

Die Zentralen JA-107K und JA-103K der Einbruch- & Gefahrenmeldeanlage JABLOTRON 100+

Eine Zentrale ist ein fundamentaler Teil des Sicherheitssystems JABLOTRON 100+ und dient dazu, kleine mittelgroße und große Gebäude zu überwachen. Sie entspricht den Anforderungen der Sicherheitsklasse 2. Die Zentrale ist mit BUS- und/oder drahtlosen Geräten (wenn das System mit einem Funkmodul ausgestattet ist) kompatibel. Es wird empfohlen, nur Geräte der Serie JABLOTRON 100+ mit dem System zu verwenden. Die korrekte Funktionsweise kann bei Verwendung von Geräten dritter Anbieter nicht garantiert werden.

Vorsicht: Das Sicherheitssystem JABLOTRON 100+ darf nur von einem geschulten Techniker mit einem von einem autorisierten Händler ausgestellten gültigen Zertifikat und lokal geltenden Richtlinien installiert werden.

Dieses Handbuch richtet sich an geschulte Facherrichter.

Einige in diesem Handbuch beschriebene Funktionen benötigen die Installation weiterer Komponenten:

- **Sprachmenü für die Fernsteuerung, Rufsteuerung, Sprachmeldungen, Klingelmeldungen, Spezielle Meldungen, SMS-Meldungen, SMS-Steuerung, GPRS-Kommunikation - GSM-Wähl- & Übertragungsgerät JA-19xY.**

Inhaltsverzeichnis

1.	Grundlegende Beschreibungen und Definitionen	4
1.1.	Grundlegende Anforderungen an die Systemkonfiguration	8
1.2.	Zugriffscodes und ihre Standardeinstellungen	9
1.2.1.	Änderung des Zugriffscodes	10
1.2.2.	Sicherheitszugriffscodes und RFID-Geräte	11
1.2.3.	Regelmäßige Prüfung des Systems (Wartung)	12
2.	Systemgröße	14
2.1.	Externe Größe	14
2.2.	Interne Größe (Systembereich)	14
2.2.1.	Konfiguration and Aufteilung	15
3.	Zentralentypen, Systemparameter	16
3.1.	Beschreibung der Zentrale JA-103K	17
3.2.	Beschreibung der Zentrale JA-107K	18
3.3.	LED-Anzeigen der Leiterplatte der Zentrale	20
3.4.	Zusätzliche Anschlüsse auf der Leiterplatte der Zentrale	20
3.5.	Verbindungsklemmen auf der Leiterplatte der Zentrale	21
4.	Vor der Installation des Systems	21
5.	Installation der BUS-Geräte	22
5.1.	Der BUS des Systems JABLOTRON 100+	22
5.2.	BUS-Kabel	23
5.3.	BUS-Layout	23
5.4.	BUS-Verzweigung und -Aufteilung	24
5.5.	BUS-Länge und Anzahl der verbundenen Geräte	24
5.6.	Berechnung von Leitungsverlusten	24
5.7.	Beispiel für eine Berechnung des Spannungsverlustes	25
5.8.	Berechnungsbeispiel des BUS-Stromverbrauchs zur Systemsicherung	26
5.9.	Anforderungen an die Stromversorgung	26
5.10.	Anforderungen der Backup-Stromquelle	27
5.11.	BUS-Isolation	27
5.12.	Nutzung bestehender Verkabelung in Sanierungsprojekten	28
6.	Verwendung drahtloser Geräte	28
6.1.	Installation eines Funkmoduls JA-111R	28
6.2.	Installation drahtloser Geräte – Anmelde-Modus	29
6.3.	Erweitern der Reichweite von drahtlosen Geräten	29
7.	EINSchalten des Systems	30
8.	Konfiguration des Systems	30
8.1.	Die Systemprofile	30
8.2.	Betriebsmodi der Zentrale	35
8.3.	Benutzerberechtigung	36
8.4.	Optionale Systemparameter	37

8.4.1.	Geräte anmelden und löschen	39
8.4.2.	Liste der anwendbaren Reaktionen	40
8.4.3.	Einschränkung von Fehlalarmen	42
8.5.	Alarmarten	43
8.5.1.	Einbruchsalarm	44
8.5.2.	Sabotagealarm	44
8.5.3.	Feueralarm	45
8.5.4.	Panikalarm	45
8.5.5.	24 Std.-Alarm	45
8.5.6.	Alarmabbruch	45
8.6.	Systemfehler	46
8.7.	Durch einen Geräteverlust verursachter Fehler	46
9.	Optionen der Systemsteuerung	48
9.1.	Berechtigungsarten	49
9.2.	Systemsteuerung über das Bedienteil	49
9.2.1.	Systemsteuerung von Bedienteilen mit Segmenten	49
9.2.2.	Systemsteuerung mit den Bedienteilen JA-110E und JA-150E	51
9.3.	Systemsteuerung über eine Fernbedienung	54
9.4.	Systemsteuerung über den Kalender & Zeitschaltuhren	55
9.5.	Systemsteuerung über das Sprachmenü des Wähl- & Übertragungsgerätes (GSM)	56
9.6.	SMS-Befehle	58
9.7.	Steuerung des System via F-Link oder J-Link	60
9.8.	Systemsteuerung von der webbasierten App MyJABLOTRON	61
9.9.	Steuerung über die mobile App MyJABLOTRON	62
9.10.	Systemsteuerung über die Erzwungene Zugriffssteuerung	62
9.11.	Hindernisse, die die Scharfschaltung des Systems verhindern	63
9.12.	Fehlgeschlagene Scharfschaltung	64
9.13.	An Benutzer gemeldete Ereignisse	65
9.14.	Akustische Anzeige des Systems	66
9.15.	Zeitlich begrenzter Zugriff für Benutzer	67
9.16.	Deaktivierungs- und Sperroptionen	68
9.16.1.	Deaktivierung	68
9.16.2.	Sperrung	68
9.17.	Nicht-Alarmfunktionen - Funktionen der PG-Ausgänge	69
10.	Einstellung des Systems über F-Link	70
10.1.	F-Link starten und die Systemgröße einstellen	72
10.2.	Start des Installationsassistenten	72
10.3.	Registerkarte Systemübersicht	73
10.4.	Registerkarte Bereichsübersicht	74
10.5.	Registerkarte Komponentenliste	75
10.5.1.	Konfiguration der Bedienteile	76
10.5.1.1.	Registerkarte Bereiche (Segmente)	76
10.5.1.2.	Registerkarte Einstellungen	78
10.5.1.3.	Registerkarte Gemeinsames Segment	81
10.5.2.	Beispiele von Einstellungen einer internen Sirene	82
10.6.	Registerkarte Benutzerübersicht	82
10.7.	Registerkarte PG-Ausgänge	83
10.7.1.	Aktivierungskarte eines PG-Ausgangs	85
10.8.	Registerkarte Benutzerbenachrichtigung	87
10.9.	Registerkarte Systemparameter	91
10.10.	Registerkarte Zeitschaltuhr	98
10.11.	Registerkarte Übertragungsgeräte	99
10.11.1.	GSM-Einstellungen	101
10.11.2.	LAN-Einstellungen	103
10.11.3.	Kameras	103
10.11.4.	GSM-Neustart	104
10.12.	Registerkarte AES - Alarmempfangsstellen	104
10.12.1.	JABLOTRON 100 + CID und SIA-Codes	105
10.12.2.	Einstellung zur Übertragung von Fotos an einen externen Speicher	108
10.13.	Registerkarte Diagnose	108

11.	Andere Optionen von F-Link	110
11.1.	Bedienteil (virtuell)	110
11.2.	Ereignisse	111
11.3.	Einstellungen	111
11.4.	Signalmessung	114
11.5.	Gebäudeplan	114
11.6.	Errichtermodus	115
11.7.	Wartungsmodus	115
11.8.	Aktualisieren	115
11.9.	Online	115
11.10.	Internet	115
11.11.	Installationsassistent	116
11.12.	Installations-Info	116
11.13.	Aktualisierung der Firmware	117
11.14.	Etikettendruck	117
11.15.	Einstellungsverlauf	117
12.	Zurücksetzen der Zentrale	118
13.	Aktualisierung der Firmware	119
13.1.	Allgemeine Regeln zur Aktualisierung der Firmware (FW)	119
13.2.	FW-Aktualisierungen für die Zentrale und Geräte, die mit dem BUS verbunden sind	119
13.3.	FW-Aktualisierungen für drahtlose Geräte	120
13.4.	Prüfung nach einer FW-Aktualisierung	120
13.5.	Tips anzeigen	120
13.6.	Abmessungen der Zentrale	121
14.	Die webbasierte Applikation MyJABLOTRON	122
14.1.	Verwaltung der Installationen und Angebote für einen Errichter	122
14.2.	WEB-Link Applikation (Konfiguration)	123
15.	Übernahme des Systems durch den Benutzer	124
16.	Technische Spezifikationen	124

1. Grundlegende Beschreibungen und Definitionen

Modulare Architektur – erlaubt dem System, für spezifische Installationen, Größen und Benutzerbedürfnisse konfiguriert zu werden.

(FW) Firmware-Aktualisierung - Verfahren zur Aktualisierung einer neuen FW-Version im System, die neue Funktionen, Verbesserungen und Anpassungen beinhaltet. Wir empfehlen, die FW sowohl während der Installationen als auch während der regelmäßigen Wartung zu kontrollieren, um auf dem neusten Stand zu sein. Neben der Aktualisierung der FW der Zentrale empfehlen wir, auch die Aktualisierung der FW bei allen Komponenten vorzunehmen, falls dies erforderlich ist (Tastaturen, Funkmodule, Bewegungsmelder mit Kamera u.s.w. ...)

Zugriffsmodule (Tastatur/Bedienteil) – ist das grundlegende modulare Element einer Steuerungstastatur und seine Aufgabe besteht darin, Benutzer zu identifizieren. Die einfachste Version enthält nur ein Lesegerät für kontaktlose RFID-Tags / -Karten. Eine Version mit einer Tastatur und einem LCD-Display ist ebenfalls verfügbar. Zugriffsmodule werden sowohl in einer BUS- als auch in einer drahtlosen Version hergestellt. Jedes Zugriffsmodul enthält einen Steuerungsbereich (Segment) (erweiterbar auf 20 Bereiche (Segmente) pro Gerät). In unserem Produktportfolio befinden sich außerdem ein RFID-Kartenleser und eine Tastatur mit integriertem RFID-Kartenleser für den Außenbereich.

Steuerungsbereich (Segment) – ist ein modulares Element der Steuerungstastatur für den Innenbereich. Ein Bereich (Segment) hat 2 Tasten (links = AUS, rechts = EIN). Mit der benötigten Anzahl der Bereiche (Segmente) auf einem Zugriffsmodul können Sie eine Tastatur erstellen, die alle erforderlichen Funktionen sehr übersichtlich erfüllt. Die Bereiche (Segmente) zeigen deutlich den Systemstatus an und können intuitiv gesteuert werden. Anhand der installierten Bereiche (Segmente) kann der Benutzer deutlich (besser als nur versteckt im Menü) sehen, welche Funktionen das System bietet und welche Zugriffsrechte dem Benutzer zugewiesen sind.

Steuerungstastatur – besteht aus einem Zugriffsmodul und den Steuerungsbereichen (Segmenten).

Alarmarten - das System kann auf Ereignisse wie Einbruch, Panik (Geiselnahme), Sabotage, Feuer, Gasaustritt, Überschwemmung u.s.w. reagieren. Durch den Einsatz von geeigneten Meldern können auch alle anderen Gefahren gemeldet werden (wenn sich jemand im Garten befindet, einen geschützten Gegenstand berührt, hohe Temperaturen, Gefrierisiko u.s.w.). Zur Reduzierung von Fehlalarmen können die Reaktionen der Melder, die strukturell oder betrieblich gesehen in einem schwierigen Umfeld angebracht wurden, so eingestellt werden, dass ihre Aktivierung bestätigt werden muss (der Melder muss wiederholt aktiviert oder durch einen anderen Melder bestätigt werden).

Visuelle Alarmverifizierung – Foto-Verifizierungsgeräte (Bewegungsmelder mit Kamera, Verifizierungskameras) können automatisch Fotos oder Videosequenzen von Ereignissen im überwachten Bereich aufnehmen und versenden.

Personenschutz – im Falle eines Überfalls bzw Geiselnahme, sowie von Gesundheitsproblemen oder Feuer kann der Benutzer nach Hilfe rufen (Betätigung der Taste auf einer Tastatur, Eingabe des Panik- oder Geiselnahmecodes durch Aktivierung einer Paniktaste oder Verwendung einer drahtlosen Fernbedienung).

Erzwungene Zugriffssteuerung – dient dazu, nur über die Berechtigungsfunktion oder die Systemsteuerung (Scharfschaltung, Unscharfschaltung, PG-Steuerung, ...) einen stummen Alarm auszulösen, wenn der Benutzer bedroht wird. Ein Panikalarm wird während einer Systemsteuerung dann ausgelöst, wenn ein Code eingegeben wird, wobei 1 mathematisch dem letzten Zahlenwert hinzugefügt wird.

Verzögerter Panikalarm – Funktion zur Auslösung eines Panikalarms mit einer zeitlichen Verzögerung, während der Alarm abgebrochen werden kann. Die Funktion ist für Benutzer geeignet, die Angst davor haben, fremden Personen, die sie vielleicht angreifen könnten, die Eingangstür zu öffnen. Der Benutzer aktiviert in dem Fall den verzögerten Panikalarm, bevor er die Tür öffnet und wenn er von der eigenen Sicherheit überzeugt ist, muss er die Funktion vor Ablauf der voreingestellten Verzögerungszeit deaktivieren. Die Zeit des verzögerten Panikalarms kann in den internen Einstellungen bestimmter Geräte, die für die Auslösung eines Panikalarms verwendet werden (Tastaturbereich, Paniktaste usw.), eingestellt werden.

Ereignismeldung – alle Ereignisse an eine Alarmempfangsstelle (AES) oder Notrufserviceleitstelle (NSL) zu melden, ermöglicht ein rechtzeitiges professionelles Eingreifen. Die Meldungen werden der AES/NSL über ein eingebautes LAN-Übertragungsgerät gesendet. Nach der Installation des GSM-Wähl- & Übertragungsgerätes werden die Meldungen direkt als Daten, SMS oder Sprachanrufe gesendet.

Spezielle Meldungen – sind SMS-Nachrichten oder Sprachanrufe. Ihre Bedeutung kann unabhängig von anderen Funktionen gesendet werden. Das Senden einer Meldung kann mit der Aktivierung eines Geräts verknüpft werden. Auf diese Weise können der Gerätestatus oder Technologien mit einem fehlerhaften Ausgang überwacht werden.

Fernsteuerung – über eine zusätzliche Einwahlmöglichkeit können berechtigte Benutzer das System anrufen und das Sprachmenü benutzen, um den eingestellten Status zu steuern oder zu prüfen. Der Status einzelner Bereiche kann per Fernzugriff über definierte SMS-Befehle gesteuert werden. SMS-Befehle können auch dazu

verwendet werden, um programmierbare PG-Ausgänge auf EIN oder AUS zu schalten. Sie können auch durch einfaches Anrufen (ohne einen Anruf aufzubauen) von berechtigten Rufnummern aus aktiviert werden. Errichter können mit Hilfe von F-Link das System steuern. Für den Systemadministrator ist auch die Software J-Link mit eingeschränkten Funktionen verfügbar. Das System kann auch per Web-Service unter www.myjablotron.com oder auch über die Smartphone-App per Fernzugriff gesteuert werden.

MyJABLOTRON – ein einzigartiger für Endbenutzer und Errichter konzipierter Service, der den Online-Zugang zu den JABLOTRON-Geräten ermöglicht. Zur Nutzung des MyJABLOTRON-Dienstes ist eine optionale **JABLOTRON Sicherheits-SIM-Karte** erforderlich. Weitere Informationen zur Anmeldung von Zentralen und der Verfügbarkeit des Service in Ihrem Land erhalten Sie von Ihrem Händler.

Zugriffsrechte der Benutzer – legt die Stufe der Zugriffsberechtigung eines Benutzers fest. Sie können Zugriffsrechte, die einen geschützten Bereich des Gebäudes steuern und die PG-Ausgänge, die ein Benutzer steuern kann, ändern. Die Benutzer verifizieren ihre Identität unter Verwendung ihres RFID-Tags oder durch Eingabe ihres Codes auf der Tastatur. Das System ermöglicht Ihnen, eine Zeitbeschränkung individuell festzulegen, um den Zugriff ausgewählter Benutzer auf geschützte Bereiche zu sperren.

Administrator – es kann eine bestimmte Anzahl an Administratoren im System festgelegt werden, die wiederum allen Standardbenutzern Ihre Zugriffsrechte zuweisen. Dabei können unterschiedliche Bereiche des Gebäudes unterschiedliche Administratoren haben. In den Standardeinstellungen gibt es einen Hauptadministrator (Master) des Systems (Position 1), der berechtigt ist, die Zugriffsrechte für alle Benutzer festzulegen (Standardcode ist 1234).

Errichter – es kann mehr als einen berechtigten Errichter zur Verwaltung des Systems geben (Standardcode 1010). Der Techniker ist mit diesem Code berechtigt, alle Funktionen des Systems anzupassen. Dabei kann es (wenn erforderlich) mehrere berechtigte Errichter geben. Die Zugriffsmöglichkeiten eines Errichters bestimmt der Administrator. Gesonderte Berechtigungen hat ein AES-Techniker. Dieser Techniker kann seinen Code benutzen, um den Zugriff zu den Einstellungen der Kommunikationsparameter mit der Alarmempfangsstelle zu sperren.

F-Link (J-Link) – zur Programmierung des Systems benötigt man einen Computer mit einem Windows-Betriebssystem. Die Zentrale wird mit dem Computer lokal über ein USB-Kabel oder per Fernzugriff über einen Computer mit einer Internetverbindung verbunden. Alle Funktionen werden über den Computer und F-Link eingerichtet. Diese Software ist nur für geschulte Techniker geeignet. Der Zugriff kann einem Administrator oder Benutzer des Systems nicht gewährt werden. Aus diesem Grund gibt es eine vereinfachte Softwareversion (J-Link), die den Systemadministratoren Zugriff auf einige Einstellungen (Benutzerverwaltungen, Diagnosen, Einstellung geplanter Ereignisse, Lesen des Ereignisverlaufs) gewährt.

Errichtermodus – ist der Modus, in dem die komplette Systemkonfiguration geändert werden kann. Nur ein Errichter (oder AES-Techniker) kann auf den Errichtermodus des Systems zugreifen. Dies erfolgt über F-Link, wobei die Zentrale lokal oder per Fernzugriff (über ein USB-Kabel oder das Internet) mit dem PC verbunden ist. Im Errichtermodus ist das System vollständig außer Betrieb und die PG-Ausgänge sind ausgeschaltet (es überwacht nichts und stellt keine Funktionen, wie Steuerung eines programmierbaren PG-Ausgangs bereit). Der Errichtermodus wird über die gelb blinkende (2x alle 2 Sekunden) Systemanzeige der Tastatur angezeigt.

Wartungsmodus – ist der Modus, der hauptsächlich für den Administrator gedacht ist. Er ermöglicht die Wartung (z. B. Batteriewechsel) in den Bereichen entsprechend den Zugriffsrechten des Administrators. Das System kann vom Administrator über die Tastatur oder J-Link in den Wartungsmodus geschaltet werden (der Errichter kann den Wartungsmodus über F-Link aufrufen). Der Wartungsmodus in einem Bereich hat keinen Einfluss auf den Status und die Funktionalität anderer Bereiche oder den Status der programmierbaren PG-Ausgänge. Der Errichter kann den Zugriff des Administrators auf den Wartungsmodus in der Registerkarte Systemparameter in F-Link einschränken. Der WARTUNGS-Modus wird durch die grün blinkende Systemanzeige der Tastatur (2 x alle 2 Sekunden) und durch das Erlöschen der Bereichstasten des jeweiligen Bereichs angezeigt.

Tag / Nacht-Modus - Die Zentrale ermöglicht Ihnen, ein individuelles Verhalten für den Tag und die Nacht einzustellen. Zum Beispiel eine andere Hintergrundbeleuchtung der Tastatur, Aktivierung des PG-Ausgangs bei Tag / Nacht (Sperrung der Beleuchtung während des Tages) usw. Der Tag- / Nachtmodus kann durch ein ausgewähltes Gerät (z.B. Dämmerungsschalter) oder durch die definierte Zeit von Sonnenaufgang und -untergang entsprechend des astronomischen Kalenders geschaltet werden. Für diese Option müssen die Koordinaten des Standorts festgelegt werden, an dem das System installiert ist.

Gerätesteuerung – das System hat programmierbare PG-Ausgänge, die zur An- und Ausschaltung verschiedener Geräte benutzt werden. PG-Ausgänge stellen eine programmierte Systemlogik dar, die die erforderliche Anzahl der Ausgangsmodule (Systemgeräte) steuert. Ein Ausgang kann über die Bereiche (Segmente) der Tastatur, durch die Aktivierung von Meldern, Fernsteuerungen, über ein Ereignis im System (z.B. Scharfschaltung eines Alarms, Auslösung eines Alarms u.s.w.), über eine Zeitschaltuhr, über SMS-Befehle, durch den Anruf eines berechtigten Benutzers oder über die Applikation MyJABLOTRON gesteuert werden. Die Aktivierung eines PG-Ausgangs kann auch von einem Bereichsstatus, einem Melder oder einem anderen PG-Ausgang gesperrt werden. Die Aktivierung und Deaktivierung eines PG-Ausgangs kann Benutzern per SMS oder dem MyJABLOTRON-Dienst über Datentransfer (Push-Benachrichtigungen) gemeldet werden.

Steuerung der Türverriegelung – eine elektrische Türverriegelung (verbunden mit einem PG-Ausgang) kann mit einem Tag oder über die Eingabe eines Codes auf der Tastatur geöffnet werden. Jeder Benutzer kann einer Tür, die er öffnen kann, zugewiesen werden. Ein Ausgang kann durch einen scharf geschalteten Bereich gesperrt werden, so dass keine Gefahr besteht, dass jemand einen Bereich betritt, wenn dieser überwacht (scharf geschaltet) ist. Das Öffnen einer Tür durch einen berechtigten Benutzer kann im Ereignisverlauf des Systems erfasst werden.

Zeitschaltuhr – mit der Verwendung der Zeitschaltuhr können Sie automatische Kalenderaktionen (Scharfschaltung/teilweise Scharfschaltung/Unscharfschaltung) zur Überwachung von Bereichen und der Steuerung (Aktivierung/Deaktivierung, Sperrung/Entsperrung) von programmierbaren Ausgängen programmieren. Jede Aktion kann für einen Tag und einen Monat festgelegt werden, in denen sie ausgeführt wird. Diese kann bis zu 4 Mal vorkommen oder in festgelegten Intervallen für den ausgewählten Tag wiederholt werden. Der Jahresplan kann verwendet werden, um Abweichungen von dem Wochenplan festzulegen (z. B. Feiertage, persönliche Feiertage).

BUS-Geräte – sind mit dem System über ein BUS-Kabel verbunden (4-Draht). Der BUS ermöglicht dabei sowohl die Stromversorgung als auch die Kommunikation. BUS-Geräte (Melder, Tastaturen, Sirenen u.s.w.) müssen an einer Position (Adresse) im System angemeldet werden, um zu funktionieren. Allerdings gibt es auch Geräte, die nur verbunden sind und funktionieren, ohne an einer Position angemeldet zu sein (einige PG-Ausgangsmodule, Statusindikatoren, BUS-Isolatoren u.s.w.).

Drahtlose Geräte – um die Kommunikation sicherzustellen, muss die Zentrale mit einem Funkmodul (Schnittstelle) ausgestattet und die drahtlosen Geräte (Melder, Tastaturen, Sirenen usw.) müssen an einer Position (Adresse) im System angemeldet sein. Jedoch gibt es auch Geräte im System, die keine Systemposition einnehmen (diese werden nur zum Empfang verwendet und senden keine Meldungen an die Zentrale), wie z.B. Module der PG-Ausgänge. Um eine große Fläche abzudecken, können bis zu 3 Funkmodule im System installiert werden (Verbindung über ein BUS-Kabel). Die Zentrale überprüft in regelmäßigen Abständen die Aktivität der ausgewählten drahtlosen Geräte (Supervisionsparameter) und prüft auch den aktuellen Batteriestand. Wenn die Kommunikation mit einem drahtlosen Gerät verloren geht, zeigt die Zentrale einen Kommunikationsfehler an. Funkmodule prüfen RF-Störungen im Frequenzbereich der JABLORTRON 100+. Bei einer Störung löst das System eine Fehlermeldung aus.

Einbruchsmelder – Gruppe von Meldern, die zur Erkennung von Einbrüchen verwendet werden. Dazu gehören Bewegungsmelder, sowie Öffnungs- Glasbruch- Neigungs- oder Schockmelder. Die Melder werden auf eine gewünschte Reaktion auf ihre Auslösung (Aktivierung) eingestellt. Dies bestimmt, wie der Melder auf seine Aktivierung reagiert. Feuer-, Gas-, Überschwemmungs-, oder Panikmelder gehören nicht zu der Gruppe dieser Einbruchsmelder.

GSM-Wähl- & Übertragungsgerät – sollte als zusätzliches Modul an der Zentrale installiert werden und stellt die Verbindung zu einem Mobilfunknetz und dem Internet her. Somit kann das System Daten an die Alarmempfangsstelle (AES) oder Notrufserviceleitstelle (NSL) übertragen. Der Kommunikator ermöglicht den Fernzugriff auf die Zentrale mithilfe von F-Link (J-Link), über die Ereignisse an die Benutzer gemeldet werden.

LAN- Übertragungsgerät – ist in der Systemsteuerung enthalten und ermöglicht eine Verbindung zum Internet. Es ermöglicht einen schnellen Fernzugriff durch F-Link und J-Link und kann auch Daten an eine Alarmempfangsstelle (AES) oder Notrufserviceleitstelle (NSL) senden, das mit einer Empfangstechnologie für das JABLOTRON-Protokoll ausgestattet ist. In den Einstellungen der Zentrale können Sie auswählen, welcher Kommunikationstyp primär und welcher als Backup verwendet wird.

Sicherungsbereich – ein System kann in verschiedene Teile (Bereiche) aufgeteilt werden, die unabhängig von einander scharf und unscharf geschaltet werden können. Ein Bereich kann ein einzelnes Appartement in einem Appartementgebäude, ein Geschäft in einem Einkaufszentrum oder eine Abteilung in einem Unternehmen oder Bürogebäude sein. Die Unabhängigkeit des Bereichs kann so eingestellt werden, als wäre er über eine eigene Zentrale geschützt (Zugriffsrechte, Meldungen, Anzeigen auf der Tastatur, akustische Anzeigen, der MyJABLOTRON-Dienst..).

Gemeinsamer Bereich – einzelner Bereich, der als Oberbereich für eine ausgewählte Gruppe anderer Bereiche dient. Wenn der letzte Unterbereich scharf geschaltet wird, wird der gemeinsame Bereich automatisch scharf geschaltet. Wenn ein Unterbereich zuerst unscharf geschaltet wird, wird der gesamte gemeinsame Bereich auch unscharf geschaltet. Dies dient dazu, Bereiche, wie Hallen, Toiletten, Küchen in Unternehmen u.s.w. zu sichern. Wir empfehlen nicht, gemeinsame Bereiche direkt zu steuern.

Gemeinsames Segment – ist eine Funktion eines Tastaturbereichs (Segments), mit dem Sie mehrere Bereiche gleichzeitig mit nur einem Segment steuern können. Diese Segmente müssen so eingestellt werden, dass sie die Segmente auf der jeweiligen Tastatur trennen. Jede Tastatur kann bis zu zwei Segmente mit der Funktion des gemeinsamen Segments haben und kann somit zwei verschiedene Bereichsgruppen steuern.

Teilweise Scharfschaltung – ist für jeden Bereich separat verfügbar. Bei einer teilweisen Scharfschaltung reagiert das System nicht auf Einbruchsmelder mit dem Parameter „Teilscharf“ scharf geschaltet (d.h. die Innenräume überwachen). Somit ist z.B. eine Bewegung im Wohnbereich des Hauses gestattet, jedoch löst das System einen Alarm oder eine Eingangsverzögerung aus, wenn durch eine Tür gegangen wird oder es eine

Bewegung z.B. in einer Garage oder im Keller gibt. Wenn ein Bereich vollständig scharf geschaltet ist, reagiert er auf die Aktivierung aller Melder, die ihm zugewiesen wurden.

Bypass – ein aktiver Gerätestatus oder ein Fehler im System wird während der Systemeinstellung bestätigt. Der Status aktiver Eingänge wird nach einem Bypass ignoriert, bis sie in den Standby-Modus (Deaktivierung) wechseln. Wenn Eingänge in den Standby-Modus wechseln (deaktiviert werden), werden sie in die Überwachung eingeschlossen. Mit dem Umgehen der Systemfehler bestätigt der Benutzer, dass er den Fehler wahrgenommen hat, sich der Status aber nicht ändert (ein Fehler ist noch immer im System). Diese Funktion hängt von den Parametern der Einstellungsarten ab.

Sperren - ein aktives Gerät wird gesperrt, um einen PG-Ausgang zu aktivieren oder um eine Reaktion zu aktivieren. Die Sperrung erfolgt manuell über eine LCD-Tastatur, F-Link, J-Link oder die MyJABLOTRON-App. Auf diese Weise kann ein Gerät jederzeit unabhängig vom Einstellungsvorgang gesperrt werden. Diese Funktion hängt von den Parametern der Einstellungsarten ab.

Autobypass – automatischer Bypass einer Systemreaktion auf ein Gerät entsprechend verschiedener Optionen. Eingangsaktivierung nach 3x Aktivierung oder 3x Alarm (optional), Fehler nach 3x fehlerhafter Aktivierung.

Deaktivierung – diese Option dient zur vorübergehenden manuellen Deaktivierung ausgewählter Bereiche, Geräte, Benutzer, programmierbarer Ausgänge (PG) oder Zeitschaltuhren. Der Bereich, dem die Zentrale zugewiesen ist kann nicht deaktiviert werden. Dies gilt auch für den Errichtercode auf Position 0, dem Administrator-Code auf Position 1. Bei Geräten unterscheiden wir zwischen der Sperrung (hier geht es nur um die Eingangsaktivierung) und der Deaktivierung des Geräts, siehe dazu Kapitel 9.16 Deaktivierungs- und Sperroptionen.

Einstellungsarten – Auswahl der Stufe zur Systemeinstellung. Hier kann man zwischen der niedrigsten Stufe, auf der das System nichts prüft (schaltet immer scharf) und der höchsten Stufe, auf der das System eine Scharfschaltung nicht zulässt, wenn ein Gerät aktiviert ist (z.B. ein offenes Fenster), wählen, siehe dazu Kapitel 9.11 Hindernisse, die die Scharfschaltung des Systems verhindern.

Ereignisverlauf – das System erfasst Ereignisse in seinem Speicher. Die Inhalte des Speichers können von F-Link (J-Link), der LCD-Tastatur oder von der MyJABLOTRON-App aus abgerufen werden. Der Beginn eines Ereignisses wird in der Regel als Aktivierung erfasst (Status eines Geräts, Fehler, Sabotage u.s.w.) und das Ende des Ereignisses als Deaktivierung. Die Status der Bereiche werden erfasst als Scharf / Unscharf, der Alarmstatus als Alarm / Alarmablauf, stummer Alarm oder Alarmabbruch.

ID	Time	Source	Section	Event	Channel
59	9/4/2014 9:59:32 AM	Detector 11: Living room	2: Section 2	Instant activation	11: Device 11
60	9/4/2014 9:59:32 AM	Detector 11: Living room	2: Section 2	Instant Deactivation	11: Device 11
61	9/4/2014 9:59:32 AM	Detector 11: Living room	2: Section 2	Instant alarm	11: Device 11
62	9/4/2014 9:59:33 AM	Detector 4: Kitchen window	1: Section 1	Instant activation	4: Device 4
63	9/4/2014 9:59:33 AM	Detector 4: Kitchen window	1: Section 1	Instant alarm	4: Device 4

Magnetaktivierung und -deaktivierung
Alarmbeginn und -ende

Einige Ereignisse haben nur einen Aktivierungseintrag (z.B. neues Bild, Panikalarm, Konfiguration geändert).

MicroSD Speicherkarte – die Zentrale verwendet eine microSD Speicherkarte als Speichermedium. Nach der Verbindung der Zentrale mit einem PC über ein USB-Kabel werden zwei Treiber im Dateimanager angezeigt. FLEXI_CFG und FLEXI_LOG. Die Kapazität der im Lieferumfang enthaltenen Karte kann bis zu 4GB (SD/SD-HC) betragen. Wenn Sie eine vollkommen neue SD-Karte verwenden, setzen Sie die Zentrale zurück, um zu den Standardeinstellungen zu gelangen. Siehe dazu Kapitel 12 Zurücksetzen der Zentrale. Führen Sie dann eine Aktualisierung der Firmware durch, siehe dazu Kapitel 13 Firmwareaktualisierungen. Mit dieser Vorgehensweise speichern Sie alle erforderlichen Daten (Standardtexte, Sprachdateien, u.s.w..) auf der SD-Karte.

FLEXI_CFG – enthält versteckte Ordner und Dateien, die die Systemeinstellungen beinhalten. Ändern Sie nicht die Inhalte des Treibers. Dies könnte eine Beeinträchtigung der Funktionsfähigkeit des Systems zur Folge haben. Dieses Laufwerk enthält auch den Ordner J-Link mit der Software JLink.exe, die vom Systemadministrator ausgeführt und verwendet werden kann.

FLEXI_LOG – enthält die Ordner BACKUP, PHOTO und die Datei FLEXILOG.TXT, wo alle Systemereignisse erfasst werden. Ausgewählte Daten der Datei können in F-Link / Ereignisverlauf eingesehen werden. Der Ordner PHOTO wird verwendet, um IMGnnnnn.JPG-Dateien zu speichern, die von Kamerageräten (z.B. von Bewegungsmeldern mit Kamera) an die Zentrale gesendet wurden. Beide Dateitypen (txt und jpg) werden verschlüsselt gespeichert, wobei ihre Inhalte normalerweise nicht mit Text- und Bildviewern angesehen werden können. Ihre Inhalte lassen sich nur dann einsehen, wenn F-Link (J-Link) gleichzeitig auf dem PC läuft und die Berechtigungsstufe Errichter oder Administrator durch Eingabe des entsprechenden Codes bestätigt wird. Ereignisse werden in der Datei FLEXILOG.TXT bis zu einer Größe von 10 MB erfasst, danach wird die Datei als FLEXILOG.OLD neu benannt und eine neue Datei erstellt.

SIMLock – eine Funktion der Zentrale, die von einer entsprechenden AES/NSL bei der Anmeldung der Zentrale bei MyJABLOTRON aktiviert werden kann. Wenn diese Funktion aktiviert ist, werden, nachdem eine benutzte

SIM-Karte durch eine neue ersetzt wird, automatisch die AES-Einstellungen gelöscht (die Anmeldung des Systems bei MyJABLOTRON muss erneut vorgenommen werden). Mit diesem Schritt wird eine unerwünschte Informationsübertragung an die AES/NSL von einer Karte verhindert, die nicht der entspricht, für die eine Anmeldung und von der die Einstellung durchgeführt wurde.

1.1. Grundlegende Anforderungen an die Systemkonfiguration

Achten Sie auf die Anforderungen der geltenden Normen, wenn Sie das System einrichten. Die Zentralen JA-103/107K können so eingestellt werden, dass sie das Verhalten entsprechend eines **voreingestellten** Systemprofils aufweisen, um den folgenden Bedingungen (Profilen) zu entsprechen:

1. Standard - Werkseitig eingestelltes Profil, alle Systemparameter sind optional.
2. EN50131-1, Klasse 2 - Das Profil gibt spezifische Systemparameter vor (gilt für die Zentrale, Tastaturen, Sirenen usw.), die den für Sicherheitsklasse 2 geltenden Normvorgaben entsprechen. Die Parameter können nicht geändert werden.
3. INCERT, Klasse 2 – Das Profil gibt spezifische Systemparameter vor (gilt für die Zentrale, Tastaturen, Sirenen usw.), die den für Sicherheitsklasse 2 geltenden Normvorgaben entsprechen. Die Parameter können nicht geändert werden.

Hinsichtlich der Alarmmeldung und unter Berücksichtigung des gewählten und für die Sicherheitsklasse 2 gültigen Profils, muss die Zentrale entsprechend einer der folgenden Konfigurationen installiert werden:

- Mindestens eine Sirene mit einer Backup-Batterie (z.B. JA-111A oder JA-163A) und ein LAN*-Übertragungsgerät oder ein GSM-Wähl- & Übertragungsgerät.
- Zwei unabhängige Kommunikatoren, z.B. LAN* + GSM- Wähl- & Übertragungsgeräte.

***Vorsicht:** Stellen Sie sicher, dass alle LAN-Geräte, die eine Verbindung zum Internet-Netzwerk herstellen, über Reservestrom verfügen!

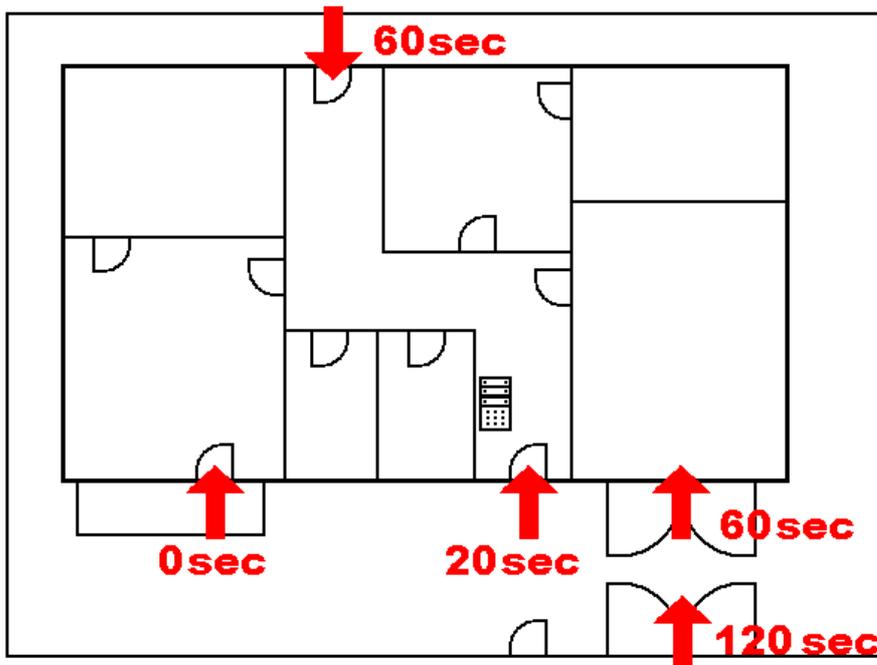
Bei der Einrichtung des Systems ist es wichtig, die Aufteilung in Bereiche und voreingestellte Eingangsverzögerungen zu berücksichtigen, um die Definition der Verzögerungszonen einzustellen. Es gibt 3 Arten von Verzögerungszonen (Verzögerung A, Verzögerung B und Verzögerung C). Jede hat zur Voreinstellung der Eingangs- und Ausgangszeiten einen eigenen Timer.

Beispiel: Ein typisches Familienhaus mit einer Garage mit einem Perimeter, das von Außenmeldern überwacht wird:

Das Haupttor oder Eingangstor und auch die Haupttür werden von einem Magnetkontakt überwacht. Das Garagentor und die hintere Tür auch. Das gesamte Gebäude mit Perimeter und die Garage werden nur von einem Bereich überwacht und die Systemtastatur befindet sich in der Eingangshalle *.

*Wir empfehlen, immer mehrere Tastaturen in der Nähe der Zutritts Türen zu den überwachten Räumen zu verwenden und sicherzustellen, dass der Zustand des Systems und der eingegebene Code von einem potenziellen Eindringling nicht erkannt werden kann.

Position und Name des Melders	Reaktion	Eingangszeit	Ausgangszeit
1. Magnetkontakt – Haupttor draußen	Verzögerung C	120 Sek.	360 Sek.
2. Bewegungsmelder – Bewegung draußen	Verzögerung C	120 Sek.	360 Sek.
3. Magnetkontakt – Garagentor	Verzögerung B	60 Sek.	120 Sek.
4. Magnetkontakt – Hintertür	Verzögerung B	60 sec	120 Sek.
5. Bewegungsmelder – PIR-Garage	Nächste Verzögerung (Verzögerung B)	60 sec	120 Sek.
6. Magnetkontakt – Haupttür	Verzögerung A	20 Sek.	60 Sek.
7. Bewegungsmelder – PIR-Halle	Nächste Verzögerung (Verzögerung A)	20 Sek.	60 Sek.
8. Magnetkontakt – Balkontür	Sofort	0 Sek.	0 Sek.
9. Bewegungsmelder – PIR-Raum	Sofort	0 Sek.	0 Sek.



Variante 1:

- Der Eingang zu den überwachten Räumlichkeiten (System ist SCHARF) durch die Haupttür löst Verzögerung A (20 Sekunden) aus und das System beginnt mit dem Zählen der Zeit zur Unscharfschaltung des Systems (Eingangsverzögerung).
- Die Eingabe eines gültigen Codes auf der Tastatur und das Drücken der grünen Taste auf dem Tastaturbereich (Segment) schaltet das System unscharf. Wenn während der Eingangsverzögerung keine Berechtigung und Unscharfschaltung des Systems durchgeführt wird, wird ein Alarm von der Verzögerungszone ausgelöst (Verzögerung A).

Variante 2:

- Der Eingang zum überwachten Gebäude (System ist SCHARF) durch die Hintertür oder das Garagentor löst die Verzögerung B (60 Sek.) aus und das System beginnt mit dem Zählen der Zeit, um das System unscharf zu schalten (Eingangsverzögerung).
- Die nächste erkannte Bewegung von Meldern mit einer Verzögerung-A-Reaktion verkürzt die Eingangsverzögerung entsprechend der Verzögerung A (20 Sek.), wenn die Verzögerung kürzer als Verzögerung B ist.
- Die Eingabe eines gültigen Codes auf der Tastatur und das Drücken der grünen Taste auf dem Tastaturbereich (Segment) schaltet das System unscharf. Wenn die Berechtigung und Unscharfschaltung des Systems während der Eingangsverzögerung nicht durchgeführt wird, wird ein Alarm aus der Verzögerungszone ausgelöst - aus der Zone, in der die Zeit zuerst abläuft (Verzögerung A, Verzögerung B).

Variante 3:

- Eingang zu dem überwachten Gebäude (System ist SCHARF) durch die Aktivierung eines Außenmelders (Öffnen des Haupttors, Eingangstor oder PIR-Aktivierung im Außenbereich) löst die Eingangszeit (120 Sek.) der Verzögerung C aus und das System beginnt mit dem Zählen der Zeit, um das System unscharf zu schalten (Eingangsverzögerung).
- Beim Öffnen des Garagentores und der Aktivierung eines Magnetmelders beginnt das System mit dem Zählen der Verzögerungszeit B (60 Sek.) und verkürzt die Zeit der bereits aktivierten Verzögerungszone C (wenn die Verzögerung C nicht kürzer als die Verzögerung B ist).
- Wenn Sie durch die Haupttür gehen, wird die Verzögerung A (20 Sek.) aktiviert und die Eingangszeit wird verkürzt (wenn Verzögerung B oder Verzögerung C nicht kürzer als Verzögerung A ist).
- Die Eingabe eines gültigen Codes auf der Tastatur und das Drücken der grünen Taste auf dem Tastaturbereich (Segment) schaltet das System unscharf. Wenn die Berechtigung und Unscharfschaltung während der Eingangsverzögerung nicht durchgeführt wird, wird ein Alarm aus der Verzögerungszone ausgelöst - aus der Zone, in der die Zeit zuerst abläuft (Verzögerung A, Verzögerung B, Verzögerung C).

1.2. Zugriffscodes und ihre Standardeinstellungen

Die Berechtigung durch einen gültigen (4-, 6- oder 8-stelligen) Code oder die Verwendung einer RFID-Karte oder Tags am Berechtigungsmodul (der Tastatur) ist für die Bedienung des Systems (Scharf-, Unscharfschaltung oder die Prüfung des Status eines Geräts oder Bereichs) erforderlich.

Gemäß der Berechtigungsstufe, die der entsprechende Benutzer hat, zeigt das System alle Informationen, zu denen der Benutzer die Zugriffsrechte hat, an und ermöglicht eine den Zugriffsrechten entsprechende Steuerung des Systems.

Die Berechtigung zur Steuerung des Systems über eine Tastatur, F-Link (J-Link), der MyJABLOTRON-App oder des Sprachmenüs muss durch Eingabe eines Zahlencodes erfolgen. Der Code kann mit einem Präfix oder ohne Präfix eingegeben werden (Standardeinstellung).

Geben Sie einen Code ohne Präfix in dem folgenden Format ein:

CCCC

wo: **cccc** ist ein 4-, 6- oder 8-stelliger Code, es sind Codes von 0000 bis 99999999 erlaubt

Die Zentrale wird mit zwei Standardcodes geliefert:

Standardcodes ohne Präfix	4-stellig	6-stellig	8-stellig
Service	1010	101010	10101010
Administrator	1234	123456	12345678

Die Standardcodes werden automatisch von F-Link ausgefüllt, so dass die Software sie von der ersten Aktivierung bis zu einem Codewechsel nicht anfordert. Aus Sicherheitsgründen sollten jedoch unmittelbar nach Fertigstellung der Installation alle Standardcodes geändert werden. Wenn beide Codes nicht geändert werden, wird beim Beenden des Errichtermodus eine SMS an die Errichter-Telefonnummer mit dem Hinweis „**Warnhinweis, Standardcodes, Bereich 1**“ gesendet (sie kann in den Parametern "Standardcodes Warnhinweis" abgebrochen werden).

Bei Systemen mit einer höheren Anzahl von Benutzern kann das Präfix aktiviert werden. Bei Präfix-Aktivierung können Benutzer ihre Codes selbst über die LCD-Tastatur ändern. Das Präfix kann auf der Registerkarte Systemübersicht in F-Link aktiviert werden.

Geben Sie einen Code mit einem Präfix in dem folgenden Format ein:

ppp*cccc

wo: **ppp** ist die laufende Nummer (Position **0 bis 600**) des Benutzers (Präfix genannt)

* ist ein Trennzeichen (* Schlüssel)

cccc ist ein 4-, 6- oder 8-stelliger Code, es sind Codes von 0000 bis 99999999 erlaubt

In diesem Fall werden der Errichter- und Administrator-Code wie folgt eingestellt:

Standardcodes mit Präfix	4-stellig	6-stellig	8-stellig
Service	0*1010	0*101010	0*10101010
Administrator	1*1234	1*123456	1*12345678

Vorsicht: Der **Errichter-Code** muss immer mit dem Präfix **0** beginnen.
Der **Administrator-Code** muss immer mit dem Präfix **1** beginnen.

Warnhinweis: Wenn das Präfix deaktiviert ist, werden die Codes immer auf die Standardwerte zurückgesetzt und alle anderen Codes werden gelöscht (alle RFID-Karten / Tags mit Zugriff bleiben erhalten). Wenn das Präfix aktiviert ist, bleiben die Einstellungen aller Codes und Karten / Tags gleich und die Präfixe werden nur hinzugefügt.

1.2.1. Änderung des Zugriffscodes

Wenn die Option "Code mit Präfix" aktiviert ist, ermöglicht die Zentrale die willkürliche Kombination eines 4 - 8-stelligen Codes für jeden Benutzer (sie können sogar denselben Code mit einem anderen Präfix haben). Jeder Benutzer mit einer Berechtigung "Benutzer" und dem aktivierten Parameter "Code-Änderung erlaubt" hat die Möglichkeit, seinen eigenen Code zu bearbeiten.

Zugriffscodes können geändert werden von:

- der LCD-Tastatur (der PC darf nicht mit der Zentrale verbunden sein, es darf keine lokale oder ferngesteuerte Verbindung geben).

- der Software J-Link, die in der Disk-Einheit der Zentrale verfügbar ist (erscheint, wenn Sie ein USB-Kabel anschließen) oder von der Software F-Link (Errichter), die von MyCOMPANY heruntergeladen werden kann.
- der MyJABLOTRON Smartphone-App (ab Version 3.5).

Wenn die Option „Code mit Präfix“ deaktiviert ist, erlaubt die Zentrale die Kombination eines 4-8-stelligen Codes für jeden Benutzer. Jedoch beschränkt die Zentrale die Verwendung des gleichen Codewerts für einen anderen Benutzer, der bereits im System verwendet wird. Nur der / die Systemadministrator (en) ist / sind voll verantwortlich für die Bearbeitung bereits bestehender Benutzercodes und die Vergabe neuer Codes.

Zugriffscodes können nur von einem Administrator geändert werden von:

- der LCD-Tastatur (der PC darf nicht mit der Zentrale verbunden sein, es darf keine lokale oder ferngesteuerte Verbindung geben).
- der Software J-Link, die in der Disk-Einheit der Zentrale verfügbar ist (erscheint, wenn Sie ein USB-Kabel anschließen) oder von der Software F-Link (Errichter), die von MyCOMPANY heruntergeladen werden kann.
- der MyJABLOTRON Smartphone-App (ab Version 3.5).

1.2.2. Sicherheitszugriffscodes und RFID-Geräte

Über die Zentrale können Sie jedem berechtigten Benutzer einen 4-, 6- oder 8-stelligen Code und bis zu zwei RFID-Tags zuweisen. Die Berechtigung ist erforderlich, wenn das System mit einer Tastatur, einem Sprachmenü, einem PC, einer webbasierten oder einer Smart-App gesteuert wird. Die Sicherheitsstufe ist hierfür ausreichend und kann über Zahlen dargestellt werden.

Die Kalkulation der Code-Kombinationen gemäß 1 Benutzer wird in den folgenden Beispielen dargestellt:

Parameter der Zentrale	4-stellig	6-stellig	8-stellig
„Code mit Präfix“ aktiviert	= 10^4 = (10,000)	= 10^6 = (1,000,000)	= 10^8 = (100,000,000)
„Code mit Präfix“ und „Erzwungene Zugriffssteuerung“ deaktiviert	= 10^4 - (Anzahl der Benutzer im System - 1)	= 10^6 - (Anzahl der Benutzer im System - 1)	= 10^8 - (Anzahl der Benutzer im System - 1)
„Code mit Präfix“ deaktiviert und „Erzwungene Zugriffssteuerung“ aktiviert	≤ 10^4 - ((Anzahl der Benutzer im System - 1) * 3)	≤ 10^6 - ((Anzahl der Benutzer im System - 1) * 3)	≤ 10^8 - ((Anzahl der Benutzer im System - 1) * 3)
Verwendung einer RFID-Karte mit nur 14 Zeichen (6 feste + 8 variable)	= 10^8 = (100,000,000)	= 10^8 = (100,000,000)	= 10^8 = (100,000,000)
„Code mit Präfix“ und „Kartenbestätigung mit einem Code“ aktiviert	= $(10^8 * 10^4)$ = 10^{12} = (1,000,000,000,000)	= $(10^8 * 10^6)$ = 10^{14} = (100,000,000,000,000)	= $(10^8 * 10^8)$ = 10^{16} = (1,000,000,000,000,000,000)
„Code mit einem Präfix“ deaktiviert und „Kartenbestätigung mit einem Code“ aktiviert	= $10^8 * (10^4 - (Anzahl der Benutzer im System - 1))$	= $10^8 * (10^6 - (Anzahl der Benutzer im System - 1))$	= $10^8 * (10^8 - (Anzahl der Benutzer im System - 1))$

Beispiel: Unter Verwendung eines 4-stelligen Standard-Zugriffscodes mit einer aktivierten Funktion, „Codes mit Präfix“ genannt, werden 104 (10.000) Code-Kombinationen für jeden Benutzer erreicht. Die Anzahl der Kombinationen wird reduziert, indem Präfixe deaktiviert und die Anzahl der Benutzer erhöht wird. Dies hängt auch vom Parameter „Erzwungene Zugriffssteuerung“ ab, da jedem Benutzer ein weiterer Code hinzugefügt wird.

Eine Lösung, um das Risiko des Codeknackens zu reduzieren, kann wie folgt aussehen:

- Verwendung eines 6- oder 8-stelligen Code(s).
- Auswahl einer höheren Berechtigungsstufe wie „Kartenbestätigung mit Code“ oder „Doppelte Berechtigung“.
- Verwendung der kontaktlosen RFID Karten / Tags (JA-19xJ) von JABLOTRON.

Die Zentrale zählt die Versuche falsch eingegebener Codes. Nach dem 10. Versuch löst das System das Manipulationsereignis „Versuch, den Code zu knacken“ aus und meldet dieses Ereignis vordefinierten Nummern. Die Eingabe anderer Codes in das System wird nicht zusätzlich gesperrt. Nach einer gültigen Codeeingabe wird der Zähler der falsch eingegebenen Codes zurückgesetzt und der ausgelöste Alarm beendet. Dieser Zähler ist auf 10 Versuche voreingestellt und kann nicht geändert werden.

1.2.3. Regelmäßige Prüfung des Systems (Wartung)

Das gesamte Sicherheitssystem muss regelmäßig auf seine korrekte Funktionsfähigkeit und die seiner Teile geprüft, sowie gereinigt und äußerlich (Staub und Schmutz, in der Regel vom Systembenutzer durchgeführt) und intern (Spinnweben, Insekten, Batteriestatus u.s.w.) vom Errichter durchgeführt werden. Einige Systemteile sind in der Lage, einen Selbsttest durchzuführen und einen möglichen Fehlerbericht an die Zentrale zu senden und über diesen Status entsprechend der Einstellungen zu informieren. Fast alle Wartungsschritte müssen von einem Errichter während der jährlichen Systemprüfung durchgeführt werden.

Die Haupt-Backup-Batterie wird in regelmäßigen Abständen einige Male pro Minute von der Zentrale getestet. Drahtlose Gerätebatterien (in Meldern, Tastaturen, Sirenen, Fernbedienungen) werden automatisch bei jeder regelmäßigen Testübertragung geprüft. Das System meldet eine schwache Batterieleistung eines anmeldeten Geräts von dem Moment an, in dem sie auftritt bis zu dem Zeitpunkt, an dem sie ersetzt wird, über eine voreingestellte SMS-Meldung und gleichzeitig auf der LCD-Tastatur. Der Austausch der Batterien kann von einem Errichter im Errichtermodus oder dem Administrator durchgeführt werden. Wenn eine Batterie herausgenommen wird, sollten Sie einen Moment (20 Sekunden) warten, bis die internen Kondensatoren entladen sind und kann dann eine neue Batterie einlegen.

Überblick der empfohlenen Wartung / Funktionssteuerung:

Gerätetyp	Beschreibung	Wer nimmt dies vor	Häufigkeit
Rauch- & Feuermelder	Funktionstests; Benachrichtigen Sie vorher die AES/NSL!	Administrator	Einmal pro Monat
	Reinigung von Staub und Schmutz	Administrator	Zweimal pro Jahr
	Prüfung der Batterie (BUS und drahtlose Geräte)	Errichter	Einmal pro Jahr
Panik- & Überfalltasten	Funktionstests; Benachrichtigen Sie vorher die AES/NSL!	Administrator	Einmal pro Monat
	Prüfung der Batterie, Spannungsmessung, physikalischer Status	Errichter	Einmal pro Jahr
Melder	Reinigung von Staub und Schmutz	Administrator	Einmal pro Jahr
	Funktionstests; Test des RF-Bereichs drahtloser Melder. Test durch Aufnahme eines Bildes bei Meldern mit eingebauter Kamera.	Errichter	Einmal pro Jahr
	Batterietest, Spannungsmessung jeder Batterie, physikalischer Status u.s.w.	Errichter	Einmal pro Jahr
Bedienteile & Tastaturen	Reinigung von Staub und Schmutz	Administrator	Zweimal pro Jahr
	Prüfung jeder Taste, Funktionstasten und RFID-Sensor; Prüfung des RF-Bereichs für drahtlose Tastaturen.	Errichter	Einmal pro Jahr
	Prüfung des Batteriestatus und des physikalischen Status, Spannungsmessung jeder Batterie u.s.w.	Errichter	Einmal pro Jahr
Sirenen	Reinigung von Staub und Schmutz, Insekten, Prüfung, ob Wasser an der Leiterplatte eingetreten ist u.s.w.	Errichter	Einmal pro Jahr
	Funktionstests; Test des RF-Bereichs für drahtlose Sirenen.	Errichter	Einmal pro Jahr
	Prüfung der Batterien oder Backup-Batterien, Messung, physikalischer Status, Spannungsmessung jeder Batterie	Errichter	Einmal pro Jahr
Fernsteuerungen (RC)	Funktionstests; RF-Bereich, Prüfung geringer Batterieleistung, Reinigung oder Austausch des Gehäuses	Administrator oder Errichter	Einmal pro Jahr
Alarmstatus	Kommunikationstest zur AES/NSL, Sprachanrufe und SMS-Berichte.	Administrator oder Errichter	Einmal pro Jahr
Backup-Batterie in der Zentrale	Test während der Trennung vom Netzstrom (AC) und Spannungsmessung einer Backup-Batterie nach 5 Minuten ohne Netzstrom.	Errichter	Einmal pro Jahr
Programmierbare Ausgänge (PG)	Funktionstests; RF-Bereich für drahtlose Module	Errichter	Einmal pro Jahr

Alle vom Systemhersteller empfohlenen Verfahren haben keine höhere Priorität als die örtlichen Vorschriften und Verordnungen.

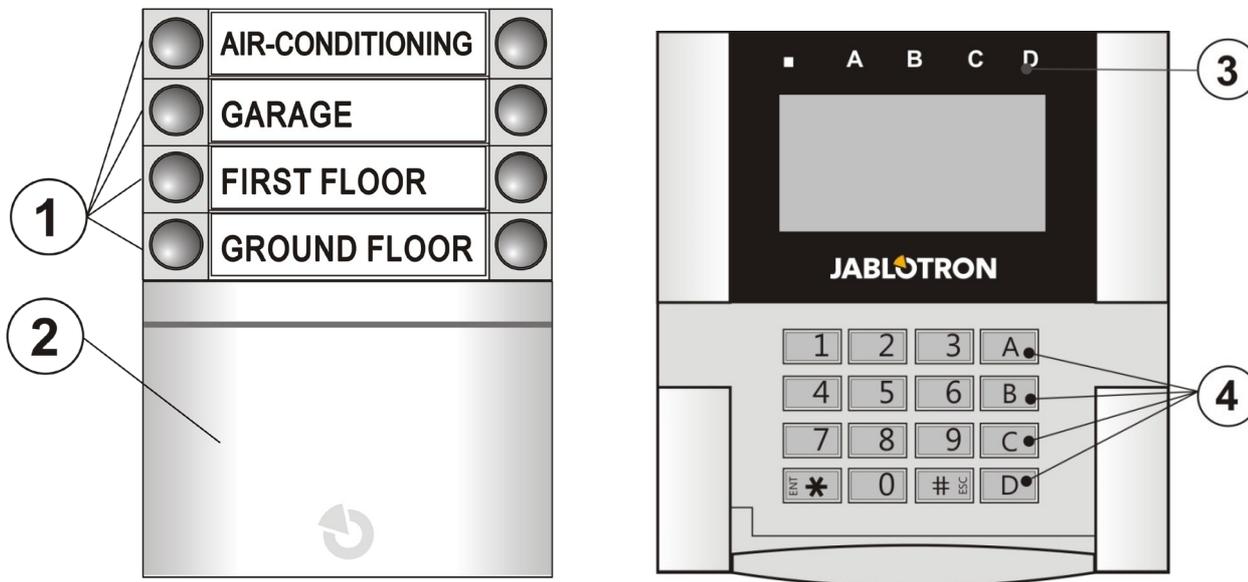


2. Systemgröße

Der Systembereich kann entsprechend der Gebäudegröße und der Benutzeranforderungen eingestellt werden.

2.1. Externe Größe

Die externe Größe des Systems, wie es von seinen Benutzern gesehen wird, kann durch die Baugruppe des Zugriffsmoduls (Bereichs- bzw. Segmenttastatur) definiert werden. Die Tastatur JA-110E / JA-150E hat 4 Funktionstasten und kann nicht verändert werden. Sie können für die Steuerung von Bereichen und PG-Ausgängen eingestellt werden.



1 – Steuerungssegmente; 2 – Zugriffsmodule; 3 – Bereichsanzeigen; 4 – Funktionstasten

Eine Tastatur kann über bis zu 20 **Steuerungsbereiche (Segmente)** verfügen. Jedes Segment hat zwei Tasten (AUS - links und EIN - rechts). Ein Segment wird verwendet, um einen Bereich zu steuern (scharf schalten / unscharf schalten), um Geräte zu steuern oder Hilfe zuzurufen. Ein Segment kann auch verwendet werden, um den Status eines Bereichs oder PG-Ausgangs anzuzeigen (es kann den aktiven Status sowohl mit einer roten LED als Standard als auch mit einer grünen LED anzeigen - Segmentfunktion „umgekehrte Anzeige“). Zum Beispiel ist es auf der Tastatur möglich, die Segmentaktivierung / -deaktivierung eines an einer Tür installierten Magnetmelders zu überwachen, wenn diese geöffnet oder geschlossen ist. Hier ist die Voreinstellung als "Gemeinsames Segment" für die gleichzeitige Steuerung mehrerer Bereiche möglich.

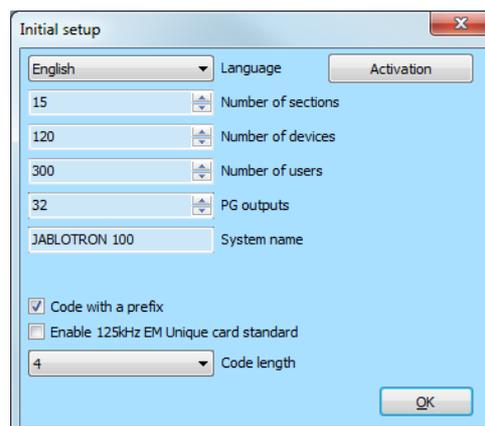
Ein **Zugriffsmodul** überprüft die Berechtigung von Benutzern. Die Berechtigungsmethode wird durch die Modulauswahl bestimmt (RFID-Karte / Tag-Leser, Tastatur + RFID-Leser, Tastatur mit einem LCD-Display + RFID-Leser). Das Modul ermöglicht auch das Öffnen eines Türschlosses durch Anwendung einer Karte / eines Tags (Codeeingabe). Module sind in einer drahtlosen und BUS-Version verfügbar. Die Funktionen gelten für beide Versionen.

Die Konfiguration der Steuerungstastatur wird in Kapitel 10.5.1 Tastaturkonfiguration beschrieben.

2.2. Interne Größe (Systembereich)

Die Zentrale kann in 15 Sicherheitsbereiche (unabhängig voneinander einstellbare Teile) unterteilt werden. Jedes Gerät hat seine eigene Adresse (Tastatur, Melder, Sirenen) und muss bei einem Bereich angemeldet werden. Jeder Benutzer kann nur auf die erforderlichen Bereiche zugreifen, wenn eine Berechtigung eingestellt wurde. Die Anzahl der Bereiche wird in F-Link in der Registerkarte Systemübersicht festgelegt. Es macht das Programmieren organisierter. Ihre Anzahl kann erhöht oder verringert werden (es sei denn, es werden Verbindungen hergestellt, die eine Verringerung der Bereichszahl unmöglich machen würden).

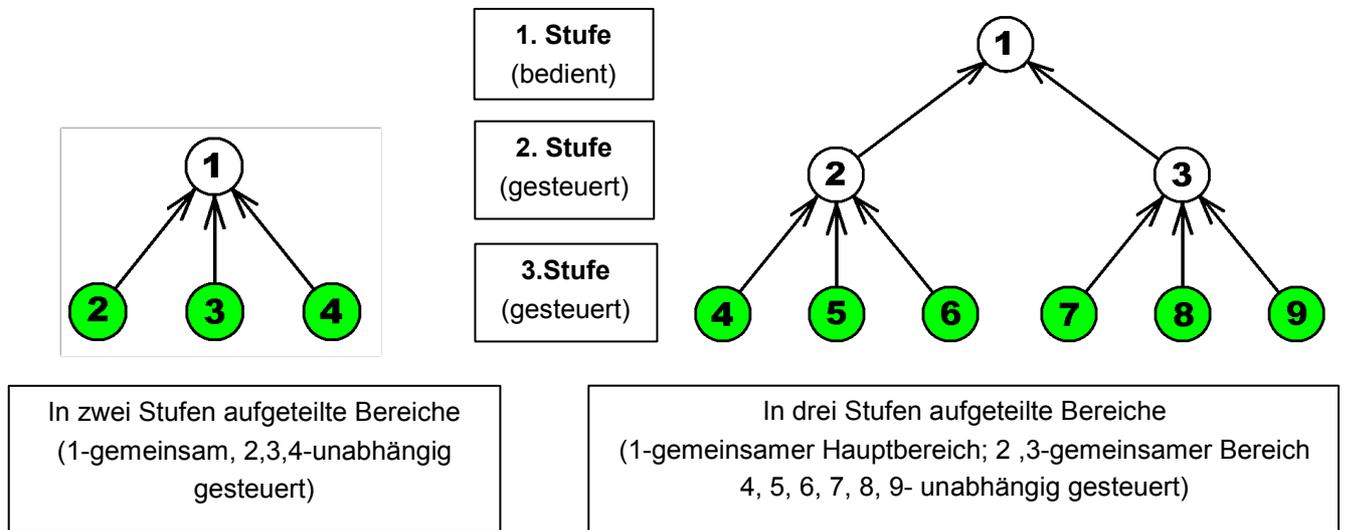
Die Anzahl der Geräte, Bereiche, Benutzer und programmierbaren Ausgänge wird über F-Link festgelegt. Sie können ein System sowohl



für eine kleine Wohnung mit einem Bereich und einigen Geräten als auch für ein großes Gebäude erstellen und das System JABLOTRON 100+ mit unabhängig gesteuerten Bereichen optimal nutzen. Ein Bereich kann mit anderen Bereichen verknüpft werden, um sie und ihre Status gemeinsam zu steuern.

2.2.1. Konfiguration and Aufteilung

Die Zentrale des Sicherheitssystems JA-103K dient zum Schutz kleiner Gebäude. Für mittlere und große Gebäude ist das System JA-107K besser geeignet. Dank seiner Reichweite, Abmessungen und Anzahl der Bereiche bietet es eine große Variabilität, um die jeweilige Installation anzupassen. Ein Sicherungsbereich ist ein Teil des Systems, dem Geräte zugewiesen sind, die sich auf einen überwachten Bereich beziehen. Kleine Gebäude können einen Grundbereich haben (Wohnung, kleines Familienhaus). In diesem Fall sind alle Geräte demselben Bereich zugeordnet. Mittlere Systeme können mehrere Bereiche (zum Beispiel Wohnungen in einem Wohnblock, Firmengebäude) und auch einen eigenen gemeinsamen Bereich auf der zweiten Stufe (Gemeinschaftsraum, Keller usw.) haben. Größere Gebäude können viele weitere Bereiche (Büros, gemeinsame Bereiche der 2. Stufe (zum Beispiel mehrstöckige Gebäude) und Gemeinschaftsräume wie eine Rezeption oder Lobby als gemeinsamen Bereich der 3. Stufe (siehe Bild) haben. Sehr wichtig für den Betrieb solcher Systeme ist das Einstellen der Benutzerberechtigung auf die niedrigste Steuerungsstufe der Bereiche, für die sie zugewiesen wurden. Wenn alle Bereiche, die der zweiten oder dritten Stufe des gemeinsamen Bereichs zugewiesen wurden, scharf geschaltet sind, wird jeder gemeinsame Bereich automatisch scharf geschaltet und automatisch unscharf geschaltet, wenn mindestens einer der Grundbereiche unscharf geschaltet wird. Benutzer können nur Bereiche der ersten Stufe steuern. Siehe die folgende Abbildung:



Es wird empfohlen, für höhere Stufen gemeinsamer Räume (2. und 3. Stufe) Tastaturen mit einer bestimmten Anzahl von Bereichen (Segmenten) zu verwenden, die den verwendeten Bereichen entsprechen, um zu bestimmen, welcher Bereich nach dem Betreten des überwachten Gebäudes aktiviert / deaktiviert wird.

Für Tastaturen der 1. Stufe ist es ausreichend, diese mit Steuerungsbereichen (Segmenten) auszustatten, die einem oder mehreren bestimmten Bereichen zugeordnet sind.

3. Zentralentypen, Systemparameter

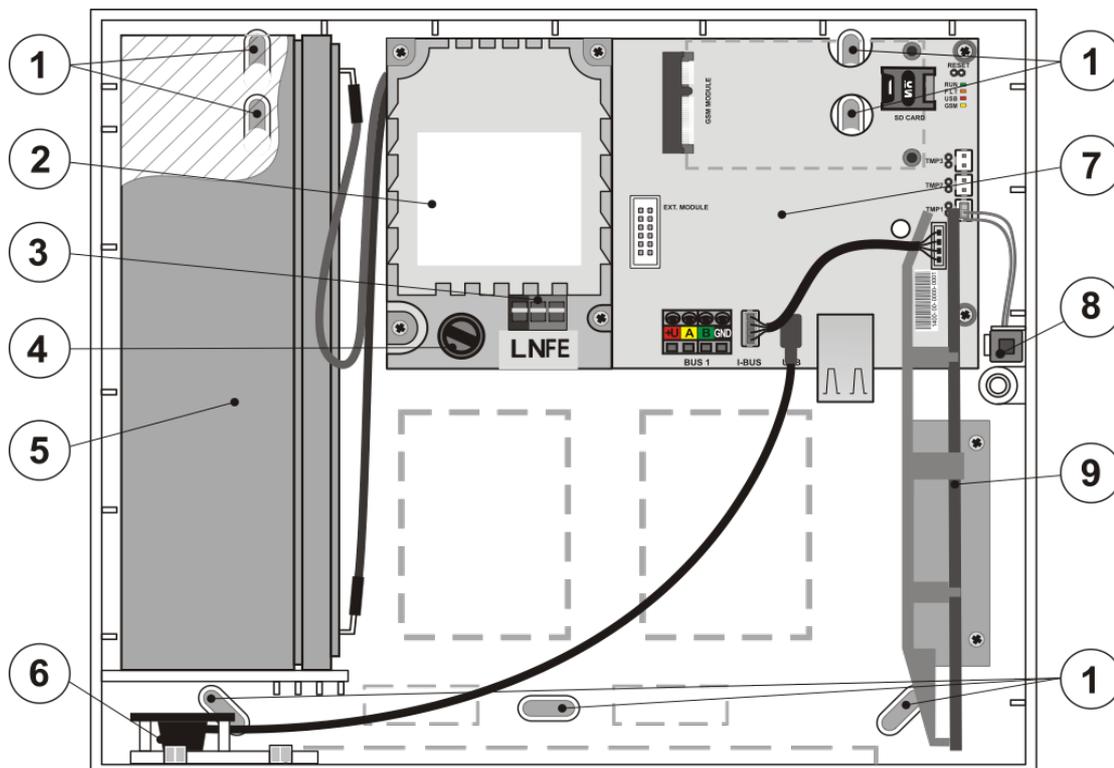
Funktion / Typ	JA-103K	JA-107K	Hinweis	
Maximale Geräteanzahl	50	230	JA-107K Max. 120 drahtlose Geräte auf den Positionen 1 – 120 und max. 60 Geräte pro 1 BUS- Klemme	
Maximale Benutzeranzahl	50	600		
Maximale Anzahl von unabhängigen Bereichen (Partitionen)	8	15		
Maximale Anzahl der programmierbaren Ausgänge	32	128	Nur die PGs 1 – 32 können für die drahtlose Übertragung verwendet werden	
GSM / GPRS-Kommunikator	Nein	Nein	Das optional verfügbare GSM-Modul JA-19xY	
IP LAN (Ethernet) Kommunikator	Ja	Ja		
Maximale Anzahl der Funkmodule	3	3	Optional verfügbarer Funkverstärker	
SMS-Meldungen	Bis zu 8 Benutzer	Bis zu 50 Benutzer	5 Meldungen pro 1 Ereignis	
Sprachmeldungen	Bis zu 8 Benutzer	Bis zu 50 Benutzer	5 Meldungen pro 1 Ereignis	
Empfohlene 12 V Backup-Batterie	2.6 Ah	7 bis 18 Ah		
Höchst möglicher kurzfristiger Strombedarf	1000 mA	2000 mA dauerhaft 3000 mA für 60 Min. (max. 2000 mA für einen BUS)		
Maximaler Dauerstromverbrauch bei einer Backup-Versorgung von 12 Std.	JA-103K – 2.6 Ah Batterie		JA-107K – 18 Ah Batterie	
	Ohne GSM- Wähl- & Übertragungs- gerät	LAN – AUS – 115 mA LAN – EIN - 88 mA	Ohne GSM- Wähl- & Übertragungs- gerät	LAN – AUS – 1135 mA LAN – EIN - 1107 mA
	Mit GSM- Wähl- & Übertragungs- gerät	LAN – AUS – 80 mA LAN – EIN - 53 mA	Mit GSM- Wähl- & Übertragungs- gerät	LAN – AUS – 1100 mA LAN – EIN - 1072 mA
BUS-Klemmen	BUS 1 + 4 -poliger Stecker (I-BUS) für das Funkmodul	BUS 1, BUS 2 + 4- poliger Stecker (BUS 3) für das Funkmodul oder den Splitter JA- 110Z-D	Die JA-107K Klemmen sind isoliert, d.h. der Kurzschluss eines Stromkreises hat keinen Einfluss auf andere Stromkreise.	
Maximale BUS-Kabellänge	500 m	3 x 500m	Kann mit den Modulen JA-110T oder JA-120Z erweitert werden.	

3.1. Beschreibung der Zentrale JA-103K

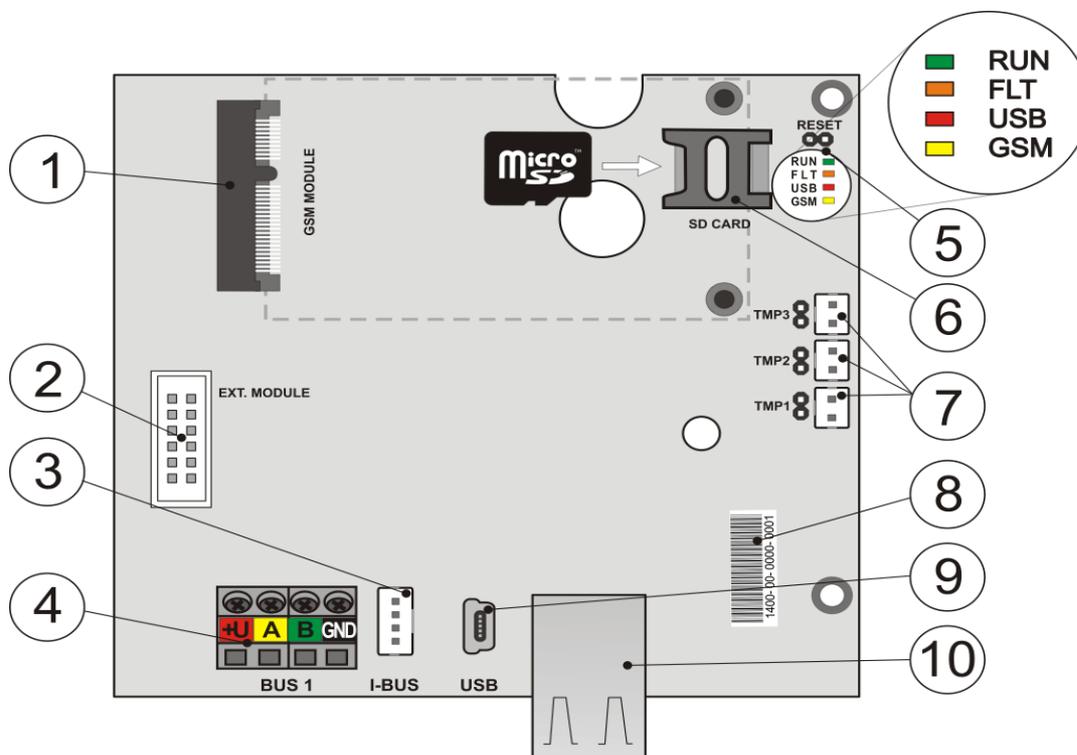
Die Zentrale JA-103K ist für **kleine BUS-Systeme** (begrenzt durch den Ausgang der Stromversorgung) und für **mittelgroße Systeme** mit drahtloser Kommunikation ausgelegt. Die Zentrale ist mit einem LAN-Übertragungsgerät ausgestattet, der mit dem Internet verbunden ist und Daten an Server (Bilder von Photoverifikationsgeräten), JABLOTRON Cloud-Dienste oder an den Server von Sicherheitsbehörden, die über die technische Ausrüstung verfügen, um diese Daten empfangen zu können, senden kann. Wenn Sie über das LAN-Übertragungsgerät mit dem Internet verbunden sind, ist der Fernzugriff auch über die F-Link (J-Link) möglich.

Die Zentrale kann um zusätzliche Übertragungsgeräte erweitert werden:

Der JA-19xY – GSM-Wähl- & Übertragungsgerät für GSM/GPRS-Kommunikation. Es ermöglicht die selben Kommunikations- und Servicemöglichkeiten wie der LAN-Übertragungsgerät.



- 1 – Wandbefestigungslöcher; 2 – Stromversorgungsmodul; 3 – Netzanschlussklemmen; 4 – Netzsicherung;
5 – Backup-Batterie; 6 - USB-Anschluss für die Verbindung mit dem PC; 7 – Zentrale Platine;
8 – Sabotagekontakt des Gehäuses; 9 – Funkmodulhalterung JA-11xR



1 - GSM-Kommunikatoranschluss; 2 – Anschluss für zusätzliche Module; 3 – BUS-Klemme für das interne Funkmodul JA-11xR; 4 – BUS-Klemmen; 5 – LED-Anzeigen und RESET-Jumper; 6 – MicroSD-Kartenhalterung; 7 – Anschluss für den Sabotagekontakt des Gehäuses, 8 – Produktionscode; 9 MiniUSB-Anschluss; 10 – LAN-Anschluss

Teile der Zentrale JA-103K (auswechselbare Teile) sind:

- MicroSD-Karte

Zur Erweiterung der Zentralenoption verwenden Sie:

- Das Funkmodul JA-11xR
- Den GSM-Wähl- & Übertragungsgerät JA-19xY

Zum Zubehör der Zentrale gehören:

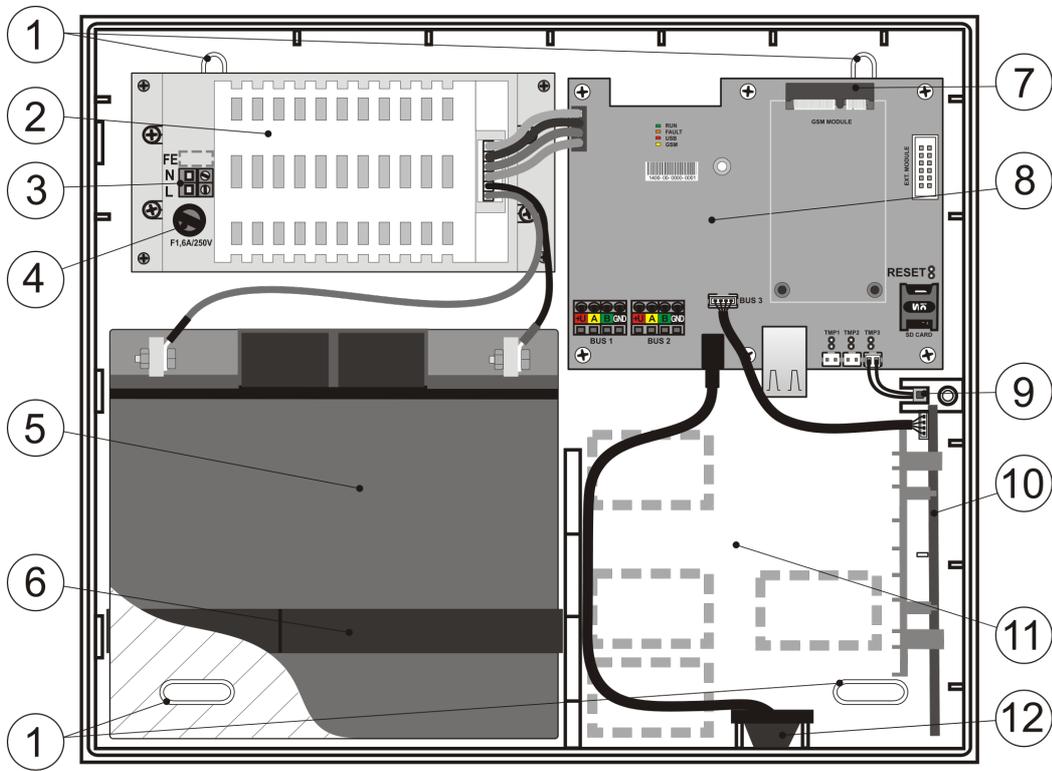
- 1x USB-Kabel (180 cm)
- 1x Verbindungskabel für das Funkmodul JA-11xR
- 1x verlängertes USB-Kabel (20 cm) in der Zentrale installiert
- 1x Sicherung T 1.6 A; 250 V
- 4x Jumper (für den Jumper-Steck-Anschluss)
- 6x Warnhinweistiketten
- 4x Verbindungselemente 8 mm
- 4x Schrauben 40 mm
- 3x Verbindungsstücke 100 mm
- Bohrschablone A4
- CZ / EN Installationshandbuch (Kurzversion)

3.2. Beschreibung der Zentrale JA-107K

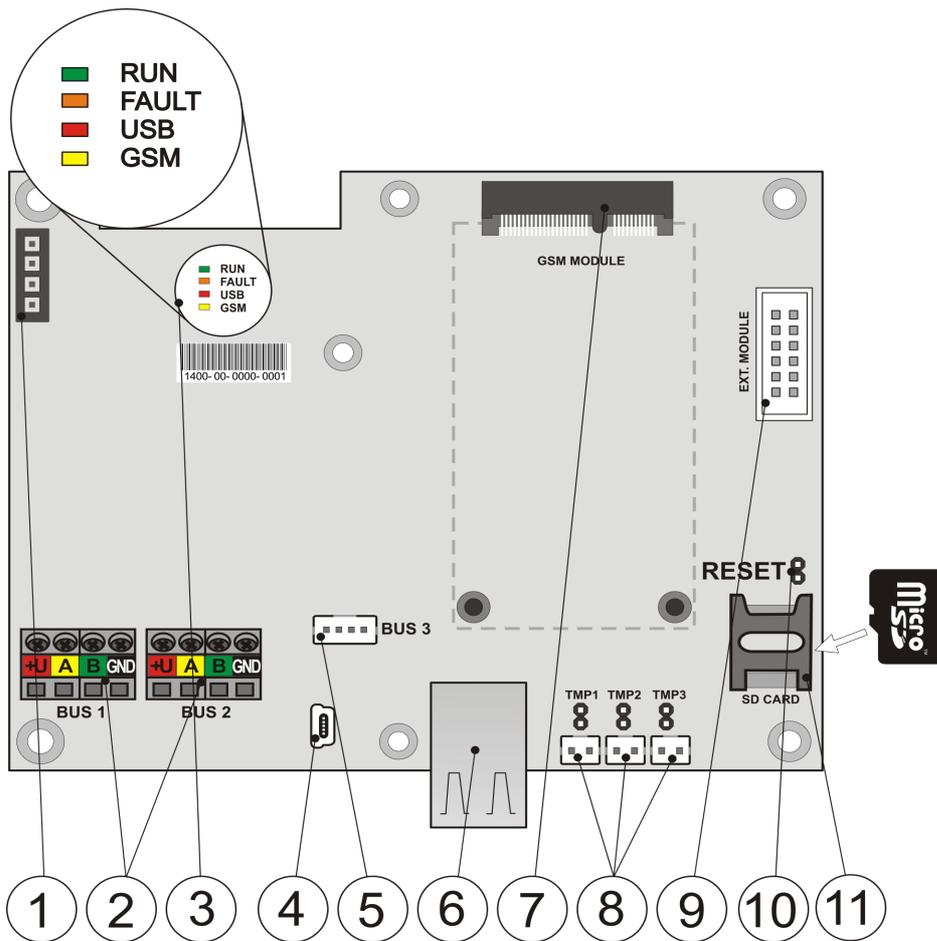
Die Zentrale JA-107K ist für **mittlere und große Installationen**, sowohl für **BUS- als auch für drahtlose Systeme** ausgelegt. Die Zentrale ist mit einem LAN-Übertragungsgerät ausgestattet, der mit dem Internet verbunden ist und Daten an Server (Bilder von Photoverifikationsgeräten), JABLOTRON Cloud-Dienste oder an den Server von Sicherheitsbehörden, die über die technische Ausrüstung verfügen, um diese Daten empfangen zu können, senden kann. Wenn Sie über das LAN-Übertragungsgerät mit dem Internet verbunden sind, ist der Fernzugriff auch über die F-Link (J-Link) möglich.

Die Zentrale kann um zusätzliche Kommunikatoren erweitert werden:

JA-19xY – GSM-Wähl- & Übertragungsgerät für GSM/GPRS-Kommunikation. Er ermöglicht die selben Kommunikations- und Servicemöglichkeiten wie der LAN-Kommunikator.



1 – Wandbefestigungslöcher; 2 – Stromversorgung der Zentrale; 3 – Netzanschlussklemmen; 4 – Netzsicherung; 5 – Backup-Batterie; 6 - Befestigungsband der Backup-Batterie; 7 – GSM-Kommunikatoranschluss; 8 – Zentrale Platine; 9 – Sabotagekontakt des Gehäuses; 10 – Funkmodulhalterung JA-11xR; 11 – Verkabelungsraum; 12 - USB-Anschluss für die Verbindung mit dem PC)



1 – Netzanschlussklemmen; 2 – Unabhängige BUS-Klemmen; 3 – LED-Anzeigen; 4 – MiniUSB-Anschluss; 5 – BUS-Klemme für das Funkmodul oder eine dritte BUS-Klemme; 6 – LAN-Anschluss; 7 – GSM-Kommunikatoranschluss; 8 – Anschluss für die Sabotagekontakte des Gehäuses; 9 – Anschluss für zusätzliche Module; 10 – RESET-Jumper; 11 – MicroSD-Kartenhalterung

Teile der Zentrale JA-107K (auswechselbare Teile) sind:

- MicroSD-Karte

Zur Erweiterung der Zentralenoption verwenden Sie:

- Das Funkmodul JA-11xR
- Den GSM-Wähl- & Übertragungsgerät JA-19xY

Zum Zubehör der Zentrale gehören:

- 1x USB-Kabel (180 cm)
- 1x Anschlusskabel für das Funkmodul JA-11xR
- 1x verlängertes USB-Kabel (20 cm) in der Zentrale installiert
- 1x Sicherung T 1.6 A; 250 V
- 4x Jumper (für den Jumper-Steck-Anschluss)
- 6x Warnhinweisetiketten
- 4x Verbindungselemente 8 mm
- 4x Schrauben 40 mm
- 2x Verbindungsstücke 150 mm
- Bohrschablone A3
- 2x Schrauben 3x8 mm
- 2x Reduktion für den Anschluss der FASTON-Klemme an die Batterie
- CZ / EN Installationshandbuch (Kurzversion)

3.3. LED-Anzeigen der Leiterplatte der Zentrale

Alle Versionen der Zentrale verfügen über folgende LED-Anzeigen auf dem Mainboard:

Beschreibung	Farbe	Bedeutung
RUN	grün	Das Blinken während des Kommunikationsbetriebs zeigt die korrekte Funktionsweise des BUS an.
FAULT	gelb	Ein dauerhaftes Leuchten zeigt einen allgemeinen Fehler im System an (weitere Informationen über F-Link oder eine Tastatur mit Display)
USB	gelb	zeigt die USB-Verbindung mit einem PC an
GSM	rot	Bei Installation eines GSM-Wähl- & Übertragungsgerät: <ul style="list-style-type: none">– Leuchtet nach der Verbindung zum Stromnetz dauerhaft auf, wenn nach einem GSM-Netz gesucht wird (maximal 1 Minute lang).– AUS, wenn GSM ok ist und keine Kommunikation stattfindet.– Blinkt in 1 Sek. / 1 Sek. EIN / AUS-Intervallen, wenn kein GSM-Netzwerk verfügbar ist. <i>Hinweis: Blinkt während der Kommunikation, mit einem kurzen wiederholten Blinken wird die Parametereinstellung angezeigt: GSM- Übertragungsgerät AUS.</i>

3.4. Zusätzliche Anschlüsse auf der Leiterplatte der Zentrale

Alle Zentralen verfügen über einen RESET-Jumper auf der Leiterplatte, über den das System in die werksseitigen Standardeinstellungen zurückgesetzt werden kann (sofern der Parameter „Reset auf Werkseinstellungen“ aktiviert ist). Diese Vorgehensweise ist in Kapitel 12 Zurücksetzen der Zentrale beschrieben.

Auf der Leiterplatte der Zentrale befindet sich ein Flachstecker für den GSM-Kommunikator JA-19xY und ein 10-poliger Stecker für ein zusätzliches Modul.

Es ist außerdem ein 4-poliger Anschluss verfügbar:

- JA-103K – I-BUS – dient ausschließlich dafür, das Funkmodul JA-11xR zu verbinden, das sich im Gehäuse der Zentrale befindet. An diesen Anschluss kann kein anderes Gerät angeschlossen werden.
- JA-107K – ein dritter BUS mit den selben Parametern wie BUS 1 und 2. Sie können das Funkmodul JA-11xR anschließen oder das System um einen dritten BUS erweitern, indem Sie den Bus-Splitter JA-110Z-D anschließen.



Es gibt 3 Anschlüsse für einen speziellen Sabotagekontakt auf der Leiterplatte der Zentrale (einen Sabotagekontakt auf der Vorderseite, einen Sabotagekontakt auf der Rückseite und einen zusätzlichen Sabotagekontakt, um den Schutzgrad zu erhöhen. Neben jedem Stecker befindet sich ein Jumper. Bei Entfernen schaltet sich der Sabotagekontakt EIN. Wenn einer der Kontakte nicht benutzt wird, muss ein Jumper angeschlossen werden.

3.5. Verbindungsklemmen auf der Leiterplatte der Zentrale

Die Zentrale muss dauerhaft an den Netzstrom (230 V / 50 Hz or 110 V / 60 Hz) angeschlossen werden.

Der Netzstrom wird über Klemmen angeschlossen, die mit einer austauschbaren Sicherung ausgestattet sind. Die Zentrale ist ein Gerät der Schutzklasse 2 mit doppelter Isolation. Aus diesem Grund reicht ein 2-adriges Kabel (ein stromführendes Kabel und ein Neutralleiter). Das Erdungskabel (falls verwendet) soll an die FE-Klemme angeschlossen werden (für JA-107K müssen Sie die Abdeckkappe entfernen). Die interne Kommunikation zwischen der Zentrale und den angeschlossenen Geräten erfolgt über den BUS. Für die Zentrale JA-103K wird dies mit einer einzigen vierfarbigen Klemme (rot, gelb, grün und schwarz) umgesetzt, für die Zentrale JA-107K gibt es zwei dieser BUS-Klemmen.

Ein eingebauter USB-Anschluss befindet sich auf der Leiterplatte der Zentrale und ist mit einem USB-Anschluss im Gehäuse der Zentrale verbunden. Dadurch ist es möglich, eine Verbindung mit einem PC über das USB-Kabel herzustellen, ohne die Zentrale zu öffnen.

4. Vor der Installation des Systems



Wählen Sie einen versteckten Platz für die Zentrale (im überwachten Bereich), in dem die Stromversorgung gewährleistet ist. Wie empfohlen, den Raum mit der Zentrale über einen Melder mit sofortiger Reaktion zu schützen. Wenn die Zentrale mit einem GSM-Kommunikator ausgestattet ist, muss es einen guten Empfang des GSM-Signals an dem Ort geben (prüfen Sie dies mit einem Telefon). Vorsicht, wenn ein potentieller Einbrecher weiss, wo sich die Zentrale befindet, birgt dies ein Risiko, dass das System beschädigt wird, ohne dass Informationen über den Einbruch gesendet werden können.

Die Zentrale darf nur von einem Elektriker mit den erforderlichen Qualifikationen an den Netzstrom angeschlossen werden.

Die Stromversorgung der Zentrale hat eine doppelte Sicherheitstrennung der Stromkreise. Bei der Installation und dem Anschluss der BUS-Komponenten der Zentrale muss die gesamte Stromversorgung der Zentrale vollständig ausgeschaltet sein oder der BUS muss in F-Link ausgeschaltet sein.

Die Zentrale bietet die Möglichkeit, ein Netzteil von ~ 110 - 230 V / 50 - 60 Hz anzuschließen.

1. Berücksichtigen Sie zuerst die Anordnung und Zieleinstellung des Systems. Klären Sie die erforderliche Steuerungsmethode mit dem Kunden. Wir empfehlen, eine Projektdokumentation für ein komplexeres System zu erstellen.
2. Gehen Sie bei der Einrichtung der Geräte entsprechend der Handbücher, der allgemeinen Konstruktionsprinzipien der Brandmeldeanlagen und den Anweisungen des Herstellers während des Zertifizierungstrainings vor. Wenn etwas unklar sein sollte, rufen Sie Ihren lokalen Jablotron-Distributor an. **Der Hersteller lehnt jegliche Haftung für Schäden ab, wenn das System nicht ordnungsgemäß installiert oder eingerichtet wurde.**
3. Bereiten Sie die Stromversorgung der Zentrale vor - verwenden Sie ein geeignetes Kabel mit doppelter Isolierung und einem Querschnitt von 0,75 bis 1,5 mm². Wir empfehlen, einen Überspannungsschutz an der Zentrale, ebenso wie ein einziges Kabel mit einem Leistungsschalter (2 A-6 A) zu verwenden, der als Hauptschalter dient.

Warnhinweis: Schließen Sie keine anderen elektrischen Geräte an diesen spezifischen Stromkreis an, nicht einmal Strom für externe PG-Ausgänge oder ein Heizsystem oder ein anderes Gerät, das mit den Funktionen der Zentrale zu tun hat.

4. Befestigen Sie die Zentrale direkt an einer Wand oder einer anderen feuerfesten Oberfläche. Stellen Sie sicher, dass keine metallischen Objekte die Übertragung oder den Empfang der Funksignale beeinträchtigen können (Funkmodule und GSM-Kommunikatoren). Verwenden Sie die mitgelieferten Schablonen, um die Löcher für die Verbindungselemente vorzubereiten. Stecken Sie die Schrauben durch die oberen Löcher in das Kunststoffgehäuse, um einen Abstand von 1cm von der Wand einzuhalten und hängen Sie dann das Gehäuse der Zentrale daran. Stecken Sie auch eine zusätzliche Schraube durch die unteren Löcher und schrauben Sie sie fest, um die Position der Zentrale zu stabilisieren. Ziehen Sie alle Schrauben fest.

5. Installation der BUS-Geräte

Verbinden Sie nur Bus-Geräte der Serie JA-1xx JABLOTRON mit dem System. Gehen Sie folgendermaßen vor:

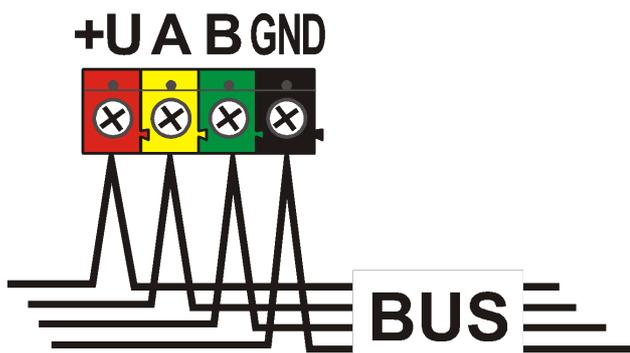
1. Während der Verbindung eines BUS-Moduls muss die Zentrale vollkommen vom Strom getrennt sein oder der BUS muss in F-Link ausgeschaltet sein.
2. Gehen Sie entsprechend der Installationsanleitungen der jeweiligen Geräte vor.
3. Das BUS-Kabel muss in einem durch das System geschützten Bereich installiert werden. Wenn sich das Kabel außerhalb des geschützten Bereichs befindet, muss dieser Teil mit einem BUS-Isolator JA-110T getrennt werden.
4. Verwenden Sie bei einer Leitungsverzweigung einen BUS-Splitter JA-110Z (und/oder JA-110Z-B, JA-110Z-C).
5. Achten Sie beim Anschluss der BUS-Geräte auf die Farben der Kabel (rot, gelb, grün, schwarz).

Geräte von Drittanbietern können über ein geeignetes Modul (wie z.B. JA-111H, JA-116H, JA-118M, JA-114HN) angeschlossen werden. Der Hersteller übernimmt weder Garantie für die korrekte Funktionsweise eines solchen Geräts noch für seine Sicherheitsstufe.

5.1. Der BUS des Systems JABLOTRON 100+

Der BUS des Systems JABLOTRON 100+ besteht aus 4 Kabeln (4-adrig). Der BUS eignet sich für das System JABLOTRON 100+ und kann nicht mit einem anderen System geteilt werden oder andere Geräte mit Strom versorgen.

Verwenden Sie zur Stromversorgung anderer Systeme über den BUS (Smart Home Automation) die Schnittstelle JA-121T oder den BUS-Isolator JA-110T.



Klemme	Farbe	Hinweis
+U	rot	positive Stromversorgungsklemme ; nur zur Stromversorgung von Geräten der Serie JABLOTRON 100+
A	gelb	Daten A
B	grün	Daten B
GND	GND	gemeinsame Klemme (negative Stromversorgungsklemme)

BUS-Klemmleiste

5.2. BUS-Kabel

Widerstand der Aderpaare (hin und zurück)		
CC-01	Widerstand des Aderpaares pro 1 m	0.0754 Ω
	Widerstand des Aderpaares pro 10 m	0.754 Ω
	Widerstand des Aderpaares 100 m	7.54 Ω
CC-02	Widerstand des Aderpaares pro 1 m	0.1932 Ω
	Widerstand des Aderpaares pro 10 m	1.932 Ω
	Widerstand des Aderpaares 100 m	19.32 Ω
CC-03	Widerstand des Aderpaares pro 1 m	0.0705 Ω
	Widerstand des Aderpaares pro 10 m	0.705 Ω
	Widerstand des Aderpaares 100 m	7.05 Ω
CC-11	Widerstand des Aderpaares pro 1 m	0.0754 Ω
	Widerstand des Aderpaares pro 10 m	0.754 Ω
	Widerstand des Aderpaares 100 m	7.54 Ω

Verbinden Sie die BUS-Geräte mit einem Kabel CC-01, CC-02 oder CC-11 von JABLOTRON.

Das Kabel CC-01 von JABLOTRON eignet sich für die Haupt-BUS-Leitung oder den Anschluss von Elementen mit einem höheren Verbrauch (Sirene) oder ferngesteuerten Elementen. Das Kabel hat 4 Adern (die Farben entsprechen den Farben des BUS). Die Stromkabel (schwarz und rot) haben im Vergleich zu den Kommunikationsleitungen (0,2 mm²) den größeren Aderquerschnitt (0,5mm²). Das Kabel wird in Packungen geliefert (1 Packung - 300 m).

Das Kabel CC-02 von JABLOTRON eignet sich für Abzweigungen von der Haupt-BUS-Leitung, den Anschluss von Elementen mit niedrigem Stromverbrauch (Melder) oder für kurze Entfernungen. Das Kabel hat 4 Adern (die Farben entsprechen den Farben des BUS). Alle Adern der Kabel CC-02 haben den gleichen Aderquerschnitt (0.2 mm²). Das Kabel wird in Packungen von 300 m geliefert.

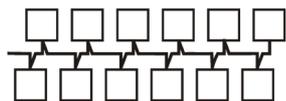
Das Kabel CC-03 von JABLOTRON eignet sich für die Haupt-BUS-Leitung oder die Verbindung von Elementen mit hohem Verbrauch (Sirene) oder ferngesteuerten Elementen. Das Kabel hat 8 Adern (8-adrig), die wie folgt aufgeteilt sind: Die Stromversorgungsleiter (rot und schwarz) haben einen größeren Querschnitt von 0,7 mm², die Kommunikationsdrähte (grün und gelb) für den Systembus und die Hilfsdrähte (braun und grau, weiß und blau) haben einen Querschnitt von 0,3 mm². Die Hilfsdrähte können als Schleifen von Magnetmeldern oder Sabotagekontakten verwendet werden. Das Kabel wird in Paketen pro 250 m geliefert.

Das Kabel CC-11 von JABLOTRON eignet sich für die Haupt-BUS-Leitung oder für den Anschluss von Elementen mit hohem Stromverbrauch (Sirenen) oder ferngesteuerten Elementen. Das Kabel hat eine orangefarbene Außenisolierung und 4 Adern (die Farben entsprechen den Farben des BUS). Die Stromkabel (schwarz und rot) haben im Vergleich zu den Kommunikationsleitungen (0,2 mm²) den größeren Aderquerschnitt (0,5mm²). Das Kabel wird in Packungen geliefert (1 Packung - 300 m) und verfügt über ein Brandschutzzertifikat.

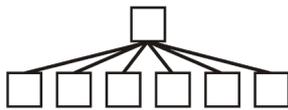
5.3. BUS-Layout

Bei der Verbindung einzelner Systemteile - Melder, Tastaturen, Sirenen, Ausgangsmodule usw. - können Sie das BUS-Kabel in die kürzest mögliche Richtung verlegen, unabhängig von den Systemteilen, zu denen die verwendeten Elemente gehören. Der BUS kann bei Bedarf verzweigt werden. Dabei ist eine lineare (Daisy-Chain), Stern- oder Baumstruktur (Daisy-Chain & Star) möglich. In der realen Installation ist eine Kombination dieser drei Optionen normalerweise die bequemste Wahl.

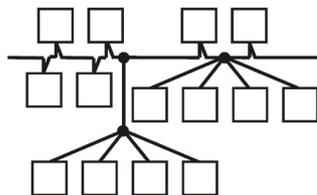
Beispiele und mögliche Verkabelungslayouts des Bus:



Daisy-Chain (lineare BUS-Struktur)



Stern-Struktur des Bus



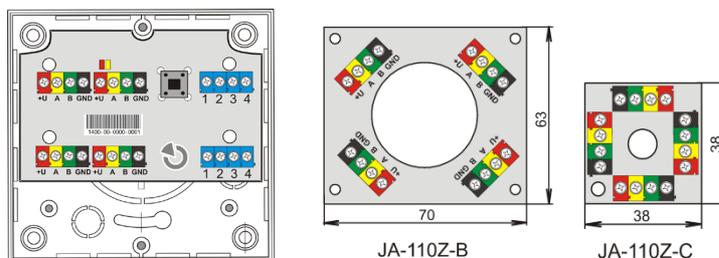
Daisy-Chain & Stern (Baumstruktur des BUS)

Das BUS-Kabel **darf nicht** so angeschlossen werden, dass eine **geschlossene Drahtschleufe** entsteht (die Enden der einzelnen Adern dürfen niemals miteinander verbunden sein und der gemeinsame GND-Draht darf auch nicht verbunden sein).

5.4. BUS-Verzweigung und -Aufteilung

Zum Verzweigen und Aufteilen des BUS können Sie bequem einen **BUS-Splitter JA-110Z** verwenden. Dieser wird in vier Varianten produziert: JA-110Z, JA110Z-B, JA110Z-C und JA110Z-D. Der JA-110Z wird in einer Installationsbox geliefert, die für die Installation auf einer Oberfläche vorgesehen ist und mit einem vorderen und hinteren Sabotagekontakt ausgestattet ist, um unerwünschte Manipulationen zu erkennen. Er besetzt eine Position im System. Alle Klemmen der gleichen Farbe sind auf der Splitter-Platine miteinander verbunden. Die Variante B ist mit ihren Abmessungen für den Einbau in die vielseitige Montagedose JA-190PL vorgesehen. Die Variante C ist mit ihren Abmessungen für den Einbau in eine Standard-Elektroinstallationsdose KU-68 vorgesehen.

Vernetzungsvarianten der Verteiler:



5.5. BUS-Länge und Anzahl der verbundenen Geräte

Die maximale BUS-Länge ohne Verstärkung (Trennung) beträgt 500m. Die Länge wird aus der Summe der Länge aller Kabel zwischen allen verbundenen Geräten errechnet. Zentralen des Typs JA-107K können bis zu 3 getrennte BUS-Adern aufweisen, d. h. die Gesamtlänge beider BUS-Leitungen kann 3x500 m betragen. Es wird empfohlen, die adressierbaren BUS-Geräte gleichmäßig zwischen beiden BUS-Leitungen zu verteilen, d. h. maximal 60 Geräte pro BUS.

Die Anzahl der BUS-Geräte wird mit der Kapazität der Backup-Batterie der Zentrale eingeschränkt. Um Sicherheitsklasse 2 zu entsprechen, muss das System im Falle eines Stromausfalls mit 230 V mindestens 12 Stunden zuverlässig über eine Backup-Stromquelle funktionieren können. Der Gesamtverbrauch aller BUS-Geräte darf also den maximalen Dauerstromverbrauch der Zentrale nicht überschreiten, siehe Kapitel 5.8 Berechnungsbeispiel des BUS-Stromverbrauchs zur Systemsicherung. Zur Berechnung des gesamten Dauerstromverbrauchs aller Elemente sind ihr **Backup-Verbrauch** zusammenzufassen (dies ist im Handbuch spezifiziert).

Ein weiterer begrenzender Parameter für die max. Länge eines BUS kann der Spannungsverlust entlang der Leitung sein (deutlich sichtbar durch die Systemdiagnose in F-Link).

5.6. Berechnung von Leitungsverlusten

Spannungsverluste entlang der Leitung hängen vom Leitungswiderstand ab, der sich aus dem verwendeten Leiter (Kabel) und dem verbrauchten Strom ergibt. Aktuelle Verbrauchswerte von Geräten finden Sie in einzelnen Handbüchern. Diese Werte können verwendet werden, um den Spannungsverlust zu berechnen und um herauszufinden, ob für das zuletzt installierte Gerät ausreichend Spannung verfügbar ist. Die Berechnung basiert auf dem Ohmschen Gesetz $U = I \cdot R$.

CC-01 Kabel (Strompaar)		CC-02 Kabel		CC-03 Kabel (Strompaar)		CC-11 Kabel (Strompaar)	
Geamtstrom	Max. Länge	Geamtstrom	Max. Länge	Geamtstrom	Max. Länge	Geamtstrom	Max. Länge
50 mA	400 m	25 mA	200 m	70 mA	400 m	50 mA	400 m
100 mA	300 m	50 mA	150 m	140 mA	300 m	100 mA	300 m
200 mA	150 m	100 mA	100 m	280 mA	150 m	200 mA	150 m
300 mA	100 m	200 mA	50 m	420 mA	100 m	300 mA	100 m
500 mA	50 m	300 mA	30 m	800 mA	50 m	500 mA	50 m

Die Daten in der Tabelle gehen vom ungünstigsten Fall aus, d. h. dass der Gesamtverbrauch am Ende des Kabels liegt.

Im normalen Betriebszustand beträgt die Spannung der Klemmen + U und GND fast 14 V. Bei der Berechnung ist zu berücksichtigen, dass die Zentrale nur von der Batterie gespeist wird und die Spannung etwa 12 V beträgt. Eine höhere Spannung als die zulässige Minimalspannung von 10 V muss für alle Geräte zur Verfügung stehen. Für eine einwandfreie Funktion der angeschlossenen Geräte beträgt der **maximal zulässige Spannungsverlust 2,0 V**.

Unerwarteter Spannungsverlust kann durch schlecht kontaktierte Klemmen (Übergangswiderstände) verursacht werden.

Die Spannungsverluste einzelner Geräte können annähernd über F-Link in der Diagnosekarte für die adressierbaren Geräte überprüft werden. Nicht adressierbare Geräte (z. B. Ausgangsmodule) bieten diese Möglichkeit nicht; Sie müssen mit einem Messgerät überprüft werden.

In einer realen Installation empfehlen wir immer, die Berechnung und Verbindung mit einer Messung der Klemmen zu überprüfen. Führen Sie diese Messung bei Geräten mit hohem Stromverbrauch (Sirene, Tastatur, Relaisausgang) während erhöhter Verbrauchszeiten durch (aktive Sirene, beleuchtete Tastatur, eingelegtes Relais).

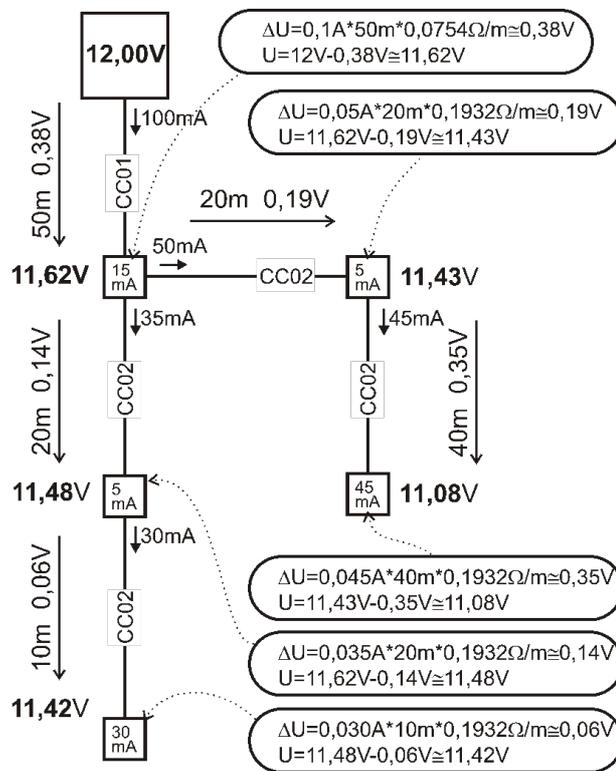
Die in der Tabelle angegebenen Einschränkungen sind allgemein gültig.

Berechnen Sie bei der Kalkulation der Gesamtbelastung der Kabel den **Verbrauch zur Kabelauswahl** (zu finden in den Handbüchern der Geräte).

5.7. Beispiel für eine Berechnung des Spannungsverlustes

1. Ermitteln Sie die Werte für den Stromverbrauch der einzelnen Geräte (in den technischen Parametern der Produkte - Stromverbrauch zur Kabelauswahl).
2. Informieren Sie sich über die Kabellängen. Sie müssen die Kabellänge von Verzweigungspunkt zu Verzweigungspunkt möglichst genau kennen.
3. Zeichnen Sie einen Plan mit Kabellängen und Verbrauch einzelner Adern.
4. Berechnen Sie den elektrischen Strom, der durch die einzelnen Adern fließt.
5. Verwenden Sie die angenommene Leitungslänge und die geschätzten Stromwerte der einzelnen Adern gemäß der obigen Tabelle, um die Eignung der Kabelauswahl zu vergleichen.

Ziehen Sie individuelle Verluste von der Versorgungsspannung ab, um die Spannung am Leitungsende zu bestimmen. Berücksichtigen Sie immer die Spannung von 12 V von der Zentrale beim Betrieb während eines Stromausfalls.



5.8. Berechnungsbeispiel des BUS-Stromverbrauchs zur Systemsicherung

Die Tabelle zeigt das Beispiel eines kleinen Systems. Der Ruhestromverbrauch im Backup-Modus beträgt 78 mA. So können Sie die Zentrale JA-103K mit einem GSM-Wähl- & Übertragungsgerät und einem ausgeschalteten LAN- Übertragungsgerät verwenden, der eine maximale Dauerbelastung von 80 mA ermöglicht.

Gerät	Beschreibung	Anzahl	Verbrauch im Backup-Modus
JA-11xR	Modul zur Funkkommunikation	1	25 mA
JA-114E	Zentrale 15 mA + 3x 1 mA Bereiche	1	18 mA
JA-110M	Modul für Magnetsensor 5 mA	1	5 mA
JA-110P	PIR-Bewegungsmelder 5 mA	2	10 mA
JA-110ST	Feuermelder 5 mA	2	10 mA
JA-110A	Interne Sirene 5 mA	1	5 mA
JA-111A	Externe Backup-Sirene 5 mA	1	5 mA
Insgesamt			78 mA

Die Zentrale JA-103K eignet sich besser für drahtlose Systeme, bei denen Geräte mit Batterien betrieben werden. Vergessen Sie bei der Planung der Konfiguration einer Funkzentrale nicht, die Funkmodule im Verbrauch zu berücksichtigen.

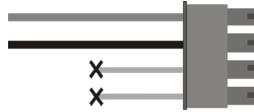
Für größere BUS-Systeme verwenden sie die Zentrale JA-107K.

5.9. Anforderungen an die Stromversorgung

Die Zentrale muss permanent über ein geschütztes AC-Stromnetz im Bereich von 110 - 230 V versorgt werden, siehe Technische Spezifikationen. Die Zentrale ist ein Gerät mit doppelter Isolierung, daher wird die Verbindung normalerweise mit einem Kabel mit doppelter Isolierung und einem Querschnitt von 0,75 bis 1,5 mm² umgesetzt. Die Zentrale hat eine schützende kleine Glassicherung. Diese ist ein Teil der

Netzanschlussklemmen. JA-103K kann nicht mit alternativen Quellen betrieben werden, z. B. mit Hochleistungsakkus, die mit einem Solar-Panel geladen werden usw..

JA-107K kann mit alternativen Quellen betrieben werden. Die Netzspannung für die Zentrale muss in einem Bereich von 10 - 15 V liegen; Es muss eine Backup-Stromquelle zur Verfügung stehen. Verbinden Sie die externe Stromquelle mit dem Netzanschluss. Verwenden Sie die roten und schwarzen Kabel, um das Netzteil der externen Stromquelle zu verbinden. Schneiden und isolieren Sie die weißen Kommunikationskabel. Der Hersteller haftet nicht für Schäden, die bei Verwendung einer alternativen Stromquelle entstehen.



5.10. Anforderungen der Backup-Stromquelle

Ein Sicherheitssystem, das der Sicherheitsklasse 2 entsprechen muss, muss während einer Unterbrechung der Stromversorgung 12 Stunden lang über eine Backup-Batterie betrieben werden und muss 72 Stunden nach der Wiederherstellung der Stromversorgung vollständig geladen und bereit sein, das System wieder hochzufahren. Um diese Anforderung zu erfüllen, darf der maximale Stromverbrauch des BUS nicht überschritten werden.

Beispiel für den maximalen Dauerstrom des System-BUS entsprechend der Kapazität der Backup-Batterie:

	JA-103K 2.6 Ah Batterie		JA-107K 18 Ah Batterie	
Maximaler Dauerstromverbrauch vom BUS	BUS 1 – 1000 mA I-BUS – 200 mA		2000 mA dauerhaft 3000 mA für 60 Min. (max. 2000 mA für einen BUS)	
Maximaler Dauerstromverbrauch bei einer Backup-Stromversorgung von 12 Std.	Ohne GSM-Wähl- & Übertragungsgerät	LAN – AUS - 115mA LAN – EIN - 88 mA	Ohne GSM-Wähl- & Übertragungsgerät	LAN – AUS - 1135mA LAN – EIN - 1107 mA
	Mit GSM-Wähl- & Übertragungsgerät	LAN – AUS - 80mA LAN – EIN - 53 mA	Mit GSM-Wähl- & Übertragungsgerät	LAN – AUS - 1100mA LAN – EIN - 1072 mA

Der Strom, der von jeder BUS-Ausgangsklemme gezogen wird, wird in F-Link in der Registerkarte Diagnose in Zeile 0 angezeigt, wo sich die Zentrale befindet. Für die Zentrale JA-107K ist es erforderlich, die Werte aller BUS-Ausgänge zu summieren. Dieser Strom wird mit dem in der obigen Tabelle angegebenen Strom verglichen. Auf diese Weise können Sie überprüfen, ob die Kapazität der Backup-Batterie den Anforderungen der Backup-Zeit des Systems entspricht. Wenn der gemessene Strom höher als in der Tabelle angegeben ist, ist es notwendig, die Systemstromversorgung zu gewährleisten, indem man z.B. die Verstärker-Einheit JA-120Z hinzufügt.

Diagnosics	Calendars	Communication
Battery status/voltage	Voltage/ loss	
13.7 V/13.1 V	13.7 V/23 mA; 13.6 V/25 mA	

5.11. BUS-Isolation

Teile des BUS, die durch ungeschützte Bereiche geführt werden, müssen vor einem möglichen Kurzschluss oder anderen Deaktivierungsversuchen des Systems geschützt werden. Dies erfolgt unter Verwendung eines BUS-Isolators JA110T. Dieses Modul kann in eine Mehrzweck-Installationsbox JA-190PL eingebaut werden. Der Isolator verbessert auch die Signalqualität des BUS. Er ist mit dem BUS verbunden und wird von ihm versorgt, er nimmt keine Position im System ein und ermöglicht es, die maximale BUS-Länge auf weitere 500 m zu verlängern. Vermeiden Sie die Verwendung von 2 oder mehr BUS-Isolatoren an einem BUS-Strang - Geräte können nicht durch 2 oder mehr von ihnen kommunizieren.

Ein Anwendungsbeispiel kann die Weiterleitung des BUS an Relaismodule sein, die beispielsweise Jalousien oder eine Sirene steuern, zu denen der BUS so geführt wird, dass er möglicherweise von außen angegriffen oder deaktiviert werden kann. Weitere Informationen finden Sie im Handbuch JA-110T.

BUS von der
Zentrale



Mögliche BUS-Schäden hinter dem
Modul, z. B. durch Kurzschluss,
haben keinen Einfluss auf den BUS
vor dem Modul!

5.12. Nutzung bestehender Verkabelung in Sanierungsprojekten

- Bei der Installation neuer Leitungen sollten Sie vorzugsweise die Kabel CC-01, CC-02, CC-03 and CC11 verwenden.
- Beim Anschluss an Kabel des Typs SYKFY 3x2x0.5 müssen die Datenkabel des BUS (A, B) mit einer ausgewählten verdrehten Doppelleitung verbunden werden. Für die Stromversorgung (+ U12, GND) können Sie die entsprechenden Drähte in den verbleibenden zwei Paaren zusammenschließen (Verdoppelung innerhalb eines Paares).
- Bei einem Anschluss an UTP-Kabel müssen die Datenkabel des BUS (A, B) mit einer ausgewählten verdrehten Doppelleitung verbunden werden. Für die Stromversorgung (+ U, GND) ist es zweckmäßig, die jeweiligen Adern der übrigen Aderpaare miteinander zu verbinden (doppelt).

Wenn ein abgeschirmtes Kabel verwendet wird, schließen Sie die Abschirmung nicht an die BUS-Klemmen an! Wir empfehlen, alle Abschirmungen (Verzinnung) in der Zentrale mit einer Hilfsklemme zu verbinden und diese Verbindung nirgendwo anders zu verbinden. Lassen Sie auch das andere Ende der Abschirmung auf der Geräteseite unverbunden.

6. Verwendung drahtloser Geräte

Im System JABLOTRON 100+ können Sie drahtlose Geräte der Serien JA-15x, JA-16x und JA-18x verwenden. Das Funkmodul JA-11xR- muss für eine Kommunikation mit den drahtlosen Geräten verwendet werden. Es können bis zu 3 Funkmodule im System vorhanden sein.

Wenn Sie die einzelnen Geräte installieren, gehen Sie entsprechend der Handbücher vor.

Vorsicht: Es können bis zu 120 drahtlose Geräte bei der Zentrale JA-107K angemeldet werden, sie können nur an den Positionen 1 bis 120 angemeldet werden. Die Positionen 121 bis 230 sind nur für BUS-Geräte. Wenn das Funkmodul JA-11xR nach dem BUS-Verstärker JA-120Z installiert wird, muss es an einer Position innerhalb des Positionsbereichs 1 - 120 angemeldet werden.

6.1. Installation eines Funkmoduls JA-111R

1. Das Funkmodul JA-11xR kann sich in einer Halterung in einer unteren rechten Ecke der Zentrale befinden.
2. Wenn die Zentrale JA-103/107K an einem Platz mit schlechtem GSM-Empfang installiert wird, erhöht das GSM-Modul seine Übertragungsleistung, was die Kommunikationsreichweite des Funkmoduls im System beeinträchtigen kann. In solch einem Fall empfehlen wir, das Funkmodul außerhalb der Zentrale zu platzieren, genau gesagt in einer Entfernung von mindestens 2 m, wo die Zentrale nicht mehr beeinträchtigt werden kann und ein qualitativ besserer Funkempfang von Geräten ermöglicht wird. Auf diese Weise wird die Reichweite erhöht und die Übertragung über größere Distanzen möglich.

Hinweis: JA-111R muss außerhalb der Zentrale in einer Installationsbox PLV-111R platziert werden (separater Verkauf).



Der Anschluss des Funkmoduls an der Leiterplatte der Zentrale JA-103K ist ausschließlich für ein Funkmodul im Gehäuse der Zentrale vorgesehen.

3. Sie können größere Bereiche mit einem Funksignal abdecken, wenn Sie bis zu 3 Funkmodule des Typs JA-11xR in ihrem eigenen Kunststoffgehäuse an verschiedenen Plätzen installieren (z.B. jedes in einer anderen Etage). Die Zentrale kommuniziert in einem bestimmten Zyklus mit den einzelnen Funkmodulen, sodass sie die von einem Gerät gesendeten Informationen von dem Funkmodul empfängt, das als erstes ein intaktes Signal empfängt und darauf reagiert. Sie wird dann nicht die selbe Information von den anderen Funkmodulen empfangen, auch wenn sie diese über ein stärkeres Signal empfängt. Bei bidirektionalen Geräten „reserviert“ die Zentrale den einmal verwendeten Kanal (Kommunikation mit dem ersten Funkmodul) und kommuniziert mit dem jeweiligen Gerät über dieses Funkmodul (nur in der

Diagnose, der Spalte des Kanals) bis das Gerät nicht mehr reagiert. Dann sucht sie das Verbindungssignal der anderen Funkmodule. Wenn Sie die Verbindungsqualität einzelner Geräte mit einzelnen Funkmodulen überprüfen möchten, nutzen Sie dafür die RF-Signalmessung in F-Link (Schaltfläche auf der oberen Symbolleiste). Wählen Sie dort die aktiven Geräte aus, ebenso wie das Funkmodul, für das Sie die Kommunikation überprüfen möchten. Eine Grafik der Funkkommunikation zeigt die RF-Signalstärke an, die von einem spezifischen Funkmodul gemessen wurde. Sie können auch unterschiedliche RF-Signalfenster geöffnet haben, sodass Sie ganz einfach die RF-Deckung in dem Gebäude überwachen können.

4. Installieren Sie ein Funkmodul vertikal an einer Wand. Es darf sich nicht in der Nähe von Gegenständen befinden, die die Kommunikation abschirmen oder stören (Metalle, elektronische Geräte, Kabel, Rohrleitungen usw.).
5. Nach dem Einschalten des Systems müssen Sie die **Funkmodule zuerst anmelden**. Erst dann können Sie die drahtlosen Geräte anmelden.

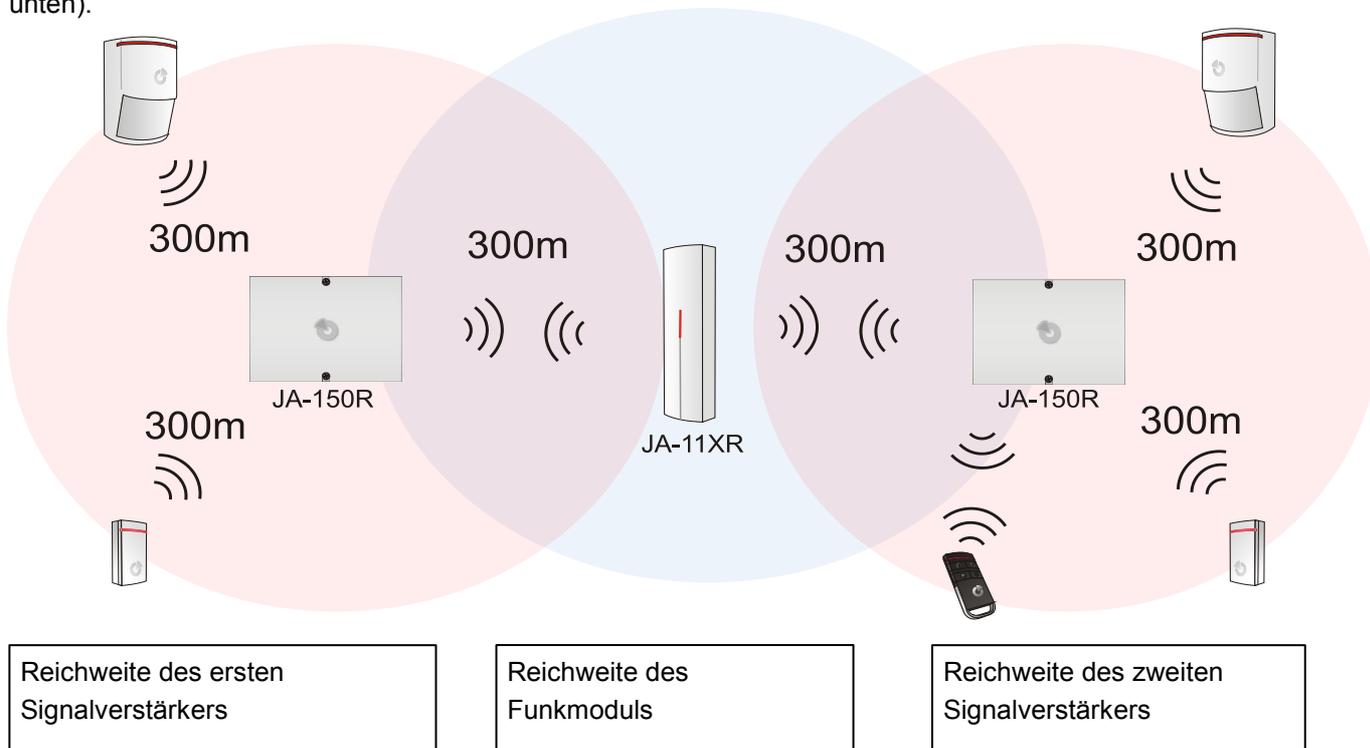
Empfehlung: Es wird empfohlen, die drahtlosen Geräte erst dann beim System anzumelden, wenn sie sich in ihrer endgültigen Position im Gebäude befinden. Diese Installationsvorgehensweise ist zwar nicht sehr bequem, hilft aber, einen besseren und zuverlässigeren Funkempfang beim Funkmodul zu erzielen, wenn das System in Betrieb genommen wird. Das Funkmodul hat einen Mechanismus zum Messen des RF-Signals im Errichtermodus implementiert. Dieser Mechanismus bietet eine Sicherheitsspanne im Falle einer Verschlechterung der Funkübertragungsbedingungen, wenn das System in vollem Betrieb ist. Weitere Informationen finden Sie in der Norm EN 50131-5-3.

6.2. Installation drahtloser Geräte – Anmelde-Modus

Drahtlose Geräte müssen beim System z.B. durch einen Produktionscode angemeldet werden. Das Anmeldeverfahren kann nur mit einem PC und der installierten Software F-Link durchgeführt werden. Siehe dazu Kapitel 8.4.1 Geräte anmelden und löschen.

6.3. Erweitern der Reichweite von drahtlosen Geräten

Wenn der Standardbereich des Funkmoduls nicht ausreicht oder es nicht möglich ist, den Abstand zwischen dem Funkmodul und den drahtlosen Geräten zu verkürzen, können Sie die Signale der drahtlosen Geräte (Melder, Fernbedienungen, PG-Modul) mit dem Funk-Signalverstärker JA-150R erweitern. Er benötigt für seine Installation nur eine dauerhafte Stromversorgung. Der Standort des Signalverstärkers JA-150R wird so gewählt, dass sowohl die Zentrale (Funkmodule) als auch die drahtlosen Geräte in Reichweite sind (siehe Abbildung unten).



7. EINschalten des Systems

1. Prüfen Sie die Verbindung der BUS-Kabel.
2. Prüfen Sie, ob sich eine microSD-Karte in der Halterung an der Zentrale befindet.
3. Prüfen Sie, ob das Netzkabel sachgemäß mit der Zentrale verbunden ist und dass das Kabel korrekt angebracht ist.
4. Legen Sie eine Batterie in die Zentrale ein und befestigen Sie sie im Gehäuse.
Vorsicht - die Backup-Batterie wird im geladenen Zustand geliefert, sie darf nicht kurzgeschlossen werden!
5. Schließen Sie die Batterieleitungen an. Achten Sie auf die korrekte Polung (rot +, schwarz -).
6. Schalten Sie den Strom ein und überprüfen Sie die LED-Anzeigen an der Zentrale:
 - a. die grüne LED beginnt zu blinken (BUS-Funktion)
 - b. die rote LED blinkt – einloggen ins GSM-Netzwerk mit Hilfe des zusätzlichen GSM-Wähl- & Übertragungsgerätes
 - c. die rote GSM-LED erlischt – der GSM-Kommunikator ist im GSM-Netzwerk eingeloggt
 - d. die rote LED leuchtet dauerhaft – die Zentrale ist nicht im GSM-Netzwerk eingeloggt
(die Punkte b, c, d gelten nur für einen installierten GSM-Kommunikator)
7. Wenn die verbundenen BUS-Geräte gelb zu blinken beginnen, ordnen Sie sie dem System zu, siehe auch Kapitel 8.4.1 Geräte anmelden und löschen.
8. Führen Sie die Konfiguration auf den Tastaturen durch, siehe auch 10.5.1 Konfiguration der Tastatur.
9. Stellen Sie die gewünschten Funktionen ein und testen Sie das System, siehe Kapitel 10.9 Registerkarte Systemparameter
10. Um die Normen EN50131-1 oder INCERT, Klasse 2, zu erfüllen, trennen Sie das verlängerte USB-Kabel von der Platine der Zentrale.

8. Konfiguration des Systems

Das Sicherheitssystem (das überwachte Gebäude) kann in unabhängige Teile, sogenannte Bereiche, aufgeteilt werden. Jeder Bereich kann komplett oder teilweise überwacht werden. Dies wird Teilscharfschaltung genannt. Melder mit dem aktivierten Parameter „Teilscharf“ unterstützen nicht diesen Modus.

Der grundlegende Teil ist der **Perimeterschutz**. Er überwacht die Eingangstüren, Garagentüren, Fenster, Balkontüren sowie Hinter- und Dacheingänge. Unter den dem Perimeterschutz zugeordneten Geräten befinden sich Magnetmelder, Glasbruchmelder, Erschütterungs- und Neigungsmelder sowie Infrarotbarrieren. Das einzige Spezifische ist, dass Eingangstüren oder Garagentore in der Regel eine verzögerte Reaktion haben und die anderen Bereiche so definiert werden, dass sie sofort reagieren.

Der nächste Teil betrifft die **Bewegungsmelder**. Dabei werden Bewegungen in überwachten Gebäuden über einen Bewegungsmelder (PIR) verfolgt. Diese werden auch mit anderen Meldern kombiniert. Melder, die im Eingangsbereich eines Gebäudes platziert werden, haben in der Regel eine voreingestellte Verzögerungsreaktion. Die anderen Melder sind in den meisten Fällen so voreingestellt, dass sie sofort reagieren. Sie können für den Eingangsweg bis zu 3 Timer auswählen (z.B. eine längere Verzögerung beim Eingang durch eine Garage).

Der **Gebäudeschutz** dient dazu, Safes und Wertgegenstände zu überwachen sowie einen gewaltsamen Einbruch zu melden. Garagentüren können bei jeder Öffnung beschädigt werden. Erschütterungs- und Neigungsmelder gehören zur Gebäudeüberwachung, ebenso wie der normale Magnetmelder zur Meldung von Türöffnungen - dieser ist typischerweise ein verzögerter Sensor.

Die Überwachung einzelner Sicherheitskomponenten wird durch Sabotagekontakte erreicht, die eine nicht berechnete Bedienung eines Geräts anzeigen.

Die Umgebungsüberwachung schließt Feuermelder, Melder zur Erkennung von brennbaren und giftigen Gasen und Überschwemmungsmelder ein. Alle genannten Melder haben eine einstellbare und dauerhaft vom Systemstatus unabhängige Reaktion, also eine 24-Stunden-Reaktion.

8.1. Die Systemprofile

Die Auswahl der Systemprofile erlaubt Ihnen, die folgenden Systemparameter global voreinzustellen, um der vorgegebenen Norm und Sicherheitsklasse zu entsprechen. Diese Optionen können gesperrt werden, wenn ein spezifisches Profil geändert werden muss.

Vorsicht: Das Einstellen einzelner Parameter durch die Auswahl eines Systemprofils garantiert nicht die Einhaltung der Sicherheitsklasse 2. Nur die korrekte Systemeinrichtung (unter Verwendung der richtigen

Geräte), die sachgemäße Installation entsprechend der Anforderungen der Norm CLC/TS 50131-7 und die Durchführung einer Leitstellenüberwachung stellen sicher, dass Sicherheitsklasse 2 eingehalten wird.

Überblick über die Systemparameter, wenn das Systemprofil „Standard“ eingestellt wird (Standardeinstellungen):

Durch die Einstellung des „Standard“-Systemprofils werden alle genannten Parameter auf die Werkseinstellungen zurückgesetzt und alle Parameter können geändert werden. Das Alarmsystem erfüllt dann nicht die Anforderungen der Sicherheitsklasse 2 und verletzt auch die Anforderungen der Versicherungsgesellschaft oder der örtlichen Vorschriften. Im Schadensfall muss die Versicherungsgesellschaft wegen des fehlerhaft programmierten Systems, das durch das Installationsunternehmen verursacht wird, nicht bezahlen.

Gerät	Parameter	Option	Blockiert (Einschränkung)
Zentrale	Codes mit Präfix	NEIN	NEIN
Zentrale	125-kHz Informationsträger (IMT) aktivieren	JA	NEIN
Zentrale	Codelänge	4	NEIN
Zentrale	Zeitabgleich zwischen PC und Zentrale	JA	NEIN
Zentrale	Sirene, wenn teilscharf (IW)	NEIN	NEIN
Zentrale	Sirenen aktivieren	JA	NEIN
Zentrale	Warnung vor „Werkseitigen Codes“	JA	NEIN
Zentrale	Admin schränkt Errichter/AES-Rechte ein	NEIN	NEIN
Zentrale	Errichter oder AES betätigt das System	JA	NEIN
Zentrale	Testbetrieb	NEIN	NEIN
Zentrale	Hinweis - Jahreswartung	NEIN	NEIN
Zentrale	Wartungsmodus erlauben	JA	NEIN
Zentrale	Überfallalarm (Geiselnahmealarm)	JA	NEIN
Zentrale	2-Melderabhängigkeit in einem Bereich	NEIN	NEIN
Zentrale	Interne Sirene bei Sabotagealarms	NEIN	NEIN
Zentrale	Rücksetzen von Sabotage Errichter	NEIN	NEIN
Zentrale	Reset auf Werkseinstellung	JA	NEIN
Zentrale	Tägliches zurücksetzen des Autobypasses	JA	NEIN
Zentrale	Bypass bei Scharfschaltung	NEIN	NEIN
Zentrale	Autorisierung hebt Alarm nicht auf	NEIN	NEIN
Zentrale	Nicht erfolgreiches Scharfschalten	NEIN	NEIN
Zentrale	Gerätefehler-Autobypass	JA	JA
Zentrale	Um 15s verzögerte Benachrichtigung an eine Notrufleitstelle	NEIN	NEIN
Zentrale	Art der Scharfschaltungs	Einstellung mit Warnhinweis	NEIN

Zentrale	Autorisierungstyp	Standard	NEIN
Zentrale	Systemsperre nach einem Alarm	NEIN	NEIN
Zentrale	Verbindungsverlust einer BUS-Komponente	Fehler	NEIN
Zentrale	Komponenten-Autobypass	dritte Aktivierung	JA
Zentrale	Alarmdauer	260 Sek.	90...1200 Sek.
Zentrale	Eingangsverzögerungszeit	30 Sek.	5...120 Sek.
Zentrale	Ausgangsverzögerungszeit	30 Sek.	5..120 Sek.
Funkmodul	Erkennung einer RF-Störung	Deaktiviert	NEIN
Tastatur	Einstellung der optischen Anzeige	1.Dauerhaft (BUS) oder 4.Änderung des Bereichsstatus (RF)	NEIN
Tastatur	Unschärf anzeigen	JA	NEIN
Tastatur	Scharf anzeigen	JA	NEIN
Tastatur	Akustische Alarmanzeige	JA	NEIN
Tastatur	Akustische Anzeige der Eingangsverzögerung	JA	NEIN
Tastatur	Akustische Anzeige der Ausgangsverzögerung	JA	NEIN

Übersicht der Systemparameter, wenn „EN50131-1, Klasse 2“ oder „INCERT“ eingestellt ist:

Gerät	Parameter	Option	Sperren (Einschränkung)
Zentrale	Codes mit einem Präfix	JA	JA
Zentrale	125-kHz Informationsträger (IMT) aktivieren	JA	NEIN
Zentrale	Codelänge	4 (INCERT 6)	NEIN, (INCERT JA)
Zentrale	Zeitabgleich zwischen PC und Zentrale	JA	NEIN
Zentrale	Sirene, wenn teilscharf (IW)	NEIN	NEIN
Zentrale	Sirenen aktivieren	JA	JA
Zentrale	Warnung vor „Werkseitigen Codes“	JA	JA
Zentrale	Admin schränkt Errichter/AES-Rechte ein	JA	JA
Zentrale	Errichter oder AES betätigt das System	NEIN	JA
Zentrale	Testbetrieb	NEIN	NEIN
Zentrale	Hinweis - Jahreswartung		
Zentrale	Wartungsmodus erlauben	NEIN	JA
Zentrale	Überfallalarm (Geiselnahmealarm)	JA	NEIN
Zentrale	2-Melderabhängigkeit in einem Bereich	NEIN	NEIN

Zentrale	Interne Sirene bei Sabotagealarms	JA	JA
Zentrale	Rücksetzen von Sabotage Errichter	JA	JA
Zentrale	Reset auf Werkseinstellung	NEIN	JA
Zentrale	Tägliches zurücksetzen des Autobypasses	NEIN	JA
Zentrale	Bypass bei Scharfschaltung	JA	JA
Zentrale	Autorisierung hebt Alarm nicht auf	JA	JA
Zentrale	Nicht erfolgreiches Scharfschalten	JA	JA
Zentrale	Gerätefehler-Autobypass	NEIN	NEIN
Zentrale	Um 15s verzögerte Benachrichtigung an eine Notrufleitstelle	JA	NEIN
Zentrale	Art der Scharfschaltungs	Je nach Systemprofil	JA
Zentrale	Autorisierungstyp	Standard	NEIN
Zentrale	Systemsperr nach einem Alarm	NEIN	NEIN
Zentrale	Verbindungsverlust einer BUS-Komponente	immer Sabotage	NEIN
Zentrale	Komponenten-Autobypass	dritte Aktivierung	NEIN
Zentrale	Alarmdauer	260	90...900 Sek.
Zentrale	Eingangsverzögerungszeit	30	5...30 Sek.
Zentrale	Ausgangsverzögerungszeit	30	5..60 Sek.
Funkmodul	Erkennung einer RF-Störung	NIEDRIG	NEIN
Tastatur	Einstellung der optischen Anzeige	2.Bereichsstatus änderung (BUS) oder 4.Bereichsstatus änderung (RF)	JA
Tastatur	Unschärf anzeigen	NEIN	NEIN
Tastatur	Scharf anzeigen	NEIN	NEIN
Tastatur	Akustische Alarmanzeige	JA	JA
Tastatur	Akustische Anzeige der Eingangsverzögerung	JA	JA
Tastatur	Akustische Anzeige der Ausgangsverzögerung	JA	JA
Fernbedienungen	Einschränkung der Steuerungsfunktionen	NEIN	JA
Kalender	Einschränkung der Steuerungsfunktionen	NEIN	JA

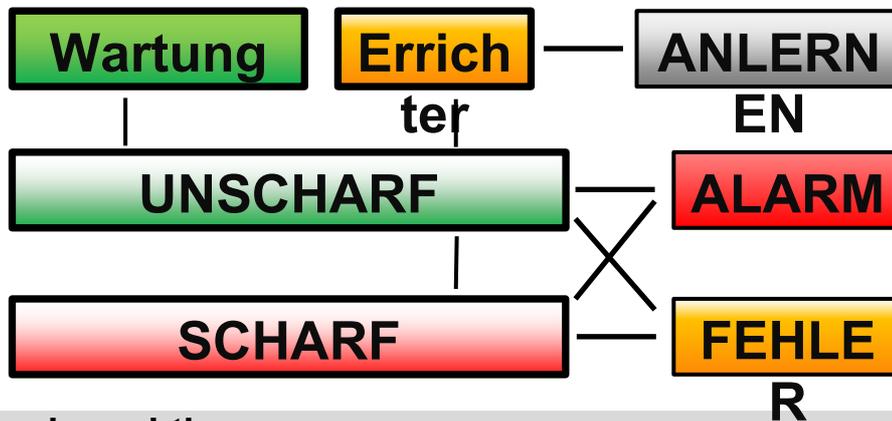
Globaler Überblick über Gründe, die die Scharfschaltung entsprechend des voreingestellten Systemprofils verhindern:

Ereignis \ Profil	Standard		EN50131-1, Klasse 2		INCERT, Klasse 2	
	Passabel	Nicht passabel	Passabel	Nicht passabel	Passabel	Nicht passabel
Sabotage aktiv	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Aktiver Eingang (jeder Eingang)					<input checked="" type="checkbox"/>	
Aktiver sofortiger Eingang	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Aktive Alarmspeicheranzeige			<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
RF-Gerät 20 Min. ohne Antwort			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Sirenenfehler				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Fehler	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Geräteverlust	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Gesperrte Melder						
Schwache Gerätebatterie	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Schwache Batterie in der Zentrale	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Batteriefehler in der Zentrale	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
AC-Fehler			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
AC-Fehler für 30 Minuten	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
System in Konfiguration				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
GSM-Fehler	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
LAN-Fehler	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
PSTN-Fehler	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
AES-Fehler				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>

8.2. Betriebsmodi der Zentrale

Das Sicherheitssystem verfügt über einige Betriebsarten. Das Umschalten zwischen den Modi hängt von den Berechtigungsstufen der Benutzer ab.

Mode	Beschreibung
Errichtermodus	Ein Modus, bei dem kein Alarm ausgelöst werden kann. Er ist nur für einen Errichter oder einen AES-Techniker bestimmt und dient dazu, neue Geräte anzumelden und das System zu konfigurieren. In diesem Modus ist keine Steuerung verfügbar (weder lokal noch ferngesteuert). Die Segmente auf den Tastaturen sind ausgeschaltet. Der Modus wird durch das gelbe Blinken der hintergrundbeleuchteten Taste gekennzeichnet (2x alle zwei Minuten blinken). Signale der Fernbedienungen oder anderen Geräten werden ignoriert. Das Eingeben oder Verlassen des Errichter-Modus wird von einer LCD-Tastatur oder über der auf einem PC installierten Software F-Link vorgenommen. Wenn ein PC online verbunden ist, kann der Errichter-Modus von der Tastatur aus nicht eingegeben oder verlassen werden.
Wartungsmodus	Ein Modus, der hauptsächlich für den Administrator gedacht ist. Er ermöglicht eine Wartung in dem Bereich (den Bereichen) entsprechend den Zugriffsrechten des Administrators (z. B. Batteriewechsel in Meldern). Der Administrator kann das System über die Tastatur oder J-Link in den Wartungsmodus setzen. Der Wartungsmodus in einem Bereich hat keinen Einfluss auf den Status und die Funktionalität anderer Bereiche oder den Status der programmierbaren PG-Ausgänge. Der Wartungsmodus wird durch das grüne Blinken der Taste mit Hintergrundbeleuchtung (2x blinkt alle 2 Sekunden) angezeigt, wobei sich die Bereichstasten (Segmenttasten) des jeweiligen Bereichs ausschalten. Das Aufrufen oder Verlassen des Wartungsmodus kann über eine LCD-Tastatur, einen PC oder F-Link (J-Link) erfolgen.
Unscharf	Ein normaler Modus, in dem Einbruchsmelder nicht überwachen. Es kann sich frei durch das Gebäude bewegt werden, das Öffnen von Fenstern und Türen ist erlaubt. Rauch-/Temperatur, Gas- oder Überschwemmungsmelder oder Paniktasten können einen Alarm jederzeit auslösen. Auch die Sabotagekontakte aller Geräte sind immer aktiv. Wenn sie ausgelöst werden, löst das System einen Sabotagealarm aus. Der Unscharf-Modus wird auf der Tastatur mit einem grünen Licht in dem spezifischen Bereich (Segment) angezeigt.
Scharf (vollständig oder teilweise)	Alle Melder sind aktiv (außer der internen Melder, wenn sie teilweise scharf geschaltet sind) und wenn sie aktiviert werden, wird ein Alarm ausgelöst (nächster Punkt). Der Scharf-Modus wird auf der Tastatur durch ein rotes Licht (gelbes Licht bei teilweise Scharfschaltung) auf einem spezifischen Bereich (Segment) angezeigt.
Alarm	Ein Alarm ist ein Status, bei dem die IW- und EW-Ausgänge für eine voreingestellte Zeit (Alarmlänge) aktiviert sind und die externen und internen Sirenen ertönen. Der Alarmstatus wird auf der Tastatur durch eine schnell blinkende rote beleuchtete Taste angezeigt. Für die Beschreibung der Unterschiede des Verhaltens von EW und IW-Ausgängen, siehe Kapitel 8.5 Alarmarten.
Fehler	Der Fehler ist ein Warnsignal des Systems, das auf einen abnormalen Zustand der Zentrale, der Kommunikatoren oder Geräte und deren Stromversorgungsprobleme (Netzstrom oder Batterie) oder auf Kommunikationsprobleme hinweist.



8.3. Benutzerberechtigung

Jeder, der das Sicherheitssystem steuern oder eine Einstellung vornehmen kann, wird Benutzer des Systems genannt. Der erste voreingestellte Benutzer mit der beinahe höchsten Berechtigung, der nicht gelöscht werden kann, ist der Servicecode (Errichter-Code). Der zweite voreingestellte Code, der nicht gelöscht werden kann, ist der Hauptadministrator. Andere Benutzer, die hinzugefügt werden, können genauso wieder gelöscht werden und verfügen über eine anpassbare Berechtigung.

Die Berechtigung der Benutzer kann wie folgt sein:

Codeberechtigung	Typbeschreibung
AES	Dieser Code entspricht der höchsten Berechtigungsstufe zur Konfigurierung des Systemverhaltens. Ein Benutzer dieses Codes kann das System nach einem ausgelösten Alarm entsperren. Er kann den Errichtermodus eingeben, hat Zugriff auf alle Registerkarten mit Optionen, einschließlich der AES-Kommunikation, auf die der Zugriff eines Errichters (Errichtercode) verweigert werden kann. Solange der Parameter „Administrator-beschränkter Service / ARC-Recht“ unbeschränkt bleibt, kann der ARC-Code alle im System verwendeten Bereiche und PG-Ausgänge steuern. Mit diesem Code kann man weitere Administratoren und andere Benutzer mit untergeordneten Zugriffsrechten hinzufügen, ihnen Codes, RFID-Tags und Karten zuweisen. Mit diesem Code ist man auch befugt, einen Alarm und den Sabotagealarmspeicher zu löschen. Die Anzahl der ARC-Codes ist nur durch die Restkapazität der Zentrale beschränkt.
Errichter (Service)	Mit diesem Code kann der Errichter den Errichtercode eingeben und das Systemverhalten konfigurieren. Er hat Zugriff auf alle Registerkarten mit Optionen, einschließlich der ARC-Kommunikation, wenn nicht der Zugriff durch einen übergeordneten ARC verweigert wurde. Solange der Parameter „Admin schränkt Errichter/AES—Rechte ein“ unbeschränkt bestehen bleibt, kann man mithilfe des Errichtercodes alle Bereiche und alle im System verwendeten PG-Ausgänge steuern. Man kann außerdem einen Benutzer mit AES-Erlaubnis, andere Errichter, Administratoren und andere Benutzer mit untergeordneten Zugriffsrechten erstellen und ihnen Zugangscodes, RFID-Tags und Karten zuweisen. Die Anzahl der Errichtercodes ist nur durch die verbleibende Kapazität der Zentrale begrenzt. Der Code ist standardmäßig 1010 und kann nicht gelöscht werden.
Administrator (Haupt)	Der Hauptadministrator hat immer vollständigen Zugriff auf alle Bereiche und ist berechtigt, alle PG-Ausgänge zu steuern. Er kann andere Administratoren und andere Codes mit untergeordneten Zugriffsrechten erstellen und ihnen Zugriffsrechte auf Bereiche, PG-Ausgänge, Zugriffscores, RFID-Chips und Karten zuweisen. Außerdem kann er mit diesem Code den Alarmspeicher löschen. Es gibt immer nur einen Administratorcode, der nicht gelöscht werden kann. Wenn die Funktion „Admin schränkt Errichter/AES—Rechte ein“ aktiviert ist, muss der Administratorcode berechtigt werden, um den Zugriff für den AES und Errichter zu bestätigen. Der Code ist standardmäßig 1234.
Administrator (Anderer)	Mit diesem Administrator-Code hat man das Zugriffsrecht auf vom Hauptadministrator festgelegte Bereiche. Der andere Administrator kann nun neue Benutzer mit den selben oder untergeordneten Zugriffsrechten hinzufügen, um Bereiche und PG-Ausgänge zu steuern und ihnen Zugangscodes, RFID-Tags und Karten zuzuweisen. Er ist berechtigt, den Alarmspeicher der zugewiesenen Bereiche zu löschen. Wenn die Funktion „Admin schränkt Errichter/AES—Rechte ein“ aktiviert ist, muss das Zugangsrecht des Administratorcodes bestätigt werden. Die Anzahl der Administratorcodes (andere) ist nur durch die Restkapazität der Zentrale beschränkt. Es ist kein Code in den Werkseinstellungen festgelegt.

Benutzer	Mit diesem Code hat man Zugriff auf Bereiche und PG-Steuerungsrechte, die von einem Administrator zugewiesen wurden. Benutzer können ihre RFID-Tags hinzufügen und löschen und ihre Telefonnummern ändern. Die Benutzer können ihren Code ändern, sofern das System Codes mit Präfixen verwendet. Mit dem Code ist man berechtigt, den Alarmspeicher in den zugewiesenen Bereichen zu löschen. Ausgewählte Benutzer können zeitlich begrenzten Zugang zu ihren Bereichen haben. Die Anzahl der Benutzercodes ist nur durch die Restkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.
Scharfschalten	Mit diesem Code darf man nur einen bestimmten Bereich scharf schalten. Benutzer dieser Berechtigungsstufe dürfen ihren Code nicht ändern und dürfen den Alarmspeicher nicht löschen. Die Anzahl der eingestellten Codes ist nur durch die Restkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.
PG-Ausgänge	Der Benutzer kann nur mit dem entsprechenden Zugriffsrecht programmierbare Ausgänge steuern. Dies gilt sowohl für das Ein- als auch das Ausschalten. Benutzer mit diesem Zugriffsrecht dürfen ihre Codes nicht ändern und können den Alarmspeicher nicht löschen. Die Anzahl der PG-Codes ist durch die Restkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.
Überfallalarm	Mit diesem Code kann nur ein Überfall oder auch Geiselnahmealarm ausgelöst werden. Der Benutzer dieses Codes kann weder diesen noch den Alarmspeicher löschen. Die Anzahl der Panikcodes ist durch die Restkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.
Wachdienst	Dieser Code ist für einen Sicherheitsdienst bestimmt. Mit dieser Zugriffsberechtigung kann man das gesamte System scharf schalten. Allerdings kann der Wachdienstcode das System nur während oder nach dem Alarm deaktivieren, solange der Alarmspeicher noch aktiv ist. Ein Benutzer dieses Codes darf weder diesen ändern noch den Alarmspeicher löschen. Die Anzahl der Wachdienstcodes ist nur durch die Restkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.
Entsperren	Dieser Code dient dazu, das System nach der Sperrung durch einen Alarm wieder zu entsperren. Der Benutzer dieses Codes ist nicht berechtigt, den Code zu ändern oder den Alarmspeicher zu löschen. Die Anzahl der Entsperrcodes ist nur durch die Restkapazität der Zentrale begrenzt. Es ist kein Code in den Werkseinstellungen festgelegt.

Die Erstellung neuer Benutzer und die Verwaltung ihrer Berechtigungsstufe wird in F-Link oder J-Link vorgenommen.

8.4. Optionale Systemparameter

Code mit Präfix – Diese Funktion bestimmt die Art der Eingabe aller Zugangscodes während der Benutzerberechtigung. Bei Aktivierung muss in das System ein 1- oder 3-stelliges Präfix gefolgt von * eingegeben werden, bevor Sie Ihren 4-, 6- oder 8-stelligen gültigen Zugangscodes eingeben (z. B. 12 * 3456). In diesem Fall ist es Benutzern erlaubt, ihre eigenen 4-stelligen Codes von einer LCD-Tastatur aus einzugeben und sie willkürlich zu bearbeiten. Durch das Deaktivieren der Funktion muss in das System kein Präfix eingegeben werden, nur ein gültiger Zugriffscode ist erforderlich. In diesem Fall kann nur der Systemadministrator die Codes aller Benutzer hinzufügen und bearbeiten. Der Administrator muss eine Code-Duplizierung vermeiden (2 Benutzer sollten nicht denselben Code haben).

Vorsicht: Durch Deaktivieren dieses Parameters werden alle Benutzercodes unwiderruflich gelöscht und die voreingestellten Errichter- und Administratorcodes auf die Standardwerte gesetzt. Benutzerberechtigung und RFID-Karten und Tags von bereits eingerichteten Benutzern bleiben gleich.

Codelänge – Um die Sicherheit des Alarmsystems während der Berechtigung zu erhöhen, ist es möglich, die **Codelänge für einen Benutzer** unabhängig von der Präfixfunktion voreinzustellen. Es kann 4-, 6- oder 8-stellige Codes geben. Wenn die Codelänge geändert wird, werden die Errichter- und Administratorcodes auf die Standardwerte (1010 und 1234) gesetzt und alle anderen Codes werden gelöscht. Standardcodes sind:

Standardcodes ohne Präfix	4-stellig	6-stellig	8-stellig
Errichter:	1010	101010	10101010
Administrator:	1234	123456	12345678

Standardcodes mit einem Präfix	4-stellig	6-stellig	8-stellig
Errichter:	0*1010	0*101010	0*10101010
Administrator:	1*1234	1*123456	1*12345678

125 kHz Informationsträger (IMT) aktivieren – Bei Deaktivierung dürfen nur vom Hersteller empfohlene RFID-Karten / Tags (JA-190J, JA-191J, JA-192J, JA-194J) verwendet werden. Bei Aktivierung sind auch Karten anderer Hersteller erlaubt, die mit der oben genannten Frequenz arbeiten.

Sirene wenn teilscharf (IW) – Diese Funktion aktiviert die interne Sirene während eines Einbruchsalarms (dies hat nichts mit Feuer oder 24 Std. Alarmen zu tun), wenn das System teilweise scharf geschaltet ist.

Warnung vor „Werkseitigen Codes“ – Bei Verlassen des Errichtermodus sendet das System eine SMS (Position 0) an den Errichter, dass die verbleibenden Codes noch in den Werkseinstellungen sind.

Adminschränkt Errichter/AES-Rechte ein - Die Berechtigung des Administrators wird benötigt, um dem ARC oder dem Errichter den Zugriff zum System zu ermöglichen. Wenn der Errichter per Fernzugriff über F-Link auf das System zugreift, erfolgt die Berechtigung des Administrators über die Tastatur im Gebäude. Wenn der Errichter lokal über ein USB-Kabel mit der Zentrale verbunden ist, erfolgt die Berechtigung des Administrators per Fernzugriff über das Sprachmenü.

Errichter oder AES betätigt das System - Dies ist für die Errichter (Service) und ARC-Techniker gedacht, um alle Bereiche (scharf / unscharf) und PG-Ausgänge zu steuern (EIN / AUS) , die eine Berechtigung erfordern.

Testbetrieb - Dieser spezielle Modus wird nach der Systeminstallation verwendet. Hier werden alle Alarmereignisse unabhängig von der tatsächlichen Einstellung der Alarmlänge auf 60 Sekunden verkürzt und über eine SMS an definierte Benutzer und den Errichter (Position 0) gemeldet, obwohl Alarmmeldungen nicht für sie aktiviert sind. Der Testbetrieb wird automatisch nach 7 Tagen nach Verlassen des Servicemodus beendet.

Hinweisfenster - Jahreswartung – Bei Aktivierung erscheint 12 Monate nach dem Verlassen des Errichter-Modus auf der LCD-Tastatur die Meldung „Systemprüfung anfordern“ und durch Drücken der Taste „I“ erscheint „Errichter anrufen“ mit seiner Telefonnummer (falls voreingestellt). Eine Meldung auf dem LCD verschwindet automatisch, wenn ein Errichter lokal auf das System zugreift. Der jährliche Check Counter führt einen Reset durch. Die Serviceanforderung kann auch in der Registerkarte Zeitschaltuhr auf ein genaues Datum als Kalenderaktion eingestellt werden (*die Kalenderfunktion „Technische Inspektion/Wartung“ kann ein Jahr nach Verlassen des Errichter-Modus mit der automatischen „Serviceanforderung“ kombiniert werden*).

Überfallalarm (Geiselnahmealarm) – Diese Funktion dient dazu, nur über die Berechtigungsfunktion oder während der Systemsteuerung (Scharfschaltung, Unscharfschaltung, PG) einen stummen Panikalarm auszulösen, wenn der Benutzer von einem Einbrecher unter Druck gesetzt wird. Während der Systemsteuerung wird ein Panik- bzw Überfallalarm ausgelöst, indem man die Zahl „1“ mathematisch der letzten Zahl eines Codes hinzufügt. Dies wird für Codes mit oder ohne Präfix unterstützt. Wenn ein Benutzercode die Zahl 9 als letzte Zahl hat, ist bei der erzwungenen Zugriffssteuerung 0 als letzte Zahl einzugeben.

2-Melderabhängigkeit in einem Bereich - Wenn eine Bestätigungsreaktion durch einen anderen Melder für einen Melder aktiviert ist, kann diese Bestätigungsoption verwendet werden, um die Bestätigung nur auf diesen Bereich zu begrenzen (andernfalls kann ein Melder eines anderen Bereichs einen Alarm bestätigen). Dies gilt sowohl für Einbruchs- als auch für Feuermelder.

Interne Sirene bei Sabotagealarm - Die Sirene mit einer IW-Reaktion zeigt einen Sabotagealarm akustisch an, wenn der Bereich unscharf oder teilweise scharf geschaltet ist. Sirenen werden immer aktiviert, wenn das System (der Bereich) vollständig scharf geschaltet ist.

Rücksetzen von Sabotage durch Errichter – Die Anzeige des Sabotagealarms wird vom Errichter zurückgesetzt - die Anzeige des Sabotage-Speichers kann nur von einem Errichter oder AES-Techniker zurückgesetzt werden. Wenn diese Option nicht aktiviert ist, kann die Anzeige auch vom Administrator zurückgesetzt werden (jedoch nicht von einem Benutzer).

Reset auf Werkseinstellung - Die Zentrale kann über einen Jumper zurückgesetzt werden. Wenn die Zurücksetzung deaktiviert und der Errichtercode nicht verfügbar ist, kann die Zentrale nur durch den Hersteller entsperrt werden. Die Zurücksetzung der Zentrale wird in Kapitel 12 Zurücksetzung der Zentrale beschrieben.

Tägliches zurücksetzen des Autobypass – Die Option bezieht sich nur auf Aktivierungseingänge (keine Sabotage- und Störungseingänge). Wenn diese Option aktiviert ist, setzt das System umgeleitete Geräte automatisch zurück, und zwar jeden Tag um 12:00 Uhr. Wenn die Option deaktiviert ist, wird der Autobypass des Geräts nur mit einer Statusänderung im Bereich zurückgesetzt. Diese Auswahl eignet sich z.B. für die Verwendung von Meldern mit einer 24-Stunden-Reaktion oder Überschwemmungsmeldern, die sich in einem Bereich befinden, in dem die Scharf- / Unscharfschaltung nicht erforderlich ist.

Bypass bei Scharfschaltung – Bei Aktivierung werden alle aktiven Eingänge während der Scharfschaltung des Bereichs gesperrt und können keinen Alarm mehr in diesem überwachten Zeitraum auslösen. Wenn diese Option deaktiviert ist, werden alle aktiven Eingänge kurzzeitig überbrückt (Autobypass), bis sie in den Standby-Modus gehen und die Melder wieder mit der Überwachung beginnen (Risiko einer Fehlalarmauslösung - z. B. nicht richtig geschlossenes Fenster).

Autorisierung hebt Alarm nicht auf – Diese Funktion bestimmt, ob ein Alarm nur durch die Berechtigung eines gültigen Codes oder durch das Deaktivieren des Bereichs mit einem Alarm abgebrochen wird. Bei Aktivierung dieser Funktion kann ein Alarm abgebrochen werden, indem entweder der Bereich, in dem der Alarm ausgelöst wurde, deaktiviert wird, oder von einem LCD-Tastaturmenü aus, indem man auf „Warnmeldung abrechnen“ drückt.

Nicht erfolgreiches Scharfschalten – Diese Funktion wird immer während des Vorgangs der Scharfschaltung ausgeführt. Wenn ein sofortiger Bereich in der Ausgangszeit aktiviert wird oder ein verzögerter Bereich nach Ablauf der definierten Zeit offen bleibt, wird das System nicht scharf geschaltet, löst eine „fehlgeschlagene Scharfschaltung“ aus und erstellt dieses Ereignis im Ereignisverlauf. Dies wird ebenso per SMS an einen vordefinierten Benutzer gemeldet, wenn das Ereignis „SMS bei nicht erfolgreichen Scharfschalten“ (Registrierkarte Übertragungsgeräte) als Benachrichtigung aktiviert ist. Dies wird über die Tastaturen und die Außensirenen angezeigt. Um die Anzeige über die fehlgeschlagene Scharfschaltung zu beenden, betätigen Sie „Warnung beenden“ im Menü der LCD-Tastatur.

Gerätefehler-Autobypass - Diese Option ist nur dann verfügbar, wenn eines der Systemprofile „EN50131-1“ oder „INCERT“ ausgewählt wurde. Sie dient dazu, die begrenzte Anzahl von ausgelösten Fehlern von maximal 3 Fehlern bis unbegrenzt zu deaktivieren.

Art der Scharfschaltung – Auswahl der Art und Weise, wie das System die Systemscharfschaltung mit einem aktiven Gerät oder einem Fehler im System erreicht. Die Auswahl reicht von der niedrigsten Stufe, bei der das System immer scharf geschaltet wird, unabhängig davon, ob ein Gerät aktiviert ist oder ein Fehler auftritt, bis zur höchsten Stufe, bei der eine Scharfschaltung nicht möglich ist, wenn ein Gerät aktiviert ist (Sofortiger Bereich).

Autorisierungstyp – Auswahl der Optionen, wie das System Benutzerberechtigungen verarbeitet. Die Optionen reichen von der Standardberechtigung (nur ein Code oder eine Karte) bis hin zur Codebestätigung einer RFID-Karte (wenn dem Benutzer beides zugewiesen ist), der doppelten Berechtigung, die bedeutet, dass sowohl die Verwendung der Karte als auch der des Codes obligatorisch ist. Die Bestätigung der Benutzercodes über eine Karte verringert das Risiko eines Zugriffs oder einer Steuerung des Systems durch unbefugte Personen.

System Sperre nach einem Alarm – Die Parameter erlauben die Sperrung des Systems nach der ersten Alarmauslösung (Einbruch oder Sabotage), um zu vermeiden, dass weitere Alarme ausgelöst werden. Das Entsperrern kann durch einen speziellen Code zum Entsperrern oder durch den berechtigten Zugriff einer AES (durchgeführt werden. Die Entsperrung nach der Auslösung eines Sabotagealarms kann auch von einem Benutzer mit Errichterberechtigung durchgeführt werden.

Verbindungsverlust einer BUS-Komponente – Die Zentrale reagiert auf den Verlust eines Geräts oder auf einen Kurzschluss am BUS-Gerät. Entsprechend der ausgewählten Option erfolgt dies bei jedem Geräteverlust entweder durch eine Fehleranzeige oder einen Sabotagealarm oder durch einen Sabotagealarm, nachdem der Verlust eines weiteren Geräts bestätigt wird.

Komponenten-Autobypass - Die Option bezieht sich nur auf Aktivierungseingänge, nicht auf Sabotage- und fehlerhafte Eingänge. Wenn die Funktion aktiviert und auf „3. Aktivierung“ eingestellt ist, ermöglicht die Zentrale 3 Aktivierungen des Geräts während einer Alarmperiode. Die zweite Option ist „3. Alarm“, das heißt, das bestimmte Gerät wird erst nach 3 Alarmperioden umgangen, d. h. das Gerät kann bis zu 9 Mal in einer Überwachungsperiode aktiviert werden.

8.4.1. Geräte anmelden und löschen

Ein installiertes Gerät (Melder, Tastatur, Sirene, Tag usw.) funktioniert, nachdem es auf einer Position (Adresse) im System angemeldet ist. Nach der Anmeldung besetzen einige Geräte mehrere Positionen (magnetische Mehrfacheingänge, Eingangserweiterungen). Es gibt auch Geräte (PG-Ausgänge, Statusanzeigen, BUS-Trenner und Splitter), die an keiner Position angemeldet werden. Detaillierte Informationen über die entsprechenden Geräte finden Sie in den jeweiligen Handbüchern.

1. Die Geräteanmeldung erfolgt über F-Link, Registerkarte Komponentenliste, **Anmelden**. Die Anmeldung **ist nur im Errichtermodus möglich**.

2. Sie können ein Gerät auf verschiedene Arten anmelden:
 - a. **durch Betätigung des Sabotagekontakts eines BUS-Geräts = Schließen der Abdeckung** (einige Geräte können über eine Taste angemeldet werden - Informationen dazu finden Sie in der Anleitung des jeweiligen Geräts).
 - b. **durch Einlegen der Batterie in einem drahtlosen Gerät** - jedoch muss zuerst mindestens ein Funkmodul in Reichweite installiert werden. Wenn die Fernbedienung über den Typ JA-186Jx vorgenommen wird, kann die Batterieverbinding durch Drücken und Halten von zwei Tasten (Tastenpaar) ersetzt werden. Fernbedienungen des Typs JA-154Jx werden durch das Betätigen irgendeiner Taste angemeldet. Drahtlose Zugriffmodule (Tastaturen) können durch Drücken der beleuchteten Aktivierungstaste angemeldet werden.
 - c. **durch Eingabe der Seriennummer in den SN Produktionscode** - (dieser befindet sich unter dem Strichcode im Gerät, z.B. 1400-00-0000-0123). Die Nummer kann auch mit einem optischen Strichcode-Lesegerät eingelesen werden. Sie sollten dann den Melder zur Prüfung aktivieren.
 - d. **durch selektives Laden nicht angemeldeter BUS-Geräte** – Wenn ein oder mehrere Geräte, die noch nicht angemeldet sind, mit dem BUS verbunden werden, wird nach Drücken von **Anmelden** in der Registerkarte **Komponentenliste**, die die Anmeldung des BUS-Geräts ermöglicht. Sie melden das Gerät an dieser Position mit einem Doppelklick an.
 - e. **durch kollektives Laden nicht angemeldeter BUS-Geräte** – wenn ein oder mehrere noch nicht angemeldete Geräte mit dem BUS verbunden werden, werden alle Geräte im Kollektiv nach Betätigen der Taste **Bus Anmeldesignal senden** angemeldet. Diese Vorgehensweise ermöglicht Ihnen nicht, die Reihenfolge der einzelnen Geräte zu bestimmen.
3. Sie können ein Gerät löschen, indem Sie seinen Produktionscode löschen (nur das gesamte Gerät wird gelöscht) oder die entsprechende Zeile in der Registerkarte Komponentenliste und die Löschoption im Menü wählen oder Sie die rechte Maustaste oder die Löschtaste drücken, die die gesamte Zeile des Geräts (einschließlich der Einstellungen des Bereichs, Reaktion, PG-Ausgangssteuerung und andere Optionen) löscht. So können Sie mehrere Geräte markieren (click+Shift or click+Ctrl) und alle löschen oder den gemeinsamen Parameter ändern.

Hinweise:

- Nicht angemeldete BUS-Geräte blinken gelb. Wenn die gelbe LED eines unangemeldeten Geräts nicht innerhalb 180 Sek. nach Aktivierung der Stromversorgung der Zentrale (im Verlauf der Initialisierung) blinkt, sollten Sie prüfen, ob das Gerät korrekt verbunden ist.
- Drahtlose Geräte mit einer unidirektionalen Kommunikation signalisieren nicht die Anmeldeanforderung.
- Wenn Sie ein Gerät im System auf die oben beschriebene Weise anmelden, wird die nächste Position automatisch angeboten. Sie müssen keine weiteren Schritte unternehmen, sondern nur die Geräte in der ausgewählten Reihenfolge anmelden. Die automatische Bewegung zur nächsten Position kann im Fenster der Geräteanmeldung beendet werden.
- Wenn Sie ein bereits angemeldetes Gerät an einer anderen Position anmelden möchten, wird es automatisch bewegt.
- Wenn ein Gerät mehrere Positionen besetzt, wird es automatisch die entsprechende Anzahl der Positionen bei einer Anmeldung besetzen (z.B. wird ein Modul JA-110M, das 2 Alarmeingänge hat, auch zwei Positionen besetzen). Vorsicht, ein Gerät, das an einer anderen Position angemeldet ist, kann versehentlich gelöscht werden!
- Wenn ein Gerät an der höchstmöglichen Position angemeldet wird, wird der Prozess der schrittweisen Anmeldung abgeschlossen.
- Freie Positionen werden standardmäßig Bereich 1 zugewiesen. Die Zuweisung eines Bereichs kann nachträglich geändert werden.
- Bei Geräten mehrerer Positionen, wie JA-116H, JA-118M, JA-150M usw. können Sie die Zahl der besetzten Positionen begrenzen, indem Sie die spezifische Zeile nach der Anmeldung des Moduls löschen. Sie führen den Löschvorgang durch Klicken der Zeile auf der entsprechenden Position (keine Spalte!) und Betätigung der Löschtaste auf der Tastatur des PCs durch.

8.4.2. Liste der anwendbaren Reaktionen

In der Registerkarte Komponentenliste können Sie die Reaktion der Systemaktivierung eines angemeldeten Geräts einstellen. Nur solche Reaktionen werden für einzelne Geräte angeboten, die für das jeweilige Produkt sinnvoll sind. Es gibt einige Geräte, denen keine Reaktion zugewiesen werden kann (z. B. eine externe Sirene).

Sofortiger Alarm (IW)	Sofortiger Einbruchalarm bei Scharfschaltung. Wenn eine Eingangsverzögerung eingestellt ist, wird ein IW-Alarm ausgelöst. Ein EW-Alarm wird erst nach Ablauf der Eingangsverzögerungszeit ausgelöst (weitere Informationen zu EW und IW siehe Kapitel 8.5 Alarmarten).
Verzögerter Alarm - A	Einbruchsalarm mit Eingangs- / Ausgangsverzögerung, Timer A.

Verzögerter Alarm - B	Einbruchsalarm mit Eingangs- / Ausgangsverzögerung, Timer B.
Verzögerter Alarm - C	Einbruchsalarm mit Eingangs- / Ausgangsverzögerung, Timer C. Einstellung der Timer A, B, C – siehe Registerkarte Systemparameters. In der Registerkarte Systemparameter können Sie für diese Reaktion festlegen, dass die Ausgangsverzögerung um einen aktiven Melder mit der Verzögerung C verlängert wird (z. B. für die Zeit des Öffnens des Garagentors).
Nachfolgend Verzögert	Einbruchsalarm. Ein Melder verfügt über die selbe Ausgangsverzögerung wie die verzögerten Melder im selben Bereich. Dieser Melder verfügt nur über eine Eingangsverzögerung, wenn er nach einem Melder, für den eine verzögerte Reaktion eingestellt wurde, aktiviert wird. Wenn er zuerst aktiviert wird, löst er sofort einen Alarm aus. Diese Einstellung ist sinnvoll, wenn ein verzögerter Melder im gleichen Bereich scharf geschaltet wird.
Abschlusstür A	Einbruchsalarm mit Eingangs- / Ausgangsverzögerung, Timer A. Die Ausgangsverzögerung wird auf 5 Sek. verkürzt, nachdem ein aktivierter Melder in den Standby-Modus geht.
Abschlusstür B	Einbruchsalarm mit Eingangs- / Ausgangsverzögerung, Timer B. Die Ausgangsverzögerung wird auf 5 Sek. verkürzt, nachdem ein aktivierter Melder in den Standby-Modus geht.
Abschlusstür C	Einbruchsalarm mit Eingangs- / Ausgangsverzögerung, Timer C. Die Ausgangsverzögerung wird auf 5 Sek. verkürzt, nachdem ein aktivierter Melder in den Standby-Modus geht.
Sofortiger Alarm (IW+EW)	Sofortiger Einbruchsalarm bei Scharfschaltung. Die Alarmwarnungen EW und IW werden gemeinsam und direkt aktiviert, auch während einer Eingangsverzögerung.
Sofortiger / Verzögerter Alarm A	Das System reagiert auf die Aktivierung eines Melders (Alarm, Eingangsverzögerung) bei einer Teilscharfschaltung als Sofortige Zone, bei einer vollständigen Scharfschaltung als Verzögerte Zone A.
Bestätigt, sofort	Sofortiger Einbruchsalarm – siehe 8.4.3 Bestätigte Einbruchsreaktion.
Bestätigt, verzögert A	Einbruchsalarm mit einer Eingangs- und Ausgangsverzögerung, Timer A - siehe 8.4.3 Bestätigte Einbruchsreaktion.
Wiederholt, sofort	Sofortiger Einbruchsalarm – siehe 8.4.3 Wiederholte Reaktion.
Wiederholt, verzögert A	Einbruchsalarm mit einer Eingangs- und Ausgangsverzögerung, Timer A – siehe 8.4.3 Wiederholte Reaktion.
Sabotage	Sabotagealarm zu jeder Zeit (der Bereich muss nicht scharf geschaltet werden).
24 Stunden	Direkter Alarm (der Bereich muss nicht scharf geschaltet werden).
Stiller Überfallalarm	Stiller Überfallalarm: 1) EW und IW nicht aktiviert (siehe Kapitel 8.5 Alarmarten); 2) Die Tastatur piept nicht, obwohl sie ansonsten so eingestellt ist; 3) Wenn das System unterscheiden kann, wer den Überfallalarm ausgelöst hat (z.B. über einen Tag mit der Identität des Benutzers oder über die Eingabe des Überfallalarmcodes durch den Benutzer), sendet es keine Überfallalarm-SMS an den Benutzer.
Lauter Überfallalarm	Lauter Überfallalarm (das Verhalten ist so wie bei einem Stillen Alarm, der einzige Unterschied besteht darin, dass ein Alarm von einer verwendeten Sirene entsprechend der Tabelle in Kapitel 8.5 Alarmarten signalisiert wird).
Brandalarm	Brandalarm zu jeder Zeit (der Bereich muss nicht scharf geschaltet sein).
Brandalarm, bestätigt	Brandalarm zu jeder Zeit (der Bereich muss nicht scharf geschaltet sein), siehe Kapitel 8.4.3 Bestätigte Brandreaktion.
Brandalarm im Scharfzustand	Brandalarm nur, wenn der jeweilige Bereich scharf geschaltet ist.

Gas	Gasleckalarm zu jeder Zeit (der Bereich muss nicht scharf geschaltet sein).
Notruf	Sendet eine Meldung bei Gesundheitsproblemen
Überschwemmung	Sendet einen Überschwemmungsalarm
Gesamtscharf/- Unscharf	Scharfschaltung (teilweise Scharfschaltung) eines Bereichs. Wenn es sich um einen gemeinsamen Bereich handelt, werden alle Bereiche, die zu ihm gehören, gleichzeitig scharf geschaltet. Diese Reaktion verfügt auch über die Unscharfschaltungsfunktion.
Sirenenberuhigung mit Bericht	Stummschaltung der internen Sirene mit einer anschließenden Meldung über die Anwesenheit einer Person im Gebäude.
Meldung A / B / C / D	Eine spezielle Meldung wird gesendet (Sondermeldungen A, B, C und D werden in der Registerkarte Benutzerbenachrichtigungen an Benutzer festgelegt), die mit einem Sprachnachrichtenanruf kombiniert werden können. Wenn das Speichern von Sondermeldungen im Ereignisverlauf aktiviert ist, werden auch Meldungen an die AES gesendet.
Schlüssel-Box	Eine spezielle Reaktion, die für den versiegelten Schlüssel im Notfall entwickelt wurde, usw., dessen Öffnung eine Meldung an die AES/NSL sendet, ohne den Alarm mit einer Sirene zu aktivieren.
Immer Sofort	Sofortige Zonenreaktion. Bei Scharfschaltung wird basierend auf der Aktivierung sofort die EW- und IW-Alarmwarnung auch während der Zeit der Ausgangsverzögerung aktiviert.
Kein Alarm	Ohne Auswirkung auf den Einbruchalarm; Das Gerät kann jedoch zur Aktivierung von PG-Ausgängen verwendet werden.
Kein Alarm und Sabotagealarm	Das System reagiert auf die Aktivierung des Melders nur durch die PG-Ausgangssteuerung. Keiner der Alarmarten wird ausgelöst (auch kein Sabotagealarm), die Fehlererkennung bleibt erhalten.

8.4.3. Einschränkung von Fehlalarmen

Bei Installationen mit einem erhöhten Fehlalarmrisiko können spezielle Reaktionsarten verwendet werden:

Bestätigte Reaktion bei einem Einbruch – Wenn ein Melder mit einer bestätigten Reaktion in einem Bereich aktiviert wird, meldet das System der AES/NSL nur einen unbestätigten Alarm und wartet auf die Bestätigung durch einen anderen Melder. Der Alarm kann von jedem Einbruchsmelder in einem Bereich bestätigt werden. In der Registerkarte Systemparameter können Sie festlegen, ob die Bestätigung von einem beliebigen Bereich aus durchgeführt werden kann oder die Bestätigung über den selben Bereich erfolgen muss. Sie können auch in der Registerkarte Systemparameter die Zeitspanne festlegen, in der das System auf die Bestätigung eines anderen Melders (bis zu 60 Min.) wartet. Wenn der Alarm innerhalb der vordefinierten Zeit nicht bestätigt wird, wird auch kein Alarm ausgelöst. Wenn eine bestätigte Verzögerungsreaktion eingestellt ist, löst die Aktivierung des Melders nur einen unbestätigten Alarm nach Ablauf der Eingangsverzögerung aus. Die bestätigte Reaktion kann nur dann verwendet werden, wenn mehrere Einbruchsmelder im Gebäude installiert sind (zur Aktivierung der Bestätigung). Diese Reaktion wird nur bei dem Systemprofil „Standard“ verwendet.

Bestätigte Reaktion bei einem Brand – Wenn ein Rauchmelder mit dieser Reaktion aktiviert wird, wird der AES/NSL nur ein unbestätigter Brandalarm gemeldet und das System wartet auf die Bestätigung eines anderen Brand- oder Rauchmelders. In der Registerkarte Systemparameter können Sie festlegen, ob die Bestätigung von einem beliebigen Bereich aus durchgeführt werden kann oder ob die Bestätigung über den selben Bereich erfolgen muss. Die Zeitspanne, in der das System auf die Bestätigung eines Feueralarms wartet, kann in der Registerkarte Parameter festgelegt werden. Wenn ein Feuer innerhalb der vordefinierten Zeit nicht bestätigt wird, wird auch kein Brandalarm ausgelöst. Die bestätigte Reaktion kann nur dann verwendet werden, wenn mehrere Brand- oder Rauchmelder im Gebäude installiert sind (zur Aktivierung der Bestätigung).

Warnung: Diese Funktion und ihre Verwendung muss in Übereinstimmung mit den lokalen Anforderungen und Normen mit größter Vorsicht betrachtet werden.

Wiederholte Reaktion – Wenn ein Melder dieser Reaktionsart aktiviert wird, wartet das System, ob die Aktivierung desselben Melders wiederholt wird. In der Registerkarte Systemparameter können Sie den Zeitraum einstellen, in dem das System auf die wiederholte Aktivierung wartet, sowie die Zeit, in der der Melder nicht berücksichtigt wird. Wenn die Aktivierung des Melders nicht innerhalb der voreingestellten Zeitspanne (einstellbar von 6 bis 120 Sekunden) wiederholt wird, wird die erste Aktivierung abgebrochen. Die wiederholte

Reaktion findet in einer Umgebung mit einem erhöhten Risiko von gelegentlichen Fehlalarmen, z.B. verursacht durch Nagetiere, kleine Insekten etc. seine Anwendung.

Three-Strikes-Funktion (3x und STOP!) - Alle Einbruchs- und Feuermelder mit einer aktivierten Alarmreaktion sind auf höchstens drei mögliche Aktivierungen der Zentrale während eines Überwachungszeitraums beschränkt. Nach drei Aktivierungen (bei der vierten Einbruchsmeldung) wird ein Bypass für diesen bestimmten Alarmeingang aktiviert und der entsprechende Sensor wird von weiteren Aktivitäten ausgeschlossen. Wenn diese drei Aktivierungen während eines Alarms auftreten, werden drei Alarm-SMS zusammen erstellt und der Melder deaktiviert. Wenn diese drei Aktivierungen in Zeitintervallen auftreten, die länger als die Alarmdauer sind, werden drei Alarm-SMS erstellt, drei Alarme werden ausgelöst und dann der Melder deaktiviert.

Diese Funktion kann um den Parameter „Gerätefehler-Autobypass“ erweitert werden. Sie finden ihn in der Registerkarte Systemparameter und der Auswahl Komponenten-Autobypass „3. Alarm“ - nun können bei maximal 3 Alarmen bis zu 3 Aktivierungen für jedes Gerät erreicht werden. Dies bedeutet, dass bis zu neun (3x3) Alarm-SMS gesendet werden können.

Ein Bypass kann beendet werden, indem man den Bereich unscharf und danach wieder scharf schaltet. Der Melder befindet sich dann wieder im Überwachungsmodus. Der Bypass für die Feuer- und Überschwemmungsreaktion wird auch automatisch am folgenden Tag um 12:00h (entsprechend dem Parameter „Tägliches zurücksetzen des Autobypasses“ in der Registerkarte Systemparameter) beendet. Der Bypass-Mechanismus 3x-und-Stop gilt nicht für Geräte, bei denen eine Überfallreaktion eingestellt ist. Die Anzahl der ausgelösten Fehler kann auf ähnliche Weise begrenzt werden (siehe „Gerätefehler-Autobypass“ in der Registerkarte "Systemparameter").

Verspätete Meldung an die AES/NSL – Gemäß Norm EN50131-1 wird die Anzahl der Fehlalarme durch den Endbenutzer verringert, die durch eine falsche Bedienung des Systems entstehen und das Einschreiten eines Sicherheitsdienstes zur Folge haben. Wenn diese Funktion aktiviert ist, wird ein interner Alarm ausgelöst (Sirene, Tastaturanzeige), nachdem die Eingangsverzögerung abgelaufen ist. Jedoch wartet das System weitere 15 Sek., bis es die AES/NSL eine Alarmmeldung sendet. Ein Benutzer hat somit 15 Sek. länger Zeit, das System unscharf zu schalten, ohne dass der ARC informiert wird. Wenn er dies innerhalb dieser Zeit schafft, wird der AES/NSL keine Alarmmeldung gesendet. Diese Verzögerung betrifft nur einen ausgelösten Alarm in einem verzögerten Bereich. Andere Alarmarten (Sofort, Brand, Sabotage u.s.w.) werden sofort und ohne Verzögerung unabhängig von ihrer Funktion gemeldet.

8.5. Alarmarten

Der Sinn eines Sicherheitssystems besteht darin, seinem Besitzer und Benutzern Ereignisse zu melden oder einen professionellen Sicherheitsdienst über Gefahren zu informieren. Diese könnten ein Einbruch, aber auch Einflüsse wie Rauch, Feuer, Gas oder Überschwemmungen im überwachten Gebäude darstellen. Die Anzeige jeder Alarmart kann entsprechend der Ursache unterschiedlich sein. Bei Sirenen wird zwischen internen (IW) und externen (EW) Alarmen unterschieden.

In der folgenden Tabelle finden Sie eine Übersicht der IW- und EW-Ausgänge entsprechend der Alarmart und dem Bereichsstatus:

Bereichsstatus	Alarmart					Systemeinstellungen - Parameter		Aktiviert	
	Einbruch	Sabotage	Lauter Überfallalarm	Feuer / Brand	24Std./Überschhwemmung	Sirene IW während teilweise Scharfschaltung	IW Sirene während Sabotage	EW	IW
Unscharf		X				N/A	NEIN		
		X				N/A	JA		X
			X			N/A	N/A	X	X
				X	X	N/A	N/A		X
Teilscharf		X				N/A	NEIN		
		X				N/A	JA		X
	X					JA	N/A		X
	X					NEIN	N/A		
			X			N/A	N/A	X	X
				X	X	N/A	N/A		X
Scharf	X	X	X	X	X	N/A	N/A	X	X

Alle Arten der Systemsirenen haben intermittierende Töne (optional Dauerton oder intermittierender Ton). Die Außensirene blinkt rot oder blau (Blinkeinrichtung). Die Anzeigenlänge wird mit dem Systemparameter zur Alarmlänge in der Zentrale definiert. Jede Sirene verfügt über eigene Einstellungen wie der Begrenzung der Alarmlänge. So können Sie eine kürzere Dauer der Alarmanzeige der externen Sirene im Vergleich zur internen Sirene einstellen. Jeder Alarm (außer stummen Panikalarmen) haben ein Anfang und ein Ende (Ablauf oder Beendigung durch den Benutzer). Zusammen mit der Ereignisursache und der Zeitmarkierung wird ein Eintrag in den Ereignissen erstellt.

Auf der Systemtastatur werden alle Alarme (außer stummen Panikalarmen) durch eine rot blinkende Systemanzeige mit einer dauerhaften akustischen Anzeige angezeigt.

8.5.1. Einbruchsalarm

Der Alarmstatus der Zentrale kann von Meldern mit verzögerten oder unverzögerten Reaktionen (und ihren Variationen) aktiviert werden. Dies gilt für ein teilweise oder vollständig scharf geschaltetes System. Angezeigt wird dies durch die internen und externen Sirenen, siehe Tabelle oben. Die Alarmlänge wird in den Einstellungen der Systemparameter der Zentrale festgelegt. Wenn ein Alarm abgelaufen ist, zeigen ihn die Tastaturen und Sirenen entsprechend nicht mehr an. Ein berechtigter Benutzer kann die akustische Anzeige aller Sirenen und Tastaturen stumm schalten, jedoch kann der Alarmstatus des Systems nicht beendet oder unscharf geschaltet werden. Es muss als Folgeaktion von einem Steuerbereich oder dem Menü der LCD-Tastatur ausgeführt werden.

8.5.2. Sabotagealarm

Die Zentrale überwacht all am System angemeldeten Geräte, unabhängig ihres Systemstatus (scharf/unscharf). Die meisten Geräte haben einen eingebauten Sabotagekontakt, der erkennt, wenn das Gehäuse des Melders geöffnet wird oder er von der Wand gerissen wird. Eine Aktivierung löst einen Sabotagealarm aus und wird durch eine interne Sirene (entsprechend des Parameters Sirene IW, wenn ein Sabotagealarm ausgelöst wird) in einem unscharf geschalteten System angezeigt. In einem scharf geschalteten System werden beide Sirenen (interne und externe Sirene) ausgelöst, siehe Tabelle oben. Ein Sabotagealarm kann auch ein Verlust von BUS-Geräten (z.B. durch einen Kurzschluss), oder durch unbefugte Versuche der Codeentschlüsselung (10x) auf der Tastatur, ferngesteuert und per Telefonanruf mit DTMF, über eine SMS-Nachricht oder der Verwendung der MyJABLOTRON-App (WEB + Smartphone) sein.

8.5.3. Brandalarm

Ein Brandalarm wird durch aktivierte Melder mit einer scharf geschalteten Reaktion auf Brand ausgelöst. Die folgenden Melder dienen als Brandmelder (Rauch, hohe Temperaturen, Melder für brennbare Gase und CO-Melder zur Erkennung des giftigen Kohlenmonoxyd). Wenn das System unscharf oder teilweise scharf geschaltet ist, wird ein Brandalarm durch eine interne Sirene angezeigt. Bei einer vollständigen Scharfschaltung wird dies durch die interne und externe Sirene angezeigt.

Es gibt unterschiedliche Alarmarten, wie z.B.:

1. **Brandalarm** – Basisreaktion für alle Brand- und Rauchmelder.
2. **Brandalarm bestätigt** – Option für höhere Zuverlässigkeit. Mindestens 2 Brand- und Rauchmelder müssen in jedem Raum mit den selben Einstellungen installiert sein.
3. **Brandalarm im Scharfzustand sofort** – Besonders bei Gebäuden verwendet, wo normalerweise Rauch ist (Restaurants, Schweißerei u.s.w.) und die Erkennung nur dann erfolgt, wenn das System scharf geschaltet ist.
4. **Gas** – Eine besondere Reaktion des Feuermelders besteht darin, brennbare und giftige Gase zu erkennen und dieses Ereignis die AES zu melden.

8.5.4. Überfall- und Geiselnahmealarm

Ein Überfall- und Geiselnahmealarm ist ein spezielles Ereignis, das als 2 unterschiedliche Ereignisse, dem **Lauter Überfallalarm** und dem **Leiser Überfallalarm**, ausgelöst werden kann. Jeder der Alarme zeigt sich über ein anderes Verhalten.

1. **Leiser Überfallalarm** – Ein spezielles Ereignis, das nicht einer Gruppe von Meldern zugeordnet ist, die durch eine Sirene oder eine Tastatur angezeigt werden. Ein leiser Überfallalarm hat keinen Timer, dieses Ereignis endet nicht. Also kann er nicht für die Systemsteuerung eines PG-Status verwendet werden. Er dient nur zur Auslösung eines leisen Überfallalarms und als Hilferuf bei einem Angriff, ohne dass der Angreifer dies bemerkt. Ein leiser Überfallalarm wird mit einer speziellen (versteckten oder tragbaren) Paniktaste ausgelöst. Normalerweise über eine für einen leisen Überfallalarm voreingestellte Taste, über eine Kombination der Tasten auf der Fernbedienung, über einen Steuerungsbereich (Segment) auf der Tastatur, der speziell für leise Überfallalarms vordefiniert ist (in diesem Fall kann ein Panikalarm mit einem Timer verzögert werden), durch Betätigen der Taste an der internen Sirene, über einen Eingang am BUS-Modul, das für verkabelte Geräte geeignet ist, oder durch die Eingabe eines speziellen Codes, der einen leisen Überfallalarm auslöst. Ein leiser Überfallalarm kann auch ausgelöst werden, wenn eine erzwungene Zugriffssteuerung durchgeführt wird, siehe Kapitel 9.10 Systemsteuerung über die Erzwungene Zugriffssteuerung, bei der der standardisierte Benutzercode geändert wird.
2. **Lauter Überfallalarm** – Ein normales Ereignis mit einem Anfang und einem Ende, das akustisch über eine Sirene und die Tastatur angezeigt wird. Er kann für die Statusteuerung eines PG-Ausgangs verwendet werden. Meistens wird er verwendet, um einen Überfallalarm mit einer optischen Anforderung auszulösen oder um elektrische Türschlösser zu sperren u.s.w. Ein Lauter Überfallalarm kann über eine spezielle (versteckte oder tragbare) Paniktaste ausgelöst werden. Normalerweise über eine voreingestellte Taste für einen stummen Alarm, über eine Tastenkombination auf der Tastatur, über eine Tastatur mit einem speziell für einen stummen Alarm voreingestellten Steuerungsbereich (in diesem Fall kann ein Panikalarm mit einem Timer verzögert werden), durch Betätigen der Taste an der internen Sirene, über einen Eingang am BUS-Modul, das für verkabelte Geräte geeignet ist.

Vorsicht: Beide Arten des Überfall- oder auch Geiselnahmealarms sind spezifisch aufgrund der Tatsache, dass sie ohne Einschränkung und automatische Sperrung wiederholt ausgelöst werden können.

8.5.5. 24 Stunden-Alarm

Melder, die eine dauerhafte Überwachung gewährleisten, sind unabhängig vom Systemstatus (scharf oder unscharf) und können eine voreingestellte Reaktionszeit von 24 Std. haben. Diese Alarmart ist den Einbruchsalarmen zugeordnet. Unabhängig von dieser Tatsache kann er jedoch ausgelöst werden, wenn das System unscharf geschaltet ist. Entsprechend des Systemstatus, wird ein Alarm durch eine interne und externe Sirene angezeigt, siehe Tabelle oben. Die Alarmmeldung erfolgt wie die anderen Alarme.

8.5.6. Alarmabbruch

Wenn ein Alarm im System ausgelöst wird, wird dessen Dauer von dem für die Alarmlänge bestimmten Timer gezählt, siehe F-Link, Registerkarte Systemparameter. Wenn sich in den überwachten Räumen ein berechtigter Benutzer befindet, kann der Alarm rechtzeitig abgebrochen werden. Die Alarmunterdrückung bewirkt ein sofortiges

Stummschalten aller Sirenen und beendet das Melden von Alarmmeldungen an alle voreingestellten Telefonnummern. Die Art des Alarmabbruchs hängt von dem Parameter in der Registerkarte Systemparameter ab:

Autorisierung hebt Alarm nicht auf

- Bei Aktivierung dieser Option wird der gerade ausgeführte Alarm abgebrochen, indem der Bereich mit einem Alarm oder nach der Berechtigung auf einer LCD-Tastatur deaktiviert und die Option „Warnmeldung abbrechen“ gedrückt wird.
- Bei Deaktivierung dieser Option kann ein momentan ausgeführter Alarm nur durch eine gültige Benutzerberechtigung mit Zugriffsrechten auf diesen Bereich abgebrochen werden, ohne dass der betreffende Bereich deaktiviert werden muss.

8.6. Systemfehler

Ein Fehler ist ein Warnsignal des Systems, das einen unnormalen Status der Zentrale, der Kommunikation oder der Geräte anzeigt. Das Problem kann in Verbindung mit der Funkverbindung, dem zusätzlichen GSM-Modul oder dem LAN-Übertragungsgerät, der Maskierung der Melder (mit einer Antimaskierungsfunktion), Stromproblemen (Netzstrom oder Batterie) oder der Backup-Stromversorgung stehen. Fehler werden optisch auf den Systemtastaturen durch die hintergrundbeleuchtete Anzeigentaste angezeigt. Fehler werden von allen Quellen gemeldet. Mit der vierten Fehlermeldung einer entsprechenden Komponente wird der Bypass der Quelle aktiviert, was bedeutet, dass der vierte Fehler nicht gemeldet wird. Diese automatisierte Fehlersperrung ist ein optionaler Parameter, siehe Registerkarte Systemparameter. Bei Aktivierung werden die Fehler nicht gezählt und es gibt keine Einschränkung hinsichtlich der Meldung. Der Parameter ist nicht verfügbar, wenn das Systemprofil „Standard“ eingestellt wurde.

In der folgenden Tabelle sehen Sie einen Überblick der allgemeinen Systemfehler:

Fehlerquelle	Ursache
Zentrale	Der Netzstrom ist für mehr als 30 Minuten nicht angeschlossen
	Fehlerhafte oder schwache Backup-Batterie in der Zentrale
Übertragungsgerät	Verlust der LAN-Verbindung, Verlust des GSM-Signals oder Fehler der PSTN-Leitung für mindestens 15 Minuten
	Nicht gesendete Ereignisse in einer vorgegebenen Zeit an eine eingestellte Leitstelle (AES)
Funkmodul	Störung des Funkbereichs 868 MHz
	BUS-Kommunikationsverlust
Tastaturen	Funk- oder BUS-Kommunikationsverlust (siehe Kapitel 8.7 Durch einen Geräteverlust verursachter Fehler)
Sirenen	
Module	
Melder	
	Maskierung der Bewegungsmelder (Antimaskierung) Interner Melderfehler (Gasaustrittsmelder) Fehler durch Verringerung der IR-Strahlenintensität (Infrarot-Barriere)

8.7. Durch einen Geräteverlust verursachter Fehler

Jedes Gerät (BUS oder drahtlos) im System wird durch die Zentrale kontrolliert. Wenn die Steuerungsparameter aktiviert sind (siehe Registerkarte Systemparameter) und ein Kommunikationsverlust mit der Zentrale besteht (keine Reaktion innerhalb einer vordefinierten Zeit), löst das System das Ereignis „Fehleraktivierung“ aus und meldet entsprechend „Verlust eines BUS-Geräts“. Daraufhin kann ein Sabotagealarm folgen. Dies ist optional und kann ausgelöst werden, wenn das Funkmodul eine RF-Störung erkennt, die mindestens 30 Sek. auf den im Funkmodul eingestellten Erkennungsstufen anhält. Ein Sabotagealarm kann auch bei einem Kurzschluss im BUS-Gerät ausgelöst werden, was die korrekte Kommunikation der BUS-Geräte verhindert. Die Unterbrechung der Kommunikation hat ein festgelegtes Zeitfenster und kann nicht geändert werden. Für BUS-Geräte beträgt dies 8 Sek. und für drahtlose Geräte 120 Min. nach der letzten Kommunikation.

Die Funktion **“Supervision - Funküberwachung”** ist optional für fast alle drahtlosen Geräte, die zur Überwachung dienen (Melder, Sirenen, Tastaturen), für einige von ihnen ist sie komplett deaktiviert (Fernsteuerungen und Automatisierungsvorrichtungen) und für einige BUS-Geräte ist sie z.B. immer aktiviert ohne dass sie deaktiviert werden kann.

Eine Option, die die Reaktion der Zentrale auf einen Verlust der BUS-Geräte ändert, heisst **„Verbindungsverlust einer Buskomponente“**, siehe F-Link, Registerkarte Systemparameter. Diese bietet die folgenden Optionen:

- **Störung** – die Zentrale verarbeitet den Verlust eines BUS-Geräts oder einen BUS-Kurzschluss als einen Fehler.
- **Immer Sabotage** – die Zentrale verarbeitet immer den Verlust eines BUS-Geräts oder einen BUS-Kurzschluss als Sabotagealarm. Wenn ein Funkmodul die Erkennung einer RF-Störung ermöglicht und diese wirklich erkannt wird, wird ein Sabotagealarm ausgelöst. Einem Sabotagealarm folgt ein Fehler und wenn der Fehler nicht mehr auftritt, wird der Sabotagealarm auch beendet.
- **Sabotage nach Bestätigung** – die Zentrale verarbeitet den Verlust des ersten Geräts als einen Fehler und wenn innerhalb einer vordefinierten Zeit, die durch den Parameter „Wartezeit auf eine Alarmbestätigung“ vorgegeben ist, ein weiterer Geräteverlust auftritt, bestätigt es das System und löst einen Sabotagealarm aus. Sobald der Fehler aller Geräteverluste behoben ist, beendet das System den Fehler und den Sabotagealarm.

9. Optionen der Systemsteuerung

Das Sicherheitssystem kann auf unterschiedliche Arten gesteuert werden. Grundsätzlich gibt es die ferngesteuerten oder lokalen Optionen. Weitere Optionen finden Sie in der folgenden Tabelle:

Art	Weg/Modus	Gerät	Bedingung	Steuerungsbeschreibung
Lokal	Tastatur mit Segmenten	JA-114E, JA-113E, JA-154E, JA-153E, JA-123E	Das Funkmodul JA-11xR für drahtlose Geräte	Die Bedienung kann nach der Benutzerberechtigung und dem Drücken eines bestimmten Steuerungs-bereichs (Segment) oder auch über das Menü der LCD-Tastatur erfolgen.
	Tastatur	JA-110E, JA-150E	Das Funkmodul JA-11xR für drahtlose Geräte	Die Bedienung kann nach der Benutzerberechtigung und dem Drücken einer bestimmten Funktions-taste oder auch über die LCD-Tastatur durchgeführt werden.
	RFID-Leser mit Steuerungsbereich	JA-112E, JA-152E; JA-122E (nur PC-Steuerung)	Das Funkmodul JA-11xR für drahtlose Geräte	Die Bedienung kann nach der Benutzerberechtigung mit einem RFID-Tag und Drücken eines bestimmten Steuerungsbereichs (Segment) durchgeführt werden.
	Fernsteuerung durch Fernbedienungen	JA-15xJ, JA-16xJ, JA-18xJ	Das Funkmodul JA-11xR für drahtlose Geräte	Ein- und Ausschalten durch Drücken einer voreingestellten Fern-steuerungstaste.
	Kalender und Zeitschaltuhren	Bis zu 64 Zeitschaltuhr-funktionen		Jede Zeitschaltuhraktion verfügt über Optionen, die ausgewählt werden können: Ereignis, Zeitpunkt der Durchführung, Wochentag. Bereiche und PG-Ausgänge können gesteuert und PG-Ausgänge gesperrt werden.
	J-Link (F-Link)	PC mit Windows	USB-Kabel	Bereiche und PG-Ausgänge können nach Berechtigung gesteuert werden.
	Steuermodul	JA-111H-AD TRB und JA-121T	BUS	Das System kann über ein beliebiges externes Gerät gesteuert werden (über eine kabelgebundene modulare Eingangs- oder Datenkommunikation).
Fern-gesteuert	Sprachmenü	Telefon	GSM-Wähl- & Übertragungsgerät	Aufruf der Systemtelefonnummer und Steuerung durch DTMF-Töne nach Berechtigung.
	SMS-Nachricht	Mobiltelefon	GSM-Wähl- & Übertragungsgerät	Berechtigter Befehl zur Scharf- und Unscharfschaltung von Bereichen und Steuerung von PG-Ausgängen.
	Einwahl von einer berechtigten Telefonnummer	Telefon (nur PG-Steuerung)	GSM-Wähl- & Übertragungsgerät	Jede berechtigte Telefonnummer kann einen spezifischen PG-Ausgang steuern.
	MyJABLOTRON webbasierte App	PC	Sicherheits-SIM-Karte im GSM-GSM-Wähl- & Übertragungsgerät von JABLOTRON	Nach der Berechtigung können Bereiche und PG-Ausgänge gesteuert, Fotos und Videos von entsprechenden Geräten aufgenommen und Thermometer und Stromzähler durchsucht werden.
	MyJABLOTRON Smartphone-App	Smartphone oder Tablet	Sicherheits-SIM-Karte im GSM-Wähl- & Übertragungsgerät von JABLOTRON	Nach der Berechtigung können Bereiche und PG-Ausgänge gesteuert, Fotos von Fotogeräten aufgenommen und Thermometer und Stromzähler durchsucht werden.
	J-Link (F-Link)	PC mit Windows	GSM- oder LAN-GSM-Wähl- & Übertragungsgerät	Bereiche und PG-Ausgänge können von einer virtuellen Tastatur gesteuert werden.

Alle genannten Möglichkeiten können für die Systemsteuerung (Scharfschaltung, Teilscharfschaltung, Unscharfschaltung) für die PG-Ausgangssteuerung (EIN, AUS, Zeitsteuerung) verwendet werden. Die einzigen Ausnahmen sind die RFIS-Leser JA-122E für den Außenbereich und das Einwählen von einer berechtigten Telefonnummer, die einen PG-Ausgang steuern kann.

9.1. Berechtigungsarten

Die Berechtigung ist ein Schlüsselfaktor, um das System zu steuern und zu verifizieren, ob ein Benutzer wirklich berechtigt für eine Bedienung ist. Je nach Berechtigungsverfahren entscheidet das System, ob der Benutzer zur Scharf- oder Unscharfschaltung eines Bereichs oder dem An- und Ausschalten eines PG-Ausgangs berechtigt ist, oder ob er den Systemstatus und den Hintergrundspeicher über das LCD-Tastaturmenü durchsuchen kann. Jedem Benutzer können zur Berechtigung die folgenden Optionen zugewiesen werden:

- Zugriffscode (4-, 6-, oder 8-stellige Nummer mit oder ohne einem Präfix).
- RFID-Karte/Tag (bis zu 2 Positionen für RFID-Identifikationselemente).
- Telefonnummer für die Berechtigung bei einem Fernzugriffs per Anruf oder SMS

Zur Anpassung der Sicherheitsstufe kann die Berechtigungsstufe auf die folgenden 3 Stufen voreingestellt werden:

1. **Standard** – Berechtigung wird über die Verwendung einer RFID-Karte/Tag oder über die Eingabe eines gültigen Zugriffscode durchgeführt
1. **Code nach Kartenbestätigung** – ein Benutzercode, der durch eine RFID-Karte bestätigt wird, muss angewendet werden (ihre Reihenfolge spielt keine Rolle). Wenn Benutzer Karten oder Codes haben, berechtigen sie sich selbst entsprechend der Option Standard, so dass die Berechtigung durch eine Person ausreicht. Wenn die Berechtigung per Fernzugriff durchgeführt wird, wird zuerst die Telefonnummer verifiziert. Als Bestätigung ist dann die Eingabe eines gültigen Zugriffscode obligatorisch. In diesem Fall kann die doppelte Berechtigung für einige Benutzer mit einer höheren Überwachungsebene verwendet werden, während für einige Benutzer nur eine Standardberechtigung erforderlich sein kann.
2. **Doppelte Autorisierung** – Die Eingabe eines Benutzercode und die Verwendung einer RFID-Karte führt zu einer gültigen Berechtigung (unabhängig von der Reihenfolge der Berechtigung). Während des Fernzugriffs wird die Telefonnummer immer verifiziert und ein gültiger Zugriffscode eingegeben. F-Link überwacht, ob einem Benutzer in der Registerkarte Benutzer ein Code und eine Karte zugewiesen wurden (andernfalls kann F-Link die Konfiguration nicht speichern).

Vorsicht: Die Bestätigung eines Benutzercode über eine RFID-Karte verringert das Risiko der unbefugten Bedienung durch Dritte.

9.2. Systemsteuerung über das Bedienteil

9.2.1. Systemsteuerung von Bedienteilen mit Segmenten

Der beste Weg, ein Sicherheitssystem und seine Überwachung zu steuern, ist die Verwendung einer Systemtastatur, wo Fehler und Alarmer dank einer farbigen LED-Anzeige der Hauptsteuertaste überprüft werden können. Der Status von Bereichen sowie PG-Ausgänge können mit anderen Steuerbereichen gesteuert werden, ebenso wie Systemoptionen wie die Alarmspeicheranzeige, die Auslösung eines Geiselnahmealarms oder eines Alarms bei gesundheitlichen Problemen. Über eine LCD-Tastatur können Sie im internen Menü nach Fehlern, Ereignissen, aktiven oder umgeleiteten Meldern oder Meldern, die die Scharfschaltung des Systems verhindern suchen - alles nach einer bestimmten Berechtigung. Keine Berechtigung = kein Zugriff auf das Menü der Tastatur. Entsprechend den Einstellungen der einzelnen Tastatureinstellungen kann die Sichtbarkeit bestimmter Segmente unterdrückt werden und das System vor unbefugter Bedienung geschützt werden.

Die Scharf- und Unscharfschaltung der Bereiche ist eine grundlegende Funktion der Systemtastatur. Das System kann vollständig oder teilweise scharf geschaltet und über das Menü der LCD-Tastatur oder über Steuerungsbereiche (Segmente) gesteuert werden. Mithilfe von Bereichen (Segmenten) können Sie Scharfschaltungen entsprechend ihrer Einstellungen vornehmen, nämlich vollständig oder teilweise und mit Berechtigung (wer die Scharfschaltung eines bestimmten Bereichs durchgeführt hat, wird im Ereignisprotokoll aufgezeichnet) oder auch ohne diese (kein Code erforderlich und im Ereignisprotokoll wird nicht angegeben, wer das System scharf geschaltet hat). Die Unscharfschaltung des Systems erfordert immer eine Berechtigung, daher wird im Ereignisprotokoll aufgezeichnet, wer das System unscharf geschaltet hat.

Die Scharfschaltung kann auf zwei Arten durchgeführt werden:

1. Vollständige Scharfschaltung des Bereichs bevor Sie das überwachte Gebäude verlassen (niemand ist im Gebäude):

Bei der Systemsteuerung von der Tastatur aus, die sich in den überwachten Räumen befindet, muss man gewährleisten, dass es einen Ausgangs- und Eingangsweg gibt, der von Meldern mit einer verzögerten Reaktion geschützt ist. Verzögerungs- und Nächste-Verzögerungs-Zonen werden nicht unmittelbar nach Scharfschaltung des Bereichs überwacht, aber Zonen mit einer Sofort-Reaktion schon. Der Benutzer muss in der Lage sein, die überwachten Räumlichkeiten nach der Scharfschaltung des Systems verlassen zu können, bevor die Zeit der Ausgangsverzögerung abläuft. Wenn die Eingangsverzögerung durch eine Verzögerungszone ausgelöst wird, muss der Benutzer in der Lage sein, durch den Eingangsweg zur Tastatur gehen zu können, von der aus das System unscharf geschaltet wird. Wenn der Benutzer den Bereich nicht rechtzeitig unscharf schaltet (Eingangszeit abgelaufen), löst das System einen Alarm in der verzögerten Zone aus. Wenn das Eindringen von einem anderen Weg als dem Eingangsweg erfolgt, löst das System einen Alarm in einer Sofort-Zone aus - die Sirene wird sofort aktiviert. Ein vollständig scharf geschaltetes/r System / Bereich wird durch einen roten Steuerungsbereich oder durch ein vollständiges Quadrat mit der Nummer des Bereichs auf der LCD-Tastatur angezeigt.

2. Teilscharfschaltung, Benutzer bleibt im Gebäude:

Wenn das System teilweise scharf geschaltet ist, bleibt der Benutzer in den überwachten Räumen und nur der Perimeterschutz ist für die Bewachung vorgesehen (er stellt die freie Bewegung innerhalb des Gebäudes sicher). Es gibt 2 Steuerungsvarianten:

- a) Steuerung über eine Tastatur, die innerhalb des überwachten Gebäudes mit Perimeterschutz (Eingangshalle usw.) angebracht ist. Alle Melder in der Eingangshalle müssen auf eine Verzögerungsreaktion voreingestellt werden, um sicherzustellen, dass ihre Aktivierung bei Scharfschaltung des Systems so viel Zeit lässt, dass das System unscharf geschaltet werden kann.
- b) Steuerung von einer Tastatur aus, die außerhalb der überwachten Räumlichkeiten mit Perimeterschutz (Innenhalle, Treppe, Schlafzimmer usw.) platziert ist. Diese Variante erlaubt nicht den Eintritt einer Person ohne sofortige Alarmauslösung. Die Räumlichkeiten können vorher per Fernbedienung, per Sprachmenü, per SMS oder über die MyJABLOTRON-App unscharf geschaltet werden. Die Melder sind in diesem Fall auf eine Sofort / Verzögerung A-Reaktion voreingestellt.

Die teilweise Scharfschaltung wird durch eine gelbe Farbe auf dem Bereich (Segment) oder durch ein Viereck um die Ziffer auf dem LCD-Tastaturdisplay angezeigt.

Systemsteuerung durch die Tastatur – Vorgehensweise:

Das System bietet ein paar Systemprofile, die den Anforderungen verschiedener Normen entsprechen. Das verändert das Verhalten der Tastatur und natürlich auch die methodische Steuerung. Das System kann auf zwei Arten gesteuert werden:

1. Variante 1 der Systemsteuerung (gültig für alle Profile)

Scharfschaltung des Systems:

Variante 1 erfordert zuerst Ihre Berechtigung, denn der Status ist nicht bei allen Bereichen (Segmenten) sichtbar, weil nicht alle Bereiche (Segmente) ihren Status entsprechend ihren Einstellungen ohne Berechtigung anzeigen müssen!

1. Bei der Verwendung der RFID-Karte / des Tags oder bei der Eingabe des Codes wird eine Berechtigung durchgeführt (wenn sowohl ein Code als auch eine Karte benötigt werden, ist ihre Reihenfolge nicht von Bedeutung).
2. Ein unscharfer Bereich wird durch eine grüne LED auf der linken Seite des Bereichs (Segments) angezeigt.
3. Wenn Sie die rote Segmenttaste auf der rechten Seite drücken, wird die Scharfschaltung des Bereichs angefordert. Unter Berücksichtigung der Anzahl der verwendeten Bereiche (Segmente) können mehrere Anfragen ausgewählt werden.
4. Wenn nach einer Auswahl die rote oder gelbe LED blinkt (8 Sek.), erkennt das System ein Hindernis, das die Scharfschaltung verhindert (siehe Kapitel 9.11 Hindernisse, die die Scharfschaltung des Systems verhindern).
5. Eine erfolgreiche Scharfschaltung oder teilweise Scharfschaltung wird durch eine rote oder gelbe Segment-LED angezeigt.

Unscharfschaltung des Systems:

Die Berechtigung ist erforderlich, um das System von einer Tastatur aus für Variante 1 zu steuern!

1. Bei der Verwendung der RFID-Karte / des Tags oder bei der Eingabe des Codes wird eine Berechtigung durchgeführt (wenn sowohl ein Code als auch eine Karte benötigt werden, ist ihre Reihenfolge nicht von Bedeutung).
2. Ein scharf geschalteter Bereich wird durch eine rote oder gelbe LED auf der rechten Seite des Segments angezeigt. Wenn ein Eindringen in die überwachten Räumlichkeiten erkannt wird, löst dies eine Eingangsverzögerung aus, die durch schnelles Blinken der grünen LED angezeigt wird.
3. Das Drücken der grünen Taste (oder verschiedener Tasten nach und nach) auf der linken Seite fordert die Unscharfschaltung des Bereichs an.
4. Die erfolgreiche Unscharfschaltung wird durch eine grüne Segment-LED bestätigt.
5. Wenn die rote LED nach Unscharfschaltung des Bereichs schnell blinkt, zeigt dies den Alarmspeicher des Bereichs an. Das Abbrechen dieser Anzeige erfolgt durch weiteres Drücken der grünen Segmenttaste zusammen mit der Berechtigung oder indem man auf der LCD-Tastatur die Option „Warnmeldung abbrechen“ auswählt.

2. Variante 2 der Systemsteuerung („Standard“ Profil)

Scharfschaltung des Systems:

Die Art der Steuerung basiert auf der Vorgehensweise: „Wählen Sie die gewünschte Aktion aus und berechtigen Sie sich selbst“.

1. Ein unscharfer Bereich wird durch eine grüne LED auf der linken Seite des Segments angezeigt.
2. Wenn Sie die rote Segmenttaste auf der rechten Seite drücken, wird eine Scharfschaltung eines Bereichs angefordert. Unter Berücksichtigung der Anzahl der verwendeten Bereiche können mehrere Anfragen ausgewählt werden.
3. Wenn die Berechtigung zur Scharfschaltung des Systems erforderlich ist, zeigt eine rote (vollständige Scharfschaltung) oder gelbe (teilweise Scharfschaltung) LED durch langsames Blinken den Ablauf des Zeitraums an, in dem die Berechtigung erwartet wird (8 Sek.).
4. Bei der Verwendung der RFID-Karte / des Tags oder bei der Eingabe des Codes wird eine Berechtigung durchgeführt (wenn sowohl ein Code als auch eine Karte benötigt werden, ist ihre Reihenfolge nicht von Bedeutung).
5. Wenn die rote oder gelbe LED nach einer Auswahl weiterhin blinkt (8 Sek.), erkennt das System ein Hindernis, das die Scharfschaltung verhindert (siehe Kapitel 9.11 Hindernisse, die die Scharfschaltung des Systems verhindern).
6. Eine erfolgreiche Scharfschaltung oder teilweise Scharfschaltung wird durch eine rote oder gelbe Segment-LED angezeigt.

Unscharfschaltung des Systems:

1. Ein scharf geschalteter Bereich wird durch eine rote oder gelbe LED auf der rechten Seite des Segments angezeigt. Wenn ein Eindringen in die überwachten Räumlichkeiten erkannt wird, löst dies eine Eingangsverzögerung aus, die durch schnelles Blinken der spezifischen LED angezeigt wird.
2. Das Drücken der grünen Taste (oder verschiedener Tasten nach und nach) auf der linken Seite fordert die Unscharfschaltung des Bereichs an. Das Segment zeigt durch langsames Blinken den Ablauf der Zeit an, in dem die Berechtigung erwartet wird.
3. Bei der Verwendung der RFID-Karte / des Tags oder bei der Eingabe des Codes wird eine Berechtigung durchgeführt (wenn sowohl ein Code als auch eine Karte benötigt werden, ist ihre Reihenfolge nicht von Bedeutung).
4. Die erfolgreiche Unscharfschaltung wird durch eine grün leuchtende Segment-LED angezeigt.
5. Wenn die rote LED nach Unscharfschaltung des Bereichs schnell blinkt, zeigt dies den Alarmspeicher des Bereichs an. Das Abbrechen dieser Anzeige erfolgt durch weiteres Drücken der grünen Segmenttaste zusammen mit der Berechtigung oder indem man auf der LCD-Tastatur die Option „Warnmeldung abbrechen“ auswählt.

9.2.2. Systemsteuerung mit den Bedienteilen JA-110E und JA-150E

Der beste Weg, ein Sicherheitssystem und seine Überwachung zu steuern, ist die Verwendung einer Systemtastatur, wo dank einer farbigen LED-Systemstatusanzeige der Hauptsteuertaste Fehler und Alarme überprüft werden können. Andere Funktionstasten steuern den Status von Bereichen sowie PG-Ausgänge, ebenso wie Systemoptionen wie die Alarmspeicheranzeige, das Auslösen eines Geiselnahmealarms oder eines

Alarms bei gesundheitlichen Problemen. Mit Hilfe einer Tastatur können Sie im internen Menü nach Fehlern, Ereignissen, aktiven oder umgeleiteten Meldern oder Meldern, die die Systemeinstellung verhindern, suchen - alles nach einer Berechtigung. Keine Berechtigung = kein Zugriff auf das Tastaturmenü. Entsprechend der individuellen Tastatureinstellungen kann die Sichtbarkeit von Menüpunkten unterdrückt und das System vor unbefugter Bedienung geschützt werden.

Die Scharf- und Unscharfschaltung der Bereiche ist eine grundlegende Funktion der Systemtastatur. Das System kann vollständig oder teilweise scharf geschaltet werden. Die Steuerung kann bequem auf verschiedene Arten durchgeführt werden:

1. Durch Funktionstasten – das Drücken der Tasten kann vollständig oder nur teilweise oder teilweise und vollständig scharf schalten. Der Scharfschaltung folgt die Berechtigung (im Verlauf wird aufgezeichnet, wer den Bereich scharf geschaltet hat). Sie kann auch ohne Berechtigung erfolgen (es wird kein Code angefordert und im Verlauf wird nicht spezifiziert, wer den Bereich scharf geschaltet hat). Bei Unscharfschaltung des Systems über die Funktionstasten ist immer die Berechtigung erforderlich, entsprechend wird im Speicher der Zentrale verzeichnet, wer die Unscharfschaltung durchgeführt hat.
2. Vom Tastaturmenü aus – drücken Sie die “*” Taste nach der Berechtigung und schalten Sie teilweise oder vollständig scharf oder unscharf.
3. Nur über die Berechtigung – bei der Einstellung über die Berechtigung kann (nur) vollständig scharf und unscharf geschaltet werden, indem die Berechtigung über einen Code oder die RFID-Karte/Tag erfolgt. Um in das Tastaturmenü zu gelangen, drücken Sie die Taste “*” bevor Sie sich selbst berechtigen.

Vorgehensweise der Scharfschaltung:

1. Vollständige Scharfschaltung des Bereichs vor dem Verlassen des überwachten Gebäudes (niemand sonst in den Räumlichkeiten):

Ein vollständig scharf geschaltetes System wird durch eine rote Funktionstaste oder eine vollständig hervorgehobene Zahl des Bereichs auf dem LCD-Display der Tastatur während der Steuerung über das Menü angezeigt.

Bei der Systemsteuerung von der Tastatur aus, die sich in den überwachten Räumen befindet, muss man gewährleisten, dass es einen Ausgangs- und Eingangsweg gibt, der von Meldern mit einer verzögerten Reaktion geschützt ist. Verzögerungs- und Nächste-Verzögerungs-Zonen werden nicht unmittelbar nach Scharfschaltung des Bereichs überwacht, aber Zonen mit einer Sofort-Reaktion schon. Der Benutzer muss in der Lage sein, die überwachten Räumlichkeiten nach der Scharfschaltung des Systems verlassen zu können, bevor die Zeit der Ausgangsverzögerung abläuft. Wenn die Eingangsverzögerung durch eine Verzögerungszone ausgelöst wird, muss der Benutzer in der Lage sein, durch den Eingangsweg zur Tastatur gehen zu können, von der aus das System unscharf geschaltet wird. Wenn der Benutzer den Bereich nicht rechtzeitig unscharf schaltet (Eingangszeit abgelaufen), löst das System einen Alarm in der verzögerten Zone aus. Wenn das Eindringen von einem anderen Weg als dem Eingangsweg erfolgt, löst das System einen Alarm in einer Sofort-Zone aus - die Sirene wird sofort aktiviert.

2. Teilscharfschaltung, Benutzer bleibt im Gebäude:

Ein teilweise scharf geschaltetes System wird durch eine gelbe Funktionstaste oder eine vollständig hervorgehobene Zahl des Bereichs auf dem LCD-Display der Tastatur während der Steuerung über das Menü angezeigt.

Wenn das System teilweise scharf geschaltet ist, bleibt der Benutzer in den überwachten Räumen und nur der Perimeterschutz ist für die Bewachung vorgesehen (er stellt die freie Bewegung innerhalb des Gebäudes sicher). Es gibt 2 Steuerungsvarianten:

1. Steuerung über eine Tastatur, die innerhalb des überwachten Gebäudes mit Perimeterschutz (Eingangshalle usw.) angebracht ist. Alle Melder in der Eingangshalle müssen auf eine Verzögerungsreaktion voreingestellt werden, um sicherzustellen, dass ihre Aktivierung bei Scharfschaltung des Systems so viel Zeit lässt, dass das System unscharf geschaltet werden kann.
2. Steuerung von einer Tastatur aus, die außerhalb der überwachten Räumlichkeiten mit Perimeterschutz (Innenhalle, Treppe, Schlafzimmer usw.) platziert ist. Diese Variante erlaubt nicht den Eintritt einer Person ohne sofortige Alarmauslösung. Die Räumlichkeiten können vorher per Fernsteuerung unscharf geschaltet werden, sofern ein zusätzliches GSM-Modul verbunden ist, auch über das Sprachmenü oder per SMS. Die Melder sind in diesem Fall auf eine Sofort / Verzögerung voreingestellt.

Systemsteuerung über die Tastatur - Vorgehensweise:

Das System bietet ein paar Systemprofile, die den Anforderungen verschiedener Normen entsprechen, was auch das Verhalten der Tastatur und natürlich die methodische Steuerung verändert.

Scharfschaltung des Systems:

1. Ein unscharfer Bereich wird durch eine grün leuchtende Funktionstaste angezeigt.
2. Wenn Sie die Funktionstaste drücken, wird eine Scharfschaltung eines Bereichs angefordert. Weitere Anfragen können unter Berücksichtigung der Anzahl der verwendeten Funktionstasten ausgewählt werden.
3. Wenn die Berechtigung zur Scharfschaltung des Systems erforderlich ist, zeigt die rote (vollständige Scharfschaltung) oder gelbe (teilweise Scharfschaltung) langsam blinkende Funktionstaste den Ablauf des Zeitraums an, in dem die Berechtigung erwartet wird (8 Sek.).
4. Bei der Verwendung der RFID-Karte / des Tags oder bei der Eingabe des Codes wird eine Berechtigung durchgeführt (wenn sowohl ein Code als auch eine Karte benötigt werden, ist ihre Reihenfolge nicht von Bedeutung).
5. Wenn die rote oder gelbe Funktionstaste nach einer Auswahl weiterhin blinkt (8 Sek.), erkennt das System ein Hindernis, das die Scharfschaltung verhindert (siehe Kapitel 9.11 Hindernisse, die die Scharfschaltung des Systems verhindern).
6. Eine erfolgreiche Scharfschaltung oder teilweise Scharfschaltung wird durch eine dauerhaft leuchtende rote oder gelbe Funktionstaste angezeigt.

Unscharfschaltung des Systems:

1. Ein scharf geschalteter Bereich wird durch eine rote oder gelbe leuchtende Funktionstaste angezeigt. Wenn ein Eindringen in die überwachten Räumlichkeiten erkannt wird, löst dies eine Eingangsverzögerung aus, die durch schnelles Blinken der spezifischen Funktionstaste angezeigt wird.
2. Das Drücken der gewünschten Funktionstaste (oder verschiedener Tasten nach und nach) fordert die Unscharfschaltung des Bereichs an und die Funktionstaste zeigt durch langsames Blinken an, dass die Berechtigung erwartet wird.
3. Bei der Verwendung der RFID-Karte / des Tags oder bei Eingabe des Codes wird eine Berechtigung durchgeführt (wenn sowohl ein Code als auch eine Karte benötigt werden, ist ihre Reihenfolge nicht von Bedeutung).
4. Die erfolgreiche Unscharfschaltung wird durch eine grün leuchtende Funktionstaste angezeigt.
5. Wenn die rote Funktionstaste nach Unscharfschaltung des Bereichs schnell blinkt, zeigt dies den Alarmspeicher des Bereichs an. Das Abbrechen dieser Anzeige erfolgt durch weiteres Drücken dieser Taste zusammen mit der Berechtigung oder indem man auf der LCD-Tastatur die Option „Warnmeldung abbrechen“ auswählt.

Hintergrundbeleuchtete Anzeigentasten auf der Tastatur – Statusüberblick:

Taste leuchtet grün EIN	Normaler Betrieb. Von der Tastatur gesteuerte Bereiche sind OK und ohne Fehler.
Taste leuchtet gelb EIN	Normaler Betrieb und in einiger der gesteuerten Bereiche wurde ein Fehler gemeldet. Mehr Informationen dazu finden Sie je nach individuellem Zugriffsrecht nach der Berechtigung im LCD-Tastaturmenü. Wenn der Fehler von einem sich auf der LCD-Tastatur drehenden JABLOTRON-Logo gefolgt wird, handelt es sich um einen Fehler der Funkkommunikation zwischen der Zentrale und der Tastatur.
Taste leuchtet rot EIN	Tastatur im BOOT-Modus, während einer FW-Aktualisierung.
Taste blinkt grün (2 Hz)	Berechtigung durchgeführt, der Benutzer kann den Systemstatus vom Segment aus ändern oder das LCD-Tastaturmenü durchsuchen. Die Berechtigung muss nun innerhalb von 8 Sek. erfolgen oder über die ESC beendet werden.
Taste blinkt gelb (8 Hz)	Warnanzeige einer fehlgeschlagenen Scharfschaltung
Taste blinkt rot (8 Hz)	Anzeige eines aktuell ausgelösten Alarms in einem spezifischen Bereich auf der Tastatur. Die Alarmart, der Name des Bereichs, in dem ein Alarm ausgelöst wurde und die Quelle des ausgelösten Alarms sind auf der LCD-Tastatur zu sehen.
Blinkt abwechselnd rot/gelb	Ausgelöster Alarm mit einem aktiven Fehler
Blinkt abwechselnd grün/rot	Berechtigung mit einem gerade ausgelösten Alarm oder einem Alarmspeicher.
Blinkt abwechselnd grün/gelb	Berechtigung mit einem aktiven Fehler

Taste blinkt gelb (2x alle 2 Sek.)	Programmierung / Errichter-Modus. Alle Steuerungsbereiche sind für die Benutzer nicht verfügbar, ebenso wie das Tastaturmenü des Administrators. Das Tastaturmenü ist nur für den Errichter verfügbar, bis der PC mit der Zentrale verbunden ist.
Taste blinkt rot (2x alle 2 Sek.)	Alarmspeicheranzeige
Taste blinkt grün (2x alle 2 Sek.)	Wartungsmodus. Die Anzeige der Steuerungsbereiche (Segmente) für die Bereiche, die in den Wartungsmodus geschaltet wurden, ist deaktiviert.
Taste blinkt gelb (1x alle 2 Sek.)	Fehleranzeige auf der Tastatur im Schlafmodus (gilt nur für die Profile EN50131-1)
Taste blinkt rot (1x alle 2 Sek.)	Alarmspeicheranzeige auf der Tastatur im Ruhemodus (gilt nur für die Profile EN50131-1).
Keine Anzeige	Tastatur in Ruhemodus

Überblick über die optische Anzeige des Steuerungsbereichs der Tastatur:

Bereich leuchtet grün	Bereichsstatus ist UNSCHARF oder der PG-Ausgang AUS.
Bereich blinkt grün (4 Hz)	Eingangsverzögerung läuft und das System wartet auf die Berechtigung, unscharf geschaltet zu werden.
Bereich leuchtet gelb	Bereichsstatus ist teilweise scharf.
Bereich leuchtet rot	Bereichsstatus ist SCHARF oder PG-Ausgang ist EIN.
Bereich blinkt gelb (4 Hz)	System erwartet eine Berechtigung bei teilweise Scharfschaltung oder es meldet einen Fehler bei der teilweisen Scharfschaltung.
Bereich blinkt gelb (8 Hz)	Warnanzeige einer fehlgeschlagenen Scharfschaltung
Bereich blinkt rot (4 Hz)	System wartet auf die Berechtigung während der Scharfschaltung oder es meldet ein Problem während der Scharfschaltung.
Bereich blinkt rot (8 Hz)	Alarmspeicheranzeige wird angezeigt, bis sie abgebrochen wird.
Bereich leuchtet gar nicht	Ausgeschaltet; Service- oder Wartungsmodus; oder gesperrter Bereich nach einem Alarm.

9.3. Systemsteuerung über eine Fernbedienung

Wenn das System vor Betreten des Gebäudes (Ankunft mit dem Auto in der Garage), das durch Melder mit einer sofortigen Reaktion überwacht wird, gesteuert werden muss, stellt es sicher, dass niemand das System von einer Tastatur im Inneren des Gebäudes aus unscharf schalten kann (kein Eingangsweg). Dies wird über eine Fernsteuerung vor Betreten des Gebäudes durchgeführt. Dazu wird ein Funkmodul JA-111R benötigt, das beim System für die Kommunikation mit einem drahtlosen Gerät angemeldet wird. Es muss an der richtigen Stelle platziert werden, um eine zuverlässige drahtlose Kommunikation in der entsprechenden Entfernung sicherzustellen.

Bei Verwendung von Fernsteuerungen (JA-15xJ, JA-16xJ) folgen die Tasten dem selben Verhalten wie die Steuerungsbereiche (Segmente) einer Tastatur. Jede Taste kann einen ausgewählten Bereich steuern (die rechte Taste schaltet immer scharf, die linke unscharf). Fernsteuerungen funktionieren nach den selben Regeln, wie ein System scharf geschaltet wird. Entsprechend wird das System eventuell nicht scharf geschaltet, wenn mögliche Hindernisse auftreten.

Steuerungsbereiche der Tastaturen und bidirektionale Fernbedienungen verfügen über die selbe Anzeigart einer dreifarbigem LED. Die Beschreibungen der individuellen Status werden in der folgenden Tabelle erklärt:

Statusanzeigen von bidirektionalen Fernbedienungen (JA-15xJ) – nachdem sie gedrückt wurden:

LED leuchtet	Bereichsstatus Unscharf oder PG-Ausgang AUS
LED leuchtet gelb	Bereichsstatus Teilscharf
LED leuchtet rot	Bereichsstatus Scharf oder PG-Ausgang EIN
LED blinkt rot	Es gibt ein Hindernis im Bereich, das die Scharfschaltung verhindert
LED blinkt gelb	Befehlsstatus unbekannt (Kommunikationsfehler, außerhalb des Kommunikationsbereichs usw.)

Bei der Verwendung einer unidirektionalen Fernbedienung (JA-16xJ, JA-18xJ) wird das System auf die selbe Weise gesteuert. Die LED zeigt an, dass die Taste betätigt und der Befehl gesendet wurde. Es gibt keine Rückmeldung von der Zentrale und der Benutzer muss eine andere Statusanzeige verwenden, um die Statusänderung zu bestätigen. Hierzu eignen sich piepende Sirenen, SMS oder optische Anzeigen, die die Scharfschaltung/Unscharfschaltung melden.

9.4. Systemsteuerung über den Kalender & Zeitschaltuhren

Die automatische Systemsteuerung kann über den internen Kalender der Zentrale durchgeführt werden. Es können bis zu 64 Zeitschaltuhraktionen, Bereiche und die Steuerung von PG-Ausgängen voreingestellt werden. Über den Kalender können Sie das genaue Datum der Service-Jahresprüfung auswählen, die unabhängig von der Option „Serviceanforderung“ in der Registerkarte Systemparameter ist.

Jede Aktion kann für Wochentage und Monate des Jahres voreingestellt werden. Eine Aktion kann daher von einem bestimmten Tag des Jahres bis zu einer regelmäßigen Wiederholung an bestimmten Tagen (z. B. wöchentlich oder monatlich) eingestellt werden. An den ausgewählten Tagen kann bis zu 4 Mal festgelegt werden, wann eine Zeitschaltuhraktion ausgeführt wird, oder es kann ausgewählt werden, dass sie in regelmäßigen Abständen wiederholt wird. Die Intervallwiederholung kann zusätzlich in einer Zeit von „von-bis“ angegeben werden. Eine typische Anwendung stellt die automatische Scharfschaltung eines Bereichs in Geschäften dar, die teilweise Scharfschaltung eines Gebäudes in der Nacht oder die Steuerung der Beleuchtung in der Nacht dar. Jedes automatische Ereignis wird im Verlaufsprotokoll mit dem Namen und der Quelle „Zeitschaltuhr“ eingetragen.

Überwachungsbezogene Steuerungsoptionen der Zeitschaltuhr:

Nur Unscharfschaltung	Den voreingestellten Bereich jeder Überwachungsstufe (vollständig oder teilweise scharf) unscharf schalten.
Teilscharfschalten	Diese Option schaltet die vordefinierten Bereiche teilweise scharf und beginnt mit dem Ausgangspiepen nach 180 Sek. (unabhängig davon, auf welche Zeit die Ausgangszeit in der Zentrale eingestellt ist). Innerhalb dieses Zeitraums verhalten sich alle Zonen wie eine Verzögerungszone. Diese verlängerte Zeit der Ausgangsanzeige dient dazu, Benutzer, die sich im überwachten Gebäude befinden, zu informieren, dass das System über einen automatischen Timer teilweise scharf geschaltet wurde. Eine teilweise Scharfschaltung wird normalerweise nicht akustisch angezeigt (siehe Registerkarte Systemparameter, um diese Funktion zu aktivieren). Die Zentrale respektiert alle Arten der Systemeinstellung und -überprüfung.
Scharf-schalten	Diese Option schaltet die vordefinierten Bereiche scharf und beginnt mit dem Ausgangspiepen nach 180 Sek. (unabhängig davon, auf welche Zeit die Ausgangszeit in der Zentrale eingestellt ist). Innerhalb dieses Zeitraums verhalten sich alle Zonen wie eine Verzögerungszone. Diese verlängerte Zeit der Ausgangsanzeige dient dazu, Benutzer, die sich im überwachten Gebäude befinden, zu informieren, dass das System über einen automatischen Timer scharf geschaltet wurde. Während dieses Zeitraums muss der Benutzer sofort den Bereich über die Systemtastatur wie üblich unscharf schalten oder das überwachte Gebäude verlassen. Wenn er dieses Warnsignal nicht beachtet und sich weiterhin im Gebäude bewegt, wird ein Alarm ausgelöst. Die Zentrale respektiert alle Arten der Systemeinstellung und -überprüfung.
Sofort scharf-schalten	Diese Option schaltet vordefinierte Bereiche sofort ohne Ausgangsverzögerung oder ein akustisches Warnsignal scharf. Das System ist sofort scharf geschaltet, sodass keine Bewegungen im Gebäude mehr möglich sind. Wenn sich jemand nach dieser automatischen Scharfschaltung noch im Gebäude bewegt, wird sofort ein Alarm in diesem Bereich ausgelöst. Diese Option dient zur schnellen und stillen Scharfschaltung ohne Warnanzeigen. Die Zentrale respektiert alle Arten der Systemeinstellung und -überprüfung.

Jetzt teilscharf-schalten	Diese Option schaltet vordefinierte Bereiche sofort ohne Verzögerung oder akustische Warnanzeige teilweise scharf. Das System wird sofort in der vordefinierten Zeit scharf geschaltet. Diese Option ist für eine schnelle und stille Scharfschaltung ohne Warnanzeige geeignet. Die Zentrale respektiert alle Arten der Systemeinstellung und -überprüfung.
Immer scharf-schalten	Diese Option schaltet die vordefinierten Bereiche scharf und beginnt mit dem Ausgangspiepen nach 180 Sek. (unabhängig davon, auf welche Zeit die Ausgangszeit in der Zentrale eingestellt ist). Innerhalb dieses Zeitraums verhalten sich alle Zonen wie eine Verzögerungszone. Die Zentrale respektiert alle Arten der Systemeinstellung und -überprüfung.
Immer teilscharf-schalten	Diese Option schaltet die vordefinierten Bereiche teilweise scharf und beginnt mit dem Ausgangspiepen nach 180Sek. (unabhängig davon, auf welche Zeit die Ausgangszeit in der Zentrale eingestellt ist). Innerhalb dieses Zeitraums verhalten sich alle Zonen wie eine Verzögerungszone. Die Zentrale respektiert alle Arten der Systemeinstellung und -überprüfung.
Immer sofort scharf-schalten	Diese Option schaltet vordefinierte Bereiche sofort ohne Verzögerung oder ein akustisches Warnsignal scharf. Das System ist sofort scharf geschaltet, sodass keine Bewegungen im Gebäude mehr möglich sind. Diese Option dient zur schnellen und stillen Scharfschaltung ohne Warnanzeigen. Die Zentrale respektiert alle Arten der Systemeinstellung und -überprüfung.
Immer und sofort teilscharf-schalten	Diese Option schaltet vordefinierte Bereiche sofort ohne Verzögerung oder akustische Warnanzeige teilweise scharf. Das System wird sofort in der vordefinierten Zeit scharf geschaltet. Diese Option ist für eine schnelle und stille Scharfschaltung ohne Warnanzeige geeignet. Die Zentrale respektiert alle Arten der Systemeinstellung und -überprüfung.
Nein	Keine vordefinierte Funktion.

PG-Ausgangssteuerung mit dem Kalender:

Aktivierung	Diese Option aktiviert programmierbare Ausgänge, wenn sie nicht gesperrt sind (z.B. durch die Kalenderfunktion, ein Gerät oder Bereich).
Deaktivierung	Diese Option deaktiviert programmierbare PG-Ausgänge
Blockierung	Diese Option sperrt vordefinierte PG-Ausgänge. Diese Ausgänge können nicht eingeschaltet werden, bis sie über die Kalenderfunktion „PG entsperren“ entsperrt werden. Den Errichter-Code eingeben und wieder verlassen führt das Entsperren nicht durch.
Entsperrung	Diese Option entsperrt vordefinierte gesperrte PG-Ausgänge.
Nein	Keine voreingestellte Sperrfunktion voreingestellt.
Technische Kontrolle	In einer voreingestellten Zeit wird das Ereignis „System fordert Service-Check an“ im System ausgelöst, das zusammen mit dem Informationssymbol auf den Tastaturen mit einem LCD-Bildschirm angezeigt wird.

Sperrung einer Aktion über die Zeitschaltuhr: Jede Zeitschaltuhraktion kann von einem ausgewählten PG-Ausgang gesperrt werden. Eine Sperrung bedeutet: Wenn ein PG-Ausgang aktiviert ist, kann eine spezifische Aktion zu einer vordefinierten Zeit nicht durchgeführt werden.

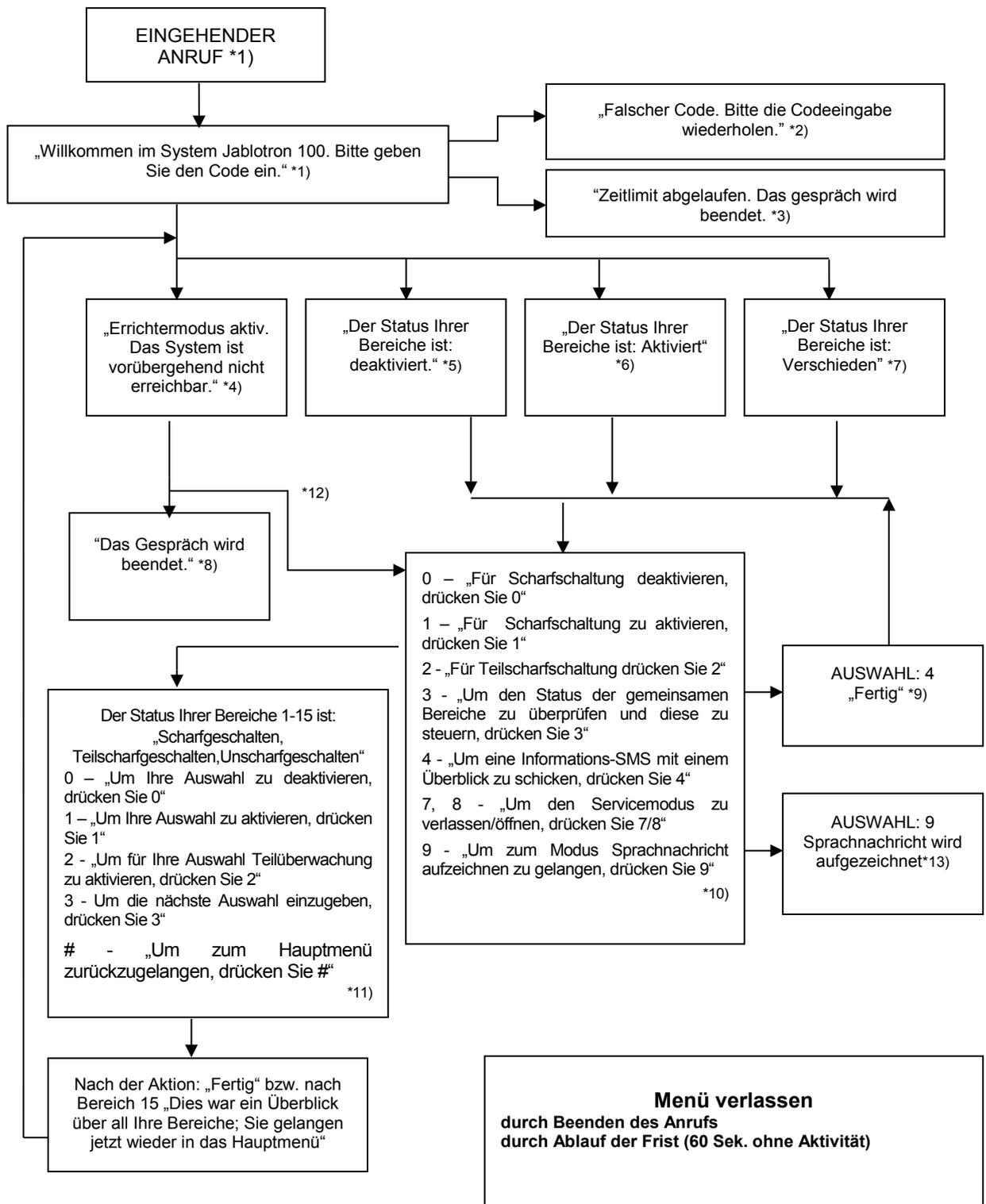
9.5. Systemsteuerung über das Sprachmenü des Wähl- & Übertragungsgerätes (GSM)

Wenn das GSM-Wähl- & Übertragungsgerät JA-19xY in der Zentrale installiert ist, kann das Sicherheitssystem dank des implementierten Sprachmenüs und der DTMF-Töne über das Handy des Anrufers ferngesteuert werden. Durch Anrufen der verwendeten SIM-Karten-Telefonnummer nimmt das System den Anruf nach einer voreingestellten Anzahl von Rufzeichen an (Standard ist 3 Rufzeichen). Die Zentrale spielt eine einführende Sprachnachricht ab und benötigt je nach Einstellung die Eingabe eines gültigen Codes. Der Anrufer muss sich über seinen Zugriffscode berechtigen. Bei erfolgreicher Verifizierung des Codes sagt das System den Status des gesamten Systems an und bietet je nach Berechtigung des Anrufers zusätzliche verfügbare Optionen an. Der Parameter „Freigabe von Sprachmenü und SMS Befehlen ohne zusätzlichen Code“ in der Registerkarte „Übertragungsgeräte“ erlaubt dem Benutzer die Berechtigung entsprechend einer in der Benutzerliste gespeicherten voreingestellten Telefonnummer, bei Aktivierung wird dann der Code nicht benötigt. Über das Sprachmenü können Bereiche gesteuert werden, der Servicecode (Errichter-Code) eingegeben und

verlassen werden, Sprachnachrichten mit den Namen der einzelnen Bereiche und spezielle Meldungen aufgenommen werden. Die Steuerung der PG-Ausgänge kann nicht über das Sprachmenü vorgenommen werden.

Vorsicht: Vergewissern Sie sich, dass sich niemand mehr im überwachten Gebäude befindet, bevor Sie das System per Fernsteuerung scharf schalten.

Überblick über das Sprachmenü:



- *1) Antwortet nach 3 Klingelimpulsen. Die Anzahl der Klingelimpulse bis zur Beantwortung (1.10) ist anpassbar in der Registerkarte Kommunikation und der Registerkarte des entsprechenden Kommunikators, wo der Zugriff zum Sprachmenü ohne Code erlaubt ist.
- *2) Falsche Codeeingabe. Nach der dritten falschen Codeeingabe wird der Anruf beendet.
- *3) Zeitlimit von 60 Sek. zur Codeeingabe. Alle 5 Sek. wird „Geben Sie den Code ein“ wiederholt.
- *4) Das Sprachmenü kann während des Service nicht verwendet werden.
- *5) Alle Bereiche, die über die Berechtigung gesteuert werden können, sind unscharf.

- *6) Alle Bereiche, die über die Berechtigung gesteuert werden können, sind scharf.
- *7) Alle Bereiche, die über die Berechtigung gesteuert werden können, haben unterschiedliche Status.
- *8) Gültig für alle Berechtigungen außer ARC / Service.
- *9) Nach Versendung einer INFO-SMS an die Nummer des Anrufers.
- *10) Irrelevante Menüpunkte werden übersprungen (z.B. wenn alles scharf geschaltet ist, ist die Auswahl 1,2,3 nicht anwendbar).
- *11) Das Menü passt sich dem aktuellen Bereichsstatus an.
- *12) Wenn ein Benutzer mit dem Errichter-Code berechtigt ist, ist die Auswahl 9 möglich - „Zur Aufnahme der Sprachnachricht, drücken Sie 9“
- *13) Modus zur Aufnahme von Sprachnachrichten **AUSWAHL 9:**
 - 0 – „Zur Aufnahme des Installationsnamens, drücken Sie 0.“ und dann „drücken Sie Stern (*).“
 - 1 – „Zur Aufnahme der Bereichsnamen, drücken Sie 1“, dann geben Sie die Nummer des Bereichs ein, den Sie aufnehmen möchten und dann „drücken Sie Stern (*).“
 - 2 (3, 4, 5) – „Um Nachrichten der Meldung A (B, C, D) aufzunehmen, drücken Sie 2 (3, 4, 5)“ und dann „drücken Sie den Stern (*).“
 - 9 – „Um alle aufgenommenen Nachrichten zu löschen, drücken Sie 9.“
 - # – „Um in das Hauptmenü zu gelangen, drücken Sie #“

Hinweise:

- 1 – „Sie sind für diese Auswahl nicht berechtigt“ – immer, wenn der Benutzer nicht für die Bedienung eines Bereichs oder für die Statusüberprüfung berechtigt ist
- 2 – „Erforderliche Meldung einer wichtigen Nachricht, der Anruf wird in 30 Sekunden beendet“ - meldet dem ARC wichtige Nachrichten, die höhere Priorität als als das laufende Sprachmenü haben.
- Die Eingabe in den Aufnahmemodus wird durch einen Piepton angezeigt. Eine aufgenommene Nachricht wird unmittelbar nach der Aufnahme noch einmal zum Hören abgespielt.
- Wenn Sie nicht mit der Aufnahme zufrieden sind, können Sie sofort Neuaufnahme wählen.
- Es wird empfohlen, sofort nach dem Piepton mit der Aufnahme zu beginnen und das Zeichen* direkt nach der Aufnahme zu drücken.
- Der Installationsname dauert maximal 40 Sek. Jede andere Nachricht dauert maximal 20 Sek.

9.6. SMS-Befehle

Die SMS-Befehle können dazu verwendet werden, um den Status individueller Bereiche einzustellen (Scharfschaltung / Unscharfschaltung) oder nur anzufragen, wie der Status der einzelnen Bereiche oder des gesamten Systems ist. PG-Ausgänge können auch per SMS-Befehl gesteuert werden. Es gibt keine werkseitigen Befehle zur Steuerung der PG-Ausgänge. Diese sollten zuerst eingestellt werden. Andere Texte sind bereits eingestellt. Die Befehlstexte können nicht geändert werden, außer der Befehle zur Steuerung der PG-Ausgänge.

Befehlsstruktur:

ppp*cccc_command

wo: **ppp** ist die Positionsnummer des Benutzercodes (nur bei einem Code mit Präfix);

* ist ein Trennzeichen (* nur bei einem Code mit Präfix);

cccc ist ein Benutzercode;

_ ist ein Leerzeichen;

command ist die Befehlsausführung (siehe Liste der Befehle unten).

Anfragenbefehle:

Informationen über den Systemstatus kann man unter Verwendung der folgenden Befehle bekommen;

DINFO, STATUS, COM and GSM

Steuerungsbefehl:

Die Steuerung der Einstellung des **Systems** als ganzes oder nur einzelner **Bereiche** wird über die folgenden Befehle durchgeführt:

SCHARF, UNSCHARF, oder SCHARF x x x, UNSCHARF x x x, wo x sind Nummern der Bereiche, die durch ein Leerzeichen getrennt sind.

Die Steuerungsbefehle für die Steuerung der **PG-Ausgänge** sind vom Hersteller voreingestellt **Ein PG-Ausgang**

x (x = 1 – 128).

Vorsicht: Wenn die Steuerungsbefehle diakritische Zeichen enthalten (wie in den Sprachen GR und RU), sollte der Parameter Diakritika in der Registerkarte Kommunikation für eine korrekte und zuverlässige Funktionsfähigkeit aktiviert werden. Es ist auch wichtig, kleine und große Buchstaben zu berücksichtigen, wenn Diakritika aktiviert sind. Bei normalen Zeichen ist dies nicht wichtig.

Commands overview:

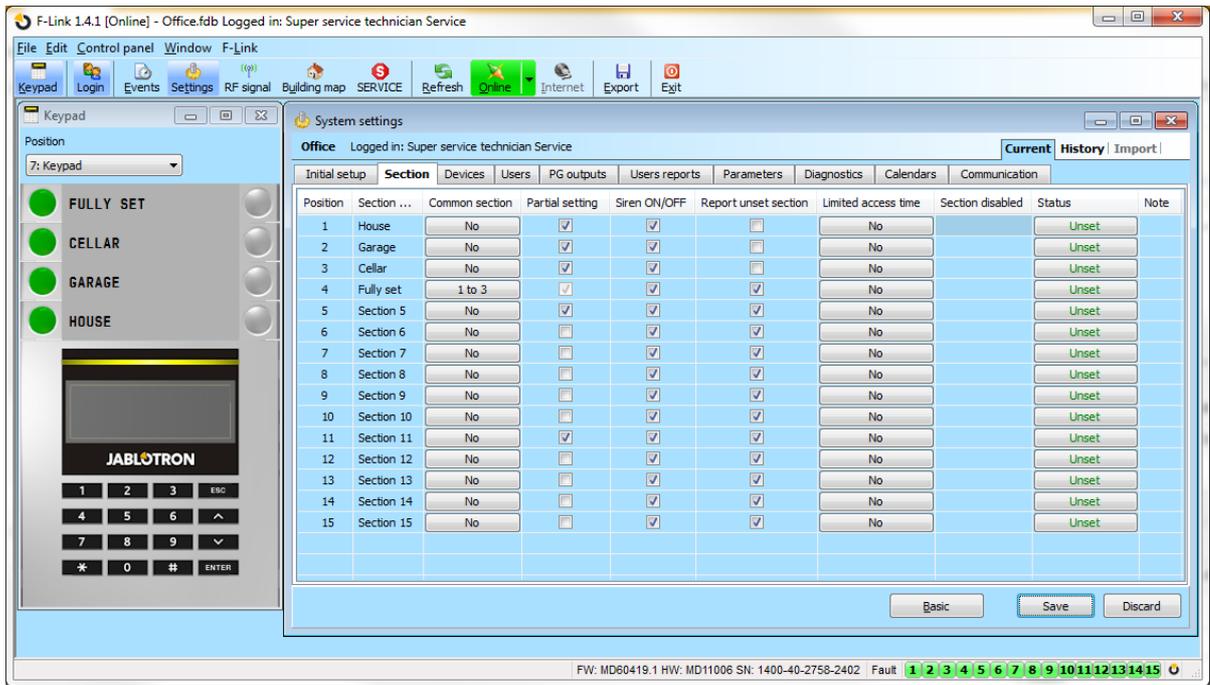
Steuerbefehl	Berechtigung	Antwort (Muster)	Hinweis
DINFO (grundsätzliche Information zur Installation)	Errichter, Administrator	JABLOTRON 100+: TYP: JA-103K, SN: 14004026532523, SW: LJ60418, HW: LJ16117, RC: C5U6G-215CP-D2A6, GSM: 90%, GPRS: Ok, LAN: aus Zeit 17:01 22.7.	Installationsname wie in der Systemübersicht Typ der Zentrale Seriennummer Version der Firmware Version der Hardware Registrierungscode (Anmeldecode) des GSM-Wähl- & Übertragungsgerätes GSM-Signalqualität, GPRS-Datenverfügbarkeit LAN Verbindungsstatus (OK oder AUS) Zeit und Datum der Versendung der SMS zum GSM-Netzwerk
STATUS (Status der Bereiche)	Service (Errichter), Administrator, Benutzer. Wenn der Benutzer nur Zugriff auf einige Bereiche hat, wird ihm der Status der Bereiche wieder zurückgesandt, auf die er zugreifen kann.	JABLOTRON 100+: Status: Bereich 1: Unscharf; Bereich 2: Scharf; Bereich 3: Unscharf; Bereich 4: Scharf, Fehler; Bereich 5: Scharf; Bereich 6: Scharf; Bereich 7: Unscharf; Bereich 8: Unscharf; GSM: 90%; Zeit 17:01 22.7.	Installationsname wie in der Systemübersicht Status: Name und Status von Bereich 1 Name und Status von Bereich 2 Name und Status von Bereich 3 Name und Status von Bereich 4 Name und Status von Bereich 5 Name und Status von Bereich 6 Name und Status von Bereich 7 Name und Status von Bereich 8 GSM-Signalqualität Zeit und Datum der Versendung der SMS zum GSM-Netzwerk
COM (Info zu Kommunikation)	Service	JABLOTRON 100+: GSM: 90%, DATA: ok, CELLID: 44905, OPID: 23003, LAN: ok, MAC: hh:hh:hh:hh:hh:hh, PSTN: aus, ARC: 1:ok, 2:ok, 3:off, 4:ok, 5:off, Zeit 17:01 22.7.	Installationsname wie in der Systemübersicht GSM-Signalqualität, GPRS-Datenverfügbarkeit Handynummer und Betreiber der GSM-Verbindung LAN-Verbindungsstatus und MAC-Adresse Verbindungsstatus der Telefonleitung (möglich mit JA-190X) Aktivierungsstatus von Übertragungen an einzelne Leitstellen. Zeit und Datum der Versendung der SMS zum GSM-Netzwerk
GSM (Neustart GSM)	Service, Administrator, Benutzer	JABLOTRON 100+: SMS verarbeitet OK: GSM; Zeit 17:01 22.7.	Installationsname wie in der Systemübersicht Bestätigung der SMS-Versendung (vor dem Neustart) Zeit und Datum der Versendung der SMS zum GSM-Netzwerk

<p>SCHARF (Steuerung des gesamten Systems)</p>	<p>(Je nach Benutzercode)</p>	<p>JABLOTRON 100+: Status: Bereich 1: Scharf; Bereich 2: Scharf; Bereich 3: Scharf; Bereich 4: Scharf; Fehler; Bereich 5: Scharf; Bereich 6: Scharf; Bereich 7: Scharf mit einer aktiven Zone, Bereich 8: Scharf mit einer aktiven Zone; GSM: 90%; Zeit 17:01 22.7.</p>	<p>Installationsname wie in der Systemübersicht</p> <p>Name und Status von Bereich 1 Name und Status von Bereich 2 Name und Status von Bereich 3 Name und Status von Bereich 4 Name und Status von Bereich 5 Name und Status von Bereich 6 Name und Status von Bereich 7 Name und Status von Bereich 8</p> <p>GSM-Signalqualität Zeit und Datum der Versendung der SMS zum GSM-Netzwerk</p>
<p>UNSCHARF (Steuerung des gesamten Systems)</p>	<p>(Je nach Benutzercode)</p>	<p>JABLOTRON 100+: Status: Bereich 1: Unscharf; Bereich 2: Unscharf; Bereich 3: Unscharf; Bereich 4: Unscharf, Fehler; Bereich 5: Unscharf; Bereich 6: Unscharf; Bereich 7: Unscharf; Bereich 8: Unscharf; GSM: 90%; Zeit 17:01 22.7.</p>	<p>Installationsname wie in der Systemübersicht</p> <p>Name und Status von Bereich 1 Name und Status von Bereich 2 Name und Status von Bereich 3 Name und Status von Bereich 4 Name und Status von Bereich 5 Name und Status von Bereich 6 Name und Status von Bereich 7 Name und Status von Bereich 8</p> <p>GSM-Signalqualität Zeit und Datum der Versendung der SMS zum GSM-Netzwerk</p>
<p>SCHARF 1 3 5 7 (Steuerung ausgewählter Systembereiche)</p>	<p>(Entsprechend des verwendeten Codes)</p>	<p>JABLOTRON 100+: Status: Bereich 1: Set; Bereich 3: Set; Bereich 5: Set; Bereich 7: Scharf mit einer aktiven Zone, GSM: 90%; Zeit 17:01 22.7.</p>	<p>Installationsname wie in der Systemübersicht</p> <p>Name und Status von Bereich 1 Name und Status von Bereich 3 Name und Status von Bereich 5 Name und Status von Bereich 7</p> <p>GSM-Signalqualität Zeit und Datum der Versendung der SMS zum GSM-Netzwerk</p>
<p>UNSCHARF 2 4 6 8 (Steuerung ausgewählter Systembereiche)</p>	<p>(Entsprechend des verwendeten Codes)</p>	<p>JABLOTRON 100+: Status: Bereich 2: Unscharf; Bereich 4: Unscharf; GSM: 90%; Zeit 17:01 22.7.</p>	<p>Installationsname wie in der Systemübersicht</p> <p>Status: Name und Status von Bereich 2 Name und Status von Bereich 4 GSM-Signalqualität Zeit und Datum der Versendung der SMS zum GSM-Netzwerk</p>

9.7. Steuerung des Systems via F-Link oder J-Link

Die Software F-Link und J-Link werden dafür verwendet, das gesamte System lokal oder per Fernzugriff zu programmieren oder Benutzer zu bearbeiten. Sie bieten einen Überblick über den Status der Bereiche und die Bereichssteuerung. Man kann Bereiche und PG-Ausgänge steuern, indem man die virtuellen Tastaturbereiche (Segmente) entsprechend der Konfiguration der Tastaturen, die physisch in dem System vorhanden sind, verwendet. Die Steuerung ist auch möglich, indem man auf die Registerkarte „Bereichsübersicht“ in der Spalte

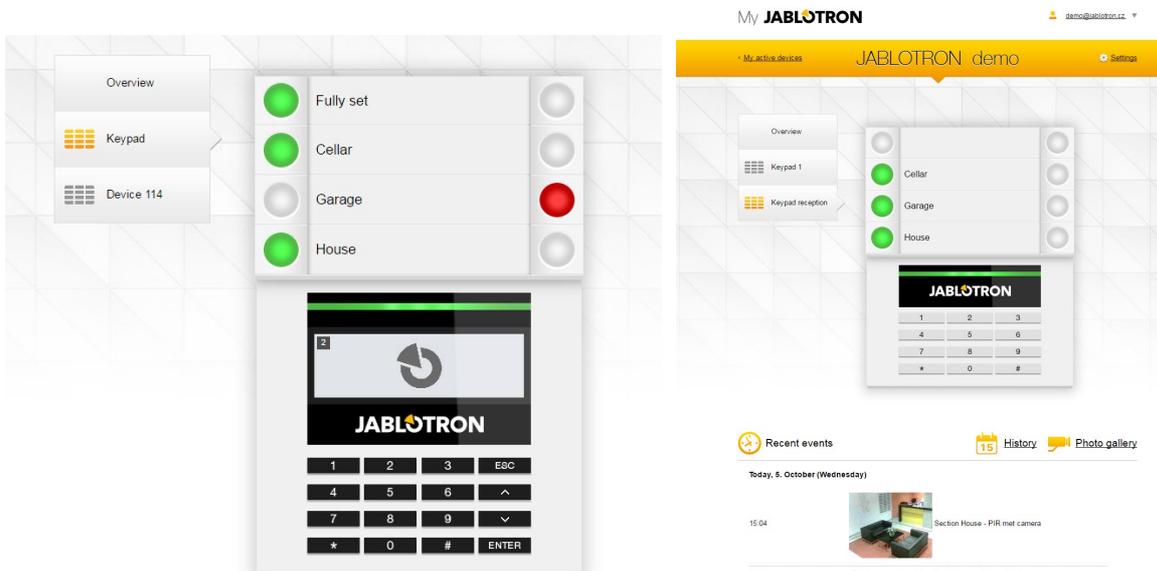
„Status“ oder auf die Nummer des Bereichs in der unteren Statusleiste klickt. Das System zeichnet die Systemsteuerung entsprechend der Benutzerberechtigung in der Software auf.



9.8. Systemsteuerung von der webbasierten App MyJABLOTRON

Die Fernsteuerung über die webbasierte App MyJABLOTRON ist der benutzerfreundlichste Weg, um das Sicherheitssystem von jedem Internetbrowser aus und unabhängig von der Computerplattform zu steuern. Wenn Sie einmal eingeloggt sind, ermöglicht Ihnen die App, das System nicht nur über eine virtuelle Tastatur, die alle physischen Tastaturen des Systems darstellt, zu steuern, sondern ermöglicht Ihnen auch, alle Bereiche und PG-Ausgänge aus einer Gesamtliste zu steuern. Der Benutzer kann außerdem einen detaillierten Ereignisverlauf einschließlich Fotos und Videos durchsuchen. Neue Fotos können sofort auf Anfrage des Benutzers aufgenommen werden. Anders als beim physischen System kann der Benutzer die aktuellen Temperaturen der Thermometer sowie Werte verschiedener Zähler einsehen und kann Nachrichten konfigurieren, die ihn über Systemereignisse oder überschrittene Werte informieren, die vom Benutzer festgelegt wurden.

Zur Steuerung des Systems müssen Sie sich jedes Mal, wenn Sie sich anmelden, über die Berechtigungsfunktion mit einem Benutzercode berechtigen. Die Steuerung der Bereiche über die Segmente ist identisch mit der realen Konfiguration. Wenn die Segmente eine teilweise Scharfschaltung ermöglichen, ist es möglich, das System per Fernzugriff teilweise scharf zu schalten. In anderen Fällen schaltet die Steuerung über die Liste immer vollständige Bereiche scharf. Für weitere Informationen, siehe Kapitel 14 Die webbasierte Applikation MyJABLOTRON

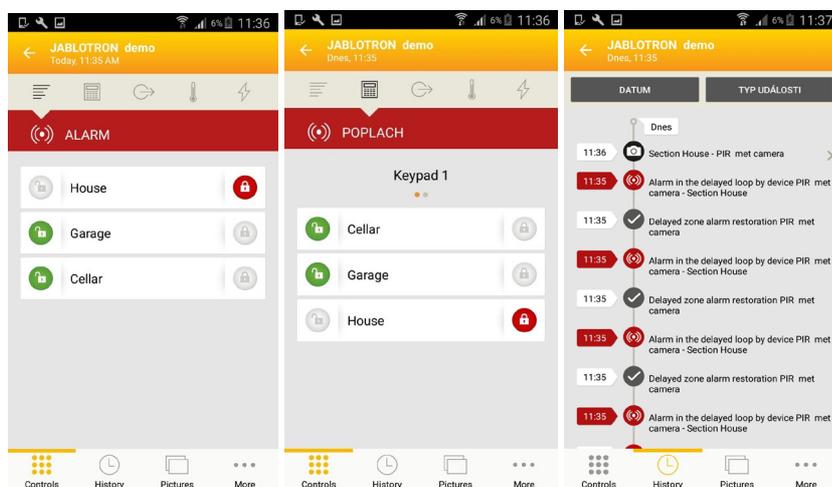


Teil der Fernprogrammierung von der Website aus (unabhängig von der Plattform des fernsteuernden Computers) ist der sogenannte WEB-Link, der in der MyCOMPANY App → Installationsmanagement → Schaltfläche Konfiguration verfügbar ist. WEB-Link ist nur für Installationsunternehmen verfügbar, die mit diesem Tool einen indirekten Fernzugriff haben, indem sie Parameter in einer Konfigurationsdatei auf dem Server ändern und diese sofort, zu einem bestimmten Zeitpunkt oder nach dem Deaktivieren des Systems speichern. Der Installateur kann über eine erfolgreiche Konfigurationsänderung per SMS oder E-Mail informiert werden.

WEB-Link								
Position	Section name	Common section	Partial setting	Siren ON/OFF	Report unset section	Limited access time	Section disabled	
1	House	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>	
2	Garage	No	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>	
3	Cellar	No	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No	<input type="checkbox"/>	
4	Fully set	1 to 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
5	Section 5	No	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
6	Section 6	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
7	Section 7	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
8	Section 8	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
9	Section 9	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
10	Section 10	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
11	Section 11	No	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
12	Section 12	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
13	Section 13	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
14	Section 14	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	
15	Section 15	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>	

9.9. Steuerung über die mobile App MyJABLOTRON

Benutzer von MyJABLOTRON können eine Applikation für Smartgeräte downloaden. Diese ist verfügbar für iOS und Android. Die mobile App ist der benutzerfreundlichste Weg zur Steuerung des Sicherheitssystems. Der Benutzer kann es sogar bei fast uneingeschränktem Internetzugang in der Tasche mit sich tragen. Nachdem einmal sicher ins System eingeloggt wurde, ermöglicht Ihnen die App, das System nicht nur über eine virtuelle Tastatur zu steuern, die alle physischen Tastaturen des Systems darstellt, sondern ermöglicht Ihnen auch die Steuerung aller Bereiche und PG-Ausgänge aus einer Gesamtliste. Also fast der gleiche Funktionsumfang wie in der webbasierten Applikation MyJABLOTRON. Für einige Plattformen bietet sie weitere Features, zum Beispiel TouchID oder FaceID anstelle eines Codes.



9.10. Systemsteuerung über die Erzwungene Zugriffssteuerung

Diese Option, die in den Standardeinstellungen ausgeschaltet ist, ermöglicht dem Benutzer, das System mit einem anderen Code zu steuern (scharf oder unscharf zu schalten), wenn er von einer anderen Person bedroht wird. Dieser Code wird unauffällig auf eine solche Situation aufmerksam machen, indem er einen stummen Geiselnahmealarm ohne akustische oder visuelle Anzeige auslöst. Ein Panik- oder auch Geiselnahmealarm wird durch das Hinzufügen von 1 zum bestehenden Code ausgelöst.

Beispiel:

Benutzercode mit Präfix = 4*4444. Erzwungener Zugriffssteuerungscode = 4*4445

Benutzercode ohne Präfix = 4444. Erzwungener Zugriffssteuerungscode = 4445

Warnhinweis: Wenn der Benutzercode mit der Nummer 9 endet, ist die letzte Nummer des Codes 0.

9.11. Hindernisse, die die Scharfschaltung des Systems verhindern

Je nach **Einstellungsart** (siehe Registerkarte Systemparameter) prüft die Zentrale den ausgelösten oder fehlerhaften Status der einzelnen Geräte oder eines einzelnen Bereichs, während die einzelnen Bereiche des Systems scharf geschaltet werden. Bei dieser Option zeigt die Zentrale einige Hindernisse während der Scharfschaltung an (**passierbare Hindernisse**). Dabei kann ein auftretender Status sogar das System an der Scharfschaltung hindern (**unpassierbare Hindernisse**).

Eines der gängigsten Hindernisse ist der Systemfehler (durch eine beleuchtete gelbe Anzeigentaste angezeigt), ein Verbindungsverlust mit einem drahtlosen Gerät oder ein aktivierter Statusmelder (typischerweise ein Magnetmelder), der in einer Zone mit verzögerter Reaktion scharf geschaltet ist (Melder der Eingangs- oder Garagentür), schwache Systembatterien, ein langanhaltender Stromausfall oder ein andauernder Stromausfall.

Ein unpassierbares Hindernis, das das System an der Scharfschaltung hindert, ist zum Beispiel ein **aktivierter Statusmelder** (normalerweise ein magnetischer Türöffnungsmelder), der auf eine **Sofortige Reaktion** eingestellt ist. Geräte dieser Gruppierung sind Fensteröffner, Balkon- oder Hintertürmelder, aber auch kritische Systemfehler, wie ein Fehler der Backup-Stromversorgung oder ein Kommunikationsfehler mit einer Leitstelle. Die Gründe, die eine Scharfschaltung des Systems verhindern, sind je nach voreingestelltem Systemprofil unterschiedlich. Eine Ausnahme stellt die automatische Scharfschaltung durch den Kalender über die Option „immer ...scharf schalten“ dar. Hier wird das System nicht an einer Scharfschaltung gehindert, da ausgelöste Melder oder Fehler nicht überprüft werden. Der Kalender wird immer jeden Bereich festlegen, sofern er für eine solche Aktion konfiguriert wurde (nur verfügbar, wenn das Systemprofil „Standard“ verwendet wird).

Die Aktivierung eines Impulsmelders (z. B. Melder: Bewegung, Glasbruch, Neigung, Schock und dergleichen) kann die Einstellung nicht verhindern.

Das System informiert Sie per SMS-Meldung über die Scharfschaltung mit einem aktiven Gerät (an eine Gruppe von Benutzern mit vordefinierten Alarmmeldungen) mit einer detaillierten Beschreibung.



Arten der Scharfschaltung – Tabellenüberblick

Arten der Scharfschaltung	Systemtastatur	Über das Sprachmenü / SMS / Kalender	MyJABLOTRON-App	F-Link J-Link
Sofortige Scharfschaltung	Schaltet immer scharf, trotz Fehler oder aktiviertem Gerätestatus	Schaltet immer scharf, trotz Fehler oder aktiviertem Gerätestatus	Schaltet immer scharf, trotz Fehler oder aktiviertem Gerätestatus	Schaltet immer scharf, trotz Fehler oder aktiviertem Gerätestatus
Scharfschalten mit Hinweis	Bei einer versuchten Scharfschaltung mit einem Fehler oder ausgelöstem Gerät blinkt die Tastatur für 8 Sek., danach wird das System automatisch scharf geschaltet. Das System kann durch Drücken der Bereichstaste oder der Enter-Taste scharf geschaltet werden.	Schaltet immer scharf, trotz Fehler oder aktiviertem Gerätestatus	Wird entsprechend den „Einstellungen“ (Scharfschaltung mit Prüfung / Scharfschaltung ohne Prüfung“) in der Registerkarte Komponentenliste scharf geschaltet.	Schaltet immer scharf, trotz Fehler oder aktiviertem Gerätestatus
Scharfschalten mit Bestätigung	Bei einer versuchten Scharfschaltung mit einem Fehler oder ausgelöstem Gerät blinkt die Tastatur für 8 Sek., danach wird das System automatisch scharf geschaltet. Das System kann NUR durch Drücken der Bereichstaste oder der Enter-Taste scharf geschaltet werden.	Schaltet immer scharf, trotz Fehler oder aktiviertem Gerätestatus	Wird entsprechend den "Einstellungen" (Scharfschaltung mit Prüfung / Scharfschaltung ohne Prüfung“) in der Registerkarte Komponentenliste scharf geschaltet.	Schaltet immer scharf, trotz Fehler oder aktiviertem Gerätestatus
Keine Scharfschaltung	Bei einer versuchten Scharfschaltung mit einem Fehler oder ausgelöstem Gerät blinkt die Tastatur für 8 Sek., danach wird das System automatisch scharf geschaltet. Das System kann NUR durch Drücken der Bereichstaste scharf geschaltet werden, wenn ein Melder in einer Sofortigen Zone NICHT aktiviert wurde.	Wird nicht scharf geschaltet, wenn ein aktivierter Melder in einer sofortigen scharf geschaltet ist. Wenn „Immer scharf“ ausgewählt ist, wird er über den Kalender trotz Fehlern oder ausgelöstem Gerätestatus scharf geschaltet.	Wird nicht scharf geschaltet, wenn ein aktivierter Melder in einer Sofortigen Zone aktiviert wurde.	Schaltet immer scharf, trotz Fehler oder aktiviertem Gerätestatus

9.12. Fehlgeschlagene Scharfschaltung

Aufgrund einer Sicherheitsfunktion prüft die Zentrale innerhalb einer Ausgangsverzögerung, ob die Scharfschaltung des Systems ausgeführt werden kann. Das System des überwachten Gebäudes wird durch die folgenden Fälle nicht eingeschränkt. Wenn diese Funktion aktiviert ist, kann die **fehlgeschlagene Scharfschaltung** von den folgenden Faktoren verursacht werden:

1. Aktivierung eines Melders mit einer sofortigen Reaktion während einer Ausgangsverzögerung (jemand betritt das bereits überwachte Gebäude)
2. Dauerhafte Aktivierung eines Melders mit einer Verzögerungsreaktion nach abgelaufener Ausgangszeit (Der Benutzer hat vergessen die Vordertür, die Garage oder das Tor zu schließen usw.)

Wenn die Scharfschaltung des Systems verhindert wird, wird das Ereignis „fehlgeschlagene Scharfschaltung“ ausgelöst. Dies wird durch eine schnell blinkende gelbe Systemanzeige auf den Tastaturen und durch ihr Piepen angezeigt. Akustisch wird dies auch über eine funktionsunterstützende Außensirene angezeigt. Gleichzeitig wird das Ereignis einem spezifischen Benutzer oder dem Systemadministrator gemeldet, wenn die Meldung „fehlgeschlagene Scharfschaltung“ aktiviert ist, siehe F-Link, Registerkarte Übertragungsgeräte.

Um die Anzeige einer fehlgeschlagenen Scharfschaltung zu beenden, wählen Sie im LCD-Tastaturmenü oder, wenn das Profilsystem „Standard“ voreingestellt ist, über die Einstellung des Bereichs die Option „Warnanzeige beenden“.

9.13. An Benutzer gemeldete Ereignisse

Alle Ereignisse, die an Benutzer gesendet werden, sind 5 Basisgruppen zugeordnet. Jede einzelne Gruppe kann den Benutzern beliebig zugewiesen werden. Benutzer, denen eine Gruppe zugewiesen wird, erhalten Meldungen dieser Gruppe. Wenn die Grundeinstellungen der Gruppen nicht ausreichen, können zwei spezielle Gruppen verwendet werden (benutzerdefinierte Gruppe 1 und 2). Zu diesen Gruppen können Ereignisse hinzugefügt werden, die nur bestimmten Benutzern zugewiesen werden können.

Übersichtstabelle der den Benutzern gemeldeten Ereignisgruppen:

Reihenfolge	Ereignis	Gruppe
1	Scharfschaltung	SMS über Scharfschaltung (3)
2	Unscharfschaltung	SMS über Unscharfschaltung (3)
3	Teilscharfschaltung	SMS über Teilscharfschaltung (3)
4	Netzfehler von 30 Minuten	SMS-Warnungen (1) / Alarmanruf (2)
5	Netzwiederherstellung nach 30 Minuten	SMS-Warnungen (1) / Alarmanruf (2)
6	Sofortiger Alarm	SMS-Warnungen (1) / Alarmanruf (2)
7	Sofortiger Alarm beendet	SMS-Warnungen (1) / Alarmanruf (2)
8	Verzögerter Alarm	SMS-Warnungen (1) / Alarmanruf (2)
9	Verzögerter Alarm beendet	SMS-Warnungen (1) / Alarmanruf (2)
10	Sabotagealarm	SMS-Warnungen (1) / Alarmanruf (2)
11	Sabotagealarm beendet	SMS-Warnungen (1) / Alarmanruf (2)
12	Feueralarm	SMS-Warnungen (1) / Alarmanruf (2)
13	Feueralarm beendet	SMS-Warnungen (1) / Alarmanruf (2)
14	Gasaustritt	SMS-Warnungen (1) / Alarmanruf (2)
15	Panik, Überfall bzw Geiselnahmealarm	SMS-Warnungen (1) / Alarmanruf (2)
16	Panik, Überfall bzw Geiselnahmealarm abgebrochen	SMS-Warnungen (1) / Alarmanruf (2)
17	Gesundheitsprobleme	SMS-Warnungen (1) / Alarmanruf (2)
18	Überschwemmung	SMS-Warnungen (1) / Alarmanruf (2)
19	Codeentschlüsselungsversuch	SMS-Warnungen (1) / Alarmanruf (2)
20	Scharfschaltung mit einer aktiven Zone (bei aktivierter Bestätigung)	SMS-Warnungen (1) / Alarmanruf (2)
21	Bereich ohne Bewegung	SMS-Warnungen (1) / Alarmanruf (2)
22	Überhitzungsaktivierung	SMS-Warnungen (1) / Alarmanruf (2)
23	Überhitzungsdeaktivierung	SMS-Warnungen (1) / Alarmanruf (2)
24	Gefrieraktivierung	SMS-Warnungen (1) / Alarmanruf (2)
25	Gefrierdeaktivierung	SMS-Warnungen (1) / Alarmanruf (2)
26	Systemstart (außerhalb des Errichter-Modus)	Fehler- und Service-SMS (5)
27	Schwache Gerätebatterie	Fehler- und Service-SMS (5)

28	Gerätebatterie OK	Fehler- und Service-SMS (5)
29	Fehler (Gerät, Kommunikator)	Fehler- und Service-SMS (5)
30	Fehlerende	Fehler- und Service-SMS (5)
31	Eingabe des Errichter-Modus	Fehler- und Service-SMS (5)
32	Errichter-Modus verlassen	Fehler- und Service-SMS (5)
33	Eingabe des Wartungsmodus	Fehler- und Service-SMS (5)
34	Wartungsmodus verlassen	Fehler- und Service-SMS (5)
35	Schwache BATTERIE	Fehler- und Service-SMS (5)
36	BATTERIE OK	Fehler- und Service-SMS (5)
37	Kommunikationsfehler mit dem ARC	Fehler- und Service-SMS (5)
38	AES-Kommunikation wiederhergestellt	Fehler- und Service-SMS (5)
39	RF-Störung	Fehler- und Service-SMS (5)
40	Ende der RF-Störung	Fehler- und Service-SMS (5)
41	Niedriges Guthaben	Fehler- und Service-SMS (5)

Die Zuordnung der Ereignisse, die das System in Gruppen unterteilt, ist in der Tabelle dargestellt. Wenn ein Ereignis auftritt, generiert das System eine SMS in dem Format: Installationsname, Zeit, Ereignis, Ereignisquelle, Bereich, Zeit.

Beispiel einer gesendeten SMS:

JABLOTRON 100	(Installationsname)
17:01:10, Verzögerter Alarm	(Ereigniszeit, Ereignis)
Türmagnet, Erdgeschoss	(Meldername, Bereichsname)
17:01:25, Sofortiger Alarm	(Ereigniszeit, Ereignis)
Bewegung im Treppenhaus, oben	(Meldername, Bereichsname)
Zeit 17:01 22.7.	(Sendezeit)

9.14. Akustische Anzeige des Systems

Die akustische Anzeige des Systems zeigt nicht nur einen Alarmstatus an, sondern informiert auch über andere Status oder Statusänderungen. Die folgende Tabelle gibt einen Überblick über die akustischen Anzeigen:

Akustische Anzeige der Tastatur / des Lesegeräts:

Ton	Beschreibung der Aktion
Ein kurzer Piepton	Bestätigung der Betätigung der Taste
Ein langer Piepton	Aktivierung der Funktionstaste, Scharfschaltung eines Bereichs oder PG-Schaltung
Zwei lange Pieptöne	Deaktivierung der Funktionstaste, Unscharfschaltung eines Bereichs oder Ausschaltung eines PG
Zwei lange wiederholte Pieptöne	Fehlgeschlagene Scharfschaltung
Drei lange Pieptöne	Unscharfschaltung eines Bereichs mit Alarmspeicheranzeige
Dauerhaftes Piepen	Ausgangsverzögerung
Anhaltendes Piepen	Eingangsverzögerung
	Alarm

Akustische Anzeige der Innen- und Außensirenen:

Ton	Beschreibung der Aktion
Ein kurzer Piepton	Scharfschaltung des Bereichs
	PG-Ausgang EIN
Zwei kurze Pieptöne	Scharfschaltung des Bereichs
	PG-Ausgänge EIN
Drei kurze Pieptöne	Unscharfschaltung des Bereichs
	PG-Ausgänge AUS
	Unscharfschaltung des Bereichs mit Alarmspeicheranzeige
Schnelles dauerhaftes Piepen	Fehlgeschlagene Scharfschaltung
Langsames dauerhaftes Piepen	Scharfschaltung mit einer aktiven Zone (nur bis FW 13)
	PG-Statusanzeige – schnelles Piepen
Dauerhafter Piepton	Ausgangsverzögerung
	PG-Statusanzeige – langsames Piepen
Hupen	Eingangsverzögerung
Melodie (1 – 4) *	PG-Statusanzeige

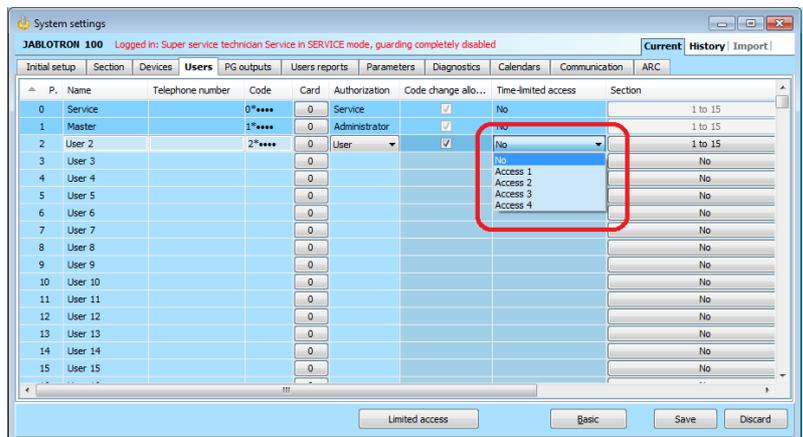
* Gilt nur für Sirenen, die die Melodiefunktion unterstützen

Akustische Anzeige der Feuermelder (Rauch, Temperatur, Gas):

Ton	Beschreibung der Aktion
Schnelles dauerhaftes Piepen	Feueralarm
Dauerhafter lauter Ton	

9.15. Zeitlich begrenzter Zugriff für Benutzer

Die zeitlich begrenzte Zugriffsfunktion ist für ausgewählte Benutzer gedacht, die in bis zu 4 Gruppen aufgeteilt sind. Diesen Gruppen können verschiedene „zeitliche Berechtigungen“ für den Zugriff auf zugewiesene Bereiche entsprechend dem Wochenkalender hinzugefügt werden. Dadurch kann jede Benutzergruppe einen ausgewählten Bereich in zwei Zeitintervallen (Intervall 1 und Intervall 2) für jeden Wochentag blockieren oder unscharf schalten. Dies dient hauptsächlich größeren Unternehmen, wo es Mitarbeiter, Leiter und Manager gibt oder in einem Kindergarten, wo es Putzfrauen, Köche, Pädagogen und Eltern mit ihren Kindern gibt.

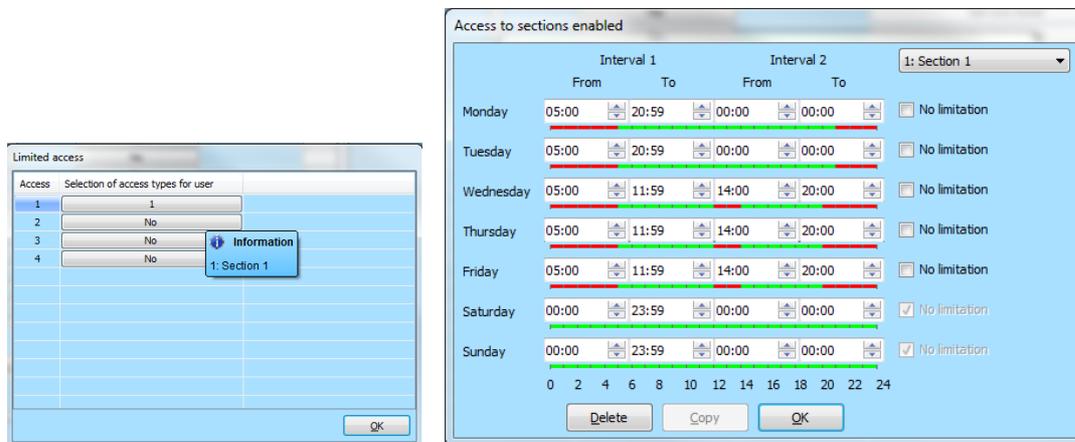


Jeder Systembenutzer, der gemäß dem voreingestellten Kalender begrenzten Zugriff haben sollte, verfügt über eine Option der Aktivierung, d.h. „zeitlich begrenzten Zugriff“ „Gruppe 1“ bis „Gruppe 4“, und dies gilt für jede einzelne Benutzergruppe.

Die Einschränkung gilt nur für die „Benutzerberechtigung“. Wenn der Benutzer mit aktivierter Zeitbegrenzung versucht, einen Bereich während des gesperrten Zeitraums zu deaktivieren, wird das System ihn ablehnen. Und

wenn sich der Benutzer bereits in den geschützten Räumlichkeiten befand, würde nach Ablauf der Eingangsverzögerungszeit ein Einbruchalarm ausgelöst werden. Der Benutzer hat die Berechtigung, den Alarm abzubrechen, jedoch wird das System innerhalb der Sperrfrist nicht zurückgesetzt.

Das folgende Beispiel ist eine Einstellungsvariante für den Zugriff, der einer ausgewählten Gruppe von Benutzern „Gruppe 1“ gewährt wird, wobei der Zugriff auf „Bereich 1“ beschränkt ist. Am Montag und Dienstag ist der Zugriff von 5:00 Uhr morgens bis 20:59 Uhr abends erlaubt. Von Mittwoch bis Freitag ist der Zugang von 5:00 bis 11:59 Uhr und dann von 14:00 bis 20:00 Uhr erlaubt. Am Wochenende (Samstag und Sonntag) ist der Zugang vollständig gesperrt.



Zur Programmierung des zeitlich begrenzten Zugriffs, klicken Sie in der Registerkarte Benutzer in F-Link den selben Namen der Taste, die Sie verwenden, um Benutzergruppen für einzelne Bereiche einzustellen.

9.16. Deaktivierungs- und Sperroptionen

9.16.1. Deaktivierung

Vor der Scharfschaltung des Systems kann es passieren, dass bei einem Gerät absichtlich die Bypass-Funktion verwendet werden muss (z.B. eine Garage, wenn dort Bauarbeiten stattfinden oder wenn sich ein Hund in einem ursprünglich überwachten Raum befindet). Diese Option wird **Gerätedeaktivierung** genannt und ist im LCD-Tastaturmenü oder in J-Link verfügbar. Diese Funktion kann je nach Benutzerberechtigung auf zwei Stufen verwendet werden:

1. **Eingangssperrung(BLK)** – die Funktion wird zur Sperrung eines Meldereingangs (seine Aktivierung wird gesperrt) verwendet. Das System ignoriert jede Melderaktivierung = es wird weder ein Alarm ausgelöst, noch ein PG-Aktivierung gemeldet. Sabotagealarme, Fehler oder schwache Batterien werden immer überwacht und gemeldet. In J-Link wird dies durch einen gelben Punkt angezeigt. Die Berechtigung für die auszuführende Sperrung haben Administrator und Errichter.
2. **Gerätedeaktivierung (DIS)** – diese Funktion dient dazu, einen Melder zu deaktivieren. Das System ignoriert alle Gerätefunktionen = weder Alarme noch Sabotagealarme, Fehler oder Meldungen werden ausgelöst. Dies wird in J-Link über einen roten Punkt angezeigt. Die Berechtigung zur Deaktivierung wird nur vom Errichter durchgeführt.

Es kann nicht nur ein Gerät, sondern auch ein Benutzer deaktiviert werden, mit Ausnahme von Benutzern in Position 0 (Errichter) und 1 (Administrator), PG-Ausgänge oder Kalenderaktionen. Die Deaktivierung ist dauerhaft, bis sie durch das gleiche Verfahren wie ihre Aktivierung abgebrochen wird.

Vorsicht: Es ist nicht möglich, eine Zentrale oder ein Gerät mit einer Panikreaktion zu **sperr**en oder zu **deaktivieren!**

9.16.2. Sperrung

Bei der Scharfschaltung von Bereichen kann es vorkommen, dass einige Geräte aktiv bleiben (zum Beispiel ein offenes Fenster oder eine Balkontür usw.). Das System reagiert schnell auf diese Situation während der Scharfschaltung des Bereichs und informiert darüber, aber nach der Bestätigung verhält sich das System entsprechend dem Parameter **Sperrung während der Scharfschaltung** in einer der folgenden Möglichkeiten:

1. **Sperrung aktiviert** – Die Aktivierung dieser Option sperrt alle aktiven Melder während der Scharfschaltung. Dies bedeutet, dass sie in diesem Zeitraum der Scharfschaltung keinen Alarm aktivieren können.

2. **Sperrung deaktiviert** – Die Deaktivierung dieser Option leitet aktive Melder nur während des Zeitraums der Scharfschaltung vorübergehend um. Dies bedeutet, dass sie nur dann einen Alarm auslösen können, wenn sie zurück in den Standby-Modus gehen (es gibt aufgrund von z.B. geöffneten Fenstern ein Fehlalarmrisiko).

9.17. Nicht-Alarmfunktionen - Funktionen der PG-Ausgänge

Funktion des PG-Ausgangs	Beschreibung	Beispiel
EIN / AUS	Bi-stabiler Status des Ausgangs, kann von einem beliebigen Befehl oder Gerät geändert werden	Manuelles EINSchalten von Geräten über einen Steuerungsbereich, SMS oder auch über ein Gerät, das ohne Einschränkung manuell ausgeschaltet werden kann. Typische Beispiele sind die Steuerung von Heizungen, Klimaanlage und Lichtern.
Impuls	Mono-stabiler Status des Ausgangs mit einer voreingestellten Zeit	Impulsschaltung von weiteren zusätzlichen Steuerschaltungen wie Torsteuerung, Rollen, Jalousien, Gartenbewässerung, Türschlösser u.s.w.
Kopieren ohne Verzögerung	Ausgangsstatus mit OR-Logik. Die Ausgänge sind aktiv, wenn mindestens ein Gerät auch aktiv ist. Die Deaktivierung erfolgt, wenn alle Steuerungsgeräte inaktiv sind.	Nützlich für die Anzeige von Einzel- oder Sammelstatus (typischerweise von offenen Fenstern, Garagentoren u.s.w.) auf dem Steuerungsbereich der Tastatur. In ähnlicher Weise können auch der Status aller Bereiche, Alarme, Alarmspeicher, Fehler und viele andere Ereignisse angezeigt werden, bei denen der Anfang und das Ende vorgegeben sind.
Kopieren nach Verzögerung	Mono-stabiler Ausgangsstatus mit voreingestellter Schaltzeit und der Option, die zu wiederholen.	Typische Ausgangseinstellung zur Steuerung der Beleuchtung, wenn eine Bewegung über einen Bewegungsmelder erkannt wird. Jede erkannte Bewegung verlängert den Impuls.
Kopieren mit Haltezeit	Verzögerter Ausgangsstatus mit einer voreingestellten Zeit dieser Verzögerung,	Hauptsächlich für die Anzeige einer geöffneten Tür für einen längeren Zeitraum als vordefiniert, weil sie nicht geschlossen wurde (Tür oder Garagentor). Die Anzeige kann optisch auf dem Steuerungsbereich der Tastatur und akustisch über die Tastatur oder die Innen- /Außensirene erfolgen.
Zustandsänderung	Bi-stabiler Ausgangsstatus.	Ausgang, der zur zyklischen Steuerung (EIN, AUS) z.B. eines Impulsgerät dient. Dies erfolgt über die Berechtigung oder über die Einwahl einer berechtigten Telefonnummer.

Das Sicherheitssystem erlaubt berechtigten Benutzern (entsprechend der Einstellungen), die Systemfunktionen zu steuern, und zwar nicht nur Funktionen, die im Zusammenhang mit der Überwachung stehen, sondern auch mit der Steuerung der programmierbaren PG-Ausgänge (EIN / AUS schalten). Mit Relaismodulen oder einem Modul mit speziellen Halbleiterausgängen können sie Geräte (z. B. Anzeiger, Ampeln, akustische Indikatoren) oder andere Geräte, die mit dem Sicherheitssystem in Verbindung stehen, (z. B. Bewegungslichter, AC beim Betreten eines Raumes, Sperrung der Heizung bei geöffnetem Fenster oder scharf geschaltetem Bereich), oder ein komplett separates Gerät, z.B. Home-Automation (z.B. ein elektrisches Tor oder Garagentor öffnen, Heizung, Gartenbewässerung) schalten.

Das System bietet auch Benutzerfunktionen wie die Messung der Temperatur mittels Temperaturmelder oder Thermostate, die auf der LCD-Tastatur und in der MyJABLOTRON-App angezeigt werden können, um den elektrischen Energieverbrauch, die Wassermenge oder andere Versorgungsleistungen zu messen und zu überwachen. Der Impulzzähler JA-150EM-DIN ist zu diesem Zweck in Kombination mit einem Messgerät (Stromzähler, Gaszähler, Hydrometer usw.) vorgesehen. Anwendungsstudien und Empfehlungen finden Sie im Abschnitt MyCOMPANY, MySTORAGE.

10. Einstellung des Systems über F-Link

Das System JABLOTRON 100+ wird ausschließlich mit einem Computer über F-Link programmiert. F-Link prüft die aktuelle Softwareversion von Version 1.4.0 an durch Aktualisierungen vom JABLOTRON-Server aus. Die neueste Version wird automatisch zum Download angeboten. Alternativ kann sie nach dem Login von der Web-Schnittstelle von MyCOMPANY unter www.myjablotron.com heruntergeladen werden.

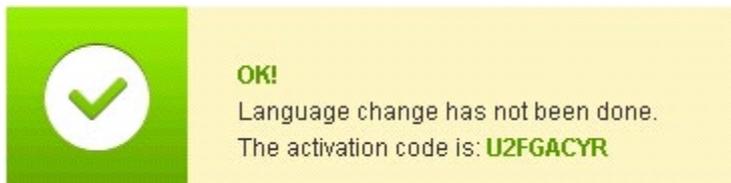
Direkt nach dem Öffnen des Eingangsfensters zur Verbindungsauswahl, kann F-Link auf die gewünschte Sprache eingestellt werden, indem man auf das Sprachsymbol (Flagge) klickt. Die Sprache kann auch zu einem späteren Zeitpunkt im Menü von F-Link geändert werden. Das Eingangsfenster bietet die folgenden Optionen:

1. **Lokale - Verbindung** – Um die Zentrale mit einem Computer zu verbinden, wird ein USB-Kabel benötigt (mit A-B-Anschlüssen).
2. **Fern - Verbindung** – Auswahl aus einer Datenbank, die es Ihnen ermöglicht, eine Verbindung per Fernzugriff herzustellen. Um eine Kommunikation mit der Zentrale herzustellen, muss der Computer über einen Internetzugang und die verwendete SIM-Karte in der Zentrale über eine aktive GPRS-Datenübertragung verfügen. Für eine problemlose Verbindung müssen andere Anforderungen erfüllt werden, z.B. aktivierte Konfiguration per Fernzugriff in der Zentrale, ordnungsgemäßer Anmeldecode, Service-Code und wenn kein LAN-Kommunikator verwendet wird, dann auch ein ausreichendes GSM-Signal am Standort der Zentrale.
3. **Offline-Modus** – bieten den Zugang zu den Einstellungsdaten der Zentrale. Hier können Sie die Geräteliste oder den letzten Batteriewechsel usw. einsehen.

F-Link kann auch verwendet werden, um die Sprache der Zentrale für die Kommunikation mit Benutzern zu ändern. Die Sprache bezieht sich nicht nur auf angezeigte Texte auf dem LCD-Bildschirm oder SMS-Nachrichten, die an Mobiltelefone von Benutzern gesendet werden, sondern auch auf das Sprachmenü der Kommunikatoren, die mit dem Benutzer kommunizieren. Wenn Sie die Sprache der Zentrale ändern, löschen Sie alle Texte im System. Daher sollte diese Auswahl als erster Schritt vor der Installation und Zuweisung von Namen zu Geräten, Abschnitten oder Benutzern vorgenommen werden.

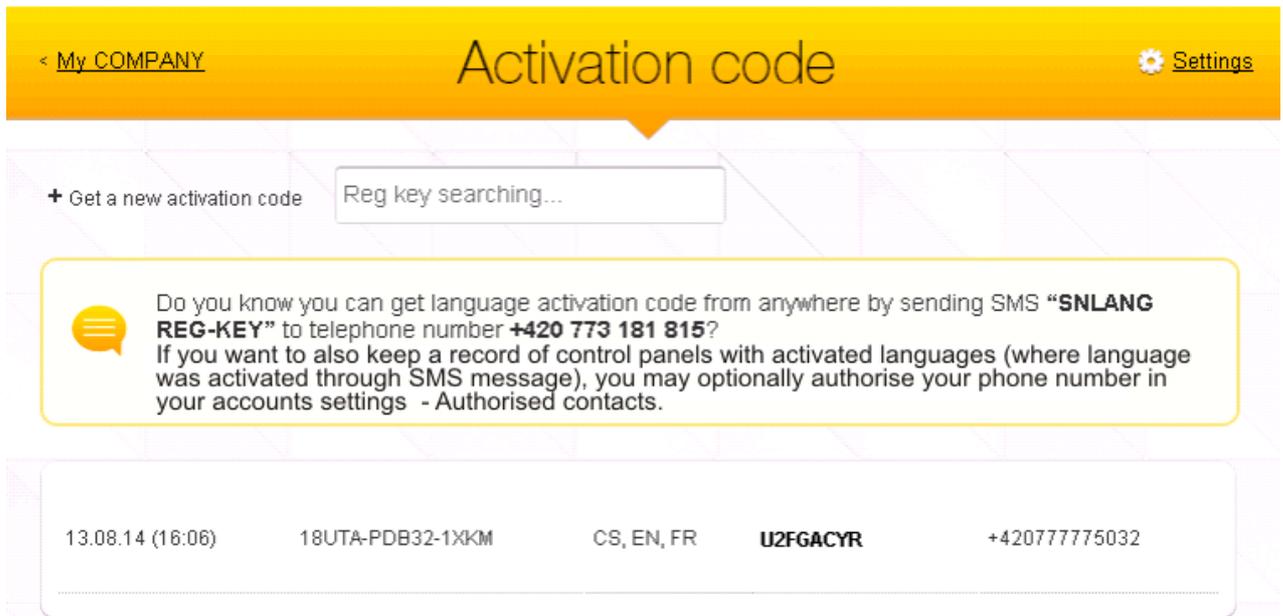
Das JABLOTRON-System wird vom Werk in der Kommunikationssprache „Englisch“ mit der Option „Tschechisch“ ausgeliefert. Andere Sprachoptionen der Zentrale sind jedoch durch eine engere Auswahl an Sprache (n) pro Land, für die die Zentrale ausgelegt ist, eingeschränkt. Das Installationsunternehmen, das im MyCOMPANY-Webdienst www.myjablotron.com angemeldet ist, kann den „Aktivierungsschlüssel“ anfordern, der an den eindeutigen Geräte-Anmeldecode gebunden ist. Der „Aktivierungsschlüssel“ erweitert die verfügbare Auswahl an Sprachen, die vom Hersteller für den jeweiligen Markt entwickelt wurden. Der Aktivierungsschlüssel kann auf drei Arten erhalten werden:

1. Von der webbasierten Schnittstelle, die nur für geschulte Errichter zugänglich ist:
 - a. Login beim MyJABLOTRON Webdienst www.myjablotron.com
 - b. Öffnen des Bereichs MyCOMPANY
 - c. Auswahl des Aktivierungscode-Dienstes
 - d. Klick auf den Posten + neuen Aktivierungscode erhalten
 - e. Den Anmeldecode der Zentrale eingeben und „Senden“ auswählen
 - f. Wenn weitere Sprachen angezeigt werden, wählen Sie die gewünschten Sprachen aus und beenden Sie die Auswahl mit „Senden“.



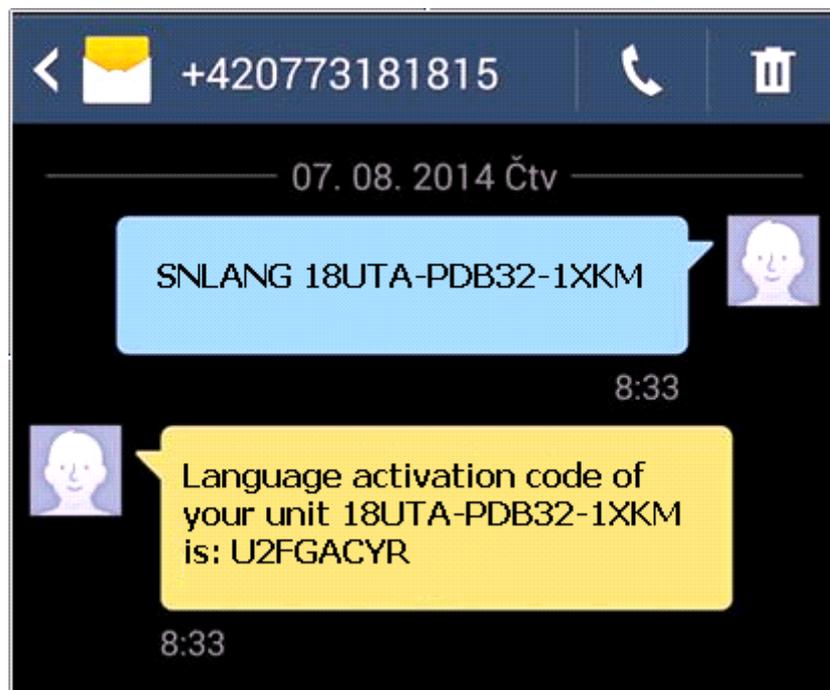
- g. Notieren Sie sich den in grün angezeigten Aktivierungscode und geben Sie ihn in F-Link ein.

Die Liste der erstellten Aktivierungs-codes wird in der Website für weitere Benutzung gespeichert.



- Wenn der Errichter gerade nicht auf das Internet zugreifen kann, kann der Aktivierungscode per SMS angefordert werden.

Es kann eine SMS in dem Format: **"SNLANG_registration code"** an die Telefonnummer **+420 773 181 815** gesendet werden. Kurz darauf wird eine Antwort mit dem Aktivierungscode gesendet. Der Aktivierungscode kann 8 bis 14 Ziffern und Groß- und Kleinschreibung enthalten. Der erhaltene Aktivierungscode sollte in der Registerkarte Systemübersicht in F-Link mit der Taste „Aktivieren“ eingegeben werden.



Beispiel der Anforderung per SMS

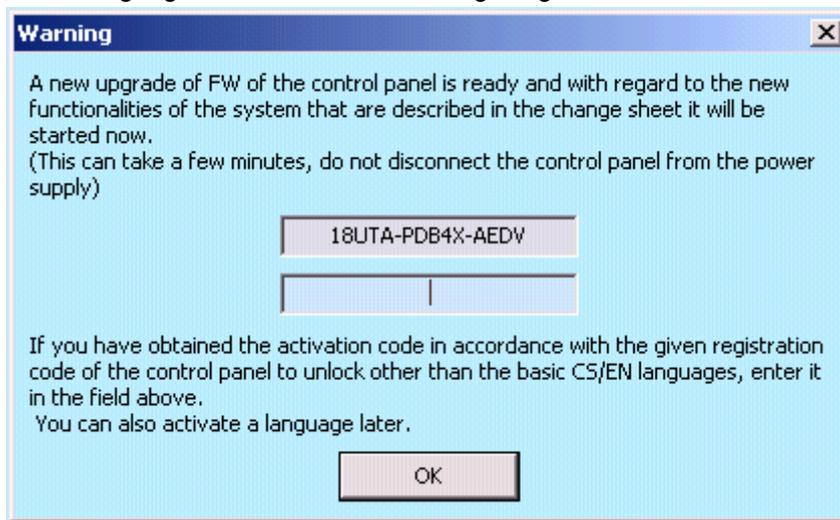
- Der Aktivierungscode kann von einem Händler erhalten werden. Wenn Sie den Aktivierungscode anfordern, müssen Sie den Anmeldecode der Zentrale angeben. Je nach Land kann sich der Aktivierungscode auch auf der Verpackung der Zentrale befinden.

10.1. F-Link starten und die Systemgröße einstellen

1. Verbinden Sie einen Computer über ein USB-Kabel mit der Zentrale - der Computer initialisiert das neue USB-Gerät (beim ersten Verbindungsaufbau mit der Zentrale es kann etwas länger dauern).
2. Nach dem Verbindungsaufbau werden zwei neue Laufwerke angezeigt: FLEXI_CFG und FLEXI_LOG. Sie können diese einfach schließen
3. Starten Sie F-Link. Bei einer Zentrale mit Standardeinstellungen öffnet sich das **Einstellungsfenster** und das System schaltet sich dann automatisch in den Servicemodus (Errichter-Modus). Wenn die Zentrale zuvor konfiguriert wurde (der Errichter-Code wurde geändert), fordert die Software die Eingabe des Codes an - dieser ist in dem Format **cccc** einzugeben (die Standardeinstellung des Errichter-Codes ist 1010). Wenn das Präfix (im Einstellungsfenster in F-Link) aktiviert wurde, ist er 0*cccc (0*1010). Sie können die Option **Merken** verwenden. Damit speichert die Software den Code, bis die Datenbank geschlossen wird. Verwenden Sie die Option **Display-Code (Code anzeigen)**, um den eingegebenen Code zu prüfen. Wenn Sie z.B. eine alphanumerische Tastatur verwenden, können Sie sehen, wo ein möglicher Eingabefehler ist.

Hinweis: Nach dem Herstellen der Verbindung mit dem USB-Kabel wird die Möglichkeit, Änderungen an den Einstellungen über die LCD-Tastatur zu programmieren, deaktiviert (der Menüpunkt Einstellungen wird deaktiviert). Nach dem Trennen des Kabels erscheint die Position nach einigen Sekunden wieder im Menü.

4. Nach der gültigen Berechtigung kann diese Nachricht angezeigt werden:



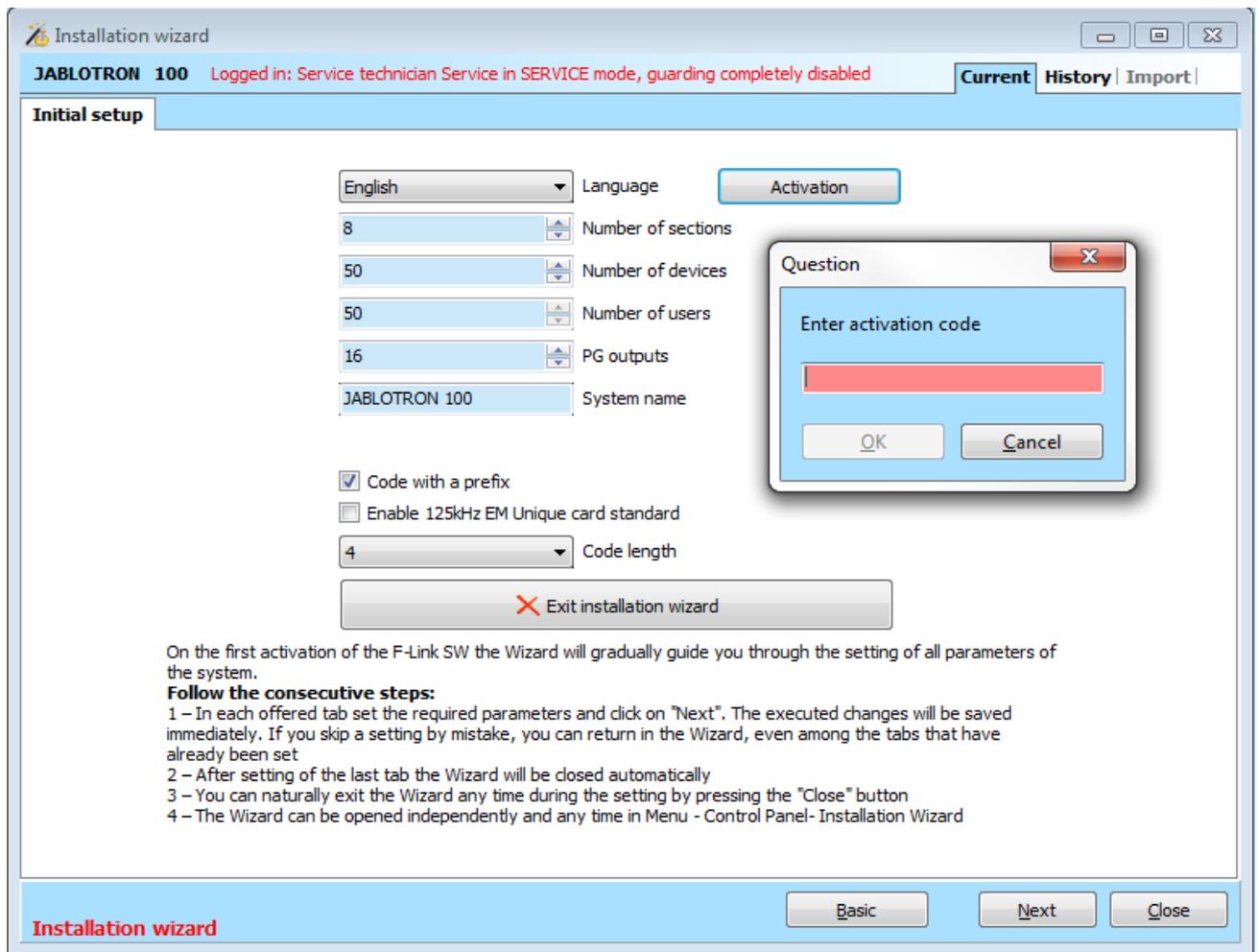
In solch einem Fall empfehlen wir, eine Aktualisierung durchzuführen. Durch Klicken auf OK wird das neue Firmware-Paket heruntergeladen, was einige Minuten dauern kann. Wenn die Aktualisierung abgeschlossen ist, erscheint der Assistent für die Erstkonfiguration.

10.2. Start des Assistenten

1. Stellen Sie in jeder angebotenen Registerkarte den gewünschten Parameter ein und klicken Sie auf „Weiter“. Wenn Sie versehentlich eine Einstellung übersprungen haben, können Sie zu der Registerkarte zurückkehren, die zuvor im Assistenten festgelegt wurde.
2. Nach dem Einstellen der letzten Registerkarte drücken Sie „Speichern“ und schließen den Assistenten mit der Schaltfläche „Beenden“.
3. Nach dem Beenden werden Sie gefragt, ob Sie den Installationsassistenten beim nächsten Start von F-Link starten möchten.
4. Sie können den Assistenten jederzeit während der Einstellung durch Drücken der Taste „Exit“ verlassen.
5. Sie können den Assistenten unabhängig und jederzeit im Menü „Systemsteuerung / Installationsassistent“ starten.

10.3. Registerkarte Systemübersicht

Diese Registerkarte wird verwendet, um die Basisgröße des Systems festzulegen. Die festgelegten Werte können jederzeit geändert werden. Die Bereichswerte beeinflussen die Größe der Datenbank und damit den Zeitaufwand für das Laden und Speichern von Daten (in der Regel per Fernzugriff). Um Änderungen auf dieser Registerkarte vorzunehmen, ist der Errichtermodus nicht notwendig. Beim ersten Start von F-Link führt Sie der Assistent schrittweise durch die Einstellung aller Systemparameter.



Aktivierung: Durch die Eingabe eines speziellen Aktivierungs-codes können Sie eine Sprache (Sprachen) zur Auswahl der Sprachen hinzufügen, die für das Land, für das Zentrale bestimmt ist, freigegeben sind.

Hinweise:

- Wenn eine der Standardsprachen (EN/CZ) benötigt wird, wird die Aktivierungsfunktion nicht benötigt.
- Wenn Sie eine andere Sprache anfordern, können Sie nach Eingabe des Aktivierungs-codes im Menü Sprache eine der verfügbaren Sprachen auswählen.
- Sie müssen auch die Firmware der drahtlosen Komponenten aktualisieren (besonders Zugriffsmodule mit Display, um auch die ausgewählte Sprache zu erhalten).

Beschreibung der Registerkarte Systemübersicht:

Codes mit einem Präfix – Diese Funktion legt fest, wie alle Zugangscodes für die Benutzerberechtigung eingegeben werden. Wenn die Funktion aktiviert ist, benötigt das System ein 1- bis 3-stelliges Präfix (Position des Codes), das mit einem * -Symbol vor einem Zugriffscode (z. B. 12 * 3456) endet. Benutzer können ihre eigenen Codes vom LCD-Tastatur aus ändern. Um das System jedoch steuern zu können, müssen Sie einen Code mit der fortlaufenden Nummer des Codes (Präfix) verwenden. Wenn dieser Parameter deaktiviert ist, muss nur ein vierstelliger Zugangscodes eingegeben werden. Die Codes dürfen nur vom Systemadministrator geändert werden, der die Codes zuweist und als einziger berechtigt ist, die Benutzerrechte zu ändern (also er / sie wird von ihnen kennen). Der Administrator ist auch dafür verantwortlich, dass keine Codes dupliziert werden.

Warnhinweis: Immer wenn dieser Parameter deaktiviert wird, werden alle Benutzer-codes und Einstellungen des Service-Codes (Errichter-Codes) und des Administrator-Codes irreversibel gelöscht und die Standardwerte wiederhergestellt. Benutzerberechtigungen und die RFID-Karte / Tags von bereits bestehenden Benutzern werden nicht geändert.

Aktivierung der standardisierten 125kHz EM UNIQUE-Karte – Bei Deaktivierung dürfen nur die von einem Hersteller empfohlenen RFID-Karten / Tags (JA-190J, JA-191J, JA-192J, JA-194J) verwendet werden. Falls aktiviert, sind auch Karten anderer Hersteller erlaubt, die mit der oben genannten Frequenz arbeiten.

Codelänge – Um die Sicherheit des Alarmsystems während der Berechtigung zu erhöhen, ist es möglich, die Benutzer-codelänge unabhängig von der Präfixfunktion vorzugeben. Es können 4, 6 oder 8-stellige Codes geben. Wenn die Codelänge geändert wird, werden die Service- und Administrator-codes auf die Standardwerte gesetzt und frühere voreingestellte Codes werden gelöscht.

10.4. Registerkarte Bereichsübersicht

Wird verwendet, um Parameter von unabhängig gesteuerten überwachten Bereichen (Zonen) zu konfigurieren. Um Änderungen in dieser Registerkarte vorzunehmen, ist der Errichter-Code nicht notwendig.

Position	Section name	Common section	Partial setting	Siren ON/OFF	Report unset ...	Limited access time	Section disabled	Status	Note
1	Groud floor	No	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No		Service mode	
2	First floor	No	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No		Service mode	
3	Garage	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No		Service mode	
4	Fully set	1, 2, 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No		Service mode	
5	Section 5	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No		Service mode	
6	Section 6	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No		Service mode	
7	Section 7	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No		Service mode	
8	Section 8	No	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No		Service mode	

* Die unten beschriebenen und mit * markierten Positionen werden nur angezeigt, wenn die **Erweiterten Einstellungen** aktiviert sind.

Bereichsname – Die Benennung der Bereiche wird verwendet, um Textmeldungen von Ereignissen zu machen (SMS), zur Anzeige auf einer LCD-Tastatur und im Speicher, zur besseren Erkennung in einer Meldung (z.B. Erdgeschoss, Geschäft, ...).

Gemeinsame Bereiche – Damit können Sie auswählen, dass ein Bereich automatisch scharf geschaltet wird, wenn alle Bereiche, für die er als gemeinsamer Bereich dient, scharf geschaltet sind (geeignet für Korridore, Treppen und andere allgemeine Bereiche). Warnhinweis zu einer Einschränkung der möglichen Verwendung des Tastaturbereichs für den gemeinsamen Bereich: Wenn einer der Bereiche separat deaktiviert wurde, kann das gemeinsame Bereich **nicht** zum Deaktivieren der übrigen Bereiche verwendet werden. Diese Bereiche müssen separat deaktiviert werden.

Teilscharf* – Damit können Sie einen Bereich teilweise scharf schalten, wenn jemand im Innenbereich bleibt (Melder mit ausgewählter Reaktion des Typs „Teilscharf“ sind nicht aktiv - siehe Kapitel 8 Systemkonfiguration). Ohne Aktivierung dieses Parameters kann die teilweise Scharfschaltung im Bereich nicht verwendet werden.

Keine Bewegung im Bereich* – Wenn ein Bereich unscharf geschaltet ist und während einer festgelegten Zeitspanne kein Melder aktiviert wird, wird die Meldung „Unscharfer Bereich“ verwendet. Die Zeitspanne wird in der Registerkarte Systemparameter / Unscharfen Bereich melden nach (1 - 48 Std.) festgelegt.

Automatische Scharfschaltung – Diese Funktion eignet sich zur automatischen Scharfschaltung eines Bereichs, der als „Unscharfer Bereich“ gemeldet wurde.

In der Registerkarte Systemparameter können Sie ein Zeitintervall in Minuten einstellen, nach dem der Bereich automatisch scharf geschaltet wird. Das Zeitintervall beginnt in dem Moment, in dem „Unscharfer Bereich“ gemeldet wird. Diese Funktion ist eine Ergänzung der Funktion „Unscharfen Bereich melden“ und kann nur verwendet werden, wenn die Funktion „Unscharfen Bereich melden“ aktiviert ist.

Zutrittszeiten* – Sie können einen wöchentlichen Zeitplan festlegen, der das Deaktivieren eines Bereichs für ausgewählte Benutzer zulässt.

Status – Die Funktion zeigt den aktuellen Status eines Bereichs an (Unscharf, Scharf, Ausgangsverzögerung, Eingangsverzögerung, Teilweise Scharf, Alarm, Alarmspeicher, Deaktiviert, Servicemodus). Durch Drücken der Taste kann das System entsprechend der Berechtigung Ihres Logins gesteuert werden (es ändert den Bereichsstatus - scharf/ unscharf).

Notiz – Sie können Details eines Bereichs zur einfacheren Orientierung bei der jährlichen Inspektionen beschreiben.

10.5. Registerkarte Komponentenliste

Ein im System installiertes Gerät wird angemeldet und seine Parameter eingestellt. Die Zentrale wird automatisch auf Position 0 im Bereich 1 angemeldet und kann nicht entfernt oder gelöscht werden. Änderungen sind nur im Servicemodus (Errichter-Modus) möglich.

Name	Type	Section	Reaction	Internal	PG activation	Interna...	Supervision	Alarm...	Disable	Status
0 Control panel	JA-101K	1: Groud floor				Enter				OK
1 Radio module	JA-110R	1: Groud floor				Enter	<input checked="" type="checkbox"/>			OK
2 LCD keypad	JA-114E	1: Groud floor				Enter	<input checked="" type="checkbox"/>			OK
3 Main door	JA-110M	1: Groud floor	Delayed zone A alarm	<input type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		ACT
4 Kitchen window	JA-110M	1: Groud floor	Instant zone alarm	<input type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
5 Garage door	JA-111M	3: Garage	Delayed zone C alarm	<input type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		ACT
6 Hall	JA-110P	1: Groud floor	Next delay zone alarm	<input checked="" type="checkbox"/>	2: Light hall	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
7 Garage PIR	JA-120PW	3: Garage	Delayed zone C alarm	<input type="checkbox"/>	3: Light garage	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
8 Indoor siren	JA-110A	1: Groud floor	Siren mute			Enter	<input checked="" type="checkbox"/>			OK
9 Balcony door	JA-150M	2: First floor	Instant always	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>			ACT
10 Balcony window	JA-150M	2: First floor	Instant always	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>			OK
11 Living room	JA-151P	2: First floor	Instant zone alarm	<input checked="" type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>			ACT
12 Interface	JA-121T	1: Groud floor				Enter	<input type="checkbox"/>			OK
13 Remote control	JA-182J	4: Fully set	Set		No	Enter	<input type="checkbox"/>			
14 Device 14	Enroll	1: Groud floor	-	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
15 Device 15	Enroll	1: Groud floor	-	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
16 Device 16	Enroll	1: Groud floor	-	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
17 Device 17	Enroll	1: Groud floor	-	<input type="checkbox"/>	Nn		<input checked="" type="checkbox"/>	<input type="checkbox"/>		

* Die unten beschriebenen und mit * markierten Positionen werden nur angezeigt, wenn die **Erweiterten Einstellungen** aktiviert sind.

Name - wird in textuellen Ereignismeldungen und beim Auslesen des Speichers verwendet (Beispiel: Eingangstür).

Bezeichnung – zeigt den zugewiesenen Gerätetyp an. Ein neues Gerät kann an einer leeren Position angemeldet werden. **Zur Anmeldung von Geräten**, siehe Kapitel 8.4.1 Geräte anmelden und löschen.

Bereich – bestimmt, welchem überwachten Bereich das Gerät Ereignisse meldet (Alarm, Sabotage, Fehler...). Hinweis: Die Unterteilung eines Gebäudes in Bereiche - siehe Kapitel 10.4 Registerkarte Bereich.

Reaktion – definiert, welche Reaktion durch die Aktivierung eines bestimmten Geräts ausgelöst wird. Wenn ein Gerät keinen Alarmeingang hat (z.B. ein BUS-Modul), kann ihm keine Reaktion zugewiesen werden. Die vollständige Reaktionsliste für Geräte wird bei Aktivierung der erweiterten Einstellungen angezeigt. Sie finden eine Beschreibung aller Reaktionen in Kapitel 8.4.2. Liste der anwendbaren Reaktionen.

Teilscharf* – Dieser Parameter ist nur für Einbruchsmelder verfügbar. Signale von Geräten mit dieser Anzeige werden nicht als Alarmsignale gewertet, wenn ein Bereich teilweise scharf ist. Teilweise Scharfschaltung eines Bereichs - siehe Kapitel 10.4 Registerkarte Bereiche.

Aktiviert PG-Ausgang* – Die Aktivierung eines Gerätes kann programmierbare PG-Ausgänge mit ihren definierten Reaktionen aktivieren. Diese Option ist mit dem Menüpunkt PG-Ausgängen / Aktivierung / durch ein Gerät verknüpft.

Interne Einstellungen – Zugriff auf die Einstellungen interner Parameter von Perimetern, die an den BUS angeschlossen sind oder bidirektionale drahtlose Kommunikation bieten. Einzelne Geräte haben unterschiedliche interne Parameter (einige haben keine). Die internen Einstellungen einer Tastatur sind in Kapitel 10.5.1 Tastaturkonfiguration beschrieben. Einstellungen anderer Geräte sind in ihren Handbüchern beschrieben.

Funküberwachung* – Damit können Sie die Überprüfung der regulären Kommunikation mit drahtlosen Geräten deaktivieren (sie kann nicht für BUS-Elemente deaktiviert werden). Standardmäßig ist die Einstellung von drahtlosen Geräten (außer Fernbedienungen und Paniktasten) immer aktiviert.



Deaktivieren – kann auf 2 Stufen vorgenommen werden und wird anhand der Berechtigung vorgegeben:

1. **Eingangssperrung** (gelber Punkt), dient zur dauerhaften Sperrung eines Meldereingangs (BLK). Das System ignoriert jede Geräteaktivierung = ein Alarm wird nicht ausgelöst und der PG wird nicht gesteuert, aber Sabotagealarme und Fehler werden wie üblich erkannt.
2. **Gerätedeaktivierung** (roter Punkt), dient zur vollständigen Gerätedeaktivierung (Deaktiviert). Das System ignoriert alle verbundenen Gerätefunktionen = kein Alarm, Sabotagealarm, PG-Aktivierung, Fehler, Meldung...).

Sie können nicht die Zentrale oder ein Gerät, dessen Reaktion auf Panik eingestellt ist, deaktivieren.

Status – zeigt den aktuellen Status eines Geräts an. OK = alles in Ordnung, TMP = Sabotage, ACT = Alarmeingang aktiviert, BLK = gesperrt, Deaktiviert = deaktiviert, ERR = Fehler, ?? = keine Kommunikation mit dem Gerät, Stromversorgung = Versorgungsausfall, Batterie = nicht aufgeladene oder nicht angeschlossene Batterie in der Zentrale, Laden – Laden der Backup-Batterie im Gerät oder der Zentrale, BOOT – Aktualisierung des Geräts ist im Gang oder die Aktualisierung ist fehlgeschlagen (Aktualisierung wiederholen). Bewegen Sie den Cursor auf dem STATUS des Geräts hin und her, um die detaillierten Daten zu sehen.

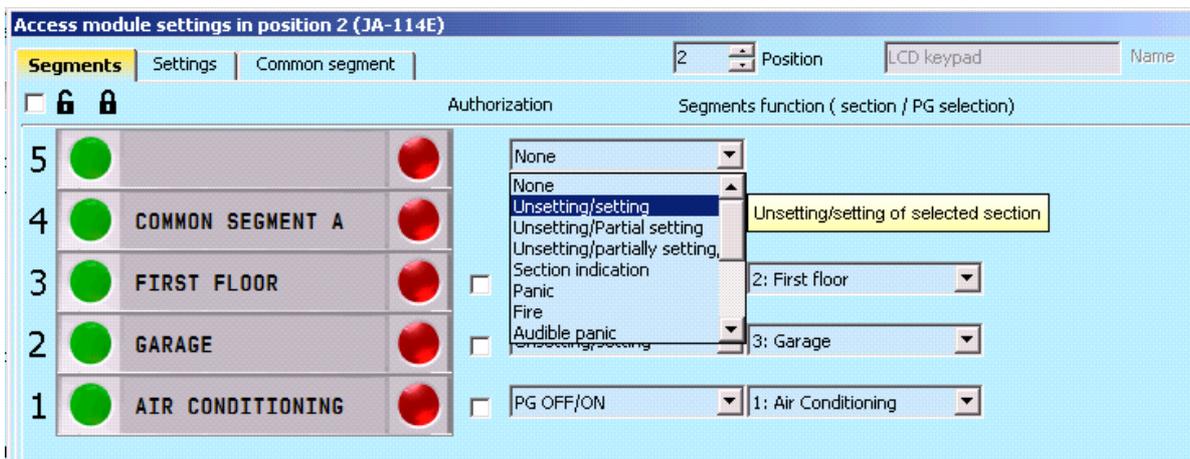
Hinweis – ermöglicht die detaillierte Beschreibung des Geräts, z.B. Ort, letzter Batteriewechsel, durchschnittliche RF-Signalstärke bei der letzten Prüfung u.s.w..

10.5.1. Konfiguration der Bedienteile

- Setzen Sie zuerst die Steuerungstastatur mechanisch zusammen. Befestigen Sie die erforderliche Anzahl von Steuerungsbereichen (Segmenten) (max. 20) an dem ausgewählten Zugriffsmodul. Ihre internen Kabel müssen miteinander verbunden sein.
- Melden Sie die Tastatur an der ausgewählten Position im System (siehe Kapitel 5 Installation von BUS-Geräten) an.
- Bei Eingabe der internen Einstellungen der Tastatur (Registerkarte Komponentenliste) öffnet sich das folgende Fenster (das Beispiel bezieht sich auf die Tastatur JA-114E), bei anderen Tastaturen kann der Einstellbereich kleiner sein.

Beispiel der internen Einstellungen einer Tastatur:

10.5.1.1. Registerkarte Segmente



Sperrung gesperrt / entsperrt – aktiviert die Anzeige der Sperrsymbole für die Tasten der Bereichssteuerung (Segmente) und die Punktsymbole (leer / voll) für die Steuerung der PG-Ausgänge. Die Symbole werden beim Drucken der Etiketten berücksichtigt.

Text der Etikette der Steuerungsbereiche (Segmente) – Der Name des Bereichs (in der Registerkarte Bereiche) oder der Name des PG-Ausgangs (in der Registerkarte PG-Ausgänge) wird angezeigt. Sie können hier auch den gesamten zu druckenden Text bearbeiten, indem Sie auf den entsprechenden Text klicken. Diese Änderungen werden nicht im System gespeichert und dienen nur dem Etikettendruck. Die Taste Etiketten drucken (in der unteren Leiste der Karte) wird zum Drucken der Beschriftungen der Bereiche (Segmente) verwendet.

Etiketten drucken – ermöglicht den direkten Druck von voreingestellten Etikettentexten mit dem installierten Drucker. Sie können die Texte bearbeiten, indem Sie auf das Segment klicken, wodurch sich nur eine Änderung für den Druck ergibt und die geänderten Texte nicht in der Datenbank gespeichert werden. Sie können bequem den Etikettendrucker PT-P700 von JABLOTRON verwenden, der automatisches Schneiden mit der erforderlichen Etikettengröße ermöglicht.

Import – ermöglicht das Kopieren der aktuellen Tastatureinstellungen auf andere Tastaturen, z. B. wenn ein überwachtes Gebäude mehrere Eingänge hat und jeder Eingang eine Tastatur mit den gleichen Funktionen benötigt. Für den gleichen Tastaturtyp ist eine Kopie möglich. Die Funktion kann ebenso verwendet werden, wenn eine Tastatur durch eine neue ersetzt wird. Die Taste Importieren bietet Ihnen den Verlauf der letzten bekannten Einstellungen der Tastatur an der angegebenen Position.

Autorisierung – Die Berechtigung des Benutzers ist für die Scharfschaltung und Unscharfschaltung erforderlich. Wenn dieser Parameter deaktiviert ist, können alle Bereiche (Segmente) ohne Berechtigung gesteuert werden, mit Ausnahme der Funktion „Bereich unscharf schalten“, für die immer eine Berechtigung erforderlich ist. Für das Aktivieren und Deaktivieren von PG-Ausgängen muss die Funktion Berechtigung / ohne Berechtigung eingestellt werden.

Segmentfunktionen – auf der linken Seite wird die Funktion des Segments ausgewählt, auf der rechten Seite der Bereich oder der PG-Ausgang, der der ausgewählten Funktion zugewiesen ist. Folgende Funktionen können einem Segment zugeordnet werden:

Keine	Segment aus, verwendet für Segmente, die als Reserve dienen.
Unscharf / Scharf	Bereichssteuerung. Segmentanzeige: Bereich unscharf = grün, scharf = rot.
Unscharf / Teilscharf	Ermöglicht die Aktivierung des Bereichsmodus teilweise scharf (Aktivierung in der Registerkarte Bereiche). Segmentanzeige: Bereich unscharf = grün, teilweise scharf = gelb.
Unscharf / Teil- / Scharf	Ermöglicht die Auswahl der Einstellungsstufe. Nach Betätigen der rechten Taste (Scharf) ist die teilweise Scharfschaltung verfügbar, nach wiederholtem Drücken ist das System vollständig scharf geschaltet. Für diese Auswahl muss die teilweise Scharfschaltung für den Bereich in der Registerkarte Bereiche aktiviert werden. Segmentanzeige: Bereich unscharf = grün, teilweise scharf = gelb, vollständig scharf = rot.
Zeigt den Status an	Das Segment zeigt nur den Status des Bereichs an, aktiviert aber nicht seine Steuerung (geeignet z.B. zur Anzeige des Status von gemeinsamen Bereichen, Treppenhaus usw.). Wenn ein Alarm ausgelöst wird, können Sie ihn durch Drücken der grünen Segmenttaste mit anschließender gültiger Berechtigung des Benutzers abrechnen.
Stiller Überfallalarm	Das Segment kann einen stummen Überfall- oder auch Geiselnahmealarm auslösen. Nach Betätigen der rechten Taste wird eine Überfallmeldung von dem Bereich, dem die Funktion zugewiesen ist, ohne akustische Anzeige gesendet. Der Panikalarm kann auch mit anpassbarer Zeit und der Möglichkeit, ihn zu beenden, bevor die voreingestellte Zeit abgelaufen ist, verzögert werden (siehe verzögerter Panikalarm). Wenn der Bereich scharf geschaltet ist, kann er nicht unscharf geschaltet werden.
Brandalarm	Das Segment löst einen Feueralarm aus. Nach Drücken der rechten Segmenttaste blinkt diese 3 Sekunden lang rot (während dieser Zeit kann der Feueralarm durch Drücken der linken Segmenttaste abgebrochen werden). Dann wird der Feueralarm von dem Bereich ausgelöst, dem das Segment zugewiesen ist.
Lauter Überfallalarm	Das Segment aktiviert einen lauten Panikalarm. Nach Betätigung wird ein lauter Panikalarm in dem Bereich aktiviert, dem das Segment zugewiesen ist. Der laute Panikalarm kann auch mit anpassbarer Zeit und der Möglichkeit, ihn zu beenden, bevor die voreingestellte Zeit abgelaufen ist, verzögert werden (siehe verzögerter Panikalarm). Wenn der Bereich scharf geschaltet ist, kann er nicht unscharf geschaltet werden.
Notruf	Mit diesem Segment können Sie einen Bericht über gesundheitliche Probleme senden (ohne eine Sirene zu aktivieren). Nach Drücken der rechten Segmenttaste blinkt diese 3 Sekunden lang rot (während dieser Zeit ist es möglich, den medizinischen Störungsbericht durch Drücken der linken Segmenttaste abzubrechen). Dann kehrt das Segment in den Standby-Modus zurück und das System sendet den medizinischen Fehlerbericht aus dem Bereich, dem das Segment zugewiesen ist.
PG AUS/ PG EIN	Mit diesem Segment können Sie einen PG-Ausgang steuern. Anzeige: PG inaktiv = grün, PG aktiv / aktiviert = rot.
PG EIN	Das Segment kann nur verwendet werden, um den PG-Ausgang zu aktivieren (z. B. das Einschalten der Lichter für eine voreingestellte Zeit).
PG AUS	Das Segment kann nur verwendet werden, um den PG-Ausgang zu sperren (z. B. Funktion einer Notfall-STOP-Taste).

Zeigt nur PG-Status an	Das Segment zeigt nur den Status des PG-Ausgangs ohne die Möglichkeit an, ihn zu steuern (rot zeigt den aktiven Status an).
Zeigt PG invers an	Das Segment zeigt nur den Status eines PG-Ausgangs mit der umgekehrten Logik (grün zeigt einen aktiven Status an) ohne Steuerungsmöglichkeit an.
Gemeinsames Segment A / B	<p>Ermöglicht die gleichzeitige Steuerung mehrerer Bereiche, die über individuelle Segmente auf der Tastatur verfügen. Nach Betätigung der Taste auf dem selben Segment wird der Befehl Unscharf/Scharf für die ausgewählten Bereichssegmente ausgeführt. Wenn einige Bereiche, die vom Gemeinsamen Segment gesteuert werden, scharf und die anderen unscharf geschaltet werden, werden die verbleibenden Bereiche nach Verwendung des Gemeinsamen Segments scharf / unscharf geschaltet. Wenn die teilweise Scharfschaltung für eine der ausgewählten Segmente aktiviert wird (siehe 9.2 Systemsteuerung über die Tastatur), verhält sich das Gemeinsame Segment wie folgt: 1. Drücken zur Scharfschaltung = teilweise Scharfschaltung, 2. Drücken zur Scharfschaltung = vollständige Scharfschaltung. Es ist nicht ratsam, die Funktion Gemeinsames Segment mit den Funktionen Bereich/Gemeinsam für Bereiche zu kombinieren.</p> <p>Anzeige des Gemeinsamen Segments: alle Bereiche unscharf = grün, alle Bereiche vollständig scharf = rot, jeder Bereich scharf (teilweise scharf) = gelb.</p> <p>Die Bereiche werden dem Gemeinsamen Segment in einem anderen Fenster zugewiesen, wenn diese Option ausgewählt ist.</p> <p>Hinweis: Der Menüpunkt „Gemeinsames Segment x“ ist nur verfügbar, wenn mehr als zwei Segmente für die Bereichssteuerung mit dem Modul verbunden sind.</p>
Zeigt PG an + steuert	Das Segment kann einen anderen PG-Ausgang steuern als den, den es optisch anzeigt. In diesem Menü wird der erste Parameter verwendet, um den PG-Ausgang für die Anzeige auszuwählen und der andere (zusätzlich), um den zu steuernden PG-Ausgang auszuwählen. Die Funktion wird z.B. verwendet, um ein Garagentor mit einem PG-Ausgangsimpuls zu steuern, während das Segment den tatsächlichen Status des Tors anzeigt, der vom Tormelder erhaltenen wird.

10.5.1.2. Registerkarte Einstellungen

Access module settings in position 7 (JA-114E)

Segments Settings Common segment 7 Position Periferie 7 Name

Acoustic indication of selected sections

- Higher volume
- Alarms
- Entrance delay
- Exit delay
- Exit delay when partially set
- Segment status change

Backlight intensity:

- Segments
- Keypads
- Display

Acoustic indication for sections:

- 1: Sekce 1
- 2: Sekce 2
- 3: Sekce 3
- 4: Sekce 4
- 5: Sekce 5
- 6: Sekce 6
- 7: Sekce 7
- 8: Sekce 8
- 9: Sekce 9
- 10: Sekce 10
- 11: Sekce 11
- 12: Sekce 12
- 13: Sekce 13
- 14: Sekce 14
- 15: Sekce 15

Function:

Permanently ON (dropdown) RFID reader

1. Indicates permanently (dropdown) Optical indication setting

- Indicates PG status changes
- Indicate Unset status
- Indicate Set status
- Unset section by authorisation only during entrance delay
- LCD backlight goes off in 5s

10 (slider) Delayed panic [s]

Display on the LCD:

1.line: JABLOTRON 100 Temperature: No (dropdown)

2.line: User-defined text Temperature: No (dropdown)

Date and time

Section control from menu:

- 1: Sekce 1
- 2: Sekce 2
- 3: Sekce 3
- 4: Sekce 4
- 5: Sekce 5
- 6: Sekce 6
- 7: Sekce 7
- 8: Sekce 8
- 9: Sekce 9
- 10: Sekce 10
- 11: Sekce 11
- 12: Sekce 12
- 13: Sekce 13
- 14: Sekce 14
- 15: Sekce 15

Print labels Import OK

Akustische Anzeige der ausgewählten Bereiche:

Erhöhte Lautstärke	Einstellung der Lautstärke außer für den Alarm
Alarm	akustischer Ausgang bei einem Alarm (Sirenton)
Eingangsverzögerung	dauerhafter Pfeifton während einer Eingangsverzögerung
Ausgangsverzögerung	langsame intermittierende Pieptöne (1/s)
Ausgangsverzögerung bei Teilscharfschaltung	langsame intermittierende Pieptöne (standardmäßig aus)
Zustandsänderung am Segment	akustische Anzeige mit einem Piepton pro Änderung

Funktionen:

RFID-Lesegerät	Um Energie zu sparen, wird die Aktivität des Lesers auf 3 Sek. nach Drücken seiner Abdeckung beschränkt. Der RFID-Leser kann auch vollständig deaktiviert werden. Diese Einstellung gilt für drahtlose Tastaturen und Zugriffsmodule mit permanenter Stromversorgung von einer externen Quelle, sonst wird sich der RFID-Leser immer automatisch ausschalten.	
	Dauerhaft eingeschaltet	Der RFID-Leser ist dauerhaft aktiviert. Bei einer BUS-Tastatur wird die Weck-Einstellung nicht berücksichtigt.
	Durch Drücken aktiv	Wecken des RFID-Lesers für 3 Sek. nach Aktivierung auf der Tastatur.
	Dauerhaft ausgeschaltet	Der RFID-Leser ist dauerhaft deaktiviert.
Einstellungen der Anzeige	Aktivierung durch Drücken oder Autorisierungsanforderung	Wecken des RFID-Lesers nach Aktivierung der Tastatur oder der Berechtigungsanforderung
	1 dauerhaft eingeschalten	Die Anzeige einer BUS-Tastatur ist permanent. Bei einer drahtlosen Tastatur ist die Anzeige nur mit einer Versorgung von einer externen Stromquelle dauerhaft. Ohne externe Stromversorgung ist das Verhalten wie bei Option 2.
	2. Zustandsänderung des Bereichs/PGs - Bedienteil	Die Tastatur zeigt eine Statusänderung eines Bereichs / PG an. Eine Änderung des Bereichsstatus wird nur über das entsprechende Segment angezeigt. Eine Eingangsverzögerung und ein Alarm werden von der ganzen Tastatur angezeigt.
	3. Zustandsänderung des Bereichs/PGs - Segment	Die Tastatur zeigt eine Statusänderung eines Bereichs/ PG an. Eine Statusänderung eines Segments, eine Eingangsverzögerung und ein Alarm werden nur für das entsprechende Segment angezeigt.
	4. Zustandsänderung des Segments	Eingangsverzögerungen und Alar me werden nur akustisch angezeigt. Die Statusänderung eines Bereichs / PG wird nur auf dem entsprechenden Segment angezeigt. Diese Option ist die Standardeinstellung.
	5. Eingangsverzögerung und Alarm	Eine Tastatur zeigt eine Eingangsverzögerung und einen Alarm auf dem entsprechenden Segment an. Eine Statusänderung eines Bereichs / PG wird nicht angezeigt.
6. Aktivierung des Zugangmoduls	Die Tastatur bietet nur optische und akustische Anzeigen nach Öffnung der Frontabdeckung, Drücken Sie eine Taste, ein Segment oder die Frontabdeckung.	

Zeigt die PG-Zustandsänderung an	Die optische Anzeige des Ausgangsstatus eines PGs ändert sich auf einem Segment. Dies bezieht sich auf die Einstellungen der Anzeige - Optionen 2 - 4. Bei Deaktivierung werden die Änderungen des PG-Ausgangsstatus nicht optisch angezeigt.
Status „Unscharf“ anzeigen	Tastatursegmente zeigen einen unscharfen Status ohne Berechtigung an. Bei Deaktivierung zeigen sie diesen Status nur während einer gültigen Berechtigung an.
Status „Scharf“ anzeigen	Tastatursegmente zeigen einen scharfen Status ohne gültige Berechtigung an. Bei Deaktivierung zeigen sie diesen Status nur während einer gültigen Berechtigung an.
Unscharfschaltung nach Autorisierung nur während der Eingangsverzögerung	Wenn diese Option aktiviert ist, wird ein Bereich, in dem die Eingangsverzögerung gestartet wurde, nur durch eine gültige RFID-Karte / Tag oder die Codeberechtigung unscharf geschaltet. Mit drahtlosen Tastaturen kann die Berechtigung ausgeführt werden, nachdem die Eingangsverzögerung ausgelöst wurde. Vorsicht: Wir empfehlen Ihnen dringend, diese Funktion zu deaktivieren, wenn die Eintrittsverzögerung normalerweise für einen gemeinsamen Bereich gilt, andernfalls werden alle Bereiche, die dem allgemeinen Bereich zugewiesen sind, durch eine bestimmte Berechtigung unscharf geschaltet.
Hintergrundbeleuchtung des Displays erlischt nach 5s	Wenn diese Option aktiviert ist, erlischt die LCD-Hintergrundbeleuchtung 5 Sekunden nach dem letzten Bedienvorgang mit einem Gerät (Drücken einer Taste, eines Segments oder einer Frontabdeckung). Bei Aktivierung wird die Hintergrundbeleuchtung im selben Moment wie die gesamte Tastatur ausgeschaltet. Die Aktivierung dieser Option verlängert die Lebensdauer der Batterie.
Verzögerungszeit Überfallalarm	Die Funktion dient dazu, das Auslösen eines stummen oder hörbaren Überfall- oder Geiselnahmealarms um eine voreingestellte Zeit hinauszuschieben. Es ist möglich, das Zeitintervall zum Abbrechen der Aktivierung zu bestimmen. Dazu drücken Sie wiederholt dieselbe für den stummen oder hörbaren Überfallalarm voreingestellte Segmenttaste. Durch Drücken der rechten (roten) Taste wird der Timer ausgelöst und durch Drücken der linken (grünen) Taste wird dieser abgebrochen. Wenn die Berechtigung aktiviert ist, ist sie auch für die Aktivierung und Deaktivierung erforderlich. Die Verzögerung ist von 1 Sekunde bis 255 Sekunden einstellbar.

Displayanzeige:

1. Zeile	Ermöglicht Ihnen, einen Text einzugeben, der in der ersten Zeile des LCD-Bildschirms der Tastatur angezeigt wird, wenn keine anderen wichtigeren Informationen angezeigt werden, z. B. Firmenname, Name des Gebäudes, Beschreibung der angezeigten Temperatur usw.
2. Zeile	Ermöglicht Ihnen, einen Text einzugeben, der in der zweiten Zeile des LCD-Bildschirms der Tastatur angezeigt wird, wenn keine anderen wichtigeren Informationen angezeigt werden, z. B. Firmenname, Name des Gebäudes, Beschreibung der angezeigten Temperatur usw.
Datum und Uhrzeit	Möglichkeit, Datum und Uhrzeit der Zentrale auf dem LCD-Bildschirm der Tastatur anzuzeigen.
Temperaturfühler	Möglichkeit, die Temperatur des 1. Thermometers oder Thermostats auf dem Bildschirm anzuzeigen.
Temperaturfühler	Möglichkeit, die Temperatur des 2. Thermometers oder Thermostats auf dem Bildschirm anzuzeigen.

Lichtintensität:

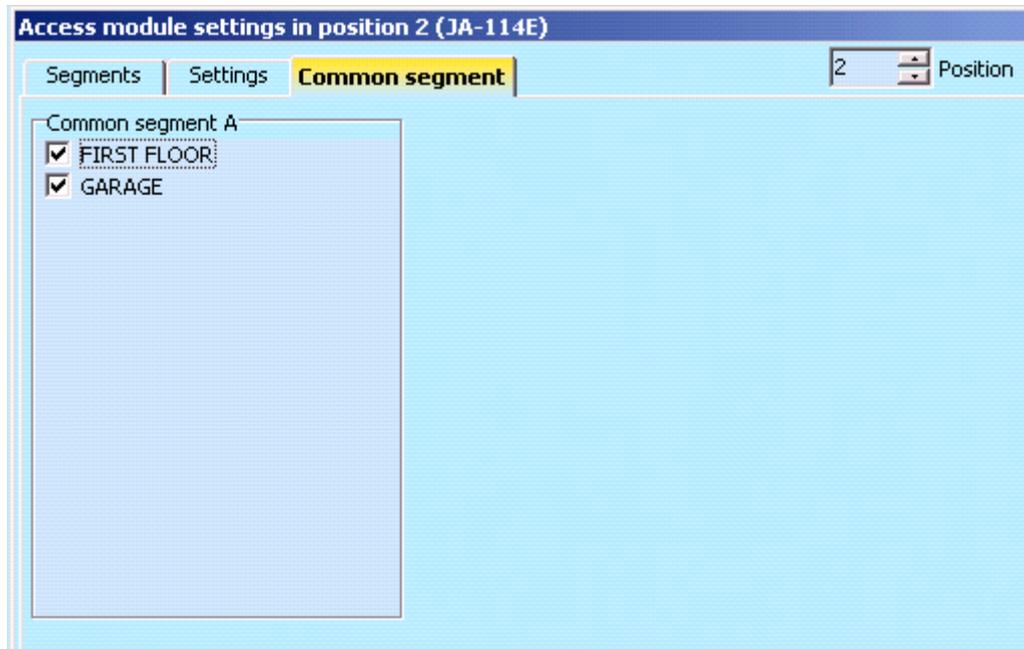
Segment	Anpassung der LED-Beleuchtung auf den Segmenten
Tastatur	Anpassung der Hintergrundbeleuchtung der Tastatur
Display	Einstellung der Hintergrundbeleuchtung des LCD-Displays

Hinweis: Die Intensität der Hintergrundbeleuchtung kann für den Tag- und Nachtmodus unterschiedlich eingestellt werden. Außerdem kann die akustische Anzeige der Tastatur stumm geschaltet werden.

Akustische Signalisierung - Bereiche – Diese Option ermöglicht Ihnen, Bereiche auszuwählen, für die die akustische Anzeige aktiv ist (Alarmer, Eingangs- / Ausgangsverzögerungen, Steuerung der PG-Ausgänge usw.).

Bereichsauswahl über das Menü – Auf einer Tastatur mit einem LCD-Bildschirm können Sie festlegen, welche Bereiche über das Menü aktiviert und deaktiviert werden können. Auf diese Weise können Sie z.B. eine Tastatur erstellen, die normalerweise zwei Bereiche unter Verwendung der Segmente steuert, aber wenn nötig, kann sie das Menü verwenden, um andere Teile des Hauses zu steuern, für die keine Segmente installiert sind.

10.5.1.3. Registerkarte Gemeinsames Segment



Ermöglicht die gleichzeitige Steuerung mehrerer Bereiche, deren einzelne Segmente auf der Tastatur zu einem Segment zusammengefasst sind. Nach dem Drücken der Taste auf den selben Segment wird der Befehl „Unschärf / Schärf“ für die ausgewählten Bereichsegmente gemeinsam ausgeführt. Wenn einige Bereiche, die vom Gemeinsamen Segment gesteuert werden, scharf und andere unscharf sind, werden die verbleibenden Bereiche mit dem Gemeinsamen Segment unscharf / scharf geschaltet. Wenn die teilweise Scharfschaltung für eines der ausgewählten Segmente aktiviert ist (Details siehe Kapitel 9.2 Systemsteuerung über die Tastatur), verhält sich das Gemeinsame Segment wie folgt: 1. Drücken von Schärf = Teileinstellung, 2. Drücken von Schärf = Vollständige Scharfschaltung. Das Gemeinsame Segment kann einen aktiven Melder in einem Bereich umgehen, wenn der Einstellmodus „Scharfschaltung mit Hinweis“ oder „Scharfschaltung nach Bestätigung“ ist, ohne die anderen Segmente mit dem zweiten Drücken zu beeinflussen, die auf „Teilweise Scharfschaltung mit einem Drücken und vollständige Scharfschaltung mit dem Zweiten“ geschaltet sind.

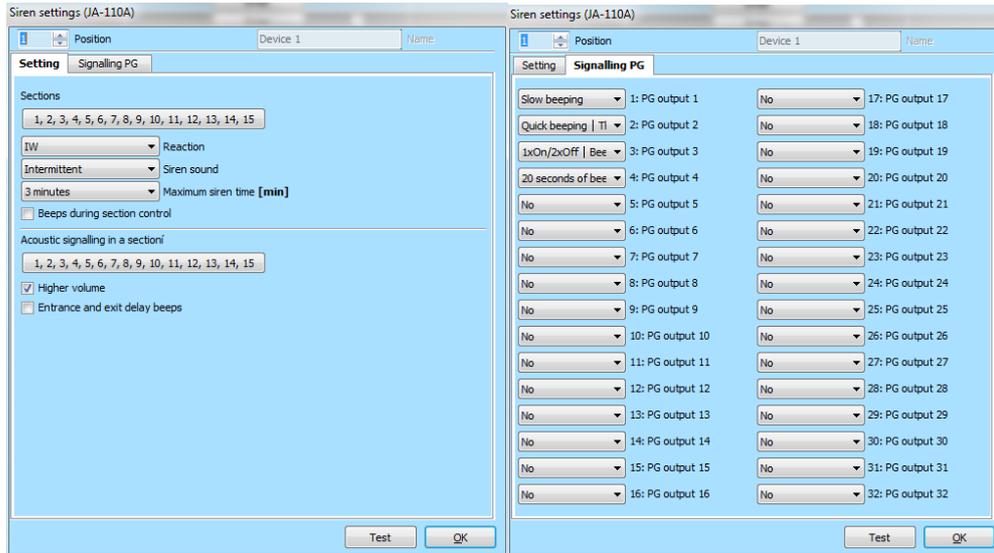
Anzeige des Gemeinsamen Segments: Alle Bereiche unscharf = grün, alle Bereiche vollständig scharf = rot, jeder Bereich scharf (teilweise scharf) = gelb. Bereiche werden einem Gemeinsamen Segment in der Registerkarte **Gemeinsames Segment** zugewiesen.

Es kann höchstens 2 Gemeinsame Segmente auf der Tastatur geben. Der ausgewählte Bereich kann für beide Gemeinsame Segmente gelten.

Hinweise:

- Das „Gemeinsame Segment“ ist nur dann verfügbar, wenn mehr als zwei Segmente für eine Bereichssteuerung mit einem Modul verbunden sind.
- Es ist nicht ratsam, die Funktion des Gemeinsamen Segments mit der Funktion des Gemeinsamen Bereichs zu kombinieren.

10.5.2. Beispiele von Einstellungen einer internen Sirene



Akustische Alarmsignalisierung von Bereichen – Diese Option wird verwendet, um Bereiche auszuwählen, bei denen ein akustischer Alarm durch Sirenen angezeigt wird

Reaktion – Auswahl von Optionen für eine Alarmanzeige, EW (externe Warnanzeige) oder IW (interne Warnanzeige). Der Unterschied wird in Tabelle 8.5 Alarmarten beschrieben.

Sirenenton – Auswahl der Art des Sirenentons: Intermittent (50/50) / Dauerhaft

Maximaler Sirenenalarm – Einschränkung der maximalen Hupton-Zeit zwischen 1 und 5 Minuten (unter der Voraussetzung, dass der Alarm der Zentrale länger ist; wenn nicht, endet der Ton zusammen mit dem Alarm der Zentrale)

Erhöhte Lautstärke – Möglichkeit, die Lautstärke der Anzeige einer Eingangs- und Ausgangsverzögerung und der Anzeige der PG-Ausgangssteuerung zu erhöhen. Dies hat keinen Einfluss auf den Alarmton, der immer auf die höchste Lautstärke eingestellt ist.

Während der Bereichssteuerung – Akustische Bestätigung einer Änderung des Bereichsstatus.

Signalisierung der Eingangs- und Ausgangsverzögerung – Akustische Anzeige einer Eingangs- / Ausgangsverzögerung

Signalisierung eines PG – Akustische Bestätigung von Änderungen der PG-Ausgänge der verwendeten Segmente. Ermöglicht die Auswahl von Tönen, die einem bestimmten PG-Ausgang zugeordnet sind, um sie akustisch zu unterscheiden. Beispielsweise hat das Drücken der Klingeltaste einen anderen Klang als der eines PG-Ausgangs, der durch Öffnen der Tür ausgelöst wird.

Test – Taste für einen 3-Sekunden-Test der akustischen und optischen Alarmanzeige

10.6. Registerkarte Benutzerübersicht

Sie wird dafür verwendet, neue Systembenutzer und ihre Rechte einzurichten. Die Registerkarte zeigt so viele Positionen an, wie Sie in der Registerkarte **Systemübersicht** ausgewählt haben. Für Änderungen in dieser Registerkarte müssen Sie nicht im Servicemodus (Errichter-Modus) sein.

P	Name	Telephone number	Code	Card	Authorization	Code change allowed	Time-limited access	Section	PG
0	Service		0*****	0	Service	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1, 2, 3, 4, 5, 6, 7, 8	1, 2, 3, 4, 5, 6, 7,
1	Master		1*****	0	Administrator	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1, 2, 3, 4, 5, 6, 7, 8	1, 2, 3, 4, 5, 6, 7,
2	User 2			0				No	No
3	User 3			0				No	No
4	User 4			0				No	No
5	User 5			0				No	No
6	User 6			0				No	No
7	User 7			0				No	No
8	User 8			0				No	No
9	User 9			0				No	No
10	User 10			0				No	No
11	User 11			0				No	No
12	User 12			0				No	No
13	User 13			0				No	No
14	User 14			0				No	No
15	User 15			0				No	No
16	User 16			0				No	No
17	User 17			0				No	No

* Die mit * markierten Positionen werden nur angezeigt, wenn die **Erweiterten Einstellungen** aktiviert sind.

Name – Namen von Benutzern werden in textuellen Ereignismeldungen in den Anzeigen des Ereignisverlaufs, in Registerkarten für Meldungen, Berechtigungseinstellungen oder zur Berechtigung auf einer Tastatur mit einem LCD-Bildschirm verwendet.

Telefonnummer – wird verwendet, um Ereignisse zu melden, ebenso wie zur Benutzeridentifikation, wenn das System über das Sprachmenü eines Telefons gesteuert wird oder zur Aktivierung von PG-Ausgängen per Anruf oder SMS. Die Telefonnummer muss immer im internationalen Format eingegeben werden (z.B. +420710123456).

Code – der Zugriffscode des Benutzers wird immer im Format **p*cccc** (**p = Präfix (Positionsnummer)**, *** = Trennzeichen**, **cccc = 4 Codenummer**) eingegeben. Wenn das Präfix deaktiviert ist, (in der Registerkarte Systemübersicht in F-Link) ist er nur **cccc**. Der Code auf den Positionen 0 und 1 kann nicht gelöscht werden (Service und Hauptadministrator). Die Codes können 4-, 6- oder 8-stellig sein.

Zutrittskarte/-Tag – wird verwendet, um RFID-Zugriffskarten zuzuweisen (Tags). Jedem Benutzer können 2 Karten zugewiesen werden. Karten können zugewiesen werden:

- über die Eingabe der Seriennummer (diese kann mit einem Strichcode-Leser eingelesen werden)
- **unter Verwendung des Lesegeräts JA-190T** (verbunden mit einem USB-Anschluss am Computer) und der Verwendung der RFID-Karte/Tag.
- unter Verwendung einer Tastatur und einer RFID-Karte/Tag.

Berechtigung – definiert die Benutzerrechte. Die Berechtigungen auf den Positionen 0 und 1 können nicht geändert werden. Einzelheiten – siehe Kapitel 8.3 Benutzerberechtigung.

Beispielbenutzer – ermöglicht das Kopieren aller Einstellungen entsprechend dem Beispiellbenutzer. Nachfolgende Änderungen in den Einstellungen des Beispiellbenutzer gelten für alle Benutzer, die entsprechend dem Modellbenutzer festgelegt wurden.

Codeänderung * – ermöglicht einem Benutzer, seinen Code zu ändern (nicht die Positionsnummer). Die Option ist nur verfügbar, wenn der Parameter Codes mit Präfixen aktiviert ist (Administrator, Service und ARC können ihren Code jederzeit ändern).

Zutrittszeit* – ermöglicht es, den Zugriff eines Benutzers entsprechend des Wochenplans in der **Registerkarte Bereichsübersicht*/ Zutrittszeiten** zu beschränken, siehe Kapitel 9.15 Zeitlich begrenzter Zugriff für Benutzer. Die Zugriffsbegrenzung kann nur auf Benutzer mit einer Benutzerberechtigung angewendet werden.

Bereich – definiert, welche Bereiche vom Benutzer (Administrator) definiert werden dürfen. Der Administrator kann auch Codes und Karten von Benutzern in den zugewiesenen Bereichen festlegen. Ein Bereich kann keinem Benutzer zugewiesen werden, der nur zur Steuerung von PG-Ausgängen berechtigt ist.

PG – legt fest, welche PG-Ausgänge der Benutzer steuern darf (wenn für die Ausgangssteuerung eine Berechtigung erforderlich ist).

Systemsteuerung – ermöglicht es einem Benutzer, das Senden von SMS-Meldungen zur Scharf- / Unscharfschaltung bei einer Steuerung für die Tastatur zu ermöglichen.

PG wird durch Durchklingeln aktiviert – Informationsfenster über die zugewiesene PG-Steuerung durch die Einwahlfunktion.

Benutzer sperren – Möglichkeit, einen Benutzer zu sperren. Der Benutzer auf Position 0 (Errichter) und 1 (Hauptadministrator) kann nicht deaktiviert werden. Die Deaktivierung eines Benutzers wird durch einen roten Punkt angezeigt. Der Administrator (über die LCD-Tastatur oder J-Link) und der Errichter (über F-Link) sind berechtigt, Benutzer zu deaktivieren.

Notiz – ermöglicht es, die Details eines Benutzers zu beschreiben, z.B. Zugangsberechtigung außerhalb der Arbeitszeiten etc.

Zeitlich begrenzter Zugriff – Die Taste dient zum Einrichten eines zeitlich begrenzten Zugriffs, siehe Kapitel 9.15 Zeitlich begrenzter Zugriff für Benutzer.

10.7. Registerkarte PG-Ausgänge

Diese wird dazu verwendet, Funktionen und Verknüpfungen der programmierbaren Ausgänge einzustellen. Die Registerkarte zeigt so viele Positionen wie Sie in der **Registerkarte Systemübersicht** ausgewählt haben, an. Um Änderungen in dieser Registerkarte vorzunehmen, müssen Sie sich nicht im Errichter-Code befinden.

Posi...	Name	Logic	Function	Time	Activation	Blocking of P...	Reports	Record PG...	PG disabled	Current status	Test PG output
1	Air Conditioning	NO	Impulse	01:00:00	Activation	Sections	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
2	Light hall	NO	Delayed copy	00:05:00	Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
3	Light garage	NO	Delayed copy	00:10:00	Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
4	Garden watering	NO	Impulse	00:20:00	Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
5	PG output 5	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
6	PG output 6	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
7	PG output 7	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
8	PG output 8	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
9	PG output 9	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
10	PG output 10	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
11	PG output 11	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
12	PG output 12	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
13	PG output 13	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
14	PG output 14	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
15	PG output 15	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output
16	PG output 16	NO	ON/OFF		Activation	None	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled	Test PG output

Name – Identifikation des Ausgangs (z.B. Klimaanlage, Warenlagertür...).

Schaltlogik – Möglichkeit zur Einstellung der umgekehrten Logik des Ausgangs (NO = Schließer, NC = Öffner).

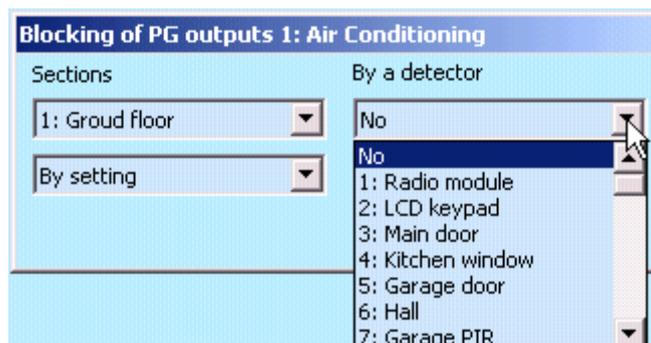
Funktion – bestimmt das Verhalten des Ausgangs nach der Aktivierung.

Impuls	ermöglicht die Aktivierung mit einer Zeiteinschränkung (die Zeit wird in der Spalte Zeit eingestellt).
EIN/AUS	Der Befehl zur Aktivierung löst die Aktivierung aus, der Befehl zur Deaktivierung die Deaktivierung, während der Status der Quelle und die Dauer nicht geprüft werden, der letzte Befehl führt immer seine Anforderung aus.
Kopieren ohne Verzögerung	kopiert die Aktivierung eines Melders oder internen Status; wenn es eine Anfrage von zwei Geräten gibt, wird die OR-Logik verwendet
Kopieren nach Verzögerung	Sendet nur dann einen Befehl, wenn die Aktivierungsbedingung länger gültig ist als in der Spalte „Zeit“ festgelegt (z. B. für die Anzeige eines vergessenen Schließens eines Garagentors).
Kopieren mit Haltezeit	kopiert die Aktivierung eines Geräts (oder internen Status) und verlängert diese um die in der Spalte Zeit eingestellte Zeit (eignet sich z. B. für die Beleuchtung eines Gangs nach dem Öffnen der Tür).
Zustandsänderung	Durch Aktivierung wird der aktuelle PG-Status in den entgegengesetzten Status umgekehrt (eignet sich nur für Impulssteuerung, z. B. mit einer Fernsteuerungstaste).

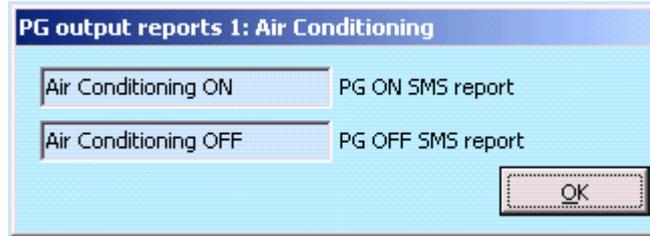
Zeitdauer – Zeiteinstellung für die Impulsfunktion, Kopieren nach einer Verzögerung und Kopieren mit Überlappung. Die Zeit wird im Format *hh:mm:ss* von 00:00:01 bis 23:59:59 eingestellt.

Aktivierung – Öffnen der Aktivierungskarte eines PG-Ausgangs– siehe Kapitel 10.7.1 Aktivierungskarte eines PG-Ausgangs.

Blockierung – Option, um einen PG-Ausgang durch einen Bereichsstatus, einen Melder oder einen anderen PG zu sperren. Die Sperrung verhindert, dass der bestimmte PG aktiviert wird. Wenn er bereits aktiviert ist, wird es deaktiviert. Es muss z.B. ein Türschloss gesperrt werden, wenn der entsprechende Bereich scharf geschaltet ist. Im Falle der Sperrung durch einen Bereichsstatus können Sie wählen, ob die Sperrung gilt, wenn der Bereich aktiviert oder deaktiviert ist, und im Falle einer Sperrung durch ein Gerät oder einen anderen PG-Ausgang, wenn das Gerät / der PG-Ausgang aktiviert bzw. deaktiviert wird. Alle Sperroptionen können gleichzeitig verwendet werden.



SMS Nachrichten – Einstellung der Texte von SMS-Meldungen, die beim Aktivieren oder Deaktivieren eines PG-Ausgangs gesendet werden. Die Benutzer, an die die Berichte gesendet werden, werden in der Registerkarte Benutzerbenachrichtigungen festgelegt. Wenn die Texte der Meldungen geändert werden, werden sie im Protokoll aufgezeichnet, sodass sie nicht vollständig gelöscht werden können.



Ereignisspeicher – Diese Option ermöglicht die Anmeldung der PG-Aktivierung im Ereignisverlauf und somit auch SMS-Meldungen an Benutzer und die Kommunikation mit dem ARC (z. B. zur Überwachung des Eintritts von Benutzern an überwachten Türen, Anmeldung in der MyJABLOTRON-App usw.).

PG deaktivieren – Möglichkeit, einen PG-Ausgang zu sperren. Die Deaktivierung (Sperrung) eines Ausgangs wird durch einen roten Punkt angezeigt. Nur der Errichter (über F-Link) ist berechtigt, einen Ausgang zu deaktivieren.

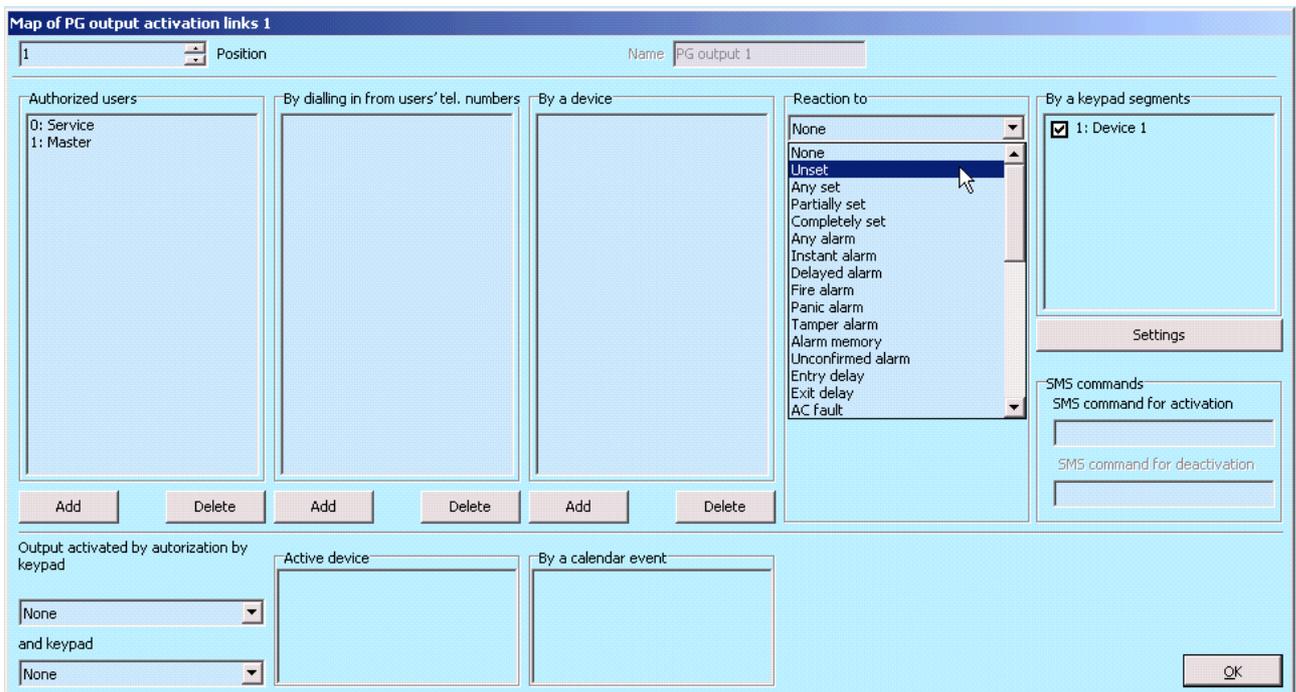
Status – farblich codierte Information über den aktuellen Status eines PG-Ausgangs. Die grüne Beschreibung entspricht dem grünen Licht des Bereichs (Segments); Die rote Beschreibung entspricht dem roten Licht des Bereichs (Segments).

Test – Möglichkeit, einen Ausgang manuell vom Computer aus zu steuern. Abhängig von der gewählten Funktion wird der jeweilige PG aktiviert (oder deaktiviert), wenn er in dem Moment nicht gesperrt ist.

Notiz – ermöglicht es, Details eines PG-Ausgangs, seine Verwendung, das spezielle Verhalten, sowie Aktivierungsbenachrichtigung zusammen mit anderen Ausgängen usw. zu beschreiben.

10.7.1. Aktivierungskarte eines PG-Ausgangs

Durch die Auswahl der Option Aktivierung in der Registerkarte PG-Ausgänge gelangen Sie zur Karte der Aktivierungsverknüpfungen. Die Karte legt fest, auf welche Aktionen der Ausgang reagiert.



Autorisierte Benutzer– Definition der Benutzer, die berechtigt sind, den PG-Ausgang mittels der Berechtigungsanforderung über eine Tastatur (mit Segmenttasten), über die App MyJABLOTRON oder per SMS zu steuern. Die Einstellung ist mit der Registerkarte Benutzer verknüpft.

Ausgangsaktivierung durch Autorisierung am Zugangsmodul – Sie können bis zu 2 Tastaturen einrichten, die den PG-Ausgang durch einfache Berechtigung aktivieren (Verwendung einer Karte / eines Tags oder über die Eingabe des Codes). Diese Funktion dient zum Öffnen eines Türschlosses (d.h. die Bedienung der Segmenttasten ist nicht erforderlich). Diese Funktion ist nur verfügbar, wenn die Ausgangsfunktion auf Impuls gesetzt ist.

Durchklingeln der Benutzer – Definition von Benutzern, die zum Aktivieren eines PG-Ausgangs berechtigt sind, indem sie von ihrem Telefon aus anrufen (Telefonnummern werden in der Registerkarte Benutzer eingegeben). Telefonnummern, die für die Rufaktivierung verwendet werden, dürfen nicht ausgeblendet sein (der CLIP-Dienst darf für sie nicht deaktiviert sein). Der Begriff „Klingeln“ bedeutet, dass der Anrufer nach dem Wählen der Telefonnummer auf mindestens einen Klingelton wartet (siehe die Anzahl der Klingeltöne eingehender Anrufe bis zur AntwortEinstellung in den Einstellungen des Kommunikators) und den Anruf beendet. Der PG-Ausgang schaltet sich ein, wenn der Anruf auflegt. Wenn der Anruf von der Zentrale beantwortet wird, wird der Ausgang nicht aktiviert.

Meldelinie – Möglichkeit der Aktivierung eines PG-Ausgangs durch ein Gerät (Melderaktivierung, Drücken eines Tags etc.). Die Einstellung ist mit der Registerkarte Geräte verknüpft.

Reaktion auf – Möglichkeit der Aktivierung eines Ausgangs durch einen ausgewählten internen Status des Systems (z. B. Scharfschaltung, Alarm, Stromversorgungsfehler, Fehler usw.). Für einen internen Status (insgesamt 39 interne Status, siehe folgende Tabelle) können Sie die Gruppe von Bereichen festlegen, von der das Signal akzeptiert wird (ODER-Logik). Der betreffende PG-Ausgang kann so eingestellt werden, dass er den Status eines anderen PG-Ausgangs oder mehrerer anderer Ausgänge kopiert, bei denen die gegenseitige Logik auswählbar ist (ODER oder UND). Mit der letzten Option im Menü „Ereignis im System“ können Sie die Aktivierung eines Ausgangs und dessen Deaktivierung als Reaktion auf ein völlig anderes Ereignis einstellen (z. B. Aktivierung im Falle eines Alarms, aber Deaktivierung nur durch Unscharfschaltung).

Bedienteile und Segmente – Zeigt eine Liste der Tastaturen und Fernsteuerungen im System an. Über die Taste Einstellung (unter der Liste der Tastaturen) können Sie das interne Menü der ausgewählten Tastatur aufrufen und dessen Einstellungen anpassen, siehe Kapitel 10.5.1 Konfiguration der Tastatur.

SMS Nachrichten – können Sie Textbefehle zum Aktivieren und Deaktivieren eines PG-Ausgangs per Telefon festlegen. Der Empfang der entsprechenden SMS hat einen ähnlichen Effekt wie das Drücken der Taste Scharf oder Unscharf auf dem Steuerungsbereich (Segment) der Tastatur. Das SMS-Format zur Steuerung von PG-Ausgängen ist **code_command, z. 2 * 2345_enable_light** (Hinweis: Das Zeichen _ ist ein Leerzeichen). Der Code vor dem Befehl ist nicht obligatorisch, wenn in der Registerkarte Kommunikation der Punkt „Sprachmenü und Steuerungs-SMS ohne Code“ aktiviert ist und die Telefonnummer eines Benutzers identifiziert wird, der berechtigt ist, den entsprechenden PG-Ausgang zu steuern.

Durch eine Komponente aktiviert – Liste der Geräte, die vom entsprechenden PG-Ausgang aktiviert werden, z. B. ein Foto von einem PIR mit einer Kamera (nur Informationsfenster, die Funktion muss in den geräteinternen Einstellungen eingestellt werden).

Mit Hilfe einer Aktion im Kalender – eine Liste der geplanten Ereignisse, die einen entsprechenden PG-Ausgang aktivieren oder deaktivieren (Informationsfenster)

Warnhinweis 1: Die Zentrale JA-107K bietet 128 PG-Ausgänge. Drahtlose PG-Ausgänge können nur den Ausgängen 1 bis 32 zugewiesen werden. Alle 128 PG-Ausgänge können für BUS-Module verwendet werden.

Warnhinweis 2: Die PG-Ausgänge sind nicht funktionsfähig, wenn sich das System im Errichtermodus befindet. Durch Drücken der Test-Taste können alle PG-Ausgänge getestet werden. Bei Aktivierung des Errichtermodus werden alle PG-Ausgänge deaktiviert. Nach dem Verlassen des Servicemodus in F-Link wird ihre Reaktivierung außer Warnhinweis 3 angeboten.

Warnhinweis 3: Wenn die Einstellung Systemparameter / Automatisch in den Errichtermodus wechseln und wenn bei der Verbindung der Zentrale mit F-Link der Menüpunkt Unscharfschaltung im Fenster Warnhinweis ausgewählt wird, meldet F-Link nach diesem direkten Wechseln in den Errichtermodus keine möglichen PG-Ausgänge mit Impulsaktivierung an (z.B. Aktivierung über den Tastaturbereich (Segment) und Aktivierungs- / Deaktivierungsfunktion oder zeitlich geplante Scharfschaltung). Das bedeutet, dass beim Verlassen des Errichtermodus die Frage, ob diese PG-Ausgänge wieder aktiviert werden sollen, nicht angezeigt wird.

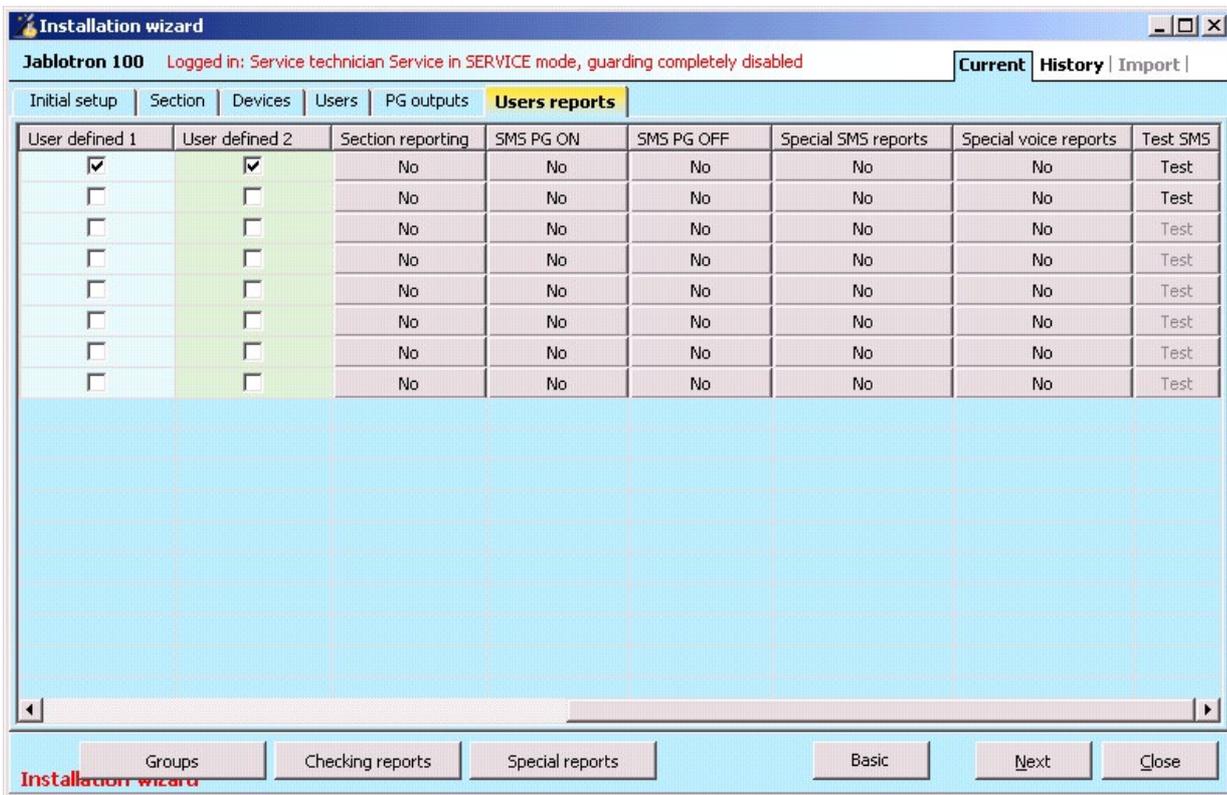
Interne Status für die Steuerung der PG-Ausgänge:

1. Unscharf	14. Ausgangsverzögerung	27. Aktive Sabotage
2. Scharf	15. AC-Ausfall	28. Keine Bewegung im Bereich
3. Teilscharf	16. AC-Ausfall / Länger 30min	29. Bereit zur Scharfschaltung
4. Gesamtscharf	17. Störung der Backup-Batterie	30. Bereit zur Teilscharfschaltung
5. Alle Alarmmeldungen	18. Interner Alarm (IW)	31. Fehlerhaftes scharfschalten
6. Sofortiger Alarm	19. Externer Alarm (EW)	32. (Anforderung zur) Jahreswartung
7. Verzögerter Alarm	20. Störung	33. Störung GSM
8. Brandalarm	21. Aktiver Melder	34. Störung LAN
9. Lauter Überfallalarm	22. Aktiver Melder ohne Verzögerung	35. Störung PSTN
10. Sabotagealarm	23. Aktiver Melder mit Verzögerung	36. Nachtmodus
11. Alarmidentifikation	24. Bypass (in einem Bereich)	37. Wartungsmodus
12. Unbestätigter Alarm	25. Kommunikationsverlust (Gerät in 20 Minuten verloren)	38. Anderer PG's
13. Eingangsverzögerung	26. Batterie schwach	39. Eigene Gruppe

10.8. Registerkarte Benutzerbenachrichtigung

Diese Registerkarte wird dazu benutzt, Benutzer zu definieren, die per SMS oder Sprachanruf vom System über ausgewählte Ereignisgruppen informiert werden. Die Gruppen und die SMS-Formate sind in der Tabelle 9.13 An Benutzer gemeldete Ereignisse beschrieben. Die Basisstruktur des Sprachmenüs ist in der Tabelle in Kapitel 9.5 Systemsteuerung über das Sprachmenü des Kommunikators beschrieben. Um Änderungen in dieser Registerkarte vorzunehmen, ist der Errichtermodus nicht notwendig.

Pos...	User	SMS alerts	Alarm Call	SMS about setting/unsetting	Alarm photo	Fault and Service SMS	User defined 1	User defined 2
1	0: Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	1: Master	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	No	<input type="checkbox"/>						
4	No	<input type="checkbox"/>						
5	No	<input type="checkbox"/>						
6	No	<input type="checkbox"/>						
7	No	<input type="checkbox"/>						
8	No	<input type="checkbox"/>						



Benutzer – ermöglicht die Auswahl eines Benutzers aus der Liste der Benutzer

Alarm SMS – Gruppe von auswählbaren Alarmmeldungen, bei denen eine Textmeldung über ein Alarmereignis im ausgewählten Bereich gemeldet wird. Dies kann ein Stromausfall, der länger als 30 Minuten ist, oder auch die Wiederherstellung des Stroms, die Scharfschaltung einer offenen Zone oder möglicherweise eine Meldung über einen unscharfen Bereich ohne Bewegung sein (siehe Registerkarte Bereichsübersicht).

Alarm Anruf – eine Gruppe von Meldungen, bei denen (nach dem Senden der SMS-Meldungen) das System eine Alarm-Sprachnachricht an den Benutzer übermittelt. Der Anruf klingelt für ca. 30 Sekunden. Wenn der Anruf nicht beantwortet wird, ruft das System den nächsten Benutzer der Reihe nach auf. Wenn der Anruf angenommen wird, wird die Sprachnachricht wiederholt gesendet. Die Struktur der Nachricht ist: Ihre Alarmmeldungen - Alarmart - Bereichs-Nr. Wenn der Benutzer auflegt, spätestens jedoch nach 50 Sek., wird der Anruf beendet und der nächste Benutzer angerufen. Der Benutzer kann den Empfang des Anrufs durch Drücken der Taste # auf dem Telefon bestätigen und nach der Sprachnachricht muss der Benutzer einen gültigen Code eingeben. Wenn ein gültiger Code eingegeben wurde, wird der Alarm gestoppt und der nächste Benutzer wird nicht mehr angerufen. Für die Sprachmeldungen sind universelle Sprachnachrichten im System voreingestellt. Die Sprachnachrichten können neu aufgezeichnet werden, indem die Namen im Sprachmenü durch die erforderlichen ersetzt werden. Für die Struktur des Sprachmenüs siehe Kapitel 9.5 Systemsteuerung über das Sprachmenü des Kommunikators (GSM).

Scharf / Unscharf SMS – eine Gruppe von Meldungen, für die eine Textnachricht über die Scharf- und Unscharfschaltung versendet wird. Eine Meldung über eine Scharfschaltung wird mit einer festgelegten **SMS bei nicht erfolgreichen scharfschalten** (Registrierkarte Übertragungsgeräte) nach der Scharfschaltung versendet. Die Scharf- und Unscharfschaltung wird nicht an den Benutzer versendet, der sie durchgeführt hat. Eine Ausnahme stellt hier die Scharfschaltung eines gemeinsamen Bereichs dar (von der Zentrale, nicht dem Benutzer, durchgeführt).

Störung und Service SMS – sendet eine Textmeldung über einen Fehler (nicht aufgeladene Batterien, Eingabe des Servicecodes usw.).

Definierter Benutzer SMS 1 – spezielle erste Gruppe, in der der Errichter bestimmte zu meldende Ereignisse (typischerweise Meldungen über Stromausfälle und Wiederherstellungen oder die Scharfschaltung eines aktiven Geräts) nur an ausgewählte Benutzer überträgt.

Definierter Benutzer SMS 2 – 2. Gruppe, in der der Errichter bestimmte Ereignisse, die gemeldet werden sollen (typischerweise niedrige Batterien in Geräten oder niedriger Ladezustand der Backup-Batterie), nur an ausgewählte Benutzer übertragen kann.

Bereichsmeldungen – bestimmt, über welchen Bereich der ausgewählten Ereignisgruppen berichtet werden soll. Wenn Fehler- und Service-SMS überprüft werden und kein Bereich ausgewählt ist, werden nur System- und Servicefehler gemeldet (diese sind immer Bereich Nr.1 zugewiesen). Es besteht keine Verknüpfung zwischen der Berechtigung und der Fähigkeit der Bereichssteuerung.

SMS PG AN* – Möglichkeit, die Aktivierung von PG-Ausgängen an einen Benutzer zu melden. Die Nachrichten werden mit einer festen Verzögerung von 60 Sek. gesendet. Die Texte der SMS-Nachrichten werden in der Registerkarte PG-Ausgänge eingestellt, siehe Kapitel 10.7 Registerkarte PG-Ausgänge.

SMS PG AUS* – Möglichkeit, die Deaktivierung von PG-Ausgängen an einen Benutzer zu melden. Die Nachrichten werden mit einer festen Verzögerung von 60 Sek. gesendet. Die Texte der SMS-Nachrichten werden in der Registerkarte PG-Ausgänge eingestellt, siehe Kapitel 10.7 Registerkarte PG-Ausgänge.

SMS Sondermeldungen* – Möglichkeit, die Aktivierung von Meldern zu melden, für die die Reaktion der Speziellen Meldung (A, B, C oder D) mit einer SMS an den Benutzer eingestellt wurde. Die Texte von Speziellen Meldungen werden über die Taste **SMS Sondermeldungen** rechts unten in der Registerkarte Benutzerbenachrichtigungen an Benutzer festgelegt.

Sondersprachmeldungen* – Möglichkeit, die Aktivierung von Meldern zu melden, für die die Spezielle Meldung (A, B, C oder D) mit einer Sprachnachricht an den Benutzer eingestellt wurde. Sprachnachrichten können durch Aufrufen der Telefonnummer der Zentrale erneut aufgezeichnet werden. Nach Beantworten des Anrufs und Berechtigung mit dem Administrator-Code können Sie mit der Taste 9 die Aufzeichnung von Sprachnachrichten eingeben, siehe Kapitel 9.5 Systemsteuerung über das Sprachmenü des Kommunikators (GSM).

Test – durch Drücken dieser Taste wird eine Test-SMS an den Benutzer gesendet: „Testbericht, Zentrale, Bereich 1“

Ereignistabelle und voreingestellte Gruppen:

Event	Alarm	Setting/Unsetting	Failures and service	User defined 1	User defined 2
AC fault 30 minutes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
AC fault after 30 min restored	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Instant alarm	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Instant alarm cancelled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Delayed alarm	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Delayed alarm cancelled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tamper alarm	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tamper alarm cancelled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fire alarm	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fire alarm cancelled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Panic alarm	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Panic alarm cancelled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health troubles	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Flooding	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Code breaking attempt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Set with active device	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
No movement in the section	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Set	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unset	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Partially set	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System BOOT	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Device low battery	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Device low battery restored	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fault	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fault restored	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Enter service mode	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Leave service mode	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Backup battery LOW	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Backup battery restored	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
ARC communication fault	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
ARC communication fault restored	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
RF jamming	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
RF jamming ended	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Low credit ballance	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Defaults OK

Checking reports

Check connection by dialling in

21:00 Time

1: Master User

Check connection by SMS report

22:00 Time

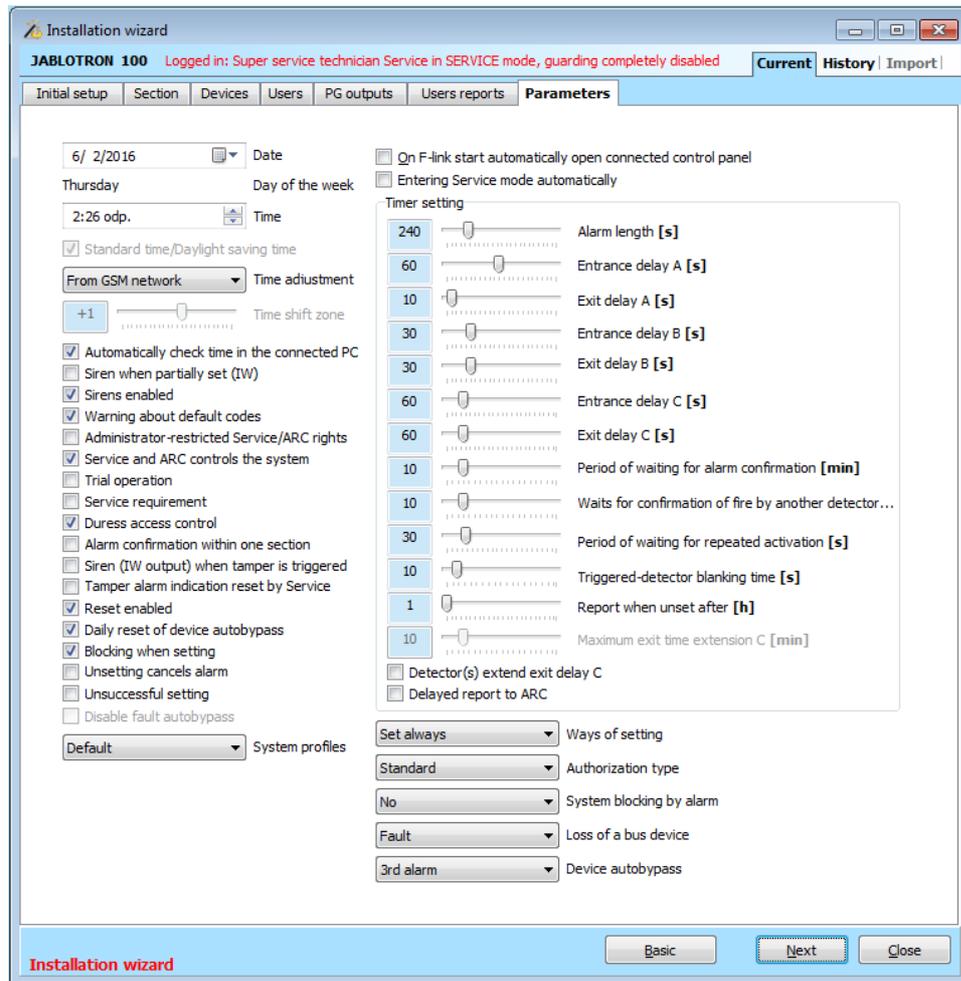
1: Master User

OK

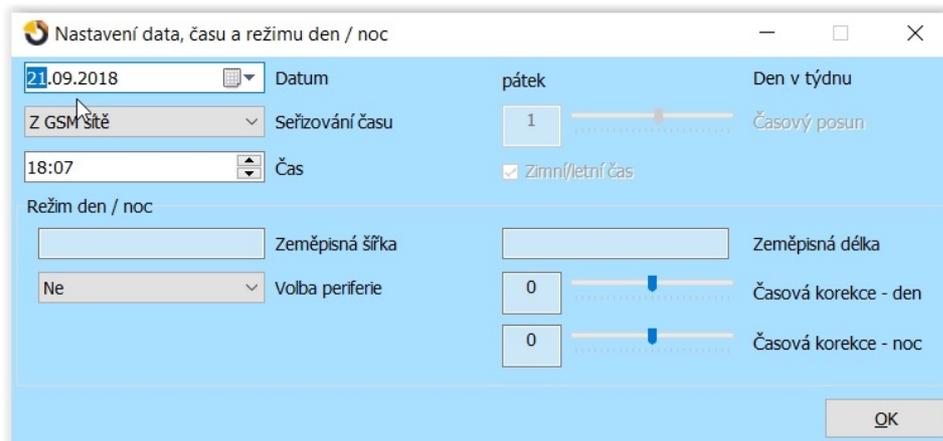
SMS Sondermeldungen – Die Taste in der unteren Symbolleiste der geöffneten Programmierstabelle dient zur Einstellung des Namen, der Aktivierungs- / Deaktivierungs-SMS und als Option zur Aufzeichnung von Meldungen von A bis D im Ereignisspeicher, was als Zonenreaktion verwendet wird, siehe Kapitel 8.4.2 Liste der anwendbaren Reaktionen.

10.9. Registerkarte Systemparameter

Sie wird dazu verwendet, Parameter und auswählbare Funktionen der Zentrale einzustellen. Die Registerkarte ist identisch mit Geräte / Zentrale / Interne Einstellungen. Um Änderungen in dieser Registerkarte vorzunehmen, ist der Errichter-Modus nicht erforderlich.



Nach Drücken der Taste **Datum/Zeit**



* Die unten beschriebenen und mit * markierten Positionen werden nur angezeigt, wenn die **Erweiterten Einstellungen** aktiviert sind.

Datum	Interne Kalendereinstellung	
Wochentag	Zeigt den Wochentag an	
Zeieinstellung*	Methode zur Einstellung von Zeit und Datum:	
	F-Link Manuell	Manuelle Einstellung der Zeit und des Datums über F-Link

	Aus dem GSM-Netzwerk	Zeit und Datum werden mit jedem Login in das GSM-Netzwerk vom GSM-Provider übernommen
	Server automatisch	Zeit und Datum werden automatisch entsprechend des Kommunikationsservers (GMT 0) eingestellt. Diese Option entfällt, wenn die Kommunikationsart auf „ohne Fernprogrammierung“ eingestellt ist (werksseitige Standardeinstellung).
Zeitzone		Einstellen der Zeitverschiebung von der Zeitzone GMT 0.
Uhrzeit		Interne Uhreinstellung
Sommer- und Winterzeit*		Die automatische Umstellung der Winter- und Sommerzeit kann nur für die manuelle Zeiteinstellung gewählt werden. Die Uhr wird am letzten Sonntag im März oder Oktober jeweils um 1:00 UTC umgestellt (d.h. beispielsweise 2:00 Uhr MEZ oder 3:00 Uhr MESZ).
Tag- / Nachtmodus	Breitengrad	Eingabeformat xx.xxxxxN (e.g. 50.729058N)
	Längengrad	Eingabeformat xx.xxxxxE (e.g. 15.176636E)
	Melder-auswahl	Activation of selected device switches the control panel to the Night mode.
	Zeitkorrektur am Tag	Option zur Zeitkorrektur für den Wechsel in den Tag-Modus.
	Zeitkorrektur in der Nacht	Option zur Zeitkorrektur für den Wechsel in den Nacht-Modus.
Zeitabgleich zwischen PC und Zentrale*		Wenn sich die Uhr des Computers und der Zentrale um mehr als 1 Minute unterscheidet, warnt F-Link den Benutzer davor.
Sirene wenn Teilscharf (IW)		Option, eines akustischen Alarmes mit dem IW-System einzustellen, wenn der Bereich teilweise scharf geschaltet ist (gilt nicht für Feuer- und 24-Stunden-Alarme).
Sirenen aktivieren*		Aktiviert alle BUS- und Funksirenen des Systems (zur Deaktivierung des akustischen Alarms während der Systemprüfung).
Warnung vor „Werksseitigen Codes“**		Nach Beendigung des Dienstes wird eine SMS an den Errichter an Position 0 gesendet, dass es noch Standardcodes im System gibt.
Admin schränkt Errichter/AES-Rechte ein		Diese Option sperrt den unabhängigen Zugriff von Servicetechnikern und ARC auf das System. Hinweis: Bei einem Fernzugriff eines Technikers auf das System über F-Link kann der Administrator über eine Tastatur im Gebäude berechtigt werden. Wenn ein Techniker über ein USB-Kabel mit der Zentrale verbunden wird, kann der Administrator über das Sprachmenü per Fernzugriff berechtigt werden.
Errichter oder AES betätigt das System*		Diese Einstellung ermöglicht dem Errichter und dem ARC-Techniker, alle Bereiche des Systems zu steuern. Wenn dieser Parameter deaktiviert ist, ist der Techniker nicht berechtigt, die Bereiche zu steuern und kann nur in den Servicemodus (Errichter-Modus) wechseln, wenn der Administrator oder ein Benutzer alle Bereiche unscharf schaltet.
Testbetrieb		Alle Alarme sind auf 60 Sekunden begrenzt und werden per SMS an definierte Benutzer und den Errichter (Position 0) gemeldet, obwohl Alarmmeldungen für ihn nicht aktiviert sind. Der Testbetrieb wird automatisch 7 Tage nach Verlassen des Servicemodus beendet.

<p>Hinweisfenster - Jahreswartung</p>	<p>Wenn diese Funktion eingeschaltet ist, löst sie 12 Monate nach dem letzten Schließen des Errichtermodus das Ereignis „System fordert Jahreswartung an“ im System aus, das zusammen mit dem Informationssymbol auf der Tastatur mit LCD-Bildschirm angezeigt und im Ereignisverlauf registriert wird. Nach Drücken der Taste "i" wird der Text „Errichter anrufen“ zusammen mit seiner Telefonnummer angezeigt. Die Meldung auf dem LCD verschwindet automatisch, wenn der Errichter lokal auf das System zugreift. Dann führt er die jährliche Inspektion mit einem Reset durch.</p>
<p>Wartungsmodus erlauben</p>	<p>Diese Funktion ermöglicht allen Administratoren, das System in den Wartungsmodus zu schalten.</p>
<p>Überfallalarm</p>	<p>Diese Funktion dient zur Auslösung eines stummen Alarms nur über die Berechtigung oder die Systemsteuerung (Scharfschaltung, Unscharfschaltung, PG-Steuerung, ...), wenn sich ein Benutzer in Anwesenheit eines Eindringlings befindet. Ein Panikalarm wird während der Systemsteuerung ausgelöst, wenn ein Code eingegeben wird, wobei 1 mathematisch zum Wert der letzten Ziffer addiert wird. Diese Funktion ist für Codes mit und ohne Präfix verfügbar. Beispiel: ein Benutzercode mit einem Präfix = 4 * 4444, für die Erzwungene Zugriffssteuerung geben Sie 4 * 4445 ein; ein Benutzercode ohne Präfix = 4444, für die Erzwungene Zugriffssteuerung geben Sie 4445 ein. Vorsicht: Wenn die letzte Ziffer des Benutzercodes 9 ist, verwenden Sie für die Erzwungene Zugriffssteuerung 0 als letzte Ziffer.</p>
<p>2-Melderabhängigkeit in einem Bereich*</p>	<p>Wenn die Bestätigungsreaktion eines anderen Melders für einen Melder eingestellt ist, kann diese Bestätigungsoption verwendet werden, um die Bestätigung auf den selben Bereich zu beschränken (andernfalls kann ein Melder von jedem Bereich einen Alarm bestätigen). Dies gilt gleichermaßen für Einbruchmelder und für Brandmelder.</p>
<p>Interne Sirne bei Sabotagealarm*</p>	<p>Eine Sirene mit der IW-Reaktion zeigt akustisch einen Sabotagealarm an, wenn die Zone nicht oder nur teilweise scharf geschaltet ist. Wenn sie vollständig scharf geschaltet ist, zeigt die Sirene immer den Sabotagealarm an.</p>
<p>Rücksetzen von Sabotage durch Errichter*</p>	<p>Die Anzeige des Sabotagespeichers kann nur von einem Errichter oder ARC-Techniker zurückgesetzt werden. Wenn diese Option nicht aktiviert ist, kann die Anzeige auch vom Administrator (aber nicht vom Benutzer) zurückgesetzt werden.</p>
<p>Reset auf Werkseinstellungen*</p>	<p>Möglichkeit, die Zurücksetzung der Zentrale mit einem Jumper auf der Platine zu sperren. Wenn das Zurücksetzen verboten ist und der Servicecode verloren geht, kann die Zentrale nur vom Hersteller entsperrt werden. Das Zurücksetzen der Zentrale wird in Kapitel 12 Zurücksetzung der Zentrale beschrieben.</p>
<p>Tägliche Zurücksetzung des Autobypasses*</p>	<p>Die Option bezieht sich nur auf Aktivierungseingänge (keine Sabotage- und Fehlereingänge). Wenn diese Option aktiviert ist, setzt das System umgeleitete Geräte (Autobypass) automatisch jeden Tag um 12:00 Uhr zurück. Wenn die Option deaktiviert ist, wird der Autobypass des Geräts nur mit einer Statusänderung des Bereichs zurückgesetzt. Diese Option ist z.B. für die Verwendung von Meldern mit einer 24-Stunden-Reaktion oder Überschwemmungsmeldern, die sich in einem Bereich befinden, in dem die Scharfschaltung / Unscharfschaltung nicht erforderlich ist.</p>
<p>Bypass bei Scharfschaltung</p>	<p>Bei Aktivierung werden alle aktiven Eingänge während der Scharfschaltung des Bereichs gesperrt und können keinen Alarm mehr in dieser Schutzperiode auslösen. Wenn diese Option deaktiviert ist, werden alle aktiven Eingänge vorübergehend überbrückt, bis sie in den Standby-Modus wechseln und die Melder wieder mit der Überwachung beginnen (Risiko einer Fehlalarmauslösung - z. B. falsch geschlossenes Fenster).</p>

Autorisierung hebt Alarm nicht auf	Eine Funktion, die bestimmt, ob ein Alarm nur durch die Berechtigung eines gültigen Codes oder durch die Unscharfschaltung des Bereichs mit einem Alarm abgebrochen wird. Wenn diese Funktion aktiviert ist, kann der Alarm durch Unscharfschaltung eines Bereichs, in dem ein Alarm ausgelöst wurde, oder durch Drücken der Taste „Warnmeldung abbrechen“ im Menü des LCD-Tastatur abgebrochen werden.	
Nicht erfolgreiches scharfschalten	Die Funktion wird bei jeder Scharfschaltung bearbeitet. Wenn eine Sofortige Zone innerhalb der Ausgangszeit ausgelöst wird oder eine verzögerte Zone nach Ablauf der Ausgangszeit geöffnet bleibt, wird das System nicht scharf geschaltet, löst das Ereignis „Fehlerhafte Scharfschaltung“ aus und zeichnet es im Verlauf auf. Dies wird auch per SMS einem voreingestellten Benutzer gemeldet, wenn das Ereignis „SMS über fehlgeschlagene Scharfschaltung“ aktiviert ist. Es wird von der Tastatur und auch durch eine Außensirene angezeigt. Um den Hinweis auf eine fehlgeschlagene Scharfschaltung abzubrechen, muss auf der LCD-Tastatur „Warnmeldung abbrechen“ gedrückt werden.	
Gerätefehler-Autobypass	Diese Option ist nur verfügbar, wenn eines der Systemprofile "EN50131-1" oder "INCERT" ausgewählt ist. Hier wird die begrenzte Anzahl der ausgelösten Fehler von maximal 3 Fehlern auf keine Begrenzung deaktiviert.	
Systemprofile	Auswahl aus voreingestellten Systemprofilen entsprechend der Anforderungen	
	Standard	Die werkseitig eingestellten Parameter mit der Option, sie entsprechend der Anforderungen zu ändern
	EN50131-1, Grad 2	Einige Parameter werden automatisch vorgegeben, um EN50131-1, Grad 2 zu entsprechen, ohne dass sie geändert werden können
	INCERT, Grad 2	Einige Parameter werden automatisch vorgegeben, um INCERT, Grad 2 zu entsprechen, ohne dass sie geändert werden können
Art der Scharfschaltung	Auswahl der Art, wie das System den Einstellungsprozess verwaltet. Von der untersten Stufe, bei der das System unabhängig von aktiven Geräten und Störungen im System scharf geschaltet werden kann bis zur höchsten Stufe, bei der das System, wenn Geräte aktiviert sind, überhaupt nicht (sofortige Zone) scharf geschaltet werden kann. Diese Einstellung ist auch mit dem Systemprofil verknüpft.	
	Sofortige Scharfschaltung	Schaltet immer scharf, unabhängig des Systemstatus (Fehler, aktive Geräte,...)
	Scharf mit Hinweis	Zeigt optisch (auf dem Bereich (Segment) und dem Display) den Systemstatus (Fehler, aktive Elemente, schwache Batterien oder Backup-Batterie) für 8 Sekunden an und schaltet dann automatisch nach Ablauf dieser Zeit scharf. Die Scharfschaltung ist auch durch wiederholtes Drücken des Segments (oder Betätigen der ENTER-Taste) möglich.
	Scharf mit Bestätigung	dem Display) den Systemstatus (Fehler, aktive Elemente, schwache Batterien oder Backup-Batterie) für 8 Sekunden an und kann NUR durch wiederholtes Drücken des Bereichs (Segment) (oder Betätigen der ENTER-Taste) scharf geschaltet werden.



	Keine Scharfschaltung	Zeigt optisch (auf dem Bereich (Segment) und dem Display) den Systemstatus (Fehler, aktive Elemente, schwache Batterien oder Backup-Batterie) für 8 Sekunden an. Das System kann durch wiederholtes Drücken des Segments (oder Betätigen der ENTER-Taste) scharf geschaltet werden, aber nur, wenn es sich um einen aktiven Melder des Reaktionstyps VERZÖGERT oder NÄCHSTER VERZÖGERT handelt. Ein aktives Element mit jeder anderen Alarmreaktion KANN NICHT auf diese Weise scharf geschaltet werden. ACHTUNG!!! Dies gilt auch für die Fernsteuerung (Sprachmenü, SMS, webbasierte oder mobile App, Aktion durch Zeitschaltuhren „Sofortige Scharfschaltung“).	
Autorisierungstyp	Auswahl der Art, wie das System eine Benutzerberechtigung verarbeitet. Auch in Zusammenhang mit der Steuerung eines PG-Ausgangs mit Berechtigung.		
	Standard	Mit der Eingabe eines Benutzercodes oder der Verwendung einer RFID-Karte/Tag erfolgt die gültige Berechtigung. Eine dieser Optionen ist zur Steuerung des Systems erforderlich.	
	Code nach Kartenbestätigung	Benutzer, denen Karten und Codes zugewiesen sind, müssen sich mit beiden Berechtigungen (unabhängig von der Reihenfolge der Berechtigung) berechtigen. Wenn Benutzer entweder Karten oder Codes haben, berechtigen sie sich selbst gemäß der Option Standard. Der Fernzugriff per Telefon ist nur für berechtigte Nummern aktiviert.	
Doppelte Autorisierung	Mit der Eingabe des Benutzercodes und der Verwendung der RFID-Karte/Tag erfolgt die gültige Berechtigung (unabhängig von der Reihenfolge der Berechtigungsschritte). F-Link überwacht, ob ein Code und eine Karte einem Benutzer in der Registerkarte Benutzer zugewiesen wird (wenn nicht, kann die Konfiguration nicht gespeichert werden). Der Fernzugriff per Telefon ist nur für berechtigte Nummern möglich.		
Systemsperrung nach einem Alarm	Der Parameter ermöglicht die Sperrung des Systems nach der ersten Alarmauslösung (Einbruch oder Sabotage), um zu vermeiden, dass weitere Alarme ausgelöst werden. Das Entsperren kann durch einen speziellen Entsperrcode oder über den berechtigten Zugriff des ARC (für Großbritannien) durchgeführt werden. Die Entsperrung nach der Aktivierung des Sabotagealarms kann auch von einem Benutzer mit einer Serviceberechtigung (für den Benelux-Bereich) durchgeführt werden.		
	Deaktiviert (AUS)	Keine Sperrung	
	Nach Sabotagealarm	Das System wird gesperrt, wenn ein Sabotagealarm ausgelöst wird (durch Öffnen des Geräts, durch eine RF-Störung oder durch 10 falsche Codeeingaben usw.).	
	Nach beliebigen Alarm	Das System wird gesperrt, indem ein Alarm ausgelöst wird (Einbruch, Feueralarm, Überflutung, 24-Stunden-Alarm oder Panikalarm).	

Verbindungsverlust einer Buskomponente	Die Zentrale verarbeitet den Verlust eines Geräts oder einen Kurzschluss am System-BUS. Entsprechend der gewählten Option reagiert das System auf die aufgetretene Situation:	
	Störung	Die Zentrale verarbeitet einen Geräteverlust am BUS oder einen Kurzschluss am BUS als Fehler.
	Immer Sabotage	Die Zentrale verarbeitet einen Geräteverlust am BUS oder einen Kurzschluss am BUS immer als einen Sabotagealarm. Wenn das Funkmodul die Erkennung von RF-Störungen ermöglicht und solch eine Störung erkannt wird, wird auch ein Sabotagealarm ausgelöst. Ein Sabotagealarm wird auch von einem Fehler gefolgt, und wenn der Fehler verschwindet, wird auch der Sabotagealarm beendet.
	Sabotage nach Bestätigung	Die Zentrale verarbeitet einen Geräteverlust als Fehler und wenn innerhalb einer vom Parameter „Wartezeit“ auf die Alarmbestätigung“ vorgegebenen Zeit ein weiterer Geräteverlust erfolgt, bestätigt dies das System und löst einen Sabotagealarm aus. Wenn die Fehler der verlorenen Geräte wiederhergestellt sind, beendet das System den Fehler und den Sabotagealarm.
Komponenten-Autobypas	Die Option dient zur Auswahl des Autobypasses.	
	Nach 3. Aktivierung	Das Gerät wird umgangen, nachdem es unabhängig von der Alarmlänge in einem Scharfschaltungszeitraum dreimal aktiviert wurde. Alle anderen Versuche, das Gerät zu aktivieren, werden ignoriert, bis der Bereich deaktiviert wird.
	Nach 3. Alarm	Ein Gerät ermöglicht eine dreimalige Aktivierung während eines Alarmzeitraums. Das jeweilige Gerät wird nach 3 Alarmzeiträumen umgangen, d.h. das Gerät könnte bis zu 9 Mal aktiviert worden sein.
Automatisch die verbundene Zentrale auslesen	Wenn das Zentrale über das USB-Kabel mit einem PC verbunden ist, wird die Verbindung automatisch hergestellt, wenn F-Link gestartet wird.	
Automatisch in den Errichtermodus wechseln	Automatische Schaltung in den Servicemodus, wenn die Zentrale über das USB-Kabel mit einem PC verbunden ist. Wenn einige Bereiche scharf geschaltet sind, werden Sie nach der Unscharfschaltung mit Berechtigung gefragt. Wenn noch Standardcodes verwendet werden, ist die Berechtigung nicht erforderlich.	
Zeitfenster	In jedem Bereich werden die Eingangs- und Ausgangsverzögerungen A, B und C getrennt gemessen. Wenn für die Melder innerhalb eines Bereichs unterschiedliche Ausgangsverzögerungen definiert sind, wird die längste Verzögerung gemessen. Bei unterschiedlichen Eingangsverzögerungen wird diejenige gemessen, die zum aktivierten Melder gehört. Wenn mehr Melder aktiviert sind, wird die kürzeste der definierten Eingangsverzögerungen gemessen. Melder mit der Verzögerung C können die Dauer der Ausgangsverzögerung verlängern (siehe die Option „Melder mit verzögerter C-Reaktion verlängert den Ausgang“ in der Registerkarte Parameter).	

Alarmdauer	Alarmlänge – gilt für alle Bereiche. Spanne von 5 Sek. – 20 Min.
Eingangsverzögerungszeit A	Timer A. Eine Spanne von 5 Sek. – 2 Min.
Ausgangsverzögerungszeit A	Timer A. Eine Spanne von 5 Sek. – 2 Min.
Eingangsverzögerungszeit B	Timer B. Eine Spanne von 5 Sek. – 2 Min.
Ausgangsverzögerungszeit B	Timer B. Eine Spanne von 5 Sek. – 2 Min.
Eingangsverzögerungszeit C	Timer C. Eine Spanne von 5 Sek. – 6 Min.
Ausgangsverzögerungszeit C	Timer C. Eine Spanne von 5 Sek. – 6 Min.
2-Melderabhängigkeit Einbruchalarm	Wartezeit für eine Alarmbestätigung durch einen anderen Melder eines scharf geschalteten Bereichs. Gilt für alle Melder mit der Reaktion Unmittelbare Bestätigung / Verzögerte Bestätigung (1 – 60 Min.)
2-Melderabhängigkeit Brandalarm	(1 – 60 Min.) Wartezeit für die Bestätigung eines Feueralarms durch einen anderen Melder. Gilt für alle Melder mit der Reaktion Feuer bestätigt.
2-fsch Auslösung desselben Melders	Wartezeit für eine wiederholte Aktivierung des gleichen Melders. Die eingestellte Zeit muss länger als die minimale Melderwiederherstellung sein, bevor sie wiederholt wird. Gültig für alle Melder mit der Reaktion wiederholt sofort / Wiederholte Verzögerung A (6 - 120 Sek.).
Minimal Zeit der inaktiven Phase	Mindestzeit, für die der Melder nicht ausgewertet wird, bevor er die Aktivierung wiederholen kann. Gültig für alle Melder mit der Reaktion wiederholt sofort / Wiederholte Verzögerung A (5 - 60 Sek.).
Benachrichtigung sofern unscharf nach	Zeit, nach der ein unscharfer Bereich eine Unscharfschaltung meldet, wenn kein Melder aktiviert wurde (die Meldung wird in der Registerkarte Bereich - Meldung über unscharfen Bereich (1 - 48 Std.) aktiviert.)
Automatische Scharfschaltung	Zeit, nach der ein Bereich, in dem ein Ereignis „unscharfer Bereich“ gemeldet wurde, automatisch scharf geschaltet wird (0 - 120 min.).
Zeitverlängerung der Ausgangsverzögerungszeit	Maximale Zeit, um die die Ausgangsverzögerung von einem aktiven verzögerten Melder im Bereich verlängert wird. Dies funktioniert nur zusammen mit der Option „Melder mit der verzögerten C-Reaktion verlängert die Ausgangsverzögerung“. Wird der Melder für längere Zeit aktiviert, wird der Bereich scharf geschaltet und der Melder wird umgangen (1 - 60 Min.).
Verlängerung der „Ausgangsverzögerungszeit C“	Die „Garagentorfunktion“ - ein aktiver Melder mit der verzögerten C-Reaktion (offenes Tor) verlängert die Ausgangsverzögerung im jeweiligen Bereich. Eine solche Verlängerung kann nur durch Melder mit einer Statusreaktion (typischerweise durch Öffnen der Melder) verursacht werden. Die maximale Zeit der möglichen Verlängerung wird durch die vorherige Option festgelegt.
Um 15s verzögerte Benachrichtigung an eine Notrufserviceleitstelle	Bei Aktivierung wird ein interner Alarm ausgelöst, nachdem die Eingangsverzögerung abgelaufen ist, jedoch wartet das System 15 Sekunden lang, um eine Alarmmeldung an den AES zu senden. Dadurch hat der Benutzer 15 Sekunden länger Zeit, um das System zu deaktivieren, ohne dabei einen Alarm auszulösen, der dem AES gemeldet wird.

10.10. Registerkarte Zeitschaltuhr

Hier können Sie den Zeitplan der Ereignisse festlegen, die das System automatisch und regelmäßig ausführt. Um Änderungen an dieser Registerkarte vorzunehmen, ist der Servicemodus (Errichter-Modus) nicht erforderlich.

Event	Days of th...	Time	Guarding	Section	PG Control	PG number	Blocking	Blocked	Note
1	Mon, Tue, ...	00:00	No	No	No	No	No		
2	Mon, Tue, ...	00:00	No	No	No	No	No		
3	Mon, Tue, ...	00:00	Set	No	No	No	No		
4	Mon, Tue, ...	00:00	Set	No	No	No	No		
5	Mon, Tue, ...	00:00	No	No	No	No	No		
6	Mon, Tue, ...	00:00	Set	No	No	No	No		
7	Mon, Tue, ...	00:00	Set	No	No	No	No		
8	Mon, Tue, ...	00:00	Set	No	No	No	No		
9	Mon, Tue, ...	00:00	Set	No	No	No	No		
10	Mon, Tue, ...	00:00	Set	No	No	No	No		
11	Mon, Tue, ...	00:00	Set	No	No	No	No		
12	Mon, Tue, ...	00:00	Set	No	No	No	No		
13	Mon, Tue, ...	00:00	No	No	No	No	No		
14	Mon, Tue, ...	00:00	No	No	No	No	No		
15	Mon, Tue, ...	00:00	Set	No	No	No	No		
16	Mon, Tue, ...	00:00	Set	No	No	No	No		
17	Mon, Tue, ...	00:00	Set	No	No	No	No		
18	Mon, Tue, ...	00:00	Set	No	No	No	No		
19	Mon, Tue, ...	00:00	Set	No	No	No	No		
20	Mon, Tue, ...	00:00	No	No	No	No	No		

Reaktion – Hier können Sie einstellen, welche Aktion für den Bereich oder die PG-Ausgang ausgeführt werden soll (Unschärf, Schärf, Teilschärf, PG-Steuerung, Technische Kontrolle (Jahreswartung)). Mögliche Varianten sind „sofort“ (keine Ausgangsverzögerung) und „immer“ (entspricht nicht der voreingestellten Einstellung). Die Aktion Jahreswartung löst dasselbe Ereignis im System wie die Option „technische Kontrolle-Jahreswartung“ in der Registerkarte Systemparameter aus.

Bereich/PG – spezifiziert, in welchen Bereichen die Aktion der entsprechend definierten Einstellungsart ausgeführt und welche PG-Ausgänge gesteuert werden sollen.

Wochentage – definiert, an welchen Wochentagen die Aktion ausgeführt wird (z.B. Montag).

Tage des Monats – definiert, an welchen Tages des Monats die Aktion ausgeführt wird.

Monate des Jahres – definiert, in welchen Monaten die Aktion im Jahr ausgeführt wird.

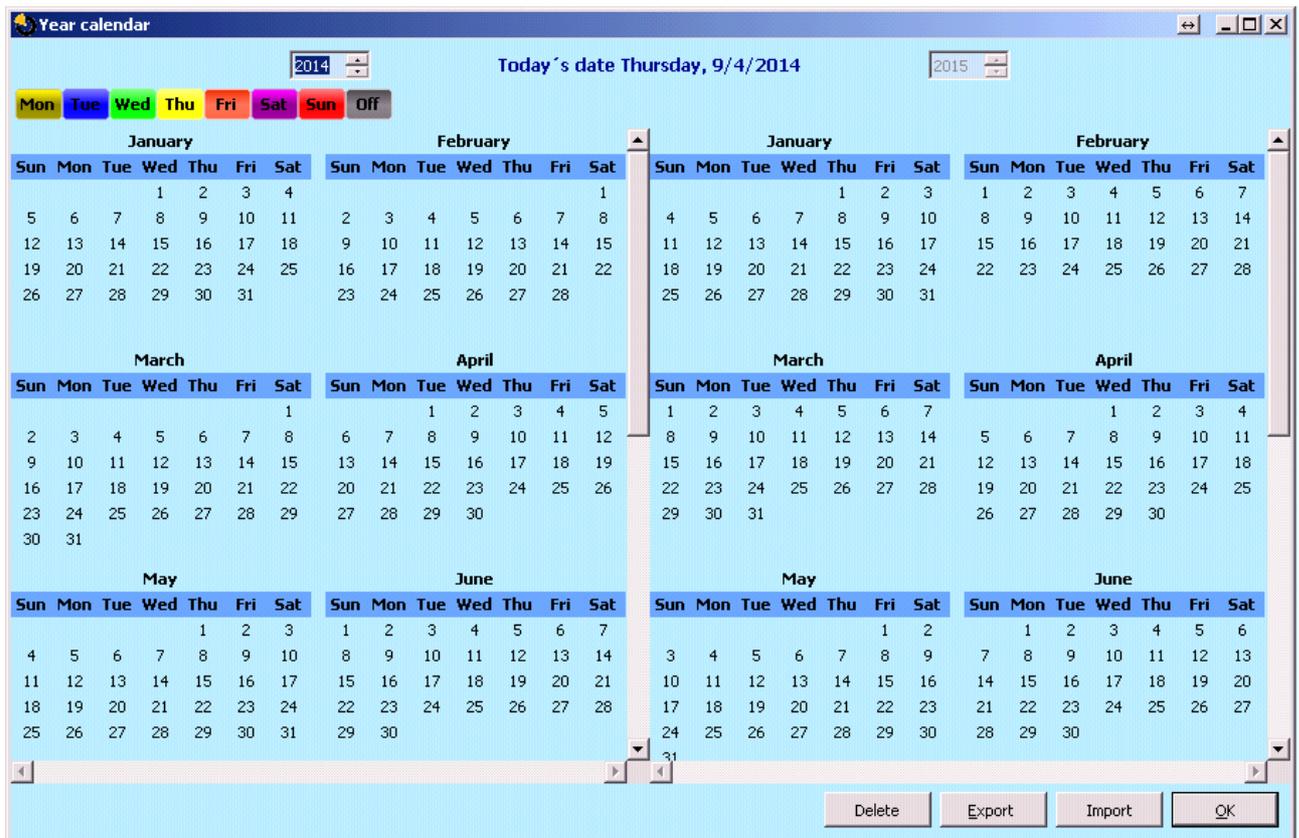
Zeitparameter – Das System ermöglicht Ihnen, eine regelmäßige Wiederholung der erforderlichen Aktion bis zu 4 Mal an einem Tag oder in einem bestimmten Zeitintervall einzurichten. Die Wiederholung kann als eine Zeit VON - BIS definiert werden.

Blockierung – PG-Ausgänge werden hier angeboten, ihre Aktivierung ermöglicht die Sperrung einer Kalenderaktion.

Programmierung deaktivieren – Möglichkeit, eine bestimmte Aktion zu sperren. Die Deaktivierung wird über einen roten Punkt angezeigt. Der Administrator (über J-Link) und der Errichter (über F-Link) ist zur Deaktivierung des Zeitplans berechtigt.

Notiz – ermöglicht die individuelle Beschreibung der geplanten Ereignisse

Jahreskalender – ermöglicht, das Attribut der Tage (Mo, Di, ...So) für einzelne Tage des aktuellen und des nächsten Jahres zu ändern. Die Änderung können Sie vornehmen, indem Sie (wiederholt) mit der Maus auf den entsprechenden Tag klicken. Ein Anwendungsbeispiel: Für einen Feiertag, an dem nicht gearbeitet wird, der aber ein Mittwoch ist, können Sie das Attribut des Tages von Mittwoch auf Sonntag ändern. Ereignisse, die automatisch und in Übereinstimmung mit den Grundeinstellungen des Zeitplans geplant sind und für Arbeitstage gelten, werden an diesem Tag nicht ausgeführt. Jedoch wird das Programm für den Sonntag beibehalten. Auf diese Weise können Sie die Steuerung der Bereiche oder PG z.B. für den Urlaub anpassen. „Aus“ bedeutet deaktiviert - an diesen Tagen wird kein geplantes Ereignis ausgeführt.

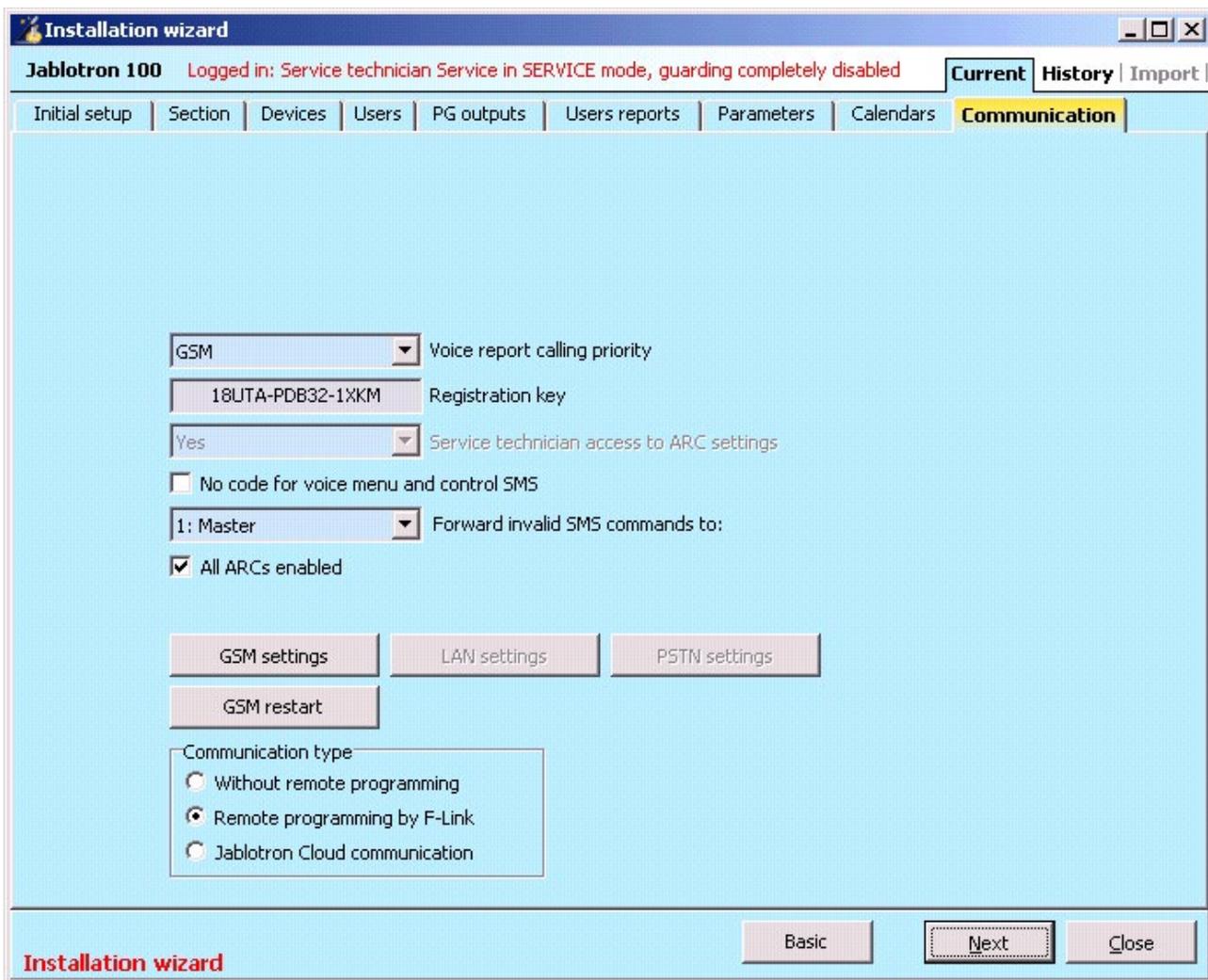


Hinweise:

- Das Ein- und Ausschalten einer Anwendung für eine bestimmte Zeit ist auf zwei Arten möglich. Sie können entweder eine Aktion zur Aktivierung und eine Aktion zur Deaktivierung des PG-Ausgangs einstellen oder nur eine Aktion zur Aktivierung einstellen und einen Impuls der erforderlichen Länge für den PG-Ausgang festlegen
- Wenn Sie die Scharfschaltung (teilweise Scharfschaltung) eines bestimmten Bereichs wählen, wird zum angegebenen Zeitpunkt zuerst eine Ausgangsverzögerung mit der festen Zeit von 3 Min. aktiviert. Alle Sensoren in den bestimmten Bereichen mit der sofortigen Reaktion werden so eingestellt, dass sie die verzögerte Reaktion während dieser Zeit von 3 Minuten haben. Wenn Sie die sofortige Scharfschaltung wählen, gibt es keine Ausgangsverzögerung und alle Melder sind sofort aktiv (einschließlich der verzögerten Melder).

10.11. Registerkarte Übertragungsgeräte

Diese Registerkarte wird zur Einstellung des Verhaltens von Wähl- und Übertragungsgeräten und der Art ihrer Kommunikation verwendet. Um Änderungen an dieser Registerkarte vorzunehmen, müssen Sie sich nicht im Errichter-Modus befinden.



Primärer Übertragungsweg von Sprachnachrichten – Auswahl des Kanals, über den die Zentrale Sprachereignisse melden soll (Optionen GSM / PSTN).

Registrierschlüssel – der spezifische Anmeldecode der Zentrale

Zugang des Errichters für AES Einstellungen – ermöglicht es dem AES-Techniker, den Zugriff des Errichters auf die Registerkarte ARC zu beschränken.

Freigabe von Sprachmenü und SMS Befehlen ohne zusätzlichen Code – wenn ein berechtigtes Telefon verwendet wird, um eine Funktion über einen Anruf zu steuern, muss der Benutzer nicht seinen Code eingeben (die Berechtigung erfolgt über den Anruf von seinem Telefon aus). Für diese Funktion muss die Identifikation des Anrufers (CLIP) aktiviert sein.

Systemfremde SMS weiterleiten an – Auswahl des Benutzers, an den SMS-Nachrichten, die für die Zentrale nicht verständlich sind, weitergeleitet werden (Rechnungsinformationen vom Betreiber usw.).

SMS bei nicht erfolgreichen Scharfschalten – Die Zentrale sendet SMS über fehlgeschlagene Scharfschaltungen. Bei einer fehlgeschlagenen Scharfschaltung mit Berechtigung (durch einen berechtigten Benutzer) wird die SMS an diesen Benutzer gesendet. Bei fehlgeschlagener Scharfschaltung ohne Berechtigung wird die SMS an den Administrator auf Position 1 gesendet.

AES global aktivieren – Option, um die gesamte Kommunikation mit dem ARES zu deaktivieren - nicht verfügbar, wenn der ARC-Techniker den Zugriff eingeschränkt hat.

Kommunikationstyp – das System bietet verschiedene Methoden der ferngesteuerten Kommunikation / Konfiguration an:

- **Keine Fernkonfiguration**– es verhält sich wie ein autonomes Gerät mit einer eigenen SIM-Karte. Das Gerät kommuniziert nach außen (sendet SMS- und Sprachnachrichten) und empfängt SMS-Befehle und verfügt über ein funktionierendes Sprachmenü. Die Fernkonfiguration mit der F-Link-Software ist nicht möglich.
- **Begrenzt auf (GSM)** – kommuniziert wie der vorherige Typ und unterstützt zusätzlich die Fernkonfiguration des Systems. Die Fernkonfiguration ist von einem Computer mit F-Link (J-Link) und einer Internetverbindung möglich. Um eine Verbindung mit der Zentrale herzustellen, stellt F-Link eine Verbindung zum Server des Herstellers her, um ihm den Anmeldecode und die Telefonnummer der SIM-

Karte bereitzustellen, die im Kommunikator der Zentrale ist. In der Zentrale muss es eine funktionsfähige Datenkommunikation geben (LAN oder GSM / GPRS / UMTS / ..).

- **Dauerhaft per LAN** – die Zentrale kommuniziert dauerhaft mit dem Server und ermöglicht eine Verbindung per Fernzugriff via F-Link.
- **JABLOTRON Fernkonfiguration** – Das Gerät kommuniziert mit dem Server des Herstellers (MyJABLOTRON-Applikation) und sendet ihm kontinuierlich Informationen über den Gerätestatus. Wenn F-Link (J-Link) eine Anforderung für eine Verbindung per Fernzugriff sendet, ist der Server sofort bereit, eine Verbindung herzustellen. Zusätzlich ermöglicht diese Kommunikation dem Benutzer, Serverdienste zu verwenden. Applikationen, mit denen der Benutzer das System bedienen kann, können in mobilen Geräten mit Android- oder iOS-Systemen installiert werden. Für diese Option muss die Sicherheits-SIM-Karte von JABLOTRON verwendet werden.

Informationen zu den Möglichkeiten der Verwendung der einzelnen Kommunikationstypen in Ihrem Land erhalten Sie von Ihrem Händler.

Einstellungen – Die Taste dient zur Anmeldung des Systems beim CLOUD-Service MyJABLOTRON. Wenn Sie das Formular ausfüllen und die Daten zur Bestätigung senden, erstellt es eine Anmeldeanfrage. Die Bestätigung des ausgefüllten Formulars erfolgt umgehend.

10.11.1. GSM-Modul

Diese Taste stellt die Parameter und das Verhalten des GSM-Wähl- und Übertragungsgerätes ein.

* Eine so markierte Position wird automatisch nach der Aktivierung der Zentrale eingestellt, wenn ein GSM-Kommunikator installiert wurde und vor der Aktivierung in diesen eine funktionsfähige SIM-Karte eingesetzt wurde (Wartung des JABLOTRON-Servers).

Wählgerät – Möglichkeit, den Kommunikator auszuschalten.

Signalstärke – Information über die Signalstärke in Prozent (dies wird einmal pro Minute gemessen). Für eine ausreichende Funktion sollte die Signalstärke bei mindestens 50% liegen. Wenn Sie Probleme mit der GSM-Signalqualität haben, empfiehlt es sich, die SIM-Karte eines anderen Betreibers zu testen. Es wird nicht empfohlen, eine Richt- oder Verstärkungs-GSM-Antenne für den Kommunikator zu verwenden (dies reduziert nur die Verbindung des Moduls = instabile Kommunikation). Informationen über die Signalqualität erhalten Sie über den SMS-Befehl STATUS (siehe Kapitel 9.6 SMS-Befehle).

SIM-Karten PIN – Wir empfehlen, eine SIM-Karte ohne PIN-Code zu verwenden.

APN Provider* – Einstellungen der GPRS/UMTS/..-Datenkommunikation. Die Datenkommunikation ermöglicht den Zugriff auf Dienste des JABLOTRON-Servers, ermöglicht den Fernzugriff eines Servicetechnikers, die Kommunikation mit dem ARC usw. Neben den APN-Einstellungen muss die verwendete SIM-Karte die Datenübertragung unterstützen.

Kontaktieren Sie Ihren JABLOTRON-Händler für weitere Informationen über die Möglichkeit dieser Kommunikation.

APN-Benutzername* – Name (geben Sie keinen ein, es sei denn, das Netzwerk verwendet ihn).

APN Passwort* – Passwort (geben Sie keins ein, es sei denn, das Netzwerk verwendet es).

Anruf-Limit in Min./Tag – schränkt Anrufe von 5 bis 250 Minuten pro Tag ein.

Limitier für gesendete SMS – Diese Beschränkung beschränkt die Anzahl der SMS, die pro Tag über die Zentrale gesendet werden. Es umfasst Alarm- und auch Nicht-Alarm-Ereignisse (Alarmereignisse - Alarm, Sabotage, Störung, Meldung, ...; Nicht-Alarm - PG, Service ...). Die zu sendende Anzahl beträgt 5 bis 250 SMS. Das System kann maximal 250 SMS pro Tag senden. Diese maximale Anzahl wird zwischen der SMS-Beschränkung und der Alarm-SMS-Beschränkung aufgeteilt (F-Link überprüft automatisch, dass die Einstellung beider Beschränkungen nicht 250 überschreitet).

Limitier für Alarm-SMS – Die Beschränkung beschränkt die Anzahl der Alarm-SMS pro Tag von der Zentrale aus, wenn die Grenze der gesendeten SMS bereits erreicht ist (SMS-Beschränkung. Sie bezieht sich auf Alarmereignisse (Alarmer, Sabotage, Störungen, Berichte, ...). Der einzustellende Bereich reicht von 0 bis 245 SMS. **Beispiel:** Die *Beschränkung der gesendeten SMS* ist auf 30 eingestellt, die Beschränkung der Alarm-SMS ist auf 20 eingestellt. Das Systemverhalten ist wie folgt: Wenn für einen Tag ein beliebiger Typ von 30 SMS gesendet wird (Alarm und Nicht-Alarm), sendet das System an diesem Tag keine Nicht-Alarm-SMS. Aber es kann immer noch Alarm-SMS senden (aber 20 ist das Maximum). Dies stellt sicher, dass das System immer eine Reserve für den Fall eines Alarms hat, um den Benutzer per SMS informieren zu können.

Diakritik (Umlaute) erlauben – Wenn internationale Zeichenakzente (ICC) erlaubt sind, können Meldungen vom System über mehr als eine SMS-Textnachricht verschickt werden. ICC muss aktiviert sein, wenn Sie z.B. das russische Alphabet in Ihren Texten verwenden u.s.w.

Fernsteuerung per Telefon – Einstellung, um das System per Fernzugriff über das Sprachmenü zu steuern. Wenn Benutzer für diese Funktion ausgewählt sind, kann nur über die Telefone der definierten Benutzer auf das Menü zugegriffen werden (in der Registerkarte Kommunikation können Sie Benutzern den Zugang zum Sprachmenü ohne Eingabe des Benutzercodes ermöglichen - das Sprachmenü ohne Codeoption). Wenn „Jeder“ ausgewählt ist, kann auf das Sprachmenü von jedem Telefon aus zugegriffen werden. Jedoch wird der Benutzer immer seinen Benutzercode eingeben müssen.

Fernsteuerung per SMS – Einstellung zur Fernsteuerung des Systems per SMS-Befehle. Wenn Benutzer für diese Funktion ausgewählt sind, akzeptiert das System nur SMS-Befehle von den Telefonen der definierten Benutzer (in der Registerkarte Kommunikation können Sie den Benutzern SMS-Befehle ohne Eingabe des Benutzercodes ermöglichen - das Sprachmenü ohne Codeoption). Wenn „Jeder“ ausgewählt ist, kann ein SMS-Befehl von jedem Telefon aus eingestellt werden. Jedoch wird der Benutzer immer seinen Zugriffscode eingeben müssen.

Guthabenabfrage – mit dieser Taste erhalten Sie sofort eine SMS des Betreibers mit Informationen über Ihr Guthaben (wenn diese Funktion aktiviert ist).

Guthabenlimit – Festlegung des unteren Limits beim automatischen Prüfen des Limits einer Prepaid-SIM-Karte. Wenn das festgelegte Guthaben unter diesem Limit ist, sendet das System eine SMS an den Benutzer, dem die Meldungen **SMS-Fehler und Service** zugewiesen sind. **Wir empfehlen Ihnen nicht, eine Prepaid-Karte im System zu verwenden - sie erhöhen das Risiko eines Kommunikationsfehlers**

Sequenz für Guthabenabfrage – Befehl zur automatischen Saldoabfrage einer Prepaid-SIM-Karte (wenn dies vom Betreiber unterstützt wird). Sie erhalten diese Befehle von Ihrem Betreiber.

Guthabenposition – Position (aufeinanderfolgende Zeichenanzahl) in der Meldung des Betreibers, an der die numerische Information zum Guthaben beginnt (der Kommunikator sucht nur nach Ziffern im Bericht und ignoriert die anderen Zeichen)

Abfragezeitraum – Einstellung, wie oft das System das Guthaben prüft (Sie können 0 bis 99 Tage einstellen, 0 ist aus).

Tel.Nr. vom Erhaltungsanruf - Wenn die Prepaid-SIM-Karte die Aufrechterhaltung von Anrufen erfordert, können Sie eine Telefonnummer festlegen, die das System automatisch wählt (z. B. den genauen Zeitdienst), wenn kein abgehender Anruf vom System für einen Zeitraum von mehr als 90 Tagen erfolgt ist (10 Sek. nach Beantwortung des Anrufs durch den angerufenen Teilnehmer legt das System auf).

SIMLock – Funktion, die die Telefonnummer der SIM-Karte mit den ARC-Einstellungen verbindet. Wenn Sie die SIM-Karte durch eine andere Karte ersetzen und die SIM-Karte im GSM-Netzwerk angemeldet ist, werden alle Einstellungen **der Registerkarte AES gelöscht**. Das Löschen ist irreversibel und andere Einstellungen (Anmeldung beim MyJABLOTRON-Webservice) müssen erneut vom ARC-Techniker vorgenommen werden.

Empfindlichkeit der DTMF-Signale – Einstellung der Empfangsempfindlichkeit des vom ARC erzeugten Signals. Die Empfindlichkeit ist in 10 Stufen einstellbar; Der optimale Standardwert ist 4.

Stufen des erzeugten DTMF-Signale – Einstellung der Intensität des übertragenen Tonwahlsignals in DTMF, das von der Zentrale erzeugt wird. Die Intensität ist in 10 Stufen einstellbar; Der optimale Standardwert ist 4.



Ruftonanzahl der eingehenden Anrufe – Anzahl der Klingelimpulse bis zur automatischen Antwort durch den Kommunikator. Sie können den Anruf von 1 bis 10 Klingelimpulsen (entsprechend 5 bis 50 Sekunden) einstellen. Der Standardwert ist 3 (15 Sekunden).

Telefonnummer der SIM-Karte – Telefonnummer der SIM-Karte, die im Kommunikator verwendet wird.

Telefonnummer des Wählgeräts abrufen – Die SMS-Anfrage wird gesendet, wenn die Taste gedrückt wird. Nach einer erfolgreichen Antwort wird die Telefonnummer im Feld „SIM-Karten-Telefonnummer“ angezeigt.

Security Data Connector™ – Der Dienst des Security Data Connector™ wird in der Zentrale verwendet. Alle GSM-Parameter sind voreingestellt und können nicht geändert werden.

GSM-Betreiber wechseln – Diese Option ermöglicht das automatische Schalten zwischen den GSM-Betreibern

1 – Die so markierten Positionen sind verfügbar, wenn der Security Data Connector™ verwendet wird.

10.11.2. LAN-Modul

Zur Einstellung des LAN-Übertragungsgerätes (wenn die Zentrale über einen verfügt).

Wählgerät – Möglichkeit, die LAN-Kommunikation zu aktivieren oder deaktivieren.

IP-Adresse automatisch (vom DHCP-Server) beziehen - Automatische Einstellung der Netzwerkparameter. Wenn diese Funktion nicht vom Netzwerk unterstützt wird, müssen die entsprechenden Parameter manuell eingegeben werden. Die Manuelle Eingabe ist nur möglich, wenn diese Option nicht ausgewählt wird.

IP-Adresse – die IP-Adresse kann nur manuell zugewiesen werden, wenn die automatische Zuweisung vom DHCP-Server nicht aktiviert ist. Die standardmäßige Einstellung ist 192.168.1.99

Subnetzmaske – die IP-Subnetzmaske kann nur manuell zugewiesen werden, wenn die automatische Zuweisung vom DHCP-Server nicht aktiviert ist. Die standardmäßige Einstellung ist 255.255.255.0

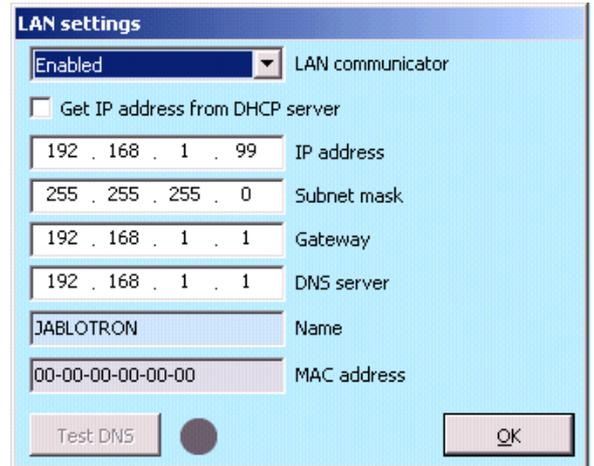
Gateway – das Standard-IP-Gateway kann nur manuell zugewiesen werden, wenn die automatische Zuweisung vom DHCP-Server nicht aktiviert ist. Die standardmäßige Einstellung ist 192.168.1.1

DNS-Server – der DNS-Server kann nur manuell zugewiesen werden, wenn die automatische Zuweisung vom DHCP-Server nicht aktiviert ist. Die standardmäßige Einstellung ist 192.168.1.1

Name im Netzwerk – der Gerätenamen für eine einfachere Identifikation im lokalen Netzwerk

MAC-Adresse – eindeutige Adresse eines LAN-Geräts (Identifikation der Datenquelle) Identifikation des LAN-Geräts als Informationsquelle

DNS-Test – wenn der LAN-Kommunikator mit dem Internet verbunden ist, kann getestet werden, ob die Einstellungen korrekt sind. Wenn ein grüner Punkt nach Tastenbetätigung erscheint, wurde eine Verbindung mit dem Server aufgebaut, wenn aber nach ein paar Sekunden ein roter Punkt erscheint, ist die Zeit für den Verbindungsaufbau abgelaufen, was bedeutet, dass die Einstellungen nicht korrekt sind oder ein Verbindungsfehler mit dem LAN-Kommunikator vorliegt.

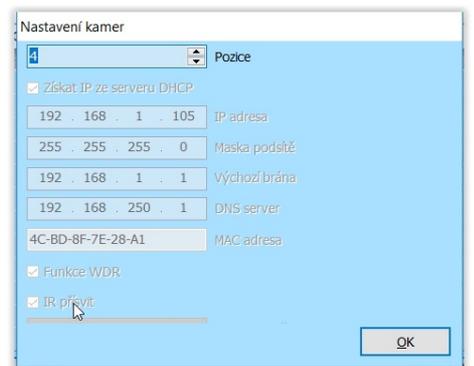


10.11.3. Kameras

Mit der Taste Kameras können Sie einen Verbindungstest (sofern die erforderlichen Ports zugelassen sind) und einen Test der Verbindungsgeschwindigkeit durchführen. Nachdem der Test erfolgreich abgeschlossen wurde, wird eine Grafik zusammen mit einer Aussage darüber angezeigt, wie viele Kameras in welcher Auflösung in diesem bestimmten Netzwerk arbeiten können. Wenn bereits eine aktive Kamera im Netzwerk angeschlossen ist, können Sie in F-Link die Grundparameter einstellen.

Position – Position im System

IP-Adresse vom DHCP-Server – automatische Einstellung der Netzwerkparameter. Wenn diese Funktion vom Netzwerk nicht unterstützt wird, müssen die entsprechenden Parameter manuell eingegeben werden. Die manuelle Eingabe ist nur möglich, wenn diese Option nicht deaktiviert ist.



IP-Adresse – Einstellung für die manuelle Zuweisung der IP-Adresse, die nur verfügbar ist, wenn die automatische Zuweisung vom DHCP-Server nicht aktiviert ist. Die Standardeinstellung ist 192.168.1.99.

Subnetzmaske – Einstellung für die IP-Zuweisung der Subnetzmaske, die nur verfügbar ist, wenn die automatische Zuweisung vom DHCP-Server nicht aktiviert ist. Die Standardeinstellung ist 255.255.255.0.

Gateway – Einstellung für die manuelle IP-Zuweisung des Standard-Gateways, das nur verfügbar ist, wenn die automatische Zuweisung vom DHCP-Server nicht aktiviert ist. Die Standardeinstellung ist 192.168.1.1.

DNS-Server – Einstellung für manuelle IP-Zuweisung des DNS-Servers, der nur verfügbar ist, wenn die automatische Zuweisung vom DHCP-Server nicht aktiviert ist. Die Standardeinstellung ist 192.168.1.1.

MAC-Adresse – eindeutige Adresse jedes LAN-Geräts (Identifikation der Datenquelle).

WDR-Funktion – Deaktivieren des WDR (Wide Dynamic Range - Gegenlichtkompensation) für z.B. Bereiche mit einem hohen Kontrast von hellen und dunklen Orten.

IR-Beleuchtung – Deaktivieren der IR-Beleuchtung für z.B. Bereiche mit dauerhafter Beleuchtung.

Kameramodus – Auswahl des Kameramodus, Sie können zwischen Tag-, Nacht- und Automatikmodus wählen.

10.11.4. GSM-Neustart

Taste zum Abmelden des Kommunikators und erneutes Anmelden im Netzwerk. Es kann einige Sekunden dauern, bis der GSM-Kommunikator im Netzwerk erneut protokolliert wird (abhängig vom aktuellen Status des Systems). GSM kann auch mit dem SMS-Befehl GSM neu gestartet werden (siehe Kapitel 9.6 SMS-Befehle).

10.12. Registerkarte AES - Alarmempfangsstelle

In dieser Registerkarte können Sie die Kommunikation für Alarmempfangszentren einstellen. Wenn in der Registerkarte Kommunikation der Zugriff des Errichters eingeschränkt ist, kann dieser Parameter nur von einer Person mit der Berechtigungsstufe AES-Techniker eingestellt werden. Die Option ist auch nicht verfügbar, wenn die JABLOTRON-Kommunikation ausgewählt ist, was die Einstellung der Kommunikation des Systems erheblich vereinfacht. Um Änderungen in dieser Registerkarte vorzunehmen, ist der Servicemodus (Errichter-Modus) nicht erforderlich.

Posi...	ARC enabled	Next ARC is the backup ...	Protocol	Communicator	Domain 1 (tel. 1)	Domain 2 (tel. 2)	Section ID	Reported events	Timing	ARC test
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CID	GSM			Enter	Enter	Enter	ARC test
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	JabloIP	LAN			Enter	Enter	Enter	ARC test
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No	GSM			Enter	Enter	Enter	ARC test
4	<input type="checkbox"/>		JabloIP	GSM			Enter	Enter	Enter	ARC test
5	<input type="checkbox"/>		JabloIP Cr...	GSM						

AES aktivieren – Möglichkeit, die eingestellte Kommunikation zu deaktivieren

Nächster AES als Redundanz - Bei Aktivierung wird die nächste Position nur dann verwendet, wenn die Daten vom aktuellen ARC nicht übertragen werden können.

Protokoll – Einstellungen des Übertragungsprotokolls

Übertragungsweg – Wenn das ausgewählte Protokoll auf mehrere Arten an die AES übertragen werden kann, wird hier der Kommunikationstyp ausgewählt. Die Optionen sind GSM, LAN, Telefonleitung und Automatisch, aber nur die aktuell verfügbaren Optionen sind sichtbar. Die Option Automatisch verwendet eine Kombination von LAN / GSM-Kommunikatoren, die hauptsächlich LAN verwendet. Wenn LAN nicht verfügbar ist, wird zum Backup-GSM geschaltet. Bei einem Ausfall der Übertragung von beiden Kommunikatoren meldet das System einen Fehler - die Daten werden nicht an die AES übertragen.

Primäre Tel./IP (Leitung 1) – Einstellung der Hauptdomain (unter Verwendung von URL oder IP-Adresse), oder der Haupttelefonnummer, je nach verwendetem Protokoll. Bei Verwendung der IP-Kommunikation, müssen Sie die Schnittstelle nach der IP-Adresse getrennt durch eine Spalte eingeben. Sie erhalten die Schnittstelle und die Daten der IP-Adresse von der AES, an den die Kommunikation geleitet wird. Wenn keine Schnittstelle eingegeben wird, wird das Ereignis nicht übertragen.

Secundäre Tel./IP (Leitung 2) – Einstellung einer Backup-Domain (unter Verwendung von URL oder IP-Adresse) oder einer Backup-Telefonnummer, je nach verwendetem Protokoll.

Identnummer – Einstellung der Gebäudeidentifikation (gemeinsam für das gesamte Gebäude oder individuell für Bereiche).
Warnhinweis: Die Standardeinstellung ist null, mit der der Kommunikator keine Meldungen schicken kann!

Ereignisse – Auswahl der gemeldeten Ereignisarten und Möglichkeit, Codes von zusätzlichen Meldungen (PG-Ausgänge, spezielle Meldungen A bis D) einzustellen

Zeitparameter – Einstellung der Zeitlimits für Übertragungen und Zeiteinstellung der Verbindungsprüfung

Test – Manuelle Prüfung, ob die Verbindung mit dem entsprechenden Protokoll gestartet wird.

Notiz – hier können Sie Einzelheiten zu den AES-Einstellungen, dem Beginn des Service u.s.w. vermerken.

10.12.1. JABLOTRON 100 + CID und SIA-Codes

CID	SIA	Ereignis EN	Meldungskategorie
1101	QA	Personennotfall	Einbruch
1110	FA	Feueralarm	Feuer
1118	FG	Bevorstehender Feueralarm	Feuer
1120	PA	Überfall- Geiselnahmealarm	Geiselnahme
1130	BA	Sofortiger Alarm	Einbruch
1130	BA	Keybox	Spezielle Meldungen
1133	BA	24 Std.-Alarm	Einbruch
1134	BA	Verzögerter Alarm	Einbruch
1138	BG	Bevorstehender Alarm	Einbruch
1138	BG	Bevorstehender Alarm	Feuer
1144	TA	Gehäusesabotage	Sabotage
1151	FA	Gasaustritt	Feuer
1154	WA	Wasserleck	Feuer
1158	KA	Übertemperatur (von FW20 aufwärts)	Nicht kategorisiert
1159	ZA	Untertemperatur (von FW20 aufwärts)	Nicht kategorisiert
1170	UA	Spezielle Reaktion A	Spezielle Meldungen
1171	UA	Spezielle Reaktion B	Spezielle Meldungen
1172	UA	Spezielle Reaktion C	Spezielle Meldungen
1173	UA	Spezielle Reaktion D	Spezielle Meldungen
1174	UA	Nicht verwendet	Nicht kategorisiert
1300	ET	Systemstörung	Fehler und Serviceereignisse
1300	ET	Systemstörung	Fehler und Serviceereignisse
1301	AT	Netz-fehlt	Fehler und Serviceereignisse
1302	YT	Schwache Batterie in der Zentrale	Fehler und Serviceereignisse
1305	RR	Systemboot	Fehler und Serviceereignisse
1306	LB	Servicemodus (Errichter-Modus) eingeben	Fehler und Serviceereignisse
1308	RE	Systemabschaltung	Fehler und Serviceereignisse
1313	YX	Gesperrt nach Alarm - Zurücksetzung durch den Techniker	Nicht kategorisiert
1314	YG	AES-Einstellung zurückgesetzt	Nicht kategorisiert
1344	XQ	RF-Störung	Fehler und Serviceereignisse
1350	YC	Ereignis nicht an die AES zugestellt	Nicht kategorisiert
1354	YS	Ereignis an die AES nicht in voreingestellter Zeit zugestellt	Fehler und Serviceereignisse
1384	XT	Schwache Batterie	Fehler und Serviceereignisse
1389	TO	Test fehlgeschlagen	Fehler und Serviceereignisse
1401	OP	S/US durch Nutzer	Scharfschaltung / Unscharfschaltung
1402	OG	Gruppe S/US	Scharfschaltung / Unscharfschaltung
1406	BC	Alarm vom Benutzer beendet	Einbruch
1406	BC	Alarm vom Benutzer beendet	Einbruch
1406	BC	Alarm vom Benutzer beendet	Einbruch
1406	BC	Alarm vom Benutzer beendet	Einbruch
1406	BC	Alarm vom Benutzer beendet	Einbruch
1407	OQ	Deaktivierung per Fernzugriff	Scharfschaltung / Unscharfschaltung
1412	LF	Download/Zugriff erfolgreich	Nicht kategorisiert
1416	LS	Konfiguration gespeichert	Nicht kategorisiert
1454	NA	Bereich ohne Bewegung - Fehler bei Scharf	Fehler und Serviceereignisse
1455	CI	Fehlgeschlagene Aktivierung	Nicht kategorisiert
1461	JA	Codeentschlüsselungsversuch überschritten	Sabotage
1521	BL	Sirene stumm	Nicht kategorisiert
1570	EB	Gerätebypass (Deaktiviert)	Nicht kategorisiert
1572	TB	Sabotagebypass	Fehler und Serviceereignisse
1573	BB	Bypassaktivierung	Fehler und Serviceereignisse
1573	BB	Bypassaktivierung	Fehler und Serviceereignisse
1574	UB	Bereichsbypass (Deaktivierung)	Nicht kategorisiert
1578	UO	Fehler Bypass	Fehler und Serviceereignisse
1601	RX	Manueller Test	Fehler und Serviceereignisse

1601	RX	Manueller Test	Fehler und Serviceereignisse
1601	RX	Manueller Test	Fehler und Serviceereignisse
1601	RX	Manueller Test	Fehler und Serviceereignisse
1602	RP	Periodischer Test	Nicht kategorisiert
1602	RP	Periodischer Test	Nicht kategorisiert
1602	RP	Periodischer Test	Nicht kategorisiert
1602	RP	Periodischer Test	Nicht kategorisiert
1602	RP	Periodischer Test	Nicht kategorisiert
1602	RP	Periodischer Test	Nicht kategorisiert
1625	JT	Zurücksetzung der Zeit	Nicht kategorisiert
1661	RC	PG1 EIN	PG-Steuerungen
1662	RC	PG2 EIN	PG-Steuerungen
1663	RC	PG3 EIN	PG-Steuerungen
1664	RC	PG4 EIN	PG-Steuerungen
1665	RC	PG5 EIN	PG-Steuerungen
1666	RC	PG6 EIN	PG-Steuerungen
1667	RC	PG7 EIN	PG-Steuerungen
1668	RC	PG8 EIN	PG-Steuerungen
1669	RC	PG9 EIN	PG-Steuerungen
1670	RC	PG10 EIN	PG-Steuerungen
1671	RC	PG11 EIN	PG-Steuerungen
1672	RC	PG12 EIN	PG-Steuerungen
1673	RC	PG13 EIN	PG-Steuerungen
1674	RC	PG14 EIN	PG-Steuerungen
1675	RC	PG15 EIN	PG-Steuerungen
1676	RC	PG16 EIN	PG-Steuerungen
1677	RC	PG17 EIN	PG-Steuerungen
1678	RC	PG18 EIN	PG-Steuerungen
1679	RC	PG19 EIN	PG-Steuerungen
1680	RC	PG20 EIN	PG-Steuerungen
1681	RC	PG21 EIN	PG-Steuerungen
1682	RC	PG22 EIN	PG-Steuerungen
1683	RC	PG23 EIN	PG-Steuerungen
1684	RC	PG24 EIN	PG-Steuerungen
1685	RC	PG25 EIN	PG-Steuerungen
1686	RC	PG26 EIN	PG-Steuerungen
1687	RC	PG27 EIN	PG-Steuerungen
1688	RC	PG28 EIN	PG-Steuerungen
1689	RC	PG29 EIN	PG-Steuerungen
1690	RC	PG30 EIN	PG-Steuerungen
1691	RC	PG31 EIN	PG-Steuerungen
1692	RC	PG32 EIN	PG-Steuerungen
3101	QR	Gesundheitsprobleme (Deaktivierung)	Einbruch
3110	FR	Feueraarm (Deaktivierung)	Feuer
3118	FH	Unbestätigter Feueralarm (Deaktivierung)	Feuer
3120	PR	Überfall- Geiselnahmealarm (Deaktivierung)	Geiselnahme
3130	BR	Sofortiger Alarm (Deaktivierung)	Einbruch
3130	BR	Schlüsselbox (Deaktivierung)	Spezielle Meldungen
3133	BR	24 Std.-Alarm (Deaktivierung)	Einbruch
3134	BR	Verzögerter Alarm (Deaktivierung)	Einbruch
3138	BH	Unbestätigter Alarm (Deaktivierung)	Einbruch
3138	BH	Unbestätigter Alarm (Deaktivierung)	Einbruch
3144	TR	Sabotage (Deaktivierung)	Sabotage
3151	FR	Gasaustritt (Deaktivierung)	Feuer
3154	WR	Überschwemmungsalarm (Deaktivierung)	Einbruch
3158	KH	Überhitzung (Deaktivierung) (von FW20 aufwärts)	Nicht kategorisiert
3159	ZH	Gefrieren (Deaktivierung) (von FW20 aufwärts)	Nicht kategorisiert
3170	UR	Spezielle Reaktion A (Deaktivierung)	Spezielle Meldungen
3171	UR	Spezielle Reaktion B (Deaktivierung)	Spezielle Meldungen
3172	UR	Spezielle Reaktion C (Deaktivierung)	Spezielle Meldungen
3173	UR	Spezielle Reaktion D (Deaktivierung)	Spezielle Meldungen
3174	UR	Nicht verwendet	Nicht kategorisiert
3300	ER	Fehler (Deaktivierung)	Fehler und Serviceereignisse
3301	AR	AC-Wiederherstellung	Fehler und Serviceereignisse
3301	AR	AC-Wiederherstellung	Fehler und Serviceereignisse
3302	YR	Batterie der Zentrale OK	Fehler und Serviceereignisse
3306	LX	Verlassen des Servicemodus	Fehler und Serviceereignisse
3313	YZ	Nicht gesperrt nach Alarm	Fehler und Serviceereignisse
3344	XH	RF-Interferenz (Deaktivierung)	Fehler und Serviceereignisse
3350	YK	Kommunikation mit dem ARC wiederhergestellt	Nicht kategorisiert
3354	YL	Ereignis dem ARC nicht in voreingestellter Zeit zugestellt (Deaktivierung)	Fehler und Serviceereignisse
3384	XR	Batterie im Gerät OK	Fehler und Serviceereignisse
3389	TI	Test OK	Fehler und Serviceereignisse
3401	CL	Scharf	Scharfschaltung / Unscharfschaltung
3402	CG	Teilscharf	Scharfschaltung / Unscharfschaltung
3407	CQ	Scharf per Fernzugriff	Scharfschaltung / Unscharfschaltung

3412	LE	Fernzugriff geschlossen	Nicht kategorisiert
3570	EU	Per Fernzugriff teilweise scharf	Scharfschaltung / Unscharfschaltung
3572	TU	Ende des Geräte-Bypass (Deaktivierung)	Nicht kategorisiert
3573	BU	Beendigung des Sabotage-Bypass	Fehler und Serviceereignisse
3573	BU	Aktivierung der Beendigung des Bypass	Fehler und Serviceereignisse
3574	UU	Beendigung des Bereichs-Bypass (Deaktivierung)	Nicht kategorisiert
3578	UP	Fehler Bypass (Deaktivierung)	Fehler und Serviceereignisse
3661	RO	PG1 AUS	PG-Steuerungen
3662	RO	PG2 AUS	PG-Steuerungen
3663	RO	PG3 AUS	PG-Steuerungen
3664	RO	PG4 AUS	PG-Steuerungen
3665	RO	PG5 AUS	PG-Steuerungen
3666	RO	PG6 AUS	PG-Steuerungen
3667	RO	PG7 AUS	PG-Steuerungen
3668	RO	PG8 AUS	PG-Steuerungen
3669	RO	PG9 AUS	PG-Steuerungen
3670	RO	PG10 AUS	PG-Steuerungen
3671	RO	PG11 AUS	PG-Steuerungen
3672	RO	PG12 AUS	PG-Steuerungen
3673	RO	PG13 AUS	PG-Steuerungen
3674	RO	PG14 AUS	PG-Steuerungen
3675	RO	PG15 AUS	PG-Steuerungen
3676	RO	PG16 AUS	PG-Steuerungen
3677	RO	PG17 AUS	PG-Steuerungen
3678	RO	PG18 AUS	PG-Steuerungen
3679	RO	PG19 AUS	PG-Steuerungen
3680	RO	PG20 AUS	PG-Steuerungen
3681	RO	PG21 AUS	PG-Steuerungen
3682	RO	PG22 AUS	PG-Steuerungen
3683	RO	PG23 AUS	PG-Steuerungen
3684	RO	PG24 AUS	PG-Steuerungen
3685	RO	PG25 AUS	PG-Steuerungen
3686	RO	PG26 AUS	PG-Steuerungen
3687	RO	PG27 AUS	PG-Steuerungen
3688	RO	PG28 AUS	PG-Steuerungen
3689	RO	PG29 AUS	PG-Steuerungen
3690	RO	PG30 AUS	PG-Steuerungen
3691	RO	PG31 AUS	PG-Steuerungen
3692	RO	PG32 AUS	PG-Steuerungen
6301	AT	Netz fehlt für länger als 30 Min (von FW10 aufwärts)	PG-Steuerungen

Quellen für JA 100	
001 – 249	Meldelinien (Geräte)
251 – 850	Benutzercodes
250	Servicecode (Errichter-Code)
901	Zentrale
921	AES1
922	AES2
923	AES3
924	AES4
925	AES5
911	GSM-Übertragungsgerät
912	LAN-Übertragungsgerät
913	PSTN-Übertragungsgerät
914	GSM-Übertragungsgerät extern

	PG	
	Bereich	CID Komposition
1. Gruppe	1 – 32 PG	Bereich 1 + 1661 – 1692 / 3661 -3692
2. Gruppe	33 – 64 PG	Bereich 2 + 1661 – 1692 / 3661 -3692
3. Gruppe	65 – 96 PG	Bereich 3 + 1661 – 1692 / 3661 -3692
4. Gruppe	97 – 128 PG	Bereich 2 + 1661 – 1692 / 3661 -3692

Beispiel: Objekt-ID 1234, 18 konstant, PG EIN Nr. 33, 02 ist ein Bereich, 901 ist eine Ereignisquelle der Zentrale = **1234 18 1 661 02 901**

10.12.2. Einstellung zur Übertragung von Fotos an einen externen Speicher

Wenn der MyJABLOTRON-Service in der Region / dem Land aktiviert ist und der Gerätebenutzer ihn verwenden möchte, werden die erforderlichen Einstellungen bei Anmeldung der Zentrale beim MyJABLOTRON-Webservice automatisch vollständig vorgenommen.

10.13. Registerkarte Diagnose

Hier können der Status der Geräte und ihre Eigenschaften geprüft und verifiziert werden.

P	Name	Type	Section	Activation...	Status	Battery status/voltage	Voltage/ loss	RF Signal level	Channel	Note
0	Control panel	JA-101K	1: Groud floor		OK	13.7 V/13.7 V	13.7 V/163 mA	100 % GSM		
1	Radio module	JA-110R	1: Groud floor		OK		-0,1 V		RJ	
2	LCD keypad	JA-114E	1: Groud floor		OK		-0,4 V		RJ	
3	Main door	JA-110M	1: Groud floor		ACT		0,0 V		Bus 1	
4	Kitchen window	JA-110M	1: Groud floor		OK		0,0 V		Bus 1	
5	Garage door	JA-111M	3: Garage		ACT		0,0 V		Bus 1	
6	Hall	JA-110P	1: Groud floor		OK		-0,1 V		Bus 1	
7	Garage PIR	JA-120PW	3: Garage	ACT	OK		-0,2 V		RJ	
8	Indoor siren	JA-110A	1: Groud floor		OK		0,0 V		Bus 1	
9	Balcony door	JA-150M	2: First floor		ACT	100 %		100 %		
10	Balcony window	JA-150M	2: First floor		OK	100 %		100 %		
11	Living room	JA-151P	2: First floor	ACT	OK	100 %		80 %		
12	Interface	JA-121T	1: Groud floor		OK		-0,3 V		RJ	
13	Remote control	JA-182J	4: Fully set							

* Die unten beschriebenen und mit * markierten Positionen werden nur angezeigt, wenn die **Erweiterten Einstellungen** aktiviert sind.

Aktivierungsspeicher – zeichnet Aktivierungen eines Geräts auf, die seit der letzten Löschung dieser Spalte aufgetreten sind. Der Speicher aller Geräteaktivierungen kann mit der Taste Speicher löschen (untere Leiste) gelöscht werden. Sie können den Speicher eines ausgewählten Geräts über die rechte Maus löschen. Die Aktivierung eines Sabotagesensors (TMP) hat die höchste Priorität bei der Aufzeichnung von Ereignissen im Speicher.

Status – zeigt den aktuellen Status eines Geräts an. OK = alles in Ordnung, TMP = Sabotage, ACT = Alarmeingang aktiviert, ERR = Fehler, ?? = keine Kommunikation mit dem Gerät, Stromversorgung = Versorgungsfehler (oder einen vollständig leere Batterie), Ladend – die Backup-Batterie im Gerät oder der Zentrale wird geladen. Batterie = nicht geladen oder nicht angeschlossene Batterie in der Zentrale, BOOT – Geräteaktualisierung ist im Verlauf oder Aktualisierungsfehler (Wiederholen Sie die Aktualisierung). Indem Sie die Maus über dem STATUS des entsprechenden Geräts hin- und herbewegen, werden die Details angezeigt.



Batterie* – Wenn das Gerät eine Batterie enthält, wird dessen Status angezeigt. Für die Zentrale (Position 0) wird die Spannung der Backup-Batterie angezeigt. Wenn die Spannungsdaten eines drahtlosen Geräts fehlen, hat das Gerät noch nicht kommuniziert - seine Übertragung wird aktiviert (z. B. über den Sabotage-Sensor oder durch Klicken der Taste Laden in F-Link). Alternativ können Sie auch warten, bis die automatische Übertragung erfolgt. Wenn drahtlose Tastaturen mit Strom über einer externen Stromquelle versorgt werden, wird „Stromversorgung von einer externen Quelle“ angezeigt. Für drahtlose Geräte (außer Geräte der Serie JA-18x) ist der Batteriestatus sichtbar. Farbliche Kodierung des Batteriestatus: 10% rot, 20% gelb, 30% und höher grün.

Spannung/Verlust* – Auf der Position der Zentrale (0) wird die Spannung der Klemmen der Zentrale und der Strom, der von den BUS-Geräten von der Zentrale gezogen wird, angezeigt. Dabei wird der Netzspannungsverlust des BUS-Geräts im Vergleich zur Zentrale angezeigt. Der Verlust darf 2 V nicht überschreiten; sonst muss dieses Problem behoben werden

Signalstärke* - An der Position der Zentrale wird hier die Qualität des GSM-Netzwerk-Signals angezeigt. Für eine zuverlässige Kommunikation sollte der Wert mindestens 50% betragen. Bei drahtlosen Geräten zeigt dies die Qualität des RF-Signals an, der Wert sollte mindestens 50% betragen. Wenn die Anzeige fehlt, hat das Gerät noch nicht kommuniziert - Sie können die Übertragung aktivieren (z.B. über den Sabotagesensor) oder bis zur automatischen Übertragung warten. Über die Interferenz zwischen Funkmodulen und dem GSM-Modul siehe auch Kapitel 6.1 Installation eines Funkmoduls JA-11xR).

Farbliche Anzeige des GSM-Signals: 0-30% rot, 40-50% gelb und über 50% grün.

Farbliche Anzeige des RF-Signals: 10% rot, 20% gelb, 30% und höher grün.

Bei bidirektionalen Geräten (die diese Funktion unterstützen) werden beim Bewegen des Cursors über den Signalpegel des Geräts beide Kommunikationskanäle zwischen der Zentrale und dem Gerät angezeigt.

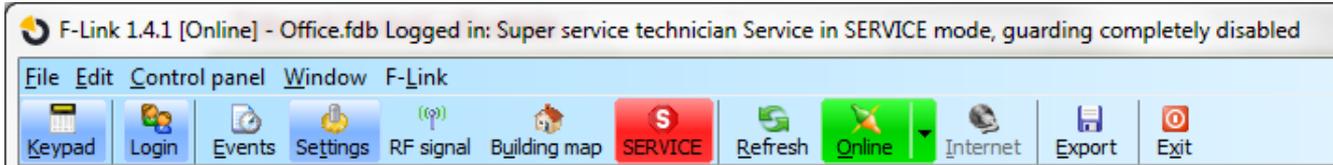


Kanal* – informiert über den BUS, über den das Gerät kommuniziert. Es werden drei Richtungen unterschieden: BUS 1, BUS 2, 3 (nur JA-107K) und der I-BUS-Stecker, der für das Funkmodul JA-11xR (JA-103K) ausgelegt ist. Bei bidirektionalen drahtlosen Geräten (Sirenen, Tastaturen usw.) zeigt die Spalte „Kanal“ das Funkmodul an, über das das Gerät gerade kommuniziert.

11. Andere Optionen von F-Link

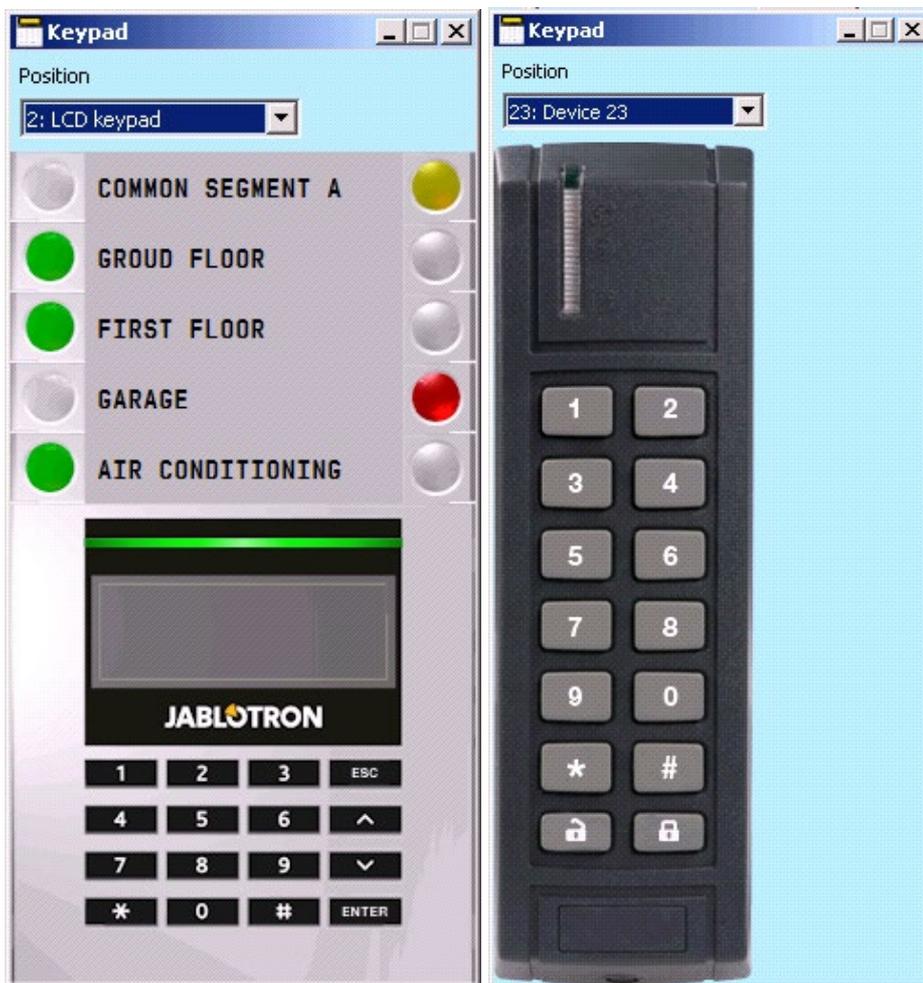
Die F-Link-Version wird immer in der oberen Leiste hinter dem Namen angezeigt.

Die Symbolleiste bietet einen direkten Zugriff auf die virtuellen Tastaturen, Modusänderungen, Systemereignisse, Einstellungen, RF-Signal von Funkmodulen oder den lokalen Zugriff und Fernzugriff auf die Zentrale.

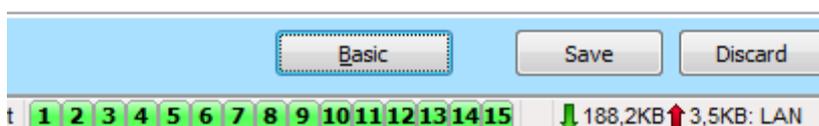


11.1. Bedienteil (virtuell)

Die virtuellen Bedienteile in F-Link (jetzt auch in J-Link) für alle Arten von Steuerungsmodulen ermöglicht Ihnen die Steuerung (von Bereichen, PG-Ausgängen) unter Verwendung von Bereichen (Segmenten) (nicht nummerierte Tasten), wenn Sie in F-Link eingeloggt sind. Dies bedeutet, dass keine Codes eingegeben werden können.



Das System kann lokal und per Fernzugriff gesteuert (scharf und unscharf geschaltet) werden, indem Sie auf die Symbole klicken, die den Systemstatus in der unteren Symbolleiste und in der Registerkarte Bereich darstellen.



11.2. Ereignisse

Der Ereignisverlauf ist in F-Link verfügbar, indem man die Taste Ereignisse klickt und „Ereignisverlauf“ auswählt. Im Speicher der Zentrale (microSD-Karte) können einige Millionen Aufzeichnungen in fortlaufender Nummerierung und mit exaktem Ereignisdatum, sowie der exakten Zeit und Ereignisquelle gespeichert werden.

ID	Time	Source	Section	Event	Channel
200	1/6/2017 3:06:46 PM	Detector 2: Periferie 2	1: Section 1	Sabotáž aktivace	0: Control panel
201	1/6/2017 3:06:46 PM	Externí komunikátor	1: Section 1	Periferie vypnuta	0: Control panel
202	1/6/2017 3:06:46 PM	Detector 0: Ústředna	1: Section 1	Varování, kódy z výroby	0: Control panel
	1/6/2017 3:06:46 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
203	1/6/2017 3:06:51 PM	Detector 2: Periferie 2	1: Section 1	Tišeň aktivace	2: Device 2
204	1/6/2017 3:06:51 PM	Detector 2: Periferie 2	1: Section 1	Tišeň deaktivace	2: Device 2
205	1/6/2017 3:06:51 PM	Detector 2: Periferie 2	1: Section 1	Tišeň!	2: Device 2
206	1/6/2017 3:06:58 PM	User 1: Správce		Autorizace OK	2: Device 2
207	1/6/2017 3:06:59 PM	User 1: Správce	2: Section 2	Zajištěno	2: Device 2
208	1/6/2017 3:06:59 PM	User 1: Správce	3: Section 3	Zajištěno	2: Device 2
209	1/6/2017 3:07:01 PM	User 1: Správce		Autorizace OK	2: Device 2
210	1/6/2017 3:07:01 PM	User 1: Správce	2: Section 2	Odstištěno	2: Device 2
211	1/6/2017 3:07:01 PM	User 1: Správce	3: Section 3	Odstištěno	2: Device 2
	1/6/2017 3:07:47 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
	1/6/2017 3:08:48 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
212	1/6/2017 3:12:24 PM	User 0: Servis 0	1: Section 1	Vstup do servis.režimu	USB
213	1/6/2017 3:12:48 PM	User 0: Servis 0	1: Section 1	Opuštění servis.režimu	USB
214	1/6/2017 3:12:51 PM	Detector 2: Periferie 2	1: Section 1	Zdravotní potříze aktivace	2: Device 2
	1/6/2017 3:12:52 PM	Detector 0: Control panel		Created backup configuration	
215	1/6/2017 3:12:59 PM	Detector 2: Periferie 2	1: Section 1	Zdravotní potříze deaktivace	2: Device 2
216	1/6/2017 3:12:59 PM	Detector 0: Ústředna	1: Section 1	Sabotáž aktivace	0: Control panel
217	1/6/2017 3:12:59 PM	Detector 2: Periferie 2	1: Section 1	Sabotáž aktivace	0: Control panel
218	1/6/2017 3:12:59 PM	Externí komunikátor	1: Section 1	Periferie vypnuta	0: Control panel
219	1/6/2017 3:12:59 PM	Detector 0: Ústředna	1: Section 1	Varování, kódy z výroby	0: Control panel
	1/6/2017 3:12:59 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
220	1/6/2017 3:13:04 PM	Detector 2: Periferie 2	1: Section 1	Zdravotní potříze aktivace	2: Device 2
221	1/6/2017 3:13:04 PM	Detector 2: Periferie 2	1: Section 1	Zdravotní potříze deaktivace	2: Device 2
	1/6/2017 3:14:00 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
	1/6/2017 3:15:01 PM	Detector 0: Control panel		SMS send failed, device busy, EXT_COM	
222	1/6/2017 3:19:43 PM	User 0: Servis 0	1: Section 1	Vstup do servis.režimu	USB
223	1/6/2017 3:44:53 PM	User 0: Servis 0	1: Section 1	Opuštění servis.režimu	USB
	1/6/2017 3:44:58 PM	Detector 0: Control panel		Created backup configuration	

Ereignisse aus der Zentrale (verfügbar über F8) – ca.100 kB der Ereignisse werden (von der microSD-Karte) geladen. Wenn dies nicht ausreichen sollte, können Sie dies wiederholen und Laden/ Nächste 100(500) kB bis zu Alles auswählen. Warnhinweis: Wenn Sie die Option Laden/Alles wählen, kann dieser Vorgang bei einer Zentrale mit längerer Betriebszeit einige Minuten dauern.

Der Verlauf zeichnet keine Ereignisse auf, die während der Einstellung auftreten (nur das Eingeben und Verlassen des Servicemodus (Errichter-Modus)). Geladene Ereignisse können in einer Datei im Dateimenü über Export (Shft+Ctrl+S) in unterschiedlichen Formaten (FDE, PDF, TXT, CSV, XML, HTM or HTML) gespeichert werden.

Hinweis: Die Option zum Laden eines Bereichs von - bis (Datum) ist nur verfügbar, wenn eine Verbindung per Fernzugriff besteht.

Ereignisverlauf online (verfügbar über F7) – in einer temporären Tabelle werden alle Ereignisse aufgezeichnet, die im Ereignisverlauf gespeichert sind und nach der Aktivierung dieser Option auftreten, einschließlich der Ereignisse, die während der Einstellung auftreten.

Gehtestmodus (verfügbar über F6) – in einer temporären Tabelle werden alle Signale aufgezeichnet, die vom BUS aufgezeichnet werden (z.B. Aktivierung und Deaktivierung von Sensoren).

Ereignisse von einer Datei öffnen - Ereignisse, die aus dem Ereignisverlauf in eine Datenbank im Dateiformat FDE gespeichert werden, können geöffnet werden (siehe Ereignisse aus dem Speicher der Zentrale).

Laden – ermöglicht das Laden weiterer Ereignisse des Verlaufs, indem 100 kB, 500 kB (100 kB entspricht ca. 1200 Ereignissen) oder alle geladen werden können.

Hervorheben – über die farbliche Hervorhebung können Ereignisarten unterschieden werden (Alarm mit rot, Steuerung mit grün, Fehler mit orange, Sabotage mit blau, neutral mit hellblau, Automatisierung oder Übertragung mit grau u.s.w.).

Filtereinstellungen – der Filter ermöglicht Ihnen, eine gewünschte Information über die Filterung des Zeitpunkts, der Ereignisart, der Bereiche, der Benutzer, der Geräte oder der PG-Ausgänge in einer detaillierten Form zu erhalten. Die Filter können auch für eine effizientere Suche im Verlauf kombiniert werden.

11.3. Einstellungen

Das Fenster wird dazu verwendet, das Verhalten des Systems, aller Geräte, Bereiche, Benutzer, PG-Ausgänge, Kommunikatoren und Übertragungen an den ARC einzustellen und ist verfügbar, indem Sie die Taste Einstellungen in der oberen Leiste drücken.

System settings Jablotron 100 Logged in: Service technician Service Current History Import

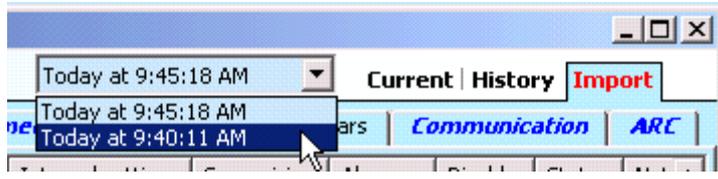
Initial setup | Section **Devices** | Users | PG outputs | Users reports | Parameters | Diagnostics | Calendars | Communication | ARC

Name	Type	Section	Reaction	Internal	PG activation	Interna...	Supervision	Alar...	Disable	Status
0 Control panel	JA-101K	1: Groud floor				Enter				TMP
1 Radio module	JA-110R	1: Groud floor				Enter	<input checked="" type="checkbox"/>			OK
2 LCD keypad	JA-114E	1: Groud floor				Enter	<input checked="" type="checkbox"/>			OK
3 Main door	JA-110M	1: Groud floor	Delayed zone A alarm	<input type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
4 Kitchen window	JA-110M	1: Groud floor	Instant zone alarm	<input type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
5 Garage door	JA-111M	3: Garage	Delayed zone C alarm	<input type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		ACT
6 Hall	JA-110P	1: Groud floor	Next delay zone alarm	<input checked="" type="checkbox"/>	2: Light hall	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
7 Garage PIR	JA-120PW	3: Garage	Delayed zone C alarm	<input type="checkbox"/>	3: Light garage	Enter	<input checked="" type="checkbox"/>	<input type="checkbox"/>		OK
8 Indoor siren	JA-110A	1: Groud floor	Siren mute			Enter	<input checked="" type="checkbox"/>			OK
9 Balcony door	JA-150M	2: First floor	Instant always	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>			ACT
10 Balcony window	JA-150M	2: First floor	Instant always	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>			OK
11 Living room	JA-151P	2: First floor	Instant zone alarm	<input checked="" type="checkbox"/>	No	Enter	<input checked="" type="checkbox"/>			TMP
12 Interface	JA-121T	1: Groud floor				Enter	<input type="checkbox"/>			OK
13 Remote control	JA-182J	4: Fully set	Set		No	Enter	<input type="checkbox"/>			
14 Device 14	Enroll	1: Groud floor	-	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
15 Device 15	Enroll	1: Groud floor	-	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
16 Device 16	Enroll	1: Groud floor	-	<input type="checkbox"/>	No		<input checked="" type="checkbox"/>	<input type="checkbox"/>		

Send enrollment signal | [ican/add new BUS device](#) Basic Save Discard



- Das Fenster zur Einstellung des Systems wird geöffnet und geschlossen über die Taste **Einstellungen** in der oberen Leiste.
- Im Fenster können Sie zwischen den folgenden **Registerkarten** schalten: **Bereichsübersicht**, **Komponentenliste**, **Benutzerübersicht**, **PG-Ausgänge**, **Systemparameter**, ...
- Das Fenster zeigt die **aktuelle Einstellung der Zentrale** an, die von F-Link beim Öffnen geladen wird. Die Taste **Aktualisieren** in der oberen Symbolleiste lädt jederzeit die aktuellen Inhalte der Zentrale.
- Wenn Sie **ältere Einstellungen der Zentrale** anzeigen möchten, verwenden Sie die **Registerkarte Einstellungsverlauf** in der rechten oberen Ecke. Der Verlauf kann nicht geändert, aber er kann in der Zentrale gespeichert werden (wenn man zu früheren Einstellungen zurückkehren muss). Die 10 vorherigen Einstellungen und auch alle Einstellungsänderungen werden im Verlauf überschrieben (nach Datum und Uhrzeit).
- Sie können **Einstellungen** von einer anderen Installation ins System importieren, z.B. wenn eine alte Zentrale durch eine neue ersetzt wird. Wenn die Zentrale durch eine neue ersetzt wird, wird eine komplett neue Datenbank nach dem Verbindungsaufbau auf dem Computer erstellt. Zum Import der Einstellungen von einer anderen Datenbank, wählen Sie in der oberen Leiste des Hauptmenüs **Datei / Import** und wählen Sie die Datei, von der Sie die Einstellungen importieren möchten. Nach dieser Auswahl wird die Schaltfläche **Import** auf der Registerkarte **Systemeinstellungen** angezeigt.



- Für einfachere Anwendungen können Sie einfach die **Grundfunktionen** des Systems einstellen. Wenn Sie alle Funktionen des Systems einstellen müssen, klicken Sie auf „Erweitert“ in der unteren rechten Ecke. Durch wiederholtes Drücken dieser Taste können Sie die erweiterten Einstellungen verbergen (ihre Einstellungen bleiben auch dann erhalten, wenn sie ausgeblendet sind). Die Taste **Erweitert/Einfach** ist auch in den anderen Fenstern verfügbar.



- Die Änderung einer Einstellung wird über einen blauen Text angezeigt.** (der Name der Registerkarte wird auch blau). Die blaue Anzeige verschwindet, sobald Sie diese Änderungen gespeichert haben.
- Sie können die **Einstellungen speichern**, indem Sie die Taste **Speichern** (unten rechts) klicken. Wenn Sie die Einstellungen in der Zentrale zum ersten Mal speichern, fordert F-Link Sie auf, den **Dateinamen** einzugeben. Im Computer wird eine Datei mit dem Suffix *FDB erstellt, wo der Einstellungsverlauf nach

und nach gespeichert wird (jedes Mal, wenn Einstellungen in der Zentrale gespeichert werden). Wenn Sie die Änderungen nicht speichern möchten, wählen Sie die Taste **Beenden** und bei der Bestätigung **Ignorieren**. Parameter können in mehreren Registerkarten geändert werden. Sie können all diese Änderungen dann speichern.

9. Die Taste **BUS-Anmeldesignal senden** (untere Symbolleiste in der Registerkarte Komponentenliste) öffnet einen Dialog zur gemeinsamen Anmeldung (ohne die Möglichkeit, Positionen auszuwählen) von Geräten, die nur mit dem BUS und nicht auf andere Weise mit dem System verbunden sind. Siehe Kapitel 8.4.1 Geräte anmelden und löschen.
10. Die Taste **Funk Anmeldesignal senden** (Registerkarte Komponentenliste und PG-Ausgänge) ermöglicht das Senden des Anmeldecodes der Zentrale an ein drahtloses Gerät, z.B. an ein drahtloses Ausgangsmodul.
11. **Die Einstellung aller Parameter ist nur im Servicemodus (Errichter-Modus) möglich** (das System überwacht nicht). Der Errichtermodus wird mit der Taste Service in der oberen Symbolleiste aktiviert und deaktiviert.
12. **Einige Parameter können während des Betriebs geändert werden.** Hierfür kann die Registerkarte Einstellungen geöffnet werden, ohne, dass Sie sich im Servicemodus (Errichter-Modus) befinden. Jedoch können nur verfügbare Optionen eingestellt werden.
13. **F-Link enthält Sprechblasen-Hilfe** – Die Textbeschreibung wird angezeigt, wenn Sie den Cursor auf einem Eintrag platzieren. Sie können die Sprechblasen-Hilfe im Roll-Down-Menü deaktivieren.

Mögliche Probleme während der Systemeinstellungen:

Problem	Möglicher Grund
Keine oder einige Parameter können nicht geändert werden	Das System befindet sich nicht im Servicemodus und Sie haben eine Funktion ausgewählt, die nur im Service-Code geändert werden kann. Beim Start von F-Link wurde der Service-Code nicht eingegeben und Sie haben keine Berechtigung. Dies ist eine Einstellung, die nicht geändert werden kann (Berechtigung des Errichters, Position der Zentrale, Gerät wird nicht unterstützt usw.). Die ARC-Einstellung wurde vom ARC-Techniker gesperrt. Sie sind offline. Sie haben den Parameter aktiviert, um Norm EN 50131 zu entsprechen.
Der benötigte Parameter kann nicht gefunden werden	Nur die einfachen Optionen werden angezeigt, verwenden Sie die Taste Erweitert. Sie sehen nicht den gesamten Einstellungsbereich auf dem Bildschirm - scrollen Sie runter oder vergrößern Sie das Fenster. Sie sind über einen Code mit einer anderen Zugriffsstufe berechtigt.
Die Positionen sind anders angeordnet	Durch Klicken auf den Titel einer Spalte können Sie auswählen, welche Spalte als Kriterium für die Anordnung der Positionen verwendet wird. Durch wiederholtes Klicken auf den Titel können Sie eine aufsteigende oder absteigende Reihenfolge auswählen.
Einige Registerkarten fehlen	Wenn die Registerkarte PG-Ausgänge nicht verfügbar ist, überprüfen Sie, ob die Anzahl der PG-Ausgänge, die in der Registerkarte Ersteinstellungen festgelegt wurden, nicht Null beträgt. Die Registerkarte AES ist nicht verfügbar, wenn Sie nicht über ausreichende Berechtigungen dafür verfügen (sie kann vom AES-Techniker gesperrt werden). Sie ist möglicherweise auch nach der Anmeldung des Systems in der Applikation My-JABLOTRON nicht verfügbar. Sie haben eine ältere Version von F-Link (J-Link).
Die internen Einstellungen können in der Registerkarte Komponentenliste nicht geändert werden	Überprüfen Sie, ob das Gerät ordnungsgemäß angeschlossen, angemeldet und funktionsfähig ist. Der Servicemodus ist nicht aktiviert. Einige Geräte haben keine internen Einstellungen. Ältere Versionen von F-Link unterstützen möglicherweise keine neuen Gerätetypen. Überprüfen Sie bei einem WLAN-Gerät, ob das Funkmodul angemeldet und funktionsfähig ist.

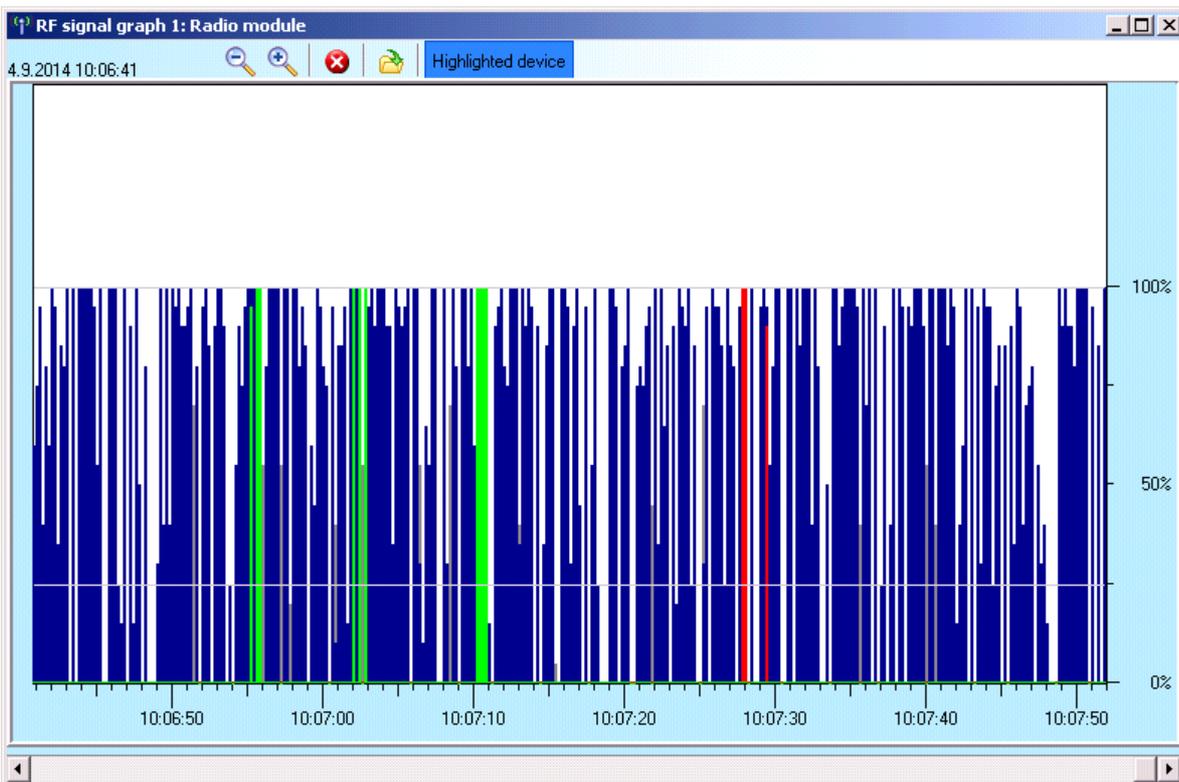
<p>Das Gerät kann nicht in der Registerkarte Komponentenliste angemeldet werden</p>	<p>Für drahtlose Geräte - Sie haben das Funkmodul JA-11xR nicht angemeldet. In einem BUS-Gerät muss die gelbe Signal-LED regelmäßig blinken. Wenn sie nicht blinkt, ist das Element nicht richtig angeschlossen oder hat sich nach der Aktivierung des Netzteils nicht stabilisiert (es kann bis zu 180 Sek. dauern). Der Servicemodus ist nicht aktiviert. Ältere Versionen von F-Link unterstützen möglicherweise keine neuen Gerätetypen.</p>
<p>Ein PG-Ausgang reagiert nicht auf die Aktivierung eines Geräts</p>	<p>Stellen Sie sicher, dass das System nicht im Servicemodus ist. Überprüfen Sie in der Registerkarte Diagnose, ob das Gerät Informationen an die Zentrale sendet. Überprüfen Sie in der Registerkarte PG-Ausgang, ob der Ausgang nicht durch einen Bereichsstatus, ein Gerät oder einen Kalender gesperrt ist. Überprüfen Sie die Spalte Funktionen auf die richtige Einstellung. Prüfen Sie in den Modulen JA-11xN, JA-15xN die DIP-Schalter auf korrekte binäre Einstellung der Adresse und Funktion des Moduls.</p>

11.4. Signalmessung

Fenster zur grafischen Darstellung der Intensität von Störungen im Funkbereich mit der Möglichkeit, ein verwendetes Funkmodul auszuwählen. Unbekannte Signale im Bereich werden in rot angezeigt. Grün kennzeichnet die Kommunikationssignale des Systems (registrierte Geräte) und Blau wird verwendet, um das ausgewählte Gerät in der Liste, **wo das Gerät hervorgehoben wird**, anzuzeigen (siehe Abbildung). Grau kennzeichnet eine Störung. Mit der Option **Unbekannte Geräte deaktivieren** ist es möglich, die unbekanntes Geräte herauszufiltern und nur die im System angemeldeten Geräte anzuzeigen.

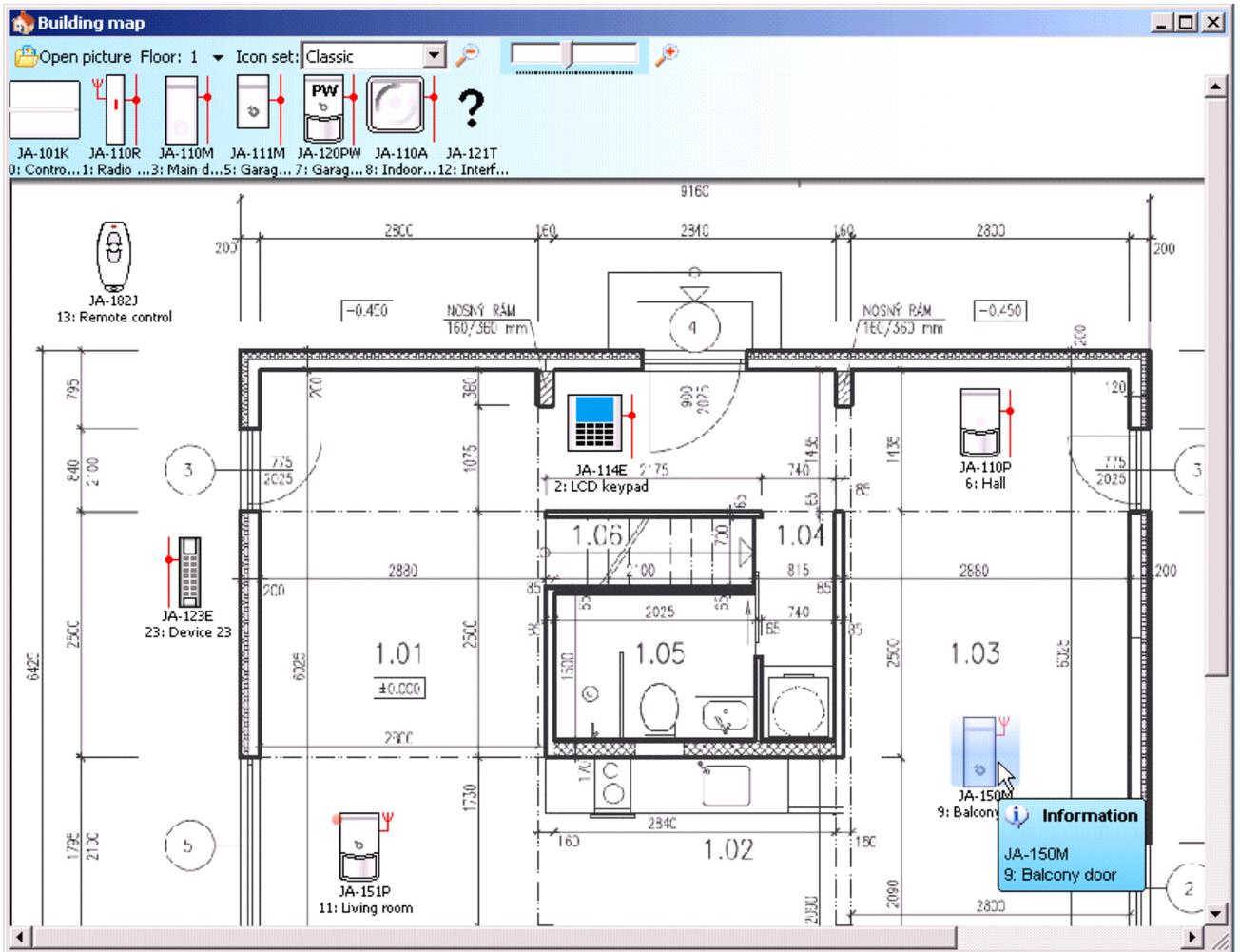
Die überwachte Aufzeichnung der Interferenz (wenn das RF-Signalfenster geöffnet ist) kann aus dem

Hauptmenü in eine Datei mit einer FDR-Erweiterung exportiert werden und die  Schaltfläche wird verwendet, um sie zur Ansicht zu importieren.



11.5. Gebäudeplan

Sie können eine Ansicht im Grundriss (jpg, gif, bmp, tif, png usw.) für jede Etage einzeln in den Gebäudeplan einfügen oder mit einfachen Linien Ihren eigenen Plan zeichnen. In jeder Etage können Sie Symbole der angemeldeten Geräte nur per Drag & Drop aus dem Symbolfeld einfügen. Sie können den Gebäudeplan mit den Symbolen drucken oder sie als BMP-Bild mit dem Menüpunkt Drucken oder Exportieren im Hauptmenü speichern.



11.6. Errichtermodus



Hier kann der Modus der Zentrale zwischen dem Status Unscharf (wenn Einstellungsänderungen in allen Registerkarten mit Ausnahme der Registerkarte Einstellungen vorgenommen werden) und dem Errichtermodus (Änderungen können in der Registerkarte Komponentenliste vorgenommen werden, einschließlich der Anmeldung, Änderung der internen Einstellungen und dem Löschen von Geräten) geschaltet werden.

11.7. Wartung

Hier kann der Modus der Zentrale zwischen dem Status Unscharf und dem Wartungsmodus geschaltet werden.

11.8. Aktualisieren



Aktualisieren der internen Einstellungen von Geräten nach einer Hardwareänderung, z.B. Hinzufügen von Bereichen zu Modulen oder Tastaturen.

11.9. Online

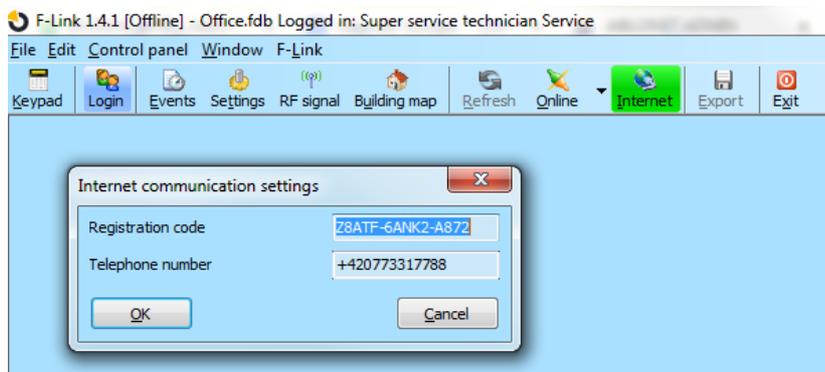


Hier können Sie F-Link über ein USB-Kabel von der Zentrale trennen oder verbinden. Nach der Verbindung findet die Software den Port, den die Zentrale für die Kommunikation verwendet.

11.10. Internet

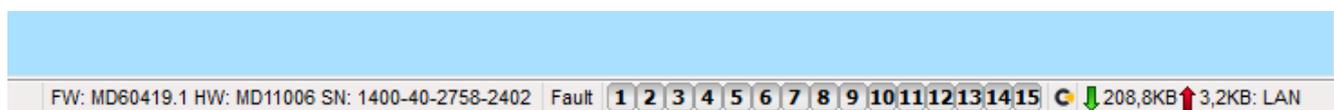


Eine Verbindung oder Trennung von F-Link von der Zentrale per Fernzugriff über das Internet. Eine Voraussetzung für den Verbindungsaufbau ist der korrekt eingegebene Anmeldecode (er wird automatisch von der Datenbank aus eingegeben, die für die Programmierung der Zentrale verwendet wurde), die Telefonnummer der SIM-Karte in der Zentrale (ebenfalls vorher einzugeben) und der mit dem Internet verbundene Computer. Der Fernzugriff kann in der Registerkarte Kommunikation / Kommunikationstyp = Ohne Fernkommunikation deaktiviert werden. Wenn die Sicherheits-SIM verwendet wird, ist diese Option deaktiviert.



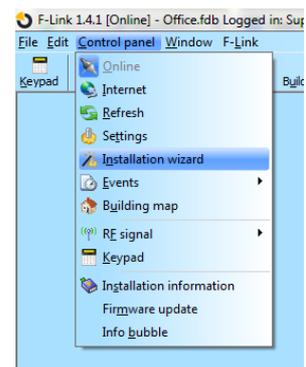
Nach dem Klicken auf die Taste Internet, wird ein Dialogfenster mit den vorab eingegebenen Daten angezeigt. Wenn Sie von einer leeren Datenbank verbunden werden, müssen Sie den Anmeldecode und die Telefonnummer hinzufügen. Bei Verwendung der Sicherheits-SIM und LAN-Verbindung muss die Telefonnummer nicht eingegeben werden. Der Verbindungsaufbau dauert nur ein paar Sekunden, aber das Herunterladen der Konfiguration hängt von der Systemgröße ab, und dies kann 1 bis 2 Minuten dauern.

Hinweis: Informationen zum Aufbau einer GPRS- / LAN-Verbindung und die gesendete und erhaltene Datenmenge wird in der unteren rechten Ecke angezeigt.



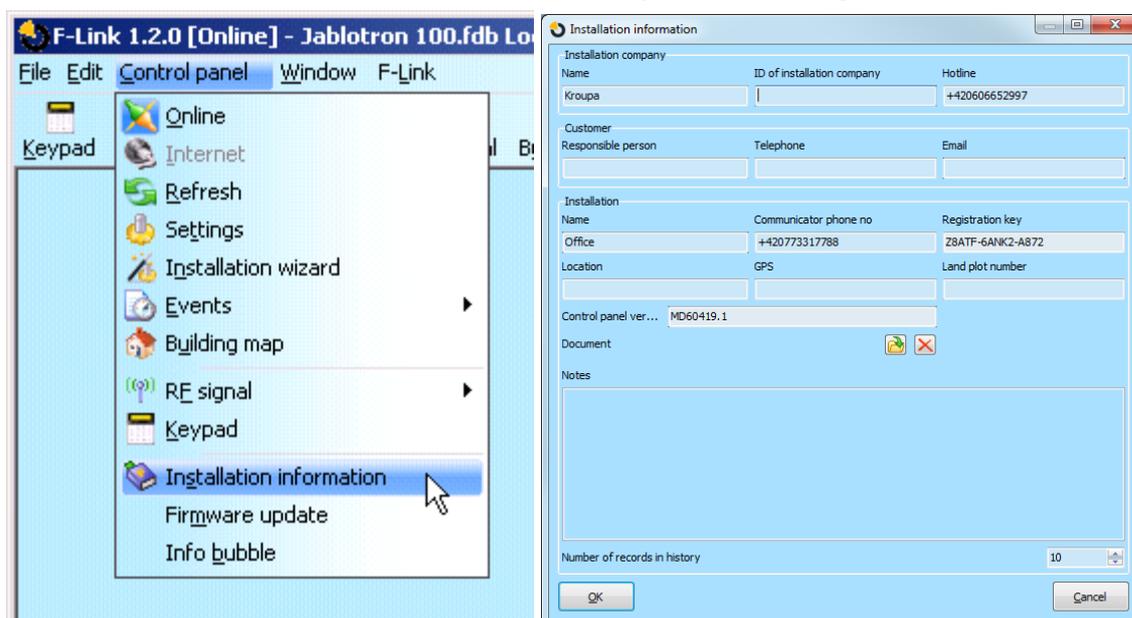
11.11. Installationsassistent

Ein Assistent zum schrittweisen Durchlaufen der Registerkarten „Einstellungen“, was die Programmierung des Systems erleichtert. Der Assistent wird im Hauptmenü der Systemsteuerung aktiviert und mit der Schaltfläche Schließen in der unteren rechten Ecke des Assistentenfensters deaktiviert.



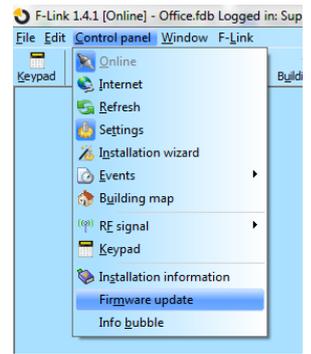
11.12. Installations-Info

Dieses Fenster enthält Einträge für das Installationsunternehmen, um wichtige Kontaktdaten über den Systembesitzer, das gesamte System und möglicherweise ein externes Dokument in Bezug auf das Gebäude (Angebot, Rechnung, Abnahmeprotokoll u.s.w.) zu speichern. Im ext. Feld kann der Errichter Notizen eintragen und hilfreiche Information zur Installation z.B. im Falle einer Systemerweiterung bekommen.



11.13. Aktualisierung der Firmware

Eine Aktualisierung oder Änderung der Firmware mit einem FW-Paket, das der Hersteller auf dem JABLOTRON-Server offiziell anbietet, ermöglicht die Verhaltensänderung aktualisierbarer Geräte (Zentrale, Funkmodule, Tastaturen, Melder u.s.w.). F-Link lädt diese Aktualisierungen automatisch (nach einer Anforderung) vom JABLOTRON-Server herunter, wenn im Menü von F-Link der Menüpunkt Automatische Aktualisierungen aktiviert ist. Wenn diese Funktion nicht aktiviert ist, ermöglicht F-Link das manuelle Auffinden der FWP-Dateien vor der Aktualisierung.



11.14. Etikettendruck

Um Etiketten mit Namen des tatsächlich verwendeten Bereichs (Segments) der Zugriffsmodule zu drucken, können Sie die Funktion Etiketten drucken im Fenster Interne Einstellungen der einzelnen verwendeten Zugriffsmodule verwenden, siehe Kapitel 10.5.1.1 Registerkarte Bereiche (Segmente).

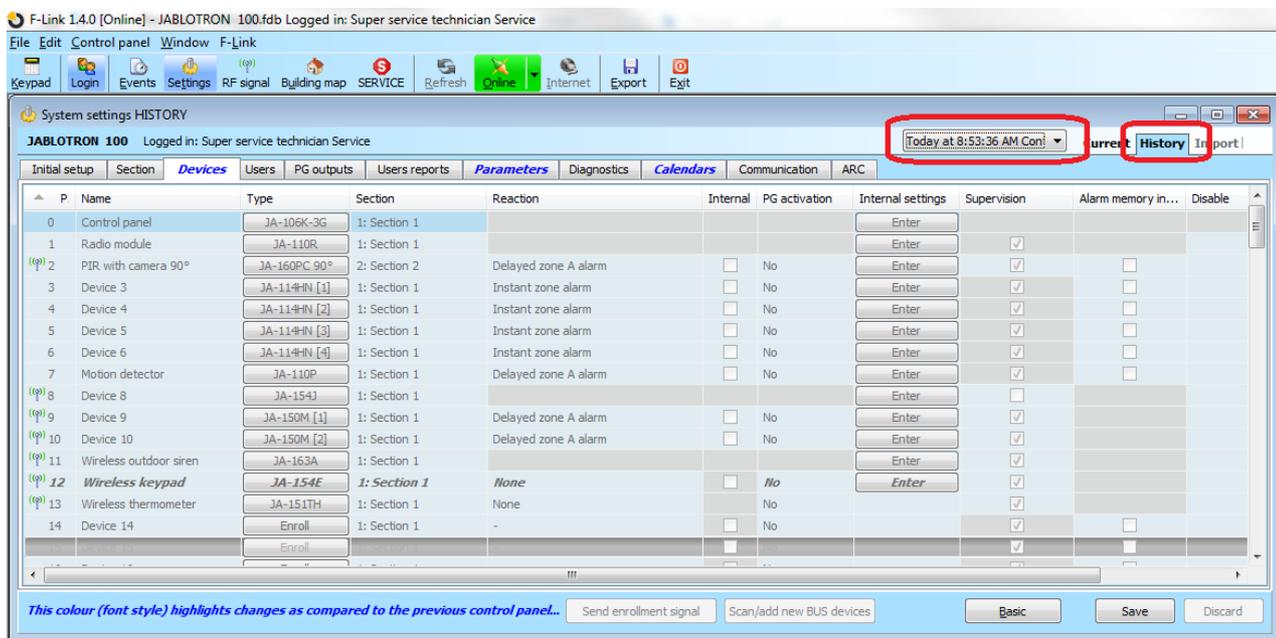
Sie können Ihren eigenen Text zum Drucken eingeben. Bearbeitete Texte werden von der Software nach dem Druck nicht gespeichert, so dass sie für einen möglichen wiederholten Druck nicht verfügbar sind. Der Text auf den Etiketten kann nach links oder zentriert ausgerichtet werden.



11.15. Einstellungsverlauf

Die Zentrale speichert die Einstellungen aller Geräte und ihrer Programmierungsänderungen auf der SD-Karte. Sie zeichnet auch das Ereignis „Konfigurationsbackup erstellt“ im Verlauf mit Informationen zum Dateinamen auf. Dies schließt auch die Konfiguration vor der Änderungsdurchführung mit ein, um sicherzustellen, dass die vorherige Konfiguration wiederhergestellt werden kann, sie zu durchsuchen oder zu prüfen, wann die Änderungen vorgenommen wurden. Um gespeicherte Konfigurationsänderungen zu durchsuchen, öffnen Sie Ereignisse im Ereignisspeicher der Zentrale und suchen Sie die Ereignisse der Konfigurationsänderung nach Datum und Zeit. Um sie mit der aktuellen Systemprogrammierung zu vergleichen, laden Sie sie, und gehen Sie in die Registerkarte „Einstellungsverlauf“, die in der linken oberen Ecke des Fensters „Systemeinstellungen“ verfügbar ist. Die Konfigurationsänderungen sind mit blauer kursiver Schrift hervorgehoben. Die Änderungen können von der gespeicherten Backup-Datei aus akzeptiert werden. Durch Klicken auf die Taste „Speichern“ werden sie in der Zentrale gespeichert. Nachdem Sie die Änderungen durchsucht haben, gelangen Sie zu den aktuellen Einstellungen über die Registerkarte „Aktuell“. Alle Konfigurationsmodifikationen werden in dem Ordner BACKUP in der Datei CFGxxxx.bak mit einer Nummer entsprechend der Reihenfolge der durchgeführten Änderungen gespeichert.

ID	Time	Source	Section	Event	Channel
24	6/3/2016 8:53:39 AM	Detector 3: Device 3	1: Section 1	Tamper activation	0: Control panel
25	6/3/2016 8:53:39 AM	Detector 10: Device 10	1: Section 1	Tamper activation	0: Control panel
26	6/3/2016 8:53:39 AM	Detector 11: Wireless outdoor si...	1: Section 1	Tamper activation	0: Control panel
	6/3/2016 8:54:05 AM	Detector 0: Control panel		Created backup configuration	
29	6/3/2016 8:54:07 AM	Detector 3: Device 3	1: Section 1	Tamper activation	0: Control panel
30	6/3/2016 8:54:08 AM	Detector 10: Device 10	1: Section 1	Tamper activation	0: Control panel
31	6/3/2016 8:54:08 AM	Detector 11: Wireless outdoor si...	1: Section 1	Tamper activation	0: Control panel
	6/3/2016 8:56:19 AM	Detector 0: Control panel		Created backup configuration	
34	6/3/2016 8:56:22 AM	Detector 3: Device 3	1: Section 1	Tamper activation	0: Control panel
35	6/3/2016 8:56:22 AM	Detector 10: Device 10	1: Section 1	Tamper activation	0: Control panel
36	6/3/2016 8:56:22 AM	Detector 11: Wireless outdoor si...	1: Section 1	Tamper activation	0: Control panel



F-Link speichert (3 bis 10 in dem Fenster Installationsinformation) den Verlauf der Einstellungen in der eigenen Datenbank rückwärts. Dieser Verlauf der Einstellungen wird von der Software für Aktualisierungen der Firmware der Zentrale verwendet, da eine Änderung immer den Verlust der vorherigen Einstellungen verursacht und dieser Verlauf zur Wiederherstellung verwendet werden kann. Die gleiche Option kann im Falle einer Zurücksetzung der Zentrale auf die Standardeinstellungen, beim Austausch der SD-Karte, bei Sprachänderungen bei der Löschung von Texten, die auf diese Weise wiederhergestellt werden können, oder aber bei einer unbeabsichtigten Änderung einer Einstellung verwendet werden.

12. Zurücksetzen der Zentrale

Die Standardeinstellungen der Zentrale können nur dann wiederhergestellt werden, wenn in F-Link in der Registerkarte Parameter die Option „Zurücksetzung aktiviert“ markiert ist. Wenn die Zurücksetzung nicht aktiviert ist und Sie den Errichter-Code nicht kennen, können Sie die Zentrale nicht zurücksetzen. In diesem Fall muss die Zentrale an den Händler zurückgeschickt werden.

Vorgehensweise:

1. Schalten Sie die Zentrale in den Errichter-Modus (nicht obligatorisch).
2. Öffnen Sie die Abdeckung der Zentrale: Für die Zurücksetzung müssen die Sabotagekontakte aktiv sein.
3. Trennen Sie das USB-Kabel von der Zentrale.
4. Schalten Sie den Strom aus (am einfachsten durch Lösen der Sicherung) und trennen Sie die Batterie.
5. Verbinden Sie die mit RESET gekennzeichneten Pins auf der Platine der Zentrale (mit den mitgelieferten Jumpern).
6. Schließen Sie zuerst die Batterie und dann den Strom der Zentrale an und warten Sie. Die grüne, gelbe und rote Signallampe am Jumper leuchtet auf (wenn nur die rote Signallampe an bleibt, ist die Einstellung Parameter / Zurücksetzung nicht aktiviert).
7. Warten Sie ca. 15 Sek. und trennen Sie den Jumper.
8. Alle LEDs blinken als Bestätigung, dass die Zentrale vollständig zurückgesetzt wurde. Dann wird die Wiederaufnahme der Spannungsversorgung der Zentrale und der BUS-Geräte durchgeführt.
9. Auf diese Weise wurde die Zentrale inkl. Sprachauswahl auf die Standardeinstellungen zurückgesetzt. Das Zurücksetzen der Zentrale führt jedoch nicht zum Löschen des Verlaufs der auf der SD-Karte gespeicherten Ereignisse. Wenn die Zurücksetzung nicht korrekt ausgeführt wurde, behält die Zentrale die ursprünglichen Einstellungen ohne Änderungen.

13. Aktualisierung der Firmware

Die Zentrale und andere Geräte des Systems JABLOTRON 100+ ermöglichen die Änderung der Firmware. Die Firmware wird normalerweise geändert, um nützliche Parameter zu erweitern oder um ein neues Produkt zu unterstützen.

13.1. Allgemeine Regeln zur Aktualisierung der Firmware (FW)

1. Eine Änderung kann nur mit einem Computer, der **F-Link** installiert hat, durchgeführt werden. Dies ist entweder lokal über ein USB-Kabel möglich oder per Fernzugriff, wo die Modifikationsmöglichkeiten auf BUS-Geräte beschränkt ist.
2. Die Firmware (FW) kann durch einen Benutzer mit einer Service-Berechtigung geändert werden.
3. Überprüfen Sie, ob Sie die aktuelle Version von F-Link verwenden. Die neueste Version ist auf der Website www.myjablotron.com, **MyCOMPANY** / **MySTORAGE** / **Software** verfügbar, auf dem nur berechtigten Techniker nach dem Login zugreifen können. Oder mit bereits installierter Software F-Link und Internetzugang bietet F-Link nach dem Start automatisch Aktualisierungen an und lädt gleichzeitig das aktuelle FW-Paket selbst herunter.
4. Verbinden Sie den Computer mit einem USB-Kabel mit der Zentrale, das Kabel ist im Lieferumfang der Zentrale enthalten.
5. Starten Sie **F-Link** mit der verbundenen Zentrale.
6. Schalten Sie die Zentrale in den Errichter-Modus.
7. Starten Sie die **Zentrale / Aktualisierung der Firmware**
Wenn die **Automatische Aktualisierung** im **F-Link**-Menü erlaubt ist (Standardeinstellung), wird eine Liste der aktualisierbaren Geräte angezeigt. Diese Datei ist Teil von F-Link im **F-Link x.x.x / Firmware** Verzeichnis und der aktuelle Status ist nur zum Zeitpunkt des F-Link-Downloads garantiert.



Ort des Parameters Automatische Aktualisierung:

13.2. FW-Aktualisierungen für die Zentrale und Geräte, die mit dem BUS verbunden sind

1. In dem Auswahlfenster Firmware-Aktualisierung werden aktualisierbare BUS und bidirektionale drahtlose Geräte der Zentrale angezeigt. F-Link wählt automatisch die Geräte, für die eine Aktualisierung benötigt wird, aus (sie haben eine ältere FW als die im FW-Paket).
2. F-Link warnt sie, wenn drahtlose Geräte aktualisiert werden können. Siehe 13.3 FW-Aktualisierungen für drahtlose Geräte in Bezug auf Informationen zu den Aktualisierungsvorgängen bei drahtlosen Geräten.
3. Weitere detaillierte Informationen zu den bestehenden oder neuen Versionen der einzelnen Geräte finden Sie in der Sprechblasen-Hilfe, wenn Sie den Cursor über die verfügbaren Geräte bewegen.
4. In den Auswahlfeldern überprüfen Sie die Geräte, für die Sie FW ändern möchten. Wenn es in den angebotenen Optionen die Zentrale mit dem Angebot einer neueren FW-Version gibt, empfehlen wir Ihnen, das Häkchen zu setzen. Einige Elemente können obligatorisch sein und somit nicht für die Beendigung einer Aktualisierung zur Verfügung stehen (grau).
5. Wenn die Aktualisierung der Zentrale geprüft wird, wird die Möglichkeit, das geänderte Benutzer-Sprachmenü zu speichern, angezeigt (falls deaktiviert, wird die Standardeinstellung des Sprachmenüs wiederhergestellt).
6. Klicken Sie auf OK, um die FW-Aktualisierung der ausgewählten Geräte zu starten. Alle Änderungen werden innerhalb weniger Minuten ausgeführt (abhängig von der Anzahl der Geräte). Dann startet die Zentrale das System neu.
7. Nach der FW-Änderung kann ein Teil des Anmeldecodes geändert werden. Diese Änderung hat keinerlei Einfluss auf den Fernzugriff (über F-Link) oder die mögliche Kommunikation der Zentrale mit dem MyJABLOTRON-Service.

8. Wenn F-Link während der Aktualisierung der Zentrale eine beschädigte Datei auf der SD-Karte findet, wird sie formatiert. Nach der Fertigstellung der Aktualisierung können die ursprünglichen Einstellungen wieder importiert werden.
9. Obwohl die FW-Aktualisierung das Systemverhalten nicht verändert, führen Sie eine Prüfung gemäß der Beschreibung im Kapitel Prüfung nach einer FW-Aktualisierung durch. 13.4 Prüfung nach einem FW-Aktualisierung.

13.3. FW-Aktualisierungen für drahtlose Geräte

1. Das FW-Aktualisierung der drahtlosen Geräte erfolgt auf die gleiche Weise wie bei den BUS-Geräten. Sollte diese Art der Aktualisierung fehlschlagen, führen Sie die folgenden Schritte aus:
2. Öffnen Sie das aktualisierbare drahtlose Gerät (z. B. JA-152E, JA-153E, JA-154E, JA-160PC, AC-160DIN usw.), indem Sie auf den Riegel drücken.
3. Wenn es Batterien enthält, entfernen Sie diese und trennen Sie jede externe Stromversorgung.
4. Starten Sie F-Link, öffnen Sie die Datenbank und verbinden Sie das USB-Kabel mit dem Computer (miniUSB oder microUSB, je nach verwendetem Gerät).
Warnhinweis: *USB-Kabel sind bei einzelnen Geräten nicht im Lieferumfang enthalten. Wir empfehlen Ihnen, eine direkte USB-Verbindung mit dem Computer zu verwenden, eine Verbindung über ein USB-HUB kann die Zuverlässigkeit verringern.*
5. Die Aktualisierungen der FW in drahtlosen Geräten muss einzeln durchgeführt werden. Eine gleichzeitige Aktualisierung mit vielen USB-Kabeln ist nicht möglich.
6. Öffnen Sie in dem zu aktualisierenden drahtlosen Gerät den Modus zum Laden der neuen FW. Verfahren Sie dabei entsprechend der Anleitungen der jeweiligen Handbücher.
7. Dann fahren Sie wie bei einer Systemaktualisierung mit **F-Link** fort: **Zentrale** → **Aktualisierung der Firmware**.
8. In der Tabelle zur Geräteauswahl, wählen Sie einen USB-Eintrag (typischerweise an der ersten Position).
9. Weitere detaillierte Informationen zu den bestehenden oder neuen Versionen der einzelnen Geräte finden Sie in der Sprechblasen-Hilfe, wenn Sie den Cursor über die verfügbaren Geräte bewegen.
10. Durch OK werden alle Geräte aktualisiert.
11. Nach Fertigstellung der Aktualisierung trennen Sie das USB-Kabel, setzen Sie die Batterien wieder ein oder schließen Sie die Stromversorgung an und bauen Sie das Modul wieder zusammen.
12. Führen Sie eine Prüfung entsprechend Kapitel 13.4 Prüfung nach einer FW-Aktualisierung durch.
13. Aktualisieren Sie nun das nächste Gerät.

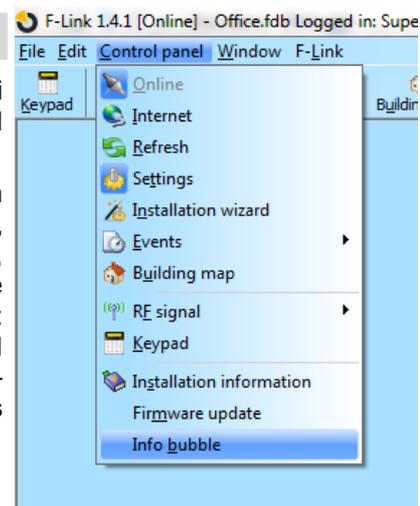
13.4. Prüfung nach einer FW-Aktualisierung

1. Prüfen Sie die Einstellungen aller geänderten Geräte und der Zentrale in **F-Link, Komponentenliste / Interne Einstellungen**. Abhängig von den Änderungen, die während der Aktualisierung vorgenommen wurden, kann die vorherige Einstellung beibehalten werden. Wenn nicht, führen Sie eine Zurücksetzung auf die standardisierten Produktionswerte durch. Wenn eine Zurücksetzung auf die Standardwerte durchgeführt wurde, können Sie die vorherigen Einstellungen über die Import-Taste in den internen Einstellungen des Geräts auswählen.
2. Wenn neue Elemente innerhalb der Aktualisierung hinzugefügt wurden, prüfen Sie sie und adaptieren Sie sie so, wie es für die Installation erforderlich ist.
3. Prüfen Sie die Einstellungen und testen Sie die Funktionen der aktualisierten Geräte.

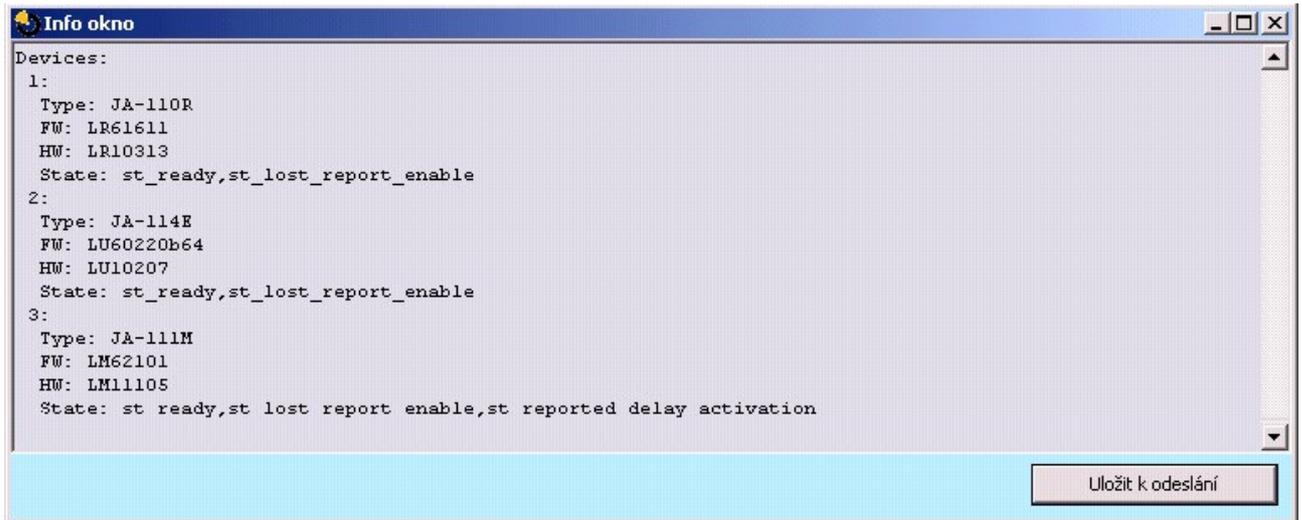
13.5. Tips anzeigen

Es wird über das Hauptmenü **Zentrale / Tips anzeigen** geöffnet. Bei Erstellung des Info-Fensters fragt die Zentrale alle angeschlossenen und drahtlosen Geräte nach ihren aktuellen Informationen.

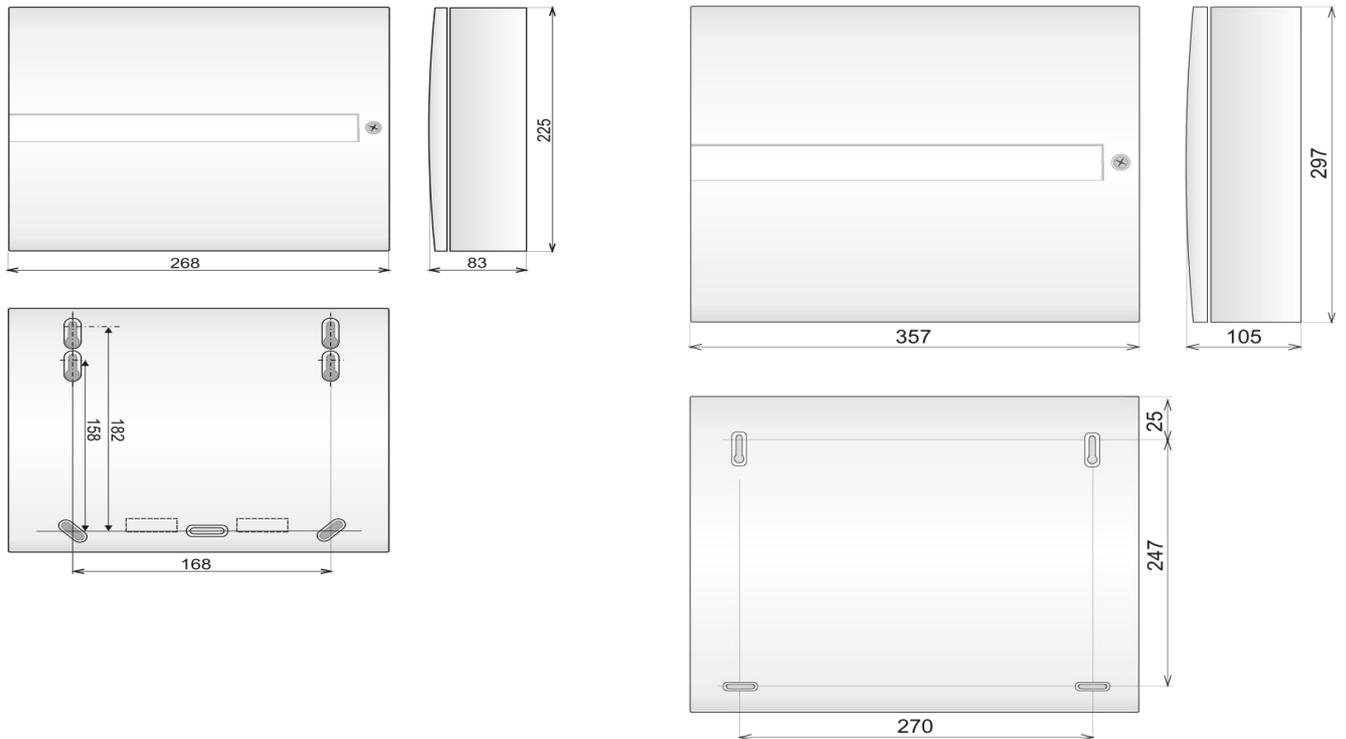
Die **Info-Blase** gibt einen allgemeinen Überblick über die technischen Daten des gesamten Systems, einschließlich der Zentrale (Seriennummer, Anmeldecode, FW- und HW-Version, Spannung und Strom des BUS, Einstellungen von: Geräten, Bereichen, PG-Ausgängen), verwendete Kommunikatoren (GSM: Telefonnummer, Signal BTS Nummer oder PSTN: Status der Telefonleitung, LAN: Status, MAC, IP, sowie alle BUS- und drahtlose Geräte (uni- und bidirektional): Gerätetyp, Identifikation von FW- / HW-Versionen individueller Geräte und ihr Status. In jedem Systemstatus verfügbar (scharf/ unscharf / Service).



Diese Daten sind z.B. für die Kommunikation mit dem technischen Berater, für den die Taste „Exportieren“ in der rechten unteren Ecke konzipiert ist. Die Datei ist eine komprimierte ZIP-Datei und enthält Daten über die Installation, einen Teil des Ereignisverlaufs (100 kB), aber sie enthält keine sensiblen Daten, wie Telefonnummern von Benutzern oder deren Zugangsodes, oder andere vertrauliche Daten.



13.6. Abmessungen der Zentrale



14. Die webbasierte Applikation MyJABLOTRON

Die webbasierte Applikation MyJABLOTRON ist ein einzigartiger Service, mit dem Benutzer und Installationstechniker online auf von Jablotron hergestellte Geräte zugreifen können. Jablotron-Kunden können damit ihre Systeme verwalten. Endbenutzer von Alarmsystemen können damit ihr Gerät steuern und überwachen. Sie bietet Installationstechnikern ein leistungsstarkes Tool, mit dem sie alle installierten Systeme überwachen und verwalten und bequem neue Angebote für neue Installationen erstellen können.

Alles, was Ihr Alarmsystem oder Ihre Installation betrifft, ist in einer einzigen Applikation verfügbar, die von überall aus zugänglich ist.

Die MyJABLOTRON-Applikation ermöglicht Benutzern

- den **aktuellen Status eines Systems** (im Assistenten sind Ihre angemeldeten Geräte zusammen mit dem letzten registrierten Ereignis und der unscharfen und scharfen der Bereiche sichtbar) zu sehen.
- einen **Alarm scharf / unscharf** zu schalten.
- programmierbare **Ausgänge zu steuern** (meistens zur Gerätesteuerung).
- den Ereignisverlauf zu einzusehen und ihn zu einer Datei zu exportieren
- **Fotos und Videos** von Verifikationsgeräten **zu sehen und, wenn erlaubt, Fotos und Videos aufzunehmen**.
- **den Temperaturverlauf** im Gebäude oder im Freien (inkl. Meldung der Überschreitung der unteren oder oberen Grenze der eingestellten Temperaturen zu einer definierten Tageszeit) zu **überwachen**.
- den **Stromverbrauch** (inkl. Einstellung einer Benachrichtigung bei Überschreitung des stündlichen / täglichen / monatlichen Verbrauchs) zu **überwachen**.
- **Nachrichten** an ausgewählte Kontakte per SMS, E-Mail, mit den Standard-PUSH-Benachrichtigungen für Mobiltelefone zu **senden**.
- weitere nützliche Funktionen.

14.1. Verwaltung der Installationen und Angebote für einen Errichter

Übersicht über alle installierten Geräte, die im Modul MyJABLOTRON - Installation Management registriert sind

Dies ist ein einzigartiges Werkzeug für Errichter, die ihre gesamten installierten Systeme an einem Ort verwalten können, inkl. einer vollständigen Übersicht über ihren aktuellen technischen Status, Ansicht des Verlaufs und der Betriebsdiagnose ... Sie finden das Modul **Installationsverwaltung** in Ihrem Konto in der Applikation MyJABLOTRON im Bereich **MyCOMPANY** (falls in Ihrer Region unterstützt).

My **COMPANY** ▾ 👤 [masaryk@jablotron.cz](#) ▾

< [My COMPANY](#) Installations Management

Search installation... Only with fault Only in service All device types ▾

Drahomil Masaryk
Pod Skalkou 4567/33
Jablonec nad Nisou
466 04

Configuration
JA-106K
+420775128581
DPAT7-XDN4T-AXG2

Sie können Ihre Installationen nach der Alarmart oder basierend auf ihrem aktuellen Status filtern. So können Sie die Benachrichtigung für ein technisches Problem vorab festlegen und mit einem Service-Eingriff schnell darauf reagieren. Auf diese Weise können Sie Ihren Kunden einen überdurchschnittlichen Service bieten, da Sie sich mit ihm in Verbindung setzen, bevor der Kunde mit der Lösung des Systemproblems beginnt.

< [Installation](#)
Drahomil Masaryk
 [Settings](#)



Status OK (20.08.2014 07:53:16)
Last check: **10:35:18**

JA-106K

DPAT7-XDN4T-AXG2

+420775128581

Contact information

Drahomil Masaryk

Pod Skalkou 4567/33
Jablonec nad Nisou
466 04

 [Configuration](#)

State
Events
Logs

Device status

	State	Lasts since
GSM:	Vodafone CZ 45 %	4.9.2014 (10:04:56)
FW:	MD60410b19	12.6.2014 (22:37:28)
CONNECTED:	Connected to LAN	4.9.2014 (01:29:16)
CLOUD COMMUNICATION:	Main channel	24.4.2014 (02:12:45)
SUPPLY STATUS:		17.8.2014 (07:25:46)
CONTROL UNIT BATTERY:		17.8.2014 (07:25:46)
DEVICE BAT:		20.8.2014 (07:53:16)
RF INTERFERENCE:		20.8.2014 (07:53:16)
SYSTEM ERROR:		20.8.2014 (07:53:16)

In der Detailansicht jeder Zentrale bekommt der Errichter einen allgemeinen Überblick in Form der Statusanzeige einzelner Fehlergruppen (Zustände der Stromversorgung, Kommunikation, Status der Batterien in Geräten, Störungen oder andere Fehler, SIM-Kartentyp im Gerät) und aktuelle GSM-Signalqualität, aktuelle FW-Version) mit dem Datum seit dem der Status aktiv ist. Außerdem erhält der Techniker einen Überblick über den gesamten Ereignisverlauf - dies muss jedoch vom Gebäudeeigentümer in seinen Einstellungen genehmigt werden.

In **Installationsverwaltung** finden Sie außerdem ein vollständiges Protokoll der technischen Ereignisse des Alarmsystems mit einer grafischen Darstellung der GSM-Verbindungsqualität, des Verlaufs der Firmwareänderungen oder der Kommunikation.

14.2. WEB-Link Applikation (Konfiguration)

Eine sehr nützliche Applikation für einen Errichter im MyJABLOTRON Web-Service ist WEB-Link. Es ist eine Applikation, die F-Link sehr ähnlich ist, mit dem Unterschied, dass diese Applikation auf dem Server läuft und von überall aus über jeden Webbrowser erreichbar ist. Starten Sie die Applikation, indem Sie auf das Symbol Konfiguration in der Installationsverwaltung in MyCOMPANY klicken. Der Errichter kann von jedem Computer aus fast alle Einstellungen in dem System ändern, die seinem Profil zugewiesen sind, unabhängig davon, wo er sich befindet und welche Plattform er verwendet. Vom Errichter vorgenommene Änderungen werden auf dem Server gespeichert und können sofort oder zu einem einstellbaren Zeitpunkt oder nachdem der Benutzer das System unscharf geschaltet hat, im System gespeichert werden. Der Errichter kann über Änderungen per SMS oder E-Mail informiert werden.

15. Übernahme des Systems durch den Benutzer

Wenn die Installation des Sicherheitssystems beendet ist, ist die Erstellung einer Dokumentation (Bericht über die Übergabe des Systems, Betriebsbuch, LOG des Sicherheitssystems u.s.w.) empfehlenswert, in der die gesamte Information über die Anzahl und Standorte der Geräte, wie Melder, Sirenen, Tastaturen, ihre Funktionstasten und wie diese konfiguriert wurden, enthalten ist. Systembenutzer sollten geschult werden, wie das System entsprechend der folgenden Punkte zu benutzen ist:

1. Steuerung der Systemtastatur. Scharf- und Unscharfschaltung der Bereiche (über die Funktionstasten oder von dem Tastaturmenü aus).
2. Vergewissern Sie sich, dass die Ausgangs-/Eingangszeit korrekt ist und auch für Garagentüren und andere Eingangswege gilt.
3. Erklären Sie die Bedeutung der Berechtigung und ihre Optionen wie Codes, RFID-Tags usw....
4. Teilweise Scharfschaltung zu Hause. Unterschied zwischen teilweiser und vollständiger Scharfschaltung.
5. Steuerung der Hausautomatisierung über die Funktionstasten und andere Funktionen (Überfall, Feuer, Gesundheitsprobleme).
6. Auslösung eines Alarms, wenn das System scharf geschaltet ist, einschließlich Sirenen, Test des Alarmanrufs.
7. Erklären des Unterschieds zwischen Alarmbeendigung über die Berechtigung und Unscharfschaltung eines Bereichs.
8. Bereichssteuerung (per Fernsteuerung über das Sprachmenü der Handytastatur).
9. Bereichssteuerung und Hausautomatisierung (PG-Ausgänge) via SMS.
10. Steuerung über die webbasierte oder mobile Applikation vom Tablet, Smartphone oder einer Website aus.
11. Bearbeitung von Benutzercodes durch den Benutzer über die Tastatur und J-Link.

Vergessen Sie nicht, Ihrem Kunden eine jährliche Systeminspektion anzubieten. Es ist sehr nützlich, die Systemfunktionen regelmäßig zu überprüfen, nicht nur die Zentrale, sondern auch alle installierten Geräte. Der Techniker erstellt einen Bericht über die jährliche Prüfungsleistung und dies kann auch für die Versicherung nützlich sein. Die fällige jährliche Inspektion kann dem Kunden automatisch über eine LCD-Tastatur angezeigt werden.

16. Technische Spezifikationen

Parameter	JA-103K		JA-107K	
Stromzufuhr der Zentrale	~ 110–230 V / 50–60 Hz, max. 0.28 A mit Sicherung F1.6 A/250 V Sicherheitsklasse II		~ 110–230 V / 50–60 Hz, max. 0.85 A mit Sicherung F1.6 A/250 V Sicherheitsklasse II	
Backup-Batterie	12 V; 2.6 Ah (Blei-Gel)		12 V; 7 to 18 Ah (Blei-Gel)	
Maximale Ladezeit der Batterie	72 Std.		72 Std.	
BUS-Spannung (rot - schwarz)	12.0 bis 13.8 V		12.0 bis 13.8 V	
Maximaler Dauerstromverbrauch von der Zentrale	1000 mA		2000 mA permanent 3000 mA für 60 Minuten (max. 2000 mA für ein BUS)	
Max. Dauerstromverbrauch für einen Backup von 12 Stunden	JA-103K – 2.6 Ah Backup-Batterie		JA-107K – 18 Ah Backup-Batterie	
	Ohne GSM Wähl- und Übertragungsgerät	LAN – AUS 115 mA LAN – EIN 88 mA	Ohne GSM Wähl- und Übertragungsgerät	LAN – AUS 1135 mA LAN – EIN 1107 mA
	Mit GSM Wähl- und Übertragungsgerät	LAN – AUS 80 mA LAN – EIN 53 mA	Mit GSM Wähl- und Übertragungsgerät	LAN – AUS 1100 mA LAN – EIN 1072 mA
Maximale Geräteanzahl	50		230	

LAN-Kommunikator	Ethernet Schnittstelle, 10/100BASE-T	Ethernet Schnittstelle, 10/100BASE-T
Abmessungen (mm)	268 x 225 x 83	357 x 297 x 105
Gewicht mit / ohne AKU	1844 g / 970 g	7027 g / 1809 g
Reaktion auf eine ungültige Codeeingabe	Alarm nach 10 falschen Codeeingaben	
Ereignisspeicher	Ca. 7 Millionen letzte Ereignisse, einschließlich Datum und Zeit	
Netzteil	Typ A (gemäß EN 50131-6)	
GSM-Kommunikator	850 / 900 / 1800 / 1900 MHz	
Klassifizierung	Sicherheitsklasse 2 / Umgebungs Klasse II (gemäß EN 50131-1)	
Betriebsumgebung	Umgebungs Klasse II (allgemeine Innenbereiche) gemäß EN 50131-1	
Betriebstemperaturbereich	-10 °C bis +40 °C	
Durchschnittliche Betriebsfeuchtigkeit	75 % RH, nicht kondensierend	
Entspricht	EN 50131-1 ed. 2+A1+A2, EN 50131-3, EN 50131-5-3+A1, EN 50131-6 ed. 2+A1, EN 50131-10, EN 50136-1, EN 50136-2, EN 50581	
Funkfrequenz (mit dem Modul JA-11xR)	868.1 MHz	
Funkemissionen	ETSI EN 300 220-1,-2 (Modul R), ETSI EN 301 419-1, ETSI EN 301 511 (GSM)	
EMC	EN 50130-4 ed. 2+A1, EN 55032 ed. 2, ETSI EN 301 489-7	
Sicherheitskonformität	EN 62368-1+A11	
Rufnummererkennung (CLIP)	ETSI EN 300 089	
Betriebsbedingungen	ERC REC 70-03	
Zertifizierungsstelle	Trezor Test s.r.o. (no. 3025)	



JABLOTRON ALARMS a.s. erklärt hiermit, dass die Zentralen JA-103K und JA-107K bei ordnungsgemäßer Verwendung den relevanten Harmonisierungsvorschriften 2014/53/EU, 2014/35/EU, 2014/30/EU, 2011/65/EU der Europäischen Union entsprechen. Das Original der Konformitätsbewertung ist unter www.jablotron.com – im Abschnitt *Downloads* einsehbar.



Hinweis: Obwohl dieses Produkt keine schädlichen Werkstoffe beinhaltet, empfehlen wir, das Produkt nach dem Ende seines Gebrauchs an den Händler oder Hersteller zurückzusenden. Weitere detaillierte Information finden Sie unter www.jablotron.com – im Abschnitt *Downloads*.

