JABLOTRON
CREATING ALARMS

BENUTZER-HANDBUCH

Sicherung von kleinen Installationen auf Basis der JA-100K

1. EINLEITUNG

Vielen Dank, dass Sie sich für das Sicherheitssystem JABLOTRON 100 entschieden haben. Diese Bedienungsanleitung ist für die Zentrale JA-100K und den Bedienteilen JA-110E oder 150E vorgesehen. Das System stellt eine einzigartige Sicherheitslösung für die gewerbliche, private und persönliche Sicherheit von Innenräumen dar. Dabei können sowohl BUS- als auch kabellose Komponenten verwendet werden. Die JABLOTRON 100 ist sehr einfach zu bedienen. Die einfache Steuerung besteht aus zwei Schritten, der Autorisierung mithilfe eines Codes oder RFID-Tags und dem Betätigen der individuellen Funktionstaste auf dem Bedienteil. Es ist auch eine umgekehrte Vorgehensweise bei aktiviertem Standardsystemprofil möglich. Drücken Sie dabei zuerst die Funktionstaste und autorisieren Sie sich dann. Ebenso ist es möglich, das Sicherheitssystem nur über die Autorisierungsfunktion zu steuern. Das System JABLOTRON 100 bietet eine große Auswahl an Meldern mit einem zeitlosen Design und kann dank des vollständigen Fernsteuerungszugriffs von überall bedient werden. Das Programm J-Link, das Webinterface MyJABLOTRON und die MyJABLOTRON--Anwendung für Smartphones ermöglichen Ihnen die Fernsteuerung, -programmierung und -überwachung des Systems.

Das Sicherheitssystem JABLOTRON 100 kann von bis zu 32 Benutzern verwendet und in vier separate Bereiche eingeteilt werden. Dabei lassen sich bis zu 32 Komponenten anmelden. Außerdem bietet das System 4 multifunktionale programmierbare Ausgänge (z.B. Hausautomatisierung).

WARNHINWEIS:
Das Sicherheitssystem JABLOTRON 100 sollte immer von einem autorisierten Jablotron Errichter/Servicetechniker installiert und programmiert werden. Ein Benutzer kann lediglich die Benutzerfunktionen und die Zugriffsrechte zum Sicherheitssystem verwalten.

Das Sicherheitssystem kann so programmiert werden, dass verschiedene Steuerungsarten verwendet werden können, die bei der Installation als Systemprofil wählbar sind, wie z.B.:

- Standard Jablotron
- EN 50131, Grad 2
- INCERT, Grad 2
- Und andere

Einige Benutzerfunktionen sind je nach ausgewähltem Profil begrenzt. Weitere Informationen und eine ausführ-liche Funktionsbeschreibung erhalten Sie von Ihrem Errichter.

2. BEDIENUNG DES SYSTEMS JABLOTRON 100

Das Sicherheitssystem kann unter anderem über ein System-Bedienteil gesteuert werden. Um die Alarmanlage unscharf zu schalten, ist immer die Autorisierung in Form einer Benutzeridentifikation erforderlich. Das System erkennt dann die Identität des Benutzers und berechtigt ihn, die Bereiche des Systems zu steuern, die ihm zur Steuerung zugewiesen wurden. Sie können auswählen, ob Sie das System mit oder ohne Autorisierung scharf schalten möchten. Bei der Einstellung ohne Autorisierung müssen Sie sich nicht selbst autorisieren, da das System einfach durch das Betätigen einer Funktionstaste auf dem Bedienteil eingestellt werden kann. Die Zentrale kann so konfiguriert werden, dass sie nur über die Autorisierungsfunktion gesteuert wird. Der Benutzername, das Datum und die Uhrzeit werden bei jedem Zugriff auf das System gespeichert. Diese Informationen sind auf unbestimmte Zeit verfügbar. Über die Autorisierungsfunktion kann jeder Benutzer (abhängig von seinen Zugriffsrechten) in jedem Sicherungsbereich einen Alarm deaktivieren (Beenden des Alarmtones). Dadurch wird das System jedoch nicht automatisch unscharf geschaltet (es sei denn, die Standardeinstellung wird geändert).

Hinweis: Abhängig von der Konfiguration der Installations- und Systemeinstellungen sind einige der unten beschriebenen Optionen möglicherweise nicht verfügbar. Lassen Sie sich bezüglich der Systemkonfiguration von Ihrem Errichter beraten.

WARNHINWEIS: Das Sicherheitssystem überwacht die Anzahl der falsch eingegebenen Benutzercodes und die Verwendung nicht korrekter Zugriffskarten. Nach 10 unkorrekten Zugriffsversuchen hintereinander wird ein Sabotagealarm ausgelöst und die Zentrale wird vorübergehend je nach Systemkonfiguration (ausgewähltem Systemprofil) gesperrt.

Benutzer und ihre Zugriffsrechte

BENUTZER--PROFIL	BESCHREIBUNG
AES	Dieser Code hat die höchste Autorisierungsstufe zum Konfigurieren des Systemverhaltens und hat die Berechtigung, das System nach einem ausgelösten Alarm und Blockierung zu entsperren. Er kann auf den Errichtermodus und auf alle Registerkarten mit Optionen zugreifen, einschließlich der AES-Kommunikation (Alarmempfangsstelle), wobei er den Zugriff des Errichters über den Errichtercode verweigern kann. Solange der Parameter „Admin schränkt Errichter/AES-Rechte ein“ unverändert bleibt, kann der AES-Code alle Bereiche und PG-Ausgänge im System steuern. Dieser Code ermöglicht das Hinzufügen von weiteren Administratoren und anderen Benutzern mit niedrigerer Autorisierungsebene sowie die Zuweisung von Codes, RFID-Anhängern und Karten. Er hat außerdem die Berechtigung, den Alarm- und Sabotagealarmspeicher zu löschen. Die Anzahl der AES-Codes ist nur durch die verbleibende Kapazität der Benutzer eingeschränkt.
Errichter (Service-techniker)	Dieser Code kann auf den Errichtermodus zugreifen und das Verhalten des Systems konfigurieren. Er hat Zugriff auf alle Registerkarten mit Optionen, einschließlich AES-Kommunikation, sofern der Zugriff nicht durch den AES-Techniker eingeschränkt ist. Solange der Parameter „Admin schränkt Errichter/AES-Rechte ein“ unverändert bleibt, kann der Errichtercode alle Bereiche und PG-Ausgänge im System steu-ern. Er kann Benutzer mit AES-Berechtigung, Errichter/Servicetechniker, Administratoren und andere Benutzer mit niedrigerer Autorisierungsebene erstellen und ihnen Zugriffscodes, RFID-Anhänger und Karten zuweisen. Hat die Berechtigung, den Alarm- und Sabotagespeicher zu löschen. Die Anzahl der Errichtercodes ist nur durch die verbleibende Kapazität der Benutzer eingeschränkt. Der werksseitig eingestellte Standardcode ist 1010 (bei gewähltem Systemprofil EN-Norm: 101010) und ist fest mit der Position 0 verbunden. Der Code kann nicht gelöscht werden.
Administrator (primär)	Dieser Code hat immer vollen Zugriff auf alle Bereiche und ist berechtigt, alle PG-Ausgänge zu steuern. Der Administrator (Hauptadministrator) kann andere Administratoren und andere Codes mit niedrigerer Autorisierungsebene erstellen und ihnen den Zugriff auf Bereiche und PG-Ausgänge, Zugriffscodes, RFID-Chips und Karten zuweisen. Hat die Berechtigung, den Alarm- und Sabotagespeicher zu löschen. Es kann nur einen primären Administratorcode geben, der nicht gelöscht werden kann. Wenn der Parameter „Admin schränkt Errichter/AES-Rechte ein“ aktiv ist, muss der Administratorcode autorisiert werden, um den Zugriff zu bestätigen. Der werksseitig eingestellte Standardcode ist 1234 (bei gewähltem Systemprofil EN-Norm: 123456) und ist fest mit der Position 1 verbunden. Der Code kann nicht gelöscht werden.
Administrator (anderere)	Hat Zugriff auf durch den primären Administrator ausgewählte Bereiche, zu denen der andere Administrator neue Benutzer mit der gleichen oder einer niedrigeren Autorisierungsebene hinzufügen kann, um Bereiche und PG-Ausgänge zu steuern. Ferner kann er ihnen Zugriffscodes, RFID-Anhänger und Karten zuweisen. Hat die Berechtigung, den Alarm- und Sabotagespeicher in zugewiesenen Bereichen zu löschen. Wenn der Parameter „Admin schränkt Errichter/AES-Rechte ein“ aktiv ist, muss der Administratorcode autorisiert werden, um den Zugriff zu bestätigen. Die Anzahl der Administratorcodes (andere) ist nur durch die verbleibende Kapazität der Benutzer eingeschränkt. Es gibt keinen werksseitig festgelegten Standardcode.
Benutzer	Dieser Code hat Zugriff auf Sicherungsbereiche und kann PG-Ausgänge steuern, die ihm durch einen Administrator zugewiesen wurden. Benutzer können ihre RFID-Anhänger und Zugangskarten hinzufügen/löschen und ihre Telefonnummern ändern. Der Benutzer hat die Genehmigung, den Alarmspeicher in zugewiesenen Bereichen zu löschen. Der Zugriff ausgewählter Benutzer auf Bereiche kann durch Zutrittszeiten eingeschränkt werden. Die Anzahl der Benutzercodes ist nur durch die verbleibende Kapazität der Benutzer eingeschränkt. Es gibt keinen werksseitig festgelegten Standardcode.
Scharfschalten	Mit diesem Code darf man nur einen bestimmten Bereich scharf schalten und kann PG-Ausgänge steuern (EIN / AUS), für die eine entsprechende Zugriffsberechtigung zugewiesen wurde. Benutzer mit dieser Autorisierungsebene sind nicht berechtigt, ihren Code zu ändern, und können den Alarmspeicher nicht löschen. Die Anzahl der Scharfschaltungscodes ist nur durch die verbleibende Kapazität der Benutzer eingeschränkt. Es gibt keinen werksseitig festgelegten Standardcode.
PG-Ausgänge	Ermöglicht dem Benutzer die Steuerung von programmierbaren Ausgängen nach Autorisierung. Dies gilt für das Ein- und Ausschalten. Benutzer mit dieser Autorisierungsebene sind nicht berechtigt, ihren Code zu ändern, und können den Alarmspeicher nicht löschen. Die Anzahl der PG-Ausgänge-Codes ist nur durch die verbleibende Kapazität der Benutzer eingeschränkt. Es gibt keinen werksseitig festgelegten Standardcode.
Überfallalarm (Panik)	Dieser Code hat nur die Möglichkeit, einen Panikalarm auszulösen. Benutzer mit diesem Code sind nicht berechtigt, ihren Code zu ändern und den Alarmspeicher zu löschen. Die Anzahl der Panikcodes ist nur durch die verbleibende Kapazität der Benutzer eingeschränkt. Es gibt keinen werksseitig festgelegten Standardcode.
Wachdienst	Dies ist ein Code für Notrufleit- oder Alarmempfangsstellen. Diese Autorisierungsebene ermöglicht die Scharfschaltung des gesamten Systems. Allerdings kann der Wachdienstcode das System nur bei Alarmen oder danach unscharf schalten, solange der Alarmspeicher noch aktiv ist. Benutzer mit diesem Code sind nicht berechtigt, ihren Code zu ändern und den Alarmspeicher zu löschen. Die Anzahl der Wachdienstcodes ist nur durch die verbleibende Kapazität der Benutzer eingeschränkt. Es gibt keinen werksseitig festgelegten Standardcode.
Entsperren	Dieser Code dient dem Entsperren des Systems nach der Sperrung des Systems durch einen Alarm. Benutzer mit diesem Code sind nicht berechtigt, die Alarmanlage zu steuern, ihren Code zu ändern oder den Alarmspeicher zu löschen. Die Anzahl der Entsperrcodes ist nur durch die verbleibende Kapazität der Benutzer eingeschränkt. Es gibt keinen werksseitig festgelegten Standardcode.

2.1 CODE-AUTORISIERUNG AM BEDIENTEIL

Die Autorisierung mit einem Benutzercode erfolgt durch Eingabe eines gültigen Codes an einem Bedienteil oder mit einem RFID-Tag.
Dabei kann ein 4- oder 6-stelliger Code in das System (abhängig vom ausgewählten Profil) eingegeben werden.

CCCC

Bedeutung:
CCCC ist ein 4 oder 6-stelliger Code. Erlaubte Codes sind von 0000 bis 9999 (000000 bis 999999)

Standard-Code der Zentrale **Administrator: 1234; 123456;**

WARNHINWEIS: Es wird empfohlen, den Administrator-Code zu ändern, wenn das Alarmsystem das erste Mal eingeschaltet wird.

Die Sicherheit der Zugangscodes und der kontaktlosen RFID-Geräte:

Für die Systemautorisierung kann einem Benutzer von der Zentrale ein 4- oder 6-stelliger Code und ein RFID-Chip zugewiesen werden. Die Benutzerautorisierung ist jedes Mal erforderlich, wenn das System über ein Bedienteil, das Sprachmenü, Computer oder die webbasierten oder mobilen Anwendung bedient werden soll. Die Codelänge bedingt die Anzahl der möglichen Kombinationen und somit die Codesicherheit.

Die Anzahl der Codekombinationen hängt von der Konfiguration ab:

PARAMETER DER ZENTRALE	4 ZIFFERN	6 ZIFFERN
Parameter „**Überfallalarm**“ deaktiviert, Autorisierungstyp auf „**Standard**” aktiviert	= 10^4 – (Anzahl der Benutzer – 1)	= 10^6 – (Anzahl der Benutzer – 1)
„**Überfallalarm**“ aktiviert, Autorisierungstyp auf „**Standard**” aktiviert	≤ 10^4 – ((Anzahl der Benutzer – 1) * 3)	≤ 10^6 – ((Anzahl der Benutzer – 1) * 3)
„Überfallalarm“ deaktiviert, **„Doppelteautorisierung”** aktiviert	= 10^8 * (10^4 – (Anzahl der Benutzer – 1))	= 10^8 * (10^6 – (Anzahl der Benutzer – 1))
„Überfallalarm“ aktiviert, **„Doppelteautorisierung”** aktiviert	≤ 10^8 * (10^4 – ((Anzahl der Benutzer – 1) * 3))	≤ 10^8 * (10^6 – ((Anzahl der Benutzer – 1) * 3))
Nur **RFID-Karte/-Tag** ohne Zugangscode	= 10^8 = (100.000.000)	= 10^8 = (100.000.000)

MÖGLICHKEITEN, WIE MAN DEN SCHUTZ GEGEN DAS ERRATEN DES GÜLTIGEN CODES VERBESSERN KANN:

- Einen Code mit mehr Ziffern benutzen (6-stellige Codes)
- Fortschrittlichere Arten der Autorisierung, beispielsweise „Doppelte Autorisierung“.

Sicherheit von Fernsteuerungen:

Die Zentrale kann über Fernbedienungen bedient werden. Die Sicherheit solcher Steuerungen wird dadurch gewährleistet, dass es mehr als 1 000 000 kombinierbare Identifikationscodes gibt und die Daten verschlüsselt übertragen werden.

2. BEDIENUNG DES SYSTEMS JABLOTRON 100

Bedienungsmöglichkeiten der Zentrale JA-100K:

vor Ort:

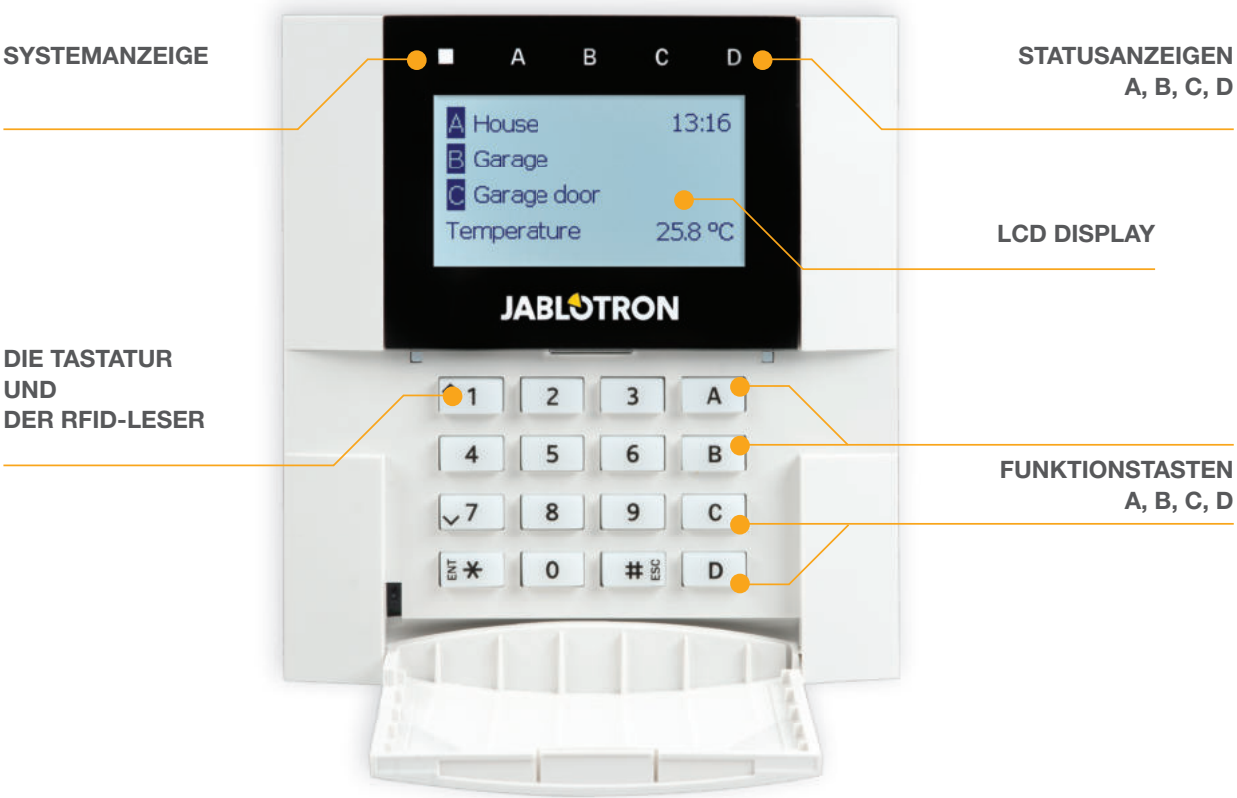
- Bedienteil des Systems
- Fernbedienung des Systems
- Computer mit einem USB-Kabel und der Software J-Link

per Fernzugriff:

- Smartphone-Anwendung MyJABLOTRON
- Computer über das Webinterface MyJABLOTRON
- Mobil per SMS
- Telefon mit Sprachmenü
- Computer - über das Internet mit der Software J-Link
- Anruf von einer autorisierten Telefonnummer (nur für die Bedienung programmierbarer Ausgänge).

WARNHINWEIS: Die Fernsteuerung kann je nach Sicherheitsumfang und ausgewähltem Systemprofil eingeschränkt sein.

2.2 VERWENDUNG DES SYSTEM-BEDIENTEILS



JABLOTRON 100 kann über System-Bedienteil gesteuert werden, über das nicht nur die Steuerung erfolgt, sondern auch der Status einzelner Bereiche angezeigt wird. Der Status der einzelnen Bereiche wird von den Statusanzeigen A, B, C, D über dem LCD-Display und den Funktionstasten angezeigt. Die Zentrale kann direkt über die Funktionstasten auf dem Bedienteil bedient werden (Scharf- oder Unscharfschalten des Alarmsystems und andere Automatisierungsfunktionen). Die Funktionstasten und die Statusanzeigen A, B, C, D leuchten farbig, um den Bereichsstatus eindeutig anzuzeigen.

GRÜN – unscharf

GELB – teilscharf

ROT – scharf

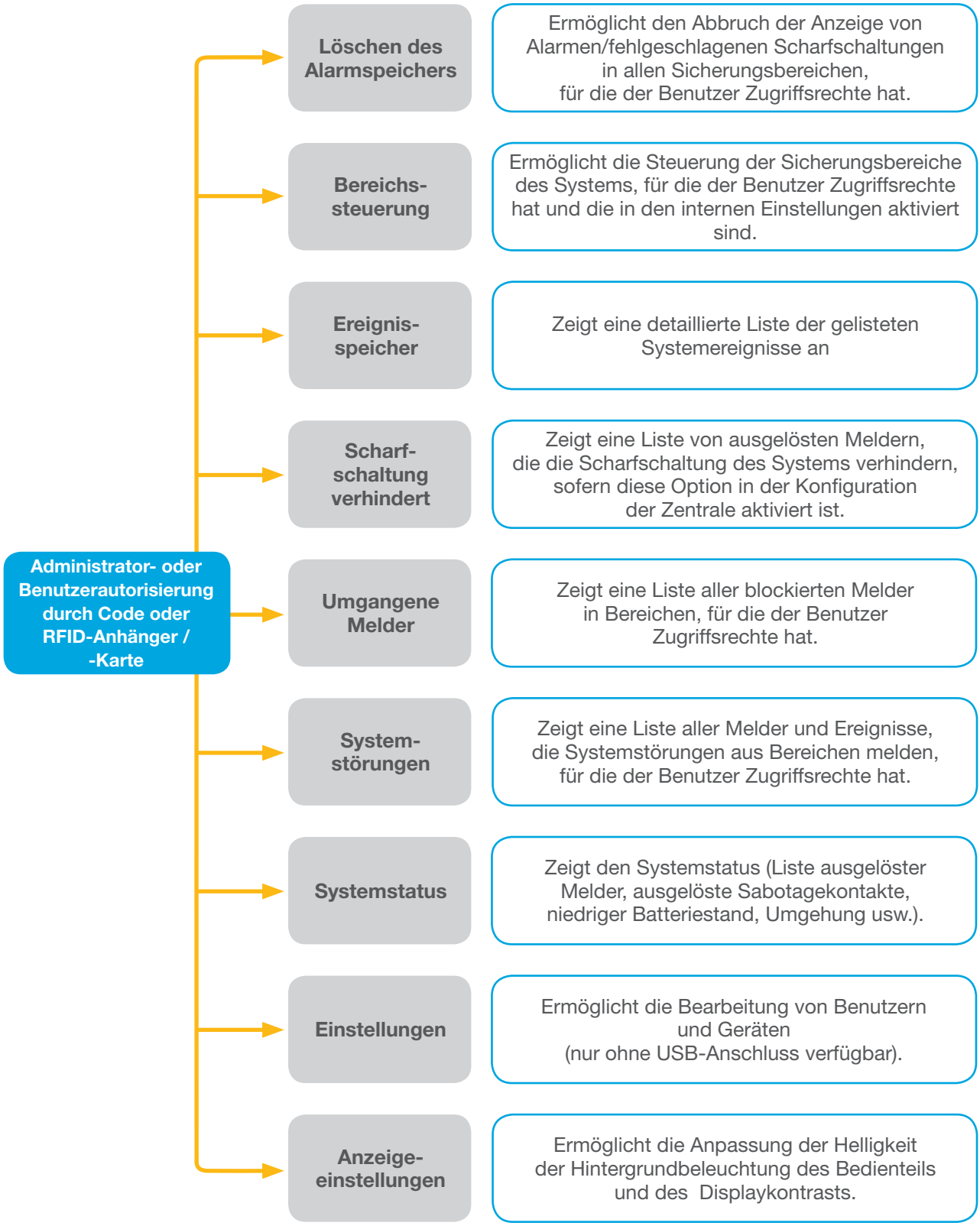
Der Autorisierungsprozess

Der Autorisierungsprozess erfolgt über die Eingabe eines Autorisierungscodes auf dem Bedienteil oder durch Verwendung einer RFID-Karte / eines RFID-Anhängers. Jedem Benutzer kann dabei ein Code und ein RFID-Chip (eine Karte oder ein Anhänger) zugewiesen werden.

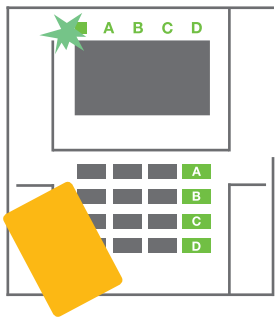
Die Zentrale unterstützt RFID-Chips, die kompatibel mit EM Unique 125 kHz sind. Im Falle einer höheren Sicherheitsstufe wird das Alarmsystem so eingerichtet, dass die doppelte Autorisierung mit RFID-Chips und Codes (eine optionale Funktion) verwendet wird.

Wenn der Benutzer mehrere Bereiche gleichzeitig steuern möchte, muss er sich selbst autorisieren und dann nachträglich die Funktionstasten der einzelnen Bereiche betätigen. Auf diese Weise kann der Benutzer alle Bereiche (z.B. Haus und Garage) innerhalb einer einzigen Autorisierung unscharf schalten.

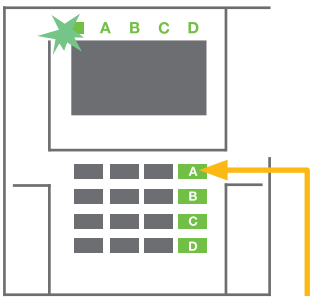
Menüstruktur und Beschreibung des LCD-Bedienteils



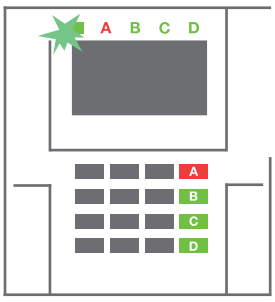
2.2.1 SCHARFSCHALTEN VON SICHERUNGSBEREICHEN



1. **Autorisieren Sie sich über das Bedienteil.** Die Funktionstasten A, B, C, D leuchten auf und die Systemanzeige blinkt grün.



2. **Betätigen Sie die Funktionstaste für die Scharschaltung des gewünschtes Bereichs.** Es können mehrere Bereiche nacheinander scharfgeschaltet werden. Der zeitliche Abstand bei der Auswahl der Bereiche darf nicht größer als 2 Sekunden sein.



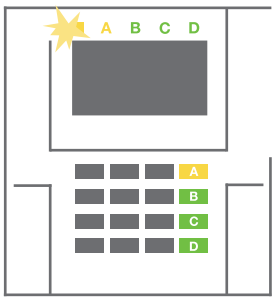
3. **Der Befehl wird ausgeführt und das Bedienteil zeigt akustisch die Ausgangsverzögerung an.** Der Bereich ist nun scharf geschaltet. Lediglich Melder des Reaktionsmodus „Verzögerter Alarm“ stellen mehr Zeit zum Verlassen des überwachten Bereichs während der Ausgangsverzögerung zur Verfügung. Die Statusanzeige und eine Funktionstaste des scharf geschalteten Bereichs leuchten nun rot.

Sollte ein Zustand-Melder bei Scharfschaltung des Sicherungsbereichsausgelöst sein (z. B. ein offenes Fenster), reagiert das System (je nach Systemkonfiguration) auf eine der folgenden Arten:

- Die Zentrale schaltet sich scharf. Ausgelöste Melder werden automatisch gesperrt.*)
- Das System zeigt ausgelöste Melder optisch über eine Funktionstaste an. Diese blinkt für 8 Sekunden rot auf. Nach Ablauf dieser Zeit wird die Zentrale automatisch scharf geschaltet (ausgelöste Melder werden gesperrt). *)
- Ein Bereich mit ausgelösten Meldern kann auch scharf geschaltet werden, indem man die Funktionstaste mehrmals betätigt. Der Benutzer muss in diesem Fall die Scharfschaltung des Bereichs mit ausgelösten Meldern (z. B. einem geöffneten Fenster) bestätigen. Andernfalls wird das System nicht scharf geschaltet.
- Ein ausgelöster Melder verhindert die Scharfschaltung des Bereichs. Dieser Status wird optisch durch eine rot blinkende Funktionstaste angezeigt. In Menü des LCD-Bedienteils sind die ausgelösten Melder, die die Scharfschaltung des Systems verhindern, abzulesen.

***) WARNHINWEIS:** Die Optionen werden von dem Systemprofil „EN 50131“ nicht unterstützt

Wenn ein Melder des Reaktionsmodus „Sofortiger Alarm“ während einer Ausgangsverzögerung ausgelöst wird oder wenn ein Melder des Reaktionsmodus „Verzögerter Alarm“ nach Ablauf der Ausgangsverzögerung ausgelöst bleibt, wird die Zentrale wieder unscharf geschaltet. Die nicht erfolgreiche Scharfschaltung wird durch eine gelb blinkende Systemanzeige angezeigt, der Leitstelle gemeldet und durch eine externe Sirene angezeigt (gilt für das Systemprofil EN50131).

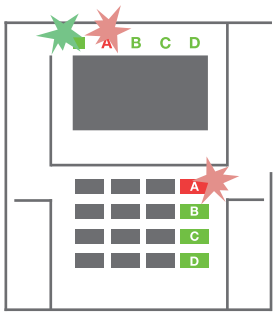


Wenn die Zentrale so konfiguriert ist, dass sie ohne Autorisierung scharf geschaltet werden kann, ist die eigene Autorisierung nicht notwendig. Betätigen Sie in diesem Fall die Funktionstaste eines bestimmten Bereichs. Es ist auch möglich, die Zentrale so zu konfigurieren, dass sie nur über die Autorisierungsfunktion scharf geschaltet werden soll.

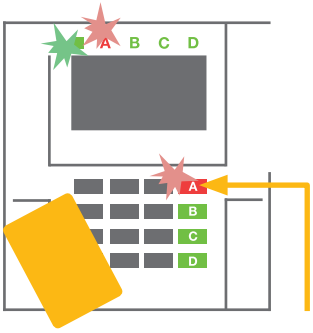
WARNHINWEIS: Durch die Scharfschaltung ohne Autorisierung wird der maximale Sicherheitsgrad automatisch auf Grad 1 heruntergestuft. Bedenken Sie deshalb die möglichen Risiken, die im Zusammenhang mit der Verwendung dieser Funktion stehen.

Zur Programmierung des gewünschten Systemverhaltens lassen Sie sich von einem Projektberater oder einem Errichter beraten.

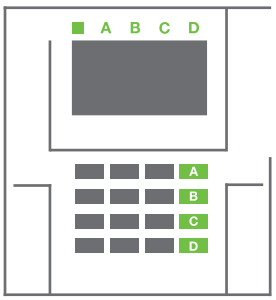
2.2.2 UNSCHARFSCHALTEN VON SICHERUNGSBEREICHEN



1. **Wenn Sie das Gebäude betreten** (und einen Melder des Reaktionsmodus „Verzögerter Alarm" auslösen), zeigt das System eine Eingangsverzögerung in dem Bereich, in dem die Eingangsverzögerung ausgelöst wurde, über einen Dauerton an. Die Systemanzeige und eine Funktionstaste des Bereichs blinken jeweils beide rot.



2. **Autorisieren Sie sich** über das Bedienteil - die Systemanzeige blinkt dann grün.
3. **Betätigen Sie die Funktionstasten** der Bereiche, die Sie unscharf schalten möchten.



4. **Der Befehl wird ausgeführt.** Die Funktionstasten und die Systemanzeige leuchten grün und zeigen somit die unscharf geschalteten Bereiche an.

Hinweis: Wenn der Parameter „Unscharfschaltung nach Autorisierung nur während der Eingangsverzögerung „ aktiviert ist, schaltet die Autorisierung den Bereich unscharf, in dem die Eingangsverzögerung aktiviert wurde. Dies muss für etwaige Bedienteile separat vorsichtig eingestellt werden.

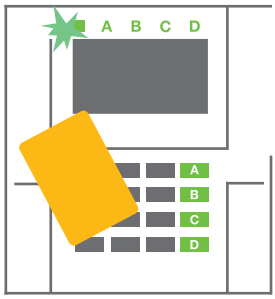
Zur Programmierung des gewünschten Systemverhaltens lassen Sie sich von einem Projektberater oder einem Errichter beraten.

2.2.3 TEILSCHARFSCHALTEN VON SICHERUNGSBEREICHEN

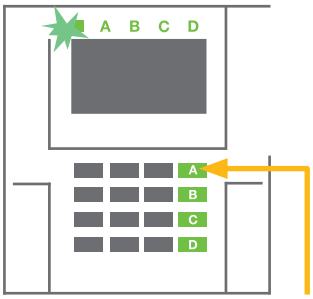
WARNHINWEIS: Dies ist eine zusätzliche Funktion des Alarmsystems.

Das System kann auch auf eine Teilscharfschaltung konfiguriert werden, die die Überwachung eines Bereichs nur durch bestimmte Melder ermöglicht.

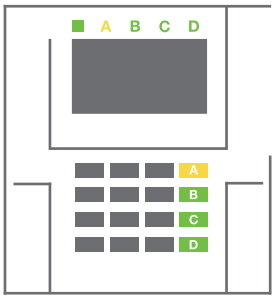
Beispiel: Es ist möglich, nur die Tür- und Fenstermelder nachts scharf zu schalten, wohingegen ausgewählte Bewegungsmelder keinen Alarm auslösen, wenn sich jemand innerhalb dieses Bereichs bewegt.



1. **Autorisieren Sie sich über das Bedienteil** (geben Sie einen Code ein oder halten Sie eine RFID-Karte oder einen RFID-Anhänger an den Leser). Die Systemanzeige beginnt dann grün zu blinken.



2. **Drücken Sie die Funktionstaste** des ausgewählten Bereichs.



3. **Der Befehl wird ausgeführt** und die Funktionstaste leuchtet dauerhaft gelb und zeigt an, dass der Bereich teilscharf geschaltet ist.

Um den gesamten Bereich scharfzuschalten, in dem die Teilscharfschaltung ermöglicht ist, halten Sie die Taste zur Scharfschaltung für 2 Sekunden gedrückt oder drücken Sie sie zweimal. Nachdem die Taste einmal gedrückt wurde, leuchtet sie dauerhaft gelb, nach dem zweiten Drücken leuchtet sie dauerhaft rot.

Falls das System bereits teilscharfgeschaltet ist – angezeigt durch durchgehendes gelbes Leuchten – kann das gesamte System durch Autorisierung und längeres Drücken der gelben Taste vollständig scharfgeschaltet werden. Nach dem Betätigen der Taste ist das System vollständig scharf geschaltet und die Taste leuchtet rot.

Die Teilscharfschaltung kann so konfiguriert werden, dass keine Autorisierung erforderlich ist.
Um den teilscharf geschalteten Bereich unscharf zu schalten, betätigen Sie die gelbe Taste. Das System wird dann unscharf geschaltet und die Taste leuchtet grün.

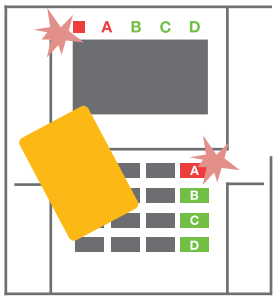
2.2.4 DIE ERZWUNGENE ZUGRIFFSSTEUERUNG (ÜBERFALLALARM)

Der Parameter „Überfallalarm“ ermöglicht die Unscharfschaltung des Systems in einem speziellen Modus. Das System wird unscharf geschaltet, löst allerdings einen stillen Überfallalarm (Panikalarm) aus, der an ausgewählte Benutzer (einschließlich NSL/AES) gemeldet wird.

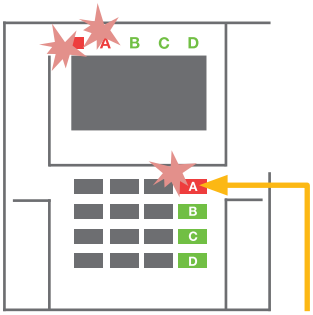
Die Unscharfschaltung in Zwangsfällen wird durch Addieren von 1 zur letzten Zahl eines gültigen Codes ausgeführt. Wenden Sie sich an Ihren Errichter/Servicetechniker, wenn Sie diese Funktion nutzen möchten.

Beispiel:
Gültiger Code: **9999**
Code für Unscharfschaltung in Zwangsfällen: **9990**

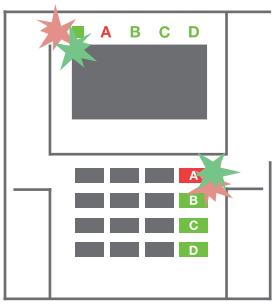
2.2.5 ABBRECHEN EINES AUSGELÖSTEN ALARMS



1. **Autorisieren Sie sich über das Bedienteil** (geben Sie einen Code ein oder halten Sie eine RFID-Karte / einen RFID-Anhänger an den Leser).



2. **Drücken Sie die Funktionstaste** des Bereichs, in dem der Alarm ausgelöst wurde.



3. **Die Unscharfschaltung wurde durchgeführt** und die Sirenen sind verstummen. Durch das schnelle abwechselnde Blinken (grün/rot) zeigen die Funktionstaste und die Statusanzeige den Alarmspeicher an.

Ein aktiver ausgelöster Alarm wird durch die Statusanzeige und durch eine schnell rot blinkende Funktionstaste angezeigt. Sie müssen sich mithilfe des Bedienteils autorisieren, um den Alarm abzubrechen. Der Bereich bleibt scharfgeschaltet, eine schnell rot blinkende Funktionstaste zeigt den Alarmspeicher an. Die Anzeige blinkt auch nach der Unscharfschaltung des Systems weiter.

WARNHINWEIS: Wenn die Alarmspeicheranzeige während Ihrer Abwesenheit aktiviert wurde, betreten Sie das Gebäude immer mit Vorsicht, suchen Sie die Ursache des Alarms im Ereignisverlauf und seien Sie bei der Überprüfung der Räumlichkeiten sehr vorsichtig. Warten Sie gegebenenfalls, bis der Sicherheitsdienst eintrifft (sofern Ihr System mit einer Alarmempfangsstelle verbunden ist).

Die Alarmspeicheranzeige bleibt so lange eingeschaltet, bis das System wieder scharf geschaltet wurde. Alternativ kann sie auch über das Menü des Bedienteils abgebrochen werden. Hauptmenü - “Löschen des Alarmspeichers“.
Die Anzeige eines ausgelösten Sabotagealarms kann nur von einem Errichter oder einem Administrator beendet werden.

Hinweis: Bei der Verwendung des Systemprofils „Standard“ ist es möglich, das folgende Verfahren zu benutzen erst durch Betätigen einer Funktionstaste eine bestimmte Aktion auszuwählen und diese dann durch Autorisierung mithilfe des Bedienteils zu bestätigen.

Das Abbrechen eines Alarms mithilfe einer Fernbedienung schaltet auch den entsprechenden Bereich unscharf.

2.2.6 BEREICHSSTEUERUNG ÜBER DIE AUTORISIERUNGSFUNKTION

Der Errichter kann die Zentrale so konfigurieren, dass sie nur über die Autorisierung gesteuert werden kann. Auf diese Weise kann das System den Status aller zugewiesenen Bereichen nur durch Autorisierung am Bedienteil ändern (durch Eingabe des Autorisierungscodes oder mithilfe eines RFID-Chips).

2.2.7 BEREICHSSTEUERUNG ÜBER DAS DISPLAYMENÜ DES BEDIENTEILS

Steuerung über das Tastaturmenü:

- Autorisieren Sie sich mit einem gültigen Code oder einem RFID-Chip
- Drücken Sie die **ENTER**-Taste, um in das Menü zu kommen
- Bereichssteuerung → **ENTER**
- Wählen Sie den gewünschten Bereich mit den Pfeilen aus
- Wiederholtes Drücken der **ENTER**-Taste ändert den Bereichsstatus (teilscharf/ scharf / unscharf)

  Teilscharf: **1**

  Vollständig scharf: **1**

- Drücken Sie ESC zum Verlassen des Menüs

2.3 BEDIENEN DES SYSTEMS MIT EINER FERNBEDIENUNG

Fernbedienungen müssen vom Errichter bei der Zentrale angemeldet werden. Um die Alarmanlage zu steuern, müssen die Fernbedienungen mit bestimmten Benutzern verknüpft werden, um ihre Identifizierung zu garantieren und das Versenden von SMS-Benachrichtigungen an den Benutzer, der zu diesem Zeitpunkt mit der Zentrale interagiert, zu vermeiden (für den Fall, dass diese Benachrichtigung entsprechend konfiguriert ist). Mit der Fernbedienung ist nicht nur eine bidirektionale Kommunikation möglich, wobei ein ausgeführter Befehl mit einer farbigen Kontrollleuchte bestätigt wird, sondern auch die Einwegkommunikation ohne Bestätigung. Fernbedienungen zeigen den Batteriestatus an und verfügen über optische und akustische Anzeigen.

Bidirektionale Fernbedienung

Die Funktionstasten sind durch die entsprechenden Schloss-Symbole gekennzeichnet. Das geschlossene Sperrsymbol schaltet programmierte Bereiche scharf; das geöffnete Sperrsymbol schaltet diese unscharf. Die korrekte Ausführung des Befehls wird durch eine aufleuchtende LED bestätigt; Unscharfschaltung – grün, Scharfschaltung – rot. Ein Kommunikationsfehler (außerhalb des Kommunikationsbereichs der Zentrale) wird durch eine einmal blinkende gelbe LED-Anzeige angezeigt. Die Tasten, die durch volle und leere Kreise symbolisiert sind, können einen anderen Bereich steuern. Die Tasten der Fernbedienung können auch so konfiguriert werden, dass sie die PG-Ausgänge in unterschiedlichen Modi steuern: Die erste Taste schaltet ein, die zweite Taste schaltet aus, jeder Taste kann bei Verwendung der Impuls- oder Kopierenfunktion eine individuelle Funktion zugeordnet werden. Für weitere Funktionen ist es möglich, zwei Tasten gleichzeitig zu drücken. Auf diese Weise kann eine Fernbedienung mit 4 Tasten bis zu 6 Funktionen haben. Zum Beispiel können zur Steuerung eines zugewiesenen Bereichs, ein Status-PG--Ausgang (z.B. schaltet die Lichter ein und aus) oder alternativ zwei Impuls PG-Ausgänge (z.B. Garatentür und eine Türverriegelung) konfiguriert sein.

Wenn das System so konfiguriert ist, dass die Scharfschaltung nach Bestätigung erfolgt (Abschnitt 2.2.1), zeigt die Fernbedienung eine nicht erfolgreiche Scharfschaltung über eine grün leuchtende LED an. Die Scharfschaltung ist durch erneutes Drücken der Taste für Scharfschaltung zu bestätigen. Ein scharf geschalteter Bereich wird durch eine rot aufleuchtende LED bestätigt.

Die Tasten der Fernbedienung können gesperrt werden, um ein versehentliches Drücken zu verhindern (Kindersicherung). Ein Befehl wird bei wiederholtem Betätigen der Taste gesendet.

Eine schwache Batterie wird akustisch (mit 3 Pieptönen) und optisch mit einer gelb blinkenden LED nach Drücken einer Taste angezeigt.

Ihr Errichter berät Sie gern bezüglich der Konfiguration der Fernbedienung. Detaillierte Informationen stehen in den Anleitungen der entsprechenden Fernbedienungen zur Verfügung.

Ein-Weg-Fernbedienung

Ein-Weg-Fernbedienungen senden bei jedem Tastendruck ein Signal, ohne eine Rückmeldung von der Zentrale zu erhalten. Das Senden eines Signals wird durch kurzes Aufleuchten der roten LED und alternativ mit einem Signalton bestätigt.

Die Tastenfunktionen sind identisch mit denen bidirektionaler Fernbedienungen.

Eine schwache Batterie wird durch eine rote LED und akustisch (3 schnelle Pieptöne) angezeigt.

2.4 BEDIENEN DES SYSTEMS MITHILFE EINES COMPUTERS UND USB-KABELS (J-LINK)

Das System JABLOTRON 100 kann lokal oder aus der Ferne (siehe Abschnitt 2.9) über einen Computer und die installierte Software J-Link bedient werden, die für die Benutzerverwaltung verwendet werden kann (Benutzer hinzufügen/entfernen, ihre Autorisierungsebene, Telefonnummern, Codes, Karten / Anhänger ändern usw.).

Über J-Link wird die lokale Verbindung mit der Zentrale hergestellt. Die Software befindet sich auf dem Speicherlaufwerk des Sicherheitssystems (FLEXI_CFG / j-link) und ist sichtbar, wenn die Zentrale über ein USB-Kabel mit einem PC verbunden ist.

Es ist möglich, das System über die Symbole auf der unteren Leiste der Software oder über „Status" in der Registerkarte „Bereichsübersicht" scharf zu schalten / unscharf zu schalten.

WARNHINWEIS: Wenn das System über einen PC gesteuert wird, wird bei der Scharfschaltung nicht geprüft, ob Geräte aktiviert werden konnten. Dies kann zur Scharfschaltung mit einer aktiven Komponente führen. Gehen Sie deshalb bei dieser Steuerungsart sehr vorsichtig vor!

WARNHINWEIS: J-Link ist nur für das Windows Betriebssystem verfügbar.

2.5 BEDIENEN DES SYSTEMS ÜBER DAS SPRACHMENÜ

Wenn ein GSM- oder ein PSTN-Kommunikationsmodul in der Zentrale installiert ist, kann das System über ein einfaches Sprachmenü des Handies oder analogen Festnetzanschlusses gesteuert werden, was den Benutzer durch eine Reihe von Optionen in der vorkonfigurierten Sprache führt. Um auf das Sprachmenü zuzugreifen, wählen Sie einfach die Telefonnummer der Zentrale.

Der Zugriff auf das Sprachmenü kann entweder uneingeschränkt für alle Telefonnummern oder nur für be-rechtigte und in der Zentrale gespeicherte Telefonnummern aktiviert werden. Je nach Konfiguration muss zur Autorisierung der gültige Code auf einer Telefontastatur eingegeben werden. Wenn der Benutzer auf das Menü zugreift, zeigt das System den aktuellen Status aller dem Benutzer zugewiesenen Bereiche an. Der Anrufer kann diese Bereiche entweder individuell oder gesammelt über die Telefontastatur entsprechend den verfügbaren Menüoptionen steuern.

WARHINWEIS: Es wird empfohlen, diese Funktion mit Vorsicht zu benutzen. Die Fernsteuerung und Unscharfschaltung können unbeabsichtigte Alarme verursachen oder die Scharfschaltung verhindern, wenn sich noch andere Personen im Gebäude befinden.

Standardmäßig ist das System so eingerichtet, dass eingehende Anrufe nach dem dritten Klingeln (ca. 15 Sekunden) beantwortet werden.

2.6 BEDIENEN DES SYSTEMS ÜBER DIE WEBASIERTE UND MOBILE ANWENDUNG MyJABLOTRON

Das System JABLOTRON 100 lässt sich einfach und bequem mit Ihrem Computer über das Internet und das Webinterface MyJABLOTRON steuern. Der Zugriff darauf ist über www.myjablotron.com möglich. Weitere Informationen über dieses Webinterface finden Sie in Kapitel 6 unten.

MyJABLOTRON - PROFI Version

Je nach Land oder Region kann ein Web-Konto in MyJABLOTRON von einem berechtigten JABLOTRON-Partner eingerichtet werden. Der Login-Name ist die E-Mail-Adresse des Benutzers. Das Passwort für die erste Anmeldung wird an diese Adresse gesendet und kann jederzeit in den Kontoeinstellungen geändert werden.

Sobald Sie sich angemeldet haben, zeigt MyJABLOTRON alle aktiven Geräte an, die überwacht oder gesteuert werden können.

Das Menü-Übersicht enthält die Registerkarten „Bereiche“ und „Automatisierung (PG)“. Je nach Typ der verwendeten Melder kann dieses Menü zusätzlich Registerkarten wie „Thermostate und Thermometer“, „Messeinheit“ , „Verlauf“ oder „Galerie“enthalten.

Registerkarten:

- **Bereiche** – ermöglicht Ihnen, alle Bereiche im System zu überblicken und diese zu bedienen, indem Sie auf das Sperrsymbol klicken. Bei der ersten Anfrage zur Systemsteuerung werden Sie aufgefordert, einen Autorisierungscode einzugeben. Während Sie angemeldet sind, werden Sie nicht noch einmal aufgefordert, den Autorisierungscode einzugeben.
- **Automatisierung (PG)** – ermöglicht Ihnen, programmierbare Systemausgänge zu sehen und durch Anklicken von ON/OFF zu steuern.
- **Thermostate und Thermometer** - ermöglicht Ihnen, die aktuelle Temperatur aller installierten Thermometer anzuzeigen. Der Verlauf und die Grafiken der Temperaturänderungen werden angezeigt. Entsprechend den Einstellungen kann die Temperatur und der Modus der Thermostate geändert werden.
- **Messeinheit** – Übersicht der installierten Module, die als Zähler von Strom, eventuell von Gas oder Wasser dienen können. Die gemessenen Werten oder die Grafiken werden angezeigt.
- **Verlauf** – Verlauf der Systemereignisse. Wobei auch Aufnahmen von Kamerameldern übersichtlich dargestellt werden.
- **Galerie** – ermöglicht es Ihnen, Aufnahmen mit jedem installierten Gerät mit Kameraüberwachung zu erstellen oder vorher gemachte Aufnahmen einzusehen (Bilderarchiv).

Im unteren Teil der Startseite finden Sie den Verlauf der letzten Systemereignisse.

MyJABLOTRON bietet kostenlose Benachrichtigungen (per SMS, E-Mail oder PUSH-Benachrichtigungen) für ausgewählte Ereignisse der Systembereiche, programmierbaren Ausgänge, Thermometer oder Zähler an. Diese Benachrichtigungen können im Menü „Einstellungen" eingestellt werden.

Jedes System kann nur einen Hauptbenutzer mit Administratorrechten (Besitzer) haben. Dieser Benutzer hat das Recht, ein ganzes Objekt oder ausgewählte Bereiche davon (einzelne Bereiche, PG-Ausgänge, Kameraüberwachung und Messgeräte) mit anderen Benutzern zu teilen, deren MyJABLOTRON-Konten automatisch nach der Konfiguration der gemeinsam geteilten Systemnutzung eingerichtet werden. Wenn ein Benutzer bereits über ein MyJABLOTRON-Konto verfügt, wird die gemeinsam genutzte Installation als weiteres aktives Gerät in der Hauptübersicht des Benutzers. Die Benachrichtigung über den gemeinsamen Zugriff erfolgt zusammen mit dem Passwort an die E-Mail-Adresse (Login-Name) des neuen Benutzers.

MyJABLOTRON - LITE Version

Je nach Land (oder Region) können Kunden ein Konto und / oder Dienste in der LITE-Version der MyJABLOTRON--Web-Anwendung erstellen.

Der LITE-Service ist in der Funktionalität begrenzt und minimiert die Anforderungen an die Datenübertragung. LITE basiert auf der PROFI-Version mit folgenden Änderungen:

Die LITE-Version im Vergleich zur PROFI-Version:

- Keine permanente Verbindung mit der Zentrale
- Der Verbindungsaufbau dauert ca. 1 Minute
- Der aktuelle Status wird nach erfolgreichem Verbindungsaufbau angezeigt
- Die Systemsteuerung (Bereiche oder PG-Ausgänge) ist nach erfolgreichem Verbindungsaufbau möglich
- Der Ereignisverlauf ist nicht verfügbar
- Das System sendet keine Benachrichtigungen über Ereignisse (SMS, Email, PUSH-Benachrichtigungen)
- Die Bildergalerie sowie die Funktion, Fotos auf Anfrage mit Kameramеldern aufzunehmen, ist nicht verfügbar
- Thermometer, Stromzähler und andere unterstützte Automatisierungsgeräte werden nicht angezeigt

Ein Passwort wird an die E-Mail-Adresse des Benutzers gesendet, die auch als Login-Name dient. Das Passwort kann jederzeit in den Einstellungen geändert werden.

Nach der Anmeldung in Ihr Konto zeigt das System alle aktiven Geräte, die überwacht oder gesteuert werden können, abhängig von der registrierten Version von MyJABLOTRON (PROFI oder LITE).

2.7 BEDIENEN DES SYSTEMS MIT DER MyJABLOTRON-SMARTPHONE-APP

Wenn der Benutzer sein Konto über das MyJABLOTRON-Webinterface erstellt hat (siehe vorherigen Abschnitt), kann das Alarmsystem über die MyJABLOTRON-App für Smartphones mit Android (ab Version 4.0.3), iOS (ab Version 7) oder Windows Mobile aus der Ferne überwacht und gesteuert werden. Die Anwendung kann nach dem Login in MyJABLOTRON oder über Google Play, AppStore usw. kostenfrei heruntergeladen werden.

Die Login-Daten der MyJABLOTRON-Smartphone-App entsprechen denen für das MyJABLOTRON-Webinterface.

2.8 BEDIENUNG DES SYSTEMS PER SMS

Wenn eine GSM-Verbindung zur Zentrale aufgebaut werden kann, ist es möglich, einzelne Bereiche und programmierbare Ausgänge wie die Funktionstasten des Bedienteils per SMS zu steuern. Die Textnachricht zur Systembedienung lautet: CODE_BEFEHL. Die eigentlichen Befehle (SCHARF / UNSCHARF) sind über einen zusätzlichen numerischen Parameter, der den individuellen Bereich identifiziert, vordefiniert.

Eine SMS kann mehrere Bereiche gleichzeitig steuern. In diesem Fall definieren zum Befehl hinzugefügte Zahlen die Bereiche.

Beispiel eines SMS-Befehls, der Bereich 2 und 4 scharf schaltet.
Das Unterstrich "_" steht für einen Leerzeichen zwischen den Wörtern.

CODE_ SCHARF_2_4

Die Befehle zur Steuerung der programmierbaren Ausgänge werden von einem Errichter programmiert. Zum Beispiel können Sie ROLLADEN RUNTER als Ihren Befehl wählen, um die Rolläden zu schließen. Ebenso kann das System so konfiguriert werden, dass kein Code vor einem Befehl eingegeben werden muss. In diesem Fall wird der Befehl automatisch erkannt, wenn das System die Telefonnummer des Benutzers identifiziert, von der die SMS gesendet wurde.

WARNHINWEIS: Es wird empfohlen, diese Funktion mit Vorsicht zu benutzen. Die Fernsteuerung und Unscharfschaltung können unbeabsichtigte Alarme verursachen oder die Scharfschaltung verhindern, wenn sich noch andere Personen im Gebäude befinden.

2.9 FERNBEDIENEN DES SYSTEMS ÜBER EINEN COMPUTER (J-LINK)

Das System JABLOTRON 100 kann durch Installation des Programms J-Link auf Ihrem Computer aus der Ferne und lokal bedient werden (siehe Abschnitt 2.4). Das Programm kann auch für die Benutzerverwaltung (Ändern von Codes, Karten/ Anhängern und Telefonnummern) verwendet werden

Um das System per Fernzugriff zu bedienen, muss das Programm aus dem Bereich „Downloads“ auf der Website www.jablotron.com heruntergeladen werden. Alternativ ist es auch auf der SD-Karte der Zentrale zu finden. Dabei ist der Registrierungscode der Zentrale (ein 14-stelliger Code) und die Telefonnummer der entsprechenden SIM-Karte (falls verwendet) für den ersten ferngesteuerten Verbindungsaufbau zum System erforderlich. Durch das Klicken auf „Internet" im Hauptmenü wird der Fernzugriff gestartet.

Wenn die Verbindung hergestellt ist, kann die Zentrale genauso gesteuert werden wie bei der Verbindung über ein USB-Kabel (siehe Abschnitt 2.4).

Das System kann über die Bereichssymbole auf der unteren Leiste der Software oder über die Schaltflächen „Status" in der Registerkarte „Bereichsübersicht“ scharf / unscharf geschaltet werden.

WARNHINWEIS: Wenn das System über einen PC gesteuert wird, kann die Scharfschaltung mit einem aktiven Melder nicht verhindert werden. Gehen Sie deshalb bei dieser Steuerungsart sehr vorsichtig vor!

WARNHINWEIS: J-Link ist nur für das Windows Betriebssystem verfügbar.

2.10 STEUERUNG VON PG-AUSGÄNGEN

Die Steuerung der PG-Ausgänge ist für Funktionen vorgesehen, die nicht im Zusammenhang mit einem Alarm sondern der Hausautomatisierung stehen. Dabei können sie für die Statusanzeige oder die Steuerung von elektronischen Schlössern verwendet werden.

2.10.1 FUNKTIONSTASTEN DES BEDIENTEILS

Ein PG-Ausgang wird durch Betätigen einer Funktionstaste (A, B, C, D) eingeschaltet und durch erneutes Betätigen der Taste wieder ausgeschaltet. Wenn der Ausgang als Impulsausgang konfiguriert ist, schaltet er sich entsprechend der voreingestellten Zeit aus.

Ob eine Autorisierung erforderlich ist, hängt von der Systemkonfiguration ab.

2.10.2 AUTORISIERUNG DES BENUTZERS AM BEDIENTEIL

Es ist möglich, einen PG-Ausgang über die Benutzerautorisierung zu aktivieren (Eingabe eines Codes oder Verwendung eines RIFD-Chips). Der PG-Ausgang muss so konfiguriert sein, dass er von einem bestimmten Bedienteil aktiviert wird.

2.10.3 FERNBEDIENUNG

Durch Drücken einer zugewiesenen Taste einer Fernbedienung.

2.10.4 EINWÄHLEN

Jede in der Zentrale gespeicherte Telefonnummer (ein Benutzer kann eine Telefonnummer haben) kann einen PG--Ausgang nur durch Einwahl (d.h. ohne Rufannahme) steuern. Das Einwählen besteht darin, die Telefonnummer der im Sicherheitssystem verwendeten SIM-Karte zu wählen und aufzulegen, bevor das System den Anruf entgegennimmt. Standardmäßig beantwortet das System den Anruf nach dem dritten Klingeln (ca. 15 Sekunden).

WARNHINWEIS: Ein PG-Ausgang kann nur dann gesteuert werden, wenn die GSM- oder PSTN-Verbindung mit der Zentrale möglich ist.

2.10.5 SMS-NACHRICHT

Das Versenden einer SMS kann einen bestimmten PG ein- / ausschalten. Ob eine Autorisierung erforderlich ist, hängt von der Systemkonfiguration ab.

Beispiel: **CODE_KONFIGURIERTER TEXT** ("_" Zeichen = Leertaste)

WARNHINWEIS: Ein PG-Ausgang kann nur dann gesteuert werden, wenn die GSM-Verbindung mit der Zentrale möglich ist.

2.10.6 WEBINTERFACE MyJABLOTRON

Durch Anklicken von ON/OFF in der Registerkarte Automatisierung (PG).

2.10.7 SMARTPHONE-APP MyJABLOTRON

Durch Antippen von ON/OFF in der Registerkarte Automatisierung (PG).

3. SPERREN/DEAKTIVIEREN DES SYSTEMS

3.1 BENUTZER SPERREN

Jeder Benutzer kann temporär gesperrt werden (z. B., wenn der Benutzer seine RFID-Karte/Anhänger verloren hat oder sein Zugangscode anderen Personen bekannt wurde). Wenn der Zugang des Benutzers gesperrt ist, wird sein Code oder seine RFID-Karte/Anhänger nicht mehr vom System akzeptiert. Der Benutzer erhält außerdem keine weiteren SMS-Benachrichtigungen oder Sprachnachrichte auf sein Telefon.

Nur der Systemadministrator oder Errichter/Servicetechniker kann Benutzer sperren. Eine Art, Zugangsrechte zu entziehen, ist die Auswahl von Einstellungen / Benutzer / Benutzer / Umgehen/Bypass und anschließend „Ja" auf dem LCD-Bedienteil. Eine weitere Option ist das lokale oder entfernte Sperren eines Benutzers über J-Link durch Anklicken des Benutzers unter der Registerkarte Benutzerübersicht / Benutzer / Benutzer sperren.
Ein gesperrter (deaktivierter) Benutzer wird mit einem roten Kreis markiert, bis die Sperrung aufgehoben wird.

3.2 MELDER DEAKTIVIEREN

Melder können ähnlich wie Benutzer temporär gesperrt-deaktiviert werden. Ein Melder wird dann gesperrt, wenn seine Aktivierung vorübergehend nicht erwünscht ist (z. B. Bewegungsmelder in einem Raum mit einem Haustier oder Deaktivierung von Sirenen). Während die Alarmfunktion des Melders deaktiviert ist, werden Sabotagekontakte weiterhin diagnostiziert und Sabotagealarme und Service-Ereignisse gesendet.

Nur der Systemadministrator oder Errichter kann über Einstellungen / Melder / Umgehen/Bypass und anschließend „Ja" auf dem LCD-Bedienteil einen Melder sperren. Optional ist dies auch in J-Link möglich, indem man unter der Registerkarte Diagnose / Deaktivieren auf den Melder klickt. Ein gesperrter Melder ist mit einem gelben Kreis markiert, bis er nach dem gleichen Verfahren wieder aktiviert wird. Komponente können ebenfalls über die MyJABLOTRON-Smartphone-App zeitweise deaktiviert bzw. blockiert werden.

WARNHINWEIS: Diese Funktion ist vom ausgewählten Systemprofil der Zentrale abhängig. Lassen Sie sich immer bezüglich der gesperrten Melder von Ihrem Errichter beraten. Wenn die Räumlichkeiten von einem Sicherheitsdienst überwacht werden, ist es empfehlenswert, diesen auch zu Rate zu ziehen.

3.3 ZEITSCHALTUHRFUNKTIONEN DEAKTIVIEREN

Um geplante automatisierte Ereignisse im System vorübergehend zu deaktivieren, können die Zeitschaltuhrfunktionen ausgeschaltet werden. Die Deaktivierung eines geplanten Ereignisses (z. B. Unscharfschaltung des Systems aus der Nachtüberwachung um eine bestimmte Zeit) verhindert die Ausführung dieses Ereignisses (z. B. während des Urlaubs).

3. SPERREN/DEAKTIVIEREN DES SYSTEMS

Eine Zeitschaltuhrfunktion kann lokal oder aus der Ferne über J-Link durch Anklicken des Bereichs unter der Registerkarte Zeitschaltuhr / Programmierung deaktivieren deaktiviert werden. Eine deaktivierte Zeitschaltuhrfunktion wird mit einem roten Punkt gekennzeichnet, bis sie mithilfe des gleichen Verfahrens wieder aktiviert wird.

4. BENUTZEREINSTELLUNGEN DES SYSTEMS

4.1 ÄNDERN DES BENUTZERZUGANGSCODES

Nur der Systemadministrator und der Errichter können die Autorisierungscodes ändern. Der Systemadministrator kann die Änderungen über das LCD-Menü auf dem Bedienteil vornehmen. Der Code kann nach der Autorisierung durch die Auswahl von Einstellungen / Benutzer / Benutzer / Code geändert werden. Um einen neuen Code einzugeben, öffnen Sie den Bearbeitungsmodus (der Code beginnt zu blinken), indem Sie Enter drücken, geben Sie den neuen Code ein und bestätigen Sie ihn durch erneutes Drücken von Enter. Nachdem die Änderungen vorgenommen wurden, müssen sie durch die Auswahl von Speichern bestätigt werden, wenn das System Sie mit „Einstellungen speichern?“ dazu auffordert.

Der Systemadministrator kann Änderungen sowohl über das Menü des LCD-Bedienteils als auch über J-Link und die MyJABLOTRON-Smartphone-App vornehmen.

4.2 ÄNDERN, LÖSCHEN UND HINZUFÜGEN EINER RFID-KARTE / EINES -ANHÄNGERS

Nur der Administrator und der Errichter können RFID-Tags oder Karten aus dem LCD-Menü über das Bedienteil hinzufügen, ändern oder löschen. Diese Änderungen werden nach der Autorisierung durch Auswählen von Einstellungen / Benutzer / Benutzer / Zugriffskarte vorgenommen. Eine neue RFID-Karte / ein -Anhänger wird über den Bearbeitungsmodus durch Enter (die Verbindung der Zugriffskarte beginnt zu blinken) eingegeben. Die RFID-Karte / der -Anhänger muss dann an den Leser (vor die Tasten) gehalten werden, alternativ ist die Seriennummer unter einem Strichcode manuell einzugeben. Die RFID-Karte / der -Anhänger wird durch Enter hinzugefügt. Um eine Zugriffskarte zu löschen, geben Sie „0" in das Feld Seriennummer ein. Nachdem die Änderungen abgeschlossen sind, muss diese Änderung über Speichern gespeichert werden, wenn Sie die Zentrale mit „Einstellungen speichern?“ dazu auffordert. Der Systemadministrator und der Errichter können RFID-Karten/-Anhänger über das LCD-Menü des Bedienteils und über J-Link hinzufügen, ändern und löschen.

4.3 ÄNDERN VON BENUTZERNAMEN ODER TELEFONNUMMERN

Nur der Administrator und der Errichter können Telefonnummern hinzufügen, ändern oder löschen oder Namen der Benutzer aus dem LCD-Menü über das Bedienteil ändern. Dies kann nach der Autorisierung durch die Auswahl von Einstellungen / Benutzer / Benutzer / Telefon durchgeführt werden. Der Benutzer muss im Bearbeitungsmodus sein, um Änderungen vornehmen zu können. Dies geschieht durch Drücken von Enter. Wenn die Änderungen vorgenommen wurden, müssen Sie durch erneutes Drücken von Enter bestätigt werden. Zum Löschen einer Telefonnummer geben Sie „0“ im Feld für die Telefonnummer ein. Wenn die Änderungen vollständig sind, müssen Sie durch die Auswahl von Speichern gespeichert werden, wenn das System Sie mit „Einstellungen speichern?“ dazu auffordert.

Der Systemadministrator und der Errichter können über das LCD-Menü des Bedienteils und über J-Link Telefonnummern von Benutzern hinzufügen, ändern oder löschen oder die Namen von Benutzern ändern.

4.4 HINZUFÜGEN / LÖSCHEN VON BENUTZERN

Nur der Systemadministrator oder Errichter kann neue Benutzer zum System hinzufügen (oder löschen). Neue Benutzer können nur uber J-Link oder, im Falle eines Errichter über F-Link zum System hinzugefügt (oder daraus gelöscht) werden.

Die Anzahl der optionalen zusätzlichen Benutzer, ist von den Systemparametern und Voreinstellungen des Errichters abhängig. Bei Fragen kontaktieren Sie bitte Ihren Jablotron Errichter.

Beim Erstellen neuer Benutzer ist es wichtig, ihnen Zugangsberechtigung (Rechte), Bereiche, die sie bedienen dürfen, programmierbare Ausgänge, die sie steuern dürfen, und die erforderliche Autorisierungsart zuzuweisen.

4.5 ERSTELLUNG VON ZEITSCHALTUHRFUNKTIONEN

Es ist möglich, bis zu 10 Kalenderereignisse zu konfigurieren (Unscharfschaltung/Scharfschaltung/Teilscharfschaltung, Steuern oder Blockieren von PG-Ausgängen). In einer einzelnen Funktion können mehrere Aktionen kombiniert werden. Beispielsweise können Sie gleichzeitig ausgewählte Bereiche scharfschalten, einen PG-Ausgang einschalten und einen anderen PG blockieren.

Zeitschaltuhrfunktionen können über J-Link in der Registerkarte Zeitschaltuhr eingestellt werden.

5. EREIGNISVERLAUF

Das Sicherheitssystem speichert alle ausgeführten Vorgänge und Ereignisse (Scharfschaltung, Unscharfschaltung, Alarme, Fehler, an Benutzer und NSL/AES versandte Nachrichten) auf der Mikro-SD-Karte der Zentrale. Jeder Eintrag enthält das Datum, die Uhrzeit (Anfang und Ende) und die Quelle (Ursache / Ursprung) des Ereignisses.

Die verschiedenen Möglichkeiten, den Ereignisverlauf des Systems zu durchsuchen:

5.1 MITHILFE DES LCD-BEDIENTEILS

Der Zugriff auf den Ereignisverlauf mithilfe des Bedienteils erfordert eine Benutzerautorisierung. Sobald der Benutzer autorisiert ist, werden die verfügbaren Optionen (basierend auf Benutzerberechtigungen) durch die Auswahl von Ereignisspeicher angezeigt. Aufzeichnungen können mithilfe der Pfeile angesehen werden.

5.2 MITHILFE VON J-LINK UND EINEM COMPUTER

Der Systemspeicher kann über J-Link durchsucht werden. Ereignisse können in kleinen (ca. 1.200 Ereignissen) oder größeren (ca. 4.000 Ereignissen) Paketen eingesehen werden. Die Ereignisse können gefiltert, für eine leichtere Orientierung farblich markiert oder in eine Datei gespeichert werden.

WARNHINWEIS: J-Link ist nur für das Windows Betriebssystem verfügbar.

5.3 DURCH EINLOGGEN IN MyJABLOTRON (WEB/SMARTPHONE)

Sofern die Anwendung MyJABLOTRON aktiviert wurde, können alle Systemereignisse nach dem Einloggen in der MyJABLOTRON-Web-/Smartphone-Anwendung angesehen werden. Das Konto zeigt den Verlauf in einem Bereich an, der den Zugriffsrechten des Benutzers entspricht.

6. WAS IST MyJABLOTRON?

MyJABLOTRONi ist ein einzigartiger Dienst, der den Online-Zugriff auf JABLOTRON-Systeme ermöglicht. Er ermöglicht Endbenutzern die Überwachung und Steuerung des Systems.

MyJABLOTRON ERMÖGLICHT BENUTZERN:

- Den aktuellen Systemstatus einzusehen.
- Sicherungsbereiche oder seperate Teile davon scharf, teilscharf oder unscharf zu schalten .
- Programmierbare Ausgänge zu steuern.
- Den Ereignisverlauf einzusehen.
- Nachrichte an ausgewählte Benutzer per SMS, Email und PUSH-Benachrichtiungen senden.
- Bilder von Kameraüberwachungsgeräten aufzunehmen und sie in der Bildergalerie oder direkt in den letzten Ereignissen durchzusuchen.
- Die aktuelle Temperatur oder den Energieverbrauch zu überwachen, einschließlich einer Verlaufsübersicht in Form von Diagrammen.
- Und viele weitere nützliche Funktionen.

7. REGELMÄSSIGE WARTUNG

Um eine zuverlässige Funktionsfähigkeit des Systems sicherzustellen, müssen regelmäßig und pünktlich Wartungsarbeiten durchgeführt werden. Die meisten Wartungsarbeiten werden mindestens jährlich im Zuge regelmäßiger Inspektionen durch einen zertifizierten Jablotron Errichter/Installationsfirma durchgeführt.

Die benutzerseitige Wartung beschränkt sich darauf, die einzelnen Geräte sauber zu halten.

Einige Geräte müssen möglicherweise regelmäßig geprüft werden (z. B. Brandmelder). Dies wird in der individuellen Anleitung eines solchen Gerätes beschrieben. Um Details abzusprechen, setzen Sie sich bitte mit Ihrem Errichter in Verbindung.

PARAMETER	JA-100K
Installationstyp	feste Installation
Nennspannung der Zentrale / Frequenz / Sicherung	~ 230 V / 50 Hz, T200 mA fuse 250 V 5 x 20 mm ~ 115 V / 60 Hz, T400 mA fuse 250 V 5 x 20 mm
Betriebsspannungsbereich	~ 195 V ÷ 250 V ~ 110 V ÷ 120 V
Elektrischer Strom / Stromstärke	Max 23 VA / 0.1 A
Sicherheitsklasse	II.
Backup-Batterie	12 V; 2.6 Ah max. (Bleisäurebatterie)
Niedrige Batteriespannung (Störmeldung)	≤ 11 V
Maximale Ladezeit der Batterie	48 ÷ 72 Std.
BUS-Spannung / max. Spannungswelligkeit (rot-schwarz)	12,0 ÷ 13,8 V DC / ± 100 mV
Max. kontinuierlicher Verbrauch von der Zentrale BUS + RJ	400 mA permanent (1000 mA für 5 Minuten)
@ 12 Stunden Backup (2.6 Ah)	LAN OFF: 125 mA – Verbrauch externer Module LAN ON: 85 mA – Verbrauch externer Module
Max. Anzahl der Komponenten	32
Alarmverbindungen	JABLOTRON BUS – dedizierte Kabelverbindung Drahtlose Verbindung (mit Funkmodul JA-111R) – nicht spezifizierte drahtlose Verbindung, JABLOTRON Funkprotokoll
Klassifizierung des Alarmsystems	Sicherheitsgrad 2 / Umgebungsklasse II
@ gemäß der Standards	EN50131-1, EN 50131-3, EN 50131-6, EN 50131-5-3, EN 50131-10, EN 50136-1, EN 50136-2
@ Umgebung	allgemeine Innenräume
@ Betriebstemperatur / Feuchtigkeit	-10 °C to +40 °C, relative Feuchtigkeit 75%, keine Kondensierung
@ Strom	Type A – Primärversorgung mit einer aufgeladenen Backup-Batterie
@ Ereignisverlauf	die ca. 7 Millionen aktuellsten Ereignisse, inkl. Datum und Uhrzeit
@ Systemreaktion auf einen Kommunikationsverlust	Fehler oder Sabotage – gemäß des voreingestellten Profils @ BUS - bis zu 10 Sek. @ drahtlose Kommunikation - innerhalb 2 Std. (Meldung) @ drahtlose Kommunikation - innerhalb 20 Min. Sperrung des Systems
@ Reaktion auf eine ungültige Codeeingabe	Nach der Eingabe 10 falschen Codes wird ein Sabotagealarm ausgelöst, je nach gewähltem Profil werden alle Steuergeräte für 10 Min. gesperrt
@ ATS-Klassifizierung	Unterstützte ATS-Klassen : SP2 – SP 5, DP2 – DP3 SPT: type Z Betriebstyp: Pass-Through Built-in LAN: SP2 – SP5 (with IP protocol) JA-190Y SP2 – SP5 (with IP protocol) JA-190X SP2 (with Contact ID protocol) LAN + JA-190Y DP2 – DP3 (with IP protocol) LAN + JA-190X DP2 (with IP / CID protocol)
@ ATS-Übertragungsprotokolle	JABLO IP, SIA IP, Contact ID, JABLO SMS
@ ATC Schutz gegen Datenaustausch und Datenschutz	JABLOTRON-Protokoll: Geschützte AES Verschlüsselung mit mindestens 128 bit Schlüssellänge ANSI SIA DC-09.2012 Protokoll mit 128 bit AES Verschlüsselung
LAN-Verbindung	Ethernet-Schnittstelle CAT 5 (RJ-45)
Abmessungen (mm)	268 x 225 x 83 (mm)
Gewicht	1450 g
Grundsätzliche Parameter der JA-111R-Module	868.1 MHz, < 25 mW, GFSK < 80 kHz
Funk-Emission	ETSI EN 300 220-2 (the JA-111R Modul)
EMC	EN 50130-4, EN 55032, ETSI EN 301 489-1, ETSI EN 301 489-3
Elektrische Sicherheit	EN 60950-1
Betriebsbedingungen	ERC REC 70-03, ERC DEC (98) 20
Zertifizierungsstelle	TREZOR TEST

JABLOTRON ALARMS a.s. erklärt hiermit, dass die Zentrale JA-100K den grundlegenden Anforderungen und den rele-vanten EU-Vorschriften no.2014/35/EU, 2014/30/EU und 2011/65/EU entspricht.
Die Originalfassung der Konformitätsbe-wertung kann unter **www.jablotron.com** im Abschnitt Downloads eingesehen werden.

Hinweis: Obwohl dieses Produkt keine schädlichen Werkstoffe beinhaltet, empfehlen wir, das Produkt nach dem Ende seines Gebrauchs an den Händler oder Hersteller zurückzusenden.

9. BEGRIFFSGLOSSAR

BUS / kabellose Geräte:
Der wichtigste Knotenpunkt des Sicherheitssystems ist die Zentrale. Sie kann mit allen Geräten auf zwei Arten kommunizieren: Über einen BUS, d.h. Datenkabeln in den bewachten Räumlichkeiten oder Teilen davon; Oder drahtlos per Funkkommunikation. BUS-Geräte werden über die Zentrale mit Strom versorgt. Drahtlose Geräte benötigen Batterien, deren Langlebigkeit von der Intensität der Nutzung abhängt. Einige der drahtlosen Geräte werden über 230V vom Stromnetz versorgt (siehe Anleitung des jeweiligen Gerätes).

RFID-Karte / -Anhänger
Mit der RFID-Karte / -Anhänger kann der Benutzer das System bedienen. Sie wird für die kontaktlose Autorisierung verwendet, indem man einfach die Karte / den Anhänger an den Bedienteilsleser hält. So werden numerische Zugangscodes ersetzt oder ergänzt. Die RFID-Karte kann in einer Brieftasche getragen werden, die zur Autorisierung auf dem Bedienteil platziert werden kann. Der RFID-Anhänger kann einem Schlüsselanhänger beigefügt werden.

Sicherungsbereich
Das Alarmsystem kann in mehrere kleinere, unabhängig voneinander funktionierende Teile unterteilt werden. Diese werden Sicherungsbereiche genannt. Jeder Bereich kann seine zugeordneten Melder, Bedienteile, sowie Sirenen, Benutzer und Telefonnummern haben. Es können bis zu 4 Bereiche pro System vorhanden sein.

Programmierbare Ausgänge (PG)
Das Sicherheitssystem kann zum Ein- / Ausschalten oder Steuern weiterer Elektro- oder Haushaltsgeräte verwendet werden. Dies ist mit programmierbaren Ausgängen, die vom Benutzer gesteuert werden (per SMS, über das Bedienteil usw.) oder je nach Systemstatus (nach Systemstatus, Alarmstatus, Fehler usw.) automatisiert möglich.

Gebäudeautomatisierung
Zusätzlich zu seiner Funktion als Gefahrenmeldeanlage bietet das System JA-100K eine Reihe weiterer Funktionen. Zu den beliebtesten Funktionen gehören: elektrische Türschlösser, automatisierte Lichtschalter mit Bewegungsmeldern und die Fernsteuerung von Geräten (Heizung, Garagentore, Tore, Eintrittsbarrieren etc.).

Überfallalarm (Panikalarm)
Wenn ein Benutzer in Gefahr ist und dringend Hilfe benötigt, kann der Panikalarm ausgelöst werden. Der Panikalarm kann als eine bestimmte Funktionstaste auf dem Bedienteil, ein spezieller Code, eine Panik-Taste oder als eine spezielle Kombination von Tasten auf einer Fernbedienung eingestellt werden. Bei Verbindung zu einer NSL/AES erzeugt die Auslösung des Panikalarms einen sofortigen Einsatz, der nicht telefonisch abgebrochen werden kann.

Notrufserviceleitstelle – NSL, Alarmempfangsstelle - AES
Bei einem Alarmempfänger (Alarmempfangsstelle, AES) handelt es sich um eine durchgehend besetzte Sicherheitsfirma (24/7/365), die sofort auf Informationen reagieren kann, die aus den geschützten Räumlichkeiten eingehen, und mit geeigneten Maßnahmen bzw. nach firmeninternen Regeln reagieren kann.
Hinweis: Für nähere Details der NSL/AES-Services, sprechen Sie Bitte ihren Errichter an.

www.jablotron.com

8 595614 120982

MNX501100