat]

4.1.3 DTMF Dialing (DTMF-Wählverfahren)

Standardeinstellung: Yes

Auswahl:

– Ja: Die Zentrale wählt Telefonnummern über DTMF (Dual-Ton-Mehrfrequenzwahlverfahren, Tonwahl).
– Nein: Die Zentrale wählt Telefonnummern mittels Impulswahl.

Stellen Sie vor dem Setzen dieses Parameters auf „Nein“ sicher, dass das mit der Zentrale verbundene öffentliche Fernsprechnetz die Impulswahl unterstützt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“):

Panel Wide Parameters > Phone and Phone Parameters > DTMF Dialing
(Zentralenübergreifende Parameter > Telefon und Telefonparameter > DTMF-Wählverfahren)

4.1.4 Phone Supervision Time (Telefonüberwachungsdauer)

Standardeinstellung: 0

Auswahl:

– 0: deaktiviert, keine Überprüfung der Telefonleitung
– 10 – 240 (Sekunden): Anzahl der Sekunden (in 10-Sekunden-Schritten), die eine Telefonleitung gestört sein muss, bevor die Zentrale ein Telefonleitungsfehlerereignis erstellt.

Die Zentrale prüft die Telefonleitung etwa neunmal pro Minute. Erkennt die Zentrale eine Telefonleitungsstörung mit der für diesen Parameter gesetzten Sekundenanzahl, erstellt sie ein Telefonleitungsfehlerereignis.

Bedienteile zeigen eine Telefonleitungsstörung an und geben einen Störungston aus, wenn die Parameter *Buzz on Fail (Störungston bei Fehler), Seite 55* und *Trouble Tone (Störungston), Seite 149* auf „Ja“ eingestellt sind. Ist der Parameter *Alarm on fail (Alarm bei Fehler), Seite 54* auf „Ja“ eingestellt, zeigen Bedienteile ein Alarmereignis an und geben einen Alarmton aus.

Wenn sich die Telefonleitung hinsichtlich der für diesen Parameter eingestellten Sekundenanzahl im Normalzustand befindet, erstellt die Zentrale ein Telefonleitungswiederherstellungsereignis.

Beim Auftreten des Ereignisses sendet die Zentrale Telefonleitungsfehler- und Telefonleitungswiederherstellungsprotokolle. Diese sind auch in *Expand Test Report (Prüfprotokoll erweitern), Seite 55* enthalten.

Telefonleitungsfehlerereignisse sind Bereich 1 zugewiesen und verwenden die Konfiguration „Bereich 1“.

Melde-Adresse des Menüs „RPS“

Panel Wide Parameters > Phone and Phone Parameters > Phone Supervision Time
(Zentralenübergreifende Parameter > Telefon und Telefonparameter > Telefonüberwachungsdauer)

4.1.5 Alarm on fail (Alarm bei Fehler)

Standardeinstellung: Nein

Auswahl:

– Ja: Alarmreaktion (Einbruchsignal, Bedienteil-Alarmton, Alarmprotokoll) bei Telefonleitungsfehlerereignissen
– Nein: keine Alarmreaktion bei Telefonleitungsfehlerereignissen

Zum Verwenden dieser Funktion „Alarm on fail“ (Alarm bei Fehler) aktivieren Sie für den Parameter „Phone Supervision Time“ (Telefonüberwachungsdauer) die Überwachung der Telefonleitung.

Siehe *Phone Supervision Time (Telefonüberwachungsdauer), Seite 54*.

Die Alarmreaktion bei Telefonleitungsfehlerereignissen umfasst:

– Aktivierung des Einbruchsignals für Bereich 1
– Aktivierung des Alarmtons an Bedienteilen
– Senden von Alarmprotokollen

Melde-Adresse des Menüs „RPS“

Panel Wide Parameters > Phone and Phone Parameters > Alarm on Fail
(Zentralenübergreifende Parameter > Telefon und Telefonparameter > Alarm bei Fehler)

4.1.6 Buzz on Fail (Störungston bei Fehler)

Standardeinstellung: Nein

Auswahl:

– Ja: Bei einem Telefonleitungsfehlerereignis wird an allen Bedienteilen ein zentralenweiter Störungston ausgegeben.
– Nein: Bei einem Telefonleitungsfehlerereignis wird kein Störungston auf einem Bedienteil ausgegeben.

Zum Verwenden dieser Funktion „Buzz on fail“ (Störungston bei Fehler) aktivieren Sie für den Parameter „Phone Supervision Time“ (Telefonüberwachungsdauer) die Überwachung der Telefonleitung.

Siehe *Phone Supervision Time (Telefonüberwachungsdauer), Seite 54*

Zentralenübergreifende Störungstöne für individuelle Bedienteile werden über den Parameter „Trouble Tone“ (Störungston) eingestellt (*Trouble Tone (Störungston), Seite 149*. Die für alle Bedienteile geltende Standardeinstellung für den Parameter „Trouble Tone“ (Störungston) ist „Nein“ (kein Störungston bei zentralenübergreifenden Störungen).

Melde-Adresse des Menüs „RPS“

Panel Wide Parameters > Phone and Phone Parameters > Buzz On Fail
(Zentralenübergreifende Parameter > Telefon und Telefonparameter > Störungston bei Fehler)

4.1.7 Expand Test Report (Prüfprotokoll erweitern)

Standardeinstellung: Nein

Auswahl:

– Ja: Benutzerprüfprotokolle sowie zeitgesteuerte Prüfprotokolle erweitern, um nicht-normale Systemstatusinformationen miteinzubeziehen
– Nein: Prüfprotokolle nicht erweitern

Ist dieser Parameter auf „Ja“ eingestellt, wird nach dem Prüfprotokoll (oder nicht-normales Prüfprotokoll) für jeden nicht-normalen Systemstatus ein Diagnoseprotokoll erstellt. Eine Liste mit enthaltenen Protokollen finden Sie unter „Zentralenübergreifende Parameter > „Protokoll-Routing > *Diagnoseprotokolle, Seite 82*.

Melde-Adresse des Menüs „RPS“

Panel Wide Parameters > Phone and Phone Parameters > Expand Test Report
(Zentralenübergreifende Parameter > Telefon und Telefonparameter > Prüfprotokoll erweitern)

4.1.8 PSTN-Kompatibilität

Standardeinstellung: USA

Auswahl:

Algerien	El Salvador	Libanon	Réunion
Argentinien	Equador	Lesotho	Rumänien
Armenien	Estland	Liechtenstein	Russland
Australien	Finnland	Litauen	Saudi-Arabien
Österreich	Frankreich	Luxemburg	Singapur
Bahamas	Georgien	Macau	Slowakei
Bahrain	Deutschland	Malaysia	Slowenien

Belarus	Ghana	Malta	Südafrika
Belgien	Griechenland	Martinique	Spanien
Bermuda	Guadeloupe	Mexiko	Sri Lanka
Brasilien	Guam	Moldavien	Schweden
Brunei	Hongkong	Marokko	Schweiz
Bulgarien	Ungarn	Niederlande	Taiwan
Kanada	Island	Neuseeland	Thailand
Karibik	Indien	Nigeria	Tunesien
Chile	Indonesien	Norwegen	Türkei
China	Irland	Oman	VAE
Kolumbien	Israel	Pakistan	Ukraine
Costa Rica	Italien	Paraguay	Großbritannien
Kroatien	Japan	Peru	Uruguay
Zypern	Jordanien	Philippinen	USA
Tschechische Republik	Kasachstan	Polen	Usbekistan
Dänemark	Korea	Französisch-Polynesien	Venezuela
Dominikanische Republik	Kuwait	Portugal	Jemen
Dubai	Kirgistan	Puerto Rico	Sambia
Ägypten	Lettland	Katar	

Mit diesem Parameter werden die Zentrale und das steckbare B430-Telefonübertragungsgerät für öffentliche Fernsprechnetze (PSTN) konfiguriert.

Hinweis!
PSTN-Anforderung für Australien/Neuseeland, RPS-Antwort scharf/unscharf
Wird dieser PSTN-Kompatibilitätsparameter auf „Australien“ oder „Neuseeland“ gesetzt, muss „Panel Wide Parameters > RPS Parameters > Answer Armed and Answer Disarmed” (Zentralenübergreifende Parameter > RPS-Parameter > Antwort scharf und Antwort unscharf) auf „0“ (deaktiviert) eingestellt sein.

Melde-Adresse des Menüs „RPS“
Panel Wide Parameters > Phone and Phone Parameters > PSTN Compatibility (Zentralenübergreifende Parameter > Telefon und Telefonparameter > PSTN-Kompatibilität)

4.2 Integriertes Ethernet (IP)-Übertragungsgerät

4.2.1 IPv6-Modus

Standardeinstellung: Nein
Auswahl:
– Ja: IPv6-Modus (Internet Protocol Version 6) für die IP-Kommunikation verwenden.
– Nein: IPv4-Modus (Internet Protocol Version 4) für die IP-Kommunikation verwenden
Wenn „IPv6 aktivieren“ auf „Ja“ eingestellt ist, setzen Sie „DHCP/AutoIP Enable“ (DHCP/AutoIP aktivieren) auf „Ja“.
Ist „IPv6 aktivieren“ auf „Nein“ gesetzt, sind die IPv6-Parameter grau dargestellt (kein Zugriff).
Ist „IPv6 aktivieren“ auf „Ja“ gesetzt, sind die IPv4-Parameter grau dargestellt (kein Zugriff).
RPS Menu Locations (Meldeadressen des Menüs „RPS“)
Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 Mode (Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > IPv6-Modus)

4.2.2 IPv6 DHCP

Standardeinstellung: Aktiviert (Ja)

Auswahl:

– Aktiviert (Ja): DHCP legt IP-Adresse, IP-Standard-Gateway und IP-DNS-Serveradresse automatisch fest. Mit AutoIP werden Geräten bei Inbetriebnahme dynamische IP-Adressen zugewiesen.
– Deaktiviert (Nein): Setzen Sie diesen Parameter auf „Deaktiviert“, wenn kein DHCP-Dienst vorhanden ist. Legen Sie IP-Adresse, IP-Standard-Gateway und IP-DNS-Serveradresse manuell fest.

DHCP erfordert einen DHCP-Server.

RPS Menu Locations (Meldeadressen des Menüs „RPS“)

Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 DHCP
(Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > IPv6 DHCP)

4.2.3 IPv4 DHCP/AutoIP Enable (IPv4 DHCP/AutoIP aktivieren)

Standardeinstellung: Aktiviert (Ja)

Auswahl:

– Aktiviert (Ja): DHCP legt IP-Adresse, IP-Standard-Gateway und IP-DNS-Serveradresse automatisch fest. Mit AutoIP werden Geräten bei Inbetriebnahme dynamische IP-Adressen zugewiesen.
– Deaktiviert (Nein): Setzen Sie diesen Parameter auf „Deaktiviert“, wenn kein DHCP-Dienst vorhanden ist. Legen Sie IP-Adresse, IP-Standard-Gateway und IP-DNS-Serveradresse manuell fest.

DHCP erfordert einen DHCP-Server.

Ist dieser Parameter auf „Ja“ eingestellt, sind die IPv4-Adresse, die IPv4- Subnetzmaske und das IPv4-Standard-Gateway grau dargestellt. Diese Einstellung kann nicht geändert werden.

Wenn der Parameter „IPv6-Modus“ auf „Ja“ eingestellt ist, ist dieser grau dargestellt (kein Zugriff).

RPS Menu Locations (Meldeadressen des Menüs „RPS“)

Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 DHCP/AutoIP Enable
(Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > IPv4 DHCP/AutoIP aktivieren)

4.2.4 IPv4-Adresse

Standardeinstellung: 0.0.0.0

Auswahl: 0.0.0.0 bis 255.255.255.255

Falls „DHCP/Auto IP Enable“ (DHCP/Auto IP aktivieren) für IPv4 auf „Ja“ gesetzt ist, wird dieser Parameter grau dargestellt (kein Zugriff).

Wenn „DHCP/Auto IP Enable“ (DHCP/Auto IP aktivieren) für IPv4 auf „Nein“ gesetzt ist, geben Sie hier die IPv4-Adresse an.

Weitere Informationen

Formate von IP-Adresse und Domainname, Seite 300

Melde-Adresse des Menüs „RPS“

Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 address
(Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > IPv4-Adresse)

4.2.5 IPv4-Subnetzmaske

Standardeinstellung: 255.255.255.0

Auswahl: 0.0.0.0 bis 255.255.255.255

Falls „DHCP/Auto IP Enable“ (DHCP/Auto IP aktivieren) für IPv4 auf „Ja“ gesetzt ist, wird dieser Parameter grau dargestellt (kein Zugriff).
Wenn „DHCP/Auto IP“ für IPv4 auf „Nein“ gesetzt ist, geben Sie hier die IPv4-Subnetzmaske ein.
Die Zentrale nutzt die Subnetzmaske zum schnelleren Identifizieren des Netzwerks und der Knotenkomponenten der Adresse.

Weitere Informationen
Formate von IP-Adresse und Domainname, Seite 300
RPS Menu Locations (Meldeadressen des Menüs „RPS“)
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 Subnet Mask (Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > IPv4-Subnetzmaske)

4.2.6 IPv4-Standard-Gateway

Standardeinstellung: 0.0.0.0
Auswahl: 0.0.0.0 bis 255.255.255.255
Falls „DHCP/Auto IP Enable“ (DHCP/Auto IP aktivieren) für IPv4 auf „Ja“ gesetzt ist, wird dieser Parameter grau dargestellt (kein Zugriff).
Ist „DHCP/Auto IP Enable“ (DHCP/Auto IP aktivieren) für IPv4 auf „Nein“ gesetzt, geben Sie hier die Standard-Gateway-Adresse an.

Weitere Informationen
Formate von IP-Adresse und Domainname, Seite 300
RPS Menu Locations (Meldeadressen des Menüs „RPS“)
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 Default Gateway4 Default Gateway (Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > IPv4-Standard Gateway4 Standard-Gateway)

4.2.7 IPv4 DNS Server IP Address (IPv4-DNS-Server-IP-Adresse)

Standardeinstellung: 0.0.0.0
Auswahl: 0.0.0.0 bis 255.255.255.255
Ein Domain Name Server (DNS) setzt Internet-Domainnamen und Hostnamen in die entsprechenden IP-Adressen um. Im DHCP-Modus wird der Standard-DNS des DHCP-Servers verwendet. Geben Sie die IP-Adresse des benutzerdefinierten DNS-Servers ein, um einen benutzerdefinierten DNS-Server im DHCP-Modus zu nutzen.

Weitere Informationen
Formate von IP-Adresse und Domainname, Seite 300
RPS Menu Locations (Meldeadressen des Menüs „RPS“)
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 DNS server IP address (Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät >IPv4-DNS-Server-IP-Adresse)

4.2.8 IPv6-DNS-Server-IP-Adresse

Standardeinstellung:
Auswahl: 0000:0000:0000:0000:0000:0000:0000:0000 bis FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Mit diesem Parameter wird die IPv6-DNS-Server-IP-Adresse auf den Modus „statische IP-Adresse“ eingestellt.
Ändern Sie diese Adresse nicht, wenn sie mit dem DHCP-Dienst festgelegt wurde.

Ein Domain Name Server (DNS) wandelt Internet-Domänennamen und Hostnamen in die entsprechenden IP-Adressen um. Im DHCP-Modus wird der Standard-DNS des DHCP-Servers verwendet. Zum Verwenden eines benutzerdefinierten DNS-Servers im DHCP-Modus ändern Sie den Parameter zur IP-Adresse des benutzerdefinierten DNS-Servers.
Diese IPv6-DNS-Serveradresse ist die einzige IPv6-Adresse, die in Form von Zahlen eingegeben wird.

Weitere Informationen
Formate von IP-Adresse und Domainname, Seite 300
RPS Menu Locations (Meldeadressen des Menüs „RPS“)
Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 DNS server IP address (Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät >IPv6-DNS-Server-IP-Adresse)

4.2.9 UPnP (Universal Plug & Play) aktivieren

Standardeinstellung: „Ja“
Auswahl:
Ja (Aktiviert): UPnP zum Öffnen einer Port-Weiterleitung für eingehende RPS- und RSC (Remote Security Control)-Verbindungen verwenden
Nein (Deaktiviert): kein UPnP verwenden
Der Parameter „UPnP“ hat keine Auswirkung auf die Übermittlung von Ereignissen an Bedienteilempfänger.
Falls dieser Parameter auf „Ja“ gesetzt ist, sendet die Zentrale eine Anfrage zum Öffnen einer Port-Weiterleitung an den Standort-Router. Die Port-Weiterleitung lässt eingehende RPS- und RSC-Verbindungen (Remote Security Control, Fernsicherheitskontrolle) zu.

Hinweis!
UPnP erfordert IP-Adresse/Hostname und Panel Port (Port Zentrale)
Überprüfen Sie auf der Registerkarte „Panel Data – View“ (Zentralendaten – Anzeigen), ob die Parameter „IP-Adresse/Hostname“ und „Panel Port“ (Port Zentrale) eingegeben sind.

RPS Menu Locations (Meldeadressen des Menüs „RPS“)
Panel Wide Parameters > Onboard Ethernet Communicator > UPnP (Universal Plug and Play) Enable [Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > UPnP (Universal Plug & Play) aktivieren]

4.2.10 ARP-Cache-Timeout (Sekunden)

Standardeinstellung: 600
Auswahl: 1 bis 600 (Sekunden)
Mit diesem Parameter wird das Timeout für ARP-Cacheeinträge festgelegt.
RPS Menu Locations (Meldeadressen des Menüs „RPS“)
Panel Wide Parameters > Onboard Ethernet Communicator > ARP Cache Timeout (Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > ARP-Cache-Timeout)

4.2.11 Hostname des Moduls

Standardeinstellung: leer
Auswahl: bis zu 63 Zeichen (Buchstaben, Zahlen, Punkte und Striche)
Der Hostname identifiziert das IP-Übertragungsgerät (integriert oder SDI2-Modul) im Netzwerk. Lassen Sie diesen Parameter leer, um den werksseitigen Standardhostnamen zu verwenden.

Hinweis!
Lassen Sie diesen Parameter leer, um den werksseitigen Standardhostnamen zu verwenden.
Der werksseitige Standardhostname beginnt mit dem Buchstaben „B“, gefolgt von den letzten sechs Stellen der MAC-Adresse des Moduls.
Verwenden Sie die RPS-Diagnose oder die Installationsprogrammdiagnose (Bedienteil), um den Hostnamen anzuzeigen.

Verwenden Sie in einem lokalen Netzwerk mit DHCP den Hostnamen. Geben Sie den Hostnamen auf dem DNS-Server ein, um den Hostnamen extern zu verwenden.
Verwenden Sie den Hostnamen zum Herstellen einer Verbindung mit der Zentrale per RPS oder RSC (Remote Security Control) oder für eine Webkonfiguration oder -diagnose des Moduls.
Melde-Adresse des Menüs „RPS“
Panel Wide Parameters > Onboard Ethernet Communicator > Module Hostname
(Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > Hostname des Moduls)

4.2.12 TCP/UDP Port Number (TCP/UDP-Portnummer)

Standardeinstellung: 7700
Auswahl: 0 bis 65535
Ändern Sie den Standardwert des TCP/UDP-Ports nicht bei IP-Kommunikation mit RPS, Automatisierung oder Remote Security Control (RSC) in typischen Installationen.

Hinweis!
Portnummer größer als „1023” wählen, um die Menge an unerwünschtem Datenverkehr zu begrenzen
Wenn Sie die Standardeinstellung für die Portnummer ändern möchten, wählen Sie eine Portnummer größer als „1023”, um die Menge an unerwünschtem Netzwerkverkehr zu reduzieren.

Melde-Adresse des Menüs „RPS“
Panel Wide Parameters > Onboard Ethernet Communicator > TCP/UDP Port Number
(Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > TCP/UDP-Portnummer)

4.2.13 TCP Keep Alive Time (TCP Keep-Alive-Zeit)

Standardeinstellung: 4 Minuten
Auswahl: Aus – 8 Stunden
Zeit zwischen TCP Keep-Alive-Zeit-Meldungen kann in Minuten oder Stunden festgelegt werden. Keep-Alive-Meldungen stellen sicher, dass eine Verbindung aktiv bleibt.
Melde-Adresse des Menüs „RPS“
Panel Wide Parameters > Onboard Ethernet Communicator > TCP Keep Alive Time
(Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > TCP Keep-Alive-Zeit)

4.2.14 IPv4-Testadresse

Standardeinstellung: 8.8.8.8
Auswahl: IPv4-Adresse oder Domänenname
Die Zentrale sendet einen Ping-Befehl an die IPv4-Testadresse, um sicherzustellen, dass die Netzwerkkonfigurationseinstellungen korrekt sind und das Netzwerk in Betrieb ist.

Die Standard-Testadresse eignet sich für die meisten Netzwerke.

Weitere Informationen

Formate von IP-Adresse und Domainname, Seite 300

RPS Menu Locations (Meldeadressen des Menüs „RPS“)

Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 Test Address (Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > IPv4-Testadresse)

4.2.15 IPv6-Testadresse

Standardeinstellung: 2001:4860:4860::8888

Auswahl: IPv6-Adresse oder Domänenname

Die Zentrale sendet einen Ping-Befehl an die IPv6-Testadresse, um sicherzustellen, dass die Netzwerkkonfigurationseinstellungen korrekt sind und das Netzwerk in Betrieb ist.
Die Standard-Testadresse eignet sich für die meisten Netzwerke.

Weitere Informationen

Formate von IP-Adresse und Domainname, Seite 300

Melde-Adresse des Menüs „RPS“

Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 Test Address (Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > IPv6-Testadresse)

4.2.16 IP-Adresse des alternativen IPv4-DNS-Servers

Standardeinstellung: 0.0.0.0

Auswahl: 0.0.0.0 bis 255.255.255.255

Wenn das IP-Übertragungsgerät keine Adresse vom primären Server abrufen kann, wiederholt es den Vorgang mit dem alternativen DNS-Server. Geben Sie die IP-Adresse für den alternativen IPv4-DNS-Server ein.

Weitere Informationen

Formate von IP-Adresse und Domainname, Seite 300

RPS Menu Locations (Meldeadressen des Menüs „RPS“)

Panel Wide Parameters > Onboard Ethernet Communicator > Alternate IPv4 DNS server (Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > Alternativer IPv4-DNS-Server)
IP-Adresse

4.2.17 IP-Adresse des alternativen IPv6-DNS-Servers

Standardeinstellung:

Auswahl: 0000:0000:0000:0000:0000:0000:0000:0000 bis FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Wenn das IP-Übertragungsgerät keine Adresse vom primären Server abrufen kann, wiederholt es den Vorgang mit dem alternativen DNS-Server. Geben Sie die IP-Adresse des alternativen IPv6-DNS-Servers ein.

Weitere Informationen

Formate von IP-Adresse und Domainname, Seite 300

RPS Menu Locations (Meldeadressen des Menüs „RPS“)

Panel Wide Parameters > Onboard Ethernet Communicator > Alternate IPv6 DNS server IP address (Zentralenübergreifende Parameter > Integriertes Ethernet-Übertragungsgerät > IP-Adresse des alternativen IPv6-DNS-Servers)

4.3 Mobilfunk-Steckplatine

4.3.1 Eingehende SMS

Standardeinstellung: Yes

Auswahl:

– Aktiviert (Ja): Sie können das Modul mit eingehenden SMS-Textnachrichten konfigurieren.
– Deaktiviert (Nein): Das Modul verarbeitet keine eingehenden SMS-Textnachrichten.

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Cellular Plug-in Module > Inbound SMSB450 Cellular > Inbound SMS (Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > Eingehende SMS/B450-Mobilfunk > Eingehende SMS)

4.3.2 Session Keep Alive Period (minutes) (Dauer des Sitzungs-Keep-Alive in Minuten)

Standardeinstellung: 0

Auswahl: 0 (deaktiviert) bis 1000 (Minuten)

Zeit in Minuten zwischen Keep-Alive-Meldungen. Keep-Alive-Meldungen stellen sicher, dass eine Verbindung aktiv bleibt.

Ändern Sie die Standardeinstellung nur für gewerbliche Hochsicherheitsanwendungen gemäß UL 1610.

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Cellular Plug-in Module > Session Keep Alive PeriodKeep Alive Period (Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > Dauer des Sitzungs-Keep-Alive)

4.3.3 Inaktivitäts-Timeout (Minuten)

Standardeinstellung: 0

Auswahl: 0 (deaktiviert) bis 1000 (Minuten)

– 0 (deaktiviert) – Zentrale überwacht den Datenverkehr nicht.
– 1 bis 1000 – Die Dauer ohne Datenverkehr, bevor die Zentrale eine Sitzung beendet.

Ändern Sie die Standardeinstellung nur für gewerbliche Hochsicherheitsanwendungen gemäß UL 1610, bei denen eine Benachrichtigung bei geringer Signalstärke erforderlich ist.

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Cellular Plug-in Module > Inactivity Timeout (Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > Inaktivitäts-Timeout)

4.3.4 Reporting Delay for Low Signal Strength (sec.) (Reportverzögerung bei geringer Signalstärke in Sek.)

Standardeinstellung: 0 (deaktiviert)
Auswahl: 0 (deaktiviert), 1-3600 (Sekunden)
Dauer mit geringer Signalstärke (rote LED auf Mobilfunkübertragungsgerät), bevor die Zentrale kann ein Ereignis zur geringen Mobilfunksignalstärke erstellt.
Die Zentrale erstellt ein Wiederherstellungsereignis für geringe Mobilfunksignalstärke, wenn die Signalstärke für die Eingabezeit bei diesem Parameter für Reportverzögerung bei geringer Signalstärke gut ist (grüne LED auf Mobilfunkübertragungsgerät).

Hinweis!
UL-Anforderung
Zum Erfüllen der UL-Anforderungen darf der Eintrag für diesen Parameter 200 Sekunden nicht überschreiten.

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Cellular Plug-in Module > Reporting Delay for Low Signal Strength (Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > Reportverzögerung bei geringer Signalstärke)

4.3.5 Reporting Delay for No Towers (sec.) (Reportverzögerung bei fehlenden Funkmasten in Sek.)

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: 0
Auswahl: 0 (deaktiviert) bis 3600 (Sekunden)
Wenn das steckbare Mobilfunkmodul für die bei diesem Parameter festgelegte Sekundenzahl keine Funkmasten erkennt, erstellt die Zentrale ein Ereignis zu fehlenden Funkmasten und fehlender IP-Adresse.
Die Zentrale erstellt ein Wiederherstellungsereignis zu fehlenden Funkmasten, wenn das steckbare Mobilfunkmodul für die bei diesem Parameter festgelegte Sekundenzahl mindestens einen Funkmast erkennt.
Die Zentrale erstellt ein Wiederherstellungsereignis zur fehlenden IP-Adresse, wenn das steckbare Mobilfunkmodul innerhalb von 60 Sekunden bei mindestens einem Funkmast registriert ist und eine IP-Adresse erhalten hat.

Hinweis!

Wenn mindestens ein Funkmast verfügbar ist, 60 Sekunden Verzögerung für Ereignis „No IP Address“ (Keine IP-Adresse)

Wenn sich das steckbare Mobilfunkmodul bei mindestens einem Funkmast registriert, aber innerhalb von 60 Sekunden keine IP-Adresse erhält, erstellt die Zentrale das Ereignis „No IP Address“ (Keine IP-Adresse).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Cellular Plug-in Module > Reporting Delay for No Towers (Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > Reportverzögerung bei fehlenden Funkmasten)

4.3.6 Reportverzögerung bei nur einem Funkmast

Hinweis!

Nur B Series-Zentralen mit Firmware v2.xx

Dieser Parameter ist nur für B Series-Zentralen mit der Firmware-Version 2.xx verfügbar.

Hinweis!

Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation

Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: 1800

Auswahl: 0 (deaktiviert) bis 3600 (Sekunden)

Lassen Sie den Standardwert dieses Parameters unverändert, sofern Sie nicht von einem Vertreter von Bosch Security Systems, Inc. dazu angewiesen werden.

Wenn das steckbare Mobilfunkmodul für die bei diesem Parameter festgelegte Sekundenzahl nur einen Funkmast erkennt, erstellt die Zentrale ein Ereignis zu nur einem Funkmast.

Wenn das Mobilfunkübertragungsgerät für die bei diesem Parameter festgelegte Sekundenzahl mindestens zwei Funkmasten erkennt, erstellt die Zentrale ein Wiederherstellungsereignis zu nur einem Funkmast.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Cellular Plug-in Module > Reporting delay for single tower (Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > Reportverzögerung bei nur einem Funkmast)

4.3.7 Outgoing SMS Length (Länge ausgehender SMS)

Hinweis!

Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation

Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: 160

Auswahl: 0 (deaktiviert) bis 3600 (Zeichen)

Mobilfunkanbieter legen den Grenzwert für die Länge von SMS-Nachrichten auf 160 Zeichen fest (Standardeinstellung). SMS-Nachrichten, die diesen Grenzwert überschreiten, werden von den Anbietern zurückgewiesen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Cellular Plug-in Module > Outgoing SMS Length
(Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > Länge ausgehender SMS)

4.3.8 Name des Netzwerkzugriffspunkts (APN)

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: eaaa.bosch.vzwentp
Auswahl: 0-9, A-Z, a-Z, **-**, **:**, **.** (bis zu 99 Zeichen)
Wenn Sie den Standardnamen des Access-Point-Names (APN) ändern möchten, können Sie bis zu 99 Zeichen eingeben. Groß- und Kleinschreibung muss beachtet werden.

Zentralenfirmware-Version 3.07 oder höher
Mit Zentralenfirmware-Version 3.07 oder höher verwendet die Zentrale eine interne Liste mit Werten für Namen des Netzwerkzugangspunkts, wenn der APN-Parameter leer ist. Wenn ein steckbares B442- oder B443-Mobilfunkübertragungsgerät angeschlossen wird, sieht die interne Liste folgendermaßen aus:
– lotst.aer.net
– gne
– wyless.apn
– wyless.com.attz
Wenn ein steckbares B444-Mobilfunkübertragungsgerät angeschlossen wird, sieht die interne Liste folgendermaßen aus:
– bssd.vzwentp
– eaaa.Bosch.vzwentp

Hinweis!
Der Standard eaaa.bosch.vzwentp ist neu.
Der vorherige APN-Standard, wyless.apn, ist immer noch gültig. Es ist nicht erforderlich, den APN für vorhandene Konten zu ändern.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point Name
(Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > Name des Netzwerkzugriffspunkts)

4.3.9 Network Access Point User Name (Benutzername des Netzwerkzugriffspunkts)

Standardeinstellung: Leer
Auswahl: ASCII-Zeichen (bis zu 30)
Der Benutzername für den Netzwerkzugriffspunkt kann bis zu 30 ASCII-Zeichen lang sein. Beim Benutzernamen muss die Groß-/Kleinschreibung beachtet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point User Name
(Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > Benutzername des Netzwerkzugriffspunkts)

4.3.10 Passwort des Netzwerkzugriffspunkts

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: Leer
Auswahl: ASCII-Zeichen (bis zu 30 Zeichen)
Das Passwort für den Netzwerkzugriffspunkt kann bis zu 30 ASCII-Zeichen lang sein. Beim Passwort muss die Groß-/Kleinschreibung beachtet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point Password (Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > Passwort des Netzwerkzugriffspunkts)

4.3.11 SIM-PIN

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: Leer
Auswahl: 0-9 (min. 4 Stellen, max. 8 Stellen)
Verwenden Sie diesen Parameter nur, wenn eine PIN für SIM-Karten erforderlich ist. Wenn keine SIM-PIN erforderlich ist, lassen Sie das Feld leer.
Die SIM-PIN wird bei der Eingabe in Form von Sternchen (********) angezeigt. Wenn Sie eine ungültige SIM-PIN eingeben, wird ein Ereignis aufgezeichnet. Ein Protokoll wird nur gesendet, wenn die Protokollfunktion festgelegt ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Cellular Plug-in Module > SIM PIN (Zentralenübergreifende Parameter > Mobilfunk-Steckplatine > SIM-PIN)

4.4 Cloud Remote Connect

4.4.1 Cloud Remote Connect (Ethernet)

Standardeinstellung: Aktivieren
Auswahl: Aktivieren, Deaktivieren
Mit diesem Parameter aktivieren Sie Remote Connect, einen cloudbasierten Service von Bosch, für die Kommunikation über eine Ethernet-Verbindung.

Hinweis!
Bosch Installer Services, Remote Connect-Abonnement erforderlich
Bevor Sie Remote Connect für RPS- oder RSC-Verbindungen verwenden, müssen Sie sich bei Bosch Installer Services registrieren. Besuchen Sie die Webseite https://installerservices.boschsecurity.com/.

Melde-Adresse des Menüs „RPS“
Panel Wide Parameters > Cloud Remote Connect > Cloud Remote Connect via Ethernet (Zentralenübergreifende Parameter > Cloud Remote Connect > Cloud Remote Connect über Ethernet)

4.4.2 Cloud Remote Connect (Cellular) [Cloud Remote Connect (Mobilfunk)]

Standardeinstellung: Deaktivieren

Auswahl: Aktivieren, Deaktivieren

Mit diesem Parameter aktivieren Sie Remote Connect, den cloudbasierten Service von Bosch, für die Kommunikation über eine Mobilfunkverbindung.

Hinweis!

Bosch Installer Services, Remote Connect-Abonnement erforderlich

Bevor Sie Remote Connect für RPS- oder RSC-Verbindungen verwenden, müssen Sie sich bei Bosch Installer Services registrieren. Besuchen Sie die Webseite https://installerservices.boschsecurity.com/.

Melde-Adresse des Menüs „RPS“

Panel Wide Parameters > Cloud Remote Connect > Cloud Remote Connect via Ethernet (Zentralenübergreifende Parameter > Cloud Remote Connect > Cloud Remote Connect über Ethernet)

4.5 IP-Kameras

B5512 unterstützt Kameras 1 bis 4. B4512 unterstützt Kameras 1 bis 2.

4.5.1 Camera name (first language) [Kameraname (erste Sprache)]

Standardeinstellung: Camera # (Kameranummer)

Auswahl: 0 bis 32 Zeichen [Latin 1-8-Bit-Zeichensatz (ISO/IEC 8859-1)]

Geben Sie einen Namen für eine IP-Kamera von Bosch in der ersten Sprache der Zentrale ein. Die erste und zweite Sprache legen Sie im Fenster „Panel Data - View“ (Zentralendaten – Anzeigen) fest. Weitere Informationen finden Sie unter „Panel Data - View > Panel Info tab > Additional Info” (Zentralendaten – Anzeigen > Registerkarte ‚Zentraleninfo > Weitere Informationen).

Verfügbare Sprachen: Englisch, Spanisch, Französisch und Portugiesisch

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > IP Cameras > Camera Name (Zentralenübergreifende Parameter > IP-Kameras > Kameraname)

4.5.2 Camera name (second language) [Kameraname (zweite Sprache)]

Standardeinstellung: Leer

Auswahl: 0 bis 32 Zeichen [Latin 1-8-Bit-Zeichensatz (ISO/IEC 8859-1)]

Geben Sie einen Namen für eine IP-Kamera von Bosch in der zweiten Sprache der Zentrale ein. Die erste und zweite Sprache legen Sie im Fenster „Panel Data - View“ (Zentralendaten – Anzeigen) fest. Weitere Informationen finden Sie unter „Panel Data - View > Panel Info tab > Additional Info” (Zentralendaten – Anzeigen > Registerkarte ‚Zentraleninfo > Weitere Informationen).

Verfügbare Sprachen: Englisch, Spanisch, Französisch und Portugiesisch

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > IP Cameras > Camera Name (second language) [Zentralenübergreifende Parameter > IP-Kameras > Kameraname (zweite Sprache)]

4.5.3 URL oder IP-Adresse

Standardeinstellung: Leer

Auswahl: 0 bis 128 ASCII-Zeichen

Dieser Parameter legt die URL oder IP-Adresse für die IP-Kamera von Bosch fest.

Mit der URL oder IP-Adresse der Kamera kommuniziert die Zentrale oder die RSC-Anwendung mit der Kamera über ein Netzwerk.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > IP Cameras > URL or IP Address (Zentralenübergreifende Parameter > IP-Kameras > URL oder IP-Adresse)

4.6 Verbundene Kameras von Bosch

Produkte
- B5512 und B4512 mit integriertem IP-Übertragungsgerät
- Alle IP-Kameras von Bosch

Anwendungen
Bosch IP-Kameras eignen sich optimal für die Anwendung in kleineren Gewerben und Privathaushalten, in denen konventionelle Videointegrationshardware und -anwendungen aus Kostengründen nicht eingesetzt werden können.

Implementierung
Diese Zentrale kommuniziert mit IP-Kameras von Bosch mittels einer maschinennahen Sprache (RCP+).
Konfigurieren Sie kompatible Zentralen, um IP-Kameras von Bosch als Eingänge oder Ausgänge (oder beides) zu nutzen.

Umgebung
Installieren Sie kompatible Zentralen und IP-Kameras von Bosch im selben Netzwerk (LAN).

Konfiguration Zentrale
Konfigurieren Sie die Zentrale mit der IP-Adresse jeder einzelnen Kamera. Mit den Parametern „RCP+ Port #“ (RCP+-Port #), „Service password” (Service-Passwort) und „Supervision period (sec)“ (Überwachungsdauer in Sek.) werden die Netzwerkkommunikation und die Überwachung mit verbundenen IP-Kameras von Bosch konfiguriert.

Andere Zentralenkonfiguration für die Verwendung von IP-Kameras
Neue Melderquellenoption „IP-Kamera“ (s. Points > Point Assignments > Source) (Melder > Melderzuweisungen > Quelle)
Neue Ausgangsquellenoption „IP-Kamera“ [s. Output Parameters > Output Configuration > Output Source (Ausgangsparameter> Ausgangskonfiguration > Ausgangsquelle)]

4.6.1 RCP+ port # (RCP+-Port #)

Standardeinstellung: 1756
Auswahl: 0 - 65535
Dieser Parameter legt die Portnummer fest, die von einer Bosch IP-Kamera auf das RCP+-Protokoll überwacht wird.
Ändern Sie die Standardeinstellung „1756” nur, wenn eine IP-Kamera für die Überwachung eines anderen Ports konfiguriert ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > IP Cameras > Bosch Connected Camera > RCP+ Port # (Zentralenübergreifende Parameter > IP-Kameras > Verbundene Kamera von Bosch > RCP+-Port #)

4.6.2 Service-Passwort

Standardeinstellung: Leer
Auswahl: Leer (deaktivieren), 1 bis 32 Zeichen

Geben Sie das für den Zugriff auf die Daten der IP-Kamera von Bosch erforderliche Passwort ein.
Beim Passwort muss die Groß-/Kleinschreibung beachtet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > IP Cameras > Bosch Connected Camera > Service Password (Zentralenübergreifende Parameter > IP-Kameras > Verbundene Kamera von Bosch > Service-Passwort)

4.6.3 Supervision period (sec.) (Überwachungszeitraum in Sek.)

Standardeinstellung: 0
Auswahl: 0 (deaktiviert), 30 - 255 (Sekunden)
Die Zeitdauer, die eine Bosch IP-Kamera als fehlend signalisiert werden muss, bevor die Zentrale ein Ereignis aufgrund einer fehlenden Kamera erstellt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > IP Cameras > Bosch Connected Camera > Supervision Period (Zentralenübergreifende Parameter > IP-Kameras > Verbundene Kamera von Bosch > Überwachungszeitraum)

4.7 Live (Video)

Produkte
- B5512 und B4512 mit integriertem IP-Übertragungsgerät
- Alle IP-Kameras von Bosch
- RSC (Remote Security Control)

Anwendungen
Livevideo eignet sich optimal für kleinere Gewerbe und Privathaushalte, in denen konventionelle Videointegrationshardware und -anwendungen aus Kostengründen nicht eingesetzt werden.

Implementierung
Diese Zentrale kommuniziert mit IP-Kameras von Bosch mittels einer maschinennahen Sprache (RCP+).
Konfigurieren Sie die Zentralen, um IP-Kameras von Bosch als Eingänge oder Ausgänge (oder beides) zu nutzen.
Die Gerätekonfiguration ist unabhängig, aber nativ.

Umgebung
Installieren Sie Zentralen und IP-Kameras von Bosch im selben Netzwerk (LAN).

Konfiguration Zentrale
RSC verwendet die Parameter „Port #“ (Portnummer), „Use HTTPS?“ (HTTPS Verwenden?) „Benutzername“ und „Passwort“, um innerhalb von IP-Kameras auf Videobilder zuzugreifen.

4.7.1 Port # (Portnummer)

Standardeinstellung: 80
Auswahl: 0 - 65535
Geben Sie die Portnummer ein, die die Fernsicherheitskontrolle (RSC) für die IP-Kommunikation und die Wiedergabe von Livevideos mit der Kamera verwendet.
Ist die Live Viewer-URL einem Router zugewiesen, konfigurieren Sie den Router mit der hier eingegebenen Portnummer.
Setzen Sie diese Portnummer bei Verwendung von HTTPS auf „443“.
B5512 unterstützt Kameras 1 bis 4. B4512 unterstützt Kameras 1 bis 2. B3512 unterstützt keine Kameras.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > IP Cameras > Live (Video) > Port # (Zentralenübergreifende Parameter > IP-Kameras > Live (Video) > Portnummer)

4.7.2 Use HTTPS? (HTTPS verwenden?)

Standardeinstellung: Nein
Auswahl:
Ja: HTTPS aktivieren (verschlüsselt Daten für die sichere Kommunikation zwischen IP-Kameras von Bosch und RSC)
Nein: HTTPS deaktivieren
Wählen Sie „Ja“, wenn Live Viewer HTTPS voraussetzt.
Ist HTTPS auf „Ja“ eingestellt, setzen Sie „Panel Wide Parameters > IP Cameras > Live (Video) > Port #” (Zentralenübergreifende Parameter“ > IP-Kameras > Live (Video) > Portnummer) auf „443“.
B5512 unterstützt Kameras 1 bis 4. B4512 unterstützt Kameras 1 bis 2. B3512 unterstützt keine Kameras.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > IP Cameras > Live (Video) > Use HTTPS? (Zentralenübergreifende Parameter > IP-Kameras > Live (Video) > HTTPS verwenden?)

4.7.3 Benutzername

Standardeinstellung: Live
Auswahl: A-Z, a-z, 0-9, bis zu 32 Zeichen
Geben Sie den Benutzernamen wie in die Kamera eingegeben ein. Die RSC-Anwendung verwendet den Benutzernamen und das Passwort, um Videos von der Kamera wiederzugeben.
B5512 unterstützt Kameras 1 bis 4. B4512 unterstützt Kameras 1 bis 2. B3512 unterstützt keine Kameras.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > IP Cameras > Live (Video) > User Name [Zentralenübergreifende Parameter > IP-Kameras > Live (Video) > Benutzername]

4.7.4 Passwort

Standardeinstellung: Leer
Auswahl: A-Z, a-z, 0-9, bis zu 32 Zeichen
Geben Sie das Passwort so ein, wie es in der Kamera eingegeben ist. Die RSC-Anwendung verwendet den Benutzernamen und das Passwort, um Videos von der Kamera wiederzugeben.
B5512 unterstützt Kameras 1 bis 4. B4512 unterstützt Kameras 1 bis 2. B3512 unterstützt keine Kameras.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > IP Cameras > Live (Video) > Password (Zentralenübergreifende Parameter > IP-Kameras > Live (Video) > Passwort)

4.8 Protokollübersicht

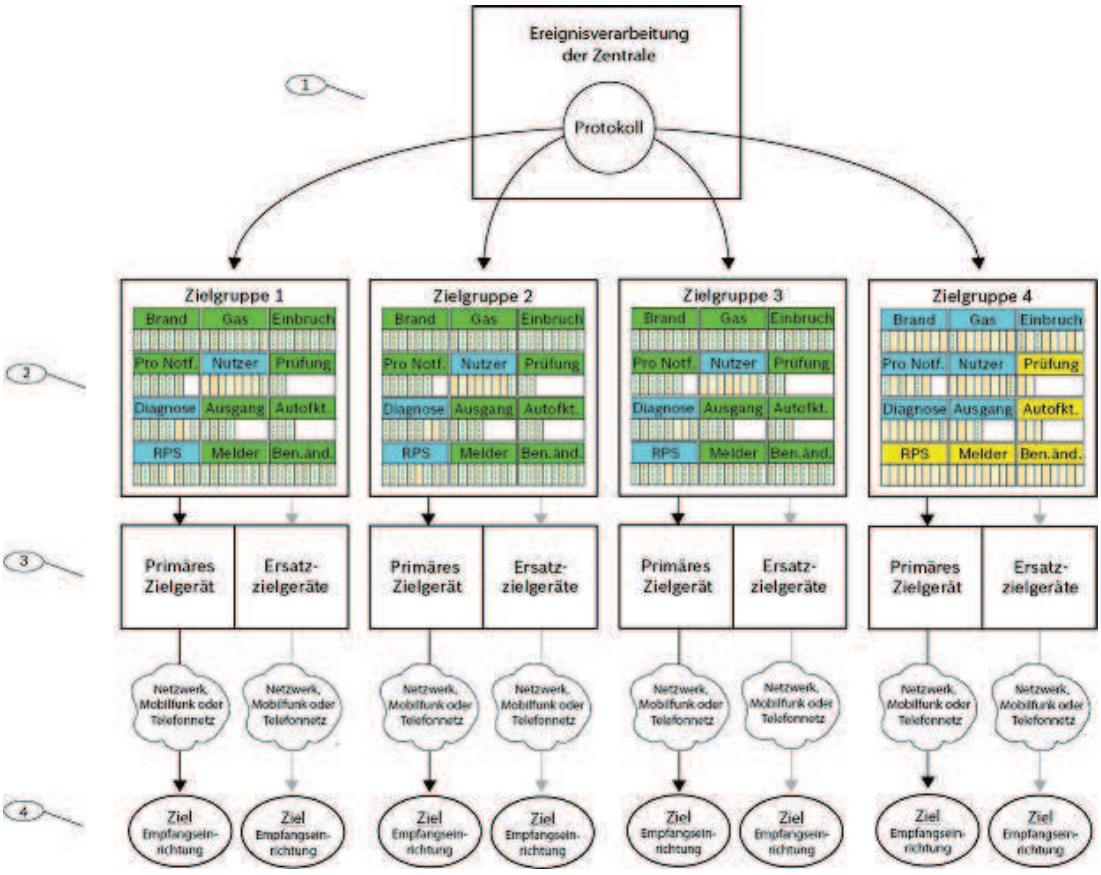


Abbildung 4.1:

1 – Protokolle beginnen mit Ereignissen

Die Zentrale überwacht Melder, Module, Bedienteile und die Stromversorgung der Zentrale (Netzstrom und Batterie) mit Blick auf nicht-normale Bedingungen. Wenn die Zentrale eine nicht-normale Bedingung (oder eine Wiederherstellung aufgrund einer nicht-normalen Bedingung) erkennt, erstellt sie ein Ereignis. Die Zentrale fügt dem Hintergrundspeicher Ereignisse hinzu und kann Ereignisse als Protokolle an einen Bedienteilempfänger oder als persönliche Benachrichtigungen an Benutzer senden.

Zu sendende Protokolle werden von der Zentrale nach Zielgruppen (1 bis 4) sortiert. Jede Zielgruppe verfügt über ein eigenes Übertragungsgerät mit einem primären Zielgerät und bis zu drei Ersatzzielgeräte (Ersatzzieladressen), um die Protokolle in der Zielgruppe an einen Bedienteilempfänger zu senden.

2 – Protokoll-Routing-Parameter

Verwenden Sie die *Report Routing (Protokoll-Routing), Seite 73* -Parameter zum Konfigurieren der vier Zielgruppen (1 bis 4). Die Parameter unterhalb der Überschrift „Report Routing“ (Protokoll-Routing) weisen Zielgruppen Protokolle nach Kategorie (z. B. alle Feuerprotokolle oder alle Einbruchprotokolle) oder individuell (z. B. Feueralarm) zu. Protokolle können auch mehreren Zielgruppen zugewiesen werden.

3 – Parameter für Übertragungsgerät

Die Parameter unterhalb der Überschrift *Übertragungsgerät – Übersicht, Seite 86* weisen jeder Zielgruppe ein primäres Zielgerät und bis zu drei Ersatzzielgeräte zu. Die Zentrale verwendet für das Senden von Protokollen zunächst das primäre Zielgerät der Zielgruppe. Wenn das

primäre Zielgerät das Protokoll nicht sendet, erstellt die Zentrale ein „Comm Trouble"-Ereignis (Kommunikationsfehler) und wechselt zum ersten Ersatzzielgerät und – falls konfiguriert – zum zweiten Ersatzzielgerät und schließlich zum dritten Ersatzzielgerät.
Die Zentrale führt maximal zehn Kommunikationsversuche aus und wechselt dabei zwischen dem primären Zielgerät und den Ersatzzielgeräten, um Protokolle einer Zielgruppe zu senden. Nach zehn erfolglosen Versuchen wird ein „Comm Fail"-Ereignis (Kommunikationsfehler) erstellt.

4 – Zieladressen

Die Zentrale sendet Protokolle aus jeder Zielgruppe mit ihrem primären Zielgerät und den Ersatzzielgeräten an die für das Gerät konfigurierte Zieladresse.
Informationen zur Konfiguration für integrierte IP-Zieladressen finden Sie hier: *Integriertes Ethernet (IP)-Übertragungsgerät, Seite 56* und hier: *Enhanced Communication (Erweiterte Kommunikation), Seite 90*.
Zur Konfiguration von IP-Zieladressen für steckbare Mobilfunkmodule siehe *Mobilfunk-Steckplatine, Seite 62* und *Enhanced Communication (Erweiterte Kommunikation), Seite 90*.
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um weitere Informationen zu erhalten.
Konfiguration für Zieladressen von steckbaren Telefonmodulen: *Telefon und Telefonparameter, Seite 53*.
Konfiguration für SDI2-Zieladressen: *(B42x) IP-Übertragungsgerät, Seite 279* oder hier: *B450 Mobilfunk, Seite 285* sowie hier: *Enhanced Communication (Erweiterte Kommunikation), Seite 90*.

Zielgruppenpriorität

Zielgruppe 1 hat die höchste Priorität. Zielgruppe 4 hat die niedrigste Priorität. Wenn Protokolle in mehreren Protokollgruppen zur gleichen Zeit gesendet werden, sendet die Zentrale zuerst Protokolle aus der Zielgruppe mit der höchsten Priorität. Liegen z. B Protokolle in Zielgruppe 2 und Zielgruppe 3 vor, sendet die Zentrale zuerst Protokolle aus Zielgruppe 2.

Priorität innerhalb einer Zielgruppe

Innerhalb einer Zielgruppe werden zu sendende Protokolle wie gezeigt priorisiert. Die Zentrale sendet Protokolle mit der höchsten Priorität zuerst. „1" signalisiert die höchste Priorität.

1. **Diagnoseprotokolle**: Zurücksetzen von Watchdog, Neustart.
   RPS-Protokolle: Fernrücksetzung.
2. **Feuerprotokolle**: Feueralarm.
3. **Gasprotokolle**: Gasalarm.
4. **Personennotfall-Protokolle**: Medizinischer Alarm, Stiller Alarm/Überfallalarm, Überfallalarm, Bedrohung.
5. **Einbruchprotokolle**: Alarmprotokoll.
6. **Feuerprotokolle**: Feuer abbrechen.
   Gasprotokolle: Gas abbrechen.
   Einbruchprotokolle: Feuerfehlalarm abbrechen.
   Diagnoseprotokolle: Fehler des SDI2-Geräts, Parameter-Prüfsummenfehler, Telefonleitung Störung, Netzstörung, Batterie fehlt, Schwache Batterie, Wiederherstellung der Batterie, Ziel-Kommunikationsfehler, Ziel-Kommunikationsfehler – Wiederherstellung.
7. **Feuerprotokolle**: Feuer –Wiederherstellung (nach Alarm), Feuer fehlt, Feuer-Störung, Feuerüberwachung, Feuer – Wiederherstellung (nach Störung), Feuerüberwachung fehlt, Wiederherstellung Feuerüberwachung).
   Gasprotokolle: Gas – Wiederherstellung bei Alarm, Gas fehlt, Gas-Störung, Gasüberwachung, Gas – Wiederherstellung bei Störung, Gasüberwachung fehlt, Gasüberwachung

Einbruchprotokolle: Feuerfehlalarm – Überwachung).
Personennotfall-Protokolle: Medizinischer Alarm – Wiederherstellung, Stiller Alarm/ Überfallalarm – Wiederherstellung, Überfallalarm – Wiederherstellung.

8. **Einbruchprotokolle**: Einbruchalarm – Wiederherstellung (nach Störung), Alarm fehlt, Störungsprotokoll, Störung fehlt, Melderbus – Fehler, Melderbus – Wiederherstellung, Alarm Wiederherstellung, Überwachung fehlt, Unbestätigtes Ereignis.
9. **Benutzerprotokolle**: Zwangsläufiger Melder, Zwangsläufig scharfgeschaltet, Zwangsläufiges Schließen, Zwangsläufiges Schließen – Unverzögerte Außenhautüberwachung, Zwangsläufiges Schließen – Verzögerte Außenhautüberwachung.
Diagnoseprotokolle: Rauchmelderwartung, Betrieb Rauchmelder Wiederherstellung.
Ausgangsprotokolle: Sensor Zurücksetzen, Ausgang festlegen, Ausgang zurücksetzen.
Autofunktionsprotokolle: Zeitgesteuerte Ereignisse ausgeführt, Zeitgesteuerte Ereignisse geändert, Fehler beim Ausführen (zeitgesteuertes Ereignis).
Melderprotokolle: Umgehen, Wiederherstellung umgehen.
Benutzeränderungsprotokolle: Stufe ändern.
10. **Einbruchprotokolle**: Benutzercode-Sabotage.
Benutzerprotokolle: Fehler beim Öffnen, Fehler beim Schließen, Schließzeit verlängern, Öffnungsprotokoll, Schließprotokoll, Melder wird geöffnet, Melder wird geschlossen, Unverzögerte Außenhautüberwachung, Verzögerte Außenhautüberwachung.
Prüfprotokolle: Statusprotokoll, Prüfprotokoll.
Diagnoseprotokolle: SDI2-Gerät – Wiederherstellung, Telefonleitung Wiederherstellung, Netzstromwiederherstellung, Prüfsummenfehler, Netzwerkfehler (und Wiederherstellung), Netzwerkzustand, HF-Interferenzstörungen (und Wiederherstellung), Geräteausfall (und Wiederherstellung), Persönliche Benachrichtigung – Kommunikationsstörung (und Wiederherstellung).
RPS-Protokolle: Schwellenwert für Ereignisprotokoll, Ereignisprotokoll – Überlauf, Parameter geändert, RPS-Zugriff OK, RPS-Zugriffsfehler, Fernrücksetzung, Parametrierung – Zugriff OK, Parametrierung – Zugriffsfehler.
Melderprotokolle: Wartung – Beginn, Wartung – Ende, Feuer-Funktionstest – Beginn, Feuer-Funktionstest – Ende, Revision – Beginn, Revision – Ende, Zusätzlicher Melder, Niedrige HF-Batteriespannung, Funkmelder-Wiederherstellung der Batterie.
Benutzeränderungsprotokolle: Datum geändert, Uhrzeitänderung, Benutzer löschen, Benutzercode geändert, Bereichsüberwachung, Funk-Handsender zugewiesen, Funk-Handsender entfernt, Stufe ändern.
Zutrittsprotokolle: Zutritt gewährt, Kein Eingang, Tür offengelassen, Tür öffnen und schließen, Tür entriegelt, Türanfrage, Tür verriegelt.

4.9 Report Routing (Protokoll-Routing)

Standardeinstellung:

Protokollkategorie	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Feuerprotokolle, Seite 74	Ja	Ja	Ja	Benutzerdefiniert
Gasprotokolle, Seite 75	Ja	Ja	Ja	Benutzerdefiniert
Einbruchprotokolle, Seite 75	Ja	Ja	Ja	Benutzerdefiniert

Protokollkategorie	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Personennotfall-Protokolle, Seite 75	Ja	Ja	Ja	Benutzerdefiniert
Benutzerprotokolle, Seite 75	Benutzerdefiniert	Benutzerdefiniert	Benutzerdefiniert	Benutzerdefiniert
Prüfprotokolle, Seite 76	Ja	Ja	Ja	Nein
Diagnoseprotokolle, Seite 76	Benutzerdefiniert	Benutzerdefiniert	Benutzerdefiniert	Benutzerdefiniert
Ausgangsprotokolle, Seite 77	Ja	Ja	Ja	Benutzerdefiniert
Autofunktionsprotokolle, Seite 77	Ja	Ja	Ja	Nein
RPS-Protokolle, Seite 77	Benutzerdefiniert	Benutzerdefiniert	Benutzerdefiniert	Nein
Melderprotokolle, Seite 77	Ja	Ja	Ja	Nein
Benutzeränderungsprotokolle, Seite 78	Ja	Ja	Ja	Nein

Auswahl:

– Ja: alle Berichte dieser Kategorie der Zielgruppe zuweisen
– Nein: keines der Protokolle dieser Kategorie der Zielgruppe zuweisen

Benutzerdefiniert: kann nicht ausgewählt werden Für eine Kategorie wird „Benutzerdefiniert“ angezeigt, wenn mindestens ein Protokoll der Kategorie individuell konfiguriert ist.

Hinweis!

Konfiguration für einzelne, beim Ändern von „Benutzerdefiniert“ auf „Ja“ oder „Nein“ verlorene Protokolle

Wenn für eine Protokollkategorie „Benutzerdefiniert“ erscheint, sind nicht alle Protokolle gleich eingestellt (alle auf „Ja“ oder alle auf „Nein“). Die Protokolle wurden einzeln festgelegt. Wenn Sie die Protokolle für eine Kategorie von „Benutzerdefiniert“ auf „Ja“ oder „Nein“ ändern, geht die Konfiguration für die einzelnen Protokolle in der Kategorie verloren. Klicken Sie im Menübaum auf die Protokollkategorie, z. B. *Feuerprotokolle, Seite 78*, um einzelne Protokolle aus einer Protokollkategorie einer Zielgruppe erneut zuzuweisen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Report Routing (Zentralenübergreifende Parameter> Protokoll-Routing)

Feuerprotokolle

Protokolle der Kategorie „Feuer“:

– Feueralarm
– Feuer – Wiederherstellung (nach Alarm)
– Feuer fehlt
– Feuer-Störung
– Feuerüberwachung
– Feuer – Wiederherstellung (nach Störung)

– Feuer Abbrechen
– Feuerüberwachung fehlt
– Wiederherstellung Feuerüberwachung

Klicken Sie im Menübaum auf *Feuerprotokolle, Seite 78*, um Protokolle der Kategorie „Feuer“ einer Zielgruppe einzeln zuzuweisen.

Gasprotokolle

Protokolle der Kategorie „Gas“:

– Gasalarm
– Gas – Wiederherstellung bei Alarm
– Gas fehlt
– Gas-Störung
– Gasüberwachung
– Gas – Wiederherstellung bei Störung
– Gas abbrechen
– Gasüberwachung fehlt
– Gasüberwachung – Wiederherstellung

Klicken Sie im Menübaum auf *Gasprotokolle, Seite 78*, um Protokolle der Kategorie „Gas“ einer Zielgruppe einzeln zuzuweisen.

Einbruchprotokolle

Protokolle der Kategorie „Einbruch“:

– Alarmprotokoll
– Einbruchalarm – Wiederherstellung (nach Störung)
– Bedrohung
– Alarm fehlt
– Benutzercode-Sabotage
– Störungsprotokoll
– Störung fehlt
– Überwachung Feuerfehlalarm
– Melderbus – Fehler
– Melder-Bus – Wiederherstellung
– Feuerfehlalarm abbrechen
– Alarm Wiederherstellung
– Überwachung fehlt
– Unbestätigtes Ereignis

Klicken Sie im Menübaum auf *Einbruchprotokolle, Seite 79*, um Protokolle der Kategorie „Einbruch“ einer Zielgruppe einzeln zuzuweisen.

Personennotfall-Protokolle

Protokolle der Kategorie „Personennotfall“:

– Medizinischer Alarm
– Medizinischer Alarm – Wiederherstellung (für spätere Verwendung reserviert)
– Stiller Alarm/Überfallalarm
– Stiller Alarm/Überfallalarm – Wiederherstellung
– Überfallalarm
– Überfallalarm – Wiederherstellung (für spätere Verwendung reserviert)

Klicken Sie im Menübaum auf *Personennotfall-Protokolle, Seite 80*, um Berichte aus der Kategorie „Personennotfall“ einer Zielgruppe einzeln zuzuweisen.

Benutzerprotokolle

Protokolle der Kategorie „Benutzer“:

- Zwangsläufiger Melder: Meldet ein Ereignis „Zwangsläufiger Melder“.
- Melder wird geöffnet: Meldet ein Melder-Öffnungsereignis.
- Melder wird geschlossen: Mit diesem Protokoll wird ein Melder-Schließereignis signalisiert.
- Zwangsläufig scharfgeschaltet: Meldet einen zwangsläufig scharfgeschalteten Melder.
- Fehler beim Öffnen: Dieses Protokoll meldet ein Ereignis „Fehler beim Öffnen“.
- Fehler beim Schließen: Mit diesem Protokoll wird ein Ereignis „Fehler beim Schließen“ kommuniziert.
- Verlängerte Schließzeit: Meldet ein Ereignis „Verlängerte Schließzeit“.
- Öffnungsprotokoll: Dieses Protokoll signalisiert Öffnungsereignisse.
- Zwangsläufiges Schließen
- Schließprotokoll
- Zwangläufiges Schließen – Unverzögerte Außenhautüberwachung
- Zwangsläufiges Schließen – Verzögerte Außenhautüberwachung
- Unverzögerte Außenhautüberwachung
- Verzögerte Außenhautüberwachung

Klicken Sie im Menübaum auf *Benutzerprotokolle, Seite 80*, um Protokolle der Kategorie „Benutzer“ einer Zielgruppe einzeln zuzuweisen.

Prüfprotokolle

Protokolle der Kategorie „Test“ (Prüfung):

- Statusprotokoll
- Prüfprotokoll

Klicken Sie im Menübaum auf *Prüfprotokolle, Seite 81*, um Protokolle der Kategorie „Test“ (Prüfung) einer Zielgruppe einzeln zuzuweisen.

Diagnoseprotokolle

Protokolle der Kategorie „Diagnose“:

- SDI2 Device Failure (Fehler des SDI2-Geräts)
- SDI2-Gerät – Wiederherstellung
- Zurücksetzen von Watchdog
- Parameter-Prüfsummenfehler
- Neustart
- Telefonleitung Störung
- Telefonleitung Wiederherstellung
- Netzstörung
- Netzstromwiederherstellung
- Batterie fehlt
- Schwache Batterie
- Wiederherstellung der Batterie
- Ziel-Kommunikationsfehler
- Wiederherstellung Zielkommunikation
- Prüfsummenfehler
- Netzwerkfehler
- Netzwerk-Wiederherstellung
- Netzwerk-Zustand
- HF-Interferenzstörungen
- HF-Interferenzstörungen – Wiederherstellung
- Geräteausfall
- Geräteausfall Wiederherstellung
- Betrieb Rauchmelder

– Betrieb Rauchmelder Wiederherstellung
– Persönliche Benachrichtigung – Kommunikationsstörung
– Persönliche Benachrichtigung – Wiederherstellung bei Kommunikationsstörung

Klicken Sie im Menübaum auf *Diagnoseprotokolle, Seite 82*, um Protokolle der Kategorie „Diagnose“ einer Zielgruppe einzeln zuzuweisen.

Ausgangsprotokolle

Protokolle der Kategorie „Output“ (Ausgang):

– Melder zurücksetzen
– Ausgang festlegen
– Ausgang zurücksetzen

Klicken Sie im Menübaum auf *Ausgangsprotokolle, Seite 83*, um Protokolle der Kategorie „Output“ (Ausgang) einer Zielgruppe einzeln zuzuweisen.

Autofunktionsprotokolle

Protokolle der Kategorie „Auto Function“ (Auto-Funktion):

– Zeitgesteuerte Ereignisse ausgeführt
– Zeitgesteuerte Ereignisse geändert
– Fehler beim Ausführen

Klicken Sie im Menübaum auf *Autofunktionsprotokolle, Seite 83*, um Protokolle der Kategorie „Auto Function“ (Autofunktion) einzeln einer Zielgruppe zuzuordnen.

RPS-Protokolle

Protokolle der Kategorie „RPS“:

– Schwellenwert Ereignisprotokoll
– Überlauf Ereignisprotokoll
– Parameter geändert
– RPS-Zugriff OK
– RPS-Zugriffsfehler
– Fernrücksetzung
– Parametrierung – Zugriff OK
– Parametrierung – Zugriffsfehler

Klicken Sie im Menübaum auf *RPS-Protokolle, Seite 84*, um Protokolle der Kategorie „RPS“ einer Zielgruppe einzeln zuzuweisen.

Melderprotokolle

Protokolle der Kategorie „Melder“:

– Beginn Betrieb
– Ende Betrieb
– Beginn Feuer-Funktionstest
– Ende Feuer-Funktionstest
– Funktionstest Start
– Funktionstest Ende
– Zusätzlicher Melder
– Meldertext senden
– Niedrige HF-Batteriespannung
– Niedrige HF-Batteriespannung – Wiederherstellung
– Abschalten
– Wiederherstellung umgehen

Klicken Sie im Menübaum auf *Melderprotokolle, Seite 84*, um Protokolle der Kategorie „Melder“ einer Zielgruppe einzeln zuzuweisen.

Benutzeränderungsprotokolle
Protokolle der Kategorie „User Change“ (Benutzeränderung) ändern:
– Datum geändert
– Uhrzeitänderung
– Benutzer löschen
– Benutzercode geändert
– Bereichsüberwachung
– Funk-Handsender zugewiesen
– Funk-Handsender entfernt
– Stufe ändern
Klicken Sie im Menübaum auf *Benutzeränderungsprotokolle, Seite 85*, um Protokolle der Kategorie „User Change“ (Benutzeränderung) einer Zielgruppe einzeln zuzuweisen.
Klicken Sie im Menübaum auf Zutrittsprotokolle, um Protokolle der Kategorie „Zugriff“ einer Zielgruppe einzeln zuzuweisen.

4.9.1 Feuerprotokolle

Standardeinstellung:

Feuerprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Feueralarm	Ja	Ja	Ja	Ja
Feuer – Wiederherstellung (nach Alarm)	Ja	Ja	Ja	Nein
Feuer fehlt	Ja	Ja	Ja	Nein
Feuer-Störung	Ja	Ja	Ja	Nein
Feuerüberwachung	Ja	Ja	Ja	Nein
Feuer – Wiederherstellung (nach Störung)	Ja	Ja	Ja	Nein
Feuer Abbrechen	Ja	Ja	Ja	Nein
Feuerüberwachung fehlt	Ja	Ja	Ja	Nein
Wiederherstellung Feuerüberwachung	Ja	Ja	Ja	Nein

Auswahl:
– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Report Routing > Fire Reports (Zentralenübergreifende Parameter > Protokoll-Routing > Feuerprotokolle)

4.9.2 Gasprotokolle

Standardeinstellung:

Gasprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Gasalarm	Ja	Ja	Ja	Ja

Gasprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Gas – Wiederherstellung bei Alarm	Ja	Ja	Ja	Nein
Gas fehlt	Ja	Ja	Ja	Nein
Gas-Störung	Ja	Ja	Ja	Nein
Gasüberwachung	Ja	Ja	Ja	Nein
Gas – Wiederherstellung bei Störung	Ja	Ja	Ja	Nein
Gas abbrechen	Ja	Ja	Ja	Nein
Gasüberwachung fehlt	Ja	Ja	Ja	Nein
Gasüberwachung – Wiederherstellung	Ja	Ja	Ja	Nein

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Report Routing > Gas Reports (Zentralenübergreifende Parameter > Protokoll-Routing > Gasprotokolle)

4.9.3 Einbruchprotokolle

Standardeinstellung:

Einbruchprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Alarmprotokoll	Ja	Ja	Ja	Ja
Einbruchalarm – Wiederherstellung (nach Alarm)	Ja	Ja	Ja	Nein
Bedrohung	Ja	Ja	Ja	Ja
Alarm fehlt	Ja	Ja	Ja	Nein
Benutzercode-Sabotage *	Ja	Ja	Ja	Nein
Störungsprotokoll	Ja	Ja	Ja	Nein
Störung fehlt	Ja	Ja	Ja	Nein
Überwachung Feuerfehlalarm	Ja	Ja	Ja	Nein
Melderbus – Fehler	Ja	Ja	Ja	Nein
Melder-Bus – Wiederherstellung	Ja	Ja	Ja	Nein
Feuerfehlalarm abbrechen	Ja	Ja	Ja	Nein

Einbruchprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Alarm Wiederherstellung	Ja	Ja	Ja	Nein
Überwachung fehlt	Ja	Ja	Ja	Nein
Unbestätigtes Ereignis	Ja	Ja	Ja	Nein

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

***** Eine Zentrale sendet ein Benutzercode-Sabotageereignis, wenn ein Benutzer 7-mal nacheinander am Bedienteil einen ungültigen Pincode eingibt.
Für Mode-2-Verbindungen, zum Beispiel für RSC-App oder Automatisierung, sendet die Zentrale ein Benutzercode-Sabotageereignis, wenn der Benutzer 15-mal in Folge ungültige Pincodes eingibt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Report Routing > Burglar Reports (Zentralenübergreifende Parameter > Protokoll-Routing > Einbruchprotokolle)

4.9.4 Personennotfall-Protokolle

Standardeinstellung:

Personennotfall-Protokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Medizinischer Alarm	Ja	Ja	Ja	Ja
Medizinischer Alarm – Wiederherstellung	Ja	Ja	Ja	Nein
Stiller Alarm/Überfallalarm	Ja	Ja	Ja	Ja
Stiller Alarm/Überfallalarm – Wiederherstellung	Ja	Ja	Ja	Nein
Überfallalarm	Ja	Ja	Ja	Ja
Überfallalarm – Wiederherstellung	Ja	Ja	Ja	Nein

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Report Routing > Personal Emergency Reports (Zentrale Breite Parameter > Protokoll-Routing > Personennotfall-Protokolle)

4.9.5 Benutzerprotokolle

Standardeinstellung:

Benutzerprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Zwangsläufiger Melder	Ja	Ja	Ja	Nein
Melder wird geöffnet	Ja	Ja	Ja	Nein

Benutzerprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Melder wird geschlossen	Ja	Ja	Ja	Nein
Wurde zwangsläufig scharfgeschaltet	Ja	Ja	Ja	Nein
Fehler beim Öffnen	Ja	Ja	Ja	Nein
Fehler beim Schließen	Ja	Ja	Ja	Nein
Verlängerte Schließzeit	Ja	Ja	Ja	Nein
Öffnungsprotokoll	Nein	Nein	Nein	Nein
Zwangsläufiges Schließen	Nein	Nein	Nein	Nein
Schließprotokoll	Nein	Nein	Nein	Nein
Zwangläufiges Schließen – Unverzögerte Außenhautüberwachung	Nein	Nein	Nein	Nein
Zwangsläufiges Schließen – Verzögerte Außenhautüberwachung	Nein	Nein	Nein	Nein
Unverzögerte Außenhautüberwachung	Nein	Nein	Nein	Nein
Verzögerte Außenhautüberwachung	Nein	Nein	Nein	Nein
Benutzertext senden	Ja	Ja	Ja	Ja

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Report Routing > User Reports (Zentralenübergreifende Parameter > Protokoll-Routing > Benutzerprotokolle)

4.9.6 Prüfprotokolle

Standardeinstellung:

Prüfprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Statusprotokoll	Ja	Ja	Ja	Nein
Prüfprotokoll	Ja	Ja	Ja	Nein

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Report Routing > Test Reports (Zentralenübergreifende Parameter > Protokoll-Routing > Prüfprotokolle)

4.9.7 Diagnoseprotokolle

Standardeinstellung:

Diagnoseprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
SDI2 Device Failure (Fehler des SDI2-Geräts)	Ja	Ja	Ja	Nein
SDI2-Gerät – Wiederherstellung	Ja	Ja	Ja	Nein
Zurücksetzen von Watchdog	Ja	Ja	Ja	Nein
Parameter-Prüfsummenfehler	Ja	Ja	Ja	Nein
Neustart	Ja	Ja	Ja	Nein
Telefonleitung Störung	Ja	Ja	Ja	Nein
Wiederherstellung nach Telefonleitungsfehler	Ja	Ja	Ja	Nein
Netzstörung	Ja	Ja	Ja	Nein
Netzstromwiederherstellung	Ja	Ja	Ja	Nein
Batterie fehlt	Ja	Ja	Ja	Nein
Schwache Batterie	Ja	Ja	Ja	Nein
Wiederherstellung der Batterie	Ja	Ja	Ja	Nein
Ziel-Kommunikationsfehler	Ja	Ja	Ja	Nein
Wiederherstellung Zielkommunikation	Ja	Ja	Ja	Nein
Prüfsummenfehler	Ja	Ja	Ja	Nein
Netzwerkfehler	Nein	Nein	Nein	Nein
Netzwerk-Wiederherstellung	Nein	Nein	Nein	Nein
Netzwerk-Zustand	Nein	Nein	Nein	Nein
HF-Interferenzstörungen	Ja	Ja	Ja	Nein
Wiederherstellung HF-Interferenzstörungen	Ja	Ja	Ja	Nein
Geräteausfall	Ja	Ja	Ja	Nein
Wiederherstellung Geräteausfall	Ja	Ja	Ja	Nein
Betrieb Rauchmelder	Ja	Ja	Ja	Nein

Diagnoseprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Wiederherstellung Rauchmelderwartung	Ja	Ja	Ja	Nein
Persönliche Benachrichtigung – Kommunikationsstörung	Nein	Nein	Nein	Nein
Persönliche Benachrichtigung – Wiederherstellung bei Kommunikationsstörung	Nein	Nein	Nein	Nein
Versionstext senden	Ja	Ja	Ja	Ja

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

Aktivieren Sie die Protokolle Ziel-Kommunikationsfehler und Wiederherstellung Zielkommunikation in nur einer Zielgruppe.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Report Routing > Diagnostic Reports (Zentralenübergreifende Parameter > Protokoll-Routing > Diagnoseprotokolle)

4.9.8 Ausgangsprotokolle

Standardeinstellung:

Ausgangsprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Melder zurücksetzen	Ja	Ja	Ja	Nein
Ausgang festlegen	Ja	Ja	Ja	Nein
Ausgang zurücksetzen	Ja	Ja	Ja	Nein
Ausgangsnamentext senden	Ja	Ja	Ja	Ja

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Report Routing > Output Reports (Zentralenübergreifende Parameter > Protokoll-Routing > Ausgangsprotokolle)

4.9.9 Autofunktionsprotokolle

Standardeinstellung:

Autofunktionsprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Zeitgesteuerte Ereignisse ausgeführt	Ja	Ja	Ja	Nein

Autofunktionsprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Zeitgesteuerte Ereignisse geändert	Ja	Ja	Ja	Nein
Fehler beim Ausführen	Ja	Ja	Ja	Nein

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Report Routing > Auto Function Reports (Zentralenübergreifende Parameter > Protokoll-Routing > Autofunktionsprotokolle)

4.9.10 RPS-Protokolle

Standardeinstellung:

RPS-Protokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Schwellenwert Ereignisprotokoll	Ja	Ja	Ja	Nein
Überlauf Ereignisprotokoll	Ja	Ja	Ja	Nein
Parameter geändert	Ja	Ja	Ja	Nein
RPS-Zugriff OK	Ja	Ja	Ja	Nein
RPS-Zugriffsfehler	Nein	Nein	Nein	Nein
Fernrücksetzung	Ja	Ja	Ja	Nein
Parametrierung – Zugriff OK	Ja	Ja	Ja	Nein
Parametrierung – Zugriffsfehler	Ja	Ja	Ja	Nein

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Report Routing > RPS Reports (Zentralenübergreifende Parameter > Protokoll-Routing > RPS-Protokolle)

4.9.11 Melderprotokolle

Standardeinstellung:

Melderprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Beginn Betrieb	Ja	Ja	Ja	Nein
Ende Betrieb	Ja	Ja	Ja	Nein
Beginn Feuer-Funktionstest	Ja	Ja	Ja	Nein
Ende Feuer-Funktionstest	Ja	Ja	Ja	Nein

Melderprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Funktionstest Start	Ja	Ja	Ja	Nein
Funktionstest Ende	Ja	Ja	Ja	Nein
Zusätzlicher Melder	Ja	Ja	Ja	Nein
Meldertext senden	Ja	Ja	Ja	Nein
Niedrige HF-Batteriespannung	Ja	Ja	Ja	Nein
Niedrige HF-Batteriespannung – Wiederherstellung	Ja	Ja	Ja	Nein
Abschalten	Ja	Ja	Ja	Nein
Wiederherstellung umgehen	Ja	Ja	Ja	Nein
Alarm bei Meldersabotage	Ja	Ja	Ja	Ja
Wiederherstellung Alarm bei Meldersabotage	Ja	Ja	Ja	Ja

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Report Routing > Point Reports (Zentralenübergreifende Parameter > Protokoll-Routing > Melderprotokolle)

4.9.12 Benutzeränderungsprotokolle

Standardeinstellung:

Benutzeränderungsprotokolle	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4
Datum geändert	Ja	Ja	Ja	Ja
Uhrzeitänderung	Ja	Ja	Ja	Nein
Benutzer löschen	Ja	Ja	Ja	Nein
Benutzercode geändert	Ja	Ja	Ja	Nein
Bereichsüberwachung	Ja	Ja	Ja	Nein
Funk-Handsender zugewiesen	Ja	Ja	Ja	Nein
Funk-Handsender entfernt	Ja	Ja	Ja	Nein
Stufe ändern	Ja	Ja	Ja	Ja

Auswahl:

– Ja: Dieses Protokoll der Zielgruppe zuweisen
– Nein: Dieses Protokoll nicht der Zielgruppe zuweisen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Report Routing > User Change Reports (Zentralenübergreifende Parameter > Protokoll-Routing > Benutzeränderungsprotokolle)

4.10 Übertragungsgerät – Übersicht

Es stehen vier Zielgruppen zur Verfügung. Protokolle sind Zielgruppen nach Kategorie (z. B. „Feuerprotokolle” oder „Einbruchprotokolle”) oder individuell (z. B. „Feueralarm“) zugewiesen. Siehe *Protokollübersicht, Seite 71*, um zu erfahren, wie Sie Protokolle einer Zielgruppe zuweisen.
Weisen Sie mit den Parametern jeder Zielgruppe ein primäres Zielgerät und bis zu drei Ersatzzielgeräte zu.
Wenn das primäre Zielgerät das Protokoll nicht senden kann, wechselt die Zentrale zum ersten Ersatzzielgerät und fährt mit allen weiteren konfigurierten Ersatzzielgeräten fort (erstes, zweites und drittes), bis das Protokoll erfolgreich gesendet wurde.

Hinweis!
B5512, B4512, B3512 V2 Zentralen haben kein zweites oder drittes Ersatzzielgerät.

Die Zentrale versucht mithilfe des primären Zielgeräts und der Ersatzzielgeräte bis zu zehnmal, Protokolle in einer Zielgruppe zu senden. Wie in der Tabelle gezeigt, wechselt die Zentrale zwischen dem primären Zielgerät und den Ersatzzielgeräten. Nach zehn erfolglosen Versuchen wird von der Zentrale ein Kommunikationsfehler-Ereignis erstellt.
Werden keine Ersatzzielgeräte konfiguriert, verwendet die Zentrale das primäre Zielgerät für alle zehn Versuche.

Konfigurierte Zieladressen	**Primäres Zielgerät und erstes Ersatzzielgerät**	**Primäre, erste und zweite Ersatzzielgeräte**	**Primäres Zielgerät, erstes, zweites und drittes Ersatzzielgerät**
Sendeversuch:			
1	Primäres Zielgerät	Primäres Zielgerät	Primäres Zielgerät
2	Primäres Zielgerät	Primäres Zielgerät	Primäres Zielgerät
3	Erstes Ersatzzielgerät	Erstes Ersatzzielgerät	Erstes Ersatzzielgerät
4	Erstes Ersatzzielgerät	Erstes Ersatzzielgerät	Erstes Ersatzzielgerät
5	Primäres Zielgerät	Zweites Ersatzzielgerät	Zweites Ersatzzielgerät
6	Erstes Ersatzzielgerät	Zweites Ersatzzielgerät	Zweites Ersatzzielgerät
7	Primäres Zielgerät	Primäres Zielgerät	Drittes Ersatzzielgerät
8	Erstes Ersatzzielgerät	Erstes Ersatzzielgerät	Drittes Ersatzzielgerät

9	Primäres Zielgerät	Zweites Ersatzzielgerät	Primäres Zielgerät
10	Erstes Ersatzzielgerät	Primäres Zielgerät	Erstes Ersatzzielgerät

COMM TROUBLE- und COMM FAIL-Ereignisse (KOMMUNIKATIONSSTÖRUNG, KOMMUNIKATIONSFEHLER)

Wenn das primäre Zielgerät nach zwei Versuchen nicht mit dem Bedienteilempfänger verbunden ist, wechselt die Zentrale zum Ersatzzielgerät. Die Zentrale sendet das ursprüngliche Protokoll zusammen mit einem COMM TROUBLE-Protokoll (KOMMUNIKATIONSSTÖRUNG). Sind keine Ersatzzielgeräte konfiguriert, wird ein COMM TROUBLE-Protokoll (KOMMUNIKATIONSSTÖRUNG) gesendet.

Die Zentrale sendet ein COMM RESTORE-Ereignis (WIEDERHERSTELLUNG KOMMUNIKATION), wenn sie über das primäre Zielgerät ein Protokoll sendet.

Wenn es sich beim primärem Zielgerät um eine IP-Zieladresse (integrierte IP-Adresse, IP-Adresse für Plug-in-Mobilfunkmodul, SDI2-Adresse 1 oder SDI2-Adresse 2) handelt, sendet die Zentrale das ursprüngliche Ereignis zusammen mit einem COMM TROUBLE-Protokoll (KOMMUNIKATIONSSTÖRUNG), das einen SDI2-Nummer-Modifizierer (SDI2 ##) enthält. Der SDI2-Modifizierer identifiziert den Typ des IP-Zielgeräts wie in den Tabellen dargestellt:

Typ der IP-Zieladresse	SDI2-Nummer-Modifizierer für IP-Zieladresse 1	SDI2-Nummer-Modifizierer für IP-Zieladresse 2	SDI2-Nummer-Modifizierer für IP-Zieladresse 3	SDI2-Nummer-Modifizierer für IP-Zieladresse 4
Integriertes Ethernet	10	20	30	40
Plug-in-Mobilfunkmodul	18	28*	38	48
SDI2-Adresse 1	11	21	31	41

* Die Bezeichnung eines COMM TROUBLE-Protokolls (KOMMUNIKATIONSSTÖRUNG) für Zielgruppe 1 mit einem „Plug-in- oder integrierten Mobilfunkmodul, Adresse 2“ zugewiesenen primären Zielgerät würde beispielsweise folgendermaßen lauten: COMM TROUBLE RG1 SDI228 (KOMMUNIKATIONSSTÖRUNG ZG SDI228).

Die Zentrale erstellt COMM TROUBLE-Ereignisse (KOMMUNIKATIONSSTÖRUNG), wenn nach der konfigurierten Anzahl an Neuversuchen keine positive Rückmeldung vom Bedienteilempfänger erfolgt ist.

Wenn alle Anmeldeversuche mit dem primären Zielgerät und den Ersatzzielgeräten scheitern, erstellt die Zentrale ein COMM FAIL RG#-Ereignis (KOMMUNIKATIONSFEHLER ZG Nr.). Bei COMM FAIL-Ereignissen (KOMMUNIKATIONSFEHLER) erstellt die Zentrale keine COMM RESTORE-Ereignisse (WIEDERHERSTELLUNG KOMMUNIKATION).

Hinweis!

CAN/ULC S304-Anforderung, anstehende Meldungen nicht löschen!

Ist „CAN/ULC S304“ auf „JA“ eingestellt, werden anstehende Protokolle von der Zentrale vor der Erstellung eines COMM FAIL-Ereignisses (KOMMUNIKATIONSFEHLER) nicht gelöscht. Die Protokolle werden in die Warteschlange eingereiht, bis eines der fehlgeschlagenen Ziele in der Zielgruppe wiederhergestellt wird. Erreicht die Warteschlange die Kapazität des Ereignisprotokolls der Zentrale, werden die ältesten Meldungen gelöscht bzw. überschrieben.

4.10.1 Primary Destination Device (Primäres Zielgerät)

Standardeinstellung: Kein Gerät

Auswahl:
- Kein Gerät
- Integrierte IP-Zieladresse 1
- Integrierte IP-Zieladresse 2
- Integrierte IP-Zieladresse 3
- Integrierte IP-Zieladresse 4
- (Plug-in-)Mobilfunkmodul – Zieladresse 1
- (Plug-in-)Mobilfunkmodul – Zieladresse 2
- (Plug-in-)Mobilfunkmodul – Zieladresse 3
- (Plug-in-)Mobilfunkmodul – Zieladresse 4
- (Plug-in-)Telefon – Zieladresse 1
- (Plug-in-)Telefon – Zieladresse 2
- (Plug-in-)Telefon – Zieladresse 3
- (Plug-in-)Telefon – Zieladresse 4
- SDI2-Adresse 1, Zieladresse 1
- SDI2-Adresse 1, Zieladresse 2
- SDI2-Adresse 1, Zieladresse 3
- SDI2-Adresse 1, Zieladresse 4

Wählen Sie das primäre Zielgerät für Zielgruppen. Über das Gerät sendet die Zentrale Protokolle an den Bedienteilempfänger.
Die Auswahl des primären Zielgeräts weist ein Übertragungsgerät (integriertes IP-Übertragungsgerät, steckbares Mobilfunkübertragungsgerät, steckbares Telefonübertragungsgerät oder SDI2-Modul) einer Zieladresse zu (*Netzwerkadresse, Seite 91* oder *Telefon und Telefonparameter, Seite 53*).

Weitere Informationen

Weitere Informationen zum Senden von Protokollen durch die Zentrale finden Sie unter *Protokollübersicht, Seite 71* und *Übertragungsgerät – Übersicht, Seite 86*.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Communicator > Primary Destination Device
(Zentralenübergreifende Parameter > Übertragungsgerät > Primäres Zielgerät)

4.10.2 Ersatzzielgeräte

Standardeinstellung: Kein Gerät

Auswahl:
- Kein Gerät
- Integrierte IP-Zieladresse 1
- Integrierte IP-Zieladresse 2
- Integrierte IP-Zieladresse 3
- Integrierte IP-Zieladresse 4
- (Plug-in-)Mobilfunkmodul – Zieladresse 1
- (Plug-in-)Mobilfunkmodul – Zieladresse 2
- (Plug-in-)Mobilfunkmodul – Zieladresse 3
- (Plug-in-)Mobilfunkmodul – Zieladresse 4
- (Plug-in-)Telefon – Zieladresse 1
- (Plug-in-)Telefon – Zieladresse 2
- (Plug-in-)Telefon – Zieladresse 3

– (Plug-in-)Telefon – Zieladresse 4
– SDI2-Adresse 1, Zieladresse 1
– SDI2-Adresse 1, Zieladresse 2
– SDI2-Adresse 1, Zieladresse 3
– SDI2-Adresse 1, Zieladresse 4

Wählen Sie bis zu drei Ersatzzielgeräte (erstes, zweites, drittes) für eine Zielgruppe. Bei Ausfall des Primärgeräts sendet die Zentrale Protokolle über das Ersatzgerät an den Bedienteilempfänger.
Die Auswahl des Ersatzzielgeräts weist ein Übertragungsgerät (integriertes IP-Übertragungsgerät, steckbares Mobilfunkübertragungsgerät, steckbares Telefonübertragungsgerät oder SDI2-Modul) einer Zieladresse zu (*Netzwerkadresse, Seite 91* oder *Telefon und Telefonparameter, Seite 53*).
Wählen Sie für eine Zielgruppe nicht dasselbe Zielgerät als primäres Zielgerät und Ersatzzielgerät.

Weitere Informationen
Weitere Informationen zum Senden von Protokollen durch die Zentrale finden Sie unter *Protokollübersicht, Seite 71* und *Übertragungsgerät – Übersicht, Seite 86*.

Melde-Adresse des Menüs „RPS“
Panel Wide Parameters > Communicator > Backup Destination Device (Zentralenübergreifende Parameter > Übertragungsgerät > Ersatzzielgerät)

4.10.3 RG Same Network Receiver (RG, selber Netzwerkempfänger)

Standardeinstellung: Yes
Auswahl:
– Ja: Die Zentrale verwendet für Primär- und Ersatzzieladressen denselben Authentifizierungsschlüssel.
– Nein: Die Zentrale verwendet für Primär- und Ersatzzieladressen unterschiedliche Authentifizierungsschlüssel.

Setzen Sie diesen Parameter in den folgenden Fällen auf Ja:
– Das primäre Zielgerät und die Ersatzzielgeräte sind unter Erweiterte Kommunikation auf IP-Geräte (Integriert, Mobilfunk oder „SDI2”) und Zieladressen konfiguriert.
– Die Zieladressen sind für dieselbe Empfangseinrichtung konfiguriert, jedoch mit verschiedenen IP-Adressen, auf die von verschiedenen Netzwerken (z. B. LAN/WAN und Internet) aus zugegriffen werden kann.

Wenn dieser Parameter auf „Ja“ gesetzt ist, die Primär- und die Ersatzzieladresse unterschiedliche Pollingraten verwenden und die Zentrale eine Kommunikationsstörung am Primär- oder Ersatzzielgerät erkennt, wechselt das funktionierende Zielgerät sofort zur schnelleren Pollingrate.
Ist dieser Parameter auf „Nein“ gesetzt, und die Zentrale erkennt eine Kommunikationsstörung am Primär- oder Ersatzzielgerät, arbeitet das funktionierende Zielgerät weiterhin mit der konfigurierten Pollingrate.
Dieser Parameter ist normalerweise auf „Nein“ eingestellt, wenn eines der Zielgeräte auf eine integrierte IP-Adresse oder ein SDI2-Gerät und das andere auf ein steckbares Mobilfunk-IP-Gerät gesetzt ist. Die Pollingrate für Mobilfunk-Zieladressen ist in der Regel auf einen niedrigen Wert (4 Stunden) eingestellt.
Pollingraten von 5 Minuten (oder schneller) könnten die Kapazitäten Ihres Mobilfunkvertrags übersteigen. Reagieren Sie auf jedes Kommunikationsstörungsereignis so schnell wie möglich.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Communicator > RG Same Network Receiver
(Zentralenübergreifende Parameter > Übertragungsgerät > ZG Gleicher Netzwerkempfänger)

4.10.4 Zeitsynchronisation

Standardeinstellung:
Zielgruppe 1: Ja
Zielgruppen 2–4: Nein
Auswahl:

- Ja: Datum und Uhrzeit der Zentrale werden mit der Empfangseinrichtung synchronisiert.
- Nein: Datum und Uhrzeit der Zentrale werden nicht mit der Empfangseinrichtung synchronisiert.

Gehen Sie folgendermaßen vor, wenn Zeitsynchronisation auf Ja eingestellt ist:

- Stellen Sie das primäre Zielgerät oder Ersatzzielgeräte auf Integriertes IP, IP über Plug-in-Mobilfunkmodul oder SDI2 ein.
- Setzen Sie das Protokollformat für die Zieladresse auf „Modem4“.

Time Synchronization“ (Zeitsynchronisation) steht für alle Zielgruppen zur Verfügung, kann jedoch nicht für mehrere Zielgruppen gleichzeitig auf „Ja“ eingestellt werden.

Zeit der Zentrale weicht um bis zu 30 Minuten von der korrekten Uhrzeit ab
Geht die Uhrzeit der Zentrale um bis zu 30 Minuten nach, werden Sekunden von der Zentrale mit einer höheren Zählfrequenz gezählt. Geht die Uhrzeit der Zentrale vor, werden Sekunden von der Zentrale mit einer niedrigeren Zählfrequenz gezählt.
Sekunden werden von der Zentrale auf diese Weise gezählt, bis die Uhrzeit der Zentrale mit dem Bedienteilempfänger synchronisiert ist. Jede Sekunde wird gezählt, und es werden keine Sekunden wiederholt. Daher werden keine zeitgesteuerten Ereignisse oder Fensteraktivierungen und -schließungen übersprungen oder wiederholt.

Uhrzeit der Zentrale weicht um mehr als 30 Minuten von der korrekten Uhrzeit ab
Weicht die Uhrzeit der Zentrale um mehr als 30 Minuten von der korrekten Uhrzeit ab, übernimmt die Zentrale das Datum und die Uhrzeit des Bedienteilempfängers.
Wenn die Änderung dazu führt, dass die Zentrale eine spätere Uhrzeit als die korrekte Uhrzeit anzeigt, werden zeitgesteuerte Ereignisse oder Fensteraktivierungen und -schließungen möglicherweise übersprungen. Führt die Änderung dazu, dass die Zentrale eine frühere Uhrzeit als die korrekte Uhrzeit anzeigt, werden zeitgesteuerte Ereignisse oder Fensteraktivierungen und -schließungen möglicherweise wiederholt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“):
Panel Wide Parameters > Communicator > Time Synchronization (Zentralenübergreifende Parameter > Übertragungsgerät > Zeitsynchronisation)

4.11 Enhanced Communication (Erweiterte Kommunikation)

4.11.1 Reporting Format (Protokollformat)

Standardeinstellungen: Conettix: Modem4
Auswahl:

- Conettix: Modem4: Die Zentrale sendet erweiterte Modem4-Kommunikationsformat-Protokolle an den Leitstellenempfänger.
- Conettix: Contact-ID: Verwenden Sie dieses Format, wenn der Leitstellenempfänger das Modem4-Format nicht unterstützt.
- DC-09: Contact-ID, TCP: Die Zentrale sendet die Contact-ID über SIA DC-09 TCP Alarmübertragungsprotokoll an Empfänger und Anwendungen.

– DC-09: Contact-ID, UDP: Die Zentrale sendet die Contact-ID über SIA DC-09 UDP Alarmübertragungsprotokoll an Empfänger und Anwendungen.
– DC-09: SIA, TCP: Die Zentrale sendet SIA-Kommunikationsformat-Protokolle über das SIA DC-09 TCP Alarmübertragungsprotokoll an Empfänger und Anwendungen.
– DC-09: SIA, UDP: Die Zentrale sendet SIA-Kommunikationsformat-Protokolle über das SIA DC-09 UDP Alarmübertragungsprotokoll an Empfänger und Anwendungen.

Wählen Sie das Protokollformat, mit dem die Zentrale Protokolle an den Leitstellenempfänger sendet.

Hinweis!
Die Auswahl für das DC-09 Protokollformat ist nicht verfügbar, wenn die europäische Anwendung in den Konformitätseinstellungen deaktiviert ist (auf „No“ (Nein) eingestellt).

Hinweis!
Zeitsynchronisation wird von Contact-ID nicht unterstützt.
Bei Auswahl von Contact-ID muss der Parameter *Zeitsynchronisation, Seite 90* auf Nein eingestellt sein.

Hinweis!
Die empfohlene Einstellung für Empfänger-Überwachungszeit beträgt 300 Sekunden oder länger bei Verwendung von DC09: SIA, TCP Alarmübertragungsprotokoll für Protokollformat.

RPS Menu Location (Melde-Adresse des Menüs „RPS“):
Panel Wide Parameters > Enhanced Communications > Reporting Format
(Zentralenübergreifende Parameter > Erweiterte Kommunikation > Protokollformat)

4.11.2 Empfänger

Standardeinstellung: k. A.
Konfigurieren Sie Protokollierungsziele, um bis zu vier unterschiedlichen Empfänger (A–D) zu nutzen.

Auswahl:
– A
– B
– C
– D

Zum Identifizieren von Zieladressen mit einem einzelnen Empfänger weisen Sie eine gemeinsame Beschriftung A, B, C oder D zu. Zum Identifizieren von unterschiedlichen Empfängern, weisen Sie eine individuelle Beschriftung A, B, C oder D zu.

Melde-Adresse des Menüs „RPS“
Panel Wide Parameters > Enhanced Communications > Receiver (Zentralenübergreifende Parameter > Erweiterte Kommunikation > Empfänger)

4.11.3 Netzwerkadresse

Standardeinstellung: Leer
Auswahl: IPv4-Adresse (0.0.0.0 bis 255.255.255.255) oder Hostname (bis zu 255 Zeichen)
Zum Weiterleiten von Ereignissen an eine IP-Adresse (in einer privaten LAN- oder WAN-Anwendung) wählen Sie eine Zieladresse (Zieladresse 1 – Zieladresse 4), und geben Sie hier die IP-Adresse für dieses Ziel ein.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Enhanced Communications > Network Address (Destinations 1-4)
[Zentralenübergreifende Parameter > Erweiterte Kommunikation > Netzwerkadresse (Zieladressen 1 – 4)]

4.11.4 Portnummer

Standardeinstellung: 7700
Auswahl: 1 bis 65535
Behalten Sie bei der IP-Kommunikation mit einem Bedienteilempfänger in gewöhnlichen Einrichtungen die Port-Standardeinstellung bei.

Hinweis!
Portnummer größer als „1023” wählen, um die Menge an unerwünschtem Datenverkehr zu begrenzen
Wenn Sie die Standardeinstellung für die Portnummer ändern möchten, wählen Sie eine Portnummer größer als „1023”, um die Menge an unerwünschtem Netzwerkverkehr zu reduzieren.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Enhanced Communications > Port Number (Destination 1 to 4)
[Zentralenübergreifende Parameter > Erweiterte Kommunikation > Portnummer (Zieladresse 1 bis 4)]

4.11.5 Receiver Supervision Time (Empfängerüberwachungsdauer)

Standardeinstellung: 4 Stunden – mittlere Sicherheit
Auswahl:
- 200 Sekunden – UL1610
- 300 Sekunden – NFPA 72 2010
- 1 Stunde – NFPA 72 2013
- 4 Stunden – mittlere Sicherheit
- 24 Stunden – täglich
- 25 – Stunden
- 90 Sekunden – hohe Sicherheit
- Ohne Polling
- 95–195, 205–1.275 Sekunden – Auswahlmöglichkeiten in Intervallen von 5 Sekunden
- 2, 3, 5–23, 26–255 Stunden
- Benutzerdefiniert

Mit Ausnahme der Auswahl Benutzerdefiniert legt die Einstellung der Überwachungsdauer des Empfängers automatisch die Parameter Pollingrate, Bestätigungswartezeit und Anzahl der Wiederholungsversuche fest.
Mit den Parametern Pollingrate, ACK-Wartezeit und Anzahl der Wiederholungsversuche wird die Überwachung von Netzwerkverbindungen mit dem Leitstellenempfänger für die Zieladressen 1 bis 4 konfiguriert.

Hinweis!
Die empfohlene Einstellung für Empfänger-Überwachungszeit beträgt 300 Sekunden oder länger bei Verwendung von DC09: SIA, TCP Alarmübertragungsprotokoll für Protokollformat.

Der Parameter „Poll Rate ” (Pollingrate) legt die Zeitdauer zwischen Anfragen fest, die die Zentrale an den Bedienteilempfänger sendet.
Über den Parameter „ACK Wait” (Bestätigungswartezeit) wird festgelegt, wie lange die Zentrale wartet, bis der Bedienteilempfänger die Bestätigung (ACK) eines Pollings sendet. Wird die Rückmeldung nicht empfangen, sendet die Zentrale das Polling entsprechend der Zahl der Eingabeversuche, die im Parameter „Retry Count“ (Anzahl der Wiederholungsversuche) eingegeben wurde. Ist die Wiederholungsanzahl erreicht, wird von der Zentrale ein „Comm Fail ##”-Ereignis (Kommunikationsfehler Nr.) erstellt. (Den korrekten Wert entnehmen Sie bitte der folgenden Tabelle.)

Gerät	Zieladresse 1	Zieladresse 2	Zieladresse 3	Zieladresse 4
SDI2-1	11	21	31	41
Onboard Ethernet (Integriertes Ethernet)	10	20	30	40
Onboard Cellular (Integrierter Mobilfunk)	18	28	38	48

Selbst nach einem „Comm Fail ##“-Ereignis (Kommunikationsfehler Nr.) sendet die Zentrale alle 10 Sekunden ein Polling, bis sie eine Bestätigung erhält.
Erhält die Zentrale eine Bestätigung vom Bedienteil, verwendet sie wieder die normale Pollingrate.

Mehrere Netzwerk-Zieladressen
Sind mehrere Netzwerk-Zieladressen konfiguriert, werden diese von der Zentrale der Reihe nach verwendet. Wenn z. B. die Bestätigung von Zieladresse 1 nicht innerhalb von 10 Sekunden empfangen wird, wechselt die Zentrale zum Senden des Pollings zu Adresse 2 und wartet dann auf das ACK, bevor sie erneut versucht, das Polling über SDI-Zieladresse 1 zu senden.
Wenn die Anzahl an Pollings, die von einer SDI-Zieladresse gesendet wurden, und die ACK-Wartezeit (Zieladressen 1 bis 4) überschritten sind, tritt ein COMM FAIL ##-Ereignis (KOMMUNIKATIONSFEHLER Nr.) ein. Bei diesem Ereignis werden alle an diese Zieladresse weitergeleiteten Ereignisse sofort an die Ersatzzieladresse gesendet.

Hinweis!
Legen Sie diesen Parameter beim Senden von Protokollen an einen Bedienteilempfänger über eine Netzwerk-Zieladresse auf einen Wert ungleich 0 fest. Ein Fehler beim Parametrieren eines Werts für diesen Parameter führt möglicherweise dazu, dass der Normalzustand eines gestörten Netzwerkkommunikationsziels nicht wiederhergestellt wird.

Ist die Zentrale so parametriert, dass sie ein Polling an den Bedienteilempfänger sendet, hält eine Rate von 75 Sekunden die virtuelle Verbindung in den meisten Netzwerkkonfigurationen aufrecht. Das Reduzieren dieses Werts für diesen Parameter führt zur Erhöhung der inaktiven Kommunikation zwischen dem SDI2-Gerät und dem Bedienteilempfänger. Erhöhte inaktive Kommunikation zwischen der Zentrale und dem Empfänger verringert die Effizienz der Zentrale beim Protokollieren von Ereignissen.

Ist die Zentrale über eine Onlineverbindung mit RPS verbunden, passt sie die Pollingrate vorübergehend von weniger als 300 Sekunden auf 300 Sekunden an. Nach dem Ende der RPS-Sitzung hat die Pollingrate wieder den parametrierten Wert.
Bei der ersten Auswahl von „Benutzerdefiniert“ sind die Parameter *Poll Rate (sec.) (Pollingrate in Sek.), Seite 94*, *ACK Wait Time (sec.) (ACK-Wartezeit in Sek.), Seite 95*und *Retry Count (Anzahl der Wiederholungsversuche), Seite 96* auf den Standardwert „Null“ eingestellt. Beim Ändern der Standardeinstellung dieser Parameter behält RPS die Werte auch dann bei, wenn der Parameter „Receiver Supervision Time“ (Überwachungsdauer des Empfängers) über die Auswahl „Benutzerdefiniert“ geändert wird. Ist „Benutzerdefiniert“ erneut ausgewählt, werden die Parameter „Poll Rate“ (Pollingrate), „ACK Wait“ (Bestätigungswartezeit) und „Retry Count“ (Anzahl der Wiederholungsversuche) auf die gespeicherten Werte zurückgesetzt.

Hinweis!
Die Einstellung der Überwachungsdauer des Empfängers ist für einen optimierten Mobilfunkdienst von entscheidender Bedeutung.
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um überhöhte monatliche Gebühren zu vermeiden und sicherzustellen, dass dieser Parameter korrekt eingestellt ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Enhanced Communication > Receiver Supervision Time
(Zentralenübergreifende Parameter > Erweiterte Kommunikation > Überwachungsdauer des Empfängers)

4.11.6 Poll Rate (sec.) (Pollingrate in Sek.)

Standardeinstellung: 12600 (bei standardmäßiger Einstellung des Parameters „Receiver Supervision Time“ (Überwachungsdauer des Empfängers) auf „4 Stunden“. Der Wert beträgt „0“, wenn der Parameter „Receiver Supervision Time“ (Überwachungsdauer des Empfängers) zunächst auf „Benutzerdefiniert“ eingestellt ist.
Auswahl: (Sekunden)
- 0: Die Pollingrate ist deaktiviert.
- 5 bis 65534: aktiviert die Pollingrate für die hier parametrierte Zeitdauer (in Sekunden)
- 65535: Das Polling erfolgt einmal täglich.

Zum Bearbeiten dieses Pollingratenparameters muss der Parameter „Receiver Supervision Time“ (Überwachungsdauer des Empfängers) auf „Benutzerdefiniert“ gesetzt sein. Geben Sie den Zeitabstand (in Sekunden) ein, in dem die Zentrale ein Polling an den Bedienteilempfänger sendet.
- 5 Minuten = 300 Sekunden
- 1 Stunde = 3600 Sekunden
- 12 Stunden = 43.200 Sekunden
- 18 Stunden = 64.800 Sekunden

Hinweis!
Zum Bearbeiten der Parameter *Poll Rate (sec.) (Pollingrate in Sek.), Seite 94*, *ACK Wait Time (sec.) (ACK-Wartezeit in Sek.), Seite 95* und *Retry Count (Anzahl der Wiederholungsversuche), Seite 96* setzen Sie den Parameter *Receiver Supervision Time (Empfängerüberwachungsdauer), Seite 92* auf „Benutzerdefiniert".
Bei der ersten Auswahl von „Benutzerdefiniert" sind die Parameter *Poll Rate (sec.) (Pollingrate in Sek.), Seite 94*, *ACK Wait Time (sec.) (ACK-Wartezeit in Sek.), Seite 95* und *Retry Count (Anzahl der Wiederholungsversuche), Seite 96* auf den Standardwert „Null" eingestellt. Beim Ändern der Standardeinstellung dieser Parameter behält RPS die Werte auch dann bei, wenn der Parameter „Receiver Supervision Time" (Überwachungsdauer des Empfängers) über die Auswahl „Benutzerdefiniert" geändert wird. Bei erneuter Auswahl von „Benutzerdefiniert" werden die Parameter „Poll Rate" (Pollingrate), „ACK Wait" (Bestätigungswartezeit) und „Retry Count" (Anzahl der Wiederholungsversuche) auf die gespeicherten Werte zurückgesetzt.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Panel Wide Parameters > Enhanced Communications > Poll Rate (Zentralenübergreifende Parameter > Erweiterte Kommunikation > Pollingrate)

4.11.7 ACK Wait Time (sec.) (ACK-Wartezeit in Sek.)

Standardeinstellung: „300" (bei standardmäßiger Einstellung des Parameters „Receiver Supervision Time" (Überwachungsdauer des Empfängers) auf „4 Stunden"). Der Wert beträgt „0", wenn der Parameter „Receiver Supervision Time" (Überwachungsdauer des Empfängers) zunächst auf „Benutzerdefiniert" eingestellt ist.
Auswahl: 5 bis 65535 (Sekunden)
Zum Bearbeiten dieses ACK-Wartezeit-Parameters muss der Parameter „Receiver Supervision Time" (Überwachungsdauer des Empfängers) auf „Benutzerdefiniert" gesetzt sein. Geben Sie an, wie lange die Zentrale wartet, bis sie eine Rückmeldung des Bedienteilempfängers auf Pollings oder Protokolle (Ereignisse) erhält. Bei Protokollen wartet die Zentrale vor dem Senden einer neuen Anfrage maximal 15 Sekunden.

Hinweis!
Zum Bearbeiten der Parameter *Poll Rate (sec.) (Pollingrate in Sek.), Seite 94*, *ACK Wait Time (sec.) (ACK-Wartezeit in Sek.), Seite 95* und *Retry Count (Anzahl der Wiederholungsversuche), Seite 96* setzen Sie den Parameter *Receiver Supervision Time (Empfängerüberwachungsdauer), Seite 92* auf „Benutzerdefiniert".
Bei der ersten Auswahl von „Benutzerdefiniert" sind die Parameter *Poll Rate (sec.) (Pollingrate in Sek.), Seite 94*, *ACK Wait Time (sec.) (ACK-Wartezeit in Sek.), Seite 95* und *Retry Count (Anzahl der Wiederholungsversuche), Seite 96* auf den Standardwert „Null" eingestellt. Beim Ändern der Standardeinstellung dieser Parameter behält RPS die Werte auch dann bei, wenn der Parameter „Receiver Supervision Time" (Überwachungsdauer des Empfängers) über die Auswahl „Benutzerdefiniert" geändert wird. Bei erneuter Auswahl von „Benutzerdefiniert" werden die Parameter „Poll Rate" (Pollingrate), „ACK Wait" (Bestätigungswartezeit) und „Retry Count" (Anzahl der Wiederholungsversuche) auf die gespeicherten Werte zurückgesetzt.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Panel Wide Parameters > Enhanced Communications > ACK Wait Time (Zentralenübergreifende Parameter > Erweiterte Kommunikation > ACK-Wartezeit)

4.11.8 Retry Count (Anzahl der Wiederholungsversuche)

Standardeinstellung: „5“ (bei standardmäßiger Einstellung des Parameters „Receiver Supervision Time“ (Überwachungsdauer des Empfängers) auf „4 Stunden“). Der Wert beträgt „0“, wenn der Parameter „Receiver Supervision Time“ (Überwachungsdauer des Empfängers) zunächst auf „Benutzerdefiniert“ eingestellt ist.

Auswahl:

0: Dauer der Wiederholungsversuche Keine Kommunikationsfehlerereignisse für Polling
1 bis 255: Dieser Wert gibt an, wie oft die Zentrale das Polling erneut sendet.
Geben Sie ein, wie oft die Zentrale das Polling vor der Erstellung eines COMM FAIL SDI2 ##-Ereignisses (KOMMUNIKATIONSFEHLER SDI2 Nr.) erneut sendet. (Den korrekten Wert entnehmen Sie bitte der folgenden Tabelle.)

Gerät	Zieladresse 1	Zieladresse 2	Zieladresse 3	Zieladresse 4
SDI2-1	11	21	31	41
Onboard Ethernet (Integriertes Ethernet)	10	20	30	40
Onboard Cellular (Integrierter Mobilfunk)	18	28	38	48

Hinweis!

Zum Bearbeiten der Parameter *Poll Rate (sec.) (Pollingrate in Sek.), Seite 94*, *ACK Wait Time (sec.) (ACK-Wartezeit in Sek.), Seite 95* und *Retry Count (Anzahl der Wiederholungsversuche), Seite 96* setzen Sie den Parameter *Receiver Supervision Time (Empfängerüberwachungsdauer), Seite 92* auf „Benutzerdefiniert“.

Bei der ersten Auswahl von „Benutzerdefiniert“ sind die Parameter *Poll Rate (sec.) (Pollingrate in Sek.), Seite 94*, *ACK Wait Time (sec.) (ACK-Wartezeit in Sek.), Seite 95* und *Retry Count (Anzahl der Wiederholungsversuche), Seite 96* auf den Standardwert „Null“ eingestellt. Beim Ändern der Standardeinstellung dieser Parameter behält RPS die Werte auch dann bei, wenn der Parameter „Receiver Supervision Time“ (Überwachungsdauer des Empfängers) über die Auswahl „Benutzerdefiniert“ geändert wird. Bei erneuter Auswahl von „Benutzerdefiniert“ werden die Parameter „Poll Rate“ (Pollingrate), „ACK Wait“ (Bestätigungswartezeit) und „Retry Count“ (Anzahl der Wiederholungsversuche) auf die gespeicherten Werte zurückgesetzt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Enhanced Communications > Retry Count (Zentralenübergreifende Parameter > Erweiterte Kommunikation > Anzahl der Wiederholungsversuche)

4.11.9 Größe des AES-Schlüssels

Standardeinstellung: No Encryption

Auswahl:

- No Encryption
- 128-Bit – 16 Byte
- 192-Bit – 24 Byte
- 256-Bit – 32 Byte

Wählen Sie die Größe des AES-Schlüssels aus.

RPS Menu Location (Melde-Adresse des Menüs „RPS“):
Panel Wide Parameters > Enhanced Communications > AES Key Size (Zentralenübergreifende Parameter > Erweiterte Kommunikation > Größe des AES-Schlüssels)

4.11.10 AES-Verschlüsselungsschlüssel

Standardeinstellung: <Standard> (nicht verschlüsselt)
Auswahl: 32 Hexadezimalzeichen, dargestellt in Form einer ID (01 bis 100).
Mit diesem Parameter konfigurieren Sie jede Empfänger-Zieladresse mit einem eindeutigen AES-Verschlüsselungsschlüssel.
Der AES-Verschlüsselungsschlüssel basiert auf der *Größe des AES-Schlüssels, Seite 96*. Bei der Konfiguration des Verschlüsselungsschlüssels werden nur Schlüssel-ID und -Name angezeigt. Wenn mindestens zwei Netzwerk-Zieladressen dieselbe Netzwerkadresse haben, teilt RPS dem Bediener mit, dass für diese Netzwerk-Zieladressen der gleiche Verschlüsselungsschlüssel verwendet werden muss.
Zeichenketten des AES-Schlüssels werden unter „Config > System > Encryption Key Tab“ (Konfiguration > System > Registerkarte „Verschlüsselungsschlüssel“) konfiguriert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Enhanced Communications > AES Encryption Key (Zentralenübergreifende Parameter > Erweiterte Kommunikation > AES-Verschlüsselungsschlüssel)

4.12 SDI2 RPS/Enhanced Communication (SDI2 RPS/Erweiterte Kommunikation)

4.12.1 Enable Enhanced Communication? (Erweiterte Kommunikation aktivieren?)

Standardeinstellung: „Ja“
Auswahl:
- Ja: Ermöglicht Protokollierung über ein IP-Übertragungsgerät [„Integriert”, „Plug-in cellular” (Steckbares Mobilfunkübertragungsgerät) oder „SDI2”].
- Nein: Deaktiviert Protokollierung über ein IP-Übertragungsgerät.

Zur Aktivierung der Protokollierung mit einem IP-Übertragungsgerät [„Integriert”, „Plug-in cellular” (Steckbares Mobilfunkübertragungsgerät) oder „SDI2”] setzen Sie diesen Parameter auf „Ja“.
Setzen Sie das *Primary Destination Device (Primäres Zielgerät), Seite 88* oder *Ersatzzielgeräte, Seite 88* für mindestens eine Zielgruppe auf eine integrierte IP-Adresse, ein steckbares Mobilfunkgerät oder ein SDI2-Gerät.

4.12.2 Answer RPS Over Network? (RPS über Netzwerk antworten?)

Standardeinstellung: „Ja“
Auswahl:
- Ja: ermöglicht automatische, per RPS initiierte Verbindungen über das integrierte Ethernet-Übertragungsgerät oder ein Netzwerk-Schnittstellenmodul auf dem SDI2-Bus.
- Nein: verhindert automatische, per RPS initiierte Verbindungen über das Netzwerk.

Ist „Nein“ ausgewählt, werden per RPS initiierte Verbindungen an einem Bedienteil durch Auswahl von „Verbinden“ im Menü „RPS“ [Actions > RPS > Answer (Maßnahmen > RPS > Verbinden)] akzeptiert.

Hinweis!

Service-Mode ermöglicht RPS-Verbindungen über ein Netzwerk

Wenn sich die Zentrale im Service-Mode befindet, akzeptiert sie automatisch per RPS initiierte Verbindungen über das Netzwerk – auch wenn dieser Parameter auf „Nein“ gesetzt ist.

Um die Zentrale in den erweiterten Modus zu versetzen, drücken Sie die RESET-Taste der Zentrale. Halten Sie sie solange gedrückt, bis die Heartbeat-LED schnell blinkt. Auf Bedienteilen erscheint „SERVICE-MODE“, und Sie werden zur Eingabe des Installationspincodes aufgefordert. Geben Sie den Installationspincode ein, und drücken Sie dann die Eingabetaste.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > SDI RPS/Enhanced Communication > Answer RPS Over Network (Zentralenübergreifende Parameter > SDI – RPS/Erweiterte Kommunikation > RPS über Netzwerk antworten)

4.12.3 RPS-Adressenverifizierung

Standardeinstellung: Nein

Auswahl:

- Ja: Die Zentrale überprüft, ob die IP-Adresse, von der aus RPS eine Verbindung herzustellen versucht, mit der RPS-Netzwerkadresse übereinstimmt.
- Nein: RPS kann über jede IP-Adresse eine Verbindung mit der Zentrale herstellen.

Weitere Informationen

RPS-Netzwerkadresse, Seite 98

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > SDI RPS/Enhanced Communication > RPS Address Verification (Zentralenübergreifende Parameter > SDI RPS/Erweiterte Kommunikation > RPS-Adressenverifizierung)

4.12.4 RPS-Netzwerkadresse

Standardeinstellung: Leer

Auswahl: IPv4-Adresse oder Hostname

Geben Sie die IP-Adresse oder den Hostnamen für RPS ein.

Wenden Sie sich an den Netzwerkadministrator, um zu erfahren, mit welcher IP-Adresse oder mit welchem Hostnamen Ihr RPS-Computer verbunden ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > SDI RPS/Enhanced Communication > RPS Network Address (Zentralenübergreifende Parameter > SDI RPS/Erweiterte Kommunikation > RPS-Netzwerkadresse)

4.12.5 RPS-Portnummer

Standardeinstellung: 7750

Auswahl: 1 bis 65535

Geben Sie den UDP-Zielport für mittels Zentrale initiierte RPS-Netzwerksitzungen ein.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > SDI RPS/Enhanced Communication > RPS Port Number (Zentralenübergreifende Parameter > SDI – RPS/Erweiterte Kommunikation > RPS-Portnummer)

4.13 Überwachung der Stromversorgung

4.13.1 Netzstromausfallzeit

Standardeinstellung: 01:00

Auswahl: 00:01 bis 90:00 (Minuten: Sekunden)

Geben Sie die Stromausfalldauer an, nach deren Ablauf die Zentrale ein Netzstromausfallprotokoll sendet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Power Supervision > AC Fail Time (Zentralenübergreifende Parameter > Überwachung der Stromversorgung > Netzstromausfallzeit)

4.13.2 Resend AC Fail (Netzstromfehler erneut senden)

Standardeinstellung: Keine Meldungen

Auswahl:

- Kein Protokoll: Netzstromausfallprotokoll nicht erneut senden
- Nach 6 Stunden: Netzstromausfallprotokoll nach 6 Stunden erneut an das Bedienteil senden.
- Nach 12 Stunden: Netzstromausfallprotokoll nach 12 Stunden erneut an das Bedienteil senden.

Die Zeit ohne Wiederherstellung der Netzstromversorgung, die die Zentrale wartet, bis erneut ein Netzstromausfallprotokoll gesendet wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Power Supervision > Resend AC Fail (Zentralenübergreifende Parameter > Überwachung der Stromversorgung > Netzstromfehler erneut senden)

4.13.3 AC Fail Display (Anzeige Netzstromfehler)

Standardeinstellung: 60

Auswahl: 10 bis 300 (Sekunden) (in Schritten von 5 Sekunden)

Zeitdauer, die die Zentrale wartet, bis auf Bedienteilen „Netzstromfehler“ angezeigt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Power Supervision > AC Fail Display (Zentralenübergreifende Parameter > Überwachung der Stromversorgung > Anzeige Netzstromfehler)

4.13.4 Netzstromfehler-/Netzstromwiederherstellungsprotokoll

Standardeinstellung: Nein

Auswahl:

- Ja: Netzstromfehler- und Netzstromwiederherstellungsprotokoll senden
- Nein: kein Netzstromfehler- und Netzstromwiederherstellungsprotokoll senden

Die Zentrale wartet die im Parameter „Netzstromausfallzeit“ eingestellte Zeit, bis Netzstromausfallprotokolle gesendet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Power Supervision > AC Fail/Restoral Report (Zentralenübergreifende Parameter > Überwachung der Stromversorgung > Netzstromfehler-/Netzstromwiederherstellungsprotokoll)

4.13.5 AC Tag Along (Netzstromprotokoll angehängt)

Standardeinstellung: Ja

Auswahl:

- Ja: Nur senden, wenn andere Ereignisse auftreten, während die Netzspannung nicht vorhanden ist.

– Nein: Keine Protokolle für Netzspannungsausfall als angehängte Ereignisse senden.

Die Zentrale sendet angehängte Protokolle für Netzspannungsausfall nur, wenn bei Netzspannungsausfall ein anderes Ereignis auftritt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Power Supervision > AC Tag Along (Zentralenübergreifende Parameter > Überwachung der Stromversorgung > Netzstromprotokoll angehängt)

4.13.6 AC / Battery Buzz (Netzstrom-/Batterie-Störungston)

Standardeinstellung: Nein

Auswahl:

– Ja: bei Wechselspannungsfehler, niedriger Batteriespannung und fehlender Batterie zentralenweiten Störungston an allen Bedienteilen ausgeben
– Nein: bei Wechselspannungsfehler, niedriger Batteriespannung und fehlender Batterie keinen zentralenweiten Störungston ausgeben

Dieser Parameter verhindert nicht, dass am Bedienteil „Wechselspannungsfehler“ oder „low battery“ (Niedrige Batteriespannung) angezeigt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Power Supervision > AC/Battery Buzz (Zentralenübergreifende Parameter > Überwachung der Stromversorgung > Netzstrom-/Batterie-Störungston)

4.13.7 Batteriefehler-/Batteriewiederherstellungsprotokoll

Standardeinstellung: Yes

Auswahl:

– Ja: Die Zentrale sendet Batteriefehler- und Batteriewiederherstellungsprotokolle an den Bedienteilempfänger.
– Nein: Batteriestörungs- und Batteriewiederherstellungsprotokolle werden NICHT an das Bedienteil gesendet. Mit diesem Parameter wird festgelegt, ob bei fehlender Batterie oder niedriger Batteriespannung ein Protokoll gesendet wird.

Batteriestörungs- und Batteriewiederherstellungsprotokolle werden an Zielgeräte geleitet. Diese Zielgeräte sind Zielgruppen zugewiesen, die für Diagnoseprotokolle konfiguriert sind. Die Batterie muss 16 Sekunden lang auf unter 12,1 VDC entladen werden, bevor die Zentrale auf eine niedrige Batteriespannung reagiert. Es dauert zwischen 10 und 60 Sekunden, bis das Fehlen einer Batterie erkannt wird.

Modem-Protokolle: BATTERY MISSING (BATTERIE FEHLT) bei „Fehlt” oder „Kurzgeschlossen”, BATTERY LOW (BATTERIESTÖRUNG) bei Entladung unterhalb von 12.1 VDC.

Kontakt-ID-Protokolle: bei „Fehlt“ oder „Kurzgeschlossen“ BATTERY MISSING/DEAD (BATTERY FEHLT/LEER); bei Entladung unter 12,1 VDC LOW SYSTEM BATTERY (SCHWACHE SYSTEMBATTERIE)

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Power Supervision > Battery Fail/Restoral Report (Zentralenübergreifende Parameter > Überwachung der Stromversorgung > Batteriefehler-/Batteriewiederherstellungsprotokoll)

4.14 RPS-Parameter

4.14.1 RPS-Zugangscode

Standardeinstellung: 999999

Auswahl: 6 bis 24 alphanumerische Zeichen (keine Leerzeichen für Zugangscode verwenden – beim Zugangscode muss die Groß-/Kleinschreibung beachtet werden).

Dies ist der Zugangscode, der von RPS gespeichert und für die Verbindungsherstellung mit der Zentrale verwendet wird.

Hinweis!
WICHTIG! Alle Zentralen werden mit einem werkseitigen Standard-Zugangscode ausgeliefert. Erstellen und synchronisieren Sie einen neuen, nicht standardmäßigen RPS-Zugangscode in Ihrer Zentralen-Kontokonfiguration, um den Zugriff auf die Zentrale zu sichern und Verbindungen mit ihr zu steuern.

Beim ersten Verbindungsaufbau mit der Zentrale muss im Fenster „Verbindung“ der werkseitige Standard-Zugangscode als RPS-Zugangscode verwendet werden. Wenn die Verbindung hergestellt ist, können Benutzer den RPS-Zugangscode durch Konfiguration oder Synchronisierung ändern.

– Bei neuen Zentralen mit Firmware v3.09+ und B465 Modulen mit Firmware v2.09+ müssen Sie den werkseitigen Cloud-ID-Standard-Zugangscode verwenden. Diesen für jede Zentrale einzigartigen Zugangscode finden Sie auf dem Etikett der jeweiligen Zentrale.
– Bei älteren Zentralen mit Firmware vor v3.09 und B465 Modulen mit Firmware vor v2.09 müssen Sie den werkseitigen Standard-Zugangscode 999999 verwenden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > RPS Parameters > RPS Passcode (Zentralenübergreifende Parameter > RPS-Parameter > RPS-Zugangscode)

4.14.2 Belegte Protokollkapazität in %

Standardeinstellung: 0
Auswahl: 0 (deaktiviert), 1 bis 99 (%)
Wenn das Zentralenprotokoll diesen Prozentsatz der vollen Kapazität erreicht, fügt die Zentrale dem Protokoll ein Protokollschwellenwert-Ereignis hinzu und sendet ein Protokoll an den Bedienteilempfänger.
Geben Sie „0“ ein, um Protokollschwellenwert- und Protokollüberlaufereignisse (keine dem Protokoll hinzugefügten Ereignisse oder gesendeten Protokolle) zu deaktivieren.
Das Protokollschwellenwertprotokoll erinnert das Bedienteil daran, eine Verbindung mit der Zentrale herzustellen und das Zentralenprotokoll zu kopieren, bevor Ereignisse überschrieben werden.
Die Zentrale fährt nach dem Senden des Protokollschwellenwertprotokolls mit dem Protokollieren von Ereignissen fort. Ist eine Kapazität von 100 % erreicht (Protokollspeicher ist voll und gespeicherte Ereignisse werden überschrieben), erstellt die Zentrale ein LOG OVERFLOW-Ereignis (Protokollüberlauf).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > RPS Parameters > Log % Full (Zentralenübergreifende Parameter > RPS-Parameter >Belegte Protokollkapazität in %)

4.14.3 Contact RPS if Log % Full (RPS bei belegter Protokollkapazität in % kontaktieren)

Standardeinstellung: Nein
Auswahl:

– Ja: Die Zentrale kontaktiert RPS automatisch, wenn der Schwellenwert für die Protokollkapazität erreicht ist.
– Nein: Die Zentrale kontaktiert RPS nicht automatisch, wenn der Schwellenwert für die Protokollkapazität erreicht ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > RPS Parameters > Contact RPS if Log % Full (Zentralenübergreifende Parameter > RPS-Parameter > RPS bei ausgelasteter Protokollkapazität kontaktieren)

4.14.4 RPS Call Back (RPS-Rückruf)

Standardeinstellung: Nein
Auswahl:
- Ja: Nachdem die Zentrale den RPS-Benutzercode von RPS erhalten hat, trennt sie die Verbindung und wählt die RPS-Telefonnummer, um eine neue Verbindung mit RPS herzustellen.
- Nein: Die Zentrale stellt nach der Bestätigung des RPS-Zugangscodes eine Verbindung mit RPS her.

Wenn Sie beim DTMF-Wählverfahren die Funktion „RPS Callback”(RPS-Rückruf) verwenden, geben Sie „C” als letztes Zeichen der RPS-Telefonnummer ein.

Weitere Informationen
RPS-Telefonnummer, Seite 104

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > RPS Parameters > RPS Call Back (Zentralenübergreifende Parameter > RPS-Parameter > RPS-Rückruf)

4.14.5 RPS Line Monitor (RPS-Leitungsüberwachung)

Standardeinstellung: Yes
Auswahl:
- Ja: Wenn die Zentrale den RPS-Leitungsüberwachungston hört, nachdem ein Anrufbeantworter, ein anderes Gerät oder eine andere Person einen eingehenden Anruf entgegennimmt, wird die Telefonleitung von der Zentrale belegt.
- Nein: Die Zentrale belegt die Telefonleitung nach dem Empfangen des RPS-Leitungsüberwachungstons nicht, um eine Verbindung mit RPS herzustellen.

Answer Armed (Antwort scharf), Seite 102 und/oder *Answer Disarmed (Antwort unscharf), Seite 103* muss eingestellt sein, und die Zentrale muss sich im verbundenen scharfgeschalteten Zustand (scharfgeschaltet oder unscharfgeschaltet) befinden.
Wenn Sie diesen RPS-Leitungsüberwachungsparameter auf „Ja“ setzen, stellen Sie Anrufbeantworter, die die Telefonleitung gemeinsam mit der Zentrale verwenden, so ein, dass Anrufe nach zwei oder mehr Klingelzeichen angenommen werden.
Ist *RPS Call Back (RPS-Rückruf), Seite 102* auf „Ja” gesetzt, legt die Zentrale nach dem Empfangen des RPS-Zugangscodes auf und ruft die RPS-Telefonnummer an.

Hinweis!
„RPS Line Monitor” (RPS-Leitungsüberwachung) auf „Nein” setzen, wenn die Zentrale die Telefonleitung fälschlicherweise belegt
Fälschliche Belegungen der Telefonleitung deuten darauf hin, dass ein Gerät, das die Telefonleitung mit der Zentrale teilt, einen Signalton mit der Frequenz des RPS-Leitungsüberwachungstons verwendet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > RPS Parameters > RPS Line Monitor (Zentralenübergreifende Parameter > RPS-Parameter > RPS-Leitungsüberwachung)

4.14.6 Answer Armed (Antwort scharf)

Standardeinstellung: 7

Auswahl: 0 bis 15 (Klingelzeichen)

– 1 bis 15: Die Zentrale wartet bis zur Antwort (Belegung der Telefonleitung) diese Anzahl der Klingelzeichen ab, wenn alle Bereiche vollscharfgeschaltet sind. Verwendet die Zentrale die Telefonleitung gemeinsam mit einem Anrufbeantworter, geben Sie für die Anzahl der Klingelzeichen eine um 2 größere Zahl ein als die, die für den Anrufbeantworter gewählt wurde.
– 0 (deaktiviert): Die Zentrale antwortet (belegt die Telefonleitung) nicht, wenn alle Bereiche vollscharfgeschaltet sind.

Hinweis!
Bei RPS ist „Außenhautüberwachung" ein unscharfgeschalteter Zustand.

Ist ein beliebiger Bereich für die Außenhautüberwachung eingeschaltet oder unscharfgeschaltet (Aus), verwendet die Zentrale *Answer Disarmed (Antwort unscharf), Seite 103* als Klingelzeichenzähler.

Hinweis!
PSTN-Anforderung für Australien/Neuseeland, RPS-Antwort scharf/unscharf
Wenn Sie den Parameter „Panel Wide Parameters > Phone Parameters > PSTN Compatibility"(Zentralenübergreifende Parameter > Telefonparameter > PSTN-Kompatibilität)) auf „Australien" oder „Neuseeland" setzen, müssen Sie für diesen Parameter „Answer Armed" (Antwort unscharf) und den Parameter „Answer Disarmed" (Antwort unscharf) den Wert „0" (deaktiviert) einstellen.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Panel Wide Parameters > RPS Parameters > Answer Armed (Zentralenübergreifende Parameter > RPS-Parameter > Antwort scharf)

4.14.7 Answer Disarmed (Antwort unscharf)

Standardeinstellung: 7
Auswahl: 0 bis 15 (Klingelzeichen)

– 1 bis 15: Die Zentrale wartet bis zur Antwort (Belegung der Telefonleitung) diese Anzahl der Klingelzeichen ab, wenn mindestens ein Bereich unscharfgeschaltet („Aus") oder für mindestens einen Bereich die Außenhautüberwachung („scharfgeschaltet") aktiv ist. Verwendet die Zentrale die Telefonleitung gemeinsam mit einem Anrufbeantworter, geben Sie für die Anzahl der Klingelzeichen eine um 2 größere Zahl ein als die, die für den Anrufbeantworter gewählt wurde.
– 0 (deaktiviert): Die Zentrale antwortet (belegt die Telefonleitung) nicht, wenn mindestens ein Bereich unscharfgeschaltet („Aus") oder für mindestens einen Bereich die Außenhautaktivierung („scharfgeschaltet") aktiv ist.

Hinweis!
Bei RPS ist „Außenhautüberwachung" ein unscharfgeschalteter Zustand.

Hinweis!

PSTN-Anforderung für Australien/Neuseeland, RPS-Antwort scharf/unscharf

Wenn Sie den Parameter „Panel Wide Parameters > Phone Parameters > PSTN Compatibility" (Zentralenübergreifende Parameter > Telefonparameter > PSTN-Kompatibilität)) auf „Australien" oder „Neuseeland" setzen, müssen sie für diesen Parameter „Answer Armed" (Antwort unscharf) und diesen „Answer Disarmed" (Antwort unscharf)-Parameter den Wert „0" (deaktiviert) einstellen.

RPS Menu Location (Melde-Adresse des Menüs „RPS")

Panel Wide Parameters > RPS Parameters > Answer Disarmed (Zentralenübergreifende Parameter > RPS-Parameter > Antwort unscharf)

4.14.8 RPS-Telefonnummer

Standardeinstellung: Leer

Auswahl: Bis zu 24 Zeichen

Geben Sie die Zielrufnummer ein, mit der die Zentrale eine Verbindung mit RPS herstellt.

Die Zentrale ruft RPS bei den folgenden Ereignissen an:

- Schwellenwert für *Belegte Protokollkapazität in %, Seite 101* erreicht, (sofern aktiviert).
- RPS ruft die Zentrale an, und der Parameter *RPS Call Back (RPS-Rückruf), Seite 102* wird auf „Ja" eingestellt.
- An einem Bedienteil wählen Sie „MENU > Actions > RPS > Call Via Phone" [MENÜ > MA NAHMEN > RPS > Über Telefon anrufen) (nur ein Versuch)].

Ist dieser Parameter leer, wählt die Zentrale keine RPS-Zielrufnummer.

Weitere Informationen zu den Zeichen, die die Zentrale wählen kann, finden Sie unter *Telefon-Zieladresse 1 (bis 4), Seite 53*.

RPS Menu Location (Melde-Adresse des Menüs „RPS")

Panel Wide Parameters > RPS Parameters > RPS Phone (Zentralenübergreifende Parameter > RPS-Parameter > RPS-Telefon)

4.14.9 Geschwindigkeit des RPS-Modems

Standardeinstellung: 1200

Auswahl:

- 300
- 1200
- 2400

Stellen Sie bei einer PSTN-Verbindung die Baudrate für die Kommunikation zwischen RPS und der Zentrale ein.

RPS Menu Location (Melde-Adresse des Menüs „RPS")

Panel Wide Parameters > RPS Parameters > RPS Modem Speed (Zentralenübergreifende Parameter > RPS-Parameter > Geschwindigkeit des RPS-Modems)

4.15 Sonstiges

4.15.1 Bedrohungstyp

Standardeinstellung: 0

Auswahl:

- 0: deaktiviert, keine Bedrohungsalarmprotokolle
- 1–+1: Benutzer fügen der letzten Stelle des Zugangscodes „1" hinzu, um bei der Eingabe des Zugangscodes an einem Bedienteil ein Bedrohungsalarmprotokoll zu senden.

– 2–+2: Benutzer fügen der letzten Stelle des Zugangscodes „2” hinzu, um bei der Eingabe des Zugangscodes an einem Bedienteil ein Bedrohungsalarmprotokoll zu senden.
– 3: Die Zentrale sendet ein Bedrohungsalarmprotokoll, wenn ein Benutzer, der einem Benutzerrecht zugewiesen ist, bei auf „ja“ gesetzter Option „Send Duress” (Bedrohungsalarm senden) einen Zugangscode an einem Bedienteil eingibt.

Beispiel: Der Bedrohungstyp ist auf „1 (+ 1)” eingestellt.
– Lautet der Zugangscode „6123”, wird mit „6124” ein Bedrohungsalarm ausgelöst.
– Wenn die letzte Stelle des Zugangscodes „0” ist, und der Benutzer „1” als letzte Stelle des Zugangscodes eingibt, tritt ein Bedrohungsalarm auf.
– Wenn die letzte Stelle des Zugangscodes „9” ist, und der Benutzer „0” als letzte Stelle des Zugangscodes eingibt, tritt ein Bedrohungsalarm auf.

Bei Einstellung des Bedrohungstyps auf „2 (+ 2)”:
– Wenn die letzte Stelle des Zugangscodes „8” ist, und der Benutzer „0” als letzte Stelle des Zugangscodes eingibt, tritt ein Bedrohungsalarm auf.
– Wenn die letzte Stelle des Zugangscodes „9” ist, und der Benutzer „1” als letzte Stelle des Zugangscode eingibt, tritt ein Bedrohungsalarm auf.

Wenn „Duress type” (Bedrohungstyp) auf „3” gesetzt ist und Benutzer, die einem Benutzerrecht zugewiesen sind, bei auf „Ja“ gesetztem *Bedrohung senden, Seite 206* einen Zugangscode an einem Bedienteil eingeben, sendet die Zentrale einen Bedrohungsalarm.
Die Bedrohungsalarmprotokollierung wird nach dem Bereich unter „Area Parameters ”(Bereichsübergreifende Parameter), (*Duress Enable (Bedrohungsalarm aktivieren), Seite 128* aktiviert oder deaktiviert.

Hinweis!
SIA CP-01-Anforderung zur Fehlalarmunterdrückung
Zur Erfüllung der SIA CP-01-Anforderungen für die Fehlalarmunterdrückung setzen Sie diesen Parameter auf „3”. Weitere Informationen finden Sie unter „SIA CP-01 Verification” (SIA CP-01-Verifizierung).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Duress Type (Zentralenübergreifende Parameter > Sonstige > Bedrohungstyp)

4.15.2 Abbruchsprotokoll

Standardeinstellung: Yes
Auswahl:
– Ja: Abbruchprotokolle, Feuerabbruchsprotokolle und Gasabbruchsprotokolle senden
– Nein: keine Abbruchprotokolle, Feuerabbruchsprotokolle und Gasabbruchsprotokolle senden

Ein Abbruch-, Feuerabbruchs- oder Gasabbruchsprotokoll wird erstellt, wenn ein Zugangscode zum Stummschalten eines Alarm-Signalgebers, eines Gasalarms oder Feueralarms vor Ablauf der Zutrittssignaldauer eingegeben wird.

Hinweis!
SIA CP-01-Anforderung zur Fehlalarmunterdrückung
Zur Erfüllung der SIA CP-01-Anforderungen zur Fehlalarmunterdrückung setzen Sie diesen Parameter auf „Ja“. Weitere Informationen finden Sie unter „SIA CP-01 Verification” (SIA CP-01-Verifizierung).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Cancel Reports (Zentralenübergreifende Parameter > Sonstige >Abbruchsprotokolle)

4.15.3 Call for Service Text - First Language (Text Überprüfungsaufruf – erste Sprache)

Standardeinstellung: Kontaktieren Sie Ihren Händler
Auswahl: Geben Sie bis zu 32 Zeichen (Text, Zahlen, Symbole oder Leerzeichen) ein.
Der Text für den Überprüfungsaufruf wird auf Bedienteilen bei Systemstörungsereignissen angezeigt.
Leerzeichen vor, nach und innerhalb einer Zeichenfolge sind in der Zeichenbeschränkung (max. 32 Zeichen) enthalten.
Auf Bedienteilen werden die ersten 20 Zeichen angegeben. Die übrigen Zeichen werden auf dem Display einmalig eingeblendet. Drücken Sie die Escape-Taste, um diese Zeichen erneut einzublenden.
Die erste und zweite Sprache wird während der Einrichtung des Zentralenkontos im Fenster „Panel Data” (Zentralendaten) parametriert. Zu den unterstützten Sprachen zählen Englisch, Spanisch, Französisch und Portugiesisch. Unter „Panel Wide Parameters > Personal Notification > User Language” (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Benutzersprache) werden die während der Kontoeinrichtung gewählten Sprachen aufgeführt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Call for Service Text - English
(Zentralenübergreifende Parameter > Sonstige > Text Überprüfungsaufruf – Englisch)

4.15.4 Call for Service Text - Second Language (Text Überprüfungsaufruf – zweite Sprache)

Standardeinstellung: Leer
Standardeinstellung: Kontaktieren Sie Ihren Händler
Auswahl: Geben Sie bis zu 32 Zeichen (Text, Zahlen, Symbole oder Leerzeichen) ein.
Der Text für den Überprüfungsaufruf wird auf Bedienteilen bei Systemstörungsereignissen angezeigt.
Leerzeichen vor, nach und innerhalb einer Zeichenfolge sind in der Zeichenbeschränkung (max. 32 Zeichen) enthalten.
Auf Bedienteilen werden die ersten 20 Zeichen angegeben. Die übrigen Zeichen werden auf dem Display einmalig eingeblendet. Drücken Sie die Escape-Taste, um diese Zeichen erneut einzublenden.
Die erste und zweite Sprache wird während der Einrichtung des Zentralenkontos im Fenster „Panel Data” (Zentralendaten) parametriert. Zu den unterstützten Sprachen zählen Englisch, Spanisch, Französisch und Portugiesisch. Unter „Panel Wide Parameters > Personal Notification > User Language” (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Benutzersprache) werden die während der Kontoeinrichtung gewählten Sprachen aufgeführt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Call for Service Text- Second Language
(Zentralenübergreifende Parameter > Sonstige > Text Überprüfungsaufruf – Zweite Sprache)

4.15.5 On Site Authorization for Firmware Update (Vor-Ort-Autorisierung für Firmware-Aktualisierung)

Standardeinstellung: Nein

Auswahl:
– Ja: Vor-Ort-Autorisierung für Firmware-Aktualisierung ist erforderlich.
– Nein: Vor-Ort-Autorisierung ist nicht erforderlich.

Dieser Parameter erfordert, dass autorisiertes Personal während des ferngesteuerten Firmware-Aktualisierungsprozesses vor Ort zu einer festgelegten Zeit eine Autorisierungskennung an einem der Bedienteile eingibt.

Hinweis!
Bei Systemen mit UL-Zulassung ferngesteuerte Firmware-Aktualisierungen vor Ort autorisieren
Stellen Sie diesen Parameter für Systeme mit UL-Zulassung auf „Ja“ ein.

Führen Sie einen vollständigen Systemtest aus, wenn Firmware vor Ort oder per Fernzugriff aktualisiert wird.

Weitere Informationen
Firmware-Aktualisierung, Seite 210

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > On-Site Authorization for Firmware Update (Zentralenübergreifende Parameter > Sonstige > Vor-Ort-Autorisierung für Firmware-Aktualisierung)

4.15.6 Systemsabotagereaktion

Standardeinstellung: Störung
Auswahl:
– Störung: Systemsabotageversuche sind Störungsereignisse.
– Always Alarm (Immer Alarm): Systemsabotageversuche sind hörbare und sichtbare Alarmereignisse.
– Alarm bei Unscharfschaltung: Ist mindestens ein Bereich scharfgeschaltet, sind Sabotageversuche am System nicht hörbare und unsichtbare Ereignisse. Bei Unscharfschaltung aller Bereiche stellen Systemsabotageversuche hörbare und sichtbare Ereignisse dar.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > System Tamper Response (Zentralenübergreifende Parameter > Sonstige > Systemsabotagereaktion)

4.15.7 Enclosure Tamper Enable (Gehäusesabotagekontakt aktivieren)

Standardeinstellung: Nein
Auswahl:
– Ja: Sabotageeingang der Zentrale aktivieren
– Nein: Sabotageeingang der Zentrale deaktivieren

Bei Aktivierung des Gehäusesabotageeingangs erstellt die Zentrale ein Gehäusesabotageereignis, wenn das Zentralengehäuse geöffnet wird.
Sabotageereignisse haben keinen Einfluss auf die Scharf- oder Unscharfschaltung.
Wenn Sie die Parametereinstellung von „Ja“ zu „Nein ”ändern, erstellt die Zentrale Sabotageereignisse erst dann, wenn sich der Sabotageeingang im Normalzustand (Gehäusetür ist geschlossen) befindet.
Wenn der Parameter von „Ja” zu „Nein” geändert wird und ein Gehäusesabotageereignis vorliegt, wird das Ereignis gelöscht. Es wird kein Wiederherstellungsereignis protokolliert oder gemeldet.

Wenn die Zentrale hochfährt oder neu startet, wird der Sabotageeingang ignoriert, bis die Zentrale den Normalzustand des Sabotageeingangs erkennt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Enclosure Tamper Enable (Zentralenübergreifende Parameter > Sonstige > Gehäusesabotagekontakt aktivieren)

4.15.8 Feuer- und Gas-Zusammenfassung beibehalten

Standardeinstellung: „Ja“
Auswahl:
- Ja: Ausgänge für Zusammenfassung Feuer und Zusammenfassung Gas bleiben nach dem Befehl „Alarm Silence” (Alarm stummschalten) aktiv.
- Nein: Ausgänge für Zusammenfassung Feuer und Zusammenfassung Gas bleiben aktiv, bis sich alle stummgeschalteten Feuer- oder Gasmelder im System wieder im Normalbetrieb befinden.

Wählen Sie „Ja”, um den Sendebetrieb von Feuer- und Gassignalgebern nach dem Stummschalten von Feuer- oder Gasalarmen aufrechtzuerhalten.

Ort im RPS-Menü
Zentralenübergreifende Parameter > Sonstige > Feuer- und Gas-Zusammenfassung beibehalten

4.15.9 Typ des Feuerüberwachungsereignisses

Standardeinstellung: Feuer-Überwachung Wiederherstellung
Auswahl:
- Feuer-Störung Wiederherstellung: Die Zentrale sendet ein FEUER-STÖRUNG WIEDERHERSTELLUNG-Protokoll, wenn sich ein Feuer-Überwachungsmelder wieder im Normalzustand befindet.
- Feueralarm Wiederherstellung: Die Zentrale sendet ein FEUERALARM WIEDERHERSTELLUNG-Protokoll, wenn sich ein Feuer-Überwachungsmelder wieder im Normalzustand befindet.
- Feuerüberwachung Wiederherstellung: Die Zentrale sendet ein FEUERÜBERWACHUNG WIEDERHERSTELLUNG-Protokoll, wenn sich ein Feuer-Überwachungsmelder wieder im Normalzustand befindet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Fire Supervision Event Type
(Zentralenübergreifende Parameter > Sonstige > Typ des Feuerüberwachungsereignisses)

4.15.10 Feuer und Gas – Signalton

Standardeinstellung: Keine
Auswahl:
- Keine: Bedienteile geben Störungston nicht erneut wieder.
- Mittag: Bedienteile geben Störungston um 12:00 Uhr erneut wieder, wenn sich ein beliebiger Feuer- oder Gasmelder im Bedienteilumfang in einem nicht normalen Zustand befindet.
- Mitternacht: Bedienteile geben Störungston um 00:00 Uhr erneut wieder, wenn sich ein beliebiger Feuer- oder Gasmelder im Bedienteilumfang in einem nicht normalen Zustand befindet.

Bei aktiviertem Signalton wird der Störungston durch zuvor rückgemeldete und stummgeschaltete Feuer- oder Gasstörungsereignisse automatisch erneut wiedergeben.

Ort im RPS-Menü
Zentralenübergreifende Parameter > Sonstige > Feuer und Gas – Signalton

4.15.11 Early Ambush Time (Zeit für zweimalige Authentifizierung)

Standardeinstellung: 10

Auswahl: 5 bis 30 (in Schritten von 1 Sekunde)

Geben Sie die Zeit ein, die einem Benutzer beim Unscharfschalten („AUS") für die Eingabe eines zweiten Zugangscodes am Bedienteil zur Verfügung steht. Wenn vor Ablauf der „Early Ambush Time" (Zeit für zweimalige Authentifizierung) kein zweiter Zugangscode eingegeben wurde, erstellt die Zentrale ein Bedrohungsereignis.

Mit dem Bereichsparameter *Zweimalige Authentifizierung?, Seite 132* aktivieren Sie die Funktion „Zweimalige Authentifizierung".

RPS Menu Location (Melde-Adresse des Menüs „RPS")

Panel Wide Parameters > Miscellaneous > Early Ambush Time (Zentralenübergreifende Parameter > Sonstige >Zeit für zweimalige Authentifizierung)

4.15.12 Second Ambush Code (Code für zweimalige Authentifizierung)

Standardeinstellung: Eindeutig

Auswahl:

- Eindeutig: Der zweite für die zweimalige Authentifizierung eingegebene Zugangscode muss sich vom ersten Zugangscode, der zum Unscharfschalten des Bereichs eingegeben wurde, unterscheiden.
- Beliebig: Der zweite Zugangscode für die zweimalige Authentifizierung kann sich vom Zugangscode, der zum Unscharfschalten des Bereichs eingegeben wurde, unterscheiden. Es kann jedoch auch der gleiche Zugangscode verwendet werden.

Informieren Sie sich über den Bereichsparameter *Zweimalige Authentifizierung?, Seite 132*.

RPS Menu Location (Melde-Adresse des Menüs „RPS")

Panel Wide Parameters > Miscellaneous > Second Ambush Code (Zentralenübergreifende Parameter > Sonstige > Code für zweimalige Authentifizierung)

4.15.13 Alarmabbruchzeit

Standardeinstellung: 30 Sekunden

Auswahl: 15 bis 45 (Sekunden, in Schritten von 1 Sekunde)

Geben Sie die Zeit (in Sekunden) ein, die die Zentrale wartet, bis sie ein Alarmprotokoll für einen Melder sendet, der einem Melderprofil mit aktivierter Funktion „Alarm Abort" (Alarmabbruch) zugewiesen ist.

Siehe *Alarmabbruch, Seite 247*, um eine Beschreibung der Funktion „Alarm Abort" (Alarmabbruch) zu erhalten.

Hinweis!

UL-Anforderung

Gemäß UL-Anforderung darf die kombinierte *Eingangsverzögerung, Seite 238* und Alarmabbruchzeit eine Dauer von 60 Sekunden nicht überschreiten.

Hinweis!

SIA CP-01-Anforderung

Für die SIA CP-01-Konformität ist der Parameter „Alarmabbruchzeit" erforderlich.

Schaltet ein Benutzer den Alarm vor Ende der Alarmabbruchzeit stumm, wird das Alarmprotokoll nicht gesendet, und auf dem Bedienteil wird eine optionale Nachricht angezeigt (siehe *Abort Display (Abbruch anzeigen), Seite 151*).

Diese Funktion gilt nicht für Feueralarme oder unsichtbare Melderalarme.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Abort Window (Zentralenübergreifende Parameter > Sonstige > Abbruchfenster)

4.15.14 Benutzercodelänge

Standardeinstellung: Deaktiviert
Auswahl:
– Deaktiviert
– 3, 4, 5 oder 6 Stellen

Bei einer Einstellung auf 3, 4, 5 oder 6 Stellen ist die Benutzercodelänge für alle Benutzercodes festgelegt. Benutzer müssen nach der Eingabe des Zugangscodes nicht die Eingabetaste drücken.
Beim Wählen der Einstellung „Deaktiviert” ist die Länge des Zugangscodes nicht festgelegt. Individuelle Zugangscodes können eine Länge von 3 bis 6 Stellen haben. Benutzer müssen nach der Eingabe des Zugangscodes die Eingabetaste drücken.

Hinweis!
SIA CP-01-Anforderung
Wählen Sie für diesen Parameter eine Länge zwischen 3 und 6 Stellen, um die SIA CP-01-Anforderung zur Fehlalarmunterdrückung zu erfüllen. Weitere Informationen finden Sie unter „SIA CP-01 Verification” (SIA CP-01-Verifizierung).

Wenn das Ändern der Zugangscodelänge zu doppelten oder unbrauchbaren Zugangscodes führt, erscheint der Warnhinweis „Duplicate/Unusable Passcodes Present” (Doppelte/unbrauchbare Zugangscodes).
Doppelt vorhandene Zugangscodes sind fettgedruckt und in rot.
Unbrauchbare Zugangscodes (länger oder kürzer als im Parameter festgelegt) sind fettgedruckt und blau.
So korrigieren Sie doppelte oder unbrauchbare Zugangscodes:

1. Wählen Sie den Zugangscode aus. Hierzu klicken Sie in der Spalte „User Passcode“ (Benutzer-Zugangscode) auf die Zelle.
2. Drücken Sie die Rücktaste auf der Tastatur, um die Zelle zu löschen.
3. Geben Sie den neuen Zugangscode ein.
4. Klicken Sie auf „Save corrected passcodes” (Korrigierte Zugangscodes speichern), um die Änderungen zu speichern. Bevor Sie auf „OK” klicken, müssen alle doppelten oder unbrauchbaren Zugangscodes korrigiert worden sein.
   Alternativ:
   Klicken Sie auf „Disable passcode length” (Zugangscodelänge deaktivieren), und speichern Sie die Daten in diesem Konto. Mit dieser Option wird der Parameter „Benutzercodelänge” auf „Deaktiviert” gesetzt, und Sie können Zugangscodes von unterschiedlicher Länge im RPS-Konto speichern.

Hinweis!
Änderung des Parameters „Benutzercodelänge”
RPS zeigt die folgende Meldung an: „Dieser Vorgang führt zur Deaktivierung der Zugangscodelänge. Der Parameter „SIA CP-01 Verification” (SIA CP-01-Verifizierung) wird auf „Nein“ festgelegt, und die bisherigen RPS-Zugangscodedaten werden gespeichert. Möchten Sie wirklich fortfahren?“

Ähnliche und doppelte Zugangscodes

– Ähnliche Zugangscodes: Wenn der eingegebene Zugangscode einem vorhandenen Zugangscode ähnlich ist, erscheint der vorhandene Zugangscode im Feld „Existing Similar Passcodes” (Vorhandene ähnliche Zugangscodes).
– Doppelte Pincodes: Wenn Sie einen Zugangscode eingeben, der mit einem bereits vorhandenen Zugangscode identisch ist, werden die bereits vorhandenen Zugangscodes im Feld „Duplicate/Duress Passcodes” (Doppelte/Bedrohungs-Zugangscodes) angegeben. Zugangscodeübereinstimmungen basieren auf doppelten Eingaben, bei denen die Zugangscodelänge auf den niedrigsten SIA CP-01-konformen Wert gesetzt ist (3).

Wenn Sie z. B. „478123" als Zugangscode für Benutzer 2 und „478321" als Zugangscode für Benutzer 3 eingeben und die Zugangscodelänge auf drei Stellen festlegen, erscheinen die Zugangscodes für Benutzer 2 und 3 im Feld „Duplicate/Duress Passcodes” (Doppelte/Bedrohungs-Zugangscodes), da die ersten drei Ziffern (478) der beiden Zugangscodes identisch sind. Wird die Länge des Zugangscodes von vier auf drei Ziffern geändert, würden diese Zugangscodes als doppelte Zugangscodes mit der Ziffernfolge „478“ behandelt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Passcode Length (Zentralenübergreifende Parameter > Sonstige > Benutzercodelänge)

4.15.15 Anzahl der Mehrfachauslösungsumgehungen

Standardeinstellung: 2
Auswahl: 1 bis 4
Mit diesem Parameter wird für einen kontrollierten Melder die maximale Anzahl von Störungen innerhalb eines Scharfschaltezyklus vor einer Swinger-Umgehung festgelegt.

Hinweis!
Zur Erfüllung der SIA CP-01-Anforderung zur Fehlalarmunterdrückung setzen Sie diesen Parameter auf „1” oder „2”. Weitere Informationen finden Sie im Abschnitt zu „SIA CP-01 Verification” (SIA CP-01–Verifizierung).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Swinger Bypass Count (Zentralenübergreifende Parameter > Sonstige > Mehrfachauslösungsumgehungen)

4.15.16 Remote Warning (Remote-Warnung)

Standardeinstellung: Nein
Auswahl:

– Ja: Wird der Bereich per Fernzugriff scharfgeschaltet, aktiviert die Zentrale den Alarm-Signalgeber einmal. Wenn der Bereich aus der Ferne unscharfgeschaltet wird, aktiviert die Zentrale den Alarm-Signalgeber zweimal.
– Nein: Keine Remote-Warnung bei Fernscharfschaltung

Scharf- oder Unscharfschaltungen per Fernzugriff sind mit einem RADION keyfob, Inovonics-Sender zum Anhängen, Schlüsselschalter oder einer Remote-Software möglich.

Hinweis!
SIA CP-01–Verifizierung
Zur Erfüllung der SIA CP-01-Anforderungen zur Fehlalarmunterdrückung setzen Sie diesen Parameter auf „Ja“. Weitere Informationen finden Sie unter „SIA CP-01 Verification” (SIA CP-01-Verifizierung).

Weitere Informationen
Alarm-Signalgeber, Seite 165

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Remote Warning (Zentralenübergreifende Parameter > Sonstige > Remote-Warnung)

4.15.17 Crystal Time Adjust (Quarzzeit anpassen)

Standardeinstellung: Nein
Auswahl:
- Ja: Die Zentrale reguliert die Uhrzeit mit der integrierten Quarzfrequenz.
- Nein: Die Zentrale verwendet zur Regulierung der Uhrzeit die Netzstromfrequenz (der primären Stromquelle).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Crystal Time Adjust (Zentralenübergreifende Parameter > Sonstige > Quarzzeit anpassen)

4.15.18 Part On Output (Ausgang Außenhautüberwachung)

Standardeinstellung: Nein
Auswahl:
- Ja: Die Ausgangsfunktion „Fehler beim Schließen” wird zur Ausgangsfunktion „Außenhautüberwachung”. Außenhautüberwachungsausgänge werden aktiviert, wenn alle Bereiche, die dem gleichen Ausgang zugewiesen sind, mit unverzögerter oder verzögerter Außenhautüberwachung scharfgeschaltet sind.
- Nein: Die „Fehler beim Schließen”-Ausgänge werden aktiviert, wenn das schließende Fenster des festgelegten Bereichs abläuft.

Wird dieser Außenhautüberwachungsparameter auf „Ja” gesetzt, verwenden Sie den Parameter *Early Area Armed Output (Ausgang frühe Bereichsscharfschaltung), Seite 112*, um festzulegen, ob der Ausgang für die Außenhautüberwachung zu Beginn oder am Ende der Scharfschalteverzögerung aktiviert wird. Entsprechend der Standardeinstellung wird der Ausgang am Ende der Scharfschaltverzögerung aktiviert.

Weitere Informationen
Fehler beim Schließen/Außenhautüberwachung scharfgeschaltet, Seite 167

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Part On Output (Zentralenübergreifende Parameter > Sonstige > Ausgang Außenhautüberwachung)

4.15.19 Early Area Armed Output (Ausgang frühe Bereichsscharfschaltung)

Standardeinstellung: Nein
Auswahl:
- Ja: aktiviert den Ausgang für die Bereichsscharfschaltung oder den Ausgang für die Außenhautüberwachung zu Beginn der Scharfschalteverzögerung.
- Nein: aktiviert den Ausgang für die Bereichsscharfschaltung oder den Ausgang für die Außenhautüberwachung am Ende der Scharfschalteverzögerung.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Early Area Armed Output (Zentralenübergreifende Parameter > Sonstige > Ausgang frühe Bereichsscharfschaltung)

4.15.20 Sommerzeit

Standardeinstellung: US-Sommerzeit

Auswahl:
- Keine Sommerzeit: Die Zentrale passt die Uhrzeit nicht an die Sommerzeit an.
- Sommerzeit USA
- Sommerzeit Brasilien
- Sommerzeit Mexiko
- Sommerzeit Paraguay
- Sommerzeit Australien
- Sommerzeit Neuseeland
- Sommerzeit EU

Die Uhr der Zentrale richtet sich nach den in den angegebenen Ländern geltenden Regeln für die Sommerzeit.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Daylight Saving Time (Zentralenübergreifende Parameter > Sonstige > Sommerzeit)

4.15.21 Date Format (Datumsformat)

Standardeinstellung: TT MM JJ

Auswahl:
- MM TT JJ
- TT MM JJ
- JJ MM TT

Wählen Sie, wie Monat, Tag und Jahr im Parameter „Date Delimiter” (Datumstrennzeichen) voneinander abgegrenzt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Date Format (Zentralenübergreifende Parameter > Sonstige > Datumsformat)

4.15.22 Date Delimiter (Datumstrennzeichen)

Standardeinstellung: / (Schrägstrich)

Auswahl:
- / (Schrägstrich)
- . (Punkt)
- - (Bindestrich)

Stellen Sie ein, wie Monat (MM), Tag (TT) und Jahr (JJ) voneinander abgegrenzt sind. Legen Sie fest, wie Monat, Tag und Jahr im Parameter „Date Format” (Datumsformat) angezeigt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Date Delimiter (Zentralenübergreifende Parameter > Sonstige > Datumstrennzeichen)

4.15.23 Zeitformat

Standardeinstellung: 12 Stunden (a.m./p.m.)

Auswahl:
- 12 Stunden (a.m./p.m.)
- 24 Stunden

Wählen Sie das 12-Stunden-Format (hh:mm, a.m./p.m.) oder das 24-Stunden-Format [hh:mm (00:00 bis 23:59)].

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Time Format (Zentralenübergreifende Parameter > Sonstige > Zeitformat)

4.15.24 Zeitzone

Standardeinstellung: UTC-05:00 (Eastern Time, USA und Kanada)
Auswahl: Zeitzonen und UTC (Koordinierte Weltzeit)
Dieser Parameter informiert über die Zeitzone des Ortes, an dem die Zentrale installiert ist.
(UTC-12:00) International Date Line West
(UTC-11:00) Midwayinseln, Samoa
(UTC-10:00) Hawaii
(UTC-09:00) Alaska
(UTC-08:00) Pazifische Zeit (USA und Kanada)
(UTC-08:00) Tijuana, Baja California
(UTC 07:00) Arizona
(UTC 07:00) Chihuahua, La Paz Mazatlan
(UTC 07:00) Mountain Time (USA und Kanada)
(UTC-06:00) Zentralamerika
(UTC-06:00) Central Time (USA und Kanada)
(UTC-06:00) Guadalajara, Mexiko-Stadt, Monterrey
(UTC-06:00) Saskatchewan
(UTC-05:00) Bogotá, Lima, Quito
(UTC-05:00) Eastern Time (USA und Kanada)
(UTC-05:00) Indiana (Osten)
(UTC-04:30). Caracas
(UTC-04:00) Asunción
(UTC-04:00) Atlantic Time (Kanada)
(UTC-04:00) Georgetown, La Paz, San Juan
(UTC-04:00) Manaus
(UTC-04:00) Santiago
(UTC-03:30) Neufundland
(UTC-03:00) Brasilia
(UTC-03:00) Buenos Aires
(UTC-03:00) Cayenne
(UTC-03:00) Grönland
(UTC-03:00) Montevideo
(UTC-02:00) Mittelatlantik
(UTC-01:00) Azoren
(UTC-01:00) Kapverdische Inseln
(UTC) Casablanca
(UTC) Koordinierte Weltzeit
(UTC) Dublin, Edinburgh, Lissabon, London
(UTC) Monrovia, Reykjavik
(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
(UTC+01:00) Belgrad, Bratislava, Budapest, Ljubljana, Prag
(UTC+01:00) Brüssel, Kopenhagen, Madrid, Paris
(UTC+01:00) Sarajevo, Skopje, Warschau, Zagreb
(UTC+01:00) West-/Zentralafrika
(UTC+02:00) Amman
(UTC+02:00) Athen, Bukarest, Istanbul

(UTC+02:00) Beirut
(UTC+02:00) Kairo
(UTC+02:00) Harare, Pretoria
(UTC+02:00 UHR) Helsinki, Kiew, Riga, Sofia, Tallinn, Wilna
(UTC+02:00) Jerusalem
(UTC+02:00) Minsk
(UTC+02:00) Windhoek
(UTC+03:00) Bagdad
(UTC+03:00) Kuwait, Riad
(UTC+03:00) Moskau, St. Petersburg, Wolgograd
(UTC+03:00) Nairobi
(UTC+03:00) Tiflis
(UTC+03:30) Teheran
(UTC+04:00) Abu Dhabi, Muskat
(UTC+04:00) Baku
(UTC+04:00) Port Louis
(UTC+04:00) Jerewan
(UTC+04:30) Kabul
(UTC+05:00) Jekaterinburg
(UTC+05:00) Islamabad, Karatschi
(UTC+05:00) Taschkent
(UTC+05:30) Chennai, Kalkutta, Mumbai, Neu-Delhi
(UTC+05:30) Sri Jayawardenepura
(UTC+05:45) Kathmandu
(UTC+06:00) Almaty, Nowosibirsk
(UTC+06:00) Astana, Dhaka
(UTC+06:30) Yangon (ehem. Rangun)
(UTC+07:00) Bangkok, Hanoi, Jakarta
(UTC+07:00) Krasnojarsk
(UTC+08:00) Peking, Chongqing, Hongkong, Ürümqi
(UTC+08:00) Irkutsk, Ulaanbaatar
(UTC+08:00) Kuala Lumpur, Singapur
(UTC+08:00) Perth
(UTC+08:00) Taipeh
(UTC+09:00) Osaka, Sapporo, Tokio
(UTC+09:00) Seoul
(UTC+09:00) Jakutsk
(UTC+09:30) Adelaide
(UTC+09:30) Darwin
(UTC+10:00) Brisbane
(UTC+10:00) Canberra, Melbourne, Sydney
(UTC+10:00 UHR) Guam, Port Moresby
(UTC+10:00) Hobart
(UTC+10:00) Wladiwostok
(UTC+11:00) Magadan, Solomonen, Neukaledonien
(UTC+12:00) Auckland, Wellington
(UTC+12:00) Fidschi, Marshallinseln
(UTC+12:00) Petropawlowsk-Kamtschatski
(UTC + 13.00) Nuku'alofa

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Time Zone (Zentralenübergreifende Parameter > Sonstige > Zeitzone)

4.15.25 Custom Text Format (Format Benutzerdefinierter Text)

Hinweis!
Schreibgeschützter Parameter
Dieser Parameter kann nicht geändert werden.
Beim Einstellen der Parameter „Panel Data - View > Panel Info > First Language and Second Language” (Zentralendaten – Anzeigen > Zentraleninfo > Erste und zweite Sprache) wird dieser Parameter durch RPS automatisch festgelegt.

Auswahl (schreibgeschützt):
- Standard: RPS setzt den Parameter „Format Benutzerdefinierter Text” auf „Standard” (Latin-1 Zeichensatz), wenn die Parameter „Zentralendaten – Anzeigen > Zentraleninfo > Erste und zweite Sprache” beide auf „Deutsch“, „Englisch”, „Französisch”, „Italienisch”, „Niederländisch“, „Portugiesisch”, „Schwedisch“, „Spanisch” oder „Ungarisch” eingestellt sind.
- Erweitert: RPS setzt diesen Parameter „Format Benutzerdefinierter Text” auf „Erweitert” (UTF-8 Unicode-Zeichensatz), wenn unter „Zentralendaten – Anzeigen > Zentraleninfo > Erste und zweite Sprache” entweder der Parameter „Erste Sprache” oder „Zweite Sprache” auf „Chinesisch”, „Griechisch” oder „Polnisch” festgelegt ist. Oder auch dann, wenn beide Parameter auf „Chinesisch”, „Griechisch” oder „Polnisch” eingestellt sind.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Miscellaneous > Custom Text Format (Zentralenübergreifende Parameter > Sonstige > Format Benutzerdefinierter Text)

4.16 Personal Notification Destinations (Persönliche Benachrichtigungsziele)

4.16.1 Beschreibung

Standardeinstellung: Leer (Text dient nur zu Referenzzwecken)
Auswahl: Länge von 0 bis 32 Zeichen
Geben Sie Text ein, um das persönliche Benachrichtigungsgerät oder den Benachrichtigungsempfänger zu bestimmen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Personal Notification > Personal Notification Destinations > Description (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Persönliche Benachrichtigungsziele > Beschreibung)

4.16.2 SMS-Zielrufnummer/E-Mail-Adresse

Standardeinstellung: Leer
Auswahl: Bis zu 255 alphanumerische Zeichen
Geben Sie entweder eine Zielrufnummer zum Empfangen von SMS-Text-Benachrichtigungen oder eine Email-Adresse zum Empfangen von E-Mail-Nachrichten ein.

SMS-Zielrufnummer
Die Zentrale sendet persönliche Benachrichtigungen an ein Mobilfunkgerät, wenn es sich bei der Zieladresse um eine Handynummer handelt, die nur Zahlen zwischen 0 und 9 enthält. Bindestriche sind nicht zulässig.

E-Mail-Adresse
Die Zentrale sendet persönliche Benachrichtigungen an E-Mail-Konten, wenn es sich bei der Zieladresse um eine E-Mail-Adresse handelt.

Hinweis!
Persönliche Benachrichtigung werden bei Falscheingaben nicht gesendet
Geben Sie weder eine korrekte Zielrufnummer noch eine korrekte E-Mail-Adresse ein, sendet die Zentrale keine persönliche Benachrichtigung. Die Zentrale protokolliert einen SMS-Sendefehler.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Personal Notification > Personal Notification Destinations > SMS Phone #/email address (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Persönliche Benachrichtigungsziele > SMS-Zielrufnummer/E-Mail-Adresse)

4.16.3 User Language (Benutzersprache)

Standardeinstellung: 1: [Sprache, die in „Panel Data – View“ (Zentralendaten – Anzeigen) als erste Sprache festgelegt wurde]
Auswahl:
– 1: [Sprache, die in „Panel Data – View“ (Zentralendaten – Anzeigen) als erste Sprache festgelegt wurde]
– 2: [Sprache, die in „Panel Data – View“ (Zentralendaten – Anzeigen) als zweite Sprache festgelegt wurde]

Wählen Sie die Sprache, in der persönliche Benachrichtigungen gesendet werden.
Die erste und zweite Sprache wird während der Einrichtung des Zentralenkontos im Fenster „Panel Data - View” (Zentralendaten – Anzeigen) parametriert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Personal Notification > Personal Notification Destinations > User Language (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Persönliche Benachrichtigungsziele > Benutzersprache)

4.16.4 Methode

Standardeinstellung: Plug in Cellular SMS (Plug-in-Mobilfunkmodul-SMS)
Auswahl:
– Ohne
– Plug in Cellular SMS (Plug-in-Mobilfunkmodul-SMS): kann bei B44x-Plug-in-Mobilfunkmodulen ausgewählt werden
– Plug in Cellular Email (Plug-in-Mobilfunkmodul-E-Mail): kann bei B44x-Plug-in-Mobilfunkmodulen ausgewählt werden.
– Bus Device Cellular SMS (Bedienteil-Mobilfunk-SMS): steht bei einem B450 v2-Modul zur Verfügung
– Bus Device Email (Bedienteil-E-Mail): kann ausgewählt werden, wenn Sie über ein B450 v2- oder B426 v3-Modul verfügen.
– On-board Ethernet Email (Integrierte Ethernet-E-Mail): steht zur Verfügung, wenn Ihre Verbindung über eine integrierte IP-Adresse hergestellt wird

Wählen Sie das persönliche Benachrichtigungsziel und das Zielgerät, das zum Senden der Benachrichtigung verwendet wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Personal Notification > Personal Notifications Destinations > Method (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Persönliche Benachrichtigungsziele > Methode)

4.17 Personal Notification Reports (Persönliche Benachrichtigungen)

WICHTIGE HINWEISE ZUM MOBILFUNKDIENST

Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297***, um zu erfahren, wie Sie Ihre Zentrale für die Mobilfunkkommunikation mit einem Bedienteilempfänger konfigurieren.**
Standardeinstellung:
Zielgruppen 1 - 3: 0 (Deaktiviert)
Zielgruppe 4: persönliche Benachrichtigung Nr. 1 - 4 (Firmware v3.xx und höher), Mobiltelefon Benutzername Nr. 1 - 4 (Firmware v2.xx)
Auswahl: 1 bis 16 (Zieladresse)
Mit diesem Parameter weisen Sie Zielgruppen persönliche Benachrichtigungen und Zielgruppen zu.
Die Zentrale sendet persönliche Benachrichtigungen an ein Mobilfunkgerät, wenn es sich bei der Zieladresse um eine Zielrufnummer handelt.
Die Zentrale sendet persönliche Benachrichtigungen an E-Mail-Konten, wenn es sich bei der Zieladresse um eine E-Mail-Adresse handelt.

Hinweis!
Persönliche Benachrichtigung werden nicht bei ungültigen Zieladressen gesendet
Wenn die Zieladresse nicht auf eine richtige Zielrufnummer oder eine korrekte E-Mail-Adresse eingestellt ist, sendet die Zentrale keine persönliche Benachrichtigung. Die Zentrale protokolliert einen SMS-Sendefehler.

Hinweis!
Mobilfunk-IP-Adresse für primäres Zielgerät oder Ersatzzieladresse nicht erforderlich
Es ist nicht erforderlich, die Parameter „Primary Destination Device” (Primäres Zielgerät) oder „Backup Destination Device” (Ersatzzielgerät) auf „Cellular IP” (Mobilfunk-IP-Adresse) einzustellen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Personal Notification > Personal Notifications Reports > Personal Notification 1-4 [Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Persönliche Benachrichtigungsprotokolle >Persönliche Benachrichtigung 1 – 4)]

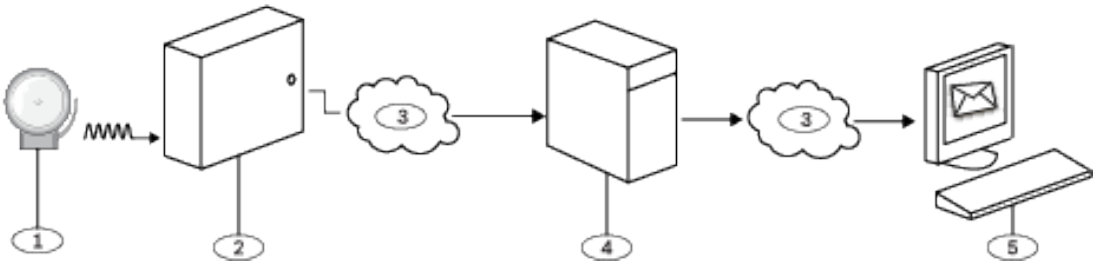
4.18 Persönliche Benachrichtigung – Routing-Versuche

Standardeinstellung: 3
Auswahl: 1 – 6
Legen Sie fest, wie oft die Zentrale versucht, eine persönliche Benachrichtigung zu senden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Personal Notification > Personal Notification Routing Attempts (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Persönliche Benachrichtigung – Routing-Versuche)

4.19 Konfiguration des E-Mail-Servers

Sie können die Zentrale so konfigurieren, dass persönliche Benachrichtigungen an bis zu 16 E-Mail-Adressen gesendet werden.
Wenn ein Ereignis auftritt, übermittelt die Zentrale über ein IP-Netzwerk ein Protokoll an einen E-Mail-Server. Der SMTP (Simple Mail Transfer Protocol)-E-Mail-Server übersetzt die eingehenden Daten in Text und überträgt diesen dann an die von Ihnen konfigurierten Adressen. Dies ist eine unidirektionale Übertragung von der Zentrale an den Benutzer.



Element – Beschreibung
1: Alarmereignis
2: Kompatible Bosch-Zentrale
3: Internet
4: SMTP-E-Mail-Server
5: PC oder ein anderes Gerät für den E-Mail-Empfang

E-Mail-Konto einrichten

So richten Sie ein E-Mail-Konto ein, das E-Mails an die persönlichen Benachrichtigungsziele sendet:

1. Registrieren Sie sich für ein E-Mail-Konto eines E-Mail-Anbieters (z. B. Google, Yahoo, AOL oder Microsoft).
2. Wählen Sie einen Benutzernamen, über den Benachrichtigungsempfänger problemlos erkennen können, welche E-Mails von der Zentrale gesendet werden (Beispiel: panelacctstore52).
3. Geben Sie die dem SMTP-E-Mail-Server zugeordnete Adresse in den Parameter „Email Server Name/Address” (Name/Adresse des E-Mail-Servers) ein.
4. Geben Sie im Parameter „Authentication User Name” (Authentifizierungs-Benutzername) den bei der Registrierung verwendeten Benutzernamen ein.
5. Geben Sie das Passwort, das Sie bei der Registrierung dieses Kontos verwendet haben, im Parameter „Authentication Password” (Authentifizierungs-Passwort) ein.

4.19.1 Email Server Name/Address (Name/Adresse des E-Mail-Servers)

Standardeinstellung: Leer

Auswahl: Domainname oder IP-Adresse

Geben Sie entweder den Domainnamen oder die Adresse des SMTP-E-Mail-Servers (Simple Mail Transfer Protocol) für den ausgewählten Anbieter an.
Mit dem Domänennamen (oder der Adresse) des Servers sendet die Zentrale persönliche Benachrichtigungen an bestimmte E-Mail-Empfänger.

SMTP-E-Mail-Server

Die folgende Tabelle enthält einige bekannte E-Mail-Anbieter und den Domainnamen ihres Servers. Falls Ihr Anbieter nicht in der Tabelle aufgeführt wird, wenden Sie sich direkt an den Anbieter, um dessen Domainnamen (oder IP-Adresse) in Erfahrung zu bringen.

E-Mail-Anbieter	Domainname
1&1	smtp.1and1.com
Airmail	mail.airmail.net
AOL	smtp.aol.com
AT&T	outbound.att.net
Bluewin	smtpauths.bluewin.ch
BT Connect	mail.btconnect.tom
Comcast	smtp.comcast.net
Earthlink	smtpauth.earthlink.net
Gmail	smtp.gmail.com
Gmx	mail.gmx.net
HotPop	mail.hotpop.com
Libero	mail.libero.it
Lycos	smtp.lycos.com
O2	smtp.o2.com
Orange	smtp.orange.net
Outlook.com (ehem. Hotmail)	smtp.live.com
Tin	mail.tin.i
Tiscali	smtp.tiscali.co.uk
Verizon	outgoing.verizon.net
Virgin	smtp.virgin.net
Wanadoo	smtp.wanadoo.fr
Yahoo	smtp.mail.yahoo.com

Weitere Informationen

Formate von IP-Adresse und Domainname, Seite 300

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Panel Wide Parameters > Personal Notification > Email Server Configuration > Email Server Name/Address (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Konfiguration des E-Mail-Servers > Name/Adresse des E-Mail-Servers)

4.19.2 Email Server Port Number (Portnummer des E-Mail-Servers)

Standardeinstellung: 25

Auswahl: 1–65535

Port 25 ist der Standard-SMTP-Port für die meisten ausgehenden Server. Wenn die IP die Standard-Portnummer verweigert (normalerweise wegen massiven Spam- und Malware-Aufkommens), verwenden Sie einen anderen häufig verwendeten Port zum Umgehen der Sperre, z. B. Port 587 oder 465.
Beispiele für allgemeine Dienstanbieter, E-Mail-Server, Ports und Sicherheit:

Anbieter	SMTP-Server-URL	Port	Authentifizierung/Verschlüsselung
Gmail	smtp.gmail.com	465	Verschlüsselt
Yahoo (unverschlüsselt)	smtp.mail.yahoo.com	25	Authentifizieren
Yahoo (verschlüsselt)	smtp.mail.yahoo.com	465	Verschlüsselt
Verizon	smtp.verizon.net	465	Verschlüsselt
AT&T	AT&T outbound.att.net	465	Verschlüsselt
Comcast	smtp.comcast.net	465	Verschlüsselt
Time Warner	smtp-server.<region>.rr.com	25	Authentifizieren

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Personal Notification > Email Server Configuration > Email (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Konfiguration des E-Mail-Servers > E-Mail)
Server Port Number (Portnummer des Servers)

4.19.3 Email Server Authentication/Encryption (Authentifizierung/ Verschlüsselung des E-Mail-Servers)

Standardeinstellung: Authenticate
Auswahl:
Basic – keine Authentifizierung, keine Verschlüsselung
Authenticate – Authentifizierung erforderlich, keine Verschlüsselung
Encrypted – Authentifizierung erforderlich, Verschlüsselung erforderlich
Wählen Sie die Sicherheitsstufe aus, die für den E-Mail-Server für den Empfang von Nachrichten von der Zentrale erforderlich ist.
Authentifizierung bedeutet, dass der E-Mail-Server einen Benutzernamen und ein Passwort für die Authentifizierung erfordert. Dies wird auch als SMTP-AUTH bezeichnet.
Die verwendete Verschlüsselung ist TLS (Transport Layer Security)/SSL (Secure Sockets Layer).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Personal Notification > Email Server Configuration > Email Server Authentication/Encryption (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Konfiguration des E-Mail-Servers > Authentifizierung/Verschlüsselung des E-Mail-Servers)

4.19.4 Authentication User Name (Authentifizierungs-Benutzername)

Standardeinstellung: Leer
Auswahl: leer, 1 bis 255 Zeichen
Geben Sie den Benutzernamen für das E-Mail-Konto ein, das persönliche E-Mail-Benachrichtigungen von der Zentrale empfangen soll.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Personal Notification > Email Server Configuration > Authentication User Name (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Konfiguration des E-Mail-Servers > Authentifizierungs-Benutzername)

4.19.5 Authentication Password (Authentifizierungs-Passwort)

Standardeinstellung: Leer
Auswahl: leer, 1 bis 49 Zeichen
Geben Sie das Passwort an, das der SMTP-Server verwendet, um E-Mails an die Ziele für persönliche Benachrichtigungen zu versenden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Panel Wide Parameters > Personal Notification > Email Server Configuration > Authentication Password (Zentralenübergreifende Parameter > Persönliche Benachrichtigung > Konfiguration des E-Mail-Servers > Authentifizierungs-Passwort)

5 Area Wide Parameters (Bereichsübergreifende Parameter)

5.1 Bereichs-/Signalparameter, Optionen für Öffnen/Schließen

Ein Bereich ist als räumlich gruppierte Menge von Meldern definiert.

Konfiguration
Die Bereichsparametrierung bietet eine große Auswahl an verschiedenen Systemkonfigurationen. Zur Definition von Ansteuerungs-, Steuerungs- und Meldefunktionen weist die Zentrale jedem Bereich eine Kontonummer zu. Falls gewünscht, können Sie die Bereichsscharfschaltung bei anderen Bereichen bedingt konfigurieren [„master" (Master) oder „associate" (Zugeordnet)]. Sie können jeden Bereich für die Außenhaut- und Innenbereichscharfschaltung konfigurieren. Für diese Funktion ist kein separater Bereich erforderlich. Verbinden Sie mehrere Bereiche zu einem gemeinsam benutzten Bereich, der automatisch gesteuert wird (z. B. Gang oder Empfangsbereich).
Bei Systemen mit mehreren Bereichen müssen alle Bereiche derselben Verantwortung und Verwaltung unterliegen. Dabei kann es sich um mehrere zusammenhängende oder unzusammenhängende Gebäude handeln, die auch unterschiedliche Adressen haben können, aber der Verantwortung einer Person oder Einheit mit gemeinsamem Interesse unterliegen, bei der es sich nicht um die Installationsfirma der Meldeanlage handelt. Dies gilt nicht für Anwendungen in Einkaufsstraßen, bei denen jedes unabhängige Unternehmen eine eigene separate Meldeanlage haben muss.
Ein Beispiel für eine gewerbliche Meldeanlage ist ein Unternehmen mit einem Bürobereich und einem Warenlager in einem Gebäude, in dem jeder Bereich voneinander unabhängig scharf- oder unscharfgeschaltet werden kann.
In einem Privathaushalt können beispielsweise Garage und Haus innerhalb eines Systems separat konfiguriert werden.
In jedem der obigen Beispiele unterliegen alle Bereiche der Verantwortung einer Person.
In Systemen mit mehreren Bereichen müssen sich das Signal (oder akustischer Signalgeber) und die Zentrale in einem der geschützten Bereiche befinden.
Das Signal bzw. der akustische Signalgeber müssen so angeordnet sein, dass sie für Benutzer, die Bereiche scharf- oder unscharfschalten, hörbar sind.

5.1.1 Area Name Text (first language) [Text Bereichsname (erste Sprache)]

Standardeinstellung: Area # (Bereichsnummer)
Auswahl: Bis zu 32 Zeichen (Text, Zahlen, Leerzeichen und Symbole)
Geben Sie einen Bereichsnamen ein, der an Bedienteilen angezeigt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Name Text (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Text Bereichsname)

5.1.2 Area Name Text (Second Language) [Text Bereichsname (zweite Sprache)]

Standardeinstellung: Leer
Auswahl: Bis zu 32 Zeichen (Text, Zahlen, Leerzeichen und Symbole)
Geben Sie einen Bereichsnamen ein, der an Bedienteilen angezeigt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Name Text
(Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/ Schließen > Text Bereichsname)
(Second Language) (Zweite Sprache)

5.1.3 Area On (Bereich an)

Standardeinstellung:
- B5512:
  - Bereich 1: Ja
  - Bereiche 2 bis 4: Nein
- B4512:
  - Bereich 1: Ja
  - Bereich 2: Nein
- B3512:
  - Bereich 1: Ja

Auswahl:
Yes: Bereich ist aktiviert.
No: Bereich ist deaktiviert.

Hinweis!
UL 864-Anforderung
Zur Einhaltung der UL 864-Anforderungen für gewerbliche Brandmeldesysteme setzen Sie diesen Parameter auf „Ja”.

Bereich ist auf „Nein” gesetzt:
- Melder, die diesem Bereich zugewiesen sind, erstellen keine Ereignisse.
- Bei Scharf- oder Unscharfschaltung wird diese Bereichsnummer nicht an Bedienteilen angezeigt, die sich in Reichweite dieses Bereichs befinden.
- Der Status dieses Bereichs wird nicht mit Statusprotokollen übermittelt.
- Alle Zugriffsberechtigungen in diesem Bereich werden ausgeschaltet, während der Bereich deaktiviert ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area On
(Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/ Schließen > Bereich An)

5.1.4 Kontonummer

Standardeinstellung:
- B5512 v3.xx: 0000
- B5512 v2.xx:
  - Bereich 1: 1111
  - Bereiche 2 bis 4: 0000
- B4512 und B3512: 0000

Auswahl: 4- oder 10-stellige Zahlen, 0 – 9, B – F
Mit diesem Parameter wird die für diesen Bereich protokollierte Kontonummer festgelegt. Jedem aktiven Bereich muss eine Kontonummer zugewiesen werden.
Wenn die Kontonummer mindestens fünfstellig ist, fügt RPS der Nummer automatisch führende Nullen hinzu, um eine zehnstellige Nummer zu erstellen.

Hinweis!
Die Automatisierungssoftware der Zentrale muss mit zehnstelligen Kontonummern kompatibel sein, bevor Sie eine zehnstellige Kontonummer in die Zentrale parametrieren.

Hinweis!
Kontonummern dürfen an keiner Stelle ein „A“ enthalten.

Mit Kontonummern werden Bereiche gruppiert. Jeder Bereich kann über eine unterschiedliche Kontonummer verfügen. Mehreren Bereichen kann jedoch auch die gleiche Kontonummer zugewiesen sein. Die Zentrale verwendet die Kontonummer als Referenz für die Scharfschaltung und Textanzeigen an Bedienteilen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Account Number (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Kontonummer)

5.1.5 Force Arm/Bypass Max (Zwangsläufiges Scharfschalten/Abschalten)

Standardeinstellung: 2
Auswahl:
B5512: 0 bis 16
B4512: 0 bis 10
B3512: 0 bis 10
Geben Sie die Anzahl kontrollierter Melder ein, die bei Scharfschaltung des Bereichs gestört oder abgeschaltet sein können.
Informieren Sie sich beim Wiederherstellen des Melders für das System im Melderprofil über die Parameter *Zwangsläufige Scharfschaltung wiederherstellbar, Seite 243* und *Übergehung wiederherstellbar, Seite 243*, wenn sich der Melder wieder im Normalzustand befindet oder der Bereich unscharfgeschaltet wird.

Hinweis!
Zum Abschalten oder zwangsläufigen Scharfschalten eines Melders muss der Parameter *Übergehen möglich, Seite 244* auf „Ja” gesetzt sein. 24-Stunden-Melder werden durch Zwangsscharfschaltung nicht abgeschaltet.

Hinweis!
Zur Erfüllung des UL1610-Standards setzen Sie diesen Parameter für Funk-Handsender auf „0“.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Force Arm/Bypass Max (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Zwangsläufiges Scharfschalten/Abschalten)

5.1.6 Delay Restorals (Wiederherstellungen bei Verzögerung)

Standardeinstellung: keine Verzögerung
Auswahl:

„No Delay“ (Keine Verzögerung): Melder-Wiederherstellungsereignisse werden protokolliert und gemeldet, wenn der Melder physisch wiederhergestellt wurde.
„Delay Until Bell is Silenced” (Verzögerung bis Stummschaltung Zutrittssignal): Melder-Wiederherstellungsereignisse werden bis zur physischen Wiederherstellung des Melders und der Stummschaltung des Zutrittssignals (oder bis zum Ablauf der Signaldauer) nicht protokolliert oder gemeldet.
Bei Feuermeldern, Gasmeldern oder für die Errichterbedienung parametrierten Meldern werden Wiederherstellungsereignisse erst dann protokolliert oder gemeldet, wenn der Melder physisch wiederhergestellt, das Zutrittssignal stummgeschaltet und das Ereignis vom Bedienteil gelöscht wurde.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Delay Restorals (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Wiederherstellungen bei Verzögerung)

5.1.7 Exit Tone (Scharfschaltungston)

Standardeinstellung: Yes
Auswahl:
Ja: Scharfschaltungston während der Scharfschalteverzögerung an allen Bedienteilen wiedergeben
Nein: Scharfschaltungstöne an Bedienteilen individuell aktivieren/deaktivieren (Bedienteilkonfiguration)

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Exit Tone (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Scharfschaltungston)

5.1.8 Scharfschalteverzögerungszeit

Standardeinstellung: 60
Auswahl: 0 bis 600 (Sekunden, in Schritten von 5 Sekunden)
Legen Sie die Zeit fest, die Benutzern zum Verlassen der Räume zur Verfügung steht, ohne das Erstellen eines Alarmereignisses
Das Verlassen der Räume muss über einen Melder erfolgen, der einem Melderprofil zugewiesen ist, das für eine kontrollierte Melderart mit verzögerter Alarmreaktionszeit konfiguriert ist (siehe *Melderreaktion, Seite 223*).
Melder, die für eine unverzögerte Alarmreaktion parametriert sind, generieren Alarme sofort (sogar während der Scharfschalteverzögerung).

Hinweis!
Zur Erfüllung von SIA CP-01 zur Fehlalarmunterdrückung legen Sie diesen Parameter auf einen Wert zwischen 45 und 255 Sekunden fest. Weitere Informationen finden Sie unter „SIA CP-01 Verification” (SIA CP-01-Verifizierung).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Exit Delay Time (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Scharfschalteverzögerungszeit)

5.1.9 Auto Watch (Automatische Überwachung)

Standardeinstellung: Manuell

Auswahl:

– Manuell: Benutzer schalten den Überwachungsmodus manuell am Bedienteil ein und aus.
– On at Disarm (An bei Unscharfschaltung): Die Zentrale schaltet den Überwachungssmodus bei Unscharfschaltung des Bereichs automatisch ein (ausgeschaltet).

Ist ein Bereich unscharfgeschaltet (Ausgeschaltet) und der Überwachungsmodus aktiviert, ertönt der Überwachungston an Bedienteilen dann, wenn als Überwachungsmelder konfigurierte Melder eine Störung aufweisen.
Siehe *Überwachungsmelder, Seite 241*, um zu erfahren, wie Sie Melder für die Überwachungsfunktion konfigurieren.
Wenn für den Bereich die Außenhautaktivierung (scharfgeschaltet) aktiv ist, wird der Überwachungston im Falle einer Störung nur bei als Überwachungsmelder konfigurierten Innenbereichsmeldern wiedergegeben. Melder der Art „Sichtbarer Überfallalarm bei intern und extern scharf (mit Verzögerung)“ protokollieren Störungen als Alarme oder Fehler.
Wenn dieser „Auto Watch” (Automatische Überwachung)-Parameter auf „Manuell” eingestellt und der Überwachungsmodus bei Scharfschaltung („Vollscharfschaltung” oder „Außenhautüberwachung”) des Bereichs aktiv ist, ist der Überwachungsmodus bei Unscharfschaltung (Ausschaltung) des Bereichs aktiviert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Auto Watch (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Automatische Überwachung)

5.1.10 Neustartzeit

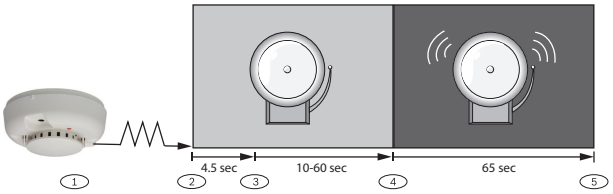
Standardeinstellung: 5
Auswahl: 5 bis 55 (Sekunden, in Schritten von 1 Sekunde)
Stellen Sie die Länge der Wartezeit für die Stabilisierung von Sensoren ein, nachdem an einem Melder zur Alarmbestätigung eine Störung aufgetreten ist und nach Zurücksetzung des Melders die Melder wieder mit Strom versorgt werden.
Die Alarmverifizierung ist ein Merkmal automatischer Branderkennungs- und Alarmsysteme zur Fehlalarmunterdrückung und kommt zum Einsatz, wenn Melder für einen Mindestzeitraum Alarmbedingungen protokollieren oder Alarmbedingungen innerhalb einer bestimmten Zeit nach dem Zurücksetzen bestätigen, damit diese als gültiges Alarmauslösesignal akzeptiert werden.

Hinweis!
Aktivieren Sie die Funktion „Cross Point” (Melderabhängigkeit) nicht in Melderprofilen, die für Feuermelder bestimmt sind.

Hinweis!
Entnehmen Sie die Stabilisierungszeit dem Datenblatt des Melders, und geben Sie einen Wert ein, der die längste Zeitdauer, die von einem Melder in der Meldeleitung festgelegt wurde, um mindestens 5 Sekunden übertrifft.

Hinweis!
Prüfen Sie die geltenden Bestimmungen zur zulässigen maximalen Erkundungszeit.

Zum Aktivieren der Alarmverifizierungsfunktion werden Alarmverifizierungsmelder individuell parametriert. Siehe „Point Profile“ (Melderprofil). Jeder zurücksetzbare Feuermelder kann die Funktion „Alarmverifizierung” für den Bereich aktivieren, dem er zugeordnet ist. Bosch empfiehlt die Verwendung unterschiedlicher Bereichsalarmausgänge.
Zum Aktivieren der Alarmverifizierung für einen Melder setzen Sie „Melderart” auf „Feuer“ und „Alarmbestätigung“ und „Resettable” (Rücksetzbar) auf „Ja“.
Ist ein Alarmverifizierungsmelder offen, unterbricht die Zentrale automatisch die Stromzufuhr für die zurücksetzbaren Melder, die mit dem Ausgang „Reset Sensors” (Melder zurücksetzen) des Bereichs verbunden sind. Die Stromversorgung wird 4,5 Sekunden lang unterbrochen. Wenn die Stromversorgung wiederhergestellt ist, ignoriert die Zentrale die Alarme von zurücksetzbaren Meldern entsprechend der Zeit, die in „Restart Time” (Neustartzeit) parametriert wurde. Nach Ablauf der Neustartzeit wird 65 Sekunden lang ein Bestätigungsfenster eingeblendet. Wenn sich der Alarmverifizierungsmelder immer noch im Alarmzustand befindet oder während der Anzeige des Bestätigungsfensters erneut eine Störung aufweist, wird ein Alarm generiert.



Element – Beschreibung
1: Der Melder erkennt ein mögliches Ereignis.
2: Die Stromversorgung für zurücksetzbare Melder wurde unterbrochen.
3: Die Stromversorgung für zurücksetzbare Melder wurde wiederhergestellt. Die Neustartzeit beginnt.
4: Das Bestätigungsfenster wird eingeblendet. Jeder Alarm, der während dieses Zeitraums auftritt, wird angekündigt.
5: Das Bestätigungsfenster wird ausgeblendet. Bei einem weiteren offenen Alarmverifizierungsmelder werden diese Schritte in obiger Reihenfolge erneut ausgeführt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Restart Time (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Neustartzeit)

5.1.11 Duress Enable (Bedrohungsalarm aktivieren)

Standardeinstellung: Nein
Auswahl:
- Ja: Bedrohungsalarm für diesen Bereich aktivieren
- Nein: Bedrohungsalarm für diesen Bereich deaktivieren

Hinweis!
SIA CP-01-Anforderung
Zur Erfüllung des SIA CP-01-Standards legen Sie diesen Parameter auf„Ja“ fest.

Verwendet ein Benutzer den Befehl „Move“ (Verschieben), um das Bedienteil an einen Bereich zu verschieben, für den dieser Parameter auf „Nein“ gesetzt ist, wird durch einen gültigen Bedrohungsbenutzercode zur Unscharfschaltung kein Bedrohungsprotokoll gesendet. Wenn Sie den Parameter für einen bestimmten Bereich auf „Nein“ einstellen, ist der Zugangscode, den Sie normalerweise für „Bedrohung“ eingeben, in diesem Bereich nicht mehr gültig. Wird dieser Parameter auf „Nein“ gesetzt und ein Zugangscode mit der entsprechenden Berechtigung zum Unscharfschalten für das Aufheben der Scharfschaltung einer Bedrohung im Bereich verwendet wird, erscheint auf dem Display des Bedienteils „KEINE BERECHTIGUNG”.

Weitere Informationen
Siehe *Bedrohungstyp, Seite 104*, um eine Erklärung von „Bedrohung“ zu erhalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Duress Enable (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen >Bedrohungsalarm aktivieren)

5.1.12 Bereichstyp

Voreinstellung: Regular (Regelmäßig)
Auswahl:
Regular (Regelmäßig): Scharf- und Unscharfschaltung unabhängig von anderen Bereichen
Master: Vor dem Scharfschalten eines Hauptbereichs müssen sich zugeordnete Bereiche mit der Kontonummer des Hauptbereichs in Scharfschalteverzögerung oder in Vollscharfschaltung mit Verzögerung befinden. Mehrere Hauptbereiche können eine Kontonummer gemeinsam verwenden.
Zugeordnet: Die Kontonummer eines gemeinsam benutzten Bereichs verbindet zugeordnete Bereiche mit Hauptbereichen. Zuordnen Bereiche können unabhängig von anderen zugeordneten Bereichen mit der gleichen Kontonummer und dem Hauptbereich scharf- und unscharfgeschaltet werden.
„Shared” (Gemeinsam): Gemeinsam benutzte Bereiche sind mit anderen Bereichen nicht nach Kontonummer verknüpft. Sie werden scharfgeschaltet, wenn sich alle zugeordneten Bereiche in der Zentrale in Vollscharfschaltung mit Verzögerung befinden. Gemeinsam benutzte Bereiche werden unscharfgeschaltet, wenn sich mindestens ein zugeordneter Bereich der Zentrale nicht in Vollscharfschaltung mit Verzögerung befindet [Außenhautaktivierung (scharfgeschaltet) aktiv oder unscharfgeschaltet].

Hauptbereich und zugeordnete Bereiche scharfschalten
Wird ein Hauptbereich scharfschaltet, während die zugeordneten Bereiche nicht scharfgeschaltet sind, erscheint eine Meldung mit dem Hinweis „Check Area” (Bereich überprüfen).
Ein Hauptbereich kann unabhängig vom scharfgeschalteten Zustand der anderen Bereiche des Kontos unscharfgeschaltet werden.

Hinweis!
Der Bedienteilbereich wirkt sich auf das Scharfschalten von Hauptbereichen aus.
Das Scharfschalten eines Hauptbereichs an einem Bedienteil mit einem auf „Panel Wide” (Zentralenweit) oder „Account Wide” (Kontoübergreifend) eingestellten Bedienteilumfang führt dazu, dass die Scharfschalteverzögerung für alle zugeordneten Bereiche (mit der gleichen Kontonummer) gestartet wird.

Hinweis!
Verwenden Sie zeitgesteuerte Ereignisse vor dem Scharfschalten eines Hauptbereichs zunächst für das Scharfschalten zugeordneter Bereiche.
Vor der Scharfschaltung eines Hauptbereichs mittels eines zeitgesteuerten Ereignisses müssen zunächst die zugeordneten Bereiche mit zeitgesteuerten Ereignissen scharfgeschaltet werden.

Hinweis!
Mit RPS, Schlüsselschaltern oder der Funktion „Auto Close" (Automatische Scharfschaltung) werden Hauptbereiche ohne die Scharfschaltung zugeordneter Bereiche scharfgeschaltet.
Die Scharfschaltung von Hauptbereichen mit RPS, Schlüsselschaltern oder der Funktion „Auto Close" (Automatische Scharfschaltung) setzt nicht voraus, dass alle zugeordneten Bereiche scharfgeschaltet werden.

Gemeinsam benutzte und zugeordnete Bereiche scharfschalten
Das Scharfschalten aller zugeordneten Bereiche führt zur Scharfschaltung gemeinsam benutzter Bereiche. Sobald der letzte zugeordnete Bereich scharfgeschaltet ist, beginnt die Scharfschaltung des zugeordneten Bereichs automatisch mit der Scharfschalteverzögerung für den Bereich, dem das Bedienteil zugewiesen ist.
Gemeinsam benutzte Bereiche können nicht mit einem Zugangscode, einer Karte, einem Schlüsselschalter, mit zeitgesteuerten Ereignissen oder mit RPS scharfgeschaltet werden.
Gemeinsam benutzte Bereiche werden automatisch unscharfgeschaltet, wenn ein beliebiger zugeordneter Bereich der Zentrale unscharfgeschaltet ist. Gemeinsam benutzte Bereiche können nicht mit einem Zugangscode, einer Karte, einem Schlüsselschalter oder mit RPS unscharfgeschaltet werden.

Hinweis!
Scharfschaltebefehle erfordern zentralenweiten Umfang
Scharfschaltebefehle für einen gemeinsam benutzten Bereich müssen auf einem Bedienteil mit zentralenweitem Umfang von einem Benutzer durchgeführt werden, der über Benutzerrechte für alle zugeordneten Bereiche verfügt.

Ein gemeinsam benutzter Bereich ist nicht in Scharfschaltebereitschaft
Wenn ein Melder im gemeinsam benutzten Bereich offen ist, wird auf dem Bedienteil des letzten zugeordneten Bereichs, der scharfgeschaltet werden soll, [„CHECK AREA" (BEREICH PRÜFEN)] angezeigt.

Hinweis!
Bedienteilumfang für zugeordnete Bereiche muss gemeinsam benutzte Bereiche umfassen
Zum Anzeigen der offenen Meldergruppen eines gemeinsam benutzten Bereichs auf einem Bedienteil eines zugeordneten Bereichs, müssen die gemeinsam benutzten und die zugeordneten Bereiche die gleiche Kontonummer verwenden. Der Umfang von Bedienteilen, die zugeordneten Bereichen zugewiesen sind, muss gemeinsam benutzte Räume umfassen.

Einen gemeinsam benutzten Bereich zwangsscharfschalten
Wird auf dem Bedienteil [„CHECK AREA" (BEREICH PRÜFEN)] angezeigt, drücken Sie die WEITER-Taste, bis die Meldung „Force Arm?" (Scharfschaltung erzwingen?) erscheint. Durch das Drücken der Eingabetaste wird der gemeinsam benutzte Bereich zwangsscharfgeschaltet,

wenn der Benutzer über das Recht zur Melderabschaltung verfügt, der Melder abschaltbar ist und die Anzahl offener Meldergruppen den „Force Arm Max" (Zwangsläufiges Scharfschalten Max.)-Grenzwert für den gemeinsam benutzten Bereich nicht überschreitet.

Scharfschaltestatus eines gemeinsam benutzten Bereichs anzeigen
Informieren Sie sich mit dem Befehl „BEREICHSSTATUS ANZEIGEN" über den scharfgeschalteten Zustand eines gemeinsam benutzten Bereichs. Benutzer müssen über ein Benutzerrecht verfügen, das dem gemeinsam benutzten Bereich zugewiesen ist.

Alarme und Störungen in gemeinsam benutzten Bereichen stummschalten
Benutzer können Alarme und Störungen in gemeinsam benutzten Bereichen an einem beliebigen Bedienteil stummschalten. Benutzer müssen über ein Benutzerrecht verfügen, das dem gemeinsam benutzten Bereich zugewiesen ist.

Auf Zutrittskontrollleser, die gemeinsam benutzten Bereichen zugewiesen sind, zugreifen
Wenn der Eingangsbereich scharfgeschaltet und ein gemeinsam benutzter Bereich ist, beginnt die Scharfschalteverzögerung erneut. Benutzer können dann zu einem zugeordneten Bereich gehen und diesen unscharfschalten. Enthält der dem gemeinsam benutzten Bereich zugewiesene Kartenleser beliebige zugeordnete Bereiche im Bereich „D## KP#" (im Abschnitt ZUTRITTSKONTROLLE), werden beim Vorzeigen der Karte sowohl der zugeordnete als auch der gemeinsam benutzte Bereich unscharfgeschaltet.

Schließprotokolle für gemeinsam benutzte Bereiche
Für Schließprotokolle benötigen Benutzer eine gültige Zugriffsberechtigung, die dem gemeinsam benutzten Bereich zugewiesen ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Type (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Bereichstyp)

5.1.13 Zwei-Mann-Regel?

Standardeinstellung: Nein
Auswahl:
Ja: Zum Unscharfschalten des Bereichs müssen am selben Bedienteil zwei unterschiedliche Zugangscodes eingegeben werden.
Nein: Die Eingabe eines Zugangscodes führt zur Unscharfschaltung des Bereichs.

Hinweis!
SIA CP-01-Anforderung
Zur Erfüllung von SIA CP-01 zur Fehlalarmunterdrückung legen Sie diesen Parameter für alle aktivierten Bereiche auf „Nein" fest. Weitere Informationen finden Sie unter „SIA CP-01 Verification" (SIA CP-01-Verifizierung).

Verwenden Sie diesen Parameter in Bereichen, die mit Bedienteilen mit dem Umfang *Scope (Bereich), Seite 145* aus dem Zustand „Vollscharfschaltung" unscharfgeschaltet worden sind. Ein Alarmereignis tritt auf, wenn die Eingangsverzögerung endet, bevor der Benutzer den zweiten Zugangscode eingibt.
Wenn das Bereichsalarmsignal ertönt, wird der Alarm durch Eingabe des ersten Zugangscodes stummgeschaltet. Die Eingabe des zweiten Zugangscodes führt zur Unscharfschaltung des Bereichs.

Falls für die Eingabe des zweiten Zugangscodes ein anderes Bedienteil als bei der Eingabe des ersten Zugangscodes verwendet wird, weist das zweite Bedienteil den Benutzer darauf hin, dass die Zwei-Mann-Regel ausgeführt wird und der Benutzer beide Zugangscodes am selben Bedienteil eingeben soll.
Sie können eine benutzerdefinierte Funktion erstellen, mit der der Bereich durch die Eingabe eines Zugangscodes unscharfgeschaltet wird.
Setzen Sie diesen Parameter in Einrichtungen, in denen für den Zutritt zum gesicherten Bereich eine höhere Sicherheitsstufe erforderlich ist, auf „Ja“. In einer Bank wird dieser Parameter möglicherweise aktiviert, um Zugriff auf den Tresor zu ermöglichen.
Ist dieser Parameter aktiviert, setzen Sie den Parameter *Scope (Bereich), Seite 145* für Bedienteile in den betroffenen Bereichen auf „Area Wide“ (Bereichsübergreifend).
Setzen Sie die Zwei-Mann-Regel nicht in einem Bereich auf „Ja“, für den *Zweimalige Authentifizierung?, Seite 132* auf „Ja ” gesetzt ist.
Diese Funktion funktioniert nur bei Unscharfschaltung durch Zugangscode.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Two Man Rule (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Zwei-Mann-Regel)

5.1.14 Zweimalige Authentifizierung?

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Early Ambush (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Zweimalige Authentifizierung)

Siehe
- *Early Ambush Time (Zeit für zweimalige Authentifizierung), Seite 109*
- *Second Ambush Code (Code für zweimalige Authentifizierung), Seite 109*
- *Zwei-Mann-Regel?, Seite 131*

5.1.15 Feuer und Gas – Zeit

Standardeinstellung: 6
Auswahl: 0 bis 90 (Minuten)
Geben Sie die Feueralarmauslösezeit (in Minuten) für Feuer- und Gasalarmmelder an.

Hinweis!
An die zuständigen lokalen Behörden wenden
Erkundigen Sie sich bei den zuständigen lokalen Behörden, um die für die Installation geeignete Signaldauer zu bestätigen.

Der für diese Zeitdauer aktivierte Ausgang wird in „A# Fire Bell” (A# Feueralarm) parametriert. Die Dauer von „A## Gas Bell” (A## Gasalarm) ist vollkommen unabhängig von der Dauer von A## Fire Bell (A## Feueralarm), richtet sich jedoch auch nach der in dieser Aufforderung parametrierten Zeit. Das Alarmsignal wird aktiviert, sobald der Feueralarm ausgelöst wird. Das Signal wird deaktiviert, wenn die in Minuten parametrierte Signaldauer abgelaufen ist. Legen Sie für diesen Parameter einen Wert von mindestens zwei Minuten fest.

Ort im RPS-Menü
Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Feuer und Gas – Zeit

5.1.16 Fire Pattern (Brandmuster)

Standardeinstellung: Pulsierend

Auswahl:

- Durchgängig: durchgängige Ausgabe
- Impuls: pulsierende March Time 60 Schläge pro Minute in gleichmäßigem Tempo (0,5 Sekunden „Ein”, 0,5 Sekunden „Aus”)
- California Standard (Standard Kalifornien): 10 Sekunden hörbar, 5 Sekunden stumm, 10 Sekunden hörbar, 5 Sekunden stumm
- Zeitcode 3: 0,5 Sekunden „Ein”, 0,5 Sekunden „Aus”, 0,5 Sekunden ein, 0,5 Sekunden „Aus”, 0,5 Sekunden „Ein”, 1,5 Sekunden „Aus”

Wählen Sie das Muster aus, das dieser Bereich für Feuermelderalarme verwendet. Muster werden bis zum Ablauf der Branddauer wiederholt.
Muster werden mindestens 3 Minuten lang mit einer Zeittoleranz von ± 10 % wiederholt. (1999 NFPA-Standards erlauben das automatische Stummschalten laut geltender Bestimmungen und ermöglichen eine Mindes-Rufsignaldauer von 5 Minuten).

Hinweis!
Zwei Melder verwenden denselben Ausgang bei Alarm
Wenn sich zwei Feuermelder mit demselben Ausgang im Alarmzustand befinden, wird das Alarmmuster des aktuellsten Feuerereignisses priorisiert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Fire Pattern (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Brandmuster)

5.1.17 Burg Time (Einbruchalarmzeit)

Standardeinstellung: 6

Auswahl: 0 bis 90 (Minuten)

Geben Sie den Zeitraum (in Minuten) an, über den hinweg das Alarmsignal für Einbruchalarmmelder aktiv ist.

Hinweis!
An die zuständigen lokalen Behörden wenden
Erkundigen Sie sich bei den zuständigen lokalen Behörden, um die für die Installation geeignete Signaldauer zu bestätigen.

Hinweis!
SIA CP-01
Zur Erfüllung der SIA CP-01-Anforderungen zur Fehlalarmunterdrückung legen Sie diesen Parameter in allen aktivierten Bereichen auf einen Wert von mindestens 6 Minuten fest.
Weitere Informationen finden Sie unter SIA CP-01-Verifizierung.

Der *Alarm-Signalgeber, Seite 165*-Ausgang A# wird aktiviert, wenn der Einbruchalarm ausgelöst wird. Er wird nach Ablauf der Einbruchalarmzeit ausgeschaltet.
Legen Sie für diesen Parameter einen Wert von mindestens zwei Minuten fest.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Burg Time (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Einbruchalarmzeit)

5.1.18 Burg Pattern (Muster für Einbruchalarm)

Standardeinstellung: Durchgängig

Auswahl:

- Durchgängig: durchgängige Ausgabe
- Impuls: pulsierende March Time 60 Schläge pro Minute in gleichmäßigem Tempo (0,5 Sekunden „Ein”, 0,5 Sekunden „Aus”)
- California Standard (Standard Kalifornien): 10 Sekunden hörbar, 5 Sekunden stumm, 10 Sekunden hörbar, 5 Sekunden stumm Wird wiederholt, bis die Signaldauer des Feueralarms abläuft.
- Zeitcode 3: 0,5 Sekunden „Ein”, 0,5 Sekunden „Aus”, 0,5 Sekunden ein, 0,5 Sekunden „Aus”, 0,5 Sekunden „Ein”, 1,5 Sekunden „Aus” Wird wiederholt, bis die Signaldauer abläuft.

Wählen Sie das Alarmmuster, das in diesem Bereich für Alarme von Nicht-Feuermeldern verwendet wird. Muster werden bis zum Ablauf der Einbruchalarmzeit wiederholt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Burg Pattern (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Muster für Einbruchalarm)

5.1.19 Gas Pattern (Gasmuster)

Standardeinstellung: Zeitcode 4

Auswahl:

- Durchgängig: durchgängige Ausgabe
- Impuls: pulsierende March Time 60 Schläge pro Minute in gleichmäßigem Tempo (0,5 Sekunden „Ein”, 0,5 Sekunden „Aus”)
- California Standard (Standard Kalifornien): 10 Sekunden hörbar, 5 Sekunden stumm, 10 Sekunden hörbar, 5 Sekunden stumm
- Zeitcode 3: 0,5 Sekunden „Ein”, 0,5 Sekunden „Aus”, 0,5 Sekunden ein, 0,5 Sekunden „Aus”, 0,5 Sekunden „Ein”, 1,5 Sekunden „Aus”
- Zeitcode 4: 0,1 Sekunden „Ein”, 0,1 Sekunden „Aus”, 0,1 Sekunden „Ein”, 0,1 Sekunden „Aus”, 0,1 Sekunden „Ein”, 0,1 Sekunden „Aus”, 0,1 Sekunden „Ein”, 5 Sekunden „Aus”.

Wählen Sie das Muster aus, das dieser Bereich für Gasmelderalarme verwendet. Muster werden bis zum Ablauf der Branddauer wiederholt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Gas Pattern (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Gasmuster)

5.1.20 Single Ring (Ein Alarmsignal)

Standardeinstellung: Nein

Auswahl:

- Ja: Nach einem Alarmereignis führen nachfolgende Alarmereignisse bei Nicht-Feuermeldern im selben Bereich während desselben Scharfschaltezeitraums nicht zur Aktivierung des Alarmausgangs.
- Nein: Der Alarmausgang wird bei jedem Alarmereignis aktiviert.

Single Ring (Ein Alarmsignal) hat keinen Einfluss auf den Bedienteil-Alarmton und verhindert nicht, dass Protokolle erstellt werden.

Feuermelder werden nicht beeinträchtigt, und die Signaldauer startet bei jedem weiteren Alarm neu.

Durch Stummschalten des Zutrittssignals wird „Single Ring” (Ein Alarmsignal) zurückgesetzt.

Hinweis!
Single Ring (Ein Alarmsignal) wird durch Schlüsselschalter nicht gelöscht.
Tritt ein Alarm an einem 24-Stunden-Melder auf, während der Bereich unscharfgeschaltet ist, führt eine Scharfschaltung dieses Bereichs mit einem Schlüsselschalter nicht dazu, dass „Single Ring" (Ein Alarmsignal) zurückgesetzt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Single Ring (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Ein Alarmsignal)

5.1.21 Zutrittssignaltest

Standardeinstellung: Nein
Auswahl:
- Ja: Aktivieren Sie zur Durchführung eines Zutrittssignaltests den Ausgang des Alarm-Signalgebers für zwei Sekunden, nachdem Sie von der Empfangseinrichtung die Quittung für das Schließprotokoll erhalten haben (alternativ am Ende der Scharfschalteverzögerung bei Zentralen, die keine Schließprotokolle senden).
- Nein: Zutrittssignaltest ist deaktiviert.

Hinweis!
Zutrittssignaltest nur bei Gesamtscharfschaltung
Die Zutrittssignaltest-Funktion funktioniert nur, wenn der Bereich vollständig scharfgeschaltet ist. Die Zutrittssignaltest-Funktion funktioniert nicht, wenn nur die Außenhautüberwachung für den Bereich aktiviert ist.

Zutrittssignaltest nach Schließprotokoll
Bei Bereichen, die zum Senden von Öffnungs- und Schließprotokollen konfiguriert sind, wird das Alarmsignal für 2 Sekunden aktiviert, wenn die Zentrale eine Schließprotokollrückmeldung von der Empfangseinrichtung erhält.
Wenn für diesen Zutrittssignaltest-Parameter „Ja" festgelegt ist, konfigurieren Sie den Bereich nicht für eingeschränkte Öffnungen und Schließungen oder Öffnen-Fenster und Schließen-Fenster.

Zutrittssignaltest nach Scharfschalteverzögerung
Wenn für diesen Zutrittssignaltest-Parameter „Ja" festgelegt ist und der Bereich nicht zum Senden von Öffnungs- und Schließprotokollen konfiguriert ist, wird das Alarmsignal für 2 Sekunden aktiviert, wenn die Austrittszeit abläuft.

Mehrere Bereiche gleichzeitig scharfschalten
Beim gleichzeitigen Scharfschalten mehrerer Bereiche (z. B. mit der Funktion „ARM ALL AREAS?" [ALLE BEREICHE SCHARFSCHALTEN?]) sendet die Zentrale parallel Schließprotokolle für jeden Bereich an die Empfangseinrichtung. Der Zutrittssignaltest erscheint, wenn die Zentrale die Bestätigung für jeden Bericht empfängt.
Wenn Schließprotokolle nicht gesendet werden und für alle Bereiche die gleiche Scharfschalteverzögerungszeit eingestellt ist, wird der Ausgang des Alarm-Signalgebers für jeden Bereich zwei Sekunden lang (mit einer jeweiligen Pause von zwei Sekunden) aktiviert.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Bell Test (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Zutrittssignaltest)

5.1.22 Account O/C (Konto öffnen/schließen)

Standardeinstellung: Nein

Auswahl:

– Ja: Öffnungs- und Schließprotokolle nach Konto für diesen Bereich senden
– Nein: Öffnungs- und Schließprotokolle nicht nach Konto senden

Die Zentrale sendet ein Kontoschließprotokoll, wenn der letzte Bereich dieses Kontos geschlossen (scharfgeschaltet) ist.
Die Zentrale sendet ein Kontoöffnungsprotokoll, wenn der erste Bereich in einem Konto geöffnet (unscharfgeschaltet) ist.
Nach dem Senden des Kontoöffnungsprotokolls führt das Unscharfschalten anderer Bereiche des Kontos nicht zur Erstellung eines weiteren Kontoöffnungsprotokolls. Kontoöffnungs- und Schließprotokolle enthalten keine Bereichsinformationen.
Setzen Sie diesen Parameter für alle Bereiche im Konto auf den gleichen Wert.
Vergewissern Sie sich, dass die Kontonummer für alle im Konto enthaltenen Bereiche dieselbe ist.
Wird ein Konto geöffnet oder geschlossen, während ein Öffnen- oder Schließen-Fenster aktiv und *Disable O/C in Window (Öffnen/Schließen in Fenster deaktivieren), Seite 137* auf „Ja" gesetzt ist, wird das Protokoll nicht gesendet. Bosch empfiehlt, dass für Bereiche mit gleicher Kontonummer die gleichen Zeitangaben für Öffnen- und Schließen-Fenster verwendet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS")

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Account O/C (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Konto öffnen/schließen).

5.1.23 Area O/C (Bereich öffnen/schließen)

Standardeinstellung: Yes

Auswahl:

– Ja: Bereichsinformationen in Öffnungs- und Schließprotokollen für diesen Bereich miteinbeziehen Protokolle für Bereiche einzeln senden
– Nein: keine Öffnungs- und Schließprotokolle für diesen Bereich erstellen

Wenn dieser Parameter auf „Ja" und der Parameter *Account O/C (Konto öffnen/schließen), Seite 136* auf „Nein" gesetzt ist, sind Bereichsinformationen in Öffnungs- und Schließprotokollen enthalten. Die Zentrale sendet Protokolle für einzelne Bereiche.
Ist „Acct O/C" (Öffnen/Schließen durch Konto) auf „Ja"eingestellt, sendet die Zentrale ein Kontoschließprotokoll (keine Bereichsinformationen), wenn der letzte Bereich mit gleicher Kontonummer scharfgeschaltet ist. Die Zentrale sendet ein Kontoöffnungsprotokoll (keine Bereichsinformationen), wenn der erste Bereich mit gleicher Kontonummer unscharfgeschaltet ist.
Setzen Sie diesen Parameter nicht auf „Ja", wenn die Zentrale Protokolle an ein Automatisierungssystem sendet, das nicht auf die Verarbeitung von Öffnungs- und Schließprotokollen für mehrere Bereiche ausgelegt ist.
Öffnungs-/Schließprotokolle werden nur für Benutzer mit folgenden *Benutzerrechte, Seite 193* gesendet:

– Scharfschaltebereitschaft: Bereich öffnen/schließen = E
– Nicht scharfschaltebereit (Zwangsläufige Scharfschaltung/Abschalten Scharfschalten): Eingeschränkt öffnen/schließen = E
– Scharfschaltung Außenhautüberwachung: Außenhautüberwachung öffnen/schließen = E

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area O/C (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Bereich öffnen/schließen)

5.1.24 Disable O/C in Window (Öffnen/Schließen in Fenster deaktivieren)

Standardeinstellung: Yes
Auswahl:

- Ja: Öffnungs- und Schließprotokolle nicht an das Bedienteil senden, wenn das Öffnungs- oder Schließereignis innerhalb eines aktiven Fenster auftritt.
- Nein: Öffnungs- und Schließprotokolle an das Bedienteil senden, auch wenn das Öffnungs- oder Schließereignis innerhalb eines parametrierten Fensters auftritt.

Wenn dieser Parameter auf „Ja” gesetzt wird und ein Öffnungs- oder Schließereignis außerhalb eines Fensters auftritt, sendet die Zentrale das Öffnungs- oder Schließprotokoll mit einem Früh- oder Spät-Modifizierer. Siehe „Fenster öffnen/schließen“
Wenn dieser Parameter auf „Nein” gesetzt ist und ein Öffnungs- oder Schließereignis außerhalb des entsprechenden Fensters auftritt, bezieht die Zentrale bei Öffnungs- oder Schließprotokollen keine Früh- oder Spät-Modifizierer mit ein.
Öffnungs- und Schließereignisse werden immer protokolliert.
Wenn alle Öffnungs- und Schließaktivitäten überwacht, aber Funktionen von Öffnen- und Schließen-Fenstern verwendet werden sollen, setzen Sie diesen Parameter auf „Nein” und parametrieren die Öffnen-/Schließen-Fenster.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Disable O/C in Window (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen >Öffnen/Schließen in Fenster deaktivieren)

5.1.25 Auto Close (Automatische Scharfschaltung)

Standardeinstellung: Nein
Auswahl:

- Ja: Der Bereich wird am Ende des Schließen-Fensters automatisch mit verzögerter Vollscharfschaltung scharfgeschaltet. Im Falle einer automatischen Scharfschaltung des Bereichs sendet die Zentrale ein Schließprotokoll, wenn Bereichs- und/oder Kontoprotokolle hierfür parametriert wurden.
- Nein: Bereich am Ende des Schließen-Fensters nicht automatisch scharfschalten

Unabhängig von *Force Arm/Bypass Max (Zwangsläufiges Scharfschalten/Abschalten), Seite 125* oder *Übergehen möglich, Seite 244* erfolgt eine zwangsläufige Zwangsscharfschaltung, die zu offenen, aus dem System ausgegrenzten Meldergruppen führt. Siehe *Zwangsläufige Scharfschaltung wiederherstellbar, Seite 243* oder *Übergehung wiederherstellbar, Seite 243*, um Informationen zur Wartung dieser Melder zu erhalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Auto Close (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Automatische Scharfschaltung)

5.1.26 Fehler beim Öffnen

Standardeinstellung: Nein
Auswahl:

– Ja: Die Zentrale sendet ein „Fail to Open”-Protokoll (Fehler beim Öffnen), wenn der Bereich zum Zeitpunkt „Open Window Stop” (Fenster öffnen – Stopp) nicht unscharfgeschaltet ist.
– Nein: „Fail to Open”-Protokolle (Fehler beim Öffnen) werden für diesen Bereich nicht gesendet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Fail To Open (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/ Schließen > Fehler beim Öffnen)

5.1.27 Fehler beim Schließen

Standardeinstellung: Nein
Auswahl:
– Ja: Die Zentrale sendet ein „Fehler beim Schließen”-Protokoll, wenn der Bereich zum Zeitpunkt „Close Window Stop ”(Fenster schließen - Stopp) nicht scharfgeschaltet ist.
– Nein: „Fehler beim Schließen”-Protokolle werden für diesen Bereich nicht gesendet.

Öffnungs- und Schließprotokolle müssen nicht für das Senden von „Fehler beim Schließen”-Protokollen parametriert werden.
Eine Scharfschalteverzögerungszeit muss in *Scharfschalteverzögerungszeit, Seite 126* parametriert werden.
Wenn *Auto Close (Automatische Scharfschaltung), Seite 137* auf „Ja” gesetzt ist, wird ein Protokoll gesendet, weil es zum Zeitpunkt der Stoppzeit des Schließen-Fensters auftritt.
Ist *Disable O/C in Window (Öffnen/Schließen in Fenster deaktivieren), Seite 137* auf „Ja” gesetzt, wird nach dem „Fehler beim Schließen”-Protokoll ein „Closing Late”-Protokoll (Spätes Schließen) oder ein „Force Close Late”-Protokoll (Erzwungenes spätes Schließen) erstellt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Fail To Close (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/ Schließen > Fehler beim Schließen)

5.1.28 Latest Close Time (Letzte Schließzeit)

Standardeinstellung: Deaktiviert
Auswahl:
– Deaktiviert – Funktion ist für den Bereich deaktiviert.

Verwenden Sie „Letzte Schließzeit“ mit der Funktion *Extend Close (Schließen verlängern), Seite 270*, um die Verlängerung der Schließzeit für einen Bereich einzuschränken. Wenn die letzte Schließzeit beispielsweise auf 19:30 eingestellt ist, können Sie die erwartete Schließzeit nur auf bis zu 19:29 verlängern.
Ist der Wert für die letzte Schließzeit ungleich 0, kann für den Paramater *Fenster schließen - Start, Seite 261* keine spätere oder die gleiche Uhrzeit festgelegt werden wie für den Parameter „Latest Close Time” (Letzte Schließzeit). Wenn z. B. der Parameter „Latest Close Time” (Letzte Schließzeit) auf „17:30” eingestellt ist, kann der Parameter „Close Window Start” (Fenster schließen - Start) nicht auf „17:30” oder höher festgelegt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Latest Close Time (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/ Schließen > Letzte Schließzeit)

5.1.29 Restricted O/C (Eingeschränkt öffnen/schließen)

Standardeinstellung: Nein

Auswahl:

– Ja: Öffnen und Schließen von Protokollen für diesen Bereich einschränken
– Nein: Öffnen und Schließen von Protokollen für diesen Bereich nicht einschränken

Wird die Einstellung auf „Ja“ gesetzt, werden Öffnungsprotokolle nur gesendet, wenn der Bereich nach einem Feuerfehl- oder Gasalarm unscharfgeschaltet wurde. Schließprotokolle werden nur gesendet, wenn der Bereich mit offenen Meldergruppen vollscharfgeschaltet wurde.

Protokolle werden bei eingeschränktem Schließen in der folgenden Reihenfolge gesendet: Zwangsläufig scharfgeschaltet, Zwangsläufiger Melder, Zwangsläufiges Schließen, Schließprotokoll.

Wenn zum Einschalten des Systems kein Zugangscode erforderlich ist, sind Schließprotokolle immer eingeschränkt, wenn „Restricted O/C” (Eingeschränkt öffnen/schließen) auf „Ja” gestellt wurde. Ist zum Einschalten des Systems ein Zugangscode erforderlich, müssen Benutzer über *Benutzerrechte, Seite 193* mit „Restricted Open/Close = E (enabled)” (Eingeschränkt öffnen/schließen = E (aktiviert) verfügen, damit das Öffnen und Schließen von Protokollen eingeschränkt werden kann.

Zum Erstellen eingeschränkter Öffnungs- und Schließprotokolle muss*Area O/C (Bereich öffnen/schließen), Seite 136* auf „Ja” gesetzt sein.

Aktive „Öffnen/Schließen”-Fenster verhindern eingeschränkte Öffnungs- und Schließprotokolle nicht. Frühe oder späte Bezeichnungen werden Öffnungs- und Schließprotokollen nicht hinzugefügt, wenn diese entsprechend den Regeln für das Öffnen/Schließen von Protokollen gesendet wurden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Restricted O/C (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Eingeschränkt öffnen/schließen)

5.1.30 Part On O/C (Außenhautüberwachung öffnen/schließen)

Standardeinstellung: Nein

Auswahl:

– Ja: Öffnungs- und Schließprotokolle bei „Part On Instant” (Unverzögerte Außenhautüberwachung) und „Part On Delay” (Verzögerte Außenhautüberwachung) senden
– Nein: keine Öffnungs- und Schließprotokolle bei „Part On Instant” (Unverzögerte Außenhautüberwachung) und „Part On Delay” (Verzögerte Außenhautüberwachung) senden

Öffnungs- und Schließprotokolle bei Außenhautüberwachung werden durch „Öffnen/Schließen”-Fenster nicht unterdrückt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Part On O/C (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Öffnen/Schließen durch Außenhautüberwachung)

5.1.31 Exit Delay Restart (Neustart der Scharfschalteverzögerung)

Standardeinstellung: Yes

Auswahl:

Ja: „Exit Delay Restart” (Neustart der Scharfschalteverzögerung) aktivieren
Nein: „Exit Delay Restart” (Neustart der Scharfschalteverzögerung) deaktivieren

Mit der Funktion „Exit Delay Restart" (Neustart der Scharfschalteverzögerung) wird die Scharfschalteverzögerung neu gestartet, wenn ein Endbenutzer die Räume vor Ablauf der Scharfschalteverzögerung erneut betritt.
So kann es beispielsweise sein, dass ein Hausbesitzer das System einschaltet (scharfschaltet), beim Verlassen des Hauses die Tür schließt und dann bemerkt, dass er den Autoschlüssel vergessen hat. Öffnet er dann die Tür, um die Schlüssel zu holen, aktiviert die Zentrale die Scharfschalteverzögerung erneut. Hierdurch steht dem Hausbesitzer ausreichend Zeit zum Abschalten des Systems zur Verfügung.
Ist dieser Parameter auf „Ja" eingestellt, führt das Ausführen der folgenden Schritte zur Reaktivierung der Scharfschalteverzögerung(*Scharfschalteverzögerungszeit, Seite 126*):

1. System in allen Bereichen oder teilweise scharfschalten
2. Lösen Sie einen Melderalarm aus, und führen Sie anschließend eine Melderwiederherstellung (durch Öffnen und Schließen einer Tür) bei einem Melder durch, der für die Melderart, Außenhautüberwachung und eine verzögerte Alarmmelderreaktion konfiguriert ist (4, 5, 6, 7 oder 8). (*Melderprofile, Seite 216*, *Melderart, Seite 218*, *Melderreaktion, Seite 223*)
3. Verursachen Sie bei weiterhin ausgeführter Scharfschalteverzögerung einen Fehler an einem beliebigen Melder (Öffnen einer Tür), der einem für die Melderart konfigurierten Melderprofil zugewiesen ist (Außenhautüberwachung), erfolgt eine verzögerte Alarmmelderreaktion (4, 5, 6, 7 oder 8). Die Scharfschalteverzögerung wird erneut gestartet.

Hinweis!
Scharfschalteverzögerung wird nur ein Mal neu gestartet
Die Scharfschalteverzögerung kann nur ein Mal neu gestartet werden. Das Auslösen einer Störung am selben Melder oder das Auslösen einer Störung an einem anderen Melder während der reaktivierten Scharfschalteverzögerung führt nicht dazu, dass die Scharfschalteverzögerung ein zweites Mal neu gestartet wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Exit Delay Restart (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Neustart der Scharfschalteverzögerung)

5.1.32 All On - No Exit (Vollscharfschaltung – Kein Austritt)

Standardeinstellung: „Ja"
Auswahl:
Ja: Die Zentrale wechselt beim Scharfschalten von „All On Delay" (Verzögerte Vollscharfschaltung) zu „Part On Delay" (Verzögerte Außenhautüberwachung), wenn kein Melder der Art „Part On Delay" (Verzögerte Außenhautüberwachung) während der Scharfschalteverzögerungszeit gestört oder wiederhergestellt wird.
Nein: Die Zentrale wechselt den Scharfschaltemodus nicht.
Der endgültige scharfgeschaltete Zustand wird gemeldet und an den Bedienteilen angezeigt. Beim Scharfschalten über Funk-Handsender oder zeitgesteuerte Ereignisse wird diese Option von der Zentrale nicht berücksichtigt.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > All On - No Exit (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Vollscharfschaltung – Kein Austritt)

5.1.33 Warnung Scharfschalteverzögerungszeit

Standardeinstellung: Nein

Auswahl:

– Ja: Alarmausgang während der letzten 10 Sekunden der Scharfschaltverzögerung alle zwei Sekunden pulsieren
– Nein: Alarmausgang während der Scharfschalteverzögerung nicht pulsieren

Hinweis!

SIA CP-01-Anforderung

Zur Erfüllung der SIA CP-01-Anforderungen zur Fehlalarmunterdrückung setzen Sie diesen Parameter auf „Ja“. Weitere Informationen finden Sie unter „SIA CP-01 Verification” (SIA CP-01-Verifizierung).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Exit Delay Warning (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Warnung Scharfschalteverzögerungszeit)

5.1.34 Warnung Eintrittsverzögerung

Standardeinstellung: Nein

Auswahl:

– Ja: Alarmausgang während der letzten 10 Sekunden der Eingangsverzögerung alle zwei Sekunden pulsieren
– Nein: Alarmausgang während der Eingangsverzögerung nicht pulsieren

Hinweis!

SIA CP-01-Anforderung

Zur Erfüllung der SIA CP-01-Anforderungen zur Fehlalarmunterdrückung setzen Sie diesen Parameter auf „Ja“. Weitere Informationen finden Sie unter „SIA CP-01 Verification” (SIA CP-01-Verifizierung).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Entry Delay Warning (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Warnung Eintrittsverzögerung)

5.1.35 Area Re-Arm Time (Zeit zum erneuten Scharfschalten des Bereichs)

Standardeinstellung: 00:00

Auswahl: 00:00 (deaktiviert) bis 23:59

Mit diesem Parameter wird die Dauer (HH:MM) der Verzögerung eines unscharfgeschalteten Bereichs festgelegt, bis er verzögert erneut vollscharfgeschaltet wird.

Wenn beispielsweise die Zeit zum erneuten Scharfschalten eines Bereichs auf vier Stunden („04:00”) eingestellt ist und der Bereich um 13:30 Uhr unscharfgeschaltet (deaktiviert) wird, erfolgt die erneute Scharfschaltung mittels verzögerter Vollscharfschaltung um 17:30 Uhr. Alle nicht scharfschaltebereiten (offenen) Melder werden zwangsläufig scharfgeschaltet.

Hinweis!

„Force Arm/Bypass Max” (Zwangsläufiges Scharfschalten/Abschalten) wird beim erneuten Scharfschalten ignoriert.

Alle nicht scharfschaltebereiten (offenen) Melder werden zwangsläufig scharfgeschaltet, wenn der Bereich am Ende der Zeit zum erneuten Scharfschalten scharfgeschaltet wird.

Die erneute Scharfschaltung des Bereichs erfolgt automatisch um 23:59 Uhr – unabhängig davon, wann der Zeitschalter für die erneute Scharfschaltezeit gestartet wurde.
Wenn z. B. der Zeitschalter für die erneute Scharfschaltung des Bereichs auf 4 Stunden („04:00”) eingestellt ist und der Bereich um 22:30 Uhr unscharfgeschaltet (deaktiviert) wird, erfolgt die erneute Scharfschaltung des Bereichs mittels verzögerter Vollscharfschaltung um 23:59 Uhr (1 Stunde und 29 Minuten nach Unscharfschaltung).
Benutzer können „Extend Close Time” (Schließzeit verlängern) an einem System-Bedienteil verwenden, um die Verzögerung der erneuten Scharfschaltung eines aktiven Bereichs zu verlängern
[On/Off Menu > Extend Close time (Menü „Ein/Aus” > Schließzeit verlängern)].

Hinweis!
Die Konfiguration der Zeitangaben für Schließen-Fenster und das erneute Scharfschalten von Bereichen können zu unvorhergesehenen Bereichsaktivitäten führen.
Wenn sowohl ein Schließen-Fenster als auch die Zeit zum erneuten Scharfschalten eines Bereichs für den gleichen Bereich konfiguriert werden, das Schließen-Fenster parallel zum Zeitschalter für die erneute Scharfschaltezeit ausgeführt wird, und ein Benutzer die verlängerte Schließzeit an einem System-Bedienteil verwendet , erweitert die Zentrale nur das Schließen-Fenster, nicht die Zeit zum erneuten Scharfschalten des Bereichs.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Re-Arm Time (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Zeit zum erneuten Scharfschalten des Bereichs)

5.2 Area Arming Text (Text Bereichsscharfschaltung)

5.2.1 Area name text (Text Bereichsname)

Standardeinstellung: Area # (Bereichsnummer)
Auswahl: Bis zu 32 Zeichen (Text, Zahlen, Leerzeichen und Symbole)
Geben Sie einen Bereichsnamen ein, der an Bedienteilen angezeigt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Arming Text > Area Name Text (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Text Bereichsscharfschaltung > Text Bereichsname)

5.2.2 Account is On text (Text für Konto aktiv)

Standardeinstellung: Leer
Auswahl: Geben Sie bis zu 32 Zeichen ein.
Geben Sie den am Bedienteil anzuzeigenden Text bei Bedarf für jeden Bereich an.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Arming Text > Account is On Text (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Text Bereichsscharfschaltung > Text für Konto aktiv)

5.2.3 Area # is On text (Text für Bereichsnr. aktiv)

Standardeinstellung: Leer
Auswahl: Geben Sie bis zu 32 Zeichen ein.
Geben Sie den am Bedienteil anzuzeigenden Text bei Bedarf für jeden Bereich an.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Arming Text > Area # is On Text (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Text Bereichsscharfschaltung > Text für Bereichsnr. aktiv)

5.2.4 Area # is not Ready text (Text für Bereichsnr. nicht bereit)

Standardeinstellung: Leer
Auswahl: Geben Sie bis zu 32 Zeichen ein.
Geben Sie den am Bedienteil anzuzeigenden Text ein, wenn der Bereich nicht scharfschaltebereit ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Arming Text > Area # Not Ready Text (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Text Bereichsscharfschaltung > Text für Bereichsnr. nicht bereit)

5.2.5 Area Nr. is Off text (Text für Bereichsnr. ist ausgeschaltet)

Standardeinstellung: Leer
Auswahl: Geben Sie bis zu 32 Zeichen ein.
Geben Sie den am Bedienteil anzuzeigenden Text ein, wenn der Bereich ausgeschaltet (unscharfgeschaltet) ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Arming Text > Area # is Off Text (Bereichsübergreifende Parameter > Bereichs-/Signalparameter, Optionen für Öffnen/Schließen > Text Bereichsscharfschaltung > Text für Bereichsnr. ist ausgeschaltet)

6 Bedienteile

6.1 Bedienteilzuweisungen

Die Zentralen B5512 und B4512 unterstützen SDI2-Bedienteile 1 bis 8. B3512 unterstützt Bedienteile 1 bis 4.

6.1.1 Keypad Name (first language) [Name des Bedienteils (erste Sprache)]

Standardeinstellung: Bedienteilnummer

Optionen: Bis zu 32 Zeichen

Geben Sie Text, Zahlen und Symbole (bis zu 32 Zeichen) zur Beschreibung des Bedienteils ein.

An Bedienteilen werden die ersten 20 Zeichen angezeigt. Werden mehr als 20 Zeichen eingegeben, wird auf dem Display des Bedienteils der vollständige Text einmal eingeblendet. Drücken Sie die Escape-Taste, um den Text erneut einzublenden.

Leerzeichen zählen als Text und sind in der Zeichenbeschränkung (max. 32 Zeichen) enthalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Keypads > Keypad Assignments > Keypad Name (Bedienteile > Bedienteilzuweisungen > Name des Bedienteils)

6.1.2 Keypad Name (second language) [Name des Bedienteils (zweite Sprache)]

Standardeinstellung: leer

Optionen: Bis zu 32 Zeichen

Geben Sie Text, Zahlen und Symbole (bis zu 32 Zeichen) zur Beschreibung des Bedienteils ein.

An Bedienteilen werden die ersten 20 Zeichen angezeigt. Werden mehr als 20 Zeichen eingegeben, wird auf dem Display des Bedienteils der vollständige Text einmal eingeblendet. Drücken Sie die Escape-Taste, um den Text erneut einzublenden.

Leerzeichen zählen als Text und sind in der Zeichenbeschränkung (max. 32 Zeichen) enthalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Keypads > Keypad Assignments > Keypad Name (second language) [Bedienteile > Bedienteilzuweisungen > Name des Bedienteils (zweite Sprache)]

6.1.3 Keypad Type (Bedienteiltyp)

Standardeinstellung:

- Adresse 1 = B92x Zweileitungs-Bedienteil
- Alle anderen Adressen = Kein Bedienteil installiert

Auswahl:

- No keypad installed (Kein Bedienteil installiert)
- Basisbedienteil B91x
- Zweileitungs-Bedienteil B92x
- ATM-Bedienteil B93x
- Touchscreen-Bedienteil B94x

Wählen Sie den Typ des Bedienteils, das über diese Adresse mit der Zentrale verbunden ist. Der Bedienteiltyp wird bei der erstmaligen Installation des Bedienteils automatisch konfiguriert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Keypads > Keypad Assignments > Keypad Type (Bedienteile > Bedienteilzuweisungen > Bedienteiltyp)

6.1.4 Area Assignment (Bereichszuordnung)

Standardeinstellung: 1

Auswahl:

– B5512: 1 bis 4
– B4512: 1 bis 2
– B3512: 1

Wählen Sie einen Bereich, den Sie einem Bedienteil zuweisen möchten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Keypads > Keypad Assignments > Area Assignment (Bedienteile > Bedienteilzuweisungen > Bereichszuordnung)

6.1.5 Bedienteilsprache

Standardeinstellung: Erste Sprache, Benutzersprache übernehmen

Auswahl:

– Erste Sprache, Benutzersprache folgen
– Erste Sprache, Benutzersprache ignorieren
– Zweite Sprache, Benutzersprache übernehmen
– Zweite Sprache, Benutzersprache ignorieren

Wählen Sie eine Sprache für das Bedienteil aus.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Keypads > Keypad Assignments > Keypad Language (Bedienteile > Bedienteilzuweisungen > Bedienteilsprache)

6.1.6 Scope (Bereich)

Standardeinstellung:

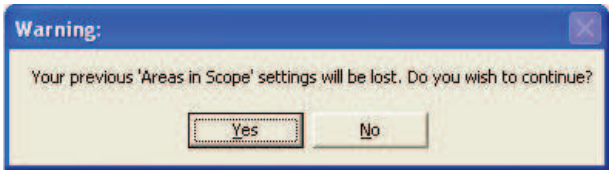
– Adresse 1: Panel Wide (Zentralenübergreifend)
– Alle anderen Adressen: Area Wide (Bereichsübergreifend)

Auswahl:

– Area Wide (Bereichsübergreifend): Am Bedienteil werden Funktionsbeschreibungen zum Scharf- und Unscharfschalten nur für den Bereich angezeigt, dem das Bedienteil zugewiesen ist.
– Account Wide (Kontoübergreifend): Am Bedienteil werden Informationen sowie Funktionsbeschreibungen zum Scharf- und Unscharfschalten für Bereiche mit der gleichen Kontonummer angezeigt. Diese Einstellung wird normalerweise für den Bereichstyp „Associate” (Zugeordnet) verwendet.
– Zentralenübergreifend: Mit einem zentralenübergreifenden Bedienteil können Informationen zu allen Bereichen sowie Scharfschalte- und Unscharfschaltefunktionsbeschreibungen für alle Bereiche in der Zentrale angezeigt werden. Diese Einstellung wird normalerweise für einen Hauptbereich verwendet.
  Die Auswahl „Panel Wide” (Zentralenübergreifend) steht nicht für Control Panels B4512 und B3512 zur Verfügung.
– Benutzerdefiniert: Wählen Sie die „Areas in Scope” (Bereiche im Umfang) für ein benutzerdefiniertes Bedienteil.
  Die Auswahl „Benutzerdefiniert” steht für Control Panels B4512 und B3512 nicht zur Verfügung.

Der Bereich gibt vor, welche Bereiche über das Bedienteil eingesehen werden können, welche Bereiche bei scharfgeschaltetem Bedienteil angesteuert werden und zu welchen Bereichen dieses Bedienteil wechseln kann.

Bei Auswahl von „Benutzerdefiniert”, zeigt RPS den folgenden Warnhinweis an:



Wenn Sie auf „Ja” klicken, wird „Areas In Scope” (Bereiche im Umfang) auf die Standardeinstellung zurückgesetzt.
Mit einem Klick auf„Nein” werden keine Änderungen durchgeführt.

Weitere Informationen

Kontonummer, Seite 124
Bereichstyp, Seite 129
Areas in Scope (Bereiche im Umfang), Seite 146

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Keypads > Keypad Assignments > Scope (Bedienteile > Bedienteilzuweisungen > Bereich)

Siehe

- *Kontonummer, Seite 124*
- *Bereichstyp, Seite 129*
- *Areas in Scope (Bereiche im Umfang), Seite 146*

6.1.7 Areas in Scope (Bereiche im Umfang)

Standardeinstellung:

- Adresse 1: Alle
- Alle anderen Adressen: Bereich 1

Auswahl:

- Klicken Sie auf „Area #” (Bereichsnr.), um einen Bereich auszuwählen oder zu entfernen.
- Klicken Sie auf „Set All” (Alle festlegen), um alle Bereiche auszuwählen.
- Mit einem Klick auf „Clear All” (Alle löschen) löschen Sie alle Bereiche (keine Auswahl).

Führen Sie einen Doppelklick aus, um Bereiche anzuzeigen und auszuwählen.
Klicken Sie auf die Bereiche, die im benutzerdefinierten Bereich dieses Bedienteils enthalten sein sollen.

Weitere Informationen

Scope (Bereich), Seite 145

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Keypads > Keypad Assignments > Areas in Scope (Bedienteile > Bedienteilzuweisungen > Bereiche im Umfang)

6.1.8 Passcode Follows Scope? (Zugangscode entspricht Anwendungsbereich?)

Standardeinstellung: „Ja“

Auswahl:

- Ja: Befindet sich ein Bereich, der einem Bedienteil zugewiesen ist, im scharfgeschalteten Zustand, werden durch die Eingabe eines Zugangscodes der Bereich und alle im Bedienteilbereich enthaltenen Bereiche unscharfgeschaltet. Ist der Bereich unscharfgeschaltet, werden der Bereich und alle anderen Bereiche im Bedienteilbereich scharfgeschaltet.
- Nein: Durch die Eingabe eines Zugangscodes wird nur der Bereich scharf- oder unscharfgeschaltet, dem das Bedienteil zugewiesen ist.

„Passcode Follows Scope” (Zugangscode entspricht Anwendungsbereich) gilt nur für das Scharfschalten per Benutzercode. Dies gilt für die Scharfschaltefunktionen in der Funktionsliste.

Benutzern müssen Benutzerrechte zugewiesen sein, für die die Parameter „Arm by Passcode” (Scharfschalten durch Zugangscode) und Disarm by Passcode (Unscharfschalten durch Zugangscode aufheben) aktiviert sind.

Weitere Informationen
Scope (Bereich), Seite 145
Bereich, Seite 212
Scharfschaltung durch Zugangscode, Seite 206
Scharfschaltung durch Zugangscode aufheben, Seite 207

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Passcode Follows Scope (Bedienteile > Bedienteilzuweisungen > Zugangscode entspricht Anwendungsbereich)

6.1.9 Enter Key Output (Ausgang Eingabetaste)

Standardeinstellung: 0

Auswahl:

- 0: Der Zugangscode-Eingabefunktion ist kein Ausgang zugewiesen, „Cycle Output” (Ausgang öffnen und schließen)
- B5512: 1 – 3, 9 – 48 – bestimmt Ausgangsnummer für Zugangscode-Eingabefunktion, „Cycle Output” (Ausgang öffnen und schließen)
- B4512: 1 – 3, 9 – 28
- B3512: 1 – 3

Wird die *Passcode Enter Function (Zugangscode-Eingabefunktion), Seite 147* auf „Cycle Output” (Ausgang öffnen und schließen) gesetzt, und drückt ein Benutzer nach der Eingabe des Zugangscodes die Eingabetaste, wird der Ausgang „Enter Key“ (Eingabetaste) zehn Sekunden lang aktiviert. Die Ereignisse werden dem Zentralenprotokoll hinzugefügt: „Output ### Set” (Ausgang ### festlegen) mit Benutzer-ID und „Output ### Reset” (Ausgang ### zurücksetzen) ohne Benutzer-ID.

Hinweis!
Verwenden Sie den Ausgang Eingabetaste nicht gemeinsam mit anderen Ausgangsfunktionen. Der Ausgang, den Sie in diesem Parameter für den Ausgang Eingabetaste zuweisen, darf keiner anderen Ausgangsfunktion zugewiesen werden. Beim Betrieb des Ausgangs können Fehler auftreten.

Mit der Zugangscode-Eingabefunktion, „Cycle Door” (Tür öffnen und schließen) sowie dem Ausgang „Enter Key“ (Eingabetaste) können Türen auch von Benutzern mit einer niedrigen Zugriffsstufe geöffnet werden. Eine Melderverzögerung ist nicht möglich.

Weitere Informationen
Passcode Enter Function (Zugangscode-Eingabefunktion), Seite 147

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Enter Key Output (Bedienteile > Bedienteilzuweisungen > Ausgang Eingabetaste)

6.1.10 Passcode Enter Function (Zugangscode-Eingabefunktion)

Standardeinstellung: Scharf-/Unscharfschalten

Auswahl:

- Scharf-/Unscharfschalten: Ist der aktuelle Bereich unscharfgeschaltet, führt die Eingabe des Zugangscodes zusammen mit dem Drücken der Eingabetaste dazu, dass für alle Bereiche innerhalb des Benutzerbereichs die verzögerte Vollscharfschaltung einsetzt. Bei Scharfschalten des aktuellen Bereichs werden alle Bereiche innerhalb des Benutzerbereichs unscharfgeschaltet.
- Cycle Output (Ausgang öffnen und schließen): Durch die Eingabe des Zugangscodes und Drücken der Eingabetaste wird der Ausgang Eingabetaste 10 Sekunden lang aktiviert.
- Automatische erneute Scharfschaltung: Wenn der dem Bedienteil zugewiesene Bereich „Vollscharfschaltung mit Verzögerung" aktiviert wurde, wird durch Eingabe des Zugangscodes und Drücken der Eingabetaste die Scharfschalteverzögerung erneut gestartet. Bei Unscharfschaltung des Bereichs wird durch die Eingabe des Zugangscodes und das Drücken der Eingabetaste keine Scharfschaltung aktiviert.
- Login Only (Nur Anmeldung): Die Anmeldung des Benutzers erfolgt durch Eingabe des Zugangscodes und Drücken der Eingabetaste. Zweifache Authentifizierung wird nicht angewendet.
- Anmeldung/Unscharfschalten: Durch Eingabe des Benutzercodes und anschließendes Drücken der Eingabetaste werden Benutzer angemeldet und alle Bereiche im Benutzerbereich unscharfgeschaltet. Zweifache Authentifizierung wird nicht angewendet.

Liegen Benutzerrechte für den aktuellen Bereich vor, führt die Eingabe eines Zugangscodes immer zur Stummschaltung von Alarmen und Störungen.
Kann eine Zugangscode-Eingabefunktion aufgrund von Konfigurationskonflikten nicht ausgeführt werden, aktiviert die Zentrale die Funktion „Scharf-/Unscharfschalten" unabhängig von der Einstellung.
Der Service-Zugangscode (Benutzer-ID 0) kann nicht für Zugangscode-Eingabefunktionen verwendet werden.
Ausgänge, die für die Funktion „Cycle Output" (Ausgang öffnen und schließen) verwendet werden, stehen nicht für andere Melder-, Melderrücksetz-, Zentralen- oder Signalfunktionen zur Verfügung. Die gemeinsame Nutzung kann zu einem fehlerhaften Betrieb des Ausgangs führen.

Hinweis!
Zweifache Authentifizierung nicht mit der automatischen erneuten Scharfschaltung kompatibel
Wenn der Parameter „Dual Authentication" (Zweifache Authentifizierung) auf „Ja" eingestellt ist, setzen Sie den Parameter „Passcode Enter Function" (Zugangscode-Eingabefunktion) nicht auf „Auto Re-arm" (Automatische erneute Scharfschaltung).

Hinweis!
SIA CP-01-Anforderung
Zur Erfüllung der SIA CP-01-Anforderungen zur Fehlalarmunterdrückung behalten Sie die Standardeinstellung dieses Parameters bei.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Keypads > Keypad Assignments > Passcode Enter Function (Bedienteile > Bedienteilzuweisungen > Zugangscode-Eingabefunktion)

6.1.11 Dual Authentication (Zweifache Authentifizierung)

Standardeinstellung: Nein
Auswahl:

– Ja: Benutzer müssen zum Scharfschalten, Unscharfschalten oder Verwenden passwortgeschützter Benutzerfunktionen an einem B94X Touchscreen-Bedienteil einen Zugangscode eingeben **und** eine Codierkarte (Karte oder Codierschlüssel) verwenden.
– Nein: Benutzer geben einen Zugangscode ein **oder** verwenden eine Codierkarte.

Bevor Sie diesen Parameter auf „Ja“ setzen, stellen Sie sicher, dass ein B94X Touchscreen-Bedienteil im System enthalten ist.

Hinweis!
Zweifache Authentifizierung nicht mit der automatischen erneuten Scharfschaltung kompatibel
Ist der Parameter „Dual Authentication” (Zweifache Authentifizierung) auf „Ja“ eingestellt, setzen Sie den Parameter „Passcode Enter Function” (Zugangscode-Eingabefunktion) nicht auf „Auto Re-arm” (Automatische erneute Scharfschaltung).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Dual Authentication (Bedienteile > Bedienteilzuweisungen > Zweifache Authentifizierung)

6.1.12 Dual Authentication Duration (Dauer der zweifachen Authentifizierung)

Standardeinstellung: 20 Sekunden
Auswahl: 10, 15, 20, 25, 30, 35, 40, 45 Sekunden
Bei Aktivierung von „Dual Authentication” (Zweifache Authentifizierung) müssen Benutzer innerhalb dieser Dauer einen Zugangscode eingeben **und** eine Codierkarte (Karte oder Codierschlüssel) verwenden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Dual Authentication Duration (Bedienteile > Bedienteilzuweisungen > Dauer der zweifachen Authentifizierung)

6.1.13 Trouble Tone (Störungston)

Standardeinstellung: Nein
Auswahl:
– Ja: An diesem Bedienteil werden zentralenweite Störungstöne und visuelle Anzeigen wiedergegeben.
– Nein: Es werden keine zentralenweiten Störungstöne wiedergegeben. Anzeigen erfolgen jedoch weiterhin.

Zentralenweite Störungstöne umfassen Netzstrom, SDI-Bus und SDI2-Bus. Sie umfassen keine Melderstörungen oder „Summeralarm bei Fehler“.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Trouble Tone (Bedienteile > Bedienteilzuweisungen > Störungston)

6.1.14 Entry Tone (Eingangston)

Standardeinstellung: Yes
Auswahl:
– Ja: An diesem Bedienteil ertönt der Eingangston während der Eingangsverzögerung.
– Nein: An diesem Bedienteil wird kein Eingangston wiedergegeben.

Wird im Bereich des Bedienteils eine Störung an einem Melder mit Verzögerung ausgelöst, setzt die Eingangsverzögerung ein.
Setzen Sie den Parameter > Melder > Melderprofil > *Eingangston aus, Seite 238* auf „Ja“, um den Eingangston an einem bestimmten Melder zu unterdrücken.
Stellen Sie diesen Parameter bei UL-Installationen auf „Ja”.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Entry Tone (Bedienteile > Bedienteilzuweisungen > Eingangston)

6.1.15 Exit Tone (Scharfschaltungston)

Standardeinstellung: „Ja“
Auswahl:
– Ja: An diesem Bedienteil wird der Eingangston während der Scharfschalteverzögerung aktiviert.
– Nein: An diesem Bedienteil wird kein Scharfschaltungston wiedergegeben.

Die Scharfschaltung über ein Bedienteil, das über einen für die Bereichsscharfschaltung erforderlichen Bereich verfügt, führt zum Einsetzen der Scharfschalteverzögerung.
Zum Unterdrücken des Scharfschaltungstons in einem bestimmten Bereich setzen Sie den Parameter „Exit Tone” (Scharfschaltungston) unter „Area Wide Parameters > Exit Tone” (Bereichsübergreifende Parameter > Scharfschaltungston) auf „Nein”.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Exit Tone (Bedienteile > Bedienteilzuweisungen > Scharfschaltungston)

6.1.16 Arm Area Warning Tone (Warnton Bereichsscharfschaltung)

Standardeinstellung: Yes
Auswahl:
– Ja: Zu Beginn eines Schließen-Fensters werden am Bedienteil ein Signalton ausgegeben und ein Warnhinweis eingeblendet.
– Nein: An diesem Bedienteil werden kein Signalton wiedergegeben und kein Warnhinweis angezeigt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Arm Area Warning Tone (Bedienteile > Bedienteilzuweisungen > Warnton Bereichsscharfschaltung)

6.1.17 Idle Scroll Lock (Bildlauf gesperrt, wenn inaktiv)

Standardeinstellung: Nein
Auswahl:
– Ja: Ist dieses Bedienteil inaktiv, werden Textanzeigen für stummgeschaltete Alarm- oder Störungsereignisse nicht automatisch gescrollt.
– Nein: automatisches Scrollen von Text zulassen

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Idle Scroll Lock (Bedienteile > Bedienteilzuweisungen > Bildlauf gesperrt, wenn inaktiv)

6.1.18 Function Lock (Funktionssperre)

Standardeinstellung: Nein
Auswahl:
– Ja: Nach dem Drücken der Taste „Abschalten”, „Menu” (Menü) oder „Shortcuts” (Verknüpfungen) ist zum Fortfahren die Eingabe eines Zugangscodes erforderlich.
– Nein: Zum Fortfahren ist kein Zugangscode erforderlich.

Ist dieser Parameter auf „Ja“ eingestellt, werden Benutzer nach dem Drücken der Taste „Abschalten”, „Menu” (Menü) oder „Shortcuts” (Verknüpfungen) dazu aufgefordert, einen Zugangscode einzugeben. Die in der Funktionsliste dieses Bedienteils parametrierten Elemente werden nach Benutzerrechten gefiltert. In der Funktionsliste werden nur die Elemente angezeigt, auf die der Benutzer gemäß Berechtigungen zugreifen kann.
Ist die Einstellung „Nein” ausgewählt, werden nach dem Drücken der Tasten „Abschalten”, „Menu” (Menü) oder „Shortcuts” (Verknüpfungen) alle Elemente, die in der Menüliste für die Bedienteiladresse parametriert wurden, angezeigt – unabhängig von den Benutzerrechten des Benutzers.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Function Lock (Bedienteile > Bedienteilzuweisungen >Funktionssperre)

6.1.19 Abort Display (Abbruch anzeigen)

Standardeinstellung: „Ja“
Auswahl:
- Ja: An diesem Bedienteil erscheint „ALARM NOT SENT”(ALARM NICHT GESENDET), wenn ein Einbruchalarm vor dem Senden eines Alarmprotokolls abgebrochen wird.
- Nein: an diesem Bedienteil wird „ALARM NOT SENT” (ALARM NICHT GESENDET) nicht angezeigt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Abort Display (Bedienteile > Bedienteilzuweisungen > Abbruch anzeigen)

6.1.20 Cancel Display (Abgebrochen anzeigen)

Standardeinstellung: „Ja“
Auswahl:
- Ja: An diesem Bedienteil wird bei Abbruch eines Einbruchalarms „CANCELLED ALARM” (ALARM ABGEBROCHEN) angezeigt.
- Nein: Die Meldung „CANCELLED ALARM” (ALARM ABGEBROCHEN) wird an diesem Bedienteil nicht angezeigt.

Wird dieser Parameter auf „Ja“ gesetzt, muss der Parameter *Abbruchsprotokoll, Seite 105* unter „Panel Wide Parameters > Miscellaneous > Cancel Reports” (Zentralenübergreifende Parameter > Sonstige > Abbruchprotokolle) ebenfalls auf „Ja” festgelegt sein.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Cancel Display (Bedienteile > Bedienteilzuweisungen > Abbrechen anzeigen)

6.1.21 Nightlight Enable (Nachtlicht aktivieren)

Standardeinstellung: Nein
Auswahl:
- Ja: Ist das Bedienteil inaktiv, werden die Hintergrundbeleuchtung des Bedienteildisplays und des Schlüssels auf der Mindeststufe betrieben.
- Nein: Bei Inaktivität des Bedienteils sind die Hintergrundbeleuchtung des Bedienteildisplayss und des Schlüssels ausgeschaltet.

Wenn dieser Parameter auf „Ja“ gesetzt ist, kann die Nachtlicht-Funktion am Bedienteil ein- oder ausgeschaltet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Nightlight Enable (Bedienteile > Bedienteilzuweisungen > Nachtlicht aktivieren)

6.1.22 Nightlight Brightness (Nachtlichthelligkeit)

Standardeinstellung: 2
Auswahl:
– 0: Nachtlicht aus
– 1 bis 6: je höher die Zahl, desto heller das Nachtlicht
Mit diesem Parameter wird der Helligkeitsgrad für die Bedienteilfunktion „Nightlight” (Nachtlicht) festgelegt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Nightlight Brightness (Bedienteile > Bedienteilzuweisungen > Nachtlichthelligkeit)

6.1.23 Silence Keypress Tone (Tastenton stummschalten)

Standardeinstellung: Nein
Auswahl:
– Ja: Das Drücken von Tasten auf dem Bedienteil erfolgt geräuschlos.
– Nein: Beim Drücken einer Bedienteiltaste wird ein Tastenton ausgegeben.
Wird dieser Parameter auf „Nein” gesetzt, kann der Tastenton nicht ausgeschaltet werden.
Wird die Einstellung „Nein” gewählt, kann der Tastenton nicht eingeschaltet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Silence Keypress Tone (Bedienteile > Bedienteilzuweisungen > Tastenton stummschalten)

6.1.24 Show Date and Time (Datum und Uhrzeit anzeigen)

Standardeinstellung: Nein
Auswahl:
– Ja: Datum und Uhrzeit werden am Bedienteil angezeigt.
– Nein: Datum und Uhrzeit werden am Bedienteil nicht angezeigt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Show Date and Time (Bedienteile > Bedienteilzuweisungen > Datum und Uhrzeit anzeigen)

6.1.25 Keypad Volume (Bedienteillautstärke)

Standardeinstellung: 7
Auswahl: 0 bis 7
Der Wert „0” steht für die niedrigste Lautstärke.
„7” signalisiert die höchste Lautstärke.
Signaltöne mit hoher Priorität (z. B. ein Alarmton) werden stets mit maximaler Lautstärke wiedergegeben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Keypad Volume (Bedienteile > Bedienteilzuweisungen > Bedienteillautstärke)

6.1.26 Keypad Brightness (Bedienteilhelligkeit)

Standardeinstellung: 6
Auswahl: 0 bis 6
0: Dieser Wert signalisiert die dunkelste Einstellung des Bedienteildisplays.

6: Steht für die hellste Einstellung des Bedienteildisplays.
Die Helligkeit des Bedienteildisplays kann am Bedienteil eingestellt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Keypad Brightness (Bedienteile > Bedienteilzuweisungen > Bedienteilhelligkeit)

6.1.27 Disable Presence Sensor (Anwesenheitsmelder deaktivieren)

Standardeinstellung: Nein
Auswahl:
– Ja: Anwesenheitsmelder deaktivieren
– Nein: Erkennt der Melder Bewegungen im Bereich des Bedienteils, werden gedimmte Displays heller geschaltet.

Nur B94x Touchscreen-Bedienteile verfügen über Anwesenheitsmelder.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Disable Presence Sensor (Bedienteile > Bedienteilzuweisungen > Anwesenheitsmelder deaktivieren)

6.1.28 Disable Token Reader (Codierschlüssel-Leser deaktivieren)

Standardeinstellung: „Ja“

Auswahl:
– Ja: Codierschlüssel-Leser deaktivieren
– Nein: Codierschlüssel-Leser aktivieren

Codierschlüssel-Leser steht nur für B94x Touchscreen-Bedienteile zur Verfügung.
Durch Deaktivierung des Codierschlüssel-Lesers wird der Stromverbrauch reduziert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Disable Token Reader (Bedienteile > Bedienteilzuweisungen > Codierschlüssel-Leser deaktivieren)

6.1.29 Enable Tamper Switch (Sabotagekontakt aktivieren)

Standardeinstellung: Nein
Auswahl:
– Ja: Sabotagekontakt aktivieren
– Nein: Sabotagekontakt deaktivieren

Dieser Parameter gilt nur für SDI-Bedienteile und das Bedienteil B915.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Enable Tamper Switch (Bedienteile > Bedienteilzuweisungen > Sabotagekontakt aktivieren)

6.1.30 Feature Button Option (Option Funktionsschaltfläche)

Standardeinstellung: Sprachauswahl
Auswahl:
– Sprachauswahl: Durch das Drücken dieser Taste wechseln Benutzer zwischen der ersten und zweiten Sprache der Zentrale.
– Aktuelle Ereignisse: Durch Klicken dieser Taste können Benutzer schnell aktuelle Ereignisse anzeigen.

Über diesen Parameter wird die Funktionstaste in der oberen linken Ecke des B94x Touchscreen-Bedienteils konfiguriert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > SDI2 Keypad Assignments > Feature Button Option (Bedienteile > Zuweisungen des SDI2-Bedienteils > Option Funktionsschaltfläche)

6.1.31 Überwachung

Standardeinstellung: Yes
Auswahl:
– Ja: diese Bedienteiladresse überwachen Nur ein SDI-Bedienteil ist auf diese Adresse eingestellt.
– Nein: diese Bedienteiladresse nicht überwachen Auf diese Adresse können mehrere SDI-Bedienteile eingestellt werden.

Dieser Parameter gilt nur für SDI-Bedienteile. SDI2-Bedienteile werden immer überwacht.
Der Parameter *Keypad Type (Bedienteiltyp), Seite 144* muss auf ein SDI-Bedienteil festgelegt werden.
Wenn dieser Parameter auf „Ja” festgelegt wird und ein Problem mit dem Bedienteil oder dem SDI-Bus auftritt, erstellt die Zentrale ein „TROUBLE SDI ##”-Ereignis (STÖRUNG SDI ##).
SDI D125xRB Brandmelderbedienteile werden auch überwacht, wenn dieser Parameter auf „Nein” gesetzt ist.
Liegen mehrere SDI-Bedienteilen mit der gleichen Adresseneinstellung vor, werden der gleiche Text und die gleichen Töne wiedergegeben, wenn an einem der Bedienteile eine Taste gedrückt wird.
SDI-Störungsereignisse werden immer für Bereich 1, Konto 1 erstellt – unabhängig davon, welchem Bereich das SDI-Gerät zugewiesen ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Supervision (Bedienteile > Bedienteilzuweisungen >Überwachung)

6.1.32 Passcode [Esc] Option (Option „Zugangscode [Esc]”)

Standardeinstellung:
– „Nein” für Bedienteil 1 (SDI2-Bedienteil), „Ja” für alle anderen Bedienteile.

Auswahl:
– Ja: Durch Eingabe eines Zugangscodes und anschließendes Drücken der Escape-Taste werden aktive Alarme stummgeschaltet. Bei bestätigten Alarmen führen die Eingabe des Zugangscodes und das Drücken der Escape-Taste dazu, dass die Anzeige gelöscht wird.
– Nein: Durch Eingabe eines Zugangscodes und anschließendes Drücken der Escape-Taste wird die letzte Stelle des Zugangscodes gelöscht. Durch längeres Drücken der Escape-Taste wird eine Stelle nach der anderen gelöscht. Sind keine Stellen mehr übrig, wird der Vorgang beendet.

Hinweis!
ZENTRALENÜBERGREIFENDE PARAMETER > Sonstige > Benutzercodelänge muss auf „Deaktiviert” eingestellt sein
Wenn der Parameter „PANEL WIDE PARAMETERS > Miscellaneous > Passcode Length” (ZENTRALENÜBERGREIFENDE PARAMETER > Sonstige > Benutzercodelänge) auf „3 Stellen”, „4 Stellen”, „5 Stellen” oder „6 Stellen” eingestellt ist, wird die Option „Passcode [Esc]” (Zugangscode [Esc]) deaktiviert – auch wenn sie auf „Ja” gesetzt ist.
Ist die Option „Pincode [Esc]” (Zugangscode [Esc]) auf „Ja“ gesetzt, muss der Parameter „Benutzercodelänge” unter „PANEL WIDE PARAMETERS > Miscellaneous > Passcode Length” (ZENTRALENÜBERGREIFENDE PARAMETER > Sonstige > Benutzercodelänge) auf „Deaktiviert” gesetzt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Keypad Assignments > Passcode [Esc] Option (Bedienteile > Bedienteilzuweisungen > Option „Zugangscode [Esc]”)

6.2 Global Keypad Settings (Globale Bedienteileinstellungen)

6.2.1 A-key Response (Funktion A-Taste)

Standardeinstellung: keine Funktion

Auswahl:

- Keine Reaktion: Ton beim Drücken einer ungültigen Taste
- Manueller Feueralarm: erstellt ein Feueralarm-Ereignis, wenn der Benutzer die A-Taste und die 1-Taste gleichzeitig 2 Sekunden lang gedrückt hält oder CMD und 7 (Befehl 7) drückt.
- Benutzerdefinierte Funktion: Führt die ausgewählte benutzerdefinierte Funktion aus, wenn Benutzer die A-Taste 2 Sekunden lang gedrückt halten. Verwenden Sie den Parameter der benutzerdefinierten Funktion für die A-Taste, um die benutzerdefinierte Funktion auszuwählen.
  Die Auswahl „Custom Function” (Benutzerdefinierte Funktion) gilt nicht für B942 Touchscreen-Bedienteile.

Wenn dieser Parameter auf „Manual Fire Alarm“ (Manueller Feueralarm) gesetzt ist, erfolgt jedes Mal ein Alarmereignis, wenn der Benutzer die entsprechenden Tasten drückt – unabhängig davon, ob vorherige Alarme vom Display gelöscht wurden.

Hinweis!
Enthält „Manual Fire Alarm ”(Manueller Feueralarm) CMD und 7, setzen Sie den Parameter „Authority Level/User Command 7” (Benutzerrechte > Benutzerbefehl 7) auf „E“.
Das Festlegen von „A-key Response” (Funktion A-Taste) auf „Manual Fire Alarm” (Manueller Feueralarm) führt auch dazu, dass CMD und 7 (Befehl 7) für manuellen Feueralarm konfiguriert wird. CMD und 7 werden gedrückt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Global Keypad Settings > A-key Response (Bedienteile > Globale Bedienteileinstellungen > Funktion A-Taste)

Siehe

- *RPS Menu Location (Melde-Adresse des Menüs „RPS“), Seite 237*

6.2.2 A-key Custom Function (Benutzerdefinierte Funktion A-Taste)

Standardeinstellung: Deaktiviert

Auswahl:

- B5512: Deaktiviert, Funktion 128 bis Funktion 131
- B4512: Deaktiviert, Funktion 128, Funktion 129
- B3512: Deaktiviert, Funktion 128

Wählen Sie die benutzerdefinierte Funktion aus, die ausgeführt wird, wenn Benutzer die A-Taste 2 Sekunden lang gedrückt halten.
Der Parameter für die Funktion der A-Taste muss auf „Custom Function“ (Benutzerdefinierte Funktion) eingestellt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Keypads > Global Keypad Settings > A-key Custom Function (Bedienteile > Globale Bedienteileinstellungen > Benutzerdefinierte Funktion A-Taste)

6.2.3 B-key Response (Funktion B-Taste)

Standardeinstellung: keine Funktion

Auswahl:

- Keine Reaktion: Ton beim Drücken einer ungültigen Taste
- Manueller medizinischer Alarm, keine Alarmausgabe: erstellt ein Ereignis aufgrund eines medizinischen Ereignisses, wenn Benutzer die B-Taste und die 4-Taste gleichzeitig 2 Sekunden lang halten. Die Alarmausgabe ist **nicht** für das Ereignis aufgrund eines medizinischen Alarms aktiviert.
- Manueller medizinischer Alarm, mit Alarmausgabe: erstellt ein Ereignis aufgrund eines medizinischen Ereignisses, wenn Benutzer die B-Taste und die 4-Taste gleichzeitig 2 Sekunden lang halten. Die Alarmausgabe ist für das Ereignis aufgrund eines medizinischen Alarms aktiviert.
- Benutzerdefinierte Funktion: führt die ausgewählte benutzerdefinierte Funktion aus, wenn Benutzer die B-Taste 2 Sekunden lang gedrückt halten. Verwenden Sie den Parameter der benutzerdefinierten Funktion für die B-Taste, um die benutzerdefinierte Funktion auszuwählen.
  Die Auswahl „Custom Function" (Benutzerdefinierte Funktion) gilt nicht für B942 Touchscreen-Bedienteile.

Wenn dieser Parameter auf „Manual Medical Alarm, no alarm output" (Manueller medizinischer Alarm, keine Alarmausgabe) oder „Manual Medical Alarm, with output" (Manueller medizinischer Alarm, mit Alarmausgabe) gesetzt ist, erfolgt jedes Mal ein Alarmereignis, wenn der Benutzer die entsprechenden Tasten drückt, unabhängig davon, ob vorherige Alarme vom Display gelöscht wurden.

RPS Menu Location (Melde-Adresse des Menüs „RPS")

Bedienteile > Globale Bedienteileinstellungen > Funktion B-Taste

6.2.4 Benutzerdefinierte Funktion B-Taste

Standardeinstellung: Deaktiviert

Auswahl:

- B5512: Deaktiviert, Funktion 128 bis Funktion 131
- B4512: Deaktiviert, Funktion 128, Funktion 129
- B3512: Deaktiviert, Funktion 128

Wählen Sie die benutzerdefinierte Funktion aus, die ausgeführt wird, wenn Benutzer die B-Taste 2 Sekunden lang gedrückt halten.

Der Parameter für die Funktion der B-Taste muss auf „Custom Function" (Benutzerdefinierte Funktion) festgelegt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS")

Bedienteile > Globale Bedienteileinstellungen > Benutzerdefinierte Funktion B-Taste

6.2.5 Funktion C-Taste

Standardeinstellung: keine Funktion

Auswahl:

- Keine Reaktion: Ton beim Drücken einer ungültigen Taste
- Manueller Notrufalarm, unsichtbare und stille Alarmausgabe: erstellt ein Notrufalarm-Ereignis, wenn Benutzer die C-Taste und die 7-Taste gleichzeitig 2 Sekunden lang gedrückt halten oder Benutzer CMD und 9 (Befehl 9) drücken.
  Das Ereignis wird in der Bedienteilanzeige **nicht** angezeigt. Die **stille** Alarmausgabe wird aktiviert.

– Manueller Notrufalarm, sichtbar mit Alarmausgabe: erstellt ein Notrufalarm-Ereignis, wenn Benutzer die C-Taste und die 7-Taste gleichzeitig 2 Sekunden lang gedrückt halten oder Benutzer CMD und 9 (Befehl 9) drücken.
  Das Ereignis wird in der Bedienteilanzeige angezeigt. Die Alarmausgabe wird aktiviert.
– Benutzerdefinierte Funktion: führt die ausgewählte benutzerdefinierte Funktion aus, wenn Benutzer die C-Taste 2 Sekunden lang gedrückt halten. Verwenden Sie den Parameter der benutzerdefinierten Funktion für die C-Taste, um die benutzerdefinierte Funktion auszuwählen.
  Die Auswahl „Custom Function" (Benutzerdefinierte Funktion) gilt nicht für B942 Touchscreen-Bedienteile.

Wenn dieser Parameter auf „Manual Panic Alarm, invisible and silent alarm output" (Manueller Notrufalarm, unsichtbare und stille Alarmausgabe) oder „Manual Panic Alarm, visible with alarm output" (Manueller Notrufalarm, sichtbar mit Alarmausgabe) gesetzt ist, erfolgt jedes Mal ein Alarmereignis, wenn der Benutzer die entsprechenden Tasten drückt, unabhängig davon, ob vorherige Alarme vom Display gelöscht wurden.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Bedienteile > Globale Bedienteileinstellungen > Funktion C-Taste

6.2.6 Benutzerdefinierte Funktion C-Taste

Standardeinstellung: Deaktiviert
Auswahl:
– B5512: Deaktiviert, Funktion 128 bis Funktion 131
– B4512: Deaktiviert, Funktion 128, Funktion 129
– B3512: Deaktiviert, Funktion 128

Wählen Sie die benutzerdefinierte Funktion aus, die ausgeführt wird, wenn Benutzer die C-Taste 2 Sekunden lang gedrückt halten.
Der Parameter für die Funktion der C-Taste muss auf „Custom Function" (Benutzerdefinierte Funktion) festgelegt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Bedienteile > Globale Bedienteileinstellungen > Benutzerdefinierte Funktion C-Taste

6.2.7 Manueller stiller Alarm hörbar bei Kommunikationsstörung

Standardeinstellung: Nein
Auswahl:
– Ja: der Alarm-Signalgeber wird aktiviert, wenn ein stilles Alarmprotokoll das Bedienteil nach zwei Versuchen nicht erreicht.
– Nein: der Alarm-Signalgeber wird **nicht** aktiviert, wenn ein stilles Alarmprotokoll das Bedienteil nicht erreicht.

Dieser Parameter wird angewendet, wenn die C-Taste eines Bedienteils oder ein RADION keyfob-Notruf ein stilles Alarmereignis erstellt.
Die Ausgabe des Alarmsignalgebers wird, wenn auf „Yes" (Ja) eingestellt, für die Zeit des Einbruchsignals abzüglich der Zeit für die zwei Versuche zum Senden des stillen Alarmprotokolls aktiviert. Die Schaltuhr für das Einbruchsignal wird gestartet, wenn das stille Alarmereignis erstellt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Bedienteile > Globale Bedienteileinstellungen > Manueller stiller Alarm hörbar bei Kommunikationsstörung

6.2.8 Kartentyp

Standardeinstellung:: 26 Bit

Auswahl:
26 Bit
37 Bit

Standortcode, Seite 178 **für Kartentypen**
26 Bit: Standardstandortcode ist 255.
37 Bit, kein Standortcode: Standardstandortcode ist leer. Der Standortcode ist nicht konfigurierbar (Standortcode-Parameter ist ausgegraut).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Bedienteile > Globale Bedienteileinstellungen > Kartentyp

6.2.9 Optionen für Übertragungsstörung

Standardeinstellung:: Übertragungsstörungen sind hörbar und sichtbar
Auswahl:
- Übertragungsstörungen sind still und unsichtbar: Übertragungsstörungsereignisse werden auf Bedienteilen angezeigt, und der Störungston erklingt.
- Übertragungsstörungen sind hörbar und sichtbar: Übertragungsstörungsereignisse werden nicht auf Bedienteilen angezeigt. Der Störungston erklingt nicht.

Hinweis!
Störungston für jedes Bedienteil aktivieren
Verwenden Sie den Parameter *Trouble Tone (Störungston), Seite 149* (Störungston) in den Bedienteilzuweisungen, um Störungstöne zentralenweit (einschließlich Übertragungsstörung) für die einzelnen Bedienteile zu aktivieren. Die Standardeinstellung für alle Bedienteiladressen für den Parameter „Trouble Tone“ (Störungston) ist „No“ (Nein) (zentralenweite Störungen werden nicht ausgegeben).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Bedienteile > Globale Bedienteileinstellungen > Sound-Optionen für Übertragungsstörungen

6.3 Globaler Funk-Handsender

6.3.1 Funk-Handsender Funktion A benutzerdefinierte Funktion

Standardeinstellung: Deaktiviert
Auswahl:
- B5512: Deaktiviert, Funktion 128 bis Funktion 131
- B4512: Deaktiviert, Funktion 128, Funktion 129
- B3512: Deaktiviert, Funktion 128

Wählen Sie die benutzerdefinierte Funktion aus, die ausgeführt wird, wenn Benutzer die Taste der Funktion A auf den RADION keyfobs drücken.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Bedienteile > Globaler Funk-Handsender > Funk-Handsender Funktion A benutzerdefinierte Funktion

6.3.2 Funk-Handsender Funktion B benutzerdefinierte Funktion

Standardeinstellung: Deaktiviert
Auswahl:
- B5512: Deaktiviert, Funktion 128 bis Funktion 131
- B4512: Deaktiviert, Funktion 128, Funktion 129
- B3512: Deaktiviert, Funktion 128

Wählen Sie die benutzerdefinierte Funktion aus, die ausgeführt wird, wenn Benutzer die Taste der Funktion B auf den RADION keyfobs drücken.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Bedienteile > Globaler Funk-Handsender > Funk-Handsender Funktion B benutzerdefinierte Funktion

6.3.3 Notrufoptionen für Funk-Handsender

Standardeinstellung:: Notrufreaktion deaktiviert
Auswahl:

- Notrufreaktion deaktiviert: die Zentrale ignoriert das Drücken des Überfalltasters von allen Funk-Handsendern.
- Hörbare Notrufreaktion aktiviert: Wenn Benutzer einen Überfalltaster auf einem Funk-Handsender drücken, erstellt die Zentrale ein Notrufalarm-Ereignis für den Funk-Handsender, zeigt den Alarm an, lässt den Alarmton auf Bedienteilen ertönen und aktiviert so die Alarmsignal-Ausgabe.
- Stille Notrufreaktion aktiviert: Wenn Benutzer einen Überfalltaster auf einem Funk-Handsender drücken, erstellt die Zentrale ein stilles Alarmereignis für einen Funk-Handsender und aktiviert den Bedrohungsausgang. Bedienteile bleiben still und zeigen den Alarm nicht an.

Wenn der Ausgang des Alarm-Signalgebers aktiv ist, wird durch Stummschalten des Alarms ein Abbruchereignis erstellt.
Wenn der Bedrohungsausgang aktiv ist, wird durch Bestätigen des Alarms ein Abbruchereignis erstellt.
Die Funktion „Alarm Abort“ (Alarmabbruch) trifft nicht zu für Notrufalarm- oder stille Alarmereignisse auf Funk-Handsendern.
Die Zentrale erstellt keine Wiederherstellungsereignisse für Notrufalarm- oder stille Alarmereignisse auf Funk-Handsendern.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Bedienteile > Funk-Handsender > Notrufoptionen für Funk-Handsender

7 Benutzerdefinierte Funktionen

Verwenden Sie die Parameter in diesem Abschnitt, um benutzerdefinierte Funktionen zu konfigurieren.
B5512 unterstützt 4 benutzerdefinierte Funktionen.
B4512 unterstützt 2 benutzerdefinierte Funktionen.
B3512 unterstützt 1 benutzerdefinierte Funktion.

7.1 Text der benutzerdefinierten Funktion (erste Sprache)

Standardeinstellung:: Funktion ###
Auswahl: Bis zu 18 Zeichen (Text, Zahlen, Leerzeichen und Symbole).
Geben Sie Text ein, um die benutzerdefinierte Funktion an Bedienteilen zu kennzeichnen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerdefinierte Funktion > Text der benutzerdefinierten Funktion

7.2 Text der benutzerdefinierten Funktion (zweite Sprache)

Standardeinstellung: (leer)
Auswahl: Bis zu 18 Zeichen (Text, Zahlen, Leerzeichen und Symbole).
Geben Sie Text ein, um die benutzerdefinierte Funktion an Bedienteilen zu kennzeichnen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerdefinierte Funktion > Text der benutzerdefinierten Funktion (zweite Sprache)

7.3 Funktionen

Standardeinstellung: nicht in Verwendung
Nicht in Verwendung: Diese Funktion ist deaktiviert und keine Funktionen nach dieser werden ausgeführt.
All On Delay (Verzögerte Vollscharfschaltung), Seite 269
All On Instant (Unverzögerte Vollscharfschaltung), Seite 269
Verzögerte Außenhautüberwachung, Seite 269
Unverzögerte Außenhautüberwachung, Seite 269
Unscharfschalten, Seite 270
Extend Close (Schließen verlängern), Seite 270
Bypass a Point (Einen Melder übergehen), Seite 270
Unbypass a Point (Einen Melder einschalten), Seite 270
Unbypass All Points (Alle Melder einschalten), Seite 270
Reset Sensors (Melder zurücksetzen), Seite 270
Ausgang einschalten, Seite 270
Ausgang ausschalten, Seite 271
Ausgang umschalten, Seite 271
Monostabiler Ausgang, Seite 271
Alle Ausgänge zurücksetzen, Seite 271
Verzögerung, Seite 271
RPS antworten, Seite 271
RPS kontaktieren, Seite 271
RPS kontaktieren – Benutzerport, Seite 272
Send Status Report (Zustandsmeldungen senden), Seite 272
Send Test Report (Prüfprotokolle senden), Seite 272
Prüfprotokoll bei nicht-normalem Zustand senden, Seite 274
Go to Area (Gehe zu Bereich), Seite 274

Überwachung einschalten, Seite 274
Überwachung ausschalten, Seite 274
Datum und Uhrzeit anzeigen, Seite 274
Überwachungston ausgeben, Seite 274
Bedienteillautstärke festlegen, Seite 275
Bedienteilhelligkeit festlegen, Seite 275
Störung stummschalten, Seite 275
Alarm stummschalten, Seite 275

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerdefinierte Funktion > Funktion 1-6

8 Kontextmenü

8.1 Funktion

Standardeinstellung:
- Kontextmenüelement 1: All On Selected Area (Vollscharfschaltung ausgewählter Bereich)
- Kontextmenüelement 2: Off Select Area (Ausgeschaltet im ausgewählten Bereich)
- Kontextmenüelement 3: View Point Status (Melderstatus anzeigen)
- Kontextmenüelement 4: Reset Sensors (Melder zurücksetzen)
- Kontextmenüelement 5: Change Watch Mode (Überwachungsmodus ändern)
- Kontextmenüelement 6: Brightness (SDI2) / Dim (SDI) (Helligkeit (SDI2)/Dunkel (SDI))
- Kontextmenüelement 7: Volume (SDI2) / Dim (SDI) (Lautstärke (SDI2)/Dunkel (SDI))
- Kontextmenüelement 8: View Log (Protokoll anzeigen)
- Kontextmenüelement 9-32: Disabled Item (Element deaktiviert)

Auswahl: Siehe Tabelle unten.

Verwenden Sie diesen Parameter, um Menüelementen Funktionen zuzuweisen.

Wählen Sie die Funktion in der Dropdown-Liste im Dialogfeld aus, das erscheint, wenn Sie doppelt auf eine Zelle in der Spalte „Function“ (Funktion) und neben der Funktion im Abschnitt „User Configuration“ (Benutzerkonfiguration) klicken.

Alle unterstützten benutzerdefinierten Funktionen sind nach ihrem konfigurierten *Text der benutzerdefinierten Funktion (erste Sprache), Seite 160* aufgelistet.

Es besteht keine Einschränkung, wie oft Sie dem Menü eine bestimmte Funktion zuweisen können. Dadurch können Sie dieselbe Funktion an verschiedenen Bedienteilen zuweisen, damit sie in einigen Bereichen in einer anderen Reihenfolge als in anderen angezeigt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Kontextmenü > Funktion

Nicht in Verwendung: Diese Funktion ist deaktiviert und keine Funktionen nach dieser werden ausgeführt.

All On Delay (Verzögerte Vollscharfschaltung), Seite 269
All On Instant (Unverzögerte Vollscharfschaltung), Seite 269
Verzögerte Außenhautüberwachung, Seite 269
Unverzögerte Außenhautüberwachung, Seite 269
Unscharfschalten, Seite 270
Extend Close (Schließen verlängern), Seite 270
Bypass a Point (Einen Melder übergehen), Seite 270
Unbypass a Point (Einen Melder einschalten), Seite 270
Unbypass All Points (Alle Melder einschalten), Seite 270
Reset Sensors (Melder zurücksetzen), Seite 270
Ausgang einschalten, Seite 270
Ausgang ausschalten, Seite 271
Ausgang umschalten, Seite 271
Monostabiler Ausgang, Seite 271
Alle Ausgänge zurücksetzen, Seite 271
Verzögerung, Seite 271
RPS antworten, Seite 271
RPS kontaktieren, Seite 271
RPS kontaktieren – Benutzerport, Seite 272
Send Status Report (Zustandsmeldungen senden), Seite 272
Send Test Report (Prüfprotokolle senden), Seite 272
Prüfprotokoll bei nicht-normalem Zustand senden, Seite 274

Go to Area (Gehe zu Bereich), Seite 274
Überwachung einschalten, Seite 274
Überwachung ausschalten, Seite 274
Datum und Uhrzeit anzeigen, Seite 274
Überwachungston ausgeben, Seite 274
Bedienteillautstärke festlegen, Seite 275
Bedienteilhelligkeit festlegen, Seite 275
Störung stummschalten, Seite 275
Alarm stummschalten, Seite 275

8.2 Set/Clear all (Alle festlegen/löschen)

Standardeinstellung:: Alle festlegen/löschen
Auswahl: Adresse 1-8
Verwenden Sie diesen Parameter, um Funktionen an allen Adressen zu aktivieren oder zu deaktivieren.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Kontextmenü > Set/Clear all (Alle festlegen/löschen)

8.3 Adresse Nr.

Standardeinstellung: Ja (Kontextmenü 1 bis 8)
Auswahl:
– Ja: in das Menü einfügen für Bedienteile, für die diese Adresse eingestellt ist.
– Keine: nicht in das Menü einfügen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Kontextmenü > Adresse Nr. (B6512: 1 bis 12, B5512, B4512: 1 bis 8, B3512: 1 bis 4)
Kontextmenü > Adresse Nr. (B9512: 1 bis 32, B8512: 1 bis 16)

9 Ausgangsparameter

Ausgänge bieten potenzialfreie (normal geöffnete/geschlossene) Ausgänge für LED-Ankündigungen und andere Anwendungen sowie feuchte Spannungsausgänge (12 VDC ein/aus) für grundlegende Alarmsystemfunktionen (wie etwa Alarmausgang, Melder zurücksetzen usw.). Die Anwendungen sind endlos, aber in erster Linie werden Ausgänge verwendet, um die Fähigkeit von Systemen zu verbessern, Ausgangsfunktionen durchzuführen.

Ausgangsarten

- Zentralenübergreifende Ausgänge: Diese Ausgänge werden verwendet, um einen Ausgang im Zusammenhang mit einer zentralenübergreifenden Anzeige bereitzustellen. Diese Ausgänge können verwendet werden, um systemübergreifende Störungen bei Stromversorgung, Telefon und eine Zusammenfassung der Alarm-, Störungs- und Überwachungsereignisse in der gesamten Zentrale anzuzeigen.
- Bereichsausgänge: Diese Ausgänge werden verwendet, um einen Ausgang nach dem Bereich bereitzustellen, dem der Ausgang zugewiesen ist. Ein Bereich kann eigene Ansagen für das Zurücksetzen von Zutrittssignal und Melder aufweisen. Ausgänge können auch verwendet werden, um den Scharfschaltungszustand des Bereichs anzuzeigen und ob nicht normale Ereignisse aufgetreten sind, wie etwa eine zwangsläufige Scharfschaltung.
- Eingebaute Ausgänge: 2 eingebaute Ausgänge mit 12 VDC Ausgangsspannung, die die Stromversorgung gewährleisten, wenn Zentrale aktiviert. Diese Ausgänge sind standardmäßig ab Werk als Ausgänge A(1), B(2) und C(3) parametriert. In der Regel wird Ausgang A(1) für das Zutrittssignal, Ausgang B(2) für einen alternativen Alarmausgang (etwa ein anderes Zutrittssignal) und Ausgang C(3) für das Zurücksetzen des Melders verwendet.
- Externe Ausgänge: Die Zentrale kann außerdem 40 potenzialfreie Form-C-Kontakt-Ausgänge für B5512 oder 24 für B4512 steuern, wenn bis zu 5 optionale B308-Module mit acht Ausgängen installiert sind. Diese Ausgänge werden für Bereichsausgang, zentralenweiten Ausgang und einzelne Melderstörungsausgänge verwendet. (B3512 unterstützt keine externen Eingänge.)

Melderpunktbezogene Ansteuerung

Ausgänge können auch so verwendet werden, dass sie aktiviert werden, wenn sich ein parametrierter Melder für den Ausgangsreaktionstyp (im Abschnitt der Melderprofile) in einem nicht normalen Status oder einem Alarmereignis befindet.

Ausgangsprotokolle

Wenn Ausgangsaktivität an den Empfänger gemeldet wird (siehe Routing), werden integrierte Ausgänge folgendermaßen protokolliert: A(1) = 253, B(2) = 254, C(3) = 255, und andere werden als 001 bis 58 gemeldet. Das Ausgangsprotokoll ist „Relay Set Output #rrrr“ (Relaissatzausgang #rrrr), wenn der Ausgang aktiviert wird und „Relay Set Output #rrrr“ (Relaissatzausgang #rrrr), wenn der Ausgang deaktiviert wird. Ausgangsprotokolle werden im Speicherprotokoll der Zentrale gespeichert.

Steuerung der Ausgänge

Wie erwähnt, können Ausgänge in Abhängigkeit von Ereignissen an der Zentrale aktiviert werden. Zudem können Ausgänge vom Benutzer anhand der Funktion [CHG OUTPUT?], zeitgesteuerter Ereignisaktivierungs-/deaktivierungsereignisse und des RPS gesteuert werden. Die folgenden Parametrierungstipps, Hinweise und Anwendungen sollten Sie vor der Parametrierung Ihrer Ausgänge durchsehen.

Hinweis!
Verwenden Sie die CHG OUTPUTS?-Funktion nicht zum Ein-/Ausschalten von Ausgängen, die für spezielle Funktionen reserviert sind. Ausgänge für spezielle Funktionen sind bereichs- und zentralenübergreifende Ausgangsfunktionen sowie Ausgänge, die KP# Entr Key Rly und dem Ausgangsreaktionstyp zugeordnet sind.

Ausgang C ist immer eingeschaltet. Durch Zuweisen eines anderen Ausgangs wird Ausgang C deaktiviert, sodass dieser Ausgang für andere Funktionen verwendet werden kann. Wenn Ausgang C zum Zurücksetzen von Meldern parametriert ist, erfolgt die Stromversorgung stets über den AUX-Anschluss der Zentrale und Ausgang C stellt einen Weg zu einer gemeinsamen Leitung bereit. Ausgang C deaktiviert die gemeinsame Verbindung während des Zurücksetzens des Melders.
Überprüfen Sie den Ausgangsstatus nach dem Umprogrammieren oder Zurücksetzen der Zentrale. Alle Ausgänge werden nach dem Zurücksetzen der Zentrale ausgeschaltet. Bestimmte Ausgangsfunktionen werden von der Zentrale jede Minute überprüft und kehren nach dem Zurücksetzen in den richtigen Zustand zurück. Andere Ausgänge müssen manuell mithilfe der Funktion „Change Output“ (Ausgang ändern) (MENU 32) in den richtigen Zustand versetzt werden.
Diese Ausgangsfunktionen stellen den richtigen Zustand innerhalb einer Minute wieder her:

Feueralarm Zusammenfassung Feuer Zusammenfassung Störung Stiller Alarm Zusammenfassung SupFire Zusammenfassung Feuer Tbl	Störung im Bereich Zusammenfassung Alarm Telefon Fehler Überwachungsmodus Alarm-Signalgeber Bereich scharfgeschaltet	Fehler bei Außenhautüberwachung Netzstromfehler Kommunikationsfehler Reset Sensors (Melder zurücksetzen) Batteriestörung Zusammenfassung SupBurg

Diese Ausgangsfunktionen müssen manuell mit der Funktion „Change Output“ (Ausgang ändern) zurückgesetzt werden:

Fehler beim Schließen Bedrohung	Zwangsläufig scharfgeschaltet Belegte Protokollkapazität in %

9.1 Bereichsübergreifende Ausgänge

9.1.1 Alarm-Signalgeber

Standardeinstellung: 1
Auswahl:
- 0 (deaktiviert), 1 bis 48 - B5512
- 0 (deaktiviert), 1 bis 28 - B4512
- 0 (deaktiviert), 1 bis 3 - B3512

Dieser Ausgang wird aktiviert, wenn ein dem Bereich zugewiesener Einbruchmelder in den Alarmzustand wechselt. Er wird auch für (Nicht-Brand-)Bedienteil und Funk-Handsender-Alarme aktiviert, die so konfiguriert sind, dass das Alarm-Signal ertönt.
Der Ausgang wird für die im Parameter *Burg Time (Einbruchalarmzeit), Seite 133* (Einbruchalarmzeit) eingegebene Zeit aktiviert. Der Ausgang hält den im Parameter *Burg Pattern (Muster für Einbruchalarm), Seite 134* (Muster für Einbruchalarm) festgelegten Rhythmus ein. Der Parameter *Stiller Alarm, Seite 169* (Stilles Zutrittssignal) muss auf „No“ (Nein) festgelegt sein, damit das Zutrittssignal bei Alarm ertönt.

Hinweis!
SIA CP-01-Anforderung
Zur Einhaltung von SIA CP-01 zur Fehlalarmunterdrückung setzen Sie diesen Parameter für jeden aktivierten Bereich auf einen anderen Wert als 0. Weitere Informationen finden Sie unter „SIA CP-01 Verification" (SIA CP-01-Verifizierung).

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Ausgangsparameter > Bereichsübergreifende Ausgänge > Alarm-Signalgeber

9.1.2 Feueralarm

Standardeinstellung: 1
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Dieser Feueralarm-Ausgang wird aktiviert, wenn ein dem Bereich zugewiesener Feuermelder in den Alarmzustand wechselt. Er wird auch für Feueralarme und Brandschutzübungen am Bedienteil aktiviert.
Der Ausgang wird für die im Parameter *Feuer und Gas – Zeit, Seite 132* (Branddauer) eingegebene Zeit aktiviert. Der Ausgang folgt dem im Parameter „Fire Pattern" (Brandmuster) eingestellten Rhythmus.

Hinweis!
UL 864-Anforderung
Zur Einhaltung der UL 864-Anforderungen für Brandmeldesysteme parametrieren Sie diesen Parameter mit einem Relais.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Ausgangsparameter > Bereichsübergreifende Ausgänge > Feueralarm

9.1.3 Reset Sensors (Melder zurücksetzen)

Standardeinstellung: 3 (OUTPUT C)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der hier eingegebene Ausgang wird beim Start der Benutzerfunktion „Reset Sensors" (Melder zurücksetzen) oder während eines Brand-Funktionstest fünf Sekunden lang aktiviert.
Wenn Sie „Reset Sensors" (Melder zurücksetzen) für mindestens zwei Bereiche einen Ausgang zuweisen, müssen Sie die Parameter unten festlegen. Wird dies nicht beachtet, kann ein Störungsereignis für Melder vom Typ *Rücksetzbar, Seite 247* (Rücksetzbar) ausgelöst werden.
– Der *Scope (Bereich), Seite 145* (Umfang) des Bedienteils muss alle Bereiche umfassen, die Ausgang gemeinsam verwenden.
– Benutzer müssen die Berechtigung für *Melder zurücksetzen, Seite 202* (Melder zurücksetzen) in allen Bereichen besitzen, die den Ausgang gemeinsam verwenden.
– *Neustartzeit, Seite 127* (Neustartzeit) muss für alle Bereiche, die den Ausgang gemeinsam verwenden, auf dieselbe Anzahl an Sekunden festgelegt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS")
Ausgangsparameter > Bereichsübergreifende Ausgänge > Melder zurücksetzen

9.1.4 Fehler beim Schließen/Außenhautüberwachung scharfgeschaltet

Standardeinstellung: 0 (deaktiviert).

Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Wenn der Parameter „Part On Output“ (Ausgang Außenhautüberwachung) auf „No“ (Nein) gesetzt ist, wird dieser Ausgang vom Typ „Fail to Close / Part On Armed“ (Fehler beim Schließen/Außenhautüberwachung scharfgeschaltet) aktiviert, wenn das Schließen-Fenster für den Bereich abläuft. Er bleibt bis Mitternacht aktiviert, bis ein anderes Schließen-Fenster gestartet oder die Zentrale zurückgesetzt wird.
Wenn der Parameter „Part On Output“ (Ausgang Außenhautüberwachung) auf „Yes“ (Ja) gesetzt ist, wird dieser Ausgang vom Typ „Fail to Close / Part On Armed“ (Fehler beim Schließen/Außenhautüberwachung scharfgeschaltet) aktiviert, wenn für alle demselben Ausgang zugewiesenen Bereiche die unverzögerte Außenhautüberwachung oder die verzögerte Außenhautüberwachung scharfgeschaltet wird.
Siehe *Part On Output (Ausgang Außenhautüberwachung), Seite 112* (Ausgang Außenhautüberwachung).
Verwenden Sie den Parameter *Early Area Armed Output (Ausgang frühe Bereichsscharfschaltung), Seite 112* (Ausgang frühe Bereichsscharfschaltung), um auszuwählen, ob ein Ausgang mit verzögerter Außenhautüberwachung zu Beginn oder am Ende der Scharfschalteverzögerung aktiviert wird. Entsprechend der Standardeinstellung wird der Ausgang am Ende der Scharfschaltverzögerung aktiviert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Ausgangsparameter > Bereichsübergreifende Ausgänge > Fehler beim Schließen/ Außenhautüberwachung scharfgeschaltet

9.1.5 Zwangsläufig scharfgeschaltet

Standardeinstellung: 0 (deaktiviert)

Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Dieser Ausgang wird aktiviert, wenn dieser Bereich zwangsläufig scharfgeschaltet ist. Er bleibt aktiviert, bis der Bereich unscharfgeschaltet oder die Zentrale zurückgesetzt wird. Dieser Ausgang wird bei Zwangsscharfschaltung der Außenhautüberwachung nicht aktiviert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Ausgangsparameter > Bereichsübergreifende Ausgänge > Zwangsläufig scharfgeschaltet

9.1.6 Überwachungsmodus

Standardeinstellung: 0 (deaktiviert)

Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Dieser Ausgang wird aktiviert, wenn ein Überwachungsmelder gestört wird, wenn der Überwachungsmodus aktiviert wird und wenn der Bereich unscharfgeschaltet wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Ausgangsparameter > Bereichsübergreifende Ausgänge > Überwachungsmodus

9.1.7 Bereich scharfgeschaltet

Standardeinstellung: 0 (deaktiviert)

Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn der Bereich komplett scharfgeschaltet wird.
Wenn mehrere Bereiche denselben Ausgang verwenden, wird der Ausgang aktiviert, wenn alle Bereiche scharfgeschaltet sind. Er wird deaktiviert, wenn der erste Bereich unscharfgeschaltet wird.
Der Ausgang bleibt aktiviert, bis der Bereich deaktiviert (unscharfgeschaltet) wird. Der Bereich wird während der Eingangsverzögerungszeit nicht deaktiviert.
Verwenden Sie den Parameter *Early Area Armed Output (Ausgang frühe Bereichsscharfschaltung), Seite 112* (Ausgang frühe Bereichsscharfschaltung), um auszuwählen, ob ein Ausgang für die Bereichsscharfschaltung zu Beginn oder am Ende der Scharfschalteverzögerung aktiviert wird. Entsprechend der Standardeinstellung wird der Ausgang am Ende der Scharfschaltverzögerung aktiviert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Bereichsübergreifende Ausgänge > Bereich scharfgeschaltet

9.1.8 Bereich unscharfgeschaltet

Standardeinstellung: 0 (deaktiviert)

Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der hier eingegebene Ausgang wird aktiviert, wenn der Bereich von der Vollscharfschaltung (verzögert oder unverzögert) zur Außenhautüberwachung wechselt (unscharfgeschaltet).
Wenn der Bereich von der Außenhautüberwachung (ein oder aus) zur Vollscharfschaltung wechselt, wird der Ausgang deaktiviert.
Wenn derselbe Ausgang für mehrere Bereiche verwendet wird, wird dieser deaktiviert, wenn alle Bereiche komplett scharfgeschaltet sind. Wenn der erste Bereich ausgeschaltet (unscharfgeschaltet) wird oder die Außenhautüberwachung eingeschaltet wird, wird der Ausgang aktiviert.
Wenn der Parameter *Early Area Armed Output (Ausgang frühe Bereichsscharfschaltung), Seite 112* (Ausgang frühe Bereichsscharfschaltung) auf „No“ (Nein) gesetzt wird, wird dieser Ausgang vom Typ „Area Off“ (Bereich unscharfgeschaltet) erst am Ende der Scharfschalteverzögerung aktiviert. Wenn der Parameter „Early Area Armed Output“ (Ausgang frühe Bereichsscharfschaltung) auf „Yes“ (Ja) gesetzt wird, wird dieser Ausgang vom Typ „Area Off“ (Bereich unscharfgeschaltet) zu Beginn der Scharfschalteverzögerung deaktiviert und der Bereich ist komplett scharfgeschaltet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Bereichsübergreifende Ausgänge > Bereich unscharfgeschaltet

9.1.9 Störung im Bereich

Standardeinstellung: 0 (deaktiviert)

Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird bei Störung eines Melders für Außenhautüberwachung, Innenbereich oder Wegmelder Innenbereich aktiviert. Der Ausgang bleibt aktiviert, bis alle Melder im Außenbereich und im Innenbereich in diesem Bereich keine Störung mehr aufweisen.
Sie können den Ausgang „Area Fault“ (Störung im Bereich) verwenden, damit der Bereich nicht scharfschaltebereit ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Bereichsübergreifende Ausgänge > Störung im Bereich

9.1.10 Bedrohungsausgang

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn ein Benutzer ein Bedrohungsereignis an einem Bedienteil erstellt, das dem Bereich zugewiesen ist.
Der Ausgang wird für die im Parameter *Burg Time (Einbruchalarmzeit), Seite 133* (Einbruchalarmzeit) eingegebene Zeit dauerhaft aktiviert. Der Parameter *Burg Pattern (Muster für Einbruchalarm), Seite 134* (Muster für Einbruchalarm) hat keinen Einfluss auf diesen Ausgang.
Der Parameter *Duress Enable (Bedrohungsalarm aktivieren), Seite 128* (Bedrohungsalarm aktivieren) muss auf „Yes“ (Ja) gesetzt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Bereichsübergreifende Ausgänge > Bedrohungsausgang

9.1.11 Fehler bei Außenhautüberwachung

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn ein dem Bereich zugewiesener Melder zur Außenhautüberwachung eine Störung aufweist. Der Ausgang wird ungeachtet Scharfschaltungszustands des Bereichs aktiviert (Vollscharfschaltung, Außenhautüberwachung oder Unscharfschaltung).
Dieser Ausgang stellt einen durchgängigen Ausgang bereit, bis kein Melder für die Außenhautüberwachung im Bereich mehr eine Störung aufweist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Bereichsübergreifende Ausgänge > Fehler bei Außenhautüberwachung

9.1.12 Stiller Alarm

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn ein einem Melderprofil zugewiesener Melder mit auf „Yes“ (Ja) gesetztem Parameter „Silent Bell“ (Stilles Zutrittssignal) in den Alarmzustand wechselt.
Verwenden Sie diesen Ausgang für Notruf-/Überfall-Anwendungen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Bereichsübergreifende Ausgänge > Stiller Alarm

9.1.13 Gasalarm

Standardeinstellung: 1
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Dieser Gasalarm-Ausgang wird aktiviert, wenn ein dem Bereich zugewiesener Gasmelder in den Alarmzustand wechselt.
Der Ausgang wird für die im Parameter *Feuer und Gas – Zeit, Seite 132* (Branddauer) eingegebene Zeit aktiviert. Der Ausgang folgt dem im Parameter *Gas Pattern (Gasmuster), Seite 134* (Gasmuster) eingestellten Rhythmus.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Bereichsübergreifende Ausgänge > Gasalarm

9.2 Zentralenübergreifende Ausgänge

9.2.1 Netzstörung

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn die Zentrale ein Netzstromstörungsereignis erstellt. Der Ausgang wird deaktiviert, wenn die Zentrale ein Netzwiederherstellungsereignis erstellt.
Die Zentrale wartet die eingegebene Dauer im Parameter *Netzstromausfallzeit, Seite 99* (Netzstromausfallzeit), bis sie die Ereignisse für Netzstromstörung und Netzwiederherstellung erstellt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Netzstörung

9.2.2 Batteriestörung

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn die Batteriespannung unter 12,1 VDC fällt oder wenn die Batterie fehlt. Der Ausgang wird zurückgesetzt, wenn die Batteriestromversorgung wiederhergestellt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Batteriestörung

9.2.3 Telefon Fehler

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512

– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn die Zentrale ein Telefonleitungsfehlerereignis erstellt. Der Ausgang wird automatisch zurückgesetzt, wenn die Telefonleitung wiederhergestellt wird. Die Zentrale wartet die eingegebene Dauer im Parameter *Phone Supervision Time (Telefonüberwachungsdauer), Seite 54* (Telefonüberwachungsdauer), bevor sie Telefonleitungsfehlerereignisse und Telefonleitungswiederherstellungsereignisse erstellt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Ausgangsparameter > Zentralenübergreifende Ausgänge > Telefon Fehler

9.2.4 Kommunikationsfehler

Standardeinstellung: 0 (deaktiviert)

Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Bei einem Kommunikationsfehlerereignis für eine beliebige Zielgruppe wird der Ausgang aktiviert. Der Ausgang wird zurückgesetzt, wenn ein Protokoll der Zielgruppe erfolgreich an den Bedienteilempfänger gesendet wird.

Weitere Informationen über Kommunikationsfehlerereignisse finden Sie unter *Übertragungsgerät – Übersicht, Seite 86* (Übertragungsgerät).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Ausgangsparameter > Zentralenübergreifende Ausgänge > Kommunikationsfehler

9.2.5 Belegte Protokollkapazität in %

Standardeinstellung: 0 (deaktiviert)

Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn das Protokoll den Prozentsatz seiner Kapazität erreicht, der im Parameter „Log % Full“ (Belegte Protokollkapazität in %) festgelegt ist. Der Ausgang wird deaktiviert, wenn RPS den Protokollmelder zurücksetzt.

Siehe *Belegte Protokollkapazität in %, Seite 101* (Belegte Protokollkapazität in %).

Weitere Informationen

Weitere Informationen finden Sie unter *Get history (Hintergrundspeicher abrufen), Seite 32* (Hintergrundspeicher abrufen).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Ausgangsparameter > Zentralenübergreifende Ausgänge > Belegte Protokollkapazität in % (Ausgänge)

9.2.6 Zusammenfassung Feuer

Standardeinstellung: 0 (deaktiviert)

Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn alle Feuermelder im System in den Alarmzustand wechseln. Der Ausgang wird deaktiviert, wenn alle Feuermelder im System wieder in den Normalbetrieb zurückkehren, und alle Feueralarmereignisse werden von den Bedienteilanzeigen gelöscht.

Hinweis!
Dieser Ausgang „Summary Fire“ (Zusammenfassung Feuer) funktioniert nur wie beschrieben, wenn der Parameter *Feuer- und Gas-Zusammenfassung beibehalten, Seite 108* (Feuer-Zusammenfassung beibehalten) auf „No“ (Nein) gesetzt ist.

Hinweis!
Weisen Sie dem Ausgang, der dieser Funktion „Summary Fire“ (Zusammenfassung Feuer) zugewiesen ist, nicht mehr als eine Funktion zu.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Zusammenfassung Feuer

9.2.7 Zusammenfassung Alarm

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn ein beliebiger Nicht-Feuermelder in den Alarmzustand wechselt. Der Ausgang wird deaktiviert, wenn alle Nicht-Feuermelder in den Normalbetrieb zurückkehren, und alle Nicht-Feueralarme werden stummgeschaltet und die Alarmereignisse werden von den Bedienteilanzeigen gelöscht.
Dieser Ausgang wird für stille Alarme nicht aktiviert.

Hinweis!
Weisen Sie dem Ausgang, der dieser Funktion „Summary Alarm“ (Zusammenfassung Alarm) zugeordnet ist, nicht mehr als eine Funktion zu.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Zusammenfassung Alarm

9.2.8 Zusammenfassung Feuerstörung

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn alle Feuermelder im System in den Störungszustand wechseln. Der Ausgang wird deaktiviert, wenn alle Feuermelder im System wieder in den Normalbetrieb zurückkehren, und alle Feuerstörungsereignisse werden von den Bedienteilanzeigen gelöscht.

Hinweis!
Weisen Sie dem Ausgang, der dieser Zusammenfassungsfunktion zugewiesen ist, nicht mehr als eine Funktion zu.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Zusammenfassung Feuerstörung

9.2.9 Zusammenfassung Feuer-Errichterbedienung

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn jeder Feuer-Errichterbedienungsmelder im System in den Alarmzustand wechselt. Der Ausgang wird deaktiviert, wenn alle Feuer-Errichterbedienungsmelder im System wieder in den Normalbetrieb zurückkehren, und alle Feuer-Errichterbedienungsalarmereignisse werden von den Bedienteilanzeigen gelöscht.

Hinweis!
Weisen Sie dem Ausgang, der dieser Zusammenfassungsfunktion zugewiesen ist, nicht mehr als eine Funktion zu.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Zusammenfassung Feuer-Errichterbedienung

9.2.10 Zusammenfassung Störung

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn ein beliebiger Nicht-Brand-/Nicht-Gasmelder in eine Störfunktion wechselt. Der Ausgang wird deaktiviert, wenn alle Nicht-Brand-/Nicht-Gasmelder im System in den Normalbetrieb zurückkehren, und alle Nicht-Brand-/Nicht-Gasstörungsereignisse werden von den Bedienteilanzeigen gelöscht.

Hinweis!
Weisen Sie dem Ausgang, der dieser Zusammenfassungsfunktion zugewiesen ist, nicht mehr als eine Funktion zu.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Zusammenfassung Störung

9.2.11 Zusammenfassung Einbruch-Errichterbedienung

Standardeinstellung: 0 (deaktiviert)
Auswahl:
– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn ein Nicht-Brand-/Nicht-Gas-Errichterbedienungs-Melder im System in den Alarmzustand wechselt. Der Ausgang wird deaktiviert, wenn alle Nicht-Brand-/Nicht-Gas-Errichterbedienungsmelder im System in den Normalbetrieb zurückkehren, und alle Nicht-Brand-/Nicht-Gas-Errichterbedienungsalarmereignisse werden von den Bedienteilanzeigen gelöscht.

Hinweis!
Weisen Sie dem Ausgang, der dieser Zusammenfassungsfunktion zugewiesen ist, nicht mehr als eine Funktion zu.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Zusammenfassung Einbruch-Errichterbedienung

9.2.12 Ausgang für Zusammenfassung Gas

Standardeinstellung: 0 (deaktiviert)
Auswahl:
- 0 (deaktiviert), 1 bis 48 - B5512
- 0 (deaktiviert), 1 bis 28 - B4512
- 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn alle Gasmelder im System in den Alarmzustand wechseln. Der Ausgang wird deaktiviert, wenn alle Gasmelder im System wieder in den Normalbetrieb zurückkehren, und alle Gasalarmereignisse werden von den Bedienteilanzeigen gelöscht.

Hinweis!
Weisen Sie dem Ausgang, der dieser Zusammenfassungsfunktion zugewiesen ist, nicht mehr als eine Funktion zu.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Ausgang für Zusammenfassung Gas

9.2.13 Errichterbedienungsausgang für Zusammenfassung Gas

Standardeinstellung: 0 (deaktiviert)
Auswahl:
- 0 (deaktiviert), 1 bis 48 - B5512
- 0 (deaktiviert), 1 bis 28 - B4512
- 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn jeder Gas-Errichterbedienungsmelder im System in den Alarmzustand wechselt. Der Ausgang wird deaktiviert, wenn alle Gas-Errichterbedienungsmelder im System wieder in den Normalbetrieb zurückkehren, und alle Gas-Errichterbedienungsalarmereignisse werden von den Bedienteilanzeigen gelöscht.

Hinweis!
Weisen Sie dem Ausgang, der dieser Zusammenfassungsfunktion zugewiesen ist, nicht mehr als eine Funktion zu.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Errichterbedienungsausgang für Zusammenfassung Gas

9.2.14 Störungsausgang für Zusammenfassung Gas

Standardeinstellung: 0 (deaktiviert)

Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Der Ausgang wird aktiviert, wenn alle Gasmelder im System in den Störungszustand wechseln. Der Ausgang wird deaktiviert, wenn alle Gasmelder im System wieder in den Normalbetrieb zurückkehren, und alle Gasstörungsereignisse werden von den Bedienteilanzeigen gelöscht.

Hinweis!
Weisen Sie dem Ausgang, der dieser Zusammenfassungsfunktion zugewiesen ist, nicht mehr als eine Funktion zu.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Zentralenübergreifende Ausgänge > Störungsausgang für Zusammenfassung Gas

9.3 Ausgangskonfiguration

9.3.1 Output Source (Ausgangsquelle)

Standardeinstellung:

– Ausgang A(1): intern A
– Ausgang B(2): intern B
– Ausgang C(3): intern C
– Alle anderen Ausgänge: nicht zugewiesen

Auswahl:

– Integriert
– Unassigned (Nicht zugewiesen)
– Acht Ausgänge
– IP-Kamera
– Bedienteil

Verwenden Sie den Parameter, um Ausgangsquellen (physikalische Geräte) Ausgangsnummern zuzuweisen. Ausgeblendete Optionen stehen nicht zur Verfügung.
B308-Module mit acht Ausgängen weisen Grenzen für Ausgangsnummern beginnend ab Ausgang 11 auf. Siehe *Schaltereinstellungen für B308-Modul mit acht Ausgängen, Seite 295*.

Die Verwendung der IP-Kamera als Ausgangsquelle ist eingeschränkt
Jede IP-Kamera (1 bis 4 für B5512, 1 bis 2 für B4512) unterstützt 4 Ausgänge. Sie können die IP-Kamera als Ausgangsquelle nur für die Ausgänge 11 bis 14, 21 bis 24, 31 bis 34, 41 bis 44 auswählen.
Wählen Sie die IP-Kamera *nicht* als Ausgangsquelle für die Ausgänge 15 bis 18, 25 bis 28, 35 bis 38, 45 bis 48 aus.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Ausgangskonfiguration > Ausgangsquelle

9.3.2 Ausgangstext (erste Sprache)

Standardeinstellung: Ausgang #

Auswahl: Bis zu 32 alphanumerische Zeichen

Geben Sie eine Beschreibung des Ausgangs in der ersten Sprache ein. Errichter, Wartungspersonal und Benutzer sehen diese Beschreibung.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Ausgangskonfiguration > Ausgangstext

9.3.3 Ausgangstext (zweite Sprache)

Standardeinstellung: Leer
Auswahl: Bis zu 32 alphanumerische Zeichen
Geben Sie eine Beschreibung des Ausgangs in der zweiten Sprache ein. Errichter, Wartungspersonal und Benutzer sehen diese Beschreibung.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Ausgangskonfiguration > Ausgangstext (zweite Sprache)

9.3.4 Für Benutzer ausblenden

Standardeinstellung: Nein
Auswahl:

- Ja: Die Zentrale erteilt die Berechtigung für diesen Ausgang nur dem Errichter. Endbenutzer können den Ausgang nicht manuell an einem Bedienteil oder mit RSC, Automation Mode 1 oder Automation Mode 2 ein- oder ausschalten.
- Nein: Die Zentrale erlaubt autorisierten Endbenutzern das manuelle Ein- oder Ausschalten an einem Bedienteil oder mithilfe von RSC, Automation Mode 1 oder Automation Mode 2.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Ausgangsparameter > Ausgangskonfiguration > Für Benutzer ausblenden

10 Benutzerkonfiguration

10.1 Benutzerzuweisungen (Zugangscodes)

10.1.1 Benutzername

Standardeinstellung:

– Benutzer 0: Errichter
– Alle anderen: USER [Benutzernummer]

Auswahl: Bis zu 32 Zeichen (Text, Zahlen, Leerzeichen und Symbole). Leerzeichen vor, nach und innerhalb des Namens werden als Text behandelt und sind in der Zeichenbeschränkung von 32 Zeichen enthalten.
Geben Sie den Benutzernamen ein, der an den Bedienteilen angezeigt werden soll. Der Benutzername ist im Modem4-Protokollformat in den Protokollen enthalten, die an Bedienteilempfänger gesendet werden.
Wenn der Benutzername länger als 20 Zeichen ist, läuft der vollständige Name einmal auf den Bedienteilen durch. Anschließend werden die ersten 20 Zeichen angezeigt. Drücken Sie [ESC], damit der Name erneut durchläuft.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen > Benutzername

10.1.2 Zugangscode

Standardeinstellung:

– Benutzer 0: 123
– Benutzer 1: 123456
– Alle anderen: leer

Auswahl: 0 bis 9
Geben Sie einen 3- bis 6-stelligen Zugangscode ein.
Der Parameter *Benutzercodelänge, Seite 110* (Länge des Zugangscodes) legt die Länge des Zugangscodes fest. Bei einer Einstellung auf 3, 4, 5 oder 6 Stellen ist die Zugangscodelänge für alle Zugangscodes festgelegt. Benutzer müssen nach der Eingabe des Zugangscodes nicht die Eingabetaste drücken.
Wenn der Parameter „Passcode Length“ (Länge des Zugangscodes) auf „Disabled“ (Deaktiviert) gesetzt ist, ist die Länge für keinen Zugangscode festgelegt. Individuelle Zugangscodes können eine Länge von 3 bis 6 Stellen haben. Benutzer müssen nach der Eingabe des Zugangscodes die Eingabetaste drücken.
Über RPS können Sie keinen Zugangscode eingeben, der mit dem Zugangscode einer Bedrohung in Konflikt stehen könnte. Sie können keinen Zugangscode innerhalb eines Bereichs von 2 von den vorhandenen Zugangscodes eintragen. Beispiel: Wenn 654327 ein vorhandener Zugangscode ist, können Sie 654325, 654326, 654328 und 654329 nicht eingeben. RPS setzt diese Regel durch, auch wenn eine Bedrohung deaktiviert ist.

Zugangscode Errichter
Benutzer 0 (Errichter) kann auf einem Bedienteil nicht hinzugefügt oder bearbeitet werden. Wenn ein anderer Benutzer als Benutzer 0 versucht, den Zugangscode für Benutzer 0 zu löschen, zeigt das Bedienteil NOT IN USE an.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen (Zugangscodes) > Zugangscode

10.1.3 Fernzugriff

Standardeinstellung:: Nein (Systemzugriff mit der RSC-App verbieten)
Auswahl:

– Ja (Diesem Benutzer Systemzugriff mit der RSC-App erlauben)
– Nein (Verhindern, dass dieser Benutzer Systemzugriff mit der RSC-App erhält)

Wenn dieser Parameter auf „Yes“ (Ja) gesetzt ist, kann der Benutzer sein Sicherheitssystem mit seinem Mobilgerät und der RSC (Remote Security Control)-App steuern.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen > Fernzugriff

10.1.4 Benutzergruppe

Standardeinstellung: 0

Auswahl:

– B5512: 0 (Benutzer gehört nicht zu einer Benutzergruppe), 1 bis 4
– B4512: 0 (Benutzer gehört nicht zu einer Benutzergruppe), 1 bis 2
– B3512: 0 (Benutzer gehört nicht zu einer Benutzergruppe), 1 bis 2

Verwenden Sie diesen Parameter, um eine Gruppe von Benutzern zu erstellen, deren Codierkarten (Zugangscode, Zugangskarte oder Token und Funk-Handsender) anhand eines Benutzergruppenfensters aktiviert und deaktiviert werden.
Geben Sie die Nummer der Benutzergruppe für jedes aktivierte Fenster unter „SCHEDULES > User Group Windows >*Benutzergruppe, Seite 263*“ (SCHEDULES > Benutzergruppenfenster > Benutzergruppe) ein.
Beispiel: Wenn Benutzergruppe 1 einem Fenster zugewiesen ist, das von 8:00 Uhr (Startzeit) bis 16:00 Uhr (Endzeit) ausgeführt wird, können die Benutzer in der Gruppe ihre eigenen Codierkarten nur zwischen 8:00 und 16:00 Uhr verwenden.
Sie können eine Benutzergruppe mehreren Benutzergruppenfenstern zuweisen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen (Zugangscodes) > Benutzergruppe

10.1.5 Bereichsberechtigungen

Standardeinstellung:

– Benutzer 0: Benutzerrechte für alle Bereichsnummern = 15
– Benutzer 1:
  – Bereich Nr. 1 Benutzerrechte = 1
  – Alle anderen Bereichsnummern Benutzerrechte = 0
– Alle anderen Benutzernummern: 0

Auswahl:

– B5512: 0 (Benutzer gehört nicht zu einer Benutzergruppe), 1 bis 4
– B4512: 0 (Benutzer gehört nicht zu einer Benutzergruppe), 1 bis 2
– B3512: 0 (Benutzer gehört nicht zu einer Benutzergruppe), 1 bis 2

Stellen Sie beim Einrichten eines neuen Benutzers sicher, dass Sie dem Benutzer Benutzerrechte für mindestens einen Bereich zuweisen. Der Parameter „Area Authorities“ (Bereichsberechtigungen) ist für neue Benutzer standardmäßig auf 0 (Null) eingestellt. Benutzerrechte 0 (null) bedeutet, dass der Benutzer keine Berechtigung für den angegebenen Bereich besitzt. Benutzerrechte 15 ist für Benutzer 0, Errichter, reserviert.
Informationen zum Anzeigen der Einstellungen für sämtliche Benutzerrechte finden Sie unter „User Configuration > *Benutzerrechte, Seite 193*“ (Benutzerkonfiguration > Benutzerrechte) in RPS.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen > Bereichsberechtigungen

10.1.6 Standortcode

Standardeinstellung (pro Kartentyp)**:**

– Kartentyp 26 Bit: 255
– Kartentyp 37 Bit, kein Standortcode: leer
– Kartentyp 37 Bit, mit Standortcode: 65535

Auswahl (pro Kartentyp)**:**

– Kartentyp 26 Bit: 0 bis 254, 255 = deaktiviert
– Kartentyp 37 Bit, kein Standortcode: leer
– Kartentyp 37 Bit, mit Standortcode: 0 bis 65534, 65535 = deaktiviert

Für den Kartentyp mit 37 Bit und ohne Standortcode ist der Parameter „Site Code“ (Standortcode) ausgeblendet.
Für die Kartentypen 26 Bit und 37 Bit mit Standortcode geben Sie den Standortcode (Anlagencode) wie auf der Verpackung der Karte oder des Tokens gezeigt ein.
Zum Abrufen des Standortcodes mit RPS fügen Sie die Karte oder das Token vor Ort mithilfe eines Readers oder Bedienteils (MENU 42) dem System hinzu. Dann verbinden Sie die Zentrale mit RPS und erhalten das Zentralenkonto.
Wenn Sie eine Karte löschen (oder die Kartendaten löschen), setzt RPS den Standortcode automatisch auf die Standardeinstellungen (255 für den Kartentyp 26 Bit, 65535 für den Kartentyp 37 Bit mit Standortcode).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen > Standortcode

10.1.7 Kartendaten

Standardeinstellung: leer

Auswahl:

– Kartentyp 26 Bit: 0 bis 65534, leer
– Kartentyp 37 Bit, kein Standortcode: 0 bis 1099511627774, leer
– Kartentyp 37 Bit, mit Standortcode: 0 bis 524286, leer

Geben Sie die Kartendaten ein, die auf die Karte oder das Token gedruckt sind.
Für die Kartentypen **26 Bit** und **37 Bit mit Standortcode** geben Sie *Standortcode, Seite 178* (Standortcode) ein, bevor Sie die Kartendaten eingeben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen > Kartendaten

10.1.8 Inovonics Funk-Handsender RFID (B820)

Standardeinstellung: k.a.

Auswahl: 0 bis 99999999

Um diesem Benutzer einen Inovonics-Funk-Handsender zuzuweisen, geben Sie die RFID (Radio Frequency Device Identification Number) ein. Die Nummer ist auf dem Funk-Handsender aufgedruckt.
Inovonics Funk-Handsender werden nicht überwacht, wenn sie einem Benutzer zugewiesen sind.
Sie können die RFID mithilfe des SDI2 Bus-HF-Empfängers und eines Systembedienteils auch automatisch lokal einlesen.
Durch Einstellen der RFID auf 0 wird der Funk-Handsender des Benutzers deaktiviert.

Hinweis!
RFID-Updates werden an den SDI2 Bus-HF-Empfänger weitergeleitet, wenn Sie RPS trennen.
Wenn Sie RFID-Updates von RPS an die Zentrale senden, lädt die Zentrale die RFIDs erst auf den SDI2 Bus-HF-Empfänger herunter, wenn Sie die Verbindung zu RPS trennen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen > RFID des Funk-Handsenders (B820 Inovonics Wireless)

10.1.9 RFID des RADION Funk-Handsenders (B810)

Standardeinstellung: 0
Auswahl: 0, 11 - 167772156
Um diesem Benutzer einen RADION keyfob zuzuweisen, geben Sie die RFID (Radio Frequency Device Identification Number) ein. Die Nummer ist auf dem Funk-Handsender aufgedruckt.
Sie können die RFID mithilfe des SDI2 Bus-HF-Empfängers und eines Systembedienteils auch automatisch lokal einlesen.
Durch Einstellen der RFID auf 0 wird der Funk-Handsender des Benutzers deaktiviert.

Hinweis!
RFID-Updates werden an den SDI2 Bus-HF-Empfänger weitergeleitet, wenn Sie RPS trennen.
Wenn Sie RFID-Updates von RPS an die Zentrale senden, lädt die Zentrale die RFIDs erst auf den SDI2 Bus-HF-Empfänger herunter, wenn Sie die Verbindung zu RPS trennen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen > RFID des Funk-Handsenders (B810 RADION Wireless)

10.1.10 Überwacht

Standardeinstellung: Nein
Auswahl:
- Ja: Der diesem Benutzer zugewiesene RADION keyfob wird überwacht.
- Nein: Der diesem Benutzer zugewiesene RADION keyfob wird nicht überwacht.

Wenn dieser Parameter auf „Yes“ (Ja) gesetzt ist, erstellt die Zentrale ein Ereignis aufgrund eines fehlenden Funk-Handsenders, wenn sich dieser 4 Stunden lang außerhalb der Reichweite des RADION-Empfängers befindet.
Inovonics-Funk-Handsender werden nicht überwacht.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen > Überwacht

10.1.11 Benutzersprache

Standardeinstellung: 1: [erste Sprache]
Auswahl:
- 1: [erste Sprache]
- 2: [zweite Sprache]

Wählen Sie die Sprache aus, die der Benutzer auf Bedienteilen sieht, die so konfiguriert sind, dass sie die Benutzersprache anzeigen.
Die erste Sprache und die zweite Sprache werden bei der Einrichtung des Zentralenkontos in der Ansicht mit den Zentralendaten eingerichtet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerzuweisungen (Zugangscodes) > Benutzersprache

10.2 Benutzergruppen

10.2.1 Name der Benutzergruppe

Standardeinstellung: Leer

Auswahl: Bis zu 32 Zeichen (Text, Zahlen, Leerzeichen und Symbole). Leerzeichen vor, nach und innerhalb des Namens werden als Text behandelt und sind in der Zeichenbeschränkung von 32 Zeichen enthalten.
Mit diesem Parameter können Sie einen Namen für die Benutzergruppe eingeben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzergruppen > Name der Benutzergruppe

10.3 Benutzerfunktionen (Bedienteil)

10.3.1 Verzögerte Vollscharfschaltung

Standardeinstellung: Z

Auswahl:

- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Benutzerfunktion schaltet Bereiche mit Eingangsverzögerung und Scharfschalteverzögerung vollständig scharf. Alle kontrollierten Melder im Bereich sind enthalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Verzögerte Vollscharfschaltung

10.3.2 Unverzögerte Vollscharfschaltung

Standardeinstellung: Z

Auswahl:

- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Benutzerfunktion schaltet Bereiche ohne Eingangsverzögerung und Scharfschalteverzögerung vollständig scharf. Alle kontrollierten Melder im Bereich sind enthalten.

Hinweis!
Zur Erfüllung der SIA CP-01-Anforderungen zur Fehlalarmunterdrückung setzen Sie diesen Parameter auf „Disabled (-)“ (Deaktiviert (-)). Weitere Informationen finden Sie unter „SIA CP-01 Verification” (SIA CP-01-Verifizierung).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Unverzögerte Vollscharfschaltung

10.3.3 Unverzögerte Außenhautüberwachung

Standardeinstellung: Z

Auswahl:

- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.

– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Benutzerfunktion schaltet die Außenhautüberwachung für Bereiche ohne Eingangsverzögerung und Scharfschalteverzögerung scharf. Nur Melder für die Außenhautüberwachung im Bereich sind enthalten. Innenbereich-Melder sind nicht enthalten.

Hinweis!
Zur Erfüllung der SIA CP-01-Anforderungen zur Fehlalarmunterdrückung setzen Sie diesen Parameter auf „Disabled (-)“ (Deaktiviert (-)). Weitere Informationen finden Sie unter „SIA CP-01 Verification” (SIA CP-01-Verifizierung).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Unverzögerte Außenhautüberwachung.

10.3.4 Verzögerte Außenhautüberwachung

Standardeinstellung: Z
Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Benutzerfunktion schaltet die Außenhautüberwachung für Bereiche mit Eingangsverzögerung und Scharfschalteverzögerung scharf. Nur Melder für die Außenhautüberwachung im Bereich sind enthalten. Innenbereich-Melder sind nicht enthalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Verzögerte Außenhautüberwachung.

10.3.5 Überwachungsmodus

Standard: A
Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Benutzerfunktion wird der Überwachungsmodus aktiviert und deaktiviert.
Bei aktiviertem Überwachungsmodus und einer Störung an einem Überwachungsmelder zeigen die Bedienteile den Meldertext und geben den Überwachungston aus.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Überwachungsmodus

10.3.6 View Area Status (Bereichsstatus anzeigen)

Standardeinstellung: Z
Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.

– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Benutzerfunktion ermöglicht dem Benutzer das Anzeigen des Scharfschaltungszustands aller Bereiche im Bereich des Bedienteils.
Die Scharfschaltungszustände:
– Unscharfgeschaltet
– Verzögerte Vollscharfschaltung
– Unverzögerte Vollscharfschaltung
– Unverzögerte Außenhautüberwachung (scharfgeschaltet)
– Verzögerte Außenhautüberwachung (scharfgeschaltet)

Alle Bereichstypen („Master“, „Associate“ (Zugeordnet), „Regular“ (Standard) und „Shared“ (Gemeinsam genutzt)) können mit dieser Funktion angesehen werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Bereichsstatus anzeigen

10.3.7 Aktuelle Ereignisse anzeigen/löschen

Standard: A
Auswahl:
– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Benutzerfunktion zeigt aktuelle Ereignisse. Die aktuellen Ereignisse werden gelöscht, wenn der Bereich scharfgeschaltet wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Aktuelle Ereignisse anzeigen/löschen

10.3.8 View Point Status (Melderstatus anzeigen)

Standard: A
Auswahl:
– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Benutzerfunktion zeigt den Meldertext und den elektrischen Zustand (normal, offen, kurzgeschlossen oder fehlt) für jeden Melder, der dem Bereich zugewiesen ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Melderstatus anzeigen

10.3.9 Revision (alle Melder für Nicht-Feueralarme und Einbruchalarme)

Standard: A
Auswahl:
– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.

– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Die Benutzerfunktion „Walk Test“ (Revision) ermöglicht Benutzern das Testen kontrollierter Melder, ohne Alarmprotokolle an den Bedienteilempfänger zu senden.
Zu Beginn der Revision wird das Alarmsignal für 2 Sekunden aktiviert. Wenn für den jeweiligen kontrollierten Melder eine Störung auftritt, geben die Bedienteile einen Signalton aus.
Feuermelder, Gasmelder und 24-Stunden-Melder können mit dieser Revisionsbenutzerfunktion geprüft werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Revision (alle Melder für Nicht-Feueralarme und Einbruchalarme)

10.3.10 Revision für alle Feuermelder

Standardeinstellung: Z
Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Dieser Parameter deaktiviert, aktiviert mit oder ohne erforderlichen Zugangscode die Benutzerfunktionen „Fire Walk Test“ (Brand-Funktionstest) und „Fire Drill“ (Brandschutzübung) (DRILL-Taste auf B926F-Bedienteilen).
Der Brand-Funktionstest umfasst Feuermelder und Gasmelder. Kontrollierte Melder und 24-Stunden-Melder können mit diesem Brand-Funktionstest nicht getestet werden.

Beim Start eines Brand-Funktionstests

– Die Zentralen sendet ein FIRE WALK START-Protokoll an den Bedienteilempfänger.
– Die Alarmankündigung erfolgt nur lokal, es werden keine Alarmprotokolle an den Bedienteilempfänger gesendet.
– Die Zentrale wird nur über die Batterie mit Strom versorgt.
– Der Ausgang *Feueralarm, Seite 166* (Feueralarm) wird für jeden getesteten Feuer- oder Gasmelder 2 Sekunden lang aktiviert.
– Alle Feuer- und Gasmelder, deren Parameter *Rücksetzbar, Seite 247* (Rücksetzbar) auf YES (Ja) eingestellt ist, werden nach dem Testen automatisch zurückgesetzt. [SENSORS RESETTING] (Melder werden zurückgesetzt) wird auf den Bedienteilen angezeigt.
– Das Bedienteil zeigt den Meldertext für jeden Melder während des Tests und eine aktualisierte Anzahl der getesteten Melder an.
– Der Test endet nach dem Testen aller Melder oder nach 20 Minuten ohne Aktivität. Die Zentrale sendet ein FIRE WALK END-Protokoll an den Bedienteilempfänger.

Wenn Feuer- oder Gasmelder am Ende des Brand-Funktionstests eine Störung aufweisen, werden die Melder gesperrt und ein Störungssignal wird ausgegeben. Die Bedienteile zeigen die gesperrten Melder und die Störfunktion.

Beim Start einer Brandschutzübung

– Die Zentrale sendet ein FIRE DRILL START-Protokoll an den Bedienteilempfänger.
– Der Ausgang *Feueralarm, Seite 166* (Feueralarm) wird aktiviert, bis ein Benutzer die Übung durch Stummschalten des Feueralarms beendet.

– Feuer- und Gasmelder sind aktiv. Ein Alarm auf einem Feuer- oder Gasmelder beendet die Übung. Die Zentrale sendet Feueralarmprotokolle.
– Am Ende der Brandschutzübung sendet die Zentrale ein FIRE DRILL END-Protokoll.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Revision für alle Feuermelder

10.3.11 Protokoll senden (Prüfung/Status)

Standard: A
Auswahl:
– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Benutzerfunktion wird dasselbe Prüfprotokoll gesendet wie mit der Funktion für zeitgesteuerte Ereignisse.
Falls ein Melder in einem beliebigen Bereich keinen normalen Zustand (Störung auf der Bedienteilanzeige nicht gelöscht) aufweist, sendet die Zentrale anstelle des Prüfprotokolls ein nicht-normales Prüfprotokoll.
Wenn der Parameter „Zentralenübergreifende Parameter“ > Protokoll-Routing > *Expand Test Report (Prüfprotokoll erweitern), Seite 55* auf „Ja“ eingestellt, wird nach dem Prüfprotokoll (oder dem nicht-normalen Prüfprotokoll) für jeden nicht-normalen Systemstatus ein Diagnoseprotokoll erstellt. Eine Liste mit enthaltenen Protokollen finden Sie unter „Zentralenübergreifende Parameter > „Protokoll-Routing > *Diagnoseprotokolle, Seite 82*.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Protokoll senden (Prüfung/Status)

10.3.12 Bedienteilhelligkeit/Lautstärke/Tastenton einstellen

Standard: A
Auswahl:
– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Funktion können Benutzer die Bedienteilhelligkeit und Lautstärke einstellen sowie Tastentöne ein- oder ausschalten.
Auf B942-Bedienteilen können Benutzer das Nachtlicht und Anwesenheitsfunktionen einstellen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Bedienteilhelligkeit/Lautstärke/Tastenton einstellen

10.3.13 Datum und Uhrzeit einstellen/anzeigen

Standardeinstellung: Z
Auswahl:
– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.

– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Benutzerfunktion kann der Benutzer Datum und Uhrzeit in der Zentrale einstellen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Datum und Uhrzeit einstellen/anzeigen

10.3.14 Zugangscodes ändern

Standardeinstellung: Z
Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Benutzerfunktion kann ein Benutzer seinen eigenen Zugangscode ändern.
Unter der Funktion *Benutzer hinzufügen/bearbeiten, Seite 186* (Benutzer hinzufügen/bearbeiten) finden Sie Informationen, um einem Benutzer das Ändern des Zugangscodes für andere Benutzer zu erlauben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Zugangscode ändern

10.3.15 Benutzer hinzufügen/bearbeiten

Standardeinstellung: Z
Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Funktion kann ein Benutzer mit der entsprechenden Berechtigung Zugangscodes hinzufügen oder ändern und Benutzerrechte für die Zentrale für andere Benutzer nach Bereichen hinzufügen oder ändern.

Hinweis!
Der Befehl „Add User“ (Benutzer hinzufügen) reagiert nicht mehr auf die Türsteuerung und RTE/REX-Anfragen
Wenn der ADD USER-Befehl ausgeführt wird, werden keine Codierkarten (Karten oder Tokens) verarbeitet. Es erfolgt keine Reaktion auf die Türsteuerungsfunktionen und RTE/REX-Anfragen. Bei starker Aktivität für eine Tür ändern Sie den Zustand der Tür in „Unlocked“ (Entriegelt), bevor Sie Benutzer hinzufügen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Benutzer hinzufügen/bearbeiten

10.3.16 Benutzer löschen

Standardeinstellung: Z
Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Funktion kann ein Benutzer mit der entsprechenden Berechtigung die Zugangscodes anderer Benutzer löschen. Benutzernamen werden nicht gelöscht.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Benutzer löschen

10.3.17 Extend Close (Schließen verlängern)

Standardeinstellung: Z
Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Funktion können Benutzer das Schließen-Fenster verlängern, wenn der Zeitpunkt „Close Early Begin“ (Frühes Schließen – Beginn) verstrichen ist und das Schließen-Fenster aktiv ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Schließen verlängern

10.3.18 Ereignisprotokoll anzeigen

Standard: A
Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Funktion kann der Benutzer das Ereignisprotokoll anzeigen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Ereignisprotokoll anzeigen

10.3.19 Benutzerbefehl 7

Standardeinstellung: Z
Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Drücken von [CMD] und [7] löst einen manuellen Feueralarm aus.

Bei B92x-Bedienteilen wird durch gleichzeitiges Gedrückthalten der Tasten [A] und [1] ebenso ein manueller Feueralarm ausgelöst.
Zum Aktivieren von Benutzerbefehl 7 legen Sie für „Keypads > Global Keypad Settings > A Key Response“ (Bedienteile > Globale Bedienteileinstellungen > Funktion A-Taste) die Option „Manual Fire Alarm“ (Manueller Feueralarm) fest.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Benutzerbefehl 7

10.3.20 Benutzerbefehl 9

Standardeinstellung: Z
Auswahl:
- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Drücken von [CMD] und [9] löst einen manuellen Notrufalarm aus.
Bei B92x-Bedienteilen wird durch gleichzeitiges Gedrückthalten der Tasten [A] und [7] ebenso ein manueller Notrufalarm ausgelöst.
Zum Aktivieren von Benutzerbefehl 9 legen Sie für „Keypads > Global Keypad Settings > C Key Response“ (Bedienteile > Globale Bedienteileinstellungen > Funktion C-Taste) die Option „Manual Panic Alarm, invisible and silent alarm output“ (Manueller Notrufalarm, unsichtbare und stille Alarmausgabe) oder „Manual Panic Alarm, visible with alarm output“ (Manueller Notrufalarm, sichtbar mit Alarmausgabe) fest.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Benutzerbefehl 9

10.3.21 Bypass a Point (Einen Melder übergehen)

Standardeinstellung: Z
Auswahl:
- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Funktion sperrt einzelne Melder in Bereichen in der Umgebung des Bedienteils. Gesperrte Melder erstellen keine Alarm- und Störungsereignisse.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Einen Melder übergehen

10.3.22 Unbypass a Point (Einen Melder einschalten)

Standardeinstellung: Z
Auswahl:
- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.

– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Funktion entsperrt einzelne Melder, die folgendermaßen parametriert sind: P## FA Returnable (Zwangsläufige Scharfschaltung wiederherstellbar) oder P## Bypass Returnable (Übergehung wiederherstellbar). Melder im Bereich des Bedienteils, an dem die Funktion aufgerufen wird, werden entsperrt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Einen Melder einschalten

10.3.23 Melder zurücksetzen

Standard: A

Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Funktion werden Melder in Bereichen in der Nähe des Bedienteils zurückgesetzt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Melder zurücksetzen

10.3.24 Ausgang ändern

Standardeinstellung: Z

Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Funktion kann der Benutzer Ausgänge manuell einstellen und zurücksetzen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Ausgänge ändern

10.3.25 Fernparametrierung

Standardeinstellung: Z

Auswahl:

– Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
– Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
– Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Benutzerfunktion werden Fernparametrierungssitzungen gestartet. Falls der Benutzer diese Funktion startet, wenn die gemeinsam mit der Zentrale genutzte Telefonleitung klingelt, übernimmt die Zentrale die Telefonleitung.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Fernparametrierung

10.3.26 Gehe zu Bereich

Standardeinstellung: Z

Auswahl:

- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Funktion weist das Bedienteil vorübergehend einem anderen Bereich zu.
Benutzer sind auf Funktionen entsprechend ihren Benutzerrechten für den Bereich beschränkt, dem das Bedienteil vorübergehend zuwiesen ist.
Nach 15 Sekunden ohne Benutzeraktivität am Bedienteil wird das Bedienteil wieder in seinen zugewiesenen Bereich zurückversetzt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Funktionen am Bedienteil > In den Bereich gehen

10.3.27 Typ und Version des Anzeigetableaus

Standard: A

Auswahl:

- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Benutzerfunktion zeigt den Zentralentyp und die Firmwareversion an.
Wenn der Standardwert des Parameters „Area Name Text“ (Text Bereichsname) geändert wird, zeigt diese Funktion den standardmäßigen Text des Bereichsnamens an.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Funktionen am Bedienteil > Typ und Version des Anzeigetableaus

10.3.28 Wartungs-Funktionstest für alle Melder

Standardeinstellung: Z

Auswahl:

- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Die Benutzerfunktion „Service Walk Test“ (Wartungs-Funktionstest) ermöglicht Benutzern das Testen aller Melder, die einer Quelle zugewiesen sind (der Quellparameter ist nicht auf „Unassigned“ (Nicht zugewiesen) gesetzt).
Wenn für den jeweiligen Melder eine Störung auftritt, geben die Bedienteile einen Signalton aus.
Feuermelder, Gasmelder oder 24-Stunden-Melder mit nicht behobener Störung werden beim Beenden des Wartungs-Funktionstests umgangen. Der Störungston wird an Bedienteilen ausgegeben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Wartungs-Funktionstest für alle Melder

10.3.29 Change Skeds (Zeitgesteuerte Ereignisse ändern)

Standardeinstellung: Z
Auswahl:
- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Funktion kann der Benutzer die Zeit für die Ausführung eines zeitgesteuerten Ereignisses bearbeiten und ob das zeitgesteuerte Ereignis an Feiertagen ausgeführt wird. Benutzer können diese Funktion über jedes Bedienteil ausführen, das einem Bereich zugewiesen ist, für den der Benutzer eine Berechtigung besitzt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Zeitgesteuerte Ereignisse ändern

10.3.30 Revision für alle unsichtbaren Melder für Einbruchalarme

Standardeinstellung: Z
Auswahl:
- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Die Benutzerfunktion „Walk Test Invisible“ (Funktionstest für unsichtbare Melder) ermöglicht Benutzern das Testen unsichtbarer Melder (Parameter „Invisible Point“ (Unsichtbarer Melder) auf „Yes“ (Ja) gesetzt) ohne Senden von Alarmprotokollen an den Bedienteilempfänger.
24-Stunden-Melder mit nicht behobener Störung werden beim Beenden des Wartungs-Funktionstests umgangen. Der Störungston wird an Bedienteilen ausgegeben.
Feuer- und Gasmelder können mit der Benutzerfunktion „Walk Test Invisible“ (Funktionstest für unsichtbare Melder) nicht getestet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Revision für alle unsichtbaren Melder für Einbruchalarme

10.3.31 Stummschalten-Funktion

Standard: A
Auswahl:
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne dass der Benutzer einen Zugangscode eingeben muss, um die Bedienteile stummzuschalten.
- Zugangscode (Z): Diese Funktion zentralenübergreifend aktivieren und vom Benutzer die Eingabe eines Zugangscode fordern, um die Bedienteile stummzuschalten.

Wenn auf Bedienteilen der Störungston ausgegeben wird, rufen Benutzer die Funktion zum Stummschalten auf, indem Sie die Taste zum Stummschalten oder die Eingabetaste drücken. Wenn dieser Parameter auf „Passcode (P)“ (Zugangscode (Z)) eingestellt ist, müssen Benutzer ihren Zugangscode eingeben, nachdem sie die Taste zum Stummschalten oder die Eingabetaste gedrückt haben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Stummschalten-Funktion

10.3.32 Benutzerdefinierte Funktion

Standardeinstellung: Zugangscode (Z)
Auswahl:

- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Mit dieser Funktion kann der Benutzer benutzerdefinierte Funktionen über das Kontextmenü, A-Taste, B-Taste, C-Taste oder einen Funk-Handsender ausführen.
B6512 unterstützt die benutzerdefinierte Funktion 128 bis 133.
B5512 unterstützt die benutzerdefinierte Funktion 128 bis 131.
B4512 unterstützt die benutzerdefinierte Funktion 128 bis 129.
B3512 unterstützt die benutzerdefinierte Funktion 128.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Benutzerdefinierte Funktion

10.3.33 Bedienteilparametrierung

Standardeinstellung: Z
Auswahl:

- Deaktivieren (-): Diese Funktion zentralenübergreifend deaktivieren ungeachtet der Benutzerrechte des Benutzers.
- Aktivieren (A): Diese Funktion zentralenübergreifend aktivieren, ohne einen Zugangscode anzufordern.
- Zugangscode (Z): Einen Zugangscode anfordern, um diese Funktion zentralenweit zu aktivieren.

Diese Funktion ermöglicht die Parametrierung von Bedieneinheiten für eine ausgewählte Liste von Parametern.
Nur der Zugangscode des Errichters verfügt über die Berechtigung für die Bedienteil-Parametrierung.
Falls ein beliebiger Bereich scharfgeschaltet oder die Zentrale mit RPS verbunden ist, können Sie die Bedienteilparametrierung nicht aufrufen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Funktionen am Bedienteil > Bedienteilparametrierung

Weitere Informationen
In der Dokumentation der Zentrale finden Sie weitere Informationen zur Bedienteilparametrierung.

10.4 Benutzerrechte

Benutzerrechte bestimmen die Merkmale und Funktionen, auf die Benutzer Zugriff haben. Verwenden Sie die Parameter in diesem Abschnitt, um die Benutzerrechte 1-14 zu konfigurieren. Benutzerrecht 15 ist für den Zugangscode des Errichters (Benutzer 0) reserviert und kann nicht bearbeitet werden.
Verwenden Sie „User Configuration > User Assignments (passcodes) > User Authorities“ (Benutzerkonfiguration > Benutzerzuweisungen (Zugangscodes) > Benutzerrechte) zum Zuweisen von Benutzern zu Benutzerrechten für den jeweiligen Bereich.

10.4.1 Name der Benutzerrechte (erste Sprache)

Standardeinstellung:: Berechtigungsstufe 1 (bis 15)
Optionen: bis zu 32 Zeichen.
Geben Sie bis zu 32 Zeichen zur Beschreibung des Bereichs ein.
Die erste Sprache und die zweite Sprache werden während der Einrichtung des Zentralenkontos parametriert. Verfügbare Sprachen: Chinesisch, Deutsch, Englisch, Französisch, Griechisch, Italienisch, Niederländisch, Polnisch, Portugiesisch (Brasilianisch), Schwedisch, Spanisch, Ungarisch.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Name der Benutzerrechte

10.4.2 Name der Benutzerrechte (zweite Sprache)

Standardeinstellung:: Berechtigungsstufe 1 (bis 15)
Optionen: bis zu 32 Zeichen.
Geben Sie bis zu 32 Zeichen zur Beschreibung des Bereichs ein.
Die erste Sprache und die zweite Sprache werden während der Einrichtung des Zentralenkontos parametriert. Verfügbare Sprachen: Chinesisch, Deutsch, Englisch, Französisch, Griechisch, Italienisch, Niederländisch, Polnisch, Portugiesisch (Brasilianisch), Schwedisch, Spanisch, Ungarisch.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Name der Benutzerrechte (zweite Sprache)

10.4.3 Auswahl unscharfschalten

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1-5, 14
- Leer (-) – Benutzerrechte 6-13, 15

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Diese Funktionen zur Unscharfschaltung sind für Benutzer mit folgenden Rechten verfügbar:
- Disarm All (Alle unscharfschalten): Alle Bereiche innerhalb der Reichweite des Bedienteils und Bereiche, die in den Zugriffsberechtigungen enthalten sind, werden unscharfgeschaltet.
- Disarm Area# (Bereich unscharfschalten): Schaltet nur den ausgewählten Bereich unscharf.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Auswahl unscharfschalten

10.4.4 Verzögerte Vollscharfschaltung

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1-5
– Leer (-) – Benutzerrechte 6-15

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer die Bereiche im Umfang des Bedienteils und die in den Benutzerrechten des Benutzers enthaltene verzögerte Vollscharfschaltung aktivieren (Melder für Außenhautüberwachung und Innenbereich-Melder mit Scharfschalteverzögerungszeit und Eingangsverzögerungszeit scharfschalten).
Wenn ein Benutzer mit Befehl 1 die verzögerte Vollscharfschaltung aktiviert, wird nur der Bereich des Bedienteils scharfgeschaltet.
Wenn ein Benutzer die verzögerte Vollscharfschaltung mit der Remote Security Control (RSC)-App aktiviert, werden alle Bereiche im Rahmen der Zugriffsberechtigung des Benutzers scharfgeschaltet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Verzögerte Vollscharfschaltung

10.4.5 Unverzögerte Vollscharfschaltung

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1 & 2
– Leer (-) – Benutzerrechte 3-15

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer die Bereiche im Umfang des Bedienteils und die in den Benutzerrechten des Benutzers enthaltene unverzögerte Vollscharfschaltung aktivieren (Melder für Außenhautüberwachung und Innenbereich-Melder ohne Scharfschalteverzögerungszeit und ohne Eingangsverzögerungszeit scharfschalten).
Wenn ein Benutzer mit Befehl 1 1 die unverzögerte Vollscharfschaltung aktiviert, wird nur der Bereich des Bedienteils scharfgeschaltet.
Wenn ein Benutzer die unverzögerte Vollscharfschaltung mit der Remote Security Control (RSC)-App aktiviert, werden alle Bereiche im Rahmen der Zugriffsberechtigung des Benutzers scharfgeschaltet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Unverzögerte Vollscharfschaltung

10.4.6 Unverzögerte Außenhautüberwachung

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1-4
– Leer (-) – Benutzerrechte 5-15

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer die Bereiche im Umfang des Bedienteils und die in den Benutzerrechten des Benutzers enthaltene unverzögerte Außenhautüberwachung scharfschalten (Melder für Außenhautüberwachung ohne Scharfschalteverzögerungszeit und ohne Eingangsverzögerungszeit scharfschalten).
Wenn ein Benutzer mit Befehl 2 die unverzögerte Außenhautüberwachung scharfschaltet, wird nur der Bereich des Bedienteils scharfgeschaltet.
Wenn ein Benutzer die unverzögerte Außenhautüberwachung mit der Remote Security Control (RSC)-App aktiviert, werden alle Bereiche im Rahmen der Zugriffsberechtigung des Benutzers scharfgeschaltet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Unverzögerte Außenhautüberwachung

10.4.7 Verzögerte Außenhautüberwachung

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1-4
– Leer (-) – Benutzerrechte 5-15

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer die Bereiche im Umfang des Bedienteils und die in den Benutzerrechten des Benutzers enthaltene verzögerte Außenhautüberwachung scharfschalten (Melder für Außenhautüberwachung mit Scharfschalteverzögerungszeit und Eingangsverzögerungszeit scharfschalten).
Wenn ein Benutzer mit Befehl 3 die verzögerte Außenhautüberwachung scharfschaltet, wird nur der Bereich des Bedienteils scharfgeschaltet.
Wenn ein Benutzer die verzögerte Außenhautüberwachung mit der Remote Security Control (RSC)-App scharfschaltet, werden alle Bereiche im Rahmen der Zugriffsberechtigung des Benutzers scharfgeschaltet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Verzögerte Außenhautüberwachung

10.4.8 Überwachungsmodus

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1-3, 15
– Leer (-) – Benutzerrechte 4-14

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer den Überwachungsmodus in den Bereichen um das Bedienteil und die in den Benutzerrechten des Benutzers enthaltenen Bereiche ein- und ausschalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Überwachungsmodus

10.4.9 View Area Status (Bereichsstatus anzeigen)

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1, 2, 15
- Leer (-) – Benutzerrechte 3-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer mit Berechtigung zum Scharfschalten/Unscharfschalten den Status „Arm/Disarm“ (Scharfschalten/Unscharfschalten) und „Ready to arm“ (Scharfschaltebereit) für Bereiche im Umfang des Bedienteils und die in den Benutzerrechten des Benutzers enthaltenen Bereiche anzeigen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Bereichsstatus anzeigen

10.4.10 View Event Memory (Aktuelle Ereignisse anzeigen)

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1-3, 15
- Leer (-) – Benutzerrechte 4-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer aktuelle Ereignisse in den Bereichen um das Bedienteil und in den Benutzerrechten des Benutzers enthaltenen Bereichen anzeigen. Die Zentrale löscht aktuelle Ereignisse, wenn Bereiche scharfgeschaltet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Aktuelle Ereignisse anzeigen

10.4.11 View Point Status (Melderstatus anzeigen)

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1-3, 15
- Leer (-) – Benutzerrechte 4-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer den Melderstatus (Normal, Kurz, Offen) in den Bereichen um das Bedienteil und in den Benutzerrechten des Benutzers enthaltenen Bereichen anzeigen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Melderstatus anzeigen

10.4.12 Revision (alle Melder für Nicht-Feueralarme und Einbruchalarme)

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1, 2, 15
- Leer (-) – Benutzerrechte 3-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer eine Revision für kontrollierte Melder durchführen (Prüfung ohne Senden von Alarmprotokollen an die Bedienteilempfänger).
Zu Beginn der Revision wird das Alarmsignal für 2 Sekunden aktiviert. Wenn für den jeweiligen kontrollierten Melder eine Störung auftritt, geben die Bedienteile einen Signalton aus.
Feuermelder, Gasmelder und 24-Stunden-Melder können mit dieser Revisionsbenutzerfunktion geprüft werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Revision (Melder für Nicht-Feueralarme und Einbruchalarme)

10.4.13 Revision für alle Feuermelder

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1, 2, 15
- Leer (-) – Benutzerrechte 3-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer einen Feuer-Funktionstest für Feuermelder und Gasmelder durchführen und die Berechtigung für die DRILL-Taste auf den B926F-Bedienteilen testen.
Kontrollierte Melder und 24-Stunden-Melder können mit diesem Brand-Funktionstest nicht getestet werden.

Beim Start eines Brand-Funktionstests
- Die Zentralen sendet ein FIRE WALK START-Protokoll an den Bedienteilempfänger.
- Die Alarmankündigung erfolgt nur lokal, es werden keine Alarmprotokolle an den Bedienteilempfänger gesendet.
- Die Zentrale wird nur über die Batterie mit Strom versorgt.
- Der Ausgang *Feueralarm, Seite 166* (Feueralarm) wird für jeden getesteten Feuer- oder Gasmelder 2 Sekunden lang aktiviert.

– Alle Feuer- und Gasmelder, deren Parameter *Rücksetzbar, Seite 247* (Rücksetzbar) auf YES (Ja) eingestellt ist, werden nach dem Testen automatisch zurückgesetzt. [SENSORS RESETTING] (Melder werden zurückgesetzt) wird auf den Bedienteilen angezeigt.
– Das Bedienteil zeigt den Meldertext für jeden Melder während des Tests und eine aktualisierte Anzahl der getesteten Melder an.
– Der Test endet nach dem Testen aller Melder oder nach 20 Minuten ohne Aktivität. Die Zentrale sendet ein FIRE WALK END-Protokoll an den Bedienteilempfänger.

Wenn Feuer- oder Gasmelder am Ende des Brand-Funktionstests eine Störung aufweisen, werden die Melder gesperrt und ein Störungssignal wird ausgegeben. Die Bedienteile zeigen die gesperrten Melder und die Störfunktion.

Beim Start einer Brandschutzübung

– Die Zentrale sendet ein FIRE DRILL START-Protokoll an den Bedienteilempfänger.
– Der Ausgang *Feueralarm, Seite 166* (Feueralarm) wird aktiviert, bis ein Benutzer die Übung durch Stummschalten des Feueralarms beendet.
– Feuer- und Gasmelder sind aktiv. Ein Alarm auf einem Feuer- oder Gasmelder beendet die Übung. Die Zentrale sendet Feueralarmprotokolle.
– Am Ende der Brandschutzübung sendet die Zentrale ein FIRE DRILL END-Protokoll.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Benutzerrechte > Revision für alle Feuermelder

10.4.14 Revision für alle unsichtbaren Melder für Einbruchalarme

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1, 15
– Leer (-) – Benutzerrechte 2-14

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer unsichtbare Melder prüfen (Parameter für unsichtbare Melder auf „Yes“ (Ja) gesetzt), ohne Alarmprotokolle an den Bedienteilempfänger zu senden. 24-Stunden-Melder mit nicht behobener Störung werden beim Beenden des Wartungs-Funktionstests umgangen. Der Störungston wird an Bedienteilen ausgegeben.
Feuer- und Gasmelder können mit der Benutzerfunktion „Walk Test Invisible“ (Funktionstest für unsichtbare Melder) nicht getestet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Benutzerrechte > Revision für alle unsichtbaren Melder für Einbruchalarme

10.4.15 Wartungs-Funktionstest für alle Melder

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1, 15
– Leer (-) – Benutzerrechte 2-14

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer den Wartungs-Funktionstest verwenden. Der Wartungs-Funktionstest enthält alle Melder, die einer Quelle zugewiesen sind (der Quell-Parameter ist nicht auf „Unassigned“ (Nicht zugewiesen) gesetzt).
Wenn für den jeweiligen Melder eine Störung auftritt, geben die Bedienteile einen Signalton aus.
Feuermelder, Gasmelder oder 24-Stunden-Melder mit nicht behobener Störung werden beim Beenden des Wartungs-Funktionstests umgangen. Der Störungston wird an Bedienteilen ausgegeben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Wartungs-Funktionstest für alle Melder

10.4.16 Protokoll senden (Prüfung/Status)

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1, 15
- Leer (-) – Benutzerrechte 2-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer ein Prüfprotokoll von Bedienteilen aus senden, die einem Bereich in den Benutzerrechten des Benutzers zugeordnet sind.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Protokoll senden (Prüfung/Protokoll)

10.4.17 Bedienteilanzeige ändern

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1, 15
- Leer (-) – Benutzerrechte 2-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer Bedienteilanzeigen (helle Anzeige, verdunkelte Anzeige) für die in den Benutzerrechten des Benutzers enthaltenen Bereiche ändern.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Bedienteilanzeige ändern

10.4.18 Datum und Uhrzeit ändern

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1, 15
- Leer (-) – Benutzerrechte 2-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer Datum und Uhrzeit der Zentrale ändern.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Datum und Uhrzeit ändern

10.4.19 Zugangscodes ändern

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1, 15
- Leer (-) – Benutzerrechte 2-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer ihren eigenen Zugangscode ändern.
Informationen zum Ändern von Zugangscodes für andere Benutzer finden Sie unter *Zugangscodes/Karte/Ebene des Benutzers hinzufügen, Seite 200* (Zugangscode/Karte/Ebene des Benutzers hinzufügen).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Zugangscode ändern

10.4.20 Zugangscodes/Karte/Ebene des Benutzers hinzufügen

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1, 15
- Leer (-) – Benutzerrechte 2-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer andere Benutzer hinzufügen und ändern (bearbeiten). Sie können Zugangscode, Name, Benutzerrechte, Bedienteil, Zugangskarte (oder -schlüssel), Sprache und Zugriff auf eine mobile App von Bosch bearbeiten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Zugangscode/Karte/Ebene des Benutzers hinzufügen

10.4.21 Zugangscode/Karte/Ebene des Benutzers löschen

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1, 15
- Leer (-) – Benutzerrechte 2-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer andere Benutzer löschen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Zugangscode/Karte/Ebene des Benutzers löschen

10.4.22 Extend Close (Schließen verlängern)

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1, 15
– Leer (-) – Benutzerrechte 2-14

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer die Schließzeit in Bereichen um das Bedienteil und in den Benutzerrechten des Benutzers enthaltenen Bereichen ändern.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Benutzerrechte > Schließen verlängern

10.4.23 Ereignisprotokoll anzeigen

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1, 15
– Leer (-) – Benutzerrechte 2-14

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer alle Ereignisse im Ereignisprotokoll der Zentrale anzeigen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Benutzerrechte > Ereignisprotokoll anzeigen

10.4.24 Benutzerbefehl 7

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1
– Leer (-) – Benutzerrechte: alle anderen

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Dieser Parameter aktiviert Benutzerbefehl 7 für Benutzer.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Benutzerrechte > Benutzerbefehl 7

10.4.25 Benutzerbefehl 9

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1
– Leer (-) – Benutzerrechte: alle anderen

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Dieser Parameter aktiviert Benutzerbefehl 9 für Benutzer.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Benutzerbefehl 9

10.4.26 Bypass a Point (Einen Melder übergehen)

Standardeinstellung:
– Aktiviert (A) – Benutzerrechte 1-4, 15
– Leer (-) – Benutzerrechte 5-14

Auswahl:
– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer Melder in Bereichen um das Bedienteil und in den Benutzerrechten des Benutzers enthaltenen Bereichen übergehen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Einen Melder übergehen

10.4.27 Unbypass a Point (Einen Melder einschalten)

Standardeinstellung:
– Aktiviert (A) – Benutzerrechte 1-4, 15
– Leer (-) – Benutzerrechte 5-14

Auswahl:
– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer das Übergehen von Meldern in Bereichen um das Bedienteil und in den Benutzerrechten des Benutzers enthaltenen Bereichen aufheben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Übergehen eines Melders aufheben

10.4.28 Melder zurücksetzen

Standardeinstellung:
– Aktiviert (A) – Benutzerrechte 1-4, 15
– Leer (-) – Benutzerrechte 5-14

Auswahl:
– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer Melder zurücksetzen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Melder zurücksetzen

10.4.29 Ausgänge ändern

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1, 2, 15
– Leer (-) – Benutzerrechte 3-14

Auswahl:
– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer Ausgänge manuell einstellen und zurücksetzen. Verwenden Sie die Funktion CHANGE OUTPUTS nicht, um für spezielle Funktionen reservierte Ausgänge ein- und auszuschalten. Ausgänge für spezielle Funktionen sind die Ausgangsfunktionen „Area“ und „Panel Wide“ (Zentralenweit) sowie die im Ausgang „Enter Key“ (Eingabetaste) zugewiesenen Ausgänge.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Ausgänge ändern

10.4.30 Fernparametrierung

Standardeinstellung:
– Aktiviert (A) – Benutzerrechte 1-4, 15
– Leer (-) – Benutzerrechte 5-14

Auswahl:
– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer Fernparametrier-Sitzungen starten. Falls Benutzer diese Funktion starten, wenn die gemeinsam mit der Zentrale genutzte Telefonleitung klingelt, übernimmt die Zentrale die Telefonleitung.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Berechtigungsstufen > Fernparametrierung

10.4.31 Go to Area (Gehe zu Bereich)

Standardeinstellung:
Aktiviert (A) – Benutzerrechte 1, 2, 15
Leer (-) – Benutzerrechte 3-14

Auswahl:
– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Diese Funktion weist Bedienteile vorübergehend einem anderen Bereich zu.
Benutzer sind auf Funktionen entsprechend ihren Benutzerrechten für den Bereich beschränkt, dem das Bedienteil vorübergehend zuwiesen ist.
Nach 15 Sekunden ohne Benutzeraktivität am Bedienteil wird das Bedienteil wieder in seinen zugewiesenen Bereich zurückversetzt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Gehe zu Bereich

10.4.32 Typ und Version des Anzeigetableaus

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1, 15
– Leer (-) – Benutzerrechte 2-14

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer die Firmware-Version der Zentrale anzeigen. Bedienteile zeigen die Firmware-Version im folgenden Format: ##.##.###.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Benutzerrechte > Typ und Version des Anzeigetableaus

10.4.33 Change Skeds (Zeitgesteuerte Ereignisse ändern)

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1, 15
– Leer (-) – Benutzerrechte 2-14

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer zeitgesteuerte Ereignisse ändern (bearbeiten). Die Bearbeitung zeitgesteuerter Ereignisse kann durch Einstellen des Parameters unter „Schedules > Skeds > *Zeitbearbeitung, Seite 266*“ (Zeitpläne > Zeitgesteuerte Ereignisse > Zeitbearbeitung) auf „No“ (Nein) eingeschränkt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Benutzerrechte > Zeitgesteuerte Ereignisse ändern

10.4.34 Benutzerdefinierte Funktion

Standardeinstellung:

– Aktiviert (A) – Benutzerrechte 1
– Leer (-) – Benutzerrechte 2-15

Auswahl:

– Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
– Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer benutzerdefinierte Funktionen verwenden.

Hinweis!

Die Zugriffsberechtigung für benutzerdefinierte Funktionen überschreibt die Berechtigung für die enthaltenen Benutzerfunktionen

Wenn ein Benutzer über das Bedienteilmenü keine Berechtigung für eine Funktion besitzt, wird nicht verhindert, dass die Funktion innerhalb einer benutzerdefinierten Funktion ausgeführt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
B9512: Benutzerkonfiguration > Benutzerrechte > Benutzerdefinierte Funktion 128 (bis 159)
B8512: Benutzerkonfiguration > Benutzerrechte > Benutzerdefinierte Funktion 128 (bis 135)
B6512: Benutzerkonfiguration > Benutzerrechte > Benutzerdefinierte Funktion 128 (bis 133)
B5512: Benutzerkonfiguration > Benutzerrechte > Benutzerdefinierte Funktion 128 (bis 131)
B4512: Benutzerkonfiguration > Benutzerrechte > Benutzerdefinierte Funktion 128 (und 129)
B3512: Benutzerkonfiguration > Benutzerrechte > Benutzerdefinierte Funktion 128

10.4.35 Erzwungenes Scharfschalten

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1-6
- Leer (-) – Benutzerrechte 7-15

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer das Scharfschalten der Zentrale erzwingen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Zwangsläufige Scharfschaltung

10.4.36 Sendebereich öffnen/schließen

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1-14
- Leer (-) – Benutzerrechte 15

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Dieser Parameter ermöglicht das Öffnen und Schließen von Protokollen für Benutzer in Bereichen, die in den Benutzerrechten des Benutzers enthalten sind.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Öffnen/Schließen des Sendebereichs

10.4.37 Eingeschränkt öffnen/schließen

Standardeinstellung: Leer (-) für alle Berechtigungsstufen

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Dieser Parameter beschränkt das Öffnen und Schließen von Protokollen für Benutzer in Bereichen, die in den Benutzerrechten des Benutzers enthalten sind. Die Zentrale sendet Öffnungsprotokolle nur bei aktivem Alarmsignal, wenn der Benutzer die Scharfschaltung aufhebt. Die Zentrale sendet Schließprotokolle nur, wenn der Benutzer Scharfschaltungen erzwingt oder umgeht.

Bereiche, denen diese Benutzerrechte zugeordnet sind, müssen für eingeschränkte Öffnungen und Schließungen parametriert werden (siehe Bereichsübergreifende Parameter > *Restricted O/C (Eingeschränkt öffnen/schließen), Seite 138*).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Eingeschränkt öffnen/schließen

10.4.38 Außenhautüberwachung öffnen/schließen

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1-14
- Leer (-) – Benutzerrechte 15

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Dieser Parameter ermöglicht das Öffnen und Schließen von Protokollen, wenn Benutzer die Außenhautüberwachung scharfschalten und dies für Benutzer in Bereichen aufheben, die in den Benutzerrechten des Benutzers enthalten sind.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Außenhautüberwachung öffnen/schließen

10.4.39 Bedrohung senden

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 14
- Leer (-) – Benutzerrechte 1-13, 15

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Dieser Parameter ermöglicht Bedrohungsprotokolle für Benutzer, wenn der Parameter „Area Parameters > Duress Enable“ (Bereichsparameter > Bedrohungsalarm aktivieren) für die in den Benutzerrechten des Benutzers enthaltenen Bereiche auf „Yes“ (Ja) gesetzt ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Bedrohungsalarm senden

10.4.40 Scharfschaltung durch Zugangscode

Standardeinstellung:
Aktiviert (A) – Benutzerrechte 1-6
Leer (-) – Benutzerrechte 7-15

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer ihren Zugangscode eingeben, um Bereiche innerhalb des Umfangs des Bedienteils und die in den Benutzerrechten des Benutzers enthaltenen Bereiche scharfzuschalten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Scharfschaltung durch Zugangscode

10.4.41 Scharfschaltung durch Zugangscode aufheben

Standardeinstellung:
Aktiviert (A) – Benutzerrechte 1-5, 14
Leer (-) – Benutzerrechte 6-13, 15

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer ihren Zugangscode eingeben, um die Scharfschaltung für Bereiche innerhalb des Umfangs des Bedienteils und die in den Benutzerrechten des Benutzers enthaltenen Bereiche aufzuheben.

Profil für Aufheben der Scharfschaltung einer Bedrohung
Zugriffsberechtigungsebene 14 ist standardmäßig als Profil für Aufheben der Scharfschaltung einer Bedrohung parametriert. Wenn „Duress Type“ (Bedrohungstyp) auf 3 festgelegt ist, wird die mit SIA CP-01 konforme Funktion „Duress Passcode“ (Bedrohungs-Zugangscode) aktiviert. Die Bedrohungstypen 1 und 2 sind in mit SIA CP-01 konformen Installationen nicht zulässig. Wenn Benutzerrechte 14 einem Zugangscode in einem Bereich zugeordnet sind, besitzt dieser Benutzer die Berechtigung zum Unscharfschalten und sendet ein Bedrohungsereignis aus diesem Bereich.
Alle für Bedrohungsalarme fähigen Zugangscodes müssen eindeutig sein und können nicht von anderen Zugangscodes abgeleitet werden. Um diese Einzigartigkeit zu erleichtern, ist die Zugriffsberechtigungsstufe 14 ab Werk als Beispiel für eine Berechtigung zum Aufheben der Scharfschaltung einer Bedrohung vorparametriert.
Eine Zugriffsberechtigung zum Aufheben der Scharfschaltung einer Bedrohung erfordert die Aktivierung der folgenden Funktionen:
- Benutzerkonfiguration > Benutzerrechte > Unscharfschalten
- Benutzerkonfiguration > Benutzerrechte > Bedrohungsalarm senden
- Und diesen Parameter „Disarm by Passcode“ (Scharfschaltung durch Zugangscode aufheben)

Legen Sie für „Area Wide Parameters > Duress Enable“ (Bereichsübergreifende Parameter > Bedrohungsalarm aktivieren) in den entsprechenden Bereichen „Yes“ (Ja) fest. Andernfalls reagiert das Bedienteil mit „No Authority“ (Keine Berechtigung).

Weitere Informationen
- *Auswahl unscharfschalten, Seite 193*
- *Bedrohung senden, Seite 206*

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Scharfschaltung durch Zugangscode aufheben

10.4.42 Sicherheitsstufe

Standardeinstellung:
- Vollscharfschaltung aktiv (A) – Benutzerrechte 1, 2
- Außenhautüberwachung (H) – Benutzerrechte 3-5
- Unscharfgeschaltet (U) – Benutzerrechte 6
- Kein Zugriff (-) – Benutzerrechte 7-15

Auswahl:

- Vollscharfschaltung aktiv (A) – Benutzer besitzen Zugriffsrechte für diesen Bereich, wenn der Bereich einen scharfgeschalteten Zustand aufweist.
- Außenhautüberwachung (H) – Benutzer besitzen Zugriffsrechte für diesen Bereich bei aktiver Außenhautüberwachung oder Unscharfschaltung, aber nicht bei Vollscharfschaltung des Bereichs.
- Unscharf (U) – Benutzer besitzen nur Zugriffsrechte für diesen Bereich, wenn er unscharf geschaltet ist.
- Kein Zugriff (-) – Benutzer besitzen keine Zugriffsrechte auf diesen Bereich.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Sicherheitsstufe

10.4.43 Unscharfschaltungsstufe

Standardeinstellung:
Unscharfschalten (U) – Benutzerrechte 1-5
Keine Rechte zum Unscharfschalten (-) – Benutzerrechte 6-15
Auswahl:

- Gesamtscharfschaltung oder Teilscharfschaltung nach Teilscharfschaltung, Unverzögert (U) – Wenn Benutzer ihre Zutritts-Codierung (Karte oder Codierschlüssel) vorzeigen und für den Bereich die verzögerte (oder unverzögerte) Gesamtscharfschaltung oder die verzögerte Teilscharfschaltung aktiviert ist, wechselt der Bereich zu „Unverzögerte Teilscharfschaltung“. Der Parameter Benutzerrechte > Sicherheitsstufe muss für den Bereich auf Gesamtscharfschaltung aktiv (A) eingestellt werden.
- Unscharfschalten (U) – Wenn Benutzer ihre Zutritts-Codierung (Karte, Codierschlüssel oder Zugangscode bei Einstellung „Ansteuerung Türöffner“ der Zugangscodeeingabefunktion am Bedienteil) vorzeigen und für den Bereich die verzögerte (oder unverzögerte) Gesamtscharfschaltung oder die verzögerte (oder unverzögerte) Teilscharfschaltung aktiviert ist, wechseln die Bereiche im Umfang des Bedienteils und die in den Benutzerrechten des Benutzers enthaltenen Bereiche zu „Unscharf“.
- Kein Unscharfschalten (-) – Benutzer können ihre Zutritts-Codierung (Karte oder Codierschlüssel) zum Aufheben der Scharfschaltung nicht vorzeigen.

Weitere Informationen über die Parametrierung dieser Aufforderung für einen gemeinsamen Bereich finden Sie im Abschnitt Zutrittskontrollleser, die dem gemeinsam benutzten Bereich zugewiesen sind für die Aufforderung *Bereichstyp, Seite 129* in den Bereichsparametern.

Hinweis!
Sirenen werden stummgeschaltet, wenn der Benutzer Codierschlüssel/Karte vorzeigt
Sirenen werden stummgeschaltet, wenn ein Benutzer einen Codierschlüssel, eine Karte oder einen Zugangscode bei Konfiguration von „Ansteuerung Türöffner“ vorzeigt.
Sirenen werden im lokalen Bereich stummgeschaltet, wenn ein Benutzer mit einem Codierschlüssel, einer Karte oder einem Zugangscode bei Konfiguration von „Ansteuerung Türöffner“ eine Unscharfschaltung durchführt oder während eines Alarms einen Codierschlüssel, eine Karte oder einen Zugangscode bei Konfiguration von „Ansteuerung Türöffner“ vorzeigt. Der Benutzer muss einen Zugangscode verwenden, um einen Feueralarmsignalgeber stummzuschalten. Protokollabbrüche werden gesendet, nachdem der Alarm durch einen gültigen Zugangscode oder einen Codierschlüssel/eine Karte stummgeschaltet wurde.

Hinweis!

Benutzerrechte 15 reserviert

Benutzerrechte 15 sind für den Service-Zugangscode (Benutzer 0) reserviert. Sie können keine Einstellungen in der Spalte „Benutzerrechte 15“ ändern.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Benutzerrechte > Unscharfschaltungsstufe

10.4.44 Funktionsebene

Standardeinstellung:

- Unscharfgeschaltet (U) – Benutzerrechte 1
- Keine Funktionsebene (-) – Benutzerrechte 2-15

Auswahl:

- Vollscharfschaltung (A) – Die benutzerdefinierte Funktion, die der Tür in diesem Bereich zugeordnet ist, wird aktiviert, wenn sich der Bereich im Zustand „Vollscharfschaltung” oder „Außenhautüberwachung“ befindet.
- Unscharfschaltung (D) - Die benutzerdefinierte Funktion, die der Tür in diesem Bereich zugeordnet ist, wird aktiviert, wenn der Bereich unscharfgeschaltet wird.
- „Vollscharfschaltung“ und „Unscharfgeschaltet“ (C) – Die benutzerdefinierte Funktion, die der Tür in diesem Bereich zugeordnet ist, wird unabhängig vom Scharfschaltungszustand des Bereichs aktiviert.
- Keine Funktionsebene (-) – Benutzer können eine benutzerdefinierte Funktion in diesem Bereich nicht aktivieren.

Benutzern muss ein Zugangscode zugewiesen sein, um eine benutzerdefinierte Funktion mit einer Zugangskarte oder einem Codierschlüssel zu starten.

Benutzer benötigen nicht die Berechtigung „Sicherheitsstufe“ oder „Unscharfschaltungsstufe“, um eine benutzerdefinierte Funktion mit einer Zugangskarte oder einem Codierschlüssel zu starten.

Wenn Benutzer, die sowohl die Berechtigung „Unscharfschaltungsstufe“ als auch „Funktionsebene“ haben, sich mithilfe einer Zugangskarte oder eines Codierschlüssels authentifizieren, wird zuerst die Berechtigung „Unscharfschaltungsstufe“ und dann „Funktionsebene“ angewendet (der Bereich wird unscharfgeschaltet und dann beginnt die benutzerdefinierte Funktion).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Benutzerkonfiguration > Benutzerrechte > Funktionsebene

10.4.45 Funk-Handsender scharfschalten

Standardeinstellung:

- Aktiviert (A) – Benutzerrechte 1-6
- Leer (-) – Benutzerrechte 7-15

Auswahl:

- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter kann ein Benutzer die Bereiche, die in den Benutzerrechten enthalten sind, mit einem RADION Funk-Handsender scharfschalten.

Bei Verwendung eines RADION Funk-Handsenders ist der Bedrohungsbetrieb beim Scharfschalten nicht möglich.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Funk-Handsender scharfschalten

10.4.46 Funk-Handsender unscharfschalten

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1-6
- Leer (-) – Benutzerrechte 7-15

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter kann ein Benutzer die Bereiche, die in den Benutzerrechten enthalten sind, mit einem RADION Funk-Handsender unscharfschalten.
Bei Verwendung eines RADION Funk-Handsenders ist der Bedrohungsbetrieb beim Unscharfschalten nicht möglich.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Funk-Handsender unscharfschalten

10.4.47 Firmware-Aktualisierung

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1-6
- Leer (-) – Benutzerrechte 7-15

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Wenn eine lokale Berechtigung erforderlich ist, kann nur ein Sicherheitsbenutzer mit der Berechtigung „Firmware-Aktualisierung“ die Aktualisierung genehmigen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Benutzerkonfiguration > Benutzerrechte > Firmware-Aktualisierung

10.4.48 Stummschalten-Funktion

Standardeinstellung:
- Aktiviert (A) – Benutzerrechte 1 und 15
- Leer (-) – Benutzerrechte 2-14

Auswahl:
- Leer (-): Diese Funktion ist nicht für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.
- Aktiviert (A) – diese Funktion ist für Benutzer aktiviert, die diesen Benutzerrechten zugewiesen sind.

Mit diesem Parameter können Benutzer Störungstöne auf den Bedienteilen stummschalten.

11 Melder-

11.1 Melderzuweisungen

11.1.1 Quelle

Standardeinstellung:
- Eingebaute Meldereingänge 1 bis 8
- Nicht zugewiesen – alle anderen Melder

Auswahl:
- Nicht zugewiesen – nicht verwendete Melder.
- Octo-Eingang – Melder wird in einem B208-Octo-Eingangsmodul installiert.
- Funk – Der Melder wird in einem SDI2 Bus-HF-Empfänger installiert.
- Eingebaut – Melder wird in der Zentrale (Melder 1 bis 8) installiert.
- Ausgang – Melder wird in der Logik an den Ausgang mit derselben Nummer angeschlossen. Mit diesem Melder ist kein physisches Gerät verknüpft.
- Bedienteil – der Melder wird in einem SDI2-Bus-Bedienteil installiert.
- IP-Kamera – der Melder wird in einer IP-Kamera installiert.

Verwenden Sie diesen Parameter, um den physischen Geräten Melder zuzuweisen. Wenn eine Option deaktiviert ist, können Sie den Melder diesem Gerät nicht zuweisen.
Die Melderquelle für die Melder 1 bis 8 ist festgelegt, da „Eingebaut“ nicht geändert werden kann.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen > Quelle

11.1.2 Text (erste Sprache)

Standardeinstellung: Melder-Nr.

Auswahl:
- Bis zu 32 Zeichen – Leerzeichen vor, nach und innerhalb einer Text-Zeichenfolge werden als Text behandelt und sind im 32-Zeichen-Limit enthalten.

Geben Sie bis zu 32 Zeichen Text, Zahlen und Symbole ein, um den Melder zu beschreiben. Der Meldertext wird auf Bedienteilen angezeigt und ist in Melderprotokollen enthalten, die an den Bedienteilempfänger gesendet werden (nur Modem4-Protokollformat).
Auf den Bedienteilen werden die ersten 20 Zeichen angezeigt. Wenn der Text mehr als 20 Zeichen umfasst, läuft der vollständige Text einmal über die Anzeige. Drücken Sie die Escape-Taste, um den Text erneut einzublenden.

Einfügen der Meldernummer kann hilfreich sein
Das Einfügen der Meldernummer in den Meldertext kann für Benutzer hilfreich sein, wenn sie sich Ereignisse ansehen, Funktionen und Befehle initiieren und eine Fehlerbeseitigung durchführen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen > Text

11.1.3 Text (zweite Sprache)

Standardeinstellung: leer

Auswahl:
- Bis zu 32 Zeichen – Leerzeichen vor, nach und innerhalb einer Text-Zeichenfolge werden als Text behandelt und sind im 32-Zeichen-Limit enthalten.

Geben Sie bis zu 32 Zeichen Text, Zahlen und Symbole ein, um den Melder zu beschreiben. Der Meldertext wird auf Bedienteilen angezeigt und ist in Melderprotokollen enthalten, die an den Bedienteilempfänger gesendet werden (nur Modem4-Protokollformat).

Auf den Bedienteilen werden die ersten 20 Zeichen angezeigt. Wenn der Text mehr als 20 Zeichen umfasst, läuft der vollständige Text einmal über die Anzeige. Drücken Sie die Escape-Taste, um den Text erneut einzublenden.

Einfügen der Meldernummer kann hilfreich sein
Das Einfügen der Meldernummer in den Meldertext kann für Benutzer hilfreich sein, wenn sie sich Ereignisse ansehen, Funktionen und Befehle initiieren und eine Fehlerbeseitigung durchführen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen> Text in zweiter Sprache

11.1.4 Profil (Index)

Standardeinstellung:
- Rauchmelder (4) – Melder 1
- Außenhautüberwachung: Verzögerung (8) – Melder 2, Melder 3
- Innenbereich: Wegmelder (13) – Melder 4, Melder 5
- Außenhautüberwachung: Unverzögert (7) – Melder 6, Melder 7
- 24-Stunden: Unverzögert beim Öffnen/Kurzschließen (1) – Melder 8
- Deaktiviert (0) – alle anderen Melder

Auswahl:
- 0-20

Mit diesem Parameter können Sie für jeden Melder ein Melderprofil auswählen. Mit dem Melderprofil wird festgelegt, wie die Zentrale auf Änderungen am Melderstatus reagiert (offen, normal, Störung, fehlt, scharfgeschaltet, unscharfgeschaltet).
Wenn der Parameter „Melderquelle“ auf „Deaktiviert“ eingestellt und der Melder einem Profil zugeordnet ist, erstellt die Zentrale ein Ereignis MELDER FEHLT.
Wenn der Parameter „Melderquelle“ nicht auf „0“ eingestellt ist und das Melderprofil auf „Deaktiviert“ festgelegt ist, erstellt die Zentrale ein Ereignis ZUSÄTZLICHER MELDER.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen > Index

11.1.5 Beschreibung des Profils (Index)

Dieses Feld enthält den Inhalt des Parameters „Melderprofiltext“. Er dient nur als Referenz und kann hier nicht bearbeitet werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen > Beschreibung

11.1.6 Bereich

Standardeinstellung: 1
Auswahl:
- 1-4 - B5512
- 1-2 - B4512
- 1 - B3512

Um einen Melder einem Bereich zuzuweisen, geben Sie die Bereichsnummer ein.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen > Bereich

11.1.7 Entprellen

Standardeinstellung: 500 ms
Auswahl:

– 250 ms
– 500 ms
– 750 ms
– 1 s
– 1,25 s
– 1,50 s
– 1,75 s
– 2 s

... bis ...

– 6 s

Mit dem Parameter „Entprellen“ wird festgelegt, wie lange die Zentrale einen Melder überprüft, bevor eine Störung ausgelöst wird.
Bosch empfiehlt eine Eingabe von 500 ms oder höher. Legen Sie für den Innenbereich-Wegmelder den Parameter „Entprellen“ auf mindestens 750 ms fest.
Wenn als *Quelle, Seite 211* des Melders „Funk“, „IP-Kamera“ oder „Ausgang“ festgelegt ist, legt der Parametrierer den Parameter „Entprellen“ automatisch auf „-“ (Bindestrich) fest, um anzugeben, dass der Parameter nicht angewendet wird.
Informationen zum Festlegen dieses Parameters finden Sie in den Herstelleranweisungen des Geräts, das an den Melder angeschlossen ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen > Entprellen

11.1.8 Ausgang

Standardeinstellung: 0
Auswahl:

– 0 (deaktiviert), 1 bis 48 - B5512
– 0 (deaktiviert), 1 bis 28 - B4512
– 0 (deaktiviert), 1 bis 3 - B3512

Verwenden Sie diesen Parameter, um einen Ausgang zu aktivieren, wenn der Melder in den Alarmzustand übergeht. Der Ausgang wird bei einer Störung oder Errichterbedienung nicht aktiviert.
Der Ausgang wird bei einem Alarm-Wiederherstellungsereignis zurückgesetzt.

Hinweis!
Alte BFSK-Relais- oder Relais-Funktion
Die Melderzuweisungsparameter für viele alte Bosch-Zentralen umfassen einen BFSK-Relais- oder Relaisparameter für jeden Melder.
Sie können die BFSK-Relais-Funktion emulieren, indem Sie diesen Ausgangsparameter für mehrere Melder auf dieselbe Ausgangsnummer festlegen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen > Ausgang

11.1.9 RADION RFID (B810)

Standardeinstellung: - leer
Auswahl: 0, 11 - 167772156
Die RFID-Nummer (Radio Frequency Identification) ist eine eindeutige Nummer, die Funkkomponenten im Werk zugewiesen wird.
Wenn der Parameter „Melderquelle“ auf „Funk“ eingestellt ist, wird dieser RFID-Parameter auf „0“ festgelegt. Die RFID kann über einen SDI2 Bus-HF-Empfänger „automatisch erlernt“ oder hier eingegeben werden.

Die RFID kann bei einem Melderaustausch bearbeitet bzw. auf „0“ eingestellt werden, um einen HF-Melder zu deaktivieren.

Der Parametrierer erzwingt Funkgrenzwerte.
Durch das Festlegen des Parameters *Typ des Funkmoduls, Seite 290* auf „B810 RADION Wireless“ wird die Zentrale auf 1.512 Funkgeräte beschränkt: 1.000 Funk-Handsender, 504 Melder (der Parameter „Melderquelle“ ist auf „Funk“ festgelegt) und 8 Repeater.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen > RADION RFID (B810)

11.1.10 RADION-Gerätetyp

Standardeinstellung: Leer
Auswahl:
- Glasbruch
- Rauch
- Erschütterung
- Tür-/Fenster-Magnetkontakt
- Tür-/Fenster-Magnetkontakt, Unterputz
- Bewegungsmelder dual
- Infrarot-Bewegungsmelder
- Bewegungsmelder zur Deckenmontage
- Universalsender
- Geldscheinkontakt
- Vorhangbewegungsmelder
- CO-Melder
- Unsichtbarer Überfallalarm, eine Taste
- Unsichtbarer Überfallalarm, zwei Tasten
- Unsichtbarer Überfallalarm, feste Position
- Wärme

Jeder RADION-Gerätetyp umfasst vier Eingangsfunktionen. Siehe folgende Tabelle.

Gerätetyp	Eingangsfunktion 1	Eingangsfunktion 2	Eingangsfunktion 3	Eingangsfunktion 4
Glasbruch	Glasbruchmelder-Alarm	Nicht verwendet	Nicht verwendet	Nicht verwendet
Rauch	Rauchalarm	Nicht verwendet	Nicht verwendet	Nicht verwendet
Erschütterung	Reedalarm	Schleifeneingang	Vibrationsalarm	Nicht verwendet
Tür-/Fenster-Magnetkontakt	Reedalarm	Nicht verwendet	Nicht verwendet	Nicht verwendet
Tür-/Fenster-Magnetkontakt, Unterputz	Reedalarm	Nicht verwendet	Nicht verwendet	Nicht verwendet
Bewegungsmelder dual	Bewegungsmelder-Alarm	Nicht verwendet	Nicht verwendet	Nicht verwendet
Infrarot-Bewegungsmelder	PIR-Alarm	Nicht verwendet	Nicht verwendet	Nicht verwendet

Gerätetyp	Eingangsfunktion 1	Eingangsfunktion 2	Eingangsfunktion 3	Eingangsfunktion 4
Bewegungsmelder zur Deckenmontage	Bewegungsmelder-Alarm	Nicht verwendet	Nicht verwendet	Nicht verwendet
Universalsender	Reedalarm	Schleifeneingang	Nicht verwendet	Nicht verwendet
Geldscheinkontakt	Geldscheinkontakt-Alarm	Nicht verwendet	Nicht verwendet	Nicht verwendet
Vorhangbewegungsmelder	PIR-Alarm	Nicht verwendet	Nicht verwendet	Nicht verwendet
CO-Melder	CO-Alarm	Nicht verwendet	Nicht verwendet	Nicht verwendet
Unsichtbarer Überfallalarm, eine Taste	Nicht verwendet	Nicht verwendet	Nicht verwendet	Nicht verwendet
Unsichtbarer Überfallalarm, zwei Tasten	Nicht verwendet	Nicht verwendet	Nicht verwendet	Nicht verwendet
Unsichtbarer Überfallalarm, feste Position	Nicht verwendet	Nicht verwendet	Nicht verwendet	Nicht verwendet
Wärme	Hitzealarm	Nicht verwendet	Nicht verwendet	Nicht verwendet

Wenn Sie den Gerätetyp auswählen, können Sie die Eingangsfunktionen mit dem entsprechenden Kontrollkästchen im Dialogfeld aktivieren bzw. deaktivieren.
Der Parametrierer legt die Eingangsfunktionen auf ihren Standardwert fest, wenn sich der Funkkomponententyp ändert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen > RADION-Gerätetyp

11.1.11 Inovonics RFID (B820)

Standardeinstellung: k.a.
Optionen: 0 bis 167772156
Die RFID-Nummer (Radio Frequency Identification) ist eine eindeutige Nummer, die Funkkomponenten im Werk zugewiesen wird.
Wenn der Parameter „Melderquelle“ auf „Funk“ eingestellt ist, wird dieser RFID-Parameter auf „0“ festgelegt. Die RFID kann über einen SDI2 Bus-HF-Empfänger „automatisch erlernt“ oder hier eingegeben werden.
Die RFID kann bei einem Melderaustausch bearbeitet bzw. auf „0“ eingestellt werden, um einen HF-Melder zu deaktivieren.

Der Parametrierer erzwingt Funkgrenzwerte.
Wenn Sie den Parameter *Typ des Funkmoduls, Seite 290* auf „B820 Inovonics Wireless“ festlegen, wird die Zentrale auf 350 Funkkomponenten beschränkt, ohne Repeater. Die Summe aus der Anzahl der Melder (der Parameter „Melderquelle“ ist auf „Funk“ festgelegt) und der Anzahl der Funk-Handsender kann maximal 350 betragen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderzuweisungen > RFID (B820 Inovonics Wireless)

11.2 Melderabhängigkeit-Parameter

11.2.1 Melderabhängigkeit-Schaltuhr

Standardeinstellung: 20
Optionen: 5 bis 255 (Sekunden)
Mit diesem Parameter wird festgelegt, wie lange die Zentrale nach einer Störung bei der Melderabhängigkeit darauf wartet, dass bei einem zweiten Melder in derselben Melderabhängigkeitsgruppe eine Störung auftritt, bevor ein Meldergruppenabhängigkeit-Alarmereignis ausgelöst wird. Wenn innerhalb der Meldergruppenabhängigkeits-Zeit keine Störung bei einem zweiten Melder auftritt, wird kein Meldergruppenabhängigkeit-Alarmereignis generiert.
Verwenden Sie die Meldergruppenabhängigkeit-Funktion nur für Nicht-Feuermelder.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderabhängigkeit-Parameter> Melderabhängigkeit-Schaltuhr

11.3 Melderprofile

Mit Melderprofilen (Melderindexen) wird bestimmt, wie die Zentrale auf Änderungen an Meldern reagiert. Verwenden Sie die Parameter in diesem Abschnitt, um Melderprofile zu erstellen. Weisen Sie die Melderprofile den Meldern in „Melderzuweisungen“ zu.

11.3.1 Melderprofiltext (Erste Sprache)

Standardeinstellung:
- Melderprofil 1 – 24-Std. Unverz., Offen/Kurz (24-Stunden, unverzögert bei offen/kurzgeschlossen)
- Melderprofil 2 – 24-Std. Uns./Stumm beim Kurz. (24-Stunden, unsichtbar und stumm beim Kurzschließen)
- Melderprofil 3 – Handfeuermelder
- Melderprofil 4 – Rauchmelder
- Melderprofil 5 – Rauch m. Bestätig. (Rauchmelder mit Bestätigung)
- Melderprofil 6 – Klg.überw. – D192G (Klingelüberwachung für D192G)
- Melderprofil 7 – Unverzögerte Außenhautüberwachung
- Melderprofil 8 – Verzögerte Außenhautüberwachung
- Melderprofil 9 – Außh.:Unverz.,Lokal unscharfg., Summen (Außenhaut, unverzögert, Lokal, wenn unscharfgeschaltet, Summen)
- Melderprofil 10 – Innenbereich: Unverzögert
- Melderprofil 11 – Innenbereich: Verzögerung
- Melderprofil 12 – InnBr:Unverz.,Lokal unscharfg. (Innenbereich, unverzögert, Lokal, wenn unscharfgeschaltet)
- Melderprofil 13 – Innenbereich: Wegmelder
- Melderprofil 14 – Schlüsselschalter
- Melderprofil 15 – Schlüsseltaster
- Melderprofil 16 - Melder öffnen/schließen bei Störung
- Melderprofil 17 – Gas
- Melderprofil 18 – Gas-Errichterbedienung
- Melderprofil 19 – AUX-AC-Überwachung
- Melderprofil 20 – Außenhautüberwachung: Überwachungsmodus aus

Auswahl: Bis zu 24 alphanumerische Zeichen
Geben Sie einen Text von bis zu 24 Zeichen ein, um das Melderprofil zu beschreiben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Melderprofiltext

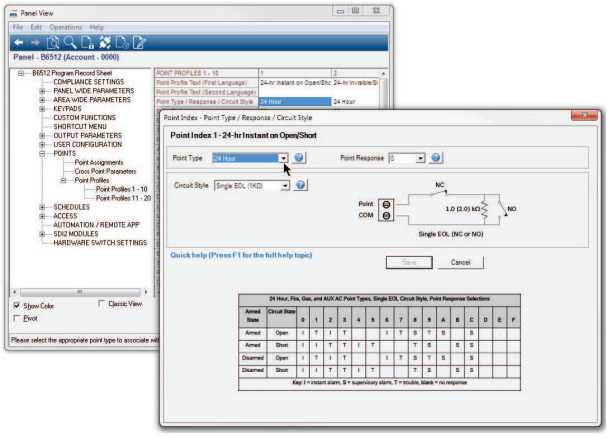
11.3.2 Melderprofiltext (Zweite Sprache)

Standardeinstellung: Leer
Auswahl: Bis zu 24 alphanumerische Zeichen
Geben Sie einen Text von bis zu 24 Zeichen ein, um das Melderprofil (Melderindex) zu beschreiben.

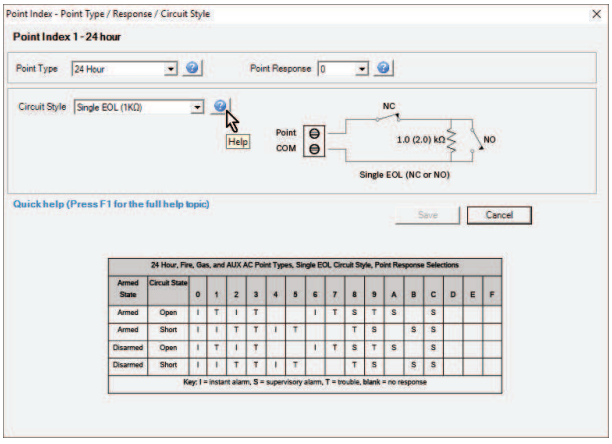
RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Melderprofiltext (zweite Sprache)

11.3.3 Melderart/Reaktion/Stromkreisbauweise

Wenn die Parameter für Melderart/Melderreaktion und Ausführungsform in einem einzigen Fenster angezeigt werden, können Sie die Interaktion zwischen den drei Parametern sehen.



Mit den beiden Parametern „Melderreaktion“ und „Melderart“ wird festgelegt, wie die Zentrale auf Änderungen an den Meldeleitungen (offen, kurz, normal) für verdrahtete Melder oder auf Melderstatusänderungen für Funkmelder (Fehler, normal, Störung) reagiert.
Informationen zu den einzelnen Parametern erhalten Sie, indem Sie auf die jeweiligen Hilfeschaltflächen im Fenster klicken.



11.3.4 Melderart

Standardeinstellung:

- 24-Stunden – Melderprofile 1-2, 6
- Außenhautüberwachung – Melderprofile 7-9, 20
- Innenbereich – Melderprofil 10-12
- Innenbereich: Wegmelder – Melderprofil 13
- Schlüsselschalter – Melderprofil 14
- Schlüsseltaster – Melderprofil 15
- Öffnen/Schließen-Melder – Melderprofil 16
- Feuermelder – Melderprofil 3-5
- AUX-AC-Überwachung – Melderprofil 19
- Gasmelder – Melderprofil 17, 18

Auswahl:

- **24 Stunden**

24-Stunden-Melder sind ständig scharfgeschaltet. Sie können für Notrufe, medizinische Alarme und Polizeialarme eingesetzt werden.
Wenn Sie einen 24-Stunden-Melder als abschaltbar konfigurieren (Parameter *Übergehen möglich, Seite 244* =„Ja“), legen Sie den Parameter *Summeralarm bei Fehler, Seite 240* auf „1“, „2“ oder „3“ und den Parameter *Übergehungsprotokoll beim Auftreten, Seite 244* auf „Ja“ fest (wenn ein Bereich nie scharfgeschaltet wird, werden keine verzögerten Umgehungsprotokolle gesendet).

Hinweis!
UL-Anforderung für Überfallgeräte
Verwenden Sie für Überfallgeräte in UL-Installationen die 24-Stunden-Melderart. Der Meldertext muss „Überfall“ enthalten.

Hinweis!
Brandschutztür, Dachluke und ähnliche Anwendungen
Für Brandschutztüren, Dachluken und ähnliche Anwendungen, die eine 24-Stunden-Überwachung benötigen, sollten Sie die Melderart „Außenhautüberwachung“ berücksichtigen. Für 24-Stunden-Melder wird nicht der Status „offen“ oder „gesperrt“ angezeigt, wenn ein Bereich scharfgeschaltet wird, für Melder mit Außenhautüberwachung aber schon.
Legen Sie den Parameter *Melderreaktion, Seite 223* auf „9“, „A“, „B“, „C“, „D“ oder „E“ fest.
Es kann sinnvoll sein, den Parameter „Summeralarm bei Fehler“ und den Parameter *Lokal, wenn unscharfgeschaltet, Seite 242* festzulegen.

- **Außenhautüberwachung**

Melder der Art „Außenhautüberwachung“ sind normalerweise der Außenseite der Räume (Türen und Fenster) zugewiesen.
Wenn ein Benutzer einen Bereich auf „Vollscharfschaltung” schaltet, werden die Melder „Außenhautüberwachung“, „Innenbereich“ oder „Wegmelder Innenbereich“ alle scharfgeschaltet.
Wenn ein Benutzer einen Bereich auf „Außenhautüberwachung” schaltet, werden nur die Melder „Außenhautüberwachung“ scharfgeschaltet. Die Melder „Innenbereich“ und „Wegmelder Innenbereich“ sind nicht scharfgeschaltet. In einem typischen System wird beim Schalten eines Bereichs auf „Außenhautüberwachung“ nur die Außenhautüberwachung scharfgeschaltet, sodass Benutzer in den Räumen bleiben können, ohne dass Innenbereichsmelder ausgelöst werden.

Mit dem Parameter „Melder“ > „Melderprofil“ > „Melderreaktion“ wird festgelegt, ob „Außenhautüberwachung” die Eingangsverzögerungszeit umfasst oder ob bei einer Störung sofort ein Alarm generiert wird.
Die Eingangsverzögerungszeit bietet Benutzern die Möglichkeit, ein Bedienteil zu erreichen und den Bereich unscharfzuschalten, ohne dass ein Alarm erzeugt wird. Wenn ein Benutzer beispielsweise die Außentür öffnet und den Melder „Außenhautüberwachung“ auslöst, beginnt die Eingangsverzögerungszeit. Der Benutzer muss zu einem Bedienteil gehen und den Bereich vor Ablauf der Scharfschalteverzögerungszeit unscharfschalten (Bereich ausschalten), damit kein Alarm ausgelöst wird.
Wenn für den Bereich eine Eingangsverzögerung vorliegt und ein zweiter Melder „Außenhautüberwachung“ ausgelöst wird, vergleicht die Zentrale die verbleibende Eingangsverzögerungszeit mit der für den zweiten Melder „Außenhautüberwachung“ parametrierten Eingangsverzögerungszeit. Wenn die Eingangsverzögerungszeit für den zweiten Melder kleiner als die verbleibende Zeit ist, wird die Eingangsverzögerungszeit gekürzt.

Hinweis!
Melder der Art „Außenhautüberwachung“ mit unverzögerter Melderreaktion erzeugen sofortige Alarme
Wenn Melder der Art „Sichtbarer Überfallalarm bei intern und extern scharf (mit Verzögerung)“ für eine unverzögerte *Melderreaktion, Seite 223* parametriert sind, wird bei einer Störung keine Eingangsverzögerungszeit gestartet. Sie generieren sofort einen Alarm, selbst bei einer Eingangs- oder Scharfschalteverzögerungszeit.

– **Innenbereich**

Innenbereichsmelder werden normalerweise verwendet, um Erkennungsgeräte für den Innenbereich zu überwachen, etwa Innentüren und Bewegungsmelder.
Innenbereichsmelder werden nur scharfgeschaltet, wenn der Bereich vollscharfgeschaltet ist. Sie werden nicht scharfgeschaltet, wenn für den Bereich die Außenhautüberwachung aktiv ist.
Mit dem Parameter „Melder“ > „Melderprofil“ > „Melderreaktion“ werden die Innenbereichsmelder für eine unverzögerte oder verzögerte Alarmreaktion konfiguriert.
Innenbereichsmelder werden normalerweise für eine unverzögerte Alarmreaktion konfiguriert.

Hinweis!
Innenbereichsmelder mit unverzögerter Melderreaktion erzeugen sofortige Alarme
Innenbereichsmelder, die für eine unverzögerte *Melderreaktion, Seite 223* parametriert sind, erzeugen bei einer Störung sofort einen Alarm, auch während einer Eingangs- oder Scharfschalteverzögerungszeit.

Wenn ein für eine verzögerte Alarmreaktion konfigurierter Innenbereichsmelder ausgelöst wird, während der Bereich komplett scharfgeschaltet ist, initiiert er eine Eingangsverzögerungszeit. Es wird kein Alarm erzeugt, sofern die Eingangsverzögerungszeit nicht abläuft, bevor der Bereich ausgeschaltet wird.
Wenn ein für eine verzögerte Melderreaktion parametrierter Innenbereichsmelder ausgelöst wird und die Eingangsverzögerungszeit bereits begonnen hat, vergleicht die Zentrale die verbleibende Eingangsverzögerungszeit mit der für den Innenbereichsmelder parametrierten Eingangsverzögerungszeit. Wenn die Eingangsverzögerungszeit für den Innenbereichsmelder kleiner als die verbleibende Zeit ist, kürzt die Zentrale die Eingangsverzögerungszeit.

Hinweis!
Verwenden Sie die Melderart *Wegmelder Innenbereich, Seite 252* **für den unverzögerten Alarm, wenn sich der Bereich nicht in der Eingangsverzögerung befindet.**
Für einige Installationen kann ein Innenbereichsmelder empfehlenswert sein, der von der Eingangsverzögerung abhängt, sie aber nicht initiiert.

– **Wegmelder Innenbereich**

Melder der Art „Wegmelder Innenbereich“ werden normalerweise verwendet, um Erkennungsgeräte für den Innenbereich zu überwachen, etwa Innentüren und Bewegungsmelder.
Melder der Art „Wegmelder Innenbereich“ werden nur scharfgeschaltet, wenn der Bereich vollscharfgeschaltet ist. Sie werden nicht scharfgeschaltet, wenn für den Bereich die Außenhautüberwachung aktiv ist.
Die Auslösung des Melders „Wegmelder Innenbereich“, während der Bereich komplett scharfgeschaltet ist, erzeugt einen unverzögerten Alarm. Wenn die Eingangsverzögerungszeit von einem anderen Melder gestartet wird, bevor der Melder „Wegmelder Innenbereich“ ausgelöst wird, verzögert der Melder „Wegmelder Innenbereich“ die Alarmreaktion, bis die Scharfschalteverzögerungszeit abläuft. Wenn der Bereich unscharfgeschaltet wird, bevor die Eingangsverzögerungszeit endet, wird kein Alarm erzeugt.
Wenn während der Scharfschalteverzögerung der Melder „Wegmelder Innenbereich“ ausgelöst wird, wird kein Alarm erzeugt.
Melder der Art „Wegmelder Innenbereich“ initiieren keine Eingangsverzögerung, selbst wenn sie für eine verzögerte Alarmreaktion konfiguriert sind (Parameter *Melderreaktion, Seite 223* ist auf „4“, „5“, „6“, „7“ oder „8“ festgelegt).

Hinweis!
Verwenden Sie die Melderart Innenbereich **und eine verzögerte Alarmreaktion für Innenbereichsmelder, die eine Eingangsverzögerung initiieren.**
Für einige Installationen empfiehlt sich ein Innenbereichsmelder, der eine Eingangsverzögerung initiiert. Wenn ein für eine verzögerte Alarmreaktion konfigurierter Innenbereichsmelder (siehe *Melderreaktion, Seite 223*) ausgelöst wird, während der Bereich komplett scharfgeschaltet ist, wird eine Eingangsverzögerung gestartet. Die Alarmreaktion wird verzögert, bis die Scharfschalteverzögerungszeit endet. Wenn der Bereich unscharfgeschaltet wird, bevor die Eingangsverzögerungszeit abläuft, gibt es keine Alarmreaktion.

– **Schlüsselschalter**

Schlüsselschalter-Melder werden zum Scharfschalten (Vollscharfschaltung) und Unscharfschalten von Bereichen verwendet.
Für Schlüsselschalter-Melder, wenn der Parameter „Melder“ > „Melderprofil“ > „Melderreaktion“ auf „1“ festgelegt ist:
- Wenn der Melderzustand **normal** ist, wird der Bereich unscharfgeschaltet („Aus“).
- Wenn der Melderzustand von „normal“ zu **offen** wechselt, wird der Bereich scharfgeschaltet (Vollscharfschaltung).
- Wenn der Melderzustand von „offen“ zu „normal“ wechselt, wird der Bereich unscharfgeschaltet („Aus“).
- Wenn der Melderzustand zu **Kurzgeschlossen** wechselt, wenn der Bereich scharfgeschaltet wird („Vollscharfschaltung“ oder „Außenhautüberwachung“), erstellt die Zentrale ein Melderalarmereignis. Wenn der Melderzustand zu „kurzgeschlossen“

wechselt, wenn der Bereich unscharfgeschaltet wird („Aus“), erstellt die Zentrale ein Melderstörungsereignis. Wenn der Melderzustand von „kurzgeschlossen“ zu „normal“ oder „offen“ wechselt, wird die Störung zurückgesetzt.

Für Schlüsselschalter-Melder, wenn der Parameter „Melder“ > „Melderprofil“ > „Melderreaktion“ auf „2“ festgelegt ist:

- Wenn der Melderzustand **offen** ist, wird der Bereich unscharfgeschaltet („Aus“).
- Wenn der Melderzustand von „offen“ zu **normal** wechselt, wird der Bereich scharfgeschaltet (Vollscharfschaltung).
- Wenn der Melderzustand von „normal“ zu „offen“ wechselt, wird der Bereich unscharfgeschaltet („Aus“).
- Wenn der Melderzustand zu **Kurzgeschlossen** wechselt, wenn der Bereich scharfgeschaltet wird („Vollscharfschaltung“ oder „Außenhautüberwachung“), erstellt die Zentrale ein Melderalarmereignis. Wenn der Melderzustand zu „kurzgeschlossen“ wechselt, wenn der Bereich unscharfgeschaltet wird („Aus“), erstellt die Zentrale ein Melderstörungsereignis. Wenn der Melderzustand von „kurzgeschlossen“ zu „normal“ oder „offen“ wechselt, wird die Störung zurückgesetzt.

Störungs- oder Wiederherstellungsprotokolle werden nicht gesendet, wenn der Parameter *Lokal, wenn unscharfgeschaltet, Seite 242* auf „Ja“ gesetzt ist.

Alarm- oder Wiederherstellungsprotokolle werden nicht gesendet, wenn der Parameter *Lokal, wenn scharfgeschaltet, Seite 242* auf „Ja“ festgelegt ist.

Hinweis!

Melderreaktion 2 ist erforderlich für die Inovonics FA113-Funkperipherie.

- **Schlüsseltaster**

Schlüsseltaster-Melder werden zum Scharfschalten (Vollscharfschaltung) und Unscharfschalten von Bereichen verwendet.

Legen Sie für Schlüsseltaster-Melder den Parameter „Melder“ > „Melderprofil“ > „Melderreaktion“ auf „1“ fest.

Wenn der Melderzustand des Schlüsseltaster-Melders von **normal** zu **kurzgeschlossen** zu **normal** geändert, wird der Scharfschaltzustand des Bereichs umgeschaltet.

Wenn der Melderzustand zu **offen** wechselt, wenn der Bereich scharfgeschaltet wird („Vollscharfschaltung“ oder „Außenhautüberwachung“), erstellt die Zentrale ein Melderalarmereignis. Wenn der Melderzustand zu **offen** wechselt, wenn der Bereich unscharfgeschaltet wird („Aus“), erstellt die Zentrale ein Melderstörungsereignis. Wenn der Melderzustand von „offen“ zu „normal“ wechselt, wird die Störung zurückgesetzt.

Störungs- oder Wiederherstellungsprotokolle werden nicht gesendet, wenn *Lokal, wenn unscharfgeschaltet, Seite 242* auf „Ja“ gesetzt ist.

Störungs- oder Wiederherstellungsprotokolle werden nicht gesendet, wenn *Lokal, wenn scharfgeschaltet, Seite 242* auf „Ja“ gesetzt ist.

- **Öffnen/Schließen-Melder**

Öffnen/Schließen-Melder werden unabhängig vom Bereich, dem sie zugeordnet sind, scharf- und unscharfgeschaltet.

Legen Sie für Öffnen/Schließen-Melder den Parameter „Melder“ > „Melderprofil“ > „Melderreaktion“ auf „1“ fest.

Wenn der Melderzustand von **kurzgeschlossen** zu **normal** wechselt, wird der Melder scharfgeschaltet. Die Zentrale sendet ein Protokoll MELDER WIRD GESCHLOSSEN.

Wenn der Melderzustand von **normal** zu **kurzgeschlossen** wechselt, wird der Melder unscharfgeschaltet. Die Zentrale sendet ein Protokoll MELDER WIRD GEÖFFNET.
Wenn der Melderzustand von **normal** zu **offen** wechselt, erstellt die Zentrale ein Alarmereignis.
Wenn der Melderzustand von **kurzgeschlossen** zu **offen** wechselt, erstellt die Zentrale ein Störungsereignis.

Protokolle MELDER WIRD GESCHLOSSEN werden nicht gesendet, wenn der Parameter *Lokal, wenn scharfgeschaltet, Seite 242* auf „Ja“ festgelegt ist.
Alarm- und Wiederherstellungsprotokolle werden nicht gesendet, wenn der Parameter *Lokal, wenn unscharfgeschaltet, Seite 242* auf „Ja“ festgelegt ist.
Protokolle MELDER WIRD GEÖFFNET werden nicht gesendet, wenn der Parameter *Lokal, wenn scharfgeschaltet, Seite 242* auf „Ja“ festgelegt ist.
Lokale Signalgeber werden über das Bedienteil stummgeschaltet.

– **Feuermelder**

Verwenden Sie Feuermelder, um Brandmelder zu überwachen.
Feueralarme sind in der Zentrale Ereignisse der höchsten Priorität.

– **AUX-AC-Überwachung**

Verwenden Sie AUX-AC-Überwachungsmelder, um die Stromquelle der zusätzlichen Stromversorgungsmodule zu überwachen.
Wenn der Melderzustand nicht-normal ist, wartet die Zentrale für die im Parameter „Netzstromausfallzeit“ eingestellte Zeit, bevor ein Melderstörungsereignis erstellt wird.
Für AUX-AC-Überwachungsmelder wird der Parameter *Melderreaktion, Seite 223* nicht verwendet. Es gibt keine Alarmereignisse für AUX-AC-Überwachungsmelder.
Wenn AUX-AC-Überwachungsmelder gesperrt werden, wird auf den Bedienteilen 24-STD.-MELDER UMGANGEN angezeigt.

– **Gasmelder**

Verwenden Sie Gasmelder, um Gaserkennungsgeräte zu überwachen.

– **Benutzerdefinierte Funktion**

Verwenden Sie Melder mit benutzerdefinierter Funktion, um benutzerdefinierte Funktionen zu aktivieren.
Verwenden Sie die Parameter im Bereich *Benutzerdefinierte Funktionen, Seite 160*, um benutzerdefinierte Funktionen zu konfigurieren.
Mit diesem Parameter wird die Melderart für das Melderprofil festgelegt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Melderart/Reaktion/Stromkreisbauweise

11.3.5 Übersicht über Melderreaktionen

Anwendungen für Melderreaktionen „9“, „T“ und „E“
Sie können die Melderreaktionen „9“, „T“ und „E“ mit der Melderart „Sichtbarer Überfallalarm bei intern und extern scharf (mit Verzögerung)“ kombinieren, um einen flexibleren 24-Stunden-Schutz zu schaffen. Anders als 24-Stunden-Melder wird ein offener Melder „Sichtbarer Überfallalarm bei intern und extern scharf (mit Verzögerung)“ mit einer Melderreaktion „D“ und „E“ bei der Scharfschaltung auf dem Bedienteil angezeigt. Wie ein 24-Stunden-Melder kann ein Melder, der auf diese Weise parametriert wurde, Alarme ausgeben, unabhängig davon, ob der Bereich scharf- oder unscharfgeschaltet ist.
Wenn die Melderreaktion 9 mit der Funktion „Lokal, wenn unscharfgeschaltet“ kombiniert wird, können Alarme an einem anderen Ort ausgegeben werden, wenn der Bereich scharfgeschaltet wird. Eine lokale Alarmankündigung erfolgt aber nur dann, wenn der Bereich unscharfgeschaltet wird.

Wenn die Melderreaktion 9 mit der Funktion „Lokal, wenn scharfgeschaltet“ kombiniert wird, können Alarme an einem anderen Ort ausgegeben werden, wenn der Bereich unscharfgeschaltet wird. Eine lokale Alarmankündigung erfolgt aber nur dann, wenn der Bereich scharfgeschaltet wird.
Die Melderreaktion E kann für grundlegende Bewegungsmelder verwendet werden. Dies ermöglicht die Protokollierung von Störungen, während die Zentrale vollscharfgeschaltet ist.
Bei der Melderreaktion F wird kein Ton auf lokalen Bedienteilen ausgegeben, aber der Ausgangsreaktionstyp und Bedienteilstörungen werden aktiviert. Um den nicht-normalen Zustand auf einem Bedienteil anzukündigen, legen Sie „Als Gerät anzeigen“ auf „Ja“ und/oder „Summeralarm bei Fehler“ auf „1“ oder „2“ fest. Bei dieser Melderreaktion werden keine Alarme generiert und kein Alarmausgang aktiviert.
Bei den Melderreaktionen 8, 9, A, B und C wird eine Protokollierung für die Errichterbedienung (24 Stunden) bereitgestellt.

Merkmale für Feuermelder

1. Protokollierung: Feuerprotokolle sind die ersten Ereignisse, die die Zentrale sendet, wenn eine Gruppe von Ereignissen auftritt.
2. Visuelle Ankündigung: Feuer-Störungen werden weiterhin eingeblendet, bis die Störung behoben ist. Nach der Reaktion wird eine FEUER-STÖRUNG eingeblendet, um den Benutzer wissen zu lassen, dass für einen Feuermelder oder eine Gruppe von Feuermeldern noch eine Störung vorliegt. Zentralenübergreifende Ausgänge mit einer Zusammenfassung Feuer und einer Zusammenfassung Feuer-Störung werden aktiviert, wenn ein Ausgang zugewiesen ist und für einen beliebigen Feuermelder ein Alarm oder eine Störung ausgelöst wird.
3. Hörbare Ankündigung: Ein Feuermelder aktiviert den Feueralarm. Dauer und Muster der Ansteuerung der Ausgänge werden durch den Bereich in „Branddauer“ und „Brandmuster“ parametriert.
4. Errichterbedienung: Ein Feuermelder kann ein Protokoll FEUER-ERRICHTERBEDIENUNG senden und die zentralenübergreifende Ausgänge „Zusammenfassung Feuer-Errichterbedienung“ und „Zusammenfassung Feuer-Störung“ mit einer Melderreaktion 8, 9, A, B, C aktivieren.
5. Alarmverifizierung: Ein Feuermelder kann einen Alarm um die Zeit verzögern, die in „Neustartzeit“ in den Bereichsparametern parametriert ist. In Kombination mit „Rücksetzbar“ setzt ein Feuermelder auch den elektrischen Stromkreis für die Zeitdauer zurück, die in „Neustartzeit“ angegeben ist.
6. Melder zurücksetzen: Ein Brandmelder, der zurückgesetzt werden muss, kann manuell mit dem Ausgang „Melder zurücksetzen“ für den Bereich zurückgesetzt werden, dem er zugewiesen ist.
7. Feuer-Funktionstest: Verwenden Sie die Funktion „Feuer-Funktionstest“, um Feuermelder innerhalb des Systems zu prüfen.

Um ein akustisches Signal auszugeben, wenn ein Melder mit Feuer-Errichterbedienung zurückgesetzt wurde, verwenden Sie „Ausgangsreaktionstyp“, und stellen Sie eine Verbindung zum grafischen Ankündigungsmodul her.
Sie sollten zuerst ein Feueransagegerät für alle Feuermelder zuordnen, wenn diese einem einzelnen Bereich in einem System mit mehreren Bereichen zugewiesen sind.

11.3.6 Melderreaktion

Standardeinstellung:

	Melderprofil

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Melderreaktion-Standardeinstellung	0	1	1	1	1	9	0	8	9	0

	Melderprofil									
	11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
Melderreaktion-Standardeinstellung	8	9	8	1	1	1	1	9	0	0

Auswahl: 0 bis 9, A bis F

Wenn die Parameter für Melderart/Melderreaktion und Ausführungsform in einem einzigen Fenster angezeigt werden, können Sie die Interaktion zwischen den drei Parametern sehen. Mit den beiden Parametern „Melderreaktion“ und „Melderart“ wird festgelegt, wie die Zentrale auf Änderungen an den Meldeleitungen (offen, kurzschluss, normal) für verdrahtete Melder oder auf Melderstatusänderungen für Funkmelder (Fehler, normal, Störung) reagiert.
Die folgenden Tabellen enthalten die Melderreaktionsoptionen für:

- 24 Stunden, Feuer, Gas und AUX-AC-Überwachung
- Gesteuerte Melderarten – „Außenhautüberwachung“, „Innenbereich“ oder „Wegmelder Innenbereich“
- Schlüsselschalter
- Schlüsseltaster
- Öffnen/Schließen-Melder
- Benutzerdefinierte Funktion

Hinweis!
Bei einer Melderartänderung wird die Melderreaktion automatisch in die Standardeinstellung geändert.
Bei Auswahl einer Melderart wird die Melderreaktion automatisch in die Standardeinstellung für diese Melderart geändert.

Optionen für die Melderarten 24 Stunden, Feuer, Gas und AUX-AC-Überwachung, Einzel-EOL, Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Öffnen	I	T	I	T			I	T	S	T	S		S			
Scharfgeschaltet	Short (Kurzgeschlossen)	I	I	T	T	I	T			T	S		S	S			
Unscharfgeschaltet	Öffnen	I	T	I	T			I	T	S	T	S		S			
Unscharfgeschaltet	Short (Kurzgeschlossen)	I	I	T	T	I	T			T	S		S	S			

Optionen für die Melderarten 24 Stunden, Feuer, Gas und AUX-AC-Überwachung, Einzel-EOL, Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Schlüssel: I = unverzögerter Alarm **S** = Errichterbedienungsalarm, **T** = Störung **leer** = keine Reaktion																	

Beispiel: Melderart = 24-Stunden und Melderreaktion = 8. 24-Stunden-Melder mit Errichterbedienungsreaktion beim Öffnen und Störungsreaktion beim Kurzschließen.

Optionen für die Melderarten 24 Stunden, Feuer, Gas, Dual-EOL-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Offen/ Kurzgeschlossen	T	I	T	I												
Scharfgeschaltet	Störung	I	I	S	S												
Unscharfgeschaltet	Offen/ Kurzgeschlossen	T	I	T	I												
Unscharfgeschaltet	Störung	I	I	S	S												
Schlüssel: I = unverzögerter Alarm **S** = Errichterbedienungsalarm, **T** = Störung **leer** = keine Reaktion																	

Beispiel: Melderart = 24-Stunden und Melderreaktion = 2. 24-Stunden-Melder mit Errichterbedienungsreaktion bei Störung und Störungsreaktion bei „offen“ oder „kurzgeschlossen“.

Optionen für die Melderarten 24 Stunden, Feuer, Gas, Einzel-EOL mit Sabotage-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Öffnen	TA	TA	TA	I	T			I	T							
Scharfgeschaltet	Short (Kurzgeschlossen)	I	T	TA	TA	TA	I	T									

Optionen für die Melderarten 24 Stunden, Feuer, Gas, Einzel-EOL mit Sabotage-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Unscharfgeschaltet	Öffnen	TA	TA	TA	I	T			I	T							
Unscharfgeschaltet	Short (Kurzgeschlossen)	I	T	TA	TA	TA	I	T									
Schlüssel: I = unverzögerter Alarm, **T** = Störung, **TA** = Sabotagealarm, **leer** = keine Reaktion																	

Beispiel: Melderart = 24-Stunden und Melderreaktion = 4. 24-Stunden-Melder mit Störungsreaktion beim Öffnen und Sabotagealarm beim Kurzschließen.

Optionen für die Melderarten 24 Stunden, Feuer, Gas, Dual-EOL mit Sabotage-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Offen/ Kurzgeschlossen	TA	TA	TA	TA												
Scharfgeschaltet	Störung	I	T	TA													
Unscharfgeschaltet	Offen/ Kurzgeschlossen	TA	TA	TA	TA												
Unscharfgeschaltet	Störung	I	T	TA													
Schlüssel: I = unverzögerter Alarm, **T** = Störung, **TA** = Sabotagealarm, **leer** = keine Reaktion																	

Beispiel: Melderart = 24-Stunden und Melderreaktion = 1. 24-Stunden-Melder mit Störungsreaktion bei Störung und Sabotagealarm bei „offen“ oder „kurzgeschlossen“.

Hinweis!
Anforderungen für Zentralen-Firmwareversion für Einzel-EOL mit Sabotage-Stromkreisbauweise und Dual-EOL mit Sabotage-Stromkreisbauweise.
Um einen Einzel-EOL mit Sabotage-Stromkreisbauweise oder einen Dual-EOL mit Sabotage-Stromkreisbauweise zu verwenden, stellen Sie sicher, dass die Version der Zentralen-Firmware v3.06 oder höher ist.

Hinweis!
Kaufen Sie für Dual-EOL-Stromkreisbauweisen separat ein zweites 1kΩ**-EOL-Modul.**
Bestellen Sie ICP-1K22AWG-10, eine Packung mit 10 Widerständen.

Hinweis!
Für Dual-EOL-Stromkreisbauweisen sind die Stromkreiszustände: „normal“, „Störung“, „kurzgeschlossen“, „offen“.
Normal – der im Schaltdiagramm angezeigte Schalter NC (Ruhekontakt) ist geschlossen.
Störung – der im Schaltkreis angezeigte NC-Schalter ist geöffnet.
Kurzgeschlossen – die Meldeleitung ist geschlossen.
Offen – die Meldeleitung ist offen

Hinweis!
Firmware-Anforderungen für Zentrale und B208 Octo-Eingang für Dual-EOL
Um die Dual-EOL-Stromkreisbauweise verwenden zu können, stellen Sie sicher, dass die Zentralen-Firmware v3.01 oder höher ist.
Wenn Sie ein B208-Octo-Eingangsmodul verwenden, stellen Sie sicher, dass die Modul-Firmware v2.1.1 oder höher ist.

Optionen: Melderarten 24 Stunden, Feuer, Gas, Stromkreisbauweise ohne EOL, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Störung	I	T	S													
Unscharfgeschaltet	Störung	I	T	S													
Schlüssel: I = unverzögerter Alarm **S** = Errichterbedienungsalarm, **T** = Störung **leer** = keine Reaktion																	

Beispiel: Melderart = 24-Stunden und Melderreaktion = 2. 24-Stunden-Melder mit Errichterbedienungsreaktion bei Störung und Störungsreaktion bei „offen“ oder „kurzgeschlossen“.

Hinweis!
Für die Stromkreisbauweise ohne EOL sind die Stromkreiszustände „normal“ und „Störung“,
und im Fenster „Melderdiagnose“ ist der Stromkreisstatus „offen“ oder „kurzgeschlossen“.
In den Tabellen mit den Melderreaktionen sind die Stromkreiszustände „normal“ und „Störung“ für die Stromkreisbauweise ohne EOL. Der Parameter *Normalzustand, Seite 250* definiert den Stromkreiszustand „Normal“ und „Störung“.
Für Melder mit Stromkreisbauweise ohne EOL wird im Fenster „Melderdiagnose“ in der Spalte für den Stromkreisstatus „offen“ oder „kurzgeschlossen“ angezeigt.

Optionen: Gesteuerte Melderarten, Einzel-EOL-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Öffnen	I	I	I	I	D	D	I	I	D	I	I	I	I	I	T	
Scharfgeschaltet	Short (Kurzgeschlossen)	I	I	I	I	I	I	D	D	D	I	I	I	I	I	I	
Unscharfgeschaltet	Öffnen		T		T				T		I	I	T	I		T	
Unscharfgeschaltet	Short (Kurzgeschlossen)			T	T		T				I	T	I		I		
Schlüssel: I = unverzögerter Alarm **D** = verzögerter Alarm **T** = Störung **leer** = keine Reaktion																	

Beispiel: Melderart = Außenhautüberwachung und Melderreaktion = 8. Melder „Sichtbarer Überfallalarm bei intern und extern scharf (mit Verzögerung)“ mit verzögerter Alarmreaktion bei Scharfschaltung (offen oder kurzgeschlossen) und keiner Reaktion beim Unscharfschalten.

Optionen: Gesteuerte Melderarten, Dual-EOL-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Offen/ Kurzgeschlossen	I	I	I	I	I	I	I	I								
Scharfgeschaltet	Störung	I	D	I	D	I	D	I	D								
Unscharfgeschaltet	Offen/ Kurzgeschlossen	T	T	I	I	T	T	I	I								
Unscharfgeschaltet	Störung					T	T	T	T								
Schlüssel: I = unverzögerter Alarm **D** = verzögerter Alarm **T** = Störung **leer** = keine Reaktion																	

Beispiel: Melderart = Außenhautüberwachung und Melderreaktion = 1. Wenn der Bereich scharfgeschaltet ist (Vollscharfschaltung, Außenhautüberwachung) wird bei einer Störung im Melder-Stromkreis eine verzögerte Alarmreaktion erzeugt. Ein offener oder kurzgeschlossener Melder-Stromkreis erzeugt einen unverzögerten Alarm.

Wenn der Bereich unscharfgeschaltet ist („Aus“), führt ein offener oder kurzgeschlossener Stromkreis zu einer Melderstörung. Es gibt keine Reaktion bei einer Störung im Melder-Stromkreis.

Optionen: Gesteuerte Melderarten, Einzel-EOL-Stromkreisbauweise mit Sabotagekontakt, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Öffnen	TA	TA	TA	TA	TA	TA	I	D	T	T	I	D				
Scharfgeschaltet	Short (Kurzgeschlossen)	I	D	T	T	I	D	TA	TA	TA	TA	TA	TA				
Unscharfgeschaltet	Öffnen	TA	TA	TA	TA	TA	TA				T	I	D				
Unscharfgeschaltet	Short (Kurzgeschlossen)				T	I	D	TA	TA	TA	TA	TA	TA				
Schlüssel: I = unverzögerter Alarm, **D** = verzögerter Alarm, **T** = Störung, **TA** = Sabotagealarm, **leer** = keine Reaktion																	

Beispiel: Melderart = Außenhautüberwachung und Melderreaktion = 3. Melder „Sichtbarer Überfallalarm bei intern und extern scharf (mit Verzögerung)“ mit Sabotagealarm, wenn offen (scharf- oder unscharfgeschaltet). Störungsreaktion bei Kurzschluss (scharfgeschaltet oder unscharfgeschaltet)

Optionen: Gesteuerte Melderarten, Dual-EOL-Stromkreisbauweise mit Sabotagekontakt, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Offen/ Kurzgeschlossen	TA	TA	TA	TA	TA	TA										
Scharfgeschaltet	Störung	I	D	I	D	T	T										
Unscharfgeschaltet	Offen/ Kurzgeschlossen	TA	TA	TA	TA	TA	TA										
Unscharfgeschaltet	Störung			T	T		I										
Schlüssel: I = unverzögerter Alarm, **D** = verzögerter Alarm, **T** = Störung, **TA** = Sabotagealarm, **leer** = keine Reaktion																	

Beispiel: Melderart = Außenhautüberwachung und Melderreaktion = 1. Melder „Sichtbarer Überfallalarm bei intern und extern scharf (mit Verzögerung)“ mit Sabotagealarm, wenn kurzgeschlossen oder offen (scharf- oder unscharfgeschaltet). Verzögerte Alarmreaktion für Störung (scharf- oder unscharfgeschaltet)

Hinweis!
Anforderungen für Zentralen-Firmwareversion für Einzel-EOL mit Sabotage-Stromkreisbauweise und Dual-EOL mit Sabotage-Stromkreisbauweise.
Um einen Einzel-EOL mit Sabotage-Stromkreisbauweise oder einen Dual-EOL mit Sabotage-Stromkreisbauweise zu verwenden, stellen Sie sicher, dass die Version der Zentralen-Firmware v3.06 oder höher ist.

Hinweis!
Kaufen Sie für die Dual-EOL-Stromkreisbauweise separat ein zweites 1kΩ**-EOL-Modul.**
Bestellen Sie ICP-1K22AWG-10, eine Packung mit 10 Widerständen.

Hinweis!
Für Dual-EOL-Stromkreisbauweisen sind die Stromkreiszustände: „normal“, „Störung“, „kurzgeschlossen“, „offen“.
Normal – der im Schaltdiagramm angezeigte Schalter NC (Ruhekontakt) ist geschlossen.
Störung – der im Schaltkreis angezeigte NC-Schalter ist geöffnet.
Kurzgeschlossen – die Meldeleitung ist geschlossen.
Offen – die Meldeleitung ist offen

Hinweis!
Firmware-Anforderungen für Zentrale und B208 Octo-Eingang für Dual-EOL
Um die Dual-EOL-Stromkreisbauweise verwenden zu können, stellen Sie sicher, dass die Zentralen-Firmware v3.01 oder höher ist.
Wenn Sie ein B208-Octo-Eingangsmodul verwenden, stellen Sie sicher, dass die Modul-Firmware v2.1.1 oder höher ist.

Optionen: Gesteuerte Melderarten, Stromkreisbauweise ohne EOL, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Störung	I	I	D	D	T											
Unscharfgeschaltet	Störung		T		T	T											
Schlüssel: I = unverzögerter Alarm **D** = verzögerter Alarm **T** = Störung **leer** = keine Reaktion																	

Beispiel: Melderart = Außenhautüberwachung und Melderreaktion = 2. Wenn der Bereich scharfgeschaltet ist (Vollscharfschaltung, Außenhautüberwachung) wird bei einer Störung im Melder-Stromkreis eine verzögerte Alarmreaktion erzeugt.
Wenn der Bereich unscharfgeschaltet („Aus“) ist, gibt es keine Reaktion bei einer Störung im Melder-Stromkreis.

Hinweis!
Für die Stromkreisbauweise ohne EOL sind die Stromkreiszustände „normal“ und „Störung“,
und im Fenster „Melderdiagnose“ ist der Stromkreisstatus „offen“ oder „kurzgeschlossen“.
In den Tabellen mit den Melderreaktionen sind die Stromkreiszustände „normal“ und „Störung“ für die Stromkreisbauweise ohne EOL. Der Parameter *Normalzustand, Seite 250* definiert den Stromkreiszustand „Normal“ und „Störung“.
Für Melder mit Stromkreisbauweise ohne EOL wird im Fenster „Melderdiagnose“ in der Spalte für den Stromkreisstatus „offen“ oder „kurzgeschlossen“ angezeigt.

Optionen: Schlüsselschalter-Melderart, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Öffnen			D													
Scharfgeschaltet	Short (Kurzgeschlossen)		I	I													
Unscharfgeschaltet	Öffnen		A														
Unscharfgeschaltet	Short (Kurzgeschlossen)		T	T													
Schlüssel: A = Beim Übergang von „Normal“ zu „Offen“ wird der Scharfschaltungszustand in „Scharfgeschaltet“ geändert, **D** = beim Übergang von „Normal“ zu „Offen“ wird der Scharfschaltungszustand in „Unscharfgeschaltet“ geändert, **I** = Unverzögerter Alarm, **T** = Störung, **leer** = keine Reaktion																	

Wenn die Melderreaktion auf „1“ eingestellt ist und der Schaltkreis des Melders normal ist, wird der Bereich unscharfgeschaltet (Aus). Wenn sich der Status des Melderstromkreises von „Normal“ zu „Offen“ ändert, wird der Bereich scharfgeschaltet (Vollscharfschaltung). Wenn sich der Status des Melderstromkreises von „Offen“ zu „Normal“ ändert, wird der Bereich unscharfgeschaltet (Aus).
Wenn die Melderreaktion auf „2“ eingestellt ist und der Schaltkreis des Melders normal ist, wird der Bereich scharfgeschaltet (Vollscharfschaltung). Wenn sich der Status des Melderstromkreises von „Normal“ zu „Offen“ ändert, wird der Bereich unscharfgeschaltet (Aus). Wenn sich der Status des Melderstromkreises von „Offen“ zu „Normal“ ändert, wird der Bereich scharfgeschaltet (Vollscharfschaltung).
Ein kurzgeschlossener Stromkreis führt zu einer Melderstörung, wenn der Bereich unscharfgeschaltet ist (Aus). Ein kurzgeschlossener Stromkreis führt zu einem unverzögerten Alarm, wenn der Bereich scharfgeschaltet ist. Wenn der Schaltkreis wieder zu „Normal“ oder „Offen“ zurückkehrt, wird die Störung zurückgesetzt.

Optionen: Schlüsseltaster-Melderart, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Öffnen		I														
Scharfgeschaltet	Short (Kurzgeschlossen)		D														
Unscharfgeschaltet	Öffnen		T														
Unscharfgeschaltet	Short (Kurzgeschlossen)		A														
Schlüssel: A = Beim Übergang von „Normal“ zu „Kurzgeschlossen“ zu „Normal“ wird der Scharfschaltungszustand in „Scharfgeschaltet“ geändert, **D** = beim Übergang von „Normal“ zu „Kurzgeschlossen“ zu „Normal“ wird der Scharfschaltungszustand in „Unscharfgeschaltet“ geändert, **I** = Unverzögerter Alarm, **T** = Störung, **leer** = keine Reaktion																	

Die Melderreaktion wird für die Schlüsseltaster-Melderart auf „1“ festgelegt. Wenn der Status des Melderstromkreises von „Normal“ zu „Kurzgeschlossen“ zu „Normal“ geändert wird, wird der Scharfschaltung des Bereichs umgeschaltet. Wenn der Bereich scharfgeschaltet ist (Vollscharfschaltung, Außenhautüberwachung), wird er unscharfgeschaltet (Aus). Wenn der Bereich unscharfgeschaltet ist, wird er scharfgeschaltet (Vollscharfschaltung).
Ein offener Stromkreis führt zu einer Melderstörung, wenn der Bereich unscharfgeschaltet ist (Aus). Ein offener Stromkreis führt zu einem unverzögerten Alarm, wenn der Bereich scharfgeschaltet ist (Vollscharfschaltung, Außenhautüberwachung). Wenn der Schaltkreis von „Offen“ wieder zu „Normal“ zurückkehrt, wird die Störung zurückgesetzt.

Optionen: Öffnen/Schließen-Melderart, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Öffnen		I														
Scharfgeschaltet	Short (Kurzgeschlossen)		D														
Unscharfgeschaltet	Öffnen		T														

Optionen: Öffnen/Schließen-Melderart, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Unscharfgeschaltet	Short (Kurzgeschlossen)		D														
Schlüssel: D = Beim Übergang von „Normal“ zu „Kurzgeschlossen“ wird der Scharfschaltungszustand in „Unscharfgeschaltet“ geändert (der Melder-Scharfschaltezustand ist „Scharfgeschaltet“, wenn der Melder-Stromkreisstatus „Normal“ ist), **I** = unverzögerter Alarm, **T** = Störung, **leer** = keine Reaktion																	

Die Melderreaktion wird für die Öffnen/Schließen-Melderart auf „1“ festgelegt.
Wenn sich der Status des Melderstromkreises in „Normal“ ändert, wird der Melder scharfgeschaltet. Die Zentrale sendet ein Melder-Schließprotokoll. Wenn sich der Status des Stromkreises von „Normal“ zu „Offen“ ändert, wird ein unverzögerter Melderalarm erzeugt. Wenn sich der Status des Melderstromkreises zu „Kurzgeschlossen“ ändert, wird der Melder unscharfgeschaltet. Die Zentrale sendet ein Melder-Schließprotokoll. Wenn sich der Status des Stromkreises von „Kurzgeschlossen“ zu „Offen“ ändert, wird eine Melderstörung erzeugt.

Optionen: Melderart mit benutzerdefinierter Funktion, Einzel-EOL-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Öffnen							CF	CF	T	CF		CF	CF	T	CF	
Scharfgeschaltet	Short (Kurzgeschlossen)						CF		CF	CF	T	CF		CF	CF	T	
Unscharfgeschaltet	Öffnen		CF	CF	T	CF		CF	CF	T	CF						
Unscharfgeschaltet	Short (Kurzgeschlossen)	CF		CF	CF	T	CF		CF	CF	T						
Schlüssel: CF = Zentrale führt benutzerdefinierte Funktion beim Übergang zum Stromkreiszustand aus. **T** = Störung, **leer** = keine Reaktion																	

Wenn sich der Status des Melderstromkreises ändert, reagiert die Zentrale mit dem Aufruf einer benutzerdefinierten Funktion.

Optionen: Melderart mit benutzerdefinierter Funktion, Dual-EOL-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Offen/ Kurzgeschlossen						T	T	T	T	T	T	T	T	T	T	
Scharfgeschaltet	Störung		T	CF		CF	CF	CF	CF	CF	CF	CF	CF	CF	CF	T	
Unscharfgeschaltet	Offen/ Kurzgeschlossen						T	T	T	T	T	T	T	T	T	T	
Unscharfgeschaltet	Störung		CF	T	CF		CF	CF	CF	T	CF	CF	CF	CF	CF	T	
Schlüssel: CF = Zentrale führt benutzerdefinierte Funktion beim Übergang zum Stromkreiszustand aus. **T** = Störung, **leer** = keine Reaktion																	

Wenn sich der Status des Melderstromkreises ändert, reagiert die Zentrale mit dem Aufruf einer benutzerdefinierten Funktion.

Optionen: Melderart mit benutzerdefinierter Funktion, Einzel-EOL mit Sabotage-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Öffnen	TA	TA	TA	TA	TA	CF	T	CF	CF							
Scharfgeschaltet	Short (Kurzgeschlossen)	CF	T	CF	CF		TA	TA	TA	TA	TA						
Unscharfgeschaltet	Öffnen	TA	TA	TA	TA	TA	CF	CF	T		CF						
Unscharfgeschaltet	Short (Kurzgeschlossen)	CF	CF	T		CF	TA	TA	TA	TA	TA						
Schlüssel: CF = Zentrale führt benutzerdefinierte Funktion beim Übergang zum Stromkreiszustand aus. **T** = Störung, **TA** = Sabotagealarm, **leer** = keine Reaktion																	

Wenn sich der Status des Melderstromkreises ändert, reagiert die Zentrale mit dem Aufruf einer benutzerdefinierten Funktion.

Optionen: Melderart mit benutzerdefinierter Funktion, Dual-EOL mit Sabotage-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Offen/ Kurzgeschlossen	TA	TA	TA	TA	TA											
Scharfgeschaltet	Störung	CF		CF	T	CF											
Unscharfgeschaltet	Offen/ Kurzgeschlossen	TA	TA	TA	TA	TA											
Unscharfgeschaltet	Störung		CF	CF	CF	T											
Schlüssel: CF = Zentrale führt benutzerdefinierte Funktion beim Übergang zum Stromkreiszustand aus. **T** = Störung, **TA** = Sabotagealarm, **leer** = keine Reaktion																	

Wenn sich der Status des Melderstromkreises ändert, reagiert die Zentrale mit dem Aufruf einer benutzerdefinierten Funktion.

Hinweis!
Anforderungen für Zentralen-Firmwareversion für Einzel-EOL mit Sabotage-Stromkreisbauweise und Dual-EOL mit Sabotage-Stromkreisbauweise.
Um einen Einzel-EOL mit Sabotage-Stromkreisbauweise oder einen Dual-EOL mit Sabotage-Stromkreisbauweise zu verwenden, stellen Sie sicher, dass die Version der Zentralen-Firmware v3.06 oder höher ist.

Hinweis!
Kaufen Sie für die Dual-EOL-Stromkreisbauweise separat ein zweites 1kΩ**-EOL-Modul.**
Bestellen Sie ICP-1K22AWG-10, eine Packung mit 10 Widerständen.

Hinweis!
Für Dual-EOL-Stromkreisbauweisen sind die Stromkreiszustände: „normal“, „Störung“, „kurzgeschlossen“, „offen“.
Normal – der im Schaltdiagramm angezeigte Schalter NC (Ruhekontakt) ist geschlossen.
Störung – der im Schaltkreis angezeigte NC-Schalter ist geöffnet.
Kurzgeschlossen – die Meldeleitung ist geschlossen.
Offen – die Meldeleitung ist offen

Hinweis!

Firmware-Anforderungen für Zentrale und B208 Octo-Eingang für Dual-EOL

Um die Dual-EOL-Stromkreisbauweise verwenden zu können, stellen Sie sicher, dass die Zentralen-Firmware v3.01 oder höher ist.

Wenn Sie ein B208-Octo-Eingangsmodul verwenden, stellen Sie sicher, dass die Modul-Firmware v2.1.1 oder höher ist.

Optionen: Melderart mit benutzerdefinierter Funktion, keine EOL-Stromkreisbauweise, Melderreaktion																	
Armed State (Scharfgeschalteter Zustand)	**Status des Stromkreises**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Scharfgeschaltet	Störung		T	CF		CF	CF	CF	CF	CF	CF	CF	CF	CF	CF	T	
Unscharfgeschaltet	Störung		CF	T	CF		CF	CF	CF	CF	CF	CF	CF	CF	CF	T	
Schlüssel: CF = Zentrale führt benutzerdefinierte Funktion beim Übergang zum Stromkreiszustand aus. **T** = Störung, **leer** = keine Reaktion																	

Wenn sich der Status des Melderstromkreises ändert, reagiert die Zentrale mit dem Aktivieren einer benutzerdefinierten Funktion.

Hinweis!

Für die Stromkreisbauweise ohne EOL sind die Stromkreiszustände „normal“ und „Störung“,

und im Fenster „Melderdiagnose“ ist der Stromkreisstatus „offen“ oder „kurzgeschlossen“.

In den Tabellen mit den Melderreaktionen sind die Stromkreiszustände „normal“ und „Störung“ für die Stromkreisbauweise ohne EOL. Der Parameter *Normalzustand, Seite 250* definiert den Stromkreiszustand „Normal“ und „Störung“.

Für Melder mit Stromkreisbauweise ohne EOL wird im Fenster „Melderdiagnose“ in der Spalte für den Stromkreisstatus „offen“ oder „kurzgeschlossen“ angezeigt.

Melderreaktion für B820 SDI2 Inovonics-Koppler

Wenn der Parameter „Melderquelle“ auf „Funk“ und der Parameter „Typ des Funkmoduls“ auf „B820 Inovonics Wireless“ festgelegt ist, senden die Funkmelder:

– „Kurzgeschlossen“ für Melderstörung (unabhängig vom Melderringleitungsstatus „Offen“/„Kurzgeschlossen“)
– „Offen“ für ein Sabotageereignis (Gehäuseabdeckung entfernt)

Melderreaktion für B810 RADION receiver SD

Wenn der Parameter „Melderquelle“ auf „Funk“ und der Parameter „Typ des Funkmoduls“ auf „B810 RADION Wireless“ festgelegt ist, senden Funkmelder:

– „Offen“ oder „Kurzgeschlossen“ für Melderstörung (elektrischer Zustand der Meldeleitung)
– „Kurzgeschlossen“ für Reedschalter (kein Magnet vorhanden)
– „Sabotage“ für ein Sabotageereignis (Gehäuseabdeckung entfernt)

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Melder > Melderindexe > Melderart/Reaktion/Stromkreisbauweise

Weitere Informationen
Melderart, Seite 218
Stromkreisbauweise, Seite 237

Siehe
– *Normalzustand, Seite 250*

11.3.7 Stromkreisbauweise

Standardeinstellung: Einzel-EOL (1 KΩ)
Auswahl:
– Einzel-EOL (1 KΩ)
– Einzel-EOL (2 KΩ)
– Dual-EOL (1 KΩ)
– Keine EOL
– Einzel-EOL (1 KΩ) mit Sabotagekontakt
– Einzel-EOL (2 KΩ) mit Sabotagekontakt
– Dual-EOL (1 KΩ) mit Sabotagekontakt

Wählen Sie die Stromkreisbauweise und den Leitungsabschlusswiderstand für die Meldeleitung aus.
Die Option „Einzel-EOL (1 KΩ)“ gilt für alle Melderquellen.
Die Option „Einzel-EOL (1 KΩ) mit Sabotagekontakt“ gilt nur für die Quellen „Octo-input (B208)“, „Integriert“, „Ausgang“, „Bedienteil“, „IP-Kamera“ und „Tür“.
Die Optionen „Einzel-EOL (2 KΩ)“, „Einzel-EOL (2KΩ) mit Sabotagekontakt“, „Dual-EOL (1 KΩ)“, „Dual-EOL (1 KΩ) mit Sabotagekontakt“ und „Keine EOL“ gelten nur für die Melderquellen „Integriert/Octo-Input (B208)“.

Hinweis!
Leitungsabschlusswiderstände für ZONEX-, Funk-, POPEX-Melder
Wenn der Parameter „MELDER“ > „Melderzuweisungen“ > „Quelle“ auf „ZONEX“, „Funk“ oder „POPEX“ festgelegt ist, legen Sie „Stromkreisbauweise“ auf „Einzel-EOL (1 KΩ)“ fest.
Obwohl „Stromkreisbauweise“ auf „Einzel-EOL (1 KΩ)“ festgelegt ist, ersetzen Sie die Leitungsabschlusswiderstände, die mit den ZONEX-, Funk-, POPEX-Meldern geliefert werden, **nicht** durch 1-kΩ-Leitungsabschlusswiderstände.

Hinweis!
Stromkreisbauweise – Firmwareanforderungen für Zentrale
Der Parameter „Stromkreisbauweise“ ist für die Zentralen-Firmware v2.xx nicht verfügbar.
Die Option des Dual-Leitungsabschlusswiderstands (1 KΩ) ist für die Zentralen-Firmware v3.01 und höher verfügbar.
Die Optionen „Einzel-EOL (2 KΩ)“ und „Keine EOL“ sind nur für die Zentralen-Firmware v3.03 und höher verfügbar.
Die Optionen „Einzel-EOL (1KΩ) mit Sabotagekontakt“, „Einzel-EOL (2 KΩ) mit Sabotagekontakt“ und „Dual-EOL (1 KΩ) mit Sabotagekontakt“ sind für die Zentralen-Firmware v3.06 und höher verfügbar.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Melderart/Reaktion/Stromkreisbauweise

Weitere Informationen
Melderart, Seite 218
Melderreaktion, Seite 223

11.3.8 Eingangsverzögerung

Standardeinstellung: 30 Sekunden

Optionen: 5 bis 600 Sekunden (5-Sekunden-Schritte)

Geben Sie die Anzahl der Sekunden der Eingangsverzögerungszeit ein. Die Eingangsverzögerung gibt dem Benutzer Zeit zum Unscharfschalten, bevor die Zentrale einen Alarm auslöst.

Wenn die Eingangsverzögerung endet, bevor der Benutzer den Bereich unscharfschaltet, löst die Zentrale einen Alarm aus.

Die Eingangsverzögerung beginnt, wenn ein Benutzer für einen Melder eine Störung auslöst, für den der Parameter *Melderart, Seite 218* auf „Außenhautüberwachung“, „Innenbereich“ oder „Wegmelder Innenbereich“ und der Parameter *Melderreaktion, Seite 223* auf „4“, „5“, „6“, „7“ oder „8“ festgelegt ist.

Wenn ein anderer Melder mit Verzögerung offen ist, während für den Bereich bereits die Eingangsverzögerung läuft, passt die Zentrale die Verzögerungszeit an die des Melders mit der kürzesten Rest-Eingangsverzögerung an.

Hinweis!

UL-Anforderung

Gemäß den UL-Standards darf die Gesamtzeit, die in „Eingangsverzögerung“ und *Alarmabbruch, Seite 247* eingegeben wird, eine Minute nicht überschreiten.

Hinweis!

SIA CP-01-Anforderung zur Fehlalarmunterdrückung

Zur Erfüllung von SIA CP-01 zur Fehlalarmunterdrückung legen Sie diesen Parameter für alle Melderprofile auf einen Wert zwischen 30 und 240 Sekunden fest. Weitere Informationen finden Sie unter „SIA CP-01 Verification” (SIA CP-01-Verifizierung).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Melder > Melderprofile > Eingangsverzögerung

11.3.9 Eingangston aus

Standardeinstellung: Nein (für alle Melderprofile)

Auswahl:

- Ja – Eingangston wird nicht gestartet, wenn für diesen Melder die Eingangsverzögerung beginnt.
- Nein – Eingangston wird gestartet, wenn für diesen Melder die Eingangsverzögerung beginnt.

Legen Sie diesen Parameter für Melder, die den Benutzer nach Betreten der Räume zum Unscharfschalten auffordern, nicht auf „Ja“ fest.

Um den Eingangston pro Bedienteil zu unterdrücken, legen Sie den Parameter „Bedienteile“ > „Bedienteilzuweisungen“ > *Entry Tone (Eingangston), Seite 149* auf „Nein“ fest.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Melder > Meldeprofile > Eingangston aus

11.3.10 Stilles Zutrittssignal

Standardeinstellung:

- Melderprofil 2 – Ja
- Alle anderen Melderprofile – Nein

Auswahl:

– Ja – Der stille Alarmausgang wird aktiviert, wenn für diesen Melder ein Alarm ausgelöst wird. Der Alarm-Signalgeber oder die Bedienteil-Alarm-Akustikmelder werden nicht aktiviert. Dieser Parameter hat keine Auswirkung auf Brand- und Gasmelder.
– Nein – Der stille Alarmausgang wird nicht aktiviert, wenn für diesen Melder ein Alarm ausgelöst wird.

Hinweis!
Der akustische Signalgeber wird nach zwei fehlgeschlagenen Versuchen am Bedienteilempfänger aktiviert.
Wenn Sie den Parameter *Hörbar nach 2 Fehlern, Seite 239* auf „Ja“ setzen, wird der *Alarm-Signalgeber, Seite 165* nach zwei Fehlversuchen aktiviert, um ein Stiller-Alarm-Protokoll an den Bedienteilempfänger zu senden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Stilles Zutrittssignal

11.3.11 Sabotagereaktion

Standardeinstellung: Immer Alarm
Auswahl:
– Immer Alarm – Alarme bei einer Meldersabotage sind immer hör- und sichtbar (Standardeinstellung).
– Alarm bei Unscharfschaltung – Alarme bei Meldersabotage sind immer still und unsichtbar, wenn der Meldebereich scharfgeschaltet ist (Standardeinstellung für CHI-Zentrale).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Option Melder > Melderprofile > Meldersabotage

11.3.12 Klingelzeichen bis Zurücksetzung

Standardeinstellung: Nein (für alle Melderprofile)

Auswahl:
– Ja – Feueralarm oder Gasalarm (und Akustikmelder des Bedienteils) können erst stummgeschaltet werden, wenn der Melder in den Normalzustand zurückgesetzt wird. Wenn der Melder zurückgesetzt wird und der Alarm nicht stummgeschaltet ist, wird der Alarm weiter ausgegeben, bis die Feuer- oder Gaszeit abläuft. Wenn der Melder nicht zurückgesetzt wird, wird die Alarmausgabe auch nach Ablauf der Feuer- oder Gaszeit fortgesetzt.
– Nein – Feueralarm oder Gasalarm (und Akustikmelder des Bedienteils) können stummgeschaltet werden, unabhängig davon, ober der Melder in den Normalzustand zurückgesetzt wird oder nicht. Wenn der Feueralarm oder Gasalarm nicht stummgeschaltet wird, wird die Alarmausgabe fortgesetzt, bis die Feuer- oder Gaszeit abläuft.

Verwenden Sie diesen Parameter für Feuer- oder Gasanwendungen, um die Voraussetzung zu erfüllen, dass akustische Alarme nicht stummgeschaltet werden können, bis die Störung zurückgesetzt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Klingelzeichen bis Zurücksetzung

11.3.13 Hörbar nach 2 Fehlern

Standardeinstellung: Nein (für alle Melderprofile)
Auswahl:

– Ja – Für stille Melder (Parameter „Stilles Zutrittssignal“ ist auf „Ja“ gesetzt) wird die Alarmausgabe nach zwei Fehlversuchen aktiviert, um ein Protokoll an den Bedienteilempfänger zu senden.
– Nein – Für stille Melder (Parameter „Stilles Zutrittssignal“ ist auf „Ja“ gesetzt) wird die Alarmausgabe nach zwei Fehlversuchen nicht aktiviert, um ein Protokoll an den Bedienteilempfänger zu senden.

Wenn ein stiller Melder (Parameter *Stilles Zutrittssignal, Seite 238* ist auf „Ja“ gesetzt) offen ist, beginnt die Einbruchalarmzeit sofort. Es kann bis zu drei Minuten dauern, bevor der zweite Versuch zum Senden eines Protokolls an den Bedienteilempfänger scheitert. Stellen Sie sicher, dass der Parameter *Burg Time (Einbruchalarmzeit), Seite 133* so festgelegt ist, dass diese 3 Minuten plus Anzahl der Minuten, für die der *Alarm-Signalgeber, Seite 165* ertönen soll, berücksichtigt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Hörbar nach 2 Fehlern

11.3.14 Unsichtbarer Melder

Standardeinstellung:
– Ja – Melderprofil 2
– Nein – Alle anderen Melderprofile

Auswahl:
– Ja – Auf den Bedienteilen wird für diesen Melder kein Alarm angezeigt. Kein Alarmton bei Bedienteilen. Auf den Bedienteilen werden Störungen angezeigt und Störungstöne erzeugt.
– Nein – Auf den Bedienteilen werden Alarme und Störungen angezeigt. Die Bedienteile erzeugen Alarm- und Störungstone für diesen Melder.

Dieser Parameter gilt nicht für Feuer- oder Gasmelder.
Um zu verhindern, dass der Bedienfeld-Alarmton und der *Alarm-Signalgeber, Seite 165* ertönen, können Sie für den Melder den Parameter *Stilles Zutrittssignal, Seite 238* auf „Ja“ festlegen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Unsichtbarer Melder

11.3.15 Summeralarm bei Fehler

Standardeinstellung:
– 1 – Melderprofil 9
– 0 – Alle anderen Melderprofile

Auswahl:
0 – „Summeralarm bei Fehler“ ist deaktiviert. Der Störungston wird nur ausgegeben, wenn beim Melder ein Störungszustand vorliegt.
1 – Der Störungston beginnt, wenn der Melder offen ist. Der Störungston kann erst stummgeschaltet werden, wenn der Melder in den Normalzustand zurückgesetzt wird.
2 – Der Störungston beginnt, wenn der Melder offen ist. Der Störungston kann erst stummgeschaltet werden, wenn der Melder in den Normalzustand zurückgesetzt wird.
3 – Der Störungston beginnt, wenn der Melder offen ist. Der Störungston wird automatisch stummgeschaltet, wenn der Melder in den Normalzustand zurückgesetzt wird. Der Störungston kann nicht stummgeschaltet werden, wenn der Melder offen ist.
Die Melderreaktionen „Unverzögerter Alarm“ (I), „Störung“ (T) und „Errichterbedienung“ (S) haben Priorität über „Summeralarm bei Fehler“. Wenn der Parameter für die Melderreaktion „leer“ ist, wird der Störungston nur durch den „Summeralarm bei Fehler“ gestartet. Unter

Melderreaktion, Seite 223 sind die verschiedenen Parameter aufgeführt. Dort finden Sie eine Beschreibung der Reaktionstypen für jede Melderart und dazu, wie sie vom scharfgeschalteten Zustand betroffen sind.
Wenn ein Alarm, eine Störung oder eine Errichterbedienung auftritt und eine Rückmeldung erfolgt, wird bei Option 1 und 3 von „Summeralarm bei Fehler“ der Störungston weiterhin ausgegeben, bis der Melder wieder in den Normalzustand zurückgesetzt wird.

Hinweis!
Dieser Parameter „Summeralarm bei Fehler“ gilt nicht für die Melderart „Benutzerdefinierte Funktion“.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Summeralarm bei Fehler

11.3.16 Überwachungsmelder

Standardeinstellung:
- Ja – Melderprofile 7 bis 8
- Nein – Alle anderen Melderprofile

Auswahl:
- Ja – Wenn sich die Zentrale im Überwachungsmodus befindet, sendet dieser Melder einen Überwachungston aus, wenn er offen ist.
- Nein – Dieser Melder sendet keinen Überwachungston aus, wenn er offen ist.

Sie hören den Überwachungston nur auf Bedienteilen, die demselben Bereich wie der Melder zugeordnet sind.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Überwachungsmelder

11.3.17 Ausgangsreaktionstyp

Standardeinstellung: 0

Auswahl:
- 0 -Deaktiviert, der Melderzustand hat keinen Einfluss auf die Funktion des zugehörigen Ausgangs.
- 1 – Wenn dieser Melder in einen anderen als den Normalzustand versetzt wird, wird der zugehörige Ausgang aktiviert. Der Ausgang wird automatisch zurückgesetzt, wenn der Melder zum Normalzustand zurückkehrt.
- 2 – Wenn für diesen Melder der Alarm ausgelöst wird, wird die zugehörige Ausgabe aktiviert. Der Ausgang bleibt aktiviert, bis der Alarm über das Bedienteil deaktiviert wird.

Mit diesem Parameter können Sie die Ausgänge konfigurieren, um ein gleichmäßiges Muster zu aktivieren, wenn ein zugehöriger Melder (mit derselben Nummer wie der Ausgang, beispielsweise Melder 8 und Ausgang 8) in einen anderen als den Normalzustand versetzt wird.
Legen Sie diesen Parameter auf „0“ fest, wenn der zugehörige Ausgang für eine andere Ausgangsfunktion konfiguriert ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Ausgangsreaktionstyp

11.3.18 Als Gerät anzeigen

Standardeinstellung: Nein

Auswahl:

– Ja – Auf Bedienteilen wird [GERÄT PRÜFEN] angezeigt, wenn dieser Melder sich nicht im Normalzustand befindet.
– Nein – Auf Bedienteilen wird nicht [GERÄT PRÜFEN] angezeigt, wenn dieser Melder sich nicht im Normalzustand befindet.

Verwenden Sie diese Funktion für Melder, die an einen Störungsausgang eines Geräts angeschlossen sind.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Als Gerät anzeigen

11.3.19 Lokal, wenn unscharfgeschaltet

Standardeinstellung:
– Ja – Melderprofil 9, 12
– Nein – Alle anderen Melderprofile

Auswahl:
– Ja – Wenn der Bereich unscharfgeschaltet ist, sendet die Zentrale keine Alarm-, Störungs- oder Wiederherstellungsprotokolle für diesen Melder.
– Nein – Die Zentrale sendet Alarm-, Störungs- oder Wiederherstellungsprotokolle für diesen Melder, wenn der Bereich unscharfgeschaltet ist.

Dieser Parameter hat keinen Einfluss auf Feuer- oder Gasmelder.
Legen Sie diesen Parameter für die Melderarten „Schlüsselschalter“, „Schlüsseltaster“ oder „Öffnen/Schließen“ nicht auf „Ja“ fest.
Legen Sie diesen Parameter für 24-Stunden-Melder nicht auf „Ja“ fest. 24-Stunden-Melder sind immer scharfgeschaltet.
Wählen Sie stattdessen eine gesteuerte Melderart aus. Verwenden Sie eine Melderreaktion, die einen Alarm sendet, unabhängig davon, ob der Melder scharfgeschaltet ist oder nicht.
Beispielsweise senden Melder, für die der Parameter *Melderart, Seite 218* auf „Außenhautüberwachung“ und der Parameter *Melderreaktion, Seite 223* auf „9“ festgelegt ist, einen Alarm bei einer Störung oder einem Kurzschluss (I), unabhängig davon, ob der Bereich scharfgeschaltet ist oder nicht.

Hinweis!
Ein Wiederherstellungsprotokoll wird auch gesendet, wenn der Bereich derzeit unscharfgeschaltet ist, aber scharfgeschaltet war, als der Alarm oder die Störung aufgetreten ist, und danach in den Normalzustand versetzt und unscharfgeschaltet wurde.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Lokal, wenn unscharfgeschaltet

11.3.20 Lokal, wenn scharfgeschaltet

Standardeinstellung: Nein

Auswahl:
– Ja – Wenn der Bereich scharfgeschaltet ist, sendet die Zentrale keine Alarm-, Störungs- oder Wiederherstellungsprotokolle für diesen Melder.
– Nein – Die Zentrale sendet Alarm-, Störungs- oder Wiederherstellungsprotokolle für diesen Melder, wenn der Bereich scharfgeschaltet ist.

Dieser Parameter hat keinen Einfluss auf Feuer- oder Gasmelder.
Legen Sie diesen Parameter für die Melderarten „Schlüsselschalter“, „Schlüsseltaster“ oder „Öffnen/Schließen“ nicht auf „Ja“ fest.
Legen Sie diesen Parameter für 24-Stunden-Melder nicht auf „Ja“ fest. 24-Stunden-Melder sind immer scharfgeschaltet.

Wählen Sie stattdessen eine gesteuerte Melderart aus. Verwenden Sie eine Melderreaktion, die einen Alarm sendet, unabhängig davon, ob der Melder scharfgeschaltet ist oder nicht. Beispielsweise senden Melder, für die der Parameter *Melderart, Seite 218* auf „Außenhautüberwachung“ und der Parameter *Melderreaktion, Seite 223* auf „9“ festgelegt ist, einen Alarm bei einer Störung oder einem Kurzschluss (I), unabhängig davon, ob der Bereich scharfgeschaltet ist oder nicht.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Lokal, wenn scharfgeschaltet

11.3.21 Wiederherstellungen deaktivieren

Standardeinstellung: Nein

Auswahl:

– Ja – Wiederherstellungsprotokolle werden für diesen Melder deaktiviert.
– Nein – Wiederherstellungsprotokolle werden für diesen Melder aktiviert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Wiederherstellungen deaktivieren

11.3.22 Zwangsläufige Scharfschaltung wiederherstellbar

Standardeinstellung: Nein

Auswahl:

– Ja – Wenn dieser Melder in den Normalzustand zurückkehrt, nachdem er zwangsläufig scharfgeschaltet wurde (zwangsläufige Melderübergehung), wird er automatisch in den scharfgeschalteten Zustand versetzt.
– Nein – Wenn dieser Melder in den Normalzustand zurückkehrt, nachdem er zwangsläufig scharfgeschaltet wurde (zwangsläufige Melderübergehung), bleibt er zwangsabgeschaltet.

Legen Sie diesen Parameter für Melder, die normalerweise offen sind, wenn der Bereich scharfgeschaltet wird, auf „Ja“ fest. Wenn dieser Melder in den Normalzustand zurückkehrt, nachdem er zwangsläufig scharfgeschaltet wurde (zwangsläufige Melderübergehung), wird er automatisch mit den anderen Meldern im Bereich in den scharfgeschalteten Zustand versetzt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Zwangsläufige Scharfschaltung wiederherstellbar

11.3.23 Übergehung wiederherstellbar

Standardeinstellung: Nein

Auswahl:

– Ja – Gesteuerte Melder mit einer Übergehung, Swinger-Übergehung oder Zwangsscharfschaltung werden automatisch wieder ohne Umgehung konfiguriert, wenn der Bereich unscharfgeschaltet wird.
– Nein – Gesteuerte Melder mit einer Übergehung, Swinger-Übergehung oder Zwangsscharfschaltung müssen mit der Bedienteilfunktion UNBYPASS? (ohne Umgehung) wieder eingeschaltet werden. Hierzu werden die Funktionen des zeitgesteuerten Ereignisses „Übergehung eines Melders aufheben“ oder „Alle Melder einschalten“ bzw. RPS verwendet.

Legen Sie diesen Parameter für Sperrmelder auf „Nein“ fest.
Um Melder zwangsläufig scharfgeschaltet (umgangen) zu lassen, wenn dieser Parameter auf „Nein“ gesetzt ist, legen Sie den Parameter *Zwangsläufige Scharfschaltung wiederherstellbar, Seite 243* auf „Nein“ fest.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Übergehung wiederherstellbar

11.3.24 Übergehen möglich

Standardeinstellung:
– Ja – Melderprofile 1, 7–13, 20
– Nein – Melderprofile 2–6, 14–19

Auswahl:
– Ja – Die diesem Profil zugeordneten Melder können umgangen und zwangsläufig scharfgeschaltet werden.
– Nein – Die diesem Profil zugeordneten Melder können nicht umgangen oder zwangsläufig scharfgeschaltet werden.

Auch wenn dieser Parameter auf „Nein“ festgelegt ist:
– Offene gesteuerte Melder werden am Ende des Schließen-Fensters zwangsläufig scharfgeschaltet, wenn der Parameter „Automatische Scharfschaltung“ auf „Ja“ eingestellt ist.
– Offene gesteuerte Melder werden zwangsläufig scharfgeschaltet, wenn der Bereich durch ein zeitgesteuertes Ereignis scharfgeschaltet wird.

Wenn ein 24-Stunden-Melder umgangen wird, läuft auf dem Bedienteil der Text 24-STUNDEN-ÜBERGEHUNG durch. Für umgangene Feuermelder läuft der Text FEUER-ÜBERGEHUNG durch. Für umgangene Gasmelder läuft der Text GAS-ÜBERGEHUNG durch.
Für eine 24-Stunden-Alarmreaktion ohne kontinuierliches Durchlaufen eines umgangenen 24-Stunden-Melders verwenden Sie den Melder „Außenhautüberwachung“ mit einer *Melderreaktion, Seite 223* von „9“ bis „E“.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Übergehen möglich

11.3.25 Swinger-Übergehung

Standardeinstellung: Nein

Auswahl:
– Ja – Die Swinger-Übergehung wird für diesen Melder aktiviert. Die Zentrale übergeht den Melder automatisch, wenn die Anzahl der Melderalarme oder Melderstörungen die Anzahl der Swinger-Übergehungen erreicht.
– Nein – Die Swinger-Übergehung wird für diesen Melder deaktiviert.

Bei jedem Melderalarm- oder Melderstörungsereignis wird der Ereigniszähler um 1 erhöht. Wenn der Bereich unscharfgeschaltet wird, wird der Ereigniszähler auf „0“ zurückgesetzt.
Die Zentrale sendet Swinger-Übergehungsprotokolle, wenn die *Anzahl der Mehrfachauslösungsumgehungen, Seite 111* erreicht wird und *Übergehungsprotokoll beim Auftreten, Seite 244* auf „Ja“ festgelegt ist.
Damit die Swinger-Übergehung funktioniert, darf der Parameter *Übergehen möglich, Seite 244* nicht auf „Ja“ festgelegt sein.
Wenn der Parameter *Übergehung wiederherstellbar, Seite 243* auf „Ja“ festgelegt ist, werden die Melder mit Swinger-Übergehung automatisch wieder ohne Übergehung konfiguriert, wenn der Bereich unscharfgeschaltet wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Swinger-Übergehung

11.3.26 Übergehungsprotokoll beim Auftreten

Standardeinstellung: Nein

Auswahl:

– Ja – Die Zentrale sendet ein Übergehungsprotokoll, wenn der Melder umgangen wird.
– Nein – Die Zentrale sendet für diesen Melder kein Übergehungsprotokoll.

Wenn dieser Parameter auf „Ja“ festgelegt ist, können Sie den Parameter *Übergehungsprotokoll verzögern, Seite 245* verwenden, um Übergehungsprotokolle für 24-Stunden-Melder zu senden, wenn der Bereich scharfgeschaltet ist, anstatt beim Auftreten des Ereignisses.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Übergehungsprotokoll beim Auftreten

11.3.27 Übergehungsprotokoll verzögern

Standardeinstellung: Nein

Auswahl:

– Ja – Die Zentrale sendet Übergehungsprotokolle für 24-Stunden-Melder, wenn der Bereich scharfgeschaltet ist.
– Nein – Die Zentrale sendet Übergehungsprotokolle für 24-Stunden-Melder, wenn die Melder umgangen werden.

Dieser Parameter hat keinen Einfluss auf Übergehungsprotokolle für gesteuerte Melder, Feuermelder oder Gasmelder.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Übergehungsprotokoll verzögern

11.3.28 Melderabhängigkeit

Standardeinstellung: Nein

Auswahl:

– Ja – Für diesen Melder besteht eine Meldergruppenabhängigkeit.
– Nein – Für diesen Melder besteht keine Meldergruppenabhängigkeit.

Wenn bei einer Meldergruppenabhängigkeit eine Störung vorliegt, startet die Zentrale die Meldergruppenabhängigkeit-Schaltuhr. Wenn bei einer anderen Meldergruppenabhängigkeit in derselben Meldergruppenabhängigkeits-Gruppe eine Störung auftritt, bevor die Meldergruppenabhängigkeit-Schaltuhr abläuft, erstellt die Zentrale Meldergruppenabhängigkeit-Alarmereignisse für beide Melder.
Wenn die Meldergruppenabhängigkeit, die die Meldergruppenabhängigkeit-Schaltuhr startet, wieder in den Normalzustand versetzt wird und bei einer anderen Meldergruppenabhängigkeit in derselben Meldergruppenabhängigkeits-Gruppe vor dem Ablauf der Schaltuhr keine Störung auftritt, erstellt die Zentrale ein unbestätigtes Ereignis (kein Meldergruppenabhängigkeit-Alarmereignis).
Wenn die Meldergruppenabhängigkeit, die die Meldergruppenabhängigkeit-Schaltuhr startet, wieder in den Normalzustand versetzt, dann offen ist und zurückgesetzt wird und bei einer anderen Meldergruppenabhängigkeit in derselben Meldergruppenabhängigkeits-Gruppe vor dem Ablauf der Schaltuhr keine Störung auftritt, erstellt die Zentrale ein unbestätigtes Ereignis (kein Meldergruppenabhängigkeit-Alarmereignis).
Wenn die Meldergruppenabhängigkeit, die die Meldergruppenabhängigkeit-Schaltuhr startet, offen bleibt, bis die Meldergruppenabhängigkeit-Schaltuhr abläuft, und bei einer anderen Meldergruppenabhängigkeit in derselben Meldergruppenabhängigkeits-Gruppe keine Störung auftritt, erstellt die Zentrale ein Melderalarmereignis (kein Meldergruppenabhängigkeit-Alarmereignis).
Die Meldergruppenabhängigkeit-Funktion gilt nur für Alarmereignisse. Sie gilt nicht für die Ereignisse „Errichterbedienung“ oder „Störung“.
Für die Meldergruppenabhängigkeit-Funktion müssen mindestens 2 Melder in der Gruppe eine Melderabhängigkeit haben.

Meldergruppenabhängigkeits-Gruppen können nicht konfiguriert werden. Jede Meldergruppenabhängigkeits-Gruppe enthält 8 Melder. Die Melder 1–8 befinden sich in der ersten Gruppe. Die Melder 9–16 befinden sich in der zweiten Gruppe usw. Die Meldergruppenabhängigkeiten in verschiedenen Meldergruppenabhängigkeits-Gruppen beeinflussen sich gegenseitig nicht.
Weisen Sie Meldergruppenabhängigkeiten in derselben Meldergruppenabhängigkeits-Gruppe demselben Melderprofil zu. Legen Sie den Parameter *Melderart, Seite 218* auf „Außenhautüberwachung“, „Innenbereich“ oder eine 4-Stunden-Melderart fest. Legen Sie für den Parameter *Melderreaktion, Seite 223* Parameter die Reaktion „Unverzögerter Alarm“ fest.
Wenn Sie Meldergruppenabhängigkeiten in derselben Meldergruppenabhängigkeits-Gruppe verschiedenen Melderprofilen zuweisen und die Funktion „Alarmabbruch“ verwenden möchten, legen Sie den Parameter *Alarmabbruch, Seite 247* für jedes Melderprofil auf „Ja“ fest.
Wenn Sie den Parameter *Übergehen möglich, Seite 244* für Meldergruppenabhängigkeits-Gruppen auf „Ja“ festlegen, können Meldergruppenabhängigkeits-Alarme verhindert werden. Wenn beispielsweise die Melder 1 und 2 in Abhängigkeit stehen, Melder 1 umgangen wird und Melder 2 offen ist, kann die Zentrale kein Meldergruppenabhängigkeits-Ereignis erstellen. Wenn Melder 2 offen bleibt, bis die Meldergruppenabhängigkeit-Schaltuhr abläuft, erstellt die Zentrale ein Melderalarmereignis (kein Meldergruppenabhängigkeit-Alarmereignis). Wenn Melder 2 offen ist und zurückgesetzt wird, bevor die Meldergruppenabhängigkeit-Schaltuhr abläuft, erstellt die Zentrale ein unbestätigtes Ereignis (kein Meldergruppenabhängigkeit-Alarmereignis), wenn die Schaltuhr abläuft.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Melderabhängigkeit

Weitere Informationen
Melderabhängigkeit-Schaltuhr, Seite 216

11.3.29 Alarmbestätigung

Standardeinstellung:
- Ja – Melderprofil 5
- Nein – Alle anderen Melderprofile

Auswahl:
- Ja – Für diesen Melder wird die Alarmverifizierung aktiviert (nur Melderart „Feuer“).
- Nein – Für diesen Melder wird die Alarmverifizierung deaktiviert.

Wenn Sie diesen Parameter auf „Ja“ festlegen, müssen Sie auch den Parameter „Rücksetzbar“ auf „Ja“ festlegen.
Wenn für einen Melder mit aktivierter Alarmverifizierung ein Alarm ausgelöst wird, startet die Zentrale die Ausgangsfunktion „Melder zurücksetzen“, um die Stromzufuhr für die zurücksetzbaren Melder zu unterbrechen. Wenn die Stromversorgung wieder eingeschaltet wird, ignoriert die Zentrale den Melder für den Zeitraum, der im Parameter „Neustartzeit“ angegeben ist. Wenn nach Ablauf der Neustartzeit innerhalb von 65 Sekunden ein Alarm für den Melder ausgelöst wird, erstellt die Zentrale ein Alarmereignis.
Die Zentrale verwendet die im Parameter „Neustartzeit“ eingestellte Zeit nicht für den Brand-Funktionstest. Die Neustartzeit beträgt 5 Sekunden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Alarmbestätigung

Weitere Informationen
Neustartzeit, Seite 127
Rücksetzbar, Seite 247

Reset Sensors (Melder zurücksetzen), Seite 166

11.3.30 Rücksetzbar

Standardeinstellung:

– Nein – Melderprofile 1–3, 6–20
– Ja – Melderprofile 4, 5

Auswahl:

– Ja – Die Zentrale ignoriert diesen Melder für die Zurücksetzungszeit in der Benutzerfunktion „Melder zurücksetzen“ und die Zurücksetzungs-/Neustartzeit in der Funktion „Alarmverifizierung“.
– Nein – Dieser Melder ist nicht zurücksetzbar.

Legen Sie diesen Parameter für Melder, für die eine Stromunterbrechung erforderlich ist, um einen aktivierten Alarm zurückzusetzen, auf „Ja“ fest. Die Funktion für zurücksetzbare Melder wird normalerweise für Rauchmelder und Glasbruchmelder verwendet. In derselben mit Netzstrom gespeisten Schleife sollten Brand- und Einbruchmeldegeräte nicht gemischt werden.

Wenn Melder mit der Benutzerfunktion „Melder zurücksetzen“, einem Funktionstest oder RPS zurückgesetzt werden, sendet die Zentrale ein Melderzurücksetzungsprotokoll an den Bedienteilempfänger.

Weitere Informationen

Alarmbestätigung, Seite 246
Neustartzeit, Seite 127
Reset Sensors (Melder zurücksetzen), Seite 166

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Melder > Melderprofile > Zurücksetzbar

11.3.31 Alarmabbruch

Standardeinstellung:

– Ja – Melderprofile 1, 7–10, 11–16, 20
– Nein – Melderprofile 2–6, 17–19

Auswahl:

– Ja – Wenn für den Melder ein Alarm ausgelöst wird, verzögert die Zentrale das Alarmprotokoll für den Zeitraum, der im Parameter „Alarmabbruchzeit“ festgelegt ist.
– Nein – Die Zentrale verzögert Alarmprotokolle nicht.

Wenn ein Benutzer den Alarm stummschaltet, bevor die Alarmabbruchzeit endet, wird der Alarm abgebrochen. Das Alarmprotokoll des Melders wird nicht an den Bedienteilempfänger gesendet.

Wenn ein Alarm abgebrochen wird, kann auf Bedienteilen die Meldung „Alarm nicht gesendet“ angezeigt werden. Siehe *Abort Display (Abbruch anzeigen), Seite 151*.

Dieser Parameter gilt nicht für Feueralarme oder unsichtbare Melderalarme.

Hinweis!

Gemäß den UL-Standards darf die Gesamtzeit, die für den Parameter *Eingangsverzögerung, Seite 238* und den Parameter *Alarmabbruchzeit, Seite 109* eingegeben wird, 1 Minute nicht überschreiten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Melder > Melderprofile > Alarmabbruch

11.3.32 Überwachungsdauer des Funkmelders

Standardeinstellung:

– 24 Stunden – Melderprofile 1–2, 7–16
– 4 Stunden – Melderprofile 3–6

Auswahl:
– Keine – Funkmelderüberwachung wird deaktiviert.
– 4 Stunden, 12 Stunden, 24 Stunden, 48 Stunden, 72 Stunden – Legen Sie die Zeit (in Stunden) für die Funkmelderüberwachung fest.

Wenn der Funkempfänger innerhalb der Überwachungsdauer des Funkmelders keine Übertragung vom Funkmelder empfängt, erstellt die Zentrale für den Melder das Ereignis „Fehlt“.
Der Parameter „Überwachungsdauer des Funkmelders“ für Feuermelder wird auf 4 Stunden eingestellt und kann nicht bearbeitet werden.
Der Parameter „Überwachungsdauer des Funkmelders“ gilt für RADION keyfobs, wenn sie als ein Melder konfiguriert sind.
Dieses Überwachungsintervall ist eine Alternative zur globalen Einstellung *Systemüberwachungsdauer (Repeater), Seite 291*.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Überwachungsdauer des Funkmelders

11.3.33 Benutzerdefinierte Funktion

Standardeinstellung: Deaktiviert
Auswahl:
– B6512 – Deaktiviert, Funktion 128-133
– B5512 – Deaktiviert, Funktion 128-131
– B4512 – Deaktiviert, Funktion 128-129
– B3512 – Deaktiviert, Funktion 128

Wählen Sie die benutzerdefinierte Funktion aus, die gestartet wird, wenn für den Melder der Zustand „kurzgeschlossen“ (S) oder „offen“ (O) ausgelöst wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Benutzerdefinierte Funktion

11.3.34 Überwachungsverzögerung

Standardeinstellung: 00:00
Optionen: 00:00 (deaktiviert), 00:01-60:00
Legen Sie die Zeit (mm: ss) fest, für die eine unscharfgeschaltete Zentrale nach einer Melderstörung wartet, bevor ein Einbruch-Errichterbedienung-Protokoll an das Bedienteil gesendet wird. Der Melder muss die gesamte Zeit offen sein.
Wenn der Melder innerhalb dieser Zeit in den Normalzustand wechselt, wird kein Protokoll gesendet.
Die Zentrale zeigt keine Überwachungsverzögerungsereignisse auf den Bedienteilen an.
Verwenden Sie die Funktion „Überwachungsverzögerung“, um Türen zu überwachen, die nicht offen gelassen werden dürfen, z. B. Müllkompaktortüren, Schmuckvitrinentüren und Gefrierschranktüren.

Hinweis!
Starten Sie einen Funktionstest, der gesteuerte Melder umfasst, oder das Scharfschalten des Melderbereichs bricht die Überwachungsmelder-Zeitschaltuhr ab. Kein Protokoll wird gesendet, nachdem die konfigurierte Zeit abgelaufen ist.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Überwachungsverzögerung

11.3.35 Verzögerte Antwort, unscharf

Standardeinstellung: 00:00

Optionen: 00:00 (deaktiviert), 00:05-60:00

Mit diesem Parameter wird festgelegt, wie lange (mm:ss) die Zentrale nach dem Auslösen eines unscharfgeschalteten Melders wartet, bevor die Störung angekündigt oder gemeldet wird.

Dieser Parameter gilt nur für die folgenden Melderarten bei Unscharfschaltung:

- *Außenhautüberwachung, Seite 250*
- *Innenbereich, Seite 251*
- *Wegmelder Innenbereich, Seite 252*

Mit dieser Funktion kann die Auswirkung der folgenden Parameter verzögert werden:

- *Melderreaktion, Seite 223*
  - Unverzögerter Alarm
  - Errichterbedienung
- *Summeralarm bei Fehler, Seite 240*
- *Überwachungsmelder, Seite 241*
- *Ausgangsreaktionstyp, Seite 241*
- *Als Gerät anzeigen, Seite 241*
- *Ausgang, Seite 213*

Hinweis!
Melderreaktion (D) – Alarmverzögerung wird von der Funktion „Alarmverzögerung“ nicht unterstützt. Wenn eine Alarmverzögerung zu einem unverzögerten Alarm führt, wird dieser Alarm von dieser Funktion nicht verzögert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Verzögerte Antwort, unscharf

11.3.36 Verzögerte Antwort, scharf

Standardeinstellung: 00:00

Optionen: 00:00 (deaktiviert), 00:05-60:00

Mit diesem Parameter wird festgelegt, wie lange (mm:ss) die Zentrale nach dem Auslösen eines scharfgeschalteten Melders wartet, bevor die Störung angekündigt oder gemeldet wird.

Dieser Parameter gilt nur für die folgenden Melderarten bei Scharfschaltung:

- *24 Stunden, Seite 250*
- *Außenhautüberwachung, Seite 250*
- *Innenbereich, Seite 251*
- *Wegmelder Innenbereich, Seite 252*

Mit dieser Funktion kann die Auswirkung der folgenden Parameter verzögert werden:

- *Melderreaktion, Seite 223*
  - Unverzögerter Alarm
  - Errichterbedienung
- *Ausgangsreaktionstyp, Seite 241*
- *Als Gerät anzeigen, Seite 241*
- *Ausgang, Seite 213*

Hinweis!
Melderreaktion (D) – Alarmverzögerung wird von der Funktion „Alarmverzögerung“ nicht unterstützt. Wenn eine Alarmverzögerung zu einem unverzögerten Alarm führt, wird dieser Alarm von dieser Funktion nicht verzögert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Verzögerte Antwort, scharf

11.3.37 Normalzustand

Standard: Offen
Auswahl:
– Offen – ein offener Stromkreis ist der Normalzustand.
– Kurzgeschlossen – ein kurzgeschlossener Stromkreis ist der Normalzustand.

Dieser Parameter legt den Normalzustand fest, wenn der Parameter „Stromkreisbauweise“ auf „Keine EOL“ festgelegt ist.
(Nicht verfügbar bei Zentralen mit der Version 2.xx.)

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Melder > Melderprofile > Melderart/Reaktion/Stromkreisbauweise

11.4 Melderprofilbeschreibungen

11.4.1 24 Stunden

Ein 24-Stunden-Melder wird nicht über ein Bedienteil ein- und ausgeschaltet. 24-Stunden-Melder sind immer scharfgeschaltet und können für Notrufe, medizinische Alarme und Polizeialarme eingesetzt werden.
24-Stunden-Melder können so parametriert werden, dass ein Übergehen möglich ist. Vor dem Verwenden der Option „Übergehen möglich“ sollte jedoch der Einsatzzweck jedoch sorgfältig überlegt werden. Übergehbare 24-Stunden-Melder sollten für *Summeralarm bei Fehler, Seite 240* parametriert werden.
Wenn ein 24-Stunden-Melder umgangen wird, sollte das Protokoll beim Auftreten gesendet werden. Wenn der Bereich alle 24-Stunden-Melder enthält, ist der Bereich nie scharf- oder unscharfgeschaltet. Daher wird kein verzögertes Übergehungsprotokoll gesendet.
24-Stunden-Schutz für Brandschutztüren, Dachluken usw. Anstatt diese Art von Schutz als 24-Stunden-Melder zu parametrieren, sollten Sie überlegen, die Melderart „Sichtbarer Überfallalarm bei intern und extern scharf (mit Verzögerung)“ mit einer *Melderreaktion, Seite 223* von „9“ bis „E“ zu verwenden. 24-Stunden-Melder zeigen keine Störungen an, wenn eine Scharfschaltungsfunktion aktiviert wird, die Melder „Sichtbarer Überfallalarm bei intern und extern scharf (mit Verzögerung)“ aber schon. Bei der Parametrierung dieser Art von Schutz empfehlen sich die Optionen „Summeralarm bei Fehler“ und *Lokal, wenn unscharfgeschaltet, Seite 242*.
Überfallmeldegeräte bei UL-Installationen: Die 24-Stunden-Melderart muss für Melder verwendet werden, die an Überfallmeldegeräte angeschlossen sind. Der Meldertext muss „Überfall“ enthalten.

11.4.2 Außenhautüberwachung

Das Konfigurieren eines Melderprofils mit der Melderart „Außenhautüberwachung“ wird es zum Melderprofil „Außenhautüberwachung“. Melder, die dem Melderprofil „Außenhautüberwachung“ zugewiesen sind, haben die Melderart „Außenhautüberwachung“. Mit Meldern der Art „Außenhautüberwachung“ wird normalerweise die Außenseite der Räume (Türen und Fenster) überwacht.
Ein Melderprofil „Außenhautüberwachung“ enthält eine konfigurierbare Eingangsverzögerungszeit. Die Eingangsverzögerungszeit bietet Benutzern die Möglichkeit, ein Bedienteil zu erreichen und den Bereich unscharfzuschalten („Aus“), ohne dass ein Alarm erzeugt wird. Wenn ein Benutzer beispielsweise die Außentür öffnet und den Melder

„Außenhautüberwachung“ auslöst, beginnt die Eingangsverzögerungszeit. Der Benutzer muss zu einem Bedienteil gehen und den Bereich vor Ablauf der Scharfschalteverzögerungszeit unscharfschalten, damit kein Alarm ausgelöst wird.
Wenn für den Bereich eine Eingangsverzögerung vorliegt und ein zweiter Melder „Außenhautüberwachung“ ausgelöst wird, vergleicht die Zentrale die verbleibende Eingangsverzögerungszeit mit der für den zweiten Melder „Außenhautüberwachung“ parametrierten Eingangsverzögerungszeit. Wenn die Eingangsverzögerungszeit für den zweiten Melder kleiner als die verbleibende Zeit ist, wird die Eingangsverzögerungszeit gekürzt.

Hinweis!
Melder der Art „Außenhautüberwachung“ mit unverzögerter Melderreaktion erzeugen sofortige Alarme
Wenn Melder der Art „Sichtbarer Überfallalarm bei intern und extern scharf (mit Verzögerung)“ für eine unverzögerte *Melderreaktion, Seite 223* parametriert sind, wird keine Eingangsverzögerungszeit gestartet. Sie generieren sofort einen Alarm, selbst bei einer Eingangs- oder Scharfschalteverzögerungszeit.

Wenn ein Benutzer einen Bereich auf „Vollscharfschaltung” schaltet, werden die Melder „Außenhautüberwachung“, „Innenbereich“ oder „Wegmelder Innenbereich“ alle scharfgeschaltet.
Wenn ein Benutzer einen Bereich auf „Außenhautüberwachung” schaltet, werden nur die Melder „Außenhautüberwachung“ scharfgeschaltet. Die Melder „Innenbereich“ und „Wegmelder Innenbereich“ sind nicht scharfgeschaltet. In einem typischen System wird beim Schalten eines Bereichs auf „Außenhautüberwachung“ nur die Außenhautüberwachung scharfgeschaltet, sodass Benutzer in den Räumen bleiben können, ohne dass Innenbereichsmelder ausgelöst werden.

11.4.3 Innenbereich

Das Konfigurieren eines Melderprofils mit der Melderart „Innenbereich“ wird es zum Melderprofil „Innenbereich“. Melder, die dem Melderprofil „Innenbereich“ zugewiesen sind, haben die Melderart „Innenbereich“. Innenbereichsmelder werden normalerweise verwendet, um Erkennungsgeräte für den Innenbereich zu überwachen, etwa Innentüren, Bewegungsmelder, Lichtschranken oder Teppichmatten.
Innenbereichsmelder werden nur scharfgeschaltet, wenn der Bereich vollscharfgeschaltet ist. Sie werden nicht scharfgeschaltet, wenn für den Bereich die Außenhautüberwachung aktiv ist.
Die *Melderreaktion, Seite 223* für Innenbereichsmelder können für eine unverzögerte oder verzögerte Alarmreaktion konfiguriert werden.

- Unverzögert – Melder, die für einen unverzögerten Alarm konfiguriert sind, erzeugen Alarmereignisse sofort, selbst während der Eingangs- oder Scharfschalteverzögerungszeit. Innenbereichsmelder werden häufig für eine unverzögerte Alarmreaktion konfiguriert.
- Verzögert – Wenn ein für eine verzögerte Alarmreaktion konfigurierter Innenbereichsmelder ausgelöst wird, während der Bereich komplett scharfgeschaltet ist, initiiert er eine Eingangsverzögerungszeit. Es wird kein Alarm erzeugt, sofern die Eingangsverzögerungszeit nicht abläuft, bevor der Bereich ausgeschaltet wird.
  Wenn für den Bereich bereits die Eingangsverzögerung aktiviert ist, wenn ein Innenbereichsmelder mit verzögerter Alarmreaktion ausgelöst wird, vergleicht die Zentrale die verbleibende Eingangsverzögerungszeit mit der für den Innenbereichsmelder parametrierten Eingangsverzögerungszeit. Wenn die Eingangsverzögerungszeit für den Innenbereichsmelder kleiner als die verbleibende Zeit ist, wird die Eingangsverzögerungszeit gekürzt.

Verzögerte Melder können auch einen Eingangston auf dem Bedienteil initiieren (siehe *Eingangston aus, Seite 238*).

Hinweis!
Verwenden Sie das Profil *Wegmelder Innenbereich, Seite 252* **für den unverzögerten Alarm, wenn sich der Bereich nicht in der Eingangsverzögerung befindet.**
Für einige Installationen empfiehlt sich ein Innenbereichsmelder, der von der Eingangsverzögerung abhängt, sie aber nicht initiieren kann. Die Auslösung des Melders „Wegmelder Innenbereich“, während der Bereich komplett scharfgeschaltet ist, erzeugt einen unverzögerten Alarm. Wenn jedoch ein anderer Melder ausgelöst wird, der die Eingangsverzögerung initiiert, und dann der Melder „Wegmelder Innenbereich“ ausgelöst wird, verzögert der Melder „Wegmelder Innenbereich“ die Alarmreaktion, bis die Scharfschalteverzögerungszeit abläuft. Wenn der Bereich ausgeschaltet wird, bevor die Eingangsverzögerungszeit abläuft, gibt es keine Alarmreaktion.

11.4.4 Wegmelder Innenbereich

Das Konfigurieren eines Melderprofils mit der Melderart „Wegmelder Innenbereich“ wird es zum Melderprofil „Wegmelder Innenbereich“. Melder, die dem Melderprofil „Wegmelder Innenbereich“ zugewiesen sind, haben die Melderart „Wegmelder Innenbereich“. Melder der Art „Wegmelder Innenbereich“ werden normalerweise verwendet, um Erkennungsgeräte für den Innenbereich zu überwachen, etwa Innentüren, Bewegungsmelder, Lichtschranken oder Teppichmatten.
Melder der Art „Wegmelder Innenbereich“ werden nur scharfgeschaltet, wenn der Bereich vollscharfgeschaltet ist. Sie werden nicht scharfgeschaltet, wenn für den Bereich die Außenhautüberwachung aktiv ist.
Melder der Art „Wegmelder Innenbereich“ sind von der Eingangsverzögerung abhängig, können sie aber nicht initiieren. Die Auslösung des Melders „Wegmelder Innenbereich“, während der Bereich komplett scharfgeschaltet ist, erzeugt eine unverzögerte Alarmreaktion. Wenn jedoch ein anderer Melder ausgelöst wird, der die Eingangsverzögerung initiiert, und dann der Melder „Wegmelder Innenbereich“ ausgelöst wird, verzögert der Melder „Wegmelder Innenbereich“ die Alarmreaktion, bis die Scharfschalteverzögerungszeit abläuft. Wenn der Bereich ausgeschaltet wird, bevor die Eingangsverzögerungszeit abläuft, gibt es keine Alarmreaktion.
Wenn während der Scharfschalteverzögerung der Melder „Wegmelder Innenbereich“ ausgelöst wird, wird kein Alarm erzeugt (auch wenn ein Melder „Außenhautüberwachung, Verzögerung“ während der Scharfschalteverzögerung nicht ausgelöst wird).
Melder der Art „Wegmelder Innenbereich“ initiieren keine Eingangsverzögerung, selbst wenn sie für eine verzögerte Alarmreaktion konfiguriert sind (*Melderreaktion, Seite 223* ist auf „4“, „5“, „6“, „7“ oder „8“ festgelegt).

Hinweis!
Verwenden Sie das Profil *Innenbereich, Seite 251* **und eine verzögerte Alarmreaktion für Innenbereichsmelder, die eine Eingangsverzögerung initiieren**.
Für einige Installationen empfiehlt sich ein Innenbereichsmelder, der eine Eingangsverzögerung initiieren kann. Wenn ein für eine verzögerte Alarmreaktion konfigurierter Innenbereichsmelder (siehe *Melderreaktion, Seite 223*) ausgelöst wird, während der Bereich komplett scharfgeschaltet ist, wird eine Eingangsverzögerung initiiert. Die Alarmreaktion wird verzögert, bis die Scharfschalteverzögerungszeit abläuft. Wenn der Bereich ausgeschaltet wird, bevor die Eingangsverzögerungszeit abläuft, gibt es keine Alarmreaktion.

11.4.5 Schlüsselschalter

Parametrieren Sie die Melderreaktion als „1“. Schließen Sie keine Auslösegeräte an einen Melder mit Schlüsseltaster oder -schalter an.

– Normal: Der Bereich wird unscharfgeschaltet.
– Offen: Wenn dieser Melder von „Normal“ zu „Offen“ wechselt, wird der Bereich scharfgeschaltet.
– Kurzgeschlossen: Ein kurzgeschlossener Stromkreis ist eine Störung, während der Bereich unscharfgeschaltet ist. Ein Kurzschluss ist ein Alarm, während der Bereich scharfgeschaltet ist. Wenn dieser Melder vom Kurzschluss in den Normal- oder offenen Zustand wechselt, wird er zurückgesetzt.

Wenn Sie als Melderreaktion „2“ parametrieren, reagiert der Melder wie folgt:

– Normal: Wenn dieser Melder von „Offen“ zu „Normal“ wechselt, wird der Bereich scharfgeschaltet.
– Offen: Der Bereich wird unscharfgeschaltet.
– Kurzgeschlossen: Ein kurzgeschlossener Stromkreis ist eine Störung, während der Bereich unscharfgeschaltet ist. Ein Kurzschluss ist ein Alarm, während der Bereich scharfgeschaltet ist. Wenn dieser Melder vom Kurzschluss in den Normal- oder offenen Zustand wechselt, wird er zurückgesetzt.

Störungs- oder Wiederherstellungsprotokolle werden nicht gesendet, wenn *Lokal, wenn unscharfgeschaltet, Seite 242* auf „Ja“ gesetzt ist.
Alarm- oder Wiederherstellungsprotokolle werden nicht gesendet, wenn *Lokal, wenn scharfgeschaltet, Seite 242* auf „Ja“ gesetzt ist.

Hinweis!
Melderreaktion 2 ist erforderlich für die Inovonics FA113-Funkperipherie.

11.4.6 Schlüsseltaster

Wird für die Scharf- und Unscharfschaltung eines Bereichs verwendet. Parametrieren Sie die Melderreaktion als „1“. Schließen Sie keine Auslösegeräte an einen Melder mit Schlüsseltaster oder -schalter an.

– N->S->N: Wenn dieser Melder vorübergehend vom Normalzustand (N) in den Kurzschlusszustand (S) und wieder in den Normalzustand wechselt, wird der Scharfschaltzustand des Bereichs umgeschaltet.
– Offen: Ein offener Stromkreis ist eine Störung, während der Melder unscharfgeschaltet ist. Ein offener Stromkreis ist ein Alarm, während der Melder scharfgeschaltet ist.

Wenn diese Melder von „Offen“ zu „Normal“ wechselt, wird er zurückgesetzt.
Störungs- oder Wiederherstellungsprotokolle werden nicht gesendet, wenn *Lokal, wenn unscharfgeschaltet, Seite 242* auf „Ja“ gesetzt ist.
Störungs- oder Wiederherstellungsprotokolle werden nicht gesendet, wenn *Lokal, wenn scharfgeschaltet, Seite 242* auf „Ja“ gesetzt ist.

11.4.7 Öffnen-/Schließen-Melder

Wird zum Scharf- und Unscharfschalten eines Melders verwendet. Parametrieren Sie die Melderreaktion als „1“. Lokale Signalgeber werden über das Bedienteil stummgeschaltet.

– Normal: Der Melder wird scharfgeschaltet und sendet MELDER WIRD GESCHLOSSEN. MELDER WIRD GESCHLOSSEN wird nicht gesendet, wenn *Lokal, wenn scharfgeschaltet, Seite 242* auf „Ja“ festgelegt ist.

- Offen: Ein offener Stromkreis ist ein Alarm, während der Melder scharfgeschaltet ist. Ein offener Stromkreis ist eine Störung, während der Melder unscharfgeschaltet ist. Alarm- oder Wiederherstellungsprotokolle werden nicht gesendet, wenn *Lokal, wenn unscharfgeschaltet, Seite 242* auf „Ja“ gesetzt ist.
- Kurzgeschlossen: Der Melder wird unscharfgeschaltet und sendet MELDER WIRD GEÖFFNET. MELDER WIRD GEÖFFNET wird nicht gesendet, wenn Lokal scharfgeschaltet auf „Ja“ festgelegt ist.

11.4.8 Feuermelder

Diese Melderart generiert einen Feueralarm. Feueralarme sind in der Zentrale Ereignisse der höchsten Priorität.

11.4.9 AUX-AC-Überwachung

Diese Melderart überwacht den Netzstrom eines Hilfsstromnetzteils. Wenn der Melder sich nicht im Normalzustand befindet, wartet die Zentrale für die in „Netzstromausfallzeit“ parametrierte Zeit, bevor eine Melderstörung generiert wird. Diese Melderart verwendet nicht die *Melderreaktion, Seite 223*. Daher wird kein Alarm ausgelöst.
Wenn diese Melderart umgangen wird, wird auf dem Bedienteil 24-STD.-MELDER UMGANGEN angezeigt.

11.4.10 Gasmelder

Diese Melderart überwacht Gaserkennungsmelder und generiert einen Gasalarm, wenn eine unverzögerte Alarmreaktion aktiviert wird (siehe Abschnitt „24-Stunden-Alarmreaktion“).

11.4.11 Benutzerdefinierte Funktion

Diese Melderart aktiviert eine benutzerdefinierte Funktion, wenn die Melderreaktion „CF“ ausgewählt ist (siehe Tabelle mit den Reaktionen der Melderarten mit benutzerdefinierter Funktion). Die aktivierte benutzerdefinierte Funktion wird mit dem Parameter „Benutzerdefinierte Funktion“ konfiguriert.

12 Zeitpläne

12.1 Fenster öffnen/schließen

Mit diesen Fenstern können Zeitpläne für Unscharfschaltung (offen) und Scharfschaltung (Schließen) festgelegt werden. Öffnen-Fenster und Schließen-Fenster können unabhängig voneinander eingerichtet werden. Wenn Sie beispielsweise nur die Funktionen verwenden möchten, die von Schließen-Fenstern bereitgestellt werden, lassen Sie die Zeitangaben in den Parametern für Öffnen-Fenster leer und parametrieren Sie die Zeitangaben für Schließen-Fenster.
Die Zeitpläne für die Unscharfschaltung und Scharfschaltung stellen mehrere unabhängige Funktionen bereit:

- Protokolle zum normalen Öffnen und/oder Schließen werden unterdrückt, wenn *Disable O/C in Window (Öffnen/Schließen in Fenster deaktivieren), Seite 137* auf „Ja“ gesetzt ist.
- Ein Protokoll FEHLER BEIM ÖFFNEN wird generiert, falls der Bereich nicht gemäß Zeitplan unscharfgeschaltet wird, wenn *Fehler beim Öffnen, Seite 137* auf „Ja“ gesetzt ist.
- Ein Warnton wird ausgegeben und [BITTE JETZT SCHLIE EN] wird auf dem Bedienteil angezeigt, wenn es Zeit ist, den Bereich scharfzuschalten.
- Ein Protokoll FEHLER BEIM SCHLIE EN wird generiert, falls der Bereich nicht gemäß Zeitplan scharfgeschaltet wird, wenn *Fehler beim Schließen, Seite 138* auf „Ja“ gesetzt ist.
- Der Bereich wird am Ende des Schließen-Fensters automatisch scharfgeschaltet, wenn *Auto Close (Automatische Scharfschaltung), Seite 137* auf „Ja“ eingestellt ist.

12.1.1 Öffnen-Fenster-Timeline

Beispiel für die Verwendung von zwei Öffnen-Fenstern am selben Tag

Für Bereiche, die zwischen Mitternacht und 6 Uhr unscharfgeschaltet werden, werden Öffnen-Protokolle generiert.
Für Bereiche, die zwischen 6 Uhr und 7 Uhr unscharfgeschaltet werden, werden Protokolle für „Frühes Öffnen“ generiert.
Wenn der Bereich zwischen 7 Uhr und 8 Uhr unscharfgeschaltet wird, werden normale Öffnen-Protokolle generiert.
Wenn „O/C in Fenster deaktivieren“ auf „Ja“ festgelegt ist, wird das Öffnen-Protokoll nicht an das Bedienteil übermittelt.
Wenn der Bereich bis 8:01 Uhr nicht unscharfgeschaltet wird, wird das Ereignis „Fehler beim Öffnen“ generiert, wenn „Fehler beim Öffnen“ in den Öffnen- und Schließen-Optionen auf „Ja“ festgelegt ist.
Wenn der Benutzer den Bereich zwischen 8:01 Uhr und 12:59 Uhr unscharfschaltet, wird das Ereignis „Spätes Öffnen“ generiert.
Für Bereiche, die zwischen 13 Uhr und 14 Uhr unscharfgeschaltet werden, werden Protokolle für „Frühes Öffnen“ generiert.
Für Bereiche, die zwischen 14 Uhr und 15 Uhr unscharfgeschaltet wird, werden normale Öffnen-Protokolle generiert.
Wenn „O/C in Fenster deaktivieren“ auf „Ja“ festgelegt ist, wird das Öffnen-Protokoll nicht an das Bedienteil übermittelt.
Wenn der Bereich bis 15:01 Uhr nicht unscharfgeschaltet wird, wird das Ereignis „Fehler beim Öffnen“ generiert, wenn „Fehler beim Öffnen“ in den Öffnen- und Schließen-Optionen auf „Ja“ festgelegt ist.

Wenn der Benutzer den Bereich zwischen 15:01 Uhr und 23:59 Uhr unscharfschaltet, wird das Ereignis „Spätes Öffnen“ generiert.

Parametrierung für zwei Öffnen-Fenstern am selben Tag (wie in der Timeline dargestellt)

		Öffnen			**Schließen**			
W#	Wochentag	Frühzeitiger Beginn	Start	Stopp	Frühzeitiger Beginn	Start	Stopp	Außer an Feiertagen
1	S**MTWT F**S	06:00	07:00	08:00			23:59	Ja/**Nein**
2	S**MTWT F**S	13:00	14:00	15:00			01:00	Ja/**Nein**

Parametrieren Sie kein einzelnes Fenster, das über die Mitternachtsgrenze verläuft. Die Fensterstoppzeit muss hinter der Fensterstartzeit liegen. Um ein Fenster zu parametrieren, das ohne Problem über die Mitternachtsgrenze verläuft, müssen Sie zwei Fenster parametrieren.
Um beispielsweise Fenster für einen Bereich zu parametrieren, der zwischen 23:30 Uhr und 00:30 Uhr an fünf Tagen in der Woche geöffnet wird, verwenden Sie zwei Fenster, wie im Beispiel unten veranschaulicht:

Parametrierung zur Verbindung von zwei Tagen über Mitternacht

	Öffnen			**Schließen**					
W#	Frühzeitiger Beginn	Start	Stopp	Frühzeitiger Beginn	Start	Stopp	Außer an Feiertagen	Feiertagsindex	Bereich(e)
1/ Montag	22:00	23:30	23:59				Ja/**Nein**	1234	**1**2345678
2/ Montag	00:00	00:00	00:30				Ja/**Nein**	1234	**1**2345678

12.1.2 Tabelle für Öffnen-/Schließen-Fenster

Montag bis Freitag, Öffnen: zwischen 5 Uhr und 6 Uhr, Schließen: zwischen 23 Uhr und 1 Uhr.

		Öffnen			**Schließen**			
W#	Wochentag	Frühzeitiger Beginn	Start	Stopp	Frühzeitiger Beginn	Start	Stopp	Außer an Feiertagen
1	S**MTWT F**S	04:00	05:00	06:00	20:00	23:00	23:59	Ja/**Nein**
2	SM**TWT F**S				00:00	00:00	01:00	Ja/**Nein**

Sonntag, Eingang: zwischen 8 Uhr und 8:30 Uhr, Ausgang: zwischen 14:30 und 17:00 Uhr.

		Öffnen		
W#	Wochentag	Frühzeitiger Beginn	Start	Stopp
4	SMTWTFS	07:00	08:00	08:30
	Alle Tage müssen auf „Nein“ parametriert werden.	Nur an Feiertagen		

Tabelle für Öffnen-/Schließen-Fenster
Mithilfe dieser Tabelle können Sie die richtigen Einträge für Ihre Anwendung bestimmen.

Wochentag	**In der Spalte unten werden kurz die Möglichkeiten zum Aktivieren eines Öffnen/ Schließen-Fensters beschrieben. Befolgen Sie in den anderen Spalten angezeigten Anweisungen, um die entsprechenden Einträge auszuwählen.**	**Außer an Feiertagen**	**Feiertagsindex**	**Bereiche**
Parametrieren Sie mindestens einen Tag als „Ja“.	Wochentag(e)	Nein	Ohne	Parametrieren Sie mindestens einen Bereich als „Ja“.
Parametrieren Sie mindestens einen Tag als „Ja“.	Tag(e) der Woche, aber NICHT an Feiertagen	Ja	Wählen Sie mindestens einen Index aus.	Parametrieren Sie mindestens einen Bereich als „Ja“.
Parametrieren Sie mindestens einen Tag als „Ja“.	Wochentag(e) PLUS Feiertage	Nein	Wählen Sie mindestens einen Index aus.	Parametrieren Sie mindestens einen Bereich als „Ja“.
Alle Tage müssen auf „Nein“ parametriert werden.	Nur an Feiertagen	Nein	Wählen Sie mindestens einen Index aus.	Parametrieren Sie mindestens einen Bereich als „Ja“.

12.1.3 Sonntag bis Samstag

Standardeinstellung (Sonntag bis Samstag): Nein

Optionen: Ja, Nein

Wählen Sie in den Parametern für die sieben Wochentage die Tage der Woche aus, an denen die Öffnen- und/oder Schließen-Fenster aktiv sind.

Um zu verhindern, dass die Fenster an bestimmten Tagen des Jahres aktiviert werden, legen Sie *Außer an Feiertagen, Seite 265* auf „Ja“ fest, und aktivieren Sie mindestens einen Feiertagsindex. Wenn *Außer an Feiertagen, Seite 265* auf „Ja“ festgelegt ist, wird das Fenster an den parametrierten Wochentagen ausgeführt, es sei denn, das Datum ist im Feiertagsindex als ein Feiertag gekennzeichnet.

Wenn Öffnen- und/oder Schließen-Fenster nur an bestimmten Tagen des Jahres benötigt werden, sollten Sie die Fenster nicht für die Ausführung an beliebigen Wochentagen parametrieren. Legen Sie stattdessen *Außer an Feiertagen, Seite 265* auf „Nein“ fest, und wählen Sie einen Feiertagsindex mit den Tagen des Jahres aus, an denen das Fenster aktiv sein soll.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Zeitpläne > Fenster öffnen/schließen > Sonntag bis Samstag

12.1.4 Frühes Öffnen – Beginn

Standardeinstellung: Deaktivieren

Optionen: Deaktivieren, HH:MM (Stunden und Minuten) 00:00 bis 23:59

Geben Sie an, zu welcher Zeit ein Benutzer einen Bereich frühestens öffnen (unscharfschalten) kann.

Dieser Parameter ist einer von drei Parametern, die erforderlich sind, um ein Öffnen-Fenster zu erstellen. Um die Parametrierung eines Öffnen-Fensters abzuschließen, müssen auch *Fenster öffnen - Start, Seite 259* und *Fenster öffnen – Stopp, Seite 259* parametriert werden.

Die in diesem Parameter eingegebene Zeit gibt an, wann der Benutzer einen Bereich frühestens vor dem Zeitpunkt *Fenster öffnen - Start, Seite 259* öffnen kann. Wenn die Öffnen- und Schließen-Protokolle aktiviert sind, wird bei der Unscharfschaltung des Bereichs zwischen Mitternacht und dem Zeitpunkt „Frühes Öffnen – Beginn“ ein Öffnen-Protokoll generiert.

- Wenn *Disable O/C in Window (Öffnen/Schließen in Fenster deaktivieren), Seite 137* auf „Ja“ festgelegt ist und der Bereich zwischen dem Zeitpunkt „Frühes Öffnen – Beginn“ und dem Zeitpunkt „Fenster öffnen - Start“ unscharfgeschaltet wird, wird das Öffnen-Ereignis mit einem Modifizierer „Frühes Öffnen“ gesendet. Wenn der Zeitpunkt „Frühes Öffnen – Beginn“ mit dem Zeitpunkt „Fenster öffnen - Start“ identisch ist, wird kein Öffnen-Ereignis gesendet.
- Wenn *Disable O/C in Window (Öffnen/Schließen in Fenster deaktivieren), Seite 137* auf „Nein“ festgelegt ist und der Bereich zu einem beliebigen Zeitpunkt unscharfgeschaltet wird, wird ein Öffnen-Ereignis ohne Modifikation „Frühes Öffnen“ oder „Spätes Öffnen“ gesendet.

Wenn der Bereich zwischen den Zeitpunkten „Fenster öffnen - Start“ und „Fenster öffnen - Stopp“ unscharfgeschaltet wird, wird im Ereignisprotokoll der Zentrale ein lokales Ereignis erstellt, aber das Öffnen-Protokoll wird nicht an das Bedienteil gesendet.

Wenn der Bereich zwischen dem Zeitpunkt „Fenster öffnen - Stopp“ und vor dem Zeitpunkt „Frühes Öffnen – Beginn“ (oder vor Mitternacht, was immer früher ist) unscharfgeschaltet wird, wird ein Öffnen-Ereignis mit dem Modifizierer „Spätes Öffnen“ generiert.

Beim Konfigurieren von mehreren Fenstern, die am selben Tag ausgeführt werden sollen, müssen Sie sicherstellen, dass sie dem System in chronologischer Reihenfolge hinzugefügt werden. Wenn beispielsweise drei Fenster für den Dienstag parametriert werden, muss Fenster 1 (W1) vor Fenster 2 (W2) und Fenster 2 vor Fenster 3 (W3) ausgeführt werden.

– Sie sollten den Zeitpunkt „Frühes Öffnen – Beginn“ nicht für eine Zeit parametrieren, die zwischen den Zeitpunkten „Fenster öffnen - Start“ und „Fenster öffnen - Stopp“ eines anderen Fensters liegt.
– Parametrieren Sie kein Fenster, das über die Mitternachtsgrenze verläuft.

Deaktivierte Fenster haben eine Startzeit von „00:00“. Wenn Sie für diesen Parameter „00:00“ eingegeben wird, aber für „Fenster öffnen - Start“ und „Fenster öffnen - Stopp“ Uhrzeiten parametriert sind, wird das Fenster deaktiviert.
Um das Fenster zu deaktivieren, muss für alle Stunden- und Minutenfelder „00:00“ eingegeben werden.
Verwenden Sie für die Zeiteingaben ein 24-Stunden-Format. Beispiel: Mitternacht = 00:00; 7:00 Uhr = 07:00; 14:45 Uhr = 14:45; 23:59 Uhr = 23:59.
Wenn das Fenster am selben Tag aktiviert werden muss, an dem Sie es parametrieren, starten Sie die Zentrale neu, um das heutige Fenster zu aktivieren.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Fenster öffnen/schließen > Frühes Öffnen – Beginn

12.1.5 Fenster öffnen - Start

Standardeinstellung: Deaktivieren
Optionen: Deaktivieren, HH:MM (Stunden und Minuten)
Dieser Parameter ist einer von drei Parametern, die erforderlich sind, um ein Öffnen-Fenster zu erstellen. Geben Sie die Uhrzeit ein, zu der die Zentrale das Öffnen-Fenster starten soll. Das Fenster wird aktiviert, wenn die Minute beginnt.
00:00 ist Mitternacht, 23:59 Uhr ist 23:59. Geben Sie Uhrzeit im 24-Stunden-Format ein (beispielsweise wird 7:00 Uhr als 07:00 und 14:45 Uhr als 14:45 eingegeben).
Um ein Öffnen-Fenster zu parametrieren, müssen auch „Frühes Öffnen – Beginn“ und „Fenster öffnen - Stopp“ parametriert werden.

Weitere Informationen
Frühes Schließen – Beginn, Seite 260
Fenster öffnen – Stopp, Seite 259

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Fenster öffnen/schließen > Fenster öffnen - Start

12.1.6 Fenster öffnen – Stopp

Standardeinstellung: Deaktivieren
Optionen: Deaktivieren, HH:MM (Stunden und Minuten)
Geben Sie die Uhrzeit ein, zu der die Zentrale das Öffnen-Fenster enden soll. Das Fenster wird gestoppt, wenn die Minute endet.
00:00 ist Mitternacht, 23:59 Uhr ist 23:59. Geben Sie Uhrzeit im 24-Stunden-Format ein (beispielsweise wird 7:00 Uhr als 07:00 und 14:45 Uhr als 14:45 eingegeben).
Dieser Parameter ist einer von drei Parametern, die erforderlich sind, um ein Öffnen-Fenster zu erstellen. Um ein Öffnen-Fenster zu parametrieren, müssen auch *Frühes Schließen – Beginn, Seite 260* und *Fenster öffnen - Start, Seite 259* parametriert werden.
Wenn der Bereich nicht vor Ablauf der Zeit *Fenster öffnen – Stopp, Seite 259* unscharfgeschaltet wird, generiert die Zentrale ein FEHLER BEIM ÖFFNEN-Protokoll, wenn dies in *Fehler beim Öffnen, Seite 137* aktiviert ist.
Öffnen-Protokolle, die zwischen den Zeitpunkten „Fenster öffnen - Start“ und „Fenster öffnen - Stopp“ generiert werden, können unterdrückt werden, indem *Disable O/C in Window (Öffnen/Schließen in Fenster deaktivieren), Seite 137* auf „Ja“ gesetzt ist. Unter „Frühes Öffnen – Beginn“ werden andere Protokollfunktionen erläutert.

Verwenden Sie 23:59 nicht als Fensterstoppzeit, es sei denn, ein anderes Fenster beginnt am Folgetag um 00:00.
Die Zentrale sendet keine FEHLER BEIM ÖFFNEN-Protokolle für Fenster, die um 23:59 stoppen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Fenster öffnen/schließen > Fenster öffnen - Stopp

12.1.7 Frühes Schließen – Beginn

Standardeinstellung: Deaktivieren
Optionen: Deaktivieren, HH:MM (Stunden und Minuten) 00:00 bis 23:59
Geben Sie die Uhrzeit ein, zu der der Benutzer frühestes vor dem Zeitpunkt „Fenster schließen - Start“ einen Bereich schließen kann.
Dieser Parameter ist einer von drei Parametern, die erforderlich sind, um ein Schließen-Fenster zu erstellen. Um die Parametrierung eines Schließen-Fensters abzuschließen, müssen auch *Fenster schließen - Start, Seite 261* und *Fenster schließen - Stopp, Seite 261* parametriert werden.
Die in diesem Parameter eingegebene Zeit gibt an, wann der Benutzer einen Bereich frühestens vor dem Zeitpunkt „Fenster schließen - Start“ schließen kann. Wenn die Öffnen- und Schließen-Protokolle aktiviert sind, wird bei der Scharfschaltung des Bereichs zwischen Mitternacht und dem in diesem Parameter eingegebene Zeitpunkt ein Schließen-Protokoll generiert.
Wenn *Disable O/C in Window (Öffnen/Schließen in Fenster deaktivieren), Seite 137* auf „Ja“ festgelegt ist und der Bereich zwischen dem Zeitpunkt „Frühes Schließen – Beginn“ und dem Zeitpunkt „Fenster schließen - Start“ scharfgeschaltet wird, wird das Schließen-Ereignis mit einem Modifizierer „Frühes Schließen“ gesendet. Wenn der Zeitpunkt „Frühes Schließen – Beginn“ mit dem Zeitpunkt „Fenster schließen - Start“ identisch ist, wird kein Schließen-Ereignis gesendet.
Wenn „O/C in Fenster deaktivieren“ auf „Nein“ festgelegt ist und der Bereich zu einem beliebigen Zeitpunkt scharfgeschaltet wird, wird ein Schließen-Ereignis ohne die Modifizierer „Frühes Schließen“ oder „Spätes Schließen“ gesendet.
Wenn der Bereich zwischen den Zeitpunkten „Fenster schließen - Start“ und „Fenster schließen - Stopp“ scharfgeschaltet wird, wird im Ereignisprotokoll der Zentrale ein lokales Ereignis erstellt, aber das Schließen-Protokoll wird nicht an das Bedienteil gesendet.
Wenn der Bereich zwischen dem Zeitpunkt „Fenster schließen - Stopp“ und vor dem Zeitpunkt „Frühes Schließen – Beginn“ (oder vor Mitternacht, was immer früher ist) scharfgeschaltet wird, wird ein Schließen-Ereignis mit dem Modifizierer „Spätes Schließen“ generiert.
Beim Konfigurieren von mehreren Fenstern, die am selben Tag ausgeführt werden sollen, müssen Sie sicherstellen, dass sie dem System in chronologischer Reihenfolge hinzugefügt werden. Wenn beispielsweise drei Fenster für den Dienstag parametriert werden, muss Fenster 1 (W1) vor Fenster 2 (W2) und Fenster 2 vor Fenster 3 (W3) ausgeführt werden.
Sie sollten für *Frühes Öffnen – Beginn, Seite 258* keine Zeit parametrieren, die zwischen den Zeitpunkten *Fenster öffnen - Start, Seite 259* und *Fenster öffnen – Stopp, Seite 259* eines anderen Fensters liegt.
Deaktivierte Fenster haben eine Startzeit von 00:00. Wenn Sie für diesen Parameter „00:00“ eingegeben wird, aber für „Fenster schließen - Start“ und „Fenster schließen - Stopp“ Uhrzeiten parametriert sind, wird das Fenster deaktiviert.
Um das Fenster zu deaktivieren, muss sowohl für Stunden- als auch Minutenfelder „00:00“ eingegeben werden.
Verwenden Sie für die Zeiteingaben ein 24-Stunden-Format. Beispiel: Mitternacht = 00:00; 7:00 Uhr = 07:00; 14:45 Uhr = 14:45; 23:59 Uhr = 23:59.

Wenn das Fenster am selben Tag aktiviert werden muss, an dem Sie es parametrieren, starten Sie die Zentrale neu, um das heutige Fenster zu aktivieren.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Fenster öffnen/schließen > Frühes Schließen – Beginn

12.1.8 Fenster schließen - Start

Standardeinstellung: Deaktivieren
Optionen: Deaktivieren, HH:MM (Stunden und Minuten)
Dieser Parameter ist einer von drei Parametern, die erforderlich sind, um ein Schließen-Fenster zu erstellen. Geben Sie die Uhrzeit ein, zu der die Zentrale das Schließen-Fenster starten soll. Das Fenster wird aktiviert, wenn die Minute beginnt.
00:00 ist Mitternacht, 23:59 Uhr ist 23:59. Geben Sie Uhrzeit im 24-Stunden-Format ein (beispielsweise wird 7:00 Uhr als 07:00 und 14:45 Uhr als 14:45 eingegeben).
Um ein Schließen-Fenster zu parametrieren, müssen auch *Frühes Schließen – Beginn, Seite 260* und *Fenster schließen - Stopp, Seite 261* parametriert werden.
Ein Warnton wird ausgegeben und [BITTE JETZT SCHLIE EN] wird auf dem Bedienteil angezeigt, falls der Bereich unscharfgeschaltet ist, wenn die Zeit „Fenster schließen - Start“ erreicht wird. Um den Ton stummzuschalten, drücken Sie die [ESC]-Taste auf dem Bedienteil. Der Warnton wird in 10 Minuten gestartet, wenn der Bereich nicht scharfgeschaltet ist.
Unter *Frühes Schließen – Beginn, Seite 260* werden andere Protokollfunktionen erläutert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Fenster öffnen/schließen > Fenster schließen - Start

12.1.9 Fenster schließen - Stopp

Standardeinstellung: Deaktivieren
Optionen: Deaktivieren, HH:MM (Stunden und Minuten)
Dieser Parameter ist einer von drei Parametern, die erforderlich sind, um ein Schließen-Fenster zu erstellen. Geben Sie die Uhrzeit ein, zu der die Zentrale das Schließen-Fenster enden soll. Das Fenster wird gestoppt, wenn die Minute endet.
00:00 ist Mitternacht, 23:59 Uhr ist 23:59. Geben Sie Uhrzeit im 24-Stunden-Format ein (beispielsweise wird 14:45 Uhr als 14:45 eingegeben).
Um ein Schließen-Fenster zu parametrieren, müssen auch „Frühes Schließen – Beginn“ und „Fenster schließen - Start“ parametriert werden.
Wenn der Bereich nicht vor Ablauf der Zeit „Fenster schließen - Stopp“ scharfgeschaltet wird, generiert die Zentrale ein FEHLER BEIM SCHLIE EN-Protokoll, wenn dies in „Fehler beim Schließen“ aktiviert ist.
Schließen-Protokolle, die zwischen den Zeitpunkten „Fenster schließen - Start“ und „Fenster schließen - Stopp“ generiert werden, können unterdrückt werden, indem „O/C in Fenster deaktivieren“ auf „Ja“ gesetzt ist. Unter „Frühes Schließen - Beginn“ werden andere Protokollfunktionen erläutert.
Verwenden Sie 23:59 nicht als Fensterstoppzeit, es sei denn, das Fenster wird am Folgetag um 00:00 fortgesetzt. FEHLER BEIM SCHLIE EN-Protokolle werden nicht gesendet, und die Funktion „Automatische Scharfschaltung“ funktioniert nicht für Fenster, die um 23:59 Uhr gestoppt werden.
Parametrieren Sie kein einzelnes Fenster, das über die Mitternachtsgrenze verläuft. Die Fensterstoppzeit muss hinter der Fensterstartzeit liegen. Um ein Fenster zu parametrieren, das ohne Problem über die Mitternachtsgrenze verläuft, müssen Sie zwei Fenster parametrieren.

Um beispielsweise Fenster für einen Bereich zu parametrieren, der zwischen 11:30 Uhr und 12:30 Uhr an fünf Tagen der Woche geschlossen wird, müssen Sie zwei Fenster verwenden, wie unten dargestellt:

		Öffnen			**Schließen**			
W#	Wochentag	Frühzeitiger Beginn	Start	Stopp	Frühzeitiger Beginn	Start	Stopp	Außer an Feiertagen
1	**SMTWT**FS				22:00	23:30	23:59	Ja/**Nein**
2	S**MTWTF**S				00:00	00:00	00:30	Ja/**Nein**

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Fenster öffnen/schließen > Fenster schließen - Stopp

12.1.10 Außer an Feiertagen

Standardeinstellung: Nein

Auswahl:

– Ja – Dieses Fenster wird an Feiertagen nicht aktiviert.
– Nein – Dieses Fenster ist auch an Feiertagen aktiviert.

Mit diesem Parameter können Sie festlegen, ob das Fenster an Feiertagen deaktiviert oder nur an Feiertagen aktiv ist.
Um zu verhindern, dass die Fenster an bestimmten Tagen des Jahres aktiviert werden, legen Sie „Außer an Feiertagen“ auf „Ja“ fest, und aktivieren Sie mindestens einen Feiertagsindex.
Wenn „Außer an Feiertagen“ auf „Ja“ festgelegt ist, wird das Fenster an den parametrierten Wochentagen ausgeführt, es sei denn, das Datum ist im ausgewählten Feiertagsindex als ein Feiertag gekennzeichnet.
Um diesen Parameter verwenden zu können, muss das Fenster so parametriert sein, dass es an mindestens einem Tag der Woche aktiviert wird. Zudem muss ein Feiertagsindex aktiviert sein.
Sie können diese Option auch verwenden, wenn Öffnen- und Schließen-Fenster nur an bestimmten Tagen des Jahres benötigt werden. Parametrieren Sie die Fenster nicht so, dass sie an beliebigen Tagen der Woche ausgeführt werden. Legen Sie stattdessen „Außer an Feiertagen„ auf „Nein“ fest, und wählen Sie mindestens einen Feiertagsindex mit den Tagen des Jahres aus, an denen das Fenster aktiv sein soll.

Weitere Informationen
Feiertags-Nr., Seite 265

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Fenster öffnen/schließen > Außer an Feiertagen

12.1.11 Feiertags-Nr.

Standardeinstellung (Feiertag 1): Nein

Auswahl:

Ja: Für dieses Fenster wird der ausgewählte Feiertagsindex verwendet.
Nein: Für dieses Fenster wird nicht der ausgewählte Feiertagsindex verwendet.
Bei diesem Parameter können bis zu vier Feiertagsindizes für Öffnen-/Schließen-Fenster verwendet werden.

Geben Sie mindestens einen Feiertagsindex ein, wenn *Außer an Feiertagen, Seite 265* für dieses Fenster auf „Ja“ festgelegt ist oder wenn Sie dieses Fensters nur an bestimmten Tagen aktivieren möchten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Fenster öffnen/schließen > Feiertag 1 bis 8

12.1.12 Bereich Nr.

Standardeinstellung: Nein
Auswahl:
– Ja – Das Fenster wird in der angegebenen Bereichsnummer aktiviert.
– Nein – Das Fenster wird in der angegebenen Bereichsnummer deaktiviert.

Mit diesem Parameter wird festgelegt, ob ein bestimmtes Fenster in den einzelnen Bereichen der Zentrale aktiviert wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Fenster öffnen/schließen > Bereichs-Nr.

12.2 Benutzergruppen-Fenster

Verwenden Sie die Parameter in diesem Abschnitt, um Benutzergruppen-Fenster zu erstellen. Wenn Sie einem der Fenster eine Benutzergruppe zuweisen, sind die Anmeldedaten (Zugangscode, Zugangskarte oder Codierschlüssel und Funk-Handsender) für jeden Benutzer in der Benutzergruppe für den Zeitraum zwischen „Aktivierungszeit“ und „Deaktivierungszeit“ für das Fenster aktiviert.
Jede Benutzergruppe kann mehreren Benutzergruppenfenstern innerhalb eines 24-Stunden-Zeitraums zugeordnet werden.
Unter „Benutzerkonfiguration“ > „Benutzerzuordnungen“ > *Benutzergruppe, Seite 178* finden Sie Informationen dazu, wie Benutzer einer Benutzergruppe zugeordnet werden. Wenn ein Benutzer keiner Benutzergruppe zugeordnet ist oder die Benutzergruppe keinem Benutzergruppen-Fenster zugeordnet ist, sind die Anmeldedaten für diesen Benutzer immer aktiviert.

12.2.1 Benutzergruppe

Standardeinstellung: (Fenster-Nr.)
Auswahl:
– B5512: 0 bis 4
– B4512: 0 bis 2
– B3512: 0 bis 1

0 = Deaktiviert
Geben Sie in diesem Parameter eine Benutzergruppennummer ein. Die Benutzeranmeldedaten (Zugangscode, Zugangskarte oder Codierschlüssel und Funk-Handsender) sind für Benutzer, die der Benutzergruppe zugeordnet sind, für den Zeitraum zwischen „Aktivierungszeit“ und „Deaktivierungszeit“ für das Fenster aktiviert.
Sie können eine Benutzergruppe in einem 24-Stunden-Zeitraum mehreren Benutzergruppen zuweisen, aber die Fenster dürfen sich nicht überschneiden oder die Mitternachtsgrenze überschreiten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Benutzergruppen-Fenster > Benutzergruppe

12.2.2 Sonntag bis Samstag

Standardeinstellung (Sonntag bis Samstag): Nein

Optionen: Ja, Nein
Wählen Sie mit den Parametern für die sieben Wochentage die Tage der Woche aus, an denen das Benutzergruppen-Fenster aktiv ist.
Um zu verhindern, dass die Fenster an bestimmten Tagen des Jahres aktiviert werden, legen Sie „Außer an Feiertagen“ auf „Ja“ fest, und aktivieren Sie mindestens einen Feiertagsindex. Wenn „Außer an Feiertagen“ auf „Ja“ festgelegt ist, wird das Fenster an den parametrierten Wochentagen ausgeführt, es sei denn, das Datum ist im Feiertagsindex als ein Feiertag gekennzeichnet.
Wenn Öffnen- und/oder Schließen-Fenster nur an bestimmten Tagen des Jahres benötigt werden, sollten Sie die Fenster nicht für die Ausführung an beliebigen Wochentagen parametrieren. Legen Sie stattdessen „Außer an Feiertagen“ auf „Nein“ fest, und wählen Sie einen Feiertagsindex mit den Tagen des Jahres aus, an denen das Fenster aktiv sein soll.

Weitere Informationen
Außer an Feiertagen, Seite 265

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Benutzergruppen-Fenster > Sonntag bis Samstag

12.2.3 Gruppenaktivierungszeit

Standardeinstellung: Deaktiviert
Optionen: Deaktivieren, HH:MM (Stunden und Minuten)
Ab dem Zeitpunkt, den Sie hier eingeben, werden die Anmeldedaten (Zugangscode, Zugangskarte oder Codierschlüssel und Funk-Handsender) für jeden Benutzer in der Benutzergruppe aktiviert. Das Fenster wird aktiviert, wenn die Minute beginnt.
Geben Sie im Popup-Fenster **Zeiteingabe** die Uhrzeit ein, zu der das Zeitfenster beginnt. Verwenden Sie das 24-Stunden-Format (beispielsweise wird 7:00 Uhr als 07:00 und 14:45 Uhr als 14:45 eingegeben).
Wenn Sie die Option **Deaktivieren** im Popup-Fenster „Zeiteingabe“ aktivieren, wird die Gruppenaktivierungszeit auf 00:00 zurückgesetzt.
Um ein Zeitfenster zu der hier eingegebenen Zeit am selben Tag zu starten, an dem Sie die Zentrale konfigurieren, wählen Sie **Zentrale zurücksetzen** aus, wenn Sie RPS von der Zentrale trennen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Benutzergruppen-Fenster > Gruppenaktivierungszeit

12.2.4 Gruppendeaktivierungszeit

Standardeinstellung: Deaktiviert
Optionen: Deaktivieren, HH:MM (Stunden und Minuten)
Die hier von Ihnen eingegebene Zeit ist das Ende des Benutzergruppen-Zeitfensters. Die Anmeldedaten (Zugangscode, Zugangskarte oder Codierschlüssel und Funk-Handsender) sind für jeden Benutzer in der Benutzergruppe deaktiviert. Das Fenster wird gestoppt, wenn die Minute endet.
Geben Sie im Popup-Fenster **Zeiteingabe** die Uhrzeit ein, zu der das Zeitfenster endet. Verwenden Sie das 24-Stunden-Format (beispielsweise wird 7:00 Uhr als 07:00 und 14:45 Uhr als 14:45 eingegeben).
Wenn Sie die Option **Deaktivieren** im Popup-Fenster „Zeiteingabe“ aktivieren, wird die Gruppendeaktivierungszeit auf 00:00 zurückgesetzt.
Um ein Zeitfenster zu der hier eingegebenen Zeit am selben Tag zu beenden, an dem Sie die Zentrale konfigurieren, wählen Sie **Zentrale zurücksetzen** aus, wenn Sie RPS von der Zentrale trennen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Benutzergruppen-Fenster > Gruppendeaktivierungszeit

12.2.5 Außer an Feiertagen

Standardeinstellung: Nein
Optionen: Ja, Nein
Mit diesem Parameter können Sie festlegen, ob das Fenster an Feiertagen deaktiviert oder nur an Feiertagen aktiv ist. Verwenden Sie die Anweisungen, die in „Außer an Feiertagen“ bereitgestellt werden.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Benutzergruppen-Fenster > Außer an Feiertagen

12.2.6 Feiertags-Nr.

Standardeinstellung: Nein
Auswahl:
Ja: Für dieses Fenster wird der ausgewählte Feiertagsindex verwendet.
Nein: Für dieses Fenster wird nicht der ausgewählte Feiertagsindex verwendet.
Mit diesem Parameter können bis zu vier Feiertagsindexe aktiviert werden, die für Benutzergruppen-Fenster verwendet werden.
Geben Sie mindestens einen Feiertagsindex ein, wenn „Außer an Feiertagen“ für dieses Benutzerfenster auf „Ja“ festgelegt ist oder wenn Sie dieses Fensters nur an bestimmten Tagen aktivieren möchten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Benutzergruppen-Fenster > Feiertags-Nr.

12.3 Zeitgesteuerte Ereignisse

Mit dem Modul „Zeitgesteuerte Ereignisse” können Sie die Zentrale parametrieren, um Funktionen, die ansonsten durch den Endbenutzer am Bedienteil initiiert werden, automatisch auszuführen. Jedes zeitgesteuerte Ereignisse kann so parametriert werden, dass es zu einer bestimmten Zeit an einem bestimmten Datum oder Wochentag auftritt.
Ein zeitgesteuertes Ereignis kann über das Bedienteil bearbeitet werden, wenn Zeitbearbeitung auf „Ja“ festgelegt ist. Datum und Uhrzeit können mithilfe der Funktion [CHANGE SKED?] geändert werden.
Jede Nummer eines zeitgesteuerten Ereignisses kann mit einer der 24 Funktionsbeschreibungen für die Funktion parametriert werden. Eine Funktion ist das, was ausgeführt wird. Neben der Funktion muss auch ausgewählt werden, was von dieser Funktion betroffen ist. (Beispiel: Wenn Sie ein zeitgesteuertes Ereignis zum Unscharfschalten auswählen, ist die Unscharfschaltung die Funktion, die sich wiederum auf die Bereiche auswirkt, die zum Unscharfschalten ausgewählt werden.)
Die Funktionsbeschreibung und die zugehörigen Parameter werden nach dem Parameter „Funktion“ ausführlich erläutert.
Für jedes zeitgesteuerte Ereignis können bis zu vier Feiertagsindexe parametriert werden. Die Feiertagsindexe können verwendet werden, um das zeitgesteuerte Ereignis nicht nur an einem bestimmten Datum oder Wochentag auszuführen, sondern auch an Feiertagen. Sie können auch eingesetzt werden, um zu verhindern, dass das zeitgesteuerte Ereignis an Feiertagen ausgeführt wird (siehe „Außer an Feiertagen“).

12.3.1 Zeitgesteuerte Ereignisse Name Text

Standardeinstellung: Zeitgesteuertes Ereignis – Namenstext

Auswahl: Bis zu 32 alphanumerische Zeichen
Geben Sie bis zu 32 Zeichen Text ein, um den Bereich zu beschreiben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Zeitgesteuerte Ereignisse > Zeitgesteuertes Ereignis – Namenstext

12.3.2 Zeitgesteuertes Ereignis – Namenstext (zweite Sprache)

Standardeinstellung: leer
Auswahl: Bis zu 32 alphanumerische Zeichen
Geben Sie bis zu 32 Zeichen Text ein, um den Bereich zu beschreiben.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Zeitgesteuerte Ereignisse > Zeitgesteuertes Ereignis – Namenstext (zweite Sprache)

12.3.3 Zeitbearbeitung

Standardeinstellung: Yes
Auswahl:
Ja: Der Benutzer kann die Uhrzeit dieses zeitgesteuerten Ereignisses über das Bedienteil bearbeiten, die in der CHANGE SKED-Anzeige erscheint.
Nein. Der Benutzer kann die Uhrzeit dieses zeitgesteuerten Ereignisses nicht über das Bedienteil bearbeiten, und es erscheint nicht in der CHANGE SKED-Anzeige.
Wählen Sie aus, ob der Benutzer die Zeit dieses zeitgesteuerten Ereignisses über das Bedienteil bearbeiten kann.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Zeitgesteuerte Ereignisse > Zeitbearbeitung

12.3.4 Funktion

Standardeinstellung: nicht in Verwendung
Optionen: Siehe Liste der Funktionen für zeitgesteuerte Ereignisse unten.
Wählen Sie in der Dropdown-Liste den Namen der Funktion aus, die über dieses zeitgesteuerte Ereignis ausgeführt werden soll.
RPS zeigt automatisch die verfügbaren Parameteroptionen und Bereichsfelder für diese Funktion an. (Beispiel: Für die Bereiche wird automatisch eine Liste aller Kontrollkästchen angezeigt, wenn Sie die Funktion zum Scharfschalten/Unscharfschalten auswählen.)

Hinweis!
Die Funktion „Vollscharfschaltung – kein Exit“ wird ignoriert, wenn eine Scharfschaltung über ein zeitgesteuertes Ereignis erfolgt.

Nicht in Verwendung: Diese Funktion ist deaktiviert und keine Funktionen nach dieser werden ausgeführt.
All On Delay (Verzögerte Vollscharfschaltung), Seite 269
All On Instant (Unverzögerte Vollscharfschaltung), Seite 269
Verzögerte Außenhautüberwachung, Seite 269
Unverzögerte Außenhautüberwachung, Seite 269
Unscharfschalten, Seite 270
Extend Close (Schließen verlängern), Seite 270
Bypass a Point (Einen Melder übergehen), Seite 270
Unbypass a Point (Einen Melder einschalten), Seite 270
Unbypass All Points (Alle Melder einschalten), Seite 270

Reset Sensors (Melder zurücksetzen), Seite 270
Ausgang einschalten, Seite 270
Ausgang ausschalten, Seite 271
Ausgang umschalten, Seite 271
Monostabiler Ausgang, Seite 271
Alle Ausgänge zurücksetzen, Seite 271
Verzögerung, Seite 271
RPS antworten, Seite 271
RPS kontaktieren, Seite 271
RPS kontaktieren – Benutzerport, Seite 272
Send Status Report (Zustandsmeldungen senden), Seite 272
Send Test Report (Prüfprotokolle senden), Seite 272
Prüfprotokoll bei nicht-normalem Zustand senden, Seite 274
Go to Area (Gehe zu Bereich), Seite 274
Überwachung einschalten, Seite 274
Überwachung ausschalten, Seite 274
Datum und Uhrzeit anzeigen, Seite 274
Überwachungston ausgeben, Seite 274
Bedienteillautstärke festlegen, Seite 275
Bedienteilhelligkeit festlegen, Seite 275
Störung stummschalten, Seite 275
Alarm stummschalten, Seite 275

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Zeitgesteuerte Ereignisse > Zeitgesteuertes Ereignis 1–80 > Funktion

12.3.5 Zeit

Standardeinstellung: Deaktiviert
Optionen: Deaktivieren, HH:MM (Stunden und Minuten)
Geben Sie die Zeit, zu der das zeitgesteuerte Ereignis ausgeführt werden soll, im 24-Stunden-Format ein (beispielsweise wird 14:45 Uhr als 14:45 eingegeben).
Für deaktivierte zeitgesteuerte Ereignisse wird in der Zelle „Deaktiviert“ angezeigt.
Führen Sie diese Schritte aus, um eine Zeit zu parametrieren:

1. Doppelklicken Sie auf das Feld, das dem zeitgesteuerten Ereignis entspricht, für das Sie die Zeit parametrieren möchten.
2. Wenn „Deaktivieren“ aktiviert ist, deaktivieren Sie die Einstellung. Das Zeitfeld wird aktiv.
3. Klicken Sie in das Zeitfeld, und legen Sie die Zeit entweder mithilfe der Nach-oben- und Nach-unten-Pfeiltasten fest, oder geben Sie die gewünschte Zeit ein.
4. Klicken Sie auf die Schaltfläche „OK“.

Führen Sie die folgenden Schritte aus, um ein zeitgesteuertes Ereignis zu deaktivieren:

1. Doppelklicken Sie auf das Feld, das dem zeitgesteuerten Ereignis entspricht, das Sie deaktivieren möchten.
2. Wählen Sie „Deaktivieren“ aus.
3. Klicken Sie auf „OK“.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Zeitgesteuerte Ereignisse > Zeit

12.3.6 Datum

Standardeinstellung: Deaktivieren
Optionen: Deaktivieren, Dag/Monat (z. B. 12. Juni)

Geben Sie das Datum ein, an dem das zeitgesteuerte Ereignis ausgeführt werden soll. Für deaktivierte zeitgesteuerte Ereignisse wird „Deaktiviert“ in der Zelle „Datum“ angezeigt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Zeitgesteuerte Ereignisse > Datum

12.3.7 Sonntag bis Samstag

Standardeinstellung (Sonntag bis Samstag): Nein
Optionen: Ja, Nein
Wählen Sie mit den Parametern für die sieben Wochentage die Tage der Woche aus, an denen das zeitgesteuerte Ereignis aktiv ist.
Um zu verhindern, dass das zeitgesteuerte Ereignis an bestimmten Tagen des Jahres aktiviert werden, legen Sie *Außer an Feiertagen, Seite 268* auf „Ja“ fest, und aktivieren Sie mindestens einen Feiertagsindex. Wenn „Außer an Feiertagen“ auf „Ja“ festgelegt ist, wird das Fenster an den parametrierten Wochentagen ausgeführt, es sei denn, das Datum ist im ausgewählten Feiertagsindex als ein Feiertag gekennzeichnet.
Wenn ein zeitgesteuertes Ereignis nur an bestimmten Tagen des Jahres benötigt wird, parametrieren Sie das zeitgesteuerte Ereignis nicht für die Ausführung an beliebigen Tagen der Woche. Legen Sie stattdessen „Außer an Feiertagen“ auf „Nein“ fest, und wählen Sie einen Feiertagsindex mit den Terminen aus, an denen das Fenster aktiv sein soll.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Zeitgesteuerte Ereignisse > Sonntag bis Samstag

12.3.8 Außer an Feiertagen

Standardeinstellung: Nein
Auswahl:

- Ja: Dieses zeitgesteuerte Ereignis wird nicht an den Feiertagen ausgeführt, die im spezifischen Feiertagsindex angegeben sind, der für dieses zeitgesteuerte Ereignis verwendet wird. In diesem Abschnitt werden spezifische Feiertagsindexe ausgewählt und im nächsten Parametrierungsmodul parametriert.
- Nein. Dieses zeitgesteuerte Ereignis wird an den Feiertagen ausgeführt, die im Feiertagsindex angegeben sind, der für dieses zeitgesteuerte Ereignis verwendet wird.

Wenn keine Wochentage parametriert sind, wird dieses zeitgesteuerte Ereignis nur an den Feiertagen ausgeführt, die im Feiertagsindex parametriert sind, der für dieses zeitgesteuerte Ereignis verwendet wird. Dieses zeitgesteuerte Ereignis wird auch ausgeführt, wenn der Feiertag auf einen parametrierten Wochentag fällt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Zeitgesteuerte Ereignisse > Außer an Feiertagen

12.3.9 Feiertags-Nr.

Standardeinstellung: Nein
Auswahl:

- Ja – Für dieses Benutzergruppen-Fenster wird der Feiertagsindex verwendet.
- Nein – Für dieses Benutzergruppen-Fenster wird der Feiertagsindex nicht verwendet.

Geben Sie mindestens einen Feiertagsindex ein, wenn „Außer an Feiertagen“ für dieses Benutzerfenster auf „Ja“ festgelegt ist oder wenn Sie dieses Fensters nur an bestimmten Tagen aktivieren möchten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Zeitpläne > Zeitgesteuerte Ereignisse > Feiertags-Nr.

12.4 Feiertagsindexe

12.4.1 Zeitplan

Feiertagsindex-Zeitplan

Mit diesem Parameter können Sie Feiertage in einem Feiertagsindex planen.
Sie können für jeden Feiertagsindex bis zu 365 Tage (oder 366 Tage in einem Schaltjahr) als Feiertage auswählen.
Klicken Sie auf den Feiertagsindex, für den Sie Feiertage planen möchten. Das Dialogfeld „Feiertags-Zeitplan“ sieht wie ein Kalender aus. Es zeigt standardmäßig den derzeitigen Monat und das aktuelle Jahr an. Das Jahr dient nur zu Referenzzwecken. Es werden nur Monats- und Tagesdaten an die Zentrale gesendet.
Wenn Sie einen Tag im Kalender als Feiertag festlegen, ist dieser Tag in allen folgenden Jahren ein Feiertag. Wenn Sie beispielsweise den 26. Oktober 2019 als Feiertag festlegen, ist der 26. Oktober auch in den Jahren 2020, 2021 usw. ein Feiertag. Der Wochentag ändert sich dem Jahr entsprechend.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Zeitpläne > Feiertagsindex > Feiertagsindex-Zeitplan

12.5 Funktion „Zeitgesteuertes Ereignis“ – Beschreibungen

12.5.1 All On Delay (Verzögerte Vollscharfschaltung)

Diese Funktion simuliert die Bedienteilfunktion „Verzögerte Vollscharfschaltung“. Mit den Optionen im „Parameter 1: Bereichs-Nr.“ werden die Bereiche definiert, die durch dieses zeitgesteuerte Ereignis scharfgeschaltet werden. Mit dem zeitgesteuerten Ereignis können mehrere Bereiche scharfgeschaltet werden. Wenn beim Ausführen der zeitgesteuerten Funktion ein Melder offen ist, wird er ungeachtet der Parametrierung von „Zwangsläufiges Scharfschalten/Übergehen” zwangsläufig scharfgeschaltet.

12.5.2 All On Instant (Unverzögerte Vollscharfschaltung)

Diese Funktion simuliert die Bedienteilfunktion „Unverzögerte Vollscharfschaltung“. Mit den Eingaben im „Parameter 1: Bereichs-Nr.“ werden die Bereiche definiert, die durch dieses zeitgesteuerte Ereignis scharfgeschaltet werden. Mit dem zeitgesteuerten Ereignis können mehrere Bereiche scharfgeschaltet werden. Wenn beim Ausführen der zeitgesteuerten Funktion ein Melder offen ist, wird er ungeachtet der Parametrierung von „Zwangsläufiges Scharfschalten/Übergehen” zwangsläufig scharfgeschaltet.

12.5.3 Verzögerte Außenhautüberwachung

Diese Funktion simuliert die Bedienteilfunktion „Verzögerte Außenhautüberwachung“. Mit den Optionen im „Parameter 1: Bereichs-Nr.“ werden die Bereiche definiert, die durch dieses zeitgesteuerte Ereignis scharfgeschaltet werden. Mit dem zeitgesteuerten Ereignis können mehrere Bereiche scharfgeschaltet werden. Wenn beim Ausführen der zeitgesteuerten Funktion ein Melder offen ist, wird er ungeachtet der Parametrierung von „Zwangsläufiges Scharfschalten/Übergehen” zwangsläufig scharfgeschaltet.

12.5.4 Unverzögerte Außenhautüberwachung

Diese Funktion simuliert die Bedienteilfunktion „Unverzögerte Außenhautüberwachung“. Mit den Optionen im „Parameter 1: Bereichs-Nr.“ werden die Bereiche definiert, die durch dieses zeitgesteuerte Ereignis scharfgeschaltet werden. Mit dem zeitgesteuerten Ereignis können mehrere Bereiche scharfgeschaltet werden. Wenn beim Ausführen der zeitgesteuerten Funktion ein Melder offen ist, wird er ungeachtet der Parametrierung von „Zwangsläufiges Scharfschalten/Übergehen” zwangsläufig scharfgeschaltet.

12.5.5 Unscharfschalten

Diese Funktion emuliert die Bedienteilfunktion „Unscharfschalten“. Mit den Optionen im „Parameter 1: „Bereichs-Nr.“ werden die Bereiche definiert, die durch dieses zeitgesteuerte Ereignis unscharfgeschaltet werden. Mit dem zeitgesteuerten Ereignis können mehrere Bereiche unscharfgeschaltet werden.

12.5.6 Extend Close (Schließen verlängern)

Mit dieser Funktion können Sie die erwartete Schließzeit für den Bereich ändern. Das Fenster kann erst dann angepasst werden, wenn „Frühes Schließen – Beginn“ vergangen ist und das Schließen-Fenster aktiv ist.

Hinweis!
Die Zeit für „Scharfschaltung verlängern“ kann Mitternacht nicht überschreiten. Falls aktiviert, kann sie die konfigurierte „Letzte Schließzeit“ eines Bereichs nicht überschreiten.

12.5.7 Bypass a Point (Einen Melder übergehen)

Diese Funktion emuliert die Bedienteilfunktion „Melder übergehen“. Mit der Eingabe im „Parameter 1: Melder-Nr.“ wird der Melder angegeben, den diese zeitgesteuerte Funktion übergeht. Der Melder kann nur umgangen werden, wenn „Übergehen möglich“ im Melderprofil, das dem Melder zugeordnet ist, auf „Ja“ parametriert ist. Die Übergehung wird gemeldet, wenn Übergehungsprotokolle im Melderprofil aktiviert sind, das dem Melder zugeordnet ist. Das zeitgesteuerte Ereignis kann einen Melder übergehen.

12.5.8 Unbypass a Point (Einen Melder einschalten)

Diese Funktion emuliert die Verknüpfung der Bedienteilfunktion „Melder ohne Übergehung“. Mit der Eingabe im „Parameter 1: Melder-Nr.“ wird der Melder angegeben, für den diese Funktion die Übergehung aufhebt. Diese Funktion kann nur auf einen Melder angewendet werden.

12.5.9 Unbypass All Points (Alle Melder einschalten)

Diese Funktion ist nicht als Bedienteil-Funktionsverknüpfung verfügbar. Mit den im „Parameter 1: Bereichs-Nr.“ ausgewählten Bereiche werden die Bereiche definiert, für die durch diese Funktion die Übergehung für alle Melder aufgehoben wird.

Hinweis!
Die Übergehung von offenen 24-Stunden-Meldern wird nicht aufgehoben.
Um einen Melderalarm oder Störungen zu vermeiden, wird bei umgangenen 24-Stunden-Meldern, die beim Ausführen dieses zeitgesteuerten Ereignisses offen sind, die Übergehung nicht aufgehoben. Diese bleiben umgangen.

12.5.10 Reset Sensors (Melder zurücksetzen)

Diese Funktion emuliert die Bedienteilverknüpfung „Melder zurücksetzen“. Falls aktiviert, wird mit dieser Funktion der bereichsweite Ausgang „Melder zurücksetzen“ für 5 Sekunden aktiviert. Mit dieser Funktion wird der Alarmausgang für die in Parameter 1 ausgewählten Bereiche für fünf Sekunden deaktiviert.

12.5.11 Ausgang einschalten

Diese Funktion emuliert die Bedienteilverknüpfung „Ausgangszustand ändern“, um Ausgänge zu einzuschalten.

Mit der Eingabe im „Parameter 1: Ausgangs-Nr.“ wird der spezifische Ausgang definiert, den diese Funktion aktiviert. Mit der Funktion kann ein Ausgang aktiviert werden.

12.5.12 Ausgang ausschalten

Diese Funktion emuliert die Bedienteilverknüpfung „Ausgangszustand ändern“, um Ausgänge zu auszuschalten.
Mit der Eingabe im „Parameter 1: Ausgangs-Nr.“ wird der spezifische Ausgang definiert, den diese Funktion deaktiviert. Mit der Funktion kann ein Ausgang deaktiviert werden.

12.5.13 Ausgang umschalten

Diese Funktion ist nicht als Bedienteilverknüpfung verfügbar. Mit der Eingabe im „Parameter 1: Ausgangs-Nr.“ wird der spezifische Ausgang definiert, den diese Funktion umschaltet. Wenn der Ausgang aktiviert ist, wird er ausgeschaltet. Wenn der Ausgang deaktiviert ist, wird er eingeschaltet. Die Funktion wirkt sich auf einen Ausgang aus.

12.5.14 Monostabiler Ausgang

Diese Funktion ist nicht als Bedienteilverknüpfung verfügbar und steht nur als benutzerdefinierte Funktion zur Verfügung. Mit dieser Funktion wird der in Parameter 1 ausgewählte Ausgang für die Anzahl von Sekunden aktiviert, die in Parameter 2 ausgewählt ist.

12.5.15 Alle Ausgänge zurücksetzen

Diese Funktion ist nicht als Bedienteilverknüpfung verfügbar. Diese Funktion deaktiviert alle Ausgänge, die durch ein zeitgesteuertes Ereignis oder eine benutzerdefinierte Funktion aktiviert werden. Diese Funktion steht auf der gesamten Zentrale zur Verfügung. Für diese Option sind keine anderen Parameter erforderlich.

12.5.16 Verzögerung

Diese Funktion dient zum Erstellen einer konfigurierbaren Verzögerung (0 bis 90 Sekunden) zwischen oder vor Funktionen. Mit dem Parameter 1 wird die Verzögerung konfiguriert.

12.5.17 RPS antworten

Diese Funktion emuliert die Bedienteilverknüpfung „RPS antworten“, die bewirkt, dass die Zentrale die nächste RPS-Anforderung zum Initiieren einer Sitzung per Telefon oder Netzwerk beantwortet. Diese Funktion ist nur als benutzerdefinierte Funktion verfügbar. Dieser Zeitraum für die automatische Antwort dauert 2 Minuten und überschreibt die Einstellungen „RPS über Netzwerk antworten“ und „RPS-Adressverifizierung“.

12.5.18 RPS kontaktieren

Mit dieser Funktion wird versucht, eine unbeaufsichtigte RPS zum konfigurierten Zeitpunkt zu kontaktieren. Über das Konto in der Zentrale wird gesteuert, welche Vorgänge bei einem erfolgreichen Kontakt ausgeführt werden.

Hinweis!
Vermeiden Sie, dass mehrere Funktionen gleichzeitig an derselben Adresse ausgeführt werden. Funktionen können in Konflikt stehen, und die Auswirkung auf die Zentrale ist unberechenbar.

Hinweis!
Sie sollten mehrere zeitbasierte Ereignisse nicht so parametrieren, dass sie auf demselben Bedienteil zur selben Zeit ausgeführt werden.

Hinweis!
Zeitgesteuerte Ereignisse sollten nicht so parametriert werden, dass in einem Zeitraum ausgeführt werden, zu dem ein Benutzer wahrscheinlich Funktionen am Bedienteil ausführt.

12.5.19 RPS kontaktieren – Benutzerport

Mit dieser Funktion wird versucht, eine unbeaufsichtigte RPS zum konfigurierten Zeitpunkt über ein Netzkommunikationsgerät am konfigurierten Port zu kontaktieren. Über das Konto in der Zentrale wird gesteuert, welche Vorgänge bei einem erfolgreichen Kontakt ausgeführt werden.

12.5.20 Send Status Report (Zustandsmeldungen senden)

Mit dieser Funktion wird ein Statusprotokoll für jeden aktivierten Bereich generiert. Das Protokoll wird an die Telefone gesendet, die für Prüf- und Statusprotokolle im Protokoll-Routing parametriert sind.
Das Statusprotokoll kann verzögert werden, wenn seit dem letzten Statusprotokoll ein anderes Protokoll gesendet wurde. Um das Statusprotokoll für bis zu 24 Stunden zu verzögern, legen Sie die Option „Parameter 1: Zurückgestellt“ auf „Ja“ fest.

12.5.21 Send Test Report (Prüfprotokolle senden)

Mit diesem zeitgesteuerten Ereignis wird dasselbe Prüfprotokoll gesendet wie mit der Benutzerfunktion „Prüfprotokoll“.
Sie können Prüfprotokolle an eine oder alle Zieladressen senden, die für eine Zielgruppe konfiguriert sind. Das primäre Zielgerät und die Ersatzzielgeräte (erstes, zweites, drittes) können manuelle und automatische (geplante) Prüfprotokolle senden.
Falls ein Melder in einem beliebigen Bereich keinen normalen Zustand (Störung auf der Bedienteilanzeige nicht gelöscht) aufweist, sendet die Zentrale anstelle des Prüfprotokolls ein nicht-normales Prüfprotokoll.
Wenn der Parameter unter „Zentralenübergreifende Parameter > Protokoll-Routing > *Expand Test Report (Prüfprotokoll erweitern), Seite 55*“ auf „Ja“ eingestellt ist, wird nach dem Prüfprotokoll (oder dem nicht-normalen Prüfprotokoll) für jeden nicht-normalen Systemstatus ein Diagnoseprotokoll erstellt. Eine Liste mit enthaltenen Protokollen finden Sie unter „Zentralenübergreifende Parameter > Protokoll-Routing > *Diagnoseprotokolle, Seite 82*“.

Optionen, Parameter 1: Zurückgestellt

- Ja – das Senden der Prüfprotokolle wird für 24 Stunden zurückgestellt, wenn die Zentrale ein anderes Protokoll sendet.
- Nein – das Senden der Prüfprotokolle wird nicht zurückgestellt.

Hinweis!
Nur das Senden des Prüfprotokolls wird verzögert
Wenn „Parameter 1: Zurückgestellt“ auf „Ja“ festgelegt ist, wird nur das Senden des Prüfprotokolls zurückgestellt. Das zeitgesteuerte Ereignis „Prüfprotokoll senden“ wird weiter mit der Häufigkeit ausgeführt, die in „Parameter 2: Häufigkeit“ festgelegt ist.

Optionen, Parameter 2: Häufigkeit

- Stündlich – das erste zeitgesteuerte Ereignis „Prüfprotokoll senden“ wird zu der Zeit ausgeführt, die im Parameter „Zeit“ für das zeitgesteuerte Ereignis eingegeben ist. Das zeitgesteuerte Ereignis „Prüfprotokoll senden“ wird danach stündlich ausgeführt.

– Monatlich – das erste zeitgesteuerte Ereignis „Prüfprotokoll senden“ wird zu dem Zeitpunkt ausgeführt, der im Parameter „Zeit“ und im Parameter „Datum“ für das zeitgesteuerte Ereignis eingegeben ist. Das zeitgesteuerte Ereignis „Prüfprotokoll senden“ wird danach monatlich ausgeführt.
– Geplant – das zeitgesteuerte Ereignis „Prüfprotokoll senden“ wird gemäß den Parametern für Zeit, Datum und Wochentage des zeitgesteuerten Ereignisses ausgeführt.

Hinweis!
Wenn Parameter 2 auf „Geplant“ festgelegt ist und im Parameter „Datum“ ein Datum eingegeben ist, werden die Parameter für Wochentage ignoriert.
Die Zentrale sendet das Prüfprotokoll an dem Datum und zu der Uhrzeit, die in den Parametern „Datum“ und „Zeit“ des zeitgesteuerten Ereignisses eingegeben sind.

Optionen, Parameter 3: Routing
Wenn „Parameter 3: Routing“ auf „Benutzerdefiniert“ eingestellt ist, ist „Parameter 4: Zieladressen“ aktiviert.

Optionen, Parameter 4: Zieladressen
Wenn „Parameter 4: Zieladressen“ aktiviert ist, werden alle konfigurierten Zielgruppen angezeigt. Aktivieren Sie das Kontrollkästchen der Zielgruppe(n), die als Zieladresse verwendet werden sollen.

Prüfprotokolle verzögern
Wenn „Parameter 1: Zurückgestellt“ auf „Ja“ festgelegt ist, wird jedes Mal, wenn die Zentrale eine Rückmeldung vom Bedienteilempfänger für ein beliebiges Protokoll empfängt, ein 24-Stunden-Countdown-Timer gesendet (oder neu gestartet).
Wenn Parameter 2 auf „Stündlich“ festgelegt ist und die Zentrale bis zum Ausführungszeitpunkt des ersten zeitgesteuerten Ereignisses „Prüfprotokoll senden“ keine Rückmeldung erhalten hat, sendet die Zentrale das Prüfprotokoll. Wenn die Zentrale eine Rückmeldung empfangen hat, werden Prüfprotokolle für 24 Stunden ab dem Empfang der letzten Rückmeldung zurückgestellt. Das stündliche zeitgesteuerte Ereignis „Prüfprotokoll senden“ sendet mindestens 24 Stunden lang kein Prüfprotokoll.
Wenn Parameter 2 auf „Monatlich“ festgelegt ist und die Zentrale innerhalb von 24 Stunden nach der Ausführungszeit des ersten monatlichen zeitgesteuerten Ereignisses „Prüfprotokoll senden“ keine Rückmeldung empfangen hat, sendet die Zentrale das Prüfprotokoll. Wenn die Zentrale innerhalb von 24 Stunden nach der Ausführungszeit des ersten monatlichen zeitgesteuerten Ereignisses „Prüfprotokoll senden“ eine Rückmeldung empfängt, wird das Prüfprotokoll für 24 Stunden ab der letzten Rückmeldung verzögert. Sobald der 24-Stunden-Countdown-Timer abgelaufen ist, sendet die Zentrale das Prüfprotokoll.
Wenn Parameter 2 auf „Geplant“ festgelegt ist und die Zentrale innerhalb von 24 Stunden nach der Ausführungszeit des ersten geplanten zeitgesteuerten Ereignisses „Prüfprotokoll senden“ keine Rückmeldung empfangen hat, sendet die Zentrale das Prüfprotokoll. Wenn die Zentrale innerhalb von 24 Stunden nach der Ausführungszeit des ersten geplanten zeitgesteuerten Ereignisses „Prüfprotokoll senden“ eine Rückmeldung empfängt, wird das Prüfprotokoll für 24 Stunden ab der letzten Rückmeldung verzögert. Sobald der 24-Stunden-Countdown-Timer abgelaufen ist, sendet die Zentrale das Prüfprotokoll.

Protokoll-Routing-Konfiguration
Informationen zur Protokoll-Routing-Konfiguration für Prüfprotokolle, nicht-normale Prüfprotokolle und erweiterte Prüfprotokolle finden Sie unter „Zentralenübergreifende Parameter > Protokoll-Routing > Prüfprotokolle > *Prüfprotokolle, Seite 81*“.

Siehe

- *Prüfprotokolle, Seite 81*
- *Expand Test Report (Prüfprotokoll erweitern), Seite 55*
- *Diagnoseprotokolle, Seite 82*

12.5.22 Prüfprotokoll bei nicht-normalem Zustand senden

Wenn dieses zeitgesteuerte Ereignis ausgeführt wird und ein Melder in einem beliebigen Bereich nicht-normal ist (Störung nicht über Bedienteil-Anzeige gelöscht), sendet die Zentrale ein Protokoll für einen nicht-normalen Zustand. Wenn sich keine Melder in einem nicht-normalen Zustand befinden, wenn dieses zeitgesteuerte Ereignis ausgeführt wird, sendet die Zentrale kein Protokoll.
Wenn der Parameter „Zentralenübergreifende Parameter“ > Protokoll-Routing > *Expand Test Report (Prüfprotokoll erweitern), Seite 55* auf „Ja“ eingestellt, wird nach einem Prüfprotokoll für einen nicht-normalen Zustand für jeden nicht-normalen Systemstatus ein Diagnoseprotokoll erstellt. Eine Liste mit enthaltenen Protokollen finden Sie unter „Zentralenübergreifende Parameter“ > „Protokoll-Routing“ > *Diagnoseprotokolle, Seite 82*.

12.5.23 Go to Area (Gehe zu Bereich)

Diese Funktion emuliert die Bedienteilverknüpfung „Gehe zu Bereich“ und ist nur für benutzerdefinierte Funktionen verfügbar, die über ein Bedienteil aktiviert werden. Wenn diese Funktion aktiviert ist, ändert sich der aktuelle Bereich der Bedienteile in den Bereich, der in „Parameter 1: Bereichs-Nr.“ parametriert ist.

12.5.24 Überwachung einschalten

Diese Funktion emuliert die Bedienteilverknüpfung „Überwachungsmodus ändern“, indem der Überwachungsmodus für die Bereiche aktiviert wird, die in „Parameter 1: Bereichs-Nr.“ parametriert sind. Der Überwachungsmodus löst auf jedem Bedienteil innerhalb des Bereichs ein Zutrittssignal aus, wenn ein unscharfgeschalteter Überwachungsmelder offen ist.

12.5.25 Überwachung ausschalten

Diese Funktion emuliert die Bedienteilverknüpfung „Überwachungsmodus ändern“, indem der Überwachungsmodus für die Bereiche deaktiviert wird, die in „Parameter 1: Bereichs-Nr.“ parametriert sind.

12.5.26 Datum und Uhrzeit anzeigen

Diese Funktion emuliert die Bedienteilverknüpfung „Datum und Uhrzeit anzeigen“, indem auf SDI2-Bedienteilen die Uhrzeit und das Datum angezeigt werden, die im „Parameter 1: Bedienteile-Nr.“ angegeben sind.

Hinweis!
Wenn die Funktion „Datum und Uhrzeit anzeigen“ mit den Funktionen „Bedienteillautstärke festlegen“ und „Bedienteilhelligkeit festlegen“ in derselben benutzerdefinierten Funktion verwendet wird, müssen diese mit der Verzögerungsfunktion ungefähr 10 Sekunden voneinander getrennt werden.

12.5.27 Überwachungston ausgeben

Diese Funktion ist nicht als Bedienteilverknüpfung verfügbar. Falls aktiviert, kann diese Funktion verwendet werden, um auf den SDI2-Bedienteilen, die im „Parameter 1: Bedienteile-Nr.“ angegeben sind, kontinuierlich einen Überwachungston auszugeben, bis der Alarm stummgeschaltet wird.

12.5.28 Bedienteillautstärke festlegen

Mit dieser Funktion werden die konfigurierten Bedienteile, die im „Parameter 1: Bedienteile-Nr.“ angegeben sind, auf die Lautstärkenstufe festgelegt, die im „Parameter 2: Lautstärkenstufe“ eingegeben ist. Informationen zu den Lautstärkeparametern finden Sie unter *Keypad Volume (Bedienteillautstärke), Seite 152* im Bedienteil-Konfigurationsabschnitt.

12.5.29 Bedienteilhelligkeit festlegen

Mit dieser Funktion werden die konfigurierten Bedienteile, die im „Parameter 1: Bedienteile-Nr.“ angegeben sind, auf den Helligkeitsgrad festgelegt, der im „Parameter 2: Helligkeitsgrad“ ausgewählt ist. Informationen zu den Helligkeitsparametern finden Sie unter *Keypad Brightness (Bedienteilhelligkeit), Seite 152* im Bedienteil-Konfigurationsabschnitt.

12.5.30 Störung stummschalten

Diese Funktion ist nicht als Bedienteilverknüpfung verfügbar, kann aber auf andere Weise auf jedem Bedienteil ausgeführt werden. Falls aktiviert, können mit dieser Funktion alle Störungstöne und System-Summer stummgeschaltet werden, die in „Parameter 1: Bereichs-Nr.“ parametriert sind.

12.5.31 Alarm stummschalten

Diese Funktion ist nicht als Bedienteilverknüpfung verfügbar, kann aber auf andere Weise auf jedem Bedienteil ausgeführt werden. Falls aktiviert, können mit dieser Funktion alle Alarme in den Bereichen stummgeschaltet werden, die in „Parameter 1: Bereichs-Nr.“ parametriert sind.

12.5.32 Benutzerdefinierte Funktion ausführen

Mit dieser Funktion wird die benutzerdefinierte Funktion, die in „Parameter 1: Nr. der benutzerdefinierten Funktion“ ausgewählt ist, zur geplanten Zeit ausgeführt.

13 Automatisierung/Remote-App

13.1 Automatisierungsgerät

Standardeinstellung: Kein

Auswahl:

- Kein. Die Automatisierungskommunikation ist deaktiviert.
- Modus 1 verwendet integrierte Verbindung ohne TLS.
- Modus 1 verwendet B42x-Modul an SDI2-Adresse 1.
- Modus 1 verwendet integrierte Verbindung mit TLS.
- Modus 2 verwendet integrierte Verbindung oder B42x-Modul an SDI2-Adresse 1, mit TLS

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

Automatisierung/Remote-App > Automatisierungsgerät

13.2 Status-Rate

Standardeinstellung: 0

Auswahl:

- 0 – Statusinformationen werden nur auf Anforderung gesendet.
- 1 bis 255 – Statusinformationen werden im parametrierten Intervall gesendet.

Mit diesem Parameter wird festgelegt, wie oft die Standardstatusinformationen an den seriellen Koppler gesendet werden.

Die Statusinformationen enthalten den aktuellen Melderstatus (normal oder nicht-normal), den Bereichsstatus der Zentrale (Vollscharfschaltung, unverzögerte Vollscharfschaltung, verzögerte Außenhautüberwachung (scharfgeschaltet), unverzögerte Außenhautüberwachung (scharfgeschaltet), unscharfgeschaltet, Eingangsverzögerung des Bereichs, Eingangsverzögerung Außenhautüberwachung, Scharfschalteverzögerung des Bereichs, Scharfschalteverzögerung Außenhautüberwachung), den Zentralenstatus (Wechselspannung Störung, Batterie fehlt, Wechselspannung Wiederherstellung, schwache Batterie usw.) und den Ausgangsstatus (Ausgang ein oder Ausgang aus).

Die Eingaben werden in Schritten von 500 Millisekunden gemacht. Wenn eine 5 eingegeben wird, werden die Statusinformationen also alle 2.500 Millisekunden (oder alle 2,5 Sekunden) gesendet. Eine Eingabe von 10 entspricht 5 Sekunden. Wenn die Status-Rate auf einen Wert unter 10 festgelegt wird und 1 bis 6 SDI-Geräte an das System angeschlossen sind, beträgt die schnellste Übertragungsgeschwindigkeit der Zentrale ungefähr 1 Sekunde. Wenn mehr als 6 SDI-Geräte an die Zentrale angeschlossen sind, beträgt die schnellste Übertragungsgeschwindigkeit der Zentrale ungefähr 1,5 bis 2 Sekunden.

Melde-Adresse der RPS-Menüstruktur

Automatisierung/Remote-App > Status-Rate

13.3 Automatischer Zugangscode

Standardeinstellung: leer

Auswahl: Bis zu 24 Zeichen.

Mit diesem Parameter wird der Zugangscode festgelegt, der eingegeben werden muss, bevor die Automatisierungssoftware mit der Zentrale verbunden werden kann.

Für diesen Parameter sind Zugangscodes mit einer Länge von 24 Zeichen oder weniger zulässig. Die minimale Länge beträgt 6 Zeichen. Beim Zugangscode muss die Groß-/Kleinschreibung beachtet werden. Der automatische Zugangscode muss eingegeben werden, bevor andere Automatisierungsbefehle von der Zentrale akzeptiert werden.

Melde-Adresse der RPS-Menüstruktur
Automatisierung/Remote App > Automatischer Zugangscode

13.4 Modus 1 – Automatisierung Ethernet-Port-Nummer

Standardeinstellung: 7702
Optionen: 1 bis 65535
Mit diesem Parameter wird die Port-Nummer für Modus 1 – Automatisierung Ethernet festgelegt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Automatisierung/Remote-App > Modus 1 – Automatisierung Ethernet-Port-Nummer

13.5 Remote-App

Standardeinstellung: Aktiviert
Auswahl:
- Aktivieren – die Zentrale kann sichere Verbindungen mit Remote-Apps herstellen.
- Deaktivieren – die Zentrale kann keine sicheren Verbindungen mit Remote-Apps herstellen.

Legen Sie diesen Parameter auf „Aktivieren“ fest, damit die Zentrale sichere Verbindungen mit Remote-Apps herstellen kann. Die App „Bosch Remote Security Control“ für Smartphones und Tablets ist ein Beispiel für eine Remote-App.
Legen Sie diesen Parameter auf „Deaktivieren“ fest, um zu verhindern, dass die Zentrale sichere Verbindungen mit Remote-Apps herstellt.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Automatisierung/Remote-App > Remote-App

13.6 Remote-App-Zugangscode

Standardeinstellung: [RPS generiert einen zufälligen 24-stelligen Zugangscode]
Optionen: Bis zu 24 Zeichen
Verwenden Sie diesen Parameter, um den Zugangscode festzulegen, den die Zentrale von einer Remote-Anwendung empfängt, um eine sichere Verbindung herzustellen (Smartphone mit App „Bosch Remote Security Control“ ist ein Beispiel für eine Anwendung).
Die Länge des Zugangscodes beträgt 6 bis 24 Zeichen. Der Zugangscode kann eine Kombination aus Buchstaben, Zahlen und Sonderzeichen sein. Beim Zugangscode muss die Groß-/Kleinschreibung beachtet werden. Der Anwendungs-Zugangscode muss empfangen werden, bevor die Zentrale andere Befehle von der Remote-Anwendung akzeptiert.
RPS generiert automatisch einen zufälligen 24-stelligen Zugangscode als Standardeinstellung, wenn Sie ein Zentralenkonto erstellen.

Hinweis!
Durch Festlegen von „Remote-App-Zugangscode“ auf „Deaktiviert“ wird die Remote-App-Anmeldung deaktiviert
Um zu verhindern, dass ein Remote-App-Benutzer (RSC-Benutzer) sich an der Zentrale anmeldet, auch wenn der Parameter „Remote-App“ auf „Aktiviert“ festgelegt ist, legen Sie „Remote-App-Zugangscode“ auf „Deaktiviert“ fest (beliebige Kombination aus Groß- und Kleinbuchstaben).

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
Automatisierung/Remote-App > Remote-App-Zugangscode

14 SDI2-Module

14.1 B208-Octo-Eingang

Das B208-Octo-Eingangsmodul stellt Eingänge (Meldeleitungen) für 8 Melder bereit. Das B208 wird an den SDI2-Bus der Zentrale angeschlossen.

Zentralentyp	Unterstützte Module
B5512	4
B4512	2
B3512	0

Tab. 14.1: Kapazität

Schaltereinstellungen
Siehe „Einstellungen des Hardwareschalters“ > „Schaltereinstellungen für das B208-Modul mit acht Eingängen“

14.1.1 Gehäusesabotage

Standardeinstellung: No – Deaktiviert
Auswahl:
– Ja – Gehäusesabotageeingang aktiviert
– Nein – Gehäusesabotageeingang deaktiviert
Wenn der Sabotageeingang aktiviert und mit einem Bosch ICP-EZTS Sabotagekontakt verbunden ist, erzeugt die Zentrale ein Sabotageereignis, wenn die Gehäusetür geöffnet oder des Gehäuse von der Wand entfernt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2-Module > B208-Octo-Eingang > Gehäusesabotagekontakt

14.2 B308-Octo-Ausgang

Der B308-Octo-Ausgang ist ein Gerät, das an den SDI2-Bus der Zentrale angeschlossen wird. Jedes Modul stellt 8 unabhängig überwachte Ausgänge bereit, die ähnlich funktionieren wie die, die von den Ausgangsmodulen bereitgestellt werden.

Zentralentyp	Unterstützte Module
B5512	5
B4512	3
B3512	0

Tab. 14.2: Kapazität

Schaltereinstellungen
Siehe „Einstellungen des Hardwareschalters“ > „Schaltereinstellungen für B308-Modul mit acht Ausgängen“

14.2.1 Modul-Gehäusesabotagekontakt

Standardeinstellung: No – Deaktiviert
Auswahl:
– Ja – Gehäusesabotageeingang aktiviert
– Nein – Gehäusesabotageeingang deaktiviert

Wenn der Sabotageeingang aktiviert und mit einem Bosch ICP-EZTS Sabotagekontakt verbunden ist, erzeugt die Zentrale ein Sabotageereignis, wenn die Gehäusetür geöffnet oder des Gehäuse von der Wand entfernt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2-Module > B308-Octo-Ausgang > Gehäusesabotagekontakt

14.3 (B42x) IP-Übertragungsgerät

Anschließen von B42x
Schließen Sie das Modul mit dem SDI2-Bus an die Zentrale an.

Konfigurieren des Moduls
Sie können ein oder beide B426/B450-Übertragungsmodule für Bedienteilmeldungen oder die RPS-Kommunikation verwenden. Alternativ können Sie eines der B42x-Module für die Kommunikation mit der Automatisierungssoftware verwenden.

Hinweis!
Um einen Kommunikationsausfall zu vermeiden, wird die an die Zentrale gesendete Konfiguration für das B42x-Modul erst wirksam, nachdem die RPS-Verbindung zur Zentrale getrennt wurde.
Wenn das Modul über die B42x-Konfigurationsweboberfläche so konfiguriert wurde, dass die Parametrierung der Zentrale deaktiviert wird (d. h. „Zentralenparametrierung aktivieren“ ist auf „Nein“ festgelegt), dann wird die RPS-Parametrierung des B42x-Moduls von der Zentrale akzeptiert, aber nicht auf das B42x-Modul angewendet. Die Parameter „Zentralenparametrierung aktivieren“ ist nicht in RPS verfügbar.

14.3.1 Modul-Gehäusesabotagekontakt

Standardeinstellung: No – Deaktiviert
Auswahl:
– Ja – Gehäusesabotageeingang aktiviert
– Nein – Gehäusesabotageeingang deaktiviert

Wenn der Sabotageeingang aktiviert und mit einem Bosch ICP-EZTS Sabotagekontakt verbunden ist, erzeugt die Zentrale ein Sabotageereignis, wenn die Gehäusetür geöffnet oder des Gehäuse von der Wand entfernt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät >Gehäusesabotagekontakt

14.3.2 IPv6-Modus

Standardeinstellung: Nein
Auswahl:
– Ja: IPv6-Modus (Internet Protocol Version 6) für die IP-Kommunikation verwenden.
– Nein: IPv4-Modus (Internet Protocol Version 4) für die IP-Kommunikation verwenden

Wenn „IPv6 aktivieren“ auf „Ja“ eingestellt ist, setzen Sie „DHCP/AutoIP Enable“ (DHCP/AutoIP aktivieren) auf „Ja“.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät > IPv6-Modus

14.3.3 IPv6 DHCP

Standardeinstellung: Aktiviert (Ja)
Auswahl:

– Aktiviert (Ja): DHCP legt IP-Adresse, IP-Standard-Gateway und IP-DNS-Serveradresse automatisch fest. Mit AutoIP werden Geräten bei Inbetriebnahme dynamische IP-Adressen zugewiesen.
– Deaktiviert (Nein): Setzen Sie diesen Parameter auf „Deaktiviert“, wenn kein DHCP-Dienst vorhanden ist. Legen Sie IP-Adresse, IP-Standard-Gateway und IP-DNS-Serveradresse manuell fest.

DHCP erfordert einen DHCP-Server.

RPS Menu Locations (Meldeadressen des Menüs „RPS“)

SDI2 > B42x-IP-Übertragungsgerät > IPv6 DHCP

14.3.4 IPv4 DHCP/AutoIP Enable (IPv4 DHCP/AutoIP aktivieren)

Standardeinstellung: Aktiviert (Ja)

Auswahl:

– Aktiviert (Ja): DHCP legt IP-Adresse, IP-Standard-Gateway und IP-DNS-Serveradresse automatisch fest. Mit AutoIP werden Geräten bei Inbetriebnahme dynamische IP-Adressen zugewiesen.
– Deaktiviert (Nein): Setzen Sie diesen Parameter auf „Deaktiviert“, wenn kein DHCP-Dienst vorhanden ist. Legen Sie IP-Adresse, IP-Standard-Gateway und IP-DNS-Serveradresse manuell fest.

DHCP erfordert einen DHCP-Server.

Der Parameter hat keine Auswirkung auf den Betrieb der steckbaren B450 Mobilfunkübertragungsgerät-Schnittstelle.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

SDI2 > B42x-IP-Übertragungsgerät > IPv4 DHCP/AutoIP aktivieren

14.3.5 IPv4-Adresse

Standardeinstellung: 0.0.0.0

Auswahl: 0.0.0.0 bis 255.255.255.255

Falls „DHCP/Auto IP Enable“ (DHCP/Auto IP aktivieren) für IPv4 auf „Ja“ gesetzt ist, wird dieser Parameter grau dargestellt (kein Zugriff).

Wenn „DHCP/Auto IP Enable“ (DHCP/Auto IP aktivieren) für IPv4 auf „Nein“ gesetzt ist, geben Sie hier die IPv4-Adresse an.

Dieser Parameter hat keine Auswirkung auf den Betrieb der steckbaren B450 Mobilfunkübertragungsgerät-Schnittstelle.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

SDI2 > B42x-IP-Übertragungsgerät > IPv4-Adresse

14.3.6 IPv4-Subnetzmaske

Standardeinstellung: 255.255.255.0

Auswahl: 0.0.0.0 bis 255.255.255.255

Falls „DHCP/Auto IP Enable“ (DHCP/Auto IP aktivieren) für IPv4 auf „Ja“ gesetzt ist, wird dieser Parameter grau dargestellt (kein Zugriff).

Wenn „DHCP/Auto IP“ für IPv4 auf „Nein“ gesetzt ist, geben Sie hier die IPv4-Subnetzmaske ein.

Der Parameter hat keine Auswirkung auf den Betrieb der steckbaren B450 Mobilfunkübertragungsgerät-Schnittstelle.

Weitere Informationen

Formate von IP-Adresse und Domainname, Seite 300

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät > IPv4-Subnetzmaske

14.3.7 IPv4-Standard-Gateway

Standardeinstellung: 0.0.0.0
Auswahl: 0.0.0.0 bis 255.255.255.255
Falls „DHCP/Auto IP Enable“ (DHCP/Auto IP aktivieren) für IPv4 auf „Ja“ gesetzt ist, wird dieser Parameter grau dargestellt (kein Zugriff).
Ist „DHCP/Auto IP Enable“ (DHCP/Auto IP aktivieren) für IPv4 auf „Nein“ gesetzt, geben Sie hier die Standard-Gateway-Adresse an.
Der Parameter hat keine Auswirkung auf den Betrieb der steckbaren B450 Mobilfunkübertragungsgerät-Schnittstelle.

Weitere Informationen
Formate von IP-Adresse und Domainname, Seite 300

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät > IPv4-Standard-Gateway

14.3.8 IPv4 DNS Server IP Address (IPv4-DNS-Server-IP-Adresse)

Standardeinstellung: 0.0.0.0
Auswahl: 0.0.0.0 bis 255.255.255.255
Ein Domain Name Server (DNS) setzt Internet-Domainnamen und Hostnamen in die entsprechenden IP-Adressen um. Im DHCP-Modus wird der Standard-DNS des DHCP-Servers verwendet. Geben Sie die IP-Adresse des benutzerdefinierten DNS-Servers ein, um einen benutzerdefinierten DNS-Server im DHCP-Modus zu nutzen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät > IPv4-DNS-Server-IP-Adresse

14.3.9 IPv6-DNS-Server-IP-Adresse

Standardeinstellung:
Auswahl: 0000:0000:0000:0000:0000:0000:0000:0000 bis FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Mit diesem Parameter wird die IPv6-DNS-Server-IP-Adresse auf den Modus „statische IP-Adresse“ eingestellt.
Ändern Sie diese Adresse nicht, wenn sie mit dem DHCP-Dienst festgelegt wurde.

Weitere Informationen
Formate von IP-Adresse und Domainname, Seite 300

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät > IPv6-DNS-Server-IP-Adresse

14.3.10 UPnP (Universal Plug & Play) aktivieren

Standardeinstellung: „Ja“
Auswahl:
Ja (Aktiviert): UPnP zum Öffnen einer Port-Weiterleitung für eingehende RPS- und RSC (Remote Security Control)-Verbindungen verwenden
Nein (Deaktiviert): kein UPnP verwenden
Der Parameter „UPnP“ hat keine Auswirkung auf die Übermittlung von Ereignissen an Bedienteilempfänger.
Der UPnP-Parameter hat keine Auswirkung auf den Betrieb der steckbaren B450 Mobilfunkübertragungsgerät-Schnittstelle.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät > UPnP aktivieren

14.3.11 HTTP-Portnummer

Standardeinstellung: 80
Optionen: 1 bis 65535
Mit diesem Parameter wird die Konfiguration der Webserver-Portnummer ermöglicht.
Wenn die erweiterte TLS-Sicherheit aktiviert ist, gilt HTTPS. Der Standardwert für HTTPS ist 443.
Wenn die erweiterte TLS-Sicherheit nicht aktiviert ist, wird der HTTP-Wert angewendet.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2-Module > IP-Übertragungsgerät > HTTP-Portnummer

14.3.12 ARP-Cache-Timeout (Sek.)

Standardeinstellung: 600
Auswahl: 1 bis 600 (Sekunden)
Mit diesem Parameter wird das Timeout für ARP-Cacheeinträge festgelegt.
Der Parameter hat keine Auswirkung auf den Betrieb der steckbaren B450 Mobilfunkübertragungsgerät-Schnittstelle.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät > ARP-Cache-Timeout

14.3.13 Zugriff über Webbrowser/USB

Standardeinstellung: Nein
Auswahl: Yes/No
Dieser Parameter ermöglicht autorisierten Benutzern abhängig von verfügbaren Optionen, die Konfigurationsparameter des Moduls über einen Standard-Webbrowser oder eine USB-Schnittstelle anzuzeigen und zu bearbeiten.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2-Module > IP-Übertragungsgerät > Zugriff über Webbrowser/USB

14.3.14 Passwort für Zugriff über Webbrowser/USB

Standardeinstellung: leer
Auswahl: leer, druckbare ASCII-Zeichen
Dieser Parameter legt ein neues Passwort fest, das für die direkte Anmeldung per Webzugriff erforderlich ist. Das Passwort muss 4 bis 10 druckbare ASCII-Zeichen lang sein. Leerzeichen verhindern die Überprüfung des Passworts.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > IP-Übertragungsgerät > Passwort für den Webzugriff

14.3.15 Firmware-Upgrade aktivieren

Standardeinstellung: Nein
Auswahl:
Ja – die Firmware wird über die Webschnittstelle geändert.
Nein – die Firmware wird über die Parametriersoftware geändert.
Mit diesem Parameter wird ermöglicht, dass die Firmware des Moduls über die externe Weboberfläche geändert werden kann.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2-Module > IP-Übertragungsgerät > Firmware-Upgrade aktivieren

14.3.16 Hostname des Moduls

Standardeinstellung: leer

Auswahl: bis zu 63 Zeichen (Buchstaben, Zahlen, Punkte und Striche)

Der Hostname identifiziert das IP-Übertragungsgerät (integriert oder SDI2-Modul) im Netzwerk. Lassen Sie diesen Parameter leer, um den werksseitigen Standardhostnamen zu verwenden.

Der Parameter hat keine Auswirkung auf den Betrieb der steckbaren B450 Mobilfunkübertragungsgerät-Schnittstelle.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

SDI2 > B42x-IP-Übertragungsgerät > Hostname des Moduls

14.3.17 Modulbeschreibung

Standardeinstellung: Leer

Optionen: Bis zu 20 alphanumerische Zeichen.

Mithilfe dieses Parameters wird das Modul (Standort, Merkmale usw.) mit bis zu 20 Zeichen beschrieben.

Verwenden Sie nur die folgenden Zeichen: A bis Z, 0 bis 9, ?, &, @, -, *, +, $, #, /

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

SDI2-Module > IP-Übertragungsgerät > Modulbeschreibung

14.3.18 TCP/UDP Port Number (TCP/UDP-Portnummer)

Standardeinstellung: 7700

Auswahl: 0 bis 65535

Ändern Sie den Standardwert des TCP/UDP-Ports nicht bei IP-Kommunikation mit RPS, Automatisierung oder Remote Security Control (RSC) in typischen Installationen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

SDI2-Module > IP-Übertragungsgerät > TCP/UDP-Portnummer

14.3.19 TCP Keep-Alive-Zeit

Standardeinstellung: 4 Minuten

Auswahl: Aus – 8 Stunden

Zeit zwischen TCP Keep-Alive-Zeit-Meldungen kann in Minuten oder Stunden festgelegt werden. Keep-Alive-Meldungen stellen sicher, dass eine Verbindung aktiv bleibt.

Der Parameter hat keine Auswirkung auf den Betrieb der steckbaren B450 Mobilfunkübertragungsgerät-Schnittstelle.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

SDI2 > B42x-IP-Übertragungsgerät > TCP Keep-Alive-Zeit

14.3.20 IPv4-Testadresse

Standardeinstellung: 8.8.8.8

Auswahl: IPv4-Adresse oder Domänenname

Die Zentrale sendet einen Ping-Befehl an die IPv4-Testadresse, um sicherzustellen, dass die Netzwerkkonfigurationseinstellungen korrekt sind und das Netzwerk in Betrieb ist.

Die Standard-Testadresse eignet sich für die meisten Netzwerke.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

SDI2 > B42x-IP-Übertragungsgerät > IPv4-Testadresse

14.3.21 IPv6-Testadresse

Standardeinstellung: 2001:4860:4860::8888

Auswahl: IPv6-Adresse oder Domänenname

Die Zentrale sendet einen Ping-Befehl an die IPv6-Testadresse, um sicherzustellen, dass die Netzwerkkonfigurationseinstellungen korrekt sind und das Netzwerk in Betrieb ist.
Die Standard-Testadresse eignet sich für die meisten Netzwerke.

Weitere Informationen
Formate von IP-Adresse und Domainname, Seite 300

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät > IPv6-Testadresse

14.3.22 Sicherheit bei Webzugriff und Automatisierung

Standardeinstellung: Aktivieren
Auswahl:
– Deaktivieren – erweiterte Sicherheit wird nicht angewendet.
– Aktivieren – erweiterte Sicherheit wird angewendet.

Legen Sie diesen Parameter auf „Aktivieren“ fest, um für die Automatisierung und den B42x-Webzugriff eine erweiterte Sicherheit zu aktivieren.
Bei Aktivierung erfolgt der B42x-Webzugriff über HTTPS, und es wird der Standardwert des Parameters „HTTP-Portnummer“ geändert. Durch diese Einstellung wird auch die TLS-Sicherheit für die Automatisierung aktiviert.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > IP-Übertragungsgerät > Sicherheit bei Webzugriff und Automatisierung

14.3.23 IP-Adresse des alternativen IPv4-DNS-Servers

Standardeinstellung: 0.0.0.0
Auswahl: 0.0.0.0 bis 255.255.255.255
Wenn das IP-Übertragungsgerät keine Adresse vom primären Server abrufen kann, wiederholt es den Vorgang mit dem alternativen DNS-Server. Geben Sie die IP-Adresse für den alternativen IPv4-DNS-Server ein.

Weitere Informationen
Formate von IP-Adresse und Domainname, Seite 300

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät > Alternative IPv4-DNS-Server-IP-Adresse

14.3.24 IP-Adresse des alternativen IPv6-DNS-Servers

Standardeinstellung:
Auswahl: 0000:0000:0000:0000:0000:0000:0000:0000 bis
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Wenn das IP-Übertragungsgerät keine Adresse vom primären Server abrufen kann, wiederholt es den Vorgang mit dem alternativen DNS-Server. Geben Sie die IP-Adresse des alternativen IPv6-DNS-Servers ein.

Weitere Informationen
Formate von IP-Adresse und Domainname, Seite 300

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B42x-IP-Übertragungsgerät > Alternative IPv6-DNS-Server-IP-Adresse

14.4 B450 Mobilfunk

14.4.1 Eingehende SMS

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: Yes
Auswahl:
– Aktiviert (Ja): Sie können das Modul mit eingehenden SMS-Textnachrichten konfigurieren.
– Deaktiviert (Nein): Das Modul verarbeitet keine eingehenden SMS-Textnachrichten.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunk > Eingehende SMS

14.4.2 Dauer des Sitzungs-Keep-Alive (Min.)

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: 0
Auswahl: 0 (deaktiviert) bis 1000 (Minuten)
Zeit in Minuten zwischen Keep-Alive-Meldungen. Keep-Alive-Meldungen stellen sicher, dass eine Verbindung aktiv bleibt.
Ändern Sie die Standardeinstellung nur für gewerbliche Hochsicherheitsanwendungen gemäß UL 1610.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunk > Dauer des Sitzungs-Keep-Alive (Min.)

14.4.3 Inaktivitäts-Timeout (Min.)

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: 0
Auswahl: 0 (deaktiviert) bis 1000 (Minuten)
– 0 (deaktiviert) – Zentrale überwacht den Datenverkehr nicht.
– 1 bis 1000 – Die Dauer ohne Datenverkehr, bevor die Zentrale eine Sitzung beendet.
Ändern Sie die Standardeinstellung nur für gewerbliche Hochsicherheitsanwendungen gemäß UL 1610, bei denen eine Benachrichtigung bei geringer Signalstärke erforderlich ist.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunk > Eingehende SMS

14.4.4 Reporting Delay for Low Signal Strength (sec.) (Reportverzögerung bei geringer Signalstärke in Sek.)

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: 0 (deaktiviert)
Auswahl: 0 (deaktiviert), 1-3600 (Sekunden)
Dauer mit geringer Signalstärke (rote LED auf Mobilfunkübertragungsgerät), bevor die Zentrale kann ein Ereignis zur geringen Mobilfunksignalstärke erstellt.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunk > Reportverzögerung bei geringer Signalstärke

14.4.5 Reportverzögerung bei nur einem Funkmast (s)

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: 1800
Auswahl: 0 (deaktiviert) bis 3600 (Sekunden)
Lassen Sie den Standardwert dieses Parameters unverändert, sofern Sie nicht von einem Vertreter von Bosch Security Systems, Inc. dazu angewiesen werden.
Wenn das steckbare Mobilfunkmodul für die bei diesem Parameter festgelegte Sekundenzahl nur einen Funkmast erkennt, erstellt die Zentrale ein Ereignis zu nur einem Funkmast.
Wenn das Mobilfunkübertragungsgerät für die bei diesem Parameter festgelegte Sekundenzahl mindestens zwei Funkmasten erkennt, erstellt die Zentrale ein Wiederherstellungsereignis zu nur einem Funkmast.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunk > Reportverzögerung bei nur einem Funkmast

14.4.6 Reporting Delay for No Towers (sec.) (Reportverzögerung bei fehlenden Funkmasten in Sek.)

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: 0
Auswahl: 0 (deaktiviert) bis 3600 (Sekunden)
Wenn das steckbare Mobilfunkmodul für die bei diesem Parameter festgelegte Sekundenzahl keine Funkmasten erkennt, erstellt die Zentrale ein Ereignis zu fehlenden Funkmasten und fehlender IP-Adresse.

Die Zentrale erstellt ein Wiederherstellungsereignis zu fehlenden Funkmasten, wenn das steckbare Mobilfunkmodul für die bei diesem Parameter festgelegte Sekundenzahl mindestens einen Funkmast erkennt.
Die Zentrale erstellt ein Wiederherstellungsereignis zur fehlenden IP-Adresse, wenn das steckbare Mobilfunkmodul innerhalb von 60 Sekunden bei mindestens einem Funkmast registriert ist und eine IP-Adresse erhalten hat.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunk > Reportverzögerung bei fehlenden Funkmasten

14.4.7 Outgoing SMS Length (Länge ausgehender SMS)

Standardeinstellung: 160
Auswahl: 0 (deaktiviert) bis 3600 (Zeichen)
Mobilfunkanbieter legen den Grenzwert für die Länge von SMS-Nachrichten auf 160 Zeichen fest (Standardeinstellung). SMS-Nachrichten, die diesen Grenzwert überschreiten, werden von den Anbietern zurückgewiesen.

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunk > Länge ausgehender SMS

14.4.8 SIM-PIN

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: Leer
Auswahl: 0-9 (min. 4 Stellen, max. 8 Stellen)
Verwenden Sie diesen Parameter nur, wenn eine PIN für SIM-Karten erforderlich ist.
Wenn keine SIM-PIN erforderlich ist, lassen Sie das Feld leer.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunk > SIM-PIN

14.4.9 Name des Netzwerkzugriffspunkts (APN)

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: eaaa.bosch.vzwentp
Auswahl: 0-9, A-Z, a-Z, **-**, **:**, **.** (bis zu 99 Zeichen)
Wenn Sie den Standardnamen des Access-Point-Names (APN) ändern möchten, können Sie bis zu 99 Zeichen eingeben. Groß- und Kleinschreibung muss beachtet werden.

Zentralenfirmware-Version 3.07 oder höher
Mit Zentralenfirmware-Version 3.07 oder höher verwendet die Zentrale eine interne Liste mit Werten für Namen des Netzwerkzugangspunkts, wenn der APN-Parameter leer ist. Wenn ein steckbares B442- oder B443-Mobilfunkübertragungsgerät angeschlossen wird, sieht die interne Liste folgendermaßen aus:
– lotst.aer.net
– gne
– wyless.apn
– wyless.com.attz
Wenn ein steckbares B444-Mobilfunkübertragungsgerät angeschlossen wird, sieht die interne Liste folgendermaßen aus:
– bssd.vzwentp
– eaaa.Bosch.vzwentp

Hinweis!
Der Standard eaaa.bosch.vzwentp ist neu.
Der vorherige APN-Standard, wyless.apn, ist immer noch gültig. Es ist nicht erforderlich, den APN für vorhandene Konten zu ändern.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunk > Name des Netzzutrittskontrollpunkts (APN)

14.4.10 Network Access Point User Name (Benutzername des Netzwerkzugriffspunkts)

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: Leer
Auswahl: ASCII-Zeichen (bis zu 30)
Der Benutzername für den Netzwerkzugriffspunkt kann bis zu 30 ASCII-Zeichen lang sein. Beim Benutzernamen muss die Groß-/Kleinschreibung beachtet werden.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunkt > Benutzername des Netzzutrittskontrollpunkts

14.4.11 Passwort des Netzwerkzugriffspunkts

Hinweis!
Wichtige Konfigurationsinformationen zur Mobilfunkkommunikation
Siehe *Konfigurieren für den Mobilfunkdienst, Seite 297*, um eine Übersicht und Konfigurationsinformationen zu erhalten.

Standardeinstellung: Leer
Auswahl: ASCII-Zeichen (bis zu 30 Zeichen)
Das Passwort für den Netzwerkzugriffspunkt kann bis zu 30 ASCII-Zeichen lang sein. Beim Passwort muss die Groß-/Kleinschreibung beachtet werden.

Melde-Adresse des Menüs „RPS“
SDI2-Module > IP-Übertragungsgerät > B450 Mobilfunk > Passwort des Netzzutrittskontrollpunkts

14.5 B520 zusätzliches Netzteil

Das zusätzliche Netzteil B520 wird an den SDI2-Bus der Zentrale angeschlossen. Es stellt ein überwachtes 12-Volt-DC-2,5 A-Hilfsstromnetzteil bereit.

Zentralentyp	Unterstützte Module
B6512, B5512	4
B4512	2
B3512	1

Tab. 14.3: Kapazität

Schaltereinstellungen
Siehe „Einstellungen des Hardwareschalters“ > SDI2-Geräte > *Schaltereinstellungen für B520-Netzteil, Seite 296*

Siehe
– *Schaltereinstellungen für B520-Netzteil, Seite 296*

14.5.1 Modul aktivieren

Standardeinstellung: Nein
Auswahl:
– Ja – Das SDI2-Modul wird überwacht.
– Nein – Das SDI2-Modul wird nicht überwacht.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SD12 > B520-Netzteil > Modul aktivieren

14.5.2 Modul-Gehäusesabotagekontakt

Standardeinstellung: No – Deaktiviert
Auswahl:
– Ja – Gehäusesabotageeingang aktiviert
– Nein – Gehäusesabotageeingang deaktiviert
Wenn der Sabotageeingang aktiviert und mit einem Bosch ICP-EZTS Sabotagekontakt verbunden ist, erzeugt die Zentrale ein Sabotageereignis, wenn die Gehäusetür geöffnet oder des Gehäuse von der Wand entfernt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > B520 Zusätzliches Netzteil > Gehäusesabotagekontakt

14.5.3 Ein oder zwei Batterien

Standardeinstellung:: Eine
Auswahl:
– Eine – An die B520-BATT 1-Anschlüsse wird eine Batterie angeschlossen.
– Zwei – Zwei Batterien werden an das B520 angeschlossen. Eine Batterie wird an die BATT 1-Anschlüsse und eine Batterie an die BATT 2-Anschlüsse angeschlossen.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2-Module > B520 Zusätzliches Netzteil > Ein oder zwei Batterien

14.6 Funkempfänger

Die Zentrale unterstützt zwei Arten von SDI2-Funk-Kopplern.

– B810 RADION receiver SD
– B820 Inovonics SDI2-Bus-Schnittstelle

Sie können jeweils nur ein Funk-Koppler verwenden.

Hinweis!
Wählen Sie die Art des Funk-Kopplers aus, **bevor** Sie dem System Melder, Benutzer oder Repeater hinzufügen. Wenn Sie die Funk-Koppler ändern, setzt RPS alle HF-Informationen auf die werksseitigen Standardeinstellungen zurück. Alle zuvor konfigurierten HF-Informationen werden gelöscht.

Schaltereinstellungen
Siehe *Einstellungen des Hardwareschalters, Seite 293*

14.6.1 Typ des Funkmoduls

Standardeinstellung: B810 RADION Wireless
Auswahl:

– Unassigned (Nicht zugewiesen)
– B810 RADION Wireless
– B820 Inovonics Wireless

Mit diesem Parameter wird das System für ein Funkmodul von RADION oder Inovonics konfiguriert.
Unassigned (Nicht zugewiesen). Sie können eine Funkkomponente nicht verwenden. Funk ist keine gültige Auswahl für den Parameter „Melderquelle“ für einen beliebigen Melder. Sie können Funk-Handsender für keinen Benutzer registrieren.

Kapazität des B820 Inovonics Wireless
Geräte: 350 (ohne Repeater)
Repeater: 4
Sie können Inovonics-Funkgeräte keinen Meldern zuweisen.
Sie können Inovonics-Funk-Handsender Benutzern zuweisen.

Kapazität des B810 RADION Wireless
Funk-Handsender: 1000
Melder: 504 (gültige Meldernummern: B5512 – 9 bis 48, B4512 – 9 bis 28 B3512 – 9 bis 16)
Repeater: 8
Wenn diese Grenzwerte erreicht sind, zeigt RPS eine Warnmeldung an. Zum Hinzufügen eines anderen Geräts dieses Typs löschen Sie mindestens eines der vorhandenen Geräte.
Melde-Adresse des Menüs „RPS“
SDI2 Modul > Funkempfänger > Funkmodultyp

14.6.2 Modul-Gehäusesabotagekontakt

Standardeinstellung: Nein – Deaktiviert
Auswahl:

– Ja – Gehäusesabotageeingang aktiviert
– Nein – Gehäusesabotageeingang deaktiviert

Wenn der Sabotageeingang aktiviert ist, erstellt die Zentrale ein Sabotageereignis, wenn das Gehäuse geöffnet oder von der Wand entfernt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)
SDI2 > Funkempfänger > Gehäusesabotagekontakt

14.6.3 Systemüberwachungsdauer (Repeater)

Standardeinstellung:: 12 Stunden

Auswahl:

– Keine: Überwachung des Funkrepeaters deaktivieren.
– 4, 12, 24, 48, 72 Stunden

Dieser Parameter legt die Überwachungsdauer für alle konfigurierten Funkrepeater fest. Wenn der Funkempfänger nicht innerhalb der anhand dieses Parameters festgelegten Stunden eine Antwort vom Repeater erhält, erstellt die Zentrale ein Ereignis aufgrund eines fehlenden Repeaters.

Hinweis!

Überwachungsdauer des Funkmelders

Konfigurieren Sie die Funküberwachungsdauer für Nicht-Feuermelder anhand des Parameters Melderprofile/*Überwachungsdauer des Funkmelders, Seite 247*. Die Überwachungsdauer für Funkmelder für Feuermelder ist auf 4 Stunden festgelegt.

Hinweis!

Überwachungsdauer für Funk-Handsender

Aktivieren oder deaktivieren Sie die Überwachungsdauer für Funk-Handsender mit dem Parameter Benutzerzuordnungen/*Überwacht, Seite 180*. Bei aktivierter Überwachung ist die Überwachungsdauer der Funk-Handsender auf 4 Stunden festgelegt.

Melde-Adresse des Menüs „RPS“

SDI2 > Funkempfänger > Systemüberwachungsdauer

14.6.4 Signalton bei schwacher Batterie

Standardeinstellung:: kein Signalton

Auswahl: kein Signalton, 4 Stunden, 24 Stunden

Dieser Parameter ist für alle Nicht-Feuermelder global. Die Zentrale behebt den Fehler bei schwacher Batterie (24 Stunden) für Feuermelder automatisch.

Melde-Adresse des Menüs „RPS“

SDI2-Module > Funkempfänger > Signalton bei schwacher Batterie

14.6.5 Störungserkennung aktivieren

Standardeinstellung: „Ja“

Auswahl:

– Ja: Erkennung von Funkstörungen (Interferenzen) aktivieren.
– Nein: Erkennung von Funkstörungen (Interferenzen) deaktivieren.

Für das B820 Inovonics Wireless-Modul ist die Erkennung von Funkstörungen (Interferenzen) stets aktiviert, wenn dieser Parameter auf „Nein“ gesetzt ist.

Melde-Adresse des Menüs „RPS“

SDI2-Module > Funkempfänger > Störungserkennung aktivieren

14.7 Wireless Repeater (Funkrepeater)

Funkrepeater sind nicht physisch mit dem SDI2-Bus verbunden. Konfigurieren Sie ein Funkschnittstellenmodul als Teil des Systems.

Die Zentrale unterstützt zwei Typen von SDI2-Funkschnittstellenmodulen:

– B810 RADION Wireless
– B820 Inovonics Wireless

Der Typ des Funkrepeaters muss dem Typ des Empfängers entsprechen. Wählen Sie den Typ des Funkempfängers, bevor Sie Repeater konfigurieren. Die Zentrale unterstützt bis zu 8 Repeater gleichzeitig. Alle Repeater müssen denselben Typ aufweisen.

14.7.1 Modul-Gehäusesabotagekontakt

Standardeinstellung: Nein – Deaktiviert

Auswahl:

– Ja – Gehäusesabotageeingang aktiviert

– Nein – Gehäusesabotageeingang deaktiviert

Wenn der Sabotageeingang aktiviert ist, erstellt die Zentrale ein Sabotageereignis, wenn das Gehäuse geöffnet oder von der Wand entfernt wird.

RPS Menu Location (Melde-Adresse des Menüs „RPS“)

SDI2 > Funkrepeater > Gehäusesabotagekontakt

14.7.2 RADION RFID (B810)

Standardeinstellung: 0

Auswahl: 0, 11 - 167772156

Die RFID (Radio Frequency Device Identification Number) ist eine eindeutige Nummer, die Funkkomponenten im Werk zugewiesen ist. Die RFID befindet sich auf dem Typenschild des Produkts.

Da es sich bei Funkrepeatern um Empfänger und Sender handelt, wird ihnen eine RFID zugewiesen.

Melde-Adresse des Menüs „RPS“

SDI2-Module > Funkrepeater > RFID (B810 RADION Wireless)

14.7.3 Inovonics RFID (B820)

Standardeinstellung: k.a.

Reichweite: 0 - 99999999

Die RFID (Radio Frequency Device Identification Number) ist eine eindeutige Nummer, die Funkkomponenten im Werk zugewiesen ist. Die RFID befindet sich auf dem Typenschild des Produkts.

Da es sich bei Funkrepeatern um Empfänger und Sender handelt, wird ihnen eine RFID zugewiesen.

Melde-Adresse des Menüs „RPS“

SDI2-Module > Funkrepeater > RFID (B820 Inovonics Wireless)

15 Einstellungen des Hardwareschalters

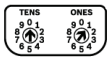
15.1 Bedienteil-Adresse

Adresse für Schaltereinstellungen des grundlegenden B91x-Bedienteils

Adresse	Schalter					
	1	2	3	4	5	6
1	ON	OFF	OFF	OFF	OFF	OFF
2	OFF	ON	OFF	OFF	OFF	OFF
3	ON	ON	OFF	OFF	OFF	OFF
4	OFF	OFF	ON	OFF	OFF	OFF
5	ON	OFF	ON	OFF	OFF	OFF
6	OFF	ON	ON	OFF	OFF	OFF
7	ON	ON	ON	OFF	OFF	OFF
8	OFF	OFF	OFF	ON	OFF	OFF
9	ON	OFF	OFF	ON	OFF	OFF
10	OFF	ON	OFF	ON	OFF	OFF
11	ON	ON	OFF	ON	OFF	OFF
12	OFF	OFF	ON	ON	OFF	OFF
13	ON	OFF	ON	ON	OFF	OFF
14	OFF	ON	ON	ON	OFF	OFF
15	ON	ON	ON	ON	OFF	OFF
16	OFF	OFF	OFF	OFF	ON	OFF
17	ON	OFF	OFF	OFF	ON	OFF
18	OFF	ON	OFF	OFF	ON	OFF
19	ON	ON	OFF	OFF	ON	OFF
20	OFF	OFF	ON	OFF	ON	OFF
21	ON	OFF	ON	OFF	ON	OFF
22	OFF	ON	ON	OFF	ON	OFF
23	ON	ON	ON	OFF	ON	OFF
24	OFF	OFF	OFF	ON	ON	OFF
25	ON	OFF	OFF	ON	ON	OFF
26	OFF	ON	OFF	ON	ON	OFF
27	ON	ON	OFF	ON	ON	OFF
28	OFF	OFF	ON	ON	ON	OFF
29	ON	OFF	ON	ON	ON	OFF

Adresse	Schalter					
	1	**2**	**3**	**4**	**5**	**6**
30	OFF	ON	ON	ON	ON	OFF
31	ON	ON	ON	ON	ON	OFF
32	OFF	OFF	OFF	OFF	OFF	ON

B92x-Zweileitungs-Bedienteil/Adresse für Schaltereinstellungen des B93x ATM-Bedienteils
Stellen Sie die Adressschalter mithilfe der Zentralenkonfiguration ein. Wenn eine Anlage über mehrere SDI2-Bedienteile verfügt, muss jedes SDI2-Bedienteil eine eindeutige Adresse haben. Bei den einstelligen Adressen 1 bis 9 stellen Sie den Zehnerschalter auf 0. Die Zahl unten zeigt die Adressschaltereinstellung für Adresse 1.



Adressschaltereinstellungen für B94x-Touchscreen-Bedienteil
Die Einer-Stelle der Adresse legen Sie mit den Nach-oben- und Nach-unten-Pfeiltasten rechts vom Schalterbild und die Zehner-Stelle mit den Pfeilen links fest. Drücken Sie den Diagonalpfeil unter den Schaltern, um die Einstellung zu speichern, und kehren Sie zum Einschaltbildschirm zurück.

15.2 Schaltereinstellungen für das B208-Modul mit acht Eingängen

In dieser Tabelle wird die Beziehung zwischen den Modulschaltereinstellungen und der Adresse des Melderbereichs beschrieben, die der Einstellung entspricht. Die Werte des in dieser Tabelle aufgeführten Melderbereichs verweisen auf PUNKTE > Melderzuweisungen.
B6512 unterstützt bis zu 9 B208-Module mit acht Eingängen.
B5512 unterstützt bis zu 4 Module.
B4512 unterstützt bis zu 2 Module.
B3512 unterstützt das B208-Modul nicht.
Beenden Sie nicht verwendete B208-Eingänge mit einem Leitungsabschlusswiderstand.

B208-Adressnummer	**B6512-Meldernummern**	**B5512-Meldernummern**	**B4512-Meldernummern**
1	11 - 18	11 - 18	11 - 18
2	21 - 28	21 - 28	21 - 28
3	31 - 38	31 - 38	
4	41 - 48	41 - 48	
5	51 - 58		
6	61 - 68		
7	71 - 78		
8	81 - 88		

B208-Adressnummer	B6512-Meldernummern	B5512-Meldernummern	B4512-Meldernummern
9	91 - 96		

15.3 Schaltereinstellungen für B308-Modul mit acht Ausgängen

In dieser Tabelle wird die Beziehung zwischen den Modulschaltereinstellungen und dem Bereich der Ausgangsnummer beschrieben, der der Einstellung entspricht.
65512 unterstützt bis zu 9 B308-Module mit acht Ausgängen.
B5512 unterstützt bis zu 5 Module.
B4512 unterstützt bis zu 3 Module.
B3512 unterstützt das B308-Modul nicht.

B308-Adressnummer	B6512-Ausgangsnummern	B5512-Ausgangsnummern	B4512-Ausgangsnummern
1	11 - 18	11 - 18	11 - 18
2	21 - 28	21 - 28	21 - 28
3	31 - 38	31 - 38	31 - 38
4	41 - 48	41 - 48	
5	51 - 58	51 - 58	
5	51 - 58		
6	61 - 68		
7	71 - 78		
8	81 - 88		

15.4 Schaltereinstellungen für das B426-Ethernet-Übertragungsmodul

In dieser Tabelle wird die Beziehung zwischen den Modulschaltereinstellungen und dem Typ der Kommunikation mit der Zentrale beschrieben, dem die Einstellung entspricht.

B426-Schaltereinstellung	Adresse	Bustyp	Funktion
0			Lokale Konfigurationseinstellung (Standardeinstellung)
1	1 (173)	SDI2	Automatisierung oder RPS-Protokollierung

15.5 Schaltereinstellungen für B450-Mobilfunkmodul

In dieser Tabelle wird die Beziehung zwischen den Modulschaltereinstellungen und dem Typ der Kommunikation mit der Zentrale beschrieben, dem die Einstellung entspricht.

B450-Schaltereinstellung	Adresse	Bustyp	Funktion
0			Lokale Konfigurationseinstellung (Standardeinstellung)
1	1 (173)	SDI2	Automatisierung oder RPS-Protokollierung

15.6 Schaltereinstellungen für B520-Netzteil

Der Drehschalterbereich für die Adresse für das B520-Netzteil liegt zwischen 1 und 4 für B5512, zwischen 1 und 2 für B4512 und bei 1 für die B3512-Zentralen. Die Adressbereiche 00 und 05 – 99 sind auf dem SDI2-Gerätebus nicht gültig. Die werksseitige Standardeinstellung ist 01. Bei Verwendung von mehreren Netzteilen weisen Sie jedem Netzteil eine andere Schaltereinstellung zu.

Gültige B520-Schaltereinstellungen
01
02
03
04

15.7 Schaltereinstellungen für B810 RADION-Funkempfänger

Die B810- und B820-Adressschalter ermöglichen die Einstellung eines einstelligen Werts für die Adresse des Moduls. Das Modul verwendet die Adresse 1. Die Adressen 0 und 2 bis 9 sind ungültig.

15.8 Schaltereinstellungen des B820 Inovonics-Funkempfängers

Die Adressschalter des B820 Inovonics ermöglichen die Einstellung eines einstelligen Werts für die Adresse des Moduls. Das Modul verwendet die Adressen 1 bis 4. Die Adressen 0 und 5 bis 9 sind ungültig.
Nur die Adresse 1 ist für diese Zentralen gültig.

16 Konfigurieren für den Mobilfunkdienst

Erst für Bosch Cellular Service anmelden

Bevor Sie die Mobilfunkübertragung für Protokollierung, persönliche Benachrichtigungen, RPS-Verbindungen oder RSC-Verbindungen nutzen können, müssen Sie sich im Bosch Installer Services Portal unter https://installerservices.boschsecurity.com/ für den Bosch Cellular Service registrieren.

Konfigurieren von RPS für den Mobilfunkdienst

Das Konfigurieren von RPS für den Mobilfunkdienst erfolgt schnell und einfach mithilfe des Konfigurations-Assistenten. Klicken Sie auf „Config“ (Konfiguration), um das Konfigurationsmenü zu öffnen. Wählen Sie „Open Configuration Assistant“ (Konfigurations-Assistent öffnen) aus.

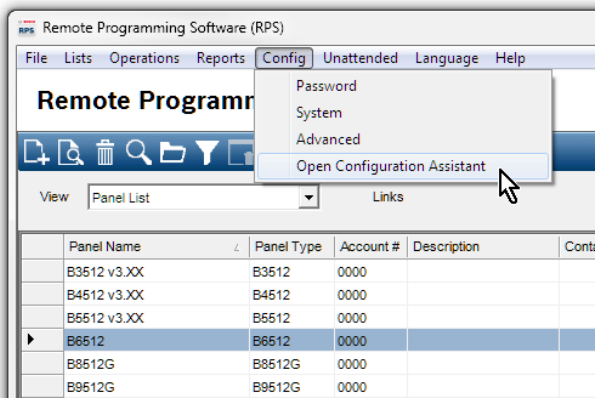


Abbildung 16.1: Konfigurations-Assistent

Falls Sie den Konfigurations-Assistenten nicht verwenden möchten, befolgen Sie die Schritte unten, um RPS für den Mobilfunkdienst zu konfigurieren.

1. Klicken Sie auf „Config“ (Konfiguration), um das Konfigurationsmenü zu öffnen. Klicken Sie auf „System“.
2. Klicken Sie auf die Registerkarte „Connectivity“ (Anschlussmöglichkeiten).
3. Klicken Sie auf „Cellular“ (Mobilfunk).
4. Wenn Sie über ein PPTP-VPN (Login wird bereitgestellt mit Bosch Cellular) mithilfe einer Mobilfunk-IP eine Verbindung zur Zentrale herstellen möchten, klicken Sie auf die Registerkarte „VPN“. Bei dieser einmaligen Einrichtung werden die PPTP-VPN-Anmeldung und die Verbindung über das Fenster „Connect“ (Verbinden) in RPS automatisiert.
   Der VPN-Client (oder Windows VPN) muss auf Ihrem PC eingerichtet werden, bevor RPS ihn verwenden kann. Diese Einrichtung ist nicht erforderlich, wenn Ihr Netzwerk für eine stets aktive IPSec-VPN-Verbindung zum Netzwerkanbieter konfiguriert ist.
   Anweisungen zum Einrichten des Windows VPN finden Sie im Bosch Cellular Services User Guide unter http://www.conettix.com/Downloads.aspx.

Konfigurieren des Zentralenkontos für Mobilfunkdienst

Das Konfigurieren eines Zentralenkontos für den Mobilfunkdienst erfolgt schnell und einfach mit dem Konto-Assistenten.

Klicken Sie in der Zentralenliste mit der rechten Maustaste auf das Zentralenkonto, das Sie für den Mobilfunk konfigurieren möchten, und klicken Sie dann auf „Open Account Assistant“ (Konto-Assistent öffnen).

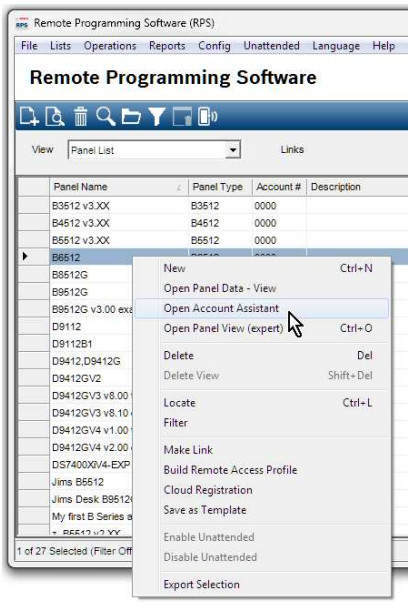


Abbildung 16.2: Konto-Assistent öffnen

Wenn Sie den Konto-Assistenten nicht verwenden möchten, befolgen Sie die Schritte zur Konfiguration eines Zentralenkontos für den Mobilfunkdienst.

1. Klicken Sie in der Zentralenliste mit der rechten Maustaste auf das Zentralenkonto, das Sie für den Mobilfunk konfigurieren möchten, und klicken Sie dann auf „Open Panel Data - View“ (Zentralendaten öffnen – Ansicht).
2. Klicken Sie auf die Registerkarte „Cellular“ (Mobilfunk).
3. Drücken Sie F1, um die Hilfe für die Registerkarte „Cellular“ (Mobilfunk) zu öffnen.
4. Befolgen Sie die Anweisungen, um Informationen in die Felder „Cellular Connectivity“ (Mobilfunkverbindungen) einzugeben. RPS verwendet die SIM oder Funk-MEID-Nummer, um die zugewiesene IP-Adresse, Telefonnummer und den zugewiesenen Vertrag abzurufen und zu speichern.
5. Klicken Sie auf „Show Plans“ (Verträge anzeigen) und dann auf „Plan Help“ (Vertragshilfe). Wählen Sie einen geeigneten Vertrag aus, um überschüssige Kosten zu vermeiden.
6. Klicken Sie auf „OK“, wenn Sie fertig sind. Sie sind zurück auf der Zentralenliste.
7. Zum Festlegen der Zentralenparameter klicken Sie auf der Zentralenliste auf das Zentralenkonto, auf das Sie in Schritt 1 geklickt haben, und klicken Sie dann auf „Open Panel View“ (Zentralenansicht öffnen).
8. Zentralenübergreifende Parameter > *Mobilfunk-Steckplatine, Seite 62*: Behalten Sie für die Parameter die Standardwerte bei. Ändern Sie sie nur bei gewerblichen UL1610-Anwendungen, die eine Benachrichtigung bei schwachem Signal erfordern.
9. Zentralenübergreifende Parameter > *Übertragungsgerät – Übersicht, Seite 86* > Primäres Zielgerät (Ersatzzielgerät): Zum Senden von Berichten für eine Zielgruppe über ein Mobilfunkübertragungsgerät wählen Sie ein (steckbares) Mobilfunkmodul als primäres oder Ersatzziel fest.
10. Zentralenübergreifende Parameter > *Enhanced Communication (Erweiterte Kommunikation), Seite 90*: Hier legen Sie Protokollierungsziele und Einstellungen für Polling/Überwachung fest. Achten Sie darauf, dass die Pollingraten für den Mobilfunk den empfohlenen Einstellungen folgen und auf Ihren Mobilfunkvertrag ausgerichtet sind.
11. Zentralenübergreifende Parameter > Persönliche Benachrichtigung > *Personal Notification Destinations (Persönliche Benachrichtigungsziele), Seite 116*: Telefonnummern für SMS, E-Mail-Adressen für E-Mails festlegen. Sie können die Methode auf „Plug in Cellular

SMS“ (Plug-in-Mobilfunkmodul-SMS), „Bus Device Cellular SMS“ (Bedienteil-Mobilfunk-SMS), „Plug in Cellular Email“ (Plug-in-Mobilfunkmodul-E-Mail) oder „Bus Device Email“ (Bedienteil-E-Mail) festlegen.

17 Formate von IP-Adresse und Domainname

IPv4-Adressformat

IPv4-Adressen sind im ASCII-Dezimalformat, xxx.xxx.xxx.xxx (xxx = 0 bis 255). Die vier Oktetten (xxx) der Adresse werden durch Punkte getrennt.
Richtig: 12.3.145.251
Falsch: C.17.91.FB

IPv6-Adressformat

IPv6-Adressen bestehen aus acht Gruppen von 4 hexadezimalen Ziffern, die durch Doppelpunkte voneinander getrennt sind: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, x = 0 bis F.

Vollständig qualifiziertes Domainnamensformat

Der vollständig qualifizierte Domainname definiert die genaue Adresse eines Geräts in der Domain Name System (DNS)-Hierarchie. Hierzu gehören der einzigartige Hostname des Geräts und das Subnetz, in dem sich das Gerät befindet, getrennt durch Punkte.
Beispiel: Empfänger01.Ihr-Alarm-Unternehmen.com
Jede Bezeichnung innerhalb des Namens muss dem RFC-921, „Domain Name System Implementation Schedule“, entsprechen.
Nur Buchstaben (A-Z), Ziffern (0-9) und das Minuszeichen (-) sind in den Textbeschriftungen im vollständig qualifizierten Domainnamen zulässig.
Der Punkt (.) darf nur Textbeschriftungen begrenzen, aus denen der vollständig qualifizierte Domainname besteht.
Vor dem Eingeben eines vollständig qualifizierten Domainnamens muss gewährleistet sein, dass der Name des betreffenden Geräts ordnungsgemäß bei den für das IP-Übertragungsgerät verfügbaren DNS-Servern registriert ist. Dies kann mit einem Pingtool überprüft werden.

Weitere Informationen

Informationen über Hostnamen und vollständig qualifizierte Domainnamensformate finden Sie auf der Website „The Internet Engineering Task Force (IETF)“ unter http://www.ietf.org/

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com
© Bosch Security Systems B.V., 2019